# Unit 8
# Wide Area Networks

## Introduction

A wide area network (WAN) is a **computer network** that covers a large geographical area comprising a region, a country, a continent or even the whole world. WAN includes the technologies to transmit data, image, audio and video information over long distances and among different **LANs** and **MANs**. WANs are often used by large organizations, business and government entities to facilitate the exchange of data and information between their various locations.

The **features** of **WANs** are:

i. WANs have a large capacity, connecting a large number of computers over a large area, and are inherently scalable.
ii. They facilitate the sharing of regional resources.
iii. WAN use devices such as routers and switches to direct data packets between different networks and ensure they reach intended destinations.
iv. They provide uplinks for connecting LANs and MANs to the Internet.
v. Communication links are provided by public carriers like telephone networks, network providers, cable systems, satellites etc.
vi. Typically, they have low data transfer rate and high propagation delay, i.e.they have low communication speed.
vii. They generally have a higher bit error rate.

**Applications** of WANs:

1. **Enterprise Connectivity:** WANs are essential for connecting branch offices, enabling seamless communication and collaboration
2. **Internet Access:** Internet Service Provider (ISPs) uses WANs to provide internet access to customers over vast geographical areas.
3. **Cloud Computing:** WANs facilitate access to cloud based services and resources, allowing business to store data and run applications in remote data centers.
4. **Telecommunication:** Telecommunication companies use WANs to provide various services, including voice calls, video conferencing, and internet connectivity.

## Dedicated-Circuit Networks

A dedicated circuit network is a separate point to point data- communication route between communicating systems. The circuit may be either **physical** or **logical.** The **physical** one is just a cable used to create permanent link between two devices. **Logically** dedicated circuits exist as a virtual part of switching networks such as the Internet, frame Relay, and ATM Networks.

Dedicated-circuit networks are sometimes called **private line services.** Dedicated- circuit remain essentials for business organizations that require reliable, high performance and high connections between their various locations.

### Advantages

1. **Reliability:** Dedicated-circuit networks offer high reliability as the connection is dedicated solely to the organizations using it, minimizing the chances of congestion and network failures.

2. **Predictable Performance:** The fixed bandwidth ensures predictable and stable network performance, allowing business to plan their operations effectively.
3. **Security:** Because these lines are private and leased specifically for the organization, the data transmitted over dedicated circuit networks is generally more secure than data sent over public networks.

**Disadvantages**

1. **Cost:** Leased lines are expensive, especially for high bandwidth requirements, making them less cost effective compared to other WAN technologies like VPN over the internet.
2. **Scalability:** It can be challenging and costly to scale the bandwidth of dedicated-circuit networks, especially if substantial increases in capacity are needed.

**Basic Architecture**

The basic architecture of dedicated circuit networks involves the use of leased lines to establish a direct private and constant connection between two or more points. With a dedicated-circuit network, the circuits are leased from common carriers. All connections are point to point, from one building in one city to another building in the same or a different city. The carrier installs the circuit connections at the two end points of the circuit and makes the connection between them.

The dedicated circuit can be **physical or logical**. The physical one is just a cable to create permanent link between two devices. The logical circuit exists as a virtual part of switching networks such as the internet, ATM networks etc.

Dedicated circuit is used by only dedicated user, it offer a high level of connection stability as the bandwidth is dedicated and high level of performance. However the connection is not supposed to be publicly shared, the costs for its development can be high.

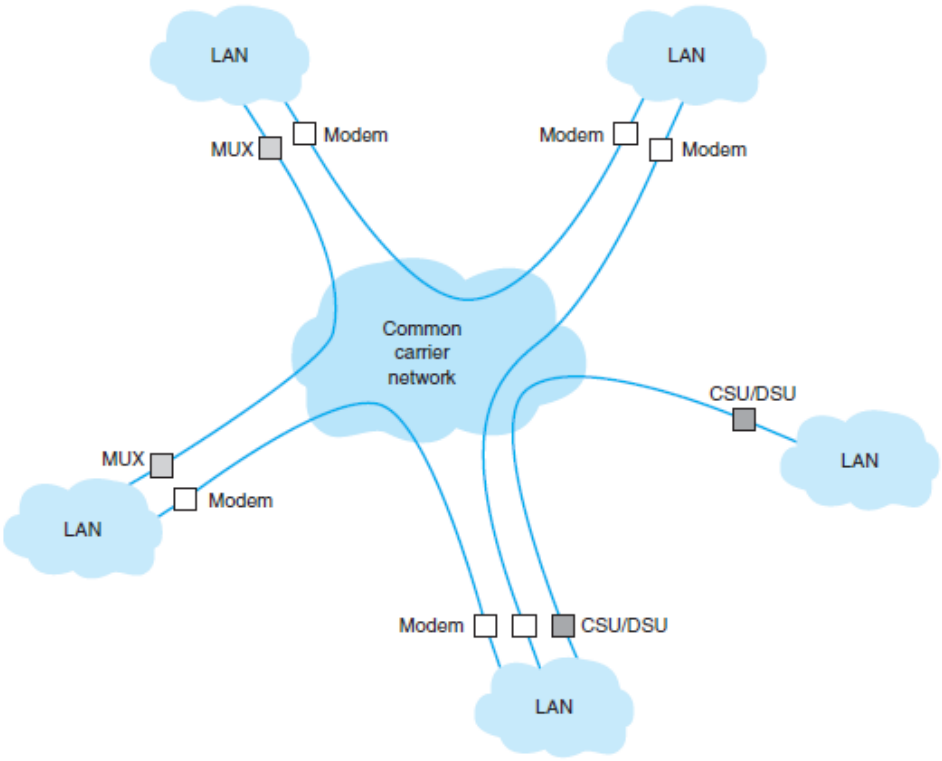


**Fig: Dedicated Circuit Service.**
**CSU= Channel Service Unit, DSU= Data Service Unit, MUX = Multiplexer**

There are three basic architectures used in dedicated-circuit networks: **ring, star, and mesh**. In practice, most networks use a combination of architectures.

