UEEN2013/UEEN2423

TCP/IP Network Fundamentals
(Topic 01)

Introduction

Network Devices:
End-Devices & Networking Devices

- There are two big classification of devices in the Internet/network:
  - <u>End-Devices</u> & <u>Networking Devices</u>.
- End devices:
  - Devices that a <u>person</u> can use for communication purposes.
  - End-devices normally attached to a network.
- Networking devices:
 - <u>Equipments that form the network</u> and help to mediate and transfer data between end-devices.

UTAR
UNIVERSITI TUNKU ABDUL RAHMAN

Example of the Devices

- ## End-devices:

PC-PT PC   Laptop-PT Laptop   Server-PT Server   Printer-PT Printer   7960 IP Phone   PDA-PT Pda   TabletPC-PT Tablet PC

- ## Networking devices:

Router-PT Router   2950-24 Switch   3560-24PS Multilayer Switch   Bridge-PT Bridge   Hub-PT Hub   Repeater-PT Repeater

CoAxialSplitter-PT Coaxial Splitter   Linksys-WRT300N Wireless Router   AccessPoint-PT Wireless Access Point   DSL-Modem-PT DSL Modem

UTAR
UNIVERSITI TUNKU ABDUL RAHMAN

- A person using an end-device to communicate with another person using another end-device via the network formed by networking-devices.
  - Servers and clients are end-devices.
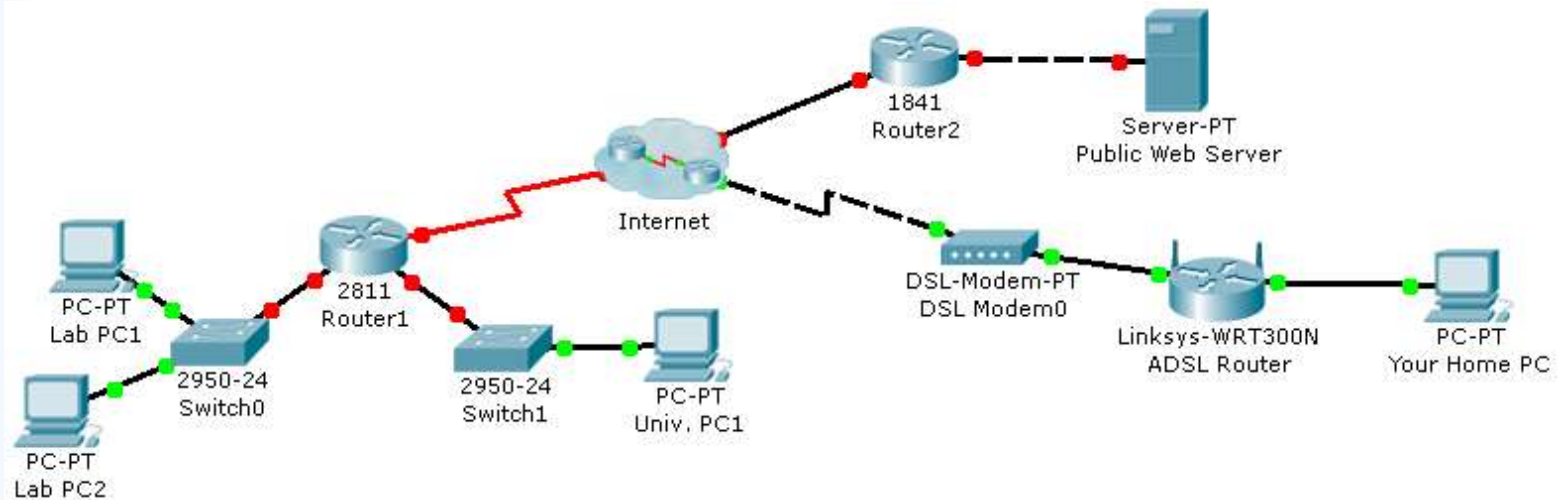
Quick Quiz

- Which of the following are end devices (or networking devices)?
  - Workstations
  - Web Server
  - Wireless access point
  - iPhone
  - Wireless router

UTAR

Addressing Scheme in Networks

- These are three sets of addresses that are very important to networks and end-devices
  - Network "location" address => IP Address
  - Network "application" address => Port Number
  - Network "hardware" address => Physical Address (MAC address)
- These addresses are used in operating-systems.
  - They are used in Windows, Linux, Solaris, Unix, and Apple MacOS computers
  - They are also used in Apple iOS, Google Android and Windows Phone mobile devices

UTAR
UNIVERSITI TUNKU ABDUL RAHMAN

IP address

- There are two versions of IP address in use today
  - IPv4 (32 bits) and IPv6 (128 bits)

An IPv4 address (dotted-decimal notation)

