Unit 8

Wide Area Network

- Introduction, Dedicated Circuit Network, packet switched network
- Best practice wan design, improving WAN performance

- Introduction
- WAN, or **Wide Area Network**, is a telecommunications network that extends over a large geographical area, often connecting multiple smaller networks such as local area networks (LANs) or metropolitan area networks (MANs). WANs are typically used by businesses, governments, and educational institutions to connect remote offices, data centers, or campuses across cities, countries, or even continents
- Key Characteristics
- **Large Geographical Coverage:** Unlike LANs, which are confined to a small area like a building or campus, WANs cover broader areas, often spanning cities, countries, or continents.

- **Public and Private Network:**
- **Public Network:**
  - A WAN may use public networks like the internet for connectivity, where data travels over shared infrastructure managed by service providers.
  - Public WANs are often less expensive but may require encryption (e.g., VPNs) for secure communication.
- **Private Network:**
  - Private WANs use dedicated infrastructure, like leased lines or Multiprotocol Label Switching(MPLS), offering more control, security, and consistent performance.
  - Private networks are typically more secure and reliable but come at a higher cost.
- **Infrastructure:**
  - Uses variety of communication technology i.e fiber optics, satellites, microwaves and other high speed data transmission medium to establish connection over long distance

- Networking devices: uses device such as routers and switches to direct data packets between network.
- Protocol: Wans uses network protocol such as TCP/IP
- Connectivity: Facilitate various type of connectivity, including point to point and point to multipoint connection.

- **Application of WAN**
- Enterprise connectivity: connecting branch offices,enabling seamless communication.
- Internet Access: ISP use WAN to provide internet access to customers over vast geographical areas
- Cloud computing: facilitate access to cloud bases services and resources, allowing business to store data and run application in remote DC.
- Telecommunication: telecommunication companies use wans to provide various service, voice call, video conference and internet connectivity

- **What is a Dedicated Circuit Network?**
- A private, constant connection between two or more points.
- Can be physical (e.g., leased lines) or logical (e.g., virtual circuits in Frame Relay).
- Used exclusively by a single user for high stability and performance.
- **Key Features of Dedicated Circuit Networks**
- **Private and Constant Connection:**
  - Offers round-the-clock stability and dedicated bandwidth.
- **High Performance:**
  - Not publicly shared, ensuring optimal performance.
- **Cost Considerations:**
  - Higher costs due to exclusive usage.
- **Complexity:**
  - Often complex to set up and maintain.

Advantages

1. Reliability

1. Offers a stable and uninterrupted connection.
2. Minimizes the risk of congestion or external interference.

2. Predictable Performance

1. Provides consistent bandwidth and low latency.
2. Ensures that critical applications run smoothly without delays.

3. Security

1. Uses exclusive communication paths, reducing exposure to unauthorized access.
2. Ideal for sensitive data transmission, such as financial transactions or confidential communications.

- **Disadvantages Cost**
    1. High installation and maintenance expenses.
    2. Requires a long-term contract with service providers, leading to significant ongoing costs.

1. **Scalability**
    1. Limited flexibility in scaling bandwidth or adding new locations.
    2. Upgrading requires additional infrastructure or reconfiguration, which can be time-consuming and costly.

- **Types of Dedicated Circuit Network Architectures**
- Ring Architecture
- Star Architecture
- Mesh Architecture

- **Ring Architecture**
- **Structure:**
  - Devices are linked in a circular pattern.
  - Data can flow in both directions for redundancy.
- **Advantages:**
  - Simple to establish, redundancy with dual paths.
- **Disadvantages:**
  - Dependent on each connected device’s performance.
  - Delays if one device is overloaded.

  - **Example: Metropolitan Area Networks (MANs) for Utility Companies:** Utility companies often use ring topology in their Metropolitan Area Networks (MANs) to connect different substations across a city. The ring structure ensures that if there is a break in one part of the network, data can still be transmitted in the opposite direction, maintaining network uptime and reliability.

- **Star Architecture**
- **Structure:**
  - All devices connect to a central computer.
  - Central hub manages data transmission.
- **Advantages:**
  - Easy to manage, faster data transmission via one central point.
- **Disadvantages:**
  - Central hub is a single point of failure.
  - Entire system affected if the hub is overloaded.

