|  |
| --- |
| THỰC HÀNH  XEM THÔNG TIN MẠNG TRÊN HỆ ĐIỀU HÀNH WINDOWS |

Nhóm học phần:

1) Mã Sinh viên01, Họ và Tên01

2) Mã Sinh viên02, Họ và Tên02

3)

MỤC LỤC

[1. Giới thiệu 2](#_Toc187236895)

[2. Chuẩn bị 2](#_Toc187236896)

[3. Thực hành 2](#_Toc187236897)

[3.1. Lệnh ipconfig 2](#_Toc187236898)

[3.2. Lệnh ping 3](#_Toc187236899)

[3.3. Lệnh tracert 5](#_Toc187236900)

[3.4. Lệnh router 6](#_Toc187236901)

[3.5. Lệnh netstat 7](#_Toc187236902)

[3.6. Lệnh nslookup 7](#_Toc187236903)

[3.7. Lệnh net 8](#_Toc187236904)

[3.7.1. net view 8](#_Toc187236905)

[3.7.2. net share 8](#_Toc187236906)

[3.7.3. net use (Chạy dưới quyền Administrator) 9](#_Toc187236907)

[3.7.4. net session 10](#_Toc187236908)

[3.7.5. net start|stop 10](#_Toc187236909)

[3.7.6. net user (Chạy dưới quyền Administrator) 10](#_Toc187236910)

[3.8. Lệnh tasklist 11](#_Toc187236911)

[3.9. Một số lệnh khác 11](#_Toc187236912)

[3.9.1. Lệnhh getmac 11](#_Toc187236913)

[3.9.2. Lệnh wmic 12](#_Toc187236914)

[3.9.3. Lệnh finger 12](#_Toc187236915)

[3.9.4. Lệnh arp 12](#_Toc187236916)

[3.9.5. Lệnh shutdown 12](#_Toc187236917)

[3.10. Lệnh cấu hình hệ thống netsh 12](#_Toc187236918)

[3.11. Xem địa chỉ IP trên Internet của máy đang sử dụng 13](#_Toc187236919)

[4. Bài tập 13](#_Toc187236920)

[5. Tham khảo 13](#_Toc187236921)

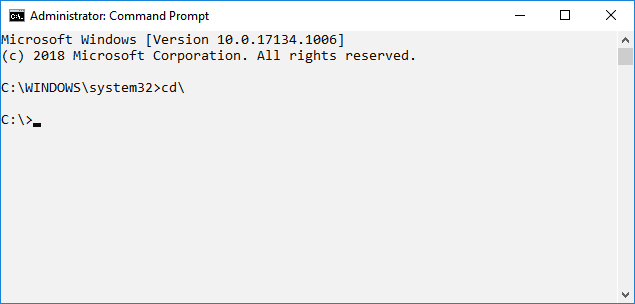
*>> Yêu cầu chụp hình ảnh là kết quả thực hành của SV. Không sử dụng lại hình ảnh của bài lab.*

# Giới thiệu

Nội dung bài Lab nhằm khai thác các lệnh truy xuất thông tin mạng trên hệ điều hành Windows.

# Chuẩn bị

* Kết nối máy tính vào mạng
* Trên Windows, vào menu Start\Windows System\CommandPrompt, nháy nút phải chọm More\Run as administrator
* Xuất hiện cửa sổ lệnh.



# Thực hành

1) Thực hiện lần lượt từng lệnh dưới, xuất hiện màn hình kết quả.

2) Nhấn tổ hợp phím *Shift + Windows + S* để chụp vùng ảnh cửa sổ kết quả.

3) Dán ảnh vào ngay dưới mỗi lệnh vừa thực hiện.

## Lệnh ipconfig

  C:\> cd\

* Hiển thị tất cả cấu hình IP của PC đang sử dụng : IP Address , Subnet Mask , Default Gateway , ....

  C:\> ipconfig   /all

Hình ảnh kết quả thực hiện lệnh: ?

Cho biết các thông tin về Card mạng đang kết nối với internet:

Description . . . . . . . . . . . : ???

Physical Address. . . . . . . . . : ???

Link-local IPv6 Address . . . . . : ???

IPv4 Address. . . . . . . . . . . : ???

