Connection-Oriented Protocols Vs Connectionless Protocols.

TCP/IP and OSI Model

IPV4 VS IPV6

Network Ports and their meaning

BY

OWOJORI MICHAEL

OLUWABUKOLA

MATRIC NO: RUN/CMP/24/17879

COMPUTER SCIENCE DEPARTMENT
COLLEGE OF POSTGRADUATE STUDIES
REDEEMER'S UNIVERSITY
EDE, OSUN STATE, NIGERIA

CSC 828 ASSIGNMENTS

LECTURER-IN-CHARGE

DR. S.A. ADEPOJU

Connection-Oriented Protocols

Definition: Communication requires a **connection to be established first** between sender and receiver before data transfer.

Analogy: Like a **phone call** – you dial, connect, then talk.

Examples: **TCP (Transmission Control Protocol), SCTP**.

Key Characteristics:

Reliable – ensures data is delivered in order and without errors (acknowledgements & retransmissions).

Handshake – connection setup (e.g., TCP's 3-way handshake).

Flow control & congestion control – manages data transmission speed.

Overhead – more complex, uses extra resources (headers, state tracking).

Use cases – web browsing (HTTP/HTTPS), email (SMTP/IMAP), file transfer (FTP), remote login (SSH).

Connectionless Protocols

Definition: No prior connection setup; data is sent as **independent packets (datagrams)**.

Analogy: Like sending a **postal letter** – you drop it in the box without checking if the receiver is ready.

Examples: **UDP (User Datagram Protocol), IP, ICMP**.

Key Characteristics:

Unreliable – no guarantee of delivery, order, or duplication control.

No handshake – sender just transmits.

Faster & lightweight – less overhead.

Best effort delivery – system tries, but no retransmission if lost.

Use cases – video streaming, online gaming, VoIP calls, DNS queries – where speed matters more than reliability.

TCP/IP Model (Transmission Control Protocol / Internet Protocol)

The TCP/IP model is a **conceptual framework** used to describe how data is transmitted over networks.

It was developed in the **1970s by DARPA** for ARPANET and became the foundation of the **Internet**.

It has **4 layers** (sometimes 5 if split further), each with specific roles:

1. Application Layer

Purpose: Provides services for end-user applications.

Functions:

Defines how applications interact with the network.

Handles things like file transfers, emails, and web browsing.

Examples of Protocols:

HTTP/HTTPS – web browsing

SMTP, POP3, IMAP – email

FTP – file transfer

DNS – domain name lookup

2. Transport Layer

Purpose: Ensures communication between applications on different devices.

Functions:

Error detection and correction.

Flow control and reliability.

Multiplexing (managing multiple conversations at once).

Main Protocols:

TCP (Transmission Control Protocol) – connection-oriented, reliable (web, email, file transfers).

UDP (User Datagram Protocol) – connectionless, faster but unreliable (streaming, gaming, VoIP).

3. Internet Layer

Purpose: Responsible for **logical addressing and routing** of packets across networks.

Functions:Assigns addresses to devices (IP addresses). Determines the best path for data to travel.

Main Protocols:

IP (Internet Protocol) – IPv4/IPv6 addressing and routing.

ICMP (Internet Control Message Protocol) – error reporting & diagnostics (e.g., ping).

ARP (Address Resolution Protocol) – maps IP addresses to MAC addresses.

4. Network Access / Link Layer

Purpose: Defines how data is physically sent across the medium (wires, Wi-Fi, fiber).

Functions:Converts packets into signals (electrical, optical, or radio). Handles physical addressing (MAC). Deals with hardware interfaces (network cards, switches, etc.).

Examples of Technologies/Protocols:

Ethernet, Wi-Fi, Bluetooth

PPP (Point-to-Point Protocol)

MAC addressing

The 7 Layers of the OSI Model

7. Application Layer (Top layer)

Purpose: Provides services directly to the user's applications.

Functions: Network services like email, web browsing, file transfer. Interface between user applications and the network.

Examples: HTTP, FTP, SMTP, DNS, Telnet.

6. Presentation Layer

Purpose: Ensures data is in a usable format for the application.

Functions: Data translation (e.g., ASCII ↔ Unicode). Data compression (reduce size).

Data encryption/decryption (e.g., SSL/TLS).

Examples: SSL/TLS, JPEG, MPEG, GIF.

5. Session Layer

Purpose: Manages sessions (conversations) between applications.

Functions: Establish, maintain, and terminate sessions. Synchronization (checkpoints in data transfer).

Examples: NetBIOS, RPC, PPTP.

4. Transport Layer

Purpose: Reliable end-to-end delivery of data.

Functions: Error detection and recovery. Flow control and segmentation. Multiplexing multiple conversations.

Examples: TCP (reliable), UDP (fast, unreliable).

3. Network Layer

Purpose: Logical addressing and routing of data between devices.

Functions: Path determination and logical addressing (IP addresses). Packet forwarding across networks.

Examples: IP (IPv4/IPv6), ICMP, OSPF, BGP.

2. Data Link Layer

Purpose: Reliable transmission of frames between nodes on the same network.

Functions:

Physical addressing (MAC addresses).

Error detection (checksums, CRC).

Organizes data into frames.

Examples: Ethernet, Wi-Fi (IEEE 802.11), PPP, Switches.

1. Physical Layer (Bottom layer)

Purpose: Transmits raw bits (0s and 1s) over the physical medium.

Functions:

Defines cables, signals, voltages, frequencies, and connectors.

