Know How DNS Works

Domain name Servers (DNS) are an important but invisible part of the internet, and form one of the largest databases on it.

 Domain name Servers (DNS) are an important but invisible part of the internet, and form one of the largest databases on it. Each machine on an internet is assigned a unique address, called an IP address, which is 32 bit number and is expressed as 4 octets. The method user to represent these IP addresses is known as dotted decimal Notation". A typical address looks like this: 199.249.150.4

It is very difficult to keep in mind the IP addresses of all the websites we visit daily, because it's not easy to remember strings of numbers. However, we do remember words. This is where domain names come into the picture. If you want to connect to a particular site, you need to know its IP address but do need to know its URL. The DNS gets the mappings of the IP addresses and the corresponding names.

Names and numbers

DNS converts the machine names (such as www.xyz.com) to IP addresses (such as 199.249.150.9). Basically, it translates from a name to an address and from an address to a name.

The mapping from the IP address to the machine name is called reverse mapping .when you type http://www.xyz.com into your browser, the browser first needs to get the IP address of www.xyz.com. The machine uses a directory service to look up IP addresses and this service is called DNS. When you type www.xyz.com your machines firsts contacts a DNS server, asking it to find the IP address for www.xyz.com. This DNS server might then contact other DNS servers on the internet. DNS is therefore is considered as the global network of servers. The great advantage of DNS is that no organization is responsible for updating it. It is what is known as distributed database.

The three letter codes

A DNS server is just a computer that's running the DNS software. The most popular DNS software is BIND (Berkeley Internet Name Domain) DNS is hierarchical, tree-structured system. The top is donated by'.'. And is known as the root of the system. Below the root there are seven immediate sub domain nodes and these are 'com', 'org', 'gov', 'mil', 'net', 'edu', 'Int', etc.

DNS consists of two components

1. Nameserver
2. Resolver

Nameserver:

This performs the task of looking up the names. Usually, there is one nameserver for a cluster of machines. If the nameserver does not contain the requested information, it will contact another nameserver. But it is not required for every server to know how to contact every other server. Every nameserver will know how to contact the root nameserver, and this in turn will know the location of every authoritative nameserver for all the second level domains.

Resolver:

This runs on a client machine to initiate DNS lookups. It contains a list of nameservers to use. As we have read, the function of each of these nameservers is to resolve name queries. There are three types of nameservers-primary nameserver, secondary nameserver, and caching nameserver. The secondary nameservers are configured for backup purposes. Caching nameservers only resolve name queries but do not maintain any DNS database files. It is important to note here that any change to primary nameservers needs to be propagated to secondary nameservers. This is because primary nameservers own the database records. The changes are propagated via a 'zone transfer'.

How 'Caching' works

DNS uses principle of 'caching' for its operation. When a nameservers receives Information about a mapping, it caches this information .further queries for the same mapping will use this cached result, thereby reducing the search cost. The nameservers don't cache forever. The caching has a component called time to live (TTL) and the TTL determines how long a server will cache a piece of information. So when the nameservers caches receive an IP address, it receives the TTL with it. The nameserver caches the IP address for the period of time then discards it.

When a process needs to determine an IP address given a DNS address, it calls upon the local host to resolve the address. This can be done in variety of ways:

Table look up. On UNIX hosts, the table is /etc/hosts.

The process communicates with a local nameservers. This is named on a UNIX system.

By sending a massage to the remote system that is identified from the information in the file/etc/resolve.conf.

When a nameserver receives a query for a domain that is does not serve, it may send back a referral to the client by specifying better nameservers. Typically operate in the recursive manner wherein any DNS server passes requests it cannot handle to higher level server and so on, until either the request can be handled or until the root of the DNS name space is reached.

The nameservers contain pointers to other nameserver with the help of which it is possible to traverse the entire domain naming hierarchy. A host with the initial nameserver addresses has to be configured. After this, it is able to use DNS protocols to locate the nameserver responsible for any part or the DNS naming hierarchy.

Thus when a nameserver receives a request, it can do one of the following:

It can answer the request with an IP address. This method is called iterative. In this, the client simply asks the server to resolve a domain name. The server accesses its database, finds its IP address and sends that back. If the server does not find the address, it sends back an error ;DNS not found'). Contact another nameserver and try to find the IP address for the requested name. Send back a referral to the client specifying the IP address of better nameservers.

A popular user interface, called 'nslookup'is available on the UNIX system. With this, you can perform any DNS function. This program also displays the result to the user. Using is nslookup, you can obtain a listing of all the hosts in a zone. In order to do this, you first need to identify the nameserver for the zone.

The threats that are associated with the DNS are due to the lack of integrity and authenticity checking of the data held within the DNS. Also, other protocols can use host names as an access control mechanism. The internet engineering task force (IETF) has come up with DNS security (DNSSEC) extensions to DNS protocol. The main objective to DNSSEC is to provide authentication and integrity to the DNS. These are provided through the use of cryptographic'

Short note about the author

Pawan Bangar, from www.birbals.com

Author: Pawan Bangar