Networking Fundamentals

Index

Computer Networks and Types of Networks

What is a Computer Network?

- A computer network consists of interconnected devices that can communicate and share resources.
- These devices are linked through physical media (cables) or wireless connections.
- Networks enable functionalities like:
    - Sharing files and printers.
    - Accessing the internet.
    - Sending emails and instant messages.
    - Playing online games.

Types of Computer Networks:

There are various ways to classify computer networks, but here are some of the most common categorizations based on their size and scope:

1. **Local Area Network (LAN):**
    - Covers a limited geographical area, typically a home, office building, or school.
    - Devices are interconnected using cables (Ethernet) or wirelessly (Wi-Fi).
    - LANs are known for their high speed and reliability.
2. **Personal Area Network (PAN):**
    - An even smaller network connecting devices in close proximity (around 10 meters).
    - Examples include Bluetooth connections for headsets or speakers, or connecting devices to a wearable fitness tracker.
3. **Metropolitan Area Network (MAN):**
    - Spans a larger area than a LAN, typically encompassing a city or town.
    - Often connects multiple LANs within a specific geographical region.
    - MANs may use higher-bandwidth connections like fiber optic cables.
4. Wide Area Network (WAN):
    - Covers a vast geographical area, even continents.
    - Connects geographically distant LANs, MANs, and individual devices.
    - WANs typically rely on leased lines, satellites, or other communication technologies.
5. **Wireless Local Area Network (WLAN):**
    - A specific type of LAN that uses wireless connections (Wi-Fi) instead of cables.
    - WLANs offer flexibility and mobility for devices within the network range.
6. **Storage Area Network (SAN):**
    - A specialized network designed for connecting high-performance storage devices to servers.
    - Focuses on providing high-speed access to storage for mission-critical applications.
7. **Virtual Private Network (VPN):**

  - Creates a secure tunnel over a public network (like the internet) to connect devices or networks remotely.
  - Encrypts data traffic, providing a secure connection for users or branch offices.

Network Devices

Network devices are the hardware components used to connect computers and other electronic devices so they can communicate with each other. These devices play a critical role in managing and facilitating data traffic within and between networks. Here is an overview of key network devices:

1. Router

- **Function**: Connects multiple networks and directs data packets between them.
- **Features**: Routes data from one network to another, often used to connect LANs to WANs, provides firewall capabilities, assigns IP addresses through DHCP.
- **Example**: A home router connecting a local home network to the internet.

2. Switch

- **Function**: Connects multiple devices within a single network segment (LAN) and filters and forwards data to the appropriate device.
- **Features**: Operates at the data link layer (Layer 2) of the OSI model, can provide PoE (Power over Ethernet), supports VLANs (Virtual LANs).
- **Example**: A network switch in an office connecting computers, printers, and servers within the same LAN.

3. Hub

- **Function**: Connects multiple Ethernet devices, making them act as a single network segment.
- **Features**: Operates at the physical layer (Layer 1) of the OSI model, broadcasts incoming data to all ports, less efficient than a switch.
- **Example**: A basic network hub connecting several computers in a small network.

4. Modem

- **Function**: Modulates and demodulates analog signals to digital signals for data transmission over telephone lines, cable systems, or satellite systems.
- **Features**: Converts digital data from a computer into a format suitable for a transmission medium and vice versa.
- **Example**: A DSL or cable modem connecting a home network to the ISP.

5. Access Point (AP)

- **Function**: Allows wireless devices to connect to a wired network using Wi-Fi.
- **Features**: Extends the range of a wireless network, supports multiple wireless standards (e.g., 802.11ac), can provide PoE.
- **Example**: A Wi-Fi access point in an office providing wireless connectivity to laptops and smartphones.

6. Network Interface Card (NIC)

- **Function**: Provides a physical interface between a computer and the network.
- **Features**: Can be wired (Ethernet NIC) or wireless (Wi-Fi NIC), operates at both the physical and data link layers of the OSI model.
- **Example**: An Ethernet NIC in a desktop computer connecting to a wired LAN.

7. Firewall

- **Function**: Monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- **Features**: Protects the network from unauthorized access, can be hardware or software-based, often includes VPN support.
- **Example**: A hardware firewall appliance used to protect a corporate network from external threats.

8. Bridge

- **Function**: Connects and filters traffic between two or more network segments.
- **Features**: Operates at the data link layer (Layer 2), reduces traffic by dividing collision domains.
- **Example**: A network bridge connecting two different segments of an office LAN.

9. Gateway

- **Function**: Acts as an entry and exit point in a network, translating data between different protocols or network types.
- **Features**: Can operate at any layer of the OSI model, often used to connect different network architectures (e.g., LAN to WAN).
- **Example**: A VoIP gateway converting voice data from a telephone system to a data network.

10. Repeater

- **Function**: Amplifies and retransmits signals to extend the range of a network.
- **Features**: Operates at the physical layer (Layer 1), regenerates weak signals to maintain data integrity.
- **Example**: A Wi-Fi repeater extending the signal of a wireless network in a large building.

11. Proxy Server

- **Function**: Acts as an intermediary for requests from clients seeking resources from other servers.
- **Features**: Provides caching, improves performance, enhances security by hiding client IP addresses.
- **Example**: A web proxy server that caches frequently accessed web pages to reduce load times and bandwidth usage.

Network devices are essential for the construction and maintenance of modern computer networks. Each device plays a specific role in managing data traffic, ensuring connectivity, and providing security. Understanding the functions and features of these devices is crucial for designing and maintaining efficient and secure networks.

IP and MAC Address

IP (Internet Protocol) addresses and MAC (Media Access Control) addresses are fundamental concepts in networking, each serving a distinct purpose in the communication and identification of devices on a network. Here’s a detailed look at both:

IP Address

Definition: An IP address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.