172 . 16 . 254 . 1

10101100.00010000.11111110.00000001

One byte = Eight bits

Thirty-two bits (4 * 8), or 4 bytes
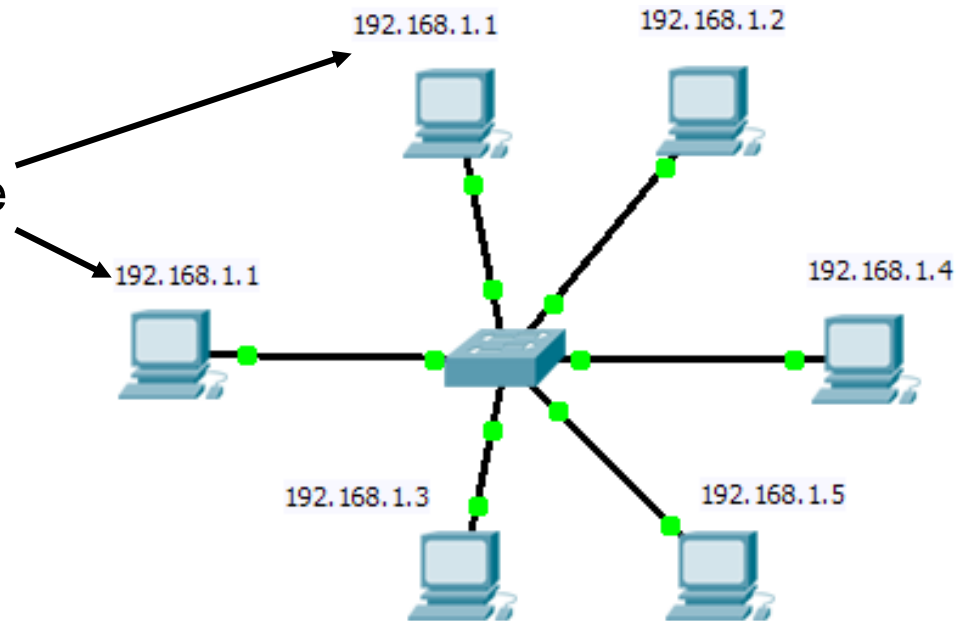
  - A decimal number of IP address can range from __ to __.

Quick Quiz

- Which of the following are valid IP addresses?
    - 0.0.0.0
    - 100.2.300.3
    - 255.255.255.1
    - 1.12.0.256
    - 7.7.7.69
    - 192.0.1.1.1
    - 200.245.80
    - 6.260.80.6
    - 1.2.3.4

Unique IP address

- Within a network, the IP address has to be unique

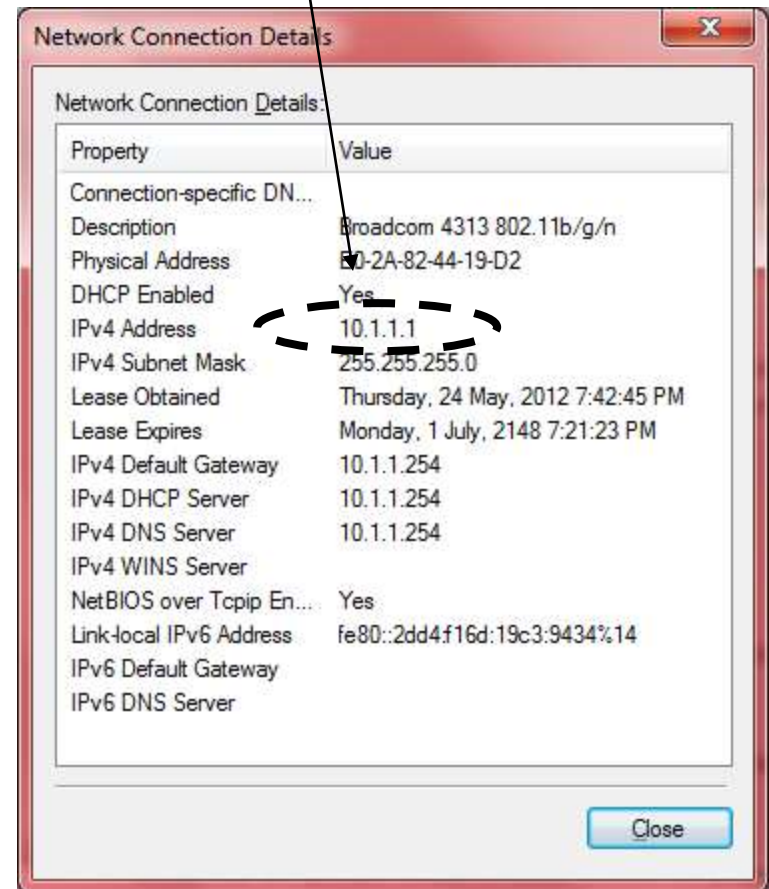CANNOT have 2 same
IP addresses within
a network

192.168.1.1

192.168.1.2

192.168.1.1

192.168.1.4

192.168.1.3

192.168.1.5

UTAR
UNIVERSITI TUNKU ABDUL RAHMAN

Source IP and Destination IP

- There are two sides of the IP address
  - Source IP (you)
  - Destination IP (where you want to go)
- Your PC <u>MUST</u> have a source IP before you can communicate with the Internet.

Source IP

Destination IP

Port Number

- A <u>port number</u> is a way to identify a specific <u>process</u> to which an Internet or other network message is to be forwarded when it arrives at an end-device.

- Port number is <u>unique within an end-device</u>.

- The size of a <u>port number</u> is 2 bytes.
  - Range => 0 to 65535

- The port numbers are categorized into:
  - <u>Server port numbers (well-known ports)</u>: 0 to 1023
  - <u>Client port numbers</u>: 1024 to 65535

UTAR
UNIVERSITI TUNKU ABDUL RAHMAN

Server Port Numbers - 1

- <u>Server port numbers</u> are the <u>standardized</u> 2-byte numbers that identify the well-known network services such as HTTP, FTP, DNS, etc..

- These server port numbers have been assigned with a <u>dedicated fixed value</u> to describe a network service, e.g:
  - Port number = 80 (HTTP)
  - Port number = 53 (DNS)
  - Port number = 23 (telnet)

Server Port Number - 2

- Network services are identified via port numbers inside the servers

- In the range of 0-1023, a particular value has already been assigned and associated with a particular network services.

- Server ports are also called listening ports or well-known port numbers.
    - 20 (FTP data), 21 (FTP control),
    - 22 (SSH), 23 (Telnet)
    - 25 (SMTP), 53 (DNS),
    - 67 (DHCP server), 68 (DHCP client)
    - 69 (TFTP), 80 (HTTP), 110 (POP3)

    The numbers used above are default port numbers for the services.

UTAR
UNIVERSITI TUNKU ABDUL RAHMAN

Client Port numbers

- Client port numbers are not fixed.
  - It is normally in the range 1024 – 65535
- Assigned by operating system randomly.
- Client ports are sometimes called <u>connection ports</u>

- The notation [IP:port_number] is called a <u>socket</u>.
- Socket can identify any network application/service in the Internet.
  - For example: 157.166.255.18:80 identify the web service of www.cnn.com
  - Question: can I change the default port number?

