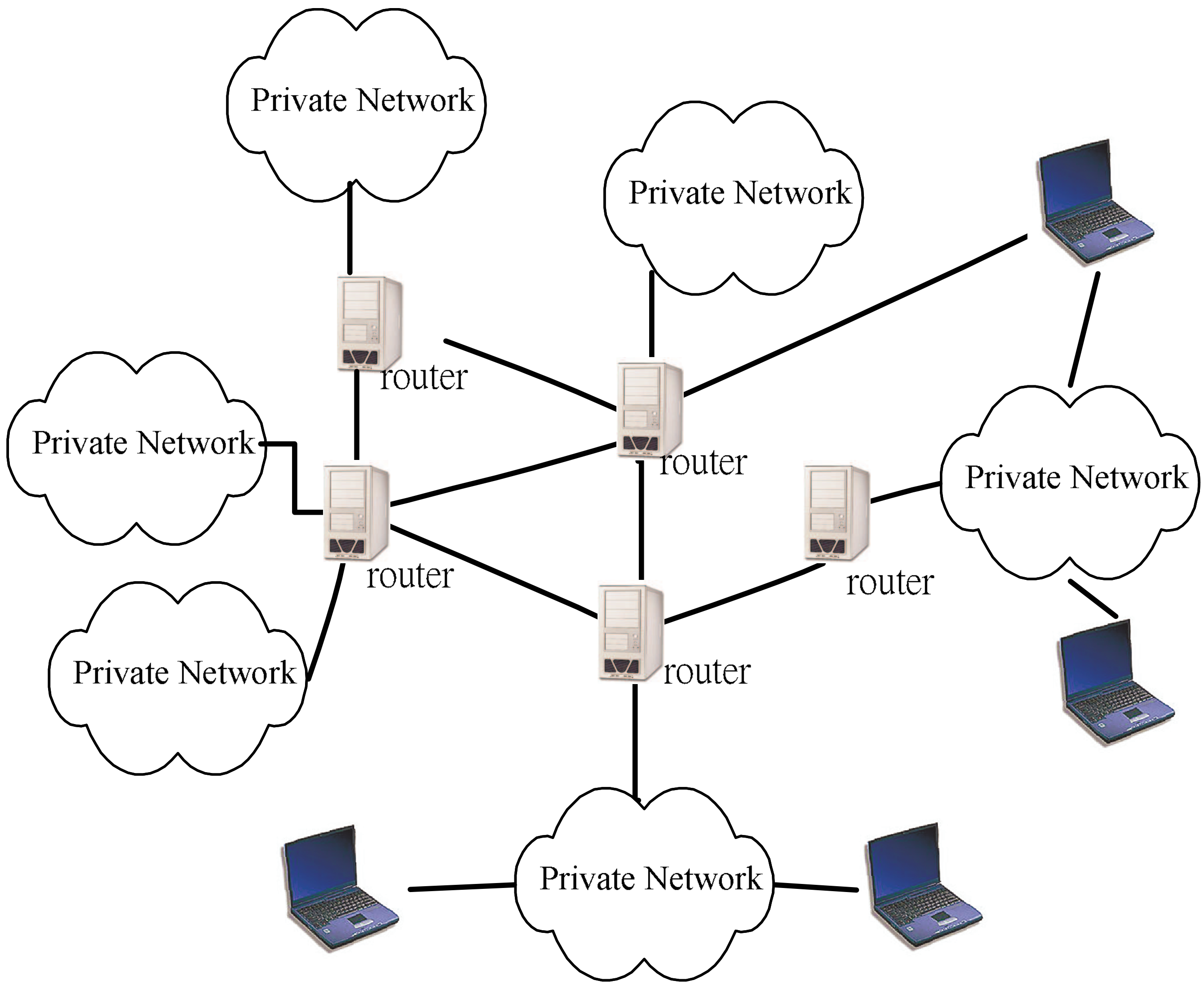
Transporting Voice by Using IP

Internet Overview

- A collection of networks
  - The private networks
    - LANs, WANs
    - Institutions, corporations, business and government
    - May use various communication protocols
  - The public networks
    - ISP: Internet Service Providers
    - Using Internet Protocol
  - To connect to the Internet
    - Using IP

Interconnecting Networks

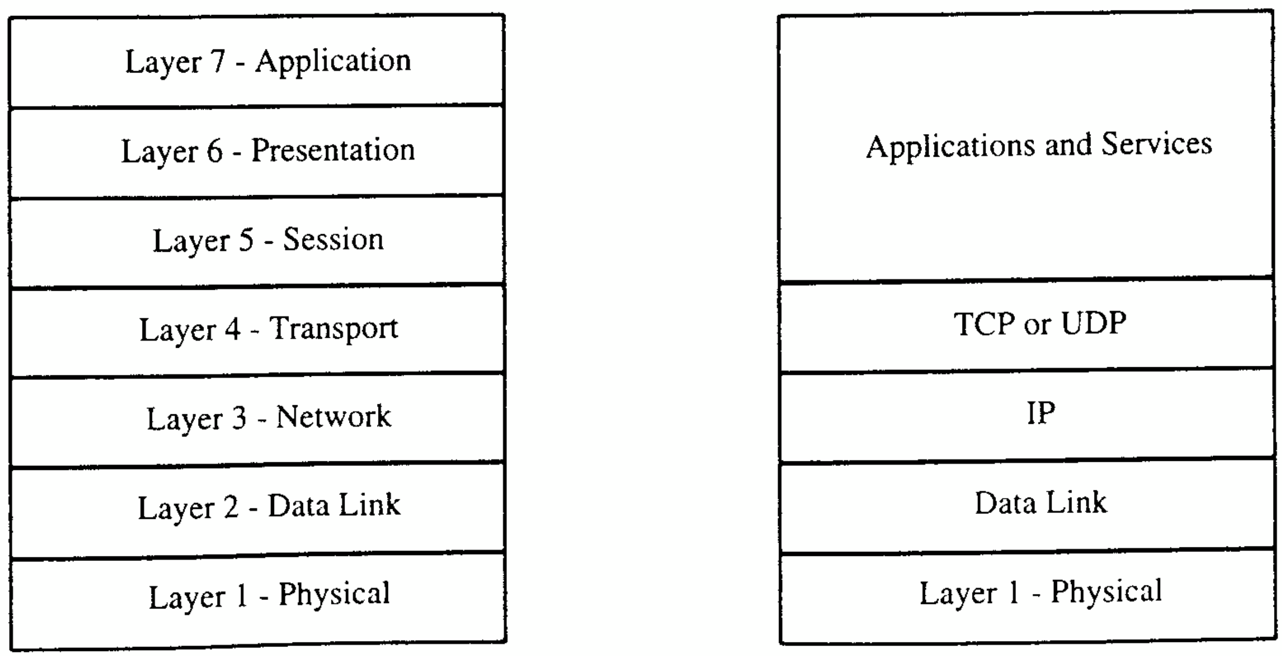


Overview of the IP Protocol Suite

- IP
  - A routing protocol for the passing of data packets
  - Must work in cooperation with higher layer protocols and lower-layer transmission systems
- The OSI seven-layer model
  - The top layer: information to be passed to the other side
  - The information must be
    - Packaged appropriately
    - Routed correctly
    - And it must traverse some physical medium

The IP suite and the OSI stack

- TCP
  - Reliable, error-free, in-sequence delivery
- UDP
  - No sequencing, no retransmission



The Internet Standards Documents

- RFC
  - "Request for Comments" document series
  - Began in 1969 as part of ARPANET project
  - An RFC number is given for each document
    - ftp://ftp.NSYSU.edu.tw/RFC/rfc2026.txt
- IANA
  - The Internet Assigned Numbers Authority
    - Publishes Technical Standards and Port Numbers that are developed by IETF RFC documents
    - In the past, these numbers were documented through the RFC document series, the last of these documents was RFC 1700, which is now outdated.
    - http://www.iana.org/assignments/port-numbers

Organizations Developing Internet Standards

- IETF
  - The Internet Engineering Task Force
  - Comprising a huge number of volunteers
    - Equipment vendors, network operators, research institutions etc.
  - Developing Internet standards
  - Detailed technical work is discussed and debated in open meetings and/or public electronic mailing lists
  - Areas
    - Routing, Security, Transport, Applications
  - Working groups
    - megaco, iptel, sip, sigtran, enum

Organizations Developing Internet Standards

- IESG
  - The Internet Engineering Steering Group
  - A group comprised of the IETF Area Directors and the IETF Chair.
  - Managing the IETF's activities
  - The standards approval board for the IETF.
- IAB
  - The Internet Architecture Board
  - Should the complainant not be satisfied with the outcome of the IESG review, an appeal may be lodged to the IAB.
  - IAB may direct that an IESG decision be annulled.

The Internet Standards Process

- RFC 2026 “The Internet Standards Process”, October 1996
  - Internet Draft
  - RFC Proposed Standard
  - RFC Draft Standard
  - RFC Internet Standard
- First, Internet Draft
  - The early version of spec.
  - Can be updated, replaced, or made obsolete by another document at any time
  - IETF’s Internet Drafts directory
  - Referenced as “Working in Progress”
  - Six-month life-time

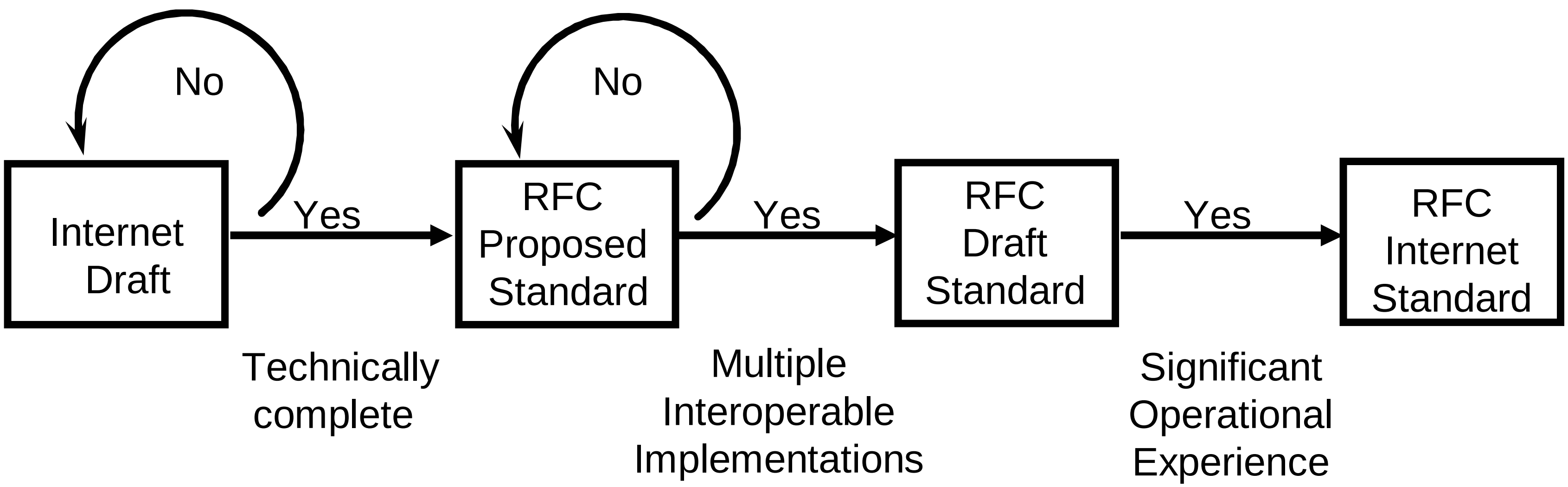
The Internet Standards Process

- Proposed standard
  - A stable, complete, and well-understood spec.
  - A specific action by the IESG is required to move a specification onto the standards track at the "Proposed Standard“ level.
- Draft standard
  - At least two independently successful implementations from different code bases have been developed
  - Interoperability operational experience is demonstrated
  - A major advance in status, indicating a strong belief that the specification is mature and will be useful.

The Internet Standards Process

- Internet Standard
  - The IESG is satisfied
  - The spec. is stable and mature
  - Significant operational experience
  - A standard (STD) number
- Not all RFCs are standards
  - Some document Best Current Practices (BCP subseries)
    - Processes, policies, or operational considerations
    - For example, RFC 1918 - Address Allocation for Private Internets (BCP 5)
      - 10.0.0.0/8 (a single class A network)
      - 172.16.0.0/12 (16 contiguous class B networks)
      - 192.168.0.0/16 (256 contiguous class C networks)
  - Others are known as applicability statements
    - How a spec. be used to achieve a particular goal, or different specs work together

The Internet Standards Process



Exercise 1

- What is the newest RFC document in
  - ftp.NCNU.edu.tw
  - ftp.NCHU.edu.tw
  - ftp.NCTU.edu.tw
  - ftp.IETF.org
- What is the Internet Draft with largest “draft number” you can find?
- What is the status of the following protocol
  - POP3
  - DNS
  - DHCP

Exercise 1 (cont.)

