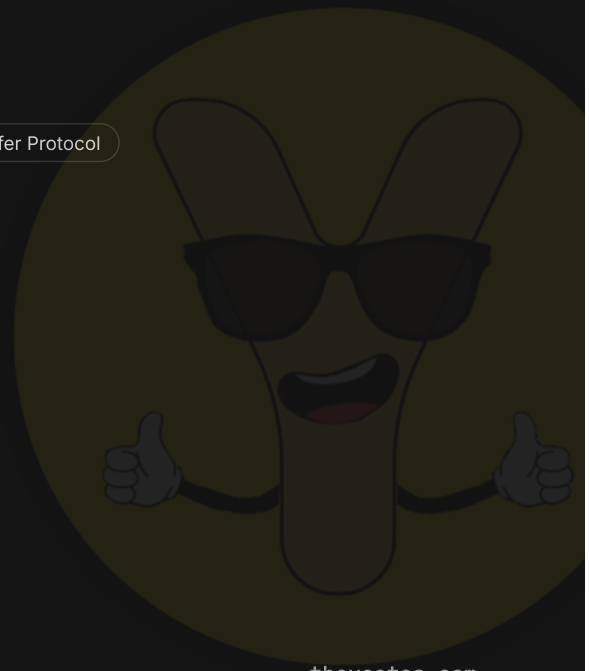
AKTU · 3RD YEAR · SEMESTER 6 · BCS603

Computer Networks

Unit 5 — Application Layer

- Domain Name System
- World Wide Web and Hyper Text Transfer Protocol
- Electronic mail
- File Transfer Protocol
- Remote login
- Network management
- Data compression
- Cryptography – basic concepts



DECODED BY

Chirag Jain

Founder, Ycotes · Gold Medalist in Artificial Intelligence, IIT Madras · taught 10,000+ students

theycotes.com

Domain Name System (DNS)

DOMAIN NAME SYSTEM (DNS)

A hierarchical and distributed naming system for computers, services, or any resource connected to the Internet or a private network. It translates human-readable domain names into numerical IP addresses.

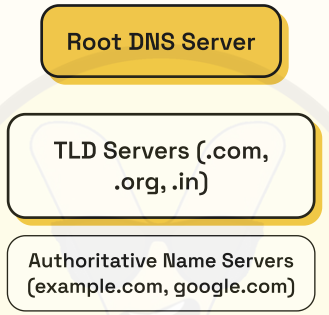
- It acts like an internet phonebook, allowing users to access websites and services using memorable names instead of complex IP addresses.
- DNS is crucial for the functioning of the internet, enabling communication between devices.

How DNS Resolution Works

The process of converting a domain name into an IP address involves several steps and different types of DNS servers.

- **1. User Request:** A user enters a domain name (e.g., www.example.com) into a web browser.
- **2. Local DNS Query:** The browser sends a query to the local DNS resolver (often provided by the ISP).
- **3. Root Server Query:** If the local resolver doesn't have the IP, it queries a Root DNS Server.
- **4. TLD Server Query:** The Root server directs the resolver to the Top-Level Domain (TLD) server (e.g., for .com).
- **5. Authoritative Server Query:** The TLD server directs to the Authoritative Name Server for the specific domain (e.g., example.com).
- **6. IP Address Return:** The Authoritative server provides the IP address to the local resolver, which then forwards it to the browser.

DNS Server Hierarchy



The hierarchical structure of DNS servers, where Root servers point to TLD servers, which in turn point to Authoritative Name Servers. Local DNS resolvers interact with this hierarchy.

World Wide Web (WWW)

The World Wide Web is a global system of interconnected computer networks that uses HTTP to transmit data.

- **Definition:** A system of interlinked hypertext documents and other web resources that are accessed via the Internet.
- **Key Components:**
- Web Browser
  - Software application used to access and view websites (e.g., Chrome, Firefox).
- Web Server
  - Stores website files and delivers them to browsers upon request.
- URL (Uniform Resource Locator)
  - The address used to locate a resource on the web (e.g., `https://www.example.com/page.html`).