**Ring Architecture**

**Ring architecture** connects all computers in a closed loop with each computer linked to the next. The circuits are full-duplex or half-duplex Circuits. Computers in the ring may send data in one direction or the other, depending on which direction is the shortest to the destination.

One **disadvantage** of the ring topology is that messages can take a long time to travel from the sender to the receiver. Messages usually travel through several computers and circuits before they reach their destination, so traffic delays can build up very quickly if one circuit or computer becomes overloaded. A long delay in any one circuit or computer can have significant impacts on the entire network.

In general, the failure of any one circuit or computer in a ring network means that the network can continue to function. Messages are simply routed away from the failed circuit or computer in the opposite direction around the ring. However, if the network is operating close to its capacity, this will dramatically increase transmission times because the traffic on the remaining part of the network may come close to doubling (because all traffic originally routed in the direction of the failed link will now be routed in the opposite direction through the longest way around the ring).

**Star Architecture**

A **star architecture** connects all computers to one central computer that routes messages to the appropriate computer. The star topology is easy to manage because the central computer receives and routes all messages in the network. It can also be faster than the ring network because any message needs to travel through at most two circuits to reach its destination, whereas messages may have to travel through far more circuits in the ring network. However, the star topology is the most susceptible to traffic problems because the central computer must process all messages on the network. The central computer must have sufficient capacity to handle traffic peaks, or it may become overloaded and network performance will suffer. In general, the failure of any one circuit or computer affects only the one computer on that circuit. However, if the central computer fails, the entire network fails. It is critical that the central computer be extremely reliable.

**Mesh Architecture**

In full-**mesh architecture,** every computer is connected to every other computer Full-mesh networks are seldom used because of the extremely high cost. **Partial-mesh architecture** (usually called just **mesh architecture**), in which many, but not all, computers are connected, is far more common. Most WANs use partial-mesh topologies.

The effects of the loss of computers or circuits in a mesh network depend entirely on the circuits available in the network. If there are many possible routes through the network, the loss of one or even several circuits or computers may have few effects beyond the specific computers involved. However, if there are only a few circuits in the network, the loss of even one circuit or computer may seriously impair the network.

In general, mesh networks combine the performance benefits of both ring networks and star networks. Mesh networks usually provide relatively short routes through the network (compared with ring networks) and provide many possible routes through the network to prevent any one circuit or computer from becoming overloaded when there is a lot of traffic (compared with star networks in which all traffic goes through one computer).

The drawback is that mesh networks use decentralized routing so that each computer in the network performs its own routing. This requires more processing by each computer in the network than in star or ring networks.

**T-Carrier Services**

T- Carrier services are a type of dedicated circuit network technology that provides high-quality digital transmission over leased lines. **T carrier circuits** are the most commonly used form of dedicated-circuit services in North America today. Costs are a fixed amount per month, regardless of how much or how little traffic flows through the circuit. There are several types of T carrier circuits among which T1 and T3 are in common use today.

A **T1 circuit** (also called a *DS1 circuit*) provides a data rate of 1.544 Mbps. T1 circuits can be used to transmit data but often are used to transmit both data and voice. In this case, inverse TDM provides 24 64-Kbps circuits.2 Digitized voice using PCM requires a 64-Kbps circuit (see Chapter 3), so a T1 circuit enables 24 simultaneous voice channels. Most common carriers make extensive use of PCM internally and transmit most of their voice telephone calls in digital format using PCM, so you will see many digital services offering combinations of the standard PCM 64-Kbps circuit. A **T2 circuit** transmits data at a rate of 6.312 Mbps.

A **T3 circuit** allows transmission at a rate of 44.736 Mbps although most articles refer to this rate as 45 megabits per second. This is equal to the capacity of 28 T1 circuits. T3 circuits are becoming popular as the transmission medium for corporate MANs and WANs because of their higher data rates. Although T2 and T4 circuits are defined standards, they are not commercially available and therefore we don't discuss them here.

**Fractional T1,** sometimes called **FT1,** offers portions of a 1.544-Mbps T1 circuit for a fraction of its full cost. Many (but not all) common carriers offer sets of 64 Kbps DS-0 channels as FT1 circuits. The most common FT1 services provide 128 Kbps, 256 Kbps, 384 Kbps, 512 Kbps, and 768 Kbps.

| T Carrier Designation | DS Designation | Speed |
|---|---|---|
| FT1 | DS0 | 64 Kbps |
| T1 | DS1 | 1.544 Mbps |
| T2 | DS2 | 6.312 Mbps |
| T3 | DS3 | 44.376 Mbps |
| T4 | DS4 | 274.176 Mbps |

**Fig: T Carrier Services**

**SONET Services**

The **Synchronous Optical Network (SONET)** is the American standard (ANSI) for high-speed dedicated-circuit services. It is a standardized optical fiber network technology used in telecommunications network which provides high-speed, reliable and scalable data transmission over fiber optics cable. SONET networks are synchronous, which ensures synchronization for high speed data transmission.