- Find an RFC document in each of the following category:
  - Obsoleted standard
  - Poetry
  - Experimental
  - History
  - Process documents

- Email your homework to TA (voip-ta@voip.edu.tw) by October 10th.
  - Subject of email: [VoIP HW1] 9232xxxx
  - Prepare your homework in a plaintext mail instead of attaching an MS-Word document.

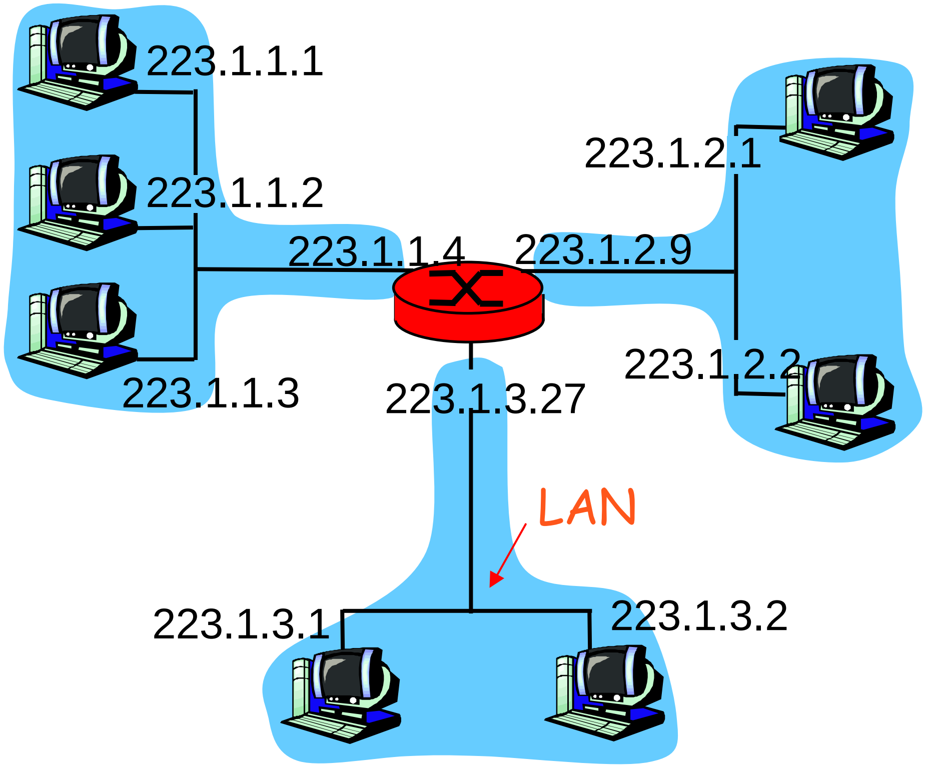
IP

- RFC 791
  - Amendments: RFCs 950, 919, and 920
  - Requirements for Internet hosts: RFCs 1122, 1123
  - Requirements for IP routers: RFC 1812
  - IP datagram
    - Data packet with an IP header
  - Best-effort protocol
    - No guarantee that a given packet will be delivered

IP Addressing

- IP address:
  - network part (high order bits)
  - host part (low order bits)
- *What's a network ?*

  (from IP address perspective)
  - device interfaces with same network part of IP address
  - can physically reach each other without intervening router

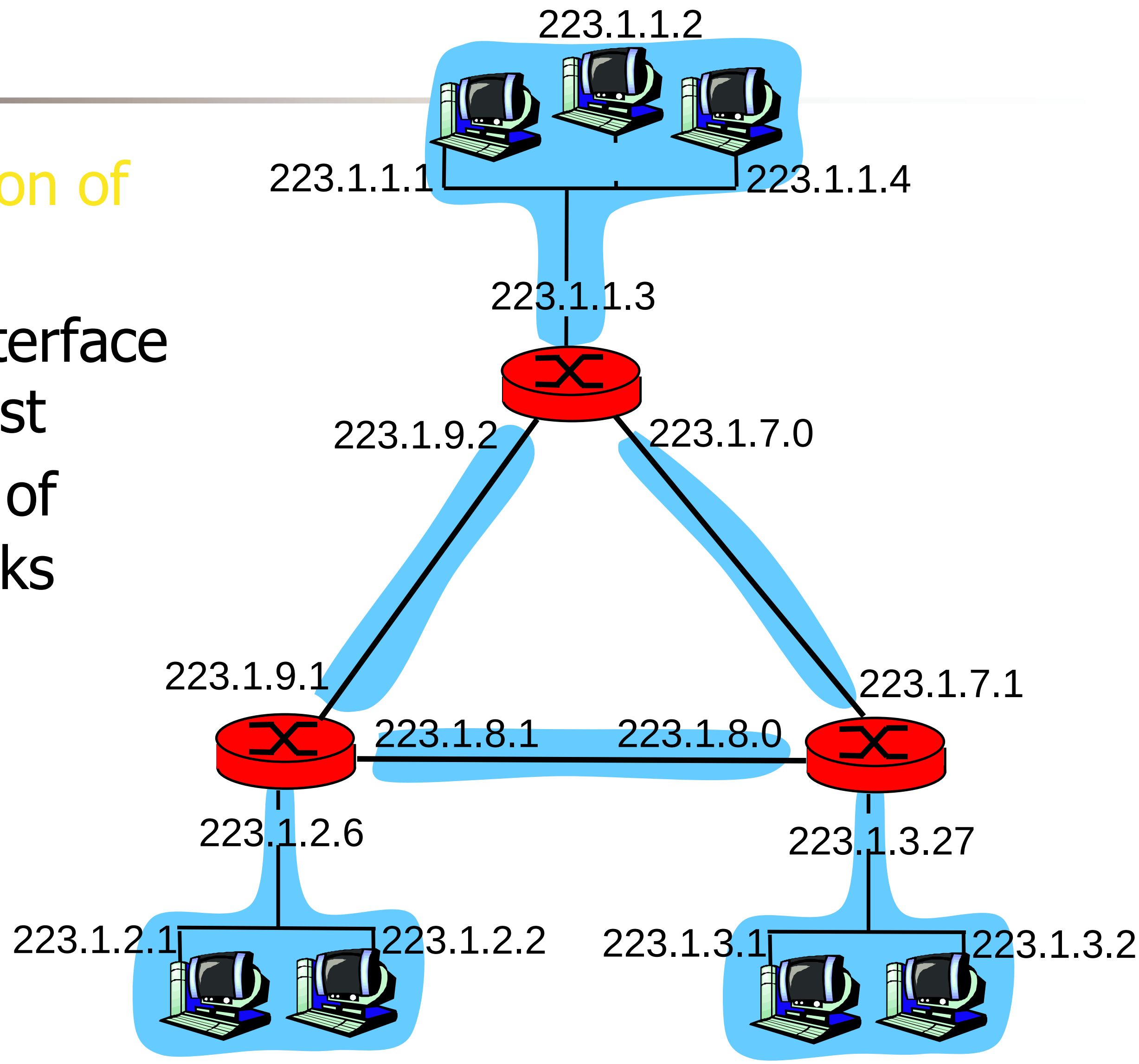


This network consists of 3 IP subnets (for IP addresses starting with 223, first 24 bits are network ids)

Routers

What is the function of routers?

- Detach each interface from router, host
- Create "islands of isolated networks



Interconnected system consisting of six networks

IP Routing

- Based on the destination address in the IP header
- Routers
  - Can contain a range of different interfaces
  - Determine the best outgoing interface for a given IP datagram
  - Routing table
    - Destination
    - IP route mask
      - For example, any address starting with 182.16.16 should be routed on interface A. (IP route mask 255.255.255.0)
      - Longest match

Sending a datagram from source to dest.

(In different subnets)

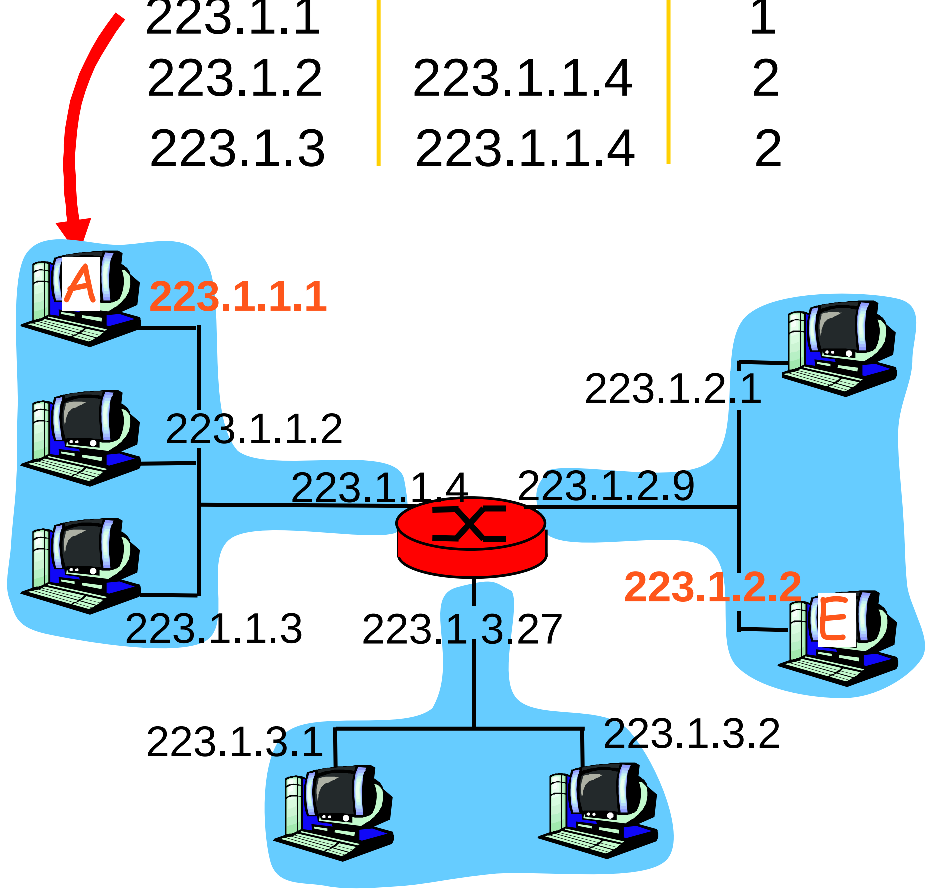
misc fields	223.1.1.1	223.1.2.2	data

forwarding table in A

Dest. Net.	next router	Nhops
223.1.1		1
223.1.2	223.1.1.4	2
223.1.3	223.1.1.4	2

Starting at A, dest. E:

- 1. use "Netmask" to look up network address of E in forwarding table
- 2. E on *different* network
  - A, E not directly attached
- 3. routing table: next hop router to E is 223.1.1.4
- 4. link layer sends datagram to router 223.1.1.4 inside link-layer frame
- 5. datagram arrives at 223.1.1.4
- continued…..



Sending a datagram from source to dest.

