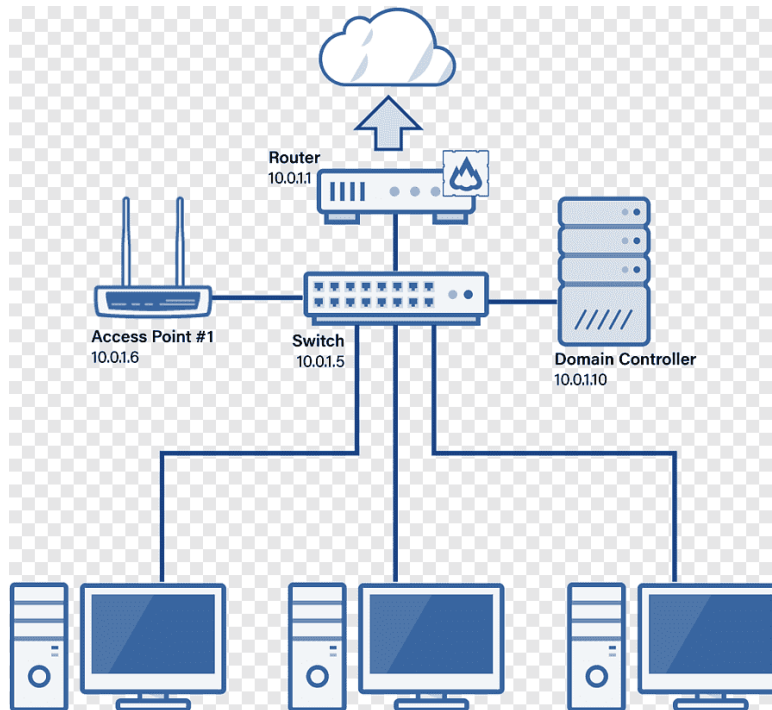


Nguyên lý mạng máy tính

Mạng cục bộ (LAN) là mạng có phạm vi hẹp dùng trong một tổ chức, cơ quan hoặc một căn nhà cũng có khi là cả một khu vực rộng lớn. Đặc điểm chính của mạng cục bộ là **các máy tính có thể kết nối trực tiếp với nhau thông qua IP cục bộ** thường có dạng 192.168.x.x, 10.0.x.x hay 10.1.x.x.



Hình trên là sơ đồ giản lược của một mạng LAN. Mạng LAN nào cũng có 4 thành phần cốt lõi là **MODEM, ROUTER, SWITCH và MÁY TÍNH**.

- MODEM dùng để chuyển tín hiệu analog (ánh sáng, điện) sang tín hiệu kỹ thuật số. Ngày nay, MODEM được tích hợp trực tiếp vào ROUTER.
- ROUTER dùng để định hướng gói tin, nó giống một điểm trung chuyển trong giao thông. Các gói tin đi từ một máy tính trước khi muốn đi đến một máy khác trong INTERNET phải đi qua ROUTER để được ROUTER dẫn đường đến ROUTER khác và đến máy đích. Ngoài nhiệm vụ chỉ đường ROUTER còn cấp phát IP cho các máy khác trong mạng LAN mà nó quản lý bằng cách dùng server DHCP cài sẵn trong nó. ROUTER cũng là một loại máy tính đặc biệt. Một máy tính cũng có thể cấu hình và lập trình để trở thành ROUTER.
- SWITCH là thiết bị cho phép các máy tính kết nối vào nó có thể giao tiếp trực tiếp với nhau, nó gần giống USB hub hoặc mấy nút giao thông như ngã 4, 5. Ngày nay SWITCH cũng được tích hợp trực tiếp vào ROUTER.
- MÁY TÍNH là thiết bị tạo, nhận, xử lý gói tin. Trong máy tính có phần mềm Trình duyệt để tạo ra gói tin sau đó gửi gói tin đi bằng driver mạng thông qua card mạng.

