

Bài 5. Kết nối mạng

1. Cấu hình mạng

1.1 Giao diện mạng

Giao diện mạng Ethernet thường được đặt tên dạng ethX, với X là số. Giao diện Ethernet đầu tiên thường là eth0. Để xem danh sách các giao diện Ethernet, chạy lệnh:

`ifconfig -a`

Có thể sử dụng lệnh lshw để xem danh sách các giao diện mạng như sau.

`sudo lshw -class network`

Tên logic của các giao diện mạng được cấu hình trong tệp

/etc/udev/rules.d/70-persistent-net.rules. Có thể thay đổi tên logic của các giao diện mạng rồi khởi động lại hệ thống để tên logic mới có hiệu lực.

Ethtool là công cụ cho phép xem và thay đổi giao diện Ethernet. Cài đặt công cụ này bằng lệnh sau:

`sudo apt install ethtool`

Sử dụng ethtool để xem cấu hình giao diện mạng như ví dụ sau:

`sudo ethtool eth0`

Những thay đổi do sử dụng ethtool chỉ có giá trị tạm thời, sẽ mất khi máy được khởi động lại.

1.2 Địa chỉ IP

Đặt IP tạm thời

Có thể sử dụng các công cụ như ip, ifconfig và route để gán địa chỉ IP tạm thời cho các giao diện mạng. Những thiết lập này có tác dụng ngay tức thì nhưng sẽ mất khi khởi động lại hệ thống. Ví dụ, sử dụng ifconfig để đặt địa chỉ IP tạm thời như sau:

`sudo ifconfig eth0 10.0.0.100 netmask 255.255.255.0`

Để xác minh lại IP tạm thời đã được sử dụng cho giao diện eth0, chạy lệnh

`ifconfig eth0`

Để thiết lập gateway mặc định tạm thời, chạy lệnh sau:

`sudo route add default gw 10.0.0.1 eth0`

Để xác minh gateway tạm thời đã có hiệu lực, chạy lệnh:

`route -n`

Để xóa các cấu hình IP tạm thời, chạy lệnh

`ip addr flush eth0`

Cấu hình IP tĩnh

Chỉnh sửa tệp /etc/network/interfaces với nội dung tương tự sau.

```
auto eth0
iface eth0 inet static
  address 10.0.0.100
  netmask 255.255.255.0
  gateway 10.0.0.1
  network 10.0.0.0
```

```
broadcast 10.0.0.255
```

Sau đó, khởi động lại giao diện mạng.

```
sudo ifdown eth0
```

```
sudo ifup eth0
```

Cấu hình IP động (DHCP client)

Chỉnh sửa tệp /etc/network/interfaces với nội dung tương tự sau.

```
auto eth0
```

```
iface eth0 inet dhcp
```

Sau đó, khởi động lại giao diện mạng.

```
sudo ifdown eth0
```

```
sudo ifup eth0
```

Giao diện Loopback

Giao diện loopback có tên logic là lo và địa chỉ IP là 127.0.0.1. Có thể xem thông tin giao diện loopback bằng lệnh.

```
ifconfig lo
```

Mặc định, tệp /etc/network/interfaces có hai dòng sau đây cho cấu hình giao diện loopback:

```
auto lo
```

```
iface lo inet loopback
```

1.3 Phân giải tên

Thiết lập DNS tạm thời

Để thiết lập DNS tạm thời, chỉnh sửa tệp /etc/resolv.conf. Dưới đây là các tham số dùng trong file /etc/resolv.conf:

- *nameserver*: Địa chỉ IP của DNS nameserver. Chỉ đặt một địa chỉ IP đối với mỗi từ khóa “nameserver”. Nếu có nhiều hơn một nameserver, sẽ cần có nhiều dòng có chứa từ khóa “nameserver” cùng với địa chỉ IP của DNS tương ứng.
- *domain*: Local domain mặc định được sử dụng. Nếu tên đầy đủ của server là pc1.my-web-site.org thì khi đó trường này sẽ có giá trị là my-web-site.org
- *search*: Nếu ta muốn tham chiếu tới một server khác bằng tên của server đó mà không cần thêm tên miền (domain), DNS trên máy trạm của ta sẽ thêm tên server vào mỗi tên miền trong danh sách này và để DNS tìm kiếm và lấy địa chỉ IP của server cần truy vấn tới. Cách này làm giảm thời gian cần truy cập tới các server trong cùng tên miền mà không cần phải chỉ rõ đầy đủ tên miền của chúng. Các tên miền trong danh sách phải được cách nhau bởi một dấu cách.