(In different subnets)

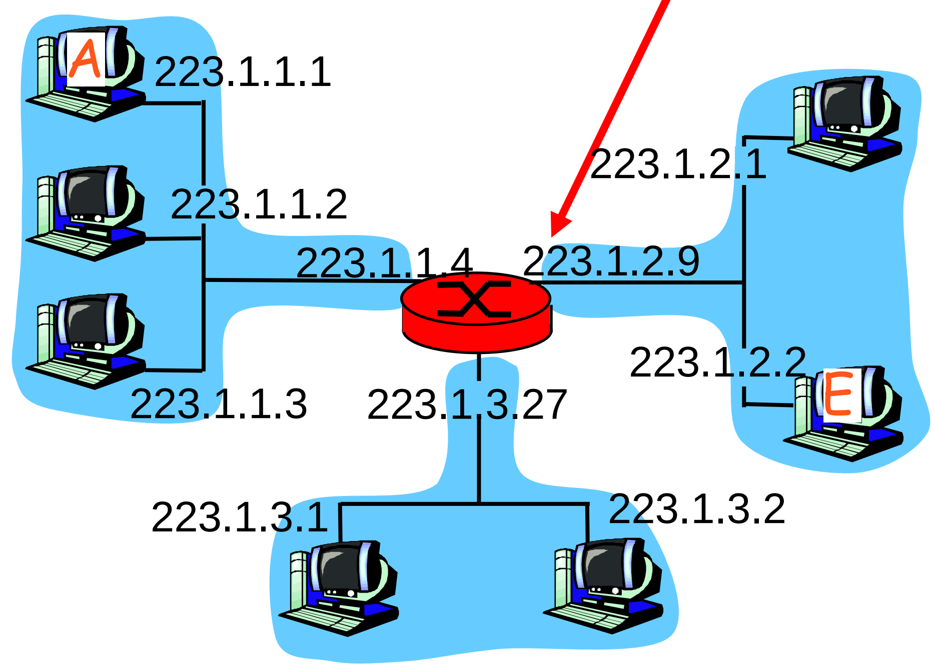
misc fields	223.1.1.1	223.1.2.2	data

Arriving at 223.1.1.4, destined for 223.1.2.2

- 6. use "Netmask" to look up network address of E in router's forwarding table
- 7. E on *same* network as router's interface 223.1.2.9
  - router, E directly attached
- 8. link layer sends datagram to 223.1.2.2 inside link-layer frame via interface 223.1.2.9
- 9. datagram arrives at 223.1.2.2!!! (hooray!)

forwarding table in router

Dest. Net	router	Nhops	interface
223.1.1	-	1	223.1.1.4
223.1.2	-	1	223.1.2.9
223.1.3	-	1	223.1.3.27



Populating Routing Tables

- Issues
  - The correct information in the first place
  - Keep the information up-to-date in a dynamic environment
  - The best path?
    - See Also “BGP flapping”
- Protocols
  - RIP (Routing Information Protocol) – RFC 1058
  - OSPF (Open Short Path First) – RFC 2328
    - 1131 - 1247 - 1583 - 2178 - 2328
  - BGP (Border Gateway Protocol) – RFC 1771

IP Header

- Source and Destination IP Addresses
- Protocol
  - The higher-layer protocol
  - TCP (6); UDP (17)

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version				Header Length				Type of Service								Total Length															
Identification																Flags			Fragment Offset												
Time to Live								Protocol								Header Checksum															
Source IP Address																															
Destination IP Address																															
Options																															
Data																															

Reference: RFC 760, http://www.faqs.org/rfcs/rfc760.html

UDP (User Datagram Protocol)

- UDP 特性
  - 記錄連接埠資訊, 達到 multiplexing 功能
  - 利用IP提供非連接式 (Connectionless)，且不可靠的傳送特性
    - 不要求對方回應，故傳輸速度較快
- 使用 UDP 的考量
  - 降低對電腦資源的需求
  - 應用程式本身已提供資料完整性的檢查機制
  - 使用多點傳送 (Multicast) 或廣播傳送 (Broadcast) 的傳送方式時
  - Real-time

連接埠

- 什麼是連接埠 (Port)？
- 連接埠編號的原則
  - Well Known Ports: 0 ~ 1023
    - 公認的port, 保留給常用的應用程式
  - Registered Ports: 1024 ~ 49151
    - 使用者應用程式可使用
  - Dynamic and/or Private Ports: 49152 ~ 65535

Reference: http://www.iana.org/assignments/port-numbers

常用的連接埠

- 使用自訂的伺服器連接埠編號。

Protocol	Port #	Application
UDP	53	DNS
UDP	67	BOOTP server
UDP	68	BOOTP client
UDP	520	RIP
TCP	20	FTP data
TCP	21	FTP Control
TCP	23	Telnet
TCP	25	SMTP
TCP	80	HTTP
TCP	119	NNTP

Client may also need a well-known port

Server may need more than one port

UDP 封包簡介

- UDP 表頭：
  - 記錄來源與目的端應用程式所用的連接埠編號。
- UDP 資料：
  - 載送上層協定 (Application Layer) 的資訊。
- UDP 封包結構

UDP表頭	UDP資料

Reference: RFC 768, http://www.faqs.org/rfcs/rfc768.html

UDP 表頭

- UDP 表頭(UDP Header) 結構

來源連接埠編號 (16 Bits)	目的連接埠編號 (16 Bits)	封包長度 (16 Bits)	錯誤檢查碼 (16 Bits)

- 來源連接埠編號 (Source Port)
  - 記錄來源端應用程式所用的連接埠編號。
- 目的連接埠編號 (Destination Port)
  - 記錄目的端應用程式所用的連接埠編號。
- 長度 (Length)
  - 記錄 UDP 封包的總長度。
- 錯誤檢查碼 (Checksum)
  - 記錄 UDP 封包的錯誤檢查碼。

錯誤檢查碼計算方式

- 計算錯誤檢查碼時, 會產生 *Pseudo Header*
  - 來源位址: IP表頭中來源端的 IP 位址
  - 目的位址: IP 表頭中目的端 的 IP 位址
  - 未用欄位: 長度為 8 Bits, 填入 0
  - 上層協定: IP 表頭中紀錄上層協定的欄位
  - 封包長度: UDP 表頭中的封包長度欄位

32 bits

<table>
<tr><td colspan="3">來源位址 (Source Address)</td></tr>
<tr><td colspan="3">目的位址 (Destination Address)</td></tr>
<tr><td>00000000</td><td>上層協定(Protocol)</td><td>封包長度 (Length)</td></tr>
</table>

上層協定

- Protocol Numbers
  - Assigned Protocol Numbers

1	Internet Control Message Protocol	17	User Datagram Protocol
2	Internet Group Management Protocol	46	Reservation Protocol (RSVP)
6	Transmission Control Protocol	89	Open Shortest Path First (OSPF)
8	Exterior Gateway Protocol		

Reference: http://www.iana.org/assignments/protocol-numbers

Summary of UDP features

- User Datagram Protocol
  - Pass individual pieces of data from an application to IP
  - No ACK, inherently unreliable
  - Applications
    - A quick, on-shot transmission of data, request/response
    - DNS (udp port 53)
    - If no response, the AP retransmits the request
    - The AP includes a request identifier
  - Checksum

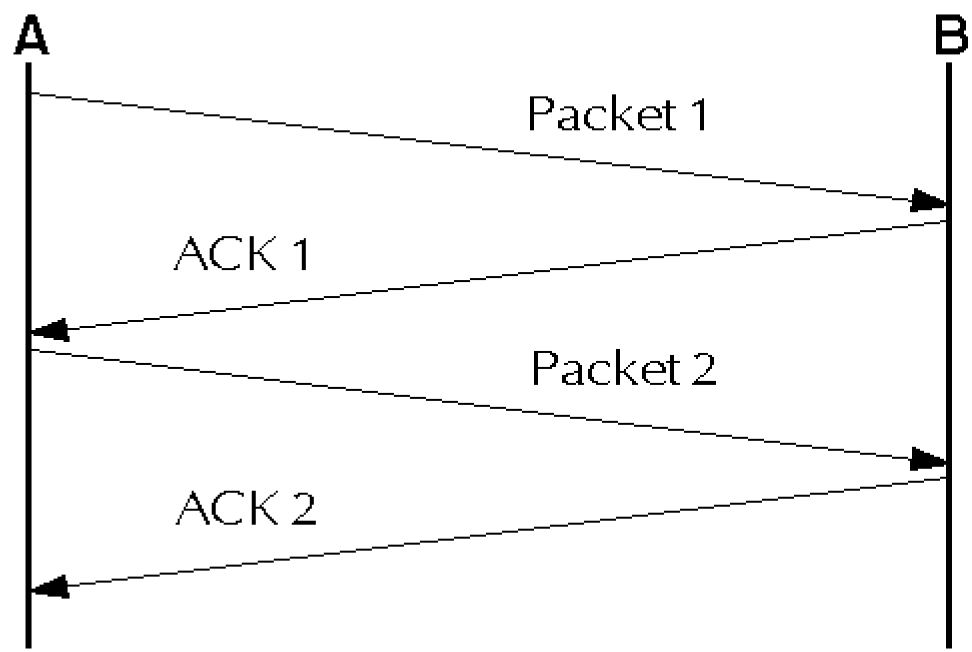
<table>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="16">Source Port</td><td colspan="16">Destination Port</td></tr>
<tr><td colspan="16">Length</td><td colspan="16">Checksum</td></tr>
</table>

TCP 特性

- 資料確認與重送
- 流量控制
- 連線導向

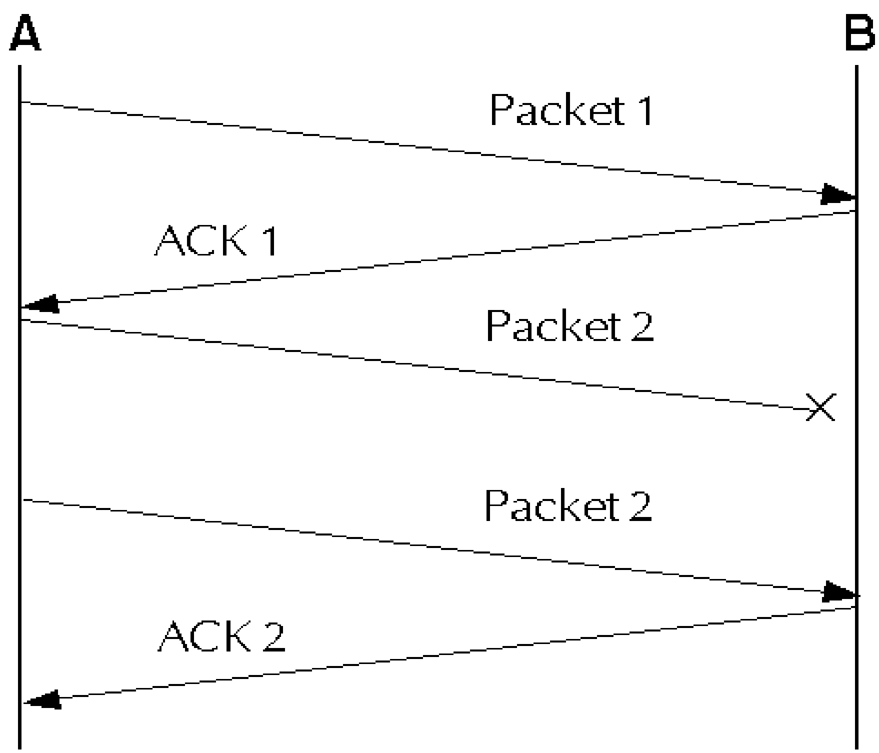
TCP 傳送機制 – 確認與重送(1)

- 利用確認與重送的機制來傳送封包



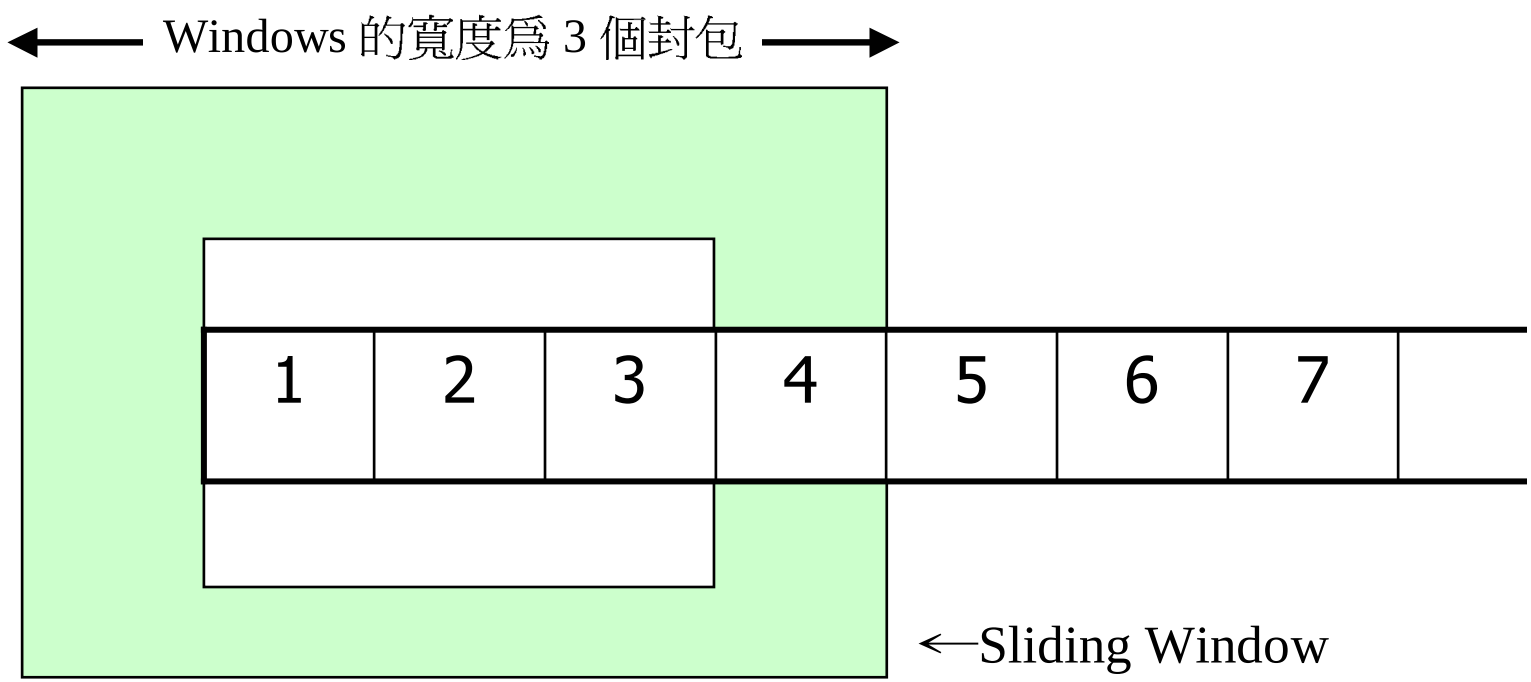
TCP 傳送機制 – 確認與重送(2)

