OSI

OSI: refers to Open System Interconnection

Layer	Function	Example
Application (7)	Services that are used with end user applications	SMTP,
Presentation (6)	Formats the data so that it can be viewed by the user Encrypt and decrypt	JPG, GIF, HTTPS, SSL, TLS
Session (5)	Establishes/ends connections between two hosts	NetBIOS, PPTP
Transport (4)	Responsible for the transport protocol and error handling	TCP, UDP
Network (3)	Reads the IP address form the packet.	Routers, Layer 3 Switches
Data Link (2)	Reads the MAC address from the data packet	Switches
Physical (1)	Send data on to the physical wire.	Hubs, NICS, Cable

DHCP

DHCP stands for **Dynamic Host Configuration Protocol**. It's a network management protocol used on IP networks. Its primary function is to automatically assign IP addresses and other network configuration information (like subnet mask, default gateway, and DNS servers) to devices on a network.

How DHCP Works:

1. **DHCP Discover**: When a device (like a computer, smartphone, or printer) connects to the network, it doesn't have an IP address yet. It sends out a DHCP Discover message to find a DHCP server on the network.
2. **DHCP Offer**: The DHCP server responds with a DHCP Offer, which includes an available IP address and other configuration details. The server also reserves that IP for a certain amount of time (the lease time).
3. **DHCP Request**: The device then responds to the DHCP Offer by sending a DHCP Request message, confirming that it wants the offered IP address.
4. **DHCP Acknowledgment**: Finally, the DHCP server sends a DHCP Acknowledgment

message to the device, completing the process. The device is now configured and can communicate over the network using the assigned IP address.

Benefits of DHCP:

- **Automation**: It eliminates the need to manually configure IP addresses, reducing human error and saving time, especially on large networks.
- **IP Address Management**: It ensures efficient use of IP addresses by automatically assigning and reclaiming them.
- **Scalability**: DHCP makes it easier to add or remove devices from the network without worrying about IP address conflicts.

Common Use Cases:

- **Home networks**: Most routers at home use DHCP to assign IP addresses to devices like laptops, smartphones, and smart TVs.
- **Corporate networks**: In large organizations, DHCP helps manage the IP addressing for thousands of devices.

DNS

DNS stands for **Domain Name System**, and it's essentially the phonebook of the internet. While humans access websites using domain names like `www.google.com`, computers and servers communicate using IP addresses (like `172.217.5.68`). DNS is what translates those easy-to-remember domain names into IP addresses that computers can understand and use.

How DNS Works:

1. **DNS Query**: When you type a website's domain name into your browser, a **DNS query** is sent to a DNS resolver (usually provided by your Internet Service Provider or a public DNS service like Google DNS or Cloudflare).
2. **DNS Resolver**: The DNS resolver checks its cache to see if it has the IP address for that domain already stored. If not, it will ask other DNS servers.
3. **Recursive DNS Lookup**: If the resolver doesn't know the IP, it starts a **recursive lookup**, querying multiple DNS servers to find the IP address.
    - **Root DNS Server**: It first asks the root DNS server, which is at the top of the DNS hierarchy.
    - **Top-Level Domain (TLD) Server**: The root server directs the query to a TLD server based on the domain's extension (like `.com`, `.org`, or `.net`).
    - **Authoritative DNS Server**: The TLD server sends the query to the authoritative DNS server for the domain, which holds the actual IP address for that domain.
4. **Return the IP**: The authoritative server responds with the correct IP address, which is sent back to your DNS resolver.
5. **Browser Connects**: Finally, the DNS resolver gives your browser the IP address, and your browser uses it to make a direct connection to the server hosting the website.

Types of DNS Records:

- **A Record**: Maps a domain name to an IPv4 address (e.g., `example.com` → `192.0.2.1`).
- **AAAA Record**: Maps a domain to an IPv6 address (e.g., `example.com` → `2001:0db8::1`).
- **CNAME Record**: Redirects one domain to another (e.g., `www.example.com` → `example.com`).
- **MX Record**: Specifies the mail servers for a domain (used for email routing).
- **NS Record**: Identifies the authoritative name servers for a domain.
- **TXT Record**: Holds text information, often for verification or security purposes (e.g., SPF, DKIM for email).

DNS Caching:

To make the system faster and reduce load on DNS servers, results of DNS queries are cached for a certain period (called **TTL**, or Time To Live). This means if the same domain is requested again within the TTL period, the resolver can return the cached IP address rather than looking it up again.

Why DNS is Important:

- **User-Friendly**: Without DNS, you'd have to remember the IP address of every website you want to visit, which is not practical.
- **Performance**: By caching DNS results, browsing is faster because your computer doesn't need to perform a full DNS lookup each time.
- **Security**: DNS is also critical for various security measures, like preventing phishing attacks through techniques like DNSSEC (Domain Name System Security Extensions).

Common DNS Issues:

- **DNS Resolution Failures**: This happens when the DNS query fails (e.g., server issues or incorrect DNS settings).
- **DNS Spoofing/Cache Poisoning**: Attackers can manipulate DNS responses to redirect traffic to malicious sites.
- **DNS Propagation**: When changes are made to DNS records, it can take time for the updates to propagate across the internet.

