Linux and TCP/IP Networking[1]

HARDNESS : 4/10

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, "Linux and TCP/IP networking," in TCP/IP Essentials: A Lab-Based Approach, Cambridge: Cambridge University Press, 2004, pp. 26–42.

0.1 Review and Guidance

First, launch GNS3. To use prepare topology that download from Github (figures):

1. Open File menu
2. Select Import portable project

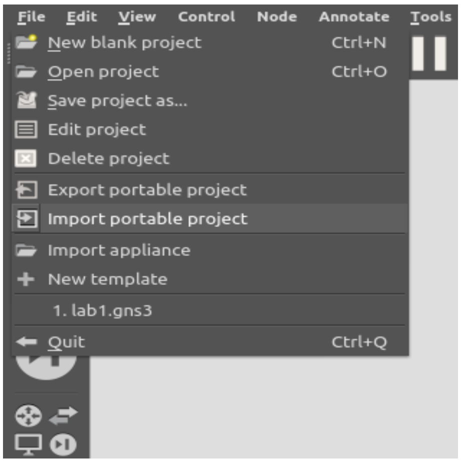
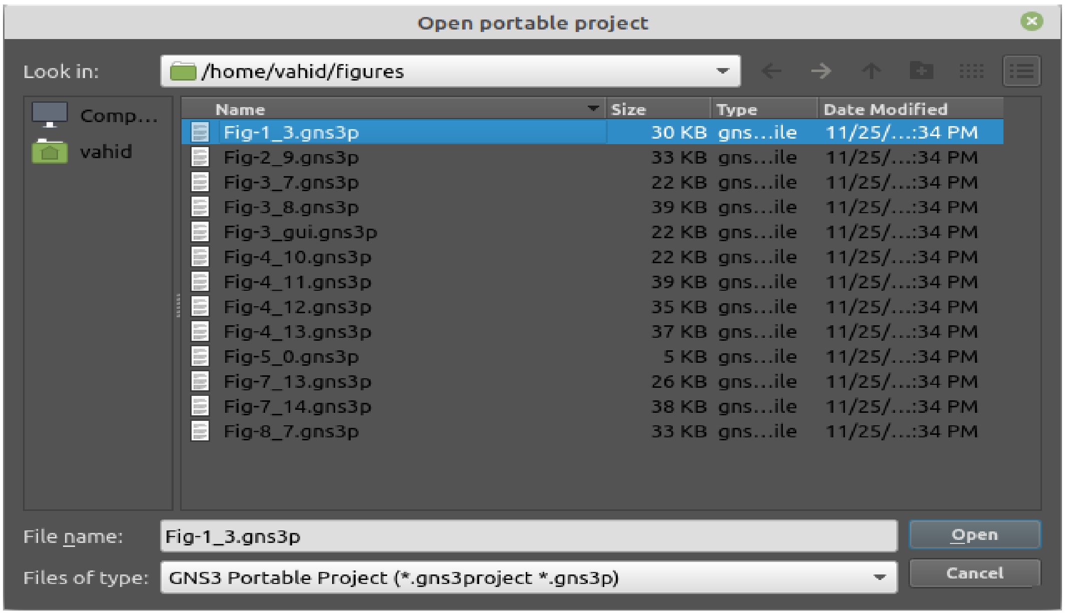


