

CHAPTER 08



IP協定

- ▶ 8-1 IP簡介
- ▶ 8-2 網路遮罩(Net Mask)
- ▶ 8-3 IP設定規則
- ▶ 8-4 特殊用途之IP位址
- ▶ 8-5 子網路遮罩
- ▶ 8-6 無等級的IP位址
- ▶ 8-7 NAT簡介
- ▶ 8-8 IP封包格式
- ▶ 8-9 IP封包的擷取分析
- ▶ 8-10 IP路由
- ▶ 8-11 IPv6簡介
- ▶ 8-12 IP Spoofing
- ▶ 8-13 IPv6 安全性

8-1 IP簡介

- ▶ Windows 7系統，請您按「開始」然後在電腦左下角的「搜尋程式及檔案」的欄位內用鍵盤輸入cmd，這時可能會出現C:\Users\ASUS>，然後用鍵盤輸入ipconfig再按Enter。
- ▶ 如圖8-1所示的框框出現IP Address，其代表您目前在網路卡設定的IP位址號碼，即192.168.1.8。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-1 IP簡介

- ▶ IP位址它是用「.」來分開此4組的十進位數字，每組數字都是由一個8bits的二進位數字組成，亦即IP位址總共由32bits組成，其共有 $2^{32} = 4,294,967,296$ 種組合。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-1 IP簡介

```
C:\Users\ASUS>ipconfig
```

Windows IP 設定

無線區域網路介面卡 無線網路連線 2:

媒體狀態 : 媒體已中斷連線
連線特定 DNS 尾碼 :

乙太網路卡 區域連線:

媒體狀態 : 媒體已中斷連線
連線特定 DNS 尾碼 : asus

無線區域網路介面卡 無線網路連線:

連線特定 DNS 尾碼 :
連結-本機 IPv6 位址 : fe80::45be:fc35:fad6:b5e8%11
IPv4 位址 : 192.168.1.161
子網路遮罩 : 255.255.255.0
預設閘道 : 192.168.1.1

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

●圖8-1 目前正在使用的IP位址號碼

8-1 IP簡介

- ▶ 32 bits的IP位址長度正是1987年所推出的網際網路協定第4版(Internet Protocol Version 4 ; IPv4)標準。
- ▶ 注意：IP位址包含網路識別號碼(Network ID ; Net ID)，用來識別所屬的網路；和主機識別號碼(Host ID)，用來識別連至網路上的主機。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-1 IP簡介

► IP位址的分類(Class A~E)：

- 如果IP位址最左邊是以「0」開頭的，此IP是一個Class A
- 如果IP位址最左邊是以「10」開頭的，此IP是一個Class B
- 如果IP位址最左邊是以「110」開頭的，此IP是一個Class C

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-1 IP簡介

- ▶ 如果IP位址最左邊是以「1110」開頭的，此IP是一個Class D
- ▶ 如果IP位址最左邊是以「11110」開頭的，此IP是一個Class E

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

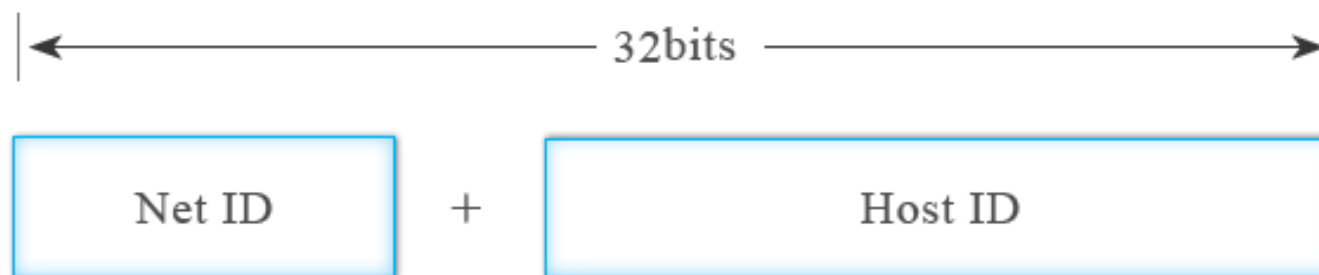
8-12

8-13

習題

8-1-1 Net ID與Host ID

- ▶ IP位址由Net ID和Host ID共32bits組成
- ▶ 圖中指出，IP位址的前段屬Net ID；後段屬Host ID。



●圖8-2 Net ID+ Host ID=32bits

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-1-1 Net ID與Host ID

- ▶ 若一公司申請IP位址時必須是唯一的Net ID，則旗下所有主機分配到相同的Net ID時，各主機的Host ID也必須是唯一的。
- ▶ 換言之，您可以指派多個唯一的主機位址給同一個NET ID；但是，在同一個NET ID時，同一個主機位址卻不能同時指定給兩個(或以上)網路裝置。IP路由就是以IP位址的Net ID來決定要將封包送至哪一個網路。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-1-2 IP Class分類-Class A

- ▶ 第一個較高位元組為網路位址(Net ID)，後面三個較低位元組為主機位址(Host ID)。
 - ▶ Net ID中的最高位元(即最左第一個位元)固定為0，其他7個位元以 xxxxxxx(代表位址在 0000000 至 1111111 之間做變化)表示，因而，Class A 的網路位址號碼在 00000000 至 01111111 之間做變化，轉換為十進位得出 0 至 127，代表 $2^7 - 2 = 126$ 個不同的 Class A 網路。



8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-1-2 IP Class分類-Class A

- ▶ 每個網路可以分配到 $2^{24}-2(=16,777,214)$ 個 Host ID，減2的原因是二進位數字不可以全部為0或1，當主機位址全為0，代表「某一個網路位址」

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-1-2 IP Class分類-Class B

- ▶ 前2個較高位元組為Net ID，後面2個較低位元組為Host ID。
 - ▶ Net ID中的最高位元與次高位元依序為10，其他6個位元以xxxxxx(代表位址在000000至111111之間做變化)表示。
 - ▶ Class B的網路位址號碼在10000000至10111111之間變化，轉換為十進位，得出128至191，代表Class B有 $2^{14}=16,384$ 個不同的網路。



8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-1-2 IP Class分類-Class C

- ▶ 前3個較高位元組為Net ID，後面1個較低位元組為Host ID。
 - ▶ Net ID中的最高位元與下2個次高位元依序為110，其他5個位元以xxxxx(代表位址在00000至11111之間做變化)表示，因而，Class C的網路位址號碼在11000000至11011111之間變化，轉換為十進位，得出192至223，代表Class C有 $2^{21}=2,097,152$ 個不同的網路。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

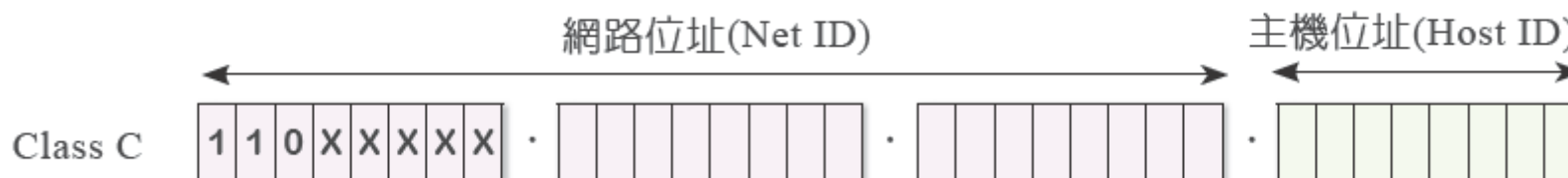
8-12

8-13

習題

8-1-2 IP Class分類-Class C

- ▶ 每個網路C可以分配 2^8-2 個Host ID。



8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-1-2 IP Class分類-Class D

- ▶ 前面4個最高位元固定為1110，此類型的位址是特別留給群播(multicasting)時所使用的群播位址。它並沒有分成Net ID+Host ID的組合，而是整個32位元全部用來定義給不同的群播位址。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

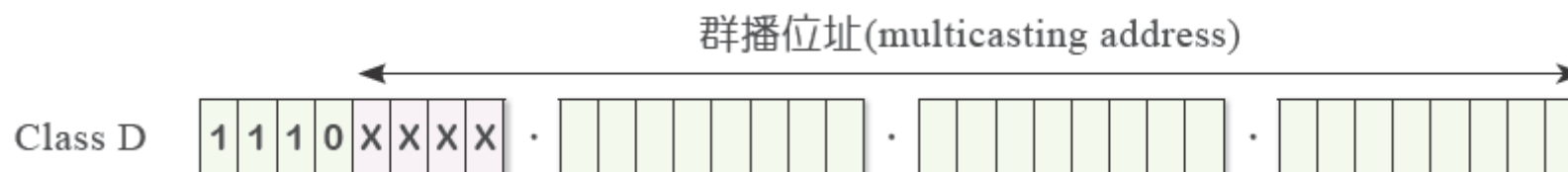
8-12

8-13

習題

8-1-2 IP Class分類-Class D

- ▶ Class D 的網路位址號碼在 11100000 至 11101111 之間做變化，轉換為十進位得出 224 至 239。



8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-1-2 IP Class分類-Class E

- ▶ 前面4個最高位元固定為1111，此類型的位址是被保留給網路實驗用。
- ▶ Class E 的網路位址號碼在 11110000 至 11111111 之間做變化，轉換為十進位，得出 240至255。