Tất cả các thiết bị ở trên đều có IP cục bộ riêng biệt được cấp bởi ROUTER và chúng có thể giao tiếp trực tiếp với nhau qua IP đó. Mạng LAN được đặc trưng bởi 2 yếu tố là **DEFAULT GATEWAY** và **SUBNET MASK** và cả 2 yếu tố này đều được đặt trong ROUTER, lưu trữ bởi ROUTER và quy định bởi ROUTER. DEFAULT GATEWAY cũng chính là địa chỉ IP cục bộ của ROUTER. SUBNET MASK dùng để xác định xem một IP cục bộ của một thiết bị khác có nằm trong mạng LAN này không.

Ví dụ một mạng có DEFAULT GATEWAY là 192.168.1.1 và SUBNET MASK là 255.255.255.0. Một máy tính trong mạng LAN này muốn gửi tin đến máy tính có IP 192.168.1.20. ROUTER muốn biết xem IP này có phải IP cục bộ của mạng LAN này không thì cho 2 máy kết nối trực tiếp với nhau thông qua SWITCH nếu không thì định hướng gói tin này ra bên ngoài LAN (ra INTERNET) để cho các ROUTER khác chỉ đường đến 192.168.1.20

Cách xác định rất đơn giản nếu IP cục bộ kia có cùng địa chỉ mạng với địa chỉ mạng của DEFAULT GATEWAY thì IP cục bộ đó nằm trong mạng LAN của con ROUTER này quản lý. Địa chỉ mạng được xác định SUBNET MASK, SUBNET MASK ở đây là 255.255.255.0 nghĩa là có 24 bit 1 (vì 11111111.11111111.11111111.00000000).

Nghĩa là ta sẽ lấy 24 bit đầu tiên của DEFAULT GATEWAY làm địa chỉ mạng. Vậy địa chỉ mạng của 192.168.1.1 là 192.168.1.0. Tương tự địa chỉ mạng của 192.168.1.20 cũng là 192.168.1.0 vậy IP này nằm trong mạng. Ví dụ có 1 IP khác là 192.168.2.30 thì địa chỉ mạng là 192.168.2.0, suy ra nó không nằm trong mạng LAN do ROUTER này quản lý.

Một IP đặc biệt là 127.0.0.1 IP này không được cấp phát bởi bất kỳ LAN nào hay INTERNET. Khi gửi 1 gói tin đến IP này, gói tin sẽ quay trở lại máy gửi. Tự gọi bản thân :) IP này dùng trong việc test, lập trình web, ứng dụng.

Vậy INTERNET trong thực tế lại là mạng của các mạng LAN. Các mạng LAN trong INTERNET giờ đây lại được coi giống như 1 “MÁY TÍNH” trong mô hình mạng LAN ở trên và các “MÁY TÍNH” này cũng được quản lý bởi một hay nhiều ROUTER khác, gần giống kiểu “đa cấp” :)

Trong INTERNET mỗi LAN cũng có IP của riêng nó do ROUTER quản lý các LAN cấp và được ROUTER của chính LAN đó lưu trữ. Như vậy 1 ROUTER phải lưu 2 IP, 1 IP cục bộ của LAN mà nó quản lý hay DEFAULT GATEWAY và 1 IP đại diện cho toàn bộ LAN đó được cấp bởi 1 ROUTER level cao hơn. Trong trường hợp một LAN được cấp IP tĩnh thì ROUTER đó liên kết trực tiếp với ROUTER tổng của nhà mạng và được nhà mạng cấu hình cố định thay vì được cấp phát động bởi DHCP. Các IP tĩnh này được quản lý bởi tổ chức IANA. Hiện nay số lượng IP tĩnh trên toàn cầu đang dần cạn kiệt nên IP version 6 ra đời, nếu dùng IP version 6 thì gần như máy nào cũng là IP tĩnh mà ko cần cơ chế cấp phát động, việc liên kết sẽ đơn giản hơn :) .

Một số định nghĩa khác

Firewall: Firewall hay tường lửa là phần mềm cài đặt trong router nó nằm giữa INTERNET và ROUTER nhằm ngăn chặn gói tin độc, gói tin không mong muốn thâm nhập từ INTERNET vào LAN. Các gói tin khi từ INTERNET đi qua ROUTER đều được Firewall kiểm duyệt.

