

Chapter 4

Part B

Pearson International Edition

J. Glenn Brookshear

Computer Science
An Overview

**Network
and the Internet**

J. Glenn Brookshear

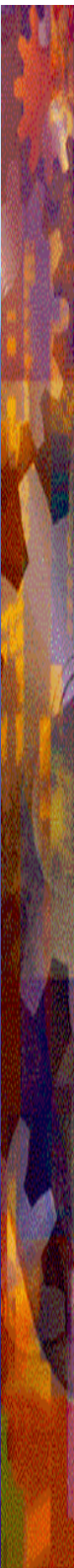
蔡文能



Slide 4b-1

Agenda

- 4.1 Network Fundamentals
 - 4.2 The Internet
 - 4.3 The World Wide Web
 - 4.4 Network Protocols**
 - 4.5 Security**
- } **Part A**
- } **Part B**



Network Protocols

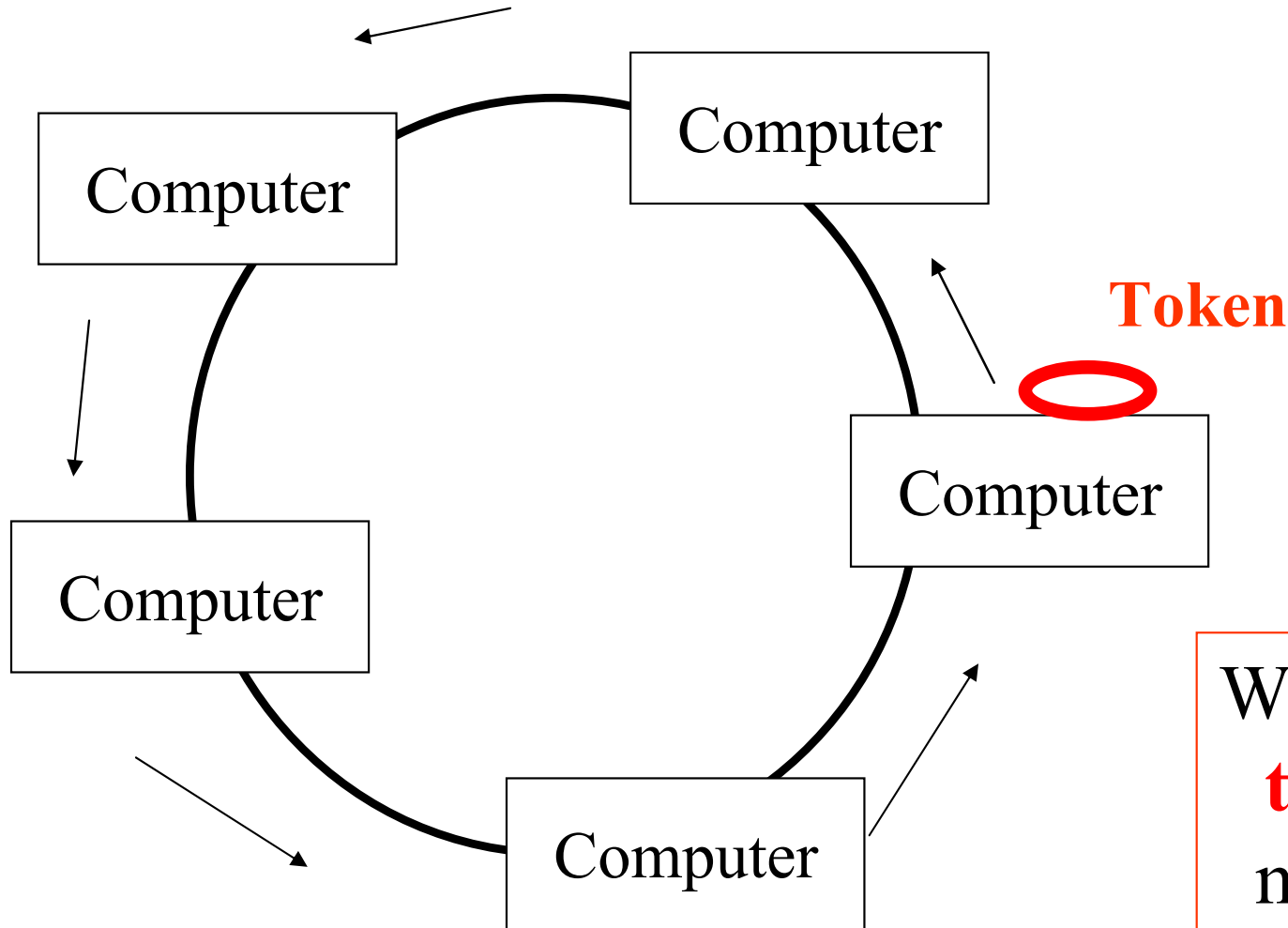
- Rules that govern the communication between different components within a computer system
- Rules Obeyed by All Parties
- Network protocols define the details of each activity
 - Delegate the right (privilege) to transmit message
 - Address messages
 - Package and unpack messages (封裝與拆封)
- Examples of **Link layer** protocol
 - Token Ring protocol (by IBM)
 - CSMA/CD (for Ethernet)
 - CSMA/CA (for Wireless) (discuss this later)

Token Ring Protocol (1/2)

- Popular in networks based on the ring topology
- All machines transmit message in a common direction
- **Token**, a unique **bit pattern** is passed around the ring
- Possession of the token gives a machine the authority to transmit its own messages (有**Token**才可送訊息)
- Without the token, a machine is only allowed to forward messages **Token** is forwarded to next machine when a message has completed its cycle along the ring

token : 象徵字, 令牌, 有特別意義的一串bits

Token Ring Protocol (2/2)



What if the **token** is missing?

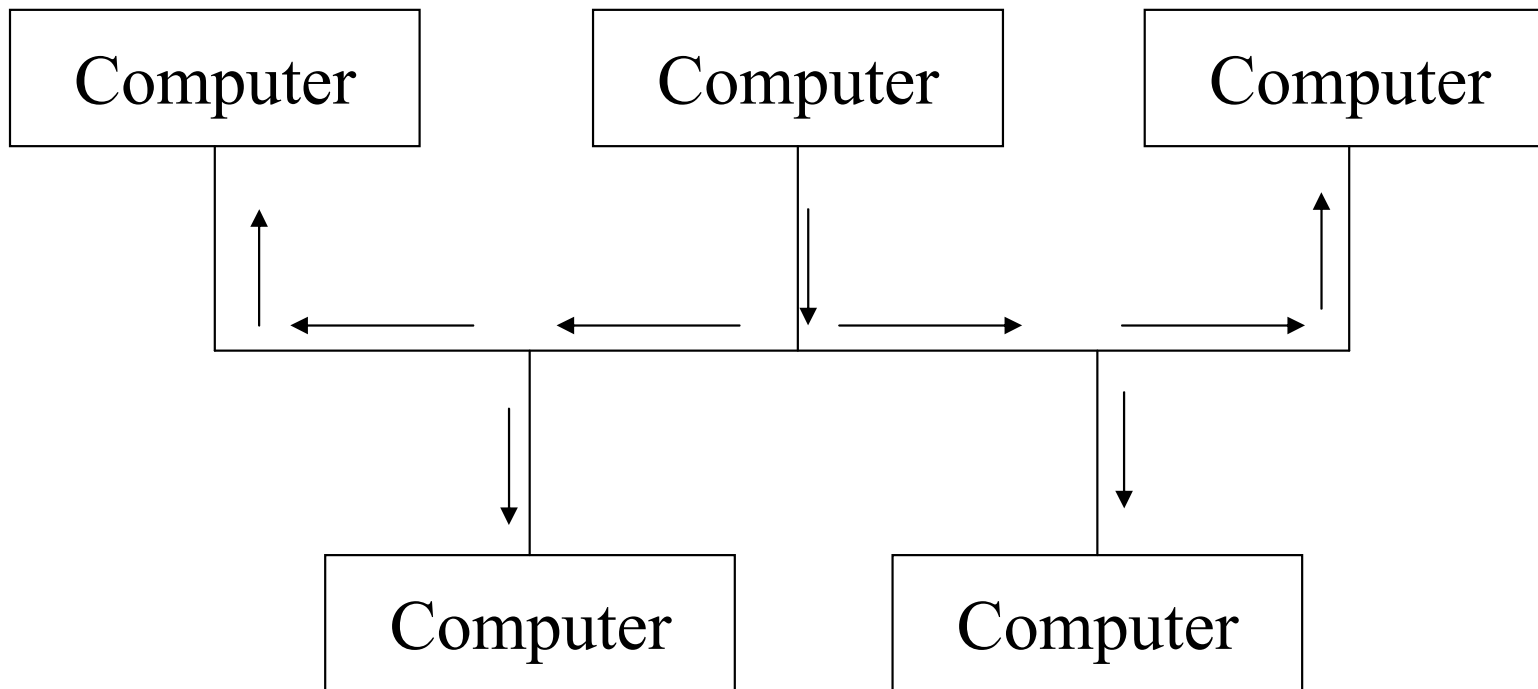
token : 記號;象徵字, 權仗, 令牌, 有特別意義的一串bits

CSMA/CD Protocol (1/2)

- **C**arrier **S**ense, **M**ultiple **A**ccess with **C**ollision **D**etection (**CSMA/CD**)
- Popular in **Ethernet**
- Each message is broadcasted on the **bus**
- Each machine monitors all messages but keeps only those addressed to itself (非禮勿視 :-)
- Wait until the bus is silent to transmit a message
- When collision occurs, both machine pause for a brief **random period of time** before trying again

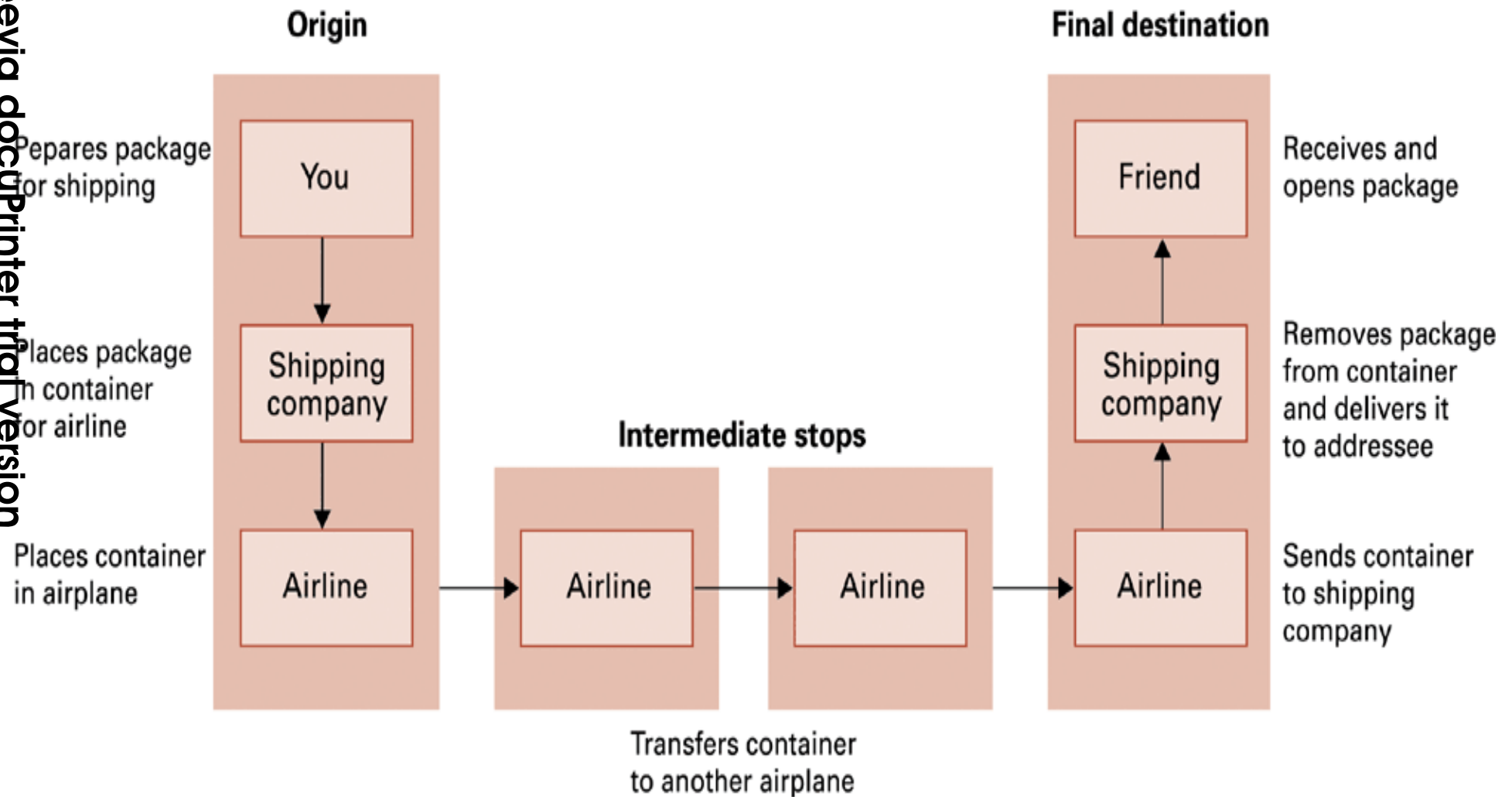
Ethernet 與 **802.3** 都使用 **CSMA/CD** protocol

CSMA/CD Protocol (2/2)

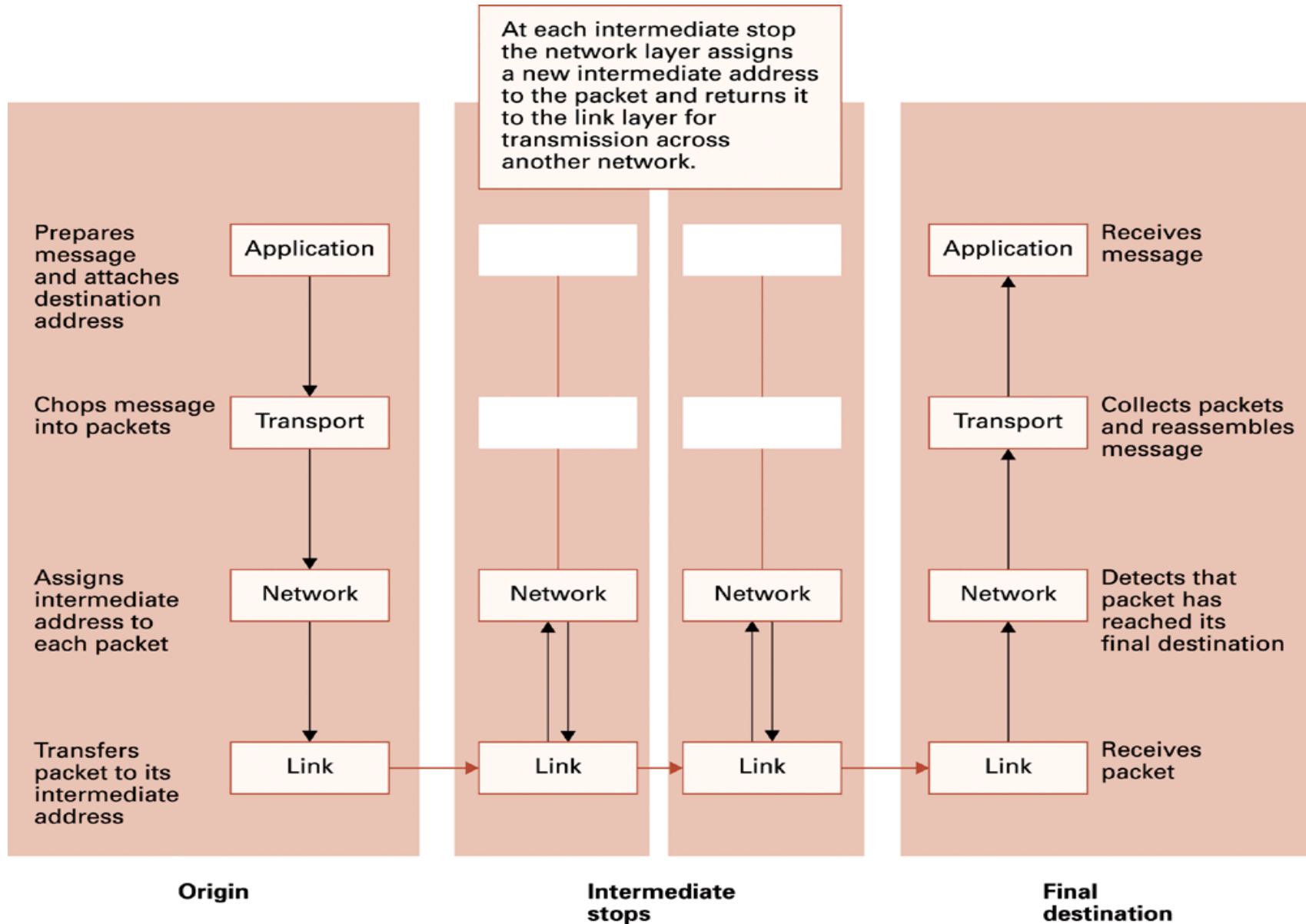


CSMA/CD: **C**arrier **S**ense, **M**ultiple **A**ccess with **C**ollision **D**etection

Package-Shipping by Air

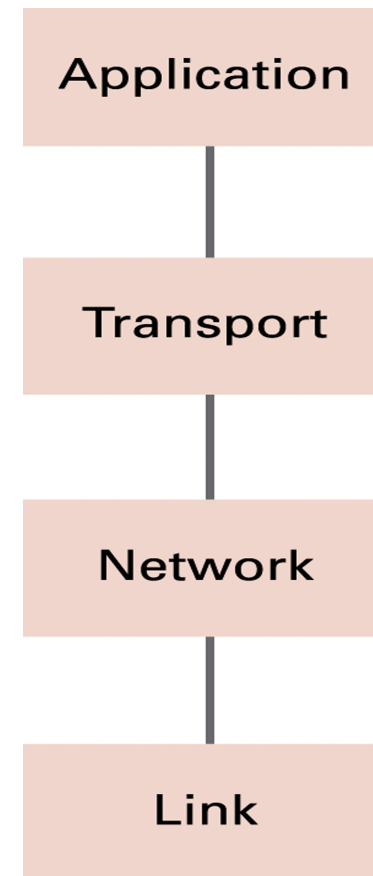


Message-Shipping by Internet



TCP/IP 4 Layers protocol stack

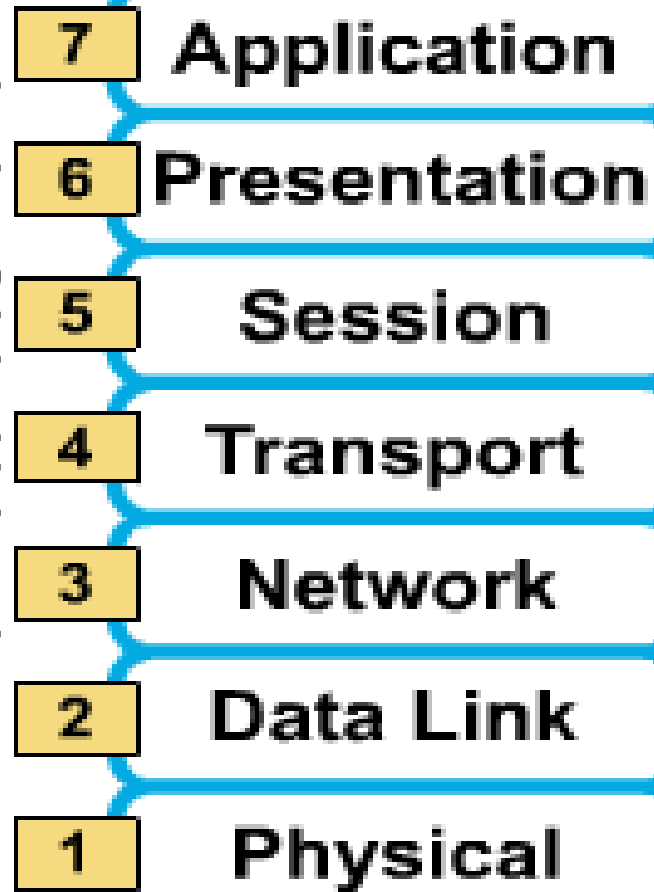
- Application layer (Layer 4)
 - HTTP, FTP, Telnet
- Transport layer (Layer 3)
 - TCP, UDP
- Network layer (Layer 2)
 - Routing
- Link layer (Layer 1) (MAC layer)
 - Token ring or Ethernet



MAC: Media Access Control

Why a Layered Network Model?

OSI 7-Layer Reference Model



上司管下司鋤頭管畚箕

分層負責; 分工合作

- Reduces complexity
- Standardizes interfaces
- Facilitates modular engineering
- Ensures interoperable technology
- Accelerates evolution
- Simplifies teaching and learning

• It prevents changes in one layer from **affecting** the other layers, so that they can develop more quickly.

