A Single Segment Network[1]

HARDNESS : 5/10

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. Panwar, S. Mao, J.-dong Ryoo, and Y. Li, "A single segment network," in TCP/IP Essentials: A Lab-Based Approach, Cambridge: Cambridge University Press, 2004, pp. 43–60.

Objectives

- Network interfaces and interface configuration.
- Network load and statistics.
- The Address Resolution Protocol (ARP) and its operations.
- ICMP messages and Ping.
- Concept of subnetting.
- Duplicate IP addresses and incorrect subnet masks.

Part I

Network Interface Exercises

The following exercises use the single segment network topology shown in Figure 1.3.

Table 1: The IP addresses of the hosts (Table 1.2)

Host	IP Address	Subnet Mask
h0	128.238.66.100	255.255.255.0
h1	128.238.66.101	255.255.255.0
h2	128.238.66.102	255.255.255.0
h3	128.238.66.103	255.255.255.0
h4	128.238.66.104	255.255.255.0
h5	128.238.66.105	255.255.255.0
h6	128.238.66.106	255.255.255.0
h7	128.238.66.107	255.255.255.0

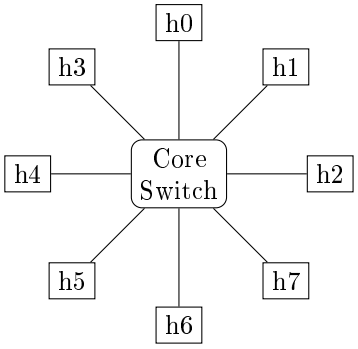

Figure 1: A single segment network (Figure 1.3)

1 Network Interfaces

Use the following command

h_0's Console

```
ifconfig -a
```

to display information about the network interfaces on *h0*. Find the IP address and the net mask of your machine.

Report

1. How many interfaces does the host have? List all the interfaces found, give their names, and explain their functions briefly.
2. What are the MTUs of the interfaces on *h0*?
3. Is network subnetted? What is the reasoning for your answer? What the experimental are the reasons for subnetting?

2 Local Host Dump

Right click on host *h0* and select Console from menu and use the following command

h_0's Console

```
tcpdump -i lo
```

While this command is running in one command window [1] , right click on host *h0* and select Auxiliary console itme from pop-up menu:

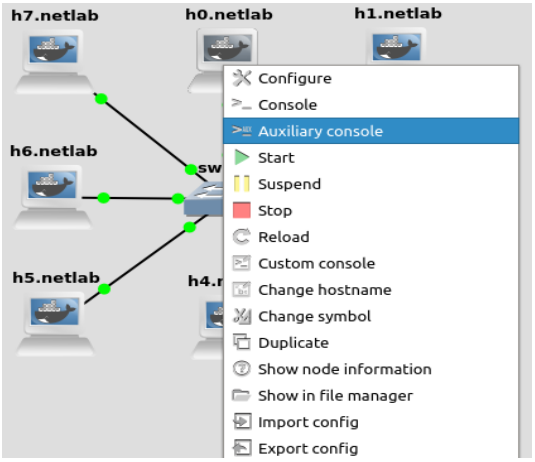

Figure 2

and run the following command

h_0's Auxiliary Console

```
ping 127.0.0.1
```

Report

1. From the `ping` output, is the 127.0.0.1 interface on? Can you see any ICMP message sent from your host in the `tcpdump` output? Why?

3 Network Statistics

By using below command, collect the statistics from all the hosts on the network [2] .

h_0's Console

```
netstat -ie
```

Since we use the same login name and password `(netlab)` , we can `telnet` to other hosts and run the following command there.[3]

h_0's Auxiliary Console

[1] In old linux use `tcpdump host your-host`

[2] You can use `ifconfig` instead.

[3] After you are done with a remote host, you should exit the `telnet` session before you `telnet` to another remote host. Recursive `telnet` will generate unnecessary data in the `tcpdump` output and cause confusion.

```
telnet 128.238.66.101
//after login to h1
netstat -ie
```

Save the `netstat -ie` outputs.