Types of IP Addresses:

1. **IPv4 (Internet Protocol version 4)**:
   - **Format**: 32-bit address, written as four decimal numbers separated by dots (e.g., 192.168.1.1).
   - **Example**: 192.0.2.1
2. **IPv6 (Internet Protocol version 6)**:
   - **Format**: 128-bit address, written as eight groups of four hexadecimal digits separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
   - **Example**: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Functions:

1. **Identification**: Identifies a device on a network.
2. **Location Addressing**: Specifies the location of the device in the network topology.

Types of IP Address Allocation:

1. **Static IP**:

- Permanently assigned to a device.
- Suitable for servers, printers, and devices needing consistent access.

2. **Dynamic IP**:
    - Temporarily assigned by a DHCP (Dynamic Host Configuration Protocol) server.
    - Common for general user devices like laptops, smartphones, and desktop computers.

Classes of IPv4 Addresses:

1. **Class A**: Large networks, 1.0.0.0 to 126.0.0.0
2. **Class B**: Medium-sized networks, 128.0.0.0 to 191.255.0.0
3. **Class C**: Small networks, 192.0.0.0 to 223.255.255.0
4. **Class D**: Multicast, 224.0.0.0 to 239.255.255.255
5. **Class E**: Experimental, 240.0.0.0 to 255.255.255.255

Private IP Addresses:

- **Used within a private network** and not routable on the public internet.
- Examples: 192.168.0.0 to 192.168.255.255 (Class C), 172.16.0.0 to 172.31.255.255 (Class B), 10.0.0.0 to 10.255.255.255 (Class A).

MAC Address

A MAC address is a unique identifier assigned to a network interface card (NIC) for communications at the data link layer of a network segment.

Format:

- **48-bit address**: Typically represented as six pairs of hexadecimal digits separated by colons or hyphens (e.g., 00:1A:2B:3C:4D:5E or 00-1A-2B-3C-4D-5E).

Functions:

1. **Unique Identification**: Ensures each device on a local network has a unique identifier.
2. **Data Link Layer Communication**: Facilitates communication within the same local network segment.

Structure:

1. **Organizationally Unique Identifier (OUI)**: The first 24 bits, assigned by the IEEE to identify the manufacturer.
2. **Device Identifier**: The last 24 bits, assigned by the manufacturer to uniquely identify the device.

Examples:

- **Example MAC Address**: 00:1A:2B:3C:4D:5E

Differences Between IP and MAC Addresses:

1. **Purpose**:
   - **IP Address**: Used for locating devices in a network (logical address).
   - **MAC Address**: Used for identifying devices within the same local network (physical address).
2. **Scope**:
   - **IP Address**: Operates at the Network Layer (Layer 3) of the OSI model.
   - **MAC Address**: Operates at the Data Link Layer (Layer 2) of the OSI model.
3. **Permanence**:
   - **IP Address**: Can be static (permanent) or dynamic (temporary).
   - **MAC Address**: Usually permanent and burned into the NIC, although it can be spoofed.
4. **Format**:
   - **IP Address (IPv4)**: Four decimal numbers (e.g., 192.168.1.1).
   - **IP Address (IPv6)**: Eight groups of hexadecimal digits (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
   - **MAC Address**: Six pairs of hexadecimal digits (e.g., 00:1A:2B:3C:4D:5E).

How They Work Together:

- When a device wants to communicate over a network, it uses the IP address to determine the destination. However, for the actual data transmission on the local network, it uses the MAC address.
- **Address Resolution Protocol (ARP)**: Used to map an IP address to a MAC address within a local network.

Both IP and MAC addresses are essential for network communication, each serving unique roles. IP addresses provide logical addressing for routing traffic across networks, while MAC addresses ensure unique identification of devices on the same local network segment. Understanding both is crucial for network configuration, troubleshooting, and management.

