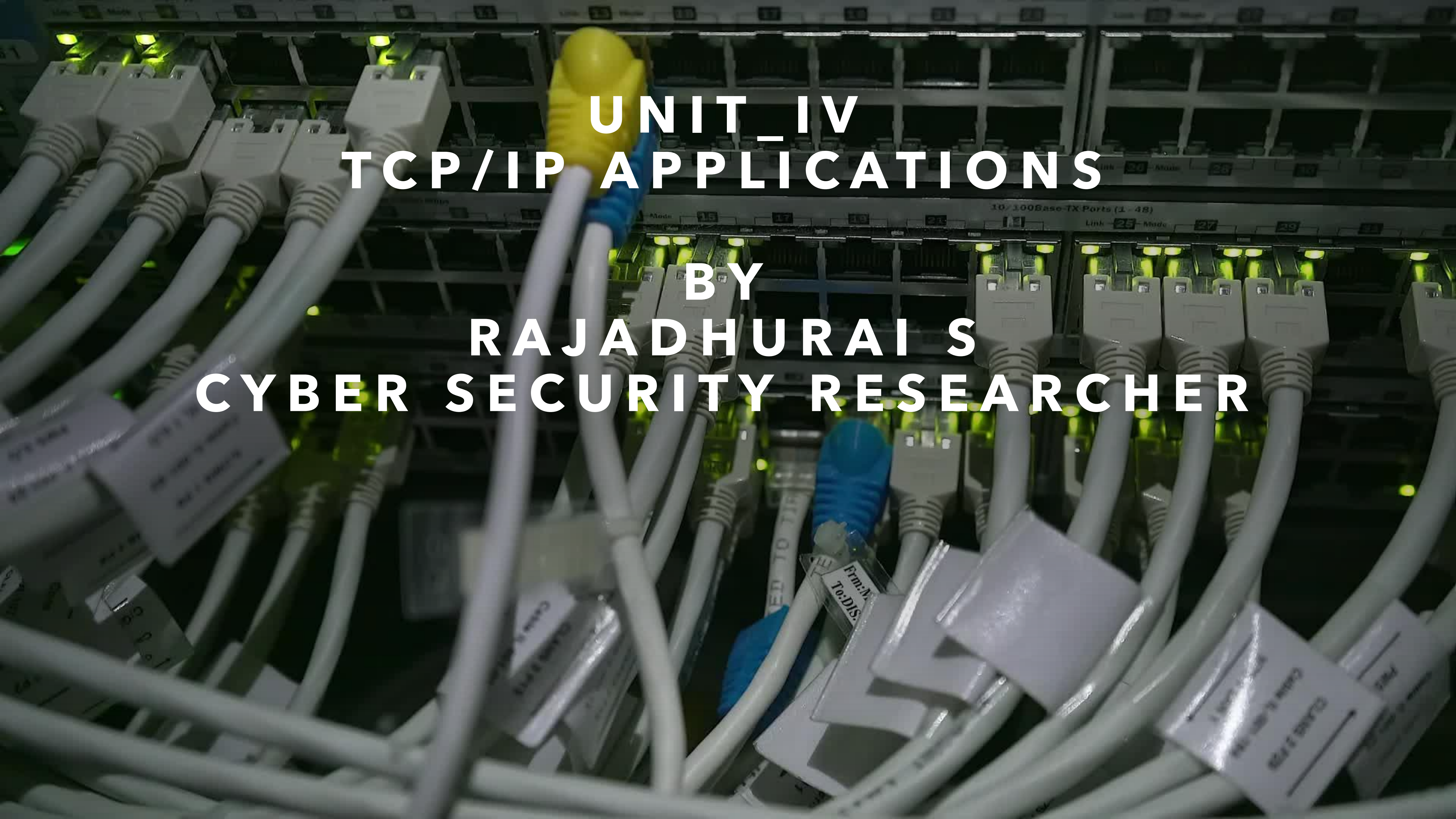


UNIT_IV
TCP/IP APPLICATIONS

BY
RAJADHURAI S
CYBER SECURITY RESEARCHER

AGENDA

- Origins of TCP/ IP and evolution of Internet
- IP Layers Vs OSI - IP number concepts.
- Network address
- Classes of Networks-Subnet masking
- Static and dynamic IP numbers
- UDP (User Datagram Protocol)
- Establishing a TCP session (Three way handshake)

ORIGINS OF TCP/ IP AND EVOLUTION OF INTERNET

ARPANET, or Advanced Research Projects Agency Network, Was a computer network that served as a precursor to the modern internet.

Purpose: ARPANET was developed by the U.S. Department of Defense's Advanced Research Projects Agency (ARPA) to enable communication and information sharing between government agencies and research institutions.

Technology

ARPANET was the first wide-area packet-switched network and one of the first to use the TCP/IP protocol suite. Packet switching allowed data to be broken down into smaller packets and transmitted across a decentralized network.

