Linux Systems and Open Source Software

Networking

Chia-Heng Tu
Dept. of Computer Science and Information Engineering
National Cheng Kung University
Fall 2022

Outline

- Basis of Networking
  - Overview
  - Computer Network Models
  - TCP/IP Model Layers
  - Gateway/Router
- Networking in Linux
  - Connect to Network
  - Management
  - Remote Login

Overview

Computer Network Models

TCP/IP Model Layers

Gateway/Router

NETWORKING BASIS

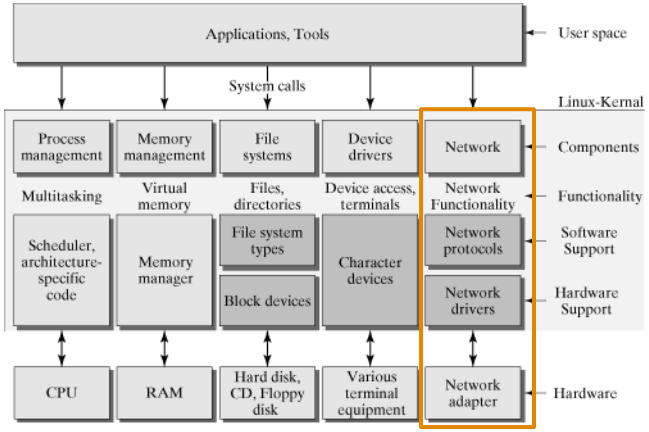
Networking

- A networking subsystem
  - relating to the ***computer network***
  - is essential to a computer system

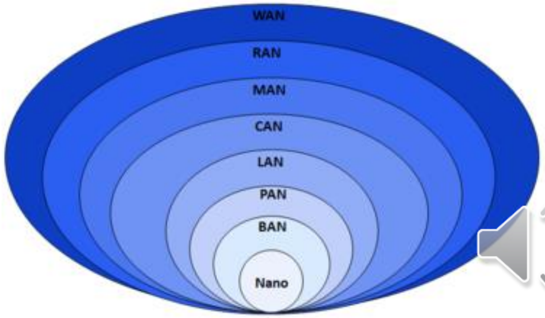
- A computer network is a group of computers
  - Using a set of common **communication protocols** over **digital interconnections** for the purpose of **sharing resources among the network nodes**
  - Network nodes are identified by **hostnames** and **network addresses**

- A computer network may be ***classified*** by many means
  - E.g., Local Area Network (LAN) as categorized by spatial scope is a network
    - connecting computers and devices in a limited geographical area such as a home, school, office building

Structure of the Linux kernel



Computer network types categorized by spatial scope

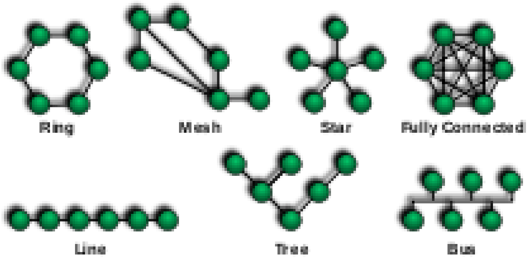


Courtesy of Computer network, Wikipedia; Linux Device Drivers, O'Reilly and Associates, 2d Ed., 2001

Digital Interconnections (Network Topology)

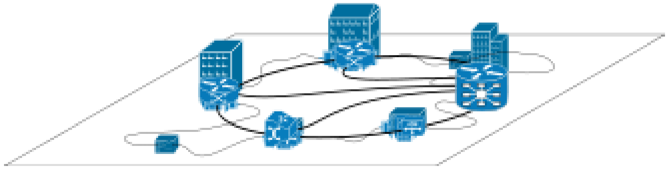
- Network topology is the layout, pattern, or organizational hierarchy of the ***interconnection of network hosts***
  - in contrast to their physical or geographic location
  - The network topology can affect throughput, but reliability is often more critical

Computer network topologies



- Overlay network
  - An overlay network is ***a virtual network*** that is built on top of another network (e.g., formed by digital interconnections)
  - Nodes in the overlay network are connected by ***virtual or logical links***
    - Each link corresponds to a path, perhaps through many physical links, in the underlying network
  - The topology of the overlay network may (and often does) differ from that of the underlying one

An example overlay network



- Gray lines are physical links among the machines, whereas the black lines are the logical links to form the overlay network on top of the physical network

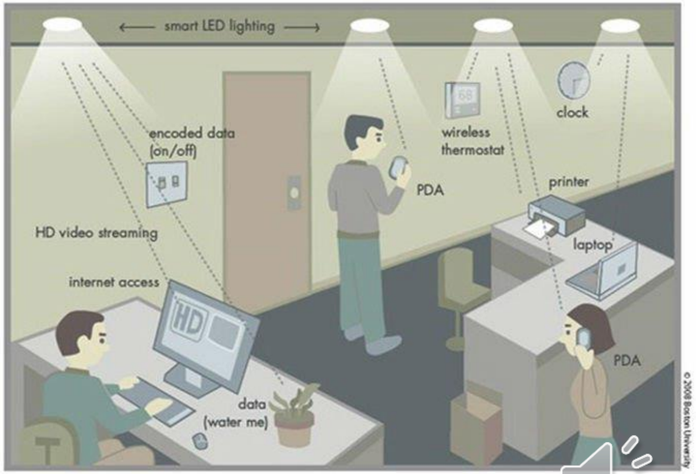
Courtesy of Computer network, Wikipedia

Network Links

- The ***transmission media*** (or physical medium) used to *link* devices to form a computer network, including
  - **wired** trans. technology: electrical cable, optical fiber
  - **wireless** trans. technology:
    - using radio or other electromagnetic means of communication
    - E.g., free space optical comm., for instance, Li-Fi uses light to transmit data between devices)

Optical fiber cables

An example of light data transmission system



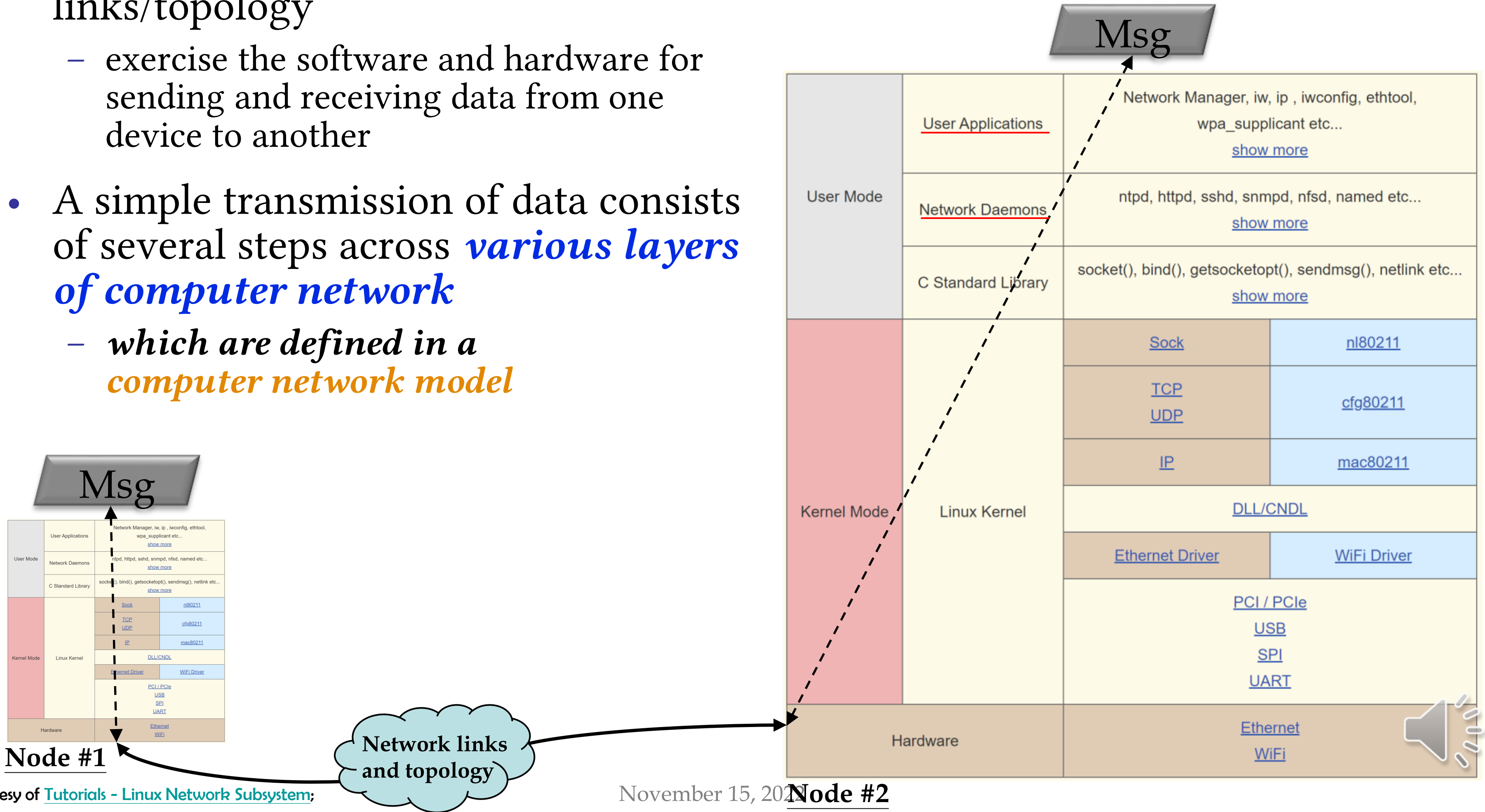
Flicking an LED on and off at extreme speeds can be used to write and transmit things in binary code

Courtesy of Computer network, Wikipedia; Li-Fi Has Just Been Tested in The Real World, And It's 100 Times Faster Than Wi-Fi

Data Exchanges between Two Devices

- Data exchanges over the network links/topology
  - exercise the software and hardware for sending and receiving data from one device to another
- A simple transmission of data consists of several steps across ***various layers of computer network***
  - ***which are defined in a computer network model***

