

# Introduction to Computer Science

## Lecture 4: NETWORKING AND THE INTERNET

Tian-Li Yu

Taiwan Evolutionary Intelligence Laboratory (TEIL)  
Department of Electrical Engineering  
National Taiwan University

tianliyu@cc.ee.ntu.edu.tw

Slides made by Tian-Li Yu, Jie-Wei Wu, and Chu-Yu Hsu

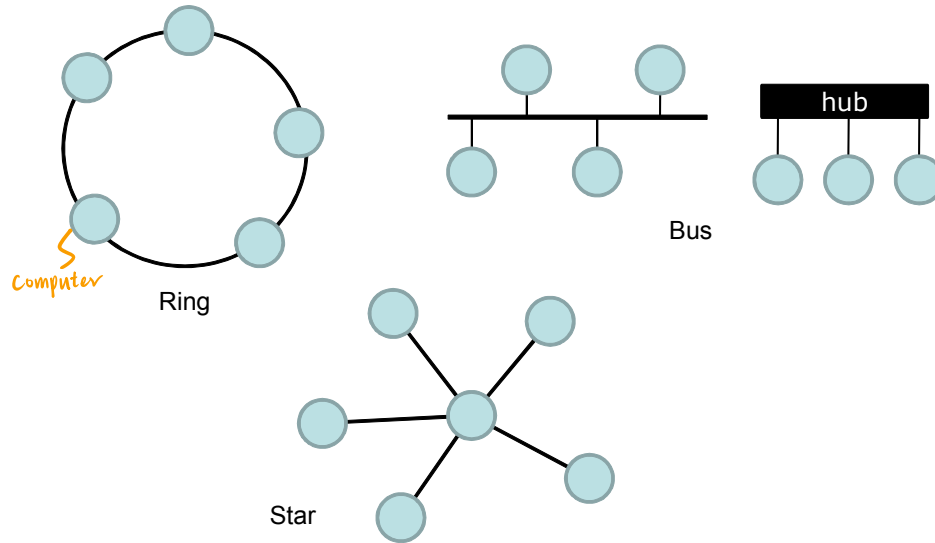


【本著作除另有註明外，採取創用CC「姓名標示—非商業性—相同方式分享」台灣3.0版授權釋出】

# Network Classifications

- Scope
  - LAN: local area network
  - MAN: metropolitan area network
  - WAN: wide area network
- Ownership
  - Closed
  - Open
- Topology

# Network Topology



# Protocols 通訊協定 → 避免傳訊時碰撞在一起

- **Token ring**
  - Popular in ring topology.
  - Token and messages are passed in one direction.
  - Only the machine that gets the token can transmit its own message. → 有token者才能發訊
- **CSMA/CD** (carrier sense, multiple access with collision detection) → 有線網路使用
  - Popular in bus topology (wired Ethernet).
  - Broadcasting.
  - When collision, both machines wait for a brief random time before trying again.
- **CSMA/CA** (carrier sense, multiple access with collision avoidance) → 無線網路使用
  - Popular in wireless Ethernet.
  - Broadcasting.
  - Detect if a channel is idle, if so, wait for a brief random time and then detect again. If the channel is still idle, start sending.

# Dilbert on Token Ring

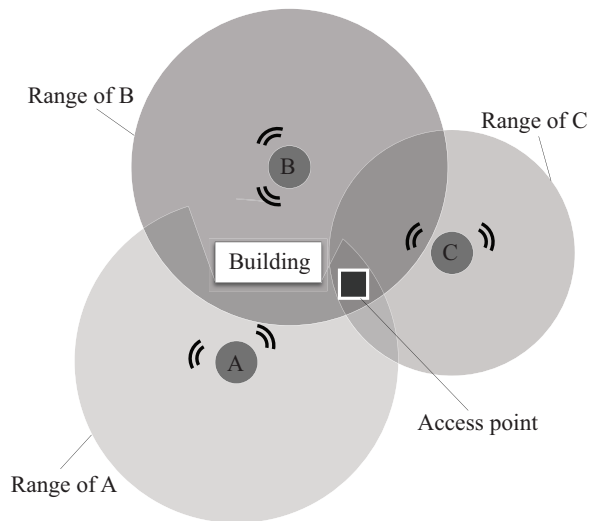


Dilbert, Scott Adams



# Wireless & Access Point

- Wi-Fi (wireless fidelity)
- IEEE 802.11 (b, g, i, n, ac, ...)