Timeline

ARPANET was in existence from 1969 to 1990.

Importance

ARPANET was a test bed for many internetworking technologies and served as the central backbone during the development of the internet.

Features

ARPANET introduced flow control mechanisms to prevent data overflow and network congestion, and it checked for errors to ensure the integrity of received data.

Initial communication protocols were basic and lacked the sophistication needed for scaling. Examples include the Network Control Protocol (NCP), which was ARPANET's first protocol.

Development of TCP/IP

- **1973:** Vint Cerf and Bob Kahn proposed the foundational concepts for what became Transmission Control Protocol (TCP). It aimed to ensure reliable communication between diverse networks.
- **1974:** Cerf and Kahn published a detailed paper describing TCP, focusing on reliable packet delivery.
- **1980:** TCP was split into TCP (handling data transport and reliability) and IP (responsible for addressing and routing).
- **1983:** ARPANET officially adopted TCP/IP as its standard, marking the protocol's practical deployment.

Evolution of the Internet:

1. Transition from ARPANET to the Internet

- **1980s:** The concept of inter-networking took off, linking independent networks into a larger "network of networks" using TCP/IP.
- **1984:** The Domain Name System (DNS) was introduced to replace hardcoded IP addresses with human-readable domain names (e.g., from "192.0.2.1" to "example.com").
- ARPANET transitioned into the Internet, supported by both academic and military funding.

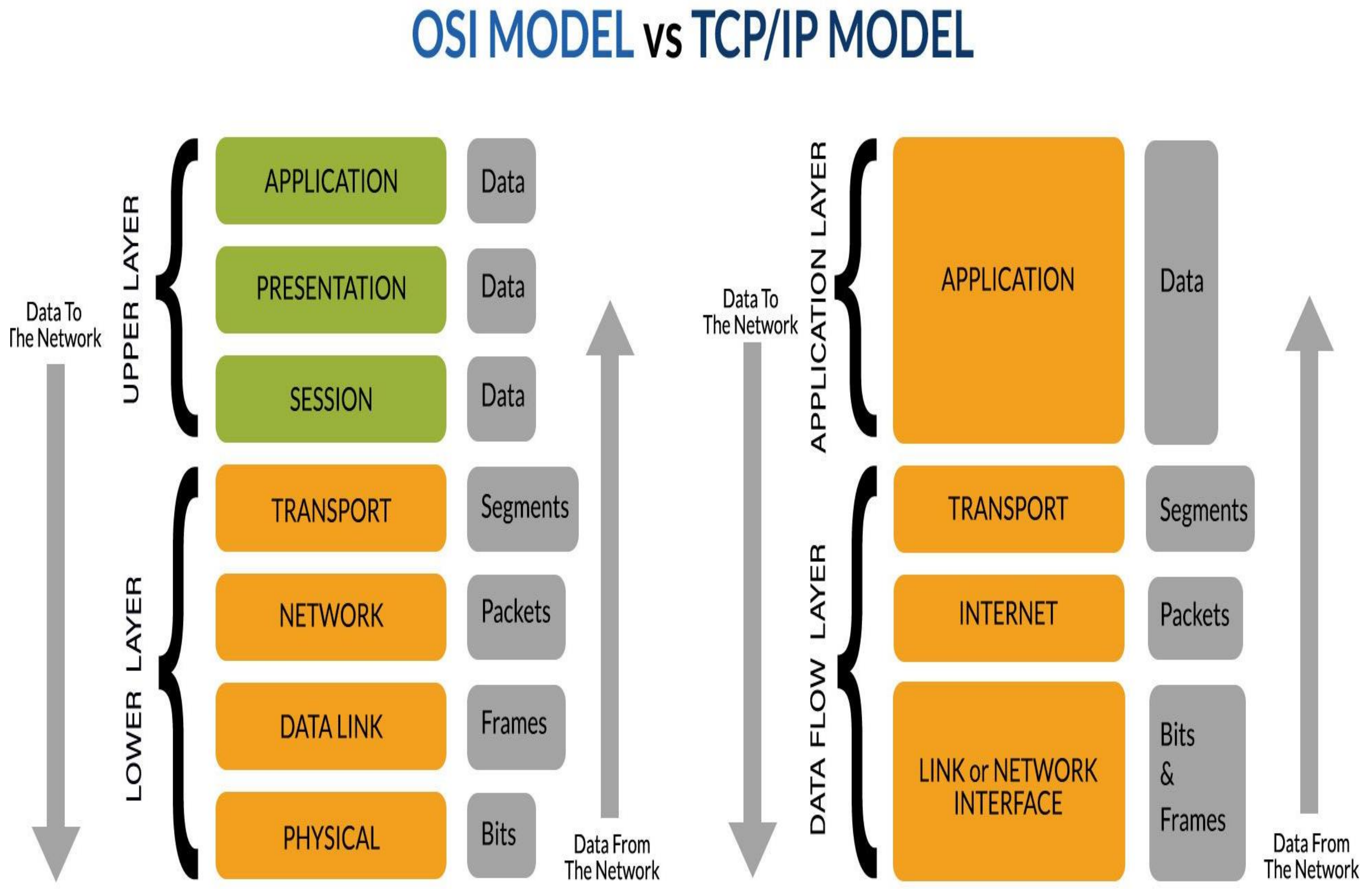
Significance of TCP/IP

TCP/IP remains the backbone of the modern Internet. It provides:

- **Scalability:** Supporting millions of devices globally.
- **Flexibility:** Adapting to new technologies and applications.
- **Interoperability:** Enabling diverse systems to communicate effectively.

IP LAYERS VS OSI - IP NUMBER CONCEPTS

The **IP layers in the TCP/IP model** and the **OSI (Open Systems Interconnection) model** serve as frameworks for understanding how networking protocols interact and operate.



Feature	TCP/IP Model	OSI Model
Layers	4	7
Focus	Practical Implementation	Conceptual Framework
Adoption	Widely used in real-world	Used as a reference model
Complexity	Simpler	More Detailed

TCP/IP Model:

The TCP/IP model is simpler and practical, consisting of **4 layers**:

1. **Application Layer**: Includes protocols like HTTP, FTP, and SMTP for user interaction and services.

2. **Transport Layer**: Ensures reliable data transfer using protocols like TCP (reliable) and UDP (unreliable).

3. **Internet Layer**: Manages addressing, routing, and packet delivery using IP.

4. **Network Interface Layer**: Handles hardware-level communication and physical connections.

Feature	TCP/IP Model	OSI Model
Layers	4	7
Focus	Practical Implementation	Conceptual Framework
Adoption	Widely used in real-world	Used as a reference model
Complexity	Simpler	More Detailed

OSI Model:

The OSI model is a theoretical framework with **7 layers**:

1. **Application**: User-facing services (e.g., HTTP, FTP).
2. **Presentation**: Data format translation and encryption.
3. **Session**: Establishes, manages, and terminates sessions.
4. **Transport**: Ensures end-to-end communication reliability (e.g., TCP).
5. **Network**: Handles logical addressing and routing (e.g., IP).
6. **Data Link**: Manages data frames and MAC addressing.
7. **Physical**: Handles raw bit transmission over physical media.

IP Number Concepts:

The Internet Protocol (IP) is central to the Internet Layer in TCP/IP. It uses IP numbers (or addresses) for communication.

Types of IP Addresses

1. **IPv4 Addresses**:
   - Format: 32-bit numeric address.
   - Representation: Dotted decimal (e.g., 192.168.1.1).
   - Range: About 4.3 billion addresses.
   - Example Classes:
     - Class A: Large networks (e.g., 10.0.0.0).
     - Class B: Medium networks (e.g., 172.16.0.0).
     - Class C: Small networks (e.g., 192.168.0.0).

IPv6 Addresses:

- Format: 128-bit alphanumeric address.
- Representation: Hexadecimal notation separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- Purpose: Solves IPv4 exhaustion and provides nearly unlimited addresses.

IP Address Components:

- Network Portion: Identifies the network (determined by the subnet mask or prefix length).

- Host Portion: Identifies a device within the network.

- **Special IP Ranges Private IPs**:

  - Used within private networks (e.g., 192.168.x.x, 10.x.x.x).**Public IPs**: Routable on the Internet.Loopback Address: Used for internal testing (127.0.0.1 for IPv4, ::1 for IPv6).

Integration of IP with TCP/IP and OSI:

•TCP/IP: IP functions as part of the Internet Layer, focusing on routing and addressing.

•OSI: IP is primarily associated with the Network Layer, which handles logical addressing and path determination.

Types of Network Addresses:

1.IP Address

•The most common type of network address, used in the Internet Protocol (IP) for identifying devices in a network.

•**IPv4**: 32-bit address written in dotted decimal format (e.g., **192.168.1.1**)

•**IPv6**: 128-bit address written in hexadecimal and separated by colons (e.g., 2001:0db8:85a3::8a2e:0370:7334).

2.MAC Address

•A physical address burned into the network interface card (NIC).

•48-bit or 64-bit address written in hexadecimal (e.g., 00:1A:2B:3C:4D:5E).

•Used in the Data Link Layer for communication within a local network.

•**Broadcast Address**

•An address that sends data to all devices in a network.

•In IPv4, a broadcast address for the network 192.168.1.0/24 is 192.168.1.255.

•**Network Address**

•Identifies the network itself, excluding the host portion of an IP address.

•Example: In 192.168.1.0/24, the network address is 192.168.1.0.

•**Subnet Address**

•A portion of a larger network divided into smaller sub-networks.

•Defined by a **subnet mask** (e.g., 255.255.255.0) or **CIDR notation** (e.g., /24).