Software Stack Related to Network Subsystem



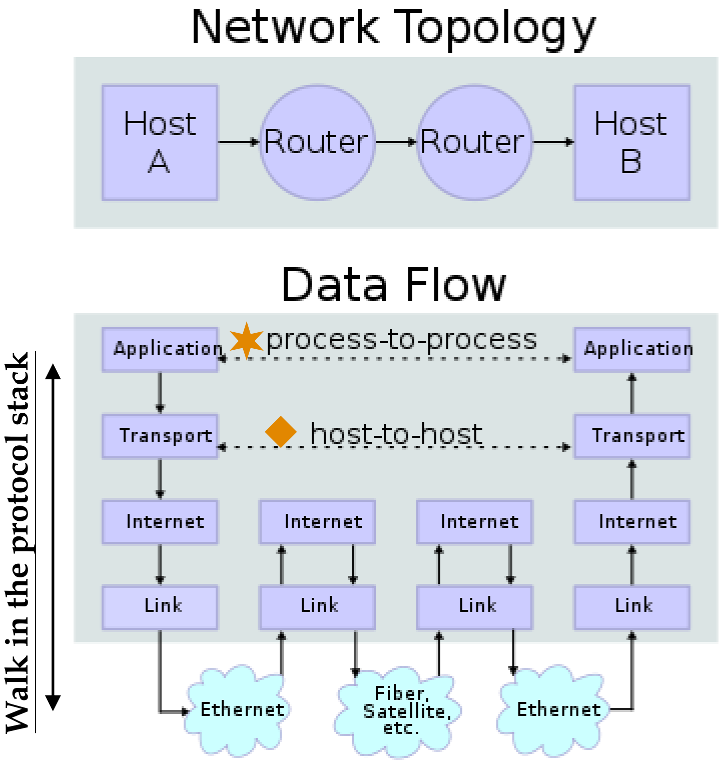
User Mode	User Applications	Network Manager, iw, ip , iwconfig, ethtool, wpa_supplicant etc... show more	
	Network Daemons	ntpd, httpd, sshd, snmpd, nfsd, named etc... show more	
	C Standard Library	socket(), bind(), getsocketopt(), sendmsg(), netlink etc... show more	
Kernel Mode	Linux Kernel	Sock	nl80211
		TCP UDP	cfg80211
		IP	mac80211
		DLL/CNDL	
		Ethernet Driver	WiFi Driver
		PCI / PCIe USB SPI UART	
Hardware		Ethernet WiFi	

Courtesy of Tutorials - Linux Network Subsystem;

Data Exchanges between Two Devices (Cont'd)

Example

- **Simple network topology**
  - of two hosts (A and B) connected by a link between their respective routers
- **Conceptual data flow across *network layers***
  - The application on each host executes read and write operations ★**as if the processes were directly connected to each other** by some kind of data pipe
  - After establishment of this pipe, most details of the communication are hidden from each process, as the underlying principles of communication are implemented in the lower protocol layers
  - In analogy, ◆**at the transport layer the communication appears as host-to-host, without knowledge of the application data structures**
  - the connecting routers, while at the internetworking layer, individual network boundaries are traversed at each router



NOTE: Hosts and Routers handle the data at the different layers

Courtesy of Key architectural principles for Internet Protocol Suite, wikipedia;

Overview

Computer Network Models

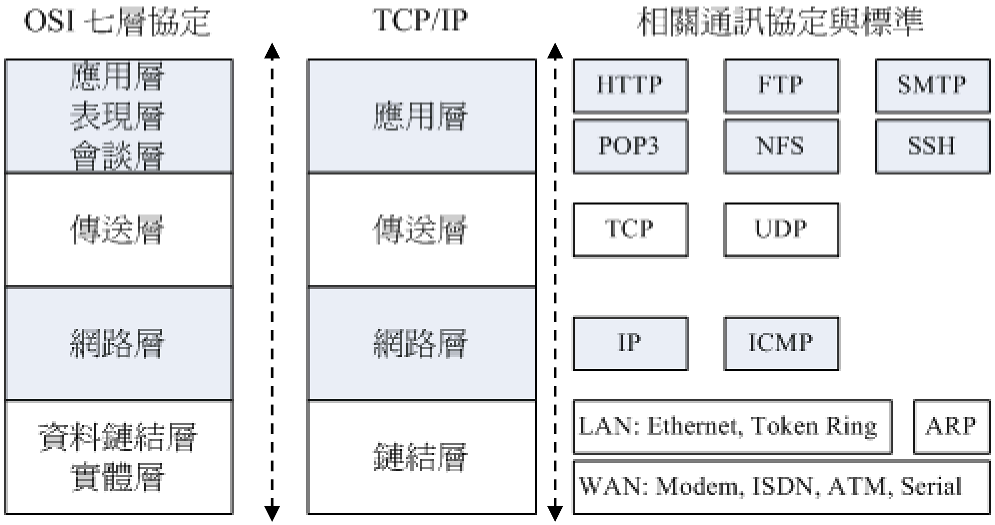
TCP/IP Model Layers

Gateway/Router

NETWORKING BASIS

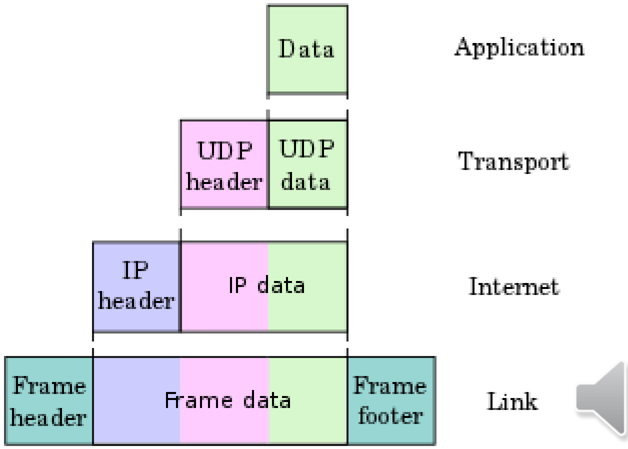
Two Major Computer Network Models

1. OSI Model
   - Stand for Open System Interconnection Model
   - **A seven-layered model** that defines how a data can be transferred between different systems
   - I.e., Application layer, presentation Layer, session layer, transport layer, network Layer, data link layer, physical layer
   - Was introduced by International Organisation for Standardisation (ISO) in 1984
2. TCP/IP Model
   - Was designed and developed by Department of Defense (DoD) in 1960s
   - **A four-layered model**: application layer, transport layer, network Layer, and data link layer & physical layer



OSI 七層協定	TCP/IP	相關通訊協定與標準
應用層 表現層 會談層	應用層	HTTP, FTP, SMTP POP3, NFS, SSH
傳送層	傳送層	TCP, UDP
網路層	網路層	IP, ICMP
資料鏈結層 實體層	鏈結層	LAN: Ethernet, Token Ring, ARP WAN: Modem, ISDN, ATM, Serial

Data Layouts



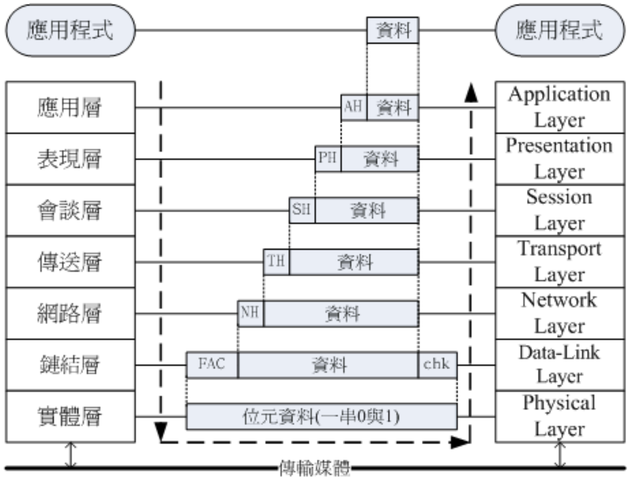
Courtesy of OSI Model in Computer Network; http://linux.vbird.org/linux_server/0110network_basic.php#whatisnetwork_osi

OSI Model

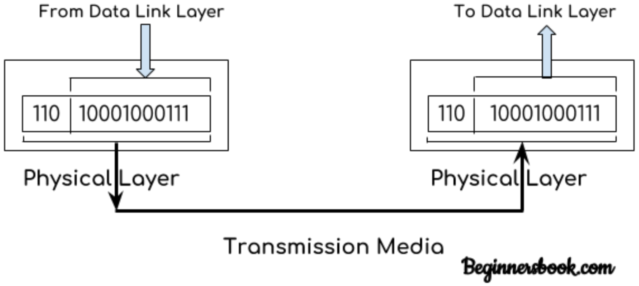
- OSI model is a conceptual model
  - Characterize and standardize the communication functions of a computing system

- Simple descriptions of **data across layers**
  - A transport layer converts the data into **segments**,
  - network layer converts the segments into ***packets*** and
  - data link layer converts the packets into frames (sent by physical layer)
  - A ***frame*** is nothing but a sequence of bits such as 1001011
  - Physical layer converts these binary sequences into **signals** and
  - transfer it through **a transmission media**, such as cables
  - You may like to which the layer does hub/switch/router work on!

