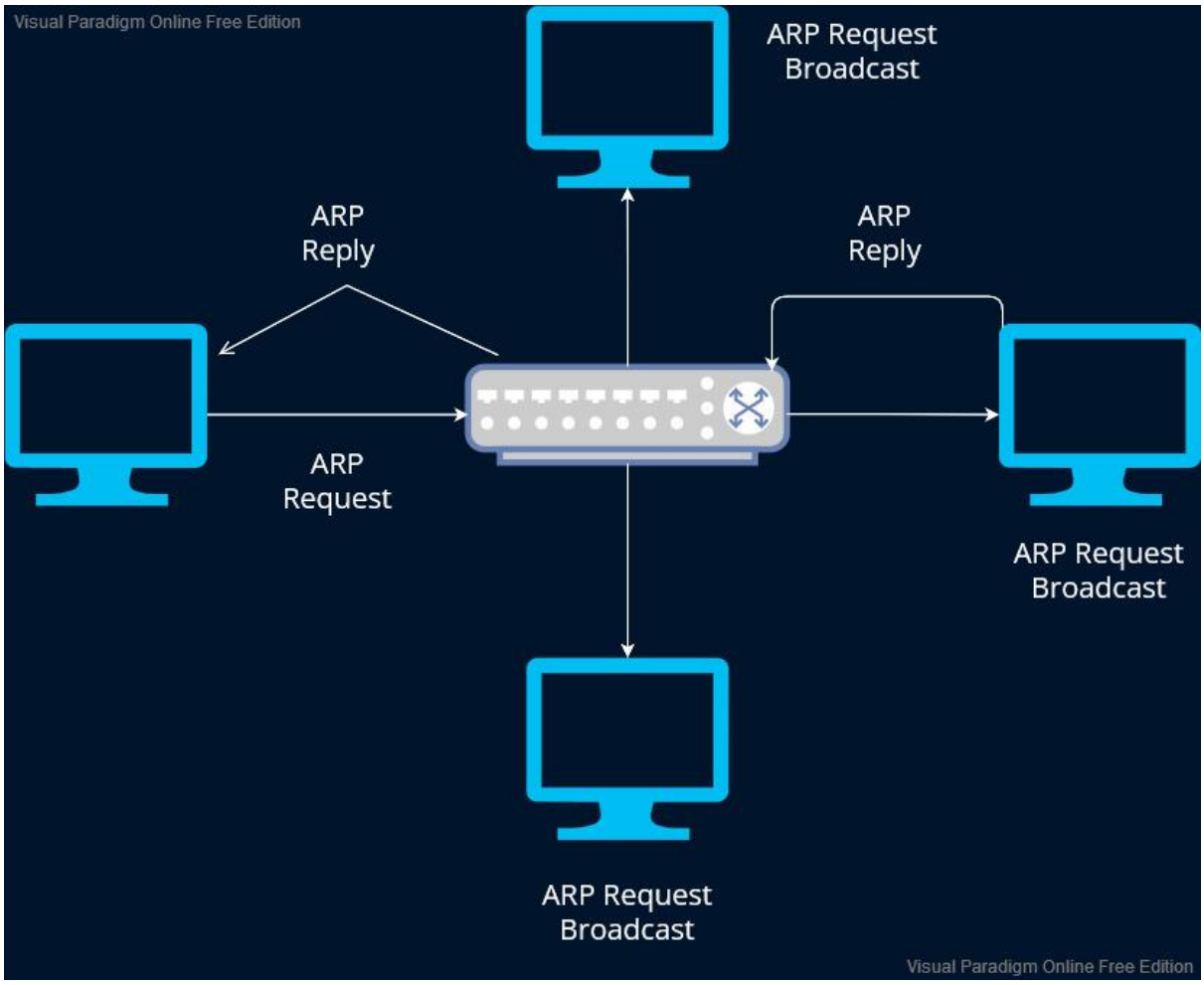
https://blueteamresources.in/common-networking-protocols-and-their-working/

Some important Protocols and how they work.

