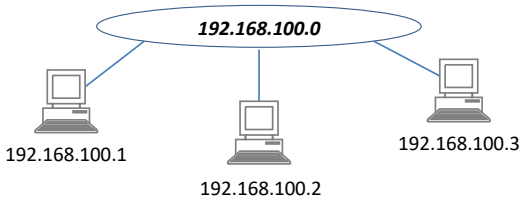
Thiết kế & triển khai mạng IP

Bài thực hành số 3: Mạng nội bộ (Private Network)

1 Bài 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.



Bước 1: Cấu hình mạng cho các trạm kết nối vào cùng một mạng LAN

Khởi động 3 máy ảo, 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*:

```
> ifconfig eth0 192.168.100.1
> 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 eth0
```

Trường hợp máy được thiết lập Gateway, khi dùng lệnh *route -n* để hiển thị bảng routing sẽ thấy xuất hiện một dòng định tuyến với mạng destination là *0.0.0.0* (để chỉ toàn bộ destination) và cột Gateway sẽ là địa chỉ IP của Gateway. Ví dụ nếu máy được thiết lập Gateway thì bảng routing sẽ có dạng như sau:

```
> 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 eth2
10.0.2.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0
0.0.0.0         10.0.2.2        0.0.0.0         UG    0      0        0 eth0
192.168.56.0    0.0.0.0         255.255.255.0   U     0      0        0 eth1
169.254.0.0     0.0.0.0         255.255.0.0     U     1002   0        0 eth0
```

Bước 2: Kết nối giữa hai trạm bằng lệnh ping và phân tích gói tin

Sử dụng lệnh *ping* để kiểm tra kết nối giữa 2 máy trong mạng, thấy *ping* thành công (tức là truyền dữ liệu trong mạng LAN không cần sự tham gia của Gateway). Có thể *ping* đến địa chỉ broadcast 192.168.100.255 hoặc địa chỉ mạng 192.168.100.0 để gửi gói tin *ICMP Echo Request* đến tất cả các máy trong mạng. Để tránh ý đồ làm tràn ngập mạng bằng cách liên lạc theo địa chỉ broadcast, CentOS cài đặt giao thức ICMP mặc định không trả lời *ping* đến địa chỉ broadcast mặc dù nhận được gói tin *ICPM Echo Request*. Do vậy, để nhìn thấy gói tin ICMP được gửi đến khi một trạm khác trong mạng *ping* đến địa chỉ broadcast, cần sử dụng chức năng log của *iptables* để hiển thị các gói tin ICMP đi đến (tham khảo bài thực hành số 2 trong chương 1).

2 Bài 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.

Bước 1: cài đặt & cấu hình DHCP server

DHCP server phổ biến trên hệ thống Linux là gói DHCP (phiên bản hiện tại là 4.1). Có thể dùng lệnh *yum* để tải về và cài đặt:

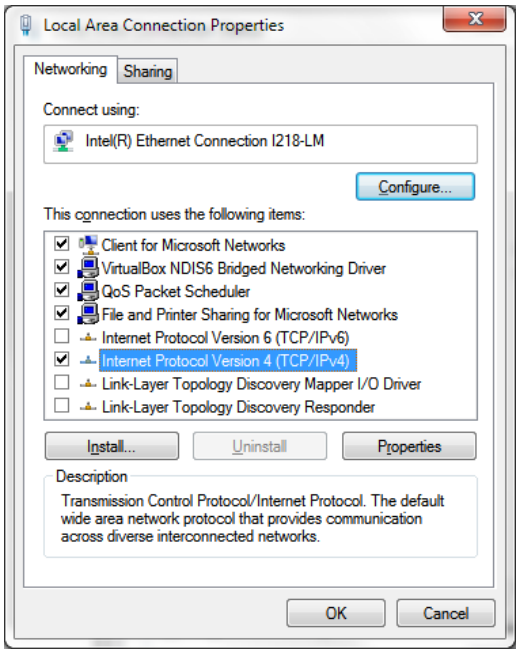
```
> yum install dhcp
Loaded plugins: fastestmirror
Setting up Install Process
Loading mirror speeds from cached hostfile
 * base: mirror.rise.ph
 * extras: mirror.pregi.net
 * updates: mirror.rise.ph
base                                                     | 3.7 kB     00:00
extras                                                   | 2.9 kB     00:00
updates                                                  | 3.4 kB     00:00
Package 12:dhcp-4.1.1-49.P1.el6.centos.x86_64 already installed and latest version
Nothing to do
[root@mydomain ~]#
```