Subnet Mask . . . . . . . . . . . : ???

Default Gateway . . . . . . . . . : ???

DHCP Server . . . . . . . . . . . : ???

* Cập nhật lại tất cả cấu hình IP trên card mạng

   C:\> ipconfig   /release

Hình ảnh kết quả thực hiện lệnh:

* Cập nhật lại địa chỉ IP mới từ DHCP Server

   C:\> ipconfig   /renew

Hình ảnh kết quả thực hiện lệnh:

* Xoá bộ nhớ đệm trên chương trình DNS Resolver Cache

   C:\> ipconfig   /flushdns

* Đăng ký mới DNS với DNS Server, đồng thời Refresh quá trình cấp IP từ DHCP Server

  C:\> ipconfig   /registerdns

* Xem tên miền được cache tạm, các địa chỉ IP tương ứng và time to live (tính bằng giây) của các bản ghi DNS

C:\>  ipconfig   /displaydns

* Xem thông tin card mạng Etthernet

C:\ >ipconfig   /all  |  findstr /IR "ipv4 ethernet adapter"

* Xem hướng dẫn sử dụng lệnh:

C:\>  ipconfig   /?

## Lệnh ping

    Lệnh Ping (Packet Internet Groper) cho phép kiểm tra xem một máy tính có thể kết nối tới một máy chủ cụ thể nào đó hay không, và ước lượng khoảng thời gian trễ trọn vòng đi và về của gói dữ liệu cũng như tỉ lệ các gói dữ liệu có thể bị mất giữa hai máy.

    Các dạng thông báo sau khi thực hiện lệnh ping:

a. Thông báo: Reply from 192.168.1.180: bytes=32 time=2ms TTL=55

    Lệnh ping đã thực hiện thành công và không có lỗi trên mạng.

    Địa chỉ IP 192.168.1.180 cho biết máy nào đang gửi thông điệp trả lời.

    bytes=32 là kích thước của gói tin ICMP được gửi đi.

    time=2ms thời gian của quá trình hồi đáp

    TTL=55 là giá trị “time to live” (thời gian sống) của gói tin ICMP. Hết thời gian này thì gói tin sẻ bị hủy.

b. Thông báo: Request timed out

    Xảy ra khi không kết nối được với máy đích, không có hồi đáp trả về. Nguyên nhân:

* Thiết bị định tuyến Router bị tắt.
* Địa chỉ máy đích không có thật hoặc máy đích đang bị tắt, hoặc cấm ping.
* Nếu máy đích khác đường mạng với máy nguồn thì nguyên nhân có thể do không có định tuyến ngược trở lại máy nguồn. Lúc này, nếu máy đích đang chạy, có thể kiểm tra đường đi về của gói tin bằng cách xem lại thông số Default Gateway trên máy đích, máy nguồn và router kết nối các đường mạng

Thông báo: Destination host unreachable: Thông báo cho biết không thể kết nối đến máy đích. Nguyên nhân gây ra lỗi này có thể là do kết nối vật lý của máy tính như cáp mạng bị đứt, không gắn cáp vào card mạng, card mạng bị tắt, Driver card mạng bị hỏng, chưa bật wifi, …

* Ping thăm dò đến máy tính đích 192.168.1.10 (là địa chỉ IP của máy người bên cạnh)

C:\>  ping  192.168.1.10

* Liên tục gửi gói tinh đến máy tính đích, nhấn *Ctrl + C* để dừng

C:\>  ping  192.168.1.10 /t

* Xem địa chỉ IP từ tên host

C:\>  ping  192.168.1.10 /a

* Gửi gói tin có độ lớn xác định

C:\>  ping 192.168.1.10 -l 65500

* Xác định số gói tin sẻ gửi đi.

C:\> ping 192.168.1.10  /n 5

>> Thử lại lệnh ping đến các địa chỉ trên Internet như sau. Chú ý quan sát thời gian gởi/nhận

C:\> ping  208.67.222.222

C:\> ping  208.67.220.220

C:\> ping  203.162.4.191

C:\> ping  203.162.4.190

C:\> ping  192.168.1.1

C:\> ping  8.8.8.8

C:\> ping  www.dut.udn.vn

C:\> ping  www.google.com

## Lệnh tracert

Lệnh traceroute cho phép xác định được đường đi của các gói packets từ máy NSD đến máy đích trên mạng Internet.

