**Assignment 1: write the network terminologies with example**

**Node:** Any device connected to a network, such as a computer, printer, or router.

**Example:**

**In a home network, a laptop, a smartphone, a printer, and a router are all considered nodes.**

**Protocol:** A set of rules and standards that define how devices on a network communicate with each other.

**Example:**  
The HTTP (HyperText Transfer Protocol) is used for transferring web pages on the internet. When you type **www.example.com** into your browser, HTTP dictates how the browser and web server communicate to display the page.

**IP Address:**A unique numerical identifier assigned to each device on a network, used to identify and communicate with other devices.

**Example:**  
A home computer might have an IP address of **192.168.1.2**, allowing it to communicate with other devices on the same network.

**Router:**A networking device that connects multiple networks together and forwards data packets between them.

**Example:**  
A home router connects your local home network (LAN) to your Internet Service Provider's network, enabling access to the internet.

**Switch:**A networking device that connects devices on a network and forwards data packets between them.

**Example:**  
In an office, a network switch connects multiple computers, printers, and servers, allowing them to communicate within the same local network.

**Firewall:** A security device or software that monitors and controls incoming and outgoing network traffic, based on a set of predefined security rules.

**Example:**  
A corporate firewall might block access to certain websites to prevent employees from visiting potentially harmful or distracting sites.

**DNS (Domain Name System):**A system that translates domain names (such as www.example.com) into IP addresses, allowing devices to locate and connect to websites and other network resources.

Example:

When you enter **www.google.com** in your web browser, the DNS translates this domain name into an IP address like **142.250.64.78**, enabling your browser to load the Google website.

**MAC Address**

**Definition:** A MAC (Media Access Control) address is a unique hardware identifier assigned to each network interface card (NIC) by the manufacturer.

**Example:**  
A laptop’s wireless network card might have a MAC address of **00:1A:2B:3C:4D:5E**, which is used to identify it on a local network.

**Subnet Mask**

**Definition:** A subnet mask is used to divide an IP address into a network and host portion, defining which part of the IP address is the network address and which part is the host address.

**Example:**  
In a network with an IP address of **192.168.1.10** and a subnet mask of **255.255.255.0**, the network portion is **192.168.1** and the host portion is **10**.

**DHCP (Dynamic Host Configuration Protocol)**

**Definition:** DHCP is a network management protocol used to automatically assign IP addresses and other network configurations to devices on a network.

**Example:**  
When you connect your smartphone to a Wi-Fi network, the DHCP server in the router assigns it an IP address automatically.

**VPN (Virtual Private Network)**

**Definition:** A VPN extends a private network across a public network, allowing users to send and receive data as if their devices were directly connected to the private network.

**Example:**  
Employees working remotely use a VPN to securely access their company’s internal network and resources as if they were in the office.

**Bandwidth**

**Definition:** Bandwidth is the maximum rate of data transfer across a given path, measured in bits per second (bps).

**Example:**  
An internet connection with a bandwidth of **100 Mbps** allows data to be transferred at 100 Megabits per second.

**Latency**

**Definition:** Latency is the time it takes for a data packet to travel from the source to the destination, measured in milliseconds (ms).

**Example:**  
A ping test might show a latency of **20 ms** between your computer and a remote server, indicating it takes 20 milliseconds for a packet to travel to the server and back.

**LAN (Local Area Network)**

**Definition:** A LAN is a network that spans a relatively small area, such as a single building or campus, and is typically confined to a limited geographic area.

**Example:**  
The network in a small office, connecting computers, printers, and servers, is a LAN.

**WAN (Wide Area Network)**

**Definition:** A WAN is a network that covers a broad area, such as a city, country, or even global connections, linking multiple LANs.

**Example:**  
The internet is the largest example of a WAN, connecting networks across the world.

**Proxy Server**

**Definition:** A proxy server acts as an intermediary for requests from clients seeking resources from other servers, providing various levels of security, privacy, and administrative control.

**Example:**  
An organization may use a proxy server to filter and monitor employee internet usage and to cache frequently accessed web pages to improve performance.

**SSID (Service Set Identifier)**

**Definition:** An SSID is the name of a wireless network, used to identify and differentiate networks.

**Example:**  
When you search for Wi-Fi networks on your smartphone, you might see SSIDs like **Home\_WiFi** or **Cafe\_Network**.

**NAT (Network Address Translation)**

**Definition:** NAT is a method used by routers to translate private IP addresses within a local network to a single public IP address for accessing external networks.

**Example:**  
A home router uses NAT to allow multiple devices (with private IP addresses) to share a single public IP address provided by the ISP.

**HTTP/HTTPS (HyperText Transfer Protocol/Secure)**

**Definition:** HTTP is the protocol used for transmitting web pages over the internet, while HTTPS is the secure version that encrypts data to protect privacy and security.

**Example:**  
Accessing **http://www.example.com** uses HTTP, while accessing **https://www.example.com** uses HTTPS, providing a secure connection.

**FTP (File Transfer Protocol)**

**Definition:** FTP is a standard network protocol used for transferring files from one host to another over a TCP-based network, such as the internet.