•**Default Gateway**

•The address of a router that connects the local network to external networks (e.g., the Internet).

•Example: 192.168.1.1 is commonly used as a default gateway.

•How to Determine a Network AddressTo calculate the network address:Convert the IP address and subnet mask to binary.Perform a bitwise AND operation between them.Example:IP Address: **192.168.1.10** → 11000000.10101000.00000001.00001010

•Subnet Mask: **255.255.255.0** → 11111111.11111111.11111111.00000000Network Address: 11000000.10101000.00000001.00000000 → **192.168.1.0**

CLASSES OF NETWORKS- SUBNET MASKING

Classes of Networks:

In computer networking, IP addresses are grouped into classes based on their range and intended use. The most common addressing standard is IPv4, which divides addresses into five primary classes (A, B, C, D, and E). Each class has a specific purpose and default subnet mask:

Class A

- **Range:** 0.0.0.0 to 127.255.255.255
- **Default Subnet Mask:** 255.0.0.0 (or /8)
- **Number of Networks:** 128 (0–127, but 127 is reserved for loopback addresses)
- **Number of Hosts per Network:** ~16.7 million
- **Purpose:** Designed for large organizations with a significant number of devices.

Class B

- **Range:** 128.0.0.0 to 191.255.255.255
- **Default Subnet Mask:** 255.255.0.0 (or /16)
- **Number of Networks:** 16,384
- **Number of Hosts per Network:** ~65,000
- **Purpose:** Suitable for medium-sized organizations.

Class C

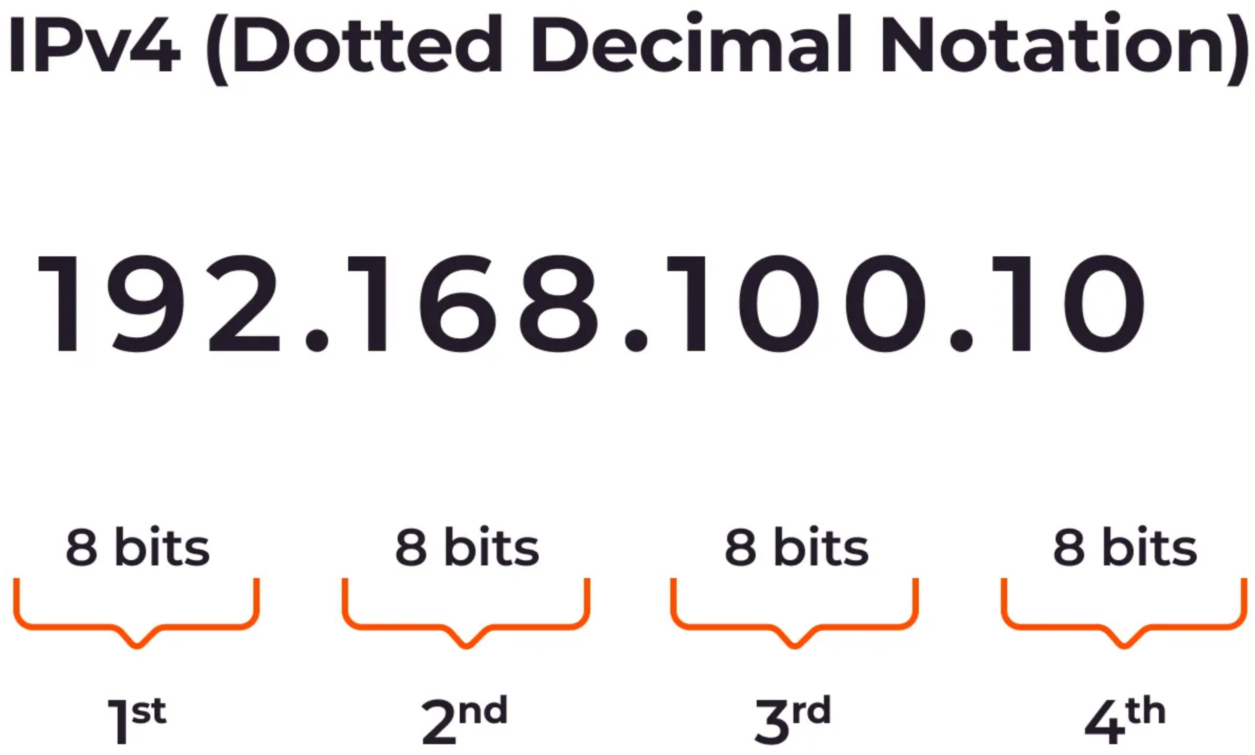
- **Range:** 192.0.0.0 to 223.255.255.255
- **Default Subnet Mask:** 255.255.255.0 (or /24)
- **Number of Networks:** ~2 million
- **Number of Hosts per Network:** 254
- **Purpose:** Commonly used for small businesses and private networks.

