RGPVNOTES.IN

Program : **B.E**

Subject Name: **Advance Computer Networks**

Subject Code: **CS-8004**

Semester: **8th**

Advance Computer Networks
Subject Notes: UNIT-IV

 # Introduction to Virtual Private Network

VPN stands for Virtual Private Network. It refers to a safe and encrypted network that allows you to use network resources in a remote manner. Using VPN, you can create a safe connection over a less secure network, e.g. internet. It is a secure network as it is completely isolated from rest of the internet. The government, businesses, military can use this network to use network resources securely.

For example, users may use a VPN to connect to their work computer terminal from home and access their email, files, images, etc.

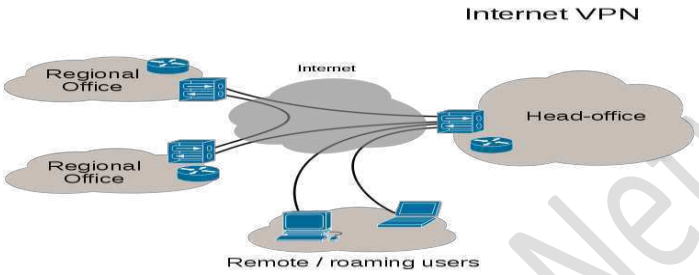


Figure No. 4.1 Virtual Private Network

VPN systems can be classified by:

- The protocols used to tunnel the traffic
- The tunnel's termination point, i.e., customer edge or network-provider edge
- Whether they offer site-to-site or remote-access connectivity
- The levels of security provided
- The OSI layer they present to the connecting network, such as layer 2 circuits or layer 3 network connectivity

Security mechanisms

#Types of VPN (Virtual Private Network)

VPN is of three kinds:

1. Remote access VPN (Virtual Private Network)

• The VPN which allows individual users to establish secure connections with a remote computer network is known as remote-access VPN.

• There is a requirement of two components in a remote-access VPN which are as follows:

I. Network Access Server (NAS)
II. Client software.

• It enables the remote connectivity using any internet access technology.

• Here, the remote user launches the VPN client to create a VPN tunnel.

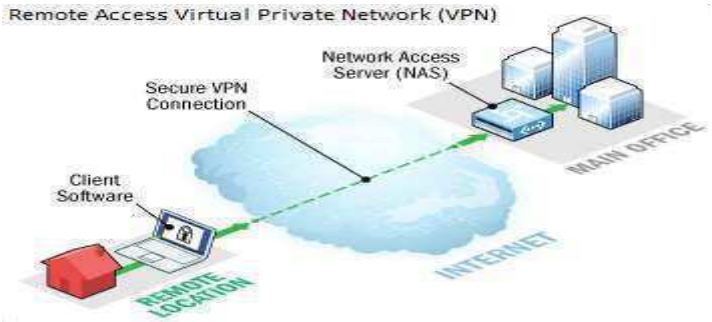


Figure No. 4.2 Remote Access Virtual Private Network

2 Intranet VPN (Virtual Private Network)

- If a company has one or more remote locations and the company wants to join those locations into a single private network, then that company can create an intranet VPN so that they can connect LAN of one site to another one.
- Intranet VPN can link corporate headquarters, remote offices and branch offices over a shared infrastructure using dedicated connections.
- If we use intranet VPN, then it reduces the WAN bandwidth costs.
- The user can also connect new sites easily by using this network.

