GENERAL

protocols used in computer networking

Published: September 3, 2026 | Index ID: #-

Introduction

In today's hyper connected world, every device—from smartphones and laptops to industrial sensors—communicates over a complex web of networks. Behind each click, each data packet, and every real time video stream lies a set of rules that dictate how information is formatted, transmitted, and interpreted. These rules are known as **protocols used in computer networking**. Understanding these protocols is essential for network engineers, developers, and anyone curious about how the internet and local networks function.

What Are Computer Networking Protocols?

Computer networking protocols are standardized sets of rules that enable devices to exchange data reliably and efficiently. They define everything from the electrical signals that travel over a cable to the syntax of a web page request. Protocols ensure that devices with different hardware, operating systems, and applications can communicate seamlessly.

Each protocol is designed for a specific purpose or layer of communication. The **OSI model** and the **TCP/IP stack** are the two most widely taught frameworks that organize these protocols into layers, helping engineers diagnose problems and design robust networks.

The OSI Model: A Framework for Protocols

The OSI (Open Systems Interconnection) model, proposed by the International Organization for Standardization (ISO), divides network communication into seven conceptual layers. While the OSI model is largely theoretical, it remains a valuable reference for understanding how protocols interact.

Physical Layer

The Physical Layer deals with the raw bitstream over a physical medium. Protocols and standards here include **Ethernet (10BASE T, 100BASE TX, 1000BASE T)**, **Wi Fi (802.11a/b/g/n/ac/ax)** and **Fiber Optic (OS1, OS2, OS3)**. These standards define voltage levels, cable types, and data rates.

Data Link Layer

At this layer, protocols manage node-to-node communication and error detection. **Ethernet**, **PPP (Point to Point Protocol)**, and **Switching** mechanisms like VLAN tagging (802.1Q) operate here. The Data Link Layer ensures that frames are delivered correctly and in order.

Network Layer

Network Layer protocols route packets across multiple networks. The most ubiquitous protocol is the **Internet Protocol (IP)**, with its two main versions: IPv4 and IPv6. Other protocols include **ICMP (Internet Control Message Protocol)** for diagnostics and **IGMP (Internet Group Management Protocol)** for multicast.

Transport Layer

Transport protocols guarantee end to end delivery. **TCP (Transmission Control Protocol)** provides reliable, ordered, and error checked delivery, while **UDP (User Datagram Protocol)** offers low latency, connectionless

communication suitable for streaming and gaming.

Session Layer

This layer manages sessions between applications. Protocols such as **NetBIOS** and **RPC (Remote Procedure Call)** operate here, establishing, maintaining, and terminating connections.

Presentation Layer

Presentation Layer protocols handle data representation, encryption, and compression. Examples include **JPEG, MPEG, ASCII**, and **SSL/TLS** (though SSL/TLS is often considered part of the Application Layer in practice).

Application Layer

The topmost layer hosts protocols that directly interact with software applications. These include **HTTP, HTTPS, FTP, SMTP, DNS, SSH, Telnet, SNMP, LDAP, RDP, MQTT, CoAP**, and many more. The Application Layer protocols are the ones most users encounter daily.

Key Protocols in the Internet Protocol Suite (TCP/IP)

The Internet Protocol Suite, also known as TCP/IP, is the foundational architecture that powers the modern internet. Unlike the OSI model, TCP/IP is a pragmatic set of protocols that evolved from real-world implementations.

IP (Internet Protocol)

IP is the core addressing and routing protocol. IPv4, with its 32 bit address space, remains dominant, but IPv6, featuring 128 bit addresses, is steadily gaining traction to address the exhaustion of IPv4 addresses. IP handles packet forwarding, fragmentation, and reassembly.

TCP (Transmission Control Protocol)

TCP ensures reliable, ordered, and error checked delivery of data streams. It performs three way handshakes, flow control via sliding windows, and congestion control using algorithms like **TCP Reno** and **TCP Cubic**.

UDP (User Datagram Protocol)

UDP offers a lightweight, connectionless alternative to TCP. It's ideal for time sensitive applications such as VoIP, live streaming, and online gaming where occasional packet loss is preferable to latency introduced by retransmissions.

HTTP/HTTPS

HTTP (Hypertext Transfer Protocol) is the backbone of the web, enabling browsers to request and receive web pages. HTTPS extends HTTP with SSL/TLS encryption, ensuring confidentiality and integrity.

