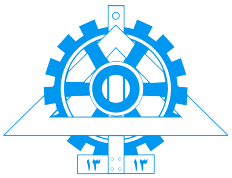
In the name of Allah

بسم الله الرحمن الرحیم

The Web, DHCP, NTP and NAT Laboratory Manual



University of Tehran
دانشگاه تهران

School of Electrical and Computer Engineering
دانشکده مهندسی برق و کامپیوتر

Computer Network Lab
آزمایشگاه شبکه‌های کامپیوتری

Dr. Ahmad Khonsari - احمد خونساری
a_khonsari@ut.ac.ir

Amir Haji Ali Khamseh'i - امیر حاجی علی خمسه‌ء
khamse@ut.ac.ir

Muhammad Borhani - محمد برهانی
Amirahmad Khordadi - امیر احمد خردادی
Sina Kashi pazha - سینا کاشی پزها
Mohammad Ali Shahsavand - محمد علی شاهسوند

March 5, 2019

۱۴ اسفند ۱۳۹۷

HTTP

Requirement:

1. Apache[1] or Nginx[2] web service
2. curl

1 HTTP Server

Config your Apache server configuration file[3] (see Section 8.2.3 Ref Book). Examine the various configuration directives used and the corresponding settings.
Start the Apache server on your host. In order to check if the server is working properly, you may start a `Mozilla` web browser to download the test page at `http://localhost/`. Then, execute **pgrep apache2** to list the process IDs of the **apache2** processes started. Save the output and the configuration file for the lab report.

Report

1. How many apache2 processes were started? Which one was the master server, and which ones were the child servers? Justify your answer using the `apache2.conf` file.
2. What is the purpose of initiating multiple apache2 processes?

2 HTTP Request

Execute **wireshark** to capture packets between your host and a remote host.
Login to the remote host's web server: **telnet** `10.0.0.2` **80**.
In the login console, type the following HTTP request line by line:

```
GET /usage/index.html HTTP/1.0
From: guest@your host
User-Agent: HTTPTool/1.0
```

Note that you need to type the `Return` key to input the last line, which is blank. When the **telnet** process is terminated, save the output for your lab report.
Terminate **wireshark** and analyze the captured HTTP packets. Print and save the HTTP request and response. Save the HTTP response's data part into a file, named `index.html`. Use `Mozilla` to view the file.

Report

1. Submit the HTTP request and response, including the start-lines and all the headers.

3 HTTP Keep-Alive

By default, Apache server supports persistent connections. Before this exercise, the lab instructor should check the `KeepAlive` directive in the server configuration file to make sure it is turned on, as `KeepAlive` on.
Execute **wireshark** to capture packets between your host and a remote host.
Start `Mozilla` on your host. Go to menu `Edit/Preferences/Advanced/HTTP Networking`, and uncheck the Enable `Keep-Alive` checkbox to disable persistent connections.
Enter the URL `http://10.0.0.2/try1.html`, to download the HTML file consisting a line of text, an embedded picture, and a hyperlink. Use **wireshark** and print the HTTP requests and responses for the lab report.

[1] `sudo apt-get install apache2 apache2-utils`
[2] `sudo apt-get install nginx`
[3] `/etc/apache2/apache2.conf`

- *You can use* ***curl -v http://www.google.com http://www.google.com*** *to get multiple query in one command.*

Restart the **wireshark** program. Goto `Mozilla` menu `Edit/Preferences/Advanced/HTTP Networking`, and enable persistent connections by checking Enable `Keep-Alive`.
Use `Mozilla` to reload the `try1.html` file.
Use **wireshark** and print the HTTP requests and responses for the lab report.

Report

1. When you browsed the `try1.html` file for the first time, how many HTTP requests were sent? Which files were requested? How many TCP connections were used?
2. Answer the above questions for when you browsed the `try1.html` file for the second time.
3. What is the purpose of using persistent connections?

4 HTTP Submit

Execute **wireshark** to capture packets between your host and a remote host.
Use `Mozilla` to download the `http://remote_host/try2.htm` file, which is an `HTML` form, from the remote host.
Fill a text string, e.g., the name of the host being used, into the text field in the form and click the submit button in the form.
When the server response is received, terminate **wireshark**.
Examine how CGI works, and identify the data string sent to the server. Save the HTTP request containing the data string for lab report.

Report

1. Submit the data string sent to the server.

DHCP

In this exercise, we use `guchi` as the DHCP server, with a configuration file shown in Table 8.3. Do the following.

