Elijah Berumen
CSCI 4113
Lab 5: IP Networking

DHCP: Add Machine F to Network and Get Other Hosts to Pull Statically Configured IPs

On Machine F

1. “# ifconfig” - We grab the MAC Address for machine F from here

2. Created Machine F network script at /etc/sysconfig/network-scripts/ifg-ens192, setting BOOTPROTO=dhcp and NETWORKING=yes

On Machine A

1. After installing dhcp, added the subnet entries and the corresponding host statements in /etc/dhcp/dhcpd.conf as follows:

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#
subnet 100.64.5.0 netmask 255.255.255.0 {
     option routers 100.64.5.1;
     # DNS Information
     # option domain-name "dundermifflin.com";
     option domain-name-servers 100.64.5.4;
     pool {
          range 100.64.5.200 100.64.5.253;
     }
host machineF {
     hardware ethernet 00:50:56:85:2b:ad;
     fixed-address 100.64.5.5;
     option host-name "saddle";
     }
host machineB {
     hardware ethernet 00:50:56:85:d2:6e;
     fixed-address 100.64.5.2;
     option host-name "carriage";
```

```
     }
host machineC {
     hardware ethernet 00:50:56:85:86:1a;
     fixed-address 100.64.5.3;
     option host-name "platen";
     }
host machineD {
     hardware ethernet 00:50:56:85:dd:57;
     fixed-address 100.64.5.4;
     option host-name "chase";
     }

}


subnet 10.21.32.0 netmask 255.255.255.0 {
     # The following is set to be our machine
     option routers 10.21.32.1;
     # DNS Information
     option domain-name "dundermifflin.com";
     option domain-name-servers 100.64.5.4;
     pool {
          range 10.21.32.200 10.21.32.253;
     }
host machineE {
     hardware ethernet 00:50:56:85:cf:da;
     fixed-address 10.21.32.2;
     option host-name "roller";
     }
}
```

Note: To Confirm Machine F is on the Network, ssh into it from Machine A

Network Interfaces on Machine A

ens192 - Internet facing
ens256 - Machine E on subnet 10.21.32.0/24
ens224 - All other hosts for the subnet 100.64.5.0/24

Elijah Berumen
CSCI 4113
Lab 5: IP Networking

Making Machine F Our Backup Web Server(Clone of B)

Install/Enable Apache and Rsync

"# yum install httpd"
"# yum install rsync"
"# systemctl enable httpd"
"# systemctl start httpd"

Drop IP Tables to allow requests on port 80

"# systemctl stop iptables"
"# systemctl disable iptables"

Changing DocumentRoot

1. In /etc/httpd/conf/httpd.conf set the following in order to server the D-M Site:

   DocumentRoot "/var/www/dundermifflin"

Sync Users/Groups/Permissions from B to F

Note: The "-a" flag is recursive

"# rsync -a root@100.64.5.2:/etc/shadow /etc/shadow"
"# rsync -a root@100.64.5.2:/etc/passwd /etc/passwd"
"# rsync -a root@100.64.5.2:/etc/group /etc/group"
"# rsync -a root@100.64.5.2:/etc/sudoers /etc/sudoers"

SSH Keys For Passwordless Authentication

"# ssh-keygen -t rsa -b 2048" - Generate them on F
"#ssh-copy-id -i ~/.ssh/id_rsa.pub root@100.64.5.2" - Send them to B

Note: Test by ssh-ing from B to F or vice versa

Create Cron Job To Sync Each Hour

Edit Crontab:

“# crontab -e”

Add the following entry:

0 * * * * rsync -a root@100.64.5.2:/var/www/ /var/www

Check if it’s loaded:

“# Crontab -l”

Check logs

/var/log/cron

DNS

Getting /etc/resolv.conf to populate with our DNS Server

1. Change hostnames of Machines A through F via /etc/hostname to the following respectively and reboot all machines:

outer.dundermifflin.com.	100.64.0.N	A	1 hour
carriage.dundermifflin.com.	100.64.N.2	A	1 hour
platen.dundermifflin.com.	100.64.N.3	A	1 hour
chase.dundermifflin.com.	100.64.N.4	A	1 hour
roller.dundermifflin.com.	10.21.32.2	A	1 hour
saddle.dundermifflin.com.	100.64.N.5	A	1 hour

2. We have B-F get their name servers from the DHCP server by adding the following in the subnet statements within /etc/dhcp/dhcp.conf:

   “option domain-name-servers 100.64.5.4;”

   Test: systemctl restart dhcpd

Install RSync and Bind
yum install rsync
yum install bind bind-utils

Create Backups
mkdir /dns_backups ; rsync -a /etc/hosts /etc/named.conf /etc/resolv.conf /etc/sysconfig/iptables /dns_backups

Note: Had to do the following on all machines to get /etc/resolv.conf on the machines to populate with our name server:

1. Comment out lines in /etc/sysconfig/network
2. Comment out line on /etc/sysconfig/network-scripts/ifcfg-ens192 #PEERDNS=no

On Machine D (DNS), /etc/named.conf

Recursive DNS Setup: In /etc/named.conf we want recursion yes; to create a recursive DNS server, and listen-on port 53 should be set to any. Lastly, allow-query should allow itself(127.0.0.1), the subnet of machines A, B, C, D, F(100.64.5.0/24), and the subnet of machine E(10.21.32.0/24).

Test Recursive DNS:

After making the specified changes to named.conf on machine D, run “# systemctl restart named”

Go into each machine and run “# systemctl restart network” and ping google.com

/etc/named.conf

