

UNIT 6

The Application Layer

(5 Hours) — Computer Networking (CACS303)

The Application Layer is the topmost layer of both the OSI model and the TCP/IP model, and it is the layer that end users and their software actually interact with. It provides the interface between network communication and user-facing software — web browsers, email clients, file transfer utilities — and defines the protocols that let those programs exchange meaningful data over the network. This unit covers the functions of the application layer, the major application-layer protocols in everyday use, and the tools used to monitor and analyze network traffic.

6.1 Functions of the Application Layer

The application layer does not carry out networking tasks such as routing or reliable delivery itself — those are handled by lower layers. Instead, it defines how application programs on different hosts cooperate and communicate meaningfully. Its principal functions are:

- **Network Virtual Terminal:** Allowing a user to log on to a remote host and interact with it as though the user's terminal were directly attached to it (e.g. TELNET).
- **File Transfer, Access, and Management:** Allowing a user to access files on a remote host, retrieve files, or manage files remotely (e.g. FTP).
- **Mail Services:** Providing the basis for email storage, forwarding, and retrieval across the network (e.g. SMTP, POP3, IMAP).
- **Directory Services:** Providing distributed access to global information about various objects and services, most notably translating human-readable names into network addresses (DNS).
- **Dynamic Host Configuration:** Automatically assigning IP addresses and other network configuration parameters to hosts joining a network (DHCP).
- **World Wide Web Access:** Providing a hypertext-based system for browsing and retrieving linked documents and resources across the Internet (HTTP/HTTPS).
- **Network Management:** Allowing administrators to monitor, configure, and troubleshoot devices across the network (SNMP and related tools).
- **Presentation and Encoding Support:** Working with data representation concerns such as encryption, compression, and character encoding so applications can exchange data meaningfully regardless of the underlying system differences.

Most application-layer protocols follow a client-server model: a client program initiates a request for a service, and a server program — typically running continuously and listening on a well-known port — responds to that request.

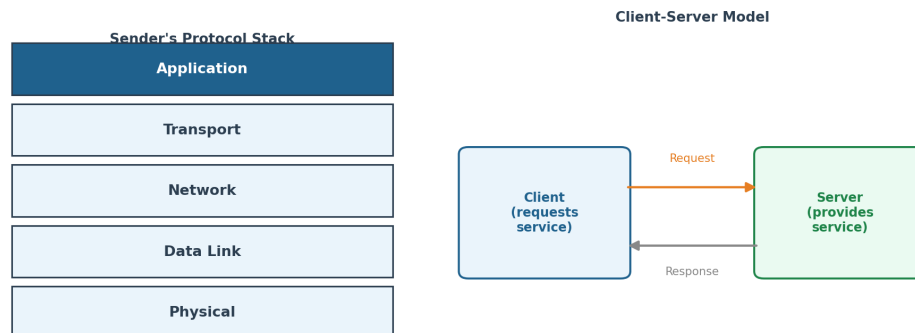


Figure 6.1: The application layer sits atop the protocol stack, and most of its protocols follow the client-server model

Key Takeaways — 6.1

- ✓ The application layer is where user-facing network software and protocols operate.
- ✓ It provides services such as remote login, file transfer, email, naming, and web access.
- ✓ Most application-layer protocols use a request-response client-server model.

6.2 Application Layer Protocols

DNS — Domain Name System

Humans find it far easier to remember names such as `www.example.com` than numeric IP addresses. DNS is a distributed, hierarchical naming system that translates domain names into IP addresses (and vice versa). The DNS namespace is organized as an inverted tree: a root level, below it top-level domains (TLDs) such as `.com`, `.org`, and country codes like `.np`, and below those the domains delegated to individual organizations. Resolution is typically iterative: a resolver starts at a root server, is referred to the appropriate TLD server, and finally to the authoritative server for the specific domain, which holds the actual DNS records.

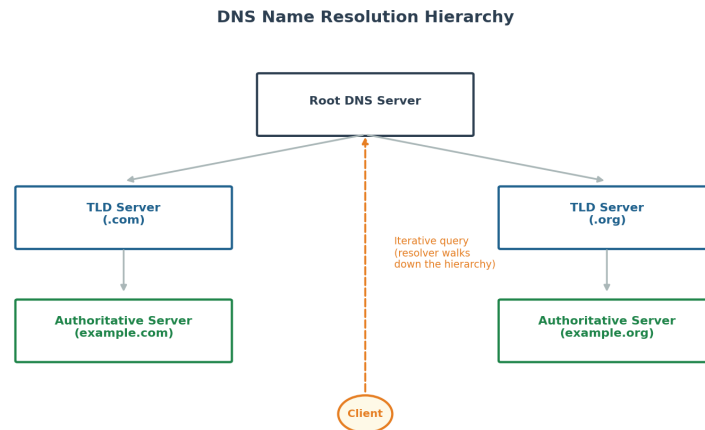


Figure 6.2: DNS name resolution hierarchy

Note: DNS runs mainly over UDP port 53 for quick lookups, falling back to TCP port 53 for larger transfers such as zone transfers between DNS servers.