8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

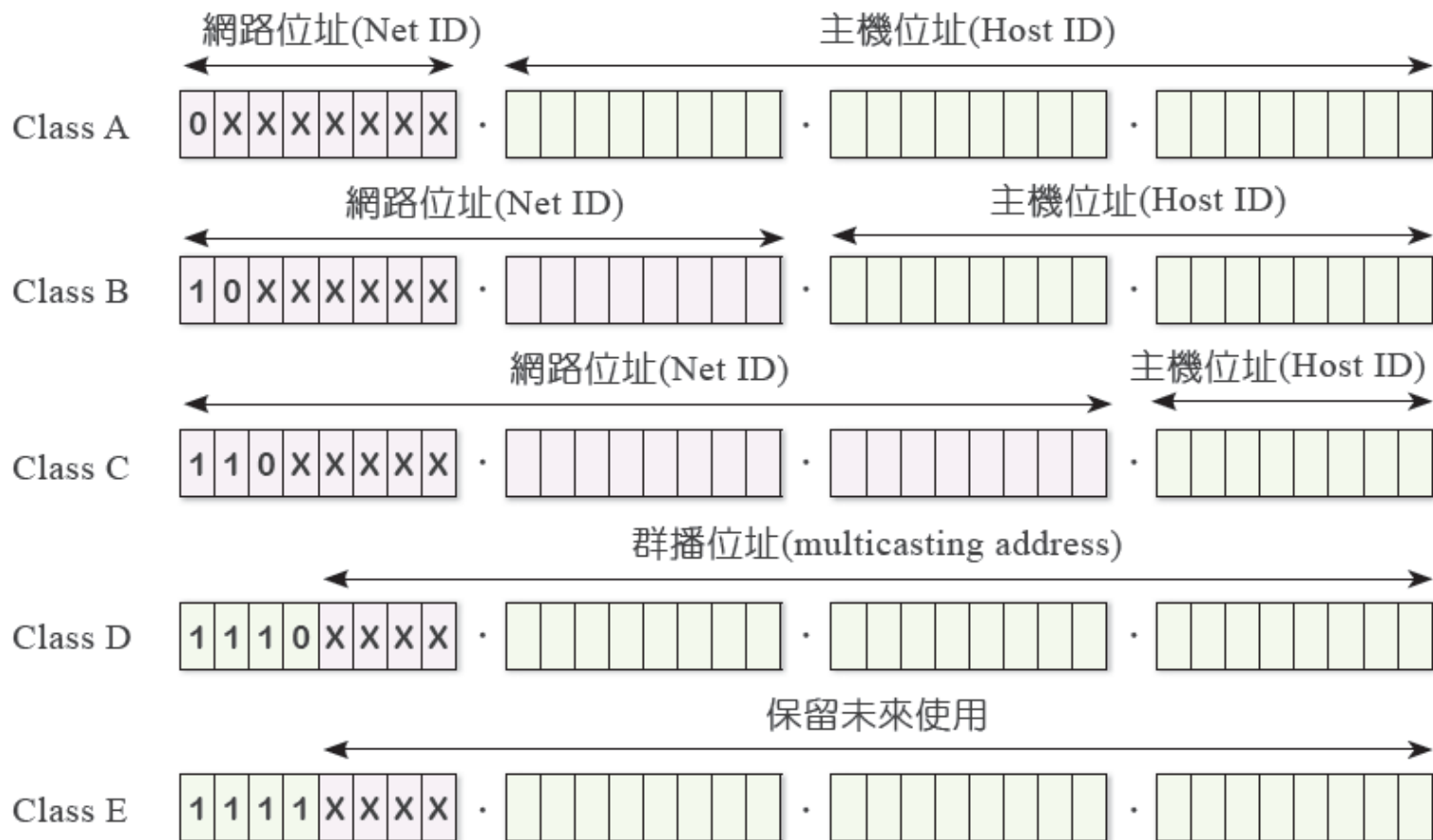
8-11

8-12

8-13

習題

8-1-2 IP Class分類



●圖8-3 各等級的網路位址號碼

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-1-2 IP Class分類

等級	開首	網路數目	主機數目	申請領域
A	0	126	16,777,214	國家級
B	10	16,384	65,534	跨國組織
C	110	2,097,152	254	企業組織
D	1110	-	-	特殊用途
E	1111	-	-	保留範圍

等級	IP範圍	網路位址說明(即網路位址範圍)
A	1.0.0.0～126.255.255.255	1.0.0.0～126.0.0.0
B	128.0.0.0～191.255.255.255	128.0.0.0～191.255.0.0
C	192.0.0.0.～223.255.255.255	192.0.0.0～223.255.255.0
D	224.0.0.0～239.255.255.255	X
E	240.0.0.0～255.255.255.255	X

●圖8-4 IP各等級的網路與主機數目及應用領域

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-2 網路遮罩(Net Mask)

- ▶ 在進行IP網路規劃時，必須經過IP位址和網路遮罩執行AND邏輯運算才能得知某一個IP位址是屬於哪一個網路位址(或稱網段)
 - ▶ 可以使用預設的網路遮罩，像Class A的網路遮罩是255.0.0.0；Class B的網路遮罩是255.255.0.0；Class C的網路遮罩是255.255.255.0。
 - ▶ 例如：IP位址194.33.53.22，網路遮罩是255.255.255.0，欲求出此IP位址的網路位址，方法如下說明。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-2 網路遮罩(Net Mask)

1. 先寫出194.33.53.22的二進位是

11000010.00100001.00110101.00010110

然後將上面IP位址的二進位值和網路遮罩

255.255.255.0做AND運算：

11000010.00100001.00110101.00010110

AND

11111111.11111111.11111111.00000000

得出

11000010.00100001.00110101.00000000

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-2 網路遮罩(Net Mask)

2. 再將得出的二進位值轉換成十進位，就可得到
Net ID=194.33.53.0。

► 換言之，這部電腦所屬的網路位址就是
194.33.53.0。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-3 IP設定規則

- ▶ 當兩部電腦欲透過網路連接來互相通訊時，兩部電腦各將其IP位址與網路遮罩執行AND運算，分別得出Net ID之後，再檢查它們各自的Net ID是否相同
 - ▶ 如果是，代表兩部電腦屬於同一個網路，則在同一個網路內的全部電腦要傳送IP封包不需路由器(router)，就可以直接互相傳遞；
 - ▶ 反之，知道兩部電腦分屬不同網路，就要透過路由器才能互相通訊。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-3 IP設定規則

- ▶ 如圖8-5所示，若網路遮罩為255.255.0.0，則141.35.57.38的電腦A和141.36.96.21的電腦D不在同一個網路，即依序分別是141.35.0.0及141.36.0.0，因此，就一定要使用路由器才能傳遞封包。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

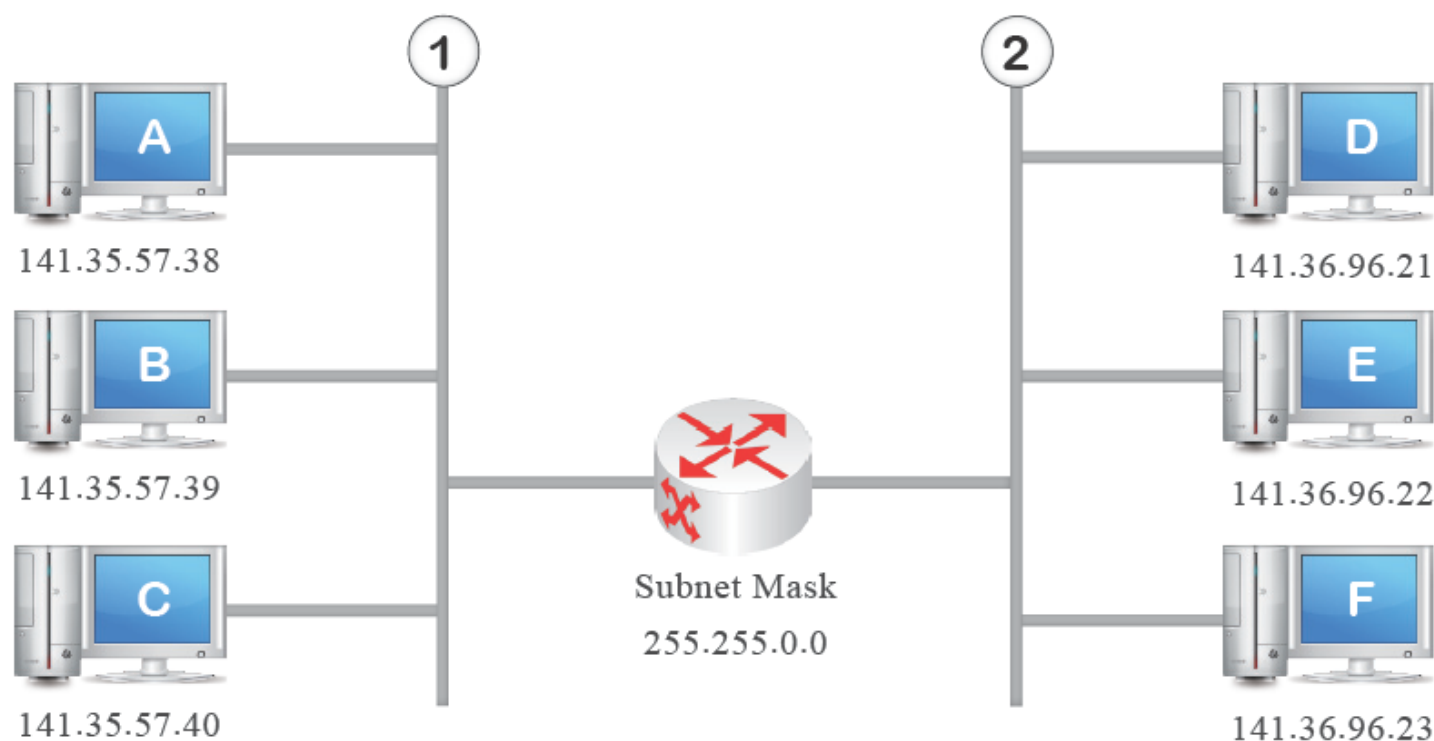
8-11

8-12

8-13

習題

8-3 IP設定規則



●圖8-5 使用路由器才能傳遞IP封包

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-4 特殊用途之IP位址-1

- ▶ 有些Net ID與Host ID在實際應用上會有特殊的用途
 - ▶ 網路位址全為0，代表屬於這個網路的主機
 - ▶ 主機位址全為0，代表這個網路
 - ▶ Net ID與Host ID皆為1(即為255.255.255.255)，代表區域性網路的廣播，只有在此區域網路上的裝置可收到此廣播
 - ▶ Class A的127.0.0.0~127.255.255.255皆可作為回路測試使用的位址，其中最常被使用的為127.0.0.1。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-4 特殊用途之IP位址-2

- ▶ 在Class A、B、C中保留了一些私有IP位址(private IP address)，這些私有IP位址不能直接與外部的網路位址進行通訊，也因而無需擔心會和其他也使用相同位址的網路相衝。
- ▶ 整個IP位址全為0時，Cisco路由器常用來指定預設路徑；也可以解釋成「任何網路」。
- ▶ 整個IP位址全為1時，表示廣播給目前網路上的所有節點

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-5 子網路遮罩

- ▶ IP位址等級在規劃時並沒有什麼彈性。舉例而言，假設一企業公司分配到Class C的IP位址可連接254部電腦，但若網路中只需連接幾10部電腦，這就會讓很多IP位址閒置。解決的方法是可將網路切割為子網路(Subnet)。
- ▶ 子網路遮罩(Subnet Mask)，其原則是：Net ID將原本屬於Host ID的一些位元借過來用，借用多少位元則與欲切割成多少的子網路數目有關。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-5 子網路遮罩-範例1