IPv4 and IPV6 Packet Structure

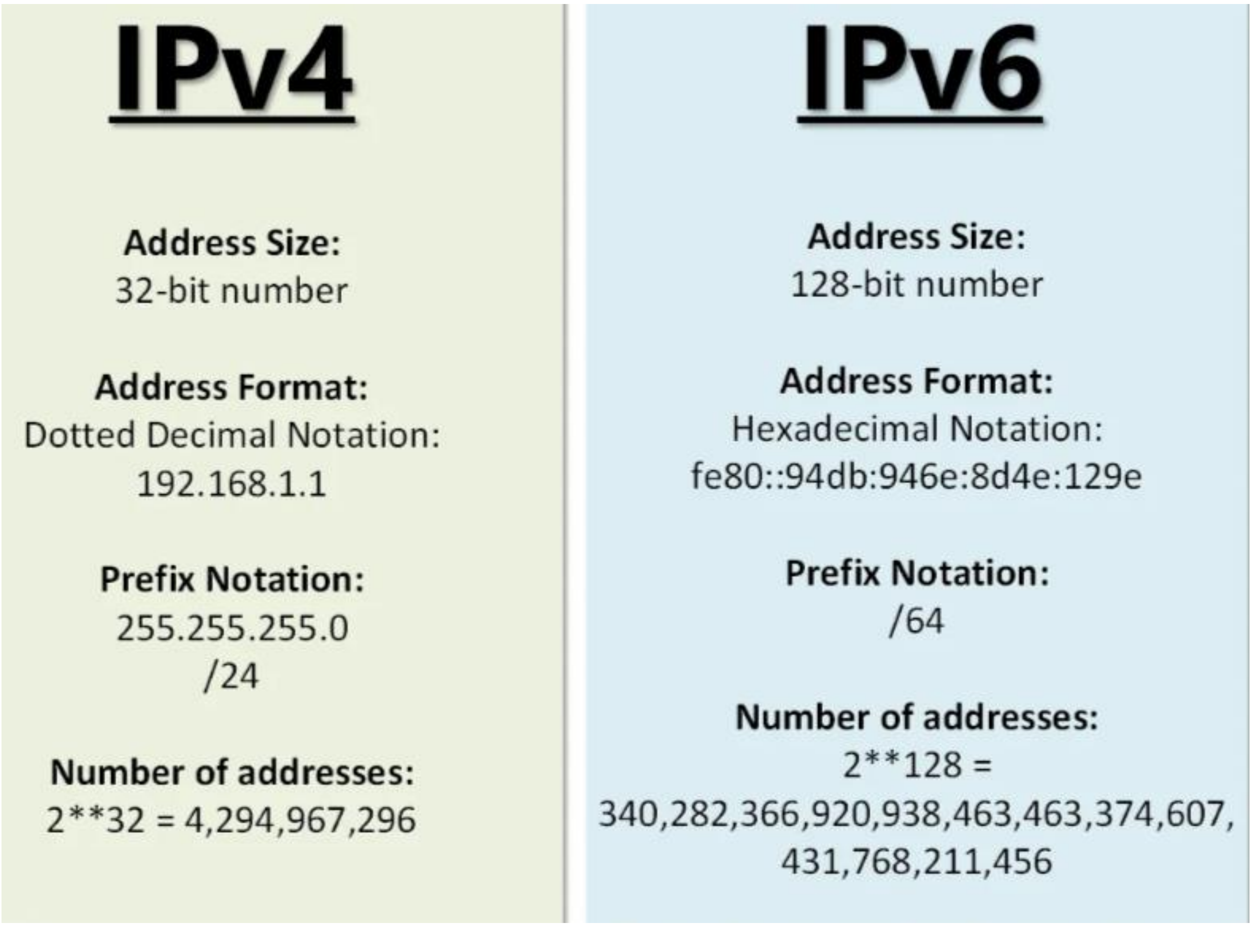
The internet relies on packets, small units of data, to transmit information across networks. These packets have a specific structure that defines how the data is encapsulated and routed to its destination. Here's a breakdown of the header structure for IPv4 and IPv6 packets:

IPv4 Packet Structure:

- **Version (4 bits):** Identifies the IP version (4 in this case).
- **Header Length (4 bits):** Indicates the number of 32-bit words (4 bytes each) in the header, typically 5 (20 bytes) for a standard header.
- **Type of Service (8 bits):** Defines priority and quality-of-service settings for the packet.
- **Total Length (16 bits):** Specifies the total length of the packet in bytes, including header and data.
- **Identification (16 bits):** A unique identifier for the packet, often used for fragmentation and reassembly.
- **Flags (3 bits):** Control flags for fragmentation and other options.
- **Fragment Offset (13 bits):** Used for fragmenting larger packets into smaller ones, if needed.
- **Time to Live (TTL) (8 bits):** A counter that decrements with each hop on the network. Packets with a TTL of zero are discarded to prevent looping.
- **Protocol (8 bits):** Identifies the protocol used for the data portion of the packet (e.g., TCP, UDP).
- **Header Checksum (16 bits):** A checksum calculated over the header to ensure its integrity during transmission. Errors can be detected by recalculating the checksum at the receiving end.
- **Source Address (32 bits):** The IP address of the sender.
- **Destination Address (32 bits):** The IP address of the intended recipient.
- **Data (variable length):** The actual data being transmitted (maximum size of 65,535 bytes for IPv4).

IPv6 Packet Structure:

- **Version (4 bits):** Identifies the IP version (6 in this case).
- **Traffic Class (8 bits):** Similar to Type of Service in IPv4, defines priority and quality-of-service.
- **Flow Label (20 bits):** Used for traffic classification and potential quality-of-service differentiation.
- **Payload Length (16 bits):** Specifies the length of the payload (data) portion of the packet in bytes.
- **Next Header (8 bits):** Indicates the protocol used for the payload (similar to Protocol in IPv4).
- **Hop Limit (8 bits):** Similar to TTL in IPv4, prevents packets from looping endlessly.
- **Source Address (128 bits):** The IPv6 address of the sender.
- **Destination Address (128 bits):** The IPv6 address of the intended recipient.
- **Payload (variable length):** The actual data being transmitted (much larger theoretical maximum size compared to IPv4).



IPv4	IPv6
Address Size: 32-bit number	**Address Size:** 128-bit number
Address Format: Dotted Decimal Notation: 192.168.1.1	**Address Format:** Hexadecimal Notation: fe80::94db:946e:8d4e:129e
Prefix Notation: 255.255.255.0 /24	**Prefix Notation:** /64
Number of addresses: 2**32 = 4,294,967,296	**Number of addresses:** 2**128 = 340,282,366,920,938,463,463,374,607, 431,768,211,456

Addressing and Subnetting:

IP addressing

An IP address is a unique identifier that assists in the recognition of different devices present over the network. Through IP addressing, we can send and receive data packets across the internet without trouble-free.