None of the end systems can hear each other but each can communicate with the **AP**

# Connecting Compatible Networks

- Repeater 中繼器

- Simply passing through messages.
- Connecting two compatible networks.

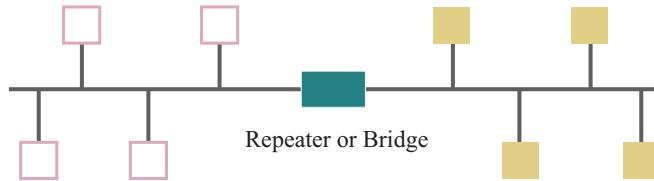
- Bridge 橋接器

- Only passing those messages addressed to the other side.
- Connecting two compatible networks more efficiently.

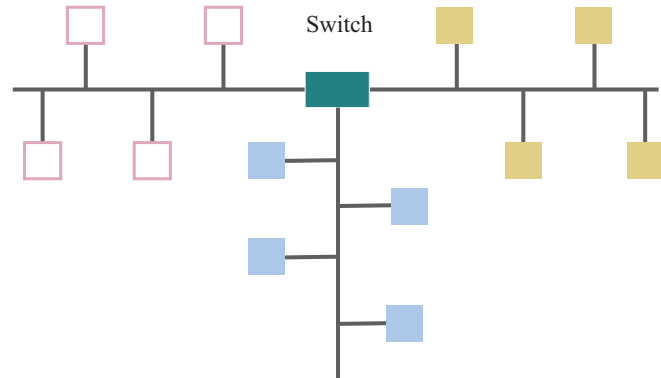
- Switch 交換器

- A bridge with multiple connections
- Connecting several compatible networks more efficiently.

# Repeater, Bridge, and Switch



(a) A repeater or bridge connecting one bus.

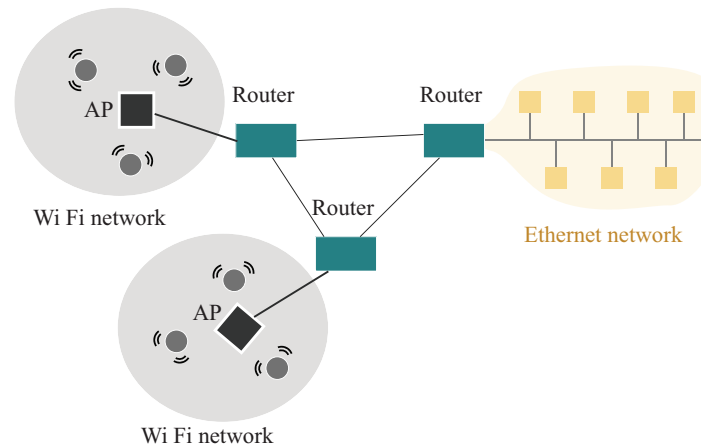
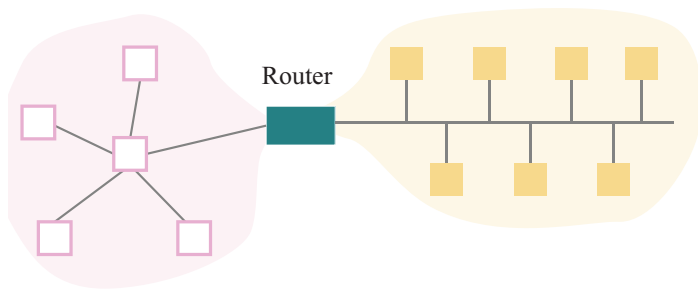


(b) A switch connecting multi bus.