ARP (Address Resolution Protocol): ARP is a OSI layer 2 protocol used to map addresses from the Network layer to the Data Link layer. It identifies the MAC Address (physical address which is on the Network Interface Card (NIC)) given the IP Address. The layer 2 device Switch maintains an ARP Table. Hosts also maintain an ARP Table. Let's see how MAC Addresses are populated. First the host device broadcasts an ARP Request with a destination IP Address for which it does not know the MAC Address. The device which owns this IP Address, replies with its MAC Address (ARP Reply) to the device which requested (unicast). Then the host updates its MAC table. When the source device sends the ARP request, if configured, other devices will also update their ARP Table with the source's MAC Address.



DHCP (Dynamic Host Configuration Protocol): DHCP is a protocol used to assign IP address to machines that join a network. It is dynamic because the IP Address can be changed the next time it joins the network. Static IP Address too can be configured which don't change. DHCP uses UDP at the Transport layer since it cannot establish connections as in TCP. For TCP, both endpoints should have IP Addresses. DHCP uses UDP Port 67 & 68. Let's see how the DHCP Protocol works. You can remember it with the abbreviation **DORA**.

1) Discover: Host connecting to network (cable or wireless) sends DHCP discover message with its MAC Address to all hosts in the subnet (broadcast). Frame with this **DISCOVER** message hits the DHCP Server.

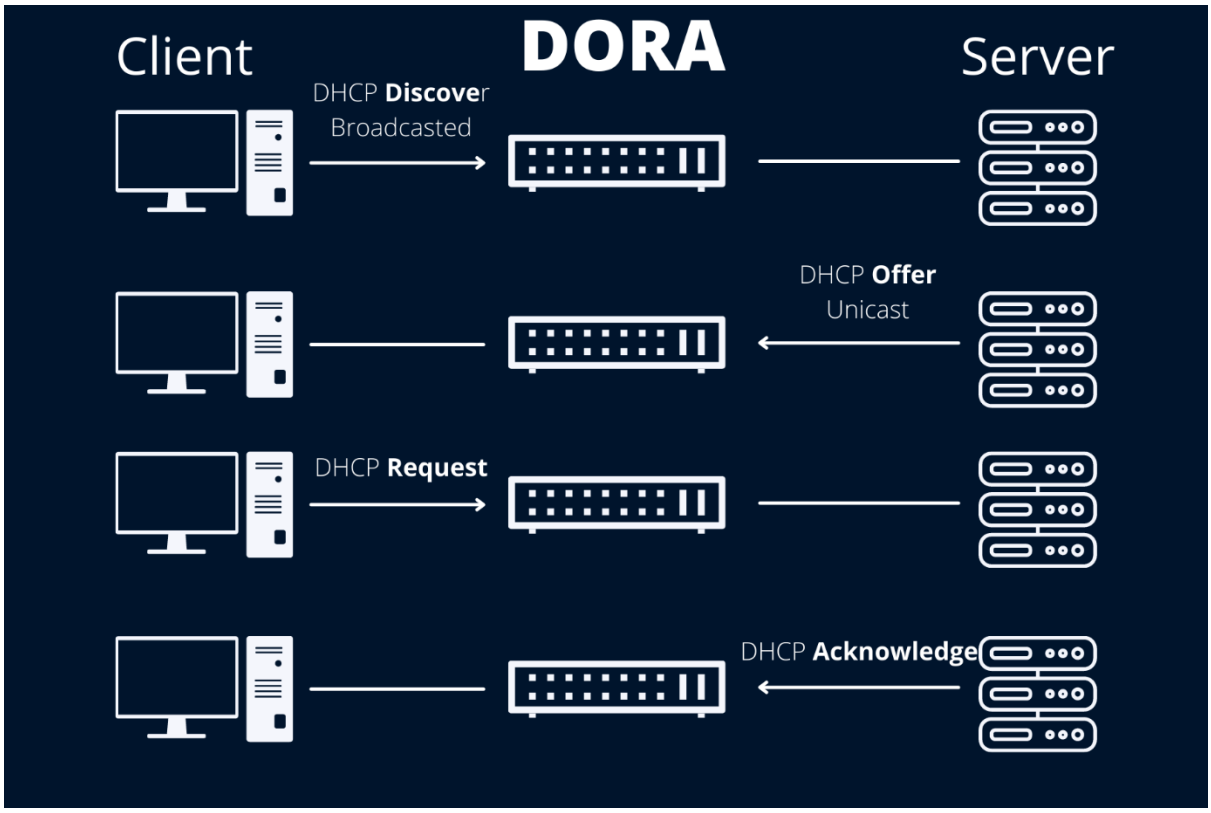
2) Offer: After the DHCP Server receives discover message it suggests the IP addressing offering to the client host by unicast based on the MAC Address. This is the **OFFER** message.