Port: Cổng là một định nghĩa trừu tượng, các phần mềm của máy tính đều chạy trên 1 cổng riêng biệt, mỗi một cổng của máy tính là 1 dịch vụ. Thay vì phải chia mỗi dịch vụ cho nhiều máy nhiều ip thì 1 máy có thể chạy nhiều dịch vụ và cung cấp các dịch vụ đó thông qua cổng như vậy chỉ cần gọi IP:PORT là có thể gọi được dịch vụ tương ứng. ví dụ mặc định cổng 80 của máy tính là http, khi gõ IP lên trình duyệt thì nó cũng mặc định chạy vào cổng 80, cổng 22 của secure shell, cổng 21 của FTP, cổng 433 của https. Một máy tính có tối đa 65535 cổng từ 0 - 65534. Cổng 5000, 3000, 8888, 8000 hay dùng để test web :)

Forward Port: Như đã nói từ trước ROUTER là 1 loại máy tính và nó cũng có cổng. Có thể cấu hình để một cổng của ROUTER gọi đến dịch vụ của 1 máy tính khác trong mạng LAN mà ROUTER đó quản lý thông qua IP và cổng của dịch vụ nằm trên máy tính đó. ví dụ cổng 3000 của ROUTER sẽ gọi đến dịch vụ nằm trên cổng 5000 của máy 192.168.1.19. Phương pháp này hay được dùng khi ta có 1 ROUTER với IP đại diện cho LAN trên INTERNET là IP tĩnh. Thì có thể forward cổng của ROUTER này đến 1 máy trong LAN để máy đó trở thành máy chủ. Hoặc forward port đến Camera trong LAN để trở thành camera IP tiện lợi. Việc này giúp mapping giữa IP đại diện cho LAN trên INTERNET và IP cục bộ của máy tính nằm trong LAN.

Proxy server: Giống khi gửi thư tình :) nếu không muốn gửi trực tiếp thì có thể gửi thông qua bạn thân. Proxy server cũng là một máy tính, nó là máy tính dịch vụ nằm giữa LAN và INTERNET. Proxy server sẽ thay mặt người dùng gửi request đến 1 máy trên INTERNET và trả về kết quả cho máy trong LAN.

DNS: Server này là một máy tính nằm trên INTERNET có nhiệm vụ đổi tên miền sang địa chỉ IP tĩnh. Các DNS hay dùng là 1.1.1.1 của Cloudflare, 8.8.8.8 của Google

DHCP server: Server này cung cấp dịch vụ cấp phát IP động cho các máy trong LAN do đó nó được cài đặt trực tiếp trong ROUTER quản lý LAN đó. Lên wiki tìm hiểu thêm thuật toán cấp phát IP động khá hay :) Một máy cũng có thể có IP tĩnh cục bộ trong LAN bằng cách disable lựa chọn dùng DHCP trên máy đó và config IP tĩnh bằng tay. Chú ý IP tĩnh phải thỏa mãn điều kiện để thuộc LAN như ở trên nếu không ROUTER sẽ không chấp nhận máy đó. Ví dụ mạng LAN của VKIST có DEFAULT

GATEWAY 10.1.8.1 và SUBNET MASK 255.255.0.0 thì config IP tĩnh cho server là 10.1.8.100 hay 10.1.9.100 đều được

Secure Shell: secure shell hay ssh là một dịch vụ cung cấp bởi máy tính cho phép máy tính khác điều khiển nó thông qua giao diện dòng lệnh (shell). Cổng mặc định của ssh là cổng 22. Điều khiển máy tính thông qua ssh rất bảo mật. Trong trường hợp máy tính không cùng LAN thì phải có IP tĩnh để kết nối 2 máy.

TCP/UDP: là các giao thức truyền gói tin trên mạng máy tính bằng cách sử dụng địa chỉ IP. Các giao thức này thuộc tầng giao vận của mạng.