IP Address & Port Number

- A PC can find cnn.com because it knows the IP address of cnn.com.

- When the data reach cnn.com, cnn.com will direct this data to a particular network service based on the port number.

- In this case, port 80 will refer to the web/http service provided by cnn.com.

- Same as IP address, port number is also divided into:
  - Source port number
  - Destination port number

- Question: Which one is correct?
  - Both server and client use port 80 for http processes.
  - The server uses port 80 for http processes and the client uses other port number.
  - The client uses port 80 for http processes and the server uses other port number.

Example of [IP:port]

- 3 PCs are accessing the web server at the same time.
- At the server, it is detected that there are 3 connections
  - 192.168.1.1:80, (IP: port number). This notation is called a <u>socket.</u>
  - Meaning the server IP is 192.168.1.1 and the port number is 80 (source port number)
  - Same service (web server application) is connected to three other applications (web browsers).
  - For example, 192.168.1.2 is having an application with a port number of 1029.
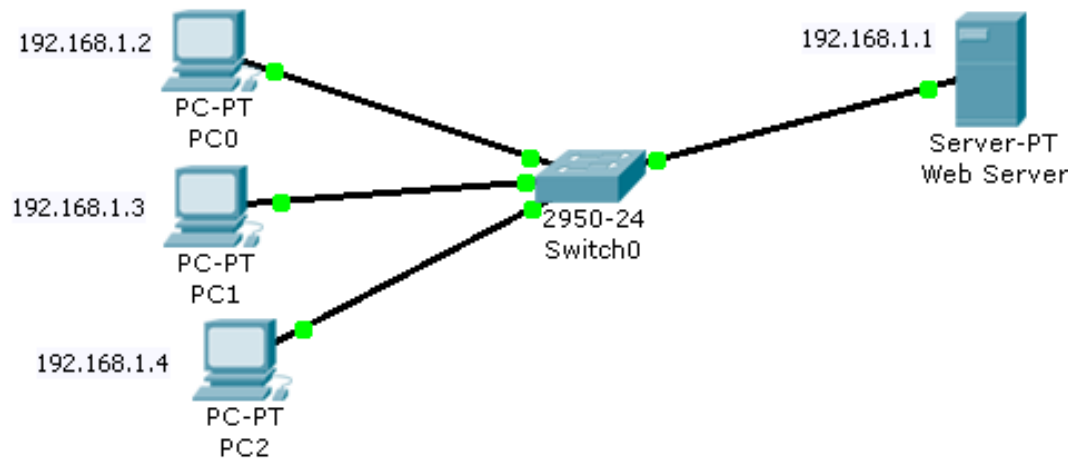
Quick Quiz

```
SERVER>netstat

Active Connections

  Proto   Local Address          Foreign Address          State
  TCP     192.168.1.1:80         192.168.1.2:1029         SYN_RECEIVED
  TCP     192.168.1.1:80         192.168.1.3:1026         CLOSED
  TCP     192.168.1.1:80         192.168.1.4:1026         CLOSED
SERVER>
```

- In this web server
  - What is the source IP address?
  - What is the destination IP address?
  - What is the source port number?
  - What is the destination port number?

Hardware Address: MAC Address

- Media Access Control address (MAC address) is a unique identifier attached to network adapters or network interface card (NICs).
  - Used in both wired and wireless NICs
  - Unique throughout the world
    - No two NIC will have the same MAC address
    - Burned in the NIC chips and can't be changed
    - Q: But what if I insist to change the MAC address? Is it Possible?
  - Contain <u>6 bytes</u> (or 6 octet or 48 bits)
    - First 3 bytes identify the manufacturer (OUI)
    - 00-00-00   XEROX CORPORATION
    - 00-00-0B   MATRIX CORPORATION
    - 00-00-0C   CISCO SYSTEMS, INC.
    - Last 3 bytes are the unique address for the NIC
  - MAC is also known as Hardware Address or Physical Address
- Usually shown in hexadecimal format, with each octet separated by a dash or colon.
  - An example of a MAC address would be "00-08-74-4C-7F-1D".

- Before the data is being sent to the network wire, the PC/host will have to "gather" 3 pair of "addresses" for encapsulation.
  - Source port & Destination port
  - Source IP & Destination IP
  - Source MAC & Destination MAC
- Encapsulation shall be discussed next.

Self-Study Quiz

1. MAC address is 48 bits.
2. Port number = 266 is a server port number.
3. Each socket is unique in the Internet.
4. You can run a network service with a port number of 509.
5. You only need the IP address to figure out the services of a remote host / server.
6. IP address is related to?

        A) User   B) Application   C) Location

        D) Cable   E) Network   F) Password
7. Port number is related to?

        A) User   B) Application   C) Location

        D) Cable   E) Network   F) Password

UTAR
UNIVERSITI TUNKU ABDUL RAHMAN

Examples of Network Software

- Network client software
  - What we use the most (acquiring information or data)
    - Web browser (Firebox), email reader/client (Outlook), etc
- Server software
  - Turn a PC into a server
    - Apache web server
- Networking software/commands
  - Help to explore and troubleshoot the network
    - tracert, ipconfig, ping, Wireshark, Free IP Tools

Networking software/commands

- There are some differences between network client software and networking software
  - Network client software help you to access services
  - Networking software help you to
    - explore the network,
    - configure the network,
    - troubleshoot the network,
    - collect network statistics,
    - access certain network status and parameters.

UTAR
UNIVERSITI TUNKU ABDUL RAHMAN

Setting IP

- Assume that you have a network interface card (NIC) and it is connected to the Internet.
- Before you explore the network, you need to configure the following:
  - Source IP address
  - Subnet mask
  - Default Gateway
  - DNS IP address
- Nowadays, the configuration is automated using the new devices.