SONET transmission speeds begin at the OC-1 level (optical carrier level 1) of 51.84 Mbps. Each succeeding rate in the SONET fiber hierarchy is defined as a multiple of OC-1, with SONET data rates defined as high as 160 Gbps. Figure below presents the commonly used SONET and SDH services. Each level above OC-1 is created by an inverse multiplexer.

Notice that the slowest SONET transmission rate (OC-1) of 51.84 Mbps is slightly faster than the T3 rate of 44.376 Mbps.

| SONET Designation | SDH Designation | Speed |
|---|---|---|
| OC-1 | | 51.84 Mbps |
| OC-3 | STM-1 | 155.52 Mbps |
| OC-12 | STM-4 | 622.08 Mbps |
| OC-24 | STM-8 | 1.244 Gbps |
| OC-48 | STM-16 | 2.488 Gbps |
| OC-192 | STM-24 | 9.953 Gbps |
| OC-768 | STM-256 | 39.813 Gbps |
| OC-3072 | STM-1024 | 159.25 Gbps |

**Fig: SONET**

**SONET Services and Benefits**

1. **High Data Rate:** SONET service offer high-speed data transmission, making them suitable for application which requires large bandwidth such as data centers, video streaming.
2. **Reliability:** SONET networks are highly reliable. It provides fault detection and restoration capabilities which ensures rapid recovery in case of network failures.
3. **Scalability:** SONET networks are scalable, allowing network operators to increase bandwidth easily by adding additional SONET modules.
4. **Support for Various Traffic:** SONET supports various types of traffic, including voice, data, video, making it versatile for different communication needs.

**Packet-Switched Networks**

It is a switching technique in which message are broken up into small packet before they are sent. Each packet is transmitted individually across the n/w. The packet may even follow different routes to destination. Each packet has information about its identity in its header to route the packet to its destination. At the destination the packet are reassembled into original message.

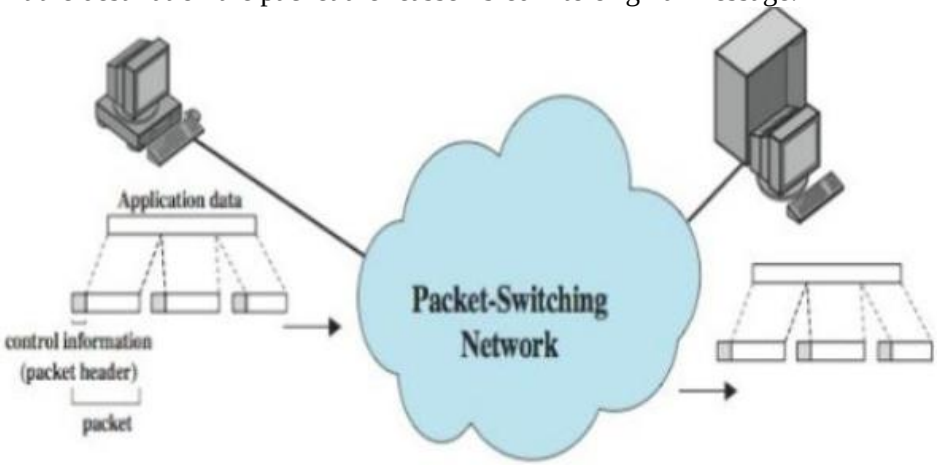


**Fig: Packet Switched Services**

**Benefits**

1. Packets are short. So, the communication links between the nodes are only allocated to transfer a single message for short period of time. Longer message requires a series of packet to be sent but don't required link to be dedicated between transmissions of each packet. The packet belonging to other message can be sent between the packets of message being sent**. This gives proper sharing of resource.**
2. Link efficiency is another advantage. It is possible due to pipe-lining feature of packet switching. The simultaneous uses of communication link represent a gain of efficiency.
3. Data rate conversion: Two stations of different data rates can be exchange packet.
4. Packets are accepted even when n/w is busy.
5. Priorities may be used.

## Basic Architecture

**Packet Switched Network (PSN)** is a kind of computer network that sends data in the form of small packets. A packet-switched is also a connectionless network as it does not create endless connection between source and destination points.

The user's connection into the network is a **packet assembly/disassembly device (PAD),** which can be owned and operated by the customer or by the common carrier. The PAD converts the sender's data into the network layer and data link layer packets used by the packet network and send them through the packet-switched network. At the other end, another PAD reassembles the packets back into the network layer and data link layer protocols expected by the destination and delivers it to the appropriate computer.

One of the key **advantages** of packet-switched services is that different locations can have different connection speeds into the common carrier cloud. The PAD compensates for differences in transmission speed between sender and receiver; for example, the circuit at the sender might be 1.5 Mbps whereas the receiver only has a 64-Kbps circuit.
In contrast, a dial-up circuit or a dedicated circuit must have the same speed at both the sender and receiver.

Packet switching is popular because most data communications consist of short bursts of data with intervening spaces that usually last longer than the actual burst of data. Packet switching takes advantage of this characteristic by interleaving bursts of data from many users to maximize use of the shared communication network. Figure below shows a packet-switching connection between six different cities.
The connection between the different locations in the packet network is called **Permanent Virtual Circuit (PVC)** which means they are defined for frequent and consistent use by network. They do not change unless the network manager changes the network. Some common carriers also permit the use of **switched virtual circuits (SVCs)** although this is not common. Changing PVCs is done using software, but common carriers usually charge each time a PVC is established or removed.