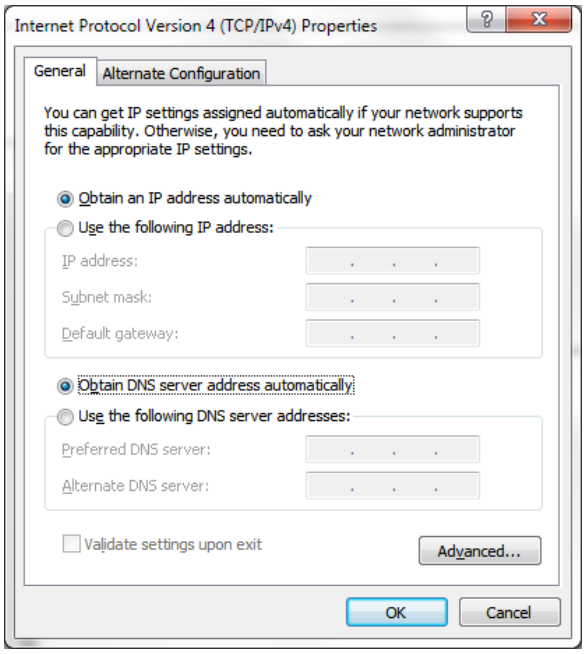
Cấu hình DHCP server được mô tả trong file */etc/dhcp/dhcpd.conf*. DHCP server sẽ cũng cấp địa chỉ IP cho các máy trong cùng mạng vật lý của máy chủ. Trong cấu hình bên dưới, DHCP server sẽ cung cấp địa chỉ IP trong dải 192.168.2.10 đến 192.168.2.20 với cấu hình mạng 192.168.2.0/25. Như vậy, máy chủ DHCP này phải có 1 kết nối mạng vào mạng 192.168.2.0/25. Ngoài ra, nó cung cấp thêm địa chỉ Default Gateway là 192.168.2.1 và DNS server là 4.4.4.4 và 8.8.8.8.

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

subnet 192.168.2.0 netmask 255.255.255.128 {
  range 192.168.2.10 192.168.2.20;

  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;
}
```

Bước 2: thiết lập DHCP client

Trên Windows, cấu hình địa chỉ IP động chỉ IP động thông qua các cửa sổ thiết lập cấu hình IP cho từng kết nối mạng.





Trên Linux, các card mạng cấu hình địa chỉ IP động được thiết lập bằng file cấu hình */etc/sysconfig/network-scripts/ifcfg-ethX* trong đó *ethX* là tên của card mạng. Ví dụ:

```
> nano /etc/sysconfig/network-scripts/ifcfg-eth2
DEVICE=eth2
BOOTPROTO=dhcp
ONBOOT=yes
```

Với cấu hình như trên, khi khởi động trạm làm việc, card mạng *eth2* sẽ tự động thực hiện giao thức DHCP để tìm kiếm DHCP server trên mạng và xin cấp địa chỉ IP.

Bước 3: Tương tác DHCP client-server

Khởi động service DHCP trên máy chủ:

```
> service dhcpd restart
Shutting down dhcpd:                                       [  OK  ]
Starting dhcpd:                                            [  OK  ]
```

Trên máy client, có thể dùng lệnh *dhclient -r* để giải phóng IP đã được gán cho card mạng khi khởi động. Sau khi giải phóng địa chỉ IP, dùng *ifconfig* để hiển thị thông tin card mạng sẽ không thấy địa chỉ IP nào được gán cho card mạng này nữa. Tiếp theo, sử dụng lệnh *dhclient -v* để yêu cầu thiết lập lại địa chỉ IP và lại dụng *ifconfig* để xem cấu hình card mạng với địa chỉ IP vừa được gán. Để kiểm tra thông số Default Gateway, sử dụng lệnh *route -n* để xem bảng routing. Default Gateway được thiết lập (cho mạng 0.0.0.0) là 192.168.2.1.

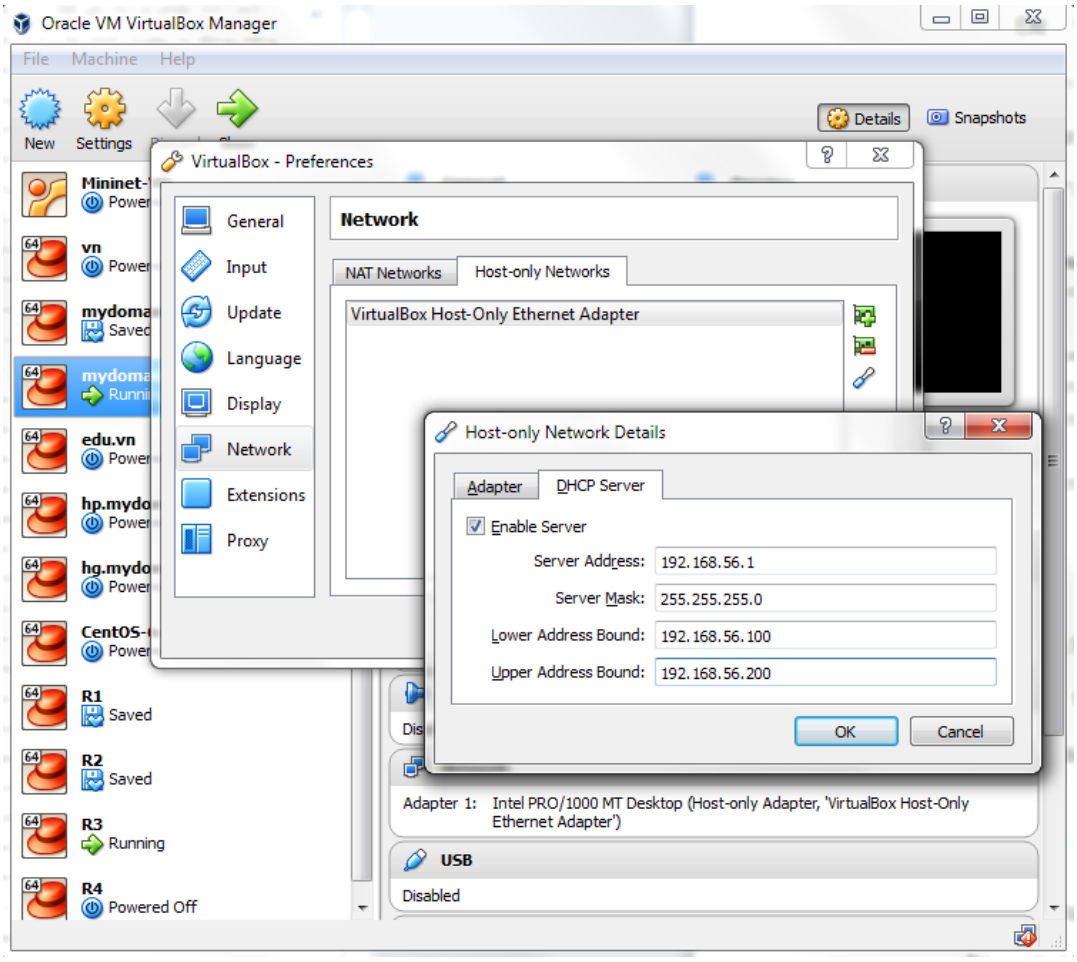
```
[root@C1 ~]# dhclient -r eth2
[root@C1 ~]# ifconfig eth2
eth2      Link encap:Ethernet  HWaddr 08:00:27:D6:C1:02
          inet6 addr: fec1::7/64 Scope:Site
          inet6 addr: fe80::a00:27ff:fed6:c102/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:63 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5334 (5.2 KiB)  TX bytes:2380 (2.3 KiB)