- 利用確認與重送機制來處理傳送過程中的錯誤



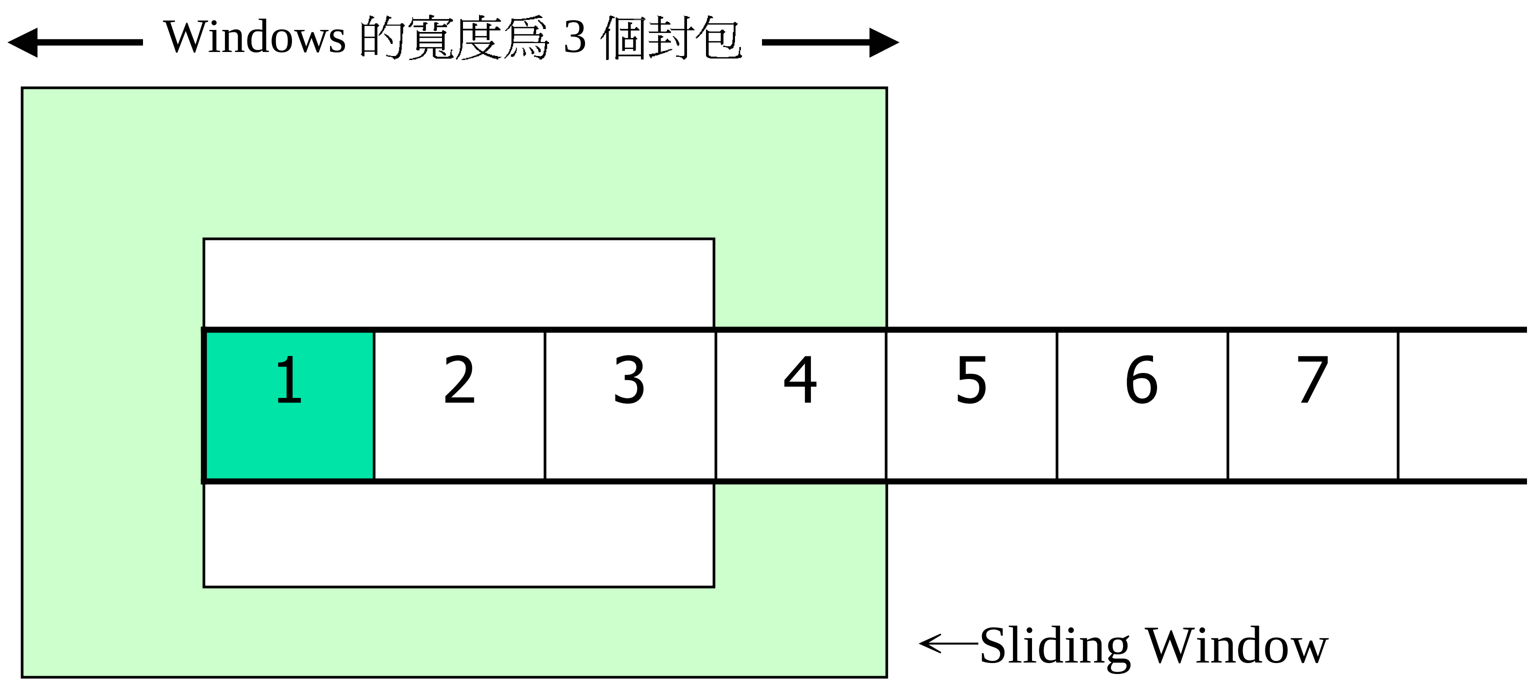
TCP 傳送機制 – Sliding Window (1)

- 開始傳送時, A 的 Sliding Window



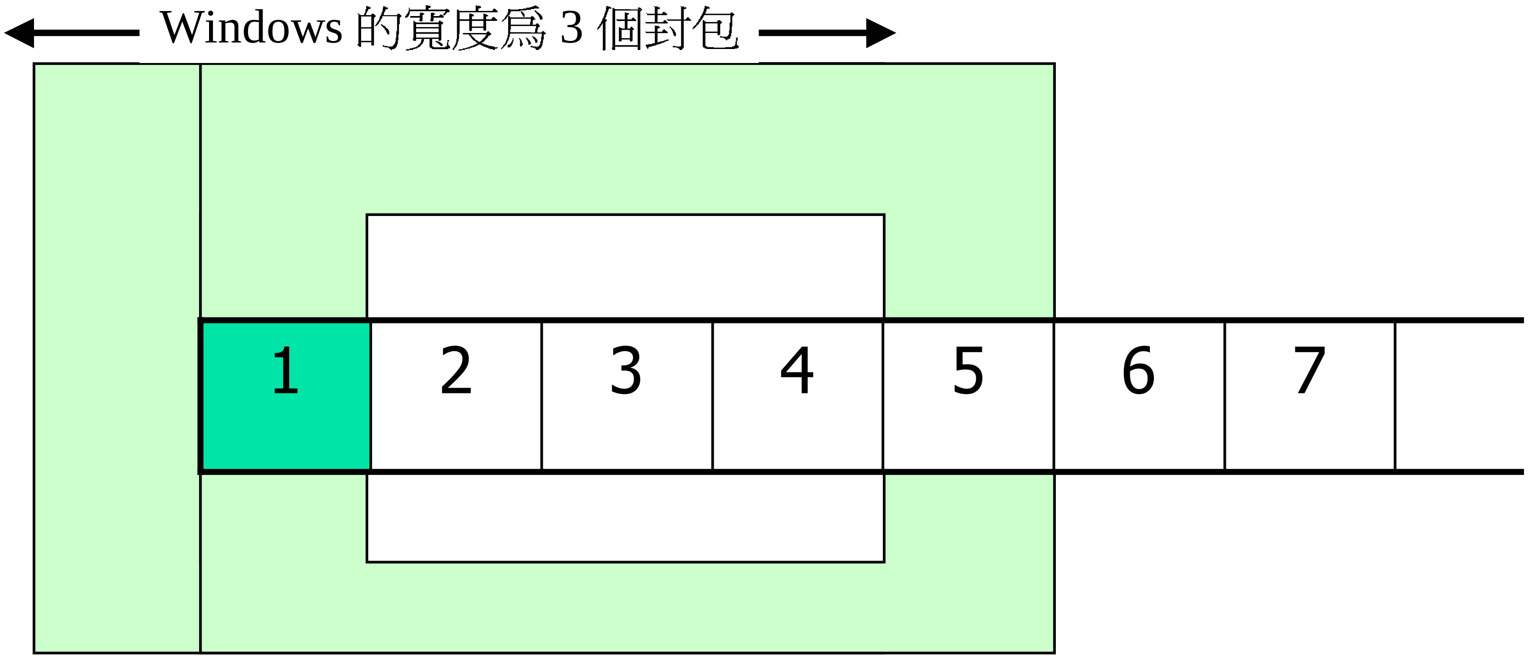
TCP 傳送機制 – Sliding Window (2)

- 收到ACK1後, A 的 Sliding Window 首先將 Packet 1 標示爲『完成』



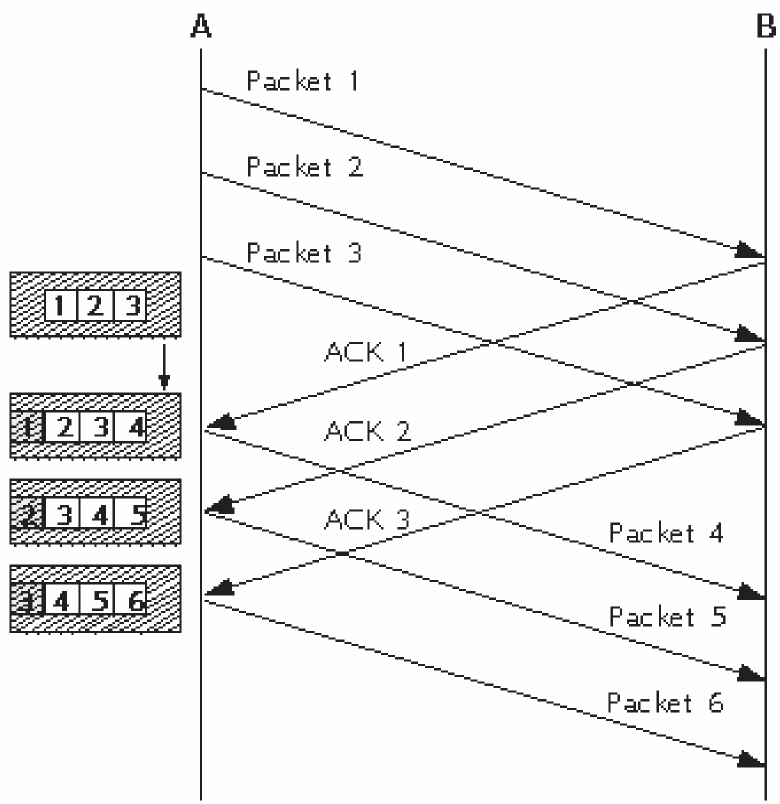
TCP 傳送機制 – Sliding Window (3)

- A 的 Sliding Window 往右滑動



TCP 傳送機制 – Sliding Window (4)

- A 的 Sliding Window 隨著收到的ACK封包變化

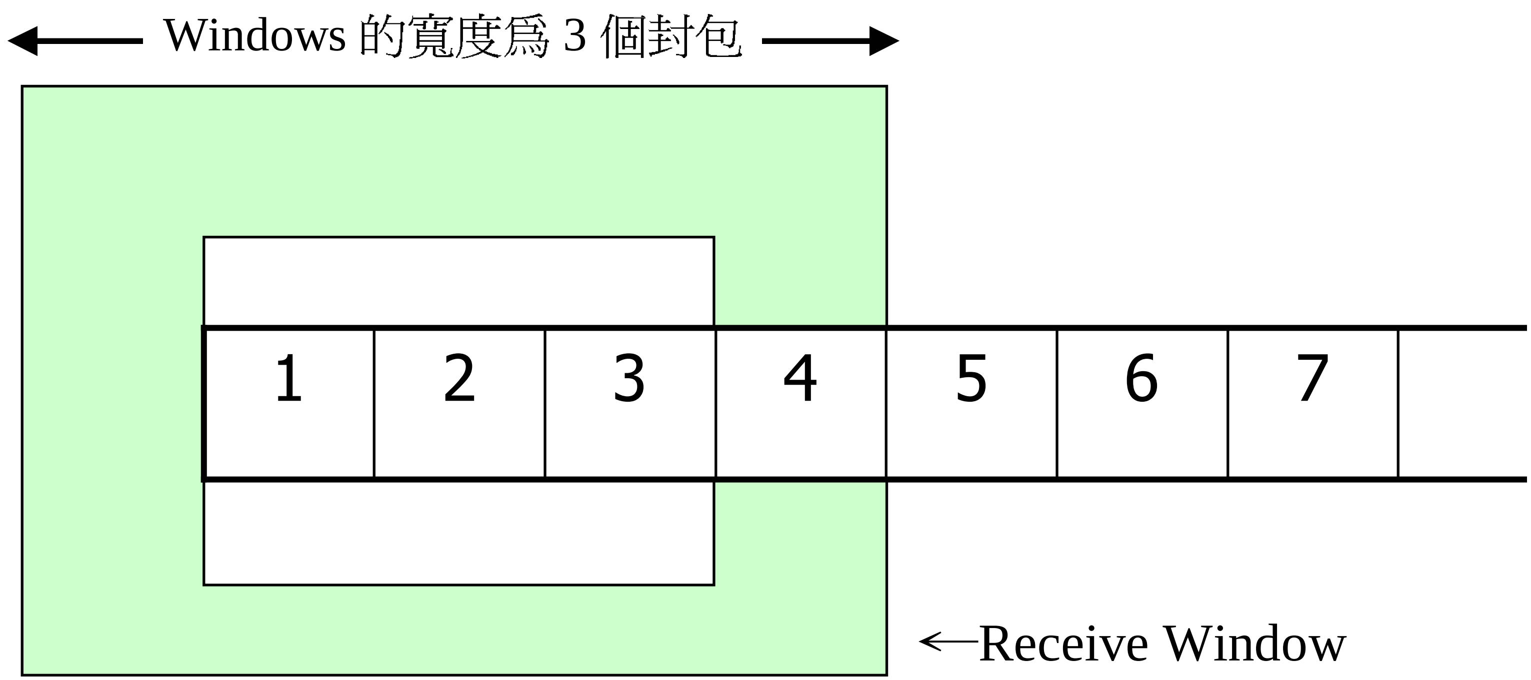


TCP 傳送機制 - Receive Window (1)

