Port

A **port** in networking is a communication endpoint that allows software applications to identify specific processes or services running on a device. Ports are essential for enabling multiple network services to run simultaneously on a single device without interference. Each port is associated with a unique number, known as the **port number**, which ranges from 0 to 65535.

Key Characteristics of Ports:

Port Numbers:

Ports are identified by numbers, which can be categorized into three ranges:

1. **Well-Known Ports (0-1023)**: These ports are reserved for specific services and applications (e.g., HTTP uses port 80, HTTPS uses port 443, FTP uses port 21).
2. **Registered Ports (1024-49151)**: These ports are assigned to user applications and services that are not as widely known as the well-known ports.
3. **Dynamic or Private Ports (49152-65535)**: These ports are typically used for temporary or dynamic connections. They are often assigned by the operating system when a client application requests a connection.

Transport Layer Protocols: Ports operate at the transport layer of the Internet Protocol Suite and are typically used with two primary protocols

1. **TCP (Transmission Control Protocol)**: A connection-oriented protocol that ensures reliable data transmission. Ports using TCP are typically associated with services that require guaranteed delivery, such as web servers and email servers.
2. **UDP (User Datagram Protocol)**: A connectionless protocol that allows for faster data transmission without the overhead of establishing a connection. UDP is used for services where speed is more critical than reliability, such as video streaming and online gaming.

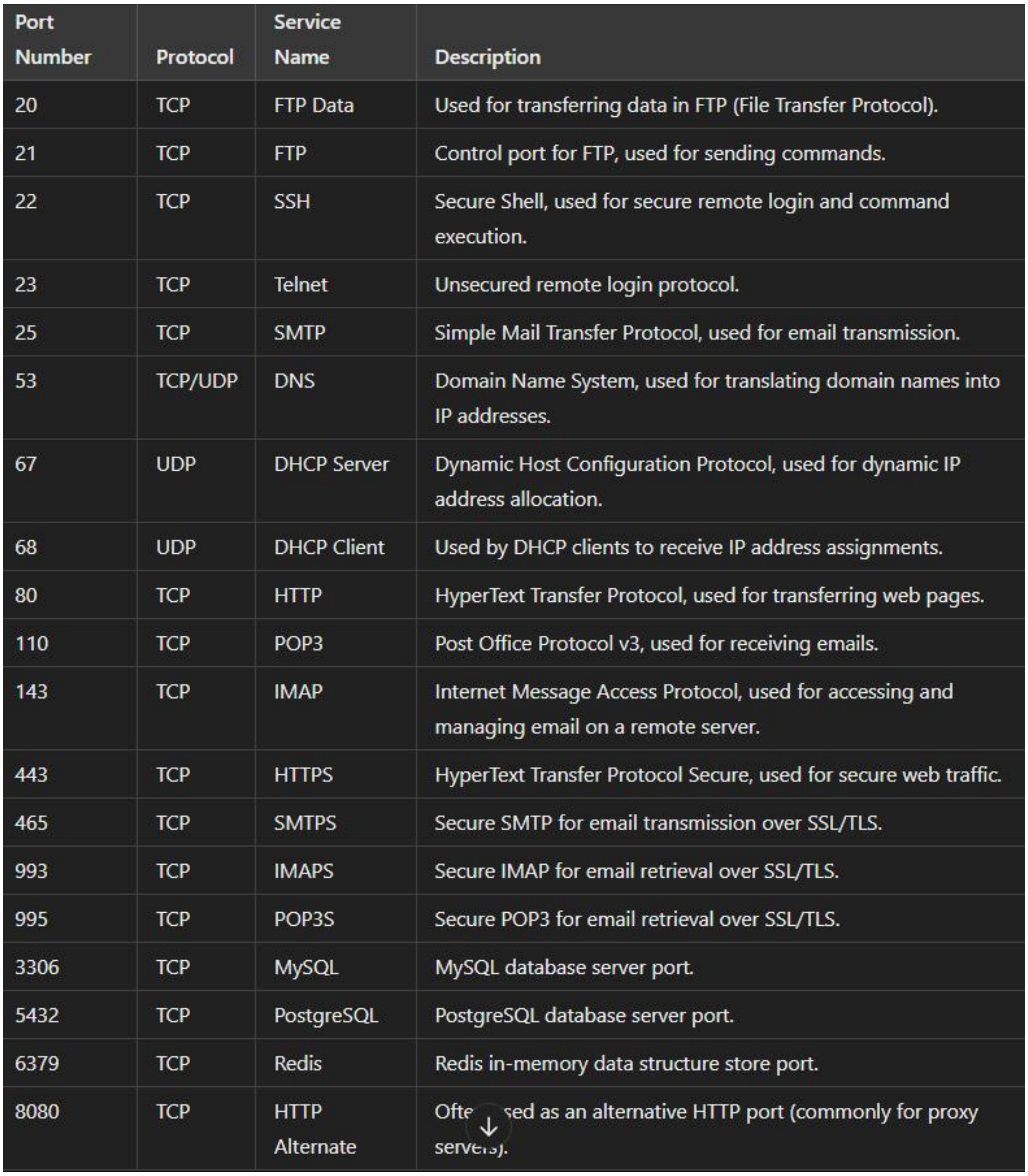
Socket: A combination of an IP address and a port number creates a socket, which uniquely identifies a connection to a specific service on a specific device. For example, the socket `192.168.1.10:80` identifies an HTTP service running on the device with the IP address `192.168.1.10`.

Firewalls and Security: Ports play a significant role in network security. Firewalls often use port numbers to control incoming and outgoing traffic. Administrators can block or allow traffic on specific ports to protect the network from unauthorized access and attacks.

Examples of Common Ports:

1. **HTTP**: Port 80 (used for web traffic)

2. **HTTPS**: Port 443 (used for secure web traffic)
3. **FTP**: Port 21 (used for file transfers)
4. **SSH**: Port 22 (used for secure shell access)
5. **DNS**: Port 53 (used for domain name resolution)



Port Number	Protocol	Service Name	Description
20	TCP	FTP Data	Used for transferring data in FTP (File Transfer Protocol).
21	TCP	FTP	Control port for FTP, used for sending commands.
22	TCP	SSH	Secure Shell, used for secure remote login and command execution.
23	TCP	Telnet	Unsecured remote login protocol.
25	TCP	SMTP	Simple Mail Transfer Protocol, used for email transmission.
53	TCP/UDP	DNS	Domain Name System, used for translating domain names into IP addresses.
67	UDP	DHCP Server	Dynamic Host Configuration Protocol, used for dynamic IP address allocation.
68	UDP	DHCP Client	Used by DHCP clients to receive IP address assignments.
80	TCP	HTTP	HyperText Transfer Protocol, used for transferring web pages.
110	TCP	POP3	Post Office Protocol v3, used for receiving emails.
143	TCP	IMAP	Internet Message Access Protocol, used for accessing and managing email on a remote server.
443	TCP	HTTPS	HyperText Transfer Protocol Secure, used for secure web traffic.
465	TCP	SMTPS	Secure SMTP for email transmission over SSL/TLS.
993	TCP	IMAPS	Secure IMAP for email retrieval over SSL/TLS.
995	TCP	POP3S	Secure POP3 for email retrieval over SSL/TLS.
3306	TCP	MySQL	MySQL database server port.
5432	TCP	PostgreSQL	PostgreSQL database server port.
6379	TCP	Redis	Redis in-memory data structure store port.
8080	TCP	HTTP Alternate	Often used as an alternative HTTP port (commonly for proxy servers).