Note: If you don't see a significant amount of output packets in the `netstat` output, the machine was probably restarted recently. You may do this experiment later, or use the following `socket` command to generate some network traffic:

h_0's Auxiliary Console

```
socket -u -i -n200 remote-host echo
```

You should replace `remote-host` with valid IP address like 128.238.66.104

Report

1. Calculate the average collision rate over all the hosts for the set of statistics you collected in this exercise.

Part II

ARP Exercises

In the following experiment, we shall examine the host ARP table and the ARP operation, including two interesting cases: proxy ARP and gratuitous ARP. You may need to find **MAC** addresses of the host and router interfaces, and record these **MAC** addresses. You need these **MAC** addresses for the exercises and lab report (as table of host and **MAC**).

4 ARP Table

use the following command to see the entire ARP table on *h0*. Observe that all the IP addresses displayed are on the same subnet.

h_0's Console

```
arp -a
```

If you find that all the remote hosts are in *h0*'s ARP table, you need to delete a remote host from the table, using: [4]

h_0's Console

```
arp -d remote-host
```

Save the ARP table for your lab report.

While the following command is running [5],

h_0's Console

```
tcpdump -en
```

`ping` a remote host that has no entry in *h0* ARP table by running following command: (for example, we assume that *h4* has no entry in *h0* ARP table)

[4] If you deleted *h0*'s IP address from the ARP table by mistake, you must add the entry back in the table. See the `arp` manual page to add. Note that, in order for *h0* to reply to the ARP requests, the ARP entry of *h0* must have the `P` flag in the ARP table.

[5] You can add `-x` flag to see hex dump.

h_0's Auxiliary Console

```
ping 128.238.66.104
```

Then terminate the `tcpdump` program. (press Ctrl+C)

You can run `wireshark &` to capture network.

Observe the first few lines of the packet trace to see how ARP is used to resolve an IP address.

Run following command to see a new line added in *h0*'s ARP table. Save the new ARP table for your lab report.

h_0's Console

```
arp -a
```

Report

1. From the saved `tcpdump` output, explain how ARP operates. Draw the format of a captured, ARP request and reply including each field and the value.

Your report should include the answers for the following questions.

- What is the target IP address in the ARP request?
- At the **MAC** layer, what is the destination Ethernet address of the frame carrying the ARP request?
- What is the `frame` type field in the Ethernet frame?
- Who sends the ARP reply?

5 ARP Timeout

While following command is running to capture traffic from your machine,

h_0's Console

```
tcpdump host 128.238.66.100
```

execute the following command. Note there is no host with this IP address in the current configuration of the lab network.

h_0's Auxiliary Console

```
telnet 128.238.66.200
```

Save the `tcpdump` output of the first few packets for the lab report.

After getting the necessary output, terminate the `telnet` session.

Report

1. From the saved `tcpdump` output, describe how the ARP timeout and retransmission were performed. How many attemps were made to resolve a non-existing IP address?

6 ARP Proxy

The network topology for this proxy ARP exercise is shown in Figure 2.9. The IP addresses and network masks for the hosts are also given in Figure 2.9. Change the IP address and network mask of *h0* accordingly (see Section 2.3.2 of reference book). Change the IP addresses and network masks of the *Router4* interfaces according to Figure 2.9. (If you use the github figures, these configurations have been sets).

Note Network mask of the hosts in the 128.238.65.0 network is 255.255.0.0.