FTP (File Transfer Protocol)

FTP facilitates file uploads and downloads between clients and servers. While secure variants like SFTP (SSH File Transfer Protocol) and FTPS (FTP Secure) are preferred today, traditional FTP remains in use in legacy systems.

SMTP (Simple Mail Transfer Protocol)

SMTP is the standard protocol for sending email across networks. It works in tandem with **POP3** and **IMAP**for retrieving messages.

DNS (Domain Name System)

DNS translates human readable domain names into IP addresses. It uses a hierarchical distributed database, enabling efficient and resilient name resolution.

DHCP (Dynamic Host Configuration Protocol)

DHCP automatically assigns IP addresses and network configuration parameters to devices, simplifying network administration.

ARP (Address Resolution Protocol)

ARP maps IP addresses to MAC addresses within a local network segment, enabling devices to locate each other at the Data Link Layer.

ICMP (Internet Control Message Protocol)

ICMP provides diagnostic and error reporting messages, such as those generated by the popular **ping** command.

Other Important Protocols Across Layers

Beyond the core TCP/IP stack, a wide array of protocols address specific needs across all OSI layers.

Link Layer Protocols

- Ethernet (IEEE 802.3) – The dominant wired LAN standard.
- Wi Fi (IEEE 802.11) – Wireless LAN standard supporting multiple frequency bands and security suites.
- PPP (Point to Point Protocol) – Used for dial up and DSL connections.
- SLIP (Serial Line Internet Protocol) – A simpler, legacy serial connection protocol.

Transport Layer Protocols

- SCTP (Stream Control Transmission Protocol) – Provides multi streaming and multi homing, useful for telecom signaling.
- QUIC (Quick UDP Internet Connections) – A modern transport protocol built on UDP, offering lower latency and built in encryption, primarily used by HTTP/3.

Application Layer Protocols

- SNMP (Simple Network Management Protocol) – Used for monitoring and managing network devices.
- LDAP (Lightweight Directory Access Protocol) – Manages directory information services.
- SSH (Secure Shell) – Provides encrypted command line access to remote systems.
- RDP (Remote Desktop Protocol) – Enables graphical remote desktop sessions.
- Telnet – An older, unencrypted remote access protocol.
- MQTT (Message Queuing Telemetry Transport) – Lightweight publish subscribe messaging for IoT.
- CoAP (Constrained Application Protocol) – Designed for low power, resource constrained devices.

Security Protocols and Encryption

Security is paramount in networking. Protocols at various layers provide encryption, authentication, and integrity checks to protect data.

SSL/TLS (Secure Sockets Layer / Transport Layer Security)

SSL/TLS secures data in transit, especially for web traffic (HTTPS). It negotiates encryption ciphers, authenticates servers (and optionally clients), and protects against eavesdropping and tampering.

IPsec (Internet Protocol Security)

IPsec operates at the Network Layer, securing all IP traffic. It can be deployed in two modes: **Transport** (end to end) and **Tunnel** (site to site VPNs).

Kerberos

Kerberos is a ticket based authentication protocol used in enterprise environments, providing mutual authentication between clients and servers.

WPA3 (Wi Fi Protected Access 3)

WPA3 enhances Wi Fi security with improved key management and protection against offline password attacks.

Emerging Protocols and Future Trends

Networking technology is constantly evolving. Several emerging protocols promise to address the demands of next generation applications, such as high speed 5G, the Internet of Things (IoT), and cloud services.

HTTP/3 and QUIC

HTTP/3, built on QUIC, reduces latency by eliminating the TCP handshake and providing multiplexed streams over UDP. It's already being adopted by major browsers and content delivery networks.

IPv6 Adoption

IPv6's vast address space, improved routing, and built in security features make it essential for the future of the internet, especially as IoT devices proliferate.

5G and Edge Computing

5G introduces new protocols like **5G NR (New Radio)** and **NG RAN (Next Generation Radio Access Network)** facilitating low latency, high throughput connections. Edge computing brings computation closer to data sources, reducing reliance on distant data centers.

IoT Protocols

Baca Juga (Artikel Terkait)

- **automaker mini software version v8 erptoboss**
  URL: http://directnilecruiseegypt.com/automaker-mini-software-version-v8-erptoboss.pdf
- **automata and computability**
  URL: http://directnilecruiseegypt.com/automata-and-computability.pdf
- **automata and languages theory and applications**
  URL: http://directnilecruiseegypt.com/automata-and-languages-theory-and-applications.pdf
- **automata and mechanical toys**
  URL: http://directnilecruiseegypt.com/automata-and-mechanical-toys.pdf

Tags: #protocols #used #computer #networking