Setting IP in Windows

- Click on start →
  Control Panel →
  Network Connections
- Right click on "Local
  Area Connection" and
  select "Properties".
- Double click on
  "Internet Protocol
  (TCP/IP)"

Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
○ Use the following IP address:
  IP address:
  Subnet mask:
  Default gateway:

○ Obtain DNS server address automatically
○ Use the following DNS server addresses:
  Preferred DNS server:
  Alternate DNS server:
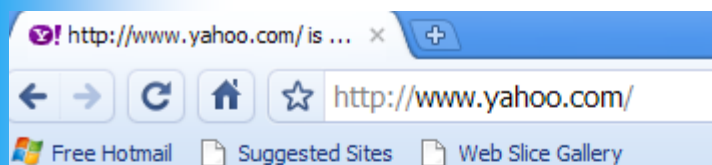
Advanced...

OK | Cancel

Dynamic IP

- You need the help of a DHCP service in your network, if you use this option.
  - Which means you need a DHCP(Dynamic Host Control Protocol) server in the network.

- Click on "obtain an IP address automatically".

- DHCP service will supply the IP address, subnet mask, default gateway, and DNS IP to your PC automatically.

UTAR
UNIVERSITI TUNKU ABDUL RAHMAN
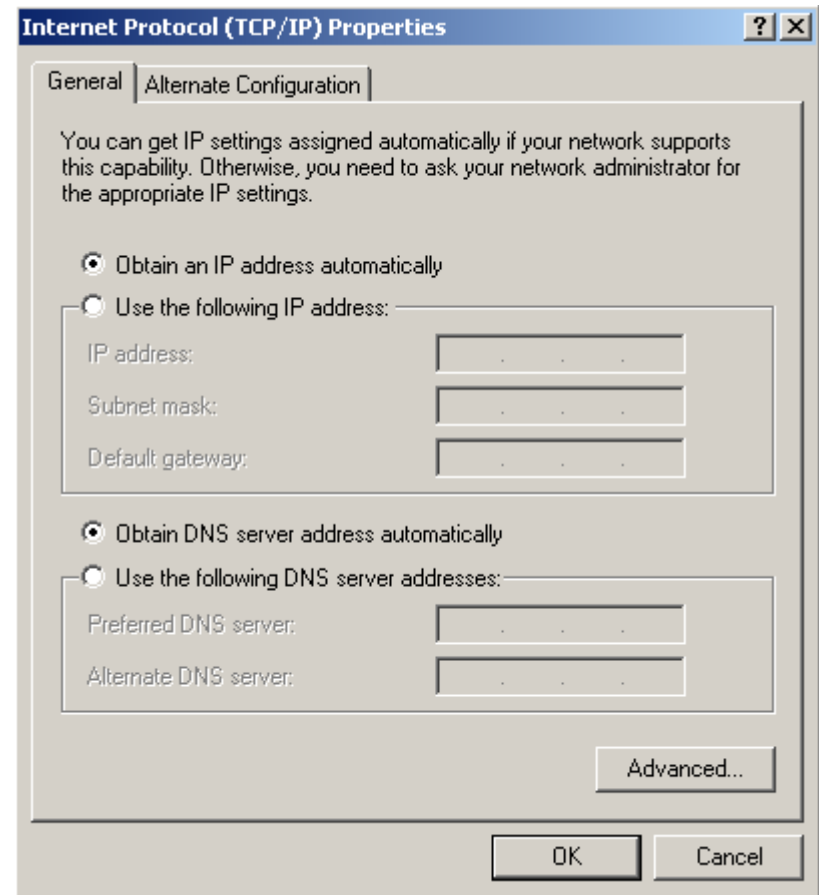
Static IP

- In static IP, you have to key-in the four parameters manually.

- Default gateway = IP address of the immediate router in your local area network.

- DNS server converts the domain name into destination IP address

- Windows allows you to enter two valid DNS IP addresses.

UTAR

If you don't have a proper DNS IP

- You have to type the IP address (64.233.181.104) of Google web site instead of www.google.com in order to access the web site or IP address (209.131.36.159) for yahoo.com
- Otherwise, the browser will prompt you an "domain name unresolved"
- Without a valid DNS IP, all the "yahoo.com", "cnn.com", "utar.edu.my", "facebook.com" will NOT work in the browser.

Extra: Alternate Configuration

- If you have a notebook, using static IP at home and the IP assigned by DHCP server at the office, you can make use of the alternate configuration to set IP and network information for these 2 different networks.

- Set "Obtain an IP address automatically" on "General" tab, so that the notebook will be assigned IP addresses automatically at the office.

- After that, click "Alternate Configuration" tab, select User configured option and key in your home network's static IP information.

- By setting this, when there is no IP information assigned due to no DHCP server at home, this alternate configuration will be applied automatically, so that you don't have to set IP manually every time at home.

Internet Protocol (TCP/IP) Properties	? X

General | Alternate Configuration

If this computer is used on more than one network, enter the alternate IP settings below.

○ Automatic private IP address

● User configured

IP address:	192 . 168 . 0 . 20
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 0 . 1
Preferred DNS server:	202 . 188 . 0 . 5
Alternate DNS server:	202 . 188 . 0 . 133
Preferred WINS server:	. . .
Alternate WINS server:	. . .

OK | Cancel

UTAR
UNIVERSITI TUNKU ABDUL RAHMAN

1. ipconfig

- "ipconfig" is used to check the IP configuration of every network interface card (NIC) of your PC
  - IP address
  - Subnet mask
  - Default gateway
- If your PC has 2 wired NICs and 1 wireless NIC, "ipconfig" will list <u>3 sets</u> of IP addresses, subnet masks and default gateways.

ipconfig /all

- Give a more detailed status of the NICs that includes
  - DNS server IP
  - DHCP server IP
  - Dynamic or static IP
  - MAC addresses/Physical address.
  - Lease of the DHCP service

2. DHCP Service

- Normally, users do not actively access the DHCP service.
  - DHCP is "transparent" to users.

