

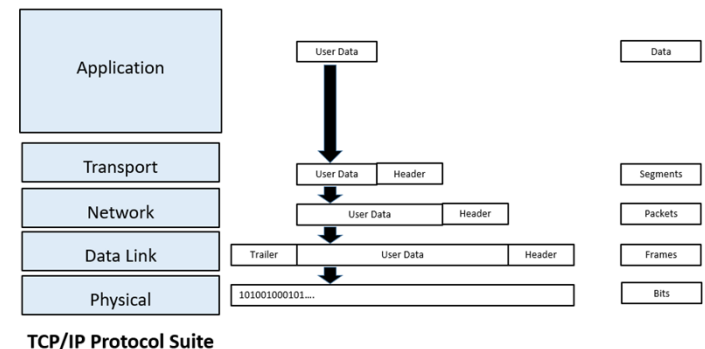
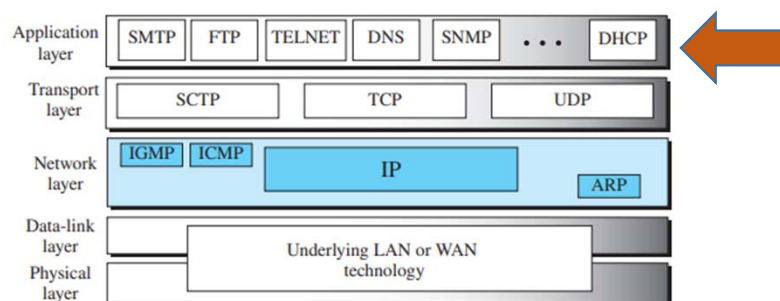
Fundamentals of Computer Networks

Understand computer network technology

Lesson 5

Application layer(Recall)

- The main duty of this layer is to take data from the applications and deliver it to the transport layer and collect data from the transport layer and deliver it to the correct applications. It contains a huge group of high-level protocols that cover a wide range of applications.
- The most common is the Hyper Text Transfer Protocol (HTTP). Other widely used application layer protocols are File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Post Office Protocol 3 (POP3), Telnet, and Domain Name Service (DNS).

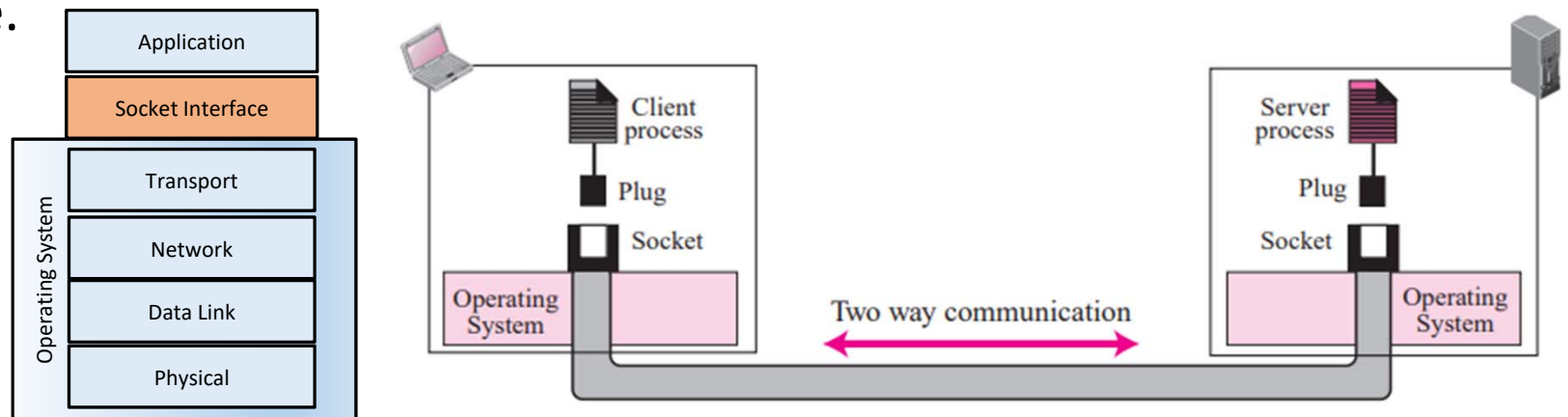


Socket

interface

Socket

- A socket is an endpoint of communication between 2 devices on a network.
- It is an interface between the application layer and transport layer.
- It is located between the operating system and application programs.
To access the services provided by the TCP/IP protocol suite, an application needs to use the instructions define in the socket interface.