3) Request: Since the host (DHCP Client) doesn't have an IP assigned yet, it still cannot communicate using IP Addresses. So, it broadcasts a **REQUEST** message which reaches the server.

4) Acknowledge: Server sends **ACKNOWLEDGE** message confirming the DHCP lease to client. Now client is allowed to use new IP settings.

The DHCP maintains an IP Pool and lease period which is the duration for which an IP address Is assigned to the client. Once this expires the DHCP server checks if the system is up. If it is, then the lease period is renewed. If not, the IP is returned back to the IP Pool.

The DHCP server assigns IP address, subnet mask, gateway, DNS server IP, lease period.

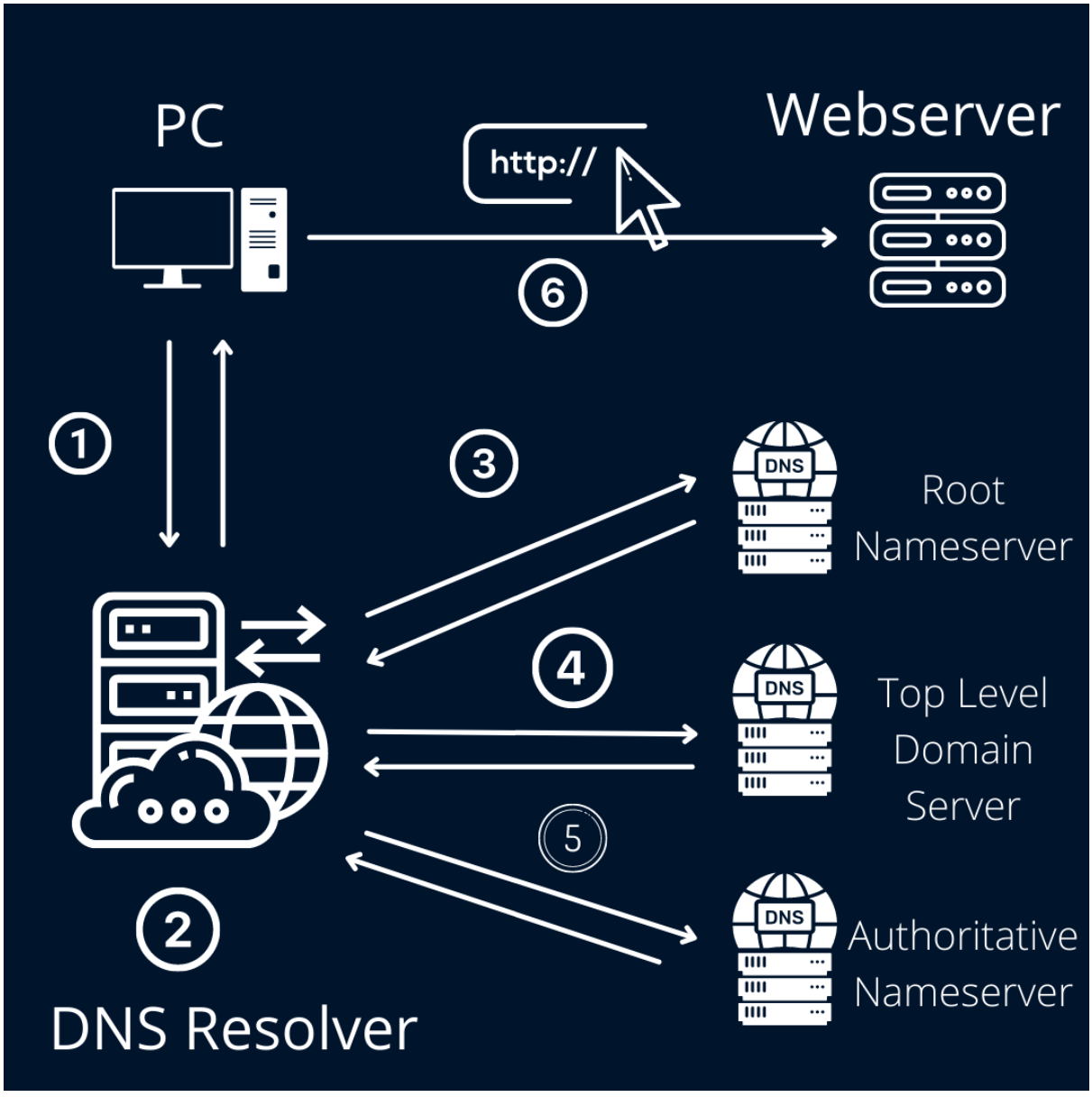


DNS (Domain Name System): The Domain Name System (DNS) is the phonebook of the Internet. IP addresses are of numerical format and hence they are not easily readable or rememberable to humans. Hence, we use Domain names (google.com). DNS takes these domain names and converts them into IP address based on DNS Records. These records contain different types of information such as A (ipv4 address), AAAA (ipv6 address), MX (email server), NS (name server), LOC (location),

PTR (pointer), SOA (start of authority), SRV (service). DNS uses UDP port 53. It is UDP because the destination IP is not available yet. Let's see how it works.

The DNS uses many servers to get the answer records back to the host. A DNS query (domain name) is parsed from right to left.

1) If the IP information is not stored in the host, it reaches out to the local DNS server (usually maintained by ISP).
2) If the information is not present there, the local DNS servers starts a recursive function where a hierarchical system is used to get the results.
3) At the top we have the root name servers which point to the Top-Level Domains (TLD) (.com OR .org OR .net etc.).
4) Then the TLD responds with the IP of the nameserver.
5) Then, the name server responds with the IP of the website (example.com).
6) After the IP is obtained, communication starts.



HTTP (Hyper-text Transfer Protocol): HTTP is a request-response protocol. The browser initiates a request and the server gives the response. There are many types of requests such as GET (get resource), POST (add/create), PUT (modify/update), DELETE, etc. It uses TCP port 80 and for secure communications, port 443 (HTTPS). The server responds along with a response code. If it starts with 1 – information, 2 – success, 3 – redirect, 4 – client error, 5 – server error.

What exactly happens when we enter a domain name in a browser?