OSI
ISO

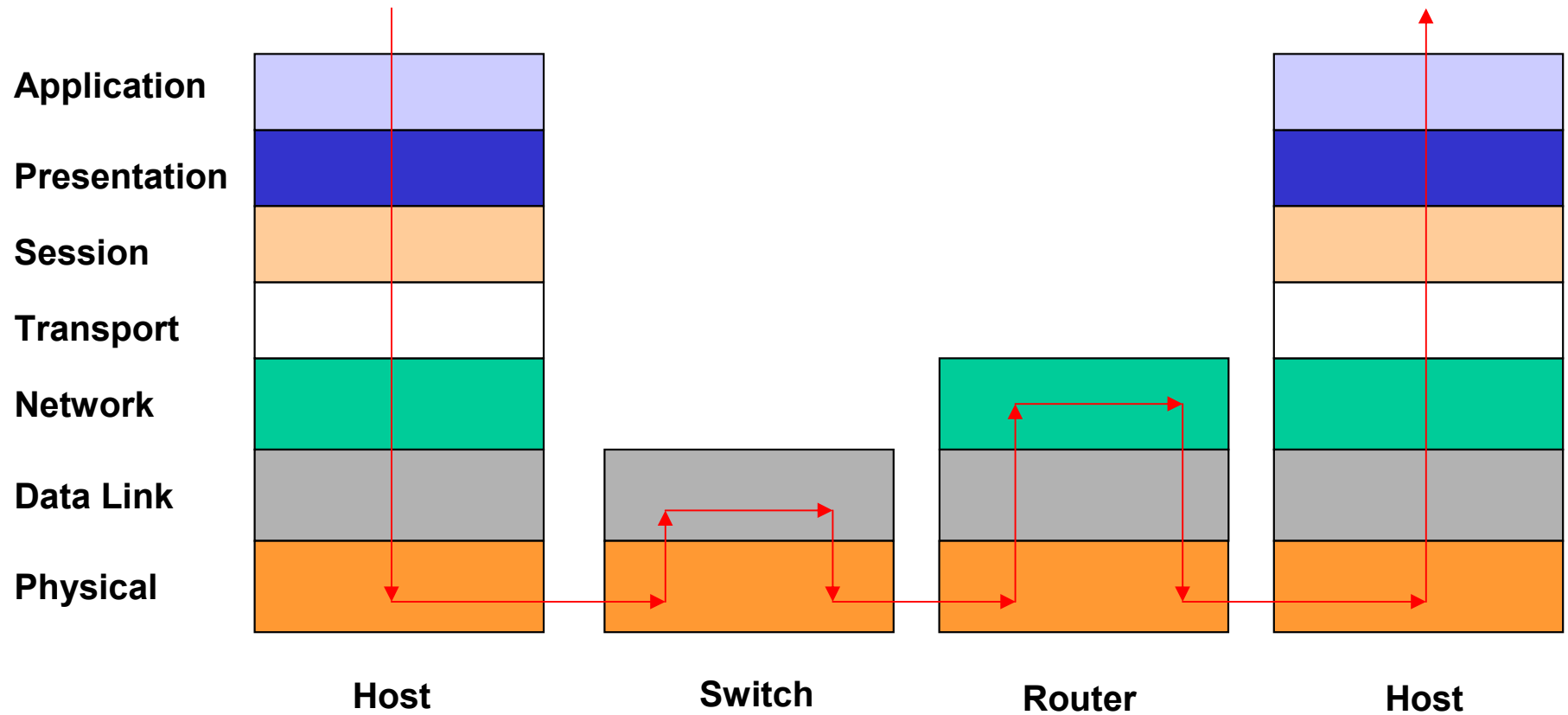
Proposed by International Organization for Standardization (ISO)

Open System Interconnection (ISO)

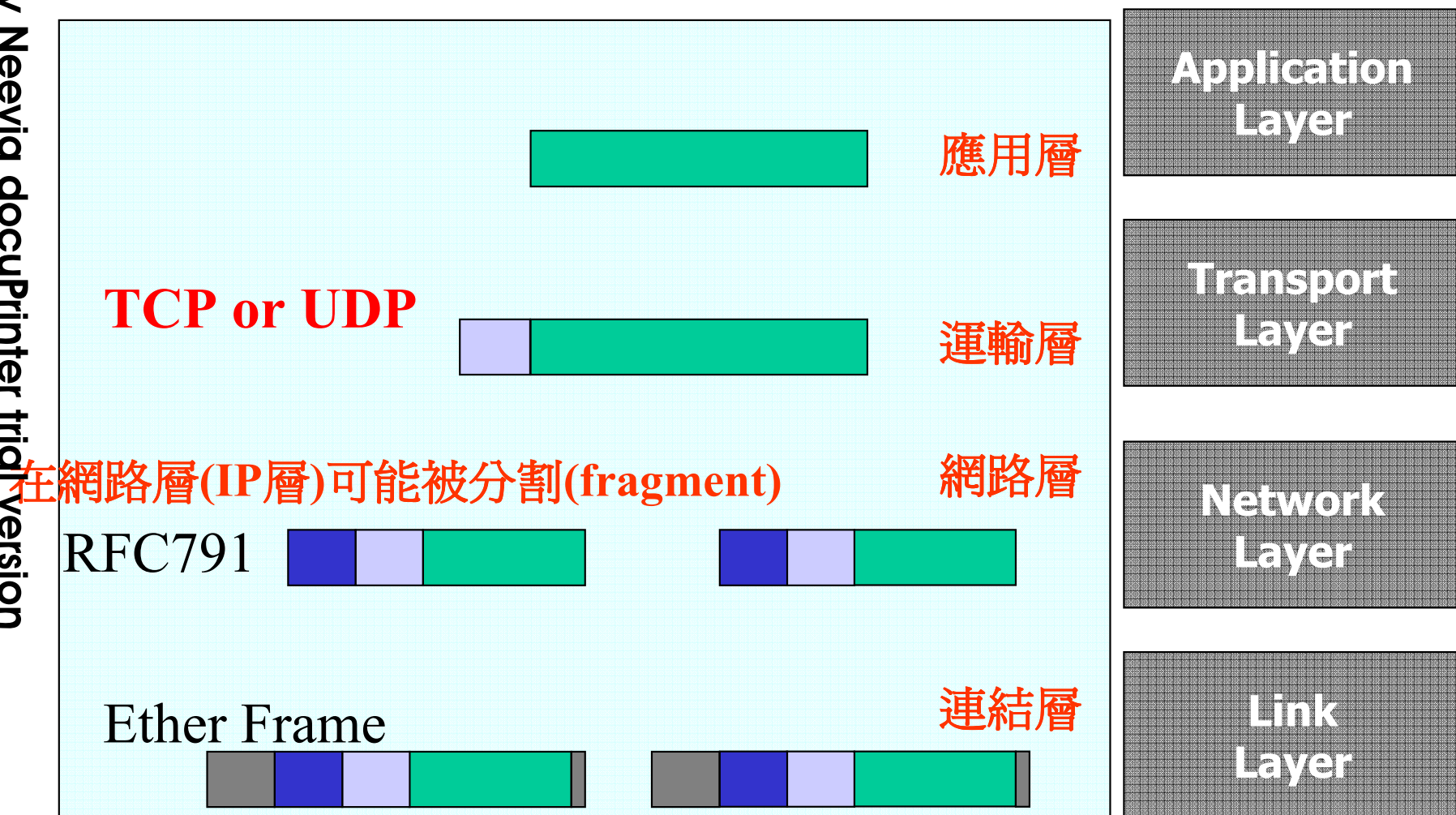
Principle of Layering (分層負責)

- Each layer relies on services from layer below and exports services to layer above
- The routines/methods of Layer N will *not* call Layer N+1.
- The routines/methods of Layer N typically do call the same layer methods.
- The routines/methods of Layer N typically do call Layer N-1 methods.
- The routines/methods of Layer N typically may call Layer N-2, N-3, ... methods.

OSI Layers and Locations



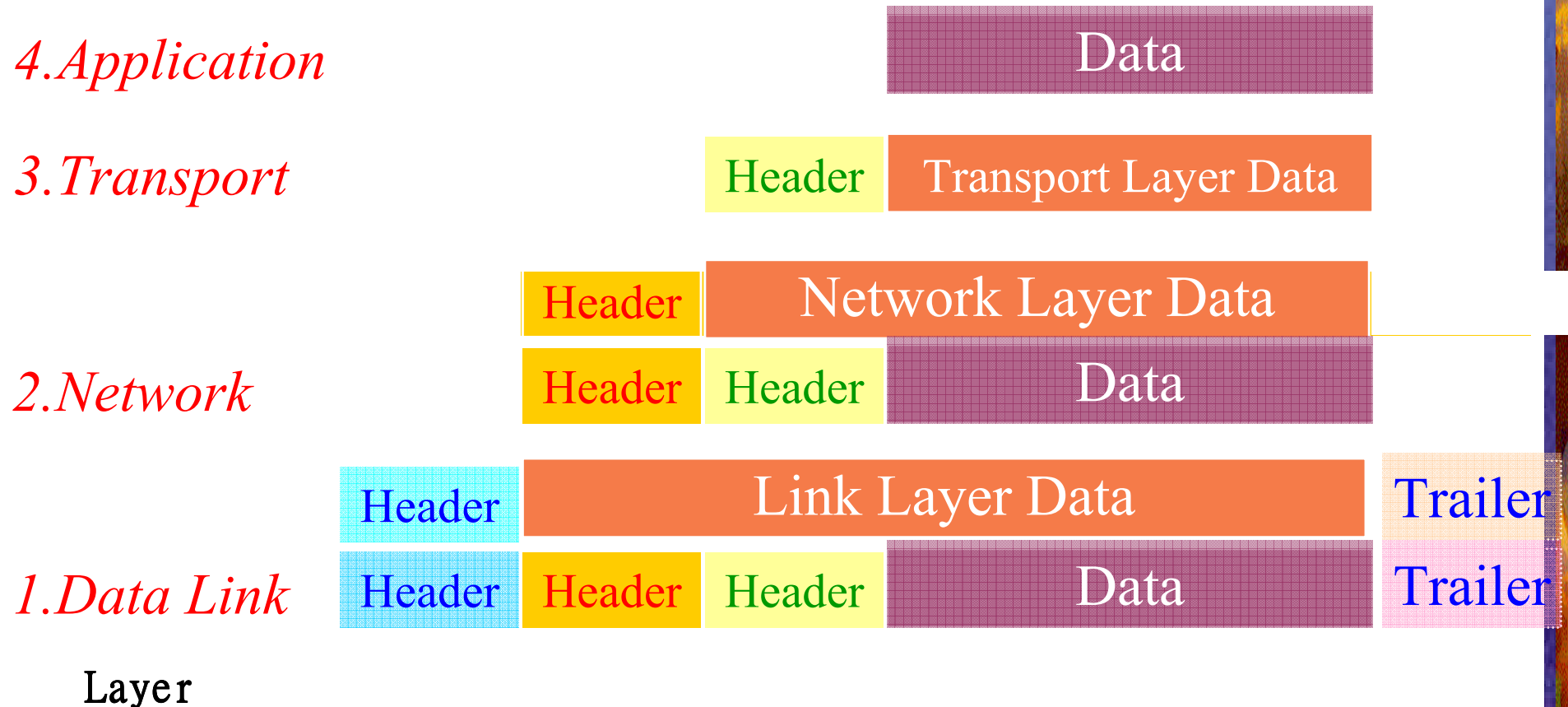
Wrapping up Messages in TCP/IP



http://en.wikipedia.org/wiki/IP_fragmentation

Encapsulation (封裝) the message

- Lower layers add headers (and sometimes trailers) to data from higher layers



Layers for Receiving Messages

- Roughly that of reversing the task performed by their counterparts at the message's origin when sending messages.
- Strips off the outer wrapping placed by their counterparts and hands the underlying packets to its upper layer
- 分工合作, 分層負責

Physical Layer (實體層)

實體層：定義網路媒介的型態、連接器的型態、以及通訊訊號的型態

Layer 1 thinks of signals and media

Defines the **electrical, mechanical, procedural, and functional** specifications for activating, maintaining, and deactivating the physical link between end systems

- Voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other.

- TCP/IP has NO Physical Layer

tsaiwn@csie.nctu.edu.tw

Data Link Layer (資料連結層)

OSI 7-Layer

- **Layer 2** creates data frames to send to Layer 1
- On receiving side, takes raw data from Layer 1 and packages into Data Frames (訊框)
 - Data Frame is basic unit for network traffic on the wire
 - Ethernet Frame on Ethernet (IEEE 802.3)
- Performs Cyclic Redundancy Check (CRC) to verify data integrity
- Detects errors and discards frames containing errors
- PDU (*Protocol Data Unit*) at Layer 2 is called a Frame
- The software component that operates at this layer is the NIC driver; the hardware components that operate here include the NIC (網路卡) and switches (交換器)

OSI 7-Layer 的第二層相當於 TCP/IP 的第一層

又稱 MAC Layer (Media Access Control)

Functions of Layer 3, 4, 5, 6

Presentation Layer: The presentation layer works to transform data into the form that the application layer can accept. This layer **formats, compresses, decompresses** and may **encrypt/decrypt** data to be sent across a **network**, providing freedom from compatibility problems. (Layer 6)

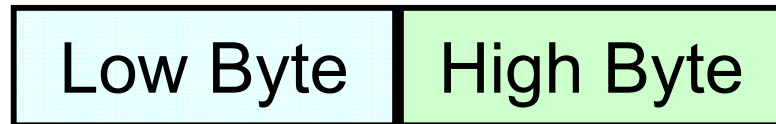
Session Layer: The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination. It ensures that the sender is **authentic** and has access rights to establish a connection. (Layer 5)

Transport Layer: This layer provides transparent transfer of data between end systems, or **hosts**, and is responsible for end-to-end error recovery and **flow control**. (Layer 4)

- **Network Layer:** This Layer determines the **path** that will be taken through the network. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing. It controls the rate at which the network accepts packets, to avoid and recover from **congestion**. (Layer 3)

Byte Ordering

Little-Endian



Addr A

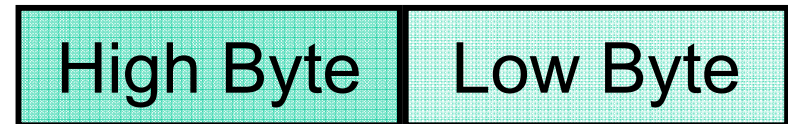
Addr A+1

Intel 80x86

DEC VAX

DEC PDP-11

Big-Endian



Addr A

Addr A+1

IBM 370

Motorola 68000

Sun Sparc

Network order adopts Big-Endian (大印第安)

TCP/IP 網路通訊協定 de facto Standard (業界標準)

- TCP/IP network model

Layer	Function
Application	End-user application programs
Transport	Communication among programs on a net (TCP/UDP)
Network	Basic communication, addressing, and routing (IP, ICMP)
Link(Data Link)	Network hardware and device drivers(ARP, RARP)

4.應用層 , 3.傳輸層(Transport Layer), 2.網路層, 1.鏈結層(Link Layer)

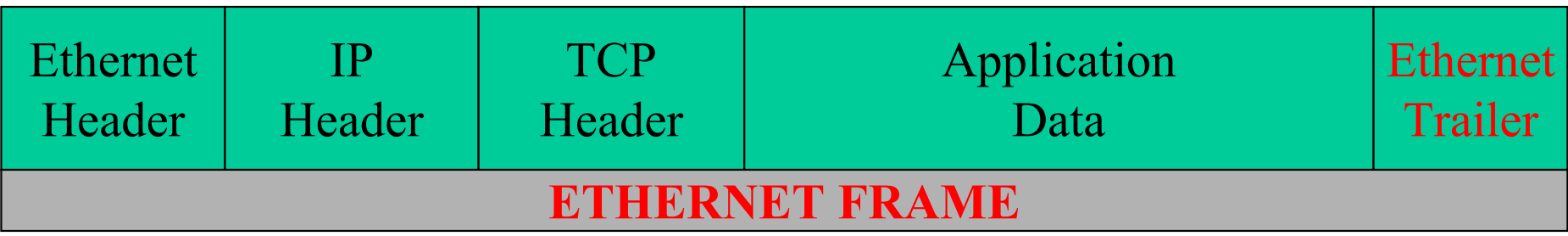
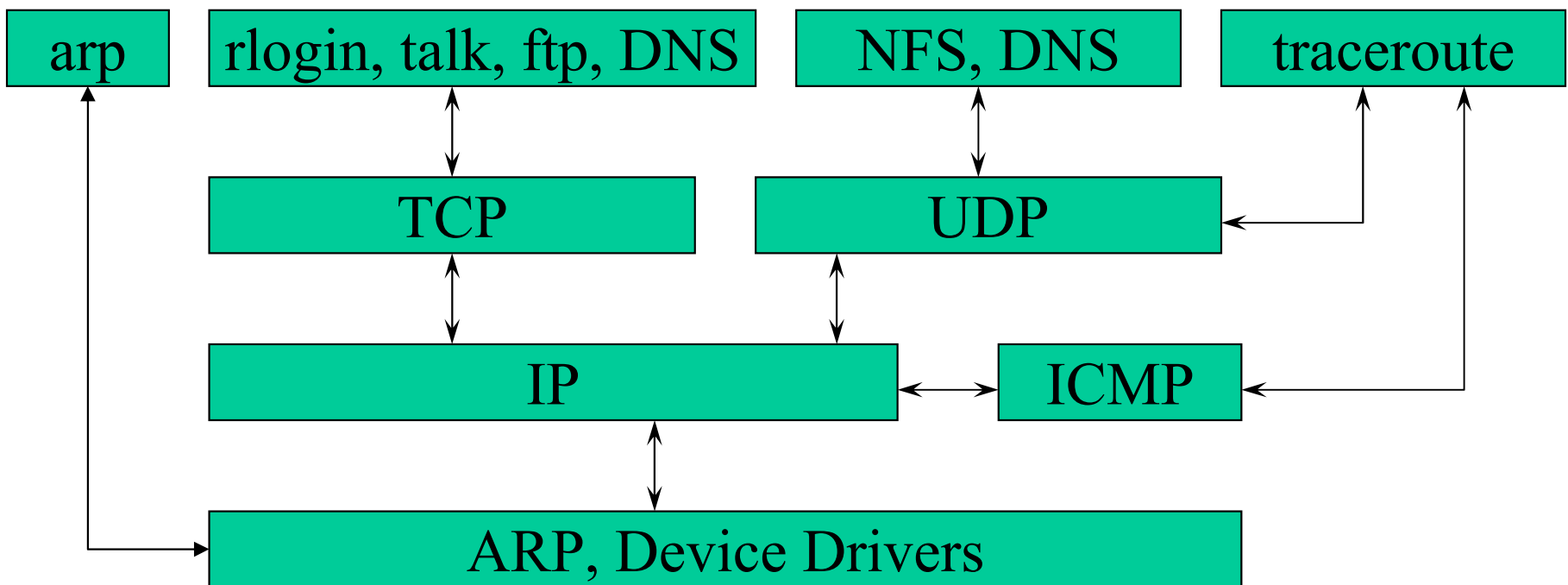
Developed in the US for the Department of Defense ARPAnet system and has become a **de facto standard** used by many vendors.

TCP/IP Protocol Suite

- Application Layer : FTP, HTTP, SMTP, Telnet, ...
- Transport Layer
 - **TCP** (Transmission Control Protocol)
 - Transport layer
 - Establish connection before sending data
 - Reliable protocol
 - UDP (User Datagram Protocol)
 - Transport layer
 - Connectionless
 - Unreliable protocol
- **IP** (Internet Protocol)
 - Network layer (aka IP Layer)
 - Handles hop count (Hop count = 經過幾個 Router)

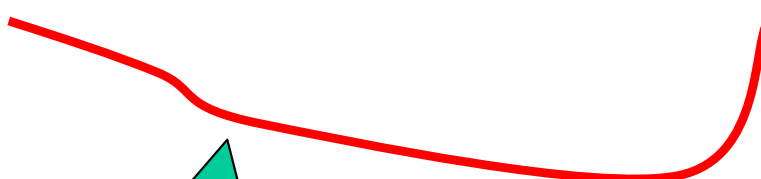
TCP/IP網路通訊協定示意圖

Layer



Example using TCP/IP

- ccsun2: **talk** mfchang@ccbsd3.csie.nctu.edu.tw
- 如何查出 ccbsd3.csie.nctu.edu.tw 的 IP address ?
 - 查 /etc/hosts 或
 - 問 DNS 伺服器
- 每次如何把打的字送到對方機器?
 - TCP → IP → [ARP] → Ether frame → bit stream

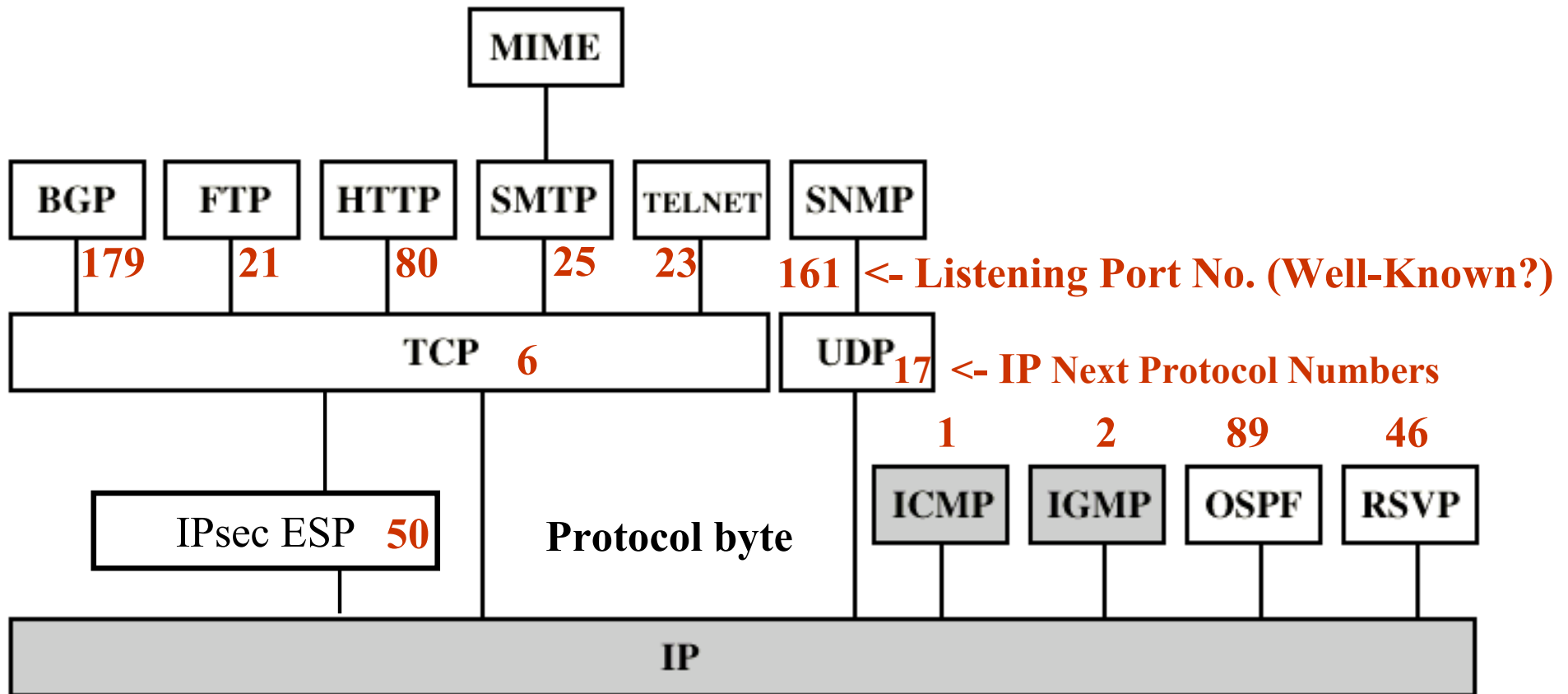


網路卡驅動程式的工作

Application Layer (Layer 4)

- Consists of software units that must communicate with each other across the internet
 - File Transfer Protocol (FTP)
 - Simple Mail Transfer Protocol (SMTP)
 - Telnet
 - Web browser (HTTP)
 - ...