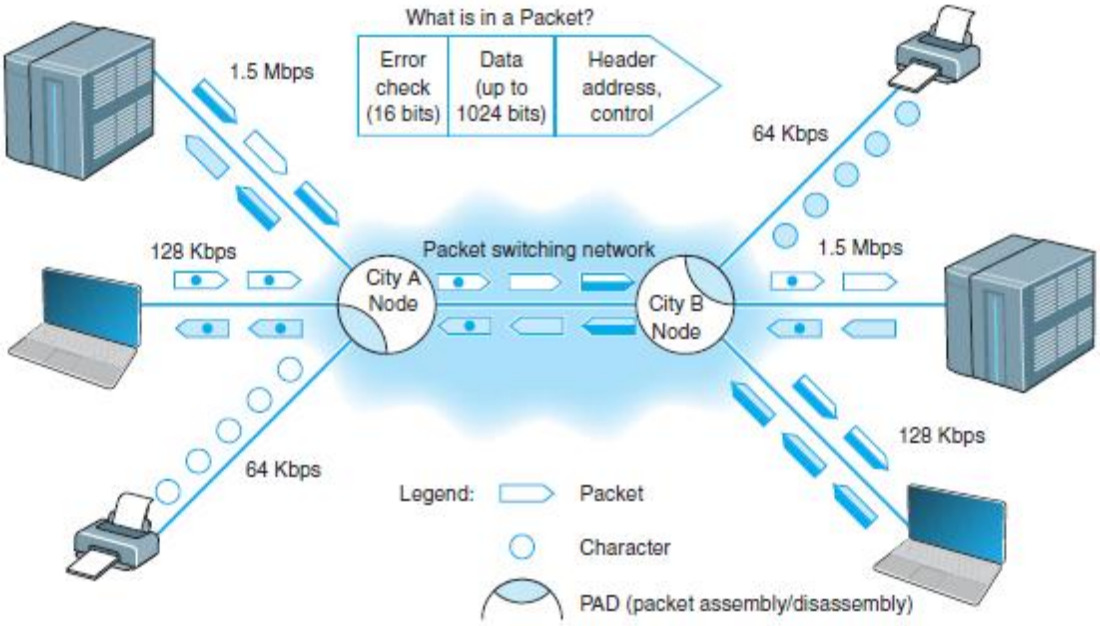


**Fig : Packet Switching Concepts**

**Types of packet Switching**

i. **Virtual circuit packet switching network**
ii. **Datagram packet switching network**

**i. Virtual circuit packet switching network**

A preplanned route is established between the intermediate routes for the packet passed during the session between the end nodes. In each intermediate node, an entry is registered in a table to indicate the route of the connection that has been set up. The packets passed through this route have a short header with a **Virtual Circuit Identifier (VCI)** instead of a destination address. Each intermediates nodes, passes the packet according to the information that was stored in the table in the set-up phase and according to the packets header content.

This is slower than circuit switching as different virtual circuit may compete over the same resources. Similar to circuit switching, if an intermediate node fails, all virtual circuit that passes through the circuit fails.

Virtual circuit packet switching is the switching techniques which merge datagram packet switching and circuit switching to extract both of their advantage.

It is a variation of datagram packet switching where packets flow on so called logical circuit for which no physical resources like frequency or time slots are allocated. As in circuit switches n/w, there are set up and disconnect phase, in addition to data transfer phase. Resources can be allocated during set-up phase as a circuit switch n/w or un-demand as a datagram n/w. As a datagram network, data are packetized and all packet flow in the same path established during connection as in a circuit switched n/w. A virtual circuit is defined by sequence of mapping between a link taken by packets and circuit identifier packets carried on this link. Routing is performed at circuit establishment time to keep packet forwarding fast.