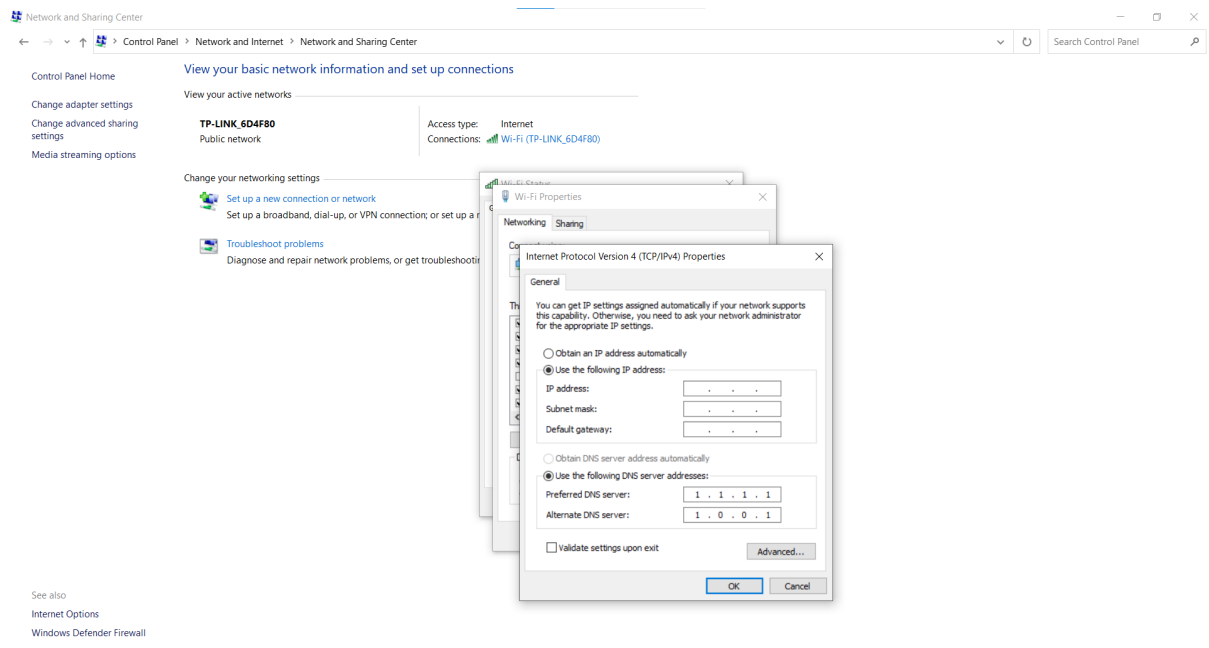
HTTP/HTTPS/FTP/SMTP: lần lượt là các dịch vụ siêu văn bản, siêu văn bản bảo mật, truyền tệp tin, gửi mail. Các dịch vụ này được lập trình dựa trên giao thức TCP/UDP. Các dịch vụ này thuộc tầng dịch vụ của mạng. Các dịch vụ này có các cổng mặc định riêng trên máy tính.

Tunneling: Cơ chế đường hầm là một cơ chế đặc biệt giúp cho 2 máy tính khác LAN có thể kết nối với nhau mà không cần IP tĩnh. Cơ chế này được thực hiện bằng một Proxy server đặc biệt, Proxy server này có địa chỉ IP tĩnh và đóng vai trò như một người trung gian để giao tiếp giữa 2 máy. Hoặc proxy server này sẽ đóng vai trò như 1 router sẽ tìm đường và thứ tự các Router để liên kết 2 máy tính IP động khác LAN. Cơ chế này được sử dụng trong Teamviewer hoặc Ngrok.