- More often, it is the operating system (OS) that deals with DHCP service.

UTAR

ipconfig /renew

- Make request to the dhcp server to get
    - IP address,
    - Subnet mask
    - DNS IP
    - Gateway IP.

ipconfig /release

- Release the IP address, netmask and default gateway back to DHCP server.
    - 0.0.0.0 = no source ip address, subnet mask

3. ping

- Function:
  - Check connectivity of between a remote IP and your PC
- A successful ping means that the communication between your PC and the remote IP is working.
- ping comes in the form of Windows command, or GUI net tools.

- `ping destination_ip` or
- `ping domain_name`
  - `c:\>ping 192.168.1.1`
  - `c:\>ping www.google.com.my`

UTAR
UNIVERSITI TUNKU ABDUL RAHMAN

Explanation of ping result

```
Reply from 203.84.202.10: bytes=32 time=349ms TTL=51
Reply from 203.84.202.10: bytes=32 time=354ms TTL=51
Reply from 203.84.202.10: bytes=32 time=379ms TTL=51
Reply from 203.84.202.10: bytes=32 time=374ms TTL=51
```

```
Ping statistics for 203.84.202.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 349ms, Maximum = 379ms, Average = 364ms
```

- time = Round Trip Time (RTT)
  - Time that the ping packet travel to the remote IP and back.
  - time = 349ms means, ping takes 349ms to travel from your PC to 203.84.202.10 and then back to your PC.

- TTL = time-to-live
  - The number of routers that the ping packet can pass before it is dropped by the router.
  - TTL = 51 means the ping packet still can travel 51 more routers.
  - TTL = 51 also mean the ping packet have travel (64 – 51) = 13 routers.

UTAR
UNIVERSITI TUNKU ABDUL RAHMAN

Free IP Tools – Ping (Successful)
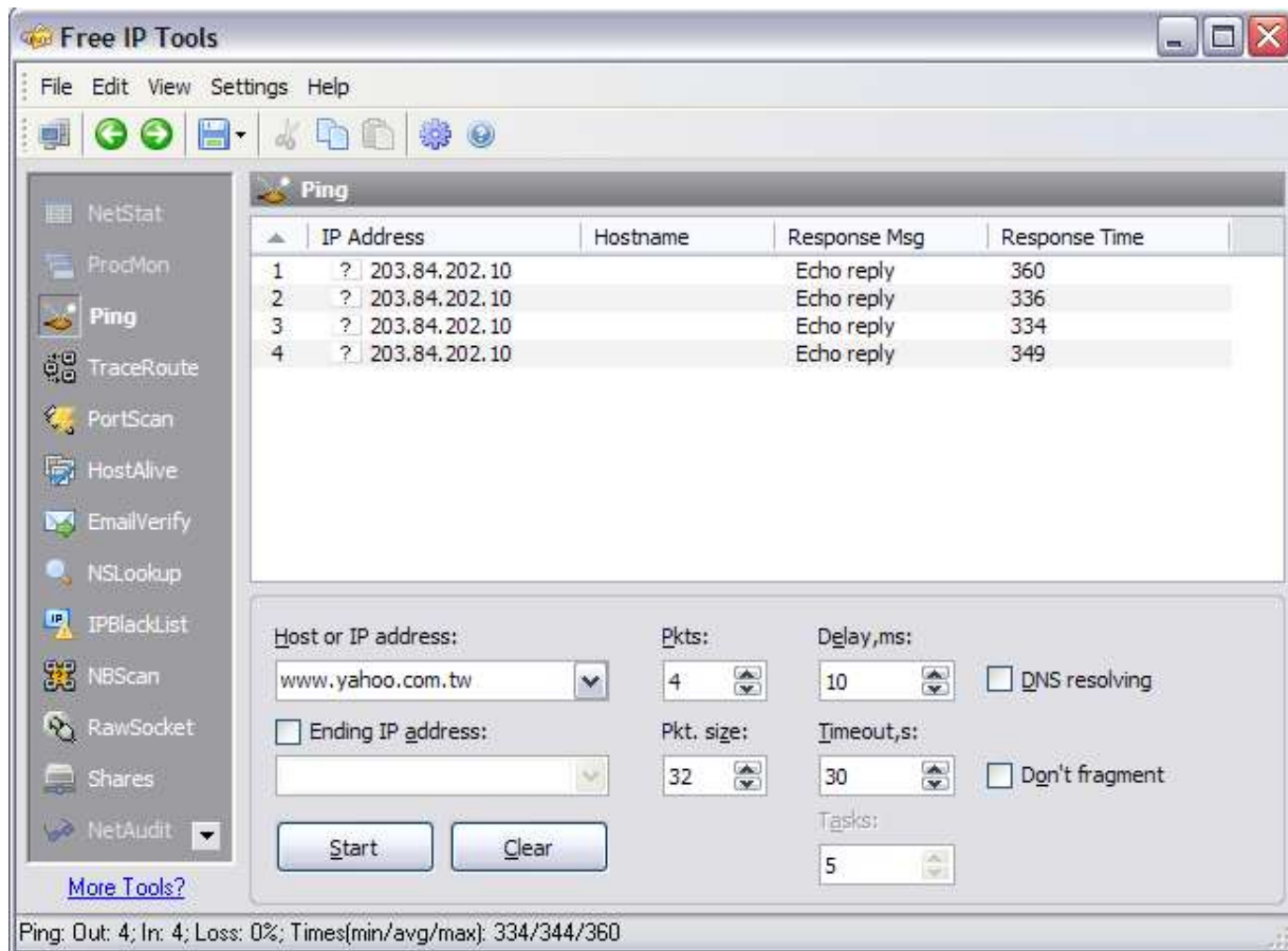
Comments on Ping

- One of best and yet simple testing tool.
    - Use ping to test a remote IP first, before you access a particular service of that remote IP, after you have set up a network.
    - ping 192.168.1.1 before you do http://192.168.1.1

- If you are very sure that your network is working fine, and yet you can't ping a particular PC, check the firewall of that PC.
    - The firewall and certain antivirus software may block the ping replies.