1. Install DHCP Server: `$sudo apt-get install isc-dhcp-server`[4]
2. Run mininet with 4 hosts `sudo mn -topo linear,4`
3. Set MAC address of h4 in dhcpd.conf for static IP assignment
4. Set ip in **h1**: `ifconfig h1-eth0 128.238.66.1 netmask 255.255.255.0`
5. Start the DHCP server on `h1` in the foreground and working in the debugging mode: **dhcpd -d -f**.
6. Execute **wireshark** to capture the DHCP messages in the network segment.
7. Then do the following to enable DHCP for the Ethernet interface on `h2`.
   Run on **h2**: `ifconfig eth0 0`
   And run `dhclient eth0`
   Run `ifconfig` to see new ip
   Save the outputs for the lab report.
8. Then, repeat 3 for `h3`.
9. Repeat 3 for h4.

[4] ubuntu->isc-dhcp-server or extera

10. Repeat 3 for h5.

Terminate **wireshark**.Print out the DHCP messages for the lab report.
Save the DHCP server output on `guchi` for the lab report.

Table 8.3: A DHCP server configuration file

```
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 128.238.66.255;
option routers 128.238.66.1;
#option domain-name-servers 128.238.2.38, 128.238.3.21;
#option domain-name "netlab.ut.ac.ir";

subnet 128.238.66.0 netmask 255.255.255.0 {
    range 128.238.66.111 128.238.66.112;
}

host h4 {
    hardware ethernet 08:00:20:79:e9:9f;
    fixed-address 128.238.66.110;
}
```

Report

1. Compare the DHCP operation captured by **wireshark** and that shown by the DHCP server output. Explain how DHCP works.
2. Did `h2` and `h3` successfully obtain a set of new parameters? Compare the ifconfig and netstat output with the parameters carried in the corresponding DHCP messages.
3. Answer the above question for agni. Explain why agni failed.
4. Answer the above question for h4. Explain why h4 succeeded.

NTP

5 NTP Local Date

Execute **date** to display the system time of your host. Display the manual page of **date**, and study its options and usages. Try the following **date** commands:

```
date --date='2 days ago'
date --date='3 months 2 days'
date --set='+3 minutes'
date -r file_name
```

You can choose any file in the current directory for the *file_ name* parameter.

Report

1. Submit the **date** outputs you saved. Explain the use of the commands.

6 NTP Remote Date

While **wireshark** is running, execute **rdate -p** *remote_host* to display the system time of the remote machine. Repeat the above **rdate** command, but use the **-u** option. Save the **wireshark** outputs for the lab report.

Report

1. What port numbers were used by the remote machine? What port numbers were used by the local host?
2. How many bytes of data were returned by the remote time server, both in the UDP case and in the TCP case?
3. What TCP header options were used?

7 NTP Sync

In this exercise, we start the NTP server daemon on `shakti` and use NTP to synchronize all the other hosts to `shakti`. Study the NTP configuration file `/etc/ntp.conf` in `shakti` and in your host. If you are using another machine, you can telnet to shakti and display the `/etc/ntp.conf` file in the telnet window. Start the NTP server on `shakti` by: **/etc/init.d/ntpd start**. To determine the status of the NTP server, use **/etc/init.d/ntpd status**. Use **wireshark** to capture packets between your host and `shakti`. Execute **ntpdate -d -v 128.238.66.100** to synchronize your host to `shakti`. Study the output of this command. Save the **ntpdate** and the **wireshark** outputs for the lab report.