Protocols over IP



Frame type = 0x0800 means “Internet Protocol”

Protocol byte = 6: TCP, 17:UDP

Transport Layer (Layer 3)

(傳輸層; 運輸層)

- Divides long messages into segments of a size compatible with the underlying layer
- Adds **sequence numbers** to these segments
- The **transport layer** involves two protocols - **T**ransmission **C**ontrol **P**rotocol (**TCP**) and **U**ser **D**atagram **P**rotocol (**UDP**)
 - **TCP**
 - *Connection oriented* (要先建立虛擬連線; 就是雙方要先講好)
 - *Header 至少 20 octets*
 - **UDP**
 - *Connectionless*
 - *Header 固定 8 octets*

Octet : 指 8 bits 的 Byte; 因一Byte 可能 6bits, 7bits, 8bits

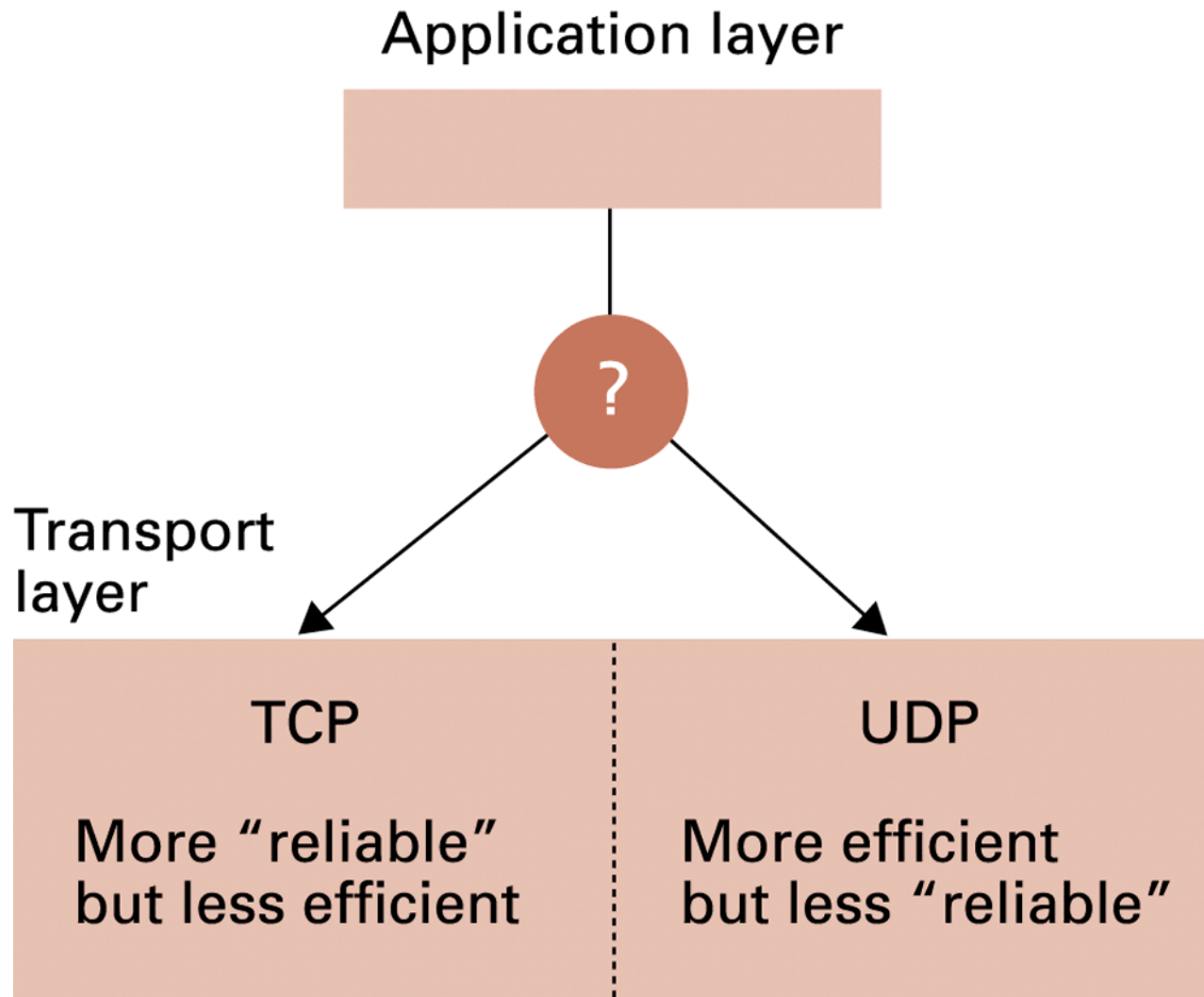
Transport Layer 運輸層

TCP segment vs. UDP datagram

TCP vs. UDP

- **TCP** - a **connection-oriented**, reliable protocol;
 - provides flow control by providing **sliding windows**, and **reliability** by providing **sequence numbers** and **acknowledgments**.
 - The advantage of **TCP** is that it provides guaranteed delivery of the segments.
- **UDP** - **connectionless** and unreliable;
 - although responsible for transmitting messages, **no software checking** for segment delivery is provided at this layer.
 - The advantage that **UDP** provides is speed.

Choosing between TCP and UDP



TCP Connections

vs.UDP Connections ?

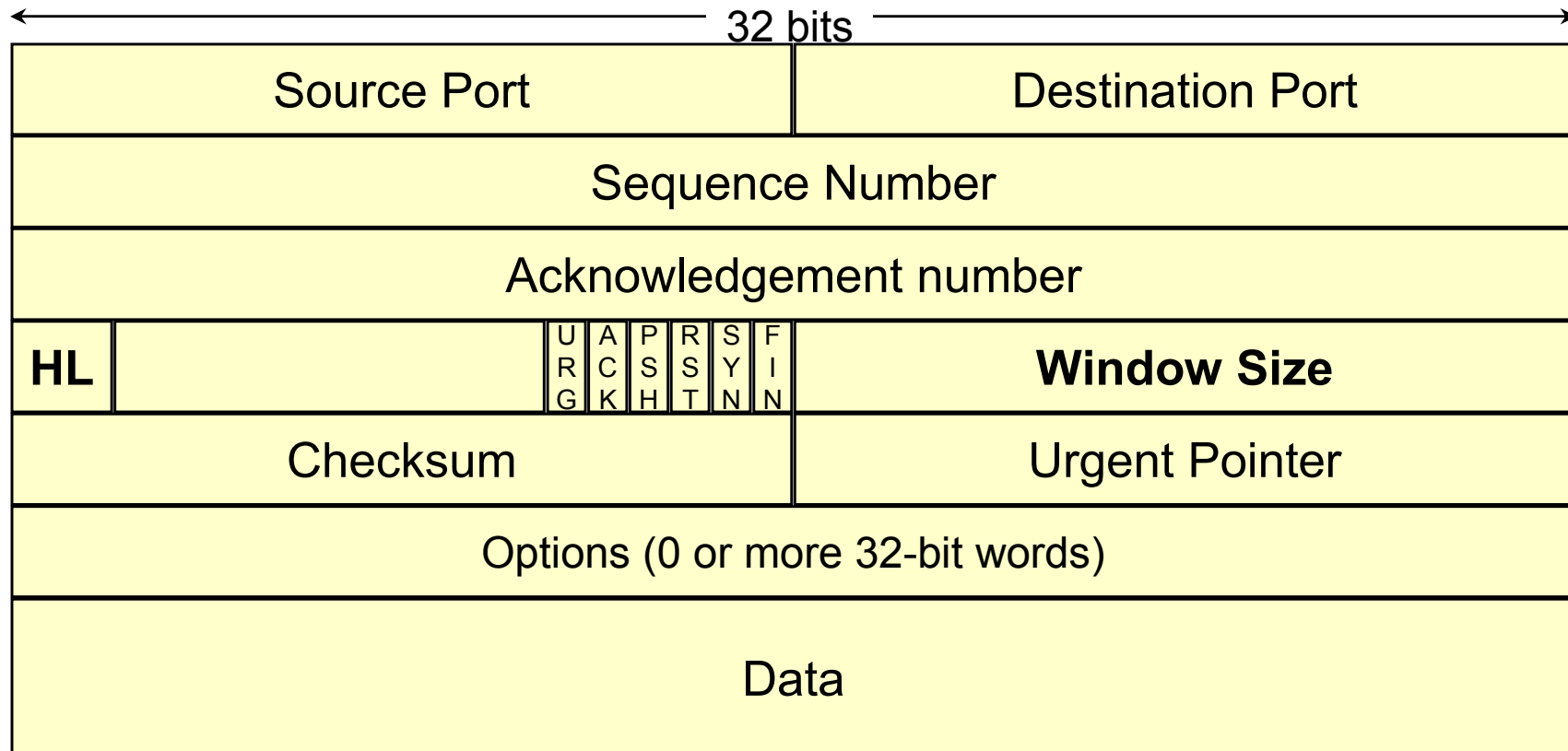
- **3-way handshaking** is required to establish virtual connection before sending any message.
- Sending message
 - Before sending a message, a transport layer sends its own message to the transport layer at the destination telling that a message is about to be sent.
 - It then waits for this message to be acknowledged before starting to send the application layer's message.
 - Use acknowledgement and packet retransmissions to confirm that all packets are successfully transferred to the destination

TCP Initial: SYN, SYN-ACK, ACK

TCP Final: FIN, ACK, FIN-ACK, ACK

TCP no connection: SYN and RES-ACK

TCP Frame Format



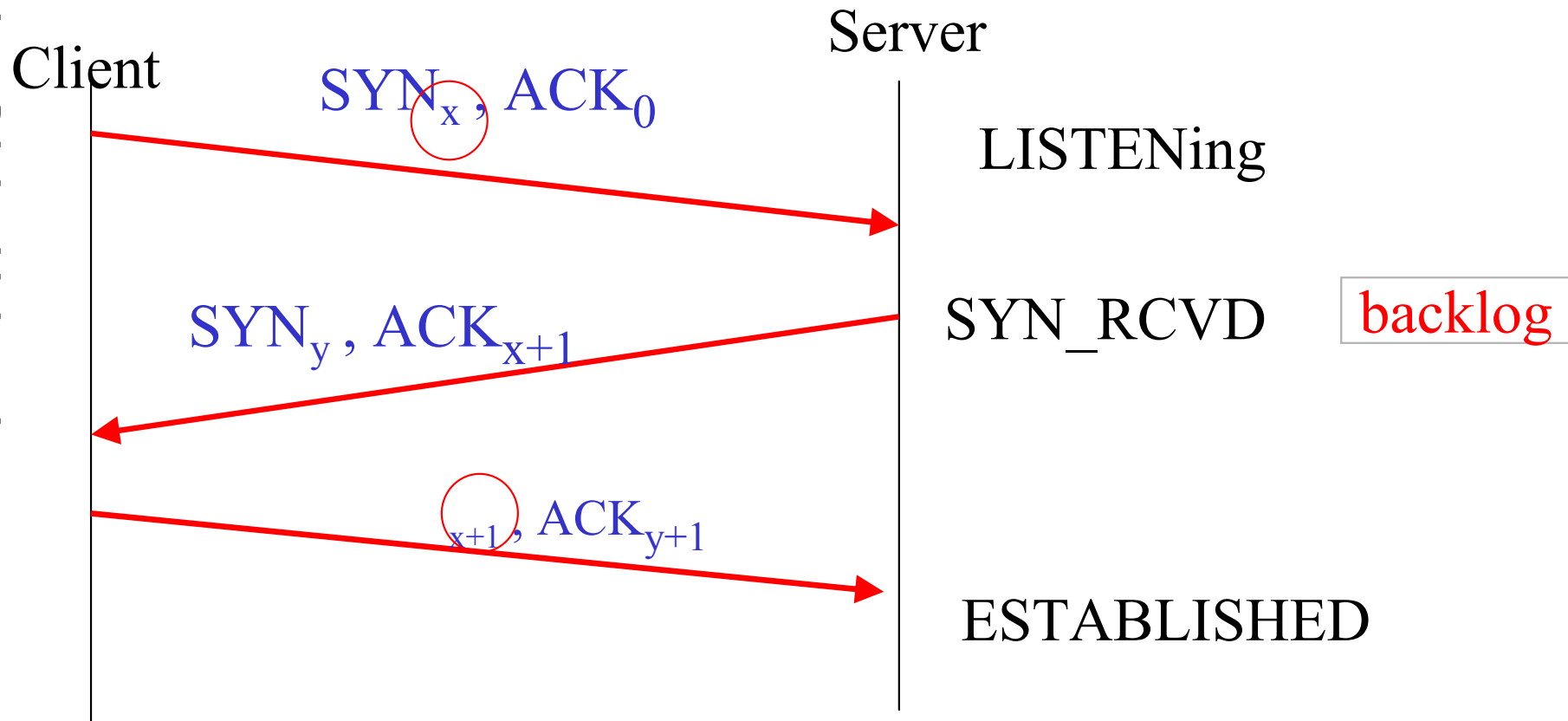
SYN : Used to establish connections

ACK = Indicates whether frame contains Acknowledgement

Window size determines how much data a receiving station can accept at one time.

TCP -- connection-oriented

3-way Hand Shaking



http://en.wikipedia.org/wiki/Transmission_Control_Protocol

Network Layer (Layer 2; IP Layer)

- Determine intermediate router address for each packet if necessary
- Append intermediate or ultimate destination address to each packet

- Also known as **Layer 3** in **OSI 7-layer Reference Model**
- Also known as **IP Layer** (**Network Layer == IP Layer**)
- A LAN connects to a WAN via a **Router**

TCP/IP **Layer 2** == **IP Layer** == **Network Layer**

Network Layer(網路層)=IP Layer (cont.)

- There is only one network protocol :
Internet **P**rotocol, or **I**P
- The **network** access layer(網路存取層), refers to the particular **LAN** or **WAN** technology that is being used
- IP header: 填入 **12 octets** 重要資訊(含TTL, protocol) 接著雙方 IP,再接著 options (if any), 再來是 IP data, 最後有 32-bit 的 CRC 檢查值

Octet : 指 8 bits 的 Byte; 因一Byte 可能 6bits, 7bits, 8bits

Link Layer (Layer 1) (MAC Layer)

- Deals with the communication details particular to the individual networks in which the machine resides
- Translates the Internet addresses appearing outside of the packets into the appropriate local addressing system
- Add these translated addresses to the packet
- Example:
 - Ethernet: **CSMA/CD** Carrier **S**ense, **M**ultiple **A**ccess with **C**ollision **D**etection
 - Token ring: one-way communication around ring network

Ethernet is the most popular medium access control protocol.

TCP/IP Layer 1 == MAC Layer == Data Link Layer

MAC

Medium Access Control

The class of protocols that handle medium access problems

Example

- Ethernet (IEEE 802.3)
- Wireless LAN (IEEE 802.11)
- Bluetooth (IEEE 802.15)
- WiMAX (IEEE 802.16) (Broadband Wireless Access Standards)
- 3GPP LTE (Long Term Evolution)

啥是 802.??
Next slides

Ethernet is the most popular Medium Access Control protocol.

3GPP: 3rd Generation Partnership Project

OSI Reference Model vs. TCP/IP Model

OSI 7-Layer

TCP/IP

7	Application			
6	Presentation		Application	4
5	Session			
4	Transport		Transport (TCP, UDP)	3
3	Network		Internet	2
2	Data Link		網路卡 Network interface	1
1	Physical			

TCP/IP 沒有定義實體層(physical layer)

Similarities of OSI 7-Layer vs. TCP/IP

- Both have layers
- Both have application layers, though they include very different services
- Both have comparable transport and network layers
- Packet-switched (not circuit-switched) technology is assumed
- Networking professionals need to know both

Differences of OSI 7-Layer vs. TCP/IP

TCP/IP combines the **presentation** and **session** layer issues into its **application** layer

TCP/IP combines the OSI data link and physical layers into one layer (或說 **TCP/IP 沒有定義實體層**)

TCP/IP appears simpler because it has fewer layers

TCP/IP protocols are the standards around which the Internet developed, so the TCP/IP model gains credibility just because of its protocols. In contrast, typically networks aren't built on the OSI protocol, even though **the OSI model is used as a guide**. (i.e., as Reference)

Addresses at Layers

- Physical Layer: no address necessary
- Data Link Layer - address must be able to select any host on the network. (MAC address)
- Network Layer - address must be able to provide information to enable routing. (IP address)
- Transport Layer - address must identify the destination process. (Port number)

CSMA/CD again

802.3 or Ethernet

*Carrier Sense Multiple Access
with Collision Detection*

-
- *Carrier Sense*: can tell when another host is transmitting
 - *Multiple Access*: many hosts on 1 wire
 - *Collision Detection*: can tell when another host transmits at the same time.

http://en.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_detection

The Mechanisms of CSMA/CD

- Each computer listens on the Ethernet
 - If not sensing data on the carrier, OK to send its own data (**C**arrier **S**ense, **M**ultiple **A**ccess)
 - If sensing data on the carrier, check whether the data is addressed for itself
- In case of simultaneous transmissions, (collisions) (**C**ollision **D**etection)
 - The computer waits a **random period** of time before re-send
 - **Exponential back-off** (binary back-off)

CSMA/CD: **C**arrier **S**ense, **M**ultiple **A**ccess with **C**ollision **D**etection

Ethernet - IEEE 802.3 (1/2)

- **Hub** (集線器)– **bus topology**
 - Collision : **CSMA/CD**
 - 10Mbps shared, 100Mbps shared
 - Cheap
- **Switch** (交換器)– **star topology**
 - No collision (送第一次仍會廣播,之後記住MAC)
 - 100Mbps each; 1Gbps each for Gbit Switch
 - Expensive for Gbit Switch at now (2005)

其實 Ethernet 與 IEEE 802.3 並非完全一樣

Ethernet - IEEE 802.3 (2/2)

- **Ethernet** developed by Xerox in mid 1970s
- Basic ideas from AlohaNet packet radio project
- Ethernet standardized by Xerox, DEC, Intel in 1978
- IEEE later standardized as 802.3 - at **MAC layer differs in one header field from Ethernet**
- 10, 100, 1000 Mbps(802.3ab 1000BaseT at 1999, 802.3z Gigabit Ethernet at 1998)
- 10 Gbps (**802.3ae 10Gbps** at 2003)
- 100 Gbps (**802.3ba 100Gbps** at 2010)
- 802.3af – Power over Ethernet (at 2003)

<http://www.ieee802.org/3/>
<http://www.ieee802.org/3/>

Ethernet Technology

Origin: Xerox in 1970

Standard: Xerox, Intel and Digital in 1978.

IEEE standard number: 802.3

Maximum distance: 500m

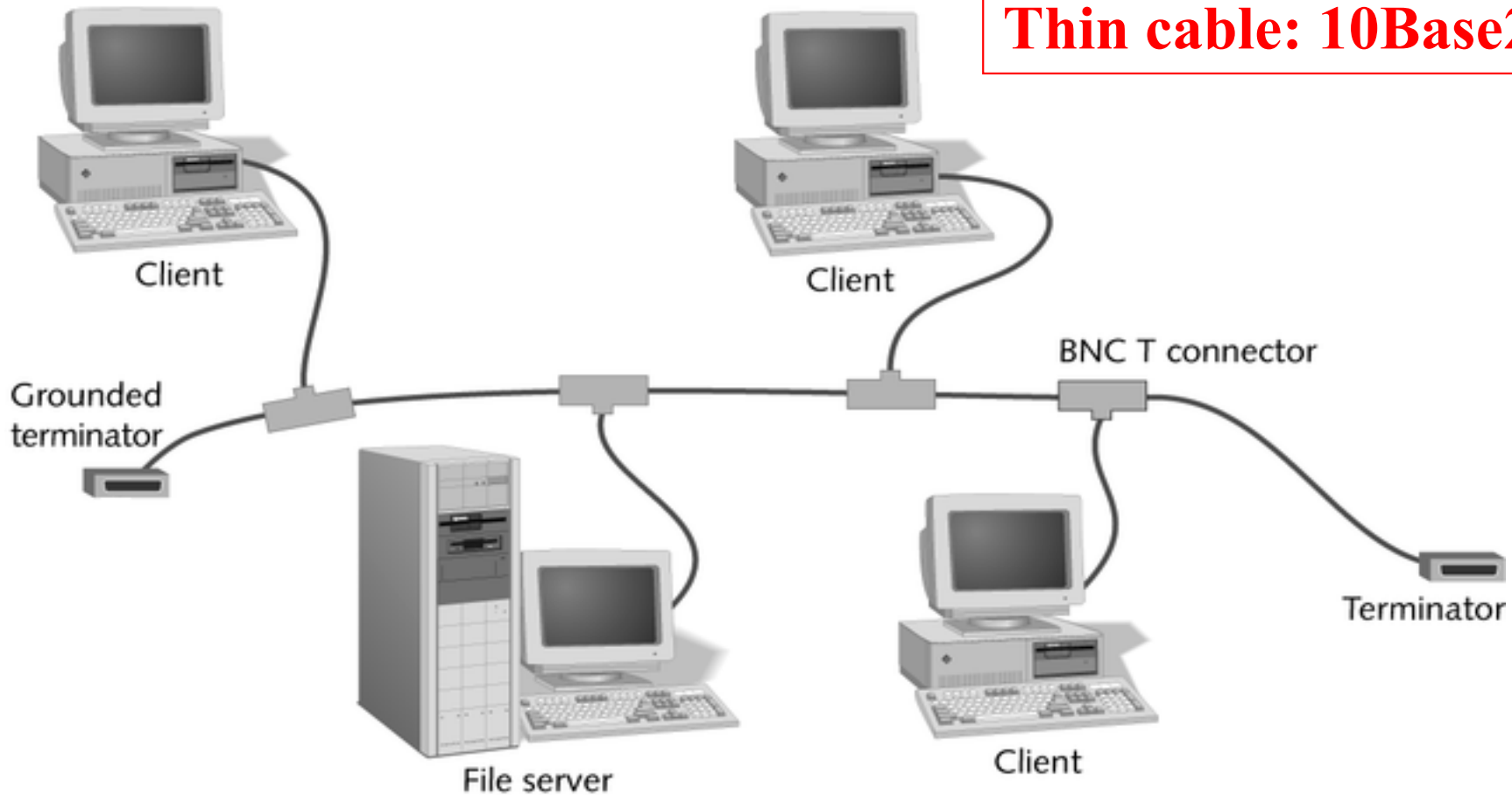
Items Types	Max. Distance	Connector	Line
Thick Ethernet	500m	AUI	10 Base 5
Thin Ethernet	185m	BNC	10 Base 2
Twisted-Pair Ethernet	100m	RJ-45	10 Base T 100Base T 1000Base T

10Base2 Network

長度不可超過 500公尺

長度不可超過185公尺

Thick cable: 10Base 5
Thin cable: 10Base2



Coaxial cable (同軸電纜)

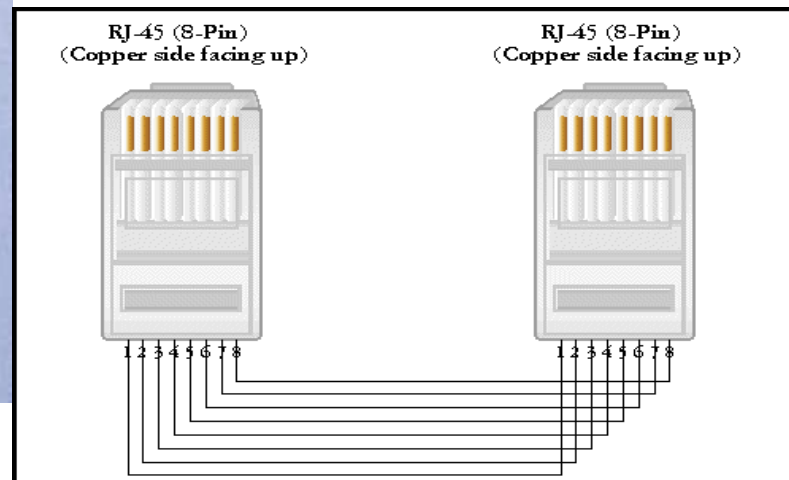
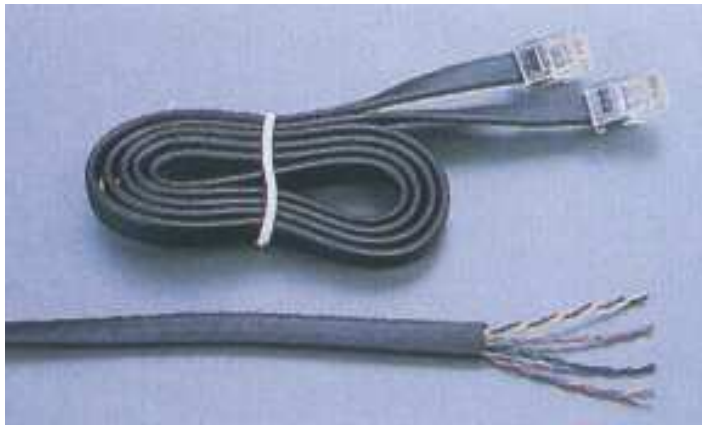
10BaseT, 100BaseT, 1000Base T

This is the current and most widely used method of hooking Ethernet devices together

