CSE301 - Linux và phần mềm mã nguồn mở

Bài 10: Quản trị mạng Linux

dungkt@tlu.edu.vn

COMPUTER SCIENCE AND ENGINEERING
THUYLOI UNIVERSITY

Mục tiêu bài học

- Hiểu biết về cấu hình mạng cơ bản cho máy chủ Linux
- Có khả năng cấu hình mạng
- Có khả năng cấu hình định tuyến tĩnh
- Có thể triển khai các dịch vụ máy chủ trên Linux như: dhcp server, dns server, web server, mail server ...
- Quản trị từ xa máy chủ Linux thông qua các công cụ sử dụng giao diện dòng lệnh hoặc dựa trên nền tảng Web

Nội dung

1) Cấu hình mạng trên Linux
2) Triển khai các dịch vụ mạng
    a) SSH server
    b) DHCP server
    c) DNS server
    d) Web server
    e) FTP server
    f) Mail server
    g) Samba Server
    h) Quản trị từ xa

1. Cấu hình mạng trên Linux

Giao diện mạng

- **Phần cứng và trình điều khiển**
  - Giao diện mạng (**Network Inferface**) được điều khiển bởi kernel bằng trình điều khiển được tải động theo yêu cầu.
  - Không giống như đĩa cứng hay máy in được truy cập như tệp qua /dev, giao diện mạng là ảo.
  - Sau khi nạp trình điều khiển, kernerl truy cập thiết bị mạng qua giao diện mạng. Các giao diện được đặt tên (Ethenet: eth0, ...)

Giao diện mạng

- **Các tệp tin cấu hình**
  - /etc/hosts, /etc/hosts.allow, /etc/hosts.deny
  - /etc/netplan
  - /etc/resolv.conf
  - /etc/services
- **Các lệnh cấu hình, debug thông tin**
  - ifconfig, ifup, ifdown
  - route
  - traceroute, netstat, tcpdump

Cấu hình card mạng sử dụng ifconfig

- Trước khi có thể sử dụng giao diện mạng để truy cập mạng, nó phải được gán địa chỉ IP, mặt nạ mạng, v.v. Theo truyền thống, điều này được thực hiện bằng tay bằng lệnh ifconfig:

```
# ifconfig eth0 192.168.0.75 up
# ifconfig eth0
eth0 Link encap:Ethernet  HWaddr 00:A0:24:56:E3:73
     inet addr:192.168.0.75 Bcast:192.168.0.255 Mask:255.255.255.0
     inet6 addr: fe80::2a0:24ff:fe56:e373/64 Scope:Link
     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
     RX packets:0 errors:0 dropped:0 overruns:0 frame:0
     TX packets:6 errors:0 dropped:0 overruns:0 carrier:6
     collisions:0 txqueuelen:100
     RX bytes:0 (0.0 b)  TX bytes:460 (460.0 b)
     Interrupt:5 Base address:0xd800
```

- Sau khi cấu hình card mạng, sử dụng lệnh ifconfig cũng để xem các thuộc tính cấu hình

Cấu hình card mạng sử dụng ifconfig

```
# ifconfig eth0 192.168.0.75 netmask 255.255.255.192 textbackslash
>      broadcast 192.168.0.64
# ifconfig eth0
eth0 Link encap:Ethernet  HWaddr 00:A0:24:56:E3:73
     inet addr:192.168.0.75 Bcast:192.168.0.64 Mask:255.255.255.192
     inet6 addr: fe80::2a0:24ff:fe56:e373/64 Scope:Link
<<<<<

# ifconfig lo 127.0.0.1 up

# ifconfig eth0:0 192.168.0.111
# ifconfig eth0:0
eth0:0 Link encap:Ethernet  HWaddr 00:A0:24:56:E3:72
     inet addr:192.168.0.111 Bcast:192.168.0.255 Mask:255.255.255.0
     UP BROADCAST MULTICAST  MTU:1500  Metric:1
     Interrupt:5 Base address:0xd800
```

Cấu hình định tuyến sử dụng route

- Mọi máy tính trong mạng TCP/IP đều yêu cầu định tuyến.
- Lệnh route dùng để xem, chỉnh sửa và quản lý Bảng định tuyến.
    - Cho phép định nghĩa đường đi mặc định theo ý người quản trị.
    - Cho phép điều chỉnh default gateway theo ý muốn.
    - Cấu hình định tuyến tĩnh
- Trước khi chỉnh sửa bảng định tuyến trên Linux, lưu ý là nếu route thông tin sai sẽ khiến cho hệ thống không thể truy cập được và lúc này sẽ phải truy cập console của hệ thống nhằm chỉnh sửa tay.
- Các thông tin route được cấu hình bằng lệnh route trên Linux chỉ có tác dụng hiện hữu trên OS vận hành cho đến khi hệ thống reboot thì sẽ mất hết thôn tin.
- Nếu muốn cấu hình route mang tính vĩnh viễn kể cả khi reboot OS, phải cấu hình trong tệp cấu hình.