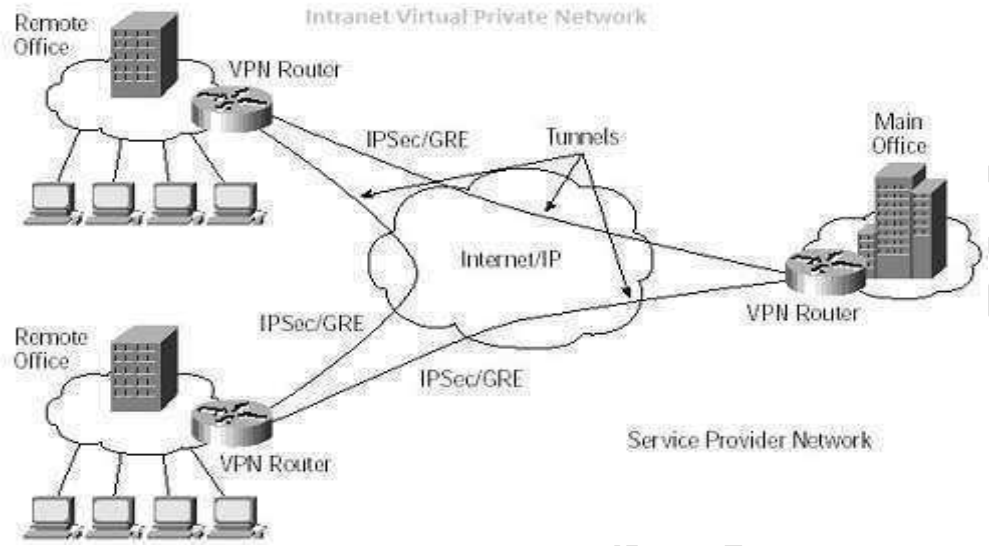


Figure No. 4.3 Intranet Virtual Private Network

3 Extranet VPN (Virtual Private Network)

- If a company has the close relationship with the other company (that company can be their customer, supplier, branch and another partner company), then those companies can build an extranet VPN so that they can connect LAN of one company to the other. It allows all of the companies to work in a shared environment.
- The extranet VPN facilitates e-commerce.

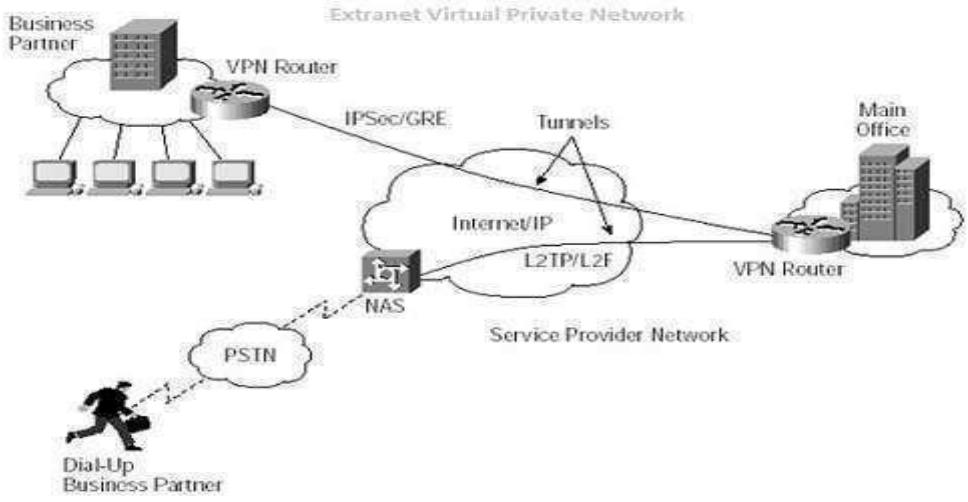


Figure No. 4.4 Extranet VPN (Virtual Private Network)

VPNs typically require remote access to be authenticated and make use of encryption techniques to prevent disclosure of private information.

There are several different VPN protocols that are used to create secure networks. Some of such protocols are given below;

- IP security (IPsec)
- Point to Point Tunneling Protocol (PPTP)
- Layer 2 Tunnelling Protocol (L2TP)
- Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

VPNs provide security through tunneling protocols and security procedures such as encryption. Their security model provides:

Confidentiality such that even if traffic is sniffed, an attacker would only see encrypted data which he/she cannot understand .Allowing sender authentication to prevent unauthorized users from accessing the VPN Message integrity to detect any instances of transmitted messages having been tampered with Secure VPN protocols include the following:

- **IPSec (Internet Protocol Security)** was developed by the Internet Engineering Task Force (IETF), and was initially developed for IPv6, which requires it. This standards-based security protocol is also widely used with IPv4. Layer 2 Tunneling Protocol frequently runs over IPSec. Its design meets most security goals: authentication, integrity, and confidentiality. IPSec functions through encrypting and encapsulating an IP packet inside an IPSec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.
- **Transport Layer Security (SSL/TLS)** can tunnel an entire network's traffic, as it does in the OpenVPN project, or secure an individual connection. A number of vendors provide remote access VPN capabilities through SSL. An SSL VPN can connect from locations where IPsec runs into trouble with Network Address Translation and firewall rules.
- **Datagram Transport Layer Security (DTLS**), is used in Cisco Any Connect VPN, to solve the issues SSL/TLS has with tunneling over UDP.
- **Microsoft Point-to-Point Encryption (MPPE**) works with the Point-to-Point Tunneling Protocol and in several compatible implementations on other platforms.
- Microsoft's **Secure Socket Tunneling Protocol (SSTP),** introduced in Windows Server 2008 and in Windows Vista Service Pack 1. SSTP tunnels Point-to-Point Protocol (PPP) or Layer 2 Tunneling Protocol traffic through an SSL 3.0 channel.
- **MPVPN (Multi Path Virtual Private Network).** Regular Systems Development Company owns the registered trademark "MPVPN".
- **Secure Shell (SSH) VPN** – Open SSH offers VPN tunneling (distinct from port forwarding) to secure remote connections to a network or inter-network links. Open SSH server provides a limited number of concurrent tunnels and the VPN feature itself does not support personal authentication.
- Authentication Tunnel endpoints must authenticate before secure VPN tunnels can be established. User-created remote access VPNs may use passwords, biometrics, two-factor authentication or other cryptographic methods.
- Network-to-network tunnels often use passwords or digital certificates, as they permanently store the key to allow the tunnel to establish automatically and without intervention from the user.

#Benefits of VPN

The main benefit of a VPN is the potential for significant cost savings compared to traditional leased lines or dial up networking. These savings come with a certain (in amount of risk, however, particularly when using the public Internet as the delivery mechanism for VPN data.

The performance of a VPN will be more unpredictable and generally slower than dedicated lines due to public Net traffic. Likewise, many more points of failure can affect a Net-based VPN than in a closed private system. Utilizing any public network for communications naturally raises new security concerns not present when using more controlled environments like point-to-point leased lines.

#Advantages of VPN (Virtual Private Network)

The benefits of VPN are as follows:

• Security: The VPN should protect data while it's travelling on the public network. If intruders attempt to capture data, they should be unable to read or use it.

• Reliability: Employees and remote offices should be able to connect to VPN. The virtual network should provide the same quality of connection for each user even when it is handling the maximum number of simultaneous connections.

• Cost Savings: Its operational cost is less as it transfers the support burden to the service providers.

• It reduces the long-distance telephone charges.

• It cut technical support.

- It eliminates the need for expensive private or leased lines.
- Its management is straightforward.
- Scalability: growth is the flexible, i.e., we can easily add new locations to the VPN.
- It is efficient with broadband technology.
- By using VPN, the equipment cost is also reduced.

#Disadvantages of VPN (Virtual Private Network)

The difficulties of VPN are as follows:

- For VPN network to establish, we require an in-depth understanding of the public network security issues.
- VPNs need to accommodate complicated protocols other than IP.
- There is a shortage of standardization. The product from different vendors may or may not work well together.
- The reliability and performance of an Internet-based private network depend on uncontrollable external factors, which is not under an organization's direct control.

 # Addressing and Routing for VPNs

A VPN connection creates a virtual interface that must be assigned a proper IP address, and routes must be changed or added to ensure that the proper traffic is sent across the secure VPN connection instead of the shared or public transit internetwork.

#Remote Access VPN Connections

For remote access VPN connections, a computer creates a remote access connection to a VPN server. During the connection process the VPN server assigns an IP address for the remote access VPN client and changes the default route on the remote client so that default route traffic is sent over the virtual interface.

#IP Addresses and the Dial-Up VPN Client

For dial-up VPN clients who connect to the Internet before creating a VPN connection with a VPN server on the Internet, two IP addresses are allocated:

- When creating the PPP connection, IPCP negotiation with the ISP NAS assigns a public IP address.
- When creating the VPN connection, IPCP negotiation with the VPN server assigns an intranet IP address. The IP address allocated by the VPN server can be a public IP address or private IP address, depending on whether your organization is implementing public or private addressing on its intranet.
- The IP address allocated to the VPN client must be reachable by hosts on the intranet and vice versa. The VPN server must have appropriate entries in its routing table to reach all the hosts on the intranet and the routers of the intranet must have the appropriate entries in their routing tables to reach the VPN clients.
- The tunneled data sent through the VPN is addressed from the VPN client's VPN server-allocated address to an intranet address. The outer IP header is addressed between the ISP-allocated IP address of the VPN client and the public address of the VPN server. Because the routers on the Internet only process the outer IP header, the Internet routers forward the tunneled data to the VPN server's public IP address.
- An example of dial-up client addressing is shown in Figure 4.5 where the organization uses private addresses on the intranet, and the tunneled data is an IP datagram.