Note Only use *h0, h1, h4, h5* hosts (Do not start extra hosts).

a. Start device *h0,h1,h4,h5* by right click on it and select start

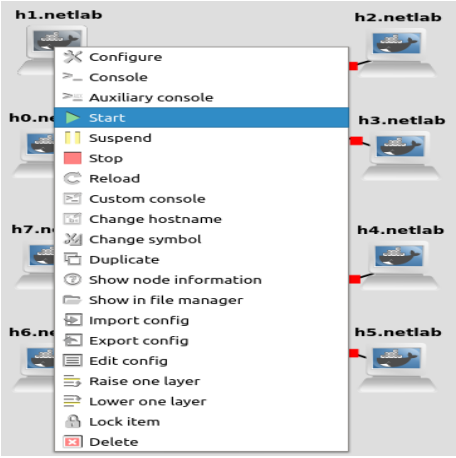

Figure 3

b. Start router by right click on it and select start

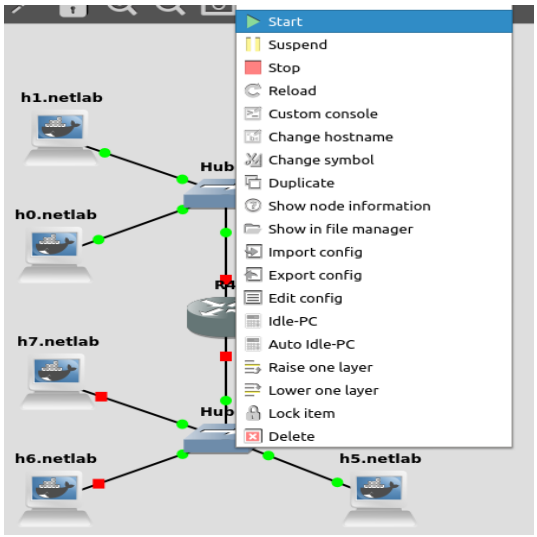

Figure 4

Next we will enable the proxy ARP function on the ethernet1 interface of *Router4* [6].

1. Right click on the router and select console
2. Enter the *Global Configuration* mode by typing below command

   `R4#`

[6] We will discuss bridge and router configuration in Chapter 3.

```
config term
```

3. Then type the following command for interface f0/0

R_4(config)#

```
interface f0/0                    !
```
[7]

R_4(config-if)#

```
ip proxy-arp
Ctrl-Z
```

4. Use following command for another interface (f0/1)

R_4#

```
config term
```

R_4(config)#

```
interface f0/1
```

R_4(config-if)#

```
ip proxy-arp
Ctrl-Z
```

Now *Router4*'s *ethernet1* interface can perform proxy ARP for the hosts in the 128.238.64.0 subnet. Run the following command or use wireshark:

h_1's Console

```
tcpdump -enx
```

Also,

h_5's Console

```
tcpdump -enx
```

Then let the hosts in the 128.238.65.0 subnet send UDP datagrams to the hosts in the 128.238.64.0 subnet. For example, on *h4* type:

h_4's Console

```
socket -i -u -n1 -w1000 128.238.64.100 echo
//after running above command
socket -i -u -n1 -w1000 128.238.64.101 echo
```

Repeat this commands for host *h5*. Save the `tcpdump` output for the lab report.

To display the new ARP table in *h1*, *h4* and *h5* run following command.

h_0's Console

[7] The name of the router interfaces may be different for various routers.You can find the names by typing **write term** in the *Privilege EXEC* mode.

```
arp -a
```

h_1's Console

```
arp -a
```

h_5's Console

```
arp -a
```

Save the ARP table for your lab report.

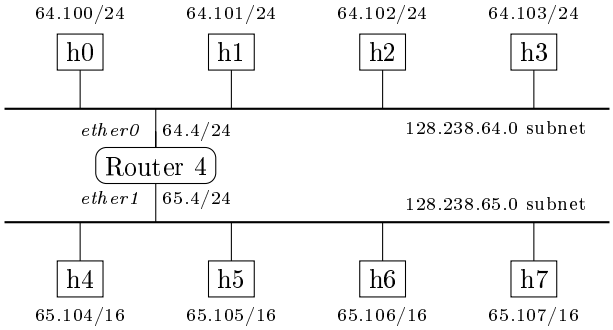

Figure 5: Network configuration (Figure 2.9)

Note: If you need the MAC address of the router interfaces, login to the router and run the following command in the router console.