Cấu hình định tuyến sử dụng route

- Bảng định tuyến chứa các quy tắc (các tuyến đường) mô tả các datagram nào sẽ được gửi ở đâu, dựa trên địa chỉ đích của chúng

```
# ifconfig eth0 192.168.0.75
# route
Kernel IP routing table
Destination  Gateway Genmask       Flags Metric Ref Use Iface
192.168.0.0  *       255.255.255.0 U     0      0   0   eth0
```

- Cú pháp route:

```
route add [-net|-host] ⟨destination⟩ [netmask ⟨netmask⟩]▷
 ◁     [gw ⟨gateway⟩] [[dev] ⟨interface⟩]
route del [-net|-host] ⟨destination⟩ [netmask ⟨netmask⟩]▷
 ◁     [gw ⟨gateway⟩] [[dev] ⟨interface⟩]
```

```
# route add -net 192.168.0.0 netmask 255.255.255.0 dev eth0
# route add -net 192.168.2.0 netmask 255.255.255.0 dev eth1
# route add -net 10.10.3.0 netmask 255.255.255.0 gw 192.168.0.1
# route add -host 112.22.3.4 dev ppp0
# route add default dev ppp0
```

Cấu hình mạng sử dụng ip

- Lệnh ip có thể được sử dụng để thiết lập cả giao diện và định tuyến mạng

```
ip [⟨options⟩] ⟨object⟩ [⟨command⟩ [⟨parameters⟩]]
```

```
# ip addr show dev eth0
2: eth0: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo-fast qlen 100
        link/ether 00:a0:24:56:e3:72 brd ff:ff:ff:ff:ff:ff
        inet 192.168.2.1/24 brd 192.168.2.255 scope global eth0
# ip link set up dev eth0
# ip addr show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo-fast qlen 100
        link/ether 00:a0:24:56:e3:72 brd ff:ff:ff:ff:ff:ff
        inet 192.168.2.1/24 brd 192.168.2.255 scope global eth0
        inet6 fe80::2a0:24ff:fe56:e372/64 scope link
```

```
# ip addr add 192.168.0.222/24 dev eth0 brd + label eth0:0
```

```
# ip route add 192.168.2.1 via 192.168.0.254
# ip route del 192.168.2.1
```

Cấu hình mạng sử dụng netplan

- Cấu hình địa chỉ ip tính, chỉnh sửa tệp tin: /etc/netplan/*_config.yaml

```
network:
  version: 2
  renderer: networkd
  ethernets:
    eth0:
      addresses:
        - 10.10.10.2/24
      gateway4: 10.10.10.1
      nameservers:
          search: [mydomain, otherdomain]
          addresses: [10.10.10.1, 1.1.1.1]
```

Tệp tin /etc/hosts

- Giống như tệp hosts trên Windows (C:\Windows\System32\drivers\etc\hosts)
- Ánh xạ giữa địa chỉ IP và tên máy tính.
  - Đóng vai trò như một DNS cục bộ
  - **Cú pháp** : IP FQDN host
  - Ví dụ : 192.168.1.10 cse.tlu.edu.vn kitudu
- Các ứng dụng sẽ ưu tiên tìm tới tệp này khi cần truy vấn máy tính theo tên

Tệp tin /etc/hosts.allow - /etc/hosts.deny

- Tệp tin cấu hình cho phép (allow) hoặc cấm (deny) máy tính được truy cập:
  - **Cú pháp**: [tên dịch vụ]:[host]
  - **Ví dụ**: trong tệp tin /etc/hosts.allow
    - ALL: 192.168.1.1 ⇨ Cho phép máy tính với địa chỉ 192.168.1.1 được phép truy cập tất cả các dịch vụ.
    - proftpd: 192.168.1.2, 192.168.1.3 ⇨ Cho phép các máy tính 192.168.1.2 và 192.168.1.3 được phép kết nối tới proftpd
  - Tệp tin hosts.allow được đọc trước tệp hosts.deny