說明IP 194.33.53.22/27子網路切割後的 1.子網路遮罩為何？2.有多少子網路？3.每個子網路有多少主機？4.有效的子網路為何？5.有效主機位址為何？6.每個子網路的廣播位址為何？

► 解：

1. 由於27 個「1 」轉換成十進位後， 可寫出子網路遮罩為255.255.255.224。
2. 因為借用3個bits， 所以切割成為8個子網路。
3. 每個子網路最多只能有 $2^5 - 2 = 30$ 部主機。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-5 子網路遮罩-範例1

4. 有效的子網路就是要找出8個子網路的網路位址為何？
這可由他們的Subnet ID分別從000到111這8個組合，
再加上原來的NetID=194.33.53.0
(11000010.00100001.00110101.00000000)，最後得
出各子網路的網路位址：

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-5 子網路遮罩-範例1

11000010.00100001.00110101.00000000 (194.33.53.0)
11000010.00100001.00110101.00100000 (194.33.53.32)
11000010.00100001.00110101.01000000 (194.33.53.64)
11000010.00100001.00110101.01100000 (194.33.53.96)
11000010.00100001.00110101.10000000 (194.33.53.128)
11000010.00100001.00110101.10100000 (194.33.53.160)
11000010.00100001.00110101.11000000 (194.33.53.192)
11000010.00100001.00110101.11100000 (194.33.53.224)

Subnet ID

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-5 子網路遮罩-範例1

- ▶ 我們也可更快速地寫出子網路的網路位址：
- ▶ 首先可先求第4個位元組區塊大小為32(即 $256-224=32$)，從0開始是第1個子網路，接著以區塊大小為32做遞增，因而下一個子網路就是32，依此類推得0、32、64、96、128、160、192及224。
- ▶ 我們也可依序寫出各子網路的網路位址為：
194.33.53.0 、 194.33.53.32 、 194.33.53.64 、
194.33.53.96 、 194.33.53.128 、 194.33.53.160 、
194.33.53.192 、 194.33.53.224 。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-5 子網路遮罩-範例1

5. 有效主機位址分別為：

194.33.53.1 ~ 194.33.53.30 ;
194.33.53.33~194.33.53.62 ;
194.33.53.65~194.33.53.94 ;
194.33.53.97~194.33.53.126 ;
194.33.53.129~194.33.53.158 ;
194.33.53.161~194.33.53.190 ;
194.33.53.193~194.33.53.222 ;
194.33.53.225~194.33.53.254 。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-5 子網路遮罩-範例1

6. 廣播位址分別為：

194.33.53.31 ;

194.33.53.63 ;

194.33.53.95 ;

194.33.53.127 ;

194.33.53.159 ;

194.33.53.191 ;

194.33.53.223 ;

194.33.53.255 。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-5 子網路遮罩-範例2

對自己本機電腦上的TCP/IP網路設定是否正確做測試。

► **解：**請您按「開始」然後「搜尋程式及檔案」，用鍵盤輸入cmd，這時可能會出現C:\Users\ASUS>，然後用鍵盤輸入ping 127.0.0.1再按Enter。此時您會看到一個視窗跑出來，如圖8-6所示，圖中顯示4個「回應至TTL=128」，表示本機電腦上的TCP/IP網路設定一切正常。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

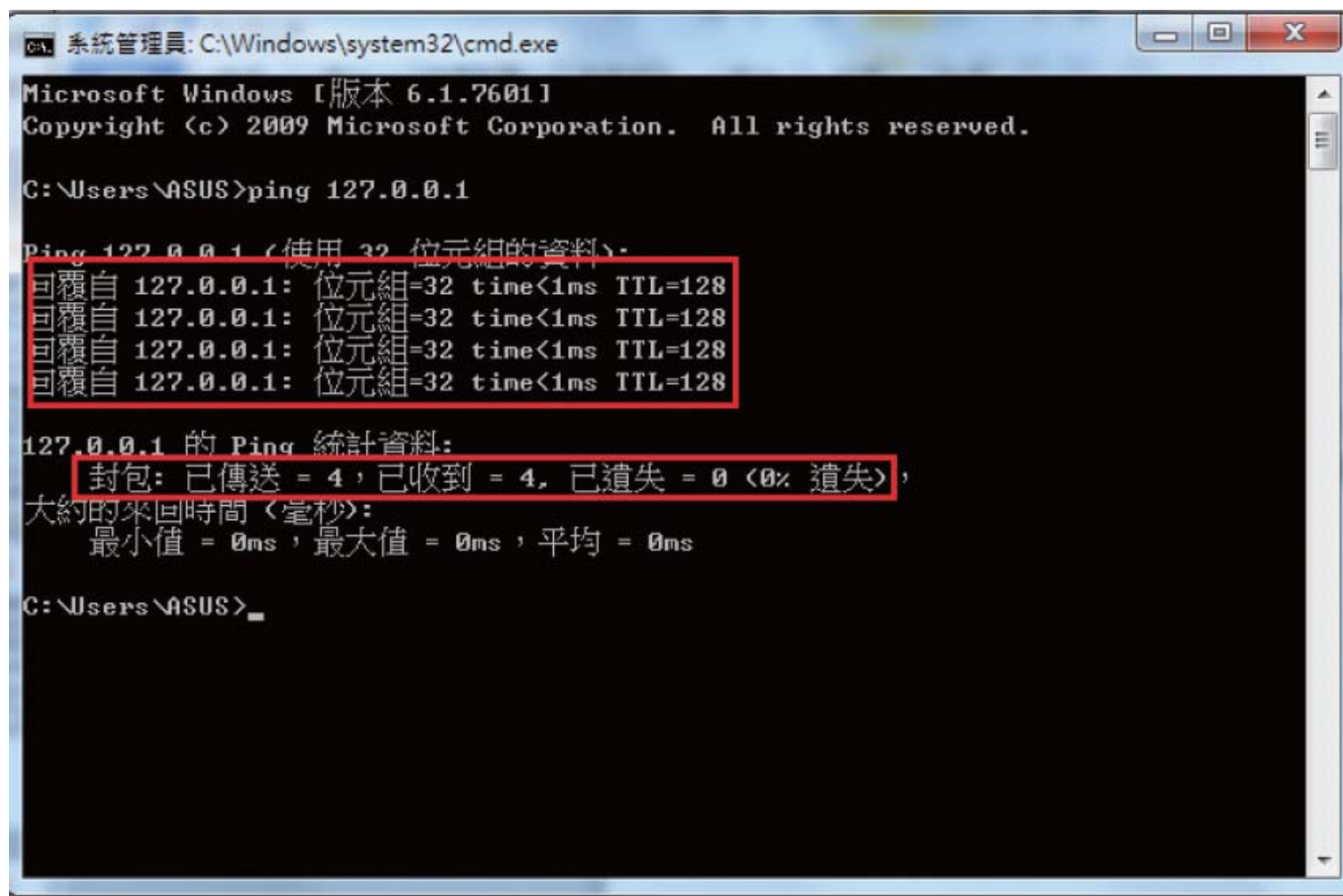
8-11

8-12

8-13

習題

8-5 子網路遮罩-範例2



```
系統管理員: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\ASUS>ping 127.0.0.1

Ping 127.0.0.1 (使用 32 位元組的資料):
回覆自 127.0.0.1: 位元組=32 time<1ms TTL=128
回覆自 127.0.0.1: 位元組=32 time<1ms TTL=128
回覆自 127.0.0.1: 位元組=32 time<1ms TTL=128
回覆自 127.0.0.1: 位元組=32 time<1ms TTL=128

127.0.0.1 的 Ping 統計資料:
    封包: 已傳送 = 4, 已收到 = 4, 已遺失 = 0 (0% 遺失),
    大約的來回時間 (毫秒):
        最小值 = 0ms, 最大值 = 0ms, 平均 = 0ms

C:\Users\ASUS>
```

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

●圖8-6 ping 127.0.0.1本機回路測試

8-6 無等級的IP位址

- ▶ 隨著Internet使用者的快速普及，各類型的網路也在各企業密集地被規劃出來，對於IP位址的需求量也以加速暴量成長。
- ▶ 然而，這也慢慢浮現Class A、B及C這3種等級在IP位址分配方式上有一些問題。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-6 無等級的IP位址

- ▶ 例如：A公司有700台主機，申請一個C Class網路不夠，看來需申請一個B Class網路，但此級可用的主機遠大於所需求，似乎太浪費
- ▶ 解決這個問題需要應用不分等級IP方式規劃，稱為CIDR (Classless Inter-Domain Routing)，亦即無等級(classless)的IP位址劃分方式。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-6 無等級的IP位址

- ▶ 我們考慮將3個C Class網路合併在一起來分配給原先要求申請Class B的公司
 - ▶ 注意：用來合併Class C的網路位址必須是連續的，網路位址數目也必須是2的冪方數。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-6 無等級的IP位址

- ▶ 使用CIDR的時候，一個C Class的網路也可以使用255.255.0.0這樣的網路遮罩，由於其具較短的網路位址(/x，斜線下的數值x會減少)，針對此類型的CIDR稱為Supernet；至於Subnet，則具較長的網路位址(/x，斜線下的數值x會增加)。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-6 無等級的IP位址

▶ 舉例來說，135.123.163.26/16 和 211.163.62.21/24，假如使用了2個bits的Subnet，/16將增加成/18，/24將增加成/26；同樣地，如果是使用了2個bits的Supernet，則/16將減少成/14，/24將減少成/22。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-6 無等級的IP位址 - 範例3

某一A公司需要1600個IP位址，數量介於Class B與Class C的範圍之間。請利用8個Class C的IP位址合併成為一Supernet，再分配給A公司。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-6 無等級的IP位址 - 範例3

解：

- ▶ 不採用CIDR時，網路連接如圖8-7(a)所示，每個網域都必須搭配一部路由器，使得成本很高，效能也很不好，注意：每一個網路的網路遮罩為255.255.255.0。
- ▶ 若藉由CIDR方式，只需一部路由器就可完成網路連接，因需分配一個長度為21bits的Network ID給A公司，Host ID將會有2048個IP位址。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-6 無等級的IP位址 - 範例3

- 1. 首先寫出8個Class C的網路位址，如下所示：

192.170.16.0 (11000000 10101010 00010000 00000000)

192.170.17.0 (11000000 10101010 00010001 00000000)

192.170.18.0 (11000000 10101010 00010010 00000000)