4. trace route

- Trace route is an "advanced" form of ping.

- Trace route lists the IP addresses that your data will travel between you and the destination IP.

- These IP addresses form a route between you and your destination IP.

- Trace route can be in the form of command and software package.
  - The better trace route software can draw the route (listed with all the IP) on the world map between your PC and the destination IP.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\          >tracert 192.168.100.107

Tracing route to websvrv1.utarict [192.168.100.107]
over a maximum of 30 hops:

  1    <1 ms     1 ms    <1 ms  192.168.39.254
  2    <1 ms    <1 ms    <1 ms  192.168.1.10
  3    <1 ms    <1 ms    <1 ms  websvrv1.utarict [192.168.100.107]

Trace complete.

C:\Users\KB607Office>
```
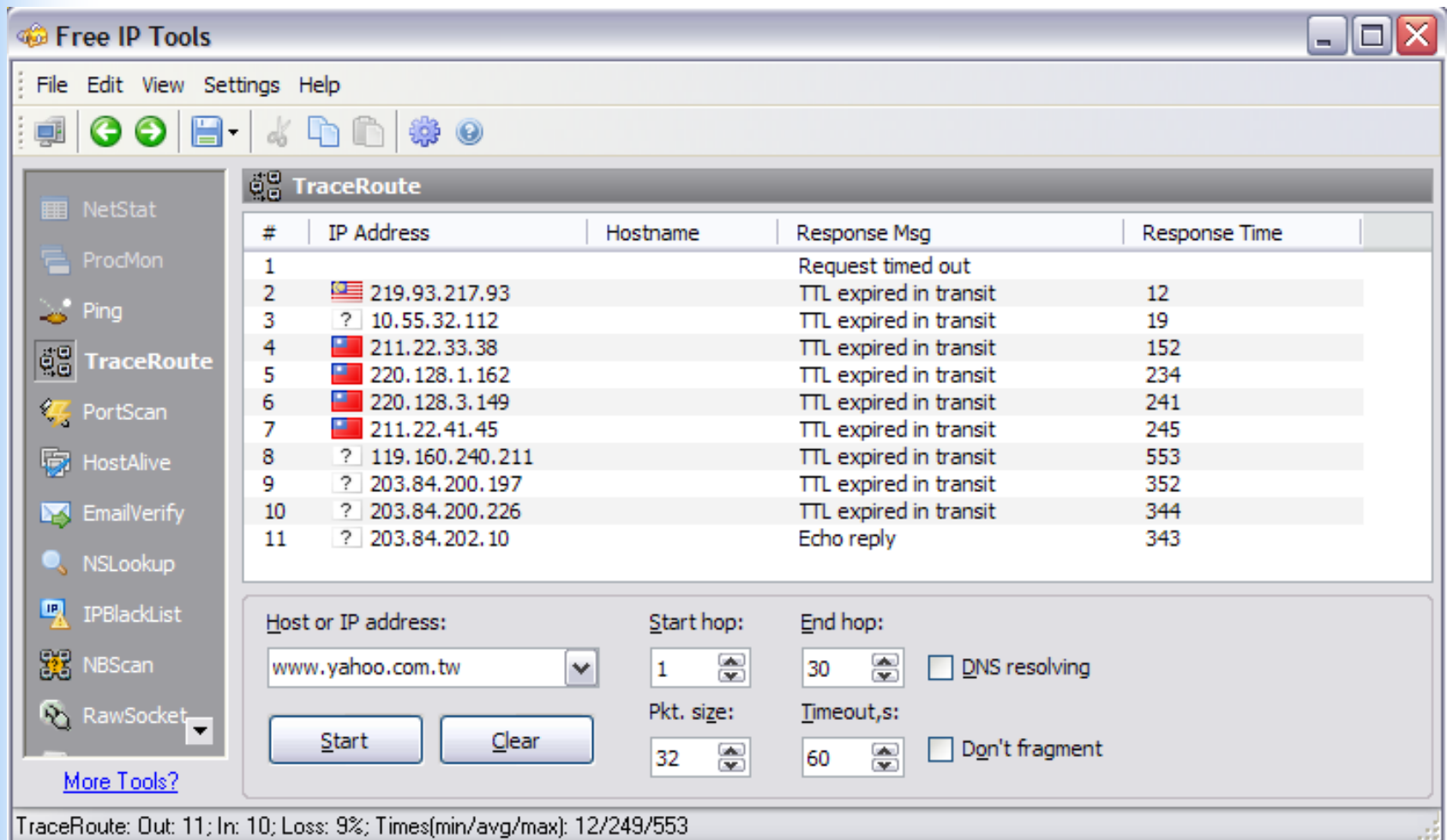
pathping

```
pathping destination_ip
pathping domain_name
```

- `C:\>pathping 192.168.1.1`
- `pathping` lists all the IP that it travels from source to destination and then computes some statistics of the route.

