DNS (Domain Name System)

PAGE NO.
DATE: / /

What happens when you make a DNS request.

1. Local cache → Computer first checks its local cache

2. Recursive DNS server → Provided by your ISP.

3. Root DNS server → DNS backbone of the internet. Their job is to redirect you to correct top level domain server (TLD server).

4. Authoritative DNS server → TLD server holds records for where to find the authoritative server to answer the DNS request. The authoritative server is also known as nameserver. (Multiple nameservers are possible as they act like backup)

When request comes back from authoritative DNS server then it is first sent to your recursive DNS server, where a local copy will be cached for future requests.

DNS records all come with a TTL (Time to live) value. This value is a number represented in seconds that the response should be saved for locally until you have to look it up again. Caching saves time.

Packet And Frames

PAGE NO.
DATE: / /

Packet and frames are small pieces of data that, when forming together, make a larger piece of information or message. However, they are two different things in the OSI model.

A frame is at layer 2 - the data link layer, meaning there is no such information as IP addresses.

Think of this as putting an envelope within an envelop and sending it away. The first envelop will be the packet that you mail, but once it is opened, the envelop within still exists and contains data (this is a frame).

We have to use a set of standards and protocols that act as a set of rules for how the packets is handled on a device.

One such protocol is Internet protocol.

When a packet is transmitted using this protocol, it includes a set of headers that contain additional information to the data that is being sent across a network.

Some of the different protocols a packet might follow can have different headers. The protocols can be :-

i) IP
ii) TCP
iii) UDP
iv) ICMP
v) etc.

Some notable headers include

i) TTL :- This field sets an expiry timer for the packet. to not clog up your network if it never manages to reach a host or escape.

ii) Checksum :- This field provides integrity checking for protocols such as TCP/IP. If any data is changed, this value will be different from what was expected and therefore corrupt.

- The checksum is performed on both sender and receiver side. (Checksum is a numerical value or code generated through a specific algorithm based on the data it is associated with.) And when the checksum of sender and receiver side matches, then only it is said to be checksum checked.

iii) Source Address :- The IP address of the device that the packet is being sent from so that data knows where to return to.

iv) Destination Address :- The device's IP address the packet is being sent to so that data knows where to travel next.

TCP/IP (The Three-Way Handshake)

PAGE:
DATE: / /

- TCP is one of the another suite used in networking for communication between 2 devices.

- The TCP/IP protocol consists of four layers and is arguably just a summarized version of the OSI model. These layers are :

  - Application
  - Transport
  - Internet
  - Network Interface.

- one defining feature of TCP is that it is connection-based, which means that TCP must establish a connection b/w both a client and a device acting as a server before data is sent.

→ Because of this, TCP guarantees that any data sent will be received on the other end. These process is named the Three-way handshake ~~which is something we'll come on to~~

Advantages of TCP

- Guarantees the integrity of data.
- Capable of synchronizing two devices to prevent each other from being flooded with data in the wrong order.
- Performs a lot more processes for reliability.

Disadvantages of TCP

- Requires a reliable connection b/w the two devices. If one small chunk of data is not received, then the entire chunk of data cannot be used and must be re-sent.
- A slow connection can bottleneck another device as the connection will be reserved on the other device the whole time.
- TCP is significantly slower than UDP because more work (computing) has to be done by the devices using this protocol.

TCP packet contain various sections of information known as headers that are added from encapsulation. Some crucial headers are:-

Source port, dest. port, source IP, dest. IP, sequence No., acknowledgement No., checksum, data, flag.

Three-way handshake

- Three-way handshake - the term given for the process used to establish a connection b/w two devices.
messages it include while communicating are:-

Step	Message	Description
1.	SYN	A SYN message is the initial packet sent by a client during the handshake. This packet is used to initiate a connection and synchronise the two devices together.
2.	SYN/ACK	This packet is sent by the receiving device (server) to acknowledge the synchronisation attempt from the client.
3.	ACK	The acknowledgement packet can be used by either the client or server to acknowledge that a series of messages / packets have been successfully received.
4.	DATA	Once a connection has been established, data (such as bytes of a file) is sent via that 'DATA' message.
5.	FIN	This packet is used to clearly close the connection after it has been complete.
+	RST	This packet ends all communication. This is the last record and indicates there was some problem during the process. For Eg. If the service of application is not working correctly, or the system has faults such as out of memory