Một số lưu ý

- 2 máy tính khác LAN bắt buộc 1 trong 2 máy phải có IP tĩnh mới kết nối được với nhau. Đơn giản vì có hàng trăm nghìn IP động của các LAN khác nhau giống nhau nhưng IP tĩnh chỉ có 1. Ngoài ra muốn kết nối với IP tĩnh thì máy có IP tĩnh cùng với ROUTER của nó phải tắt hết Firewall.
- Một ROUTER1 kết nối vào một ROUTER2 khác thì 2 ROUTER đó cùng 1 LAN và ROUTER1 là 1 LAN con của ROUTER2 hay được gọi là subnet của ROUTER2. SUBNET MASK của subnet sẽ có phạm vi bé hơn SUBNET MASK của ROUTER2. Các máy tính của ROUTER1 hay ROUTER2 đều kết nối trực tiếp được với nhau do cùng 1 LAN.
- Giả sử ROUTER1 kết nối vào INTERNET và ROUTER2 cũng kết nối vào INTERNET thì 2 ROUTER này quản lý 2 LAN khác nhau. Máy tính trong LAN của ROUTER1 quản lý sẽ không thể gọi đến máy tính trong LAN của ROUTER2 quản lý. => Bắt buộc phải có IP tĩnh hoặc Tunneling :)))
- Config IP tĩnh trong LAN rất đơn giản giống như đã nói ở trên chỉ cần Disable DHCP server trên máy tính muốn có IP tĩnh cục bộ trong LAN. Ảnh dưới là ví

dụ với Window (bỏ chọn obtain an ip address automatically sau đó set ip thủ công)



Một số lệnh hữu ích cho networking của Window và Linux

ping: lệnh này giúp kiểm tra kết nối giữa máy này và máy đích. lệnh ping sẽ gửi đi 4 gói tin tcp đến máy đích và nhận về 4 gói tin tcp. Trong trường hợp nhận đủ 4 gói thì kết nối thành công.

ifconfig (Linux) / ipconfig (Window): Lệnh này giúp kiểm tra thông tin kết nối mạng của máy tính. Dùng lệnh này để kiểm tra DEFAULT GATEWAY, SUBNET MASK của mạng LAN mà máy kết nối đến và IP cục bộ hiện tại của máy. Ngoài ra còn có thể check được thông tin thiết bị kết nối mạng, đối với wifi là Wi-Fi mạng dây có thể là eth0 hoặc eth1.

route (Linux): Lệnh này giúp kiểm tra DEFAULT GATEWAY

nmap: Lệnh này giúp tìm tất cả các port đang mở của 1 IP, rất hay

wget: Lệnh tải file từ mạng về dùng url hoặc IP

tracert (Linux) / traceroute (Window): Lệnh này giúp show quãng đường mà gói tin đã di chuyển, các ROUTER mà gói tin đã đi qua để đến máy đích theo thứ tự lần lượt. Đây chính là nguyên lý Proxy server tạo tunneling bằng cách traceroute đến máy 1 để lấy route1 sau đó traceroute đến máy 2 để lấy route2 sau đó kết hợp route1 và route2 để tạo ra 1 đường hầm kết nối giữa 2 máy mà không cần IP tĩnh.

netstat: Lệnh này để kiểm tra trạng thái kết nối mạng, các cổng đang hoạt động trong máy tính.

cd: Lệnh chuyển thư mục

ls (Linux): Lệnh liệt kê thư mục

cat (Linux): Lệnh đọc nội dung file

nano (Linux): Lệnh edit nội dung file

ps: Lệnh xem tất cả các process đang chạy

df: Lệnh xem thông tin bộ nhớ của máy

pwd: Lệnh xem thư mục hiện tại

systemctl (Linux): quản lý các service

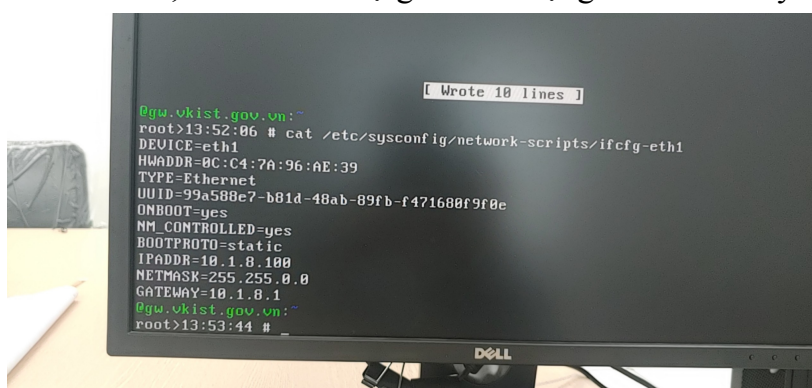
ssh: Lệnh điều khiển máy tính thông qua giao diện dòng lệnh bằng địa chỉ IP. Điều kiện 2 máy phải kết nối với nhau thông qua IP tĩnh, Tunnelling hoặc cùng LAN. Lệnh này cực kỳ hữu dụng trong hầu hết trường hợp. Có toàn quyền kiểm soát máy tính nếu được cấp quyền root. Có khả năng gọi cả các IP khác trong cùng mạng LAN với máy tính đang được điều khiển (đặc biệt là ROUTER). Khóa học 1 tiếng về ssh tại đây :)

