Application Layer

PANA ACADEMY

Application Layer Services

The application layer in the OSI model is responsible for providing **network services directly to end-users and application processes**.

WEB HTTP and HTTPS

HTTP (Hypertext Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) are protocols used on the web to transfer data between a client (such as a web browser) and a server.

HTTP is a protocol used for transmitting hypertext (HTML) documents on the World Wide Web.

HOW WEB WORKS ?

How It Works:

- HTTP follows a **request-response** model where the client sends a request to the server, and the server responds with the requested resource (e.g., a web page).
- Common HTTP methods include **GET (retrieve data), POST (submit data), PUT (update data), and DELETE (remove data)**.

HTTP is stateless, meaning each request from a client to a server is independent and does not retain session information between different requests.

Statelessness can be managed using cookies, sessions, or tokens to maintain stateful information.

1. **Port Number:**
    - By default, HTTP operates over port 80.
    - HTTPS operates over port 443.

FTP

File transfer protocols and tools are essential for transferring files over a network. Here's an overview of FTP, PuTTY, and WinSCP, filezilla.

FTP uses two channels: a command channel for sending commands and receiving responses, and a data channel for transferring files.

Clients can use FTP commands to upload, download, delete, rename, and list files on the server.

Default ports are 21 for command/control and 20 for data transfer in active mode.

PUTTY

PuTTY is a free, open-source terminal emulator, serial console, and network file transfer application.

It supports various network protocols, including SSH, Telnet, and SCP (Secure Copy Protocol).

Usage:

- **SSH Connections:** Used for remote server management and command-line access.

Electronic Mail

Electronic mail, commonly known as email, is a method of exchanging digital messages over the internet or other computer networks.

Components of an Email

1. **Email Address**: An identifier for an email account, typically in the format username@domain.com.
2. **Subject Line**: A brief summary of the email's content.
3. **Body**: The main content of the email, which can include text, images, links, and attachments.
4. **Attachments**: Files sent along with the email, such as documents, images, or other data files.

SMTP (Simple Mail Transfer Protocol): Used to send emails from a client to a server or between servers.

IMAP (Internet Message Access Protocol): Allows users to access their email on a server from multiple devices.

POP3 (Post Office Protocol 3): Downloads emails from a server to a single device and typically deletes them from the server afterward.

DNS

The Domain Name System (DNS) is a fundamental component of the internet that translates human-readable domain names (like www.example.com) into IP addresses (like 192.0.2.1) that computers use to identify each other on the network.

DNS functions much like a phone book for the internet, allowing users to access websites and other resources using easy-to-remember names rather than complex numerical addresses.

- **Domain Name**: A readable name for a resource on the internet (e.g.,www.example.com).
- **IP Address**: A numerical label assigned to each device connected to a computer network (e.g., 192.0.2.1 for IPv4 or 2001:0db8:85a3:0000:0000:8a2e:0370:7334 for IPv6).

DNS Hierarchy

DNS Hierarchy:

- **Root Level**: The top level of the DNS hierarchy, represented by a dot (.). Root servers handle requests for top-level domains (TLDs).
- **Top-Level Domains (TLDs)**: The second level in the hierarchy (e.g., .com, .org, .net, country codes like .uk).
- **Second-Level Domains**: Directly below TLDs (e.g., example in example.com).
- **Subdomains**: Domains that are part of a larger domain (e.g., www in www.example.com)

DNS Query Process

DNS Query Process:

- **User Request**: When a user types a domain name into a browser, a DNS query is initiated.
- **Recursive Resolver**: The query is sent to a DNS resolver, often provided by the user's Internet Service Provider (ISP).
- **Root Server**: If the resolver doesn’t have the answer cached, it queries a root server.
- **TLD Server**: The root server responds with the address of a TLD server (e.g., for .com).
- **Authoritative Name Server**: The TLD server responds with the address of the authoritative name server for the domain.
- **IP Address**: The authoritative name server returns the IP address associated with the domain name.
- **Website Access**: The resolver returns the IP address to the user’s browser, which then connects to the web server at that IP address.

DNS Records

DNS Records:

- **A Record**: Maps a domain to an IPv4 address.
- **AAAA Record**: Maps a domain to an IPv6 address.
- **CNAME Record**: Maps a domain to another domain (canonical name).
- **MX Record**: Specifies mail servers for a domain.
- **TXT Record**: Holds text information for various purposes, often used for verification and security.
- **NS Record**: Indicates the authoritative name servers for a domain.

P2P

Peer-to-peer (P2P) applications refer to software systems where nodes (peers) in a network share resources and communicate directly with each other without relying on a centralized server. Each peer in the network can act as both a client and a server, enabling resource sharing such as files, processing power, or network bandwidth.