[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 5 (xid=0x3ddd558b)
DHCPOFFER from 192.168.2.2
DHCPREQUEST on eth2 to 255.255.255.255 port 67 (xid=0x3ddd558b)
DHCPACK from 192.168.2.2 (xid=0x3ddd558b)
bound to 192.168.2.10 -- renewal in 41397 seconds.

[root@C1 ~]# ifconfig eth2
eth2      Link encap:Ethernet  HWaddr 08:00:27:D6:C1:02
          inet addr:192.168.2.10  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         192.168.2.1     0.0.0.0         UG    0      0        0 eth2
```

Để bắt và phân tích gói tin DHCP, sử dụng file log của hệ thống Linux */etc/log/messages*. Thực hiện chạy DHCP server và tiến hành giải phóng địa chỉ IP (*dhclient -r*) rồi cấp lại IP (*dhclient -v*) ở máy client như trên. Tại máy server, hiển thị thông tin log (lọc theo DHCP):

```
> tail -f /var/log/messages | grep DHCP
Jan 11 03:23:59 mydomain dhcpd: DHCPRELEASE of 192.168.1.14 from 08:00:27:56:81:0c via eth2 (found)

Jan 11 03:24:04 mydomain dhcpd: DHCPDISCOVER from 08:00:27:56:81:0c via eth2
Jan 11 03:24:05 mydomain dhcpd: DHCPOFFER on 192.168.1.14 to 08:00:27:56:81:0c via eth2
Jan 11 03:24:05 mydomain dhcpd: DHCPREQUEST for 192.168.1.14 (192.168.1.1) from 08:00:27:56:81:0c via eth2
Jan 11 03:24:05 mydomain dhcpd: DHCPACK on 192.168.1.14 to 08:00:27:56:81:0c via eth2
```

Chú ý rằng VirtualBox mặc định cũng thiết lập một máy chủ DHCP để tự động gán địa chỉ IP cho các máy ảo sử dụng card mạng kiểu Host-only. Có thể cấu hình DHCP của VirtualBox thông qua menu File/Preference… và chọn mục Network.



Bước 4: Kịch bản tương tranh nhiều DHCP server

Cũng trong mạng LAN hiện tại, thiết lập thêm một DHCP server tại địa chỉ IP 192.168.2.5 với các thông số sau:

```
[root@hack ~]# cat /etc/dhcp/dhcpd.conf
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#   see 'man 5 dhcpd.conf'
#
subnet 192.168.2.0 netmask 255.255.255.128 {
  range 192.168.2.40 192.168.2.50;