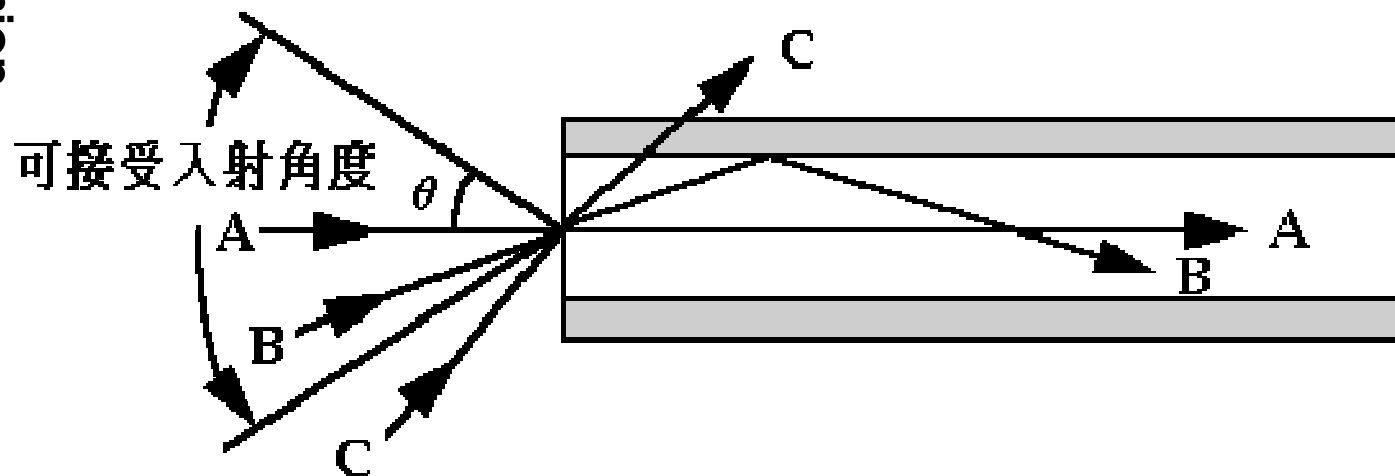
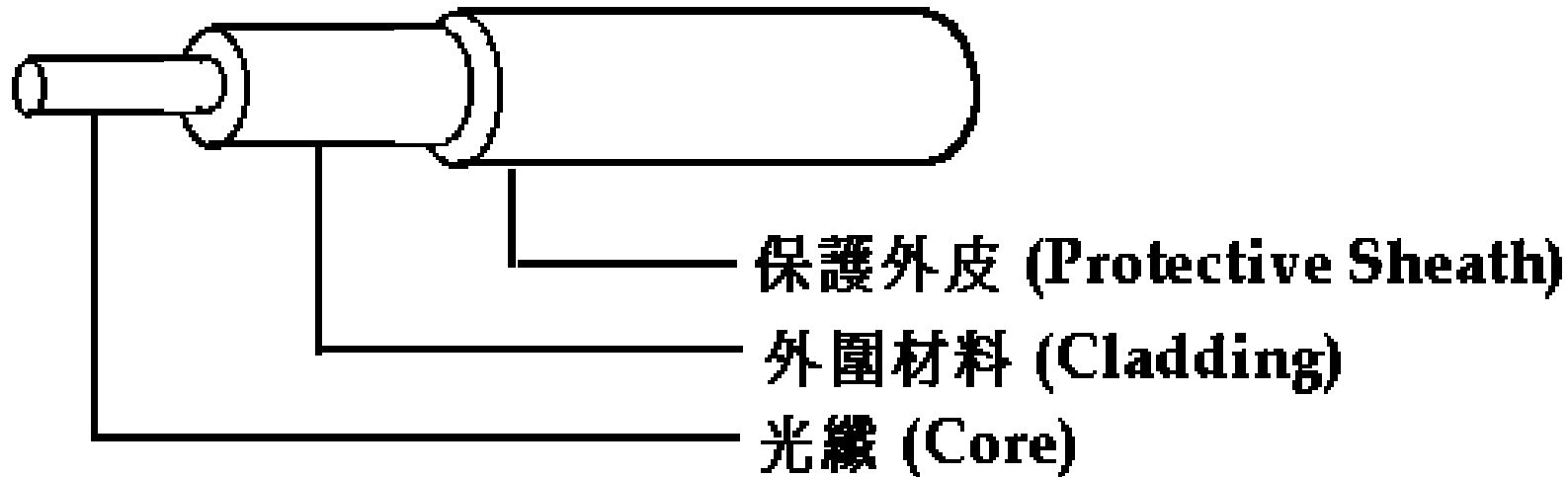
This layout requires a central hub and wiring in a star pattern using Cat 5 Unshielded **Twisted Pair** wiring (UTP)

The wiring is terminated using RJ45 connectors

Twisted-pair
(雙絞線)



Fiber optical cable (光纖)



IEEE 802 Family : 802.3? 802.11?

- 802.1 → 高層介面、網路互連
- 802.2 → 邏輯鏈結控制 (LLC = *Logical Link Control*)
- **802.3 → CSMA/CD 乙太網路 (Carrier-Sense Multiple Access with Collision Detection)**
- 802.4 → 權杖匯流排 (Token bus) 網路，或稱記號匯流排網路
- 802.5 → 權杖環 (Token ring) 網路，也有人稱記號環網路
- 802.6 → 都會網路 (MAN, Metropolitan Area Network)
- 802.7 → 寬頻區域網路 (Broadband LAN)
- 802.8 → 光纖區域網路 (Fiber Optic LAN)
- 802.9 → 多媒體傳輸 (Multimedia traffic)，整合聲音與網路資料
- 802.10 → 網路保全 (Security)
- **802.11 → 無線網路 (Wireless Network)**
- 802.12 → 需求優先存取 *Demand Priority* 區域網路 (100BaseVG-AnyLAN)
- 802.14 → 有線電視通訊網 (Cable modems)
- 802.15 → Wireless Personal Area Network (WPAN), 802.15.1 Bluetooth certification; 802.15.4 Low Rate WPAN = ZigBee; 802.15.3 High Rate WPAN
- 802.16 → WiMAX
- **802.1x → Port Based Network Access Control (Authentication)**

802.11 or WiFi

Wireless: Intended Use Any Time Any Where

隨時隨地都可上網遨遊

Wireless Internet access inside hotel lobbies, conference rooms, etc.



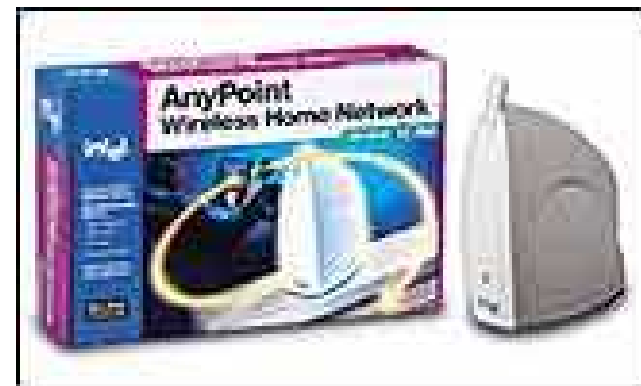
← Wireless at the Airport



- Wireless with your Latte?



- Wireless home networking →



AnyPoint Wireless Home Network

802.11 or WiFi

Wireless LAN (Wi-Fi)



CSMA/CA

*Carrier Sense Multiple Access
with Collision Avoidance*

- Wi-Fi 是與 802.3 Ethernet 相容的**無線**通信協定
- Wi-Fi技術代號是**IEEE 802.11**，也叫做Wireless LAN
- 適用範圍在 **50 到 150 公尺**之間，**Transmission rate** 可到 **11Mbps** (802.11b) 甚至到 54Mbps (802.11g, 802.11a) (802.11n 有些廠商宣稱可到 300Mbps 甚至 600Mbps)

http://en.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_avoidance

Differences between IEEE 802.11?

	IEEE 802.11	IEEE 802.11 b	IEEE 802.11 a	IEEE 802.11 g
Frequency	2.4G Hz	2.4G Hz	5 G Hz	2.4G Hz
Transmission Rate	1~2 Mbps	1~11Mbps	6~54 Mbps	22~54Mbps
Modulation Technique	FHSS/DSSS	FHSS/DSSS	OFDM	PBCC-22 + CCK-OFDM

802.11n = a + b + g; multiple-input multiple-output (MIMO)

IEEE 802.11 Work Groups (1/3)

http://grouper.ieee.org/groups/802/11/QuickGuide_IEEE_802_WG_and_Activities.htm

Group	Label	Description	Status
IEEE 802.11 Working Group	WG	The Working Group is comprised of all of the Task Groups together	
Task Group	TG	The committee(s) that are tasked by the WG as the author(s) of the Standard or subsequent Amendments	
MAC Task Group	MAC	develop one common MAC for Wireless Local Area Networks	IEEE Std. 802.11-1997
PHY Task Group	PHY	three PHY's for Wireless Local Area Networks (WLANs) applications, using Infrared (IR), 2.4 GHz Frequency Hopping Spread Spectrum (FHSS), and 2.4 GHz Direct Sequence Spread Spectrum (DSSS)	IEEE Std. 802.11-1997
Task Group a	TGa	develop a PHY to operate in the newly allocated UNII band	IEEE Std. 802.11a-1999

<http://www.ieee802.org/11/>

IEEE 802.11 Work Group(2/3)

Group	Label	Description	Status
Task Group b	TGb	develop a standard for a higher rate PHY in the 2.4GHz band	IEEE Std. 802.11b-1999
Task Group b-cor1	TGb-Cor1	correct deficiencies in the MIB definition of 802.11b	Part of 802.11-2007
Task Group c	TGc	add a subclause under 2.5 Support of the Internal Sub-Layer Service by specific MAC Procedures to cover bridge operation with IEEE 802.11 MACs	Part of IEEE 802.1D
Task Group d	TGd	define the physical layer requirements	Part of 802.11-2007
Task Group e	TGe	Enhance the 802.11 Medium Access Control (MAC) to improve and manage Quality of Service, provide classes of service, and enhanced security and authentication mechanisms	Part of 802.11-2007

http://grouper.ieee.org/groups/802/11/QuickGuide_IEEE_802_WG_and_Activities.htm

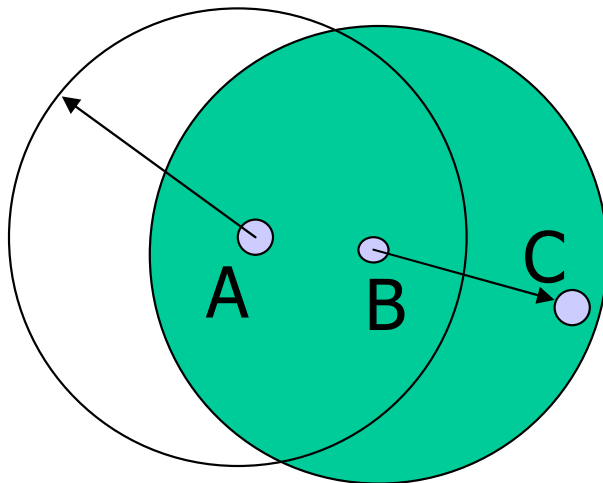
IEEE 802.11 Work Group(3/3)

Group	Label	Description	Status
Task Group f	TGf	develop recommended practices for an Inter-Access Point Protocol (IAPP) which provides the necessary capabilities to achieve multi-vendor Access Point interoperability	802.11F-2003; withdrawn on 2006
Task Group g	TGg	develop a higher speed(s) PHY extension to the 802.11b standard	Part of 802.11-2007
Task Group h	TGh	Enhance the 802.11 Medium Access Control (MAC) standard and 802.11a High Speed Physical Layer (PHY) in the 5GHz Band	Part of 802.11-2007
Task Group I	TGi	Enhance the 802.11 Medium Access Control (MAC) to enhance security and authentication mechanisms	ditto
Task Group n	TGn	Improves upon the previous 802.11 standards by adding multiple-input multiple-output (MIMO) and many other newer features. ($n = a + b + g$)	
Study Group	SG	Investigates the interest of placing something in the Standard	

IEEE 802.11 (Wireless Ethernet)

802.11 or WiFi

- CSMA/CA
- Why can't we use regular Ethernet for wireless?
 - **Ethernet**: A sees B, B sees C, $\rightarrow$ A sees C
 - Wireless: Hidden node problem
A sees B, B sees C, yet A does not see C



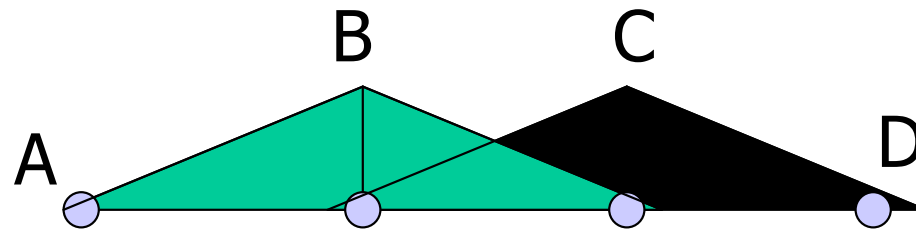
CSMA/CA

*Carrier Sense Multiple Access
with Collision Avoidance*

IEEE 802.11 vs. 802.3 (Wireless Ethernet) vs. Ethernet

802.11 or WiFi

- Why can't we use regular Ethernet for wireless?
 - **Ethernet**: B sees C, C sees D $\rightarrow$ B & C can't send together
 - Wireless: B can send to A while C sends to D

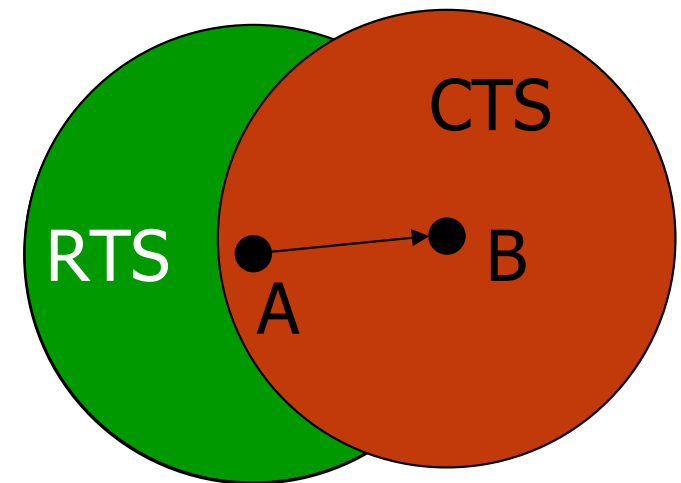


802.11 transmission Protocol

CSMA/CA

802.11 or WiFi

- **Sender A** sends Request-to-Send (RTS)
- Receiver B sends Clear-to-Send (CTS)
 - Nodes who hear **CTS cannot** transmit concurrently with A (**red region**)
 - Nodes who hear RTS but not CTS still can transmit (**green region**) (might collision)
- **Sender A** sends data frame
- Receiver B sends ACK
- Nodes who hear the ACK can now transmit



http://en.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_avoidance

802.11 Collision Resolution

MAC Layer : CSMA/CA

- Collision still might happen
 - Two senders might send RTS at the same time; Collision will occur corrupting the data if this happens
 - No CTS will follow if collision occurs
 - Senders will time-out waiting for CTS and retry with exponential backoff

Carrier Sense Multiple Access
/Collision Avoidance

RTS: **R**equ**e**st-**T**o-**S**end
CTS: **C**lear-**T**o-**S**end

Status of IEEE 802.11i

http://grouper.ieee.org/groups/802/11/Reports/tgi_update.htm

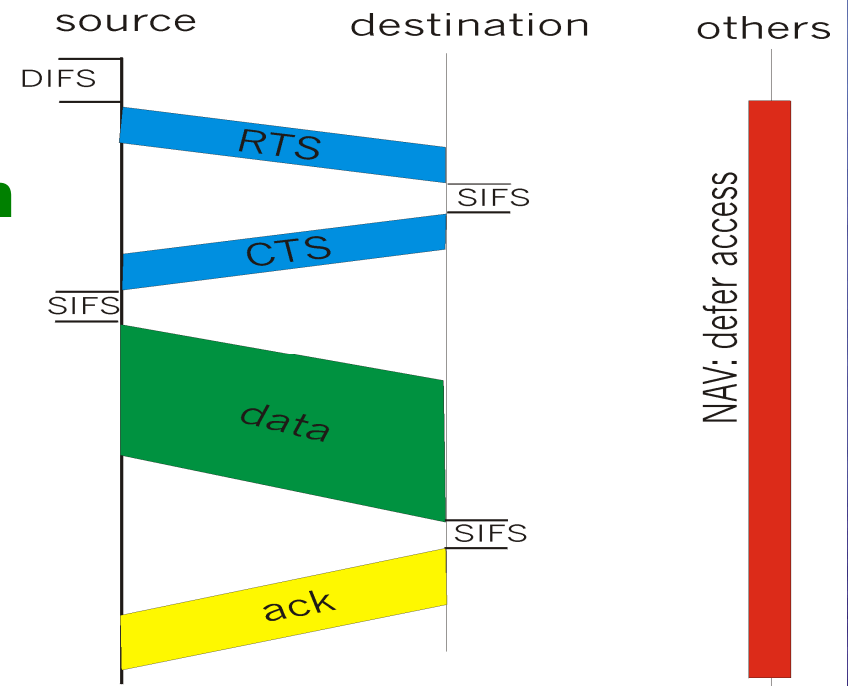
- 2002/2 – preparing TGi draft
- Used to improve the **network security**
- WEP2 – Increases IV spaces to 128Bits.
- Kerberos
- **802.1X Authentication**
 - 注意不是 802.11x

IV : Initial Vector

Collision Avoidance: RTS-CTS exchange

802.11 or WiFi

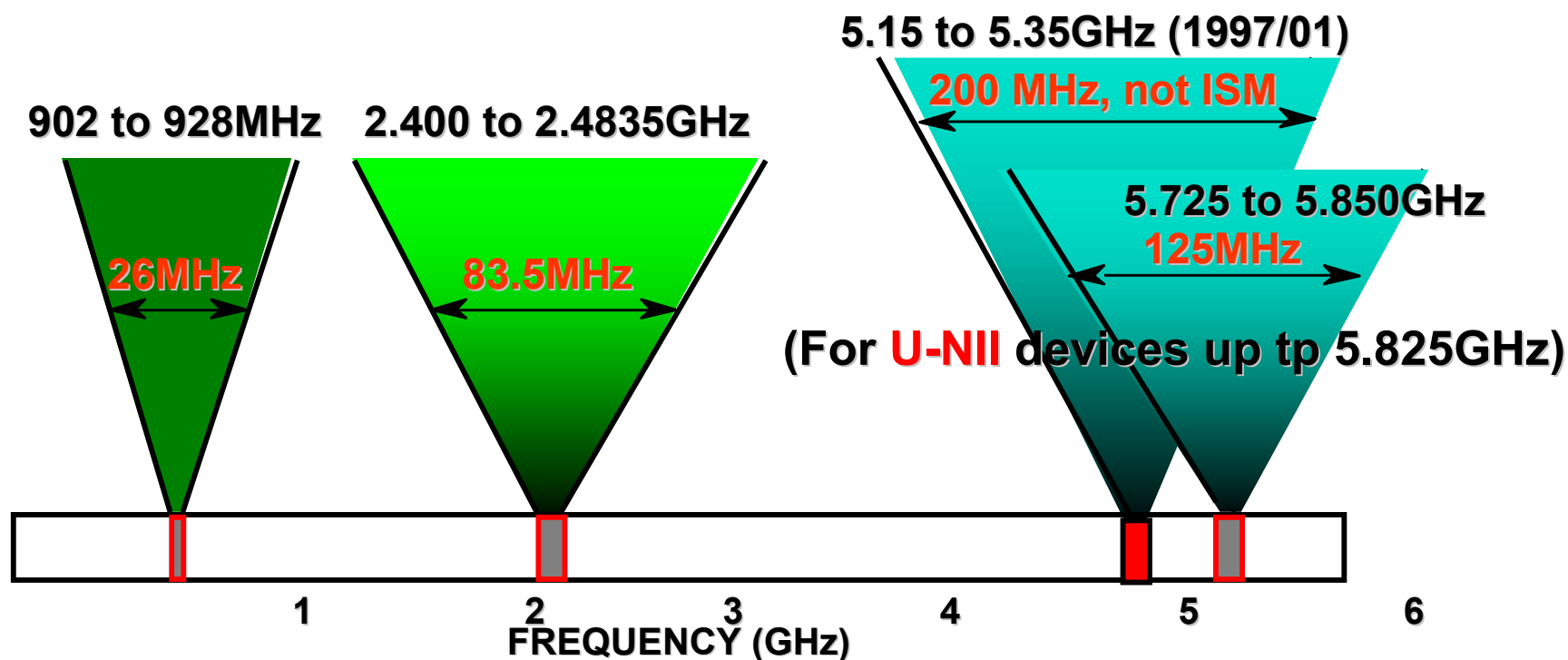
- **CTS “freezes” stations within range of receiver (but possibly hidden from transmitter); this prevents collisions by hidden station during data**
- **RTS and CTS are very short: collisions during data phase are thus very unlikely (the end result is similar to Collision Detection)**



Note: IEEE 802.11 allows CSMA, CSMA/CA and “polling” from AP

Industrial, Scientific and Medical (ISM) Bands

http://www.fcc.gov/Bureaus/Engineering_Technology/Orders/1997/fcc97005.pdf



- UNLICENSED OPERATION GOVERNED BY FCC DOCUMENT 15.247, PART 15
- SPREAD SPECTRUM ALLOWED TO MINIMIZE INTERFERENCE
- 2.4GHz ISM BAND
 - More Bandwidth to Support Higher Data Rates and Number of Channels
 - Available Worldwide
 - Good Balance of Equipment Performance and Cost Compared with 5.725GHz Band
 - IEEE 802.11 Global WLAN Standard

UNII band : **U**nlicensed **N**ational **I**nformation **I**nfrastructure band

AP96358 3-4

Slide 4b-62

Channel allocation for 802.11b

每channel佔22MHz, 但只相隔5MHz

Ch1: 2.401 ~ 2.412GHz ~ 2.423GHz

Ch2: 2.406 ~ 2.417GHz ~ 2.428GHz

Ch3: 2.411 ~ 2.422GHz ~ 2.433GHz

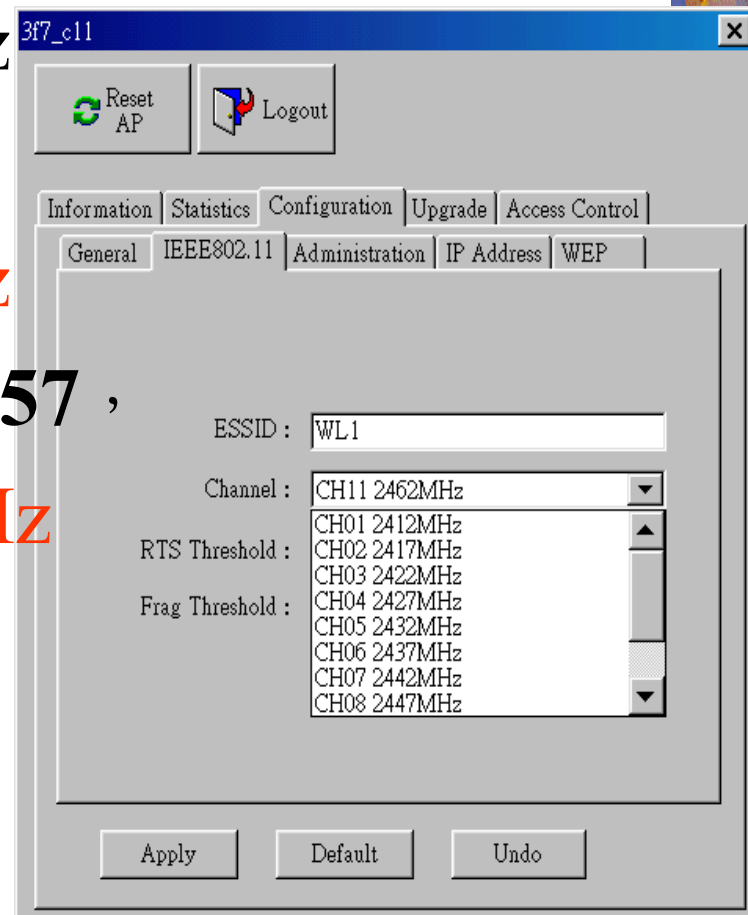
2.427GHz , 2.432GHz

Ch6: 2.426 ~ 2.437GHz ~ 2.448GHz

2.442 , 2.447 , 2.452 , 2.457 ,

• Ch11: 2.451 ~ 2.462GHz ~ 2.473GHz

歐洲 ~ ch 13, 日本 ~ ch14



tsaiwn@csie.nctu.edu.tw

The Frequencies of Various Wireless Media

Frequency (H_z)

Ultraviolet : 0.75P ~30PHz ; 10nm ~ 400nm

Infrared light : 1T~430THz; 0.7~300micrometers

極超高頻 SHF Super High Frequency, 頻率範圍 GHz~30GHz.