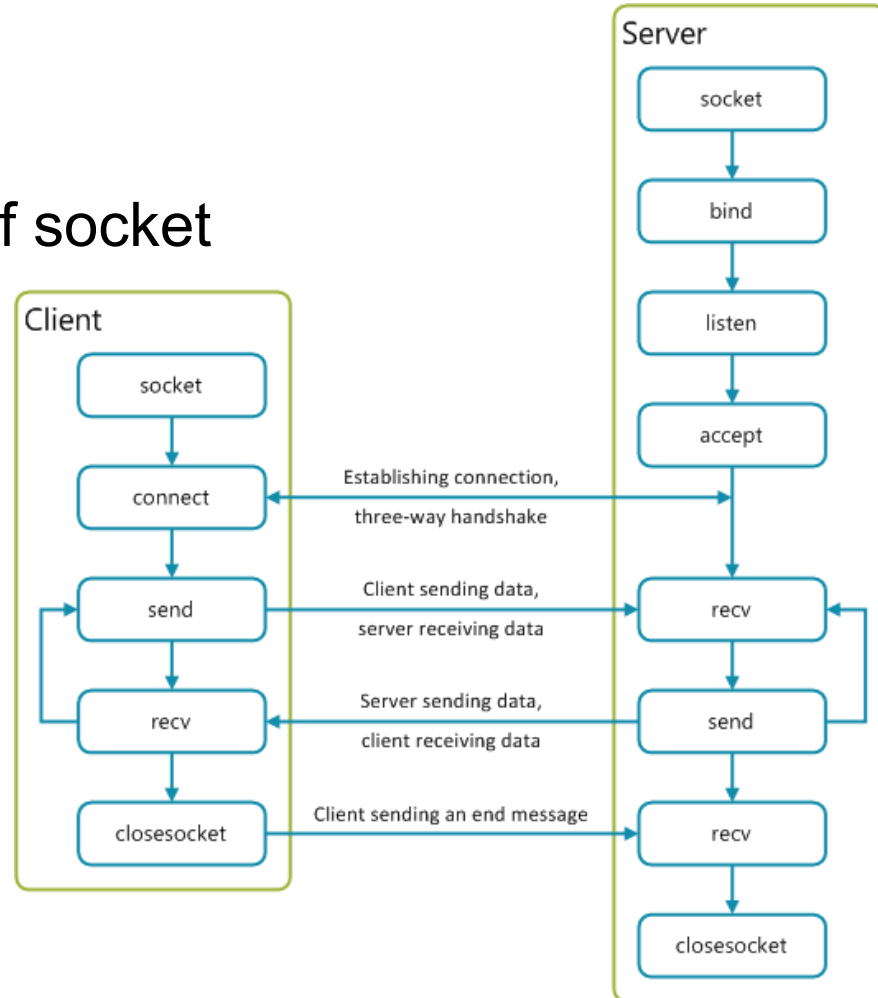


Socket

- Type of socket:
 - Stream Socket (TCP)
 - connection oriented, reliable, ordered , error-checked delivery
 - Datagram Socket (UDP)
 - fast, unreliable , connectionless communication
- Socket Address consists of a combination of IP address and port number

Socket

Basic communication flow of socket



https://www.keil.com/pack/doc/mw6/network/html/using_network_sockets_bsd.html

Client-Server

Architecture

Client-server architecture - Server

- Client-server architecture is a network design model in which multiple client devices communicate with and request services from a central server.
- A server is a computer or program that provides services or resources to clients over a network.
- A server program is an infinite program. When it starts, it runs infinitely unless a problem arises or shuts down.
- It waits for incoming **requests from clients**. When a request arrives, it **responds to the request**.
- Eg. Web server, file server, database server, email server

Client-server architecture - Client

- A client is a computer or program that initiates a request for services or resources from a server over a network.
- A client program is finite - it is started by the user (or another application program) and terminates when the service is complete.
- A client opens the communication channel using the IP address of the remote host and the well-known port address of the specific server program running on that machine.
- After a channel of communication is opened, the client sends its request and receives a response. Although the request-response part may be repeated several times, the whole process is finite and eventually comes to an end.
- Example : Web browser, Email program

Client and Server – Advantage

- Centralized resource management
 - Server holds and manages resources – files, databases, applications etc
 - Allow for central control of data, security policies, backups and user access
- Scalability
 - New clients can be added easily without changing the system
 - Server can be upgraded (add more resources – RAM or using load balancing) to serve more clients.
- Improved security
 - Enforce security policies from the server side
 - Example: user authentication, file permissions and monitoring network traffic

Client and Server - Advantage

- Ease of maintenance
 - Software updates, backups and system configuration are done on the server – reduce the need to configure every client device
- Reliability and consistency
 - Data stored on the server is kept consistent, all clients access from one source which should be most up-to-date
- Remote access support
 - Clients can access servers from anywhere over the internet, enabling remote work, cloud services and web applications

Client and Server - Disadvantage

- Single point of failure
 - If server is down, all clients lose access to services
- High cost of setup and maintenance
 - Servers are expensive and require skilled administrators.
 - Initiate infrastructure and licensing costs can be high
- Network congestion and overload
 - Possibility of network congestion, server overload, slow down the network
- Complexity
 - Configuration and management of a secure and efficient server environment can be complex
- Network dependence
 - Clients rely heavily on a stable network connection required

Peer-to-peer (P2P) Architecture

- A Peer-to-Peer (P2P) architecture is a decentralized network model where each computer (*peer*) acts both as a client and a server.
- There is no central server. Each peer can request and provide services or resources directly to other peers
- Key features :
 - All peers have equal role – they can initiate (sent a request) or response to a request
 - Decentralized – no central point of control – resources are distributed among peers
 - Resource sharing – resources or services are shared among peers
 - Autonomy – each peer manages its own resources and may be online or offline at anytime
- Example: BitTorrent peer-to-peer file sharing, blockchain networks

Peer-to-peer (P2P) – Advantage

- Low cost – no need for expensive server hardware or infrastructure.
- Scalability – New peers can join the network easily to contribute resources. System can grow without major reconfiguration.
- No single point of failure – one peer fails does not affect the whole network – limited impact to the network.
- Resource sharing – peers can share files, processing power or bandwidth directly with others.