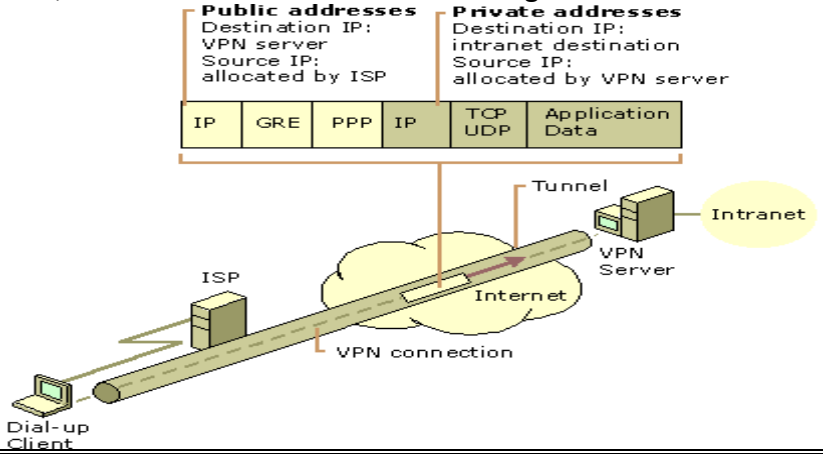


Figure No. 4.5 Default Routes and Dial-Up Clients

When a typical dial-up client dials the ISP, it receives a public IP address from the ISP NAS. A default gateway address is not allocated as part of the IPCP negotiation process. Therefore, in order to reach all Internet addresses, the dial-up client adds a default route to its routing table using the dial-up interface connected to the ISP. As a result, the client can forward the IP datagram's to the ISP NAS from where they are routed to its Internet location.

For dial-up clients with no other TCP/IP interfaces, this is the wanted behaviour. However, this behaviour can cause confusion for dial-up clients that have an existing LAN-based connection to an intranet. In this scenario, a default route already exists pointing to the local intranet router. When the dial-up client creates a connection with their ISP, the original default route remains in the routing table but is changed to have a higher metric. A new default route is added with a lower metric using the ISP connection.

#To prevent the default route from being created

In the properties of the TCP/IP protocol of the dial-up connection object, in the **Advanced TCP/IP Settings** dialog box, click the **General** tab, and then clear the **Use default gateway on remote network** check box.

#Default Routes and VPNs over the Internet

When the dial-up client calls the ISP, it adds a default route using the connection to the ISP as shown in Figure 4.6 .At this point; it can reach all Internet addresses through the router at the ISP NAS.

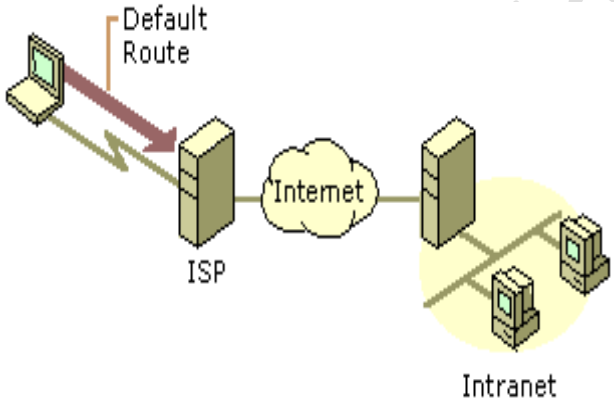


Figure No. 4.6 Default Route Created When Dialling an ISP

When the VPN client creates the VPN connection, another default route and a host route to the IP address of the tunnel server are added, as illustrated in Figure 4.7. The previous default route is saved but now has a higher metric. Adding the new default route means that all Internet locations except the IP address of the tunnel server are not reachable for the duration of the VPN connection.