Socket Programming

socket(): Creates a new socket.

bind(): Binds a socket to an IP address and port.

listen(): Listens for incoming connections (TCP).

accept(): Accepts an incoming connection (TCP).

connect(): Connects to a remote socket.

send() and **recv()**: Send and receive data (TCP).

sendto() and **recvfrom()**: Send and receive data (UDP).

close(): Closes a socket.

Traffic Analyzer

A traffic analyzer is a tool or software application used to **monitor, capture, and analyze network traffic**. It helps network administrators and security professionals understand **what is happening on their networks**, **identify potential issues**, and optimize network performance. Traffic analyzers can provide detailed insights into the data being transmitted over the network, including the types of traffic, sources, destinations, and patterns of usage.

Types of Analysis

Analysis:

- **Real-Time Monitoring**: Continuously monitors network traffic to provide real-time insights and alerts.
- **Historical Analysis**: Stores captured data for later analysis, allowing for trend analysis and forensic investigations.
- **Traffic Patterns**: Identifies patterns such as peak usage times, common sources and destinations, and typical traffic types.

1. **Which protocol is used for transferring files over the internet?**
    - A) HTTP
    - **B) FTP**
    - C) SMTP
    - D) DNS
2. **Which protocol is used to retrieve emails from a remote server to a local email client?**
    - A) HTTP
    - B) FTP
    - **C) POP3**
    - D) SNMP
3. **What is the primary function of the DNS protocol?**
    - A) Transferring files
    - B) Sending emails
    - C) **Resolving domain names to IP addresses**
    - D) Monitoring network devices
4. **Which protocol is used for web browsing?**
    - **A) HTTP**
    - B) FTP
    - C) SMTP
    - D) SNMP
5. **Which protocol is used for securely transmitting HTTP data over the internet?**
    - **A) HTTPS**
    - B) FTP
    - C) SMTP
    - D) IMAP
6. **Which application layer protocol is used for network management?**
    - A) DNS
    - B) HTTP
    - **C) SNMP**
    - D) FTP
7. **What does SMTP stand for?**
    - **A) Simple Mail Transfer Protocol**
    - B) Secure Mail Transfer Protocol
    - C) Simple Message Transfer Protocol
    - D) Secure Message Transfer Protocol
8. **Which protocol allows users to access and manipulate remote files as if they were local?**
    - A) HTTP
    - **B) FTP**
    - C) Telnet
    - D) IMAP
9. **Which protocol is used to send emails from a client to a server?**

- A) POP3
- B) IMAP
- **C) SMTP**
- D) HTTP

10. **Which of the following is a distributed database that translates domain names to IP addresses?**
    - A) DHCP
    - **B) DNS**
    - C) FTP
    - D) NTP
11. **What is the default port number for HTTP?**
    - A) 20
    - B) 21
    - **C) 80**
    - D) 443
12. **What is the main purpose of the IMAP protocol?**
    - A) To send emails
    - **B) To retrieve and manage emails on a remote server**
    - C) To transfer files
    - D) To monitor network devices
13. **Which protocol is used to synchronize the clocks of computers over a network?**
    - **A) NTP**
    - B) FTP
    - C) HTTP
    - D) SMTP
14. **Which protocol is commonly used for remote command-line login and remote execution of commands?**
    - A) FTP
    - **B) Telnet**
    - C) HTTP
    - D) DNS
15. **What is the function of the DHCP protocol?**
    - A) To resolve domain names
    - **B) To assign IP addresses to devices on a network**
    - C) To transfer files
    - D) To send emails
16. **Which protocol uses port 53?**
    - A) HTTP
    - B) FTP
    - **C) DNS**
    - D) SMTP
17. **Which protocol is used for accessing web pages securely over the internet?**
    - A) HTTP
    - **B) HTTPS**

    - C) FTP
    - D) SNMP
18. **Which application layer protocol provides a method for end users to upload and download files from a remote server?**
    - A) SMTP
    - **B) FTP**
    - C) IMAP
    - D) SNMP
19. **Which of the following protocols is used to receive emails by downloading them from a remote mail server?**
    - A) SMTP
    - **B) POP3**
    - C) HTTP
    - D) SNMP
20. **Which protocol helps in translating human-friendly domain names to IP addresses?**
    - A) DHCP
    - **B) DNS**
    - C) HTTP
    - D) IMAP

Answers:

1. B) FTP
2. C) POP3
3. C) Resolving domain names to IP addresses
4. A) HTTP
5. A) HTTPS
6. C) SNMP
7. A) Simple Mail Transfer Protocol
8. B) FTP
9. C) SMTP
10. B) DNS
11. C) 80
12. B) To retrieve and manage emails on a remote server
13. A) NTP
14. B) Telnet
15. B) To assign IP addresses to devices on a network
16. C) DNS
17. B) HTTPS
18. B) FTP
19. B) POP3
20. B) DNS