  - **Example: Corporate Branch Network:se Case:** A large retail chain uses star topology to connect its branch offices to the central headquarters. Each branch is directly connected to the central office using a dedicated line, typically a leased T1 or MPLS circuit. This setup allows for centralized management of the network and ensures secure data transfer between branches and the main office.

- **Mesh Architecture**
- **Structure:**
  - Full-Mesh: All devices are interconnected.
  - Partial-Mesh: A significant number of devices are interconnected.
- **Advantages:**
  - Multiple paths prevent network failure.
  - High reliability and redundancy.
- **Disadvantages:**
  - Requires significant processing power.
  - Complex to implement and maintain.
  - **Example: Global Financial Institutions :Use Case:** A global financial institution with offices in major financial hubs (New York, London, Tokyo, etc.) uses a full-mesh WAN topology to ensure that each office can communicate directly with any other office. This design provides maximum redundancy and low-latency communication, which is crucial for real-time financial transactions and data synchronization across global markets.

- **Comparison of Architectures**
- **Ring vs. Star vs. Mesh:**
  - **Reliability:** Mesh > Ring > Star
  - **Performance:** Star > Mesh > Ring
  - **Complexity:** Mesh > Ring > Star

- **Use Cases:**
  - Ring: Small networks.
  - Star: Medium-sized networks with centralized control.
  - Mesh: Large, critical networks needing high reliability.

- **T- Carrier Service**
- T carrier service are a type of dedicated circuit network technology that provides high quality digital transmission over leased line.
- Mostly used in North America and some part of world.
- In this service the cost are fixed amount per month, regardless of how much traffic flows through the circuit.

There are several type of T carrier

- T1 circuit
- T2 Circuit
- T3 Circuit
- T4 Circuit

T1 Line:

- Bandwidth: 1.544 Mbps
- Channels: 24 digital channels (each 64 kbps)
- Usage: Often used for connecting branch offices, providing internet access, or interconnecting PBX systems.
- Structure: Each T1 line is composed of 24 individual channels that can carry voice, data, and video.

T2 Line:

- Bandwidth: 6.312 Mbps
- Channels: 96 digital channels (each 64 kbps)
- Usage: Typically used by large organizations or as a backbone connection between network nodes.

T3 Line:

- **Bandwidth:** 44.736 Mbps
- **Channels:** 672 digital channels (each 64 kbps)
- **Usage:** Used for high-capacity connections, often as a backbone link between major network nodes or data centers.
- **Structure:** A T3 line aggregates 28 T1 lines, providing substantial bandwidth for large-scale application

T4 Line:

- **Bandwidth:** 274.176 Mbps
- **Channels:** 4,032 digital channels (each 64 kbps)
- **Usage:** Mostly used in large-scale networks or telecommunications infrastructure requiring extremely high bandwidth.

- **SONET Service**
- **Synchronous Optical Networking (SONET)** is a technology used in telecommunications to transmit data over fiber optic cables. Here’s a simplified breakdown:
- **High-Speed and Reliable:** SONET provides fast and dependable data transmission.
- **Standardized:** It was designed so different telecom equipment from various vendors can work together smoothly.
- **Synchronous Transmission:** Data is transmitted in sync with a specific clock signal, ensuring precise timing.
- **Fiber Optic Use:** SONET primarily uses fiber optic cables, which offer high bandwidth, low latency, and are immune to electromagnetic interference.
- **SONET Speed Levels:**
- SONET speeds start at **OC-1**, which is **51.84 Mbps**.
- Higher speeds are achieved by combining lower speeds using inverse multiplexing.(Inverse multiplexing starts by taking a high-speed data stream and splitting it into multiple lower-speed streams. Each of these streams is then sent over a separate physical link.)
- SONET can reach speeds up to **160 Gbps**.