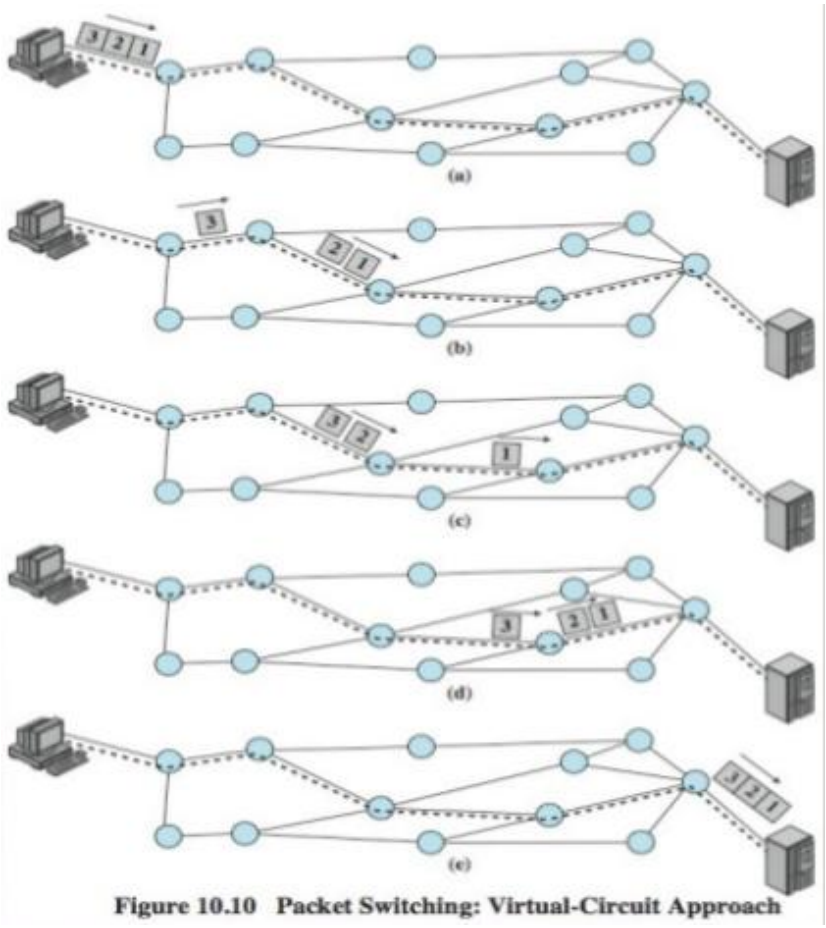

Figure 10.10 Packet Switching: Virtual-Circuit Approach

**ii. Datagram Packet Switching Network**

Packets are broken down into smaller size called datagram. Each packet is treated independently. The full information about the destination of packet is contained in its header. Intermediate nodes examine the header of the packet and decide the next hop of the packet. While deciding the next hop, considerations are made to find shortest path to destination and to find the free node to reach the destination.

No pre-established route is used in datagram packet switching n/w. Packet can take any practical route and may arrive out of order in the destination i.e. in different order as they were sent from the source. They are sorted and rearranged at the destination to get the exact order. Each packet must carry the address of destination host and use the destination address to make a forward decision.

In datagram circuit if a router goes down only those user whose packet were queued up in a router at that time will suffer. The loss or fault on communication line can be easily compensated in a datagram circuit. Datagram allow the router to balance the traffic throughout the n/w, since router can be changed through a connection.

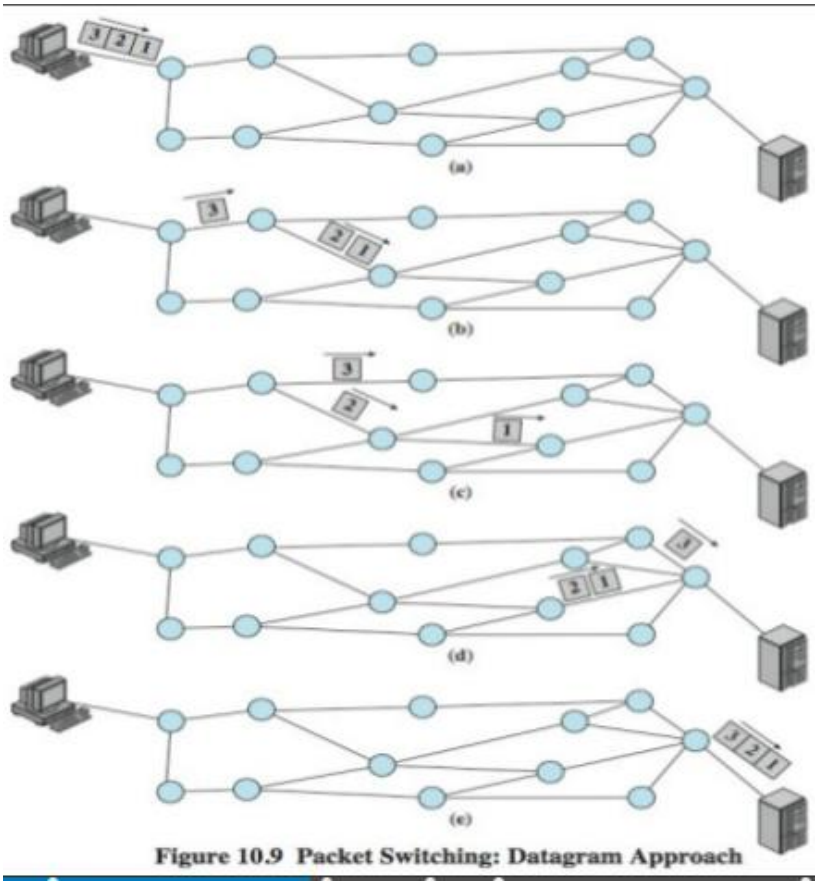

Figure 10.9 Packet Switching: Datagram Approach

There are three types of packet switched services. They are:

1. **Frame Relay**
2. **IP Services**
3. **Ethernet Services**

## Frame Relay Services

Frame Relay is an efficient data transmission technique used to send digital information such as voice, data, LAN, WAN traffic quickly and cost efficiently. Frame Relay is characterized by connection oriented, permanent or switched virtual circuit at speeds upto 50 mbps. It is one oldest used packet services in US which uses T carrier and SONET as its wiring. Frame Relay is unreliable packet service because it does not perform error control. Frame relay checks for errors but simply discards packets with errors. It is up to the software at the source and destination to control for lost messages.

Frame relay does not yet provide QoS capabilities, but this is under development.
Different common carriers offer frame relay networks with different transmission speeds.
Most offer a range of Committed Information Rate (CIR) speeds that include 56 Kbps, 128 Kbps, 256 Kbps, 384 Kbps, 1.5 Mbps, 2 Mbps, and 45 Mbps.

## IP Services

It is believed that IP services will replace frame relay because it is simpler to implement and uses IP. With IP services, the **Packet Assembly/Disassembly Device (PAD)** at source site takes outgoing message (Ethernet frame with IP packet), strips off the Ethernet frame and uses the IP address in the IP packet to route the packet. The PAD at destination site has an Ethernet port, so a new Ethernet packet is added before the packet enters the customer's network at the destination

because the carrier's packet switched network uses IP addresses, this network looks and feels like Internet, although it is a separate network for use only by customers of the carrier.