- 目的端只會將連續收到的封包交給上層應用程式, 並發出對應的ACK

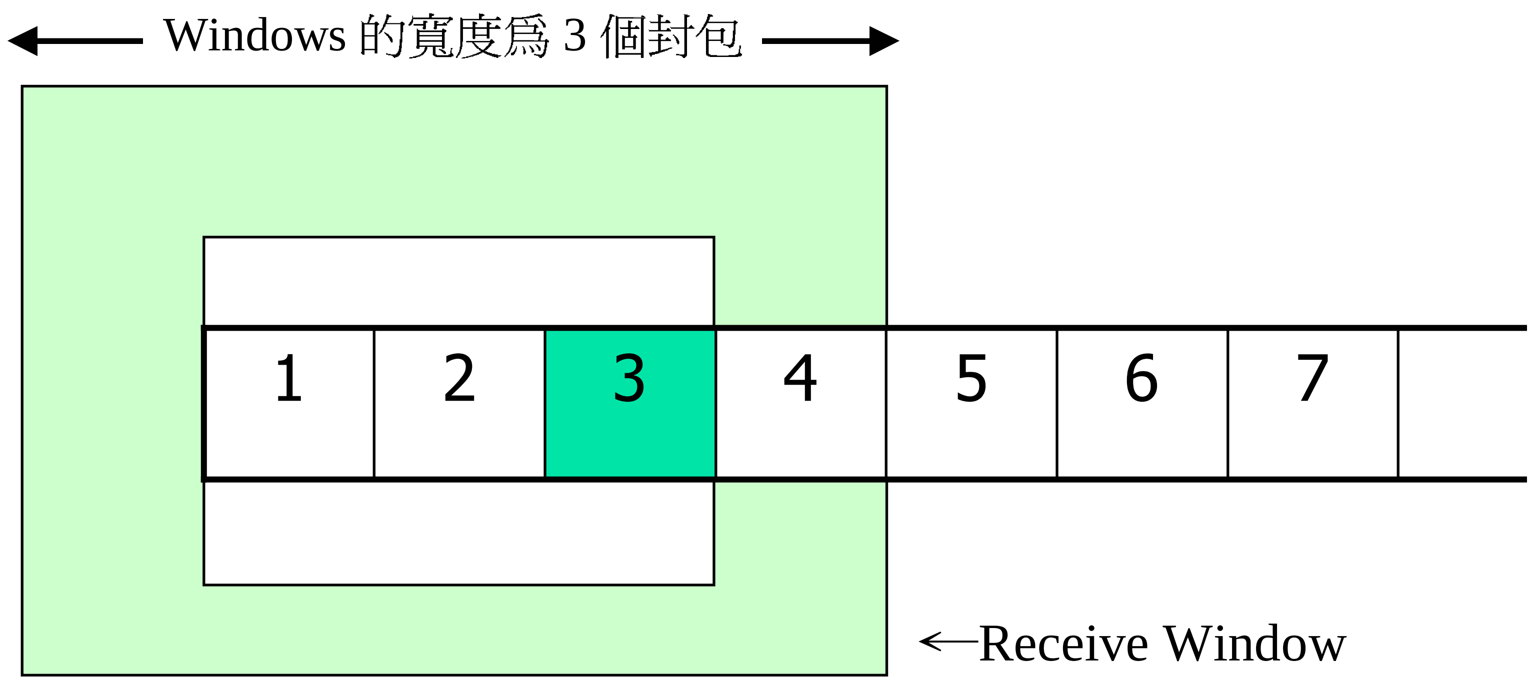
TCP 傳送機制 - Receive Window (2)

- 開始傳送時, B 的 Receive Window



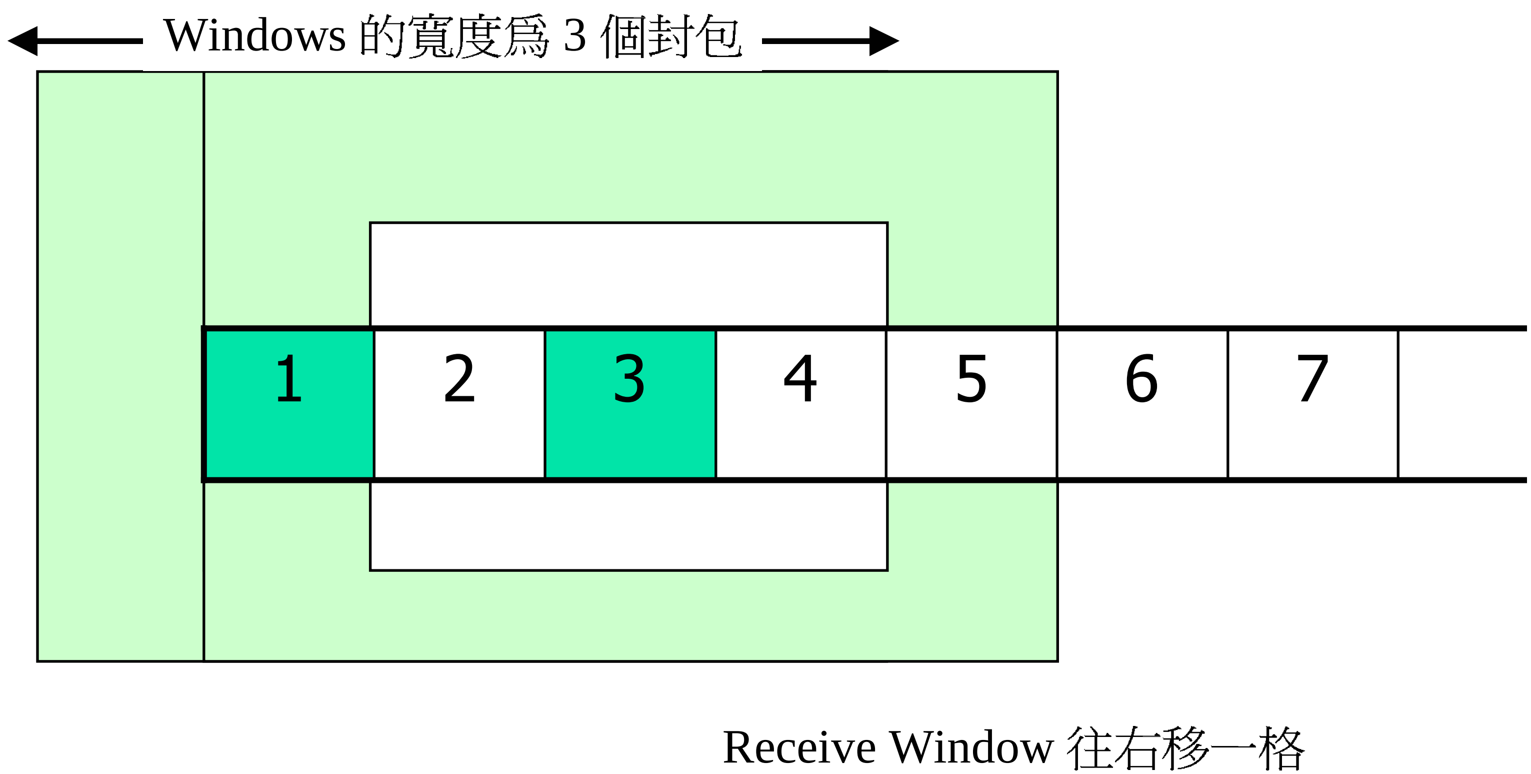
TCP 傳送機制 - Receive Window (3)

- 收到 Packet 3 後, B 的 Receive Window



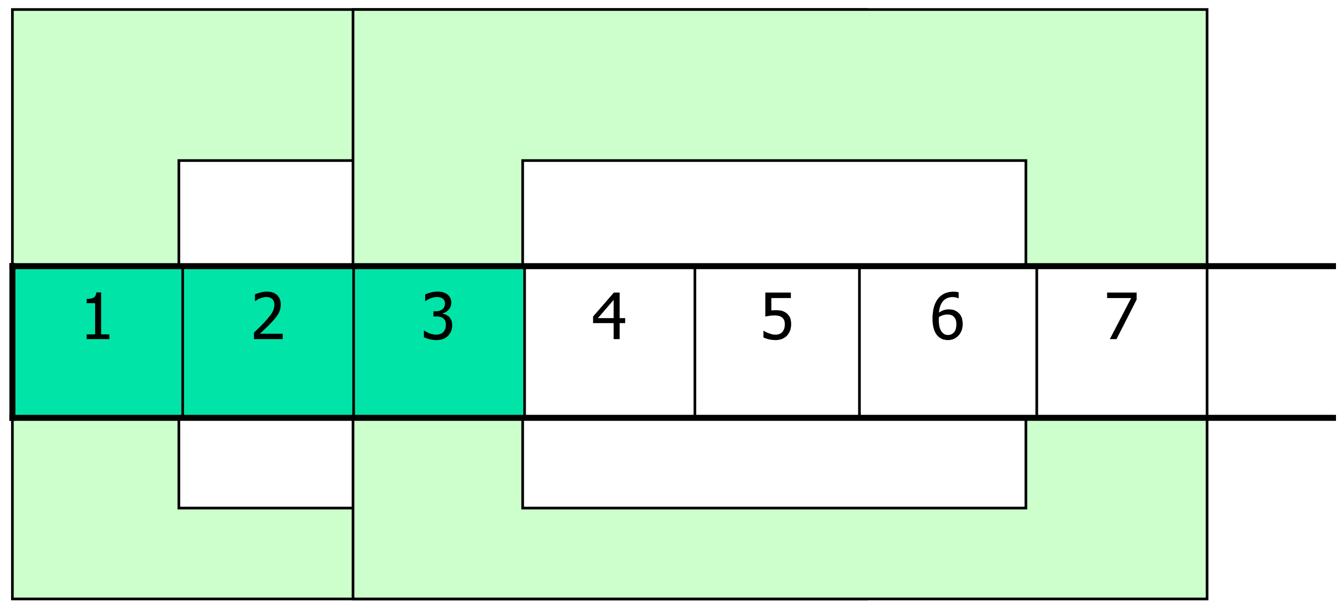
TCP 傳送機制 - Receive Window (4)

- 收到 Packet 1 後, B 的 Receive Window 的變化



TCP 傳送機制 - Receive Window (5)