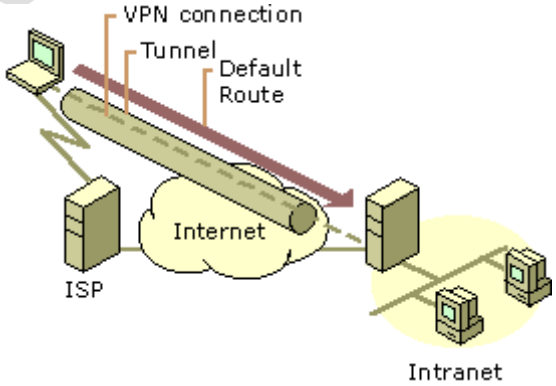


Figure No. 4.7 Default Route Created When Initiating the VPN

Just as in the case of a dial-up client connecting to the Internet, when a dial-up VPN client using voluntary tunneling creates a VPN connection to a private intranet across the Internet, one of the following occurs:

- Internet locations are reachable and intranet locations are not reachable when the VPN connection is not active.
- Intranet locations are reachable and Internet locations are not reachable when the VPN connection is active.

- Based on the type of intranet addressing you use, enable concurrent access to intranet and Internet resources as follows:
- Public Addresses Add static persistent routes for the public network IDs of the intranet using the IP address of the VPN server's virtual interface as the gateway IP address.
- Private Addresses Add static persistent routes for the private network IDs of the intranet using the IP address of the VPN server's virtual interface as the gateway IP address.
- Overlapping or Illegal Addresses If the intranet is using overlapping or illegal addresses (IP network IDs that are not private and have not been registered by Internet Network Information Center [InterNIC] or obtained from an ISP), those IP addresses might be duplicated by public addresses on the Internet. If static persistent routes are added on the VPN client for the overlapping network IDs of the intranet, the locations on the Internet for the overlapping addresses are not reachable.

 # Router-to-Router VPN Connections

For router-to-router VPNs, the routing interface used to forward packets is a demand-dial interface configured as follows:

• On the **General** tab, type the host name or IP address of the VPN server.

• On the **Security** tab, select either **Secure my password and data** or **Custom**. If you select **Custom**, you must also select the appropriate encryption and authentication options.

• On the **Networking** tab, select the appropriate server type and protocols to be routed. If you set the server type as **Automatic**, an L2TP over IPSec connection is attempted first, and then a PPTP connection.

• Under **Interface** credentials, type the user name, password, and domain name used to verify the calling router.

#Asynchronous Transfer Mode (ATM)

Asynchronous Transfer Mode (ATM) also called cell relay (transferring data in cells of a fixed size) that is operates at the data link layer (Layer 2) of OSI Model over fiber or twisted-pair cable, a high-speed switched network technology based on ITU-T Broadband Integrated Services Digital Network (B-ISDN) standard, developed by the telecommunications industry to implement the next generation network. ATM was designed for use in wans such as the public telephone system and corporate data networks, though it has also been applied to create super-fast LANs.

ATM can carry all kinds of traffic: voice, video and data simultaneously at speeds up to 155 megabits per second. It Convert voice, video data to packets and passing large packet data through the same medium. ATM is differing from TCP/IP because it use fixed channel routing protocol routes between two end points. A real-time low-latency application such as VoIP and video takes precedence on an ATM network.

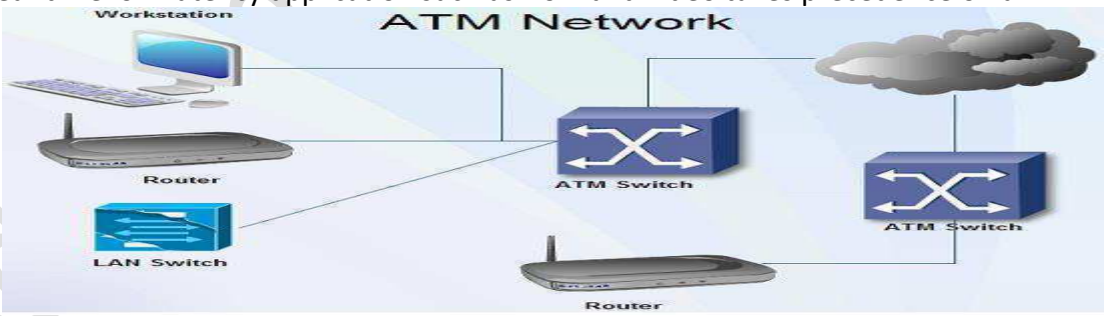
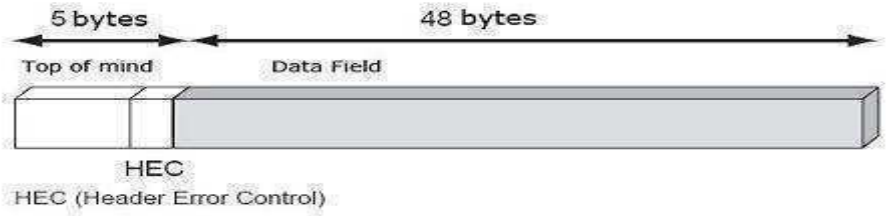