Dưới đây là ví dụ file cấu hình của DNS client với tên miền chính là **my-site.com**, nhưng nó cũng là một thành viên của tên miền **my-site.net** và **my-site.org**, điều này làm giảm bớt thời gian tìm kiếm để truy vấn tới các server khác. Trong file này cũng khai báo 2 DNS server có địa chỉ IP là 192.168.1.100 và 192.168.1.102:

```
search my-site.com my-site.net my-site.org
```

```
nameserver 192.168.1.100
```

```
nameserver 192.168.1.101
```

Thiết lập DNS với IP tĩnh

Chỉ định các nameservers trong tệp /etc/network/interfaces, như ví dụ sau.

```
auto eth0
```

```
iface eth0 inet static
```

```

address 112.137.130.29
netmask 255.255.255.192
network 112.137.130.0
broadcast 112.137.130.63
gateway 112.137.130.1
dns-search example.com sales.example.com dev.example.com
dns-nameservers 192.168.3.45 192.168.8.10

```

Nếu tìm host với tên là server1, hệ thống sẽ thực hiện các truy vấn DNS với tên đầy đủ (FQDN) theo thứ tự sau:

```

server1.example.com
server1.sales.example.com
server1.dev.example.com

```

Thiết lập DNS với IP động

Nếu IP được cấp động, DHCP server sẽ thay mặt client yêu cầu các nameserver phân giải tên.

Phân giải tên cục bộ

Tệp /etc/hosts xác định các ánh xạ hostname-to-IP. Các phần tử trong tệp này có thứ tự ưu tiên cao hơn DNS. Ví dụ nội dung tệp /etc/hosts như sau:

```

127.0.0.1      localhost
127.0.1.1      ubuntu-server
10.0.0.11      server1 server1.example.com vpn
10.0.0.12      server2 server2.example.com mail

```

Cấu hình Name Service Switch

Thứ tự hệ thống lựa chọn phương thức phân giải tên sang địa chỉ IP được điều khiển bởi tệp cấu hình Name Service Switch (NSS) /etc/nsswitch.conf. Thông thường, các host tĩnh có thứ tự cao hơn các tên được phân giải bởi DNS. Ví dụ nội dung tệp /etc/nsswitch.conf như sau:

```
hosts:      files mdns4_minimal [NOTFOUND=return] dns mdns4
```

Trong đó:

- files – tìm kiếm trong /etc/hosts.
- mdns4_minimal - Multicast DNS.
- [NOTFOUND=return] - nếu kết quả của mdns4_minimal trả về là NOTFOUND thì dừng tìm kiếm.
- dns - unicast DNS query.
- mdns4 - Multicast DNS query.

2. Một số tiện ích mạng

ping

Lệnh **ping** gửi các gói ECHO_REQUEST tới địa chỉ chỉ định. Câu lệnh nhằm kiểm tra máy tính có thể kết nối với Internet hay một địa chỉ IP cụ thể nào đó hay không. Tuy nhiên có rất nhiều hệ thống được cấu hình để không hồi đáp với các lệnh ping.

Không giống lệnh **ping** trên Windows, câu lệnh **ping** trên Linux sẽ duy trì gửi các gói tin cho đến khi bạn kết thúc nó. Có thể định số lượng gói tối đa gửi đi bằng cách gõ thêm tùy chọn **-c**.

Cú pháp:

```
ping [ -c count] [ -t ttl] destination
```

Ví dụ:

[ping -c 4 google.com](#)

tracepath, traceroute

Lệnh **tracepath** cũng tương tự như **traceroute** nhưng nó không đòi hỏi các quyền quản trị. Lệnh **tracepath** lần dấu đường đi trên mạng tới một đích chỉ định và báo cáo về mỗi nút mạng (hop) dọc trên đường đi. Nếu gặp phải các vấn đề về mạng, lệnh **tracepath** có thể chỉ ra vị trí lỗi mạng.

Ví dụ:

[tracepath google.com](#)

nmap, zenmap

Nmap là một trình quét bảo mật mạng được sử dụng để phát hiện các máy tính và các dịch vụ trên mạng máy tính, sau đó sẽ tạo một “bản đồ” mạng. Cũng giống như các bộ quét cổng đơn giản, **nmap** có khả năng phát hiện các dịch vụ thụ động (passive) trên một mạng dù các dịch vụ như vậy không tự khuyếch trương bản thân chúng bằng một giao thức phát hiện dịch vụ.Thêm vào đó, **nmap** có thể phát hiện các thông tin chi tiết khác nhau về các máy tính từ xa. Chúng có thể phát hiện ra hệ điều hành, kiểu thiết bị, thời gian và sản phẩm phần mềm chạy dịch vụ, số phiên bản chính xác của sản phẩm đó, sự hiện diện của một số công nghệ tường lửa trên một mạng nội bộ hoặc thậm chí cả hằng sản xuất card mạng từ xa.

