Static and Dynamic Routing[1]

HARDNESS : 8/10

University of Tehran
School of Electrical and Computer Engineering

دانشگاه تهران

دانشکده‌ی مهندسی برق و کامپیوتر

Computer Network Lab

آزمایشگاه شبکه‌های کامپیوتری

Professor:
Dr. Ahmad Khonsari
دکتر احمد خونساری
a_khonsari@ut.ac.ir

Amir Haji Ali Khamseh'i
امیر حاجی‌علی‌خمسه‌ء
khamse@ut.ac.ir

Reza Sharifnia
رضا شریف نیا
Reza.sharifnia@ut.ac.ir

Muhammad Borhani
محمد برهانی
borhani.m@ut.ac.ir

AmirAhmad Khordadi
امیراحمد خردادی
a.a.khordadi@ut.ac.ir

Sina Kashipazha
سینا کاشی‌پزها
sina_kashipazha@ut.ac.ir

Hadi Safari
هادی صفری
hadi.safari@ut.ac.ir

October 24, 2021

۲ آبان ۱۴۰۰

[1] S. S. Panwar, S. Mao, J.-dong Ryoo, and Y. Li, “Static and dynamic routing,” in TCP/IP Essentials: A Lab-Based Approach, Cambridge: Cambridge University Press, 2004, pp. 77–99.

Objectives

- Comparison of router and bridge.
- IP forwarding.
- Use of ICMP messages in routing.
- The Routing Information Protocol (RIP).
- The Open Shortest Path First (OSPF) protocol.
- Static routing by manually building the routing tables in the routers and hosts.
- Use of **Traceroute** to find an end-to-end route.

Part I

A Simple Router Experiment

In this lab, you need two hosts, a bridge, and two hubs, which are required to be connected as shown in Table 4.2 and Table 4.3.

Table 1: Router and Host IP addresses for Figure 4.10 (Table 4.2, Table 4.3)

Router		$Host_A$		$Host_B$	
eth0	eth1	Name	IP Address	Name	IP Address
128.238.61.1/24	128.238.62.1/24	h0	128.238.61.101/24	h1	128.238.62.101/24

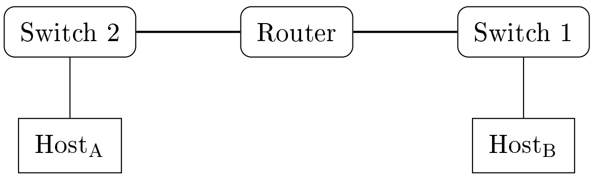

Figure 1: Simple router experiment (Figure 4.10)

1 Simple Routing

Configure the IP addresses of your hosts and the router as shown in Figure 4.10, Table 4.2 and Table 4.3 (select one of row in table).

Note: in Figure 4.10 that downloaded from Github, the above topology is configured.

Initially all hosts' routing table has no entry for the subnet on the other side of the router. In order to be connected, you need to add a routing entry for the other subnet in the routing table of all hosts (see section 4.3.1).

You can use one of the following commands to add routing in hosts.

```
# by ip command
ip route add remote-subnet dev eth0        # with interface name
ip route add remote-subnet via gateway-ip # with default gateway
# or by route command
route add -net remote-subnet dev eth0       # with interface name
route add -net remote-subnet gw gateway-ip # with default gateway
```

- *remote-subnet* is a subnet ip with mask number. It must be like `128.238.62.0/24`.
- *gateway-ip* is a gateway ip in your network. It must be like `128.238.61.1`
- *eth0* is a pyhisical interface name. It is shown in `ifconfig` or `ip a` commands.

***Note:* for example, enter the below commands in *h0* and *h1*'s Console:**

h_0's Console

```
ip route add 128.238.62.0/24 dev eth0
```

h_1's Console

```
    ip route add 128.238.61.0/24 dev eth0
```

Run `tcpdump -en` on first machine, and `tcpdump -en` on second machine in the other subnet simultaneously:

h_0 and h_1's Console

```
tcpdump -en host 128.238.62.101 and 128.238.61.101
```

Send `ping` messages continuously to other machine:

h_0's Auxiliary Console

```
ping -sv 128.238.62.101
```

After receiving the tenth echo reply, quit `ping` and save the `tcpdump` outputs from both machines. Also, copy the `ping` output.

During this exercise, don't run the `ping` program at the same time. For clean results, do your experiments in turn.