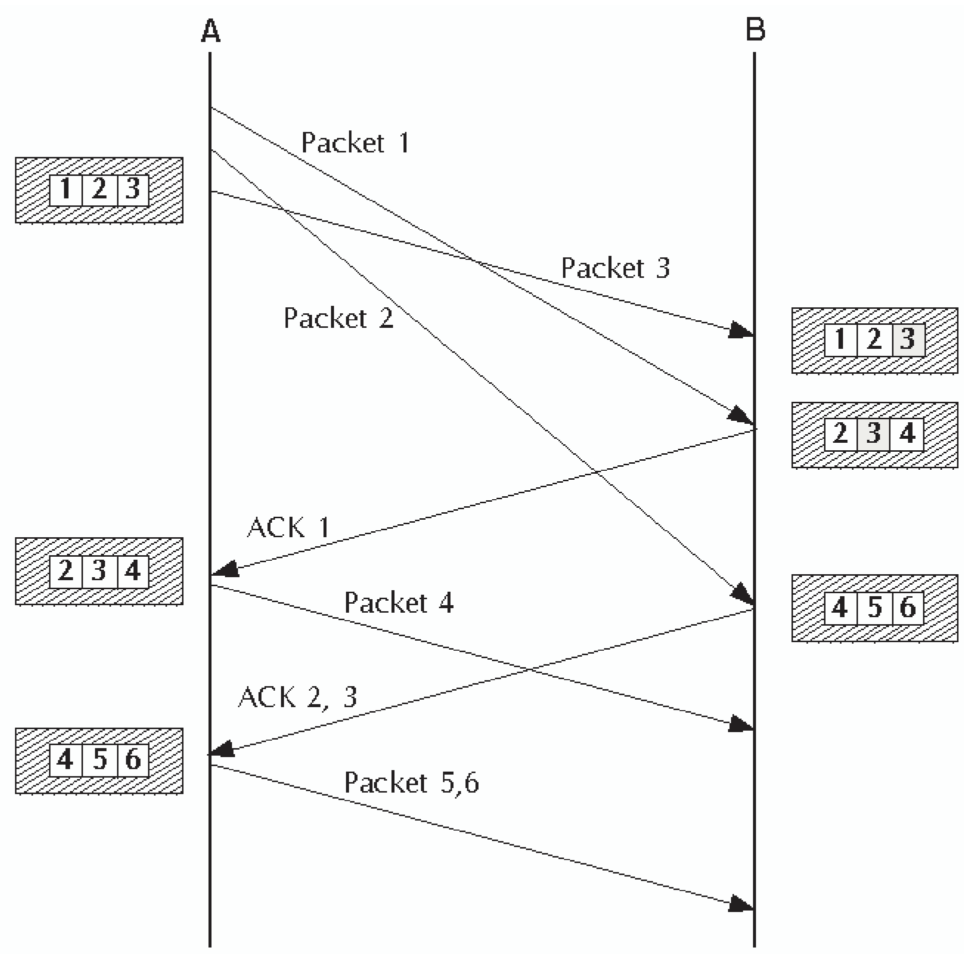
- 收到 Packet 2後, B 的 Receive Window



Receive Window 往右移兩格

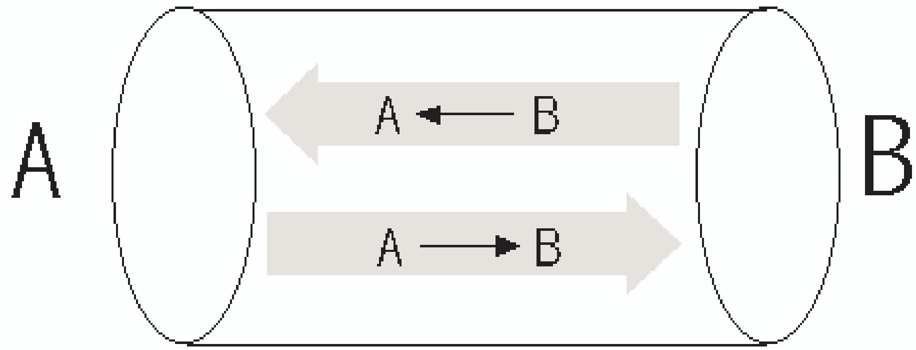
TCP 傳送機制 - Receive Window (6)

- Send/Receive Window 的變化情形



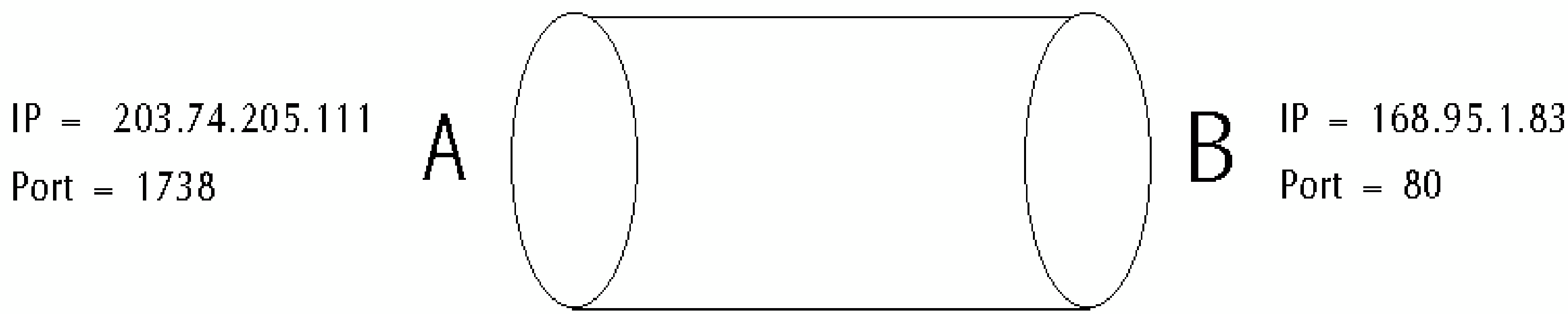
TCP 傳送機制 – 雙向傳輸

- TCP 連線是由兩條單向傳輸的管道結合而成



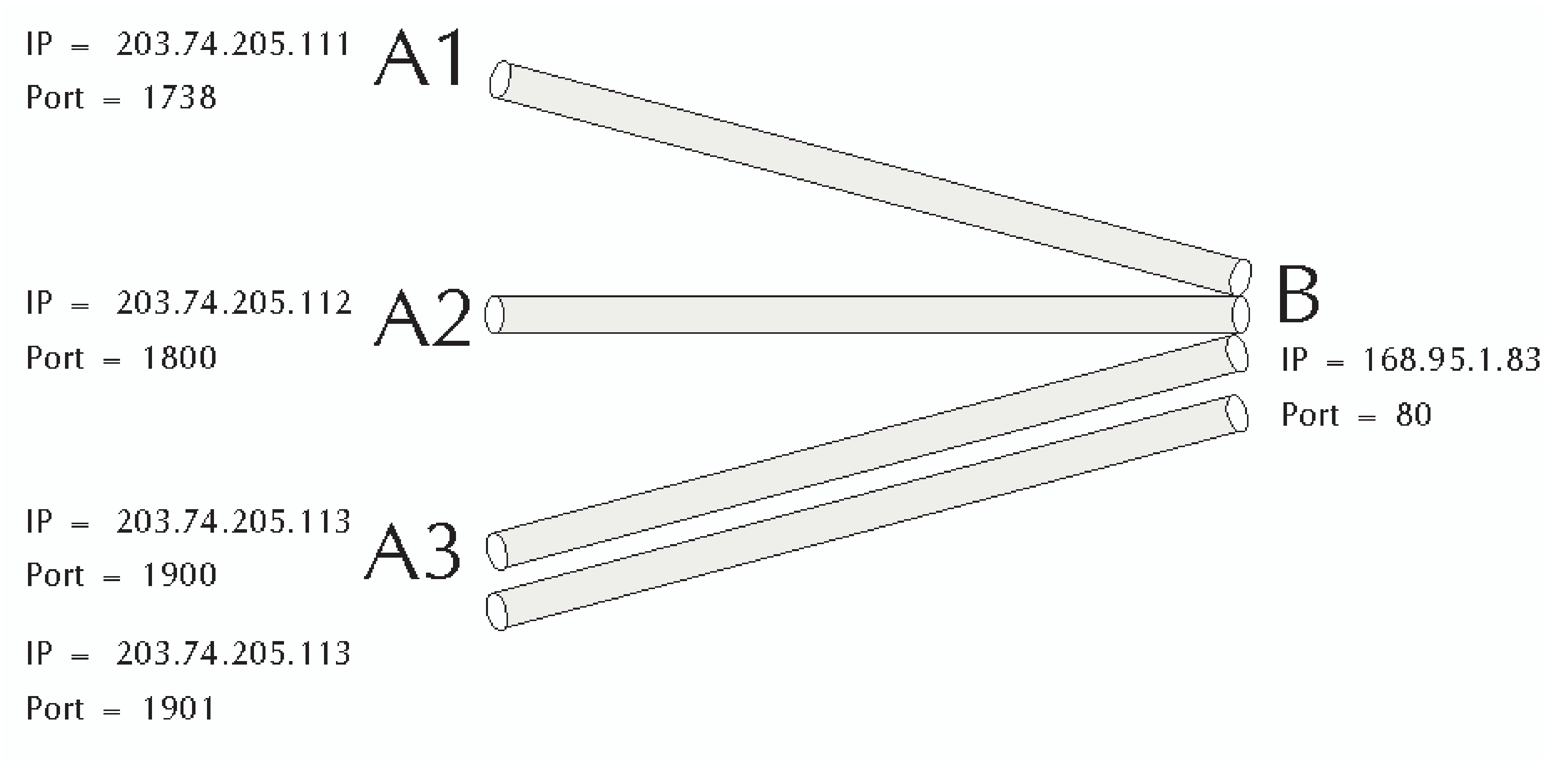
TCP 連線 – 連線定義

- TCP 連線是由連線兩端的 IP 位址與連接埠編號所定義



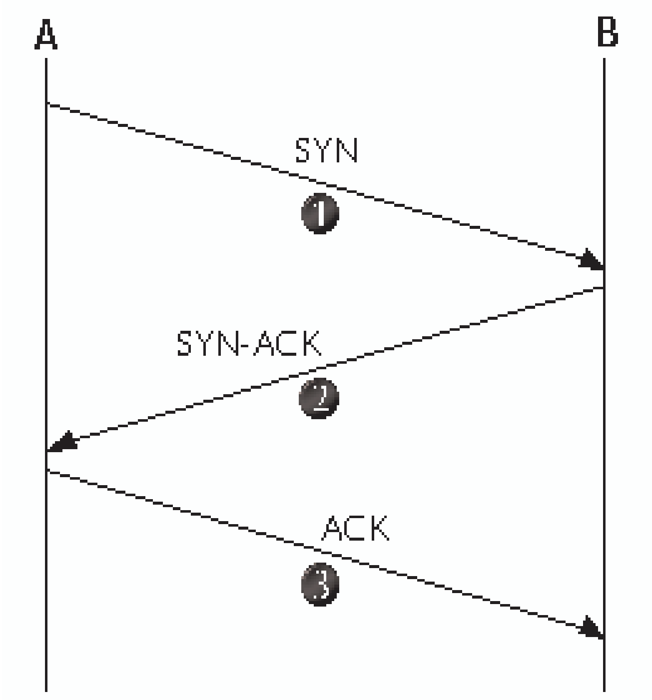
TCP 連線 – 連線定義

- 伺服器可以和多個用戶端, 或同一用戶端的不同連接埠建立多條連線



TCP 連線 – 建立連線(1)

- Basic 3-Way Handshaking



❶ Seq:X, SYN

❷Seq:Y, SYN, ACK: X+1

❸ Seq:X+1, ACK: Y+1

TCP 連線 – 建立連線(2)

- 例如

```
     TCP A                                                  TCP B

1.   CLOSED                                                 LISTEN

2.   SYN-SENT     --> <SEQ=100><CTL=SYN>                --> SYN-RECEIVED

3.   ESTABLISHED <-- <SEQ=300><ACK=101><CTL=SYN,ACK>  <-- SYN-RECEIVED

4.   ESTABLISHED --> <SEQ=101><ACK=301><CTL=ACK>       --> ESTABLISHED

5.   ESTABLISHED --> <SEQ=101><ACK=301><CTL=ACK><DATA> --> ESTABLISHED
```

TCP 連線 – 中止連線(1)

