Routing Basics

1 Overview

This exercise explores basic network routing concepts in a Linux environment. These include use of the `route` command, defining a DNS server in the /etc/resolv.conf file, and using Network Address Translation (NAT).

This exercise, (and manual), is not intended to replace instruction or independent reading on the topic of network routing and routing in Linux systems. The exercise is intended to provide students with an environment with which they can experiment with the mechanics of routing network traffic.

2 Lab Environment

This lab runs in the Labtainer framework, available at http://my.nps.edu/web/c3o/labtainers. That site includes links to a pre-built virtual machine that has Labtainers installed, however Labtainers can be run on any Linux host that supports Docker containers.

From your labtainer-student directory start the lab using:

```
labtainer routing-basics
```

A link to this lab manual will be displayed.

3 Network Configuration

This lab includes four networked computers as shown in Figure 1. When the lab starts, you will get four virtual terminals, one connected to each component. The gateway is configured to perform routing between LAN1 and LAN2, and to route external addresses to an external gateway, e.g., to reach the Internet. The ws1 and ws2 workstations are pre-configured to route traffic to the gateway component. The ws3 workstation is not yet configured for routing.

The gateway is configured to use NAT to translate sources addresses of traffic from internal IP addresses, e.g., 192.168.1.1, to our external address, i.e., 203.0.113.10.

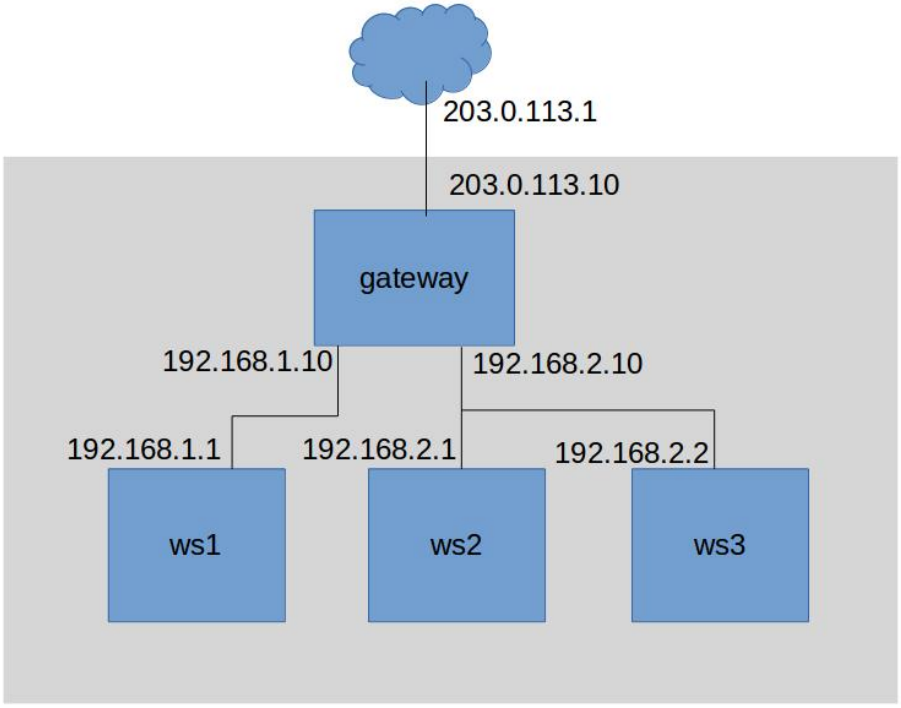

Figure 1: Network topology for routing-basics lab

4 Lab Tasks

4.1 Internal Routing

From each of the three workstations, enter the following command:

```
route -n
```

Note how ws1 and ws2 include routing table entries that name the gateway as the *default gateway*. This allows ws1 and ws2 to address each other, which can be demonstrated by using `ping` from ws1 to reach ws2:

```
ping [ws2 IP]
```

Now consider ws2 and ws3. Since they are both on the same LAN, they can ping each other. Try that for yourself. Then try to ping ws1 from ws3. That will fail because ws3 has no routing table entry defining what to do with traffic that is not destined for a LAN directly connected to ws3.

On ws3, define the gateway component as the *default gateway* using the `route` command, but this time using `sudo` because we are altering the routing:

```
sudo route add default gw [gateway IP]
```

Then try to ping between ws1 and ws3.

4.2 Routing to the Internet

The gateway component is configured to route to a simulated ISP at 203.0.113.1, which is a hidden component that provides routing to the Internet for this lab. From ws2, try to ping www.google.com. Then do the same from ws3. The problem with ws3 is that it has no domain name service (DNS) definition. Note, routing from ws3 to the Internet works fine, which you can confirm by pinging the IP address of www.google.com (as displayed when you pinged from ws2). The ws3 component simply lacks a DNS definition. On ws2, the DNS is defined to be the gateway component, and this is achieved in the `/etc/resolv.conf` file [1]. If you modify that file on ws3 to match that of ws2, that will tell ws3 to use the gateway as its DNS.

4.3 Use of Network Address Translation (NAT)

Finally, review how the gateway component implements NAT using the `iptables` utility. Consider traffic from ws1 destined for www.google.com. The source IP address on those packets is 192.168.1.1. The ws1 component sends the packets to its default gateway, i.e., our gateway component. The gateway routing table is configured to send external traffic to 203.0.113.1. However, before that traffic is sent, we need to translate the source IP address to our exernal 203.0.113.10 address so that google knows where to send replies. Use this command:

```
sudo iptables -L -v -t nat
```

to view our NAT rule, having a target of `MASQUERADE`, which will translate source addresses for all traffic destined for our external network interface. Then use this command:

```
sudo iptables -L -v
```

to see that we are forwarding traffic received from the two LANs.

Our iptables NAT rules are defined in the /etc/rc.local file on the gateway component.

[1] Many Linux systems include tools for defining your DNS, and these tools will overwrite the resolv.conf file. That is not an issue in these labs

5 Submission

After finishing the lab, go to the terminal on your Linux system that was used to start the lab and type:

```
stoplab routing-basics
```

When you stop the lab, the system will display a path to the zipped lab results on your Linux system. Provide that file to your instructor, e.g., via the Sakai site.