Report

1. When a packet was sent to a host in the other subnet, explain how the source and destination Ethernet addresses were changed.
2. What are the source and destination addresses in the IP and Ethernet headers of a packet that went from your machine to the router?
3. What are the source and destination addresses in the IP and Ethernet headers of a packet that went from the router to your partner's machine?
4. Answer the above two questions, but now for the echo reply that was returned from your partner's machine.
5. Use the `tcpdump` outputs from both machines to calculate the average delay that a packet experienced in the router. Note that the system times of the two machines might be different. Show all the steps and submit the `tcpdump` outputs with your report.
6. Compare this value with the previous value in the case of the bridge. Which, a router or a bridge, is faster? Why?

Part II

RIP Exercises

Consider Figure 4.11 as our network topology for this section.

In this section, we will examine the operation of RIP. To enable the RIP routing process in a router, use the following commands in the *Global Configuration* mode (use `config term` command).

R1#

```
config term
R1(config)# router rip
R1(config-router)# network network-number
```

where *network-number* could be 128.238.0.0 (Note: this means that you must replace *network-number* with 128.238.0.0 in above command).

Note: Repeat above command for all routers.

To remove the network, use:

R1(config-router)#

```
no network network-number
```

To shutdown the RIP process, use:

R1(config)#

```
no router rip
```

Configure network router and host's as Figure 4.11. Since our host's don't have `routed` package, you need to add route for subnet *128.238.0.0/16* to each host.

h_i's Console , i ∈ {0,1,...,7}

```
ip route add 128.238.0.0/16 dev eth0
```

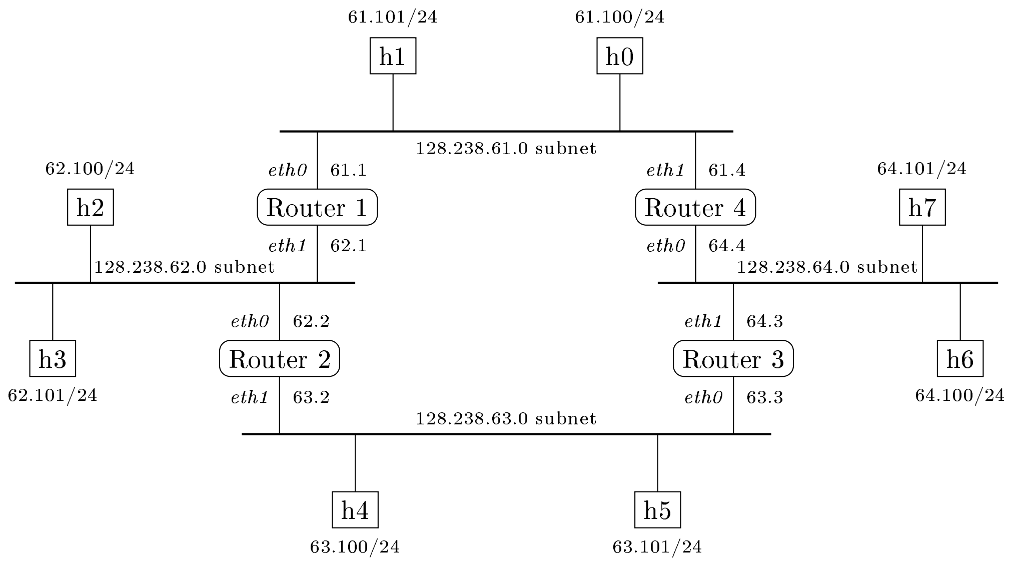

Figure 2: Network Configuration for RIP Exercises (Figure 4.11)

2 RIP Messages

Connect the routers and hosts and change the IP addresses of the hosts and router4 as shown in Figure 4.11.

Note: in Figure 4.11 that downloaded from Github, the above topology is configured.

Also, make sure that your host has no other routing entries than your own subnet and your loopback interface. For how to remove an entry from the host routing table, see Section 4.3 of reference book.

Configure the RIP in each router. For this purpose, enter below commands for all routers (R_i, i ∈ {1,...,4}).

R_i#

```
config term
Ri(config)# router rip
Ri(config-router)# network 128.238.0.0
```

After starting RIP in all the routers, test connections to other hosts by pinging them. (For example, run the below commands in *h0'* Console:)

h_0's Console

```
ping 128.238.62.100          #you should see ICMP packets
Ctrl+c
ping 128.238.63.100          #you should see ICMP packets
Ctrl+c
ping 128.238.64.100          #you should see ICMP packets
Ctrl+c
```

Once you can successfully reach all the hosts, run the following command to capture the RIP messages sent on your subnet, or run `wireshark` on link:

h_1' Console

```
tcpdump -x -s 100 -c 4 udp port 520
```

Save the routing table of router (`sh ip route` in *User EXEC* mode).

R_1#

```
sh ip route
```

Note the number of hops needed to reach destinations other than in your own subnet.

Mark and print two different RIP messages captured in your subnet (see Exercise 6 of Chapter 1 of reference book). Exchange the printed RIP messages with students in other groups. You need four different RIP messages for your lab report.