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

  option routers 192.168.2.13;
  option domain-name-servers 1.2.3.4;
}

[root@C0 ~]# service dhcpd start
Starting dhcpd:                                            [  OK  ]
```

Có thể thấy DHCP server này cũng cung cấp dải địa chỉ IP trong mạng 192.168.2.0/25 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:

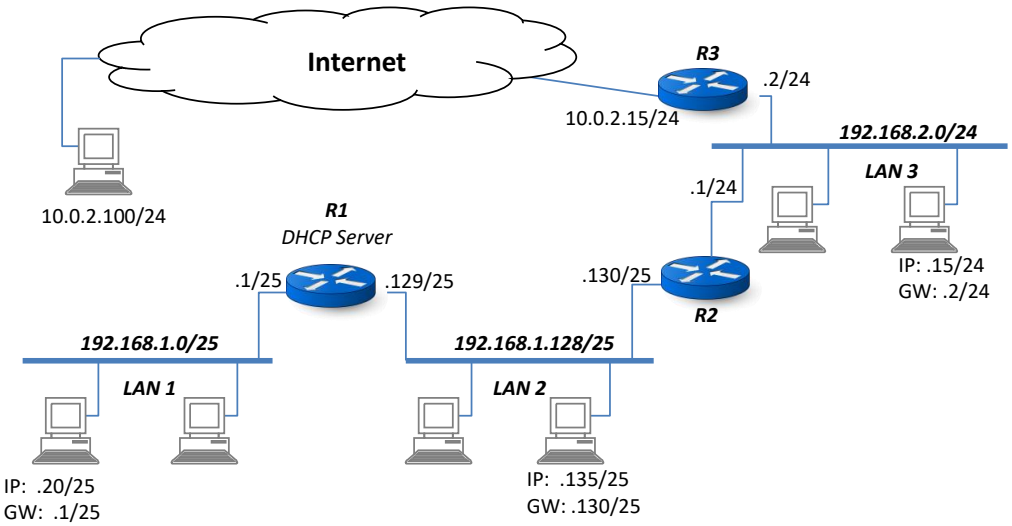
```
[root@C1 ~]# dhclient -r eth2
[root@C1 ~]# dhclient -v eth2
Internet Systems Consortium DHCP Client 4.1.1-P1
Copyright 2004-2010 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

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 Bài 3: Qui hoạch Gateway cho mạng Intranet

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



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
```

Bước 3: Cấu hình router R2 và R3

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
```

Bước 5: 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
```

Bước 6: 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 lựa 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.

Bước 1: Kiểm tra kết nối Internet từ 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
```

Bước 2: Thiết lập NAT trên R3 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
```

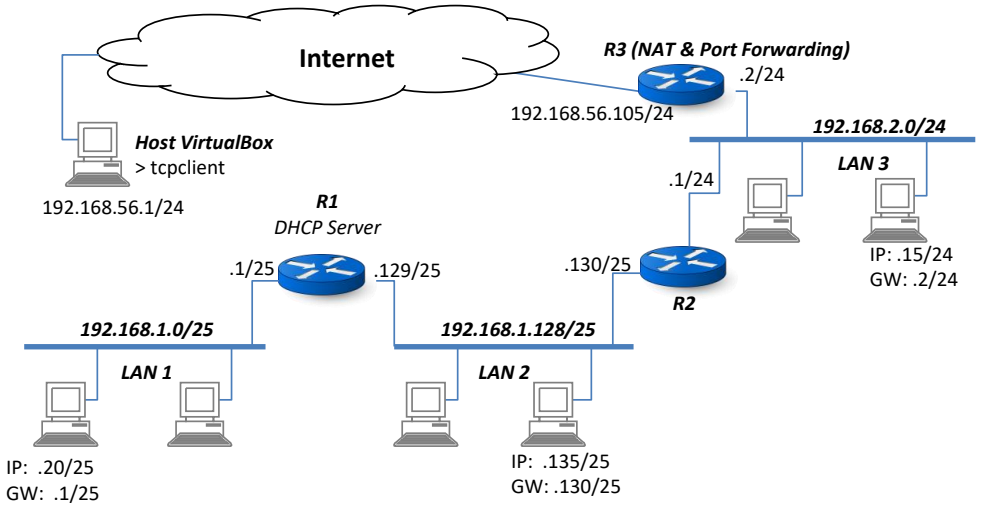
Chú ý kiểm tra đúng card mạng *eth1* là kết nối mặt ngoài của router R3. Sau khi bổ sung luật này, trạm trong mạng LAN3 đã có thể kết nối ra Internet:

```
> 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.