Data Layouts across seven layers



Data Layout of a physical layer



- Data link layer uses a **Media Access Controller (MAC)** to generate the frames that will be transmitted
- The wireless transmission media used for Wi-Fi (or 802.11) has different requirements from the wired transmission media used for Ethernet (or 802.3), and therefore needs a different MAC and PHY

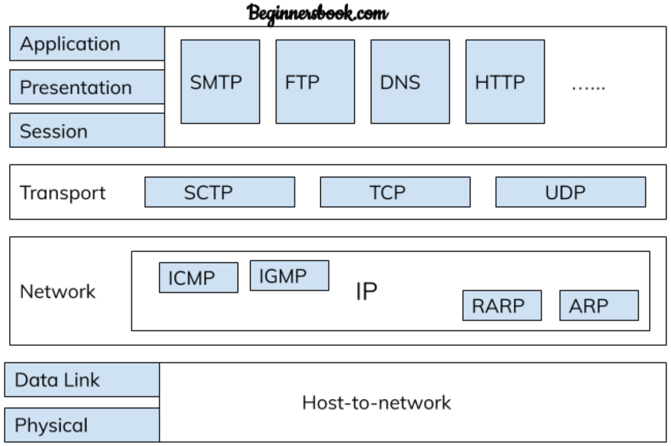
Courtesy of http://linux.vbird.org/linux_server/0110network_basic.php#whatisnetwork_osi; OSI Model in Computer Network; TCP/IP Data Link Layer (Layer 2)

TCP/IP Model

- Application Layer (presentation and session layers)
  - Is used for interaction between user and application
  - Use several protocols for user interaction, e.g., HTTP, SNMP, SMTP, DNS, TELNET, and FTP
- Transport Layer
  - Represented by three protocols: Transmission control protocol (TCP), User data gram protocol (UDP) and Stream Control Transmission Protocol (SCTP)
- Network Layer
  - Support internetworking protocol (IP)
  - IP uses four protocols internally: ARP, RARP, ICMP & IGMP
- Physical and Data Link Layer
  - Does not define any protocols
  - Support all the standard protocols
  - They are combined known as **host-to-network layer**
  - A network in TCP/IP internetwork can be **LAN** or **WAN**

TCP/IP Protocol Stack

Beginnersbook.com



Examples of OSI and TCP/IP Protocol Stacks

OSI Ref. Layer No.	OSI Layer Equivalent	TCP/IP Layer	TCP/IP Protocol Examples
5,6,7	Application, session, presentation	Application	NFS, NIS, DNS, LDAP, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP, and others
4	Transport	Transport	TCP, UDP, SCTP
3	Network	Internet	**IPv4**, IPv6, ARP, ICMP
2 1	Data link Physical	Data link Physical network	PPP, IEEE 802.2 **Ethernet** (IEEE 802.3), **Wi-Fi** (IEEE 802.11), Token Ring, RS-232, FDDI, and others

Courtesy of TCP/IP Protocol Architecture Model

Overview

Computer Network Models

TCP/IP Model Layers

Gateway/Router

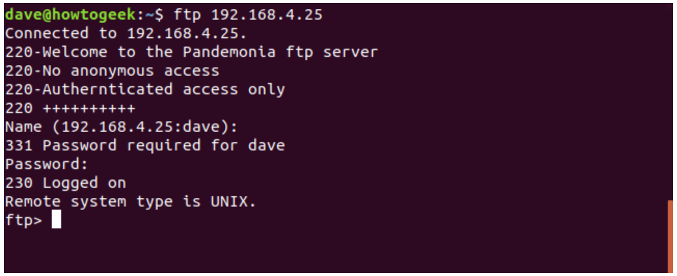
NETWORKING BASIS

Application Layer

- An abstraction layer
  - Specify the shared ***communications protocols and interface methods*** used by hosts in a computer network

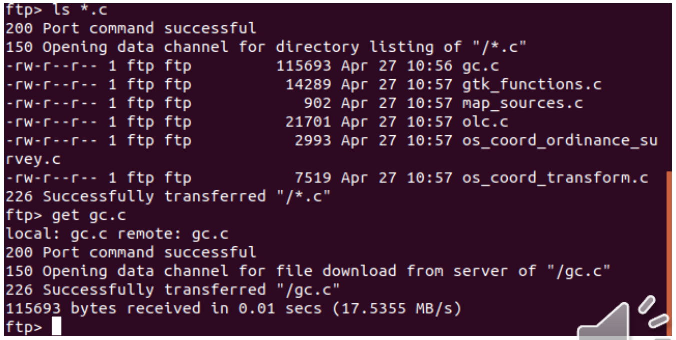
- A summary of **popular protocols** at the application layer
  - Hyper Text Transfer Protocol (HTTP)
    - It is the underlying protocol for world wide web. It defines how hypermedia messages are formatted and transmitted
  - **File Transfer Protocol (FTP)**
    - It is a client-server based protocol for transfer of files between client and server over the network
  - Secure Shell (SSH)
    - It provides a secure channel over an unsecured network by using a client–server architecture, connecting an SSH client application with an SSH server
  - SSH File Transfer Protocol (SFTP)
    - It is a network protocol that provides file access, file transfer, and file management over any reliable data stream
  - Simple Mail Transfer Protocol (SMTP)
    - It lays down the rules and semantics for sending and receiving electronic mails (e-mails)
  - Domain Name System (DNS)
    - It is a naming system for devices in networks. It provides services for translating domain names to IP addresses
  - Simple Network Management Protocol (SNMP)
    - It is for managing, monitoring the network and for organizing information about the networked devices

Logging into the FTP server (192.168.4.25)



```
dave@howtogeek:~$ ftp 192.168.4.25
Connected to 192.168.4.25.
220-Welcome to the Pandemonia ftp server
220-No anonymous access
220-Autherticated access only
220 ++++++++++
Name (192.168.4.25:dave):
331 Password required for dave
Password:
230 Logged on
Remote system type is UNIX.
ftp> 
```

List and download files from the FTP server



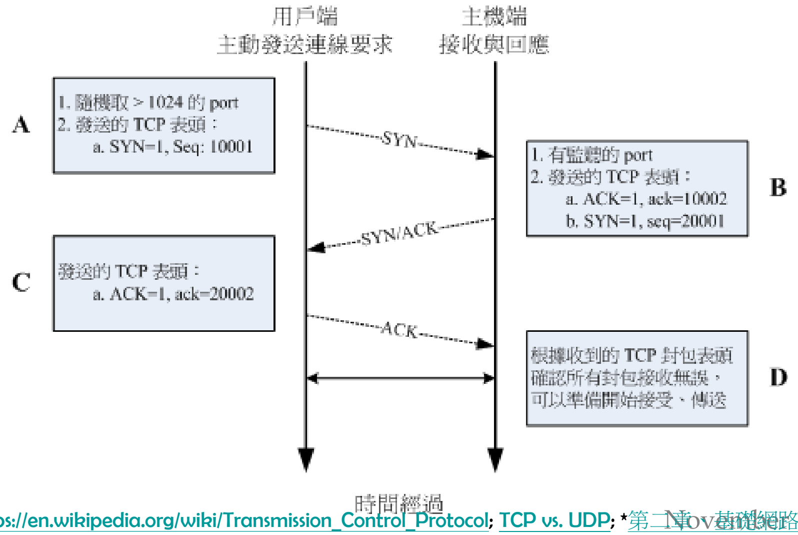
```
ftp> ls *.c
200 Port command successful
150 Opening data channel for directory listing of "/*.c"
-rw-r--r-- 1 ftp ftp         115693 Apr 27 10:56 gc.c
-rw-r--r-- 1 ftp ftp          14289 Apr 27 10:57 gtk_functions.c
-rw-r--r-- 1 ftp ftp            902 Apr 27 10:57 map_sources.c
-rw-r--r-- 1 ftp ftp          21701 Apr 27 10:57 olc.c
-rw-r--r-- 1 ftp ftp           2993 Apr 27 10:57 os_coord_ordinance_su
rvey.c
-rw-r--r-- 1 ftp ftp           7519 Apr 27 10:57 os_coord_transform.c
226 Successfully transferred "/*.c"
ftp> get gc.c
local: gc.c remote: gc.c
200 Port command successful
150 Opening data channel for file download from server of "/gc.c"
226 Successfully transferred "/gc.c"
115693 bytes received in 0.01 secs (17.5355 MB/s)
ftp> 
```

Courtesy of Application layer, Wikipedia; Protocols in Application Layer; The Application Layer in TCP/IP Model; How to Use the FTP Command on Linux

Transport Layer (TCP vs. UDP)

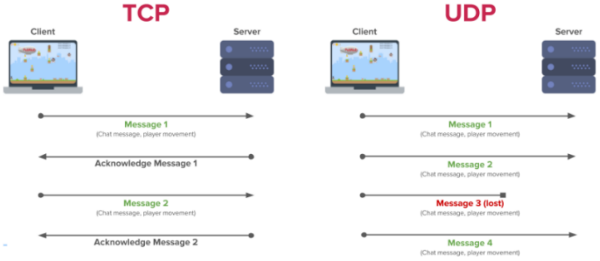
- TCP: Transmission Control Protocol
  - Provide ***reliable data delivery*** w/ ***connections*** btw hosts communicating via an Internet Protocol (IP) network
- The most famous mechanism in TCP is
  - **three-way handshake** establishing a stable connection
  1. **SYN**: Client sending a SYN to the server.
  2. **SYN-ACK**: In response, the server replies with a SYN-ACK
  3. **ACK**: Finally, the client sends an ACK back to the server

TCP connection handshake flow



- *UDP: User Datagram Protocol
  - A ***connectionless*** communication protocol
  - A very thin protocol over an IP network

Communication patterns of TCP and UDP


TCP
Client
Server
Message 1
(Chat message, player movement)
Acknowledge Message 1
Message 2
(Chat message, player movement)
Acknowledge Message 2
UDP
Client
Server
Message 1
(Chat message, player movement)
Message 2
(Chat message, player movement)
Message 3 (lost)
(Chat message, player movement)
Message 4
(Chat message, player movement)

Features comparison between TCP and UDP

Feature	TCP	UDP
Reliability	Yes	No
Data loss	No	Yes
Data transfer speed	Slow	Fast
Header size	20 bytes	8 bytes
Error checking	Yes	Yes
Error recovery	Yes	No
Flow control	Yes	No

Courtesy of https://en.wikipedia.org/wiki/Transmission_Control_Protocol; TCP vs. UDP; *第二章、基礎網路概念 - 鳥哥的 Linux 私房菜

Internet Layer

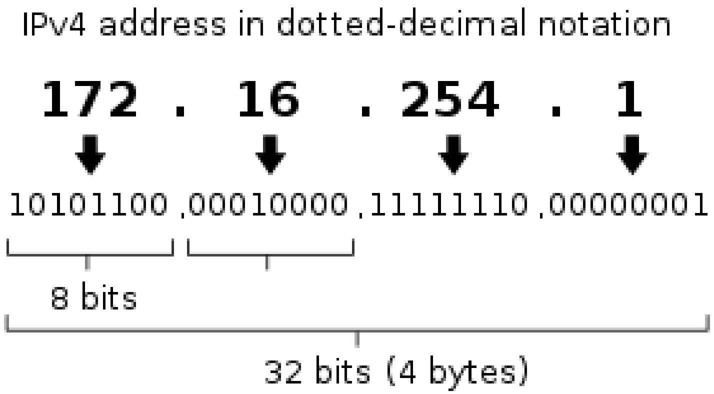
- A group of **internetworking methods, protocols, and specifications** in the Internet protocol suite
  - that are used to transport network packets from the originating host across network boundaries; if necessary, to the destination host specified by an IP address
- The internet layer has **three basic functions**:
  1. For outgoing packets, select the next-hop host (gateway) and transmit the packet to this host by passing it to the appropriate link layer implementation (for protocol stack walk)
  2. For incoming packets, capture packets and pass the packet payload up to the appropriate transport layer protocol, if appropriate
  3. Provide error detection and diagnostic capability