Free IP Tools

5. nslookup

- nslookup communicates with a DNS so that it can check the IP address of a valid domain name.

- Must have a valid DNS IP in the source IP configuration, otherwise this command won't work.

- C:>nslookup domain_name

  (c:\>nslookup www.utar.edu.my)

UTAR
UNIVERSITI TUNKU ABDUL RAHMAN

Free IP Tools
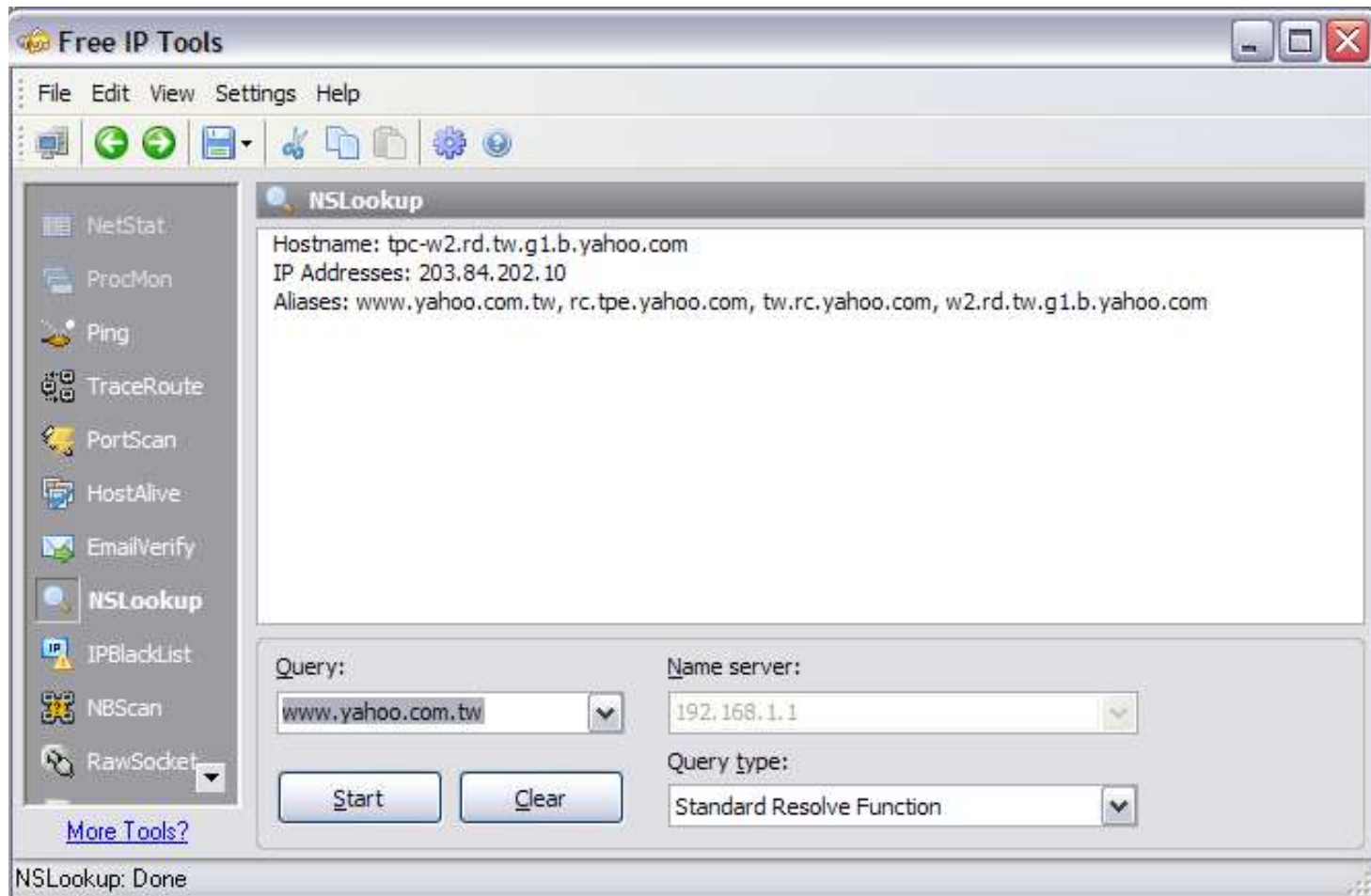
6. `hostname`

- Displays the computer name shown in the network.
- Special hostname for 127.0.0.1 = localhost

7. `getmac, getmac /v`

- Displays MAC addresses for the local system and network adapter name.

UTAR
UNIVERSITI TUNKU ABDUL RAHMAN

8. arp

ARP => Address Resolution Protocol
- "Linking" IP address to a MAC address in a lookup table
- arp lookup table is stored in a cache and it is not permanently stored.
- `arp –a`
  - show all cache
- `arp –d`
  - delete entries in cache

Port Scanning

- Test a remote IP to see whether it offers any service.

- Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer.

