A. Slow Learners

Application Layer Protocol Functions:

HTTP (Hypertext Transfer Protocol)
HTTP is used to transfer text, images, and multimedia from web servers to browsers. It operates over port 80 and is not encrypted.

HTTPS (Hypertext Transfer Protocol Secure)
HTTPS is HTTP over SSL/TLS, providing secure encrypted communication for web traffic. It runs on port 443 and is essential for protecting sensitive data.

FTP (File Transfer Protocol)
FTP enables the uploading and downloading of files between systems over a TCP/IP network. It uses ports 20 and 21 but lacks encryption.

SFTP (Secure File Transfer Protocol)
SFTP provides secure file transfer using SSH encryption over port 22. It ensures confidentiality and integrity of file exchanges.

SMTP (Simple Mail Transfer Protocol)
SMTP is used for sending emails between clients and servers. It runs on port 25 and is responsible for email delivery, especially outgoing mail.

IMAP (Internet Message Access Protocol)
IMAP allows users to access and manage emails on a remote mail server. It uses port 143 and supports server-side message storage and folder syncing.

POP3 (Post Office Protocol version 3)
POP3 downloads emails from a server to a local device and deletes them from the server. It operates over port 110 and is suitable for single-device use.

DNS (Domain Name System)
DNS resolves domain names to IP addresses, enabling user-friendly access to websites. It uses UDP/TCP port 53 and is essential for web browsing.

DHCP (Dynamic Host Configuration Protocol)
DHCP automatically assigns IP addresses and other network parameters to devices. It uses ports 67 (server) and 68 (client).

Telnet
Telnet allows users to remotely access and manage devices via command-line interface. It operates on port 23 and sends data in plain text.

SSH (Secure Shell)
SSH enables secure remote login and command execution over an encrypted connection. It uses port 22 and replaces insecure protocols like Telnet.

SNMP (Simple Network Management Protocol)
SNMP is used to monitor and manage network devices such as routers and switches. It operates over UDP ports 161 and 162.

TFTP (Trivial File Transfer Protocol)
TFTP is a simple protocol for transferring files with minimal overhead. It operates over UDP port 69 and lacks authentication and security.

B. Moderate Learners: Protocol-Purpose Matching

Protocol-Purpose Matching

Instructions: Match the listed protocols with their functions.

Protocol	Purpose
HTTP	Transfers web content in plaintext between server and client (non-secure)
HTTPS	Secures web communication using SSL/TLS encryption
FTP	Allows uploading/downloading files over TCP-based connection
SMTP	Sends emails from client to mail server and between servers
DNS	Converts human-readable domains to numeric IPs for routing
DHCP	Automatically provides IP configuration to hosts in network

C. Fast Learners

Activity 1: Packet Routing Simulation using Graph/Tree Structures

Instructions:

1. Use a weighted graph to represent routers and links
2. Assign weights to links based on cost/distance
3. Use Dijkstra's Algorithm to simulate routing table update from source router

Example:

Routers: R1, R2, R3, R4

Links: R1-R2 (2), R1-R3 (5), R2-R4 (1), R3-R4 (2)

From R1: shortest path to R4 is R1 → R2 → R4 (total cost: 3)

Activity 2: Technical Summary / Presentation Prepare a report/presentation covering:

ICMP (Internet Control Message Protocol)

Helps diagnose issues in networks
Tools like ping send echo requests, responses confirm reachability
traceroute maps route by measuring time from each hop

ARP (Address Resolution Protocol)

Resolves IP address to MAC address within LAN
Essential for communication on Ethernet networks
Uses broadcast to find MAC for a given IP in same subnet

RIP vs OSPF

RIP:

Simple distance-vector protocol, max 15 hops
Updates entire routing table every 30 sec
Slower convergence, suitable for small networks

OSPF:

Link-state protocol, maintains complete map of network
Sends triggered updates, uses Dijkstra's algorithm
Scalable, secure, efficient for large networks

Activity 3: HTTP vs HTTPS Case Study

Instructions: Analyze a real-world breach due to absence of HTTPS

Case study:

In 2015, a popular e-commerce site failed to implement HTTPS for its login page. This allowed attackers to intercept usernames and passwords over public Wi-Fi.

What Went Wrong:

HTTP transmits data in plaintext; any device in the network path can view it, without encryption, sensitive information is exposed to MITM attacks

Solutions:

Use HTTPS to encrypt communication using SSL/TLS, Implement HSTS (HTTP Strict Transport Security) and Use certificate pinning and secure cookies

Recommendations:

Always enforce HTTPS for user login and data transactions, Renew SSL certificates before expiration, educate developers on secure web practices and Enable automatic redirection from HTTP to HTTPS.

Some other breaches in past refer [The 18 biggest data breaches of the 21st century | CSO Online]