- Internet protocol suite
  - The conceptual model and set of communications protocols used in the Internet and similar computer networks
  - The principal communication protocol in the suite is **Internet Protocol (IP)** **for relaying datagrams across network boundaries; its routing function enables internetworking**
  - It is commonly known as TCP/IP, which is the fundamental protocols in the suite
  - The communications protocol that provides **an identification and location system** for computers on networks and routes traffic across the Internet

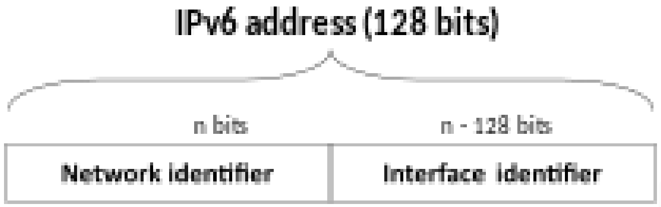
Courtesy of Internet layer, Wikipedia; Internet protocol suite, Wikipedia;

Internet Layer (IPv4 and IPv6)

- IPv4 (Internet Protocol version 4) is the fourth version of IP
  - It is one of the core protocols of standards-based internetworking methods in the **Internet** and other packet-switched networks
  - Designed for delivering packets from the source host to the destination based on the **IP addresses in the packet headers**
- IPv4 uses 32-bit addresses
  - which limits the address space to 4,294,967,296 (2^{32}) addresses
  - They are most often written in dot-decimal notation, which consists of four octets of the address expressed individually in decimal numbers and separated by periods, as shown below



- IPv6 (Internet Protocol version 6) is the most recent version of IP
  - IPv6 is intended to replace IPv4
- IPv6 uses 128-bit addresses
  - theoretically allowing 2^{128}, or approximately 3.4×10^{38} addresses
- An IPv6 address is represented in 8 groups of 16 bits each
  - **2001:0db8:0000:0000:0000:ff00:0042:8329**
- Address space consists of network and interface identifiers similar to IPv4
  - **Network identifier** is the most-significant 64 bits, used as the routing prefix
  - **Interface identifier** is the following 64 bits for the host portion of address within a local area subnet



Courtesy of IPv4, Wikipedia; IPv6, wikipedia

Internet Layer
More about IPv4

- The range of a 32-bit IP address
  - 0.0.0.0 ~ 255.255.255.255
  - An IP address is comprised of the **network identifier** and the **host identifier**
  - Allow uniquely identify a host
- A classful network address architecture is used to establish sufficient *networks*
  - by introducing different bit lengths for network identification for creating **five different network classes**

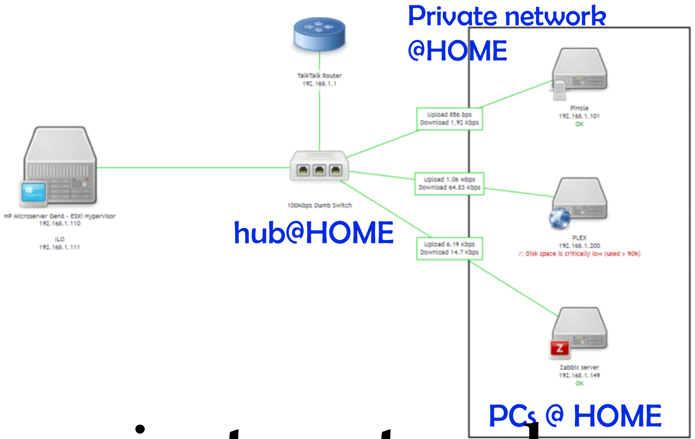
```
The bit-length of network identifier in different network clases
Class A : 0xxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx ==> Net ID 的開頭是 0
          |--net---|-----------host-----------|
Class B : 10xxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx ==> Net ID 的開頭是 10
          |------net--------|-------host-------|
Class C : 110xxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx ==> Net ID 的開頭是 110
          |-----------net-----------|---host--|
Class D : 1110xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx ==> Net ID 的開頭是 1110
Class E : 1111xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx ==> Net ID 的開頭是 1111
五種分級在十進位的表示：
Class A : 0.xx.xx.xx ~ 127.xx.xx.xx
Class B : 128.xx.xx.xx ~ 191.xx.xx.xx
Class C : 192.xx.xx.xx ~ 223.xx.xx.xx
Class D : 224.xx.xx.xx ~ 239.xx.xx.xx
Class E : 240.xx.xx.xx ~ 255.xx.xx.xx
```

- Create subnets with ***netmask***
  - The subset (192.168.0.0 – 192.168.0.255) within the Class C domain
  - The netmask expression: **192.168.0.0/24** means the IPs from 192.168.0.0 – 192.168.0.255 (as shown in the image below)
    - The **/24** means the netmask has 24 bit 1s for network identifier
  - Usable IPs: 192.168.0.1~192.168.0.254
    - The network segment is represented by: 192.168.0.0
    - The broadcast address: 192.168.0.255

```
A subnet within Class C
11000000.10101000.00000000.00000000 IP: 192.168.0.0
11000000.10101000.00000000.11111111 IP: 192.168.0.255
11111111.11111111.11111111.00000000 Netmask: 255.255.255.0
Network:   192.168.0.0     <==第一個 IP
Broadcast: 192.168.0.255   <==最後一個 IP
可用以設定成為主機的 IP 數：
192.168.0.1 ~ 192.168.0.254
```

Courtesy of IPv4, Wikipedia;第二章、基礎網路概念 2.3 TCP/IP 的網路層相關封包與資料, 鳥哥的 Linux 私房菜;

Internet Layer
IPv4 Private Networks



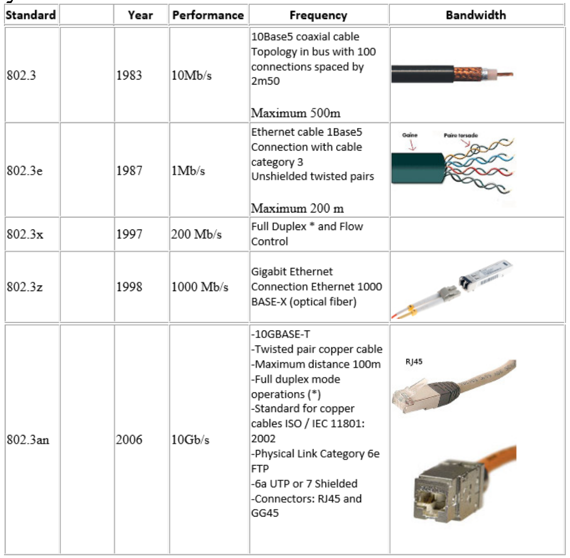
- IPv4 reserves special address blocks for **private networks**
  - Approximately four billion addresses in total defined in IPv4
  - About 18 million addresses in three ranges are reserved for use in private networks
    - Class A：10.0.0.0 - 10.255.255.255
    - Class B：172.16.0.0 - 172.31.255.255
    - Class C：192.168.0.0 - 192.168.255.255 (most common one; used in your home)
- Packets addresses in these ***private*** ranges are not routable in the public Internet
  - they are ignored by all public routers
  - Therefore, private hosts cannot **directly communicate with** public networks,
  - but require network address translation at a routing gateway for this purpose

Courtesy of 第二章、基礎網路概念 2.3 TCP/IP 的網路層相關封包與資料, 鳥哥的 Linux 私房菜; image source

Physical Layer
(Ethernet Cables and Wi-Fi Networks)

Ethernet cables (IEEE 802.3)

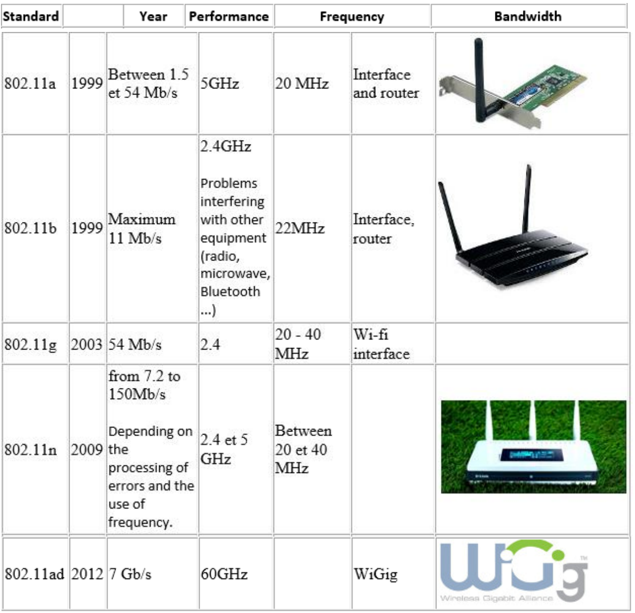
- This standard specifies what happens at the level of the layer of **wired networks**
- Check this page for the complete list of 802.3 standards
  - defining the physical layer and data link layer's MAC of wired Ethernet



Standard		Year	Performance	Frequency	Bandwidth
802.3		1983	10Mb/s	10Base5 coaxial cable Topology in bus with 100 connections spaced by 2m50 Maximum 500m	
802.3e		1987	1Mb/s	Ethernet cable 1Base5 Connection with cable category 3 Unshielded twisted pairs Maximum 200 m	
802.3x		1997	200 Mb/s	Full Duplex * and Flow Control	
802.3z		1998	1000 Mb/s	Gigabit Ethernet Connection Ethernet 1000 BASE-X (optical fiber)	
802.3an		2006	10Gb/s	-10GBASE-T -Twisted pair copper cable -Maximum distance 100m -Full duplex mode operations (*) -Standard for copper cables ISO / IEC 11801: 2002 -Physical Link Category 6e FTP -6a UTP or 7 Shielded -Connectors: RJ45 and GG45	

Wi-Fi Networks (IEEE 802.11)

- This standard specifies what happens at the level of the layer of **wireless networks**
- The latest standard 802.11ax (Wi-Fi 6) is announced in 2019
  - Check this page for the list of Wi-Fi generations



Standard	Year	Performance	Frequency	Bandwidth		
802.11a	1999	Between 1.5 et 54 Mb/s	5GHz	20 MHz	Interface and router	
802.11b	1999	Maximum 11 Mb/s	2.4GHz Problems interfering with other equipment (radio, microwave, Bluetooth ...)	22MHz	Interface, router	
802.11g	2003	54 Mb/s	2.4	20 - 40 MHz	Wi-fi interface	
802.11n	2009	from 7.2 to 150Mb/s Depending on the processing of errors and the use of frequency.	2.4 et 5 GHz	Between 20 et 40 MHz		
802.11ad	2012	7 Gb/s	60GHz		WiGig	

