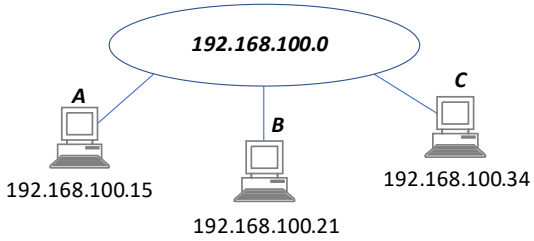
Thiết kế & triển khai mạng IP

Bài thực hành số 3: Mạng nội bộ - Private Network (version 3.0 – chuyển sang Ubuntu)

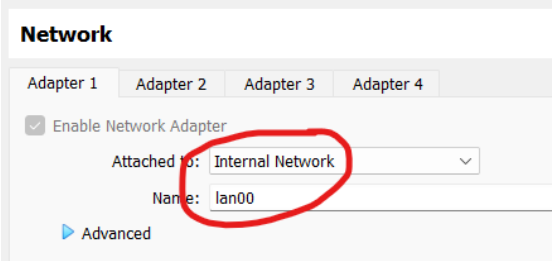
Contents

1 Thiết lập mạng nội bộ đơn giản

Bài thực hành này thực hiện thiết lập một mạng gồm nhiều máy trạm kết nối trực tiếp với nhau trong một mạng LAN và tìm hiểu cơ chế truyền dữ liệu giữa các trạm trong một mạng nội bộ.



1. Cấu hình kết nối mạng của các máy trạm A, B, C để kết nối vào cùng một mạng LAN *(lan00)*



2. Khởi động 3 máy ảo A, B, C, và thiết lập địa chỉ IP cho các card mạng với lệnh *ifconfig* và kiểm tra máy chưa được thiết lập Gateway với lệnh *route -n*:

```
hp@pcA:~$ sudo ifconfig enp0s3 192.168.100.15/24
hp@pcA:~$ ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.15  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::a00:27ff:fee3:a01  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e3:0a:01  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 936 (936.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

hp@pcA:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.100.0   0.0.0.0         255.255.255.0   U     0      0        0 enp0s3
```

3. Tại máy A, gửi gói tin broadcast bằng lệnh *ping -b* đến địa chỉ broadcast. Bắt gói tin trên các máy khác (B, C) sẽ thấy dữ liệu được gửi broadcast đến địa chỉ MAC *ff:ff:ff:ff:ff:ff*:

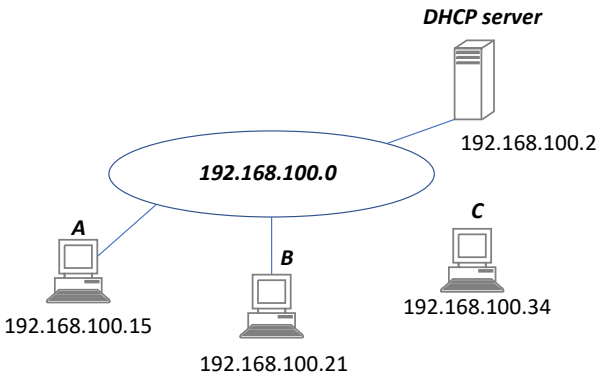
```
hp@pcA:~$ ping -b 192.168.100.255
WARNING: pinging broadcast address
PING 192.168.100.255 (192.168.100.255) 56(84) bytes of data.

hp@pcB:~$ sudo tcpdump -i enp0s3 -ne
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
09:55:25.582014 08:00:27:e3:0a:01 > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 98:
192.168.100.15 > 192.168.100.255: ICMP echo request, id 17, seq 83, length 64
09:55:26.605186 08:00:27:e3:0a:01 > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 98:
192.168.100.15 > 192.168.100.255: ICMP echo request, id 17, seq 84, length 64
09:55:27.629597 08:00:27:e3:0a:01 > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 98:
192.168.100.15 > 192.168.100.255: ICMP echo request, id 17, seq 85, length 64
09:55:28.653630 08:00:27:e3:0a:01 > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 98:
192.168.100.15 > 192.168.100.255: ICMP echo request, id 17, seq 86, length 64
09:55:29.677602 08:00:27:e3:0a:01 > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 98:
192.168.100.15 > 192.168.100.255: ICMP echo request, id 17, seq 87, length 64
```

Để lệnh *ping* nhận được gói tin phản hồi (Echo Reply), cần hủy chế độ bỏ qua gói tin ICMP Echo Request (mặc định là chế độ này được bật). Khi đó lệnh *ping* trên máy A sẽ nhận được ICMP Echo Reply từ máy B và C

```
hp@pcB:~$ sudo sysctl net.ipv4.icmp_echo_ignore_broadcasts
net.ipv4.icmp_echo_ignore_broadcasts = 1

hp@pcB:~$ sudo sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=0
net.ipv4.icmp_echo_ignore_broadcasts = 0

hp@pcA:~$ ping -b 192.168.100.255
WARNING: pinging broadcast address
PING 192.168.100.255 (192.168.100.255) 56(84) bytes of data.
64 bytes from 192.168.100.21: icmp_seq=1 ttl=64 time=1.50 ms
64 bytes from 192.168.100.34: icmp_seq=1 ttl=64 time=1.50 ms (DUP!)
64 bytes from 192.168.100.21: icmp_seq=2 ttl=64 time=1.65 ms
64 bytes from 192.168.100.34: icmp_seq=2 ttl=64 time=2.45 ms (DUP!)
64 bytes from 192.168.100.21: icmp_seq=3 ttl=64 time=1.57 ms
64 bytes from 192.168.100.34: icmp_seq=3 ttl=64 time=1.57 ms (DUP!)
```

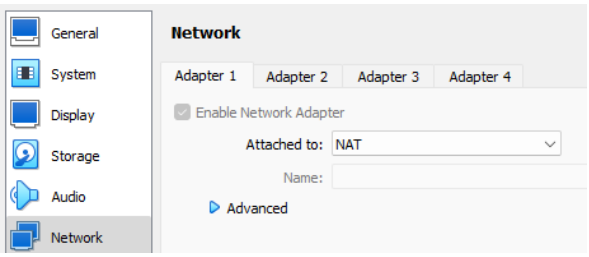
2 Làm việc với DHCP

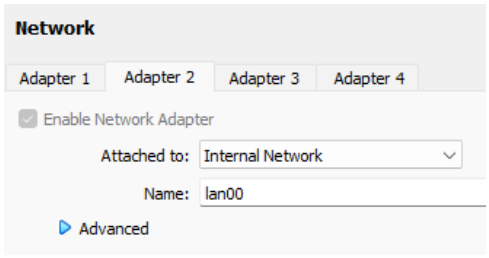
Bài này yêu cầu thiết lập cơ chế gán địa chỉ tự động cho các trạm bằng giao thức DHCP.