# Connecting Incompatible Networks

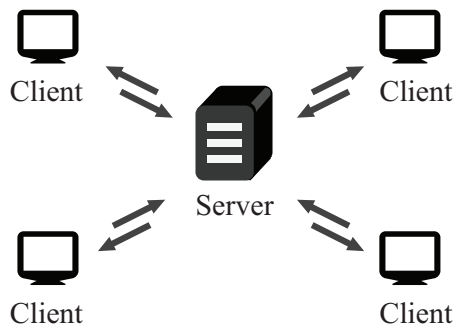
- Router 路由器 → 可連接不同協定
  - Building a network of networks, known as an **internet**.
  - Most come with **firewall** management.  
防火牆



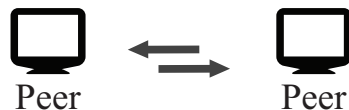
# Interprocess Communication

- **Server-client**
  - One server, several clients.
  - Clients initiate communications by sending requests.
  - Server serves.
- **P2P** (peer-to-peer)
  - Two processes communicating as equals.
  - The most popular distribution mode nowadays.

# Interprocess Communication (contd.)



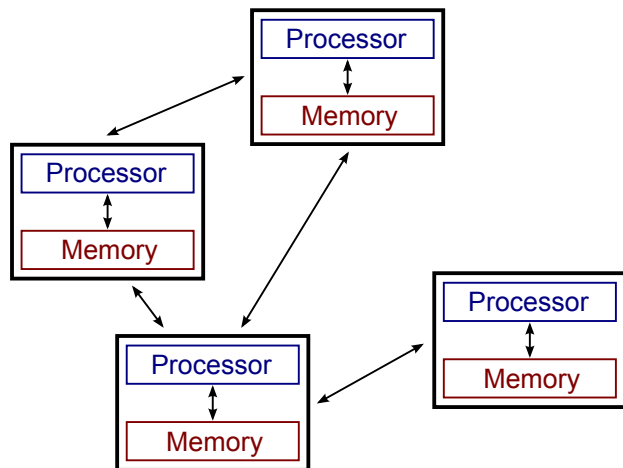
Server must be prepared to serve multiple clients at any time.



Peers communicate as equals on a one-to-one basis.

# Distributed Systems

- Infrastructure can be provided by standardized toolkits.
  - Enterprise Java Beans by Sun Microsystems
  - .NET framework by Microsoft



# The Internet

- The most notable example of an internet is the **Internet**.
- Original goal was to prevent disruptions caused by local disaster.
  - Deviated from the advanced research projects agency network (ARPANet) around 1960.
  - 4 nodes — UCLA, SRI, UCSB, UTAH,
- Now it's a commercial undertaking.



Left to right: Vinton Cerf, Robert Kahn, and US President George Bush  
White House, Wednesday, Nov. 9, 2005

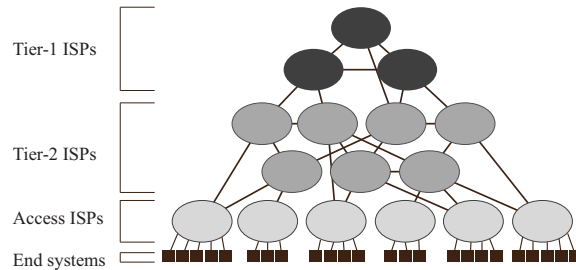
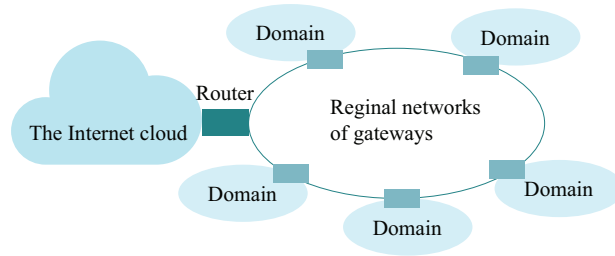
# Internet Architecture

- Domain
  - a network or an internet controlled by one single authority.
- ICANN (Internet corporation for assigned names and numbers)
  - Oversee the registration of domains.
  - Registrar
- Gateway 關道
  - A router that connects a domain to the rest of the Internet (the Internet cloud).

