DNS and DHCP

COS 461

Muneeb Ali
DNS is a "lookup service"
In 1983, HOSTS.TXT files on each computer

Image source: Olafur Guomundsson & Peter Koch
DNS - Query

- QNAME: www.dnsop.org
- QCLASS: IN
- QTYPE: A

Image source: Olafur Guomundsson & Peter Koch
DNS – Packet Format

UDP 512 bytes Payload (TCP fallback)

+ Domain name | type | class | TTL | RL | RDATA |
+---------------+------|-------+-----|----|-------|
<variable> 2 2 4 2 <variable>

- Owner name (domain name)
  - Encoded as sequence of labels
    - Each label contains
      - Length (1 byte)
      - Name (n bytes [1..63])
    example.com ➔ 07example03com00

- Type: MX, A, AAAA, NS ...
- CLASS: IN (other classes exist, but none global)
- TTL: Time To Live in a cache
- RL: RD LENGTH: size of RDATA
- RDATA: The contents of the RR
  - Binary blob, no TLV (XXX Type Length Value).

A - address record
MX - mail exchange
AAAA - IPv6 address
NS - name server
CNAME - alias

RR: a single Resource Record

Image source: Olafur Guomundsson & Peter Koch
DHCP

- Dynamic Host Configuration Protocol
- Runs over UDP (port 67, 68 client)

- DHCPDISCOVER (by-client)

- DHCPOFFER (by-server)

- DHCPREQUEST (client identify server) (also to renew)

- DHCPRELEASE (release)
Demo

- Dig - DNS lookup utility
- BIND (Berkeley Internet Name Domain)
- Named (Internet domain name server) part of BIND 9
- Dnsmasq - Lightweight DHCP (and DNS caching)
Demo - Dig

Download VirtualBox and some flavor of Linux (Fedora or CentOS can do)

dig www.princeton.edu
#will trace the entire path from root servers
dig +trace www.princeton.edu

dig www.dritte.org A +short
dig www.muneeb.org A +short

#mail exchange records
dig www.muneeb.org mx +short
#reverse lookup
dig -x 18.9.22.169 +short

#asking a specific nameserver
dig @ns2.google.com muneeb.org +short
dig @ns1.webhostingpad.com muneeb.org +short
#contains name server configuration, can change it

cat /etc/resolv.conf

#local name->IP binding, overrides everything else
# e.g., adding “127.0.0.1 penguins.cs.princeton.edu” will incorrectly point, but will work

cat /etc/hosts

#install named, if not already there – yum is a package manager

su # need to have proper permissions

yum install named

#this is the config file, you need to edit

vi /etc/named.conf

service named start

#using your server to query!

dig @localhost muneeb.org +short

#contains all mapping files

cd /var/named
you probably want to install dhcpd, but dnsmasq will also work (it’s lightweight)
yum install dnsmasq

#edit the config file, some example things
cat /etc/dnsmasq.conf | grep dhcp-range
#dhcp-range=192.168.0.50,192.168.0.150,12h

#MAC to IP binding, and many other things …
cat /etc/dnsmasq.conf | grep dhcp-host

#a caveat; dnsmasq is DHCP + DNS, so uses the same port as named
# stop named to test dnsmasq (we used it only for DHCP)
service named stop
service dnsmasq start
Questions?

Thank you!
Happy digging!