

Useful DNS commands

“Learn by Doing Hands-on”

Hands-on for Information Network 1 - 2017

Recap

- DNS information into three primary types:
 - NS (Name Server) records,
 - MX (Mail Exchange) records, and
 - A (Address) records. NS records indicate the name servers.
- MX records indicate the hosts that handle email delivery;
 - the priority (pri) number indicates the order in which mail servers are used, with the lowest number receiving the highest priority.
- The A (Address) records map hostnames to IP addresses, the real names of machines.

1st command - host

- simplest of the DNS commands. It is a quick way to determine the IP address of a hostname:

- `:~$ host www.your-domain-name.com`

1st command - host

- Now that you know the IP address for www.your-domain-name.com, try a reverse lookup:
 - :~\$ host <IP address>

1st command - host

- :~\$ host -a www.your-domain-name.com

- The -a option will return all of the DNS information in verbose format

2nd command - dig

- “Domain Information Groper” gathers and returns DNS information in a format the name server can use directly.
- You will find it easy to query specific name servers with dig.

2nd command - dig

- You can quickly determine the Name servers of your host or any other host:

- `:~$ dig ns your-host.com`

2nd command - dig

- Then you check your (or another) website against the host's name servers:

- `:~$ dig www.your-domain-name.com @ns.your-host.com`

2nd command - dig

- Dig can provide output that is in the same format as the zone file itself. Here is how to get the whole zone file:
- `:~$ dig any your-domain-name.com`

2nd command - dig

- Here are the most useful dig query types: dig any (gathers all DNS information), dig ns (gathers name server information), dig mx (gathers mail exchanger information) and dig a (gathers network address information).
 - :~\$ dig **any** your-domain-name.com
 - :~\$ dig **ns** your-domain-name.com
 - :~\$ dig **mx** your-domain-name.com
 - :~\$ dig **a** your-domain-name.com

2nd command - dig

- The dig command can also do reverse lookups with output formatted for the zone file:

- :~\$ dig -x <IP Address>

Any Question?