Courtesy of IEEE standards, Ethernet cables and Wi-Fi networks

Overview

Computer Network Models

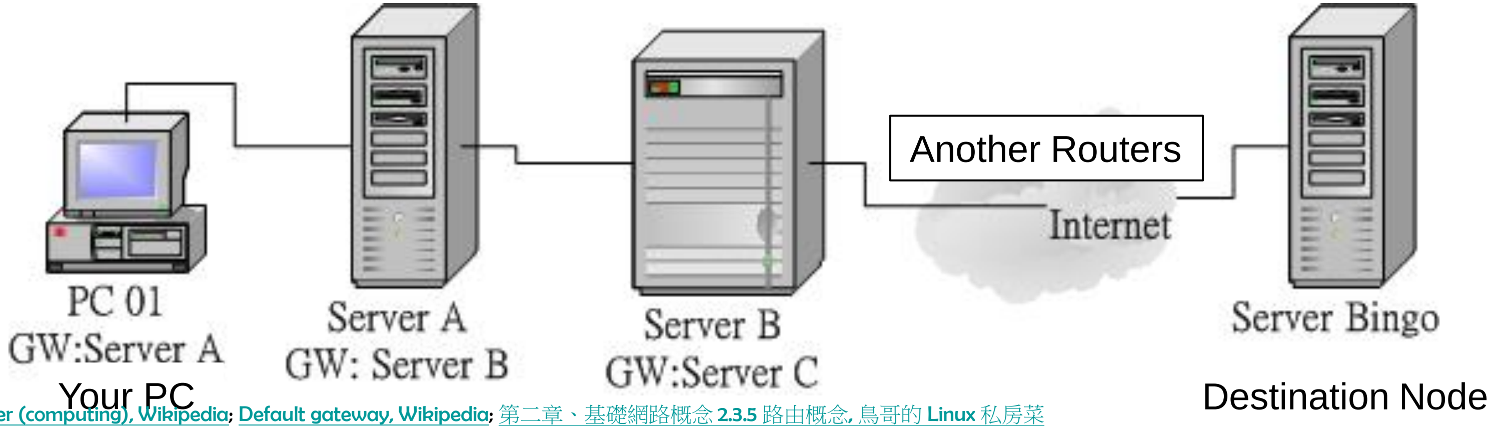
TCP/IP Model Layers

Gateway/Router

NETWORKING BASIS

Router and Gateway

- A **router** is a networking device that forwards data packets between different computer networks (e.g., different network segments)
  - There is a ***route table*** on each router to assist the routing decision
- A **default gateway**
  - is the node in a computer network using the internet protocol suite that
  - serves as the forwarding host (router) to other networks when no other route specification matches the destination IP address of a packet
- A packet is forwarded from one router to another router
  - through the networks that constitute an internetwork (e.g., the Internet) until it reaches its destination node (by examining the packet's target IP address)
- An illustration of sending data from PC01 to Server Bingo



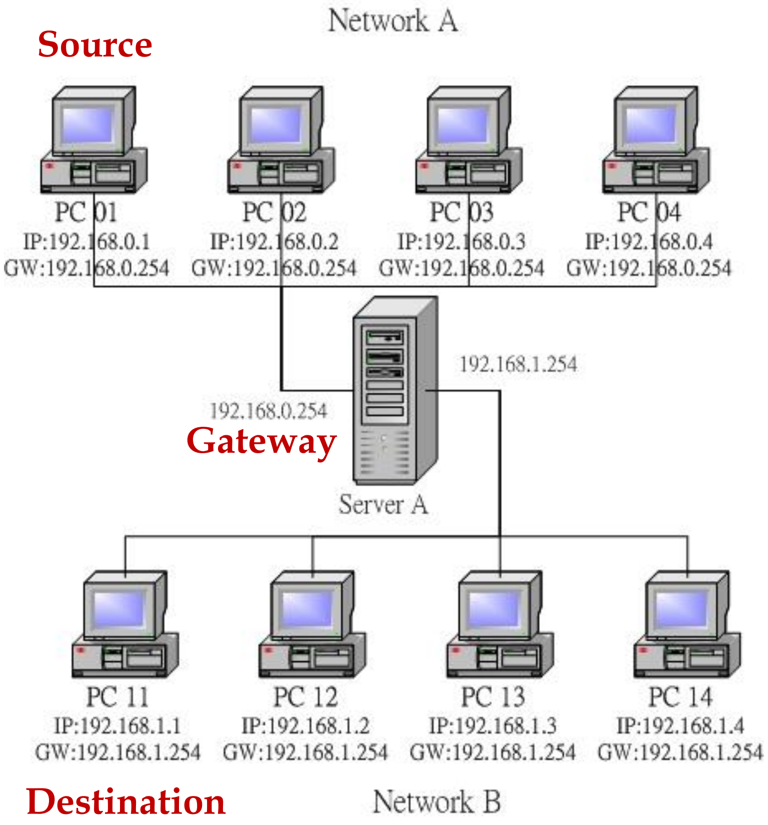
Courtesy of Router (computing), Wikipedia; Default gateway, Wikipedia; 第二章、基礎網路概念 2.3.5 路由概念, 鳥哥的 Linux 私房菜

Packet Delivery

- Routing different networks
  - Interior router: A router in a local area network (LAN) of a single organization
  - Exterior router: A router that is operated in the Internet backbone
  - **Gateway router** (border router): A router connects a LAN with the Internet or a wide area network (WAN)
- Example: sending data from PC01 in Network A to PC11 in Network B
  - Source IP: 192.168.0.1; dest IP: 192.168.1.1
  - The IPs 192.168.0.0/24 and the IPs 192.168.1.0/24 are in different network segments
  - Packets are processed in the following steps:

1. PC01 check its routing table for the matching rule for dest IP address: 192.168.1.1
2. As dest IP is not within the same segment with PC01 and there is no matching routing rule, the data packets are sent to the default gateway (Server A: 192.168.0.254)
3. The gateway receives the packets and check for its routing table
4. As the gateway happens to link Network A and Network B, it is able to forward the received packets from PC01 to PC11 in Network B

Example of routing data from Network A to Network B.



- Usually, a gateway server has several NICs connecting with different networks, which is how they can do routing
- E.g., Server A is in Network A and B at the same time

Courtesy of http://linux.vbird.org/linux_server/0110network_basic.php#tcpip_network_route

Connection

Management

Remote Login

NETWORKING IN LINUX

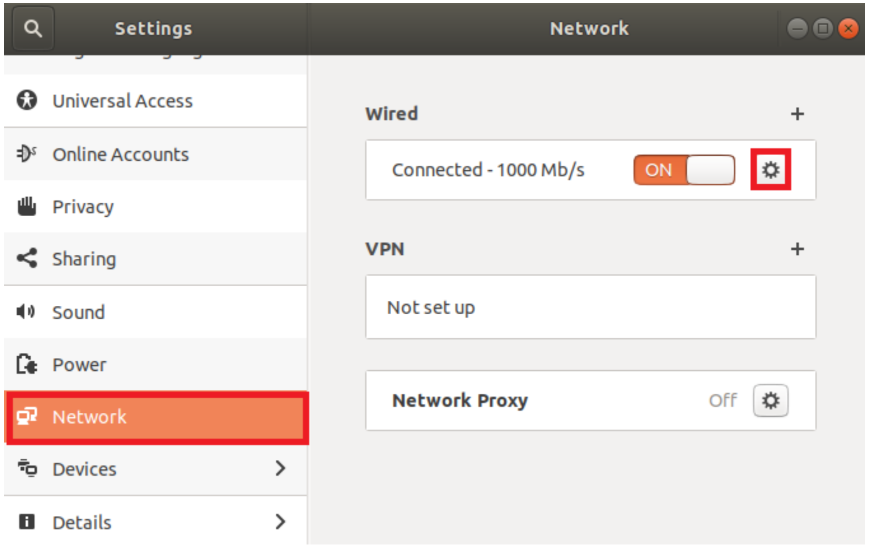
Acquire an IP

- Several ways to obtain an IP to get online
  1. Issued by **your academic department** (e.g., Taiwan Academic Network, TANet)
  2. Obtained from **Internet Service Provider** (ISP) (e.g., Chunghwa Telecom ADSL)
  3. Use **dynamic host configuration protocol** (DHCP) to get a random IP from ISP (the most common way)
  4. …
- With **a static IP address** for your computer,
  - you will need to manually set up network configurations to surf Internet
  - A static IP address could be either public or private address

Courtesy of 第四章、連上 Internet 4.2 連上 Internet 的設定方法, 鳥哥的 Linux 私房菜;

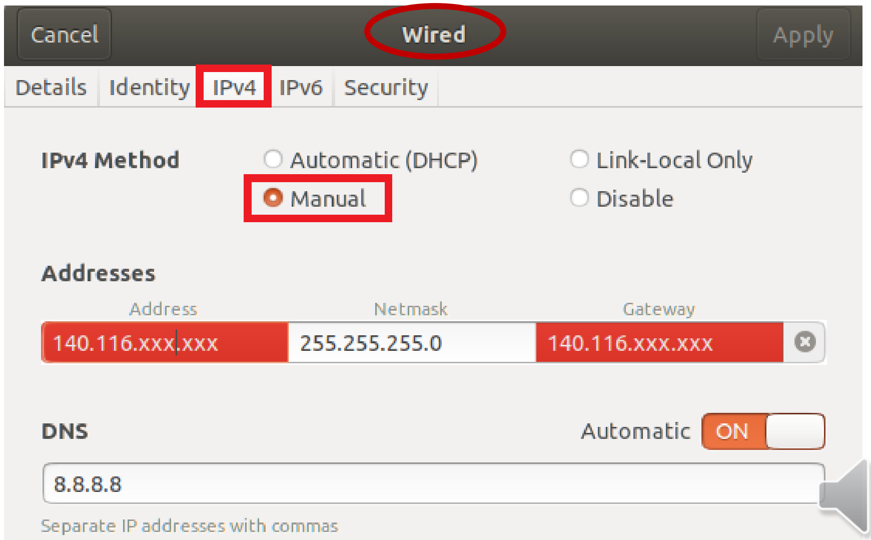
Configure Static IP in Ubuntu 18.04

- You can set up the static IP in ubuntu 18.04 w/ GUI
  1. Ubuntu18.04 Settings → Network → IPv4
  2. **Address** (static IP), **Netmask**, and **Gateway** (Your router IP)
     - Example: Static IP: : 140.116.xxx.xxx, Netmask: 255.255.255.0 (a common setting), Gateway: 140.116.xxx.254 (the last valid IP address in the segment)
  3. DNS (IP for Domain Name System Service)
     - E.g., 8.8.8.8 (Google) or 163.28.113.1 (NCKU)