Deals with network hardware (hubs, repeaters).

Examples: Cables, Fiber optics, Radio signals, Hubs.

What is IPv4?

IPv4 is the **fourth version of the Internet Protocol** and the first widely deployed version.

It was introduced in **1983** and became the **foundation of the Internet**.

It provides **unique addresses** for devices so they can communicate across networks.

IPv4 Address Structure

32-bit address → written in **dotted decimal** format.

Example: 192.168.1.1

Divided into **4 octets** (8 bits each), values range **0–255**.

Total possible addresses: **2^{32} = ~4.3 billion**.

IPv4 Address Classes

Originally, IPv4 used **classful addressing** (later replaced by CIDR – Classless Inter-Domain Routing).

Class	Range of First Octet	Example	Use
A	1–126	10.0.0.1	Very large networks
B	128–191	172.16.0.1	Medium networks
C	192–223	192.168.1.1	Small networks
D	224–239	Multicast	Special use
E	240–255	Experimental	Reserved

Features of IPv4

Uses **connectionless protocol** (best effort delivery, no guarantee).

Supports **fragmentation** (breaking large packets into smaller ones).

Header size: 20–60 bytes (variable).

Security: Limited (IPsec optional, not mandatory).

QoS (Quality of Service): Limited support.

Address exhaustion – 4.3 billion is not enough for billions of devices.

Requires NAT (Network Address Translation) to allow private networks to connect to the Internet.

Security not built-in (relies on add-ons like IPsec).

Broadcasts increase unnecessary traffic.

What is IPv6?

IPv6 is the **newest version of the Internet Protocol**, designed to replace IPv4.

Developed in the **late 1990s by the IETF (Internet Engineering Task Force)**.

Solves IPv4's **address exhaustion problem** and improves performance, efficiency, and security.

IPv6 Address Structure

128-bit address → written in **hexadecimal**, separated by colons (:).

Example:2001:0db8:85a3:0000:0000:8a2e:0370:7334

Can be **shortened**: Remove leading zeros: 2001:db8:85a3:0:0:8a2e:370:7334

Replace continuous zeros with :: (only once): 2001:db8:85a3::8a2e:370:7334

Total addresses: $2^{128} \approx 3.4 \times 10^{38}$ (practically unlimited).

Types of IPv6 Addresses

Unicast – one-to-one communication.

Global unicast: Public Internet address (similar to IPv4 public IP).

Link-local: Automatically assigned for local communication (fe80::/10).

Multicast – one-to-many communication (replaces IPv4 broadcast).

Anycast – one-to-nearest communication (delivered to the closest of multiple servers).

No **broadcast** in IPv6 (uses multicast instead).

IPv6 Features

Huge address space (128-bit vs IPv4's 32-bit).

Simplified header (fixed 40 bytes, faster processing).

Built-in IPsec (security features mandatory).

No need for NAT (every device can have a unique global address).

Auto-configuration (stateless address autoconfiguration – SLAAC).

Better QoS support with the Flow Label field.

Efficient routing – hierarchical addressing reduces routing table sizes.

Support for mobility and IoT – billions of devices can connect.

IPv6 Address Examples

Global unicast: 2001:db8::1 (Internet-routable).

Link-local: fe80::1 (used within the same LAN segment).

Multicast: ff02::1 (all nodes in a network).

Loopback: ::1 (same as 127.0.0.1 in IPv4).

What is a Network Port?

A **port** is a **logical number** used by computers to identify specific processes or network services.

It works like an **apartment number** in a building: the **IP address** is the building, and the **port number** is the apartment where data should go.

Ports allow multiple applications to share the same network connection.

How Ports Work

When data is sent over the Internet, it travels in **packets**.

Each packet contains:

Source IP + Source Port (where it's from).

Destination IP + Destination Port (where it should go).

Example: When you visit a website:

Your computer → uses a **random high port** (e.g., 49533).

Server (e.g., Google) → listens on **port 80 (HTTP)** or **443 (HTTPS)**.

Port Number Ranges

0 – 1023 → Well-Known Ports

Assigned to standard services (HTTP, FTP, DNS, etc.).

1024 – 49151 → Registered Ports

Used by software applications.

49152 – 65535 → Dynamic / Private / Ephemeral Ports

Temporary ports chosen by client apps for communication.

Common Network Ports & Their Meanings

Port Number	Protocol/Service	Use
20, 21	FTP (File Transfer Protocol)	File transfer
22	SSH (Secure Shell)	Secure remote login
23	Telnet	Unsecure remote login (legacy)
25	SMTP (Simple Mail Transfer Protocol)	Sending emails
53	DNS (Domain Name System)	Translates domain names to IPs
67, 68	DHCP	Automatic IP assignment
69	TFTP (Trivial FTP)	Simple file transfer
80	HTTP	Web browsing (insecure)
110	POP3	Retrieve emails (legacy)
143	IMAP	Manage emails
161, 162	SNMP	Network management/monitoring
389	LDAP	Directory services (Active Directory)
443	HTTPS	Secure web browsing (SSL/TLS)
445	SMB (Server Message Block)	Windows file/printer sharing
3389	RDP (Remote Desktop Protocol)	Remote access to Windows desktop

Why Ports Matter

Networking – allow multiple services on one machine (e.g., web server + mail server).

Firewalls – control traffic by allowing/blocking ports.

Security – attackers scan for open ports to exploit vulnerabilities.

Troubleshooting – checking if the right ports are open can fix connection issues.