Tệp tin /etc/resolv.conf

- Định nghĩa name server mà máy tính dùng để truy vấn phân giải tên miền.
- Một số cú pháp thông dụng:
  - domain:DNS domain của máy tính
    - Ví dụ: domain tlu.edu
  - nameserver: IP hoặc tên của nameserver mà máy tính sẽ sử dụng
    - Ví dụ: nameserver 192.168.1.1

Tệp tin /etc/services

- Chứa danh sách các Cổng (Port) và các dịch vụ sử dụng các Cổng này
- Khi định nghĩa 1 services mới, phải định nghĩa 1 cặp gồm [service name] và [post/protocol]
  - Ví dụ: http 80/tcp
- Port 1 – 1024: dành riêng
- Port 1025 trở đi được phép sử dụng thêm vào

```
ktdung@ktdung:~$ cat /etc/services  | grep 80
http            80/tcp          www             # WorldWideWeb HTTP
socks           1080/tcp                        # socks proxy server
socks           1080/udp
http-alt        8080/tcp        webcache        # WWW caching service
http-alt        8080/udp
nbd             10809/tcp                       # Linux Network Block Device
amanda          10080/tcp                       # amanda backup services
amanda          10080/udp
omirr           808/tcp         omirrd          # online mirror
omirr           808/udp         omirrd
canna           5680/tcp                        # cannaserver
zope-ftp        8021/tcp                        # zope management by ftp
tproxy          8081/tcp                        # Transparent Proxy
omniorb         8088/tcp                        # OmniORB
omniorb         8088/udp
ktdung@ktdung:~$ _
```

Lệnh traceroute, netstat, tcpdump

- **traceroute**: theo dõi đường đi của gói tin trên mạng

  sudo apt-get install traceroute

```
traceroute to tlu.edu.vn (203.113.135.55), 30 hops max, 60 byte packets
 1  gateway (192.168.1.1)  1.243 ms  1.231 ms  1.220 ms
 2  100.123.0.183 (100.123.0.183)  5.172 ms  5.975 ms  6.829 ms
 3  42.112.1.187 (42.112.1.187)  7.580 ms  8.409 ms  8.401 ms
 4  100.123.0.167 (100.123.0.167)  7.542 ms  7.529 ms  8.299 ms
 5  42.112.0.91 (42.112.0.91)  9.036 ms  9.034 ms  9.757 ms
 6  113.22.4.110 (113.22.4.110)  7.412 ms  5.510 ms  5.487 ms
 7  203.113.158.105 (203.113.158.105)  5.479 ms  4.830 ms  6.510 ms
 8  localhost (27.68.228.37)  5.787 ms localhost (27.68.228.25)  8.646 ms  11.749 ms
 9  localhost (27.68.228.198)  7.565 ms  6.144 ms  7.433 ms
10  mail.wru.edu.vn (220.231.101.18)  8.324 ms  10.384 ms  8.195 ms
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  *
```

Lệnh traceroute, netstat, tcpdump

- **netstat**: liệt kê các cổng đang lắng nghe, kết nối đang mở đến máy tính và tình trạng kết nối.