```
options {
     listen-on port 53 { any; };
     listen-on-v6 port 53 { ::1; };
     directory      "/var/named";
     dump-file      "/var/named/data/cache_dump.db";
     statistics-file "/var/named/data/named_stats.txt";
     memstatistics-file "/var/named/data/named_mem_stats.txt";
     recursing-file  "/var/named/data/named.recursing";
     secroots-file   "/var/named/data/named.secroots";
     allow-query     { 127.0.0.1; 100.64.5.0/24; 10.21.32.0/24;
};

     /*
      - If you are building an AUTHORITATIVE DNS server, do NOT
enable recursion.
      - If you are building a RECURSIVE (caching) DNS server,
you need to enable
        recursion.
      - If your recursive DNS server has a public IP address,
you MUST enable access
        control to limit queries to your legitimate users.
Failing to do so will
        cause your server to become part of large scale DNS
amplification
        attacks. Implementing BCP38 within your network would
greatly
        reduce such attack surface
     */
     recursion yes;

     dnssec-enable yes;
     dnssec-validation yes;

     /* Path to ISC DLV key */
     bindkeys-file "/etc/named.root.key";

     managed-keys-directory "/var/named/dynamic";
```

```
     pid-file "/run/named/named.pid";
     session-keyfile "/run/named/session.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "dundermifflin.com." {
     type master;
     file "dundermifflin.com";
};

zone "." IN {
     type hint;
     file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

Authoritative DNS Setup: In /etc/named.conf specify the zone and tell it to look at our zone file that is named “dundermifflin.com”. Configure the zone file to have all of the A records, CNAME records and TTLs.

Testing: Run “**# systemctl restart named**”

Zone File: /var/named/dundermifflin.com

```
$TTL 1H
dundermifflin.com. 1D IN SOA chase.dundermifflin.com.
admin.dundermifflin.com. (
     2020110901 ; serial
```

```
     3H ; time-to-refresh
     15 ; time-to-retry
     1W ; time-to-expire
     1H ; minimum-TTL
)
dundermifflin.com.            IN   NS   chase.dundermifflin.com.
router.dundermifflin.com.     1H   IN   A    100.64.0.5
carriage.dundermifflin.com.   1H   IN   A    100.64.5.2
platen.dundermifflin.com.          1H   IN      A
100.64.5.3
chase.dundermifflin.com.      1H   IN      A       100.64.5.4
roller.dundermifflin.com.     1H   IN      A       10.21.32.2
saddle.dundermifflin.com.     1H   IN      A       100.64.5.5
dundermifflin.com.       5M   IN   A    100.64.5.2
machinea.dundermifflin.com.   7D   IN   CNAME
router.dundermifflin.com.
machineb.dundermifflin.com.     7D IN      CNAME
carriage.dundermifflin.com.
machinec.dundermifflin.com.     7D IN      CNAME
platen.dundermifflin.com.
machined.dundermifflin.com.     7D IN      CNAME
chase.dundermifflin.com.
machinee.dundermifflin.com.     7D IN      CNAME
roller.dundermifflin.com.
machinef.dundermifflin.com.     7D IN      CNAME
saddle.dundermifflin.com.
;dundermifflin.com.      5M   IN   CNAME
carriage.dundermifflin.com.
www.dundermifflin.com.        5M   IN   CNAME
carriage.dundermifflin.com.
www2.dundermifflin.com.       5M   IN   CNAME
saddle.dundermifflin.com.
ftp.dundermifflin.com.        5M   IN   CNAME
platen.dundermifflin.com.
files.dundermifflin.com. 7D   IN   CNAME
roller.dundermifflin.com.
```