

Review of MacMini Configure After Ansible Build of Platform

Contents

1	Overview	1
2	Review Network Configuration	2
2.1	Initial network interfaces	2
2.2	br-wan	2
2.3	br-lan	2
2.4	br-wan.cfg	2
2.5	br-lan.cfg	3
2.6	gateway	3
2.7	DHCP Configuration	4
2.8	DNS Configuration	4
2.9	Git pull to update files in workshop-kit Git Repository	6

1 Overview

The ansible configuration scripts have done quite a bit of installation of software and configuring to help build your virtualized training platform. Here are a few items we will take a look at:

- br-lan configuration (internal, private address)
- br-wan configuration (external, public or outside address)
- gateway (10.10.0.254)
- DNS configuration and zone files
- DHCP configuration

- DHCP with fixed MAC addresses to allocation IPs there are referenced in our DNS
- Running a git pull for the workshop-kit Git repository to update your local files

2 Review Network Configuration

2.1 Initial network interfaces

Log in on your MacMini (if you are not already logged in) and take a look at how your network is now configured:

```
$ ifconfig br-wan
$ ifconfig br-lan
$ brctl show
```

2.2 br-wan

You should see the external IP of your MacMini on the “br-wan” entry. This is associated with your eth1 interface, or the USB to Ethernet dongle on your machine.

2.3 br-lan

On the br-lan interface you will see the statically assigned address of 10.10.0.241 that represents your MacMini to your virtualized environment. In the DNS this IP represents sl.ws.nsrc.org. This interface is associated your eth0 interface, or the built-in NIC on your MacMini.

To view where these interfaces are configured take a look at the following files:

```
$ less /etc/network/interfaces.d/br-wan.cfg
$ less /etc/network/interfaces.d/br-lan.cfg
```

2.4 br-wan.cfg

You should see that the eth1 physical interface is being bridged to the br-wan interface. This will work if your outside interface is a public IP, is a private IP or is obtained via DHCP.

2.5 br-lan.cfg

This file is much larger, so you should look at it on your own.

The configuration is more complex, but if you look you'll see that eth0 is bridged to br-lan, and the br-lan interface has a static IP address assigned as well as multiple routes for our various workshop topologies. In addition for the br-lan interface configuration you can see the bridge_ports option that maps the TAP interfaces to allow our virtual routers to attach to our backbone network on one of their network interfaces. By definition a "TAP (namely network tap) simulates a link layer device and it operates with layer 2 packets like Ethernet frames."

2.6 gateway

We use the iptables firewall facility in linux to do masquerading - that is NAT with no firewall rules applied to our traffic. You could apply rules if you want, but we just want our MacMini to pass all traffic from the outside address (br-wan) destined to 10.0.0.0/8 address on our internal network to be passed along. And, any traffic outside of the 10.0.0.0/8 network range to go out the br-wan interface.

You can view our iptables rules in the file /etc/iptables/rules.v4:

```
$ less /etc/iptables/rules.v4
```

These rules are loaded in to iptables at system start time.

To enable forwarding for ipv4 on our network interfaces you need to issue the command:

```
$ sudo sysctl net.ipv4.ip_forward
```

You can see this setting in the file /etc/sysctl.conf

```
$ cat /etc/sysctl.conf
```

Or, to just find the line:

```
$ grep net.ipv4.ip_forward /etc/sysctl.conf
```

2.7 DHCP Configuration

You can view the configuration of the DHCP server in the directory `/etc/dhcp`. The order in which the DHCP server configuration files are read is:

```
dhcpd.conf
dhcpd.local.conf
dhcpd.ws.conf
dhcpd.nmm.conf
dhcpd.svc.conf
```

Follow through the files using `less` to see what they are doing. That is:

```
$ less /etc/dhcp/dhcpd.conf
$ less /etc/dhcp/dhcpd.local.conf
$ less /etc/dhcp/dhcpd.ws.conf
$ less /etc/dhcp/dhcpd.nmm.conf
$ less /etc/dhcp/dhcpd.svc.conf
```

Essentially the configuration is set up like this:

- *dhcpd.conf*: setting domain, dns servers, default lease times, logging
- *dhcpd.local.conf*: we include multiple local files for specific workshop configurations
- *dhcpd.ws.conf*: general workshop entries for machines on the backbone in the address range 10.10.0.100 - 10.10.0.219 with a gateway of 10.10.0.254 (the MacMini). Then some individual machine names with specific MAC addresses. *Note* the MAC addresses - these are generated by a special script when we build a vm of the name of the host listed. We finish with a range of machine host1-host199 and vm1-99. Again, each host name has a MAC address that is generated based on the name and that ensure each host gets a specific IP and this IP is represented in our DNS configuration.
- *dhcpd.nmm.conf*: includes specific IPs for VMs that are in groups behind routers in our Network Monitoring and Management classes. Note the address ranges are 10.10.1.0/24-10.10.9.0/24. Note the “options routers” line - this represents the inside address or interface of the router for each group.
- *dhcpd.svc.conf*: is used in our cloud virtualiation workshop.

2.8 DNS Configuration

DNS is configured in two locations. You can see the general DNS configuration directives in the `/etc/bind` directory. The configuration is fairly complex so we’ll discuss this during class for a few minutes. If you wish to see where hostname IP addresses are defined look in:

```
$ less /etc/bind/db.ws.nsrc.org
```

You should note that the hostname and IP addresses match what you saw in the DHCP configuration. This is how we can ensure that IP and hostnames stay constant for our workshops. The reverse DNS information is configured in the file db.10.10.in-addr.arpa:

```
$ less /etc/bind/db.10.10.in-addr.arpa
```

In addition to defining IPs for hostnames we use dynamic dns to push the IP of your Mac Mini's name kitX.lab.nsrc.org to our dns server on nsrc.org so that it become visible in the public Internet in an automated fashion. In some cases you may not be allowed to use port 53 on some networks. The majority of the bind configuration is in the file:

```
$ less /etc/bind/named.conf.options
```

Here you can see what subnets our server will respond to:

```
allow-recursion {
    127.0.0.1;
    ::1;
    10.0.0.0/8;
    172.16.0.0/12;
    192.168.0.0/16;
};
```

What to do if dnssec is broken on the network where you are working:

```
# If you are somewhere where filtering breaks DNSSEC use this
# dnssec-validation no;
dnssec-validation auto;
```

and, detailed logging configuration for bind. If you would like to view the bind logging files they are in /var/log/named and include the file:

```
dnssec
general
notify
query
transfers
```

Try viewing some of these file using less to see the type of information that is provided.

2.9 Git pull to update files in workshop-kit Git Repository

To finish we can practice pulling the workshop-kit Git repository to see if any changes have been made. This is good practice to do from time to time:

```
$ cd /home/nsrc/workshop-kit  
$ git pull
```

If prompted for a username or password provide what you used when you first cloned the workshop-kit Git repository in our prior exercises.