- A port scanner is a software application designed to probe a network host for open ports.

- May be blocked by firewall.
  - Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer.

Free IP Tools
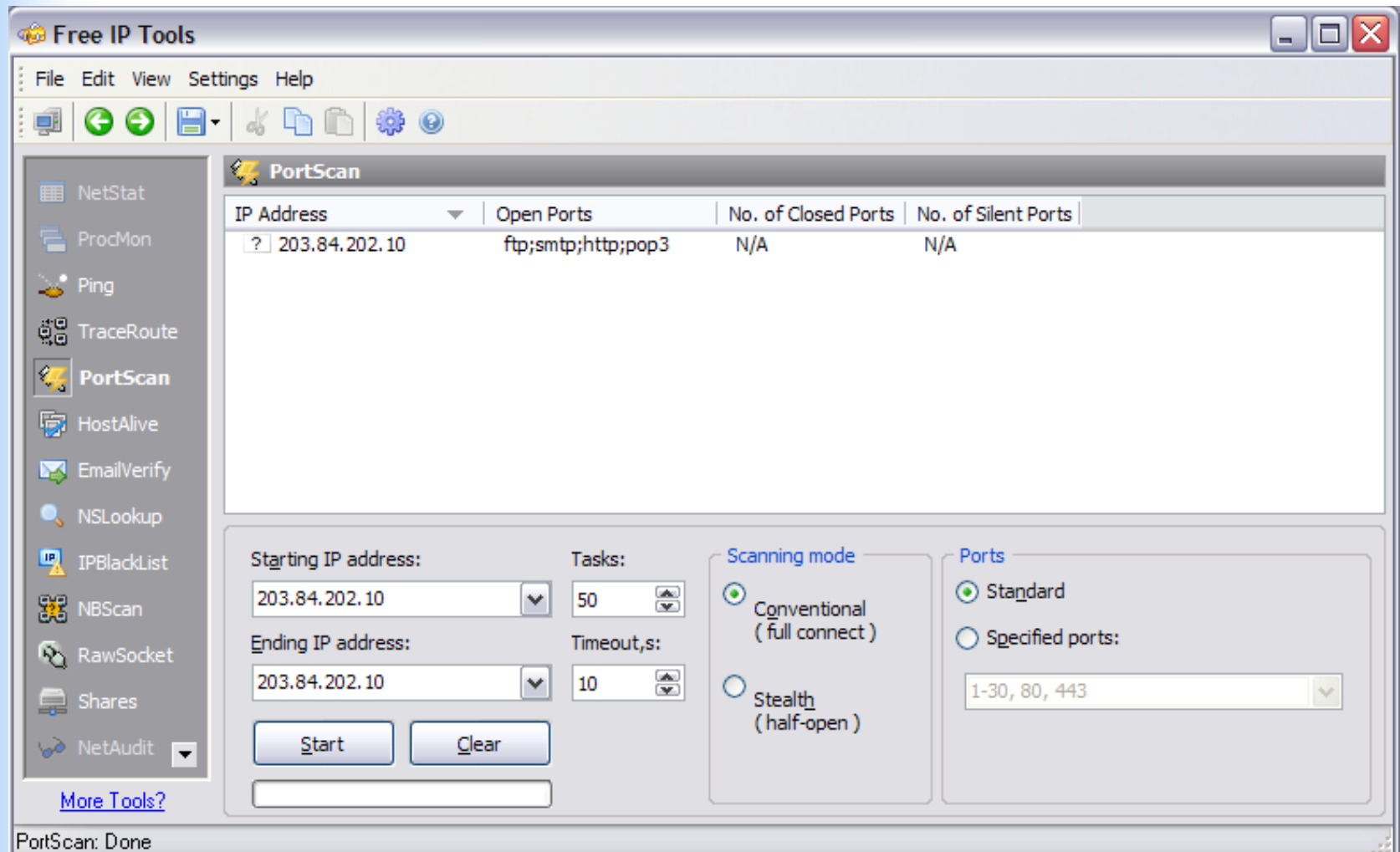
Command Line Client Software
1.telnet

- `telnet` is used to remote login to a particular server to perform remote configuration.
- You can telnet to router, modem, and server as long as these machine provide the service.
- `telnet destination_ip` or telnet `domain_name`
  - `c:\>telnet 192.168.1.1`
  - `c:\>telnet www.google.com.my`

You must have the login name and password to continue.
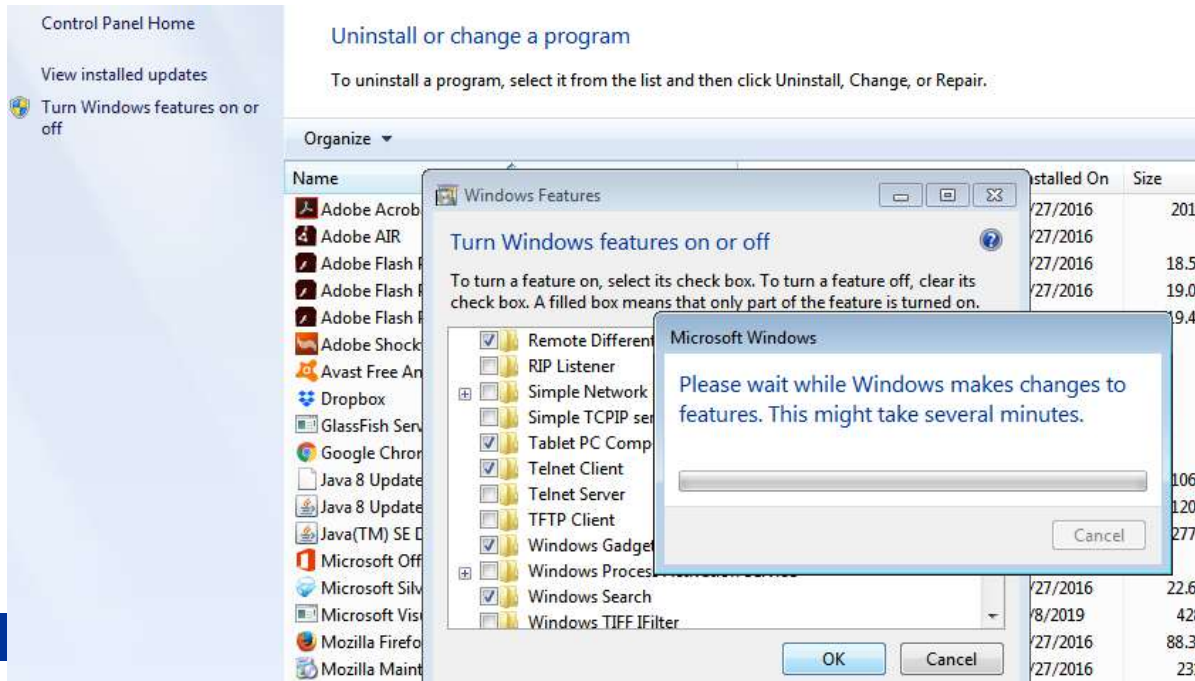
2. `ftp`

- `ftp 192.168.72.5`
- `ftp` is used to login to a file server.
  - You haven't transferred any file yet.
- You need the login name and the password.

- There is whole suite of commands after you successfully log in to the file server.
- `put` is to upload a file
- `get` is to download a file

PuTTY

- A GUI software that helps you to perform remote configuration.