Peer-to-peer (P2P) – Disadvantage

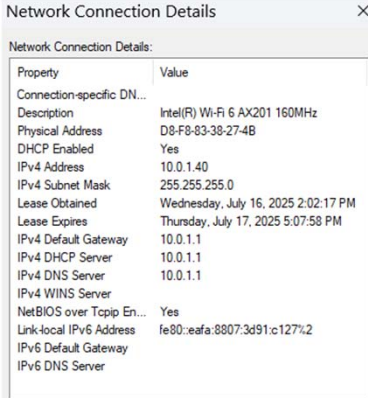
- Lack of centralized control – no central authority to manage users, resources and security. Harder to enforce rules and monitor activity
- Security risks – each peer is responsible for its own security. Malicious peers can spread malware or unauthorized content
- Data Consistency issues – files in peers not guarantee to be up-to-date. Synchronization is difficult
- Performance – performance suffers if there are few online peers or peers have low bandwidth

Application Layer

Protocols

DHCP

- Dynamic Host Configuration Protocol (DHCP)
- Automatically assign IP addresses and other network configuration parameters to devices (clients) on a network.
 - IP address
 - Subnet masks
 - Default gateways
 - DNS server addresses
 - Lease duration
- without DHCP, every device would need to be manually configured
 - error-prone
 - inefficient
 - unscalable



A screenshot of the 'Network Connection Details' window in Windows. The window title is 'Network Connection Details' with a close button. Below the title bar, it says 'Network Connection Details:'. The main content is a table with two columns: 'Property' and 'Value'. The table lists various network properties and their current values.

Property	Value
Connection-specific DN...	
Description	Intel(R) Wi-Fi 6 AX201 160MHz
Physical Address	D8-F8-83-38-27-4B
DHCP Enabled	Yes
IPv4 Address	10.0.1.40
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Wednesday, July 16, 2025 2:02:17 PM
Lease Expires	Thursday, July 17, 2025 5:07:58 PM
IPv4 Default Gateway	10.0.1.1
IPv4 DHCP Server	10.0.1.1
IPv4 DNS Server	10.0.1.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::eafa:8807:3d91:c127%2
IPv6 Default Gateway	
IPv6 DNS Server	

DHCP

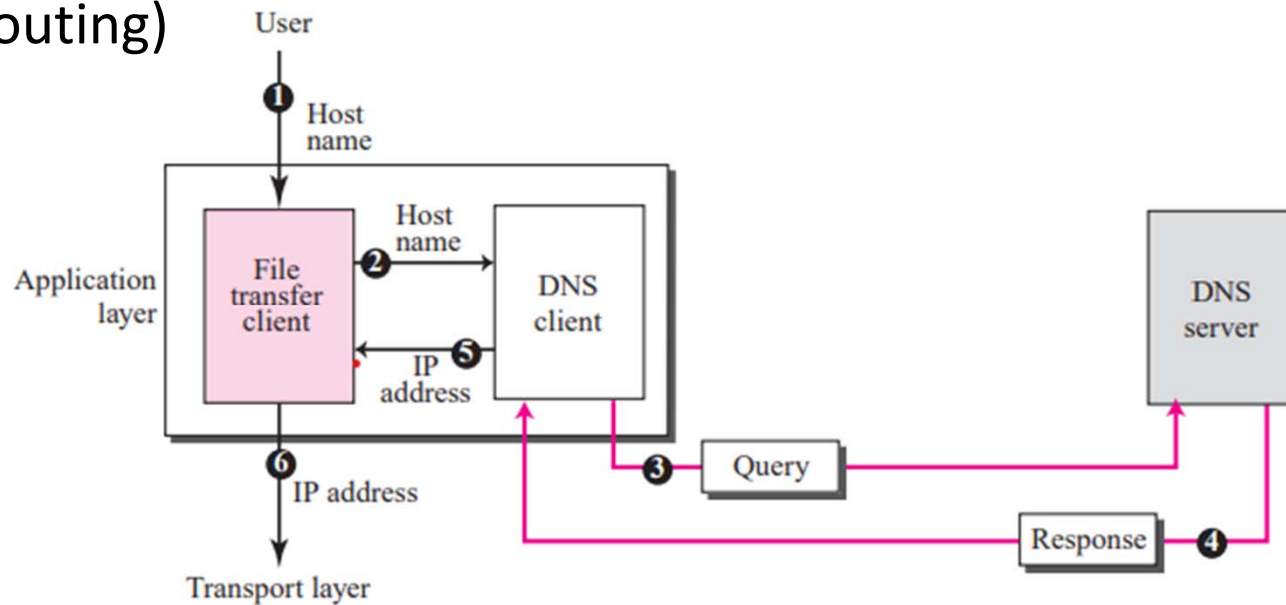
- How it works? (DORA)
 - **D**iscover – client sends a broadcast to find available DHCP servers
 - **O**ffer – DHCP server replies with an offer including an IP address and configuration
 - **R**quest – client requests to use the offered IP address
 - **A**cknowledge – server confirms and leases the IP address to the client
- Uses UDP for sending a broadcast to find available DHCP servers
 - Client device does not have an IP address – cannot use TCP as connection needs to be established
 - Light-weight, minimal overhead
 - Connectionless – no handshakes, no session setup

DHCP

- Type of IP address allocation:
 - Static IP address
 - Manual configuration – device manually configured with its IP address, subnet mask, gateway and DNS. DHCP server is not involved – no DHCP request is sent
 - DHCP reservation - using MAC address of the specific device – always get the same IP address from the DHCP pool. A DHCP request is required to obtain the IP address.
 - Dynamic IP address
 - DHCP server leases a dynamic IP address (reusable) to the client for a period of time. (previously mentioned)