Report

1. Explain why you can only get two different RIP messages in your subnet. Was a RIP packet forwarded by the routers? Why?
2. Draw the format of one of the saved RIP response packets from your sub-net, including the IP and UDP headers and the RIP message (see Figs 0.13, 0.14, and 4.4). Identify each field, and express their values in decimal format.
3. For the other seven RIP response packets collected, explain the contents of the RIP messages only, excluding IP and UDP headers.
4. Draw the distance tables and the routing tables in the routers based on Figure 4.11, assuming that number of hops is used as the metric.
5. Verify the routing tables using the RIP messages you captured.

3 RIP recover on Link Failure

In this exercise we will examine how RIP responds to link failures. Send `ping` message continuously from *h3* to *h4* and start `tcpdump` on *h3*. Let the two programs run during this exercise.

h_3's Console

```
ping 128.238.63.100
```

h_3's Auxiliary Console

```
tcpdump
```

Disconnect the cable from the *ethernet0* port of *router2* from the hub in the 128.238.62.0 subnet (use `Router(config-interface)# shut` for interface in **GNS3**), and type the `date` command to get the current time.

To `shut` the above port in R_2, run the below commands:

R_2#

```
config term
R2(config)# interface f0/0
R2(config-if)# shut
R2(config-if)# end
```

Observe the `ping` and `tcpdump` windows. When the connection is re-established, type the `date` command again. See how much time RIP takes to alter the routing table in your hsot to the new topology.

Once you can successfully reach other hosts, connect the cable to the original position. For this purpose, run below command:

R_2#

```
config term
R2(config)# interface f0/0
R2(config-if)# no shut
R2(config-if)# end
```

Again, measure the time that RIP takes to change your routing table.

Report

1. Compare this time with the previous value in the spanning tree experiment.
2. Explain why it takes this time for RIP to react to the route change. Refer to Section 4.2.4 of reference book for RIP operation and default timer values.

Part III

Routing Experiments with ICMP

This exercise can run on Figure 4.11.

4 ICMP redirect

ICMP redirect is disabled by default in linux system for security (ICMP Redirect Attacks). You can enable this by this command:

h_i's Console , $i \in \{0,1,...,7\}$

```
sysctl -w net.ipv4.conf.all.accept_redirects=1
```

Create a default routing entry using one of the routers directly connected to your host (add route with default gateway). Also may you need to delete previously added route. For example you can set default route for *h1* to *R1->f0/0*.

any linux terminal

```
# by ip command
ip route add remote-subnet via gateway-ip # with default gateway
# or by route command
route add -net remote-subnet gw gateway-ip # with default gateway
```

For example, in *h0*'s Console run below command:

h_0's Console

```
ip route add 128.238.62.0/24 via 128.238.61.4
```

Open wireshark or run below command :

h_1's Console

```
tcpdump -enx -s 100 ip proto 1
```

While `tcpdump -enx -s 100 ip proto 1` is running, send `ping` messages to a host that is three hops away through the default router.

h_0's Console

```
ping 128.238.62.100
```

After capturing an ICMP redirect message, save the `tcpdump` output, the `ping` output, and your host's routing table. You may need to `ping` the same host several times in order to get your routing table updated.

Report

1. Submit what you saved in this exercise.
2. Identify every field in the ICMP redirect message (see Figure 4.2).
3. Compare the original routing table with the new routing table. Explain the meaning of the flags of the new entry.

5 ICMP router discovery

This exercise is on ICMP router discovery.

Connect the routers and hosts and change the host IP addresses as shown in Figure 4.11.

Telnet to the *R1* and *R4* routers (in GNS3, open routers console) shown in Figure 4.11. Enable ICMP router discovery on these two interfaces by the following interface configuration command:

Router(config-if)#

```
ip irdp
```

For example in R_1's Console, enter below commands:

R_1#

```
config term
R1(config)# interface f0/0
R1(config-if)# ip irdp
R1(config-if)# exit
R1(config)# interface f0/1
R1(config-if)# ip irdp
R1(config-if)# end
```

Repeat above command for *R4*.

Run Wireshark on *h1*'s link. Now, run `/home/netlab/code/rdisc -s #solicitation mode` on *h0*. Save the captured route discovery requests and replies for the lab report. Save *h0* routing table for the lab report.

h_0's Console

```
cd /home/netlab/code
-- When you go to the specified directory, run below command
/home/netlab/code# rdisc -s
```

Report

1. What is the destination IP address of the ICMP router solicitation message? Who sends the ICMP router advertisement message?
2. What are the type and code of the ICMP messages captured?
3. What are the advertised router IP addresses and their preference levels?
4. How many default router entries are there in *h0* routing table? Why?