192.170.19.0 (11000000 10101010 00010011 00000000)

192.170.20.0 (11000000 10101010 00010100 00000000)

192.170.21.0 (11000000 10101010 00010101 00000000)

192.170.22.0 (11000000 10101010 00010110 00000000)

192.170.23.0 (11000000 10101010 00010111 00000000)

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-6 無等級的IP位址 - 範例3

- ▶ 2.接著利用子網路遮罩為255.255.248.0(也可表示成192.170.16.0/21)比預設遮罩(/24)少3個，可使網路的空間愈來愈大。亦即將192.170.16.0開始至192.170.23.0共8個Class C的網路位址空間合併起來形成一個S u p e r n e t，得到如圖8 - 7 (b)。
- ▶ 注意：子網路此時的遮罩為255.255.248.0。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-6 無等級的IP位址 - 範例3



●圖8-7(a) 不採用CIDR機制

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

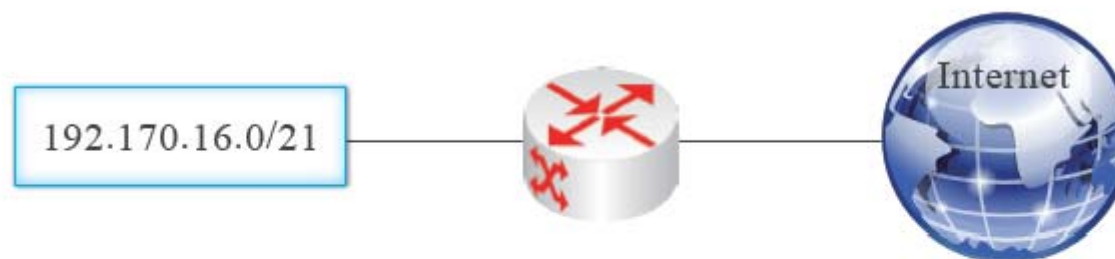
8-11

8-12

8-13

習題

8-6 無等級的IP位址 - 範例3



網路遮罩均為 255.255.248.0

●圖8-7 (b)採用CIDR機制

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-7 NAT簡介

- ▶ 由於Internet使用者愈來愈普及，相對可使用的IP位址也愈來愈吃緊。加上IPv4的位址欄位長度已經固定，因此，解決的替代方案紛紛出籠，主要是以節省位址空間為前提。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-7 NAT簡介

- ▶ 較常用的解決方案是1994年發表的網路位址轉換(Network Address Translator ; NAT)技術。
NAT是在路由器中進行一個交換IP標頭(header)的動作，以使多台電腦能共用一個IP連線至Internet的技術，這也使IP位址不足之問題帶來新的突破。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-7 NAT簡介-靜態NAT

- ▶ 此類型是在內部網路中的每個主機都被固定映射至外部網路中的某個合法的位址。一個私有IP位址對應一個固定的合法IP位址，私有的IP位址個數與合法的IP位址個數一樣。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-7 NAT簡介-動態NAT

- ▶ 此類型是在外部網路中定義了一些合法IP位址，每個使用者上網連線時會先向NAT主機取得一個對應的合法IP位址，其採用動態分配的方法映射到內部網路。
- ▶ 動態NAT只是對IP位址做轉換，每一個內部的IP位址會分配到一個暫時的外部IP位址。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-7 NAT簡介-NAPT

- ▶ NAPT(Network Address Port Translation)是動態NAT的改良版，簡單的說，它是把內部所有的位址映射到外部網路的一個IP位址的不同連接埠上。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-7 NAT簡介-NAPT

- ▶ NAPT也稱為PAT(Port Address Translation)或超載(overloading)，它們只需一個合法的IP位址，就可以讓幾百個或幾千個使用者與Internet連線，這也是利用不同的連接埠，而只靠一相同的IP位址就可讓很多台主機互相連線，亦是造成IPv4位址至今尚未耗盡的原因。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

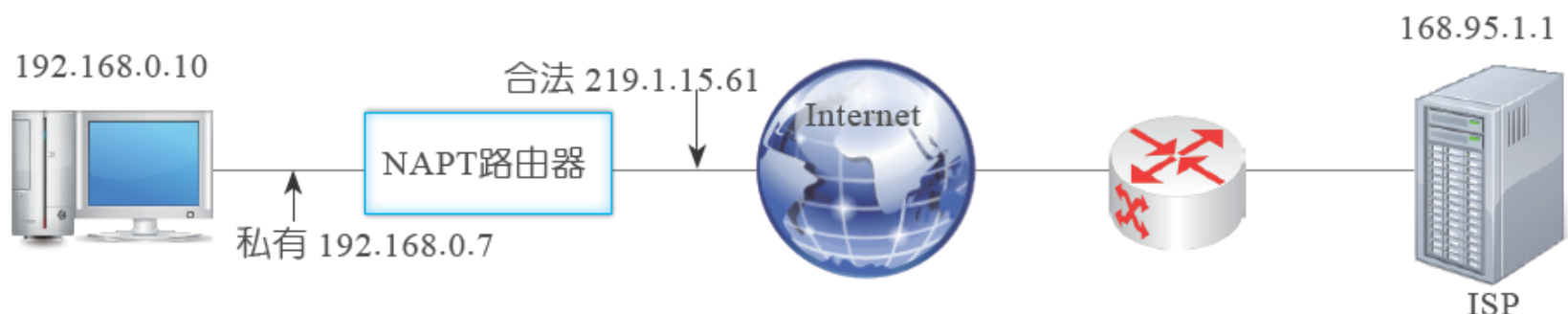
8-11

8-12

8-13

習題

8-7-1 NAT動作原理



1.Request

來源	192.168.0.10	1028
目的	168.95.1.1	80

2.Request(經NAPT轉換)

來源	219.1.15.61	1722
目的	168.95.1.1	80

4.Response(經NAPT轉換)

來源	168.95.1.1	80
目的	192.168.0.10	1028

3.Response

來源	168.95.1.1	80
目的	219.1.15.61	1722

●圖8-8 NAT轉換原理的過程

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-7-1 NAPT動作原理

- ▶ **步驟1**：假設內部網路中某一部電腦使用的私有IP為192.168.0.10，要連線至中華電信的網站168.95.1.1，因此送出Request訊息，包含來源端的IP192.168.0.10與隨機產生的連接埠1028，目的端的IP 168.95.1.1與連接埠80。此也代表Request封包送入LAN端。
- ▶ **步驟2**：當Request訊息經過NAPT路由器時，來源端的IP 192.168.0.10會改為它本身WAN端的IP 219.1.15.61與隨機產生的連接埠1722，NAPT路由器收到並記錄此Request訊息，然後轉換至目的端的IP 168.95.1.1，此也代表NAPT路由器收到Request封包。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-7-1 NAPT動作原理

- ▶ **步驟3**：ISP伺服器Response訊息回傳至NAPT路由器。注意：訊息含來源端的IP 168.95.1.1與連接埠80，目的端為NAPT路由器的IP 219.1.15.61與連接埠1722。
- ▶ **步驟4**：NAPT路由器將依據記錄，將目的端的IP轉換為192.168.0.10與連接埠1028，這表示來源端電腦將收到ISP伺服器Response過來的訊息。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-8 IP 封包格式

- ▶ IP封包(又稱資料包)是由IP標頭及IP Payload組成，如圖8-9所示的各欄位(除Data欄位外)就是IP標頭，用來記錄有關IP位址、路由、封包識別等資訊，長度以32bits為單位
- ▶ IP Payload(即指IP封包中的Data欄位)就是用來承載上層協定的封包(如TCP封包)，長度最長可達65,536bytes。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-8 IP 封包格式

Version(4)	IHL(4)	Type of Service(8)	Total Length(16)	
Identification(16)			Flags(3)	Fragment Offset(13)
Time to Live(8)		Protocol(8)	Header Checksum(16)	
Source Address(32)				
Destination Address(32)				
Options(變動長度)				
Padding(變動長度)				
Data				

●圖8-9 IP封包格式

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-8 IP 封包格式

► Version佔4bits

- 記錄IP的版本編號。目前為IP Ver.4，即第4版，欄位值為4(十進位)或0100(二進位)。後續版本為IP Ver. 6，亦是第6版，但目前仍不普及。

► IP標頭長度(IP Header Length ; IHL)佔4bits

- 長度不定，預設值為20bytes。有些會加上Options欄位，則值會大於20bytes。在IP標頭中，除了Options與Padding欄位為非固定長度外，其他的欄位都是固定長度。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-8 IP 封包格式

► 服務類別(Type of Service ; TOS)佔8bits

- 包含了6個參數。第1個參數Precedence(佔3bits)是用來決定IP封包的優先等級，參數值愈大，代表優先等級愈高(7表最高)。接下來4個參數Delay(0為normal delay ; 1為low delay)、Throughput(0為normal throughput ; 1為high throughput)、Reliability(0為low reliability ; 1為high reliability)、Cost(0為一般成本 ; 1為高成本)用來提供路由器作為選擇路徑時的參考。最後一個參數設為0未定義，則是保留未使用。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-8 IP 封包格式

► 服務類別(Type of Service ; TOS)

Precedence (3)	D (1)	T (1)	R (1)	C (1)	保留 (1)
-------------------	----------	----------	----------	----------	-----------

●圖8-10 服務類別(TOS)

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-8 IP 封包格式

- ▶ 後來IETF將TOS欄位的位元定義成差異性服務 (Differentiated Service ; DS)(參考RFC 2474) , 這對寬頻網路的分析很重要。DS由DSCP及ECN組成，共佔8bits。
- ▶ 圖8-11指出寬頻網路的QoS(Quality of Service)及優先權定義就是以DSCP(佔6bits)來區分，其中左邊3bits定義優先權；右邊3bits定義服務品質QoS。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-8 IP 封包格式

DSCP(佔6bits)	ECN(2bits)
--------------	------------

101110代表Expedited Forwarding (EF)。

001010/001100/001110依序代表AF 1(Assured Forwarding Class 1)的低中高優先權等級。

010010/010100/010110依序代表AF 2(Assured Forwarding Class 2) 的低中高優先權等級。

011010/011100/011110依序代表AF 3(Assured Forwarding Class 3) 的低中高優先權等級。

100010/100100/100110依序代表AF 4(Assured Forwarding Class 4) 的低中高優先權等級。

ECN(Explicit Congestion Notification)=01 or 10 指具壅塞指示能力，由來源端設定(參考RFC3168)。

ECN=11 通知端點發生壅塞，由路由器設定。

ECN=00 未用ECN。

●圖8-11 DSCP欄位定義與壅塞時的指示

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-8 IP 封包格式

▶ 封包總長度(Total Length)佔16bits

▶ 以乙太網路為例，整個IP封包最大傳輸單位 (Maximum Transmission Unit ; MTU) 可達 1500bytes。

▶ 注意，IP資料封包長度理論值可到 65,535bytes。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-8 IP 封包格式