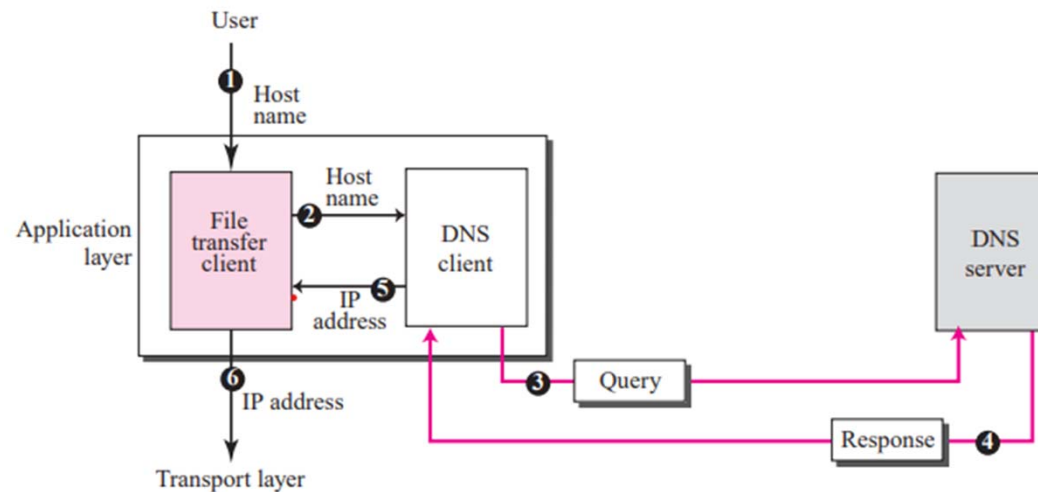
DNS

- Domain Name System (DNS)
- Translates domain names (www.google.com) into IP address (for routing)



User uses a file transfer client to access file transfer server at a remote host. Only the server name abc.com is known, but TCP/IP suite needs IP address of the server to make a connection.

DNS

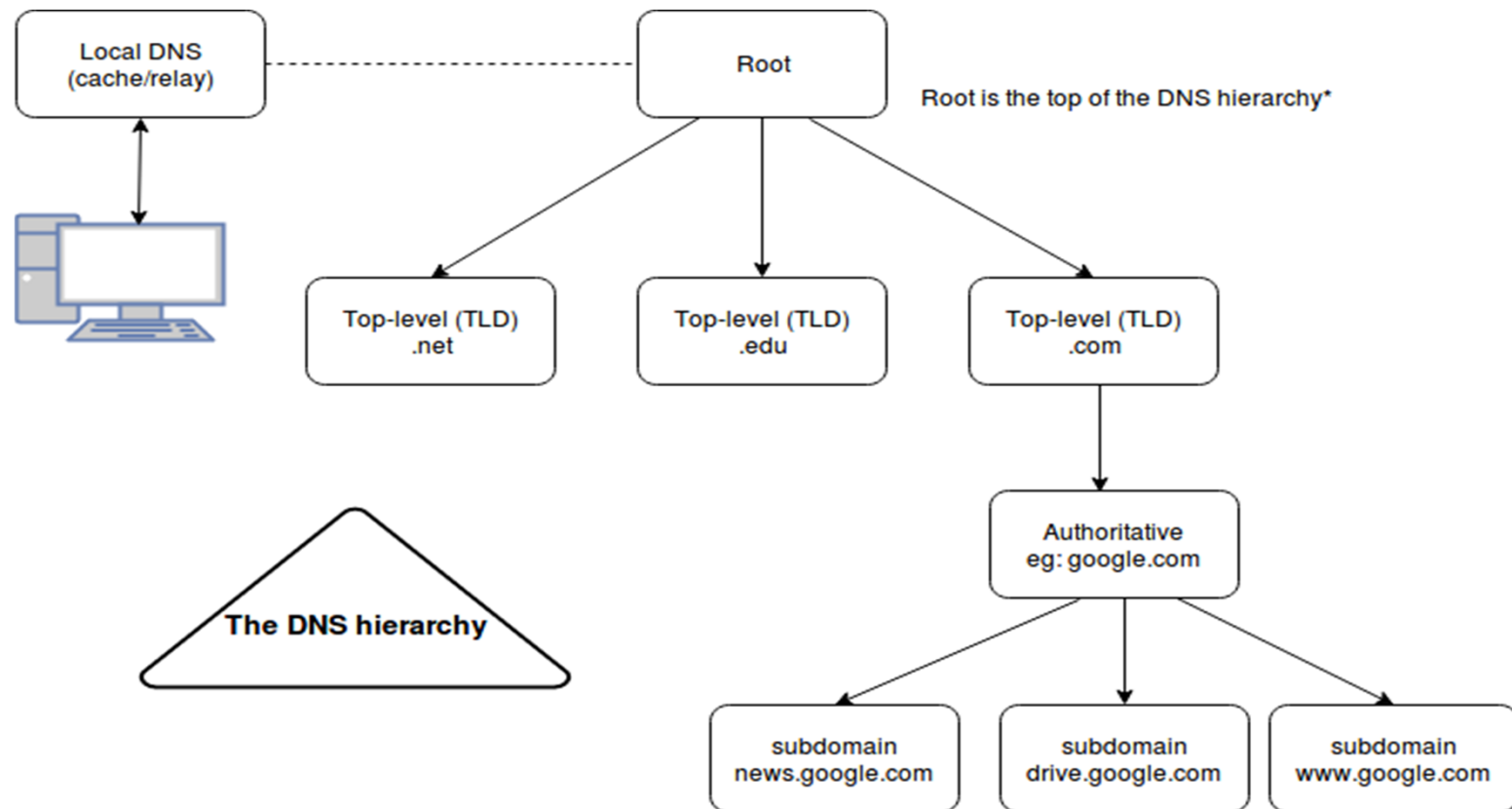


The following steps (simplified) map host name to IP address:

1. User passes host name to file transfer client (FTC).
2. FTC passes the host name to DNS client.
3. DNS client sends a message to DNS server with a query containing the FT server name, using IP address of DNS server.
4. DNS server responds with IP address of the FT server
5. DNS client passes the IP address to the FT client
6. FT client uses IP address to access the FT server