Xem đường đi từ máy NSD đến host xyz.com

C:\WINDOWS\system32>tracert tin247.com

Tracing route to tin247.com [118.27.5.85]

over a maximum of 30 hops:

  1     3 ms     2 ms     2 ms  192.168.1.1

  2     3 ms     5 ms     5 ms  static.vnpt.vn [123.29.8.28]

  3    18 ms     5 ms     7 ms  static.vnpt.vn [113.171.58.93]

  4    11 ms     5 ms     4 ms  static.vnpt.vn [113.171.56.222]

  5    55 ms    55 ms    55 ms  210.173.176.63

  6    56 ms    55 ms    55 ms  tkort4-crt2.bb.sakura.ad.jp [157.17.130.45]

  7    56 ms    56 ms    56 ms  tkwrt2x-ort4-1.bb.sakura.ad.jp [157.17.131.94]

  8    56 ms    58 ms    56 ms  as2519-tkwrt2x.bb.sakura.ad.jp [210.188.225.34]

  9    58 ms    56 ms    56 ms  ae0.transit2.nihonbashi.vectant.ne.jp [163.139.128.118]

 10    57 ms    57 ms    56 ms  222.228.239.34

 11    57 ms    56 ms    57 ms  aha.33.s-port.biz [202.94.181.33]

 12    76 ms    74 ms    76 ms  unused-133-130-015-090.interq.or.jp [133.130.15.90]

 13    73 ms    73 ms    73 ms  unused-133-130-015-102.interq.or.jp [133.130.15.102]

 14    73 ms    73 ms    72 ms  unused-133-130-014-246.interq.or.jp [133.130.14.246]

 15    73 ms    73 ms    74 ms  v118-27-5-85.ps18.static.cnode.io [118.27.5.85]

Giải thích

+ Dòng thứ 1 cho biết hostname và địa chỉ IP của hệ thống đích. Giá trị TTL<=30 và kích thước của datagram là 40 bytes (20-bytes IP Header + 8-bytes UDP Header + 12-bytes user data).

+ Dòng thứ 2 cho biết router đầu tiên nhận được datagram là 202.xy.34.12, giá trị của TTL khi gởi đến router này là 1. Router này sẻ gởi trở lại cho chương trình traceroute một ICMP message error "Time Exceeded". Traceroute sẻ gởi tiếp một datagram đến hệ thống đích.

+ Dòng thứ 3, xyz.com (202.xx.12.34) nhận được datagram có TTL=1(router thứ nhất đã giảm một trước đó - TTL=2-1=1). Tuy nhiên, xyz.com không phải là một router, nó sẻ gởi trở lại cho traceroute một ICMP error message "Port Unreachable". Khi nhận được ICMP message này, traceroute sẻ biết được đã đến được hệ thống đích xyz.com và kết thúc nhiệm vụ tại đây.

+ Trong trường hợp router không trả lời sau 5 giây, traceroute sẻ in ra một dấu sao "\*" (không biết) và tiếp tục gởi datagram khác đến host đích.

Trong Windows: tracert hostname

Trong Unix: traceroute hostname

Hiển thị các tuyến mà packet đi qua để tới được host đích. Lệnh này hoạt động dựa trên trường time-to-live (TTL). Khi đó mỗi gateway trên tuyến trả lại gói tin ICMP TIME\_EXCEEDED.

## Lệnh router

C:\ >route print

===========================================================================

Interface List

  9...00 e0 4c 68 00 16 ......Realtek PCIe GBE Family Controller #2

  4...60 57 18 d8 34 1c ......Microsoft Wi-Fi Direct Virtual Adapter

 15...62 57 18 d8 34 1b ......Microsoft Wi-Fi Direct Virtual Adapter #3

 14...60 57 18 d8 34 1b ......Intel(R) Dual Band Wireless-N 7265

  1...........................Software Loopback Interface 1

===========================================================================

IPv4 Route Table

===========================================================================

Active Routes:

Network Destination        Netmask          Gateway       Interface  Metric

          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.144     25

        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331

        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331

  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331

      192.168.1.0    255.255.255.0         On-link     192.168.1.144    281

    192.168.1.144  255.255.255.255         On-link     192.168.1.144    281

    192.168.1.255  255.255.255.255         On-link     192.168.1.144    281

        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331

        224.0.0.0        240.0.0.0         On-link     192.168.1.144    281

  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331

  255.255.255.255  255.255.255.255         On-link     192.168.1.144    281

===========================================================================

Persistent Routes:

  None

IPv6 Route Table

===========================================================================

Active Routes:

 If Metric Network Destination      Gateway

  1    331 ::1/128                  On-link

  9    281 fe80::/64                On-link

  9    281 fe80::6c2d:4094:b290:9ff1/128

                                    On-link

  1    331 ff00::/8                 On-link

  9    281 ff00::/8                 On-link

===========================================================================

Persistent Routes:

 If Metric Network Destination      Gateway

  0 4294967295 ::/0                     2001:db8:1:2::1

===========================================================================

## Lệnh netstat

    Lệnh netstat cho phép xem thông tin hoạt động của mạng TCP/IP.

    Cú pháp : **netstat [-a][-e][-n]**

    - Tham số -a: Hiển thị tất cả các kết nối và các cổng đang lắng nghe (listening)

    - Tham số -e: hiển thị các thông tin thống kê Ethernet

    - Tham số -n: Hiển thị các địa chỉ và các số cổng kết nối...

    - Tham số -o thông báo cho netstat hiển thị số processID của mỗi chương trình đang tương tác với cổng TCP hoặc UDP.

  C:\>   netstat  -nao

   Xem cổng TCP 443 bắt đầu được sử dụng trên máy tính, cùng với process ID đang sử dụng trên cổng.

C:\>  netstat –nao 1 | find "443"

C:\>  netstat  -n

C:\>  netstat  -nr

C:\>  netstat  -na             //Xem danh sách các cổng TCP và UDP trên máy tính

C:\>  netstat  -nab            //Xem tên file EXE đang sử dụng trên mỗi cổng

C:\>  netstat  -s -p TCP       //Thống kê gói tin TCP.

C:\>  netstat  -na 2           //Xem cổng TCP và UDP trên máy tính theo chu kỳ 2 giây:

## Lệnh nslookup

 Dùng để truy vấn thông tin DNS trong phân giải tên miền.

-        Hiển thị thông tin có thể được dùng để chẩn đoán cấu trúc của DNS.

-        Giúp tìm kiếm thêm địa chỉ IP nếu DNS biết được whois.

-        Bản ghi MX cho biết địa chỉ IP của mail server.

  Kết quả xuất hiện thông tin hostname và địa chỉ IP của DNS server được cấu hình.