Most IP services use **Multiprotocol Label Switching (MPLS)** as the data link layer protocol, but as long as the customer receives the contracted data speed packets are delivered in a reliable manner, the customer never needs to know what protocols are used. IP services use T carrier and SONET as its wiring, so its speeds are identical to them e.g. 1.5 Mbps, 45 Mbps 622 Mbps etc.

## Ethernet Services

Although we have seen rapid increases in capacities and sharp decreases in costs in LAN and BN technologies, changes in WAN services offered by common carriers saw only modest changes in the 1990s. That changed in 2000 with the introduction of several Internet startups (e.g., Yipes) offering

Most organizations today use Ethernet and IP in the LAN and BN environment, yet the WAN packet network services (ATM and frame relay) discussed earlier use different layer-2 protocols. Any LAN or BN traffic, therefore, must be translated or encapsulated into a new protocol and destination addresses generated for the new protocol. This takes time, slowing network throughput. It also adds complexity, meaning that companies must add staff knowledgeable in the different WAN protocols, software, and hardware these technologies require. This is one reason many common carriers are starting to call these technologies "legacy technologies," signaling their demise.

Each of the preceding **packet services (frame Relay & IP Services)** uses the traditional PSTN provided by the common carriers such as AT&T and BellSouth. In contrast, Ethernet services bypass the PSTN; companies offering Ethernet services have laid their own gigabit Ethernet fiber-optic networks in large cities. When an organization signs up for service, the packet network company installs new fiber-optic cables from their citywide backbone into the organization's office complex and connects it to an Ethernet switch. The organization simply plugs its network into its Ethernet switch and begins using the service. All traffic entering the packet network must be Ethernet, using IP.

## Virtual Private Networks

A **VPN (Virtual Private Network)** is a service that creates a safe, encrypted online connection over a less secure network such as Internet. Internet users may use a VPN to give themselves more privacy and anonymity online or circumvent geographic-based blocking and censorship. VPNs essentially extend a private network across a public network, which should allow a user to securely send and receive data across the internet.

VPNs can be used to hide a user's browser history, Internet Protocol (IP) address and geographical location, web activity or devices being used. Anyone on the same network will not be able to see what a VPN user is doing. This makes VPNs a go-to tool for online privacy. A VPN uses tunneling protocols to encrypt data at the sending end and decrypts it at the receiving end. The originating and receiving network addresses are also encrypted to provide better security for online activities.

**Benefits of VPNs**

1. **Privacy Protection:** VPN hide the IP address and encrypt the online activities, making it difficult for websites and advertisers to track the browsing habits.
2. **Security:** VPN adds an extra layer of security, especially when using public Wi-Fi networks , protecting our data from potential hackers and cybercriminals.
3. **Access Restricted Content:** VPN allow us to bypass geographical restrictions and access content that might be blocked or restricted in our region. For example, we can access streaming services, websites, or social media platforms that are geo-blocked.
4. **Anonymity:** VPNs can mask our online identity, allowing us to browse the internet anonymously. However, it is important to note that while VPNs enhance privacy, they are not completely anonymous, and our activities can still be traced back under certain circumstances.

5. **Remote Access:** VPNs enable secure remote access to corporate resources for employees working from home or traveling. This is especially important for business that needs to ensure communication and data access for remote employees.

## Basic Architecture

With a VPN, we first lease an Internet connection at whatever access rate and access technology we choose for each location you want to connect. For example, we might lease a T1 circuit from a common carrier that runs from office to **Internet Service Provider (ISP)**. You pay the common carrier for the circuit and the ISP for Internet access. Then connect a **VPN gateway** (a specially designed router or switch) to each Internet access circuit to provide access from your networks to the VPN. The VPN gateways enable you to create PVCs (Permanent Virtual Circuit) through the Internet that are called **tunnels** shown in fig below.

The VPN gateway at the sender takes the outgoing packet and encapsulates it with a protocol that is used to move it through the tunnel to the VPN gateway on the other side. The VPN gateway at the receiver strips off the VPN packet and delivers the packet to the destination network. The VPN is transparent to the users; it appears as though a traditional packet-switched network PVC is in use. The VPN is also transparent to the ISP and the Internet as a whole; there is simply a stream of Internet packets moving across the Internet. **VPN software** is commonly used on home computers or laptops to provide the same secure tunnels to people working from offsite.

VPNs operate either at layer 2 or layer 3. A **layer-2 VPN** uses the layer-2 packet (e.g., Ethernet) to select the VPN tunnel and encapsulates the entire packet, starting with the layer-2 packet. Layer-2 tunneling protocol (**L2TP**) is an example of a layer-2 VPN. A **layer-3 VPN** uses the layer-3 packet (e.g., IP) to select the VPN tunnel and encapsulates the entire packet, starting with the layer-3 packet; it discards the incoming layer-2 packet and generates an entirely new layer-2 packet at the destination. **IPSec** is an example of a layer-3 VPN.

There are **two important disadvantages**. **First, traffic on the Internet is unpredictable**. Sometimes packets travel quickly, but at other times, they take a long while to reach their destination. Although some VPN vendors advertise QoS capabilities, these apply only in the VPN devices themselves; on the Internet, a packet is a packet. **Second, because the data travel on the Internet, security is always a concern**. Most VPN networks encrypt the packet at the source VPN device before it enters the Internet and decrypt the packet at the destination VPN device.