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    24458    /run/user/1000/systemd/notify
unix  3      [ ]         DGRAM                    13573    /run/systemd/notify
unix  6      [ ]         DGRAM                    13599    /run/systemd/journal/dev-log
unix  8      [ ]         DGRAM                    13604    /run/systemd/journal/socket
unix  2      [ ]         DGRAM                    13979    /run/systemd/journal/syslog
unix  3      [ ]         STREAM     CONNECTED     19620
unix  3      [ ]         STREAM     CONNECTED     17037
unix  3      [ ]         STREAM     CONNECTED     14469    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     21390    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     18231    /run/systemd/journal/stdout
unix  2      [ ]         DGRAM                    16409
unix  2      [ ]         DGRAM                    14320
unix  3      [ ]         STREAM     CONNECTED     19763    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     19626    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     18228
unix  2      [ ]         DGRAM                    19071
```

- **tcpdump**: bắt gói tin di chuyển trong network

Các hướng dẫn cấu hình mạng

- https://www.tecmint.com/configure-network-static-ip-address-in-ubuntu/
- https://linuxconfig.org/how-to-switch-back-networking-to-etc-network-interfaces-on-ubuntu-20-04-focal-fossa-linux

2. SSH server

SSH

- Giao thức truy cập từ xa bằng dòng lệnh
  - Dữ liệu truyền đi được mã hóa
- SSH lắng nghe ở cổng 22
- Chứng thực trên SSH:
  - Chứng thực rhosts
  - Chứng thực mật khẩu: Username và Password
  - Chứng thực RSA: sử dụng ssh-keygen và ssh-agent để chứng thực cặp khóa.

Cài đặt SSH

- sudo apt install ssh
- hoặc sudo apt install openssh*.
- Tệp cấu hình của SSH:
  - Server : /etc/ssh/sshd_config
  - Client : /etc/ssh/ssh_config

Công cụ SSH