Figure No. 4.8 Asynchronous Transfer Mode (ATM)

ATM is a dedicated connection-oriented switching technology, in which switches create a virtual connection or virtual circuit between the sender and receiver of a call that permanent or switched for the duration of the call. It is a small-packet switched system or similar to circuit-switched network, which breaks down messages into very small, fixed length packets called cells generally organizes digital data into 53 bytes in length (48 bytes of data plus a 5-byte header). ATM frame structure



ATM Frame Structure

Figure No. 4.9 ATM frame structure

An ATM header can have User-Network Interface (UNI) and Network-Node Interface (NNI) two formats.
• User-Network Interface (UNI) used for communication between end systems.
• Network-Node Interface (NNI) used for communication between switches.

#Types of connections in ATM

Two type of connections are supported by ATM (Asynchronous Transfer Mode)

Point-to-point connections: It connects either unidirectional or bi-directional two end-systems.

Point-to-multipoint connections: It connects one unidirectional ATM to number of destination ATM.

- It is different in packet sizes from Ethernet data or frames.
- ATM is a core protocol for SONET that is the backbone of ISDN. The advantage conferred by such small cells is that they can be switched entirely in hardware, using custom chips, which makes ATM switches very fast (and potentially very cheap).
- The asynchronous part of the name refers to the fact that although ATM transmits a continuous stream of cells over a physical medium using digital signal technology, some cells may be left empty if no data is ready for them so that precise timings are not relevant.
- Every cell is encoding data with asynchronous time-division multiplexing (TDM) and it queued before being multiplexed over the transmission path.
- Every cell are encodes data and processed within their time slot allocated to it. When cell time slot allocated is finished, the next cell starts same procedure. That's why it's called asynchronous time-division multiplexing (TDM);
- This is ATM's greatest strength, as it enables flexible management of the quality of service (qos) so; an operator can offer different guaranteed service levels (at different prices) to different customers even over the same line. This ability will enable companies to rent virtual private networks based on ATM that behave like private leased lines but in reality share lines with other users. Available ATM service: Generally four data bit rates are available for ATM services: constant bit rate (CBR), variable bit rate (VBR), available bit rate (ABR) and unspecified bit rate (UBR).

#Benefits of ATM Networks are

1. It provides the dynamic bandwidth that is particularly suited for bursty traffic.
2. Since all data are encoded into identical cells, data transmission is simple, uniform and predictable.
3. Uniform packet size ensures that mixed traffic is handled efficiently.
4. Small sized header reduces packet overload, thus ensuring effective bandwidth usage.
5. ATM networks are scalable both in size and speed.

#ATM reference model comprises of three layers

1. **Physical Layer:** This layer corresponds to physical layer of OSI model. At this layer, the cells are converted into bit streams and transmitted over the physical medium. This layer has two sub layers: PMD sub layer (Physical Medium Dependent) and TC (Transmission Convergence) sub layer.
2. **ATM Layer:** This layer is comparable to data link layer of OSI model. It accepts the 48 byte segments from the upper layer, adds a 5 byte header to each segment and converts into 53 byte cells. This layer is responsible for routing of each cell, traffic management, multiplexing and switching.
3. **ATM Adaptation Layer (AAL):** This layer corresponds to network layer of OSI model. It provides facilities to the existing packet switched networks to connect to ATM network and use its services. It accepts the data and converts them into fixed sized segments. The transmissions can be of fixed or variable data rate. This layer has two sub layers: Convergence sub layer and Segmentation and Reassembly sub layer.

4. **ATM endpoints:** It contains ATM network interface adaptor. Examples of endpoints are workstations, routers, CODECs, LAN switches, etc.
5. **ATM switch:** It transmits cells through the ATM networks. It accepts the incoming cells from ATM endpoints (UNI) or another switch (NNI), updates cell header and retransmits cell towards destination.