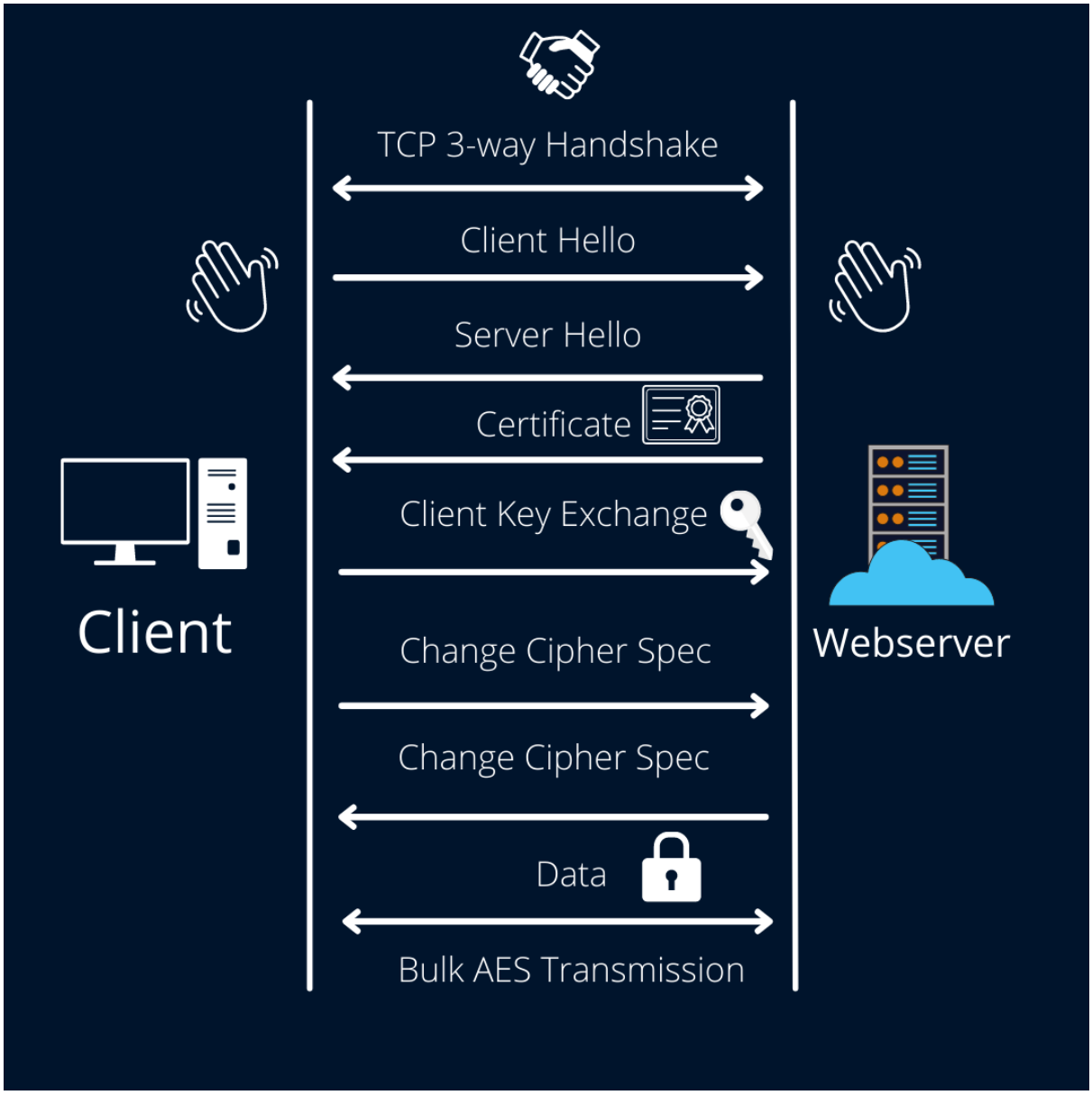
1) Check the browser cache first if the content is present in cache and display the same.
2) If not, the browser checks if the IP of the URL is present in the cache (browser and OS) if not then it requests the OS to do a DNS lookup using UDP to get the corresponding IP address of the URL from the DNS server to establish a new TCP connection.
3) A new TCP connection is set between the browser and the server using the three-way handshake.
4) An HTTP request is sent to the server using the TCP connection.
5) The web servers running on the Servers handle the incoming HTTP request and send the HTTP response.
6) The browser process the HTTP response sent by the server.
7) If the response data is cacheable then browsers cache the same.
8) Browser decodes the response and renders the content.

How does HTTPS work?

HTTPS is similar to HTTP but the added advantage is that it uses encryption. The protocol used is TLS (Transport Layer Security) formerly known as SSL (Secure Sockets Layer). TLS is an improvised version of SSL. It uses both asymmetric and symmetric encryption. First, the asymmetric connection is used to secure the connection. Then, the symmetric encryption is used to send data securely. The private key is controlled by the website/server and the public key is available to everyone who wants to connect.

Steps:

1. Since it is a TCP Protocol, a 3-way handshake takes place
2. After the 3-way handshake, the client sends a Client Hello stating the cipher suite it has available in the browser. A cipher suite is a set of encryption algorithms that are used for both the asymmetric and symmetric cryptography. It also includes additional information that the server needs to connect with the client.
3. The Server responds with a server hello deciding which cipher suite will be used and the version of SSL (like TLS v1.3). This way, the connection is established.
4. Now, the server has to prove its identity that it is the actual website that is being contacted. This is done by SSL certificate. The SSL contains general info about the server and the certificate's public key and digital signature.
5. The client now encrypts a Pre-master secret key using the server's public key. This can only be read by the server as only it has the private key.
6. Based on this pre-master secret key, both will generate the symmetric key required for encryption of data. The client confirms this with a Change-Cipher-Spec message.
7. The server too sends a similar message to confirm the key.
8. Now, data can be transmitted back and forth by encrypting it based on the calculated symmetric key and decrypting it with the same key on the other end.