IP format

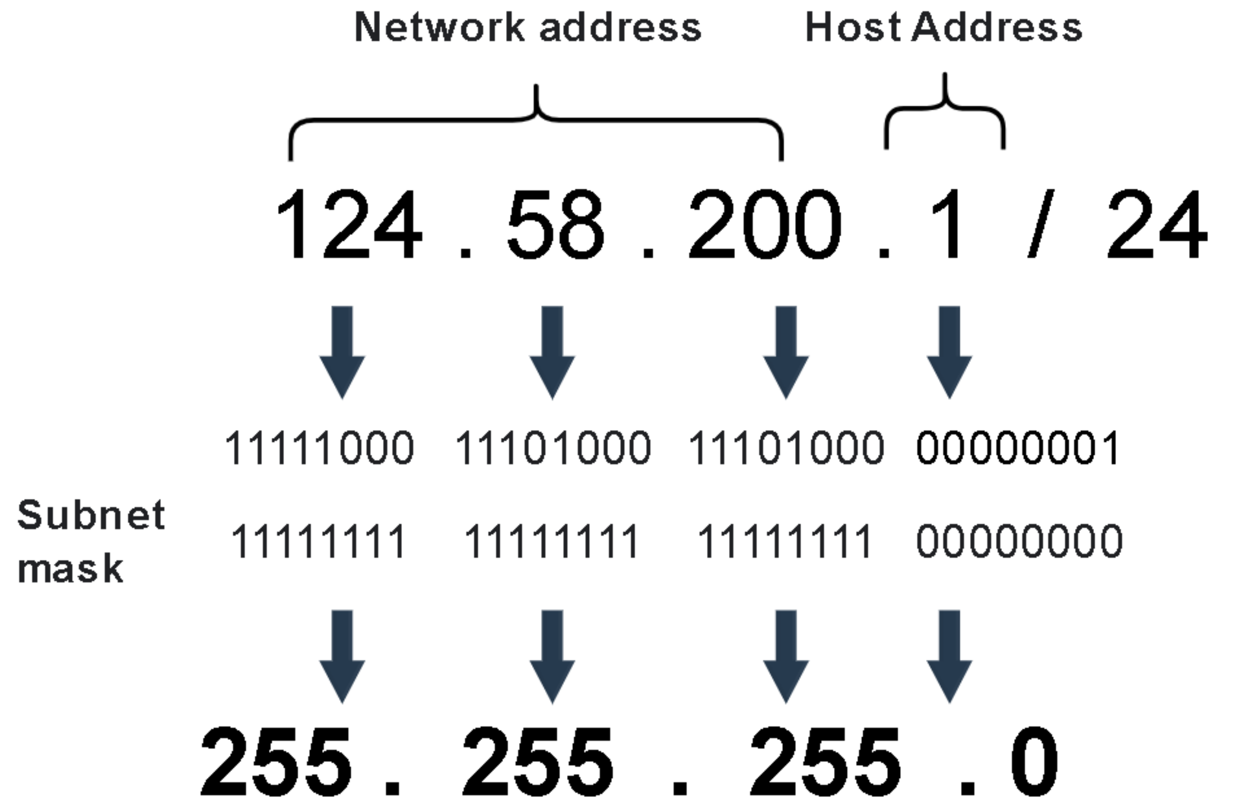
An IP address is a 32-bit numerical address separated by periods (.)(.) represented in dotted decimal notation. It is expressed in a set of four pairs, where each set ranges from 00 to 255255. Slash notation (/)(/) identifies the number of network bits reserved for the allocated IP address. The IP address has two parts: the network address and the host address. The network address is essential for the recognition of the network. In the host address part, we always reserve the first address for the network address, and the last address for the broadcast address. The broadcast address transmits data to all the hosts present in the network at once.

Subnetting

Subnetting is a process of partitioning a complex network into multiple smaller logical sub-networks, or subnets.

Subnet masks

A **subnet mask** is a 3232-bit number that divides the existing IP into network and host addresses.



Example

To find the subnet mask of a particular IP address, let's set all network bits to 11s and the host bits to 00s. The given IP address has 24 bits reserved as a network address. So, its default subnet mask is 255.255.255.0255.255.255.0.

OSI Model and TCP/IP Model

The OSI (Open Systems Interconnection) model and the TCP/IP (Transmission Control Protocol/Internet Protocol) model are two conceptual frameworks used to understand how networks operate and communicate. They both define layers and protocols but have some key differences in their approach and implementation.

OSI Model (Open Systems Interconnection Model)

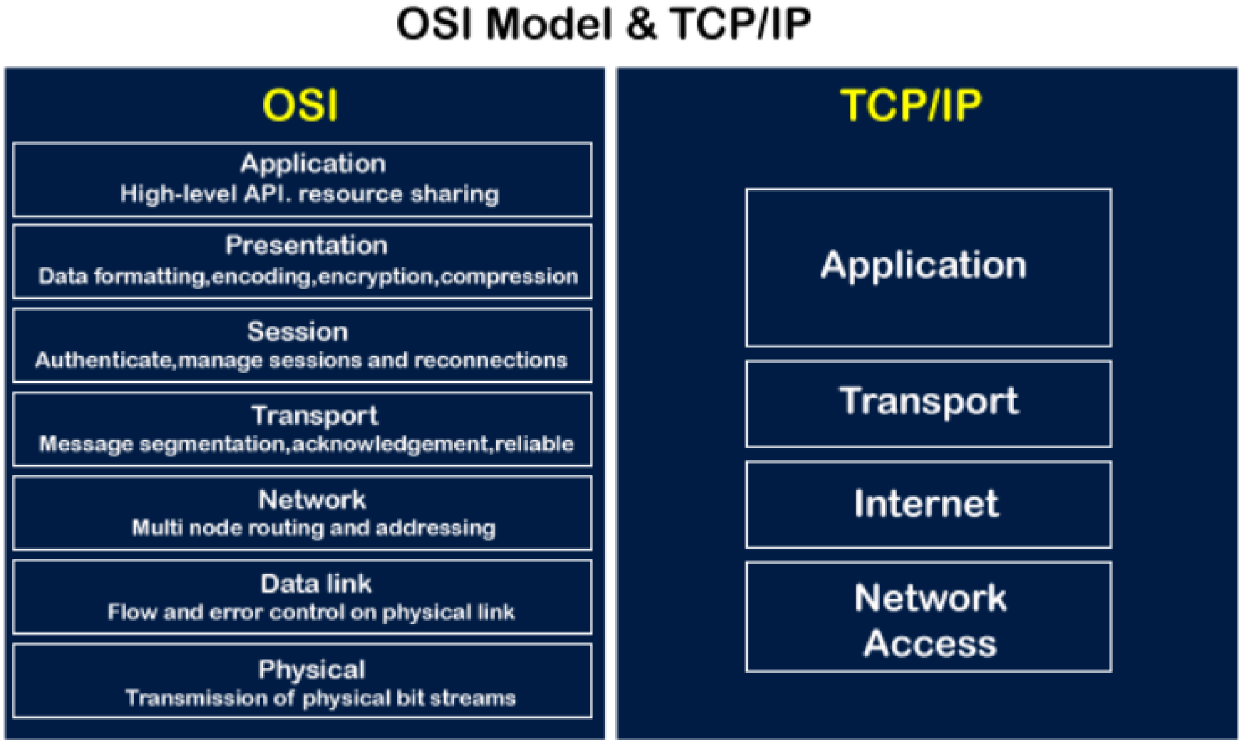
The OSI model is a theoretical framework that standardizes the functions of a telecommunication or computing system into seven distinct layers. Each layer has specific functions and interacts with adjacent layers, providing a clear separation of responsibilities in network communication.