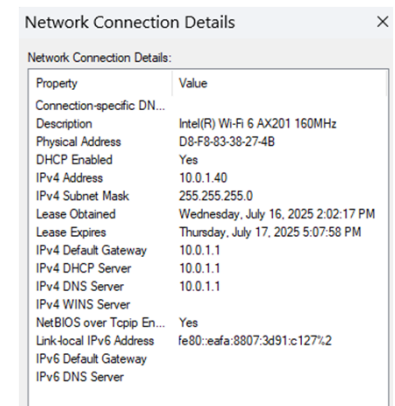
Network Connection Details	
Network Connection Details:	
Property	Value
Connection-specific DN...	
Description	Intel(R) Wi-Fi 6 AX201 160MHz
Physical Address	D8-F8-83-38-27-4B
DHCP Enabled	Yes
IPv4 Address	10.0.1.40
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Wednesday, July 16, 2025 2:02:17 PM
Lease Expires	Thursday, July 17, 2025 5:07:58 PM
IPv4 Default Gateway	10.0.1.1
IPv4 DHCP Server	10.0.1.1
IPv4 DNS Server	10.0.1.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::eafa:8807:3d91:c127%2
IPv6 Default Gateway	
IPv6 DNS Server	

DNS – Domain Name System Hierarchy



DNS - Name-address Resolution Steps

1. Check local cache (on the host/ DNS client):
 - The client (resolver) checks its own cache.
 - If IP address is found, client uses the IP address to route the message in the network
2. Query Local DNS server (ISP's DNS resolver)
 - If not found locally, the client sends the query to the DNS server specified in the IP configuration
 - The server checks its own cache



Property	Value
Connection-specific DN...	
Description	Intel(R) Wi-Fi 6 AX201 160MHz
Physical Address	D8-F8-83-38-27-4B
DHCP Enabled	Yes
IPv4 Address	10.0.1.40
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Wednesday, July 16, 2025 2:02:17 PM
Lease Expires	Thursday, July 17, 2025 5:07:58 PM
IPv4 Default Gateway	10.0.1.1
IPv4 DHCP Server	10.0.1.1
IPv4 DNS Server	10.0.1.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::eafa:8807:3d91:c127::2
IPv6 Default Gateway	
IPv6 DNS Server	

DNS - Name-address Resolution Steps

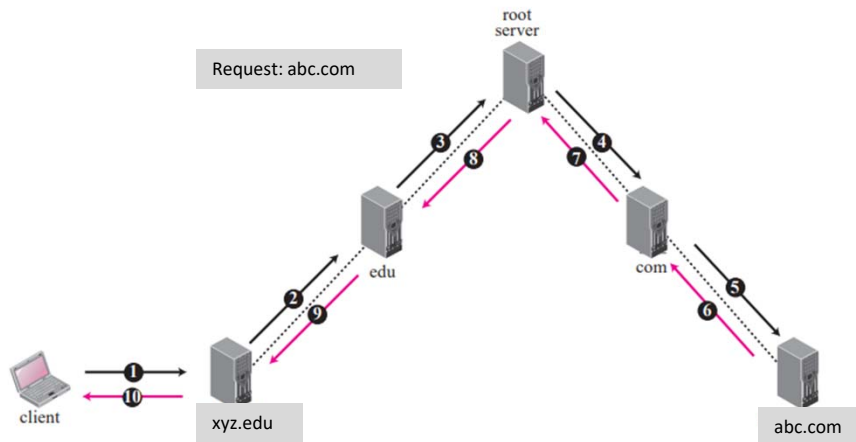
3. Query the Global DNS hierarchy (if not cached)

- If the ISP DNS resolver does not have the answer, it must contact the DNS hierarchy.
- 2 resolution methods (based on client resolver)
 - Recursive resolution – ISP DNS resolver will resolve the name.
 - Root DNS Server → direct to the Top-Level Domain (TLD) server (eg. .com, .org, .sg)
 - TLD Server → direct to the Authoritative DNS Server for the domain
 - Authoritative DNS Server → returns the actual IP address
 - Iterative resolution -client resolver/local ISP DNS resolver performs queries step by step, using referrals from each server
 - Root DNS Servers → returns address of a TLD server
 - TLD Server → returns the address of authoritative DNS server
 - Authoritative DNS Server → returns the actual IP address

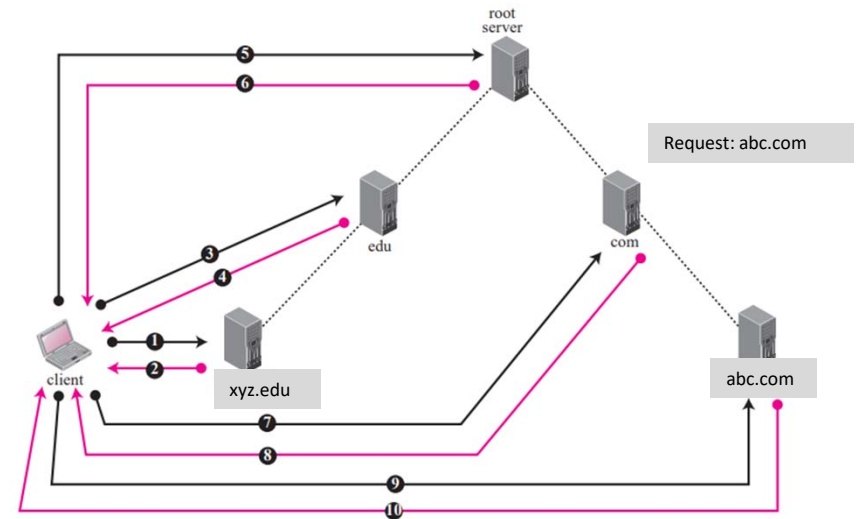
DNS - Name-address Resolution Steps (Info)