2.1 Cài đặt & cấu hình DHCP server

1. Tạo máy ảo đóng vai trò là DSCP server. Gồm có 1 kết nối vào *lan00* (địa chỉ 192.168.100.2/24) và một kết nối NAT để có thể truy nhập Internet qua máy Host. Kết nối này dùng để cài đặt phần mềm DHCP server.





2. DHCP server phổ biến trên Ubuntu Linux là gói isc-dhcp-server. Thiết lập kết nối NAT cho máy ảo, kiểm tra có thể truy nhập Internet bằng DNS. Sau đó dùng lệnh apt-get để tải về và cài đặt:

```
:~$ ping google.com
PING google.com (142.250.204.142) 56(84) bytes of data.
64 bytes from hkg07s41-in-f14.1e100.net (142.250.204.142): icmp_seq=1 ttl=57 time=24.3 ms
64 bytes from hkg07s41-in-f14.1e100.net (142.250.204.142): icmp_seq=2 ttl=57 time=24.0 ms
64 bytes from hkg07s41-in-f14.1e100.net (142.250.204.142): icmp_seq=3 ttl=57 time=25.0 ms
```

```
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 24.010/24.440/25.034/0.433 ms

:~$ sudo apt-get install isc-dhcp-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libirs-export161 libisccfg-export163
Suggested packages:
  isc-dhcp-server-ldap policycoreutils
The following NEW packages will be installed:
  isc-dhcp-server libirs-export161 libisccfg-export163
0 upgraded, 3 newly installed, 0 to remove and 28 not upgraded.
Need to get 529 kB of archives.
After this operation, 1,546 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
. . . . .
```

3. Cấu hình IP tĩnh cho máy DCHP server bằng netplan (kết nối mạng *lan00*) và thử *ping* vào máy trạm A trong cùng mạng:

```
:~$ sudo nano /etc/netplan/00-installer-config.yaml
network:
  ethernets:
#    enp0s3:
#      dhcp4: true
#      addresses: [10.1.0.1/24]
    enp0s8:
      dhcp4: false
      addresses: [192.168.100.2/24]
:~$ sudo netplan apply
:~$ ping 192.168.100.15
PING 192.168.100.15 (192.168.100.15) 56(84) bytes of data.
64 bytes from 192.168.100.15: icmp_seq=1 ttl=64 time=0.819 ms
64 bytes from 192.168.100.15: icmp_seq=2 ttl=64 time=1.30 ms
64 bytes from 192.168.100.15: icmp_seq=3 ttl=64 time=1.14 ms
```

4. Ngắt hết các kết nối mạng khác của DHCP server và restart lại máy. Đảm bảo máy chỉ còn 1 kết nối mạng *lan00* được cấu hình IP tĩnh 192.168.100.2

```
:~$ sudo reboot now
:~$ ifconfig -a
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.2  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::a00:27ff:feb6:102  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b6:01:02  txqueuelen 1000  (Ethernet)
        RX packets 5  bytes 414 (414.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26  bytes 2040 (2.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
network:
```

5. Cấu hình dịch vụ DHCP bằng file config */etc/dhcp/dhcpd.conf* với nội dung đơn giản nhất. Khởi động lại dịch vụ DHCP và xem trạng thái:

```
:~$ sudo nano /etc/dhcp/dhcpd.conf
subnet 192.168.100.0 netmask 255.255.255.0 {
  range 192.168.100.101 192.168.100.150;
}

:~$ sudo systemctl restart isc-dhcp-server
:~$ sudo systemctl status isc-dhcp-server
● isc-dhcp-server.service - ISC DHCP IPv4 server
     Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-12-13 16:23:19 +07; 6s ago
       Docs: man:dhcpd(8)
   Main PID: 1213 (dhcpd)
      Tasks: 4 (limit: 1013)
     Memory: 4.5M
        CPU: 8ms
     CGroup: /system.slice/isc-dhcp-server.service
             └─1213 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf
```

2.2 Sử dụng DHCP client trên các máy trạm

1. Trên một máy trạm đã được kết nối vào lan00, thiết lập cấu hình netplan để được cấp địa chỉ IP tự động. Thấy địa chỉ IP đã được cấp phát theo dải cấu hình trên DHCP server:

```
pcX:~$ sudo nano /etc/netplan/00-installer-config.yaml
network:
  ethernets:
    enp0s8:
      dhcp4: true
  version: 2

pcX:~$ sudo netplan apply
ifconfig -a
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.101  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::a00:27ff:fe9d:202  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:9d:02:02  txqueuelen 1000  (Ethernet)
        RX packets 11  bytes 1620 (1.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 43  bytes 4228 (4.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Có thể debug quá trình cấp phát địa chỉ IP với tool *dhclient -d*:

```
pcX:~$ sudo dhclient enp0s8 -d
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/enp0s8/08:00:27:9d:02:02
Sending on   LPF/enp0s8/08:00:27:9d:02:02
Sending on   Socket/fallback
DHCPREQUEST for 192.168.100.102 on enp0s8 to 255.255.255.255 port 67 (xid=0x10f0076b)
DHCPACK of 192.168.100.102 from 192.168.100.2 (xid=0x6b07f010)
RTNETLINK answers: File exists
bound to 192.168.100.102 -- renewal in 18067 seconds.
```

3. Hủy địa chỉ IP đang được cấp:

```
pcX:~$ sudo dhclient enp0s8 -r
pcX:~$ ifconfig enp0s8
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::a00:27ff:fe9d:202  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:9d:02:02  txqueuelen 1000  (Ethernet)
        RX packets 44  bytes 8966 (8.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 94  bytes 15070 (15.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

4. Cấp mới địa chỉ IP:

```
pcX:~$ sudo dhclient enp0s8 -v
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/enp0s8/08:00:27:9d:02:02
Sending on   LPF/enp0s8/08:00:27:9d:02:02
Sending on   Socket/fallback
DHCPDISCOVER on enp0s8 to 255.255.255.255 port 67 interval 3 (xid=0x2c1df377)
DHCPOFFER of 192.168.100.102 from 192.168.100.2
DHCPREQUEST for 192.168.100.102 on enp0s8 to 255.255.255.255 port 67 (xid=0x77f31d2c)
DHCPACK of 192.168.100.102 from 192.168.100.2 (xid=0x2c1df377)
bound to 192.168.100.102 -- renewal in 20919 seconds.

pcX:~$ ifconfig enp0s8
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.102  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::a00:27ff:fe9d:202  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:9d:02:02  txqueuelen 1000  (Ethernet)
        RX packets 47  bytes 9712 (9.7 KB)
```

```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 97  bytes 15824 (15.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2.3 Bổ sung cấu hình DHCP để cấp địa chỉ gateway, DNS, v.v..

Ngoài việc cấp phát địa chỉ IP cho các máy trạm, dịch vụ DHCP còn có thể cấu hình tự động các thông số mạng như gateway, DSN server, v.v.. hoặc xử lý cấp phát địa chỉ IP theo kịch bản riêng từng máy trạm.

1. Cấu hình tự động default gateway. Thêm option vào file cấu hình và restart lại service:

```
:~$ sudo nano /etc/dhcp/dhcpd.conf
subnet 192.168.100.0 netmask 255.255.255.0 {
  range 192.168.100.101 192.168.100.150;
  option routers 192.168.100.1;
}

:~$ sudo systemctl restart isc-dhcp-server
```

2. Trên máy trạm, xin cấp lại địa chỉ IP. Sau đó kiểm tra bảng routing để thấy cấu hình default gateway được thiết lập là 192.168.100.1:

```
pcX:~$ sudo dhclient enp0s8 -r
Killed old client process
pcX:~$ sudo dhclient enp0s8 -v
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/enp0s8/08:00:27:9d:02:02
Sending on   LPF/enp0s8/08:00:27:9d:02:02
Sending on   Socket/fallback
DHCPDISCOVER on enp0s8 to 255.255.255.255 port 67 interval 3 (xid=0xa153bc5e)
DHCPOFFER of 192.168.100.102 from 192.168.100.2
DHCPREQUEST for 192.168.100.102 on enp0s8 to 255.255.255.255 port 67 (xid=0x5ebc53a1)
DHCPACK of 192.168.100.102 from 192.168.100.2 (xid=0xa153bc5e)
bound to 192.168.100.102 -- renewal in 21223 seconds.

pcX:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.100.1   0.0.0.0         UG    0      0        0 enp0s8
192.168.100.0   0.0.0.0         255.255.255.0   U     0      0        0 enp0s8
```

3. Cấu hình tự động DNS server:

```
:~$ sudo nano /etc/dhcp/dhcpd.conf
subnet 192.168.100.0 netmask 255.255.255.0 {
  range 192.168.100.101 192.168.100.150;
  option routers 192.168.100.1;
  option domain-name-servers 8.8.8.8;
}

:~$ sudo systemctl restart isc-dhcp-server
```

4. Cấu hình DHCP server chỉ hoạt động trện một kết nối mạng cụ thể. Thiết lập trong file cấu hình /etc/default/isc-dhcp-server:

```
:~$ sudo nano /etc/default/isc-dhcp-server
sudo nano /etc/default/isc-dhcp-server

:~$ sudo systemctl restart isc-dhcp-server
```

2.4 Kịch bản tương tranh nhiều DHCP server

Cũng trong mạng LAN hiện tại, thiết lập thêm một DHCP server tại địa chỉ IP 192.168.100.3 với các thông số sau:

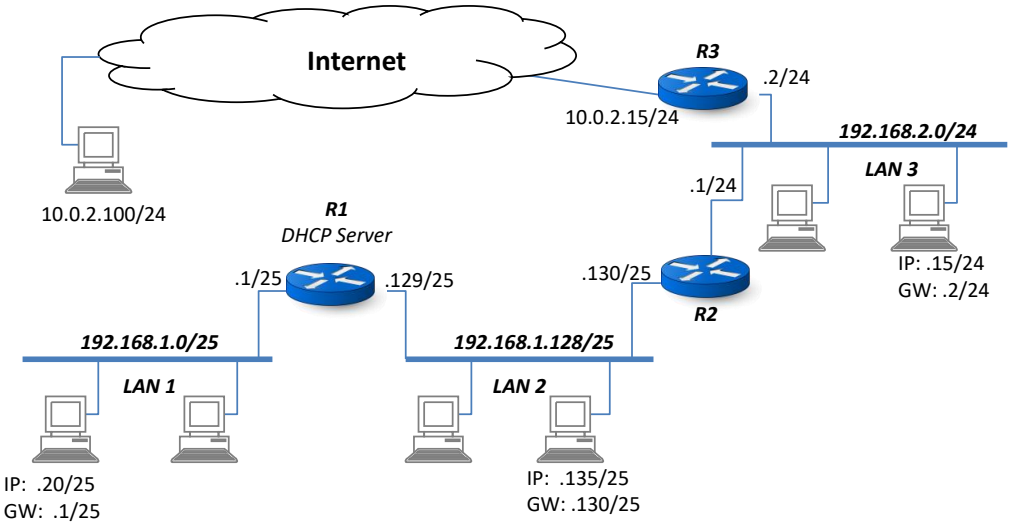
Có thể thấy DHCP server này cũng cung cấp dải địa chỉ IP trong mạng 192.168.100.0/24 nhưng gán các thông số Default Gateway và DNS Server khác với DHCP server trước. Khởi động cả hai DHCP server này và kết nối một DHCP Client vào mạng:

```
[root@C1 ~]# dhclient -r eth2
[root@C1 ~]# dhclient -v eth2
Internet Systems Consortium DHCP Client 4.1.1-P1
Copyright 2004-2010 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth2/08:00:27:d6:c1:02
Sending on   LPF/eth2/08:00:27:d6:c1:02
Sending on   Socket/fallback
DHCPDISCOVER on eth2 to 255.255.255.255 port 67 interval 7 (xid=0x3072be37)
DHCPOFFER from 192.168.2.5
DHCPREQUEST on eth2 to 255.255.255.255 port 67 (xid=0x3072be37)
DHCPACK from 192.168.2.5 (xid=0x3072be37)
bound to 192.168.2.40 -- renewal in 39348 seconds.

[root@C1 ~]# ifconfig eth2
eth2      Link encap:Ethernet  HWaddr 08:00:27:D6:C1:02
          inet addr:192.168.2.40  Bcast:192.168.2.127  Mask:255.255.255.128
          inet6 addr: fec1::7/64 Scope:Site
          inet6 addr: fe80::a00:27ff:fed6:c102/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:68 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6198 (6.0 KiB)  TX bytes:3148 (3.0 KiB)

[root@C1 ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.2.13    0.0.0.0         UG    0      0        0 eth2
```

Nhìn vào thông tin hiển thị log khi máy trạm nhận địa chỉ IP có thể thấy, một cách ngẫu nhiên, máy trạm nhận lời mời của DHCP server mới (thay vì sử dụng DHCP server cũ) và được gán địa chỉ IP cùng với các thông số cấu hình theo server này. Đây là điểm yếu của giao thức DHCP cho phép hacker đột nhập vào một trạm trong mạng và tự tạo ra DHCP server với cấu hình Gateway, DNS giả mạo để ăn cắp các thông tin người dùng trên mạng.

3 Qui hoạch Gateway cho mạng riêng

Bài này yêu cầu qui hoạch Gateway cho 3 mạng LAN như hình vẽ bên trên. Ngoài ra, đối với LAN1, sử dụng DHCP để cấp địa chỉ IP động cho các trạm trong mạng



3.1 Cấu hình mạng LAN1

Bước 1: Cấu hình router R1

Cấu hình địa chỉ IP cho các kết nối mạng của R1:

```
> ifconfig eth1 192.168.1.1/25
> ifconfig eth2 192.168.1.129/25
> ifconfig -a
eth1      Link encap:Ethernet  HWaddr 08:00:27:96:4A:E6
          inet addr:192.168.1.1  Bcast:192.168.1.127  Mask:255.255.255.128
          inet6 addr: fe80::a00:27ff:fe96:4ae6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:181 errors:0 dropped:0 overruns:0 frame:0
          TX packets:30 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20910 (20.4 KiB)  TX bytes:1928 (1.8 KiB)

eth2      Link encap:Ethernet  HWaddr 08:00:27:D7:D8:3E
          inet addr:192.168.1.129  Bcast:192.168.1.255  Mask:255.255.255.128
          inet6 addr: fe80::a00:27ff:fed7:d83e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:199 errors:0 dropped:0 overruns:0 frame:0
          TX packets:30 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:24412 (23.8 KiB)  TX bytes:1928 (1.8 KiB)
```

Chú ý kiểm tra và bật chức năng “forward” của router R1 bằng tham số hệ thống *net.ipv4.ip_forward*:

```
> sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 0
> sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
```

Cấu hình DHCP server cho router R1 để cung cấp địa chỉ IP cho các trạm trong mạng LAN1, ngoài ra thiết lập cấu hình Default Gateway cũng là R1 luôn (địa chỉ 192.168.1.1/25) và khởi động lại dịch vụ DHCP trên R1:

```
> nano /etc/dhcp/dhcpd.conf

subnet 192.168.1.0 netmask 255.255.255.128 {
  range 192.168.1.20 192.168.1.30;

  default-lease-time 86400;
  max-lease-time 86400;

  option routers 192.168.1.1;
  option domain-name-servers 4.4.4.4,8.8.8.8;
}

> service dhcpd restart
```

```
Starting dhcpd:                                            [  OK  ]
```

Cấu hình bảng routing cho router R1. Do tất cả các định tuyến gián tiếp từ R1 đến các mạng khác (gồm LAN3 và Internet) đều đi qua R2 tại địa chỉ 192.168.1.130 nên cấu hình routing của R1 như sau:

```
> route add -net 0.0.0.0/0 gw 192.168.1.130
> route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags   Metric  Ref    Use     Iface
0.0.0.0         192.168.1.130   0.0.0.0         UGH     0       0        0      eth2
192.168.1.0     0.0.0.0         255.255.255.128 U       0       0        0      eth1
192.168.1.128   0.0.0.0         255.255.255.128 U       0       0        0      eth2
```

Bước 2: Cấu hình máy trạm cho LAN1

Các máy trạm của LAN1 có thể được cấu hình theo 2 cách tĩnh hoặc động. Với cấu hình tĩnh, sử dụng lệnh *ifconfig* hoặc cấu hình mặc định trong file cấu hình của card mạng */etc/sysconfig/network-scripts/ifcfg-eth1*. Lưu ý rằng dải địa chỉ IP từ 192.168.1.20 đến 192.168.1.30 đã được đặt trước để DHCP server sử dụng và cung cấp cho các client. Vì vậy, khi cấu hình tĩnh cần tránh các địa chỉ này:

```
> ifconfig eth1 192.168.1.15/25
>  nano /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE="eth1"
IPADDR=192.168.1.15
NETMASK=255.255.255.128