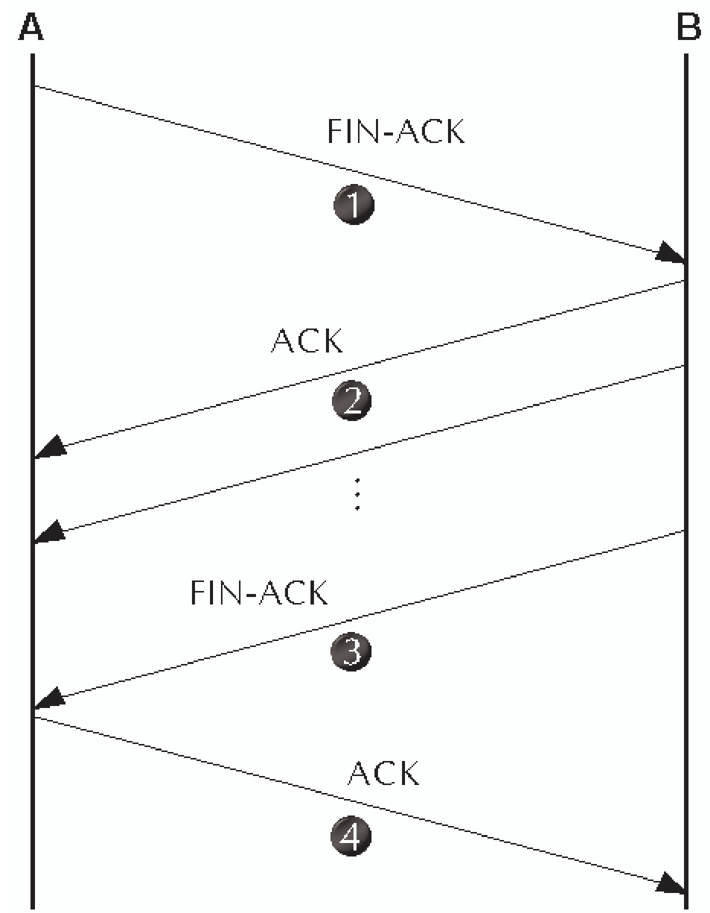
- 結束 TCP 連線的 4 個步驟

❶ Seq:X, ACK: Y. ACK..FIN

❷Seq:Y, ACK: X+1,
ACK

❸Seq:Y, ACK: X+1,
ACK..FIN

❹ Seq:X+1, ACK: Y+1, ACK



TCP 連線 – 中止連線(2)

- 例如

```
     TCP A                                                TCP B

 1.  ESTABLISHED                                          ESTABLISHED

 2.  (Close)
     FIN-WAIT-1  --> <SEQ=100><ACK=300><CTL=FIN,ACK>  --> CLOSE-WAIT

 3.  FIN-WAIT-2  <-- <SEQ=300><ACK=101><CTL=ACK>      <-- CLOSE-WAIT

 4.                                                       (Close)
     TIME-WAIT   <-- <SEQ=300><ACK=101><CTL=FIN,ACK>  <-- LAST-ACK

 5.  TIME-WAIT   --> <SEQ=101><ACK=301><CTL=ACK>      --> CLOSED

 6.  (2 MSL)
     CLOSED
```

MSL: Maximum Segment Lifetime

The TCP Header

<table>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="16">Source Port</td><td colspan="16">Destination Port</td></tr>
<tr><td colspan="32">Sequence Number</td></tr>
<tr><td colspan="32">Acknowledge Number</td></tr>
<tr><td colspan="4">Data Offset</td><td colspan="6">Reserved</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td colspan="16">Window</td></tr>
<tr><td colspan="16">Checksum</td><td colspan="16">Urgent Point</td></tr>
<tr><td colspan="21">Options</td><td colspan="11">Padding</td></tr>
<tr><td colspan="32">Data</td></tr>
</table>

Summary of TCP features

- Transmission Control Protocol
  - In sequence, without omissions and errors
  - End-to-end confirmation, packet retransmission, flow control, congestion control
  - RFC 793
  - Break up a data stream in segments
  - Attach a TCP header
  - Sent down the stack to IP
  - At the destination, checks the header for errors
    - Send back an ACK
  - The source retransmits if no ACK is received within a given period.

Socket Programming

- UDP
- TCP

- Homework:

Voice over UDP, not TCP

- Speech
  - Small packets, 10 – 40 ms
  - Occasional packet loss is not a catastrophe
  - Delay-sensitive
    - TCP: connection set-up, ack, retransmit → delays
  - 5 % packet loss is acceptable if evenly spaced
    - Resource management and reservation techniques
    - A managed IP network
  - In-sequence delivery
    - Mostly yes
- UDP was not designed for voice traffic

The Real-Time Transport Protocol

- Disadvantage of UDP
  - Packets may be lost or out-of-sequence
- RTP: A Transport Protocol for Real-Time Applications
  - RFC 1889; RFC 3550
  - RTP – Real-Time Transport Protocol
  - RTCP – RTP Control Protocol
- RTP over UDP
  - A sequence number to detect packet loss
  - A timestamp to synchronize play-out
  - Does not solve the problems; simply provides additional information

RTCP (RTP Control Protocol)

- A companion protocol
- Exchange messages between session users
- # of lost packets, delay and inter-arrival jitter
- Quality feedback
- RTCP is implicitly open when an RTP session is open
- E.g., RTP/RTCP uses UDP port 5004/5005

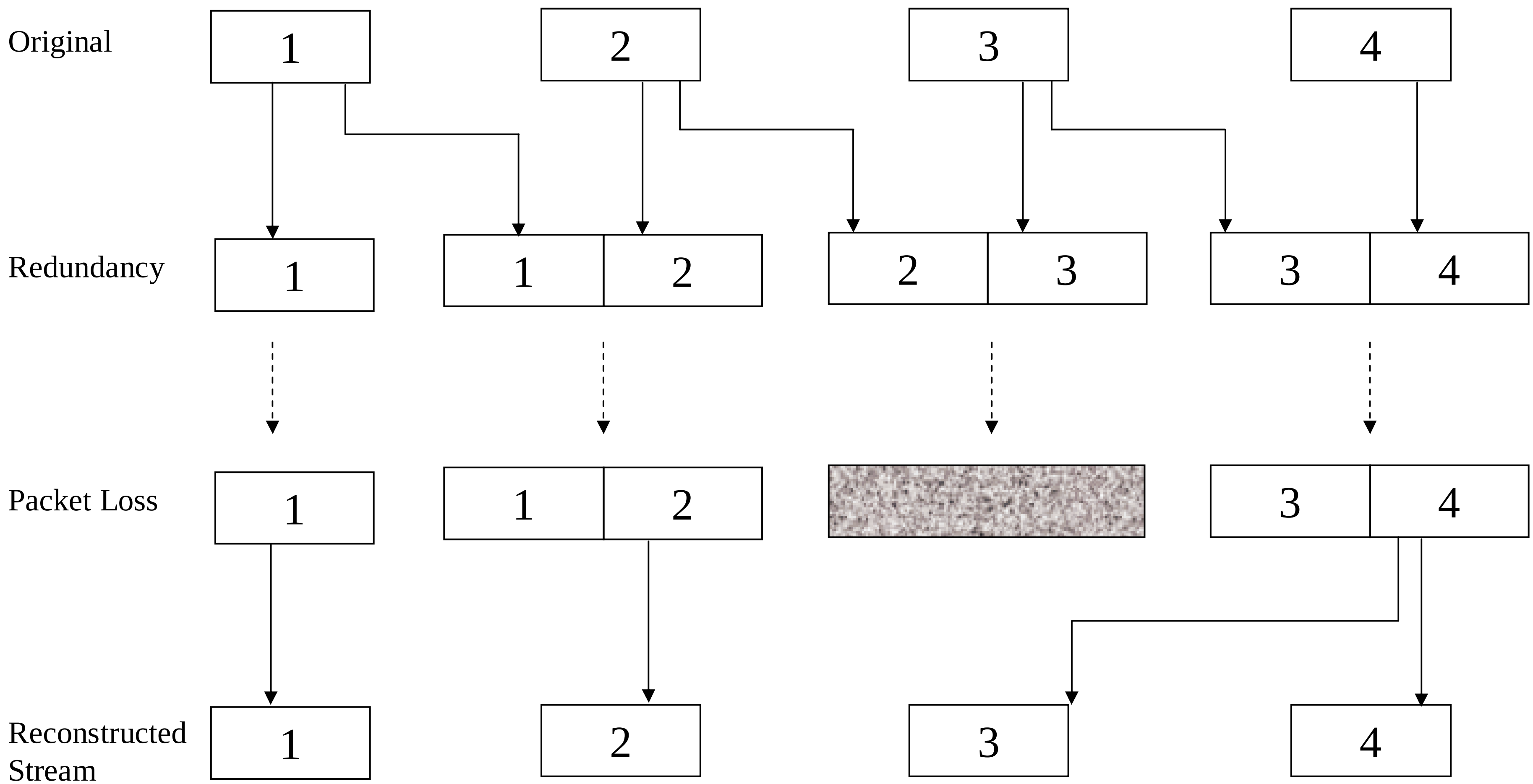
RTP Payload Formats [1/2]

- RTP carries the actual digitally encoded voice
  - RTP header + a payload of voice/video samples
  - UDP and IP headers are attached
- Many voice- and video-coding standards
  - A payload type identifier in the RTP header
    - Specified in RFC 1890
    - New coding schemes have become available
    - See Table 2-1 and Table 2-2
  - A sender has no idea what coding schemes a receiver could handle.

RTP Payload Formats [2/2]

- Separate signaling systems
  - Capability negotiation during the call setup
  - SIP and SDP
  - A dynamic payload type may be used
    - Support new coding scheme in the future
    - The encoding name is also significant.
      - Unambiguously refer to a particular payload specification
      - Should be registered with the IANA
- RED, Redundant payload type
  - Voice samples + previous samples
  - May use different encoding schemes
  - Cope with packet loss

Recovery from Packet Loss



RTP Header Format

<table>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="2">V=2</td><td>P</td><td>X</td><td colspan="4">CC</td><td>M</td><td colspan="7">PT</td><td colspan="16">Sequence Number</td></tr>
<tr><td colspan="32">Timestamp</td></tr>
<tr><td colspan="32">Synchronization Source (SSRC) Identifier</td></tr>
<tr><td colspan="32">Countributing Source (CSRC) Identifier (0 to 15 entries)</td></tr>
</table>

<table>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="16">Profile-specific informaiton</td><td colspan="16">Length</td></tr>
<tr><td colspan="32">Header extension</td></tr>
</table>

The RTP Header [1/4]

- Version (V)
  - 2
- Padding (P)
  - The padding octets at the end of the payload
  - The payload needs to align with 32-bit boundary
  - The last octet of the payload contains a count of the padding octets.
- Extension (X)
  - 1, contains a header extension

The RTP Header [2/4]

- CSRC Count (CC)
  - The number of contributing source identifiers
- Marker (M)
  - Support silence suppression
  - The first packet of a talkspurt, after a silence period
- Payload Type (PT)
  - In general, a single RTP packet will contain media coded according to only one payload format.
  - RED is an exception.
- Sequence number
  - A random number generated by the sender at the beginning of a session
  - Incremented by one for each RTP packet

The RTP Header [3/4]

- Timestamp
  - 32-bit
  - The instant at which the first sample
  - The receiver
    - Synchronized play-out
    - Calculate the jitter
    - The clock freq depends on the encoding
      - E.g., 8000Hz
    - Support silence suppression
    - The initial timestamp is a random number chosen by the sending application.

