How to Work a DNS Request

**What is DNS?**

DNS stands for Domain Name Service. DNS translates the name of a device to its physical IP address, which is referred to as forward mapping. DNS also translates the physical IP address to the name of a device, usually called reverse mapping.

Without DNS, every device that wanted to access to the Internet would need to know its physical IP address. With 100 of millions of hosts and billions of web pages it is impossible to track.

With a DNS server present in a network, the end host only needs to know the physical address of the DNS server and the name of the device it wishes to access. When an end device needs to look up an address, it will query the DNS server. This greatly simplifies network management.

**Master and Slave DNS Servers**

A master DNS server defines zones for which it is authoritative. A slave DNS server gets all its data from the master DNS server.

**Hidden Master Server**

A hidden master is defined as being a DNS server that does not appear publically. Usually the company has a hidden master because it does not want the world / Internet to see all its internal hosts should the public DNS server becomes compromised. An external server is configured to slave to these hidden masters and only announce systems or services that are visible to the public, e.g., A records for the external web sites.

**DNS Record Types**

To be able to understand DNS, you need to understand DNS record types. These record types will help you understand the DNS output via dig.

**A** - IPv4 Address record. An IPv4 address for a host.

**CNAME** - Canonical Name. An alias name for a host.

**MX** - Mail Exchanger. A preference value and the host name for a mail server.

**NS** - Name Server. Defines the authoritative name server(s) for the domain.

**PTR** - IP address (IPv4 or IPv6) to host. Used for reverse DNS.

**SOA** - Start of Authority. Defines the zone name and e-mail contacts.

There are two types of Corporate DNS servers, internal and external. The internal DNS servers are for Hilton employees only. The external DNS servers are for people who connect via the Internet. Here is a quick list of internal and external Corporate DNS servers:

**Corporate DNS Servers**

xxx.xxx.xxx.xxx - Enterprise

xxx.xxx.xxx.xxx or xxx.xxx.xxx.xxx – Foghorn

**Corporate EXTERNAL DNS SERVERS**

xxx.xxx.xxx.xxx

xxx.xxx.xxx.xxx

When we do an nslookup of sftp.corporate.com with a DNS server of xxx.xxx.xxx.xxx, it shows that there is not an entry already in DNS for this record:

**host-name : nslookup sftp.corporate.com xxx.xxx.xxx.xxx**

**Server: xxx.xxx.xxx.xxx**

**Address: xxx.xxx.xxx.xxx#53**

**\*\* server can't find sftp.corporate.com: NXDOMAIN**

**host-name :**

You can also check via the dig command:

**host-name: dig sftp.corporate.com @xxx.xxx.xxx.xxx**

**; <<>> DiG 9.2.4 <<>> sftp.corporate.com @xxx.xxx.xxx.xxx**

**; (1 server found)**

**;; global options: printcmd**

**;; Got answer:**

**;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 39832**

**;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0**

**;; QUESTION SECTION:**

**;sftp.corporate.com. IN A**

**;; AUTHORITY SECTION:**

**corporate.com. 600 IN SOA hostname.corporate.com. domain\_tech.corporate.com. 4049 3600 1800 604800 600**

**;; Query time: 40 msec**

**;; SERVER: xxx.xxx.xxx.xxx#53(xxx.xxx.xxx.xxx)**

**;; WHEN: Wed Aug 24 21:18:52 2011**

**;; MSG SIZE rcvd: 95**

**host-name :**