- **Synchronous Digital Hierarchy (SDH)**
- is a standardized protocol used in telecommunications to transmit large amounts of digital data over optical fiber. It is closely related to SONET (Synchronous Optical Networking), which is used mainly in North America, while SDH is more commonly used in the rest of the world. Both SDH and SONET are designed to ensure high-speed, reliable, and scalable data transmission.
- **SDH (**Synchronous Digital Hierarchy) **and SONET Relationship:**
- SDH and SONET are similar in function and purpose, but they differ in their framing structures and terminology. SDH uses a basic unit called STM-1 (Synchronous Transport Module), which corresponds to SONET's OC-3 (Optical Carrier Level 3). Both technologies work together to ensure that different telecommunications equipment and networks can interoperate smoothly across regions.

1.High Data Rates:

- **Service**: SONET provides various levels of optical carrier services, starting from OC-1 (51.84 Mbps) up to OC-768 (39.813 Gbps) and beyond.
- **Benefit**: These high data rates allow SONET to support a wide range of applications, from simple voice communication to high-bandwidth video streaming and data transfer.

2. Reliability:

- **Service**: SONET networks use a ring topology that offers self-healing capabilities. In case of a failure in the network, data can be rerouted automatically.
- **Benefit**: This ensures continuous and reliable data transmission, minimizing downtime and service interruptions.

3. Scalability:

- **Service**: SONET networks can be easily scaled by upgrading to higher levels of optical carrier services (e.g., from OC-3 to OC-12).
- **Benefit**: This allows the network to grow with increasing demand, making it cost-effective and future-proof

4. Support for Various Traffic Types:

- **Service**: SONET can carry different types of traffic, including voice, data, and video, over the same network.
- **Benefit**: This versatility simplifies network management and reduces the need for multiple network infrastructures, lowering operational costs.

5. Compatibility:

- **Service**: SONET is designed to work with various types of telecommunications equipment and networks, including legacy systems and newer technologies.
- **Benefit**: This compatibility ensures seamless integration with existing infrastructure, making it easier to adopt and deploy across diverse environments.

- **Packet-Switched Network**

1. Data Segmentation:

- **Process**: Original data is broken into smaller units called **packets**.
- **Benefit**: Easier to manage and transmit over the network.

2. Packet Transmission:

- **Mechanism**: Packets are sent independently across the network.
- **Flexibility**: Packets can take different paths based on network conditions.

3. Reassembly:

- **Function**: At the destination, packets are reassembled into the original data.
- **Ensures Accuracy**: Sequencing information in each packet ensures the correct order.

4. Error Checking:

- **Reliability**: The receiving system checks for errors using packet headers.
- **Error Handling**: If errors or missing packets are detected, the system can request retransmission.

Benefits of Packet-Switched Networks

- **Efficient Resource Use**: Optimizes network bandwidth by dynamically routing packets.
- **Scalability**: Easily scales from small local networks to the global Internet.
- **Robustness**: Capable of rerouting packets around network failures or congestion, enhancing reliability.

