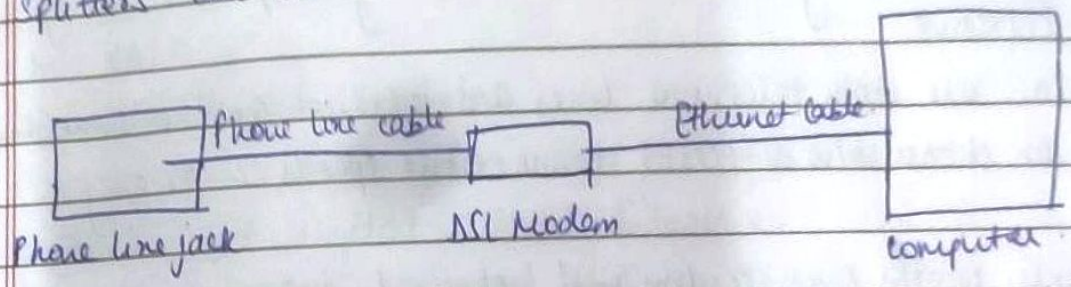
UNIT 5

① DSL (Digital Subscriber Line)

→ Communication medium used to transfer high speed internet over standard copper wire telecommunication line.
→ Offers best cost and connectivity services over other internet access types like broadband.
→ Data transfer and telephone conversation can be done simultaneously
→ Voice signal is transmitted using low frequencies.
→ Digital signals are transmitted through high frequencies.
→ To make sure that phone calls are not interrupted, DSL filters or splitters are used.



Types of DSL:

① SDSL → Symmetric DSL. Provides equal bandwidth for both uploading and downloading. Preferred by small organizations.
② ADSL → Asymmetric DSL. Most users download more data than they upload. 20 Mbps for downloading & 1.5 Mbps for uploading.
③ HDSL → High bit Rate DSL. Used within a corporate site and between the telephone company and its customers. It is a symmetrical line, offers equal bandwidth in both directions.
④ RADSL → Rate Adaptive DSL. The modem is capable of adjusting bandwidth and operating speed to maximize the data transfer. Supports both symmetrical & asymmetrical applications.
⑤ VDSL → Very High Data Rate DSL. A developing DSL technology. Offers more reliable internet experience than basic broadband. Offers much higher data transfer rate.

Features:
→ Widely available.
→ less costly
→ Offers more security.
→ Reliable
→ Offers less speed than broadband service.
→ Provides a limited range.

Benefits:
→ No additional wiring: Makes use of existing telephone wiring.
→ Cost-Effective.
→ Users can use both telephone lines and internet at the same time
→ Users can choose b/w different connections speeds & pricing.

- DSL only works over a limited physical distance.
- The connection is faster for receiving data over the internet than it is for sending data.

② Computer Cables:

→ also known as a cord, plug or connector.
→ transmits power / data b/w devices.
→ Usually covered in plastic by one or more wires.
→ 2 primary types of computer cables:
ⓐ Power Cable: A cable that powers the device is known as power cable. Eg. Molex-style cable and power cord.
ⓑ Data Cable: The cable that creates communication b/w devices. Eg: HDMI.
Used to attach to computer monitor and enable it to display an image or picture.

* Types of Computer Cables:

→ HDMI Cable:
① Transmits audio and video signals with the original quality of images.
② Stands for High Definition Multimedia Interface.
③ Can send crystal clear Images.
④ Used to connect electronic devices.
⑤ Ability to transmit audio and video signals in one go.

→ DVI cable:
① Video display Interface.
② Used to connect video cards and LCD monitor.
③ Stands for Digital Visual Interface.
④ Users can see pictures of high quality without any disturbance.
⑤ Able to transmit video content at high resolutions.

→ VGA cable:
① Stands for Video Graphics Array / Video Graphics Adapter.
② Used to link monitor and CPU to transfer video signals.
③ HD televisions use VGA cable.
④ 256 colors are shown if resolution is lowered to 320X200.
⑤ Offers 640 X 480 resolution color display screens.

→ Ethernet Cable:
① Generally used for a wired network.
② Quality of connection is described by length and durability of the ethernet cable.
③ Can be used to connect devices such as PCs, routers, switches, etc within a LAN.
④ Quality will not be the best if the cable is not durable & too long.

④ It contains eight wires.