- **ssh**: công cụ kết nối vào SSH server qua kênh truyền bảo mật
  - ssh [-l username] remotehost
- **scp**: công cụ sao chép tệp tin từ SSH server qua kênh truyền bảo mật
  - scp [username@]remotehost:/path_to_source /path_to_destination
- putty
- filezilla
- winscp
- sftp

Các hướng dẫn về SSH

- https://websiteforstudents.com/?s=SSH

Chứng thực SSH key

- https://www.digitalocean.com/community/tutorials/how-to-set-up-ssh-keys-on-ubuntu-1804

SSH File Transfer Protocol (SFTP)

- https://www.digitalocean.com/community/tutorials/how-to-enable-sftp-without-shell-access-on-ubuntu-18-04
- https://www.server-world.info/en/note?os=Ubuntu_18.04&p=samba&f=1

3. DHCP server

Mục tiêu

- Hiểu khái niệm DHCP và vai trò của DHCP server trong mạng.
- Hiểu quá trình phát sinh địa chỉ mới và quá trình xin gia hạn địa chỉ cũ.
- Cài đặt được DHCP server trên Linux.
- Cấu hình và quản trị một DHCP server với các yêu cầu cơ bản.
- Cấu hình máy trạm Linux nhận địa chỉ IP động từ DHCP server.

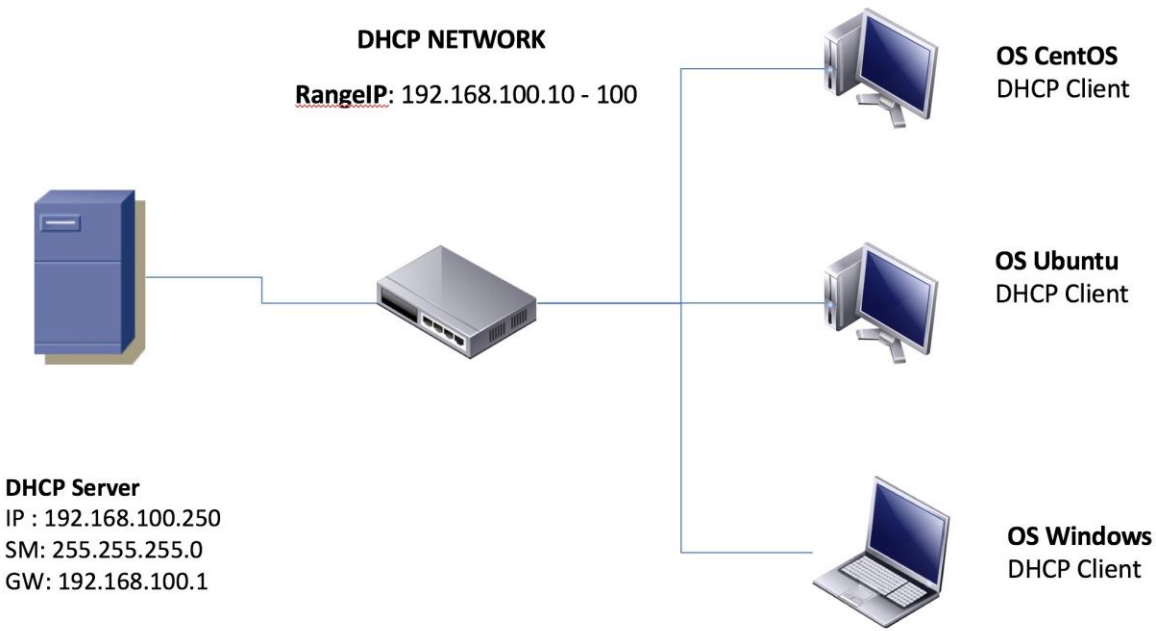
Nội dung

- Cơ bản về DHCP
- Quá trình cấp phát IP
- Cài đặt DHCP server
- Cấu hình DHCP server
- Quản trị DHCP server
- Cấu hình DHCP client

DHCP – Giới thiệu

- DHCP = Dynamic Host Configuration Protocol (Tiền thân: BOOTP)
- Hoạt động: tầng ứng dụng trong mô hình OSI
- Chức năng: cấp phát địa chỉ IP động
- Mô hình Client - Server:
  - Server
    - Port: 67
    - Cung cấp địa thông tin cấu hình TCP/IP cho các client
  - Client:
    - Port: 68
    - Yêu cầu server cấp thông tin cấu hình TCP/IP

DHCP – Giới thiệu



DHCP là dịch vụ cung cấp địa chỉ IP động cho các máy tính trong hệ thống.
DHCP cũng cung cấp động các tham số khác: DNS, gateway

Vì sao dùng DHCP?

- DHCP làm giảm độ phức tạp và chi phí quản trị vì sử dụng quá trình cấu hình TCP/IP động

Cấu hình thủ công

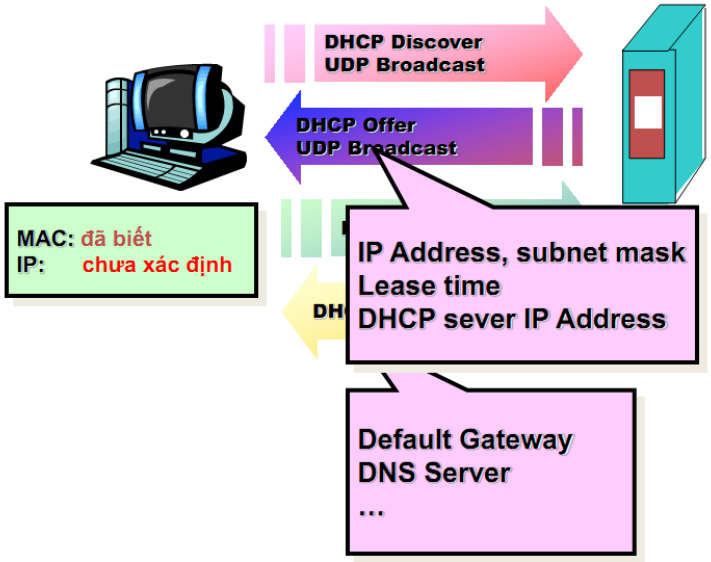