超高頻 UHF Ultra High Frequency, 頻率範圍 300MHz~3000MHz.

極高頻 VHF Very High Frequency, 頻率範圍 30MHz~300MHz.

高頻 HF High Frequency, 頻率範圍 3MHz~30MHz.

10^{16}
 10^{15}
 10^{14}
 10^{13}
 10^{12}
 10^{11}
 10^{10}
 10^9
 10^8
 10^7
 10^6
 10^5
 10^4
 10^3
 10^2
 10^1

X rays, gamma rays

Ultraviolet light

Visible light

Infrared light

紫外線

紅外線

Millimeter waves

Microwaves

UHF television

VHF television

VHF TV (high band)

FM radio

VHF TV (low band)

Short-wave radio

AM radio

毫米波

微波

Very Low Frequency

Electromagnetic Spectrum

waveLength * frequency = Light Speed = 299,792,458 m/second (3×10^8 米/秒)

γ = Gamma rays

HX = Hard X-Rays

X = Soft X-Rays

EUV = Extreme UltraViolet

NUV = Near UltraViolet

NIR = Near Infrared

MIR = Mid Infrared

FIR = Far Infrared 遠紅外線

EHF = Extremely High Freq.

SHF = Super High Freq.

UHF = Ultra High Freq.

VHF = Very High Freq

High / Medium / Low Freq.

VLF = Very Low Frequency

VF/ULF = Voice Frequency

SLF = Super Low Frequency

ELF = Extremely low freq.

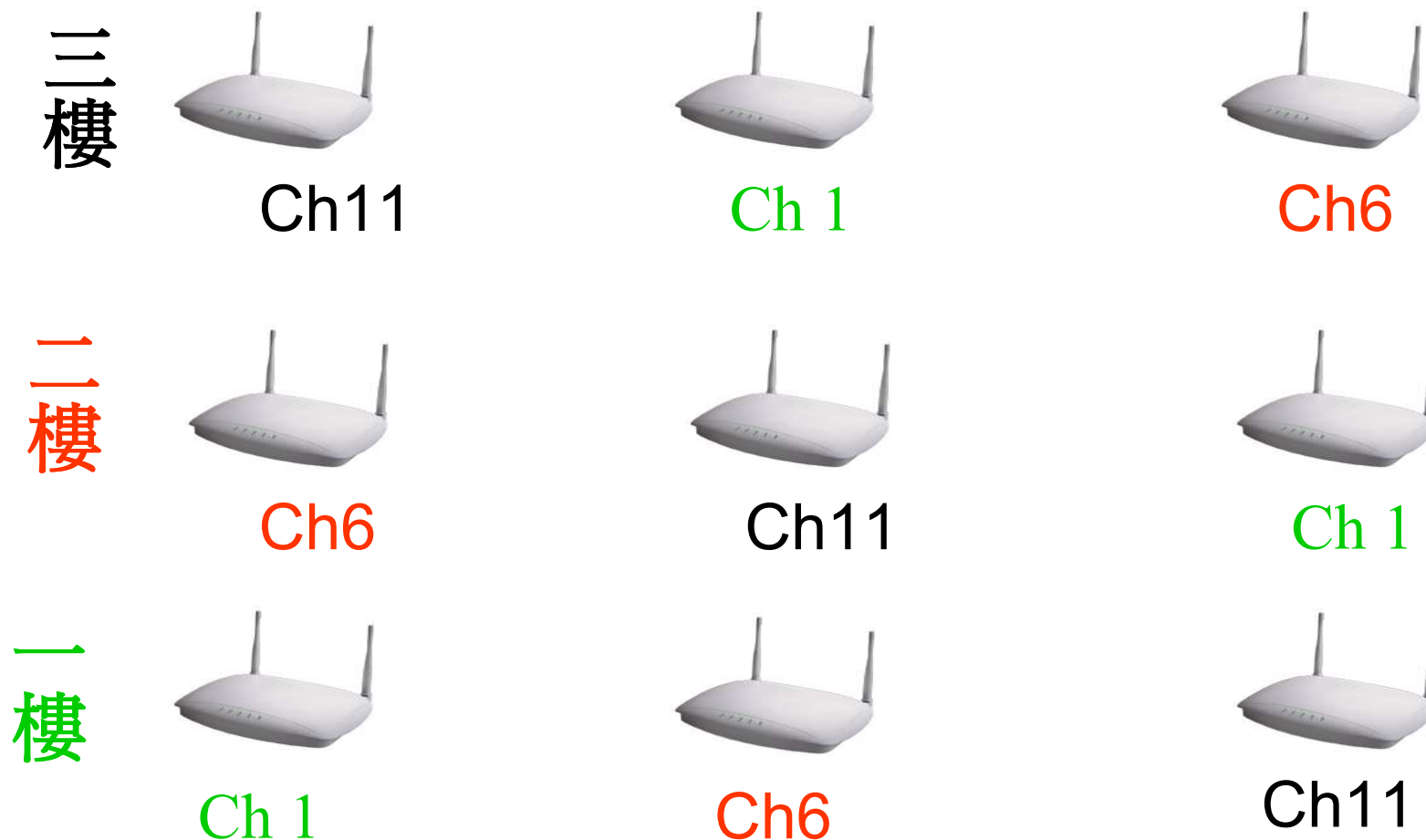
CLASS	FREQUENCY	WAVELENGTH	ENERGY
Y	300 EHz	1 pm	1.24 MeV
HX	30 EHz	10 pm	124 keV
	3 EHz	100 pm	12.4 keV
SX	300 PHz	1 nm	1.24 keV
EUV	30 PHz	10 nm	124 eV
NUV	3 PHz	100 nm	12.4 eV
	300 THz	1 μ m	1.24 eV
NIR	30 THz	10 μ m	124 meV
MIR	3 THz	100 μ m	12.4 meV
FIR	300 GHz	1 mm	1.24 meV
EHF	30 GHz	1 cm	124 μ eV
SHF	3 GHz	1 dm	12.4 μ eV
UHF	300 MHz	1 m	1.24 μ eV
VHF	30 MHz	10 m	124 neV
HF	3 MHz	100 m	12.4 neV
MF	300 kHz	1 km	1.24 neV
LF	30 kHz	10 km	124 peV
VLF	3 kHz	100 km	12.4 peV
VF/ULF	300 Hz	1 Mm	1.24 peV
SLF	30 Hz	10 Mm	124 feV
ELF	3 Hz	100 Mm	12.4 feV

Source: <http://en.wikipedia.org>

Slide 4b-65

Channel assignment

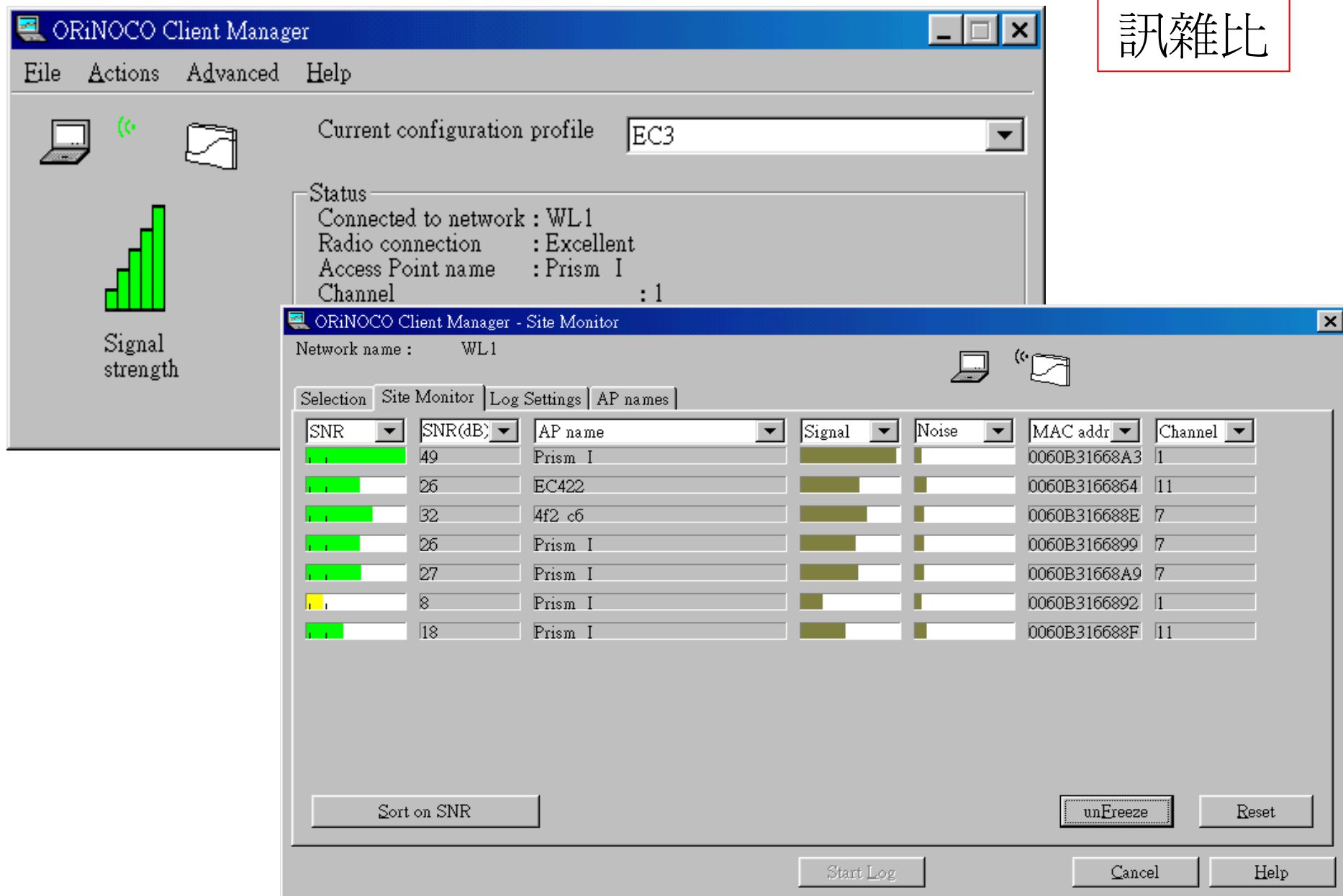
802.11 or WiFi



Channel 不能亂設定!

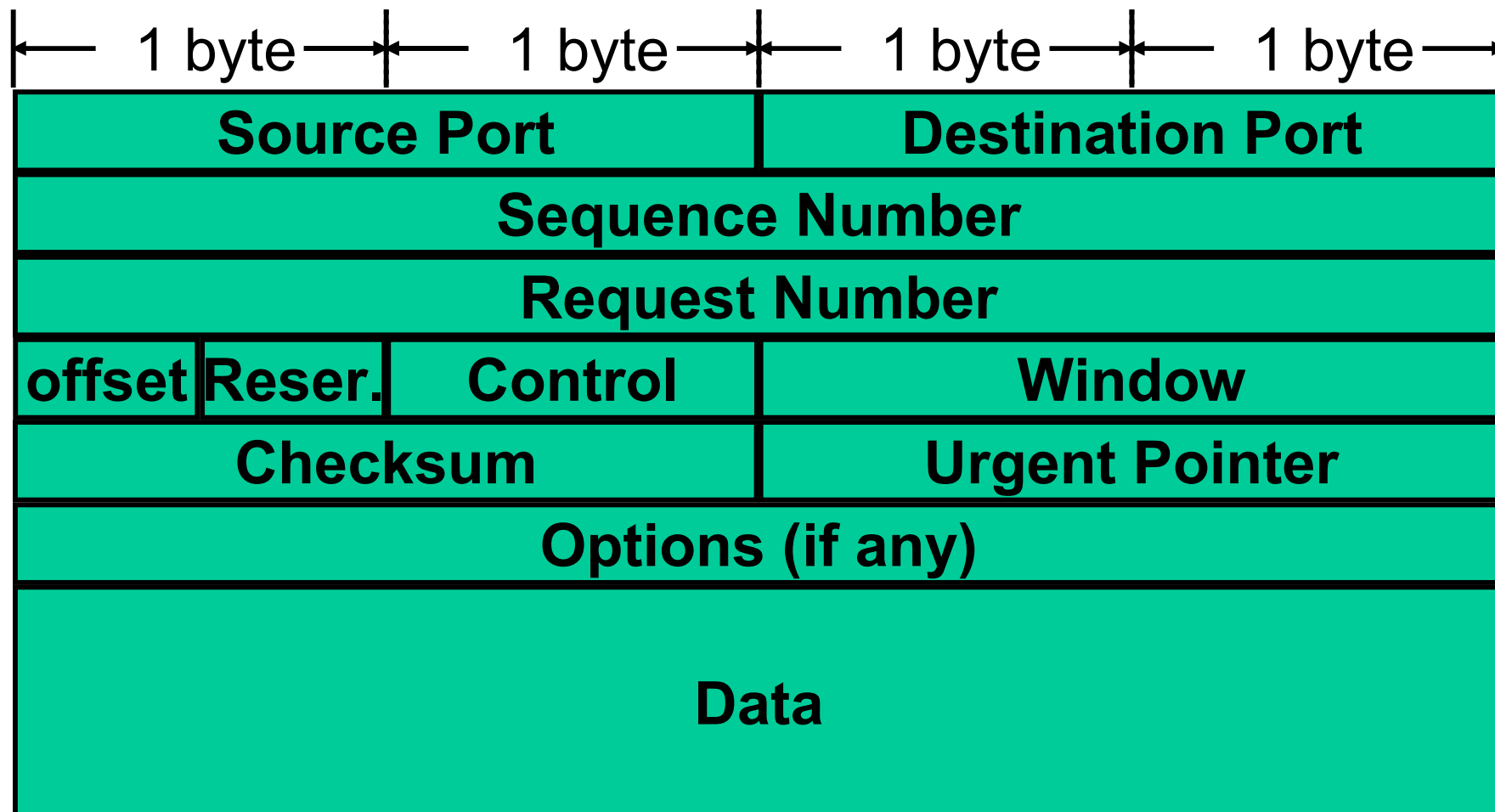
Wireless Signal /Noise Ratio (S/N Ratio)

訊雜比



TCP Segment Format

TCP/IP



UDP (User Datagram Protocol)

Datagram Delivery
Connectionless
Unreliable
Minimal

UDP is a transport layer protocol

– communication between processes

- UDP uses IP to deliver **datagrams** to the right host.

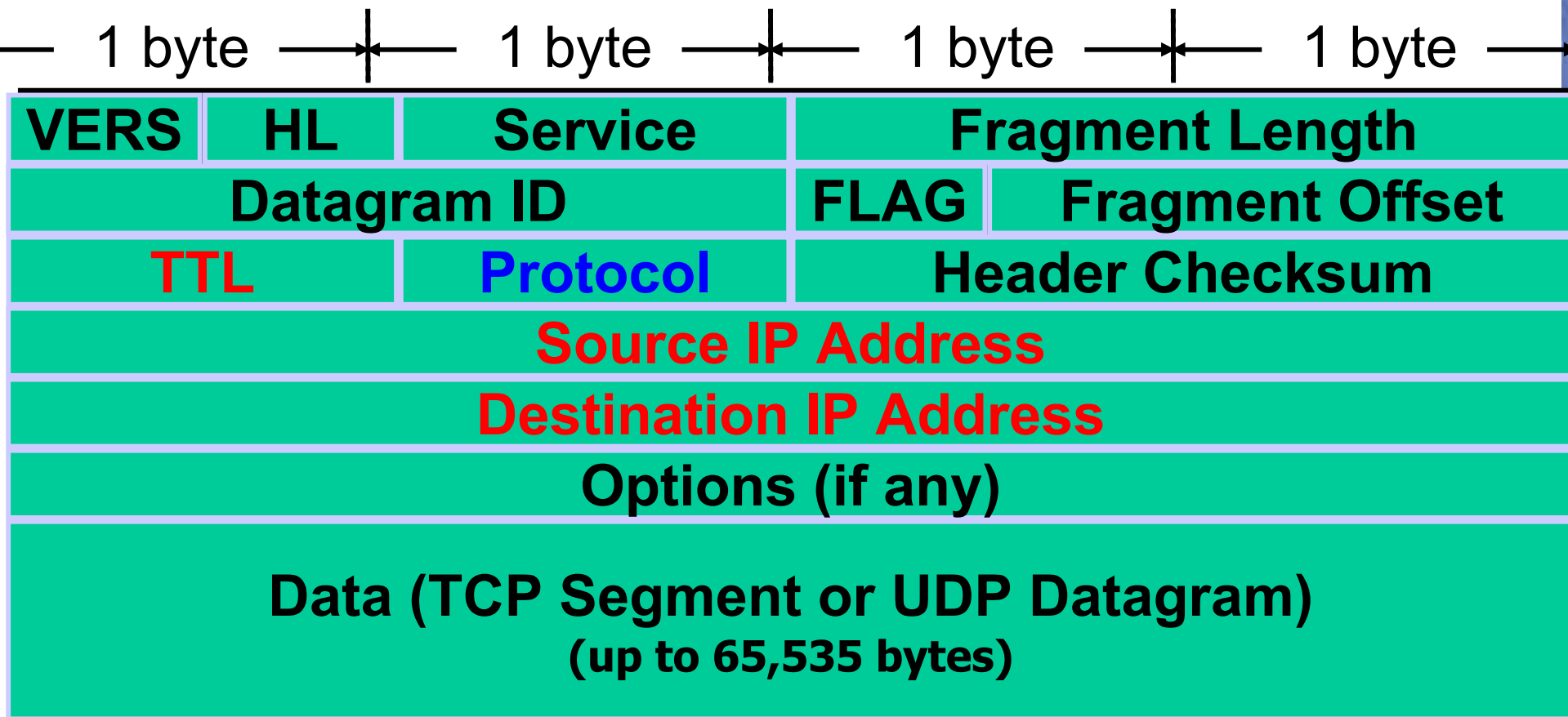
UDP Datagram Format

Source Port	Destination Port
Length	Checksum
Data	

IP Datagram (Frame type = 0x0800)

TCP/IP

<http://en.wikipedia.org/wiki/IPv4>



IP datagram is encapsulated in an **Ethernet frame**

TTL = Time-To-Live ; **Protocol** = upper Layer protocol

Protocol : 1=ICMP 6=TCP 17=UDP

Slide 4b-70

Ethernet Frame Structure

網路卡

Octet 就是
8-bit 的 Byte

Sending **adapter** encapsulates IP datagram (or other network layer protocol packet) in **Ethernet frame** :

<i>Preamble</i>	<i>Destination Address</i>	<i>Source Address</i>	<i>Frame Type</i>	<i>Frame Data</i>	<i>CRC</i>
8 octets	6 octets	6 octets	2 octets	46-1500 octets	4 octets

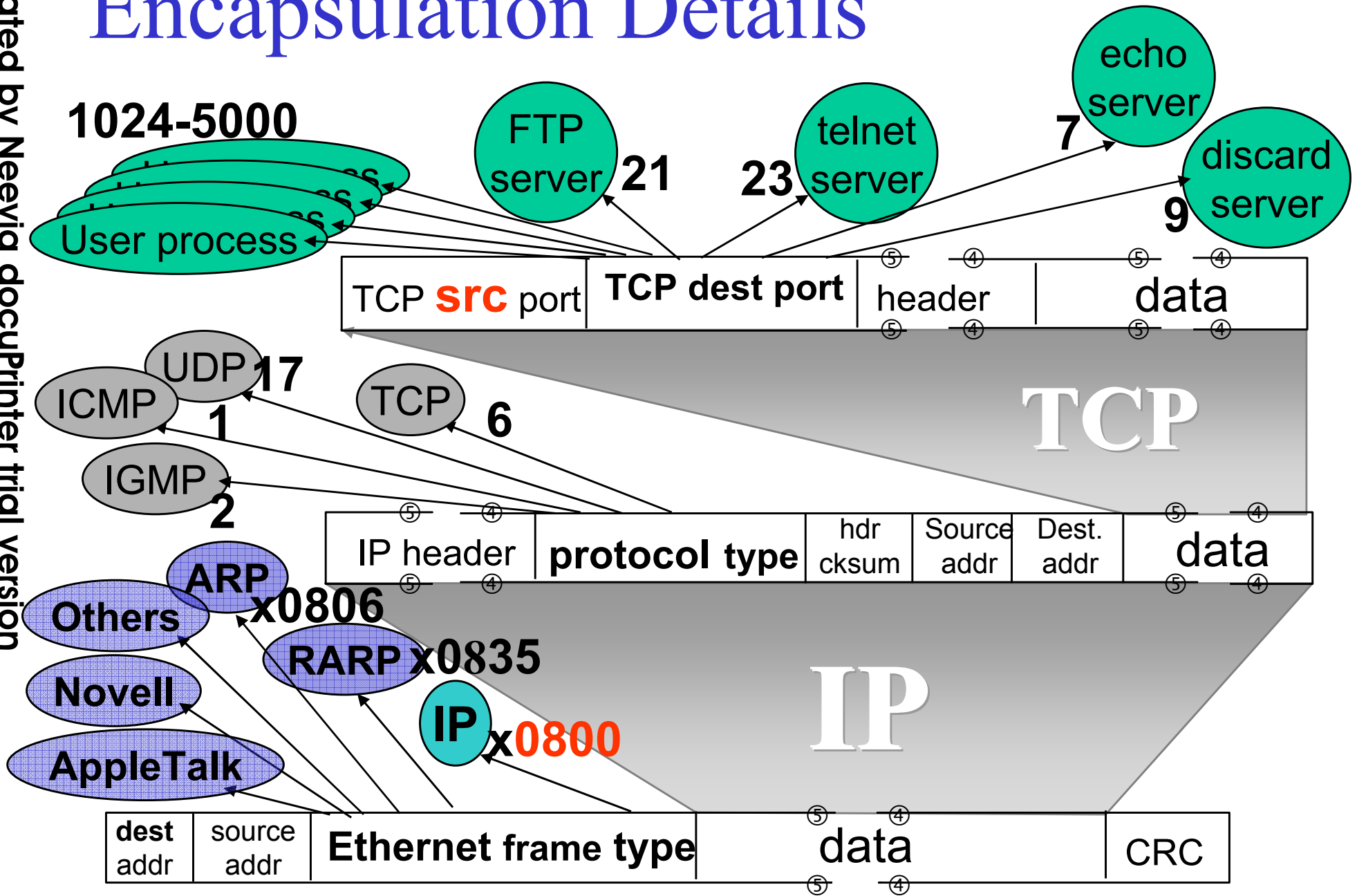
先填對方的 MAC address

(0800 表示 IP datagram)

Preamble:

- 7 bytes with pattern **10101010** followed by one byte with pattern **10101011**
- used to **synchronize** receiver, sender clock rates

Encapsulation Details



(Ethernet Frame types in hex, others in decimal)

Ether Frame Protocol Headers

06=TCP

Frame type = **0x0800** = **IP Datagram**

0000	00	08	e9	7c	22	fc	00	12	93	85	e3	c4	08	00	45	00
0010	00	2c	db	26	40	00	3f	06	0e	77	8c	e2	20	37	8c	e2
0020	24	33	01	bd	12	3f	3d	fa	0f	b6	a8	6f	87	c0	50	18
0030	bc	40	8a	7c	00	00	85	00	00	00	36	2f	a3	9e		

...|".....E.
 .,.&@.?.w.. 7..
 \$3...?=...o..P..
 .@.|.....6/..