1. **Physical Layer (Layer 1)**:
   - Concerned with the physical transmission of data over the network media (e.g., cables, wires).
   - Defines electrical, mechanical, procedural, and functional specifications.
2. **Data Link Layer (Layer 2)**:
   - Provides error-free transfer of data frames between nodes over a physical link.
   - Handles issues such as framing, physical addressing (MAC addresses), error detection, and flow control.
3. **Network Layer (Layer 3)**:
   - Manages logical addressing (IP addresses) and routing of data packets between different networks.
   - Determines the best path for data to travel from source to destination across multiple networks.
4. **Transport Layer (Layer 4)**:
   - Provides end-to-end communication between devices.
   - Ensures data reliability, flow control, and error checking.
   - Examples include TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).
5. **Session Layer (Layer 5)**:
   - Manages sessions or connections between applications on different devices.
   - Establishes, maintains, and synchronizes the interaction between communicating systems.
6. **Presentation Layer (Layer 6)**:
   - Translates, encrypts, and compresses data sent by the application layer.
   - Ensures that data sent from the application layer of one system can be read by the application layer of another.
7. **Application Layer (Layer 7)**:
   - Provides interface between the user and the network.
   - Supports various applications such as web browsers, email clients, and file transfer protocols.

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

The TCP/IP model is a simpler and more practical model that directly maps to the functionalities of the TCP/IP protocol suite, which is the basis of the internet. It consists of four layers, combining the functionality of several OSI layers into fewer layers:

1. **Network Interface Layer (Link Layer or Network Access Layer)**:
   - Equivalent to the combination of OSI Layers 1 and 2.
   - Handles physical transmission of data and access to network media.
2. **Internet Layer**:
   - Equivalent to OSI Layer 3 (Network Layer).
   - Responsible for routing packets across multiple networks.
   - Uses IP (Internet Protocol) for addressing and packet forwarding.
3. **Transport Layer**:
   - Equivalent to OSI Layer 4.
   - Provides reliable, end-to-end data transmission and error checking.
   - Includes TCP for connection-oriented transmission and UDP for connectionless transmission.
4. **Application Layer**:
   - Combines OSI Layers 5, 6, and 7.
   - Provides network services directly to applications and end-users.
   - Includes protocols such as HTTP, FTP, SMTP, and DNS.


OSI Model & TCP/IP
OSI
Application
High-level API. resource sharing
Presentation
Data formatting,encoding,encryption,compression
Session
Authenticate,manage sessions and reconnections
Transport
Message segmentation,acknowledgement,reliable
Network
Multi node routing and addressing
Data link
Flow and error control on physical link
Physical
Transmission of physical bit streams
TCP/IP
Application
Transport
Internet
Network Access

Network Protocols (TCP, UDP, ICMP, ARP)

Network protocols are essential for enabling communication between devices on a network. Each protocol serves specific purposes, from reliable data transmission to network management and troubleshooting. Here's an overview of some key network protocols: TCP (Transmission Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol), and ARP (Address Resolution Protocol).

TCP (Transmission Control Protocol)

- **Purpose**: TCP is a connection-oriented protocol that ensures reliable and ordered delivery of data between devices. It establishes a connection, manages data flow, and handles error detection and recovery.
- **Features**:
  - **Reliability**: Provides acknowledgment of data delivery and retransmits lost packets.
  - **Flow Control**: Regulates data transmission to prevent overwhelming the receiver.
  - **Connection Management**: Establishes and terminates connections between devices.
- **Usage**: Commonly used for applications requiring reliable transmission, such as web browsing (HTTP), email (SMTP), file transfer (FTP), etc.

UDP (User Datagram Protocol)

- **Purpose**: UDP is a connectionless protocol that offers low-latency, unreliable data transmission between devices. It does not guarantee delivery or order of packets.
- **Features**:
  - **Minimal Overhead**: Lightweight protocol without the overhead of connection setup and acknowledgment.
  - **Low Latency**: Suitable for applications where speed is crucial, such as real-time communication (VoIP), video streaming (UDP-based RTP), DNS queries (UDP-based DNS).
- **Usage**: Used when speed and efficiency are more critical than reliability, or when error correction is handled at the application level.

ICMP (Internet Control Message Protocol)

- **Purpose**: ICMP is used for network management and troubleshooting. It provides error messaging and diagnostics functionalities between devices on an IP network.
- **Features**:
  - **Error Reporting**: Reports errors encountered during packet processing (e.g., destination unreachable, time exceeded).
  - **Network Testing**: Supports tools like Ping (ICMP Echo Request/Reply) and Traceroute (ICMP Time Exceeded) for network diagnostics.
- **Usage**: Integral for network administrators to monitor and troubleshoot network connectivity and performance issues.