DHCP — Dynamic Host Configuration Protocol

DHCP automatically assigns IP addresses and related configuration information (subnet mask, default gateway, DNS server addresses) to hosts as they join a network, removing the need for manual configuration. The typical exchange, often remembered by the acronym DORA, involves four messages:

- Discover: The client broadcasts a request looking for any DHCP server.
- Offer: A DHCP server responds, offering an available IP address and lease terms.
- Request: The client broadcasts a message accepting one particular offer.
- Acknowledge: The chosen server confirms the lease, finalizing the assignment.

WWW, HTTP, and HTTPS

The World Wide Web (WWW) is a system of interlinked hypertext documents and resources, identified by URLs and accessed over the Internet. The Hypertext Transfer Protocol (HTTP) is the application-layer protocol that governs how web browsers (clients) and web servers exchange requests and responses for these resources. HTTP is a stateless, request-response protocol: the client sends a request (such as GET or POST) for a resource, and the server replies with a status code and, typically, the requested content.

HTTP Request-Response Cycle



Figure 6.3: A basic HTTP request-response cycle

HTTPS (HTTP Secure) is HTTP layered over an encrypted connection (TLS/SSL). It protects the confidentiality and integrity of data in transit, and also allows the client to verify the identity of the server via digital certificates. HTTPS normally uses port 443, whereas plain HTTP uses port 80.

Aspect	HTTP	HTTPS
Security	No encryption — data sent in plaintext	Encrypted using TLS/SSL
Default port	80	443
Server authentication	None	Verified via digital certificate
Typical use	Non-sensitive, public content	Login pages, payments, sensitive data

TELNET

TELNET (Telecommunication Network) provides a bidirectional, text-based remote terminal connection, allowing a user on one host to log in and run commands on a remote host as if sitting directly at its console. A significant drawback of TELNET is that it transmits data — including login credentials — in plaintext, making it insecure over untrusted networks. It has largely been replaced by SSH (Secure Shell), which provides the same remote-login functionality with encryption.

FTP — File Transfer Protocol

FTP is used to transfer files between a client and a server. It is unusual among application-layer protocols in that it uses two separate TCP connections: a control connection (port 21), which stays open for the duration of the session and carries commands and responses, and a separate data connection (typically port 20 in active mode), which is opened only when a file transfer or directory listing actually takes place and is closed once that transfer finishes.

Note: Because FTP normally sends usernames, passwords, and file contents in plaintext, secure alternatives such as FTPS (FTP over TLS) or SFTP (FTP over SSH) are preferred for sensitive transfers.

SMTP, POP3, and IMAP — Email Protocols

Sending and retrieving email involves a combination of protocols, each responsible for a different part of the journey.

- **SMTP (Simple Mail Transfer Protocol):** Used to send mail from a client to its mail server, and to relay mail between mail servers, moving it closer to the recipient. SMTP uses port 25 (or 587 for authenticated client submission).
- **POP3 (Post Office Protocol version 3):** Used by a mail client to retrieve messages from the recipient's mail server. By default, POP3 downloads messages to the client and removes them from the server, making it best suited to checking mail from a single device.
- **IMAP (Internet Message Access Protocol):** Also used to retrieve mail, but messages remain on the server and are simply synchronized with the client, allowing the same mailbox to be accessed consistently from multiple devices.

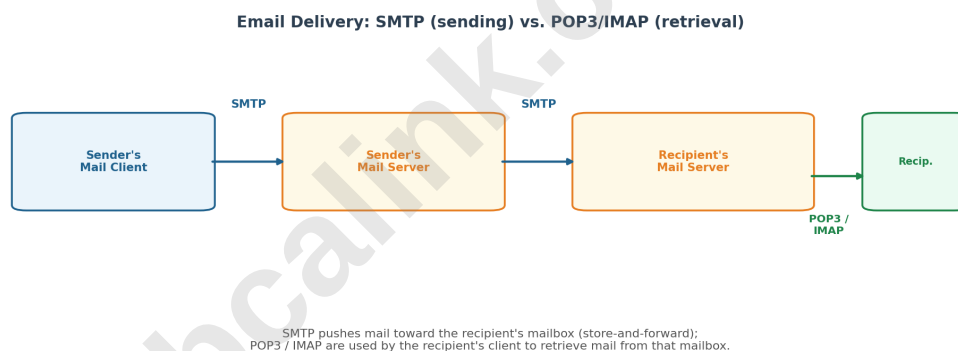


Figure 6.4: SMTP is used to send/relay mail toward the recipient's server; POP3/IMAP are used by the recipient to retrieve it

Aspect	POP3	IMAP
Mail storage	Typically downloaded and removed from server	Remains on the server
Multi-device access	Not well suited (mail moves to one client)	Well suited — mailbox stays in sync
Offline access	Full messages available offline after download	Requires periodic sync or caching
Default port	110 (995 for POP3S)	143 (993 for IMAPS)

Key Takeaways — 6.2

- ✓ DNS resolves domain names to IP addresses through a hierarchical server structure.
- ✓ DHCP automatically assigns IP configuration to hosts via the Discover-Offer-Request-Acknowledge exchange.
- ✓ HTTP/HTTPS govern web browsing; HTTPS adds TLS encryption and server authentication.
- ✓ TELNET and FTP are older, plaintext protocols for remote login and file transfer.
- ✓ SMTP sends/relays mail; POP3 downloads and removes mail; IMAP keeps mail synced on the server.