► Fragment Offset(FO)佔13bits

- 當一個網路層收到上層送來較大的位元組資料封包(如TCP)並加上20bytes的IP標頭，一旦此IP封包(即IP資料包)太大，就需要分割產生好幾個IP Fragment(分段)，Fragment Offset就是用來記錄這些IP Fragment屬於哪一段的資料。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

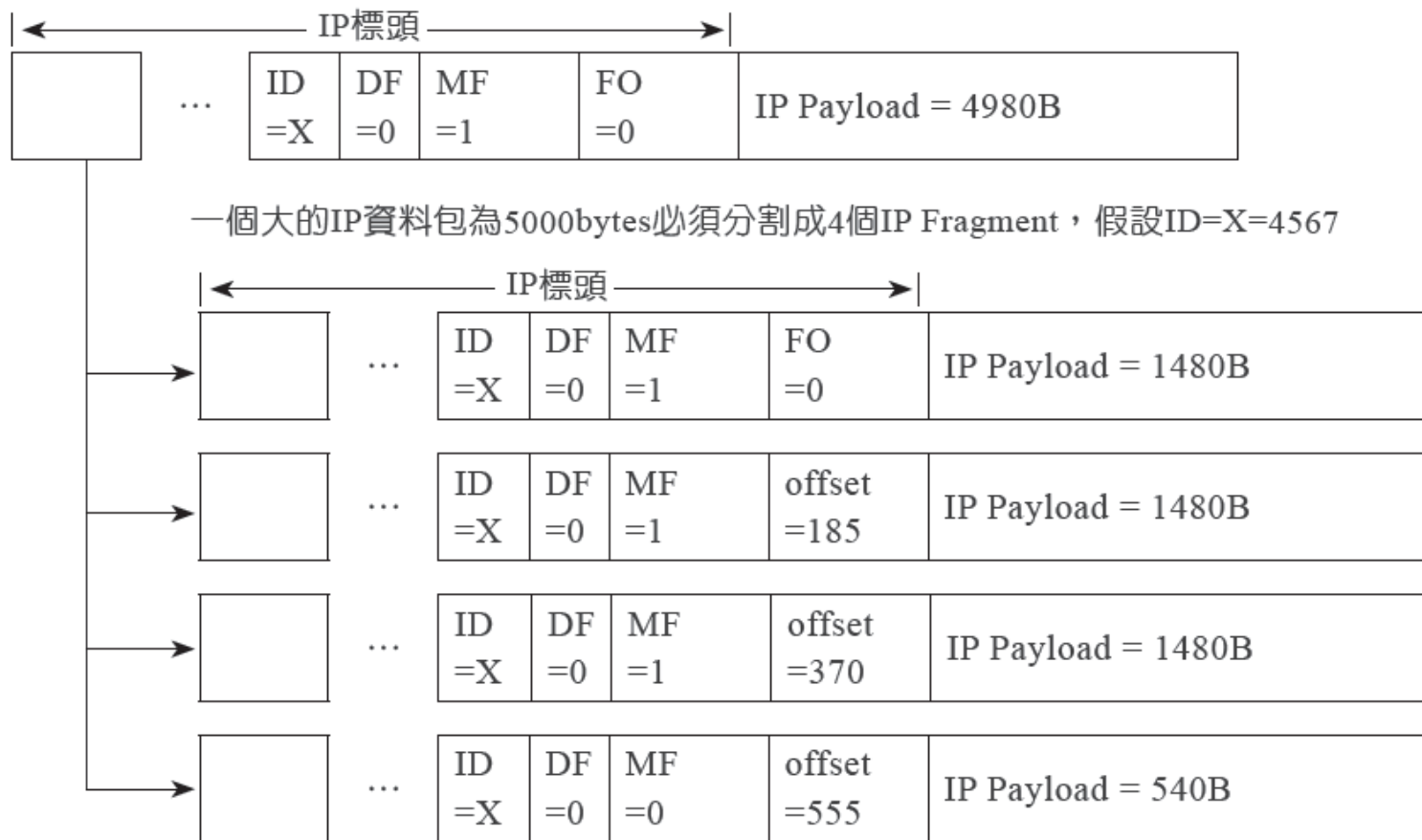
8-11

8-12

8-13

習題

8-8 IP 封包格式



●圖8-12 一IP封包太大，需要分割產生4個IP Fragment

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-8 IP 封包格式

► Flag(旗標)佔3bits

- 共有3個參數，每參數由1 bit來表示。
- 第1個參數為保留(以0表示)，第2個參數為DF(0表示封包可分割；
- 1表示封包不可分割)，MF(More Fragment)為1，表示資料包分割後的其中一個封包；MF為0表示封包分割後的最後一個封包。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-8 IP 封包格式

► Identification (ID)佔16bits

- 記錄IP封包的識別碼。
- 識別碼由來源主機決定，按照IP封包發出的順序遞增1。由於每個IP封包所走的路徑可能不一樣，因此到達目的端主機的先後順序也可能會與出發時的順序不同，目的端可利用Identification(識別)欄位，判斷IP封包並組合成為原來的順序。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-8 IP 封包格式

► 生存期(TTL ; Time to Live)佔8bits

- 為了避免IP封包會有意外到不了目的端，因而以TTL欄位來記錄IP封包的存活時間，它限制IP封包在路由器之間轉送的次數。最大初值設定為255，每經過一部路由器時，路由器便會將TTL欄位值減1。
- 當路由器收到TTL=0的IP封包時，就直接將它丟棄，不再傳送出去。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-8 IP 封包格式

► 協定(PROT ; Protocol)佔8bits

► 用來記錄上層所使用的協定種類。

► 常見的Protocol識別值如下所示：

1 (ICMP) , 2 (IGMP) , 3 (GGP) , 6 (TCP) , 8 (EGP) , 9 (IGP) , 17 (UDP) , 41 (IPv6) , 47 (GRE) , 50 (ESP) , 51 (AH) , 88 (EIGRP) , 89 (OSPF) 。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-8 IP 封包格式

▶ 標頭檢查和 (Header Checksum ; HC) 佔 16bits

▶ 用以檢查標頭內容是否正確。IP標頭檢查和計算過程如下說明：

▶ 發送端先在此欄位全部填入0，並對IP標頭以16bits為單位，經過檢查碼演算法進行加總，再將得出的結果取1的補數，正是所要找出的HC。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-8 IP 封包格式

▶ 標頭檢查和(Header Checksum ; HC) 佔16bits

- ▶ 當接收端收到此IP封包時，就進行如同在發送端的計算方式，但此時標頭檢查和欄位不再全部填入0，而是填入剛從發送端算出來的HC之值進行加總，得到的結果值若為0，表示該IP封包從發送端送到接收端沒有發生錯誤；反之，則IP封包發生問題。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-8 IP 封包格式

▶ 來源端位址(Source Address ; SA)佔32bits

- ▶ 是用來記錄來源主機的IP位址。

▶ 目的端位址(Destination Address ; DA) 佔32bits

- ▶ 這是用來記錄目的主機IP位址。

▶ Options(選項)與Padding

- ▶ 長度不定，此欄位可進行偵錯與測試。Options大都用在除錯或量測。因Options長度不是4bytes的倍數，因而設計Padding欄位，讓Options與Padding加起來剛好是4bytes的倍數。Padding欄位不管長度為何，資料填補時一律填入0。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-8 IP 封包格式-範例4

► 利用圖8-12說明圖8-13的ID、MF及FO關係。

► 解：

► 以圖8-12來說，假設其ID等於4567，因原始的IP資料包佔5000bytes，所以IP Payload長度為4980bytes(看成一個較大資料包)，則可分割成4個IP Fragment(即4個小資料包)，而每一個IP Fragment的ID均等於4567。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-8 IP 封包格式-範例4

- ▶ 至於4個MF，依序為1、1、1、0，FO如圖8-11所示依序為0、185、370、555。注意：ID、MF、FO為IP封包分割與重組時所需的重要資訊，藉由這3個欄位，目的端主機便可將圖8-12的4個IP Fragment重組成為原始的IP資料包，如圖8-13所示。注意，DF值此時因處在封包分割狀態，故DF皆=0。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