Class D (Multicast)

- **Range:** 224.0.0.0 to 239.255.255.255
- **Default Subnet Mask:** Not applicable
- **Purpose:** Reserved for multicast communication (e.g., streaming media or conferencing).

Class E (Experimental)

- **Range: 240.0.0.0 to 255.255.255.255**
- **Default Subnet Mask:** Not applicable
- **Purpose:** Reserved for experimental and research purposes.



IPv4 (Dotted Decimal Notation)

192.168.100.10

SUBNETTING

Subnet Masking

A subnet mask is used to divide an IP address into two parts:

1.Network Portion: Identifies the network.

2.Host Portion: Identifies individual devices (hosts) within the network.

Default Subnet Masks

Each class has a default subnet mask that determines the boundary between the network and host portions:

- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

Custom Subnet Masks

Custom subnet masks (variable-length subnet masking, or VLSM) are used to create smaller subnets, optimizing IP address allocation.

For example:

- Subnet mask 255.255.255.128 (or /25) splits a Class C network into two subnets, each with 126 usable host addresses.
- Subnet mask 255.255.255.192 (or /26) divides a Class C network into four subnets, each with 62 usable host addresses.

Subnetting Example

Given an IP address of 192.168.1.0/24:

Subnet mask: 255.255.255.0

Splitting into two subnets:

Subnet 1: 192.168.1.0/25 (hosts: 192.168.1.1 to 192.168.1.126)

Subnet 2: 192.168.1.128/25 (hosts: 192.168.1.129 to 192.168.1.254)

NEED FOR SUBNETTING

- Efficient Use of IP Addresses
- Improved Network Performance
- Enhanced Network Security
- Simplified Network Management
- Support for Hierarchical Addressing
- Facilitate Network Growth
- Compliance with IPv4 Addressing Limitations

Feature	Static IP Address	Dynamic IP Address
Assignment	Manually configured	Automatically assigned by DHCP
Change Frequency	Fixed, does not change	May change periodically
Ease of Use	Require manual efforts to set up	Fully automated
Cost	Often higher	Typically included in ISP package
Reliability	Highly reliable for critical services	Suitable for general purpose connectivity
Security	Easier to target for attacks	Harder to track due to IP changes

Static IP Address

A **static IP address** is a fixed IP address manually assigned to a device. It does not change over time unless manually reconfigured.

Features:

- **Permanence:** The IP address remains constant.
- **Manual Configuration:** Requires manual setup by a network administrator.
- **Best for Specific Use Cases:** Used for devices that require a consistent address.

Use Cases:

- **Web Servers:** Websites need a fixed IP for reliable DNS mapping.
- **Email Servers:** Ensures consistent communication.
- **CCTV Systems:** Static IPs allow remote access to surveillance systems.
- **Networked Printers:** Simplifies access for all users on a network.
- **Remote Access:** Facilitates easier setup of VPNs or remote desktop services.

Static IP Address

Advantages:

- Easier to configure devices requiring consistent connectivity.
- Better suited for hosting and services requiring DNS mappings.
- Simplifies troubleshooting as the IP address is predictable.

Disadvantages:

- Time-consuming to configure, especially for large networks.
- Limited flexibility if devices frequently join or leave the network.
- Typically, more expensive when assigned by ISPs.

Dynamic IP Address

A **dynamic IP address** is automatically assigned by a DHCP (Dynamic Host Configuration Protocol) server and can change over time.

Features:

- **Temporary Assignment:** The IP address may change periodically.
- **Automated Configuration:** DHCP assigns and manages IP addresses dynamically.
- **Common in Consumer Networks:** Used by most residential ISPs and private networks.

Use Cases:

- **Home Networks:** Simplifies setup for non-technical users.
- **Public Wi-Fi:** Efficient for networks with devices connecting and disconnecting frequently.
- **Corporate Networks:** Reduces administrative overhead for a large number of devices.

Advantages:

- Easy and quick to configure, reducing administrative tasks.
- Conserves IP address space by reassigning unused addresses.
- More cost-effective for end-users and ISPs.
- Enhanced security in some cases, as IP changes make tracking harder.

Disadvantages:

- Unpredictable changes in IP can disrupt services requiring consistent addresses.
- Harder to maintain for remote access or hosting without additional configuration (e.g., Dynamic DNS services).

Advantages:

- Easy and quick to configure, reducing administrative tasks.
- Conserves IP address space by reassigning unused addresses.
- More cost-effective for end-users and ISPs.
- Enhanced security in some cases, as IP changes make tracking harder.

Disadvantages:

- Unpredictable changes in IP can disrupt services requiring consistent addresses.
- Harder to maintain for remote access or hosting without additional configuration (e.g., Dynamic DNS services).

UDP (User Datagram Protocol) is one of the core protocols of the Internet Protocol Suite. It operates on top of the Internet Protocol (IP) and provides a lightweight, connectionless communication mechanism. UDP is particularly useful for applications where speed and low overhead are more critical than reliability.