Wired: Connected - 1000 Mb/s ON

VPN: Not set up



IPv4 Method: ○ Automatic (DHCP) ● Manual ○ Link-Local Only ○ Disable

Addresses

Address	Netmask	Gateway
140.116.xxx.xxx	255.255.255.0	140.116.xxx.xxx

DNS — Automatic ON

8.8.8.8

Separate IP addresses with commas

Configure Static IP in Ubuntu 18.04 (Cont'd)

- You can set up the static IP in ubuntu 18.04 w/ ***netplan*** package in command line
  - **/etc/netplan/50-cloud-init.yaml** file keeps the configuration for every network interfaces (cards) in Ubuntu 18.04; use the commands in the following pages to change the setting

```
[root@study ~]# cat /etc/netplan/50-cloud-init.yaml
# The network interface for Linux 2020
network:
    ethernets:
        ens192:                             網卡代號
            addresses: [192.168.32.231/24]  your static IP + mask
            gateway4: 192.168.32.1          your router IP
            nameservers:
              addresses: [8.8.8.8,8.8.4.4]  你選用的 DNS 服務，此處是 Google
            dhcp4: no                       是否啟用 dhcp
version: 2
[root@study ~]# sudo netplan try
```

  - **dhclient** - Dynamic Host Configuration Protocol Client

```
[root@www ~]# dhclient {interface}
[root@www ~]# dhclient eth0 //Use DHCP to configure the NIC: eth0
```

- Sometimes, you need to restart the NIC for your changes to apply
- Check the following pages for the NIC management commands

Courtesy of 第四章、連上 Internet 4.2 連上 Internet 的設定方法, 鳥哥的 Linux 私房菜;

Connection

Management

Remote Login

NETWORKING IN LINUX

Networking Management Commands

- **ifconfig** - configure a network interface

```
[root@www ~]# ifconfig {interface} {up|down} <== 觀察與啟動介面
選項與參數: interface：網路卡介面代號，包括 eth0, eth1, ppp0 等等
#範例1：觀察所有的網路介面(直接輸入 ifconfig)
[root@www ~]# ifconfig
eth0    Link encap:Ethernet HWaddr 08:00:27:71:85:BD              HWaddr硬體地址MAC
        inet addr:192.168.1.100 Bcast:192.168.1.255 Mask:255.255.255.0   IPv4地址
        inet6 addr: fe80::a00:27ff:fe71:85bd/64 Scope:Link           IPv6地址
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:2555 errors:0 dropped:0 overruns:0 frame:0          接收封包情形
        TX packets:70 errors:0 dropped:0 overruns:0 carrier:0          傳輸封包情形
        collisions:0 txqueuelen:1000                              封包碰撞情形
        RX bytes:239892 (234.2 KiB) TX bytes:11153 (10.8 KiB)          總計
#範例2： Use ifconfig to set eth0 IP address
[root@www ~]# ifconfig eth0 192.168.1.99
```

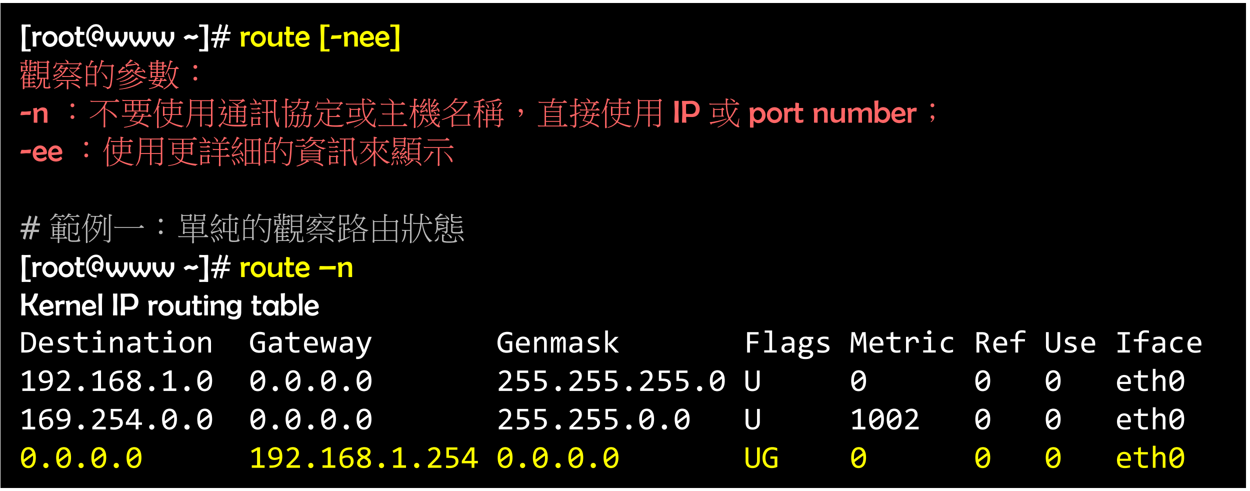
- **ifup** - bring a network interface up
- **ifdown** - take a network interface down

```
[root@www ~]# ifup {interface}
[root@www ~]# ifdown {interface}

#啟動 eth0 網卡
[root@www ~]# ifup eth0
```

Courtesy of 第五章、 Linux 常用網路指令 5.1.1 手動/自動設定與啟動/關閉 IP 參數, 鳥哥的 Linux 私房菜;

Networking Management Commands (Cont'd)

- **route** - show and manipulate the IP routing table
  - **Destination** - the destination network or destination host
  - **Genmask** - the netmask for the destination net
    The destination network segment: **Destination/Genmask**
  - **Flags** - States, e.g., **U** (route is up), **G** (use gateway)
  - **Metric** - The *distance* to the target (usually counted in hops)
  - **Iface** - Interface to which packets for this route will be sent
- NOTE: usually, there is a routing table for a NIC

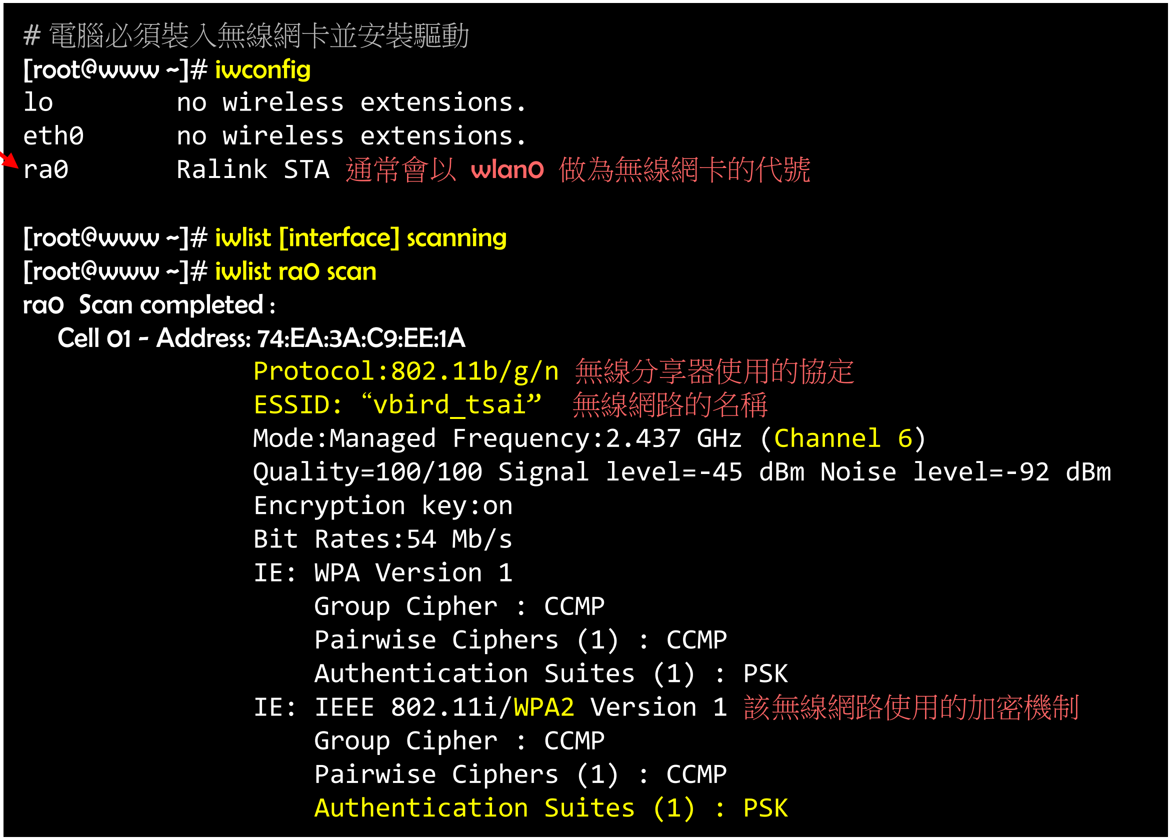


```
[root@www ~]# route [-nee]
觀察的參數：
-n ：不要使用通訊協定或主機名稱，直接使用 IP 或 port number；
-ee ：使用更詳細的資訊來顯示

# 範例一：單純的觀察路由狀態
[root@www ~]# route –n
Kernel IP routing table
Dest. HOST Name  Destination   Gateway        Genmask         Flags Metric Ref Use Iface
                 192.168.1.0   0.0.0.0        255.255.255.0   U     0      0   0   eth0
      link-local 169.254.0.0   0.0.0.0        255.255.0.0     U     1002   0   0   eth0
      default    0.0.0.0       192.168.1.254  0.0.0.0         UG    0      0   0   eth0
```

Courtesy of 第五章、 Linux 常用網路指令 5.1.2 路由修改, 鳥哥的 Linux 私房菜; route(8): show/change IP routing table - Linux man page