Report

1. Which port does the NTP server use? Justify your answer using the **wireshark** output.

NAT

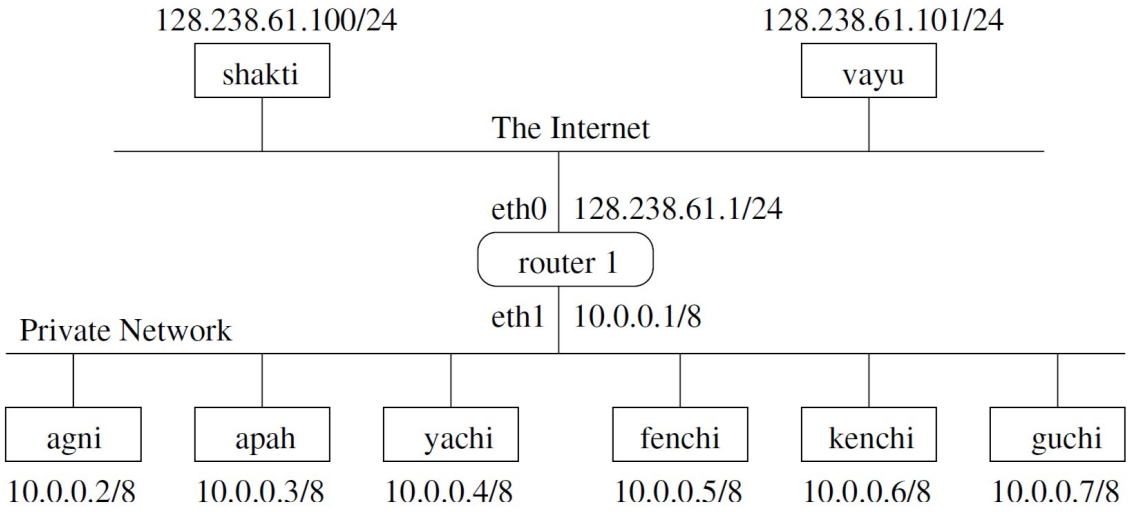


Figure 7.1: **Figure 8.7.** The network configuration for the NAT exercises.

8 NAT

Connect the hosts and Router 1 as shown in Fig. 8.7.[5] Then set the IP address and the network mask of your host as shown in the figure. In addition, you need to add a default route in your host's routing table, using the router interface on your subnet as the default router. One student should **telnet** to the router and configure the router as shown in Table 8.5. Note that there is a static translation that maps 10.0.0.7, or `guchi`, to 128.238.61.104. Login to the router, execute **write term** to display the current router configuration. Execute **show ip nat translations** in the *Privileged EXEC* mode to display the translation table. Save both outputs for the lab report.
We use linux instead a router and config it to use as **NAT** and **PAT**[6]

Report

1. How many entries were there in the translation table? Why?

NAT Visibility

Keep the login session to the router running. Execute **wireshark** on all the hosts.
Before any host in the private network send any packets out, ping an inside host (e.g., `fenchi`) from an outside host (e.g., **vayu**). You may try to ping 10.0.0.5, 128.238.61.102, 128.238.61.103, or 128.238.61.104. Can you ping these IP addresses?
Let an inside host send packets to an outside host, e.g., from `fenchi`, execute ping 128.238.61.100. Can you ping `fenchi` from an outside host now? Why? Which IP address should be used in the ping command in order to ping `fenchi`?
Execute show ip nat translations in the router login window to display the translation table. Save the output for the lab report.
Exchange the data you saved with a student in the other subnet.

Report

1. Answer the above questions. Use the saved translation table to justify your answers.
2. Compare the IP header of the ICMP query captured in the private network with that of the same ICMP query captured in the upper subnet, list their differences. Explain how NAT works.
3. In addition to the IP address, what else was changed in the ICMP query packet?

NAT Table

Keep the login session to the router running. Execute **wireshark** to capture ICMP messages.
Execute **socket -i -u -n1 128.238.61.101 8888** on `agni` to generate an ICMP port unreachable error.
Print the ICMP error message for the lab report.
Execute **show ip nat translations** in the router login window or **sudo iptables -t nat -L -n -v** in linux router command line to display the translation table. Save the output for the lab report. Exchange the data you saved with a student in the other subnet.

Report

1. Analyze the IP headers, the ICMP headers, and the ICMP payloads of the ICMP port unreachable errors captured in the private network and in the public network from the first experiment. Explain how ICMP error was handled by the NAT router.

[5] For the exercises in this section, we use a network setting as shown in Fig. 8.7. The lower subnet is a private network where the hosts are assigned with the Class A addresses with the 10.0.0.0/8 prefix. The upper subnet represents the Internet. The hosts, i.e., shakti and vayu are assigned with public IP addresses. Router 1 is used as the stub router, which performs address or port translation for the private network.
[6] linxu-iptables-NAT-PAT

NAT with PAT

Reboot the router to restore its default configuration. Then, configure the router to use PAT, as given in Table 8.6. Now all the hosts in the private network use the same IP address 128.238.61.1. However, note that there is a static translation that maps guchi's port 80 to 128.238.61.1 port 80.
Execute **wireshark** on all the hosts.
Generate traffic between the inside and outside hosts. Examine the **wireshark** output to see how PAT works. Start the Apache web server on `guchi`. Also, start the web browser `Mozilla` on an outside host (e.g., `shakti`), and enter the URL `http://128.238.61.1`. Save the **wireshark** output. Use **show ip nat translations** to display and then save the translation table. Exchange the data you saved with a student in the other subnet.