<https://www.youtube.com/watch?v=hQWRp-FdTpc>

Một số quy trình hay gặp

Config IP Tĩnh trong LAN

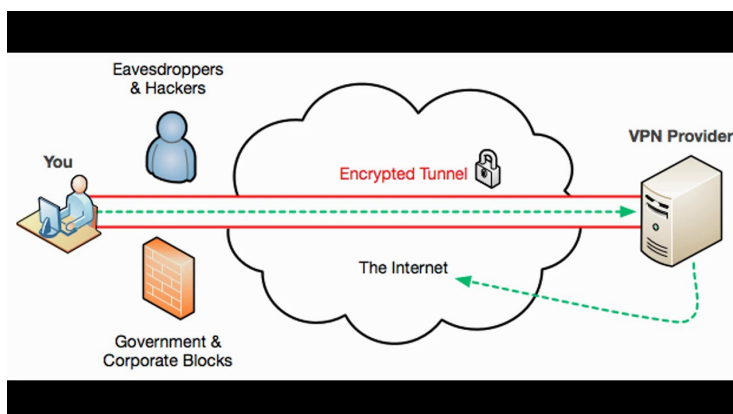
- **Window:** Control Panel => Network and Internet => Network and Sharing center => bấm vào mạng đã kết nối => Properties => Internet Protocol Version 4 => use the following address => sửa các tham số default gateway, ip address, subnet mask theo mạng LAN mà máy kết nối.
- **Linux:** ifconfig (xem thông tin kết nối mạng) => cd /etc/sysconfig/network-scripts/ (di chuyển vào thư mục chứa config mạng) => ls (xem có những thiết bị nào) => nano <thiết bị tương ứng trong ifconfig (ví dụ thiết bị eth1 kết nối mạng cho máy thì ghi ifcfg-eth1)> => sửa nội dung theo hình bằng cách dùng phím mũi tên để di chuyển (các tham số IPADDR, NETMASK, GATEWAY tự ghi theo mạng LAN mà máy kết nối)



Config Port Forward: Đầu tiên kiểm tra thông tin DEFAULT GATEWAY bằng cách dùng ifconfig/ipconfig. Sau đó mở trình duyệt Chrome gõ địa chỉ DEFAULT GATEWAY lên thanh địa chỉ để vào giao diện quản lý router. Trong giao diện quản lý router có mục Port Forwarding trong một số trường hợp mục đó có tên liên quan đến Forwarding hoặc Port hoặc IP hoặc NAT tùy từng ROUTER của các nhà sản xuất. Đối với ROUTER của Cisco là Port Forwarding. Các tham số cốt lõi luôn có là External Port là cổng mà máy bên ngoài gọi đến, Internal Port là cổng mà máy trong LAN cung cấp dịch vụ muốn forward cho cái cổng External Port, Internal IP địa chỉ IP cục bộ của máy cung cấp dịch vụ trong LAN. Như vậy nếu máy trên Internet hay máy người dùng khi gọi đến IP tĩnh của ROUTER kia trên INTERNET kèm cổng External Port (static_IP:External Port) thì cũng đồng nghĩa đang truy cập đến dịch vụ trên cổng Internal Port của máy Internal IP trong mạng LAN mà ROUTER kia quản lý.

ví dụ port forwarding trên ROUTER của TP-LINK

Tạo tunneling để kết nối khi chưa có static IP: Cách làm phổ biến là sử dụng Ngrok tại trang web <https://ngrok.com/>