- Địa chỉ IP được gán bằng tay trực tiếp trên từng máy trạm.
- Khả năng gán sai địa chỉ IP cao.
- Việc cấu hình sai có thể dẫn đến nhiều vấn đề trong truyền thông và mạng.
- Chi phí quản trị tăng cao trong mạng có các máy tính thường xuyên thay đổi.

Cấu hình tự động

- Địa chỉ IP được cấp phát tự động xuống máy trạm.
- Đảm bảo tất cả các máy trạm được cấu hình đúng.
- Cấu hình tại máy trạm được cập nhật động khi có sự thay đổi trong cấu trúc mạng.
- Loại các bỏ nguy cơ cơ bản trên mạng

DHCP – Mô hình hoạt động

- Xin cấp mới:
  - Discover: client tìm DHCP Server
  - Offer: DHCP gợi ý một địa chỉ IP
  - Request: Client yêu cầu cấp 1 địa chỉ IP
  - Ack: Server xác nhận đồng ý và giải phóng địa chỉ IP
- Xin cấp lại:
  - Request
  - Ack
- Huỷ thông tin được cấp:
  - Release

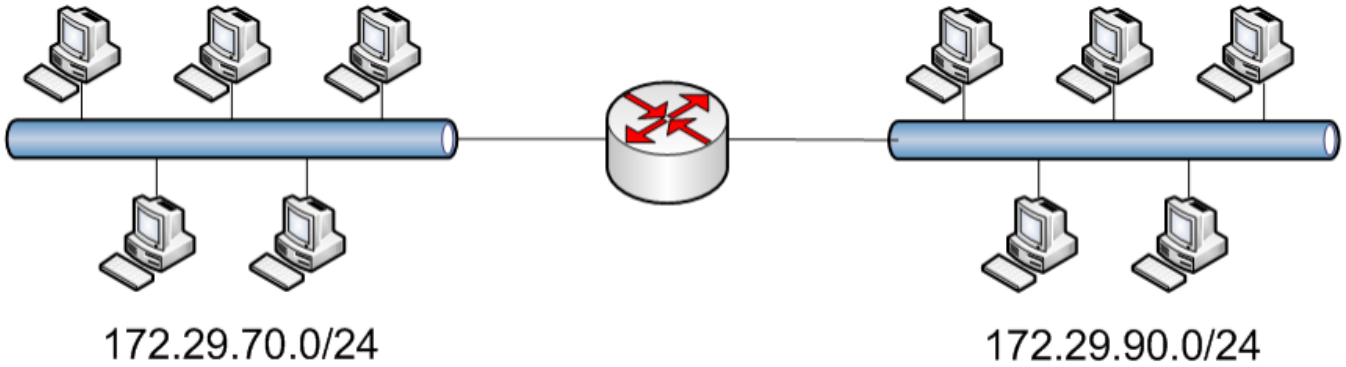


Cài đặt DHCP

- https://linuxhint.com/install_dhcp_server_ubuntu/

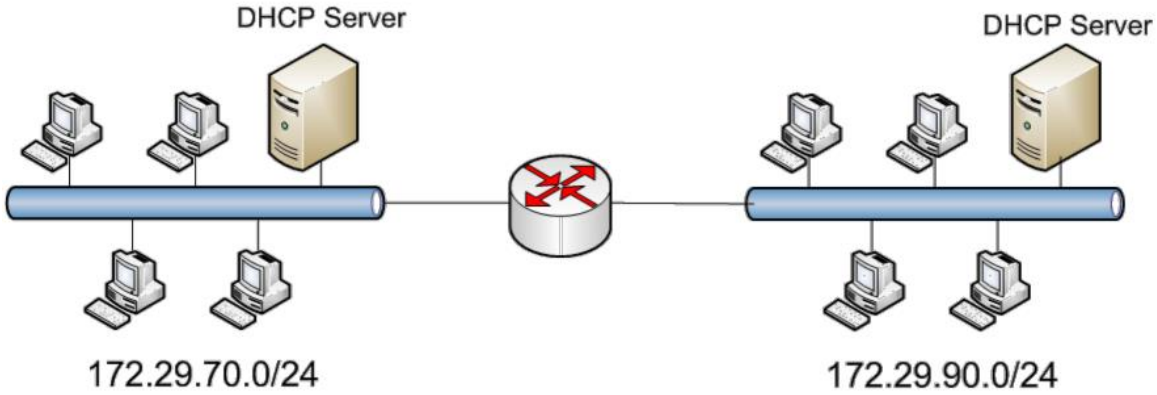
Bài toán

- Triển khai dịch vụ DHCP để các máy trong đường mạng 172.29.70.0/24 và 172.29.90.0/24 có thể xin IP động



Giải pháp 01

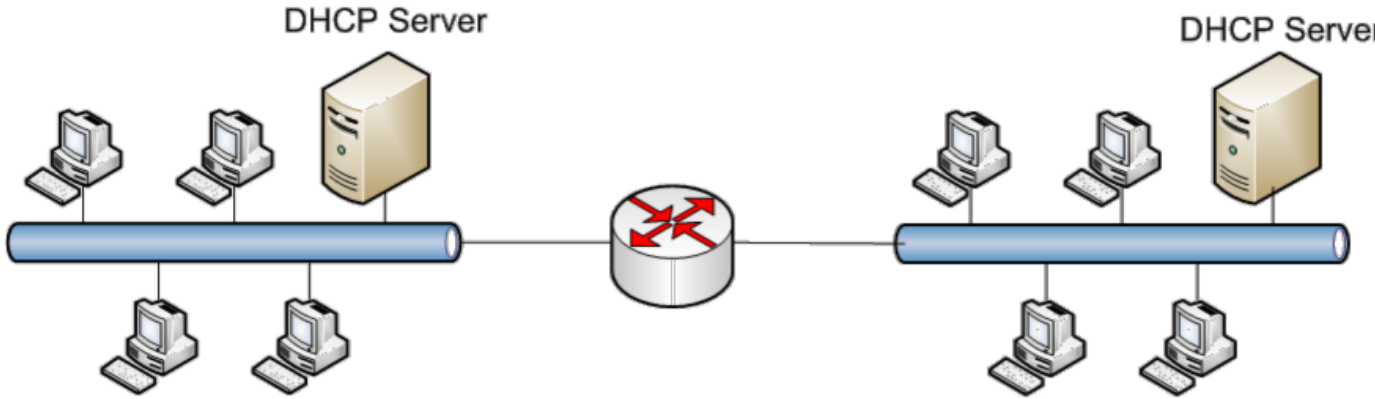
- DHCP trên mỗi Segment



Giải pháp 01

- Xác định tham số:
  - Dãy IP mà server sẽ cấp cho các client yêu cầu
    - Start IP – End IP
    - Subnet mask
  - Địa chỉ IP không được cấp tự động (Exclusions Range)
  - Default gateway, DNS, ...
  - Địa chỉ dành riêng (Reservation)

Giải pháp 01



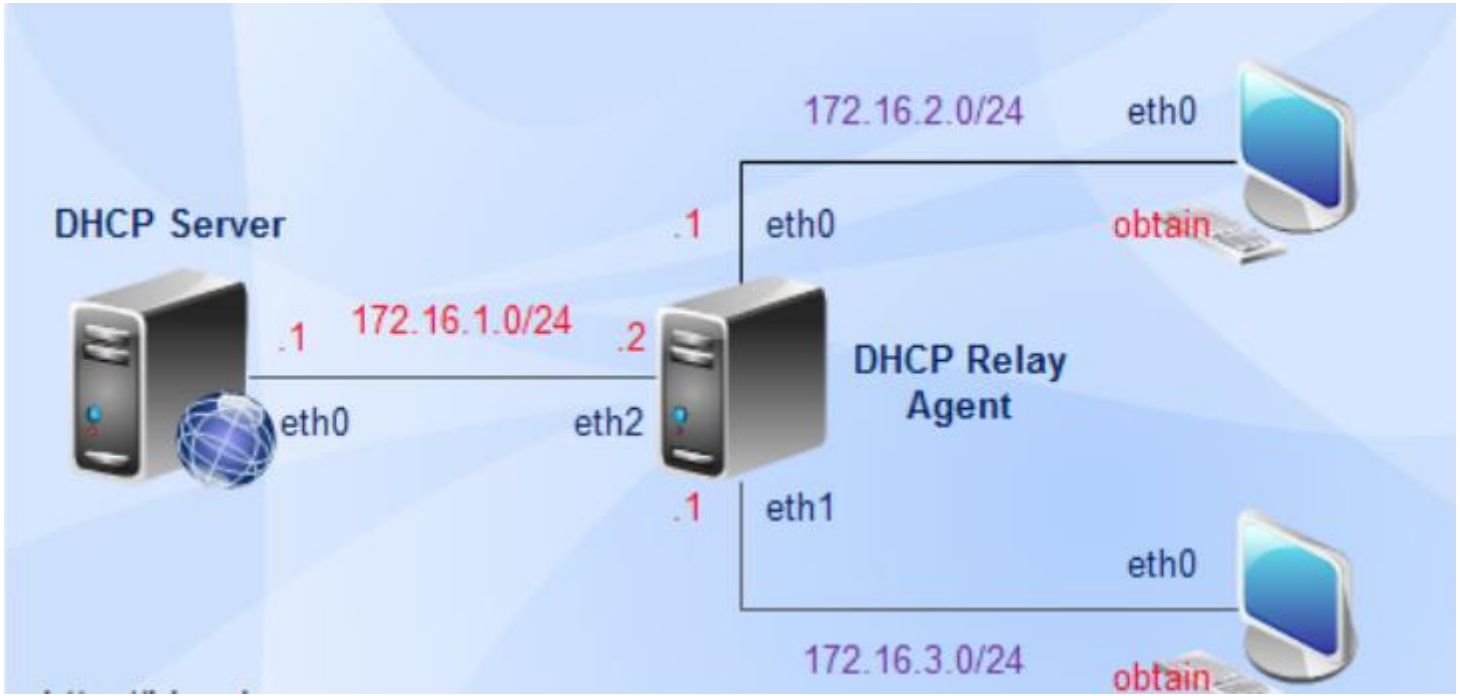
Range: 172.29.70.x – 172.29.70.y
Subnetmask: /24
Default gateway: .....

Range: 172.29.90.x – 172.29.90.y
Subnetmask: /24
Default gateway: .....

Giải pháp 01

- Có nhiều segment mạng
- Cần nhiều DHCP server
- Tốn kém: bảo trì + phần cứng
- **Giải pháp**: DHCP Relay Agent

Giải pháp 02: DHCP Relay Agent



Giải pháp 02: DHCP Relay Agent

- https://github.com/hocchudong/thuctap012017/blob/master/TamNT/DHCP/LAB%20DHCP%20server%20%20-%20DHCP%20Relay%20Agent.md