Hypertext Transfer Protocol (HTTP)

HYPERTEXT TRANSFER PROTOCOL (HTTP)

An application-layer protocol for transmitting hypermedia documents, such as HTML. It is the foundation of data communication for the World Wide Web.

- HTTP follows a client-server model, where the web browser acts as the client and the web server acts as the server.
- It is a stateless protocol, meaning each request from a client to the server is treated as an independent transaction, without any memory of previous requests.

HTTP Request-Response Cycle



A typical HTTP interaction where a client sends a request to a server, which processes it and sends back a response.

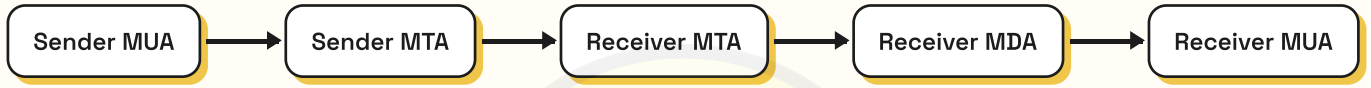
Common HTTP Request Methods

Method	Description	Purpose
GET	Requests data from a specified resource.	Retrieving information.
POST	Submits data to be processed to a specified resource.	Sending data to create/update resources.
PUT	Uploads a representation of the specified resource.	Updating an existing resource or creating a new one.
DELETE	Deletes the specified resource.	Removing a resource from the server.

Persistent vs. Non-Persistent HTTP

Feature	Non-Persistent HTTP	Persistent HTTP
Connection	A new TCP connection is established for each request/response pair.	A single TCP connection is maintained for multiple request/response pairs.
Overhead	High overhead due to repeated TCP connection setup and teardown.	Reduced overhead as TCP connection setup is done once.
Latency	Higher latency for multiple objects due to connection setup for each.	Lower latency for multiple objects as connection is reused.
Performance	Less efficient for retrieving multiple objects from the same server.	More efficient for retrieving multiple objects from the same server.
Example	HTTP/1.0 (default)	HTTP/1.1 (default)

Electronic Mail (Email) System Architecture



The flow of an email from sender to receiver, involving Mail User Agents (MUA), Mail Transfer Agents (MTA), and Mail Delivery Agents (MDA).

Simple Mail Transfer Protocol (SMTP)

SMTP is the standard protocol for sending email messages between servers.

- **Definition:** An application-layer protocol used for sending and receiving email messages.
- **Purpose:** Primarily used by Mail Transfer Agents (MTAs) to send mail from a source host to a destination host, and by Mail User Agents (MUAs) to send mail to an MTA.
- **Working:**
- Client-Server Model
  - An SMTP client (MUA or MTA) establishes a TCP connection on port 25 with an SMTP server (MTA).
- Commands
  - The client sends commands (e.g., `HELO`, `MAIL FROM`, `RCPT TO`, `DATA`) and the server responds with status codes.
- Message Transfer
  - The actual email message content is transferred after the `DATA` command.

POP3 vs. IMAP

Feature	POP3 (Post Office Protocol 3)	IMAP (Internet Message Access Protocol)
Purpose	Downloads emails from the server to a single device and typically deletes them from the server.	Synchronizes emails across multiple devices, keeping them on the server.
Storage	Emails are stored locally on the client device.	Emails remain on the server, with local copies for caching.
Access	Best for single-device access.	Ideal for accessing email from multiple devices.
Offline Access	Full offline access once emails are downloaded.	Limited offline access (cached emails).
Server Space	Frees up server space after download.	Consumes server space as emails are kept on server.
Folders	Limited support for server-side folders.	Full support for server-side folders and organization.