Figure 1

3. Choose the figures (from your Figures folder address)



Look in: /home/vahid/figures

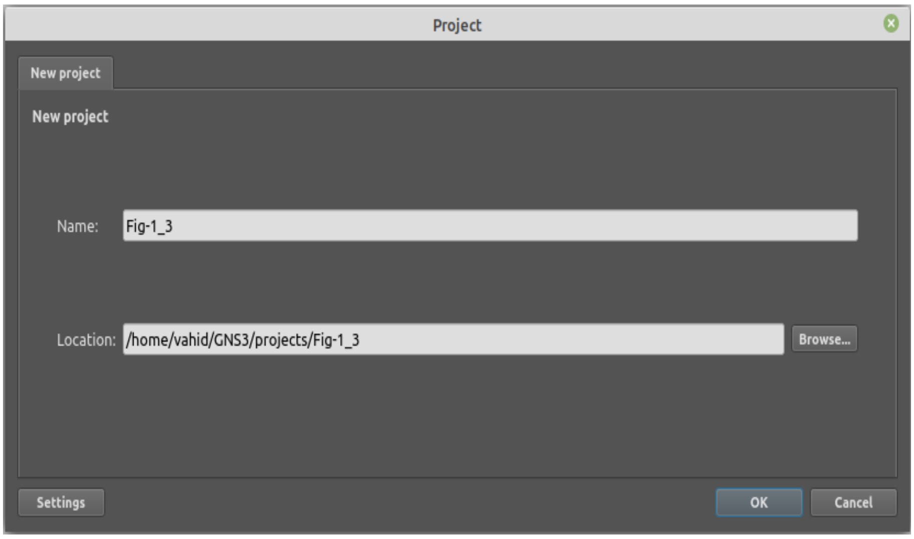
Name	Size	Type	Date Modified
Fig-1_3.gns3p	30 KB	gns...ile	11/25/...:34 PM
Fig-2_9.gns3p	33 KB	gns...ile	11/25/...:34 PM
Fig-3_7.gns3p	22 KB	gns...ile	11/25/...:34 PM
Fig-3_8.gns3p	39 KB	gns...ile	11/25/...:34 PM
Fig-3_gui.gns3p	22 KB	gns...ile	11/25/...:34 PM
Fig-4_10.gns3p	22 KB	gns...ile	11/25/...:34 PM
Fig-4_11.gns3p	39 KB	gns...ile	11/25/...:34 PM
Fig-4_12.gns3p	35 KB	gns...ile	11/25/...:34 PM
Fig-4_13.gns3p	37 KB	gns...ile	11/25/...:34 PM
Fig-5_0.gns3p	5 KB	gns...ile	11/25/...:34 PM
Fig-7_13.gns3p	26 KB	gns...ile	11/25/...:34 PM
Fig-7_14.gns3p	38 KB	gns...ile	11/25/...:34 PM
Fig-8_7.gns3p	33 KB	gns...ile	11/25/...:34 PM

File name: Fig-1_3.gns3p

Files of type: GNS3 Portable Project (*.gns3project *.gns3p)

Figure 2

4. Enter a name for new project and click OK



Name: Fig-1_3

Location: /home/vahid/GNS3/projects/Fig-1_3

Figure 3

5. Now you can see a network like Figure 4

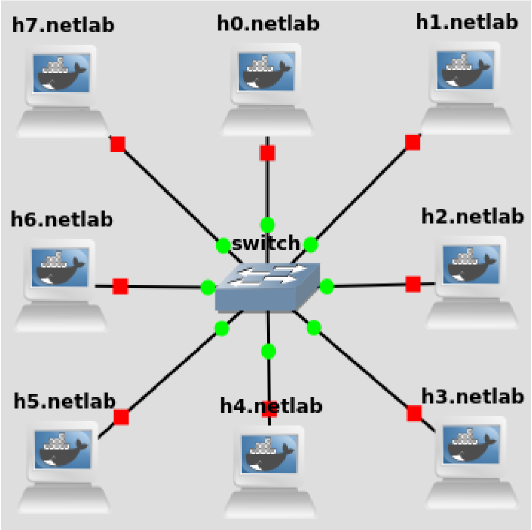


Figure 4

6. Start all devices by clicking on the Start/Resume button (green triangular button)

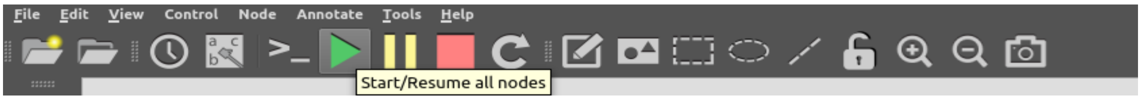


Figure 5

7.All devices turn on slimilar to Figure 6 .

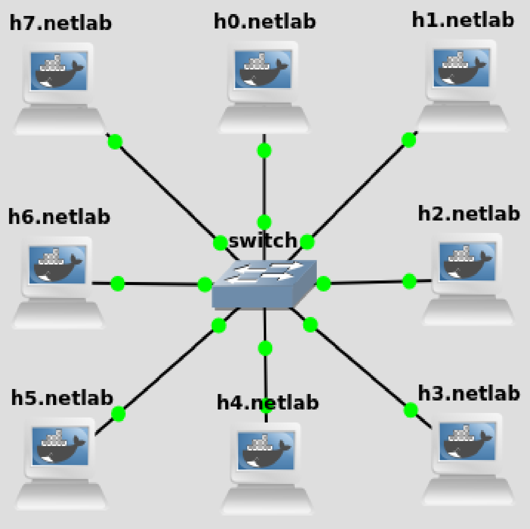


Figure 6

0.2 Attention

You don't need to set IP address for each host in all figures that download from Github, because the IP addresses set by default in all hosts. However, if you want to set IP address for a host, you can open console terminal by right-clicking on a host and selecting console and type the following command. For example, we set IP address for host `h0`.