SSH vào máy tính để điều khiển thông qua IP: Để có thể ssh máy tính được điều khiển cần có IP tĩnh, Tunneling hoặc nằm trong cùng LAN với máy điều khiển. tiến hành gõ lệnh trên giao diện dòng lệnh cmd hoặc terminal

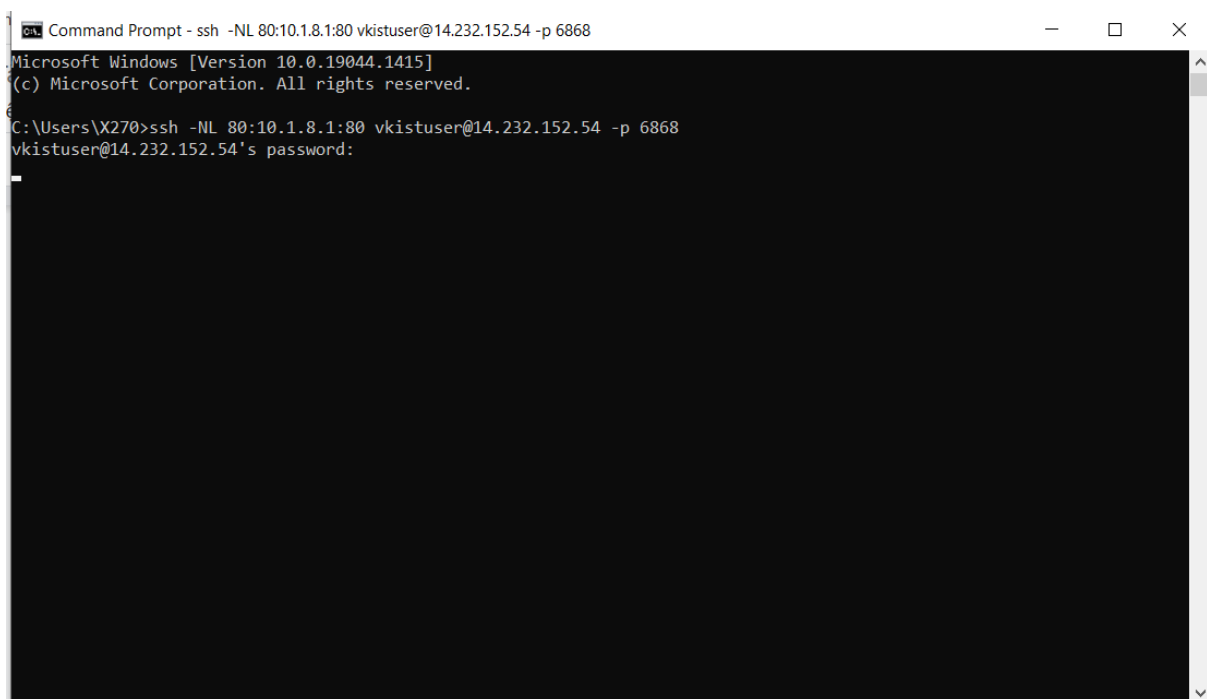
`ssh <username>@<ip> -p <port>`

Trong đó <username> là tên đăng nhập vào máy tính được điều khiển <ip> là địa chỉ ip của máy có thể kết nối, <port> là cổng cung cấp dịch vụ ssh mặc định là 22

Sau khi enter, tiến hành nhập mật khẩu là kết nối đã hoàn tất và có thể điều khiển máy tính. Để forward giao diện ROUTER mạng LAN của máy được điều khiển vào cổng 80 máy điều khiển tiến hành gõ lệnh