Report

1. From the **wireshark** data, explain how PAT worked, both for a dynamic translation and a static translation. With PAT, can you have two web servers in the private network? If not, why? If yes, explain how this can be done.

NAT Router Configuration in Fig. 8.7

```
ip nat pool mypool 128.238.61.102 128.238.61.103 netmask 255.255.255.0
ip nat inside source list 8 pool mypool

ip nat inside source static 10.0.0.7 128.238.61.104

interface ethernet 0
ip address 128.238.61.1 255.255.255.0
ip nat outside

interface ethernet 1
ip address 10.0.0.1 255.0.0.0
ip nat inside

access-list 8 deny host 10.0.0.7
access-list 8 permit 10.0.0.0 0.0.0.255
```

PAT Router Configuration in Fig. 8.7

```
ip nat inside source list 8 interface ethernet 0 overload

ip nat inside source static tcp 10.0.0.7 80 128.238.61.1 80

interface ethernet 0
ip address 128.238.61.1 255.255.255.0
ip nat outside

interface ethernet 1
ip address 10.0.0.1 255.0.0.0
ip nat inside

access-list 8 deny host 10.0.0.7
access-list 8 permit 10.0.0.0 0.0.0.255
```

Appendices

A DHCP Header

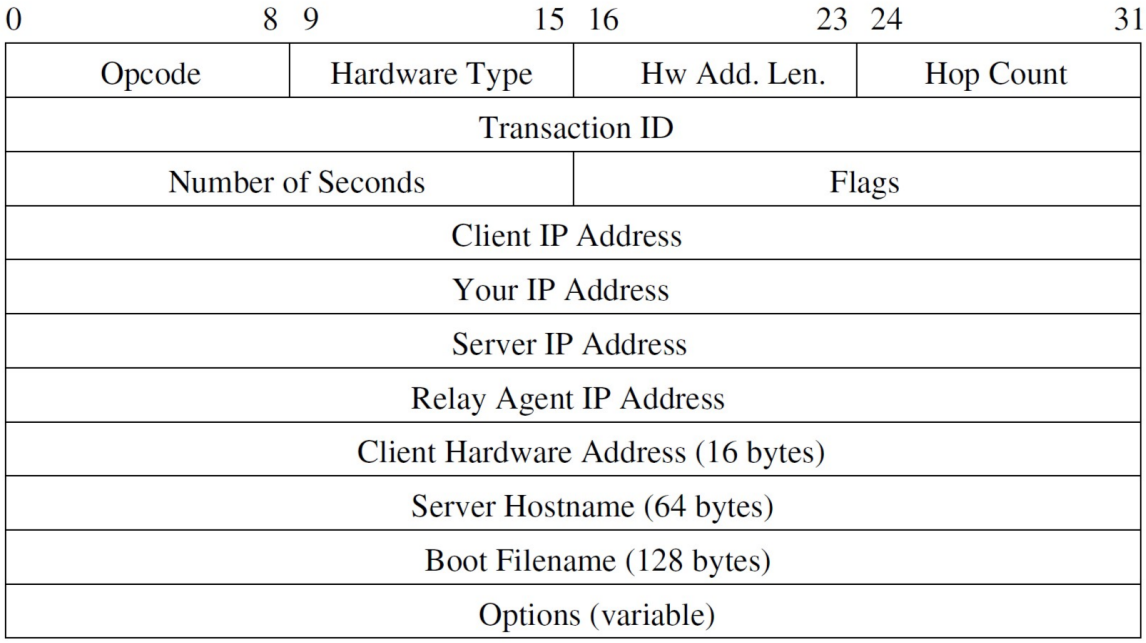


Figure .1: The DHCP message format

Reference: TCP/IP Essential

B Linux Nat

Assuming your public interface is eth1 and local interface is eth0

1. Enable forwarding on the box with
   `echo 1 > /proc/sys/net/ipv4/ip_forward`
2. Set natting the natting rule with
   `iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE`
3. Accept traffic from eth0:
   `iptables -A INPUT -i eth0 -j ACCEPT`
4. Allow established connections from the public interface.
   `iptables -A INPUT -i eth1 -m state -state ESTABLISHED,RELATED -j ACCEPT`
5. Allow outgoing connections:
   `iptables -A OUTPUT -j ACCEPT`

You can use following example for see linux NAT in MiniNet:
http://csie.nqu.edu.tw/smallko/sdn/mininet-operations.htm