Key Features of UDP:

1.Connectionless Protocol:

1. UDP does not establish a connection before sending data. This makes it faster but less reliable than TCP (Transmission Control Protocol).

2.No Error Correction:

1. It does not guarantee the delivery of packets, their order, or that they will not be duplicated. This is left to the application layer if needed.

3.Low Overhead:

1. UDP headers are only 8 bytes, which is significantly smaller than TCP headers. This reduces protocol overhead.

•**Broadcast and Multicast Support**:

•UDP can send messages to multiple recipients at once using broadcast or multicast, making it suitable for certain network applications.

•**Applications**:

•Commonly used for time-sensitive and loss-tolerant applications, such as:

- •Streaming media (audio, video)
- •Online multiplayer games
- •Voice over IP (VoIP)
- •Domain Name System (DNS) queries
- •Simple Network Management Protocol (SNMP)

Structure of a UDP Datagram:

A UDP datagram contains:

- **Source Port (16 bits)**: The port of the sending application.
- **Destination Port (16 bits)**: The port of the receiving application.
- **Length (16 bits)**: The length of the UDP header and data.
- **Checksum (16 bits)**: Used for error checking of the header and data.
- **Data**: The payload carried by the UDP datagram.

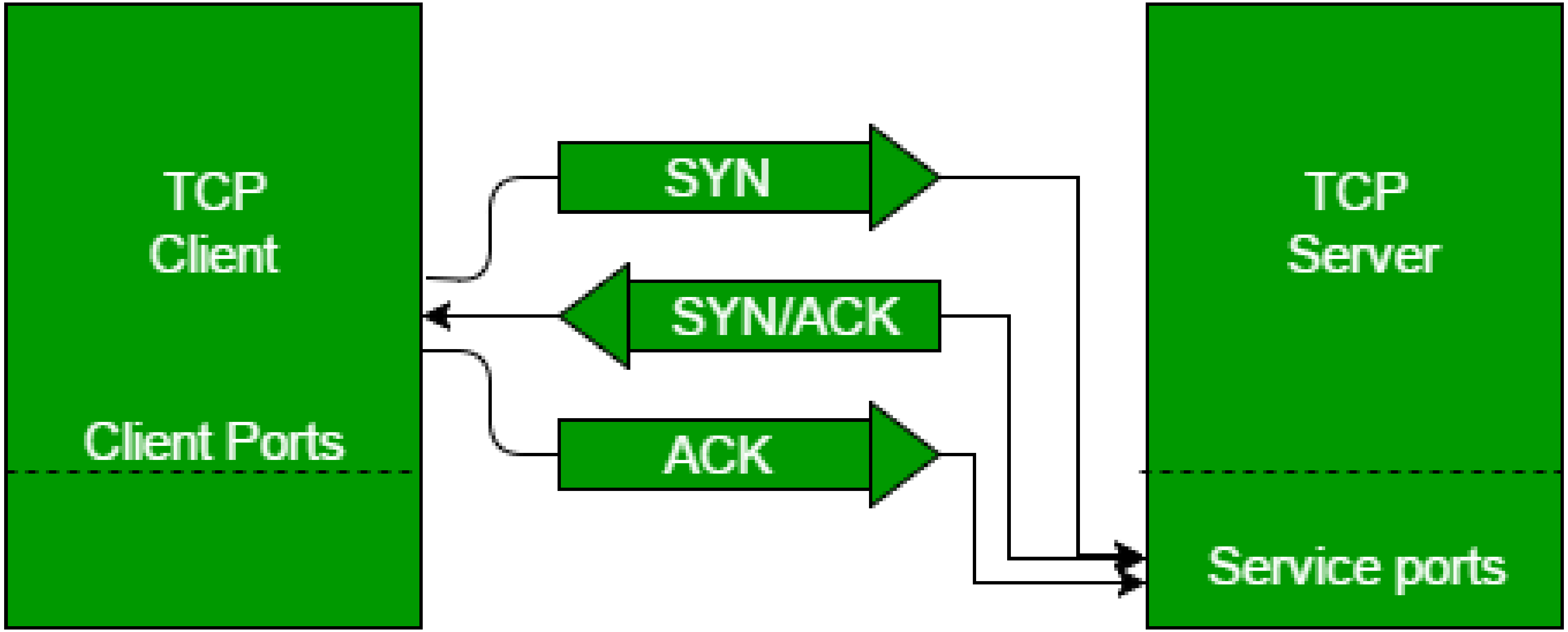
1.Advantages of UDP:

- Minimal latency and overhead.
- Suitable for real-time communication.
- Can handle a high rate of message transmission.