**Example:**  
Web developers use FTP to upload and download website files to and from a web server.

**Assignment 2: Draw your Home Network Topology and explain how you are accessing the RPS Lab environment.**

### Home Network Topology

**Diagram:**

#### 

#### ISP Modem

#### 

#### Router

#### 

#### PC Laptop Smartphone

1. **ISP Modem**: The Internet Service Provider (ISP) modem connects my home to the internet. It typically receives the signal from the ISP through a coaxial cable, fiber optic, or DSL line.
2. **Router**: The router is connected to the ISP modem. Its primary function is to distribute the internet connection to multiple devices within the home. It typically offers both wired (Ethernet) and wireless (Wi-Fi) connections.
3. **Devices**:
   * **PC**: Connected to the router via an Ethernet cable for a stable and fast connection.
   * **Laptop**: Connected to the router via Wi-Fi, providing flexibility and mobility within the home.
   * **Smartphone**: Also connected to the router via Wi-Fi, allowing access to the internet from anywhere within the Wi-Fi range.

### Accessing the RPS Lab Environment

To access the RPS (Remote PowerShell) Lab environment, the following steps are taken:

1. **VPN Connection (if required)**:
   * Some labs might require a VPN connection for secure remote access. This involves using VPN client software to connect to the lab's network.
2. **Remote Desktop Connection**:
   * Using Remote Desktop Protocol (RDP), I can connect to the remote machine provided by the RPS Lab environment. This is done by entering the IP address or hostname of the remote machine along with my login credentials.
3. **Web-Based Interface**:
   * Some lab environments offer a web-based interface to access virtual machines and resources. This can be accessed via a web browser by navigating to the provided URL and logging in with the appropriate credentials.
4. **PowerShell Session**:
   * Once connected to the remote machine, I open a PowerShell session. This can be done either directly on the remote machine's desktop interface or through a remote PowerShell session using **Enter-PSSession** or **Invoke-Command** cmdlets if the necessary permissions and network configurations are in place.
5. **RPS Lab Tools and Resources**:
   * The lab environment typically provides various tools and resources required for the assignments, including pre-configured scripts, datasets, and other utilities.

**Assignment 3: Identify a real-world application for both parallel computing and networked systems. Explain how these technologies are used and why they are important in that context.**

**Parallel Computing: Weather Forecasting**

**Application:**  
Weather forecasting models are a prime example of parallel computing. These models require vast computational power to simulate and predict weather patterns accurately.

**How It Is Used:**

1. **Data Collection:** Weather forecasting begins with the collection of data from various sources, such as satellites, weather stations, and ocean buoys. This data includes temperature, humidity, wind speed, and other meteorological factors.
2. **Data Processing:** The collected data is then processed using complex mathematical models. These models use differential equations to simulate atmospheric behavior.
3. **Parallel Processing:** To handle the immense computational load, the task is divided into smaller sub-tasks, which are processed simultaneously across multiple processors. High-performance computing (HPC) systems, equipped with thousands of CPUs or GPUs, perform these calculations in parallel.
4. **Model Execution:** Different sections of the atmosphere are modeled concurrently. Each processor might handle a specific geographical region or a particular aspect of the weather system, such as wind or precipitation.
5. **Result Integration:** The results from all processors are then integrated to produce a comprehensive weather forecast.

**Importance:**  
Parallel computing is crucial in weather forecasting because it significantly reduces the time required to generate accurate forecasts. Rapid and precise weather predictions are essential for:

* **Public Safety:** Timely forecasts help in preparing for severe weather conditions, such as hurricanes, tornadoes, and floods, thereby saving lives and reducing property damage.
* **Agriculture:** Farmers rely on weather forecasts to plan activities like planting, irrigation, and harvesting.
* **Aviation:** Accurate weather predictions are vital for flight planning and safety.
* **Energy Management:** Forecasting helps in managing renewable energy resources, such as wind and solar power.

**Networked Systems: Online Banking**

**Application:**  
Online banking is a critical real-world application that relies heavily on networked systems. It allows customers to perform banking transactions over the internet securely and conveniently.

**How It Is Used:**

1. **Client-Server Model:** Online banking operates on a client-server model, where the client's device (computer, smartphone) communicates with the bank's server over the internet.
2. **Authentication and Security:** Secure network protocols like HTTPS and SSL/TLS ensure that data transmitted between the client and server is encrypted and secure. Multi-factor authentication (MFA) adds an additional layer of security.
3. **Database Management:** Networked systems manage and access vast databases containing customer account information, transaction histories, and other financial data.
4. **Transaction Processing:** When a customer performs a transaction, such as transferring money or paying bills, the request is sent to the bank's server. The server processes the request, updates the databases, and sends a confirmation back to the client.
5. **API Integration:** Banks often integrate with third-party services (like payment gateways and financial apps) through APIs (Application Programming Interfaces), which operate over networked systems.

**Importance:**  
Networked systems are essential for online banking due to several reasons:

* **Accessibility:** Customers can access banking services from anywhere, at any time, enhancing convenience and customer satisfaction.
* **Efficiency:** Networked systems enable real-time transaction processing, reducing wait times and improving service efficiency.
* **Cost-Effectiveness:** Online banking reduces the need for physical branch operations, lowering operational costs for banks.
* **Scalability:** Networked systems allow banks to scale their services to accommodate a growing number of users without significant physical infrastructure investments.
* **Security:** Advanced network security measures protect sensitive financial data and prevent unauthorized access and fraud.