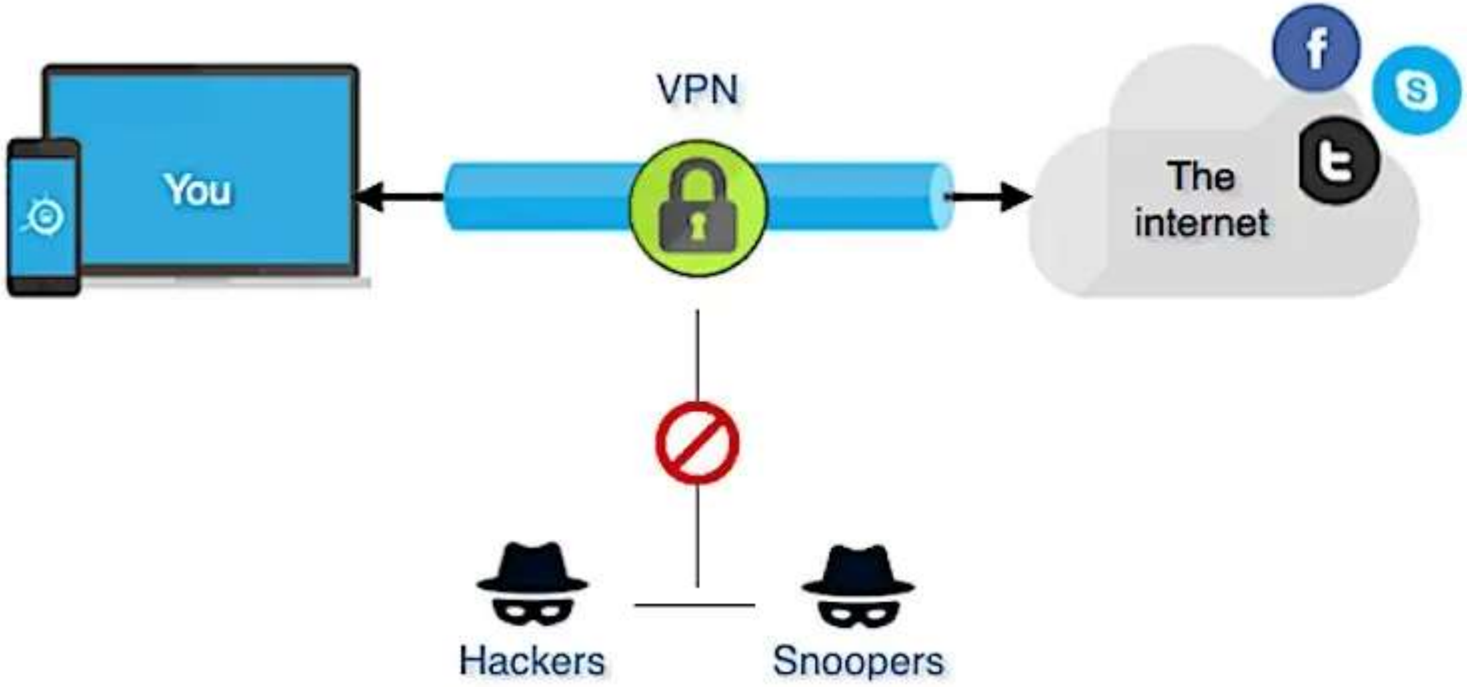
- **What is a Packet-Switched Network?**
- A **Packet-Switched Network (PSN)** is a type of network that sends data in small packets.
- Data is sent from the source to the destination across a shared network channel.
- PSN is **connectionless**, meaning it doesn’t create a continuous connection between the sender and receiver.
- **2. Packet Assembly/Disassembly (PAD):**
- **PAD** devices convert data into packets and send them through the network.
- At the destination, another PAD reassembles the packets into their original form.
- PADs can adjust for different connection speeds between the sender and receiver.

- **3. Key Advantages of Packet-Switched Networks:**
- **Flexible Speeds**: Different locations can have varying connection speeds, and the network adapts.
- **Efficient Use**: Packets from different messages can be mixed and transmitted together, making better use of network resources.
- **4. Virtual Circuits:**
- **Permanent Virtual Circuits (PVCs)**: These are fixed connections within the network used frequently.
- **Switched Virtual Circuits (SVCs)**: These change dynamically based on network traffic, though they are less common.
- **5. Connections and Services:**
- Organizations often lease dedicated circuits (like T1 lines) to connect to the packet-switched network.
- The **Point of Presence (POP)** is where the network connects to the local telephone exchange.

- Three types of packet switched
- **Frame Relay (Frame Relay Service):**
- **Description:** Frame Relay is a packet-switched technology used for connecting multiple LANs (Local Area Networks) across wide areas. It provides a method for sending data between different points using a network of switches, which can handle variable-length packets.
- **Usage:** Commonly used for connecting branch offices to a central office or for linking various locations within a wide-area network (WAN).
- **IP Service (Internet Protocol Service):**
- **Description:** IP service refers to the use of Internet Protocol to transmit data across networks. This can include a variety of services such as IP-based VPNs (Virtual Private Networks), IP-based voice services, and general internet connectivity.
- **Usage:** Ideal for providing internet access, remote access to networks, and supporting various applications that rely on IP networking.

- **Ethernet Service:**
- **Description:** Ethernet service involves using Ethernet technology to provide network connectivity. This can be used for high-speed, reliable connections over a WAN or within a LAN. Ethernet service often includes options like Ethernet over Fiber (EoF) or Ethernet over Copper (EoC).
- **Usage:** Frequently used for connecting different sites within a corporate network, offering scalable and high-speed network solutions. It's also used in data centers and for high-bandwidth applications.