Cách sử dụng:

- Lấy thông tin từ máy từ xa và xác định hệ điều hành của máy

[nmap -sS -P0 -sV -O <target>](#)

Trong đó

- o <**target**> có thể là địa chỉ IP, tên máy hoặc subnet mạng.
- o **-sS** quét TCP SYN (được biết như là mở một nửa hoặc quét trộm)
- o **-P0** cho phép tắt ping ICMP.
- o **-sV** tùy chọn bật khả năng phát hiện phiên bản
- o **-O** xác định hệ điều hành máy ở xa

Tùy chọn khác:

- o **-A** bật tính năng phát hiện fingerprinting và phiên bản hệ điều hành
- o **-v** sử dụng 2 lần để verbosity.

[nmap -sS -P0 -A -v <target>](#)

- Lấy danh sách các máy chủ với các cổng mở được định nghĩa trước

[nmap -sT -p 80 -oG – 192.168.1.* | grep open](#)

Thay đổi tham số **-p** thành cổng muốn kiểm tra. Xem “**man nmap**” để biết chỉ ra phạm vi địa chỉ.

- Tìm tất cả các địa chỉ IP đang hoạt động trong mạng LAN (192.168.0.*)

[nmap -sP 192.168.0.*](#)

Có vài tùy chọn khác. Ví dụ trên là đơn giản nhất.

Ví dụ dưới là kiểm tra cả subnet:

[nmap -sP 192.168.0.0/24](#)

- Ping một dải địa chỉ IP (từ 192.168.1.100 đến 192.168.1.254)

[nmap -sP 192.168.1.100-254](#)

- Tìm các địa chỉ IP chưa dùng trong một subnet

nmap -T4 -sP 192.168.2.0/24 && egrep "00:00:00:00:00:00" /proc/net/arp

- Sử dụng bù nhìn khi quét cổng mà không bị quản trị hệ thống biết

nmap -sS 192.168.0.10 -D 192.168.0.2

Quét cổng mở trên thiết bị/máy tính đích (192.168.0.10) trong khi thiết lập một địa chỉ bù nhìn (192.168.0.2). Cái này sẽ hiển thị một địa chỉ IP mà thay cho địa chỉ IP thực của bạn được ghi trong hệ thống log. Địa chỉ bù nhìn cần phải hoạt động. Xem log bảo mật tại **/var/log/secure** để xem nó có làm việc không.

- Liệt kê danh sách các bản ghi DNS ngược cho một subnet

nmap -R -sL 209.85.229.99/27 | awk '{if(\$3=="not")print"\"\$2\" no PTR";else print\$3" is \"\$2\""}' | grep '('

Lệnh này để kiểm tra DNS ngược trên một subnet. Nó liệt kê một danh sách các địa chỉ IP với các bản ghi PTR tương ứng của một subnet. Ta có thể thêm “-dns-servers x.x.x.x” sau “-sL” nếu bạn cần kiểm tra trên một DNS Server mà bạn biết.

- Kiểm tra có bao nhiêu thiết bị Windows và Linux hoạt động trong mạng

nmap -F -O 192.168.0.1-255 | grep "Running: " > /tmp/os; echo "\$(cat /tmp/os | grep Linux | wc -l) Linux device(s)"; echo "\$(cat /tmp/os | grep Windows | wc -l) Window(s) devices"

zenmap là GUI cho nmap. Zenmap chạy trên mọi hệ điều hành. Download <https://nmap.org/zenmap/>

netstat

Lệnh **netstat -nr** sẽ cung cấp nội dung của bảng định tuyến. Các mạng với gateway of 0.0.0.0 luôn được kết nối trực tiếp với thiết bị mạng. Không gateway cần để kết nối thiết bị kết nối trực tiếp, như vậy một gateway có địa chỉ 0.0.0.0 là thích hợp. Tuyến đường với địa chỉ đích là địa chỉ gateway mặc định.

```
[root@testweb tmp]# netstat -nr
```