The **OSI Model** (Open Systems Interconnection Model) is a conceptual framework used to understand how different network protocols interact in a network system. It divides the networking

process into **seven layers**, each responsible for a specific aspect of communication. By breaking down the communication process into layers, the OSI model helps network professionals design, troubleshoot, and understand networks more effectively.

The Seven Layers of the OSI Model:

1. **Layer 1: Physical Layer**
    - **Function**: Deals with the actual physical connection between devices and the transmission of raw binary data (1s and 0s) over physical media (cables, fiber optics, wireless).
    - **Key Elements**:
        - Cables, switches, routers (in terms of physical connectivity)
        - Hubs, modems
        - Signals (electrical, optical, or radio signals)

Examples: Ethernet cables, fiber-optic cables, wireless radio signals.

2. **Layer 2: Data Link Layer**
    - **Function**: Responsible for creating a reliable link between two directly connected nodes. It handles error detection and correction, and manages access to the physical transmission medium.
    - **Key Elements**:
        - MAC (Media Access Control) address
        - Frame formatting
        - Error detection and correction (e.g., CRC)

Examples: Ethernet, Wi-Fi, PPP (Point-to-Point Protocol), switches, bridges.

3. **Layer 3: Network Layer**
    - **Function**: Manages the logical addressing and routing of data packets between devices across different networks. It is responsible for packet forwarding, routing, and addressing.
    - **Key Elements**:
        - IP addresses
        - Routers
        - Packet forwarding and routing algorithms

Examples: IP (Internet Protocol), routing protocols (like OSPF, BGP), routers.

4. **Layer 4: Transport Layer**
    - **Function**: Ensures end-to-end communication and reliable data transfer between devices. It handles flow control, error control, and retransmission of lost data.
    - **Key Elements**:

- TCP (Transmission Control Protocol) – provides reliable, connection-oriented communication.
- UDP (User Datagram Protocol) – provides unreliable, connectionless communication.
- Ports (to address specific processes on devices)

Examples: TCP, UDP, flow control, and error detection.

5. **Layer 5: Session Layer**
    - **Function**: Manages sessions or connections between two applications. It establishes, maintains, and terminates communication sessions.
    - **Key Elements**:
        - Session establishment, maintenance, and termination
        - Dialog control (full-duplex or half-duplex communication)

Examples: SMB (Server Message Block), NetBIOS, RPC (Remote Procedure Call).

6. **Layer 6: Presentation Layer**
    - **Function**: Responsible for translating, encrypting, and compressing data. It ensures that data is in a readable format for the application layer (e.g., converting from one character encoding to another).
    - **Key Elements**:
        - Data encoding (ASCII, UTF-8, etc.)
        - Encryption (e.g., SSL/TLS for HTTPS)
        - Compression (e.g., ZIP, JPEG)

Examples: SSL/TLS, JPEG, GIF, encryption, character encoding.

7. **Layer 7: Application Layer**
    - **Function**: The topmost layer where end-user applications interact with the network. It provides network services directly to applications, such as web browsing, email, and file transfers.
    - **Key Elements**:
        - Interfaces directly with the user (or user software)
        - Application protocols that define specific network services

Examples: HTTP, FTP, SMTP, DNS, POP3, IMAP, web browsers, email clients.

Summary of the OSI Model Layers

Layer	Name	Key Functions	Examples
7	Application	Network services for user applications	HTTP, FTP, DNS, SMTP
6	Presentation	Data translation, encryption, compression	SSL/TLS, JPEG, ASCII

Layer	Name	Key Functions	Examples
5	Session	Managing sessions between apps	NetBIOS, SMB, RPC
4	Transport	End-to-end communication, error control, flow control	TCP, UDP
3	Network	Routing and logical addressing	IP, routers
2	Data Link	Reliable node-to-node communication, error correction	Ethernet, Wi-Fi, MAC
1	Physical	Transmission of raw bits over the physical medium	Cables, switches, wireless

Why is the OSI Model Important?

- **Standardization**: It provides a common reference model that standardizes the functions of networking systems and helps professionals understand network architecture.
- **Troubleshooting**: It’s easier to diagnose problems at each layer (e.g., is it a physical layer problem, or a transport layer issue?).
- **Modularization**: By dividing networking into distinct layers, each one can be independently modified or updated without affecting others. For example, new protocols can be introduced at higher layers without affecting lower layers.
- **Education**: The OSI model is a great tool for understanding how different protocols and devices work together in a network. It’s commonly taught in networking and computer science courses.

OSI vs TCP/IP Model

While the **OSI Model** is theoretical and provides a general guideline, the **TCP/IP Model** (which is used practically on the Internet) has fewer layers (4 layers instead of 7) and combines some of the OSI layers.

- **Application Layer** in TCP/IP combines OSI’s **Application**, **Presentation**, and **Session** layers.
- **Transport Layer** in both models is the same.
- **Internet Layer** in TCP/IP corresponds to the **Network Layer** in OSI.
- **Link Layer** in TCP/IP combines OSI's **Data Link** and **Physical** layers.