- VPN
- A VPN, or Virtual Private Network, is a technology that creates a secure, encrypted connection over a less secure network, such as the internet. Here are some key benefits of using a VPN:



- Benefits of a VPN:

1. **Privacy Protection:** VPNs shield your personal data from prying eyes, including ISPs and websites, by encrypting your internet traffic and masking your IP address.
2. **Security:** They enhance security by encrypting your data, which helps protect it from hackers and cybercriminals, especially when using public Wi-Fi.
3. **Access to Restricted Content:** VPNs allow you to bypass geographic restrictions and access content that may be limited or blocked in your location.
4. **Anonymity:** By masking your IP address, VPNs help maintain your anonymity online, making it harder for third parties to track your activities.
5. **Remote Access:** VPNs enable secure access to your company's network and resources from anywhere, making them ideal for remote work and travel.

- **How a VPN Works: Overview**

1. Internet Connection and Setup:

1. **Lease Internet Access:** First, you lease an internet connection from a common carrier (e.g., through DSL, cable modem, or other access technologies). This connection links your office to the Internet Service Provider (ISP).
2. **VPN Gateway:** At each location, you set up a VPN gateway (a specially designed router) connected to the internet access circuit. This gateway is responsible for creating and managing the VPN connection.

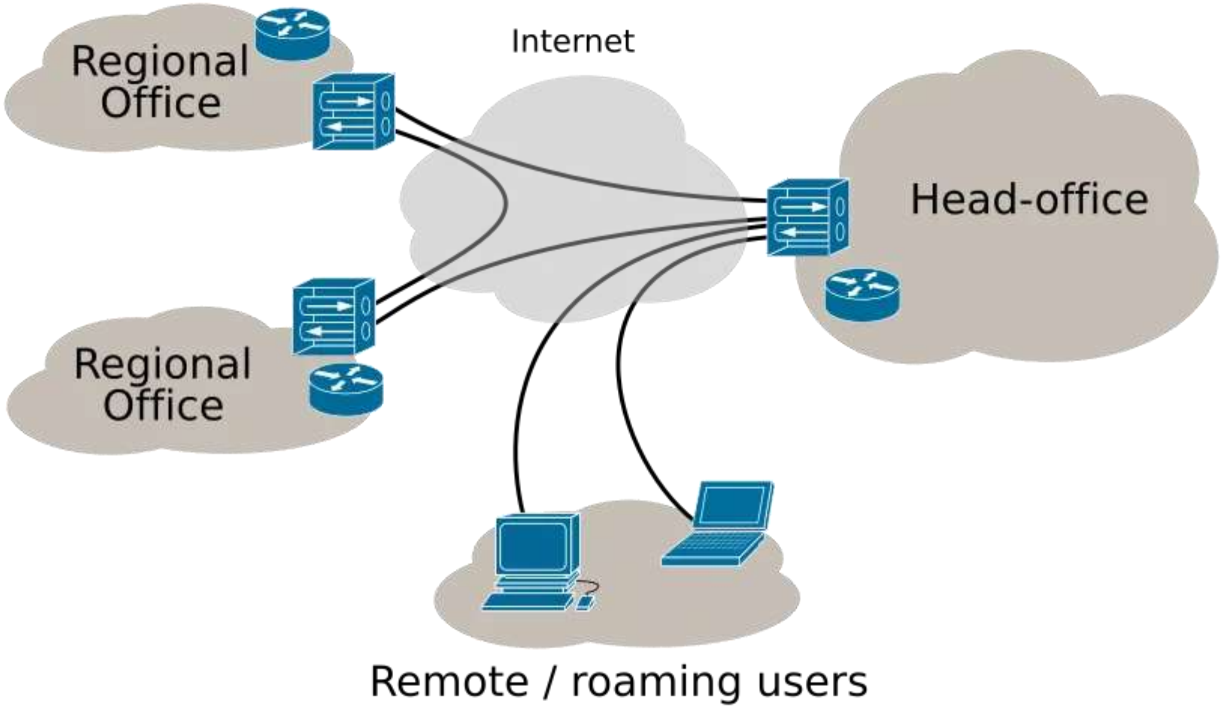
2. VPN Tunnel Creation:

1. **Encapsulation:** The VPN gateway at the sending location takes outgoing data packets and encapsulates them with a VPN protocol. This encapsulated data travels through a secure tunnel over the internet.
2. **Decryption and Delivery:** The VPN gateway at the receiving end strips off the VPN encapsulation and delivers the original packet to its intended destination network.