Ethernet
 Header:
 bytes

Dest addr: **00 08 e9 7c 22 fc**
 Src addr: **00 12 93 85 e3 c4**
 frame type: **08 00**

IP Header:
 src addr: **140.226.36.55**
 dest addr: **140.226.36.51**

TCP Header:
 src port: **445**
 dest port: **4671**

NetBios Information

Header Information

$0x1bd = 256 + 11 * 16 + 13 = 445$

Payload (4 bytes)

Fragment Length = 002c = 44 bytes = (20+20+4) (TCP segment)

Network traffic (packet) analyzer

- **WireShark** (EtherReal)
- Kismet
- Tcpdump (and Libpcap)
- Cain and Abel
- Ettercap
- Dsniff
- NetStumbler
- **Sniffer** / NetXray (Sniffer Pro)

NIC:

Network Interface Card

NIC can be in promiscuous Mode : 任意模式 , 監聽模式

IP Datagram 分類 (看protocol byte)

ip 0 IP # internet protocol, pseudo protocol number
icmp 1 **ICMP # internet control message protocol**
lgmp 2 IGMP # Internet Group Management
ggp 3 GGP # gateway-gateway protocol
ipencap 4 IP-ENCAP # IP encapsulated in IP (officially ``IP")
st 5 ST # ST datagram mode
Tcp 6 **TCP # transmission control protocol**
egp 8 EGP # exterior gateway protocol
pup 12 PUP # PARC universal packet protocol
udp 17 **UDP # user datagram protocol**
hmp 20 HMP # host monitoring protocol
xns-idp 22 XNS-IDP # Xerox NS IDP
rdp 27 RDP # "reliable datagram" protocol
iso-tp4 29 ISO-TP4 # ISO Transport Protocol class 4
xtp 36 XTP # Xpress Transfer Protocol
ddp 37 DDP # Datagram Delivery Protocol
idpr-cmtp 39 IDPR-CMTP # IDPR Control Message Transport
rsfp 73 RSPF #Radio Shortest Path First.
vmtp 81 VMTP # Versatile Message Transport
ospf 89 OSPFIGP # Open Shortest Path First IGP
ipip 94 IPIP # Yet Another IP encapsulation
encap 98 ENCAP # Yet Another IP encapsulation

IP: Internet Protocol

See IP header

- IP Header: 20 ~ 60 bytes
 - Frame type = **0x0800**
 - TOS, identification, flags, **TTL**, **protocol**, options, ...

Classless Inter-Domain Routing

- IP Routing
 - routing table
- Subnetting, CIDR, and netmask
- Private IP addresses
 - 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16

- Related Commands:
 - ifconfig, netstat, route

• **netstat -r**

• **route print**

什麼意思?

試一試以上這些 command

ARP: Address Resolution Protocol

- ARP (RFC826): frame type = **0x0806**
- ARP cache

```
% arp -a  
ccsun1 (140.113.209.101) at 0:40:45:0:4:38  
ccsun2 (140.113.209.102) at 0:40:45:0:7:4  
? (140.113.209.203) at (incomplete)  
e3rtn-209 (140.113.209.254) at 0:20:9c:8:e9:d
```

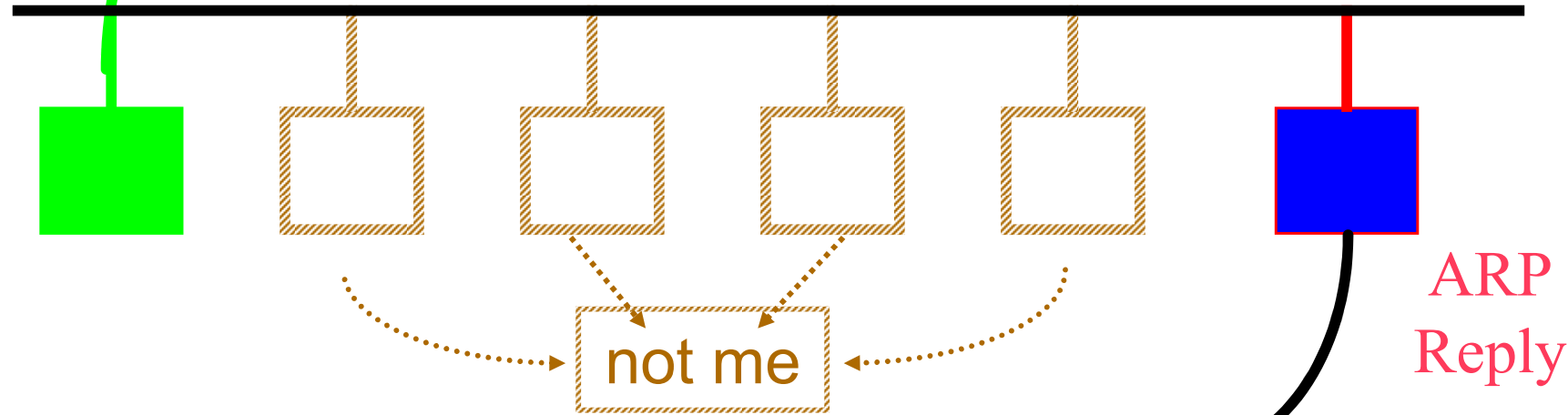
- ARP packet format: 28 bytes
 - hardware addr type/size, protocol addr type/size
 - op field (1, 2, 3, 4)
- Proxy ARP ?
- Gratuitous ARP ?

tcpdump -ntex arp

ARP conversation

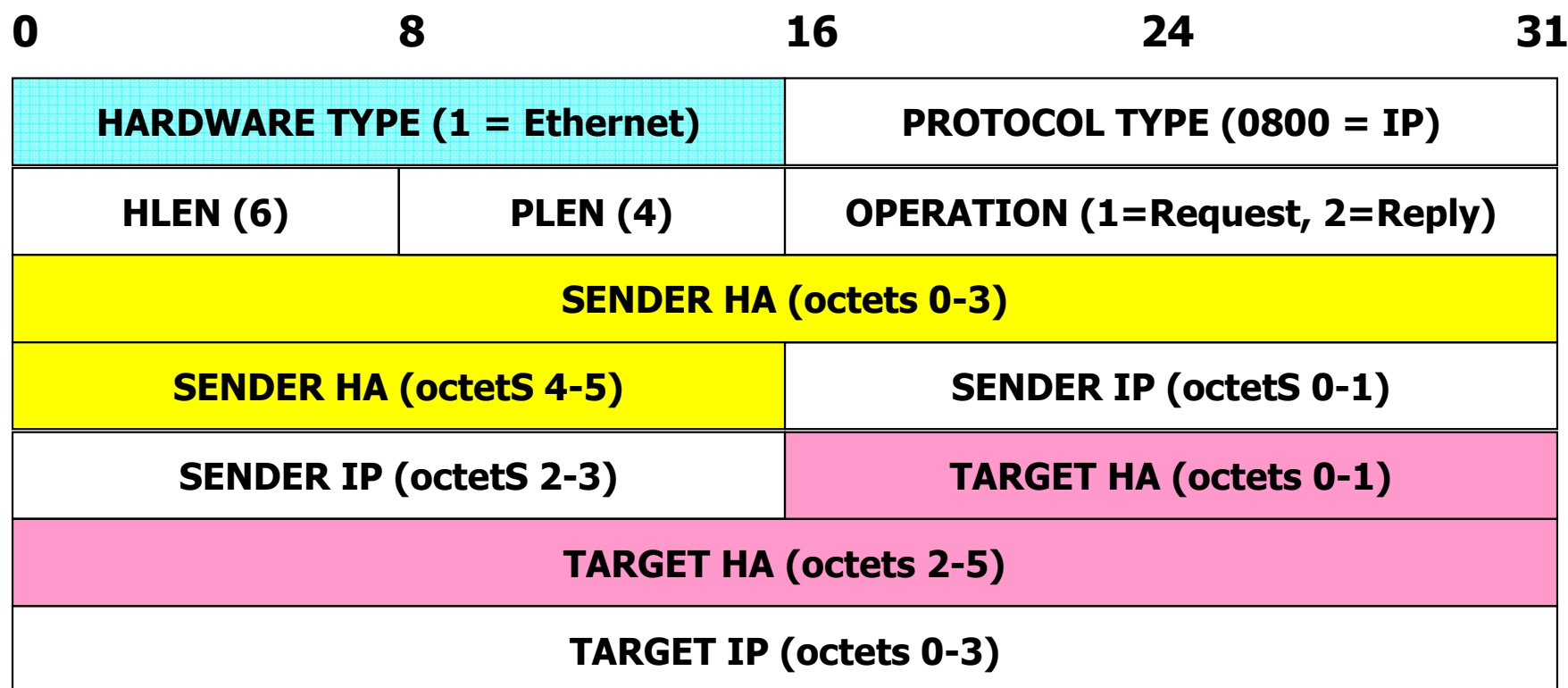
ARP
Request

HEY - Everyone please listen!
Will 140.113.1.5 please send me
his/her Ethernet address?



Hi Green! I'm 140.113.1.5, and
my Ethernet address is
00:0D:15:35:02:C3

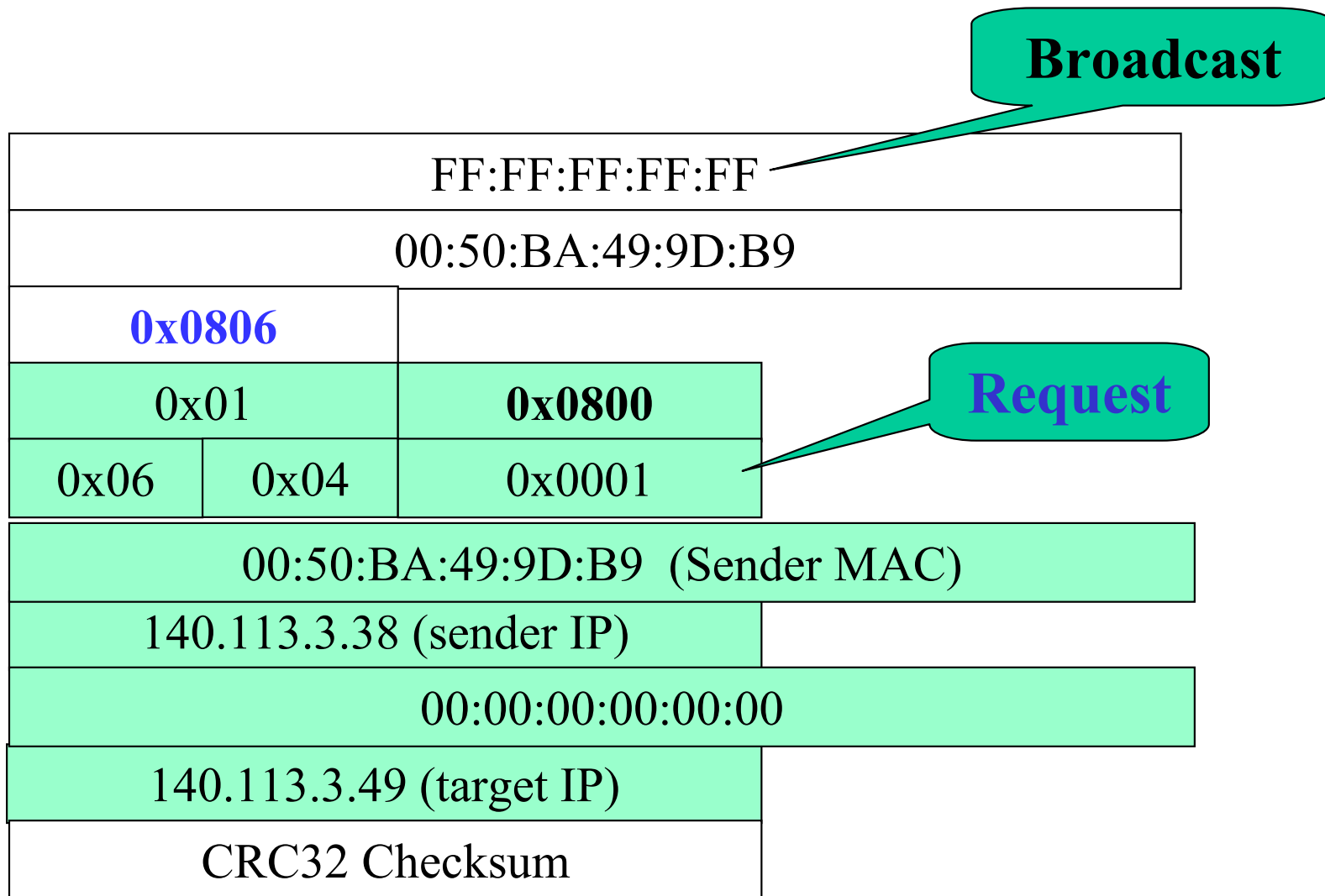
ARP Message Format



Ethernet frame type

Sample ARP Request Packet

ARP
Ethernet

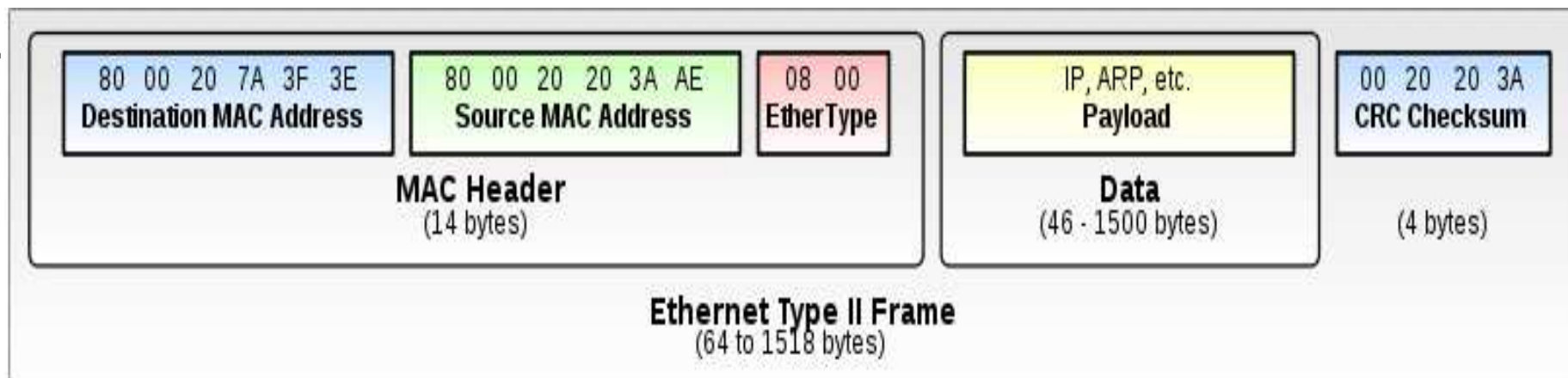


ARP Mechanism

- Each node maintains the ARP cache
 - It first looks in the cache to find entry first
 - if the entry is not used for a period (approximate 15 minutes), it is deleted
- Receive node can add a MAC address entry for source node in its own cache
- ARP traffic load
 - Hosts quickly add cache entries
 - What if all of hosts on a subnet are booted at the same time? → Flurry of ARP request and reply

ARP Spoofing

- to send fake, or "spoofed", ARP Reply messages to an Ethernet LAN
- also known as **ARP flooding**, **ARP poisoning** or **ARP Poison Routing (APR)**
- may allow an attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether



http://en.wikipedia.org/wiki/ARP_spoofing

RARP: Reverse ARP

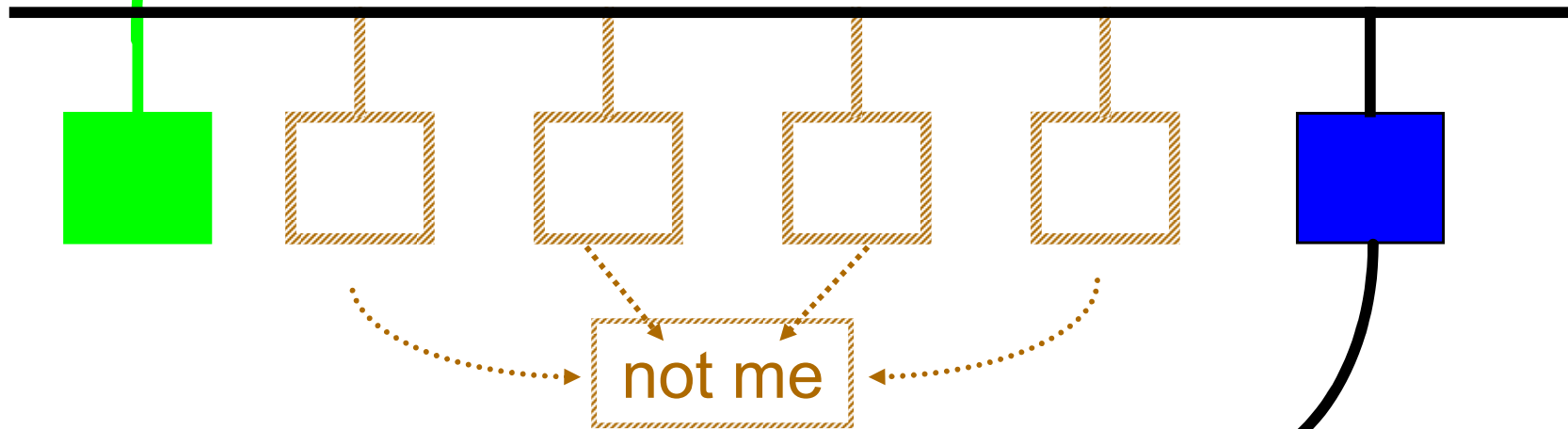
- RARP (RFC903): frame type = **0x0835**
 - For diskless system
- rarpd, /etc/ethers
- RARP server design
 - System dependent and complex
 - RARP servers as user processes
 - Must have some way of sending and receiving ethernet frames
 - Multiple RARP servers per network
 - RARP can not operate across router
 - Network traffic
 - Collision rate

RARP conversation

HEY - Everyone please listen!

**My Ethernet address is
00:00:66:17:01:75.**

Can anyone give me an IP address ?



DHCP

**Hi Green! Your IP address is
140.113.24.138.**

ICMP: Internet Control Message Protocol

- ICMP message format
 - 15 types and various codes for each type
- An ICMP error message always contains
 - IP header
 - the first 8 bytes of the IP datagram
- An ICMP error message is never generated in response to
 - An ICMP error message
 - A datagram destined to an IP **multicast/broadcast** message
 - A link-layer **broadcast** message
 - A fragment **other than the first**
 - A datagram whose source address does not define a single host

ICMP messages are carried in IP datagrams and are used to send ERROR and CONTROL messages.

ICMP (cont.)

- ICMP Types:
 - ICMP Echo Request (type 8)
 - ICMP Echo Reply (type 0)
 - ICMP Address Mask Request and Reply (type 17, 18)
 - Subnet mask
 - ICMP Timestamp Request and Reply (type 13, 14)
 - orig timestamp, rcv timestamp, xmit timestamp
 - Calculating the clock difference
 - ICMP Destination Unreachable (type 3, code 0~15)
 - Network unreachable (code 0)
 - Host unreachable (code 1)
 - Port unreachable (code 3)
 - Source route failed (code 5)

tracert (traceroute) (或也有系統用 tr)

The image shows two overlapping screenshots of a Windows command prompt window titled "cmd.exe (java-green-20)".

The left screenshot shows the help text for the `tracert` command:

```
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97      rhino.acme.com      # source server
#      38.25.63.10      x.acme.com         # x client host
127.0.0.1      localhost
140.113.1.1     a.b.c.d      hehehe
140.113.216.27  jctsay
^C
C:\WINDOWS\system32\drivers\etc>dir h*
磁碟區 C 中的磁碟是 IBM_PRELOAD
磁碟區序號:  FC62-AF9F
C:\WINDOWS\system32\drivers\etc>
2004/05/27 下午 03:42
1 個檔案
0 個目錄
317,300
C:\WINDOWS\system32\drivers\etc>
```

The right screenshot shows the output of the `tracert` command:

```
C:\WINDOWS\system32\drivers\etc>dir h*
磁碟區 C 中的磁碟是 IBM_PRELOAD
磁碟區序號:  FC62-AF9F
C:\WINDOWS\system32\drivers\etc 的目錄
2004/05/27 下午 03:42
1 個檔案
0 個目錄
828 hosts
828 位元組
317,300,736 位元組可用
C:\WINDOWS\system32\drivers\etc>tracert 140.113.1.1
Tracing route to a.b.c.d [140.113.1.1]
over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms   140.113.1.1
  1  2 ms    2 ms    2 ms   e3rtn-24.csie.nctu.edu.tw [140.113.24.254]
  2  2 ms    2 ms    2 ms   140.113.0.210
  3  26 ms   37 ms   57 ms   140.113.0.166
  4  153 ms  83 ms   65 ms   140.113.0.149
  5  97 ms   85 ms   49 ms   a.b.c.d [140.113.1.1]

Trace complete.
C:\WINDOWS\system32\drivers\etc>
```

利用封包中的 **TTL**

tracert 140.113.1.1

Public vs. Private IP (公共 IP 與私有 IP) 1/2

✓ 公共 IP (Public IP)

- 當我們要將網路連上 Internet 的時候，我們必須先註冊好 Net ID，如果該 ID 已經被使用了，您就必須選用另外的 ID 了。負責 Internet IP 註冊的機構叫做 InterNIC (Network Information Center)，他們的網路位址是 <http://www.internic.net>。不過，實際上的運作，一般機構或個人是不太可能直接從 InterNIC 上註冊 IP 的，而是經您的 ISP 分配下來。這些經過合法授權使用的 IP，我們稱之為 **公共 IP (Public IP)**。

✓ 私有 IP 位址 (Private IP address)

- 由於 Internet 的爆炸性成長，IP 的位址越來越少，而且在很多機構裡，也不是所有機器都有必要使用註冊的 IP 位址。於是，我們就在 A、B、C 這三個 class 裡面，各劃出一些位址範圍保留給私有位址所用，它們分別是：
 - **10.0.0.0 - 10.255.255.255 (Class A)**
 - **172.16.0.0 - 172.31.255.255 (Class B)**
 - **192.168.0.0 - 192.168.255.255 (Class C)**
- 這些無需註冊就能自由使用的 IP，我們稱之為 **私有 IP (Private IP)**。

Public vs. Private IP (公共 IP 與私有 IP) 2/2

- ✓ Private IP 之封包在網路上的限制
 - 10.0.0.0 - 10.255.255.255 (Class A)
 - 172.16.0.0 - 172.31.255.255 (Class B)
 - 192.168.0.0 - 192.168.255.255 (Class C)
 - 當您使用這些private位址的時候，當然是有所限制的：
 - 私有位址的路由資訊不能對外散播
 - 使用私有位址作為來源或目的位址的封包，不能透過 Internet 來轉送
 - 關於私有位址的參考紀錄，只能限於內部網路使用
- ✓ 正是由於這些限制，當我們使用這些私有位址來設定網路的時候，就無需擔心會和其它也使用相同位址的網路衝突。
- ✓ 那這些使用 private IP 的電腦如何與外界機器溝通？
 - NAT --- Network Address Translation

NAT ? 寬頻分享器?

