# Network Protocols

🟦 Protocol: **HTTP** (Hypertext Transfer Protocol)

* **Purpose**: Transfers web pages between client and server.
* **Security**: No encryption (data is sent in plain text).
* **Port**: 80
* **Layer**: Application Layer (Layer 7)
* **Used for**: Basic web browsing without sensitive data.

🔵 Protocol: **HTTPS** (HTTP Secure)

* **Purpose**: Transfers web pages securely using encryption (SSL/TLS).
* **Security**: Encrypted connection – protects data from eavesdropping and tampering.
* **Port**: 443
* **Layer**: Application Layer (Layer 7)
* **Used** for: Secure browsing, login forms, online banking, and transactions.

**Secure Protocols:**

🟩 Protocol: **SSL** (Secure Sockets Layer)

* **Purpose**: Provides encryption for data in transit.
* **Status**: Deprecated – replaced by TLS due to security flaws.
* **Layer**: Between Application and Transport Layers.
* **Used for**: Securing connections like HTTPS, FTPS, SMTPS.

🟢 Protocol: **TLS** (Transport Layer Security)

* **Purpose**: Provides secure communication through encryption, authentication, and integrity.
* **Status**: Current and widely used protocol (successor of SSL).
* **Layer**: Between Application and Transport Layers.
* **Used for**: Secure versions of HTTP, FTP, SMTP, IMAP, etc.

**1**

**Transport Protocols:**

🔵 Protocol: **TCP** (Transmission Control Protocol)

* **Type**: Connection-oriented (reliable)
* **Purpose**: Ensures accurate and ordered delivery of data.
* Mechanism: Uses 3-way handshake (SYN, SYN-ACK, ACK)
* **Port Examples**: HTTP (80), HTTPS (443), FTP (21), SMTP (25)
* **Layer**: Transport Layer (Layer 4)
* **Used for**: Web browsing, email, file transfer.

🟠 Protocol: **UDP** (User Datagram Protocol)

* **Type**: Connectionless (unreliable but faster)
* **Purpose**: Sends data without guaranteeing delivery or order.
* **Mechanism**: No handshake – sends directly.
* **Port Examples**: DNS (53), DHCP (67/68), VoIP, Streaming
* **Layer**: Transport Layer (Layer 4)
* **Used for**: Video/audio streaming, online gaming, DNS.

**File Transfer Protocols:**

🟦 Protocol: **FTP** (File Transfer Protocol)

* **Purpose**: Transfers files between client and server.
* **Security**: Not encrypted (plain text).
* **Port**: 21 (and 20 for data)
* **Transport**: TCP
* **Used for**: Basic file transfers (not recommended for secure environments).

🟨 Protocol: **TFTP** (Trivial File Transfer Protocol)

* **Purpose**: Lightweight file transfer without authentication.
* **Security**: No encryption, no login.
* **Port**: 69
* **Transport**: UDP
* **Used for**: Firmware updates, booting devices over network.

**2**

🟩 Protocol: **SFTP** (SSH File Transfer Protocol)

* **Purpose**: Secure file transfer over SSH.
* **Security**: Encrypted, authenticated, integrity checked.
* **Port**: 22
* **Transport**: TCP (via SSH)
* **Used for**: Secure file transfers in production systems.

🟧 Protocol: **SCP** (Secure Copy Protocol)

* **Purpose**: Fast and secure file copy over SSH.
* **Security**: Encrypted via SSH
* **Port**: 22
* **Transport**: TCP (via SSH)
* **Used for**: Quick file transfers between systems.

**Email Transfer Protocols:**

🟨 Protocol: **SMTP** (Simple Mail Transfer Protocol)

* **Purpose**: Sends email from client to server, or between mail servers.
* **Direction**: Outgoing mail only.
* **Port**: 25 (or 465/587 with SSL/TLS)
* **Transport**: TCP
* **Used for**: Email delivery (sending).

🟦 Protocol: **POP3** (Post Office Protocol v3)

* **Purpose**: Downloads email from server to local device and deletes it from server.
* **Direction**: Incoming mail.
* **Port**: 110 (or 995 with SSL)
* **Transport**: TCP
* **Used for**: One-device email access (no synchronization).

**3**

🟩 Protocol: **IMAP** (Internet Message Access Protocol)

* **Purpose**: Accesses and manages email on the server without deleting.
* **Direction**: Incoming mail.
* **Port**: 143 (or 993 with SSL)
* **Transport**: TCP
* **Used for**: Multi-device email access with synchronization.