- **Transparent Operation:**
- **User Transparency:** The VPN is transparent to users; it appears as if they are using a traditional packet-switched network.
- **ISP Transparency:** The ISP sees only a stream of standard internet packets, not VPN-specific traffic.
- **Layer 2 vs. Layer 3 VPNs:**
- **Layer 2 VPN:** Operates at the data link layer (Layer 2) and encapsulates the entire data link packet. Example: Layer 2 Tunneling Protocol (L2TP).
- **Layer 3 VPN:** Operates at the network layer (Layer 3) and encapsulates the network layer packet, generating a new data link packet at the destination. Example: IPsec.

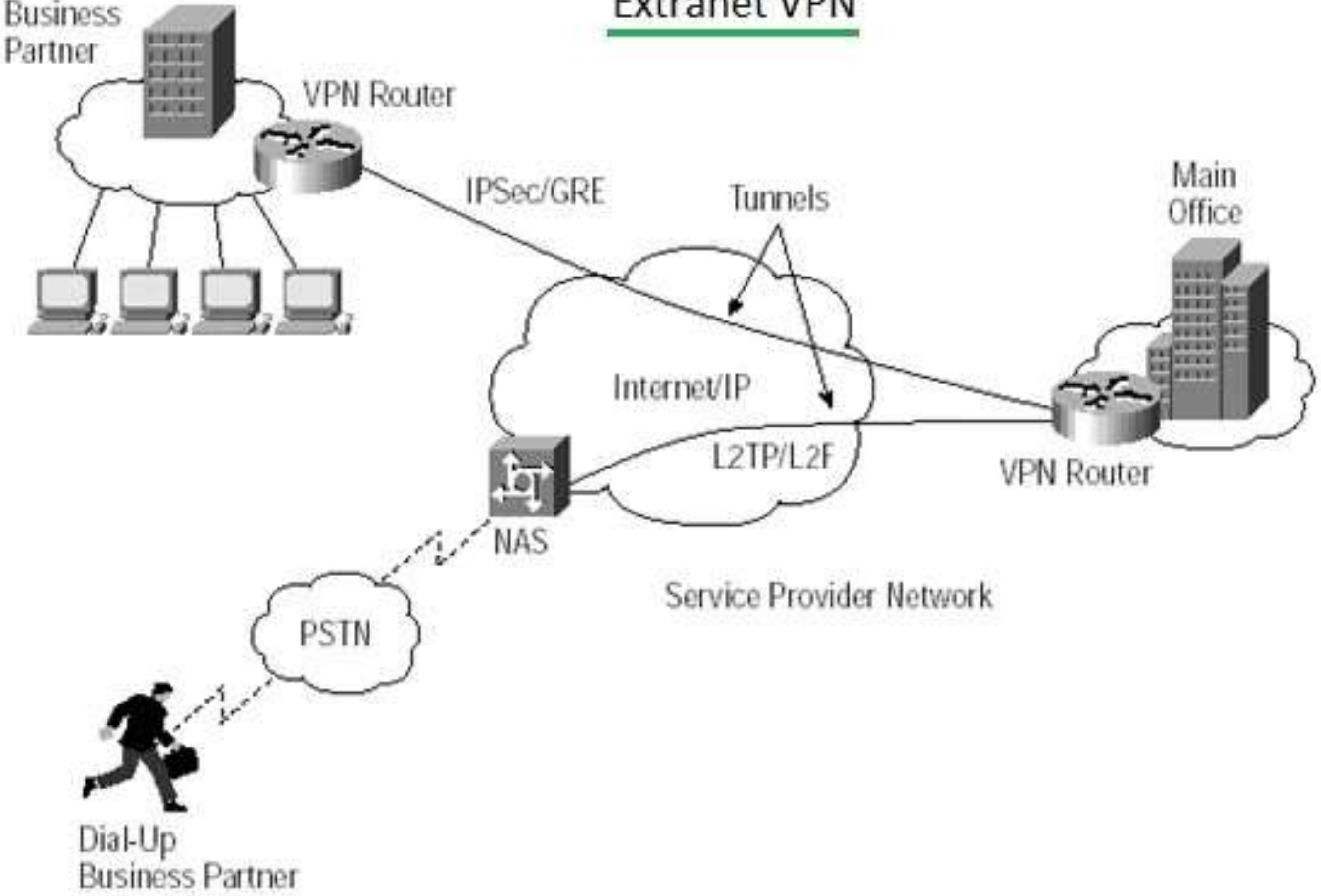
- 3 types of vpn
- **1. Intranet VPN**
- **Description:**
  - An **Intranet VPN** is used to connect multiple internal sites or offices of an organization securely over a public or private network. It creates a private network that allows seamless communication between these internal sites.
- **Functionality:**
  - **Private Network:** All communication occurs within the organization's network, keeping internal data and resources isolated from the public internet.
  - **Security:** Ensures secure and encrypted communication between different offices or locations of the same organization.
- **Usage Example:**
  - A corporation with multiple branch offices across different cities uses an Intranet VPN to connect these offices, allowing them to communicate and share resources as if they were on the same local network.