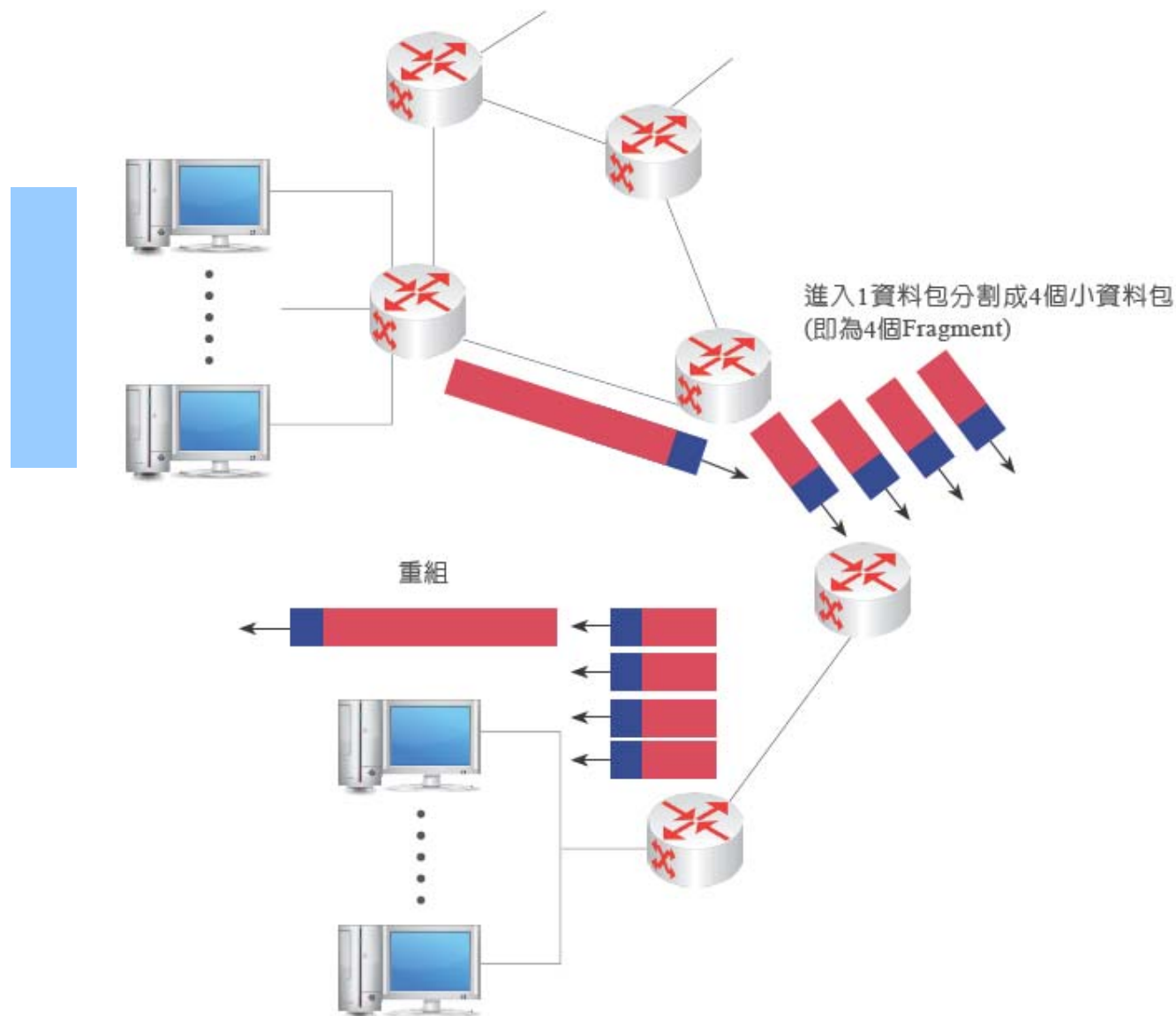
8-10

8-11

8-12

8-13

習題



●圖8-13 IP Fragment被重組成為原始的IP封包

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-9 IP封包的擷取分析

- ▶ IP封包的擷取方式可以利用手提電腦內的瀏覽器向Google網站連線並隨意下載一些資料做說明。為說明方便，透過Wireshark工具程式抓取所要的IP封包，並在封包內容列的IP層點兩下再進行對IP標頭欄位分析，如圖8-14所示。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-9 IP封包的擷取分析-IP標頭欄位分析