ARP (Address Resolution Protocol)

- **Purpose**: ARP resolves IP addresses to MAC addresses within a local network segment. It maps IP addresses to MAC addresses, enabling communication between devices on the same subnet.
- **Operation**:
  - **ARP Request**: Broadcasts a request to find the MAC address associated with a specific IP address.
  - **ARP Reply**: Receives a response containing the MAC address, which is then cached in an ARP table for future reference.
- **Usage**: Essential for data link layer communication (Layer 2) in Ethernet networks, enabling devices to communicate directly based on MAC addresses.

Network Services (DNS, DHCP, SNMP, FTP)

Network services play vital roles in managing and facilitating communication within computer networks. Here's an overview of some key network services: DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), SNMP (Simple Network Management Protocol), and FTP (File Transfer Protocol).

DNS (Domain Name System)

- **Purpose**: DNS translates domain names (e.g., www.example.com) into IP addresses (e.g., 192.0.2.1) and vice versa. It resolves human-readable domain names to numerical IP addresses that computers use to identify each other on the network.
- **Operation**:
  - **DNS Query**: When a user enters a domain name, their device sends a DNS query to a DNS server.
  - **DNS Resolution**: The DNS server looks up the corresponding IP address in its database (or forwards the request to other DNS servers) and sends the IP address back to the user's device.
- **Usage**: Essential for web browsing, email delivery, and other internet services that rely on domain names.

DHCP (Dynamic Host Configuration Protocol)

- **Purpose**: DHCP automates the process of assigning IP addresses, subnet masks, default gateways, DNS server addresses, and other network configuration parameters to devices on a network.
- **Operation**:
  - **IP Address Allocation**: DHCP servers dynamically allocate IP addresses from a pool to devices requesting network connectivity.
  - **Lease Management**: Assigns IP addresses for a specific period (lease), renewing or releasing them as needed.

- **Usage**: Simplifies network administration by centralizing IP address management, especially in large networks with many devices that frequently connect and disconnect.

SNMP (Simple Network Management Protocol)

- **Purpose**: SNMP facilitates network management and monitoring by allowing devices to collect and exchange management information. It provides a standardized framework and a set of commands for managing network devices, monitoring performance, and troubleshooting issues.
- **Operation**:
    - **Management Information Base (MIB)**: Defines the structure of managed objects representing device parameters (e.g., CPU utilization, interface status).
    - **SNMP Managers and Agents**: Managers collect data and issue commands, while agents on network devices provide information and execute commands.
- **Usage**: Used extensively by network administrators for monitoring and managing network infrastructure, detecting faults, and optimizing performance.

FTP (File Transfer Protocol)

- **Purpose**: FTP is a standard network protocol used for transferring files between a client and a server on a computer network. It provides a straightforward method for uploading, downloading, and managing files across networks.
- **Operation**:
    - **Client-Server Model**: Clients connect to FTP servers using TCP connections.
    - **Commands**: Supports commands for navigating directories, transferring files (upload/download), deleting files, and setting file permissions.
- **Usage**: Widely used for website maintenance, file sharing, software distribution, and backup purposes.

Packet Analysis using Wireshark

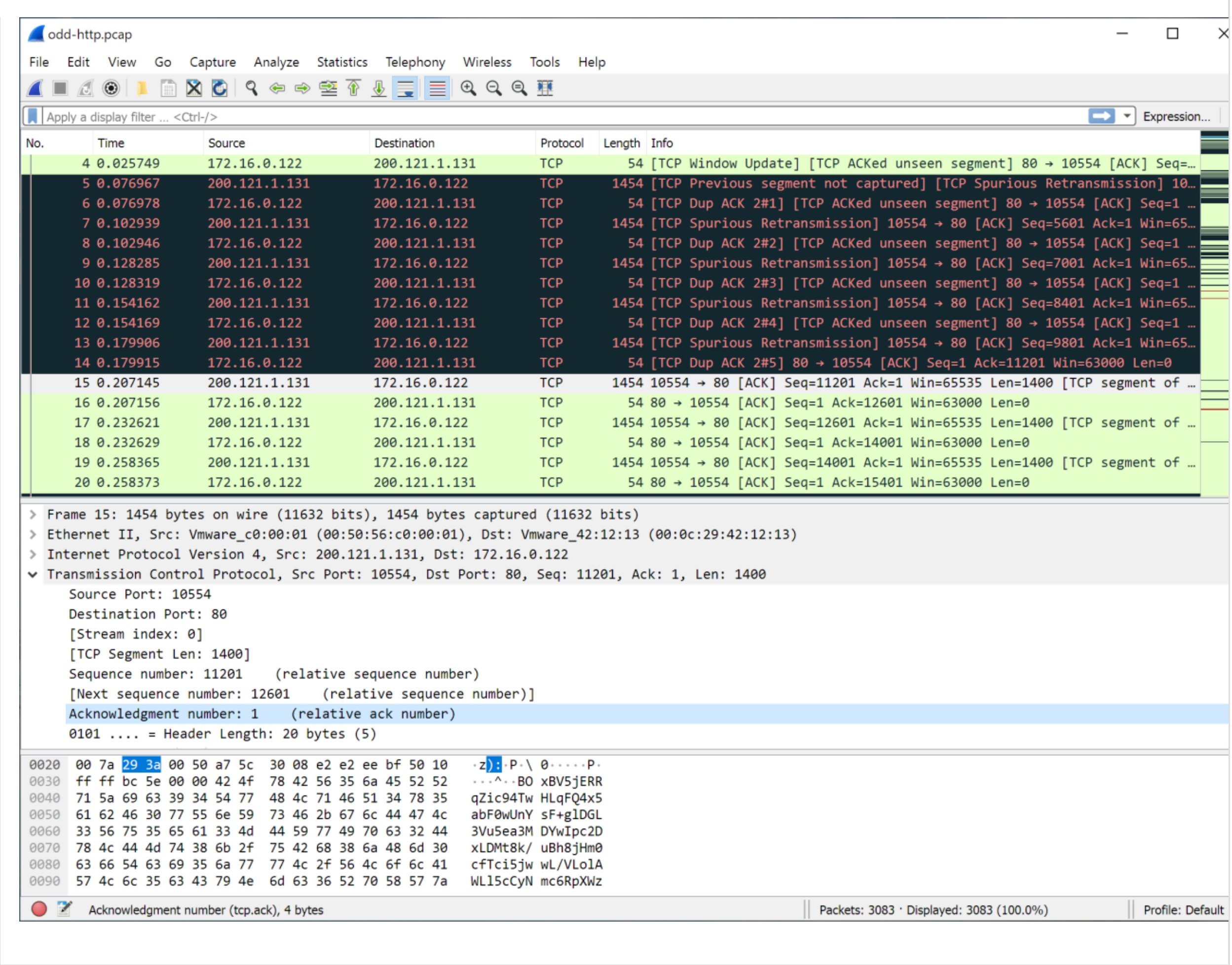
Packet analysis using Wireshark is a powerful method for examining network traffic, diagnosing issues, and troubleshooting network problems. Wireshark is a widely-used network protocol analyzer that captures and displays packet data on a network in real-time.