Kernel IP routing table

Destination	Gateway	Genmask	Flags	MSS	Window	Irtt	Iface
255.255.255.255	0.0.0.0	255.255.255.255	UH	40	0	0	wlan0
192.168.1.0	0.0.0.0	255.255.255.0	U	40	0	0	wlan0
127.0.0.0	0.0.0.0	255.0.0.0	U	40	0	0	lo
0.0.0.0	192.168.1.1	0.0.0.0	UG	40	0	0	wlan0

3. DHCP Server

DHCP (Dynamic Host Configuration Protocol) được sử dụng với mục đích tập trung hoá việc quản lý và ấn định cấu hình TCP/IP của các máy client. Với những đặc điểm thuận lợi giúp cho người quản trị tiết kiệm thời gian trong việc cài đặt và quản trị một hệ thống mạng TCP/IP như sau:

- Quản lý việc cấp phát địa chỉ IP cho các máy client khi có yêu cầu.
- Cung cấp những thông tin cấu hình mạng như subnet mask, default router, DNS Server.
- DHCP có thể làm việc thông qua nhiều TCP/IP router và ấn định IP dựa theo subnet mask gửi tới do đó bạn không cần phải cấu hình lại máy tính khi di chuyển qua những subnet khác nhau.
- Địa chỉ IP chỉ được cấp phát trong một khoảng thời gian nhất định, những địa chỉ IP không tiếp tục sử dụng sẽ bị thu hồi lại.
- Hỗ trợ BOOTP (Bootstrap Protocol) client

Để sử dụng DHCP ta cần phải có một DHCP Server để đáp ứng (cung cấp địa chỉ IP và thông tin cấu hình mạng) các yêu cầu từ các máy DHCP client gửi tới, đồng thời trên các máy client cần phải có DHCP client để gửi yêu cầu, nhận đáp ứng và thực hiện thay đổi cấu hình IP của client.

Có thể tóm tắt quá trình hoạt động **DHCP request-response** như sau:

- **Lease request:** dhcp client gửi broadcast gói tin dhcp request (địa chỉ nguồn là 0.0.0.0, địa chỉ đích là 255.255.255.255 và địa chỉ MAC của client), gói tin này được mở bởi DHCP Server.
- **Ip lease offer:** DHCP Server ấn định cho client địa chỉ ip, subnet mask, domain name, địa chỉ name server, khoảng thời gian mà những thông tin cấu hình này client được phép sử dụng hợp lệ.
- **Lease selection:** client chọn một dhcp offer, rồi broadcast để thông báo với các DHCP Servers.
- **DHCP Server** gửi đến client một gói tin ack và khi đó client đã được cấu hình TCP/IP và hoạt động bình thường.
- **Lease renew:** khi sử dụng những thông tin cấu hình được cung cấp đến một nửa khoảng thời gian được phép (default-lease-time) DHCP client nếu muốn tiếp tục sử dụng sẽ gửi một request mới tới DHCP Server.

Thành phần của một DHCP server bao gồm bốn mục chính sau:

- **Options:** Dùng để cung cấp các yếu tố cho phía client như địa chỉ IP, địa chỉ subnet mask, địa chỉ Gateway, địa chỉ DNS .v.v...
- **Scope:** Một dải địa chỉ được quy định trước trên DHCP server mà chúng ta sẽ dùng để gán cho các máy client.
- **Reservation:** Là những dải địa chỉ dùng để “để dành” trong một scope mà chúng ta đã quy định ở trên.
- **Lease:** Thời gian “cho thuê” địa chỉ IP đối với mỗi client.

3.1 Cài đặt

Để cài đặt DHCP server, chạy lệnh sau:

`sudo apt install isc-dhcp-server`

3.2 Cấu hình

Tệp cấu hình DHCP là /etc/dhcp/dhcpd.conf. Dưới đây sẽ giải thích các phần quan trọng trong /etc/dhcp/dhcpd.conf.

Chú ý: **Bắt buộc phải có một phần subnet cho mỗi giao diện mạng (interface) trong Linux.**

```
ddns-update-style interim;
option domain-name "vnu.edu.vn";
option domain-name-servers ns1.vnu.edu.vn, ns2.vnu.edu.vn;
default-lease-time 86400;
max-lease-time 86400;
```