Hướng dẫn cài đặt DHCP server

- https://www.server-world.info/en/note?os=Ubuntu_18.04&p=dhcp&f=1

4. DNS Server

Cài đặt DNS server

- https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-private-network-dns-server-on-ubuntu-18-04
- https://www.server-world.info/en/note?os=Ubuntu_18.04&p=dns&f=1

Cài đặt DNS server

- Cài đặt dịch vụ DNS bằng các gói bind
  - bind-utils-[version]
  - bind-libs-[version]
  - bind-[version]
- File cấu hình chính của dịch vụ DNS:
  - /etc/bind/named.conf

5. Web Server

Mục tiêu

- Hiểu khái niệm WWW và vai trò của Web server trong mạng.
- Hiểu cách thức hoạt động của WWW.
- Cài đặt được Web server trên Linux.
- Cấu hình và quản trị một Web server với các yêu cầu cơ bản.

Nội dung

- Giới thiệu dịch vụ Web.
- Giới thiệu Apache.
- Cài đặt Apache.
- Cấu hình Apache
- Access control
- Log Files
- Performance

Apache

- Nhiều phần mềm được sử dụng để hiện thực tính năng của web server: IIS, Apache...
- Apache là một phần mềm mã nguồn mở được sử dụng để làm web server phổ biến nhất trên Linux.
- Apache tương thích với hầu hết hệ điều hành UNIX, và cả Windows.
- Apache hoạt động linh hoạt, cho phép mở rộng nhiều tính năng, có thể biên dịch thêm nhiều module từ: https://httpd.apache.org/docs/2.4/mod

Cài đặt Apache và Web server

- https://websiteforstudents.com/?s=web+server
- https://www.server-world.info/en/note?os=Ubuntu_18.04

Cấu hình Apache

- Tệp tin cấu hình:
  - /etc/apache2/sites-available/000-default.conf

Cài đặt Web server

- https://websiteforstudents.com/?s=web+server

Điều khiển truy cập

- Access control giúp kiểm tra user nào được phép truy cập trang web.
- User có thể truy cập trang web nào, không thể truy cập trang web nào.
- Có thể giới hạn truy cập qua dãy IP của user.
- Có thể giới hạn truy cập bằng cách chỉ chấp nhận những user đã được xác thực (valid user).