6.1. Viewing Packets You Have Captured

Once you have captured some packets or you have opened a previously saved capture file, you can view the packets that are displayed in the packet list pane by simply clicking on a packet in the packet list pane, which will bring up the selected packet in the tree view and byte view panes.

You can then expand any part of the tree to view detailed information about each protocol in each packet. Clicking on an item in the tree will highlight the corresponding bytes in the byte view. An example with a TCP packet selected is shown in Figure 6.1, “Wireshark with a TCP packet selected for viewing”. It also has the Acknowledgment number in the TCP header selected, which shows up in the byte view as the selected bytes.

Figure 6.1. Wireshark with a TCP packet selected for viewing


odd-http.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

No.	Time	Source	Destination	Protocol	Length	Info
4	0.025749	172.16.0.122	200.121.1.131	TCP	54	[TCP Window Update] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=…
5	0.076967	200.121.1.131	172.16.0.122	TCP	1454	[TCP Previous segment not captured] [TCP Spurious Retransmission] 10…
6	0.076978	172.16.0.122	200.121.1.131	TCP	54	[TCP Dup ACK 2#1] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 …
7	0.102939	200.121.1.131	172.16.0.122	TCP	1454	[TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=5601 Ack=1 Win=65…
8	0.102946	172.16.0.122	200.121.1.131	TCP	54	[TCP Dup ACK 2#2] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 …
9	0.128285	200.121.1.131	172.16.0.122	TCP	1454	[TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=7001 Ack=1 Win=65…
10	0.128319	172.16.0.122	200.121.1.131	TCP	54	[TCP Dup ACK 2#3] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 …
11	0.154162	200.121.1.131	172.16.0.122	TCP	1454	[TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=8401 Ack=1 Win=65…
12	0.154169	172.16.0.122	200.121.1.131	TCP	54	[TCP Dup ACK 2#4] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 …
13	0.179906	200.121.1.131	172.16.0.122	TCP	1454	[TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=9801 Ack=1 Win=65…
14	0.179915	172.16.0.122	200.121.1.131	TCP	54	[TCP Dup ACK 2#5] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
15	0.207145	200.121.1.131	172.16.0.122	TCP	1454	10554 → 80 [ACK] Seq=11201 Ack=1 Win=65535 Len=1400 [TCP segment of …
16	0.207156	172.16.0.122	200.121.1.131	TCP	54	80 → 10554 [ACK] Seq=1 Ack=12601 Win=63000 Len=0
17	0.232621	200.121.1.131	172.16.0.122	TCP	1454	10554 → 80 [ACK] Seq=12601 Ack=1 Win=65535 Len=1400 [TCP segment of …
18	0.232629	172.16.0.122	200.121.1.131	TCP	54	80 → 10554 [ACK] Seq=1 Ack=14001 Win=63000 Len=0
19	0.258365	200.121.1.131	172.16.0.122	TCP	1454	10554 → 80 [ACK] Seq=14001 Ack=1 Win=65535 Len=1400 [TCP segment of …
20	0.258373	172.16.0.122	200.121.1.131	TCP	54	80 → 10554 [ACK] Seq=1 Ack=15401 Win=63000 Len=0

```
> Frame 15: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)
> Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware_42:12:13 (00:0c:29:42:12:13)
> Internet Protocol Version 4, Src: 200.121.1.131, Dst: 172.16.0.122
v Transmission Control Protocol, Src Port: 10554, Dst Port: 80, Seq: 11201, Ack: 1, Len: 1400
    Source Port: 10554
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 1400]
    Sequence number: 11201    (relative sequence number)
    [Next sequence number: 12601    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
```