  Liệt kê các bản ghi MX của domain gmail.com

      C:\> nslookup –type=mx gmail.com

      gmail.com MX preference=30, exchanger = alt3.gmail-smtp-in.l.google.com

      gmail.com MX preference=20, exchanger = alt2.gmail-smtp-in.l.google.com

      gmail.com MX preference=5, exchanger = gmail-smtp-in.l.google.com

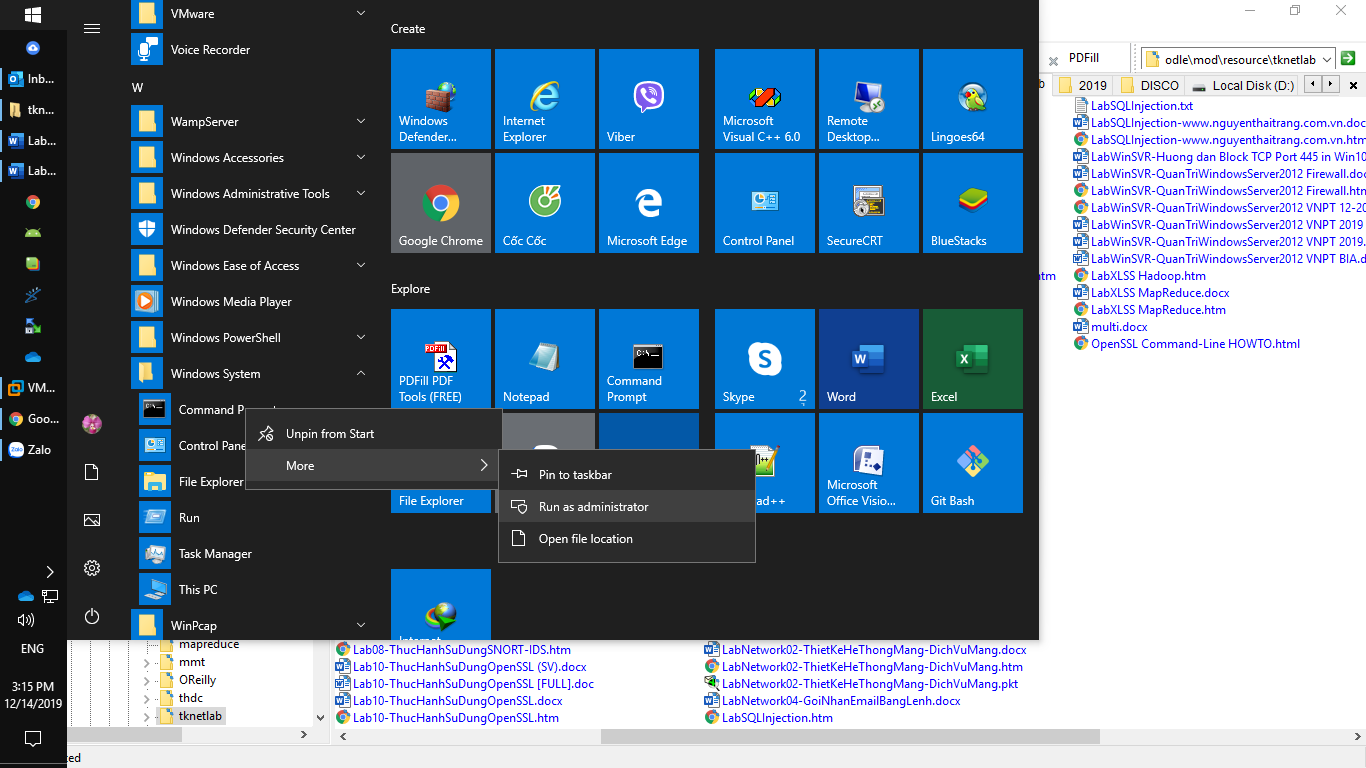
      gmail.com MX preference=10, exchanger = alt1.gmail-smtp-in.l.google.com

      gmail.com MX preference=40, exchanger = alt4.gmail-smtp-in.l.google.com

## Lệnh net

Chuẩn bị: *Máy chủ Linux có IP = 192.168.0.10, chạy dịch vụ Samba, đã tạo các tài khoản NSD*. Liên hệ GV để lấy địa chỉ IP chính xác.

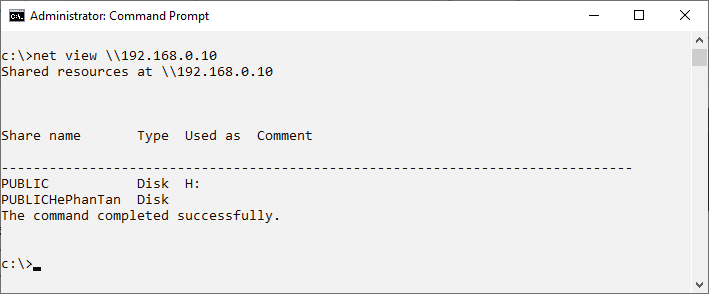
### net view



* Xem danh sách các chia sẻ trên một mạng

C:\>  net view

C:\>  net view \\192.168.0.10



### net share

* Xem danh sách các chia sẻ trên máy đang dùng:

C:\> net share

* Tạo một chia sẻ:

C:\> md C:\ThucHanh

* Chia sẻ thư mục để truy xuất từ xa (Chạy dưới quyền Administrator)