The RTP Header [4/4]

- Synchronization Source (SSRC)
  - 32-bit identifier
  - The entity setting the sequence number and timestamp
  - Chosen randomly, independent of the network address
  - Meant to be globally unique within a session
  - May be a sender or a mixer
- Contributing Source (CSRC)
  - An SSRC value for a contributor
  - Used to identify the original sources of media behind the mixer
  - 0-15 CSRC entries
- RTP Header Extensions

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Profile-specific informaiton																Length															
Header extension																															

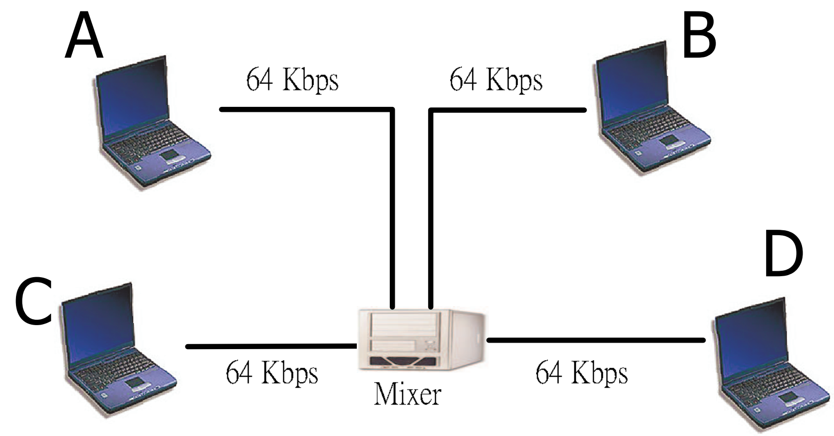
Example of an RTP Packet

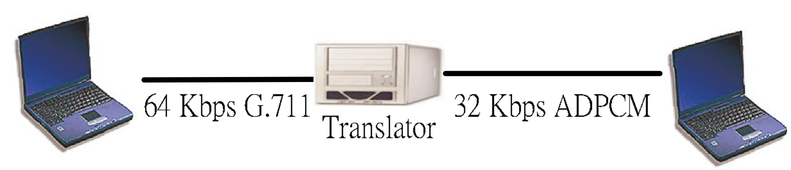
No.	Time	Source	Destination	Protocol	Info
2	0.001519	10.10.2	163.22.20	RTP	Payload type=ITU-T G.711 PCMU, SSRC=354614489, Seq=7333, Time=338620
4	0.022286	10.10.2	163.22.20	RTP	Payload type=ITU-T G.711 PCMU, SSRC=354614489, Seq=7334, Time=338780
6	0.041622	10.10.2	163.22.20	RTP	Payload type=ITU-T G.711 PCMU, SSRC=354614489, Seq=7335, Time=338940
8	0.062197	10.10.2	163.22.20	RTP	Payload type=ITU-T G.711 PCMU, SSRC=354614489, Seq=7336, Time=339100
10	0.081623	10.10.2	163.22.20	RTP	Payload type=ITU-T G.711 PCMU, SSRC=354614489, Seq=7337, Time=339260
12	0.102207	10.10.2	163.22.20	RTP	Payload type=ITU-T G.711 PCMU, SSRC=354614489, Seq=7338, Time=339420
14	0.121743	10.10.2	163.22.20	RTP	Payload type=ITU-T G.711 PCMU, SSRC=354614489, Seq=7339, Time=339580

```
⊞ Frame 2 (214 bytes on wire, 214 bytes captured)
⊞ Ethernet II, Src: PlanetCo_74:26:d4 (00:90:cc:74:26:d4), Dst: Cisco_56:a7:bf (00:18:19:56:a7:bf)
⊞ Internet Protocol, Src: 10.10.20.170 (10.10.20.170), Dst: 163.22.20.151 (163.22.20.151)
⊞ User Datagram Protocol, Src Port: 45714 (45714), Dst Port: 26168 (26168)
⊟ Real-Time Transport Protocol
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    0... .... = Marker: False
    Payload type: ITU-T G.711 PCMU (0)
    Sequence number: 7333
    Timestamp: 338620
    Synchronization Source identifier: 354614489
    Payload: FB7F7B79FCFCFBFE7F7C797A7C7EFFFD79797DFDF6FE7D7F...
```

Mixers and Translators

- Mixers
  - Enable multiple media streams from different sources to be combined into a single stream
    - If the capacity or bandwidth of a participant is limited
  - An audio conference
  - The SSRC is the mixer
    - More than one CSRC values
- Translators
  - Manage communications between entities that does not support the same coding scheme
  - The SSRC is the participant, not the translator.





Homework

- Read RFC 3550 to study how the protocol guarantee the global uniqueness of SSRC.
- Draw a flow chart of the algorithm in a PowerPoint file and send it to voip-ta@voip.edu.tw.
- Due:

The RTP Control Protocol [1/3]

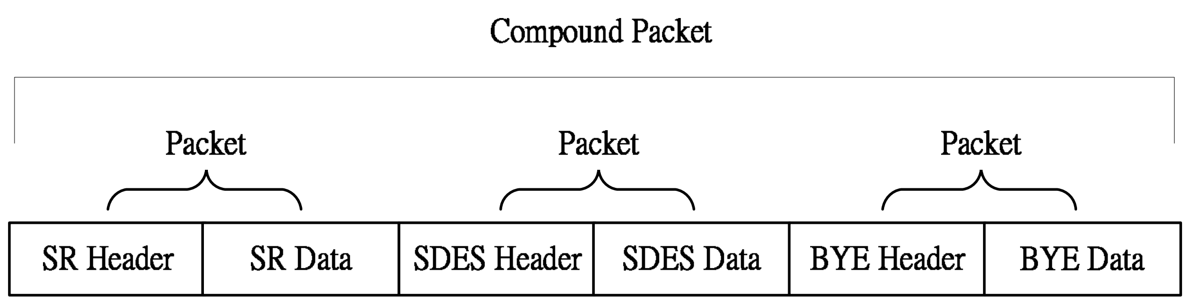
- RTCP
  - A companion control protocol of RTP
  - Periodic exchange of control information
    - For quality-related feedback
  - A third party can also monitor session quality and detect network problems.
    - Using RTCP and IP multicast
- Five types of RTCP packets
  - Sender Report: transmission and reception statistics
  - Receiver Report: reception statistics

The RTP Control Protocol [2/3]

- Source Description (SDES)
  - One or more descriptions related to a particular session participant
  - Must contain a canonical name (CNAME)
    - Separate from SSRC which might change
    - When both audio and video streams were being transmitted, the two streams would have
      - different SSRCs
      - the same CNAME for synchronized play-out
    - If a participant generates multiple streams in one RTP session, for example from separate video cameras, each MUST be identified as a different SSRC
- BYE
  - The end of a participation in a session
- APP
  - For application-specific functions

The RTP Control Protocol [3/3]

- Two or more RTCP packets may be combined
  - SRs and RRs should be sent as often as possible to allow better statistical resolution.
  - New receivers in a session must receive CNAME very quickly to allow a correlation between media sources and the received media.
  - Every RTCP packet must contain a report packet (SR/RR) and an SDES packet
    - Even if no data to report
- An example RTP compound packet



RTCP Sender Report

- SR
  - Header Info
  - Sender Info
  - Receiver Report Blocks
  - Option
    - Profile-specific extension

<table>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="2">V=2</td><td>P</td><td>X</td><td colspan="4">RC</td><td colspan="8">PT=SR=200</td><td colspan="16">Length</td></tr>
<tr><td colspan="32">SSRC of sender</td></tr>
<tr><td colspan="32">NTP Timestamp (most significant word)</td></tr>
<tr><td colspan="32">NTP Timestamp (least significant word)</td></tr>
<tr><td colspan="32">RTP Timestamp</td></tr>
<tr><td colspan="32">sender's packet count</td></tr>
<tr><td colspan="32">sender's octet count</td></tr>
<tr><td colspan="32">SSRC_1(SSRC of first source)</td></tr>
<tr><td colspan="8">fraction lost</td><td colspan="24">fraction lost</td></tr>
<tr><td colspan="32">extended highest sequence number received</td></tr>
<tr><td colspan="32">interarrival jitter</td></tr>
<tr><td colspan="32">last SR (LSR)</td></tr>
<tr><td colspan="32">Delay since last SR (DLSR)</td></tr>
<tr><td colspan="32">SSRC_2(SSRC of second source)</td></tr>
<tr><td colspan="32">:
:</td></tr>
<tr><td colspan="32">profile-specific extensions</td></tr>
</table>

Header Info

- Resemble to an RTP packet
  - Version
    - 2
  - Padding bit
    - Padding octets?
  - RC, report count
    - The number of reception report blocks
    - 5-bit
      - If more than 31 reports, an RR is added
  - PT, payload type (200)
  - Length: [(RTCP bytes #) – 4] / 4

Sender Info

- SSRC of sender
- NTP Timestamp
  - Network Time Protocol Timestamp
    - The time elapsed in seconds since 00:00, 1/1/1900 (GMT)
    - 64-bit
      - 32 MSB: the number of seconds
      - 32 LSB: the fraction of a seconds (200 picoseconds)
- RTP Timestamp
  - Corresponding to the NTP timestamp
  - The same as used for RTP timestamps
  - For better synchronization
- Sender's packet count
  - Cumulative within a session
- Sender's octet count
  - Cumulative within a session

Report blocks [1/2]

- SSRC_n
  - The source identifier of the session participant to which the data in this RR block pertains.
- Fraction lost
  - Fraction of packets lost since the last report issued by this participant
  - By examining the sequence numbers in the RTP header
- Cumulative number of packets lost
  - Since the beginning of the RTP session
- Extended highest sequence number received
  - The sequence number of the last RTP packet received
  - 16 lsb, the last sequence number
  - 16 msb, the number of sequence number cycles

Report blocks [2/2]

- Inter-arrival jitter
  - An estimate of the variance in RTP packet arrival
- Last SR Timestamp (LSR)
  - Timestamp of the last SR received
  - Used to check if the last SR has been received
- Delay Since Last SR (DLSR)
  - The duration in units of 1/65,536 seconds between the reception of the last SR and issuance of this RR.

RTCP Receiver Report

- RR
  - Issued by a participant who receives RTP packets but does not send, or has not yet sent
  - Is almost identical to an SR
    - PT = 201
    - No sender information

RTCP Source Description Packet

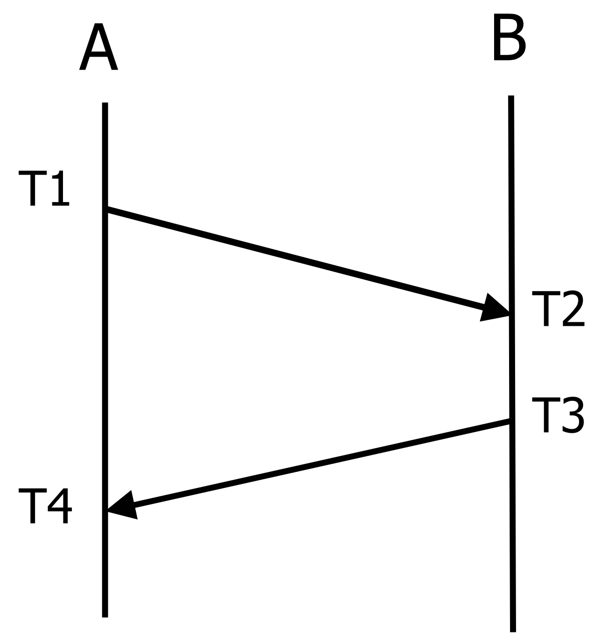
- Provides identification and information regarding session participants
  - Must exist in every RTCP compound packet
- Header
  - V, P, SC, PT=202, Length
- Zero or more chunks of information
  - An SSRC or CSRC value
  - One or more identifiers and pieces of information
    - A unique CNAME
    - Email address, phone number, name

Infrequent RTCP types

- RTCP BYE Packet
  - Indicate one or more media sources are no longer active
- Application-Defined RTCP Packet
  - For application-specific data
  - For non-standardized application

Calculating Round-Trip Time

- Use SRs and RRs
- E.g.
  - Report A: A, T1 $\rightarrow$ B, T2
  - Report B: B, T3 $\rightarrow$ A, T4
  - RTT = T4-T3+T2-T1
  - RTT = T4-(T3-T2)-T1
  - Report B
    - LSR = T1
      - Last Sender Report Timestamp
    - DLSR = T3-T2
      - Delay since Last SR
    - Participant A receives Report B at T4.



Calculation Jitter

- The mean deviation of the difference in packet spacing at the receiver
  - S_i = the RTP timestamp for packet i
  - R_i = the time of arrival
  - $D(i,j) = (R_j - S_j) - (R_i - S_i) = (R_j - R_i) - (S_j - S_i)$
- The Jitter is calculated continuously
  - $J(i) = J(i-1) + (| D(i-1,i) | - J(i-1))/16$

Timing of RTCP Packets

- RTCP provides useful feedback
  - Regarding the quality of an RTP session
  - Delay, jitter, packet loss
  - Be sent as often as possible
    - Consume the bandwidth
    - Should be fixed at 5% of bandwidth
- An algorithm in RFC 1889 to achieve these goals:
  - Senders are collectively allowed at least 25% of the control traffic bandwidth.
    - New participants can quickly receive the CNAME.
  - The interval > 5 seconds
  - 0.5 – 1.5 times the calculated interval
    - To prevent all participants sending RTCP at the same time
  - A dynamic estimate the avg. RTCP packet size

Homework

- Goal: Given a sequence of RTP packets received on a device, write a C program to calculate the deviation and jitter.
- Pcap file format:
  - http://wiki.wireshark.org/Development/LibpcapFileFormat
- Input file:
  - http://Course.ipv6.club.tw/Measurement/hw3-jitter.cap
- Output:

1	D(0,1)	J(1)
2	D(1,2)	J(2)
3	D(2,3)	J(3)
. . .	. . .	. . .