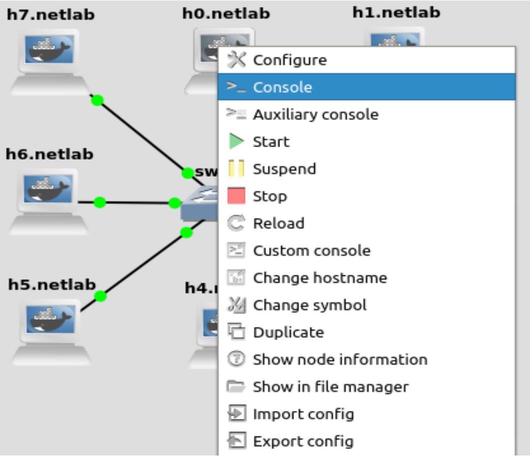


Figure 7

h_0's Console

```
    ip address add 128.238.66.100/24 dev eth0
```

0.3 Tips

h_0's Console

```
    ifconfig -a
```

This box means that, Right click on host *h0* and select Console item from Pop-up menu:

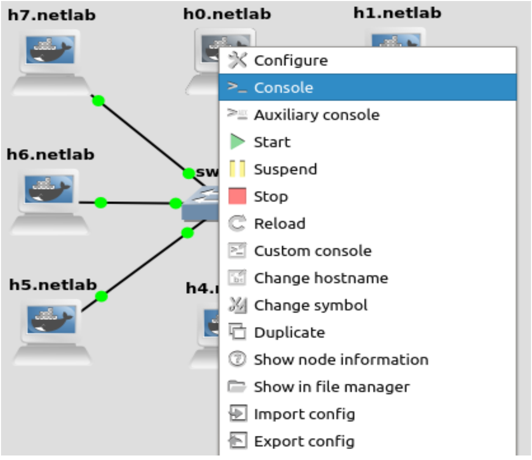


Figure 8

In Console window type(run) the below command:

```
ifconfig -a
```

Objectives

- Getting acquainted with the lab environment.
- Getting acquainted with the Linux operating system.
- Preview of some TCP/IP diagnostic tools.
- Capturing and analyzing the link layer, IP, and TCP headers.
- Understanding the concept of encapsulation.
- Understanding the concept of multiplexing using *port numbers*, the IP *protocol* field, and the Ethernet *frame type* field.
- Understanding the client–server architecture.

Part I

Systems Configuration

Launch GNS3 and make a network as below. You can use `ifconfig eth0 192.168.0.1 netmask 255.255.255.0` to set ip.

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

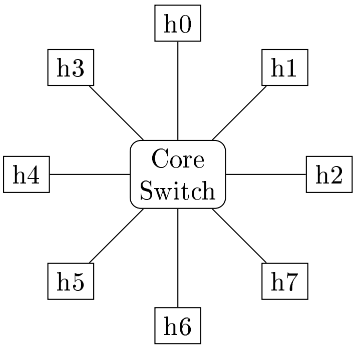


Figure 9: A single segment network (Figure 1.3)

1 Telnet Service

Run `ps -e` to list the processes running in the *h1*.

h_1's Console

```
ps -e
```

After starting a new process by running `telnet` in another command window (open new auxiliary console):

h_1's Auxiliary Console

```
telnet
```

then execute `ps -e` again in a third window to see if there is any change in its output.

h_1's Console

```
ps -e
```

Find the process id of the `telnet` process you started, by:

h_1's Console

```
ps -e | grep telnet
```

Then use `kill` ***process-id-of-telnet*** to terminate the `telnet` process.

Report

1. What is Internet Service Daemon (`inetd`)?
2. Is `inetd` started in your system? Why?
3. Is `xinetd` started in your system? What is its PID?

2 Default Network Services

Display the file `/etc/services` on the *h1* screen, using:

h_1's Console

```
more /etc/services
```

Then in another console (Auxiliary console), use the redirect operator to redirect the `more` output to a file using `more /etc/services > ser-more` .

h_1's Auxiliary Console

```
more /etc/services > ser-more
```

Compare the file `ser-more` with the original `more` output in the other command window.

Copy `/etc/services` file to a local file named `ser-cp` in your working directory (use `pwd` to see working directory path), using `cp /etc/services ser-cp` .

h_1's Console

```
cp /etc/services ser-cp
```

Compare files `ser-more` and `ser-cp`, using `cmp ser-more ser-cp` . Are these two files identical?

h_1's Console

```
cmp ser-more ser-cp
```

Concatenate these two files using `cat ser-more ser-cp > ser-cat` .

h_1's Console

```
cat ser-more ser-cp > ser-cat
```

Display the file sizes using `ls -l ser*` . Save the output.

h_1's Console

```
ls -l ser*
```

Report

1. What are the sizes of files `ser-more`, `ser-cp`, and `ser-cat`?

3 Network Command Manual

Read the `man` pages for the following programs:

1. `arp`
2. `arping`
3. `ifconfig`
4. `tcpdump`
5. `ping`
6. `netstat`
7. `route`
8. `wireshark`
9. `iptables`

For example, run the following command:

h$_1$'s Console

```
man arp
```

Study the different options associated with each command. Throughout this lab you will use these commands rather extensively.

