ABHYASMITRA.IN
STUDY NOTES

COMPUTER NETWORKS

Unit V — Application Layer Protocols & Case Studies

Topics Covered (09 Hours)

Principles of Application Layer Protocols
Client-Server vs. Peer-to-Peer Models
Web and HTTP (Requests, Responses & Cookies)
Non-Persistent vs. Persistent Connections & Caching
DNS Architecture (Name Spaces, Resource Records & Security)
Electronic Mail (SMTP, MIME, POP3, IMAP, & Webmail)
Core Network Services: FTP, TELNET, and DHCP
Network Management & SNMP Structure
Multimedia Streaming, P2P & Cloud Applications
Case Studies: DNS Spoofing, CDN Caching, and Enterprise SMTP

Compiled in a simple, easy-to-understand, book style format
for students of Computer Science and Engineering

© Copyright — abhyasmitra.in — All Rights Reserved

TABLE OF CONTENTS

5.1 Principles of the Application Layer

The Application Layer is the top layer in the network reference models. It interfaces directly with user software applications, defining the protocols they use to exchange data across network sockets.

Network Architecture Paradigms

Applications generally organize their communicating processes into one of two paradigms:

- **1. Client-Server Model:** A centralized model. An always-on host (the server) services requests from many other hosts (clients). Clients do not communicate directly with each other. The server typically has a fixed, well-known IP address. (Examples: Web servers, database servers).
- **2. Peer-to-Peer (P2P) Model:** A decentralized model. Communication occurs directly between arbitrary pairs of hosts, called peers. Peers are not owned by any central company; instead, they are personal computers located on the edges of the internet. The network scales organically: as more peers join, they add workload, but also provide additional file serving bandwidth. (Examples: BitTorrent, Skype).

5.2 Web and HTTP

The Hypertext Transfer Protocol (HTTP) is the foundation of the World Wide Web. It defines the structure of messages that web browsers (clients) and web servers exchange.

HTTP Connections

- **Non-Persistent Connection:** Each TCP connection handles exactly one request message and one response message. If a web page contains 10 images, 11 separate TCP connections must be opened and closed sequentially or in parallel, adding propagation delay (RTT overhead) for each file.
- **Persistent Connection:** The server leaves the TCP connection open after sending a response. Subsequent requests and responses between the same client and server can be sent over the same connection. In Persistent with Pipelining, the client can send requests back-to-back without waiting for responses, maximizing speed.

Cookies and Caching

HTTP is a stateless protocol—the server does not keep state memory about past client requests. To track user sessions, web servers use Cookies. A cookie is a small identification string sent in a header from the server, stored on the client's browser, and returned on every subsequent request.

Web Caching (Proxy Servers) stores copies of recently requested web pages closer to the client. When a browser requests a page, it is intercepted by the local proxy cache. If the page is stored there and is fresh, it is returned immediately, reducing backbone network traffic and server load.

Cache validation is managed using Conditional GET requests. The client sends a request containing the header 'If-Modified-Since' or 'If-None-Match' (using an ETag identifier). If the resource has not changed at the server, the server returns a lightweight '304 Not Modified' response without the body, saving bandwidth.

5.3 The Domain Name System (DNS)

While humans prefer symbolic names (like 'google.com'), routers route packets using numeric IP addresses. The Domain Name System (DNS) is a distributed database that translates these user-friendly hostnames into their corresponding logical IP addresses.

DNS Namespace Hierarchy

DNS is organized hierarchically as a tree structure of domains. The root node is managed by ICANN. Below the root are Top-Level Domains (TLDs like .com, .org, .edu, .in), followed by Second-Level Domains (like google.com, wikipedia.org). The database is split into zones managed by different organizations.

DNS Record Types

Record Type	Value Representation	Functional Role / Description
A	IPv4 address	Maps a hostname directly to a 32-bit IPv4 address.
AAAA	IPv6 address	Maps a hostname directly to a 128-bit IPv6 address.
NS	Authoritative domain name	Specifies the domain name of the authoritative name server for a zone.
MX	Mail server hostname	Identifies the mail server responsible for accepting emails on behalf of a domain.
CNAME	Canonical hostname	Specifies an alias name mapping to the true canonical domain name.

DNS Name Resolution

When a client queries DNS, it contacts a Local DNS Server (Resolver). If the name is not in the resolver's local cache, it queries the DNS hierarchy using one of two methods:

- **Recursive Query:** The client asks the local server, which takes full responsibility for finding the address by querying other servers on behalf of the client, returning a final answer.
- **Iterative Query:** The local server queries a root server, which replies with the address of a TLD server. The local server then queries the TLD server, which replies with the address of the authoritative server. The local server finally queries the authoritative server to get the IP.