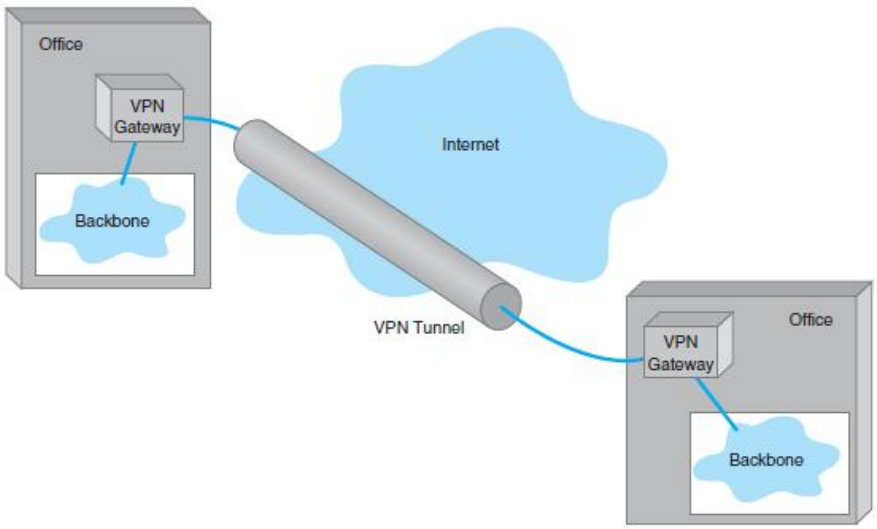


**Fig: VPN Architecture**

**VPN Types**

Three types of VPNs are in common use:

1. Intranet VPN
2. Extranet VPN
3. Access VPN.

An **intranet VPN** also called **internal VPN, site to site VPN** provides virtual circuits between organization offices or multiple locations of a company securely over the Internet. It allows different branches, offices or data centers within the same organization to communicate with each other as if they were on the same private network even if they are geographically distributed. Each location has a VPN gateway that connects the location to another location through the Internet.

An **extranet VPN** is the same as an intranet VPN, except that the VPN connects several different organizations, often customers and suppliers, over the Internet. It extends the concept of a corporate intranet, allowing authorized users from external organizations to access specific resources on a company's network securely.

An **access VPN** enables employees to access an organization's networks from a remote location. Employees have access to the network and all the resources on it in the same way as employees physically located on the network. The user uses VPN software on his or her computer to connect to the VPN device at the office. The VPN gateway accepts the user's log-in, establishes the tunnel, and the software begins forwarding packets over the Internet. An access VPN provides a less expensive connection than having a national toll-free phone number that connects directly into large sets of modems at the organization's office. Compared with a typical ISP-based remote connection, the access VPN is a more secure connection than simply sending packets over the Internet.

**How VPNs Work**

A VPN works by routing a device's internet connection through a private service rather than the user's regular internet service provider (ISP). The VPN acts as an intermediary between the user getting online and connecting to the internet by hiding their IP address.

Using a VPN creates a private, encrypted tunnel through which a user's device can access the internet while hiding their personal information, location, and other data. All network traffic is sent through a secure connection via the VPN. This means that any data transmitted to the internet is redirected to the VPN rather than from the user's computer.

When the user connects to the web using their VPN, their computer submits information to websites through the encrypted connection created by the VPN. The VPN then forwards that request and sends a response from the requested website back to the connection.

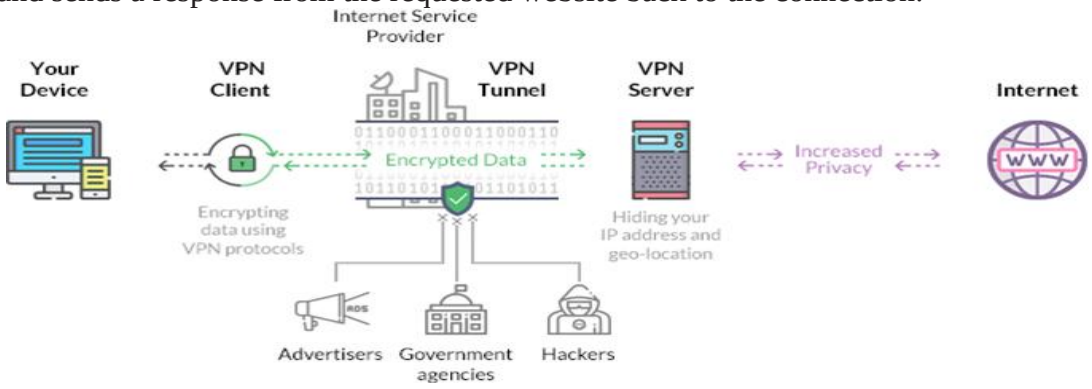


**Fig: VPN Working Process**

**How VPN Work in Practice**

A VPN masks a user's true location to the one they set their VPN to. This enables them to access content or websites typically restricted to that region. For example, a user in the U.S. can set their location to the United Kingdom and watch content from streaming websites aimed at British audiences. A U.S. citizen can also continue streaming their favorite shows even when they are away from the country on holiday.

**Some common uses of VPN are:**

1. Protecting Browsing History
2. Securing IP Address and Location Data
3. Hiding Streaming Location
4. Protecting Devices
5. Ensuring Internet Freedom

**The Best Practice WAN Design**

Developing best practice recommendations for WAN design is more difficult than for LANs and backbones because the network designer buys services from different companies rather than buying products. The relatively stable environment enjoyed by the WAN common carriers is facing sharp challenges by VPNs at the low end and Ethernet and MPLS (Multiprotocol Label Switching) services at the high end. As larger IT and equipment firms begin to enter the VPN and Ethernet services markets, we should see some major changes in the industry and in the available services and costs.