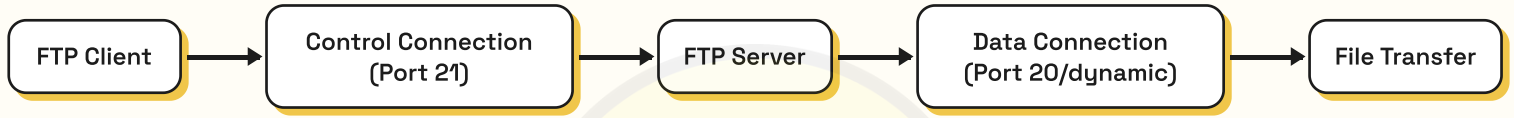
File Transfer Protocol (FTP)

FILE TRANSFER PROTOCOL (FTP)

An application-layer protocol used for transferring files between a client and a server on a computer network.

- FTP uses two separate TCP connections: one for control information (commands and replies) and another for data transfer.
- The control connection is established on port 21, and the data connection is typically established on port 20 (active mode) or a dynamic port (passive mode).

FTP Control and Data Connections



FTP uses separate control and data connections for robust and efficient file transfer. The control connection manages commands, while the data connection handles the actual file content.

Remote Login

Remote login allows a user to access and control a computer system from a different location over a network.

- **Concept:** Enables users to execute commands or access resources on a remote machine as if they were physically present at that machine.
- **Need:**
- System Administration
  - Managing servers and network devices from a central location.
- Resource Sharing
  - Accessing files or applications on a remote computer.
- Collaboration
  - Working on shared projects or accessing specialized software remotely.

Telnet vs. SSH for Remote Login

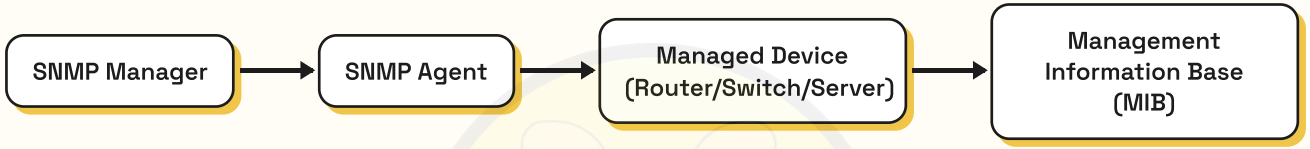
Feature	Telnet	SSH (Secure Shell)
Security	Sends data in plain text, highly insecure.	Encrypts all data, highly secure.
Port	Uses TCP port 23.	Uses TCP port 22.
Authentication	Basic password authentication, vulnerable to eavesdropping.	Strong authentication (passwords, public-key), resistant to attacks.
Data Integrity	No data integrity checks.	Ensures data integrity using cryptographic hashes.
Usage	Rarely used in modern networks due to security risks.	Widely used and recommended for secure remote access.

Network Management

Network management involves the processes and tools used to monitor, control, and maintain a computer network.

- **Definition:** The process of administering and managing computer networks, including fault analysis, performance management, security management, and accounting management.
- **Goals:**
- Fault Management
  - Detecting, isolating, correcting, and logging network faults.
- Configuration Management
  - Tracking network device configurations and software versions.
- Performance Management
  - Monitoring network performance (e.g., throughput, latency) to ensure optimal operation.
- Security Management
  - Controlling access to network resources and protecting data.
- Accounting Management
  - Tracking network resource usage for billing or capacity planning.

SNMP Architecture



SNMP uses a manager-agent model where the manager queries agents on managed devices to retrieve or set information stored in the Management Information Base (MIB).

Data Compression

DATA COMPRESSION

The process of encoding information using fewer bits than the original representation, reducing the size of data.

- **Purpose:** Reduces storage space, decreases transmission time over networks, and lowers bandwidth requirements.
- **Types:**
- Lossless Compression
  - Allows the original data to be perfectly reconstructed from the compressed data (e.g., ZIP, PNG).
- Lossy Compression
  - Achieves higher compression ratios by discarding some information, which cannot be recovered (e.g., JPEG, MP3).

Common Lossless Compression Techniques

Lossless compression methods are crucial where data integrity is paramount, such as text files or executable programs.