6.3 Concept of Traffic Analyzers

Beyond simply using the network, administrators need tools to monitor traffic, measure performance, and diagnose problems. This is the role of traffic analyzers and network management protocols.

SNMP — Simple Network Management Protocol

SNMP is the application-layer protocol underlying most network monitoring tools. It defines three main components: a central SNMP Manager (the monitoring station), SNMP Agents running on managed devices (routers, switches, servers), and a Management Information Base (MIB) — a structured database on each device describing the variables (counters, statistics, configuration values) that can be queried. The manager periodically sends GET requests to agents to read these variables, can send SET requests to change configuration, and agents can send unsolicited TRAP messages to alert the manager of significant events.

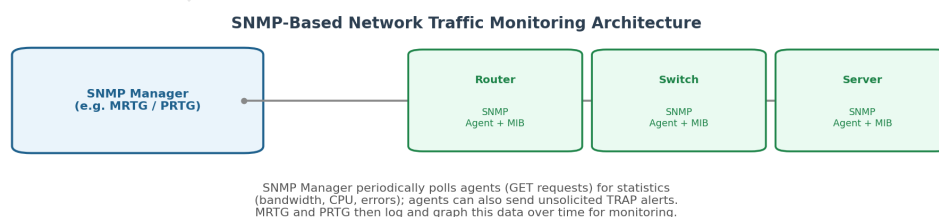


Figure 6.5: SNMP manager-agent architecture used by tools like MRTG and PRTG

MRTG — Multi Router Traffic Grapher

MRTG is a widely used, free tool that polls network devices (typically via SNMP) at regular intervals — commonly every 5 minutes — to collect interface traffic statistics, and generates HTML pages containing graphs of traffic load over time (daily, weekly, monthly, and yearly views). It is lightweight and simple, making it a long-standing choice for basic bandwidth monitoring.

PRTG — Paessler Router Traffic Grapher

PRTG is a more feature-rich, commercial network monitoring solution that also relies heavily on SNMP (alongside other methods such as WMI, packet sniffing, and flow protocols like NetFlow). It provides a broader set of monitoring sensors covering bandwidth, uptime, CPU/memory usage, and application-specific metrics, along with dashboards, alerting, and reporting features beyond what MRTG offers.

Aspect	MRTG	PRTG
Cost / licensing	Free and open source	Commercial (with a limited free tier)
Monitoring scope	Primarily interface traffic (SNMP)	Broad — bandwidth, uptime, apps, etc.
Data collection	SNMP polling	SNMP, WMI, packet sniffing, NetFlow, and more
Interface	Simple static HTML graphs	Interactive dashboards and alerting

Packet Tracer

Cisco Packet Tracer is a network simulation tool rather than a live traffic analyzer — it lets students and administrators design, build, and test virtual network topologies (routers, switches, PCs, cabling) and observe how packets would flow through them, without needing physical hardware. It is widely used for learning networking concepts and validating designs before deployment, and supports step-by-step simulation of packet movement across a modeled topology.

Wireshark

Wireshark is a free, open-source packet analyzer (packet sniffer) that captures live traffic passing through a network interface and displays it in detail, decoded down to individual protocol fields. Unlike SNMP-based tools, which report summary statistics, Wireshark inspects the actual content and headers of packets, making it valuable for deep troubleshooting — diagnosing failed connections, inspecting handshakes (e.g. TCP three-way handshake, TLS negotiation), and detecting unusual or malicious traffic. It supports filtering (e.g. by protocol, IP address, or port) to isolate the traffic of interest from a large capture.

Example 6.1 — Choosing the Right Tool

A network administrator needs to (a) get a long-term graph of how much bandwidth a router's WAN link has used over the past month, and (b) figure out exactly why a specific application's connection is failing right now. Which tools are appropriate for each task?

Solution

(a) A long-term bandwidth trend is a monitoring task best suited to an SNMP-based traffic grapher such as MRTG or PRTG, which poll and log statistics over time.

(b) Diagnosing exactly why a specific connection is failing requires inspecting the actual packets exchanged, which calls for a packet analyzer such as Wireshark.

Key Takeaways — 6.3

- ✓ SNMP (manager, agents, MIB) underlies most network monitoring tools.
- ✓ MRTG and PRTG poll devices (mainly via SNMP) and graph traffic/performance over time.
- ✓ Packet Tracer is a simulation tool for designing and testing virtual network topologies.
- ✓ Wireshark captures and decodes live packets for detailed, real-time troubleshooting.

— *End of Unit 6* —