> nano /etc/sysconfig/network
NETWORKING=yes
GATEWAY=192.168.1.1
```

Với phương pháp cấu hình động, thiết lập file cấu hình */etc/sysconfig/network-scripts/ifcfg-eth1* để card mạng tự động nhận địa chỉ IP khi khởi động hoặc sử dụng lệnh *dhclient* để yêu cầu cấp địa chỉ IP (xem bài thực hành số 2):

```
> nano /etc/sysconfig/network-scripts/ifcfg-eth6
DEVICE=eth1
BOOTPROTO=dhcp
ONBOOT=yes
```

Cuối cùng, kiểm tra cấu hình mạng trên các máy trạm bằng lệnh *route -n*. Địa chỉ mạng 0.0.0.0 đại diện cho các mạng bên ngoài và tương ứng với nó, default gateway được sử cấu hình là 192.168.1.1:

```
> route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags   Metric  Ref    Use     Iface
192.168.1.0     0.0.0.0         255.255.255.128   U       0       0        0      eth1
0.0.0.0         192.168.1.1     0.0.0.0         UG      0       0        0      eth1
```

3.2 Cấu hình các router trong hệ thống

Cấu hình cho router R2 như sau:

```
> ifconfig eth1 192.168.1.130/25
> ifconfig eth2 192.168.2.1/24
ifconfig -a
eth1      Link encap:Ethernet  HWaddr 08:00:27:56:81:0C
          inet addr:192.168.1.130  Bcast:192.168.1.255  Mask:255.255.255.128
          inet6 addr: fe80::a00:27ff:fe56:810c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1275 errors:0 dropped:0 overruns:0 frame:0
          TX packets:607 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:126622 (123.6 KiB)  TX bytes:91395 (89.2 KiB)

eth2     Link encap:Ethernet  HWaddr 08:00:27:C4:D5:BA
          inet addr:192.168.2.1  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec4:d5ba/64 Scope:Link
```

```
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:221 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:25373 (24.7 KiB)  TX bytes:468 (468.0 b)

> route add -net 192.168.1.0/25 gw 192.168.1.129
> route add -net 0.0.0.0/0 gw 192.168.2.2
> route -n
Kernel IP routing table
Destination       Gateway           Genmask           Flags    Metric   Ref    Use        Iface
192.168.1.0       192.168.1.129     255.255.255.128   UG       0        0        0        eth1
192.168.1.128     0.0.0.0           255.255.255.128   U        0        0        0        eth1
192.168.2.0       0.0.0.0           255.255.255.0     U        0        0        0        eth2
0.0.0.0           192.168.2.2       0.0.0.0           UG       0        0        0        eth2
```

Router R3 có một kết nối mạng ra Internet và một kết nối mạng nội bộ LAN3. Cấu hình máy ảo VirtualBox sử dụng card mạng NAT để kết nối Internet và card mạng Internal Network để kết nối mạng LAN3. Khi khởi động máy ảo, card NAT sẽ được tự động gán địa chỉ IP theo cấu hình NAT của Oracle VirtualBox, thông thường là 10.0.2.15 và Gateway ra Internet (chính là máy host Windows) có địa chỉ 10.0.2.2. Trường hợp card mạng này chưa được cấp địa chỉ IP thì có thể sử dụng lệnh *dhclient -v* để yêu cầu Virtual Box cấu hình địa chỉ IP cho nó. Với card mạng còn lại, cấu hình địa chỉ IP:

```
> ifconfig eth1 192.168.2.2/24
> ifconfig -a
eth1      Link encap:Ethernet  HWaddr 08:00:27:98:CA:2E
          inet addr:192.168.2.2  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe98:ca2e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:158 errors:0 dropped:0 overruns:0 frame:0
          TX packets:45 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20307 (19.8 KiB)  TX bytes:6399 (6.2 KiB)

eth2      Link encap:Ethernet  HWaddr 08:00:27:81:E6:AD
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe81:e6ad/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1580 (1.5 KiB)  TX bytes:1684 (1.6 KiB)

> ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=43 time=66.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=43 time=65.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=43 time=66.1 ms
```

Có thể thấy rằng router R3 đã được cấu hình tự động trên card mạng *eth2* với địa chỉ 10.0.2.15 (đây là địa chỉ mặt ngoài của router R3). Sử dụng lệnh ping đến máy chủ DNS của Google (địa chỉ 8.8.8.8) để kiểm tra kết nối Internet. Cuối cùng, cần cấu hình bảng routing cho router R3. Cần bổ sung thêm 2 đường định tuyến đến LAN1 và LAN2. Ngoài ra, do được cấu hình NAT tự động, đường định tuyến mặc định ra Internet (0.0.0.0) đã được thêm vào từ trước với gateway là 10.0.2.2 (chính là máy host của Virtual Box):

```
> route add -net 192.168.1.0/25 gw 192.168.2.1
> route add -net 192.168.1.128/25 gw 192.168.2.1
> route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     192.168.2.1     255.255.255.128 UG    0      0        0 eth3
192.168.1.128   192.168.2.1     255.255.255.128 UG    0      0        0 eth3
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 eth3
10.0.2.0        0.0.0.0         255.255.255.0   U     0      0        0 eth4
0.0.0.0         10.0.2.2        0.0.0.0         UG    0      0        0 eth4
```

Bước 4: Cấu hình máy trạm cho LAN3

Khác với LAN1, do không có DHCP server, các máy trạm của LAN3 chỉ có thể được cấu hình tĩnh. Có thể thiết lập thông số cấu hình mặc định cho trạm như trong bước 2, hoặc thiết lập tức thời như sau:

```
> ifconfig eth0 192.168.2.15/24
> route add -net 0.0.0.0 gw 192.168.2.2
> route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
0.0.0.0         192.168.2.2     0.0.0.0         UG    0      0        0 eth0
```

3.3 Kịch bản kiểm tra hệ thống

Dùng lệnh *ping* để kiểm tra kết nối từ máy trạm trong LAN1 đến máy trạm trong LAN3. Lưu ý rằng vì lý do an ninh, *iptables* mặc định chặn tất cả các gói tin được chuyển tiếp qua và thông báo cho trạm gửi bằng một gói tin ICMP "*Destination Host Prohibited*". Điều này thể hiện khi ping từ một trạm đến một trạm khác và nhận được thông báo lỗi:

```
> ping 192.168.2.15
PING 192.168.2.15 (192.168.2.15) 56(84) bytes of data.
From 192.168.1.1 icmp_seq=1 Destination Host Prohibited
From 192.168.1.1 icmp_seq=2 Destination Host Prohibited
From 192.168.1.1 icmp_seq=3 Destination Host Prohibited
```

Để xử lý vấn đề này, cần tắt chức năng chặn gói tin tại các router. Trên các router R1,R2,R3, hiển thị các luật *iptables*:

```
> iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Có thể thấy ở chain FORWARD đang có một luật reject tất cả các gói tin và trả về bằng một gói tin ICMP. Cần bỏ luật này đi:

```
> iptables -D FORWARD -j REJECT --reject-with icmp-host-prohibited
> iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Sau khi bỏ luật này trên tất cả các router, trạm tại LAN1 sẽ *ping* thành công đến trạm LAN3. Cũng có thể hiển thị đường đi của gói tin giữa 2 trạm này bằng lệnh *traceroute*:

```
> ping 192.168.2.15
PING 192.168.2.15 (192.168.2.15) 56(84) bytes of data.
64 bytes from 192.168.2.15: icmp_seq=1 ttl=61 time=7.19 ms
64 bytes from 192.168.2.15: icmp_seq=2 ttl=61 time=2.02 ms
64 bytes from 192.168.2.15: icmp_seq=3 ttl=61 time=2.10 ms

> traceroute -n 192.168.2.15
traceroute to 192.168.2.15 (192.168.2.15), 30 hops max, 60 byte packets
```

```
 1  192.168.1.1  0.693 ms  0.522 ms  0.485 ms
 2  192.168.1.130  5.982 ms  5.936 ms  5.236 ms
 3  192.168.2.15  6.734 ms  6.572 ms  6.362 ms
```

3.4 Xử lý tình huống Redirect Host

Một điều rất thú vị là khi đứng ở trạm trong mạng LAN3 và *ping* đến trạm mạng LAN1 thì thành công nhưng nhận được thêm thông tin *Redirect Host*:

```
> ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
From 192.168.2.2: icmp_seq=1 Redirect Host(New nexthop: 192.168.2.1)
64 bytes from 192.168.1.20: icmp_seq=1 ttl=62 time=4.24 ms
From 192.168.2.2: icmp_seq=2 Redirect Host(New nexthop: 192.168.2.1)
64 bytes from 192.168.1.20: icmp_seq=2 ttl=62 time=5.05 ms
From 192.168.2.2: icmp_seq=3 Redirect Host(New nexthop: 192.168.2.1)
64 bytes from 192.168.1.20: icmp_seq=3 ttl=62 time=1.90 ms
```

Thông điệp được gửi về máy trạm từ địa chỉ 192.168.2.1 (là router R2). Lý do như sau. Khi gói tin gửi đi từ trạm trong LAN3, nó được chuyển đến Gateway của LAN3 là router R3. R3 kiểm tra bảng routing và chuyển tiếp gói tin đến R2. Tại đây, R2 kiểm tra gói tin có địa chỉ nguồn là 192.168.2.15, nằm cùng một mạng với một kết nối của mình (có địa chỉ 192.168.2.1). Như vậy, đã có tình huống định tuyến vòng, tức là gói tin đáng nhẽ có thể đi trực tiếp đến R2 từ trạm nguồn, nhưng thực tế nó đã phải đi qua một router khác (là R3). Điểm không hợp lý này đã được trình bày trong phần **Error! Reference source not found.** khi l ựa chọn R2 hay R3 là Gateway của LAN3. Giải pháp là các trạm trong LAN3 cần được cung cấp thêm một Gateway nữa (là R2). Khi gửi gói tin ra bên ngoài, trạm này nếu nhận được thông điệp *Redirect Host* từ R2 sẽ tự điều chỉnh để sử dụng sang Gateway này:

```
> route add default gw 192.168.2.1
> route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
0.0.0.0         192.168.2.1     0.0.0.0         UG    0      0        0 eth0
0.0.0.0         192.168.2.2     0.0.0.0         UG    0      0        0 eth0

> ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=62 time=2.45 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=62 time=1.88 ms
64 bytes from 192.168.1.20: icmp_seq=3 ttl=62 time=1.70 ms
64 bytes from 192.168.1.20: icmp_seq=4 ttl=62 time=2.04 ms
```

4 Bài 4: Kết nối Internet với NAT Gateway

Tiếp tục sử dụng môi trường mạng đã thiết lập trong bài trước, cần cấu hình NAT trên router R3 để tất cả các trạm nội bộ của mạng Intranet có thể kết nối ra ngoài Internet.

4.1 Kiểm tra kết nối Internet từ gateway R3

Trước tiên, cần kiểm tra đảm bảo kết nối mạng Internet của máy host VirtualBox. Tiếp theo, kiểm tra cấu hình R3 đã được cấu hình NAT chính xác với mạng của máy host VirtualBox hay chưa. Thông thường, khi thiết lập một giao diện kết nối mạng của R3 để đi ra Internet bằng kiểu NAT, địa chỉ kết nối này của R3 có dạng 10.0.2.15. Ngoài ra, Default Gateway của R3 được thiết lập là 10.0.2.2 (chính là địa chỉ của máy host VirtualBox).