→ PS/2 Cable:
① Standard cable contains a round connector and a total of 6 pins.
② It is used to attach mouse and keyboard to the computer system.
③ It stands for Personal System /2.

→ 5mm Audio Cable:
① Used to connect earphones & headphones to the system.
② Also used for connecting portable CD player to any multimedia speaker.

→ USB cables:
① Popular standard cable that enables a computer to interact with peripheral and other devices.
② Stands for Universal Serial Bus.
③ Various devices can be connected through USB cable such as keyboards and mice, music players, flash drives, etc.
④ USB ports are present on the computer system.

→ MIDI:
① Simple procedure to connect two different musical components of different brands.
② Stands for Musical Instrument Digital Interface.
③ Provides more control over the other equipment as it does not transfer the audio signal and transfers the messages in the form of data.

→ Molex:
① Power cable used inside the computer.
② Molex is the name of the company that develops computers and

other related equipment.
⑤ Also referred to as a 4-pin connector or Molex power connector.

→ SATA:
① Also known as Serial ATA.
② Interface used with hard drives.
③ Provides a small, thin cable solution that transfer rates start at 150 Mbps.

→ SCSI:
① Pronounced as "Scuzzy". Stands for Small Computer Systems Interface.
② Has a potential to support eight or sixteen devices.
③ Designed to connect devices to a computer.
④ SCSI connector is either Internal or External.

→ Thunderbolt:
① Used to connect peripheral devices with computer.
② Primarily used with Apple displays and devices.
③ Developed by Apple and Intel.

* Advantages of Computer Cables:

① To connect several devices to computer.
② For performing different operations.
③ Used to transmit the digital and analog signals.
④ Some cables have the ability to transmit electric power.
⑤ Other tasks include listening to music, watching movies, playing games, etc.

DATE / /
PAGE

* DSL

① Uses telephone lines.
② Slowest option
③ Carries less bandwidth.
④ Great option for people in rural areas.
⑤ Better if you only check your mail once in a while

Cable.

① Transmits data over copper TV lines.
② Works faster.
③ Carries more bandwidth.
④ Great option for people who want to choose Satellite Internet.
⑤ Ideal if you stream on multiple devices, download large files, etc.

* Cable

① less bandwidth as compared to fiber.
② Speed slows down during peak use times.
③ Average speed of 10 to 500 Mbps.

Fiber

① Higher bandwidth than a cable.
② Offers speed upto 1 Gbps.
③ Great for competitive online gamers.

* DSL

① DSL is old
② More coverage than fiber
③ Usually runs over pre-existing lines.

Fiber.

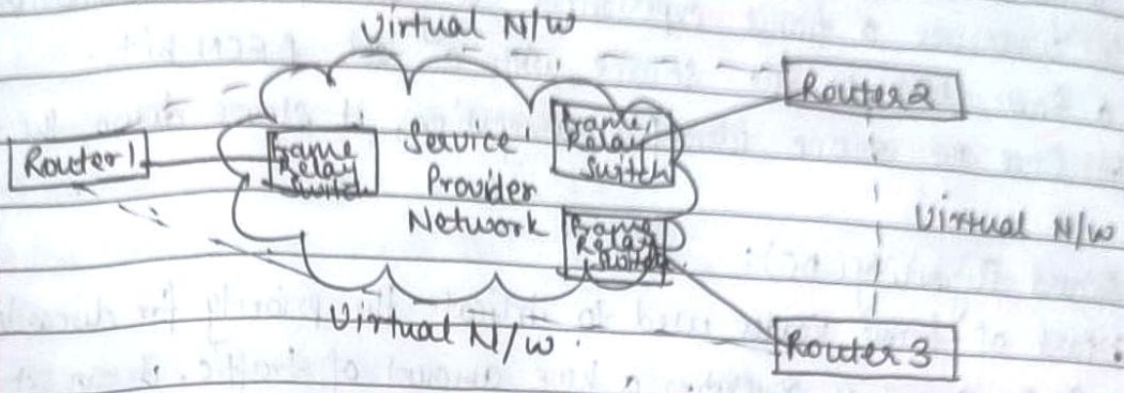
① Fiber is New.
② Less coverage than DSL.
③ Fiber requires professional installation services.

* Frame Relay:

① Packet Switching network protocol.
② Designed to work at data link layer
③ Used to connect LANs and transfer/transmit data across WANs
④ Alternative for a point-to-point network for connecting multiple nodes.
⑤ Allows transmission of different size packets.