C:\> net share thuchanh=C:\ThucHanh

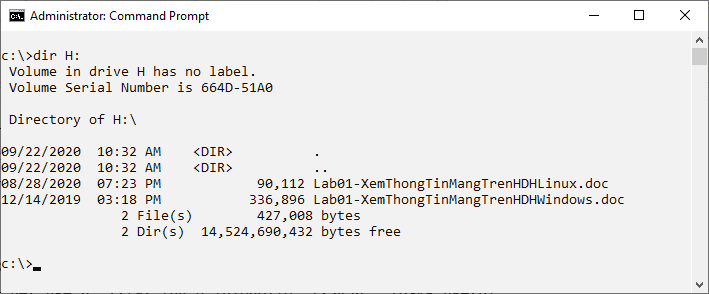
### net use (Chạy dưới quyền Administrator)

* Tạo một ổ đĩa ánh xạ kết nối đến thư mục chia sẻ PUBLIC trên máy 192.168.1.10 (là máy Windows trong mạng)

C:\> net use H: \\192.168.1.10\public  123456   /USER:user01

* Mở cửa sổ Windows Explorer để xem thư mục chia sẻ. Sao chép và tạo mới thư mục.

C:\>  dir H:



* Tạo một ổ đĩa ánh xạ kết nối đến thư mục chia sẻ PUBLIC trên máy 192.168.0.10

 C:\> net use \*  \\192.168.1.10\public  123456  /USER: <taikhoanNSD>

Drive Z: is now connected to \\192.168.0.10\public.

* The command completed successfully.

C:\>  dir Z: // Z là tên ổ đĩa ánh xạ

* Tạo một ổ đĩa ánh xạ kết nối đến thư mục của người dùng trên máy Linux 192.168.0.10 theo tài khoản là mã sinh viên:

C:\> net use \*  \\192.168.1.10\<taikhoanNSD>  123456  /USER:<taikhoanNSD>

C:\> dir K:

* Mở cửa sổ Windows Explorer để xem nội dung ổ đĩa vừa được ánh xạ. Sao chép và tạo mới thư mục trong ổ đĩa này.
* Xem danh sách các ánh xạ ổ đĩa trên máy:

C:\>  net use

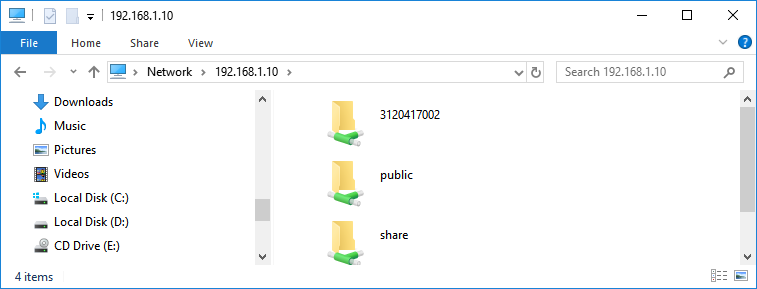
* Xóa ổ đĩa ánh xạ Z:

 C:\>  net use Z: /DELETE

* Xóa tất cả ổ đĩa ánh xạ:

C:\>  net use \* /DELETE /YES

>> Trên cửa sổ Windows Explorer có thể gõ lệnh : \\192.168.0.10 để truy xuất đến các thư mục chia sẻ trên máy ở xa.



Từ máy NSD, kết nối đến một máy Windows có IP = 192.168.1.12 trong mạng.

Kết nối đến thư mục gốc D$ dưới quyền Administrator

C:\> net use \* \\192.168.1.12\D$ \* /USER:Administrator

>> Mở cửa sổ Windows Explorer để xem thư mục chia sẻ. Sao chép và tạo mới thư mục.

>> Thực hành chia sẻ thư mục trên máy người dùng và kết nối từ xa đến thư mục chia sẻ này.