# Internet Composition

- Internet Service Provider (ISP) *ex: 中華電信 (Hi-net)*
  - Allow customers to connect their domain to the ISP's equipment or join the domain already established by the ISP.
  - Tier-1
  - Tier-2
  - Access ISP: Provides connectivity to the Internet
    - Traditional telephone (dial-up connection)
    - Cable connections
    - DSL
    - Wireless

# Domains, Gateway, and the Internet





# IP Addresses

- IP (Internet protocol) addresses
  - 32 bits in IPv4 (all are allocated in Feb. 2011)
  - 128 bits in IPv6
- Network identifier (by ICANN)
- Host address (domain administrator)
- Dotted decimal
  - 140.112.18.33  
↳ TW

# Host Names

- Mnemonic address made up of two parts
- Domain name
  - Assigned by a registrar
  - edu.tw
  - Top-level domain
    - By usage: .edu = education
    - .tw = Taiwan
- Subdomains and individual host names
  - Assigned by domain owner
  - www.ee.ntu.edu.tw
- Name server & domain name server (DNS)
  - www.ee.ntu.edu.tw → 140.112.18.33

# Internet Applications

- VoIP (voice over Internet protocol)
- email (electronic mail)
- FTP (file transfer protocol)
- telnet & ssh (secure shell)
- P2P: bittorrent, edonkey, emule...

# World Wide Web

- www, w3, web
- hypertext, hyperlink, hypermedia.
- Web page: hypertext document
- Website: a collection of closely related web pages.

# Browsers

- Presenting the web pages downloaded from the Internet.
- HTTP (hypertext transfer protocol) 超文本傳輸協定
- URL (uniform resource locator)

(1)                      (2)                      (3)                      (4)

`http://www.ee.ntu.edu.tw/hischool/excellence.html`

- ① Protocol required to access the document. Here it is hypertext transfer protocol (http).
- ② Mnemonic name of host holding the document. → Domain Name
- ③ Directory path indicating the location of the document within the host's file system.
- ④ Document name

# Hyper-Text Markup Language



## HTML Code

```
<html>
<head>
  <title>Demo</title>
</head>
<h1>My Web Page</h1>
<p>
  Click <a href="http://www.ee.ntu.edu.tw">here</a>
  to visit NTUEE.
</p>
</html>
```

# eXtensible Markup Language

- XML
- Standard style to represent data as text.
- Restricted mapping each opening to each ending.
- `<x property="yyy" > ..... </x>` → 自己定的tag
- XHTML
  - HTML that follows XML format.

```
<name code="ISO-8859-1"> Tian-Li Yu </name>  
<education>  
  <BS> NTUEE, 1997</BS>  
  <MS> UIUCCS, 2003 </MS>  
  <PhD> UIUCCS, 2006 </PhD>  
</education>
```

↓  
ending

# Client-side & Server-side

- Client-side

- Java applets
- Javascripts
- Flash

} 在客戶端執行 → 減少 server 負擔

- Server-side

- CGI
- Servlets (jsp, asp)
- PHP (Personal Home Page, PHP Hypertext Processor)