Report

1. Explain the above commands briefly. (Two or three sentences per command would be adequate.)

4 Packet Capturing

In this exercise, we will use `tcpdump` to capture a packet containing the link, IP, and TCP headers and use `wireshark` to analyze this packet.

Note: In GNS3 you can capture and see packet in `wireshark` with right click on wire between *host* and *switch* and select *Start Capture*.

First, run `tcpdump` in the *h1* or run `wireshark`.

h$_1$'s Console

```
tcpdump
```

Then, you may want to run `telnet 128.238.66.102` in the *h1* to generate some TCP traffic.[1]

h$_1$'s Auxiliary Console

```
telnet 128.238.66.102
```

After you login to *h2* (*Note:* use **netlab** for username and password), terminate the `telnet` session (press *CTRL+D* or run *kill* command) and terminate the `tcpdump` program (press *CTRL+C* in `tcpdump` terminal window.

Next, you will use `tcpdump` or `wireshark` to see the packet trace captured by `tcpdump` or `wireshark` and analyze the captured packets.

The `wireshark` Graphical User Interface (GUI) will pop up and the packets captured by `tcpdump` will be displayed. Select any one of the packets that contain the link, IP, and TCP headers.

[1] Remember to run `/etc/init.d/xinetd restart` in the *h2* to start telnet server on it.

Report

1. What is the value of the `protocol` field in the IP header of the packet you saved? What is the use of the `protocol` field?
2. What is the value of the `frame type` field in an Ethernet frame carrying an IP datagram?

5 ARPing

This time we will run `wireshark` to capture an ARP request and an ARP reply in real-time. Simply run `wireshark` on the *h1* link with right click and select **start capture** item to start capturing[2]. If there is no arp requests and replies in the network, generate some using `arping 128.238.66.102` command in the *h1* terminal.

h$_1$'s Console

```
arping 128.238.66.102
```

Now you should see several ARP replies in the `arping` output.

Report

1. What is the value of the `frame type` field in an Ethernet frame carrying an ARP request and in an Ethernet frame carrying an ARP reply, respectively?
2. What is the use of the `frame type` field?

6 Packet Filtering

Using the `tcpdump` utility, capture any packet on the LAN and see the output format for different command-line options. Study the various expressions for selecting which packets to be dumped.

For this experiment, use the `man` page for `tcpdump` to find out the options and expressions that can be used.

If there is no traffic on the network, you may generate traffic with some applications (e.g. `telnet` , `ping` , etc.).

Report

1. Explain briefly the purposes of the following `tcpdump` expressions.

If you are using `tcpdump` , explain the following filters:

- `tcpdump udp port 520`
- `tcpdump -x -s 120 ip proto 89`
- `tcpdump -x -s 70 host ip-addr1 and (ip-addr2 or ip-addr3)`
- `tcpdump -x -s 70 host ip-addr1 and not ip-addr2`

If you are using `wireshark` explain the following filters:

- `udp.port == 520`

[2] On physical machine, can start capture with `wireshark &` command.

- `ip.proto == 89`
- `ip.addr == ip-addr1 and (ip.addr == ip-addr2 or ip.addr == ip-addr3)`
- `ip.addr == ip-addr1 and not ip.addr ip-addr2`

7 Connection Port

Run `wireshark` on the *h1* link and select an interface to capture packets between hosts.

Execute a TCP utility, `telnet` for example, in command window:

h_1's Console

```
telnet 128.238.66.102
```

Report

1. What are the port numbers used by the *h1* (local machine) and the *h2* (remote machine)?
2. Which port numbers matches the port number listed for `telnet` in the `/etc/services` file?

8 Random Port

Run `wireshark` on the *h1* link and select an interface to capture packets between hosts.

Then, `telnet` to the *h2*, from a command window by typing `telnet 128.238.66.102` .

h_1's Console

```
telnet 128.238.66.102
```

Again issue the same `telnet 128.238.66.102` command from another command window.

h_1's Auxiliary Console

```
telnet 128.238.66.102
```

Now you are opening two `telnet` sessions to *h2* simultaneously, from two different command windows.

Check the port numbers being used on both sides of the two connections from the output in the `wireshark` window.

Report

1. When you have two `telnet` sessions with your machine, what port number is used on the *h2* (remote machine)?
2. Are both sessions connected to the same port number on the *h2* (remote machine)?
3. What port numbers are used in the *h1* (local machine) for the first and second `telnet` , respectively?
4. Explain briefly what a `socket` is.