#Architecture of ATM

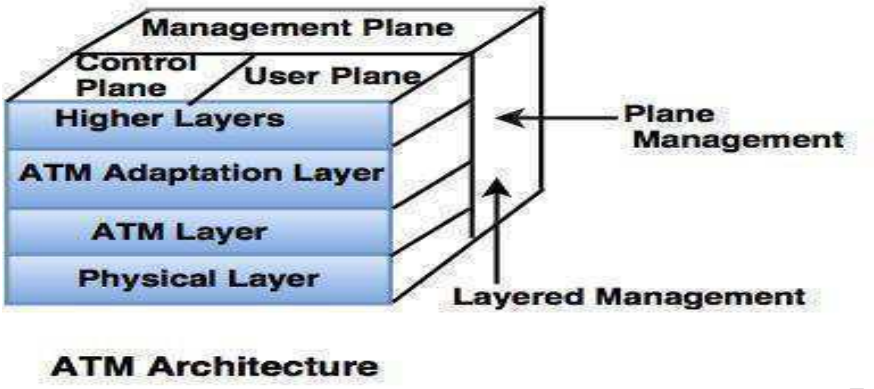


Figure No. 4.10 Architecture of ATM

1. Physical layer

- Physical layer is a point-to-point transfer mechanism at the top of hardware (it may be wire also).
- Physical layer adds its own information to each cell which is transmitted for link management.

Physical layer performs four functions:

i) Physical layer converts bits into cells.
ii) It transmits and receives the bits on physical medium.
Iii) Tracks the cell boundaries.
iv) Packaging of cell into frames.
ATM layer is common to all services which can have the packet transfer capabilities.

2. ATM layer

- ATM layer provides the routing information to the data cells.
- ATM interfaces with the AAL and the Physical layer.
- Functions of ATM layer are under the network management, signalling and OAM protocol.

3. ATM Adaptation Layer

- AAL provides the flexibility of a single communication process to carry the multiple types of traffic such as data, voice, video and multimedia.
- **AAL** is divided into two major parts.
- Upper part of the AAL is called as the **convergence sub layer.** Its task is to provide the interface to the application. The lower part of the AAL is called as the segmentation and reassembly (SAR) sub layer. It can add headers and trailers to the data units given to it by the convergence sub layer to form cell payloads.

#ATM Bit Rates

ATM supports four different types of bit rate:

1. Constant bit rate (CBR)

- CBR traffic is derived from the source, where the information is transmitted at a constant rate. Example: Telephonic speech without silencer.

2. Variable Bit Rate (VBR)

- Variable traffic is derived from a variable source. Example: Compressed voice or video with silence suppression.

3. Available Bit Rate (VBR)

- When a carrier has allocated the necessary bandwidth on the links to carry CBR traffic and minimum VBR is guaranteed. The ABR is the mechanism to share the remaining bandwidth fairly between the links.

4. Unspecified Bit Rate (UBR)

- In **UBR,** there is no guarantee about the bandwidth traffic delay and loss. The control of flow in UBR can be provided from the end device.
- The protocol which performs the operation of braking frames into the cells is known as **ATM Adaptation Layer (AAL).**
- Cells carrying speech and video must be received in the order they were sent. This is known as preserving data integrity and it is a function of ATM layer.
- Any link which preserves the order of data entering and leaving is known as **channel.**
- In ATM protocols, an end-to end connection is established before traffic and starts to flow. Then, the traffic follows the same path through the network to achieve a true quality of service.
- The connection-less services are implemented with the help of **AAL.**

#ATM Equipments:

Two main types of equipment exist on ATM networks –

- ATM switches
- ATM endpoints.

An ATM switch handles cell-switching functions across an ATM network. This includes accepting incoming cells from other ATM switches or endpoints, modifying cell header information as necessary, and then sending cells on to the next switch or end device. An ATM endpoint is a network device equipped with an ATM network interface card, such as a router, computer, LAN switch, and so forth. Cisco router models in the 5500 series are commonly equipped with ATM expansion cards for the purpose of connecting to an ATM backbone.

Special terms are used to describe the connection points between ATM equipment. –

User Network Interface (UNI) and Network Node Interface (NNI).

UNI represents a connection between an endpoint such as an ATM-enabled PC and an ATM switch. NNI is the term used to describe connections between ATM switches. ATM equipment and connection points.

#ATM Applications:

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

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in