**Network Services Protocols:**

🟩 Protocol: **DHCP** (Dynamic Host Configuration Protocol)

* **Purpose**: Automatically assigns IP addresses and network settings to devices.
* **Security**: Basic – can be spoofed if unsecured.
* **Port**: 67 (server), 68 (client)
* **Transport**: UDP
* **Used for**: Automatic IP configuration.

🟦 Protocol: **DNS** (Domain Name System)

* **Purpose**: Resolves domain names into IP addresses.
* **Security**: Basic (DNSSEC adds authentication).
* **Port**: 53
* **Transport**: UDP (TCP used for zone transfers)
* **Used** **for**: Website access by name instead of IP.

🟨 Protocol: **NTP** (Network Time Protocol)

* **Purpose**: Synchronizes clocks between devices over a network.
* **Security**: Limited (NTPsec and Chrony provide improvements).
* **Port**: 123
* **Transport**: UDP
* **Used** **for**: Accurate timekeeping in networks and systems.

**4**

**Network Management Protocols:**

🟩 Protocol: **SNMP** (Simple Network Management Protocol)

* **Purpose**: Monitors and manages network devices.
* **Security**: SNMPv1/v2 are insecure, SNMPv3 supports encryption and authentication.
* **Port**: 161 (UDP), 162 for traps
* **Transport**: UDP
* **Used** **for**: Network monitoring tools like Zabbix, Nagios.

🟨 Protocol: Telnet (Terminal Network)

* **Purpose**: Remote command-line access to devices.
* **Security**: No encryption – not secure.
* **Port**: 23
* **Transport**: TCP
* **Used** **for**: Legacy remote management (replaced by SSH).

🟦 Protocol: SSH (Secure Shell)

* **Purpose**: Secure remote command-line access.
* **Security**: Encrypted and authenticated.
* **Port**: 22
* **Transport**: TCP
* **Used** **for**: Remote server access, file transfers (SFTP, SCP).

🟧 Protocol: RDP (Remote Desktop Protocol)

* **Purpose**: Remote graphical desktop access.
* **Security**: Supports encryption and multi-user features.
* **Port**: 3389
* **Transport**: TCP
* **Used** **for**: Remote access to Windows desktops and servers.

**5**

**Control Protocols:**

🟩 Protocol: **ICMP** (Internet Control Message Protocol)

* **Purpose**: Sends control and error messages (e.g., unreachable, timeout).
* **Usage**: Used by ping and traceroute tools.
* **Transport**: No port – works directly with IP.
* **Layer**: Network Layer (Layer 3)
* **Used** **for**: Network diagnostics and error reporting.

🟦 Protocol: **IGMP** (Internet Group Management Protocol)

* **Purpose**: Manages multicast group memberships.
* **Usage**: Used in video streaming and group communication.
* **Transport**: No port – works directly with IP.
* **Layer**: Network Layer (Layer 3)
* **Used** **for**: Multicast communication management.

**Multimedia / Communication Protocols:**

🟦 Protocol: **SIP** (Session Initiation Protocol)

* **Purpose**: Establishes, modifies, and terminates VoIP calls and video sessions.
* **Security**: Can use TLS for secure signaling.
* **Port**: 5060 (UDP/TCP), 5061 (TLS)
* **Transport**: TCP/UDP
* **Used** **for**: VoIP call signaling and control.

🟨 Protocol: **RTP** (Real-time Transport Protocol)

* **Purpose**: Transmits audio and video data in real-time.
* **Security**: No native encryption (can be used with SRTP).
* **Port**: Dynamic (usually > 1024)
* **Transport**: UDP
* **Used** **for**: Media streaming in VoIP, video calls.

**6**

🟩 Protocol: **MGCP** (Media Gateway Control Protocol)

* **Purpose**: Controls media gateways in VoIP networks.
* **Security**: Limited; usually protected by network isolation.
* **Port**: 2427 (gateway), 2727 (controller)
* **Transport**: UDP
* **Used** **for**: Managing gateways between IP and PSTN.

🟧 Protocol: **H.323**

* **Purpose**: Standard for real-time audio, video, and data communication.
* **Security**: Basic; can integrate with encryption.
* **Port**: 1720 (H.225)
* **Transport**: TCP/UDP
* **Used** **for**: Video conferencing, VoIP systems.

**7**