Internet VPN

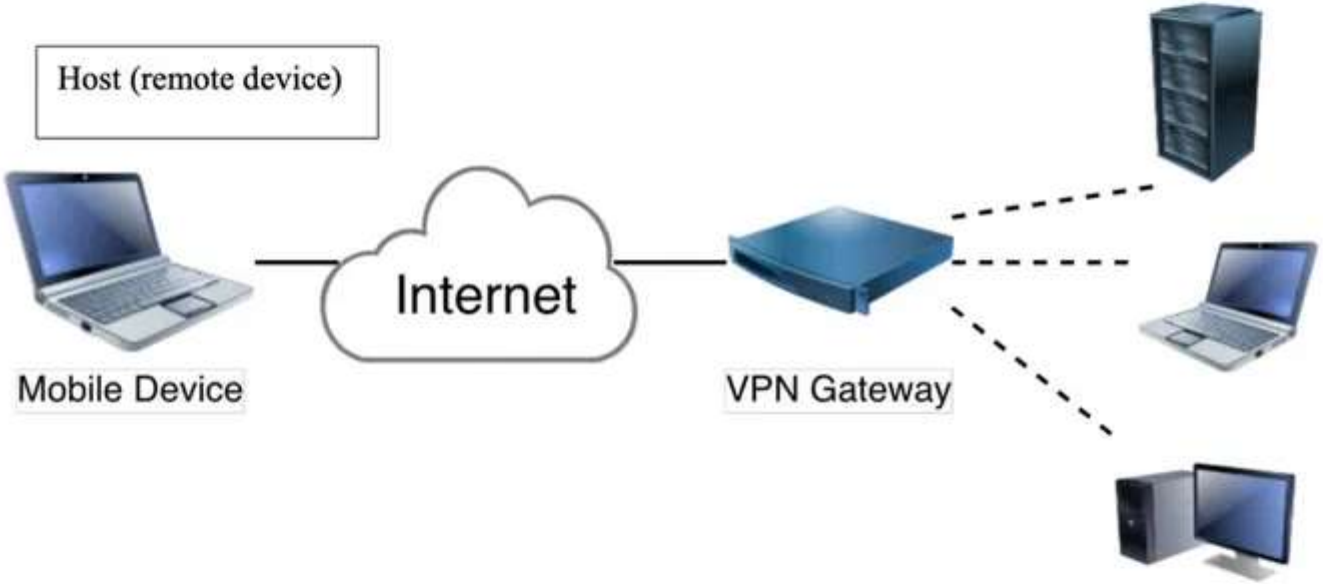


- **2. Extranet VPN**
- **Description:**
  - An **Extranet VPN** extends a portion of an organization's internal network to external partners, clients, or suppliers while maintaining security. It allows secure access to specific resources or data from outside the organization.
- **Functionality:**
  - **Controlled Access:** Provides controlled access to specific parts of the internal network or applications for authorized external entities.
  - **Segmentation:** Typically, access is restricted to certain resources rather than the entire internal network, protecting sensitive internal data.
- **Usage Example:**
  - A company allows its suppliers or business partners to access its inventory management system through an Extranet VPN, enabling collaboration while keeping other internal systems secure.