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

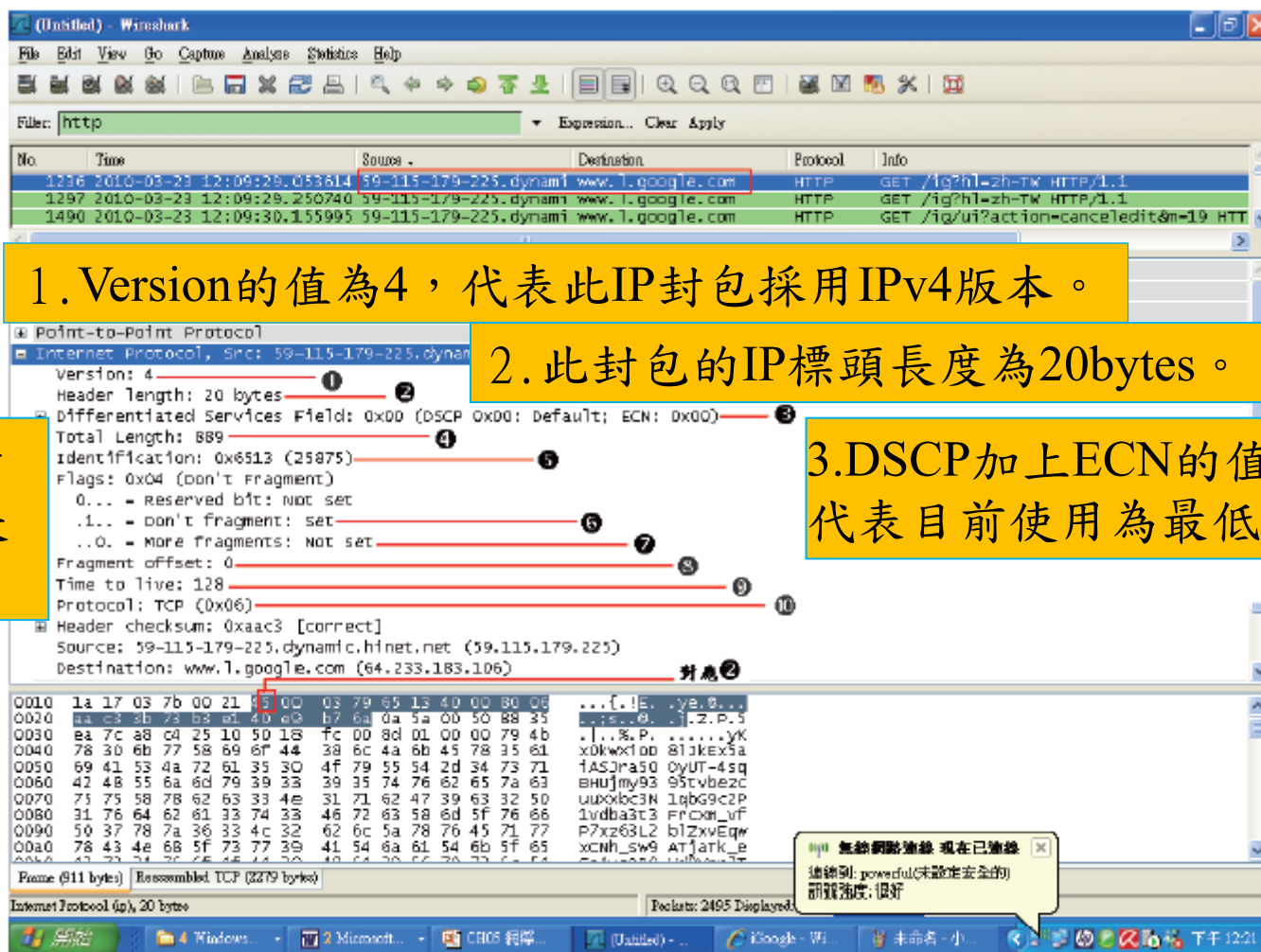
8-10

8-11

8-12

8-13

習題



1. Version的值為4，代表此IP封包採用IPv4版本。

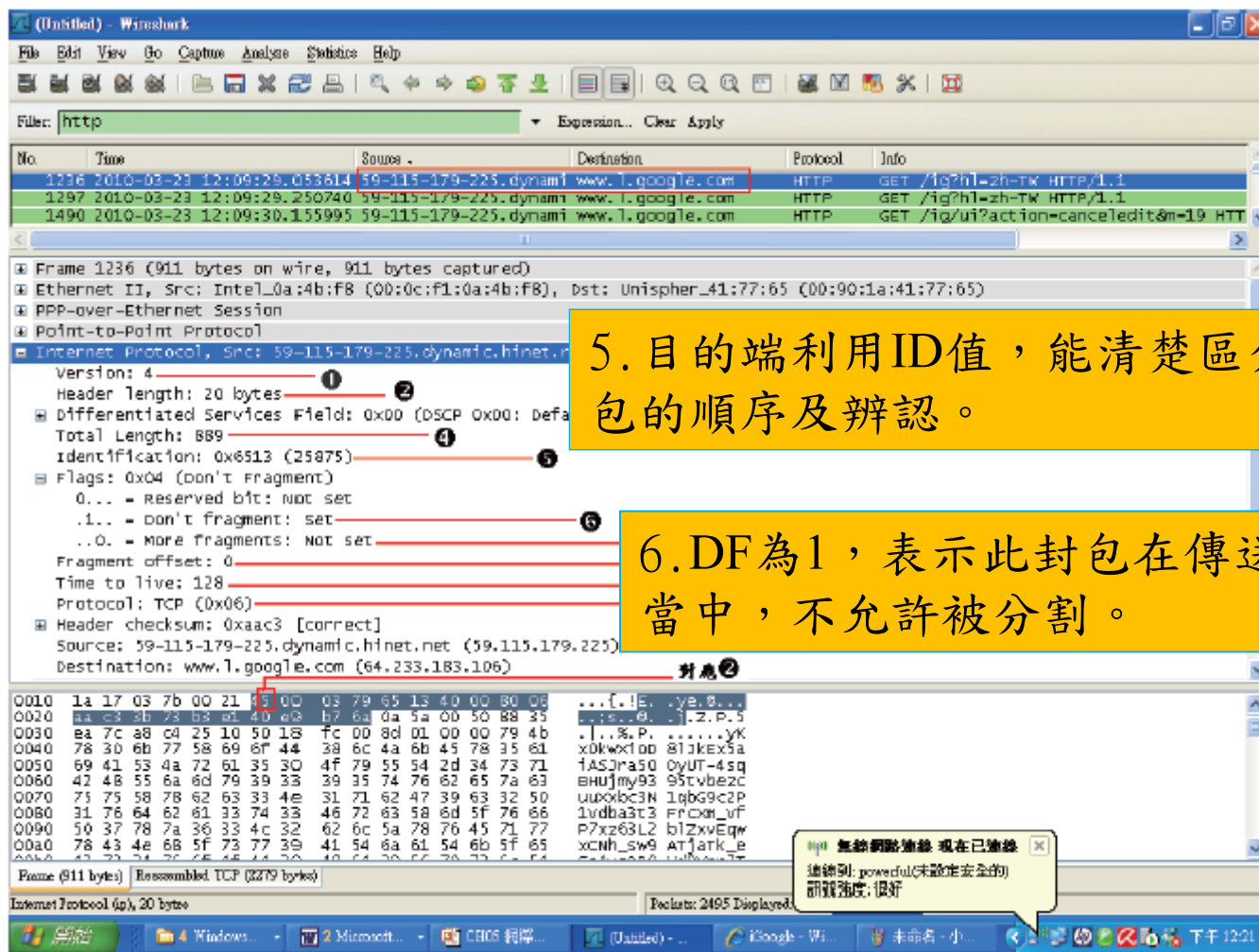
2. 此封包的IP標頭長度為20bytes。

4. 此IP封包的總長度。

3.DSCP加上ECN的值為0x00，代表目前使用為最低優先權。

圖8-14 IP標頭欄位分析

8-9 IP封包的擷取分析-IP標頭欄位分析



●圖8-14 IP標頭欄位分析

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-9 IP封包的擷取分析-IP標頭欄位分析

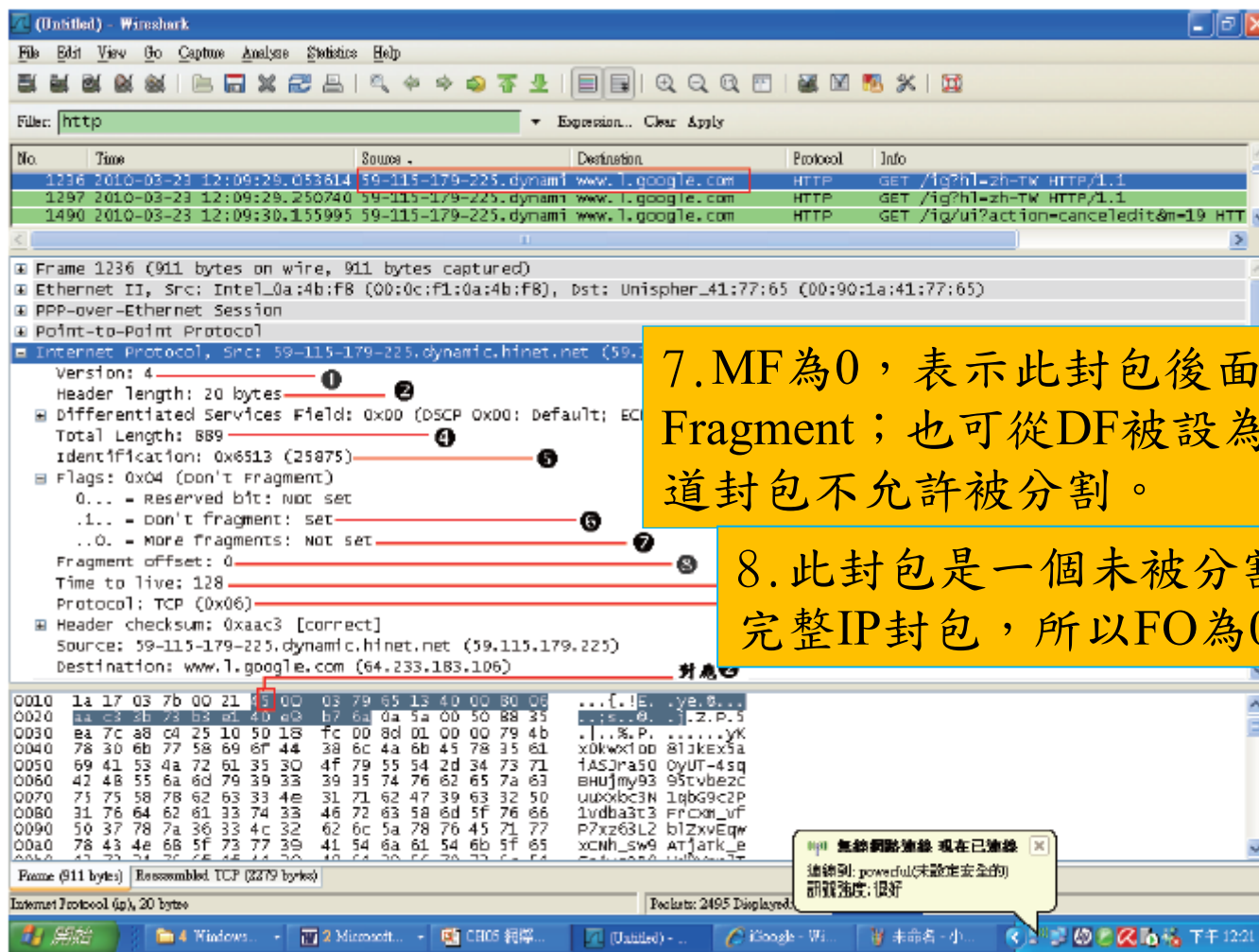


圖8-14 IP標頭欄位分析

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-9 IP封包的擷取分析-IP標頭欄位分析

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

Wireshark packet capture analysis of an IP header. The packet list shows an HTTP GET request. The packet details pane shows the IP header fields with numbered annotations 1 through 10. The packet bytes pane shows the raw hex and ASCII data. A yellow box highlights the TTL field (128) and the Protocol field (6, TCP).

9. IP封包的生存期間。

10. 指出上一層所使用的通訊協定為TCP。若為UDP，此值應該是0x11(十進位17)。

●圖8-14 IP標頭欄位分析

8-9 IP封包的擷取分析-範例5

說明圖8-14中的第6~8(對應的16進位值為4000 ; 另外，標頭檢查和值等於0xaac3)的演算過程。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-9 IP封包的擷取分析-範例5

- 解：圖8-14標頭長度為典型長度，佔20bytes；我們可以在圖中的封包內容列點選「Internet Protocol」，就可以得出20bytes的標頭長度如圖8-14中的最下視窗16位元格式列顯示出的反白數字，它是以16進位表示

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-9 IP封包的擷取分析-範例5

► 解：圖中的第6~8對應的16進位值代表標頭資料「4000」，它是由圖8-13中的「Flag」所指的3個位元，依序為bit 15、bit 14、bit 13等於010，加上「Fragment offset」13個位元，依序為bit 12、bit 11、bit 10.....bit0等於0000000000000000，總共16個位元，等於01000000000000000000，轉換成16進位，得出0x4000。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-9 IP封包的擷取分析-範例5

► **解**：接著我們要求出發送端標頭檢查和等於0xaac3的演算過程：首先將16進位表示的IP標頭長度每2bytes為一組，共分為10組的資料，再轉成2進位，如圖8-15(a)所示。

► **注意**：在圖8-15(a)中的第6組(標頭檢查和欄位的初始值)必須先全部填入0

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-9 IP封包的擷取分析-範例5

► 解：一旦求出標頭檢查和等於0xaac3後，還會隨IP資料包一起被傳送出去，當接收端收到此IP封包時，就進行如同在發送端的計算方式。但此時，第6組的標頭資料計算檢查和欄位不再全部填入0，而是填入剛從發送端算出來的0xaac3之值再進行加總，得到的結果值等於0，表示沒有發生錯誤，如圖8-15(b)所示。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-9 IP封包的擷取分析-範例5

組別	標頭資料(16進位)	運算	2進位表示
1	45 00		0100 0101 0000 0000
2	03 79	+	0000 0011 0111 1001
			0100 1000 0111 1001
3	6513	+	0110 0101 0001 0011
			1010 1101 1000 1100

圖8-15(a) 發送端標頭檢查和等於
0xaac3的演算過程

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

組別	標頭資料(16進位)	運算	2進位表示
4	40 00	+	0100 0000 0000 0000
			1110 1101 1000 1100
5	80 06	+	1000 0000 0000 0110
		產生溢位1	0110 1101 1001 0010
		加1	0110 1101 1001 0011
6	00 00	+	0000 0000 0000 0000
			0110 1101 1001 0011
7	3b 73		0011 1011 0111 0011
		+	1010 1001 0000 0110
8	b3 e1		1011 0011 1110 0001
		產生溢位1	0101 1100 1110 0111
		加1	0101 1100 1110 1000
9	40 e9		0100 0000 1110 1001
			1001 1101 1101 0001

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

圖8-15(a) 發送端標頭檢查和等於0xaac3的演算過程

8-9 IP封包的擷取分析-範例5

組別	標頭資料(16進位)	運算	2進位表示
10	b7 6a		1011 0111 0110 1010
		產生溢位1	0101 0101 0011 1011
		加1	0101 0101 0011 1100
標頭檢查和	aac3	取1's補數	1010 1010 1100 0011

圖8-15(a) 發送端標頭檢查和等於
0xaac3的演算過程

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-9 IP封包的擷取分析-範例5

組別	標頭資料(16進位)	運算	2進位表示
1	45 00		0100 0101 0000 0000
2	03 79	+	0000 0011 0111 1001
			0100 1000 0111 1001
3	6513	+	0110 0101 0001 0011
			1010 1101 1000 1100
4	40 00	+	0100 0000 0000 0000
			1110 1101 1000 1100
5	80 06	+	1000 0000 0000 0110
		產生溢位1	0110 1101 1001 0010
		加1	0110 1101 1001 0011

圖8-15(b) 接收端標頭檢查和的演算過程

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-9 IP封包的擷取分析-範例5

組別	標頭資料(16進位)	運算	2進位表示
6	aac3	+	1010 1010 1100 0011
		產生溢位1	0001 1000 0101 0110
		加1	0001 1000 0101 0111
7	3b 73	+	0011 1011 0111 0011
			0101 0011 1100 1010
8	b3 e1	+	1011 0011 1110 0001
		產生溢位1	0000 0111 1010 1011
		加1	0000 0111 1010 1100
9	40 e9		0100 0000 1110 1001
			0100 1000 1001 0101
10	b7 6a		1011 0111 0110 1010
			1111 1111 1111 1111
標頭檢查和		取1's補數	0000 0000 0000 0000

●圖8-15(b) 接收端標頭檢查和的演算過程

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-10 IP路由

- ▶ 什麼是IP路由？簡單的說，在網路之間將IP封包(或稱IP資料包)傳送到目的節點的過程即稱為IP路由。
- ▶ 除非IP資料包是在同一個網路內互相傳送，就不需要透過網路的裝置——路由器，否則在傳送IP資料包時，就必須經歷IP路由的過程。
- ▶ 要了解IP路由，首先必須了解路由器：路由器在實體上可連結多個網路，還必須具有能夠轉送IP資料包的能力，以達到將IP封包送達目的節點。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-10 IP路由

► 路由器必須具有以下特性：

1. 具有兩個(或以上的)網路介面。所謂網路介面就是指所有可連接網路的裝置，像電腦上的網路卡。
2. 具有OSI模型第3層功能的資訊分析能力。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-10 IP路由

- ▶ IP路由器具具有路由表登錄功能。這樣路由器才能判斷要將IP封包轉送(forward)到哪一個網路，並為IP資料包選擇出最佳的路徑。
- ▶ 所謂路徑包含了兩種重要因素：
 1. 路徑位於路由器的哪一個網路介面。
 2. 路徑的下一部路由器。
- ▶ 如果目的節點是直接連接於路由器的網路上，就將IP資料包直接送至目的節點，而不必再轉送給其他路由器。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