2022/11/10

⑤. Dynamic Bandwidth Allocation.
⑥. Provides congestion control Mechanism.
⑦. Does not have error and flow control mechanism.



Frame Relay Network.

Working:
① frame relay switches set up virtual circuits to connect multiple LANs to build a WAN (wide Area Network).
② frame relay transfers data b/w LAN by dividing it in packets.
③ It supports communication with multiple LANs.
④ Routers and service provider N/w connect all the LAN N/ws.
⑤ frame relay switch is responsible for providing services.
⑥ for data transmission, LAN sends the data packets over access link.
⑦ The packet sent is then examined by a frame Relay switch.
⑧ Frame Relay Switch has information about the addresses of LANs connected to the Network.

* frame relay also deals with congestion within a Network. following methods are used to identify the congestion:

①. Forward Explicit Congestion N/w (FECN) - (i) a part of frame header.
(ii) Used to notify destination.
(iii) whenever a frame experiences congestion, the frame relay switch sets the FECN bit that allows destination to identify that packet has experienced congestion.

② Backward Explicit Congestion N/w (BECN):
(i) Part of frame header that is used to notify the source about congestion in the network.
(ii) Whenever a frame experiences congestion, the destination sends a frame back to the source with a set BECN bit.
(iii) Once the source identifies congestion, it slows down the transmission.

③ Discard Eligibility (DE):
(i) Part of frame header used to indicate the priority for discarding frames.
(ii) If the source is generating a huge amount of traffic, it can set DE bits of less significant packets.
(iii) Packets with set DE bits are discarded before the packets with unset DE bits in case of congestion.

* Types:

① Permanent Virtual Circuit (PVC):
→ Permanent connection b/w frame relay nodes that exist for long duration.
→ Always available for communication even when not in use.
→ Static connections. They do not change with time.

② Switched Virtual Circuit (SVC):
→ Temporary connection b/w frame relay nodes.
→ Exists only for the duration for which nodes are communicating with each other.
→ Closed / discarded after communication.
→ Connections are dynamically established as per requirements.

* Advantages → ① High Speed ④ Cost-efficient
② Scalable ⑤ Secured Connection
③ Reduced N/w congestion

* Disadvantages: ① Lacks error control mechanism.
② Delay in Packet transfer.
③ Less Reliable.

* ATM : Automated Teller Machine.
→ facilitates easy transactions without involving a bank employee.
→ Reduction in Bank workload.
→ For transactions using an ATM, it is necessary to have a Credit/Debit card.
→ Successful transactions can be made without filling slips, forms and without standing in long queues.
→ An ATM charges fees for cash withdrawal. This fee is charged by the bank, the ATM operator, or both.
→ To avoid cash withdrawal fees, one should use the ATM of one bank in which they hold their account.

* How to use:
① After visiting the ATM, insert the card in the card slot.
② Select the options from the display.
③ Select the function to be performed. (deposit, balance enquiry, transfer, etc)
④ Select the account type.
⑤ Type the amount & provide ATM pin.
⑥ Collect your cash from cash slot and receipt from the printer.

* ATM cards:
→ Help the user to access their accounts through ATM.
→ Contains the customer account information in the form of magnetic strip.
→ An identification code is encrypted in the magnetic strip & contains all the account details of the customer.
→ ATM cards are available in different forms: Visa, MasterCard, Rupay cards, etc.

* Functions of ATM:

1. Cash withdrawal
2. Cash deposit
3. Cash transfer
4. Balance Enquiry.

* Types of ATMs: (a). Complex: Responsible for multiple functions like displaying account info. & providing transaction History & cash deposit.
(b). Basic: facilitating cash withdrawal along with an available balance statement.

Other types of ATMs are:

→ Brown label ATM: Service provider of ATM owns lease of the machine.
→ Cash Dispensor: ATMs that only dispense cash & are used for balance inquiry & mini statement.
→ Green label: facilitates agricultural transactions.
→ Mobile ATM: Moves from one place to another providing service to customers.
→ Off-site ATM: Machines are installed outside bank premises.
→ On-site ATM: Machines are installed within bank premises.
→ Orange label: facilitates share transactions.
→ Pink label: Specially made for women.
→ Work site: Machines in bank premises but only bank employees can use.
→ Yellow label: Used for online shopping.