Extranet VPN



- **3. Access VPN**
- **Description:**
  - An **Access VPN**, often referred to as a **Remote Access VPN**, allows individual users to connect to a private network remotely via a secure connection. It’s typically used by employees who need to access the organization's resources from outside the office.
- **Functionality:**
  - **Remote Access:** Provides secure access to the organization's internal network for remote users, such as employees working from home or traveling.
  - **Encryption:** Encrypts data transmitted between the user's device and the organization's network, ensuring secure communication.
- **Usage Example:**
  - An employee working from home uses an Access VPN to connect to the company’s internal network, allowing them to access files, applications, and resources as if they were in the office.


Host (remote device)
Mobile Device
Internet
VPN Gateway

- The best Practice WAN Design
- **Engage with Key Stakeholders:** Work closely with business leaders, IT staff, and end-users to understand their needs and expectations.
- **Monitor Traffic Patterns:** Analyze current bandwidth usage and identify peak usage times and growth trends.
- **Redundant Paths:** Implement multiple redundant connections to prevent single points of failure.
- **Implement Strong Security Measures: Use** encryption protocols (e.g., IPsec, SSL/TLS) to protect data in transit. Deploy firewalls and VPNs to secure data a
- **Network Monitoring Tools:** Use network monitoring tools to track performance, detect issues, and analyze traffic patterns.
- **Develop a DR Plan:** Create a comprehensive disaster recovery plan that outlines procedures for recovering from network failures or disasters.

- **Backup Solutions:** Implement backup solutions for critical network configurations and data.
- **Upgrade Infrastructure:** Periodically upgrade network infrastructure to leverage new capabilities and improve performance.
- **Staff Training:** Provide ongoing training for IT staff to ensure they are knowledgeable about WAN technologies, security practices, and troubleshooting techniques.

- Improving WAN Performance
- Increase computer and device performance
- Change to more appropriate routing protocols
- Increase circuit
- Analyze message traffic and upgrade faster circuit
- Reduce network demand
- Change user behavior
- Move data close to user.

- **Improving Circuit Capacity in WAN**
- **1. Analyze Network Traffic:**
- **Identify Bottlenecks:** Monitor message traffic to find circuits nearing capacity.
- **Upgrade or Downgrade:** Increase capacity for heavily used circuits; reduce capacity for less-used ones to optimize costs.
- **2. Address Peak Demand:**
- **Analyze Usage Patterns:** Determine if circuits are adequate for peak demand.
- **Implement Backup Solutions:** Use packet-switched services as backup during peak times to complement dedicated circuits and ensure consistent performance.
- **3. Monitor Circuit Health:**
- **Check for Faults:** Regularly monitor circuits for errors and deteriorations that can affect performance.
- **Error Management:** Address faulty circuits promptly to prevent reduced throughput and increased retransmissions.
- **4. Regular Maintenance:**
- **Continuous Monitoring:** Ensure circuits are functioning properly; involve common carriers if needed.
- **Preventive Actions:** Implement maintenance practices to avoid future capacity issues.

- **Reducing Network Demand**
- **1. Require Network Impact Statements**
- **Early Evaluation:** Mandate a network impact statement for all new applications to assess and address network implications early in development.
- **2. Utilize Data Compression**
- **Efficiency:** Apply data compression techniques across the network to reduce data size and lower bandwidth usage.
- **3. Shift Usage to Off-Peak Times**
- **Timing Optimization:** Schedule non-urgent tasks, like detailed reports, during off-peak hours to take advantage of lower costs and avoid peak traffic interference.
- **4. Redesign Network for Efficiency**
- **Data Proximity:** Move data closer to users and applications to minimize network traffic. For example, use distributed databases to store data regionally rather than in a central location.