5.4 Electronic Mail Systems

The Internet email system consists of three main components: User Agents (mail readers), Mail Servers (which store and forward mail), and protocols.

Core Email Protocols

- **SMTP (Simple Mail Transfer Protocol):** A connection-oriented, text-based protocol used to send email from a client user agent to a mail server, and between mail servers. It operates on TCP port 25.
- **MIME (Multipurpose Internet Mail Extensions):** Allows SMTP (which was originally designed for ASCII text only) to carry binary data, attachments, images, and non-ASCII character sets.
- **POP3 & IMAP:** Mail access protocols used by user agents to retrieve emails from their mail servers. POP3 (Post Office Protocol 3) downloads the emails to the client machine and usually deletes them from the server. IMAP (Internet Message Access Protocol) keeps all emails on the server, synchronizing folders across multiple devices.

5.5 Core Infrastructure Protocols

Several utility protocols are essential for daily network operations and administration.

- **DHCP (Dynamic Host Configuration Protocol):** Automatically assigns IP addresses, subnet masks, default gateways, and DNS server addresses to client devices as they join a network. It avoids manual configuration errors.
- **SNMP (Simple Network Management Protocol):** Used by network administrators to monitor and manage routers, switches, and servers. Administrators query Management Information Bases (MIBs) on devices to check CPU load, link status, or error rates.
- **FTP (File Transfer Protocol):** A legacy protocol for copying files between hosts. It uses two separate connections: a Control Connection (port 21) for commands and a Data Connection (port 20) for actual file transfer.
- **TELNET:** A legacy remote login utility. It sends all commands and passwords in cleartext over the network, making it highly insecure. It has been replaced by SSH (Secure Shell).

5.6 Application Layer Case Studies

Below are three case studies highlighting real-world security, performance, and architecture design in the application layer.

1. DNS Security Attacks (DNS Spoofing)

DNS Spoofing (or cache poisoning) is an attack where malicious DNS data is injected into a resolver's cache. When a user requests a site like 'bank.com', the resolver returns the IP address of a fake phishing site controlled by the attacker. Because DNS historically lacked encryption and validation, attackers could forge UDP response packets. To prevent this, DNSSEC (DNS Security Extensions) was introduced, using cryptographic signatures to verify the authenticity of DNS resource records.

2. HTTP Caching in CDNs (Content Delivery Networks)

A Content Delivery Network (CDN) is a massive network of proxy servers deployed in edge locations worldwide. CDNs use advanced HTTP caching rules. When a user requests a video or image, the CDN directs the client to the closest edge cache node. If the file is cached, it is served immediately. If not, the edge node fetches it from the origin server, caches it, and serves it. CDNs use HTTP headers like Cache-Control, ETag, and Max-Age to manage cache validation and expiration.

3. SMTP in Enterprise Email Systems

In large enterprises, email systems process millions of messages daily, requiring high security and availability. SMTP is configured with SPAM filtering, transport layer security (STARTTLS), and sender verification protocols. These include: SPF (Sender Policy Framework, listing authorized sender IPs in DNS), DKIM (DomainKeys Identified Mail, cryptographically signing headers), and DMARC (Domain-based Message Authentication, Reporting, and Conformance, specifying how receivers should handle failed SPF/DKIM checks).

Unit Summary

This unit explored the Application Layer and core internet protocols.

- The Application Layer defines protocols for user software processes communicating over network sockets.
- Paradigms include Client-Server (centralized) and Peer-to-Peer (decentralized, peer-to-peer).
- HTTP runs the web. Persistent connections reduce RTT overhead compared to legacy non-persistent ones.
- Cookies enable session state tracking, while Web Caching reduces network latency.
- DNS resolves domain names hierarchically using root, TLD, and authoritative servers.
- Email uses SMTP (sending), MIME (non-text attachments), and POP3/IMAP (retrieving mail).
- Utility protocols include DHCP (IP auto-config), SNMP (management), FTP (file transfer), and TELNET (insecure terminal login).
- Security and scale case studies highlight DNS spoofing (prevented by DNSSEC), CDNs (edge caching), and enterprise SMTP filters (SPF/DKIM/DMARC).

© Copyright — abhyasmitra.in — All Rights Reserved