* Design of ATM: ①. Screen: To display.
②. Keypad: To type.
③. Card Reader: Interprets the account information.
④: Cash dispensor: Slot that provides cash to the customers.
⑤. Printer: Used to print receipts.

* Advantages of ATM:

1. Convenience: Way more convenient than standing in long queues.
2. Not time bound: Unlike banks, ATMs provide service 24x7 hours a week.
3. Faster transactions: ATM transactions are faster as compared to bank transactions.
4. Easy Accessibility: Accessible in any area.
5. Minimize bank workload: Bank employees can manage people efficiently.
6. Minimize transaction cost: ATM usage has reduced overall cost of transactions.

* Disadvantages of ATM:

1. Cash withdrawal limit: Restrictions on daily cash withdrawal.
2. Transaction charges: Fees is charged for various bank transactions.
3. Increased fraud: Online transactions and ATMs transactions are more susceptible to fraud.
4. Non-Reachable in Remote areas: Due to lack of proper structure and maintenance.

* Point to Point Protocol (PPP)

1. It can share multiple types of packets along with IP packets.
2. Usually provides framing methods to describe frames.
3. It can support the responsibility and management of IP addresses.

* PPP Components:

→ Encapsulating Diagrams: Encapsulates diagrams over point-to-point connection.

PPP frame adds protocol field to primary HDLC frame to identify the type of packet transferred/transported.

→ Implementing LCP: Extensible link-Control Protocols can start, generate and test data-link connections.
→ Implementing NCP: Network connection protocols.

* PPP frame:

1Byte	1Byte	1Byte	2Bytes	Variable, 2 or 4 Bytes
Flag	Address	Control	Protocol	Data	FCS

→ Flag → Indicates starting/ending of a frame.
→ Address → Includes the binary sequence.
→ Control → Contains the binary sequence which calls for user data communication.
→ Protocol → Identify the protocol encapsulated in frame's data field.
→ Data → Containing the datagram of protocol.
→ FCS (Frame check sequence) → for error detection.

* HDLC (High-level Data link Control):

① Each and every frame begins and ends with flag sequence field (F
② Six fields.
③ Ending flag field of one frame can serve as beginning flag field of next frame.

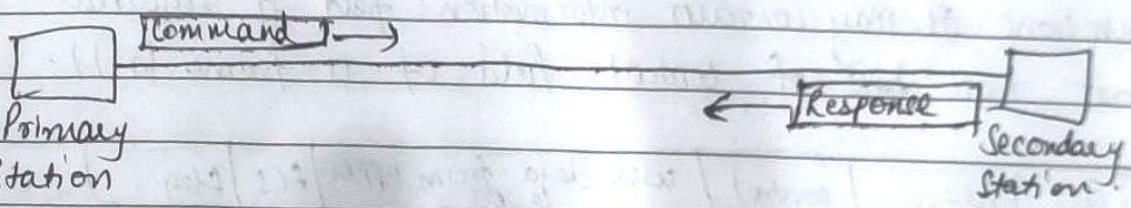
Flag	address	Control	Information	FCS	Flag.
8 bits	8bits	8 or 16 bits	variable	16 or 32 bits	8 bits

→ Group of communication protocols of Data link layer.
→ for transmitting data b/w network points or nodes.

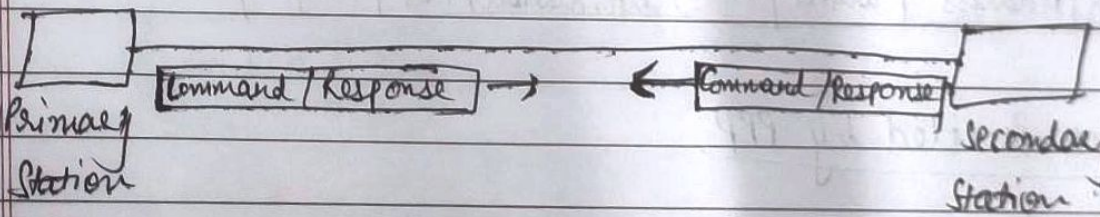
→ Data is organized into frames.
→ Frame is transmitted via network to the destination that verifies its successful arrival.
→ It is bit-oriented protocol.
→ Available for both point to point and multipoint communications.