R_4#

```
show interfaces
```

Report

1. Explain the operation of proxy ARP.
2. Why can a host in the 128.238.65.0 subnet reach a host in the 128.238.64.0 subnet, even though they have different subnet IDs?
3. What are the **MAC** addresses corresponding to hosts in the 128.238.64.0 subnet, in the ARP table of a host in the 128.238.65.0 subnet?
4. Give one advantage and one disadvantage of using proxy ARP.

7 ** Gratuitous (Unsolicited) ARP

Start all devices and capture traffic on link connected to host `h0` by right click on it and select start capturing

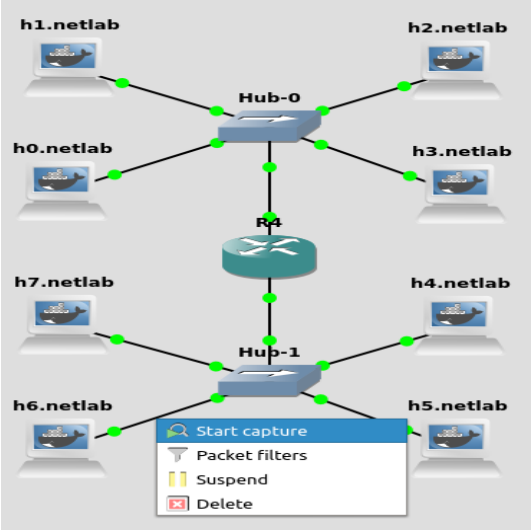

Figure 6

After these steps right click on host `h6` and select console and use the following command

h_6's Console

```
tcpdump -ex
```

Right click on host `h7` and select console, you can send the gratuitous ARP manually by use the following command

h_7's Console

```
arping -c 4 -A -I eth0 128.238.65.106
```

see ARP Table in host `h6` by use the following command

h_6's Console

```
arp -a
```

Now reboot host `h7` by right click on host `h7` and select console and use the following command again

h_7's Console

```
arping -c 4 -A -I eth0 128.238.65.106
```

h_6's Console

```
arp -a
```

print the gratuitous ARP request for your lab report.

Report

1. What is the purpose of gratuitous ARP?
2. List the sender IP address, target IP address, sender **MAC** address, and target **MAC** address of the gratuitous ARP you saved.
3. What is the ARP table in *h5*?

Part III

Exercise with ICMP and ping

The following exercises use the previous network topology shown in Figure 2.9.

8 ping ICMP

While running the following command:

h_0's Console

```
tcpdump -enx host 128.238.64.100 and remote-host
```

Execute this command to test whether the remote host is reachable.

h_0's Auxiliary Console

```
ping -sv remote-host
```

(remote-hast can be *h1*, *h4* or *h5* IP address)

Save the `tcpdump` and `ping` output for the future study on `ping`.

Report

1. What ICMP messages are used by `ping`?

9 ICMP Port Unreachable

While running the following command,

h_0's Console

```
tcpdump -x -s 70 host 128.238.64.100 and remote-host
```

execute the following `socket` command to send a UDP datagram to the remote host

h_0's Auxiliary Console

```
socket -i -u -n1 -w1000 remote-host 88888
```

(remote-hast can be *h1*, *h4* or *h5* IP address) Save the `tcpdump` output for the lab report.

Report

1. Study the saved ICMP port unreachable error message (See Figure 2.7 of reference book.). Why are the first 8 bytes of the original IP datagram payload included in the ICMP message?

10 ICMP Network Unreachable

While `tcpdump` is running in host *h2* to capture the ICMP messages,

h_2's Console

```
tcpdump
```

`ping` a host with IP address `128.238.60.100` by use the following command

h_2's Auxiliary Console

```
ping 128.238.60.100
```

and Save the `ping` output.

Report

1. Can you see any traffic sent on the network? Why? Explain what happened from the `ping` output.
2. List the different ICMP messages you captured in Exercise with ICMP and `ping`. Give the values of the type and code fields.

Part IV

Exercises with IP address and subnet mask

In this section, we will observe what happens when the same IP address is assigned to two different hosts. We will also set an incorrect subnet mask for hosts and see what are the consequences. For the next two exercises, we use only four host from single segment network (Figure 1.3).