- Có thể giới hạn truy cập qua thông tin users. Những user được kiểm tra username/pass đúng mới được truy cập.

Log Files

- access_log – liệt kê từng request truy cập vào trang web.
- agent_log – liệt kê những chương trình được web server gọi chạy. Log này là option, có thể chọn lúc biên dịch apache, hoặc cấu hình trực tiếp trong file cấu hình httpd.conf
- error_log – Lỗi phát sinh trong quá trình chạy của web server.
- refer_log – liệt kê những URL trước đó browser đã sử dụng. Log này cũng là option, có thể chọn trong khi biên dịch, khi cấu hình, hoặc có thể không cấu hình.

Virtual Host

- Lưu trữ nhiều tên miền (với việc xử lý riêng từng tên) trên một máy chủ (hoặc nhóm máy chủ).
- Cho phép một máy chủ chia sẻ tài nguyên của nó, như chu kỳ bộ nhớ và bộ xử lý, mà không yêu cầu tất cả các dịch vụ được cung cấp để sử dụng cùng tên máy chủ.

```
<VirtualHost *:80>
    ServerAdmin admin@example.com
    ServerName example.com
    ServerAlias www.example.com
    DocumentRoot /var/www/example.com/public_html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Virtual Directory

- Cho phép truy cập dạng: http://example.com/~user/
  - https://httpd.apache.org/docs/2.4/mod/mod_userdir.html
  - https://www.server-world.info/en/note?os=Ubuntu_18.04&p=httpd&f=6

Cấu hình ssl (https)

- Cho phép truy cập dạng: https://example.com
- https://www.server-world.info/en/note?os=Ubuntu_18.04&p=httpd&f=8

6. FTP Server

Hướng dẫn cài đặt và cấu hình

- https://www.server-world.info/en/note?os=Ubuntu_18.04&p=ftp&f=1
- https://websiteforstudents.com/?s=FTP+server

7. Mail Server

Hướng dẫn cài đặt và cấu hình

- https://www.server-world.info/en/note?os=Ubuntu_18.04&p=mail&f=1
- https://websiteforstudents.com/?s=Mail+server

8. Samba Server

Hướng dẫn cài đặt và cấu hình

- https://www.server-world.info/en/note?os=Ubuntu_18.04&p=samba&f=1
- https://websiteforstudents.com/?s=samba+server