ComS 252 Homework 13: Build a Router

Extra credit (points divided by group size)

Due December 7, 2021

1 Objectives

For this assignment, you will build a NAT/Router on a Linux (virtual) machine with two interfaces. The following HOWTOs may be helpful for this assignment, as supplements to the lecture material.

- DHCP: `http://tldp.org/HOWTO/DHCP/x369.html`
- NAT: `http://tldp.org/HOWTO/IP-Masquerade-HOWTO`
- DNS: `http://tldp.org/HOWTO/DNS-HOWTO.html`

2 Downloads

There are two virtual machines for this assignment:

1. `Client13.ova`, the client machine. **This machine is already configured, and should not be changed.** Account `user` has password `userpw`. You should not need root access at all on the client; all debugging of the server on the client side can be done as an ordinary user.
2. `Server13.ova`, the server machine. Accounts `root` and `user` have passwords `rootpw` and `userpw`. You should not need to install any software on the server.

2.1 Network setup

The server VM has two network adapters:

1. A "NAT" adapter for connecting to the Internet, on device `enp0s3`.
2. An "Internal network" adapter for connecting to the private network, on device `enp0s8`.

The client VM, instead, has a single network adapter:

1. An "Internal network" adapter for connecting to the private network.

The objective of this assignment is to set up the server VM just like a home router, so that the client can connect to the Internet by "sharing" the server's Internet connection. The desired network topology is shown in Figure 1.

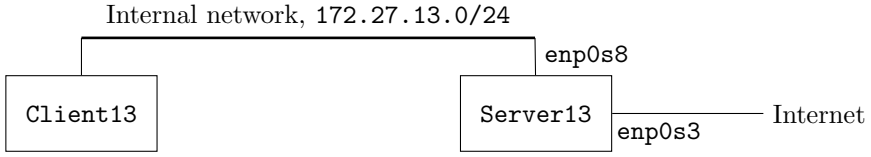

Figure 1: Network topology

3 Configuring the network interfaces

3.1 Server's `enp0s3` interface

This interface is already configured, *except* you should add the appropriate

```
HWADDR=xx:xx:xx:xx:xx:xx
```

line to the configuration file.

3.2 Server's `enp0s8` interface

Configure the `enp0s8` interface (the one on the private, internal network) so that it comes up at boot time. You will also need to add the appropriate

```
HWADDR=xx:xx:xx:xx:xx:xx
```

line to the configuration file. Reboot and make sure both network interfaces have IP addresses.

4 Set up the server for DHCP

The client VM is already configured to use DHCP to obtain an IP address for its network adapter. You will need to configure the server VM as a DHCP server for the private network, so that it gives out addresses on the `172.27.13.0/24` subnet[1]. Configure the DHCP server on the server VM as follows.

- The DHCP server should start at boot time.
- A generic client should obtain an IP address in the range `172.27.13.100` to `172.27.13.199`.
- The client VM should *always* obtain an IP address of `172.27.13.42`, based on the MAC address of the client's network adapter.
- All clients should receive a router (gateway) IP address of `172.27.13.1`.
- All clients should receive, *for now*, DNS server IP addresses of `8.8.8.8` and `8.8.4.4`. You will change this later, after you set up the server VM as a DNS server.

Once the server is set up, you can test it by starting the client VM and checking the client's obtained IP address, and the contents of file `/etc/resolv.conf`. When it works, you should be able to `ping` the server IP address from the client machine. You will not be able to `ping` any other addresses from the client, yet.

On the server, verify that you can ping the client's IP address, an Internet IP address (such as `8.8.8.8`), and an Internet FQDN (such as `google.com`).

Note: Complex file structure (for example, nested braces) in your `dhcpd.conf` configuration file will confuse the Turnin script. To ensure that your work can be automatically graded, you should have most options as "global" (not within any braces) and use braces only when you must. The script will warn you if your configuration file is too complex.

5 Set up the server as a NAT gateway router

To configure the server as a router, do the following.

- Make sure `firewalld` is running.
- Configure the firewall so that interface `enp0s8` belongs to zone `internal`, and interface `enp0s3` belongs to zone `external`.

[1] Contact the instructor if your server VM happens to use the same subnet for the `enp0s3` interface.

- Turn on masquerading for the `external` zone. This should turn on packet forwarding.

Make sure that all these changes persist across reboots of the server VM.

The easiest way to test if this works is to (re)start the server and then try to ping `google.com` from the client machine. If you can, then your router is functioning properly. You should also try to view a webpage on the client machine using `lynx` or `curl`.

6 Set up a forwarding DNS server

6.1 Changing DNS servers used by the client

Re-configure DHCP on the server VM to use the server's IP address as the (only) domain name server. To test, reboot the client and make sure `/etc/resolv.conf` shows only the server VM as the DNS server.

6.2 Configuring DNS

- Make sure service `named` is running. The utilities `named-checkconf` and `named-checkzone` are useful to check for errors in `named` configuration files.
- Edit the configuration file `/etc/named.conf` to set up a recursive (forwarding) nameserver (see section 4 of the DNS–HOWTO). Use `8.8.8.8` and `8.8.4.4` as the "forwarders".
- Edit the configuration file `/etc/named.conf` so that the nameserver responds to queries from any host on the `172.27.13.0/24` subnet; add this subnet to the `listen-on port` and `allow-query` lines in `/etc/named.conf`.
- Allow service `dns` through the firewall, for zone `internal`.

Make sure these changes persist across reboots of the server VM. To test, reboot the server and client. Then, on the client, ping `www.google.com` (or any other FQDN) on the client. If this works, then your recursive DNS server is working.

7 Set up an authoritative DNS server

Define your own domain, `cs252.local`, where the IP addresses are in the `172.27.13.0/24` subnet. Machines in your domain will be named `<hostname>.cs252.local`. Your server should know about the following machines:

- `server.cs252.local`, with appropriate IP address.
- `client.cs252.local`, with appropriate IP address.
- `username.cs252.local`, for each ISU `username` in your group. Arrange the ISU usernames alphabetically and start IP addresses at `172.27.13.10`. For example, for ISU usernames `ciardo`, `jil`, and `asminer`, we would set up IP addresses:

```
asminer   172.27.13.10
ciardo    172.27.13.11
jil       172.27.13.12
```

Configure your DNS server as the master server for your domain. Be sure to include inverse queries, so you can convert from an IP address to a hostname. If you can ping `server.cs252.local` and `client.cs252.local` on the client, then your authoritative DNS server is working. Use `dig` to test the inverse queries on the client. You can use ping `username.cs252.local` to make sure the IP address is correct, but of course no packets will get to this non-existant machine.

8 Finishing touches

Configure the server as follows.

- Edit the DHCP server configuration so that the line

  ```
  search cs252.local.
  ```

  automatically appears in the client's `/etc/resolv.conf` file when the client obtains its IP address. When this works, you will be able to drop the domain name and simply use `ping server`, `ping client`, and `ping username` on the client.

- When the server VM boots up, the firewall should allow *only* the following services through: `ssh` for zones `external` and `internal`; `dns` for zone `internal`. No other services or ports should be allowed.

9 Submitting your work

Login as `root` on the server, and run `Turnin yourISUusername` to automatically submit your work. If you worked in a group, run `Turnin` once with the usernames of everyone in your group (for example: `Turnin alice bob chuck`). Check the `man` page for `Turnin` for more information. Note that there is nothing to submit on the client.