Khai báo Subnet:

```
subnet 192.168.1.0 netmask 255.255.255.0 {
```

```
    # Dải địa chỉ IP mà máy chủ DHCP sẽ cấp phát cho các máy trạm trên mạng
    range 192.168.1.201 192.168.1.220;
```

```
    # Thời gian (tính theo giây - second) cho một máy trạm được phép sử dụng địa chỉ IP đã
    # được cấp phát
```

```

# Gateway mặc định cho máy trạm
option routers 192.168.1.1;
# Tên miền cho các máy
option domain-name "mydomain.example";
# Cấm chuyển tiếp các gói tin yêu cầu DHCP từ card mạng này tới các card mạng khác
option ip-forwarding off;
# Thiết đặt địa chỉ Broadcast và Subnet Mask cho máy trạm sử dụng
option broadcast-address 192.168.1.255;
option subnet-mask 255.255.255.0;
# Thiết đặt máy chủ Network Time Protocol (NTP) cho máy trạm sử dụng
option ntp-servers 192.168.1.100;
# Thiết đặt máy chủ DNS cho máy trạm sử dụng
option domain-name-servers 192.168.1.100;
# Nếu muốn máy trạm sử dụng dịch vụ WINS, ta cần thêm dòng khai báo sau:
option netbios-name-servers 192.168.1.100;
# Nếu ta cần thiết đặt địa chỉ IP cố định cho một máy trạm nào đó thông qua địa chỉ MAC,
cần khai báo thêm các máy trạm đó như dưới đây (VD: máy trạm đó có tên laser-print):
host my-printer {
    hardware ethernet 08:00:2b:4c:59:23;
    fixed-address 192.168.1.222;
}
}

```

```

#
# Danh sách các Interface chưa sử dụng được khai báo như dưới đây
#
subnet 192.168.2.0 netmask 255.255.255.0 {
}

```

Còn rất nhiều các lựa chọn khác ta có thể sử dụng trong file cấu hình dịch vụ DHCP. Để biết thêm chi tiết các lựa chọn này, ta có thể sử dụng lệnh trợ giúp sau:

```
# man dhcp-options
```

Sau khi cấu hình xong, chạy lệnh sau để khởi động lại dhcpcd.

```
sudo systemctl restart isc-dhcp-server.service
```

Để sử dụng dịch vụ DHCP sau khi chạy dhcpcd, nhớ thiết lập IP động cho các máy trong mạng. Hoạt động cấp phát địa chỉ IP và thông tin cấu hình mạng của dhcp server sẽ được ghi vào file log theo đường dẫn /var/lib/dhcp/dhcpd.leases

```

lease172.16.1.100 {
    starts 2 2012/02/28 20:14:44;
    ends 3 2012/02/29 02:14:44;
    tstp 3 2012/02/29 02:14:44;
    binding state active;
    next binding state free;
    hardware ethernet 00:0d:14:l1:12:90;
}

```

```

lease172.16.1.99 {
    starts 2 2012/02/28 21:59:09;
    ends 3 2012/02/29 03:59:09;
    binding state active;
    next binding state free;
    hardware ethernet 00:0c:29:75:8a:b5;
    uid "\001\000\014u\212\265";
    client-hostname "black-fe4062c4f";
}

```

4. Thực hành

Bài 1. Dò quét mạng

Sử dụng bảng định tuyến trên gateway của phòng thực hành, hãy dùng những công cụ: ping, traceroute, nmap để vẽ được sơ đồ kiến trúc mạng trong phòng thực hành và những mạng liền kề với độ chi tiết càng nhiều càng tốt.

Bài 2. Thiết lập phân mạng

Chia các máy tính trong phòng thực hành thành 5 nhóm, mỗi nhóm gồm 3 máy trên một hàng. Sau đó, cấu hình các nhóm theo yêu cầu sau:

- Mỗi nhóm sử dụng một máy có 2 card mạng (thêm vào trong máy ảo theo cơ chế bridge).
- Mỗi card mạng trên máy này nối vào một mạng (nhóm 1 sẽ là 10.10.11.0/24 và 10.10.12.0/24, nhóm 2 sẽ là 10.10.21.0/24 và 10.10.22.0/24...). Sử dụng lệnh netconfig và sửa bằng tay file cấu hình để thực hiện việc này
- Hai máy tính còn lại, mỗi máy có IP thuộc một mạng được cấp và default gateway chỉ đến IP tương ứng tại máy tính có 2 card mạng.
- Thiết lập là ip_forward trên máy tính có 2 card mạng bằng 2 cách để nó chuyển tiếp các gói tin.

Bài 3. Thiết lập DHCP server

Thiết lập DHCP server trên các máy tính (172.16.2.1, 172.16.3.1, 172.16.4.1, 172.16.5.1) sao cho:

- Chỉ lắng nghe yêu cầu trên mạng con (192.168....)
- Ngoài IP/Subnetmask còn cung cấp các thông số về gateway, dns, dns postfix.