11 Duplicate IP

Change the IP address of your hosts as shown in Table 2.3.

Table 2: Host IP addresses and network masks for Duplicate IP (Table 2.3)

Host	IP Address	Subnet Mask
h0	128.238.66.100	255.255.255.0
h1	128.238.66.100	255.255.255.0
h2	128.238.66.102	255.255.255.0
h3	128.238.66.103	255.255.255.0

Delete the entries for all hosts other than your host from ARP table.

- Start device *h0, h1, h2, h3* by right click on it and select start.
- Right click on host *h1*, then select Console item and change IP address of it by run the following command:

h_1's Console

```
ip address del 128.238.66.101/24 dev eth0
ifconfig eth0 128.238.66.100 netmask 255.255.255.0
```

Run the following command on all the hosts.

h_0, h_1, h_2 and h_3's Auxiliary Console

```
tcpdump -enx
```

Now, do the following three experiments:

1. Execute `telnet` from one of two hosts with the duplicate IP address to a host with unique IP address by run following commands(e.g. *h0* → *h2*).

   h_0's Console

   ```
   telnet 128.238.66.102
   ```

   Now, from the other host with the duplicate IP address, execute `telnet` command to the same host by run following command(*h1* → *h2*).

   h_1's Console

   ```
   telnet 128.238.66.102
   ```

   h_0, h_1 and h_2's Console

   ```
   arp -a
   ```

   Observe what happens and save the `tcpdump` output and the ARP tables in all the hosts in your group.

2. Execute the following commands

   h_2's Console

   ```
   telnet 128.238.66.100
   ```

   Which host provides the telnet connection? Why?

3. Execute the following command

   h_3's Console

   ```
   telnet 128.238.66.100
   ```

   Which host is connected to *h3*? Why?

Report

1. Explain what happened in the first case and why. Answer the questions for the second and third cases.

12 IP Subnets

Change the host IP addresses and the subnet masks as shown in Table 2.4. Note that two hosts in each group (*h0* and *h3*) are assigned an incorrect subnet mask.

Table 3: Host IP addresses and network masks for IP Subnets (Table 2.4)

Host	IP Address	Subnet Mask
h0	128.238.66.100	255.255.255.240
h1	128.238.66.101	255.255.255.0
h2	128.238.66.102	255.255.255.0
h3	128.238.66.120	255.255.255.240

- Start hosts *h0, h1, h2, h3* by right click on them and select start.
- Right click on host *h0* and select Console to change its IP address by running the following command

h_0's Console

```
ip address del 128.238.66.100/24 dev eth0
ifconfig eth0 128.238.66.100 netmask 255.255.255.240
```

(note: you can used `ip address add 128.238.66.100/28 dev eth0` command instead of `ifconfig eth0 128.238.66.100`)

- Right click on host *h3* and select Console to change its IP address by running the following command

h_3's Console

```
ip address del 128.238.66.103/24 dev eth0
ip address add 128.238.66.120/28 dev eth0
```

Capture the packets with below command for the following cases:

h_0, h_1 and h_3's Auxiliary Console

```
tcpdump -e
```

1. When *h0* `ping`s one of the hosts that have the correct subnet mask.(Used the following command)

   h_0's Console

   ```
   ping 128.238.66.101
   ```

2. When *h3* `ping`s one of the hosts that have the correct subnet mask. (Used the following command)

   h_3's Console

   ```
   ping 128.238.66.101
   ```

3. When a host with the correct subnet mask `ping`s *h0*. (Used the following command)

   h_1's Console

   ```
   ping 128.238.66.100
   ```

4. When a host with the correct subnet mask `ping`s *h3*. (Used the following command)

   h_1's Console

   ```
   ping 128.238.66.120
   ```

Report

1. Explain what happened in each case according to the `tcpdump` outputs saved. Explain why *h3* could not be reached from other hosts, whereas *h0*), which has the same incorrect subnet mask, could communicate with the other hosts.