4. Return IP address to client

- DNS resolver sends the resolved IP address back to the client
- client uses the IP address to route the message in the network



Recursive resolution



Iterative resolution

DNS –Caching (Info)

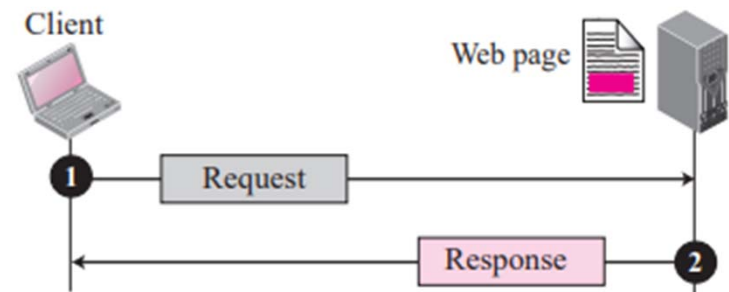
- Caching - mechanism used by DNS to reduce search time
 - When a server asked for a mapping from another server and receives the mapping, it stores this mapping in its cache memory before sending it to the client.
 - When a client asks for the same mapping, the server checks its cache memory and resolve it. To inform the client that the mapping is from the cache and not from an authoritative source, the server marks the mapping as unauthoritative.
- Problem with caching – mapping might be outdated.
 - Time-to-live (TTL) – time in seconds that the server can cache
 - TTL is added to each mapping.
 - Mapping with expired TTL will be purged periodically

DNS –Why uses UDP?

- Why uses UDP ?
 - Speed – fast as users expect pages to load fast – UDP does not need to establish a connection setup
 - Small size – DNS queries and responses easily fit in one UDP datagram
 - Low overhead – simple header –requires less processing time and bandwidth
 - Stateless – simple request and response – does not need to maintain connection
- DNS will sometime use TCP (Info)
 - DNS servers syncing data
 - Response are large (eg IPv6)

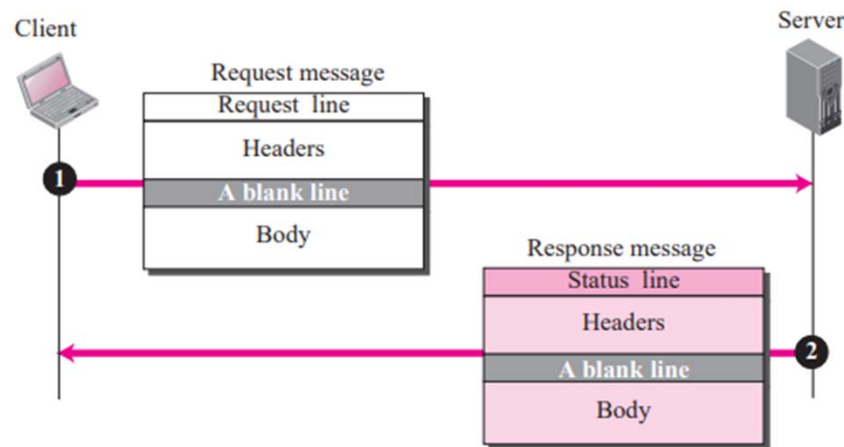
HTTP

- Hypertext Transfer Protocol (HTTP) –allow clients (eg. browsers) to fetch hypertext documents, images, scripts etc from the web server.
- Uses Port 80, 443 (HTTPS)
- Uses client-server model:
 - Client sends a **HTTP request**
 - Server responds with a **HTTP response**
- Stateless – Server does not keep information about the client. Each request-response pair is independent.



HTTP

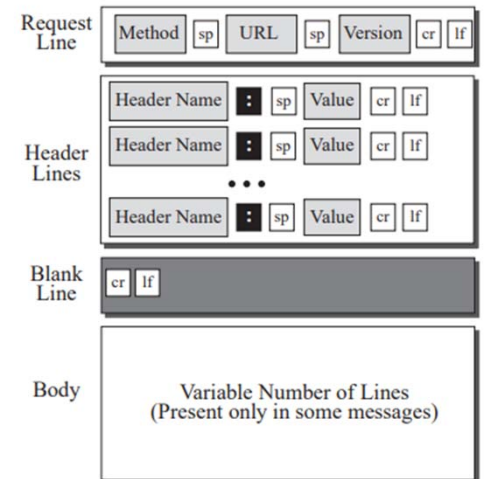
- HTTP transaction between the client and server.
- HTTP is a stateless protocol –server does not keep information about the client. The client initializes the transaction by sending a **request**. The server replies by sending a **response**.



HTTP

- HTTP request includes
 - Request line – GET /test.html HTTP/1.1
 - HTTP command/method that the client wants to perform - GET
 - Path of the relevant document - test.html
 - Version of the HTTP used by the client - HTTP/1.1
 - Header fields – provide additional information to the web server – Host: example.com
 - Message body (optional) – for POST requests message body contains the data submitted.

```
GET /home HTTP/1.1
Host: www.example.com
User-Agent: Mozilla/5.0
Accept: text/html
Connection: keep-alive
```



sp: Space
cr: Carriage Return
lf: Line Feed

HTTP

- HTTP response includes

- Status line - summarises whether the server is able to perform the request from the client - HTTP/1.1 200 OK
 - HTTP version used by the server – HTTP/1.1
 - Status code: reason phrase – 200: OK, 404: Not found, 500: Internal Server Error
- Header fields – provide additional information
Content-Type: text/plain
- Message body – contain document in format specified by Content-Type header field