Networking Management Commands for Wireless Network

- **iwconfig** - configure a wireless network interface
- **iwlist** - get more detailed wireless information from a wireless interface
  - **scan** - Scan and give the list of Access Points and Ad-Hoc cells in range



```
# 電腦必須裝入無線網卡並安裝驅動
[root@www ~]# iwconfig
lo        no wireless extensions.
eth0      no wireless extensions.
ra0       Ralink STA 通常會以 wlan0 做為無線網卡的代號

[root@www ~]# iwlist [interface] scanning
[root@www ~]# iwlist ra0 scan
ra0  Scan completed :
    Cell 01 - Address: 74:EA:3A:C9:EE:1A
                    Protocol:802.11b/g/n 無線分享器使用的協定
                    ESSID: "vbird_tsai"  無線網路的名稱
                    Mode:Managed Frequency:2.437 GHz (Channel 6)
                    Quality=100/100 Signal level=-45 dBm Noise level=-92 dBm
                    Encryption key:on
                    Bit Rates:54 Mb/s
                    IE: WPA Version 1
                        Group Cipher : CCMP
                        Pairwise Ciphers (1) : CCMP
                        Authentication Suites (1) : PSK
                    IE: IEEE 802.11i/WPA2 Version 1 該無線網路使用的加密機制
                        Group Cipher : CCMP
                        Pairwise Ciphers (1) : CCMP
                        Authentication Suites (1) : PSK
```

Courtesy of 第五章、 Linux 常用網路指令 5.1.4 無線網路, 鳥哥的 Linux 私房菜; iwlist(8) - Linux man page; iwconfig(8) - Linux man page

Test the Connection of Your PC

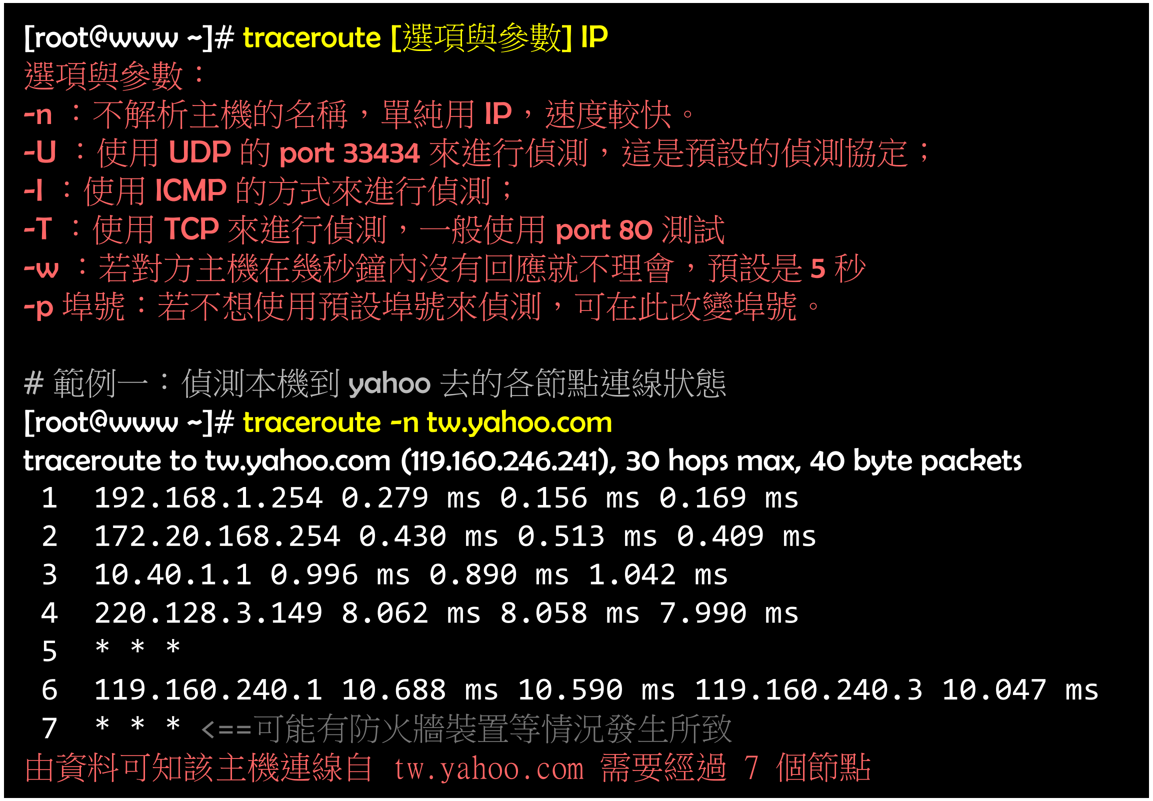
- **ping** - send ICMP (ICMP6) ECHO_REQUEST packets to network hosts
  - The ping lets you know how long the network took to transmit that data and get a response

```
[root@www ~]# ping [選項與參數] IP
選項與參數：
-c 數值：後面接的是執行 ping 的次數，例如 -c 5 ；
-s 數值：發送出去的 ICMP 封包大小，預設為 56bytes；
-W 數值：等待回應對方主機的秒數。

 # 範例一：偵測 168.95.1.1 這部 DNS 主機是否存在？
[root@www ~]# ping -c 3 168.95.1.1
PING 168.95.1.1 (168.95.1.1) 56(84) bytes of data.
64 bytes from 168.95.1.1: icmp_seq=1 ttl=245 time=15.4 ms
64 bytes from 168.95.1.1: icmp_seq=2 ttl=245 time=10.0 ms
64 bytes from 168.95.1.1: icmp_seq=3 ttl=245 time=10.2 ms
封包大小                  第幾次偵測     ↑    回應時間
                                 (255-經過節點數量)

--- 168.95.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2047ms
rtt min/avg/max/mdev = 10.056/11.910/15.453/2.506 ms
```

Courtesy of 第五章、 Linux 常用網路指令 5.1.4 無線網路, 鳥哥的 Linux 私房菜; iwlist(8) - Linux man page; iwconfig(8) - Linux man page

Trace Packets Route

- **traceroute** - print the trace of route packets to network host at **IP**
  - Use different methods to do the test: **-U** (default), **-I**, **-T**

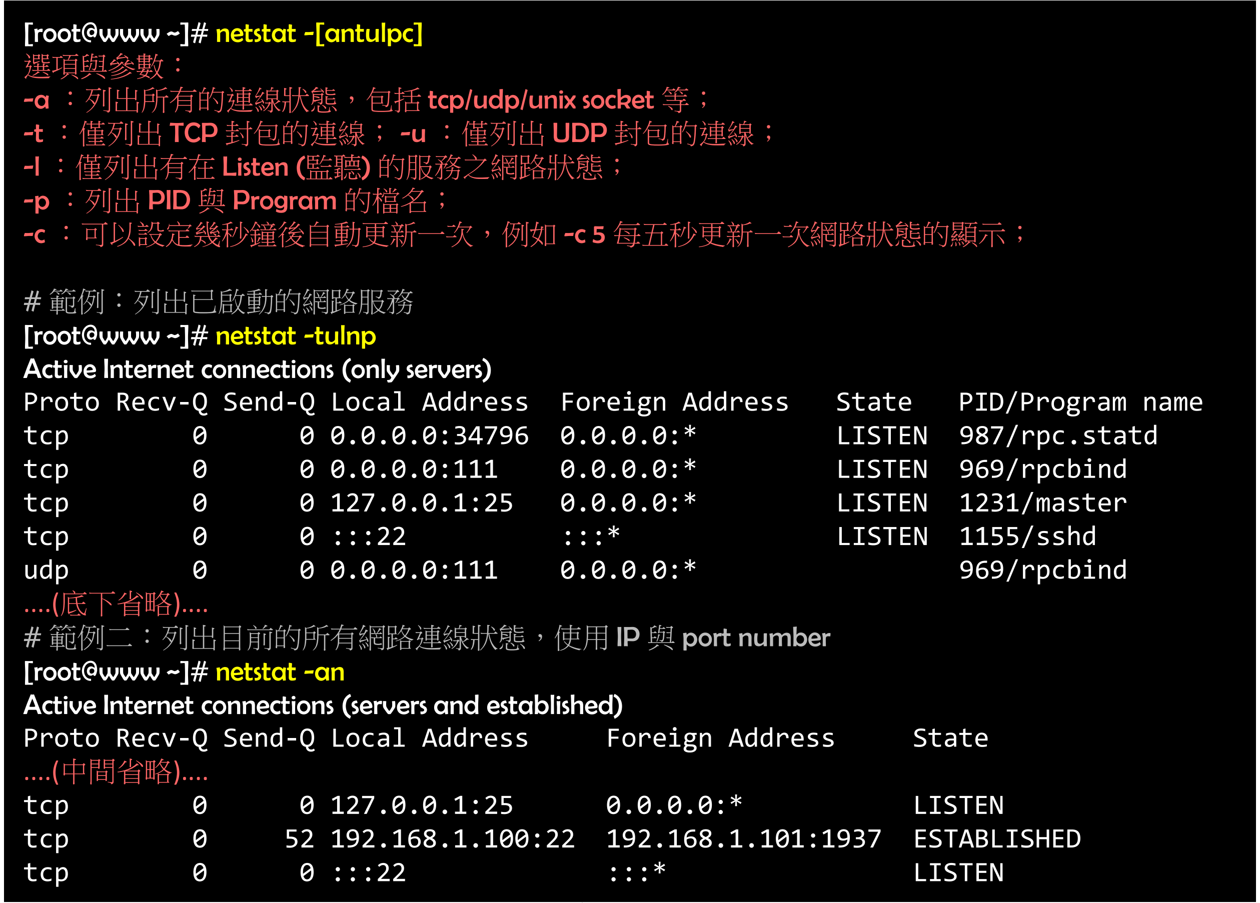


```
[root@www ~]# traceroute [選項與參數] IP
選項與參數：
-n ：不解析主機的名稱，單純用 IP，速度較快。
-U ：使用 UDP 的 port 33434 來進行偵測，這是預設的偵測協定；
-I ：使用 ICMP 的方式來進行偵測；
-T ：使用 TCP 來進行偵測，一般使用 port 80 測試
-w ：若對方主機在幾秒鐘內沒有回應就不理會，預設是 5 秒
-p 埠號：若不想使用預設埠號來偵測，可在此改變埠號。

# 範例一：偵測本機到 yahoo 去的各節點連線狀態
[root@www ~]# traceroute -n tw.yahoo.com
traceroute to tw.yahoo.com (119.160.246.241), 30 hops max, 40 byte packets
 1  192.168.1.254 0.279 ms 0.156 ms 0.169 ms
 2  172.20.168.254 0.430 ms 0.513 ms 0.409 ms
 3  10.40.1.1 0.996 ms 0.890 ms 1.042 ms
 4  220.128.3.149 8.062 ms 8.058 ms 7.990 ms
 5  * * *
 6  119.160.240.1 10.688 ms 10.590 ms 119.160.240.3 10.047 ms
 7  * * * <==可能有防火牆裝置等情況發生所致
由資料可知該主機連線自 tw.yahoo.com 需要經過 7 個節點
```