* Transfer Modes:

① Normal Response Mode: 2 types of stations.
Primary station that sends commands and secondary that can respond to received commands. Used for both point to point & multipoint communications.



② Asynchronous Balanced Mode (ABM): Each station can both send commands and respond to commands. For only point to point communication.



* HDLC frame:

① Flag → Marks the beginning and end of the frame.
② Address → Contains the address of receiver.
③ Control → Contains flow & error control information.
④ Payload → Carries data from N/w layer.
⑤ FCS → Frame check sequence for error detection.

* Types of HDLC frames: Type of frame is determined by the control field.

① I-frame: Information frames carry user data from N/w layer. Include flow & error control information.
The first bit of of control field of I-frame is 0.

② S-frame: Supervisory frames do not contain information field. Used for flow and error control when piggybacking is not required. first two bits of control field of S-frame is 10.

③ U-frame: Un-numbered frame are used for miscellaneous functions. It may contain information field if required. first two bits of control field of U-frame is 11.

I-frame | Flag | Address | control | user data from upper layers | FCS | Flag |

S-frame | Flag | Address | Control | FCS | Flag |

U-frame | Flag | Address | control | Management information | FCS | Flag |

* Services Provided by PPP

① Defines format of frames through which transmission occurs.
② It defines the link establishment Process.
③ It defines data exchange process.
④ It provides encapsulation.
⑤ It defines authentication process blw 2 devices. How the password will be exchanged blw two devices.

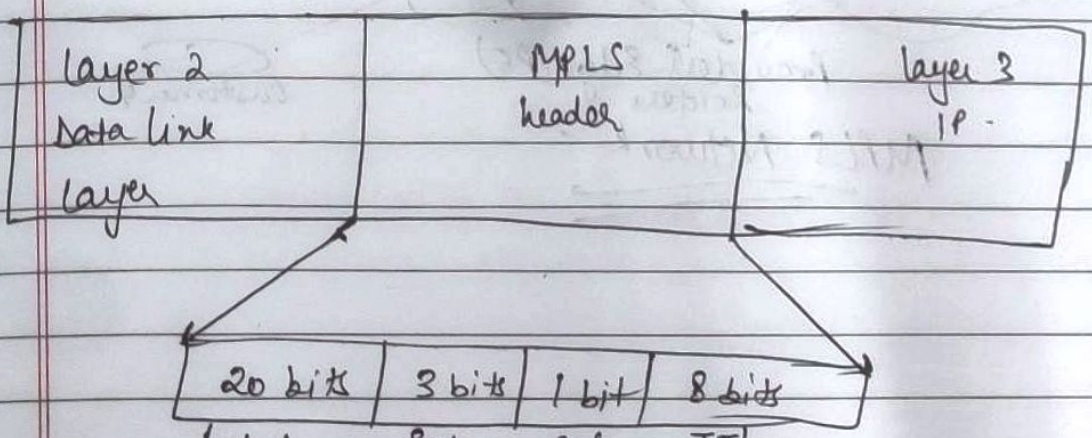
(PPP → byte oriented)

* Services Not Provided by PPP:

① Does not support flow control. Mech
② very simple Error Control Mech.
③ Lacks addressing mech. to handle frames in multipoint configuration.