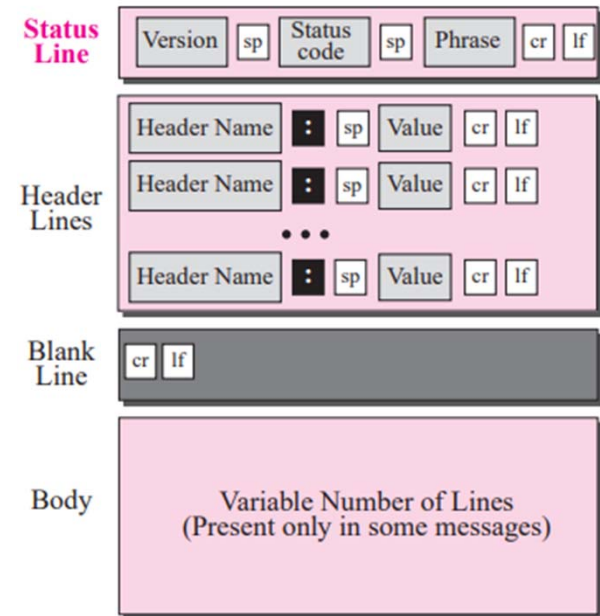
HTTP/1.1 200 OK

Date: Mon, 18 Aug 2025 10:00:00 GMT

Server: Apache/2.4.1

Content-Type: text/html; charset=UTF-8

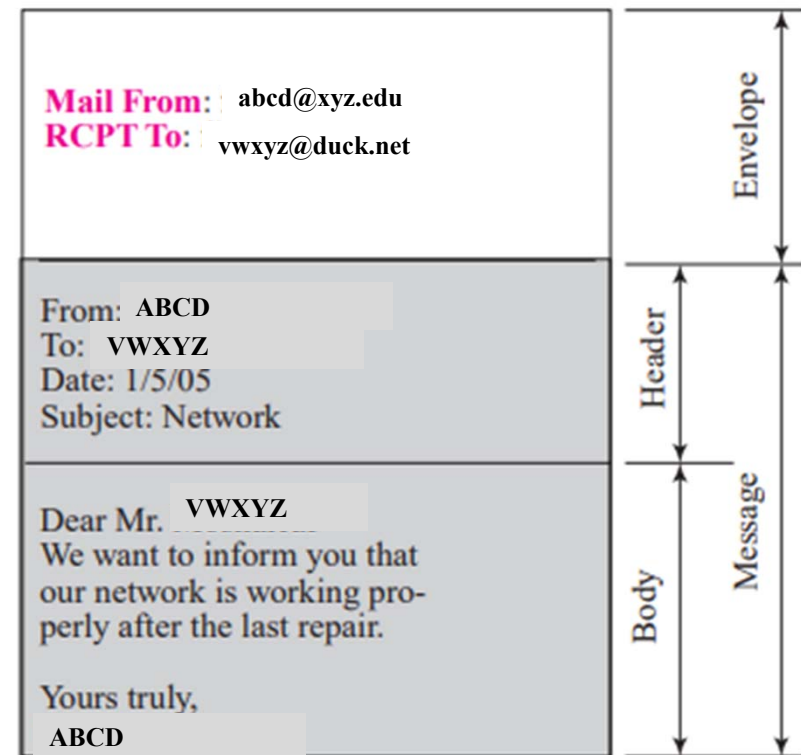
Content-Length: 1256



sp: Space
cr: Carriage Return
lf: Line Feed

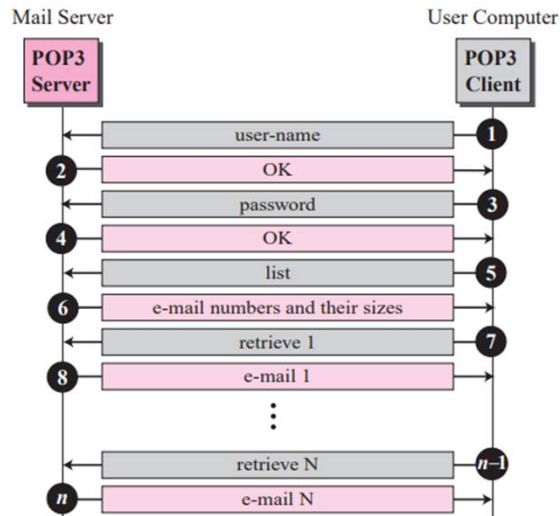
SMTP

- Simple Mail Transfer Protocol – protocol used to send/relay email across the internet, **not for retrieving email**.
- Uses Port 25/587 (secure)
- Uses client-server model
- SMTP Message Structure:
 - Envelope (Control Information)
 - MAIL FROM – sender address
 - RCPT TO – recipient address
 - DATA – begin message content
 - Message Headers – describes sender, receiver, content type etc
 - Message Body – content of email



POP3

- Post Office Protocol v3 – protocol to download emails from server to client and delete the message from the mailbox on the server
- Uses Port 110/995 (secure)
- Uses client-server model – email client and server



- Mail access starts with the client.
- The client opens a connection to the server on TCP port 110.
- It then sends its user name and password to access the mailbox.
- The user can then list and retrieve the mail messages, one by one.