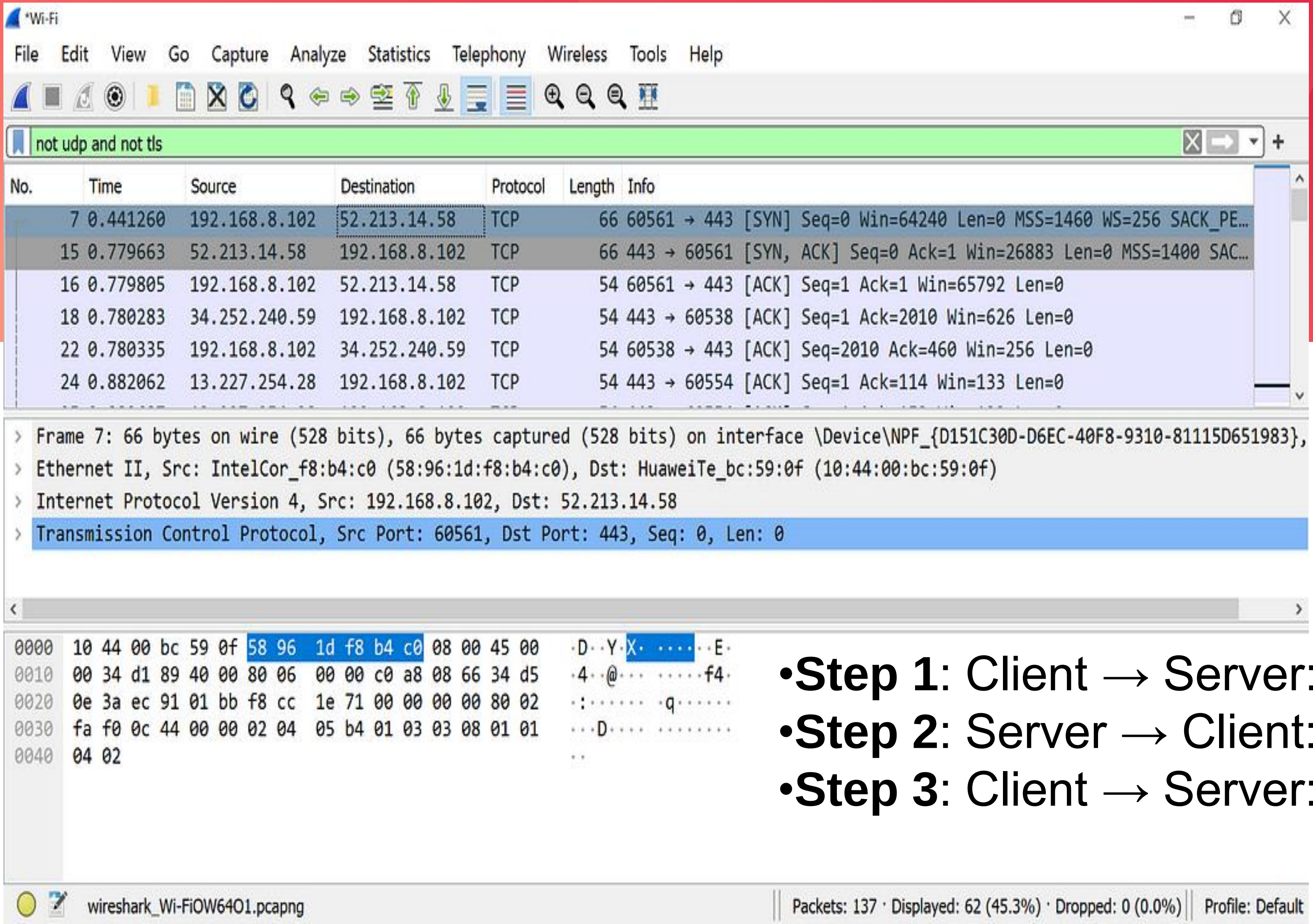
Disadvantages of UDP:

- No built-in mechanisms for reliability (no acknowledgment, retransmission, or flow control).
- Packets may arrive out of order or be dropped.

The **three-way handshake** is a process used in the **Transmission Control Protocol (TCP)** to establish a reliable connection between a client and a server before data transmission begins. It ensures that both parties are ready to communicate and agree on initial parameters, such as sequence numbers.