Some best practices for WAN design are:

1. **Understand Business Requirement**
   a) **Collaborate with Stakeholders:** Involve key stakeholders to understand their current and future requirement.

b) **Application Requirements:** identify the applications and services that will be accessed over the WAN. Different applications may have varying bandwidth and latency requirement.

2. **Bandwidth Planning**
   a) **Traffic Analysis:** Conduct thorough analysis of network traffic patterns. Identify peak usage time and the types of data being transmitted.
   b) **Scalability:** Design the network with scalability in mind. Choose WAN technologies than can be easily upgraded to accommodate future growth.
3. **Redundancy and High Availability**
   a) **Redundant Connections: :** Implement redundant WAN connections to ensure high availability. Use diverse paths and providers to minimize the risk of single point failure.
   b) **Failover Mechanisms:** Implement automatic failover mechanisms to switch traffic to backup links in case of a primary link failure.
4. **Security**
   a) **Encryption:** Encryptions protocols should be used to secure data transmitted over the WAN, especially for sensitive and confidential data.
   b) **Firewall and Intrusion Detection:** Deploy firewalls and intrusion detection system to protect WAN from unauthorized access.

5. **Quality of Services (QoS)**
   a) **Prioritize Traffic**: Implement QoS policies to Prioritize critical applications over less sensitive traffic. This ensures that essential applications receive necessary bandwith and low latency.
   b) **Traffic Shaping:** Use traffic shaping to control the flow of traffic, preventing network congestion and optimizing performance for all applications.
6. **WAN Optimization**
   a) **Compression and Caching:** Implement compression and caching techniques to reduce the amount of data transmitted over WAN. Optimizing the bandwidth usages.
   b) **Content Delivery Network:** Utilize CDN to cache content closer to end users, reducing latency and improving the delivery of applications
7. **Monitoring and Management**
   a) **Network Monitoring Tools:** Deploy network monitoring tools to continuously monitor the WAN's Performance, bandwidth utilization and security.
   b) **Centralized Management:** Implement centralized management solutions to efficiently configure, monitor and manage WAN devices and policies.
8. **Documentation and Disaster Recovery:** Maintain detailed documentation of the WAN design, configuration IP Addressing schemes and security policies. It is essential for troubleshooting and future expansion. Also develop robust recovery plan that includes backup connections, data replication and failover procedures to ensure connectivity and business continuity in case of network failures.
9. **Compliance and Regulations:** Ensure WAN design complies with industry regulations and data protection laws applicable for organizations. It is crucial for healthcare and finance organization.

10. **Regular Updates and Training:** Keep WAN equipment and software up-to-date. Also provide Training to IT staff responsible for managing the WAN. Ensure they are well – versed in best practices, security protocols, and troubleshooting techniques.

**Improving WAN Performance**

Improving WAN performance is crucial for business, especially when dealing with remote offices, cloud applications and data – intensive tasks. Improving the performance of WANs is handled in the same way as improving LAN performance. It is done by **checking the devices in the network, by upgrading the circuits between the computers, and by changing the demand placed on the network**

**Improving Device Performance**

In some cases, the key bottleneck in the network is not the circuits; it is the devices that provide access to the circuits (e.g., routers). One way to improve network performance is to upgrade the devices and computers that connect backbones to the WAN. Most devices are rated for their speed in converting input packets to output packets (called **latency**). Not all devices are created equal; some vendors produce devices with lower latencies than others.

Another strategy is examining the routing protocol, **either static or dynamic**.
Dynamic routing will increase performance in networks that have many possible routes from one computer to another and in which message traffic is "bursty"—that is, in which traffic occurs in spurts, with many messages at one time, and few at others.
But dynamic routing imposes an overhead cost by increasing network traffic.

**Improving Circuit Capacity**

The first step is to analyze the message traffic in the network to find which circuits are approaching capacity. These circuits then can be upgraded to provide more capacity.
Less-used circuits can be downgraded to save costs. A more sophisticated analysis involves examining why circuits are heavily used. The capacity may be adequate for most traffic but not for meeting peak demand. One solution may be to add a circuit-switched or packet-switched service that is used only when demand exceeds circuit capacity. The use of a service as a backup for heavy traffic provides the best of both worlds. The lower-cost dedicated circuit is used constantly, and the backup service is used only when necessary to avoid poor response times.

Sometimes a shortage of capacity may be caused by a faulty circuit. As circuits deteriorate, the number of errors increases. As the error rate increases, throughput falls because more messages have to be retransmitted. Before installing new circuits, monitor the existing ones to ensure that they are operating properly or ask the common carrier to do it.

**Reducing Network Demand**

There are many ways to reduce network demand. One simple step is to require a network impact statement for all new application software developed or purchased by the organization. This focuses attention on the network impacts at an early stage in application development.

Another simple approach is to use data compression techniques for all data in the network. Another sometimes more difficult approach is to shift network usage from peak or high-cost times to lower-demand or lower-cost times. For example, the transmission of detailed sales and inventory reports from a retail store to headquarters could be done after the store closes. This takes advantage of off-peak rate charges and avoids interfering with transmissions requiring higher priority such as customer credit card authorizations.

The network can also be redesigned to move data closer to the applications and people who use them. This also will reduce the amount of traffic in the network. Distributed database applications enable databases to be spread across several different computers.
For example, instead of storing customer records in one central location, you could store them according to region.