IMAP4

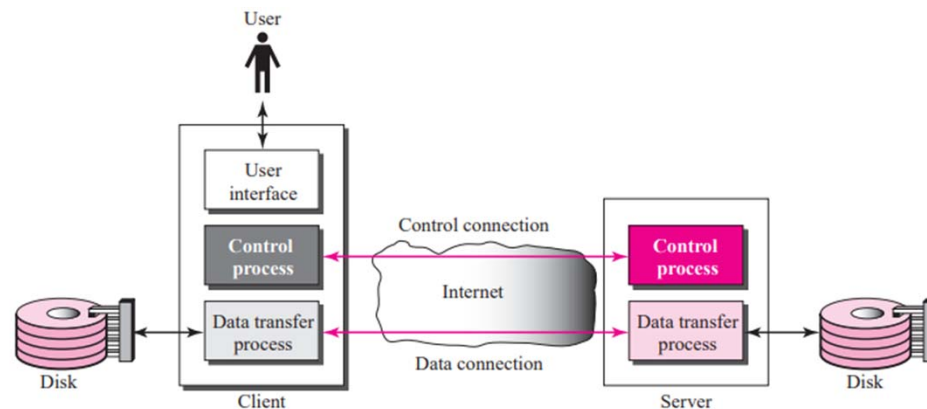
- Internet Message Access Protocol v4 – similar to POP3 and allow user to view and manage messages on the server.
- It allows user to access mail messages from multiple locations (email clients) and ensure that all copies are synchronized and consistent.
- Extended functionality:
 - Obtain information about the message or examine header fields without retrieving the entire message
 - Search and retrieve portions of a message – partial retrieval is useful for slow-speed connections.
- Uses Port 143/993 (secure)
- Microsoft Outlook, Apple Mail, Mozilla Thunderbird, Webmail email client uses IMAP4

FTP

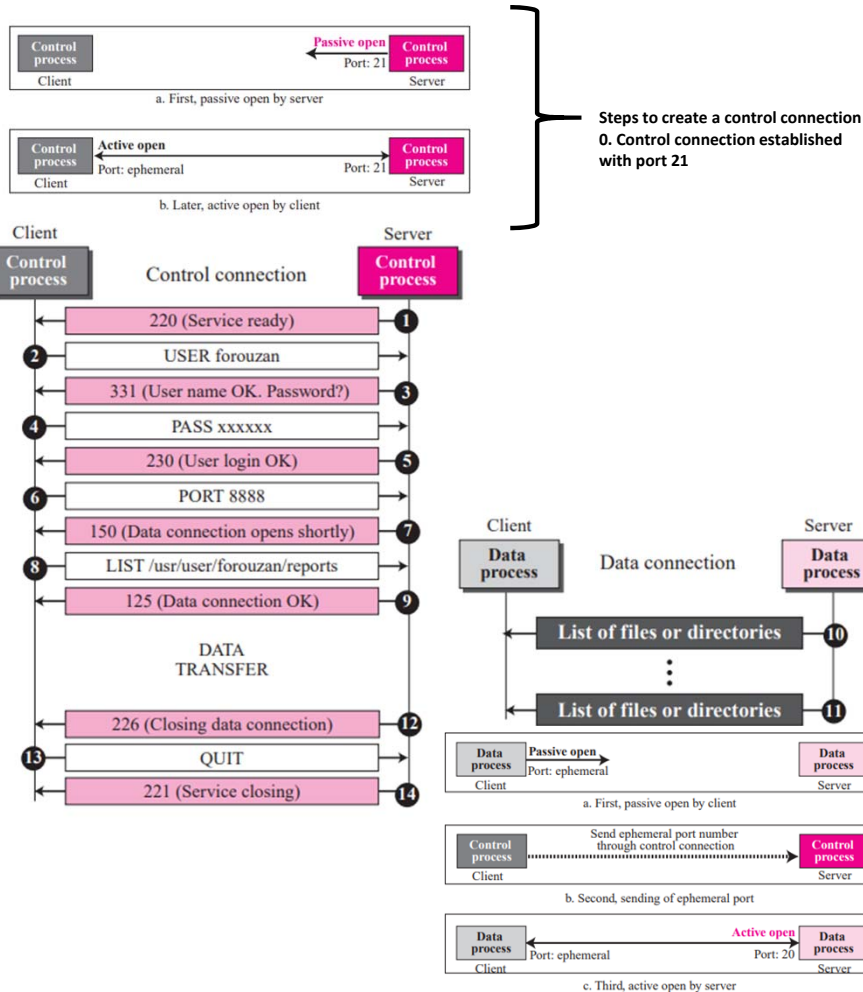
- File Transfer Protocol - protocol for copying a file from one host to another.
- FTP resolves some problems with 2 host having
 - different file name conventions
 - different ways of representing text and data
 - different directory structures
- FTP differs from other client-server applications as it establishes 2 connections between the hosts. One for control information (port 21) and the other for data transfer (port 20).

FTP

- Control Connection (port 21)
 - Used for commands from clients and response from server
 - Remains open during the session
- Data Connection (port 20)
 - Used for file transfer – upload, download and directory listing
 - Open when needed and closed after data transfer



FTP (Info)



0. Control connection established with port 21.

1. FTP Server sends 220 (service ready) response on the control connection.

2. Client sends USER command

3. Server responds with 331 (user name is OK, password is required)

4. Client sends PASS command

5. Server responds with 230 (user login is OK)

6. Client issues an ephemeral port for data connection and sends PORT command to give this port number to server

7. Server prepares itself for issuing an active open on the data connection between port 20 and the ephemeral port received from the client. Sends response 150 (data connection will open)

8. Client send LIST message

9. Server responds with 125 (data connection OK) and opens data connection.

10. Server sends list of files/directories on data connection. When the whole list is sent, server responds with 226 (closing data connection) over control connection.

11. Client either sends QUIT command to request closing control connection or send another command to start new activity (open another data connection)

12. Server responds with 221 (service closing) after receiving QUIT command and then closes the control connection.

Steps to create a data connection

6. Client issues an ephemeral port

7. Server issue an active open on data connection

END