ESTABLISHING A TCP SESSION (THREE -WAY HANDSHAKE)



not udp and not tls

No.	Time	Source	Destination	Protocol	Length	Info
7	0.441260	192.168.8.102	52.213.14.58	TCP	66	60561 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PE…
15	0.779663	52.213.14.58	192.168.8.102	TCP	66	443 → 60561 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1400 SAC…
16	0.779805	192.168.8.102	52.213.14.58	TCP	54	60561 → 443 [ACK] Seq=1 Ack=1 Win=65792 Len=0
18	0.780283	34.252.240.59	192.168.8.102	TCP	54	443 → 60538 [ACK] Seq=1 Ack=2010 Win=626 Len=0
22	0.780335	192.168.8.102	34.252.240.59	TCP	54	60538 → 443 [ACK] Seq=2010 Ack=460 Win=256 Len=0
24	0.882062	13.227.254.28	192.168.8.102	TCP	54	443 → 60554 [ACK] Seq=1 Ack=114 Win=133 Len=0

```
> Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{D151C30D-D6EC-40F8-9310-81115D651983},
> Ethernet II, Src: IntelCor_f8:b4:c0 (58:96:1d:f8:b4:c0), Dst: HuaweiTe_bc:59:0f (10:44:00:bc:59:0f)
> Internet Protocol Version 4, Src: 192.168.8.102, Dst: 52.213.14.58
> Transmission Control Protocol, Src Port: 60561, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  10 44 00 bc 59 0f 58 96  1d f8 b4 c0 08 00 45 00   ·D··Y·X· ······E·
0010  00 34 d1 89 40 00 80 06  00 00 c0 a8 08 66 34 d5   ·4··@··· ·····f4·
0020  0e 3a ec 91 01 bb f8 cc  1e 71 00 00 00 00 80 02   ·:······ ·q······
0030  fa f0 0c 44 00 00 02 04  05 b4 01 03 03 08 01 01   ···D···· ········
0040  04 02                                              ··
```

wireshark_Wi-FiOW64O1.pcapng | Packets: 137 · Displayed: 62 (45.3%) · Dropped: 0 (0.0%) | Profile: Default

- **Step 1**: Client → Server: SYN, Seq = 100
- **Step 2**: Server → Client: SYN, ACK, Seq = 300, Ack = 101
- **Step 3**: Client → Server: ACK, Seq = 101, Ack = 301

The four-way handshake is a process used in the **Transmission Control Protocol (TCP)** to terminate a connection between a client and a server. Unlike the three-way handshake, which establishes a connection, the four-way handshake ensures an orderly and reliable closure.

Purpose of the Four-Way Handshake:

1. To ensure an orderly and reliable shutdown of the TCP connection.
2. To allow both parties to finish sending any remaining data before closing.
3. To ensure that all packets are acknowledged before the connection is terminated.

Time-Wait State:

- The **TIME-WAIT** state in the client ensures that any delayed packets from the server are properly handled before the connection is fully closed. It prevents issues like retransmission of FIN segments causing errors.

Steps in the Four-Way Handshake:

1. **FIN (Finish)**:
   - The party initiating the termination (e.g., the client) sends a TCP segment with the **FIN** flag set to 1.
   - This indicates that it has finished sending data and wants to close its side of the connection.
   - The client enters the **FIN-WAIT-1** state.
2. **ACK (Acknowledge)**:
   - The receiving party (e.g., the server) responds with a TCP segment that has the **ACK** flag set to 1.
   - This acknowledges receipt of the FIN segment by setting the acknowledgment number to the next sequence number.
   - The server continues to send data if it has any remaining to send. The client enters the **FIN-WAIT-2** state.
3. **FIN (Finish)**:
   - When the server has no more data to send, it sends its own TCP segment with the **FIN** flag set to 1, indicating it is ready to close its side of the connection.
   - The server enters the **LAST-ACK** state.
4. **ACK (Acknowledge)**:
   - The client responds with a TCP segment with the **ACK** flag set to 1, acknowledging the server's FIN.
   - The client enters the **TIME-WAIT** state to ensure the server receives the acknowledgment. After a timeout (typically twice the Maximum Segment Lifetime, or MSL), the client transitions to the **CLOSED** state.
   - The server, upon receiving the ACK, transitions to the **CLOSED** state immediately.

Troubleshooting physical connectivity problems involves systematically identifying and resolving issues with physical network components such as cables, connectors, network devices, and ports

Verify Physical Connections

- **Check cables**:
  - Ensure cables are securely plugged into the correct ports.
  - Inspect for visible damage, such as fraying, cuts, or bent pins.
  - Verify that the correct cable type is used (e.g., straight-through for most connections, crossover for specific scenarios, or fiber optic where applicable).
- **Inspect connectors**:
  - Ensure connectors (e.g., RJ45 or fiber optic) are not damaged or dirty.
  - For fiber optics, check for dirt or scratches on the ends and clean them if necessary.
- **Test cable functionality**:
  - Use a cable tester to confirm the integrity of the cables and identify faults like breaks or short circuits.

Verify Device Power and Status

- **Ensure devices are powered on**:
  - Check that all network devices (e.g., routers, switches, and computers) are receiving power.
  - Look for LEDs indicating power or activity.
- **Inspect device indicators**:
  - Examine LED indicators for ports or connections:
    - **Green**: Typically indicates an active connection.
    - **Amber**: May indicate errors, slower speed, or other issues depending on the device.
    - **Off**: Could indicate no connection, disabled port, or a physical issue.

THANK YOU

Rajadhurai S

Cyber Security Researcher