IPv6 (IPng = 下一代 IPnext generation)

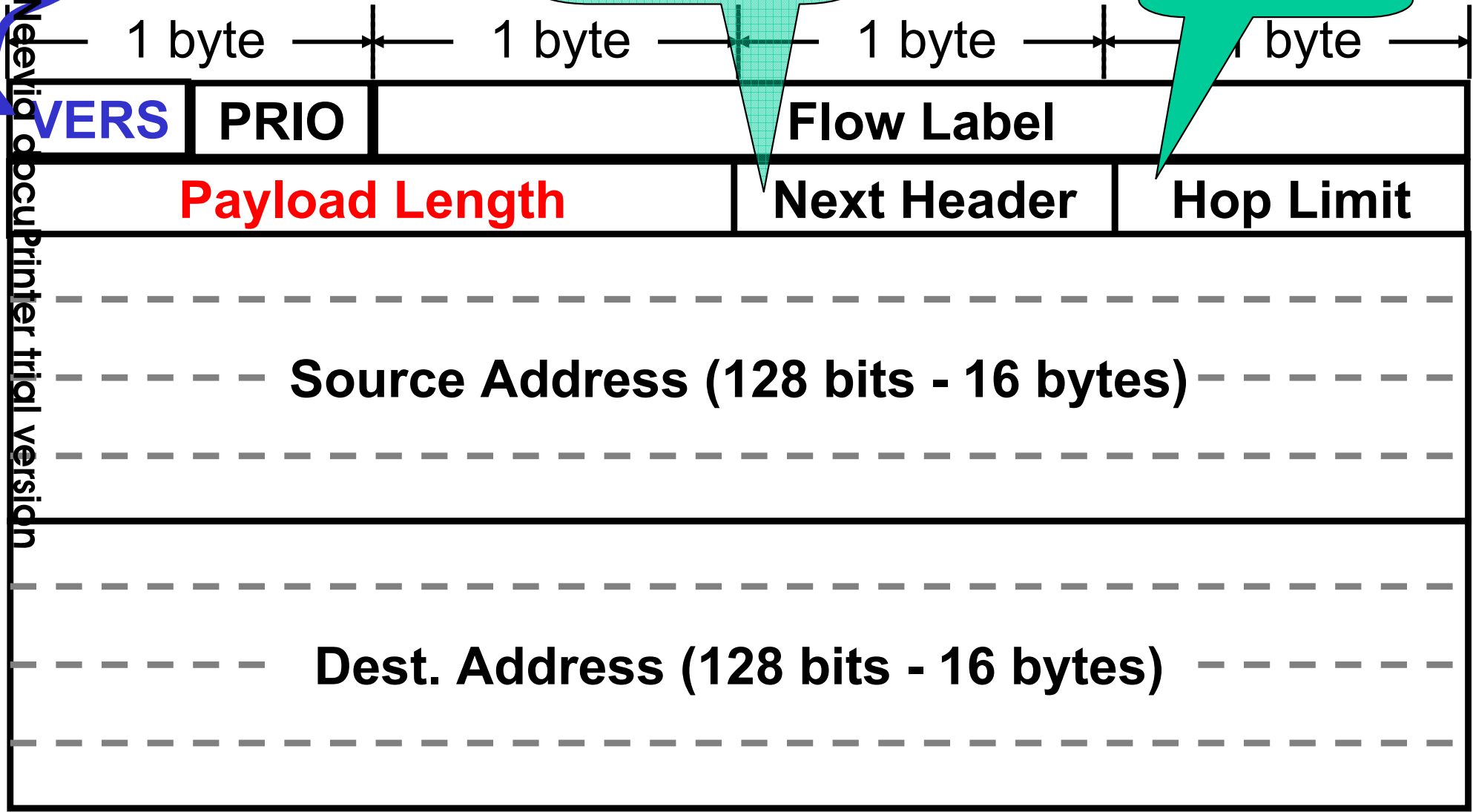
- 1992 年 6 月 IETF 發 啓 IPng 提 議 徵 文
- 1995 年 1 月 RFC 1752, “The Recommendation for the IPNext Generation Protocol”
- IPv6 實 驗 網 路(6Bone)
 - 爲 了 在 Internet 上 推 廣 IPv6 的 一 個 全 球 性 IPv6 測 試 平 臺
 - 1997 年 6 月 開 始 運 作

6 for IPv6

IPv6 Header

就是protocol

就是TTL



Determining the Application that Should Accept the Message

- Assign unique **port numbers** to various application units
- Require that an application sending a message append the appropriate port number to the message's address
- Some universally accepted **port** numbers
 - HTTP server: 80
 - FTP server: 21
 - Telnet server: 23

WAN

- Wide Area Network
- A large number (usually) of connected computers spreading across a wide area
- Connecting LANs (Local Area Network)
 - A LAN connects to a WAN via a router
- Irregular

Routing

- How to get the data to go where you want them to be?
 - Destination in this Subnet: broadcast the Ether frame
 - Destination in other Subnet: send it to Gateway

Router (路由器)

- Finding a route from the source to the destination

tracert

Hub, Switch, **Router**

Traceroute is a program that is available on many systems, and is similar to PING, except that traceroute provides more information than PING. Traceroute traces the path a packet takes to a destination, and is used to debug routing problems.

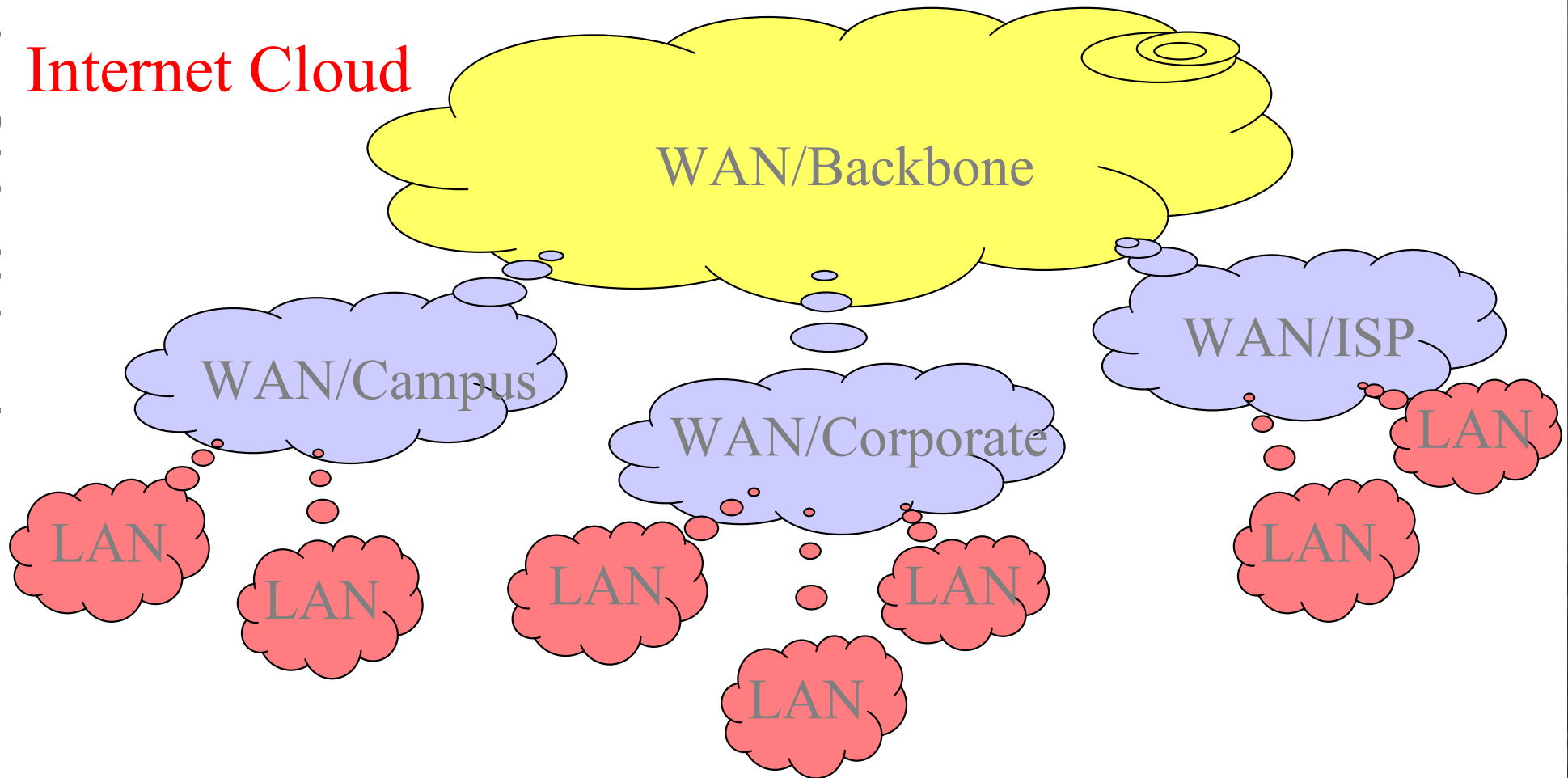
IP Routing (IP 封包繞送) protocols

- **Internet Protocol Routing**
- The class of protocols that handle routing problems
- Example of **Routing protocols**
 - RIP (IETF RFC 1058) Routing Information Protocol
 - **OSPF (IETF RFC 2328)** Open Shortest Path First
 - BGP (IETF RFC 1771) Border Gateway Protocol

Routing protocols vs. Routable protocols ?

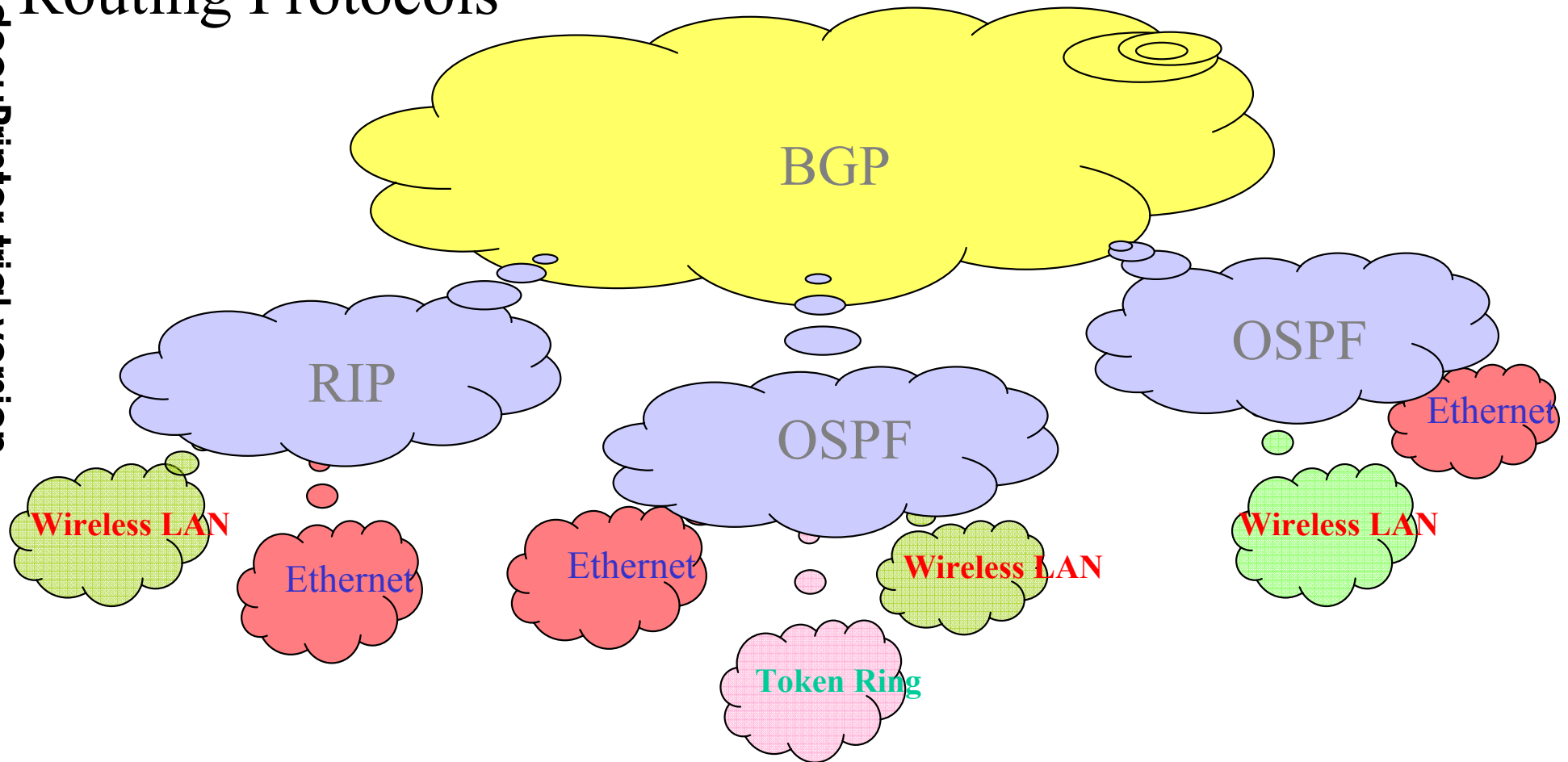
IP is a Routable protocol

Internet – Structural View



Internet - Protocol View

Routing Protocols

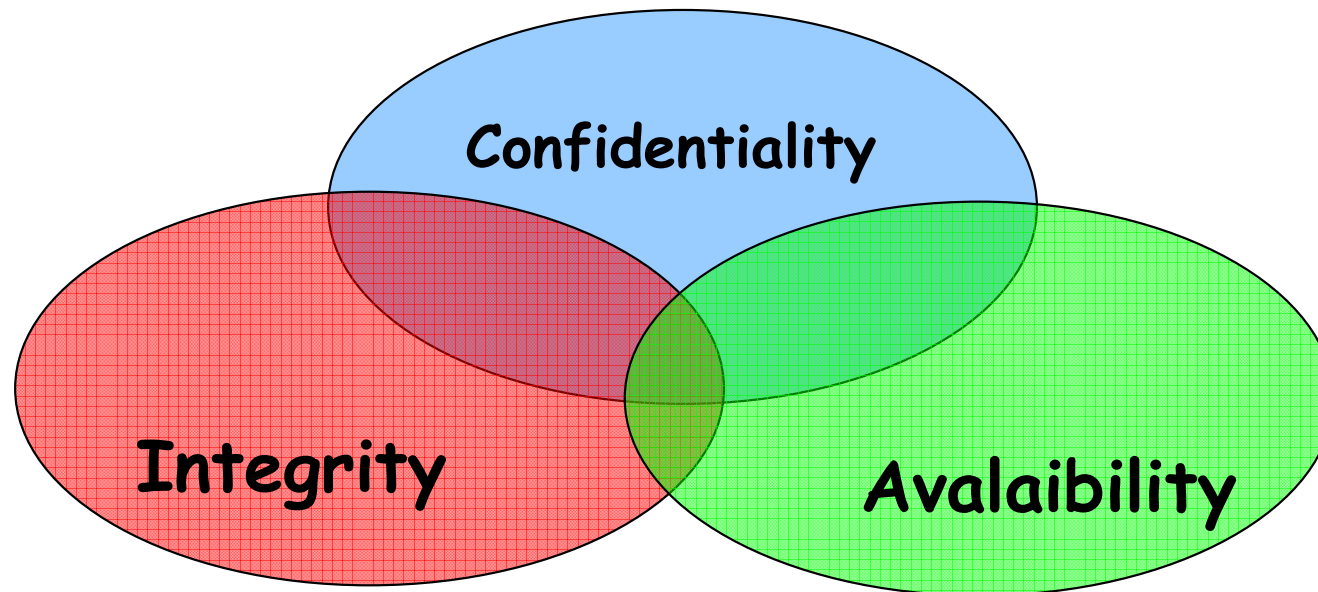


Agenda

- 4.1 Network Fundamentals
- 4.2 The Internet
- 4.3 The World Wide Web
- 4.4 Network Protocols
- 4.5 Network Security

Network security

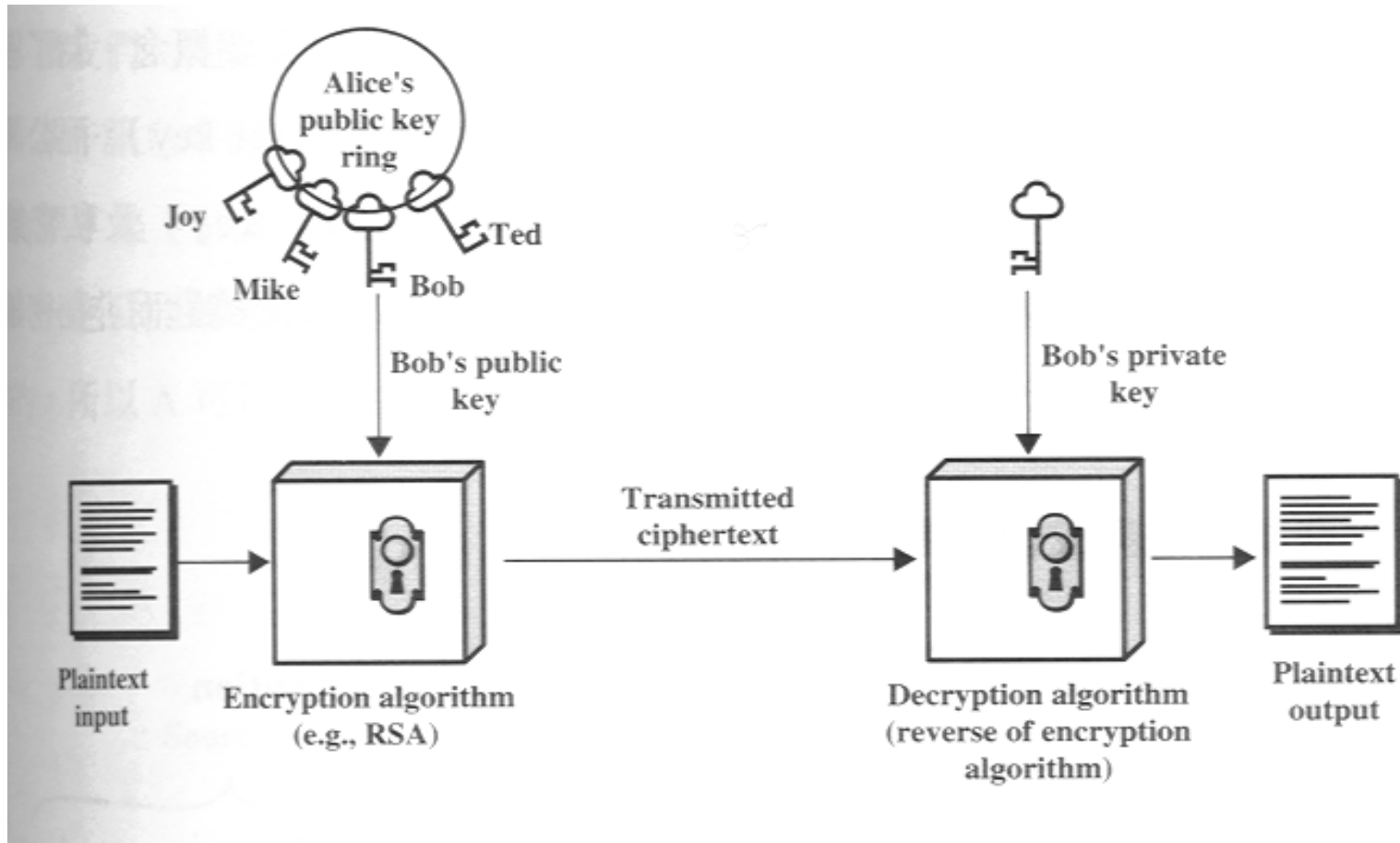
- Privacy of communication
 - Public-key encryption
- Integrity of machine exposed to internet
 - Attacks: viruses, worms, and intrusion
 - Defense: Anti-virus, Firewall, IDS/IPS



Public-Key Encryption (1/2)

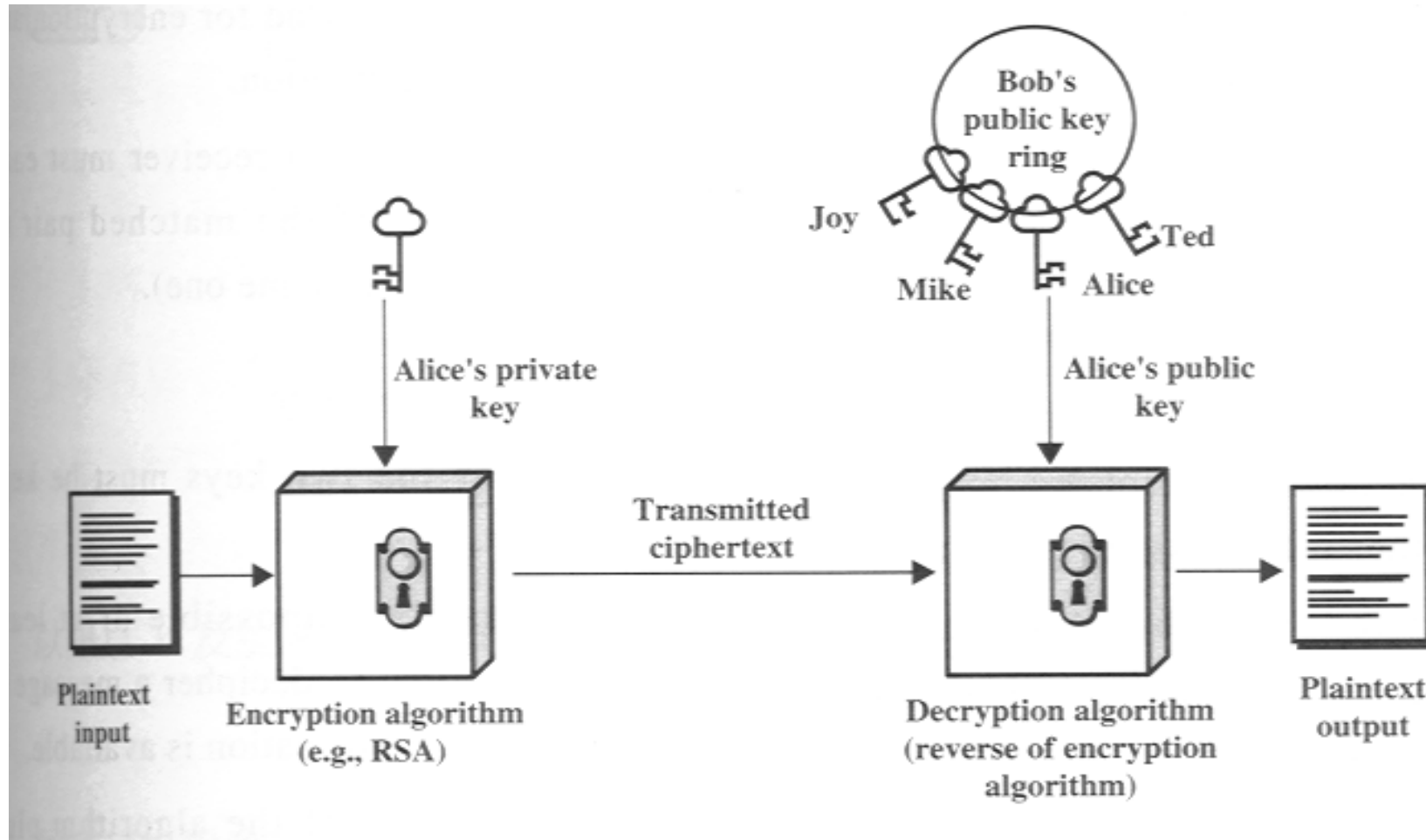
- Public key is used to encode messages and is known by all people authorized to generate messages
- Private key is required to decode messages and is known by only the person who is to receive messages