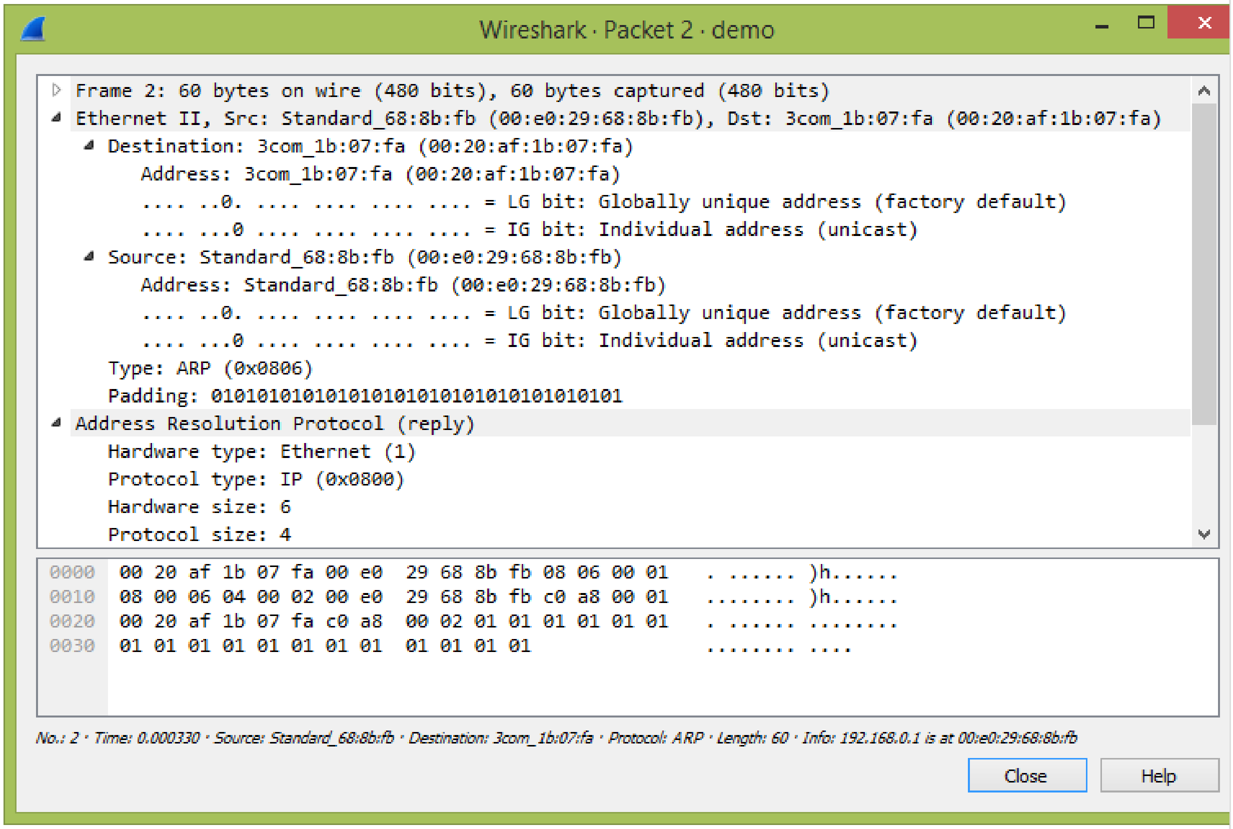
```
0020  00 7a 29 3a 00 50 a7 5c  30 08 e2 e2 ee bf 50 10   ·z):·P·\ 0·····P·
0030  ff ff bc 5e 00 00 42 4f  78 42 56 35 6a 45 52 52   ···^··BO xBV5jERR
0040  71 5a 69 63 39 34 54 77  48 4c 71 46 51 34 78 35   qZic94Tw HLqFQ4x5
0050  61 62 46 30 77 55 6e 59  73 46 2b 67 6c 44 47 4c   abF0wUnY sF+glDGL
0060  33 56 75 35 65 61 33 4d  44 59 77 49 70 63 32 44   3Vu5ea3M DYwIpc2D
0070  78 4c 44 4d 74 38 6b 2f  75 42 68 38 6a 48 6d 30   xLDMt8k/ uBh8jHm0
0080  63 66 54 63 69 35 6a 77  77 4c 2f 56 4c 6f 6c 41   cfTci5jw wL/VLolA
0090  57 4c 6c 35 63 43 79 4e  6d 63 36 52 70 58 57 7a   WLl5cCyN mc6RpXWz
```

Acknowledgment number (tcp.ack), 4 bytes
Packets: 3083 · Displayed: 3083 (100.0%)
Profile: Default

You can also select and view packets the same way while Wireshark is capturing if you selected “Update list of packets in real time” in the “Capture Preferences” dialog box.

In addition you can view individual packets in a separate window as shown in Figure 6.2, “Viewing a packet in a separate window”. You can do this by double-clicking on an item in the packet list or by selecting the packet in which you are interested in the packet list pane and selecting View → Show Packet in New Window. This allows you to easily compare two or more packets, even across multiple files.

Figure 6.2. Viewing a packet in a separate window



```
▷ Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
◢ Ethernet II, Src: Standard_68:8b:fb (00:e0:29:68:8b:fb), Dst: 3com_1b:07:fa (00:20:af:1b:07:fa)
   ◢ Destination: 3com_1b:07:fa (00:20:af:1b:07:fa)
        Address: 3com_1b:07:fa (00:20:af:1b:07:fa)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   ◢ Source: Standard_68:8b:fb (00:e0:29:68:8b:fb)
        Address: Standard_68:8b:fb (00:e0:29:68:8b:fb)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
     Type: ARP (0x0806)
     Padding: 010101010101010101010101010101010101
◢ Address Resolution Protocol (reply)
     Hardware type: Ethernet (1)
     Protocol type: IP (0x0800)
     Hardware size: 6
     Protocol size: 4
```

```
0000  00 20 af 1b 07 fa 00 e0  29 68 8b fb 08 06 00 01   . ...... )h......
0010  08 00 06 04 00 02 00 e0  29 68 8b fb c0 a8 00 01   ........ )h......
0020  00 20 af 1b 07 fa c0 a8  00 02 01 01 01 01 01 01   . ...... ........
0030  01 01 01 01 01 01 01 01  01 01 01 01               ........ ....
```

No.: 2 · Time: 0.000330 · Source: Standard_68:8b:fb · Destination: 3com_1b:07:fa · Protocol: ARP · Length: 60 · Info: 192.168.0.1 is at 00:e0:29:68:8b:fb