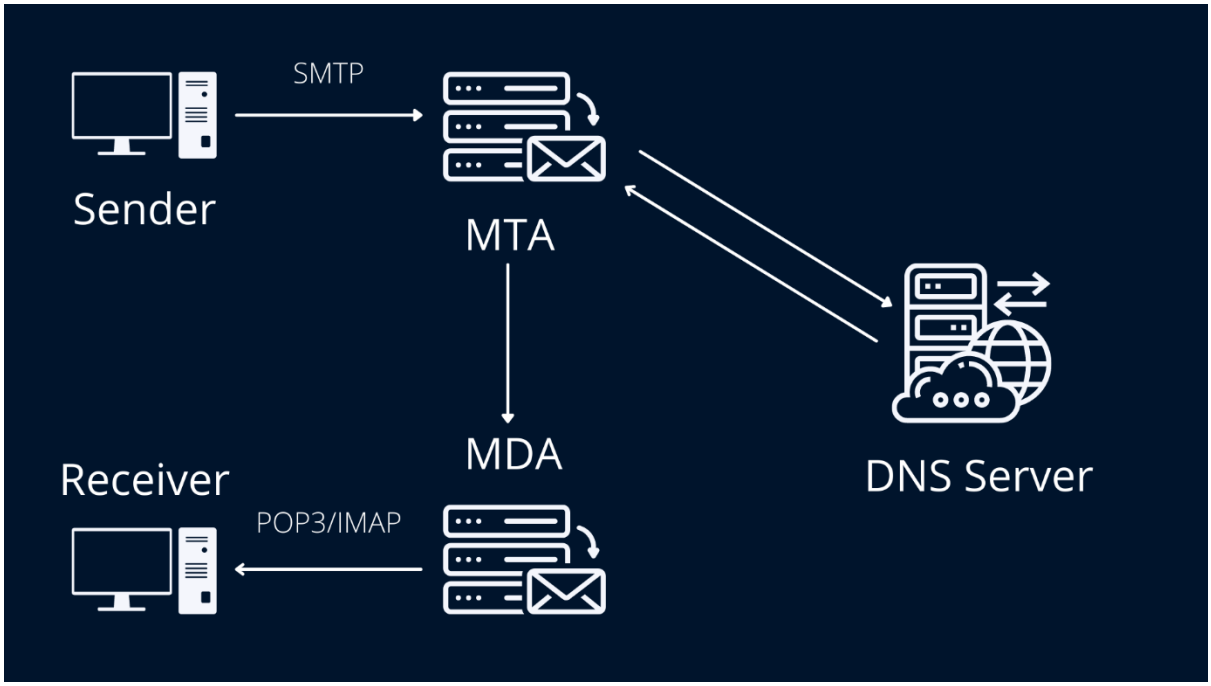


How do email protocols work?

Sending and receiving emails, work over 3 protocols usually which are: IMAP, POP, SMTP. SMTP (Simple Mail Transfer Protocol) is used to send the email to the email server whereas IMAP and POP are used to receive an email from the email server. The main difference between IMAP and POP is that while using IMAP (Internet Mail Access Protocol), the mail is stored in the server whereas, in POP, the mail once received will be downloaded to the device and will be deleted on the server. Current version of POP (Post Office Protocol) is POP3.

Firstly, the sender enters the email address, types in the message and sends the email using an email application. This is sent to the Mail Transfer Agent (MTA) of sender's email client which is done by using SMTP. The IP of receiver MTA is found by using DNS record MX of the email ID's domain and the mail exchange takes place between the servers (MTA). Now, the mail is received by the recipient by using POP3 or IMAP from their MTA.

SMTP uses port 25, POP3 uses port 110, IMAP uses port 143.



How does FTP work?

FTP stands for File Transfer Protocols and is used to transfer files between a client and server. FTP uses port 20 to send the data (Data Connection) and port 21 for the connection and to control it (Control Connection). Hence, there are two separate connection that work together for the files to be transferred. Using and FTP client, we can download and upload data and also rename, move them. Some FTP clients are FileZilla, CyberDuck, Core FTP, WinSCP.