Public-Key Encryption (2/2)



Source: William Stallings

Digital Signature 數位簽章 for Authentication



Source: William Stallings

Public-Key Cryptographic Algorithms

- **RSA** and **Diffie-Hellman**
- **RSA** - Ron **R**ives, Adi **S**hamir and Len **A**dleman at MIT, in 1977.
 - RSA is a **block cipher**
 - The most widely implemented
- **Diffie-Hellman** in 1976
 - Exchange a secret key securely
 - Compute discrete logarithms

一次切取一區塊(例
64Bytes)來加解密

Block cipher vs. Stream cipher

The RSA Algorithm – Key Generation

1977

1. Select p, q p and q both prime
2. Calculate $n = p \times q$
3. Calculate $\Phi(n) = (p-1)(q-1)$
4. Select integer e $\gcd(\Phi(n), e) = 1; 1 < e < \Phi(n)$
5. Calculate d $d = e^{-1} \bmod \Phi(n)$
6. Public Key $KU = \{e, n\}$
7. Private key $KR = \{d, n\}$

Example of RSA Algorithm (1/2)

1. Select p, q $p = 7, q = 17$
2. Calculate $n = p \times q = 7 \times 17 = 119$
3. Calculate $\Phi(n) = (p - 1)(q - 1) = 96$
4. Select integer $e = 5$ $\gcd(\Phi(n), e) = 1; 1 < e < \Phi(n)$
5. Calculate $d = 77$ $d = e^{-1} \bmod \Phi(n)$
6. Public Key $KU = \{e, n\} = \{5, 119\}$
7. Private key $KR = \{d, n\} = \{77, 119\}$

因為 $77 \times 5 = 385 = 4 \times 96 + 1$

Example of RSA Algorithm (2/2)

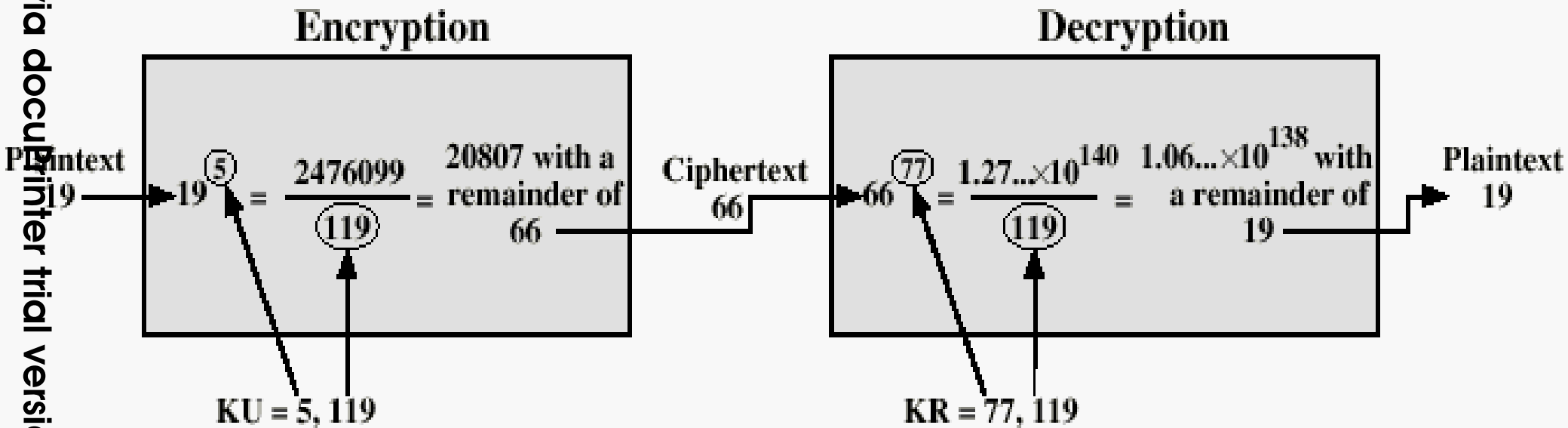
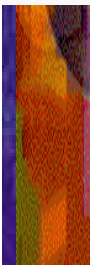


Figure 3.9 Example of RSA Algorithm

Diffie-Hellman Key Exchange

1976

α 和 q 是雙方先約好或由一方送給另一方(A送給B)

User A

Generate
random $X_A < q$;
Calculate
 $Y_A = \alpha^{X_A} \bmod q$

Calculate
 $K = (Y_B)^{X_A} \bmod q$

Y_A

Y_B

User B

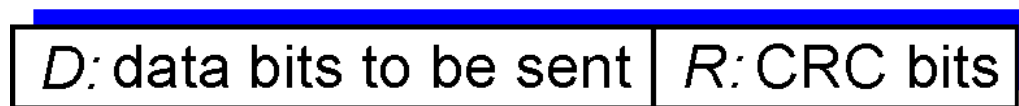
Generate
random $X_B < q$;
Calculate
 $Y_B = \alpha^{X_B} \bmod q$;
Calculate
 $K = (Y_A)^{X_B} \bmod q$

雙方算出的 K 會相等

Checksumming: Cyclic Redundancy Check(CRC)

- view data bits, **D**, as a binary number
- choose $r+1$ bit pattern (generator), **G**
- goal: choose r CRC bits, **R**, such that
 - $\langle D, R \rangle$ exactly divisible by G (modulo 2)
 - receiver knows G , divides $\langle D, R \rangle$ by G . If non-zero remainder: error detected!
 - can detect all burst errors less than $r+1$ bits
- widely used in practice (ATM, HDCL)

← d bits → ← r bits →



*bit
pattern*

$$D * 2^r \text{ XOR } R$$

*mathematical
formula*

CRC Example

Want:

$$D \cdot 2^r \text{ XOR } R = nG$$

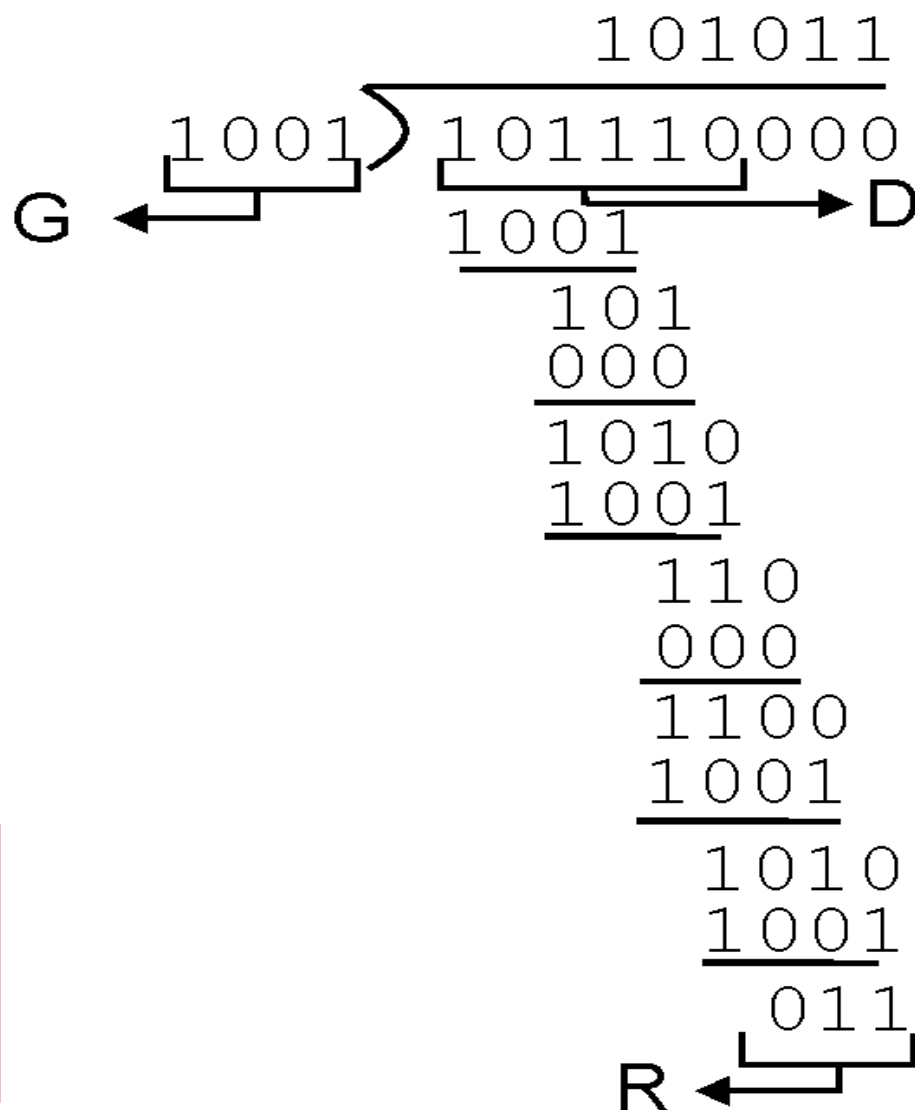
equivalently:

$$D \cdot 2^r = nG \text{ XOR } R$$

equivalently:

if we divide $D \cdot 2^r$ by
G, want remainder
R

$$R = \text{remainder} \left[\frac{D \cdot 2^r}{G} \right]$$



Security Attacks

- **Interruption:** This is an attack on availability
- **Interception:** This is an attack on confidentiality
- **Modification:** This is an attack on integrity
- **Fabrication:** This is an attack on authenticity

Denial of Service (DoS) 簡介

- DoS：阻絕服務攻擊 --- 讓大家都不能用!
- 攻擊對象：
連上Internet 的網路和裝置
- 目的：
讓被攻擊的網路伺服器因忙碌著回應不合法的存取要求或拒絕合法使用者的存取，導致：
 - ➔ 伺服器無法正常運作
 - ➔ 使用者無法再存取網路資源

DoS 攻擊型態

- 皆是利用 TCP/IP 相關的漏洞，讓網路充滿了垃圾封包，攻擊型態包含：
 - 利用主機系統 TCP/IP 程式漏洞，例如：
 - Ping of Death
 - Teardrop
 - 利用 TCP/IP 協定規格本身的漏洞，例如：
 - SYN Flood
 - LAND
 - Smurf 攻擊

DoS攻擊型態 – Ping of Death

Ping 呼伊死

- 方式：
 - 利用 "ping" 這支工具程式來產生超過 IP 協定所能允許的最大封包 (>65535 bytes based on RFC-791)。
 - 當這封包送到沒有檢查功能的系統，則可能發生系統當機
 - 或者是因為過長的封包會被切成可接受長度的片段 (fragments) 再逐一傳送至遠端電腦，再將這些片段組合還原成完整封包，但此舉有時會造成對方電腦 Buffer overflow 而當機或重開。

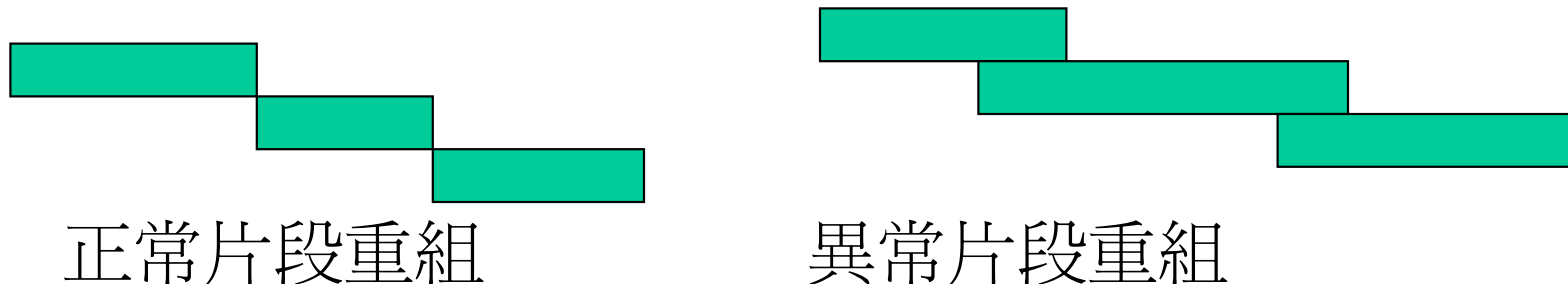
DoS攻擊型態 – Land attack

- 原理：
 - 傳輸層在 three way handshake 過程中，每一步都有一組：
(**來源**位址，**來源埠號**，目的位址，目的埠號)
 - 來源位址與目的位址可以相同
 - 當來源位址與目的位址不同，來源埠號與目的埠號相同也是可以
 - **當來源位址與目的位址相同，同時來源埠號與目的埠號也相同 ???**
- 攻擊方式：
 - 送出一連串偽造的封包，使得目的位址與來源位址都是受攻擊系統的位址，並且目的埠號與來源埠號也相同。
- Ex : land.c

DoS攻擊型態 – Teardrop

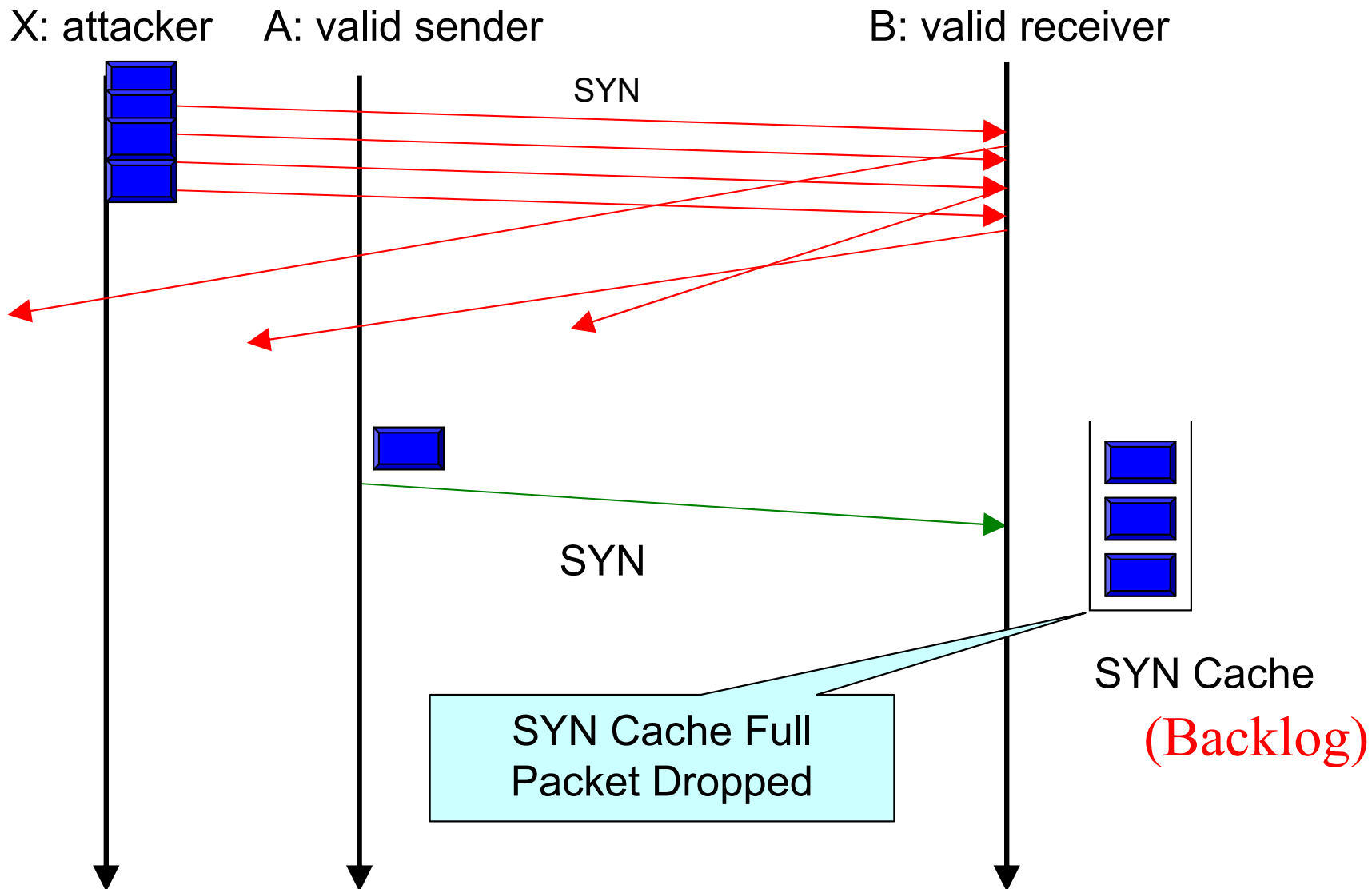
利用 IP Fragmentation 功能

- 攻擊方式：
 - 利用IP封包重組的漏洞
 - 送出一對經過特別設計封包片段，使得這一對封包片段在目標電腦重新組合後，造成與原來資料不合的封包。
- 原理：
 - 網路層(Network layer)的IP(Internet Protocol)主要負責路由與資料包分割 (fragmentation)及重組(re-assembly)。



Example: teardrop.c

TCP/IP: SYN Flood Attack



Reset	Fin	Syn	Ack	Comment
0	0	0	1	OK
0	0	1	0	1st Packet
0	0	1	1	2nd Packet
0	1	0	0	Needs Ack
0	1	0	1	OK
0	1	1	0	Illegal
0	1	1	1	Illegal
1	0	0	0	Needs Ack
1	0	0	1	OK
1	0	1	0	Illegal
1	0	1	1	Illegal
1	1	0	0	Illegal
1	1	0	1	Illegal
1	1	1	0	Illegal
1	1	1	1	Illegal

Illegal flag combinations are used to determine Operating System

Malicious codes (Malware)

- Undesired code that might cause damage to your computer system
 - Virus
 - Worm
 - Trojan horse

<http://en.wikipedia.org/wiki/Malware>

http://en.wikipedia.org/wiki/Buffer_overflow

http://en.wikipedia.org/wiki/Stack_buffer_overflow

Viruses

- Program segment that attaches itself to other programs in the computer system
- When executed the virus may perform malicious acts that are readily noticeable or merely search for other programs to which it can attach copies of itself
- If an infected program is transferred to a new machine, the virus will begin to infect programs on the new machine as soon as it is executed

http://en.wikipedia.org/wiki/Computer_virus

[http://en.wikipedia.org/wiki/CIH_\(computer_virus\)](http://en.wikipedia.org/wiki/CIH_(computer_virus))

參考: 趨勢科技網站<http://www.trend.com.tw/>

Worms

http://en.wikipedia.org/wiki/Computer_worm

- Autonomous program that **transfers itself through a network**, taking up residence in the machines and forwarding copies of itself through the network
- Can be designed merely to replicate themselves or to perform additional vandalism
- 蠕蟲
電腦蠕蟲病毒是一種惡意程式（或一組程式），可將本身的功能或程式碼透過網路散播到其他電腦。

Morris worm: 1988/11/02 by Robert Morris@Cornell Univ.

CodeRed : 2001/07/13 ; Nimda : 2001/09/18

[http://en.wikipedia.org/wiki/Code_Red_\(computer_worm\)](http://en.wikipedia.org/wiki/Code_Red_(computer_worm))

Trojan Horse

- Propagation
 - A program that **does not replicate**
- Spreading model
 - Someone **emails** a Trojan Horse to you
 - You copy a program with embedded Trojan Horse
 - Visit a Web site contains Trojan Horse

[http://en.wikipedia.org/wiki/Trojan_horse_\(computing\)](http://en.wikipedia.org/wiki/Trojan_horse_(computing))

http://en.wikipedia.org/wiki/Trojan_Horse

Distinction between them

- **Virus**
 - Fast spreading within a system
- **Worm**
 - Fast spreading across systems
- **Trojan horse vs. the other two**
 - **No self-replication**

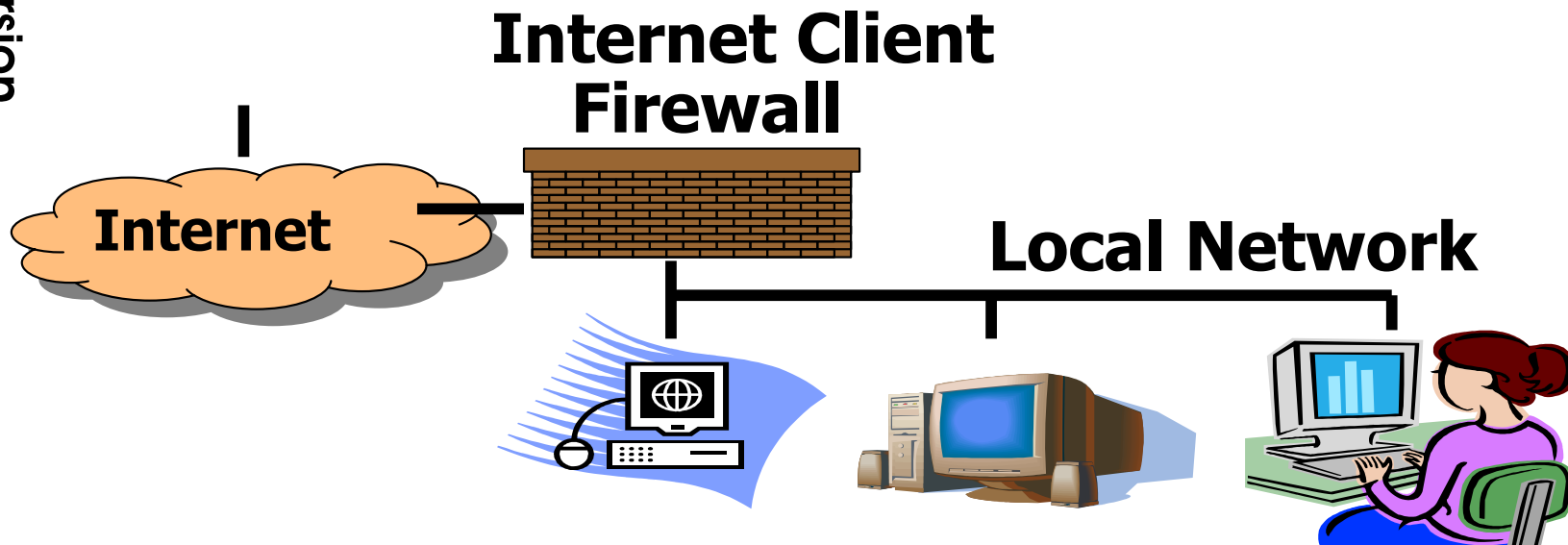
http://en.wikipedia.org/wiki/Computer_virus

http://en.wikipedia.org/wiki/Computer_worm

[http://en.wikipedia.org/wiki/Trojan_horse_\(computing\)](http://en.wikipedia.org/wiki/Trojan_horse_(computing))

Firewalls

- Filter the traffic entering or passing through a machine
- Examples
 - Scan all incoming traffic and reject messages containing certain words
 - Reject all traffic from or to a given **port** number
 - Filter out all messages from certain **IP** addresses
- Placed on **gateway** or individual machines



SSH (usually use TCP port 22)

- Designed to replace rlogin, rdist, rsh, rcp
- Custom designed protocol but includes encryption
 - RFC 4250~4256, 4335, 4344, 4345, 4419, 4432, 4716
- Can safely tunnel X11 or arbitrary TCP ports
- Commercial and Open versions
 - OpenSSH on most Linux
 - Putty is a free windows client
 - Pietty is a modified version of Putty
 - Can tunnel other protocols through a firewall

SSH : Secured **S**hell

http://en.wikipedia.org/wiki/Secure_Shell

Thank You!

CHAPTER 4

Networking and the Internet

Part B



謝謝捧場

tsaiwn@csie.nctu.edu.tw

蔡文能