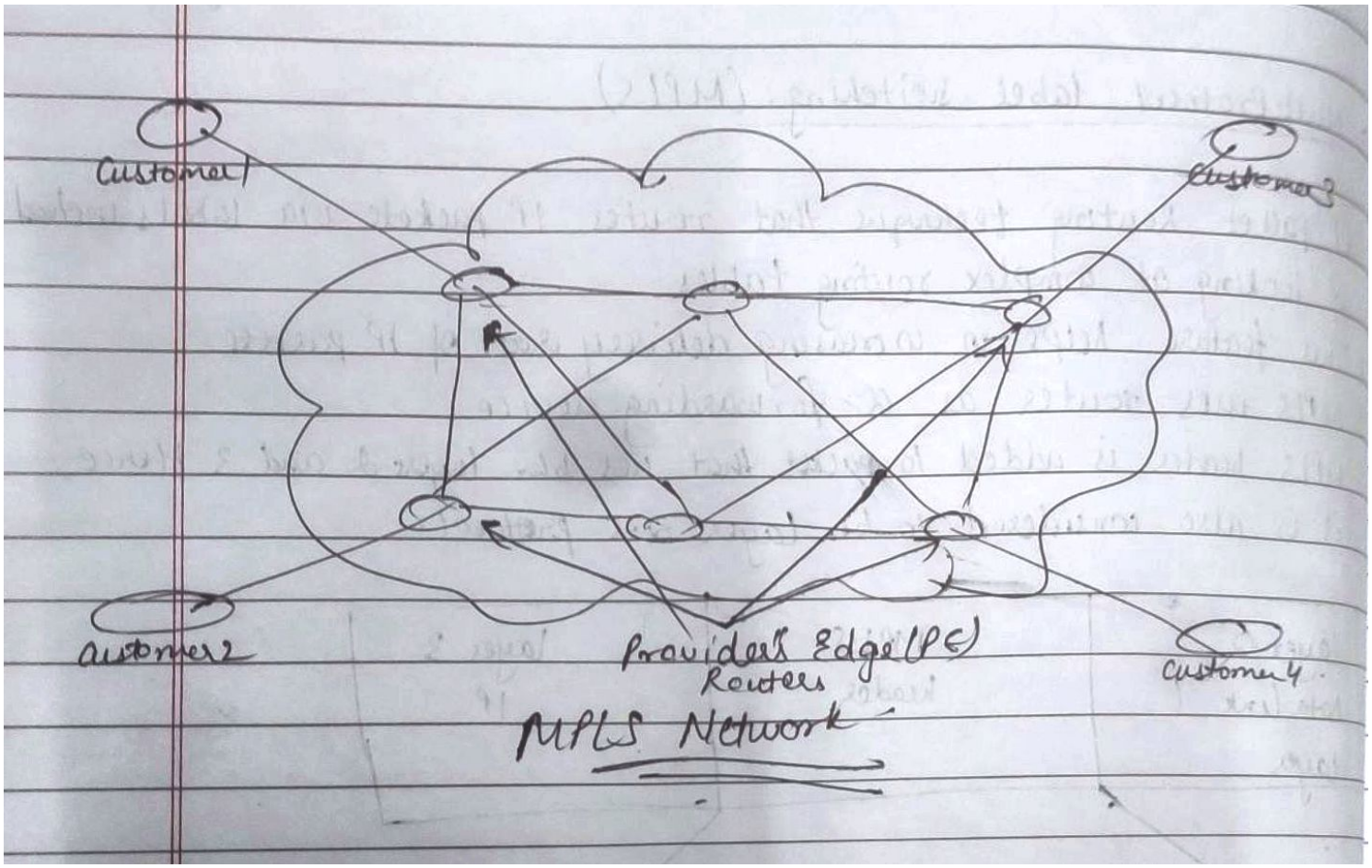
* Multi Protocol label Switching (MPLS)

① IP packet Routing technique that routes IP packets via labels instead of looking at complex routing tables.
② This feature helps in increasing delivery rate of IP packets.
③ MPLS uses router as a forwarding device.
④ MPLS header is added to packet that lies b/w layers 2 and 3. Hence it is also considered to be layer 2.5 protocol.



→ BoS → Bottom of stack: If there is only one label remained in MPLS header, then its value is 1 otherwise 0.
→ Time to live (TTL): value is decreased by one at each hop.

⇒ Push, Pop and Swap: Action of addition, removal and swapping of labels.


Customer1
Customer3
Customer2
Provider's Edge (PE) Routers
Customer4
MPLS Network

Asynchronous Transfer Mode (ATM)

A wide-area network (WAN) technology, **asynchronous transfer mode (ATM)** is a transfer mode for switching and transmission that efficiently and flexibly organizes information into cells; it is asynchronous in the sense that the recurrence of cells depends on the required or instantaneous bit rate. Thus, empty cells do not go by when data is waiting. ATM's powerful flexibility lies in its ability to provide a high-capacity, low-latency switching fabric for all types of information, including data, video, image and voice, that is protocol-, speed- and distance-independent. ATM supports fixed-length cells 53 bytes in length and virtual data circuits between 45 megabits per second (Mbps) and 622 Mbps. Using statistical multiplexing, cells from many different sources are multiplexed onto a single physical circuit. The fixed-length fields in the cell, which include routing information used by the network, ensure that faster processing speeds are enabled using simple hardware circuits. The greatest benefit of ATM is its ability to provide support for a wide range of communications services while providing transport independence from those services.

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.

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.

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.

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.