} 在伺服器端執行 → 保密程式



# Internet Protocol

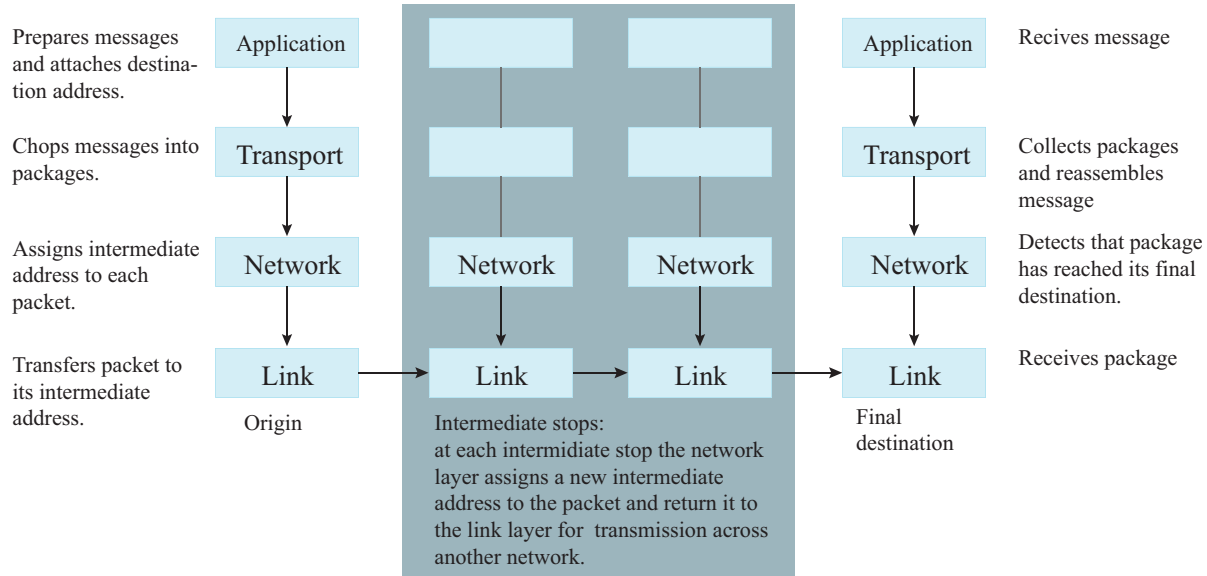
- Layers

- **Application:** constructs message with address
- **Transport:** chops message into packets
- **Network:** handles routing through the Internet
- **Link:** handles actual transmission of packets



- For OSI 7-layer model, check out [http://en.wikipedia.org/wiki/OSI\\_model](http://en.wikipedia.org/wiki/OSI_model).
- Port (not the I/O port)
  - Incoming messages are delivered to different applications by unique port numbers.
  - Some typical ports: ftp (21), telnet (23), ssh (22), http (80), etc.

# Layers



# TCP/IP Suite

- Transport Layer
  - TCP (transmission control protocol)
  - UDP (user datagram protocol)
    - No notification before sending message, no retransmission service, no acknowledge of receiving message.
- Network Layer
  - routing based on IP (IPv4 and IPv6)
- TCP and IP are two protocols, TCP/IP refers to a collection of protocols more than just TCP and IP.
  - TCP: more reliable, less efficient → 需要 hand-shaking
  - UDP: more efficient, less reliable

# Security

- Attacks

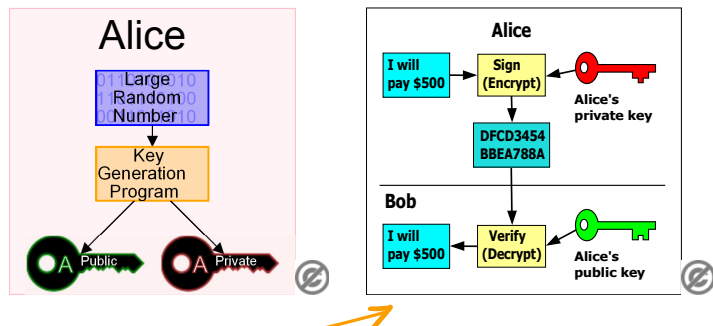
- Malware (malicious software)
  - Virus, worm, Trojan horse, spyware, phishing 釣魚 (騙取機密的)
- Denial of service (DoS) → 癱瘓伺服器
- Spam 垃圾信件

- Protections

- Firewall
- Spam filter
- Proxy 代理伺服器
- Antivirus, antispyware

# Public/Private keys

- **SSL** (secure socket layer).
- **sftp** (ftps as in the textbook), **https**, **ssh**,
- Sending secret message:
  - Sender encrypt  $m$  with the receiver's public key  $\rightarrow s$ .
  - Receiver decrypt message  $s$  with its private key.



# Public/Private Key Issues

- Authentication 驗證
  - Make sure the author of a message is, in fact, the party it claims to be.
  - Use private key to encrypt; public key to decrypt.
- Certificate authority (CA) → 具公信力的第三者機構
  - Ensure the public key is given by the trusted one.

# RSA

- 1977, 1978
- Ron Rivest, Adi Shamir, Leonard Adleman in MIT.
- Security greatly depends on integer factoring.
- Currently no known polynomial-time algorithm exists (only sub-exponential).