```
[root@R3 ~]# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 08:00:27:36:E2:01
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:101941 errors:0 dropped:0 overruns:0 frame:0
          TX packets:46548 errors:0 dropped:0 overruns:0 carrier:0
```

```
          collisions:0 txqueuelen:1000
          RX bytes:113153758 (107.9 MiB)  TX bytes:2820938 (2.6 MiB)

[root@R3 ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.2.0     0.0.0.0         255.255.255.128 U     0      0        0 eth3
192.168.2.128   0.0.0.0         255.255.255.128 U     0      0        0 eth4
192.168.3.0     192.168.2.130   255.255.255.0   UG    0      0        0 eth4
192.168.3.0     192.168.2.2     255.255.255.0   UG    0      0        0 eth3
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 eth4
10.0.2.0        0.0.0.0         255.255.255.0   U     1      0        0 eth1
192.168.1.0     192.168.2.1     255.255.255.0   UG    0      0        0 eth3
0.0.0.0         10.0.2.2        0.0.0.0         UG    0      0        0 eth1

[root@R2 ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=44 time=95.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=44 time=90.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=44 time=100 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2499ms
rtt min/avg/max/mdev = 90.123/95.479/100.663/4.319 ms
```

4.2 Thiết lập NAT trên gateway với iptables

Mặc dù R3 có thể kết nối đến địa chỉ 8.8.8.8 trên Internet, tuy nhiên, nếu đứng tại một trạm trong LAN3 và *ping* đến địa chỉ này sẽ thấy không thành công (lỗi time out). Lý do là gói tin ICMP có địa chỉ nguồn là 192.168.2.15 và địa chỉ đích là 8.8.8.8 được chương trình *ping* gửi đi qua Gateway R3 có thể đi đến máy 8.8.8.8 (vì R3 đã được kiểm tra có thể *ping* đến 8.8.8.8). Tuy nhiên, máy 8.8.8.8 khi gửi gói tin ICMP trả lời theo địa chỉ 192.168.2.15 sẽ không bao giờ đến được máy trong LAN3 do địa chỉ này không được định tuyến trên các router của mạng Internet. Giải pháp là thiết lập chức năng NAT cho router R3 để khi chuyển tiếp các gói tin từ mạng nội bộ (LAN3 hoặc LAN1, LAN2) ra ngoài Internet, nó sẽ thay thế địa chỉ nguồn bằng địa chỉ mặt ngoài của R3 (là 10.0.2.15). Điều này được thực hiện rất đơn giản bằng cách bổ sung luật MASQUERADE vào table *nat*:

```
[root@mydomain ~]# iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
[root@mydomain ~]# iptables -t nat -L -v
Chain PREROUTING (policy ACCEPT 46 packets, 5273 bytes)
 pkts    bytes    target     prot   opt      in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts    bytes    target                    prot     opt      in     out     source               destination
    1             84       MASQUERADE        all      --       any  eth2   anywhere       anywhere

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts    bytes    target     prot   opt      in     out     source               destination
```

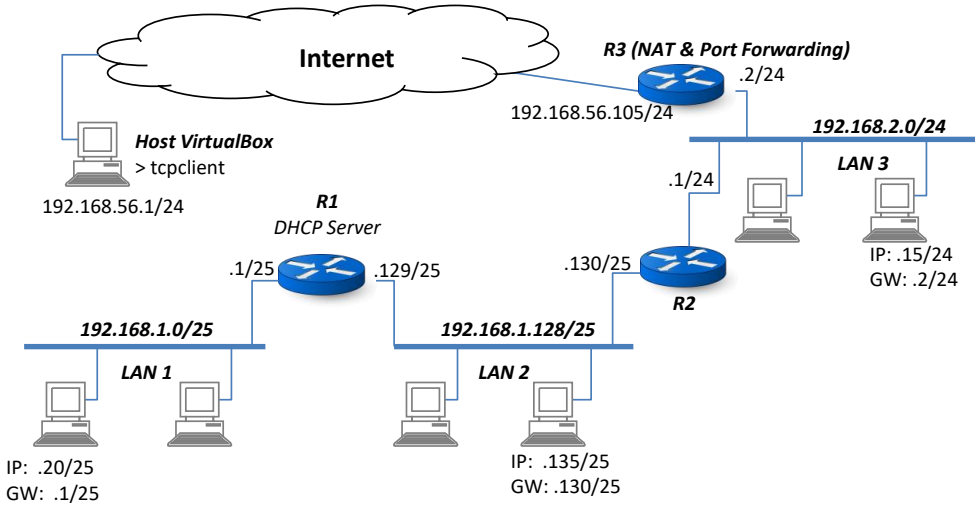
Chú ý kiểm tra đúng card mạng *eth1* là kết nối mặt ngoài của router R3. Sau khi bổ sung luật này, trạm trong mạng LAN3 đã có thể kết nối ra Internet:

```
> ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=42 time=67.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=42 time=65.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=42 time=65.3 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2761ms
rtt min/avg/max/mdev = 65.360/66.064/67.141/0.773 ms

> traceroute -n 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  192.168.2.1  1.838 ms  0.889 ms  0.755 ms
 2  192.168.2.2  2.223 ms  2.173 ms  2.112 ms
 3  10.0.2.2  2.051 ms  2.307 ms  10.234 ms
 4  * * *
```

Không chỉ các trạm thuộc LAN3 mà bất cứ trạm nào của LAN1 hay LAN2 cũng như các router R1, R2 bây giờ đã có thể kết nối Internet thông qua chức năng NAT tại R3. NAT làm việc độc lập với giao thức tầng ứng dụng. Kiểm chứng điều này bằng cách đứng tại một trạm bất kỳ trong các mạng LAN và dùng browser duyệt các trang web trên Internet.

5 Bài 5: Kết nối từ Internet với cơ chế Port forwarding trên Gateway

Bài này thực hiện phương án kết nối ngược với bài trên, tức là cho phép kết nối từ ngoài mạng Internet vào mạng nội bộ.



Bước 1: Kiểm tra kết nối ngược từ Internet vào R3

Để tránh phải xử lý phức tạp tại Gateway kết nối Internet của máy host VirtualBox, tạm coi môi trường bên ngoài Internet là máy host VirtualBox này. Trường hợp muốn kết nối từ một trạm ngoài Internet, cần thiết lập thêm Port Forwarding trên máy Gateway kết nối Internet của máy host VirtualBox.

Chuyển kết nối Internet của R3 từ NAT sang kiểu Host-only Adapter và được gán địa chỉ 192.168.56.105. Máy host VirtualBox có địa chỉ 192.168.56.1. Kiểm tra bằng lệnh *ping* từ R3 sang máy host VirtualBox:

```
[root@R3 ~]# ifconfig eth1
eth2      Link encap:Ethernet  HWaddr 08:00:27:4D:E2:02
          inet addr:192.168.56.105  Bcast:192.168.56.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2980 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:464620 (453.7 KiB)  TX bytes:6790 (6.6 KiB)

[root@R3 ~]# ping 192.168.56.1
PING 192.168.56.1 (192.168.56.1) 56(84) bytes of data.
64 bytes from 192.168.56.1: icmp_seq=1 ttl=128 time=0.614 ms
64 bytes from 192.168.56.1: icmp_seq=2 ttl=128 time=0.641 ms
64 bytes from 192.168.56.1: icmp_seq=3 ttl=128 time=0.602 ms
^C
--- 192.168.56.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2430ms
rtt min/avg/max/mdev = 0.602/0.619/0.641/0.016 ms
```

Kiểm tra kết nối ngược lại, từ máy host VirtualBox vào R3:

```
C:\Users\HP>ipconfig /all

Ethernet adapter VirtualBox Host-Only Network #2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter #2
```

```
   Physical Address. . . . . . . . . : 0A-00-27-00-00-0D
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::659b:1f2b:17ba:955a%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 285868071
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1B-4E-AB-07-EC-F4-BB-4F-20-42
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Dell Wireless 1506 802.11b/g/n (2.4GHz)
   Physical Address. . . . . . . . . : 18-CF-5E-5D-17-C7
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.247.158.105(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, August 29, 2016 10:13:18 PM
   Lease Expires . . . . . . . . . . : Wednesday, August 31, 2016 12:31:24 AM
   Default Gateway . . . . . . . . . : 10.247.158.131
   DHCP Server . . . . . . . . . . . : 10.247.158.131
   DNS Servers . . . . . . . . . . . : 4.4.4.4
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\HP>ping 192.168.56.105

Pinging 192.168.56.105 with 32 bytes of data:
Reply from 192.168.56.105: bytes=32 time<1ms TTL=64
Reply from 192.168.56.105: bytes=32 time<1ms TTL=64
Reply from 192.168.56.105: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.56.105:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
```

Bước 2: Kết nối ứng dụng client-server từ máy host VirtualBox vào R3

Để thực hiện kịch bản kết nối ngược từ Internet vào mạng nội bộ, sử dụng lại các chương trình *tcpserver* và *tcpclient* trong các bài tập chương 2, trên máy R3 chạy *tcpserver*, trên máy host VirtualBox chạy *tcpclient*. Mặc định, tiến trình *iptables* trong Linux ngoài việc chặn tất cả các gói tin được route qua các card mạng (chain FORWARD), nó còn chặn tất cả các gói tin đi vào (chain INPUT). Cần bỏ các rule này ra để *tcpclient* ngoài mạng Internet có thể liên lạc với *tcpserver*

```
[root@R3 ~]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited
```

Cần bỏ các rule này ra để *tcpclient* ngoài mạng Internet có thể liên lạc với *tcpserver* trên router R3 tại cổng 6789:

```
[root@R3 ~]# iptables -D FORWARD -j REJECT --reject-with icmp-host-prohibited
[root@R3 ~]# iptables -D INPUT -j REJECT --reject-with icmp-host-prohibited
[root@R3 ~]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
```

```
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
```

Sau khi bỏ các rule REJECT nêu trên, chạy *tcpserver* trên R3 và chạy *tcpclient* trên máy host Windows, kết quả là các chương trình đã kết nối và trao đổi thông tin thành công:

```
C:\Users\HP> java tcpclient 192.168.56.105 6789
Connecting to TCP Server at: [192.168.56.105:6789]
Server connected. Local client port: 40776
Enter a sentence to send to server: test from windows machine
Received from server: TEST FROM WINDOWS MACHINE
```

Kết quả chạy *tcpserver* trên R3:

```
[root@R3 ~]# java tcpserver 6789
TCP Server is listening for client connect at port: 6789
  - Got client connect from: 192.168.56.1:40776
  - Received from client: test from windows machine
  - Send to client: TEST FROM WINDOWS MACHINE
  - Finish working with client.
```

Bước 3: Thiết lập Port forwarding trên R3 bằng iptables

Như vậy là client ngoài mạng Internet đã truy nhập được vào cổng 6789 của router R3. Tuy nhiên, chưa thể truy nhập đến một dịch vụ bất kỳ trong mạng nội bộ. Ví dụ, tại máy trạm trong LAN3 (có địa chỉ 192.168.2.15), chạy *tcpserver* ở cổng 6789. Từ client host Windows bên ngoài (có địa chỉ 192.168.56.1), chạy *tcpclient* và thấy rằng không thể truy nhập đến dịch vụ *tcpserver* trên máy 192.168.2.15. Để có thể truy nhập từ ngoài vào trong, cần thiết lập port forwarding trên router R3:

```
[root@R3 ~]# iptables -t nat -A  PREROUTING -i eth2 -p tcp --dport 6789 -j DNAT --to-destination 192.168.2.15:6789
```

Sau lệnh này, *tcpclient* trên máy Windows khi kết nối với địa chỉ mặt ngoài của R3 (là 192.168.56.105) đã có thể liên lạc với *tcpserver* tại máy trạm của LAN3 (có địa chỉ 192.168.2.15):

```
C:\Users\HP> java tcpclient 192.168.56.105 6789
Connecting to TCP Server at: [192.168.56.105:6789]
Server connected. Local client port: 40776
Enter a sentence to send to server: test port forwarding from external host (192.168.56.1)
Received from server: TEST PORT FORWARDING FROM EXTERNAL HOST (192.168.56.1)
```

Sử dụng *tcpdump* để bắt các gói tin trên 2 card mạng của R3 (mặt ngoài và mặt trong) sẽ thấy các gói tin IP mà gửi đến cổng 6789 của card mạng mặt ngoài được forward sang card mạng mặt trong và thay đổi địa chỉ đích thành 192.168.2.15.