`ssh -NL 80:<default gateway>:80 <username>@<ip> -p <port>`

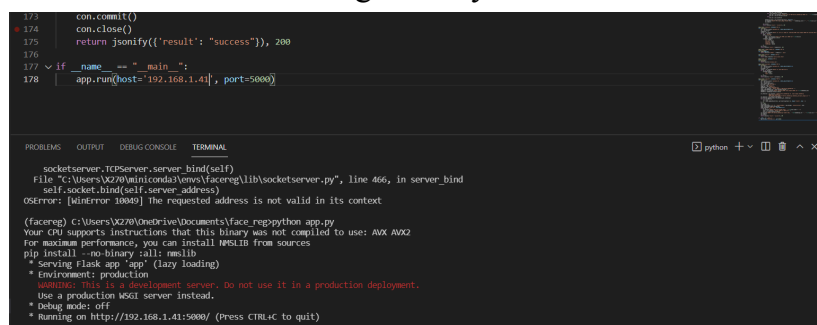
Trong đó <default gateway> là DEFAULT GATEWAY của mạng LAN mà máy được điều khiển kết nối đến. ví dụ hình dưới



```
Command Prompt - ssh -NL 80:10.1.8.1:80 vkistuser@14.232.152.54 -p 6868
Microsoft Windows [Version 10.0.19044.1415]
(c) Microsoft Corporation. All rights reserved.

C:\Users\X270>ssh -NL 80:10.1.8.1:80 vkistuser@14.232.152.54 -p 6868
vkistuser@14.232.152.54's password:
```

Chạy hệ thống web: Với mỗi nền tảng web khác nhau thì cách khởi động code server lại khác nhau. Đối với nodejs là node tên file, python là python tên file, ... tùy theo cách nhà phát triển lập trình và cài đặt. Trong đa số trường hợp code và môi trường chạy được đóng gói trong docker và chạy tự động. Code của server cũng cần được thay đổi lại IP theo IP tĩnh và chọn cổng để chạy dịch vụ từ trước. ví dụ về code web



```
173     con.commit()
174     con.close()
175     return jsonify({'result': "success"}), 200
176
177 if __name__ == "__main__":
178     app.run(host='192.168.1.41', port=5000)
```

```
socketserver.TCPServer.server_bind(self)
File "C:\Users\X270\miniconda3\envs\face\lib\socketserver.py", line 466, in server_bind
    self.socket.bind(self.server_address)
OSError: [WinError 10049] The requested address is not valid in its context

(facereg) C:\Users\X270\OneDrive\Documents\face_reg>python app.py
Your CPU supports instructions that this binary was not compiled to use: AVX AVX2
For maximum performance, you can install NMSLIB from sources
pip install --no-binary :all: nmslib
* Serving Flask app "app" (lazy loading)
* Environment: production
  WARNING: This is a development server. Do not use it in a production deployment.
  Use a production WSGI server instead.
* Debug mode: off
* Running on http://192.168.1.41:5000/ (Press CTRL+C to quit)
```


Check port: Khi muốn xem 1 địa chỉ IP đang mở những port nào có mở port ssh hay không để vào hack :) thì dùng lệnh nmap. Lệnh này không có sẵn trên Win và Lin phải tải về tại trang <https://nmap.org/download.html>

tiến hành chạy nmap <địa chỉ IP>

nmap sẽ scan toàn bộ port đang open của ROUTER hoặc MÁY TÍNH có địa chỉ IP kia.

ví dụ con ROUTER 14.232.152.54 của viện có 1 port ssh đang mở :)

```
C:\Users\X270>nmap 14.232.152.54
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-25 09:11 SE Asia Standard Time
Nmap scan report for static.vnpt.vn (14.232.152.54)
Host is up (0.018s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
2000/tcp  open  cisco-sccp
3000/tcp  open  ppp
3001/tcp  open  nessus
8291/tcp  open  unknown
8888/tcp  open  sun-answerbook

Nmap done: 1 IP address (1 host up) scanned in 8.50 seconds
C:\Users\X270>
```

Ấn port, bảo mật port, limit port, quản lý port-IP, phân cấp IP, bảo mật ROUTER ... Đợi chuyên gia về :))))))

Tài liệu tham khảo

Networking:

<https://www.youtube.com/watch?v=Mad4kQ5835Y&list=PL7zRJGi6nMRzg0LdsR7F3olyLGoBcIvvg> (rất hay)

https://en.wikipedia.org/wiki/Computer_network

<https://ngrok.com/>

<https://kinsta.com/blog/linux-commands/>

<https://www.noip.com/support/knowledgebase/general-port-forwarding-guide/>

<https://www.configserverfirewall.com/ubuntu-linux/ubuntu-systemctl-command/>