CSCI322 Lab Exercises

Lab 7

Objective

You will

- configure a Linux server as a NAT router for an internal network;
- reconfigure the DNS server for the new network;
- enable port forwarding on the host machine.

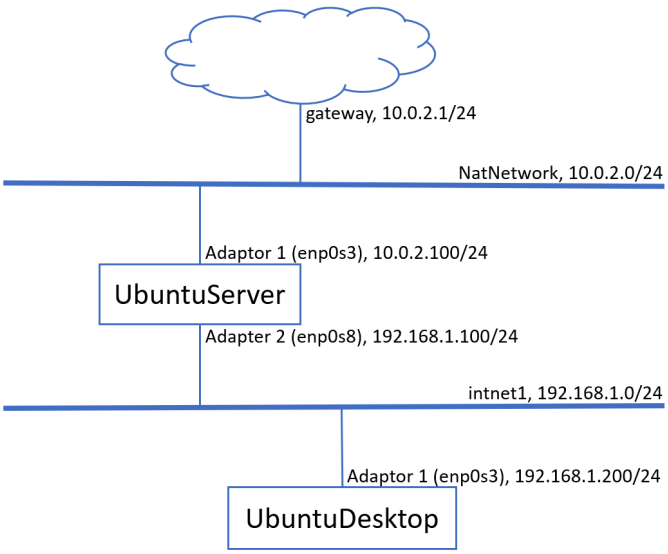
---

1. **Setup an internal network**

   Before you start any VMs, you will connect your server and desktop VMs to an internal network.

- Select the server from the left pane of the VirtualBox Manager and click the **Network** link on the **Details** pane.
- Enable **Adapter 2** and attach it to **Internal Network**; change the **Name** to `intnet1`.
- Then select desktop from the left pane of the VirtualBox Manger and click the **Network** link on the **Details** pane.
- Change the **Adapter 1** to attach to **Internal Network**; change the **Name** to `intnet1`.

  Now the network is set up as depicted in the following diagram.



2. **Configure the network adapters**

   You will set up static IP addresses for the Adapter 2 of the server VM and the Adapter 1 of the desktop VM according to the above network diagram. What will be the gateway for the desktop VM? You will still use 10.0.2.100 as the DNS server.

- You can use the `ip link` command to find out the adapter interface names. They may be different from the names indicated on the above diagram.
- Do not forget using the `netplan` command to apply the new network configurations. In some cases, you may need to restart your VMs.

Once you finish configuring the adapters, you can `ping` to each other VMs using their IP addresses to verify the configurations.

If your VMs can ping each other, you can try to `ping google.com` from both server and desktop VMs. Can you explain the results?

If you can `ping` from both VMs, you can proceed to the next task, otherwise fix the issues.

3. **Configure the server as a NAT router for the internal network**

You will configure the server VM as a NAT router for the internal network.

- The server VM gets the Internet on the other end of the Adapter 1 (`enp0s3`) through the default gateway (10.0.2.1). You will configure it as a gateway for the internal network (`intnet1`) to allow the desktop VM which connected to the internal network to access Internet through it. On the server, do the following.

```
sudo su
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
exit
```

These commands enable the packet forwarding in the server to work as a router and add the rules for the `iptables`. The rule in POSTROUTING chain in the NAT table indicates that the interface `enp0s3` should be used for outgoing packets and MASQUERADE indicates that the interface will mask the internal IP address (192.168.1.0/24) with the external IP address (10.0.2.100) of the router.

- Now you should able to `ping google.com` from the desktop VM.

- To make the packet forwarding persistent across boots, edit `/etc/sysctl.conf` on the server and make sure the `net.ipv4.ip_forward` variable is set to true as follows:

```
net.ipv4.ip_forward = 1
```

- To make the `iptables` rules persistent across boots, you need install a package and save the rules for boot.

```
sudo apt install iptables-persistent
```

If you does not save the rules while install the package, you need to save current rules.

```
sudo netfilter-persistent save
```

The `netfilter-persistent` package has been installed along with the `iptables-persistent` package.

4. **Reconfigure the DNS server**

You will reconfigure the DNS for the new hosts on the internal network. If your DNS still not working properly, this is the chance to make it work.

You will need to modify the forward zone file to change the IP address for the desktop VM. You will also modify the reverse zone file to remove the old entry for the desktop VM and create a new reverse

zone file for the internal network 192.168.1.0/24. You will need to modify the `named.conf.local` file to include the new reverse zone.

- Do not forget restart the `bind9` service;
- You should check the DNS configuration for errors; (How ?)
- You may need to clear the local DNS cache using the command `sudo systemd-resolve --flush-caches`.

Now you can `ping` each other VMs using their host names. Test the reverse zone as well.

5. **Enable port forwarding on the host machine**

   You will configure the NAT Network on the host machine to allow port forwarding that enables the host machine to access your web server on the server VM.

- On the VirtualBox Manager, select the `Preferences` from the `File` menu. Then select the `Network` and the configuration icon with a gear. Press the Port Forwarding button then add Rule 1. Set the values as follows.

```
Protocol: TCP
Host IP: 0.0.0.0
Host Port: 80
Guest IP: 10.0.2.100
Guest Port: 80
```

  This will forward the request on port 80 on the host machine to the port 80 on the virtual guest machine.

- Let's disable the name based virtual host of the Apache server on the server VM.

```
sudo a2dissite racktables
sudo systemctl reload apache2
```

- From your host machine (the physical machine, not virtual machines), open a browser to point to `http://localhost/dokuwiki`. You should see your Dokuwiki home page.

Submission and mark

Show your work to the lab tutor.

Of 3 marks, you can get

- 0.5 for demonstrating that the internal network is working by `ping`ing each other VMs using their IP addresses (Task 2);
- 1 for demonstrating that the NAT router is working by `ping`ing google.com from the desktop VM (Task 3);
- 1 for demonstrating that the DNS is working by `ping`ing each other VMs using their host names (Task 4);
- 0.5 for demonstrating that the port forwarding is working by accessing the Dokuwiki from the host machine (Task 5).

You should be ready to answer any questions to demonstrate that all work is done by yourself otherwise you may receive 0 mark.

IMPORTANT NOTE: You will need to document all of your lab work in CSCI322 in your wiki.