Courtesy of 第五章、 Linux 常用網路指令 5.2.2 兩主機間各節點分析, 鳥哥的 Linux 私房菜; traceroute(8) - Linux man page

Check Network Status

- **netstat** - print network status on the computer
  - I.e., network connections, routing tables, interface statistics, masquerade connections, and multicast memberships



```
[root@www ~]# netstat -[antulpc]
選項與參數：
-a ：列出所有的連線狀態，包括 tcp/udp/unix socket 等；
-t ：僅列出 TCP 封包的連線； -u ：僅列出 UDP 封包的連線；
-l ：僅列出有在 Listen (監聽) 的服務之網路狀態；
-p ：列出 PID 與 Program 的檔名；
-c ：可以設定幾秒鐘後自動更新一次，例如 -c 5 每五秒更新一次網路狀態的顯示；

# 範例：列出已啟動的網路服務
[root@www ~]# netstat -tulnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address   Foreign Address   State   PID/Program name
tcp        0      0 0.0.0.0:34796   0.0.0.0:*         LISTEN  987/rpc.statd
tcp        0      0 0.0.0.0:111     0.0.0.0:*         LISTEN  969/rpcbind
tcp        0      0 127.0.0.1:25    0.0.0.0:*         LISTEN  1231/master
tcp        0      0 :::22           :::*              LISTEN  1155/sshd
udp        0      0 0.0.0.0:111     0.0.0.0:*                 969/rpcbind
....(底下省略)....
# 範例二：列出目前的所有網路連線狀態，使用 IP 與 port number
[root@www ~]# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address      Foreign Address      State
....(中間省略)....
tcp        0      0 127.0.0.1:25       0.0.0.0:*            LISTEN
tcp        0     52 192.168.1.100:22   192.168.1.101:1937   ESTABLISHED
tcp        0      0 :::22              :::*                 LISTEN
```

Courtesy of 第五章、 Linux 常用網路指令 5.2.3 察看本機的網路連線與後門, 鳥哥的 Linux 私房菜; netstat(8) - Linux man page

Connection

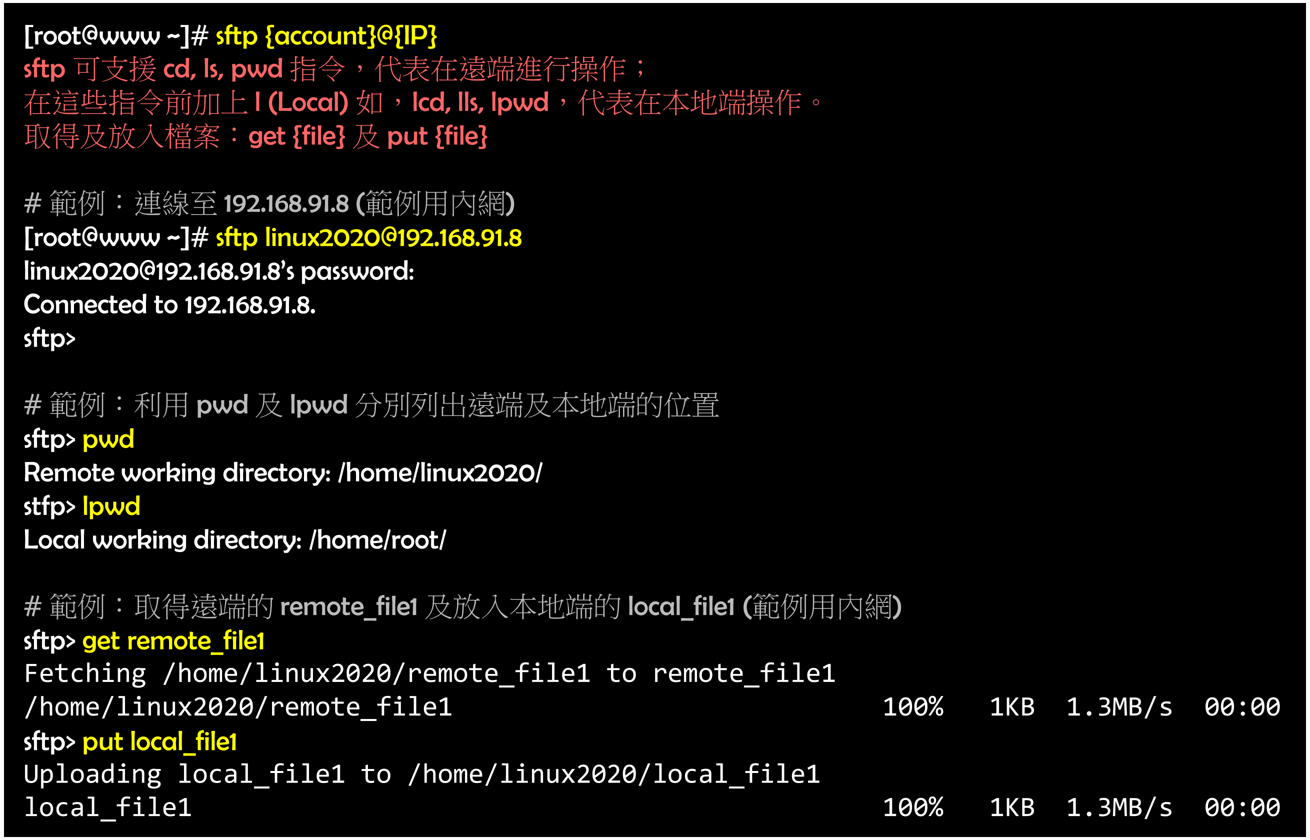
Management

Remote Login

NETWORKING IN LINUX

Secure File Transfer Program

- **sftp** - secure file transfer program
  - Has interactive commands to transfer files



```
[root@www ~]# sftp {account}@{IP}
sftp 可支援 cd, ls, pwd 指令，代表在遠端進行操作；
在這些指令前加上 l (Local) 如，lcd, lls, lpwd，代表在本地端操作。
取得及放入檔案：get {file} 及 put {file}

# 範例：連線至 192.168.91.8 (範例用內網)
[root@www ~]# sftp linux2020@192.168.91.8
linux2020@192.168.91.8’s password:
Connected to 192.168.91.8.
sftp>

# 範例：利用 pwd 及 lpwd 分別列出遠端及本地端的位置
sftp> pwd
Remote working directory: /home/linux2020/
stfp> lpwd
Local working directory: /home/root/

# 範例：取得遠端的 remote_file1 及放入本地端的 local_file1 (範例用內網)
sftp> get remote_file1
Fetching /home/linux2020/remote_file1 to remote_file1
/home/linux2020/remote_file1                        100%   1KB  1.3MB/s  00:00
sftp> put local_file1
Uploading local_file1 to /home/linux2020/local_file1
local_file1                                         100%   1KB  1.3MB/s  00:00
```

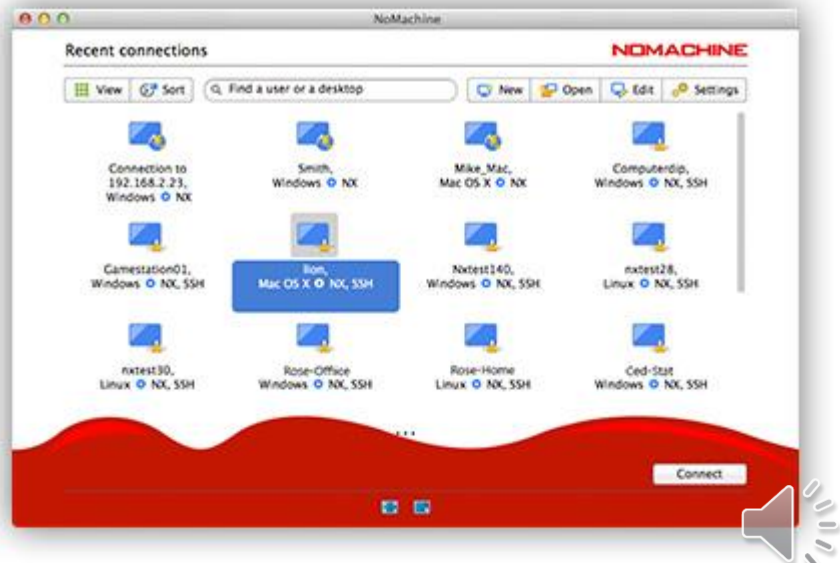
Courtesy of 第十一章、遠端連線伺服器 11.2.3 ssh 用戶端連線程式, 鳥哥的 Linux 私房菜; sftp(1) - Linux man page

Remote Login w/ Textual and Graphical Interfaces

- **ssh** - OpenSSH SSH client for logging into a remote machine and for executing commands on a remote machine
  - The remote machine should install and run the SSH service/daemon
- The workflow of remote processing is illustrated below
  - For Windows users, you can use PieTTY as SSH client

- Run the remote programs as if on the local machine using GUI
  - A client and server software pairs for remote accesses
  - Many solutions are available:
    - VNC
    - AnyDesk
    - NoMachine (Installation)
    - TeamViewer (Installation)
    - …

```
[root@www ~]# ssh {account}@{IP}
[root@www ~]# ssh -l {account} {IP}

# 範例：連線至 192.168.91.8 (範例用內網)
[root@www ~]# ssh linux2020@192.168.91.8
linux2020@192.168.91.8's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-47-generic x86_64)
....(底下為登陸提示，省略)....
登陸後即可如一般使用者操作

# 範例：利用 ctrl+D 登出 192.168.91.8 (範例用內網)
[linux2020@www ~]# logout     (ctrl+D)
Connection to 192.168.91.8 closed.

# 範例：利用 exit 登出 192.168.91.8 (範例用內網)
[linux2020@www ~]# exit
Connection to 192.168.91.8 closed.
```



Courtesy of 第十一章、遠端連線伺服器 11.2.3 ssh 用戶端連線程式, 鳥哥的 Linux 私房菜; ssh(1) - Linux man page

THANK YOU!