CHAPTER 2: COMMUNICATION AND INTERNET TECHNOLOGIES

2.1 PROTOCOLS

2.1.1 Introduction to Protocols

Definition: A protocol is a set of rules governing communication between computers. It ensures the computers that communicate understand each other.

Key Terms:

- **MAC Address:** Unique number assigned to each device's networking hardware worldwide
- **IP Address:** Unique number assigned to each node/networking device in a network
- **Port Number:** Software-generated number specifying an application or process communication endpoint

2.1.2 TCP/IP Protocol Suite

Four Layers:

Layer	Purpose
Application	Encodes the data being sent
Transport	Breaks data into packets, adds port numbers
Network/Internet	Adds IP addresses for routing
Link	Adds MAC addresses, handles transmission
Physical	Converts to signals for transmission

Data Flow - Sender Side:

1. **Application Layer:** Encodes data in appropriate format
2. **Transport Layer:** Creates packets with port numbers
3. **Network Layer:** Adds sender and receiver IP addresses
4. **Link Layer:** Formats into frames, adds error checking
5. **Physical Layer:** Converts to signals for transmission

Data Flow - Receiver Side: Reverse of sender side, stripping headers at each layer

2.1.3 Key Protocols

Protocol	Full Name	Purpose
HTTP	Hyper Text Transfer Protocol	Handles transmission of data to/from websites
HTTPS	Hyper Text Transfer Protocol Secure	Secure HTTP with encryption
FTP	File Transfer Protocol	Handles file transmission across networks
SMTP	Simple Mail Transfer Protocol	Sending emails (push protocol)
POP3	Post Office Protocol 3	Receiving emails (pull protocol)
IMAP	Internet Message Access Protocol	Advanced email retrieval
BitTorrent	-	Peer-to-peer file sharing

2.1.4 BitTorrent Protocol

Components:

- **Torrent File:** Contains details regarding the tracker
- **Tracker:** Server that keeps track of peers
- **Peers:** Users downloading and uploading simultaneously
- **Swarm:** Network of peers sharing the torrent
- **Seeding:** Uploading file after/complete download
- **Leeching:** Downloading without uploading

How It Works:

1. Peers obtain torrent file (small)
2. Torrent file points to tracker
3. Tracker lists all peers in swarm
4. Peers download chunks from each other
5. Peers upload chunks to other peers

2.2 CIRCUIT SWITCHING AND PACKET SWITCHING

2.2.1 Circuit Switching

Definition: A method of data transfer where a dedicated communication channel is established before transmission begins.

Characteristics:

- Dedicated path between sender and receiver
- Path remains open for entire duration
- Like traditional telephone system

Advantages:

- Guaranteed bandwidth
- Consistent quality
- No delay from routing decisions

Disadvantages:

- Inefficient if data is sporadic
- Connection setup takes time
- Line unavailable if circuit busy

Example Use:

- Traditional landline phones

2.2.2 Packet Switching

Definition: A method of data transfer where the message is broken into parts and sent over optimum routes to reach its destination.

Characteristics:

- Data divided into packets
- Each packet can take different route
- Packets reassembled at destination
- Used in the Internet

Advantages:

- Efficient use of network capacity
- If one route fails, packets can reroute
- Better for bursty data

Disadvantages:

- Packets may arrive out of order
- Variable delays
- More complex infrastructure

2.2.3 Router Function

Definition: A device that connects two or more computer networks and directs incoming packets to their receiver according to network traffic.

Functions:

- Examines packet destination IP address
- Determines best route for each packet
- Manages network traffic congestion
- Connects LAN to WAN

2.3 SSL/TLS

2.3.1 SSL and TLS

SSL (Secure Socket Layer):

- Provides secure communication
- Functions between TCP and application layer
- Creates "socket" for secure connection

TLS (Transport Layer Security):

- Improved version of SSL
- Provides encryption, compression, integrity checking

When to Use:

- Online shopping websites
- Online banking
- Any site requiring secure data transmission

Handshake Process:

1. Client sends request to server
2. Server sends digital certificate (includes public key)
3. Client validates certificate
4. Client generates session key, encrypts with server's public key
5. Server decrypts session key
6. Secure session established

Revision #1
Created 2026-03-16 12:15:37 UTC by Samuel Lee
Updated 2026-03-16 12:15:56 UTC by Samuel Lee