**UDP:**

UDP(User Datagram Protocol) is a lightweight transport protocol, providing minimal services. UDP is connectionless, so there is no handshaking before the two processes start to communicate. UDP provides unreliable data transfer service, that is , when a process sends a message into a UDP socket, UDP provides no guarantee that the message will ever reach the receiving process. Furthermore, messages that do arrive at the receiving process may arrive out of order.

**Real-time application of User Datagram Protocol:**

One of the real time application of UDP is DNS(Domain Name System).

**DNS:**

Just like humans can be identified in many ways(like name, driver’s licence number), so too can Internet hosts. One identifier for a host is its **hostname**. Hostnames provide little information about the location within the internet of the host. For ex , A hostname such as [www.eurecom.fr](http://www.eurecom.fr), which ends with the country code .fr tells us that the host is probably in France, but deosn’t say much more. Moreover, because hostnames can consist of variable-length alphanumeric characters, they would be difficult to process by routers. For these reasons, hosts are also identified by IP Addresses.

Domain Name System , translates human readable domain names(for ex, [www.amazon.com](http://www.amazon.com)) to machine readable IP addresses(for ex, 192.0.0.42).

Service Provided by DNS:

There are two ways to identify a host – by a hostname and by IP address. People prefer the hostname, while routers prefer fixed-length, hierarchically structured IP addresses. In order to reconcile these preferences, we need a directory service that translates hostnames to IP addresses. This is the main task of the Internet’s Domain Name System(DNS). The DNS is a distributed database implemented in a hierarchy of DNS servers, and an application-layer protocol that allows hosts to query the distributed database. The **DNS protocol runs over UPD** and uses port 53. DNS is commonly employed by other application-layer protocols including HTTP and SMTP to translate user-supplied hostnames to IP addresses.

Other than translating hostnames to IP addresses , DNS also provides few other important services:

* Host Aliasing
* Mail Server Aliasing
* Load distribution

**How DNS works:**

Suppose that some application (such as a Web browser or mail reader) running in a user’s host needs to translate a hostname to an IP address, the application will invoke the client side of DNS, specifying the hostname that needs to be translated. DNS in the user’s host then takes over, sending a query message into the network. All DNS query and reply messages are sent within UDP datagrams to port 53. After a delay, ranging from milliseconds to seconds, DNS in the user’s host receives a DNS reply message that provides the desired mapping. This mapping is then passed to the invoking application. Thus, from the perspective of the invoking application in the user’s host, DNS is a black box providing a simple, straightforward translation service. But in fact, the black box that implements the service is complex, consisting of a large number of DNS servers distributed around the globe, as well as an application-layer protocol that specifies how the DNS servers and querying hosts communicate.

**Design of DNS :**

In order to deal with the issue of scale, the DNS uses a large number of servers, organized in a hierarchial fashion and distributed around the world. No single DNS server has all of the mappings for all of the hosts in the internet. Instead, the mappings are distributed across the DNS servers. To a first approximation, there are three classes of DNS servers – root DNS servers, top-level domain(TLD) DNS servers, and authoritative DNS servers – organized in a hierarchy.

* **Three classes of DNS servers:**

1. **Root DNS servers:**

There are over 400 root name servers scattered all over the world. They provide the IP addresses of the TLD servers.

1. **Top-level domain servers:**

For each of the top level domains – top-level domains such as com, org, net, edu, and gov, and all of the country top-level domains such as uk, fr, ca and jp – there is TLD server. TLD servers provide the IP addresses for authoritative DNS servers.

1. **Authoritative DNS servers:**

Every organization with publicly accessible hosts on the Internet must provide publicly accessible DNS records that map the names of those hosts to IP addresses. Most universities and large companies implement and maintain their own primary and secondary(backup) authoritative DNS server.

There is another important type of DNS server called the Local DNS server. A local DNS server does not strictly belong to the hierarchy of servers but is nevertheless central to the DNS architecture. Each ISP – such as residential ISP or institutional ISP – has a local DNS server. When a host connects to an ISP, the ISP provides the host with the IP addresses of one or more of its local DNS servers. When a host makes a DNS query, the query is sent to the local DNS server, which acts a proxy, forwarding the query into the DNS server hierarchy.

**DNS Caching:**

DNS extensively exploits DNS caching in order to improve the delay performance and to reduce the number of DNS messages ricocheting around the internet. The idea behind DNS caching is very simple. In a query chain, when a DNS server receives a DNS reply(containing, for example, a mapping from a hostname to an IP address), it can cache the mapping in its local memory. If a hostname/IP address pair is cached in a DNS server and another query arrives to the DNS server for the same hostname, the DNS server can provide the desired IP address, even If it is not authoritative for the hostname. Because hosts and mappings between hostnames and IP addresses are by no means permanent, DNS servers discard cached information after a period of time. A local DNS server can also cache the IP addresses of TLD servers, thereby allowing the local DNS server to bypass the root DNS servers in a query chain. In fact, because of caching, root servers are bypassed for all but a very small fraction of DNS queries.

How to use 8.8.8.8 DNS?

While the ISP will set a default DNS server, the user can use it under no obligation. Some users may have reason to avoid their ISP’s DNS – for instance, some ISPs use their DNS serveers to redirect requests for nonexistent addresses to pages with advertising. For an alternative, user can instead point the computer to a public DNS server that will act as a recursive resolver. One of the most prominent public DNS servers is Google’s ,its ip address is 8.8.8.8. Google’s DNS services tend to be fast.

DNS Cache poisoning:

DNS Cache poisoning can divert users to malicious websites. Attackers manage to insert false address records into the DNS so when a potential victim requests an address resolution for one of the poisoned sites, the DNS responds with the IP address for a different site, one controlled by the attacker. Once on these phony sites, victims may be tricked into giving up passwords or suffer malware downloads.