# RSA Key Generation

- Choose 2 big distinct primes:  $p$  and  $q$ . 先選兩個大質數
- Let  $N = pq$ . 算  $p \times q$
- Compute  $\phi = (p - 1)(q - 1)$ .
  - There are  $\phi$  integers  $\leq N$  that are co-prime with  $N$ . 互質
- Choose an integer  $e$  that is co-prime with  $\phi$ .
- Compute  $d$  such that  $d \times e \equiv 1 \pmod{\phi}$ . 同餘
- Destroy to record of  $p$  and  $q$ .
- $(N, e)$  is the public key (everyone can get it).
- $(N, d)$  is the private key (only the owner has it).



# Encryption

- Bob wants to send a message  $m$  to Alice.
  - $\gcd(m, p) = 1$        $\gcd(m, q) = 1$
  - What if not? Prob. same as guessing  $p, q$  right.
- He gets Alice's public key  $(N, e)$ .
- He then computes

$$m^e \equiv s \pmod{N} \quad \text{加密}$$

and then send  $s$  to Alice.

# Decryption

- Alice got  $s$  from Bob. She has her own private key  $(N, d)$ .
- She then computes

$$s^d \equiv m \pmod{N}$$

解密

and got the message back.

# Why? 證明

費馬小定理

$$s^d \equiv (m^e)^d \pmod{N} \equiv m^{ed} \pmod{N}$$

Fermat's little theorem

$$a^p \equiv a \pmod{p}. \quad \text{If } a \text{ co-primes } p, a^{p-1} \equiv 1 \pmod{p}$$

$$ed \equiv 1 \pmod{p-1} \Rightarrow \text{Let } ed = k(p-1) + 1.$$

$$m^{ed} \equiv m \cdot (m^{p-1})^k \pmod{p} \equiv m \pmod{p}$$

$$\text{Similarly, } m^{ed} \equiv m \pmod{q}$$

By **Chinese remainder theorem**,

$$m^{ed} \equiv m \pmod{pq}$$

$$s^d \equiv m \pmod{N}$$

\* 舉例 ( $p=3, q=11$ )

$$N = 3 \times 11$$

$$\phi = (3-1)(11-1) = 20$$

選  $e$  和  $\phi$  互質: 3

$b$	20	3	1
	18	2	
	2	(1)	

$$\rightarrow 3 - 2$$

$$= 3 - (20 - b \times 3)$$

$$= (-1) \times 20 + 7 \times 3$$

$$\Rightarrow 1 \pmod{20} \equiv 7 \times 3 \pmod{20}$$

$$(N, e) = (33, 3) \text{ public}$$

$$(N, d) = (33, 7) \text{ private}$$

$$\text{今有 } m = 4 \Rightarrow \text{加密: } s = 4^3 \% 33 = 31$$

$$\Rightarrow \text{解密: } 31^7 \% 33 = (-2)^7 \% 33 = (-128) \% 33 = 4$$

# License

Page	File	Licensing	Source/ author
5	 Dilbert, Scott Adams		"Dilbert" .,Author:Scott Adams, May 2, 1996 Source: <a href="http://dilbert.com/strips/comic/1996-05-02/">http://dilbert.com/strips/comic/1996-05-02/</a> , Date:2013/03/06, Fair use under copyright law 46,52,65.
13			"Cerf Kahn Medal Of Freedom" .,Author:Paul Morse, Nov 9, 2005 Source: <a href="http://en.wikipedia.org/wiki/File:CerfKahnMedalOfFreedom.jpg">http://en.wikipedia.org/wiki/File:CerfKahnMedalOfFreedom.jpg</a> , Date:2013/05/14, The image is in the public domain.
29			"Public-key-crypto" .,Author:KohanX, Sep 7, 2009 Source: <a href="http://en.wikipedia.org/wiki/File:Public-key-crypto-1.svg">http://en.wikipedia.org/wiki/File:Public-key-crypto-1.svg</a> , Date:2013/05/14, The image is in the public domain.
29			"Public key encryption" .,Author:David Gthberg, Sep 7, 2009 Source: <a href="http://commons.wikimedia.org/wiki/File:Public_key_encryption.svg">http://commons.wikimedia.org/wiki/File:Public_key_encryption.svg</a> , Date:2013/05/14, The image is in the public domain.