### net session

* Xem danh sách các kết nối trên hệ thống

C:\>  net session

### net start|stop

* Xem danh sách các dịch vụ đang hoạt động trên máy:

C:\>  net start

* Dừng một dịch vụ đang hoạt động (Chạy dưới quyền Administrator)

C:\>   net stop "Task Scheduler"

* Khởi động một dịch vụ  (Chạy dưới quyền Administrator)

C:\>  net start "Task Scheduler"

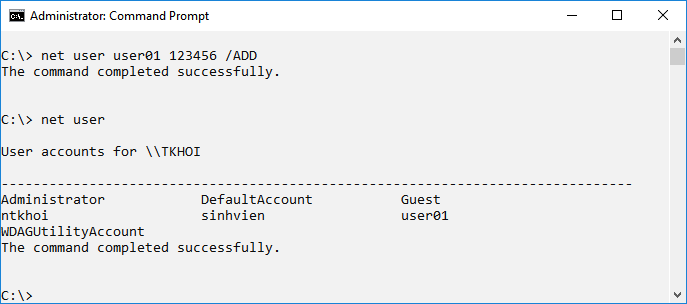
### net user (Chạy dưới quyền Administrator)

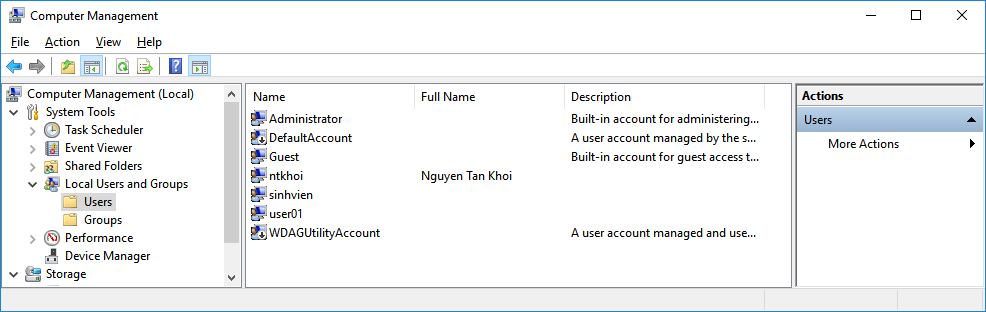
    Tạo một tài khoản mới với tên user01, mật khẩu: 123456

    C:\>  net user user01 123456 /ADD

    Xem các tài khoản trên máy:

    C:\>  net user





* Thay đổi mật khẩu của tài khoản user01

C:\>  net user user01 999

* Xóa tài khoản user01

C:\>  net user user01 /DELETE

## Lệnh tasklist

* Lệnh tasklist hiển thị tất cả các tiến trình đang chạy, số process ID và dung lượng bộ nhớ sử dụng cho mỗi tiến trình:

C:\>  tasklist /svc

* Xem các DLLs, các thư viện mã lệnh được tải bởi các tiến trình khi chúng thực thi mệnh lệnh trên máy

C:\>  tasklist /m

## Một số lệnh khác

### Lệnhh getmac

C:\>  getmac

### Lệnh wmic

* Hiển thị tên, ID của quá trình và quyền ưu tiên của mỗi quá trình đang chạy cũng như các thuộc tính khác:

C:\>  wmic process

* Xem tất cả các thông tin chi tiết bao gồm có đường dẫn của file thực thi liên kết với từng tiến trình:

C:\>  wmic process list brief

C:\>  wmic process list full

### Lệnh finger

* Liệt kê tất cả danh sách các tên login, full name, tên terminal, trạng thái, idle time, login time, office location, phone number cho mỗi user hiện đang login vào mạng.

C:\> finger -l user01@192.168.1.12

### Lệnh arp

* Hiển thị giá trị hiện tại trong bảng ARP (chuyển địa chỉ IP - địa chỉ MAC) của giao thức ARP trong máy tính

C:\>  arp - a

C:\>  arp -a 192.168.0.10 *//Địa chỉ của máy bên cạnh*

* Thêm một entry vào bảng ARP với địa chỉ IP inet\_addr với địa chỉ MAC giả mạo

C:\>  arp -s 192.168.0.100 aa-bb-cc-dd-ee-ff

* Xóa địa chỉ IP 192.168.0.100 trong bảng ARP:

C:\>  arp -d 192.168.0.100

* Xem thiết lập của một reistry key cho trước:

C:\>  reg query hklm\software\microsoft\windows\currentversion\run

### Lệnh shutdown

* Shutdown máy tính sau 10s

C:\> shutdown  /s  /t 10

* Shutdown máy sau 30s

C:\> shutdown   -s -f -t 30

## Lệnh cấu hình hệ thống netsh

>> Cẩn thận khi sử dụng các lệnh này

1) Thiết lập biến

   C:\>  set varip=192.168.1.2

   C:\>  set varsm=255.255.255.0

   C:\>  set vargw=192.168.1.1

   C:\>  set vardns1=203.162.0.11

   C:\>  set vardns2=203.162.4.190

2) Thiết lập địa chỉ IP mới và các thông tin mạng khác

C:\>  netsh int ip set address name = "Local Area Connection" source = static addr = %varip% mask = %varsm%

C:\>  netsh int ip set address name = "Local Area Connection" gateway = %vargw% gwmetric = 1

C:\>  netsh int ip set dns name = "Local Area Connection" source = static addr = %vardns1%

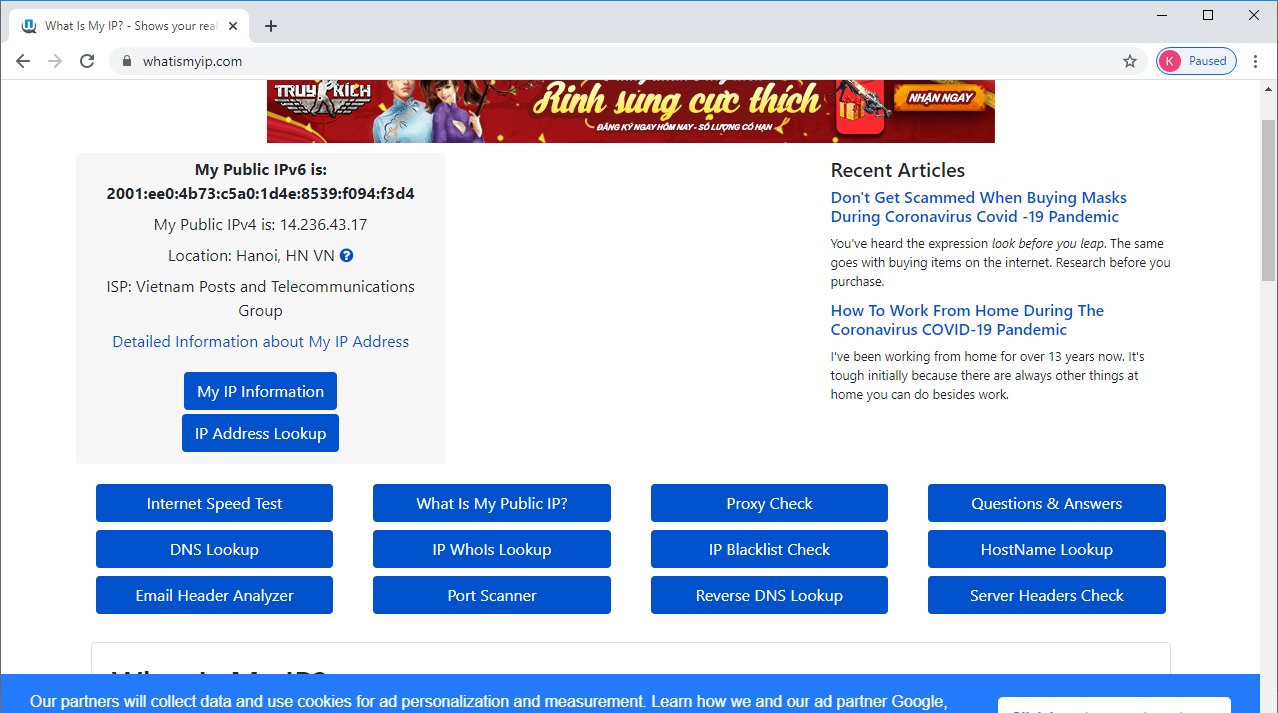
C:\>   netsh int ip add dns name = "Local Area Connection" addr = %vardns2%

C:\>   netsh int ip show config

## Xem địa chỉ IP trên Internet của máy đang sử dụng

Sử dụng Website: https://www.iplocation.net/

Sử dụng Website: https://www.whatismyip.com/



----------------------------

# Bài tập

# Tham khảo

1. ..

(Tài liệu lưu hành nội bộ)

-----------------------------------------------

DANH MỤC HÌNH

**No table of figures entries found.**