- **1. Run-Length Encoding (RLE):**
- Concept
  - Replaces sequences of identical data values with a count and the value itself (e.g., `AAAAABBC` becomes `5A2B1C`).
- Use Case
  - Effective for data with long runs of repeated characters, like simple graphics or fax images.
- **2. Huffman Coding:**
- Concept
  - Assigns variable-length codes to input characters, with shorter codes for more frequent characters and longer codes for less frequent ones. Builds a binary tree based on character frequencies.
- Algorithm Steps (Basic)
  - 1. Calculate frequency of each character. 2. Create a leaf node for each character and add to a min-priority queue. 3. While queue has more than one node, extract two nodes with lowest frequency, create a parent node with their combined frequency, and add it back. 4. Assign codes by traversing the tree.
- Use Case
  - Widely used in file formats like JPEG (for entropy coding), ZIP, and GZIP.

Cryptography – Basic Concepts

CRYPTOGRAPHY

The practice and study of techniques for secure communication in the presence of third parties (adversaries). It involves transforming information into an unreadable format (encryption) and back (decryption).

- **Goals of Cryptography (CIA Triad + Non-repudiation):**
- Confidentiality
  - Ensuring that information is accessible only to those authorized to have access.
- Integrity
  - Ensuring that information has not been altered or destroyed in an unauthorized manner.
- Authentication
  - Verifying the identity of a user, process, or device.
- Non-repudiation
  - Preventing a sender from denying having sent a message, or a receiver from denying having received a message.

Symmetric vs. Asymmetric Key Cryptography

Feature	Symmetric-Key Cryptography	Asymmetric-Key Cryptography (Public-Key)
Keys Used	Uses a single, shared secret key for both encryption and decryption.	Uses a pair of keys: a public key for encryption and a private key for decryption.
Key Distribution	Challenging to securely distribute the shared secret key.	Public key can be freely distributed; private key is kept secret.
Speed	Generally faster for bulk data encryption.	Computationally slower than symmetric-key algorithms.
Security	Requires secure key exchange; compromise of key compromises all data.	Stronger for key exchange and digital signatures.
Examples	AES (Advanced Encryption Standard), DES (Data Encryption Standard).	RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography).
Use Case	Encrypting large amounts of data.	Secure key exchange, digital signatures, small data encryption.

Hashing

Hashing is a one-way function that transforms data into a fixed-size string of characters, known as a hash value or message digest.

- **Definition:** A cryptographic hash function takes an input (or 'message') and returns a fixed-size alphanumeric string, which is a unique representation of the input.
- **Properties of Cryptographic Hash Functions:**
- One-way function
  - Computationally infeasible to reverse the hash to find the original input.
- Collision Resistance
  - Extremely difficult to find two different inputs that produce the same hash output.
- Deterministic
  - The same input will always produce the same hash output.
- **Use Cases:**
- Data Integrity
  - Verifying if a file has been altered by comparing its hash before and after transmission.
- Password Storage
  - Storing hashes of passwords instead of plain text passwords for security.
- Digital Signatures
  - Used to create a digest of a document before signing it.

Digital Signature Process



Digital signatures provide authentication, integrity, and non-repudiation by using cryptographic hashing and asymmetric-key encryption.

Exam Corner

Q1 Explain the working of the Domain Name System (DNS) with a suitable diagram. Discuss the different types of DNS servers.

Q2 Differentiate between Persistent and Non-Persistent HTTP. List and explain the common HTTP request methods.

Q3 Describe the architecture of an email system. Compare and contrast POP3 and IMAP protocols.

Q4 Explain the File Transfer Protocol (FTP) architecture and its operation. How does it manage control and data connections?

Q5 Compare Telnet and SSH protocols, highlighting their key differences, especially concerning security.

Q6 What is Network Management? Explain the components and basic operation of the Simple Network Management Protocol (SNMP) with a diagram.

Q7 Define data compression. Differentiate between lossless and lossy compression techniques, providing examples of each.

Q8 Explain the basic concepts of cryptography. Differentiate between symmetric-key and asymmetric-key cryptography, outlining their advantages and disadvantages.

Unit 5 done. You are exam-ready.

Revise the Exam corner once more, then open Unit 1 on theycotes.com. Every AKTU subject, unit by unit, free. Notes by Chirag Jain, Ycotes.