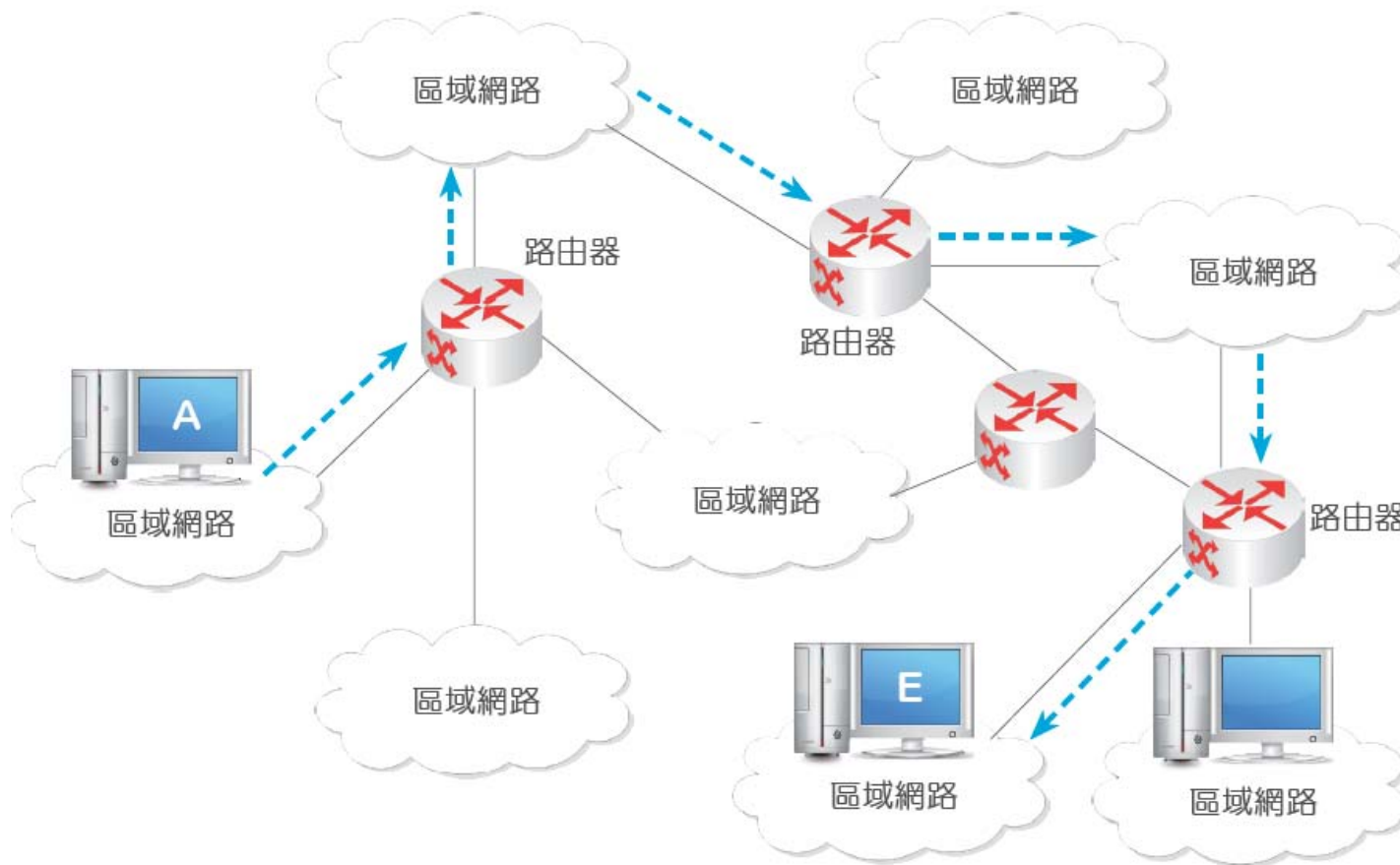
8-11

8-12

8-13

習題

8-10 IP路由



●圖8-16 IP封包由電腦A端送到E端

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-10 IP路由-範例6

分析圖8-17的IP路由的過程。

解：如下說明：

1. John的主機在送出IP封包前，先將IP封包內的目的地位址與本身的路由表比對，以便判斷Marry主機之位置。若John的主機和Marry的主機位於同一個LAN，John會利用ARP(位址解析協定)取得Marry的MAC位址，然後IP封包可直接送給Marry。
2. 反之，John的主機從路由表判斷IP封包應由哪一部路由器送出。此例中，John的主機會利用ARP取得R1路由器的網路介面MAC位址，再將IP封包送給R1。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-10 IP路由-範例6

3. 一旦R1路由器收到IP封包時，會讀取IP封包標頭的資訊。若TTL值大於1，則先減1後並讀取目的端的IP位址(即Marry主機的IP位址)，再根據目的端的IP位址，以及R1路由器本身的路由資訊選擇出一條適當路徑；若TTL的值等於0，路由器就停止轉送此IP封包，並將它丟棄。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-10 IP路由-範例6

4. 若Marry的主機位置坐落在R1所連接的A、B或C網路中，透過ARP得到Marry主機的實體位址(即MAC位址)，IP封包就可送給Marry。
5. 反之，Marry的主機位置坐落在D、E或F網路，根據路由表，IP封包會被轉送至R2路由器。然後R1再透過ARP取得R2路由器的MAC位址，IP封包就轉送至R2路由器。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

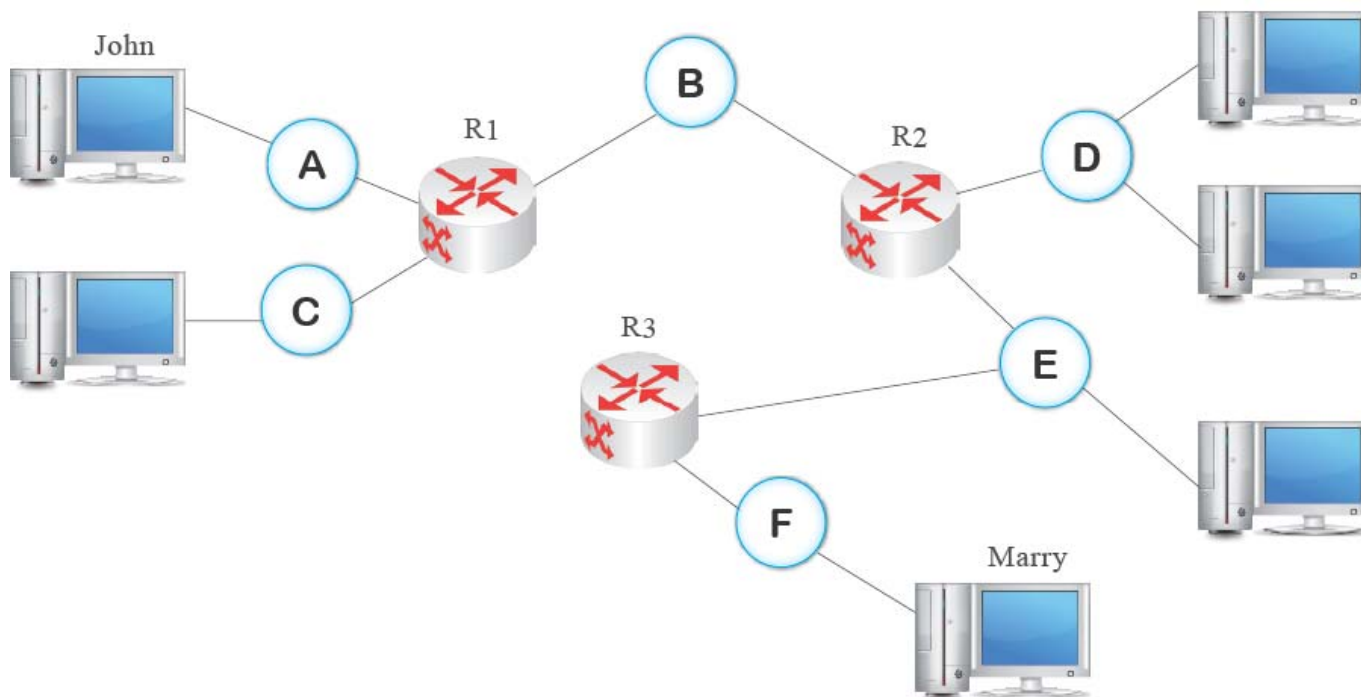
8-12

8-13

習題

8-10 IP路由-範例6

6. 如同R1路由器之操作，R2路由器會將IP封包轉送至R3路由器。一旦R3路由器透過ARP取得Marry的MAC位址，John的IP封包就可傳送給Marry。



8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

圖8-17 IP封包路由典例

8-11 IPv6簡介

- ▶ 由於現實情況對於IP位址的需求愈來愈多，在可預見的未來，IPv4位址的數量恐怕會不夠用，根據IETF工作小組估計，IPv4位址將在2018年使用殆盡。
- ▶ 特別是近幾年來，寬頻電信及網路服務量不斷提升，加上無線網路技術、4G等應用，IP位址的需求量更加速成長。為了解決這個惱人的問題，加上各方面的考量，下一版的IP版本——IPv6就被發展出來。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11 IPv6簡介

► 改用IPv6的主要理由如下：

- IPv6的IP位址是由128bits所組成， 2^{128} 比IPv4位址增加79個千的9次方，這保證了未來世界絕不會有IP位址欠缺之問題。有興趣請參考RFC 2373。
- IPv6具有不需人為設定的情形下，可讓電腦自動向路由器取得IPv6位址的自動定址(auto-configuration)機制。
- IPv6整合了當前廣泛為人使用的IPSec(IP Security)加密協定，保密性很好。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11 IPv6簡介

- ▶ IPv6封包的標頭長度為固定的40bytes，因此在處理與轉送上可以更快速；標頭的改良也增加QoS功能。
- ▶ IPv6有IPv4所無法滿足的技術，如可移動性(mobility)、階層性位址架構、高封包轉送效能等。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11 IPv6簡介

- ▶ IPv6位址分成8段(segment)，每段由16bits組成，各段間以冒號(:)隔開，例如1A25 : 23CB : 2C45 : ED11 : 3FD2 : 0000 : A012 : 89AB，各數字代表16進位。為了方便表示IPv6位址，開頭的0可以不寫，例如：0A1B簡化為A1B；000C簡化為C。
- ▶ 另外，0000可以省略掉，例如A123 : 0000 : 0000 : 0000 : 0000 : 0000 : 0005 : 00CD簡化為A123 : : : : : 5 : CD。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11 IPv6簡介

- ▶ 注意：雙冒號表示連續、數個不固定的0。假如位址為2A35 :: A126 :: AB22，有可能是2A35 : 0 : 0 : 0 : A126 : 0 : 0 : AB22或2A35 : 0 : 0 : A126 : 0 : 0 : 0 : AB22；為避免使用者錯誤解讀，故只能限用1次雙冒號。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

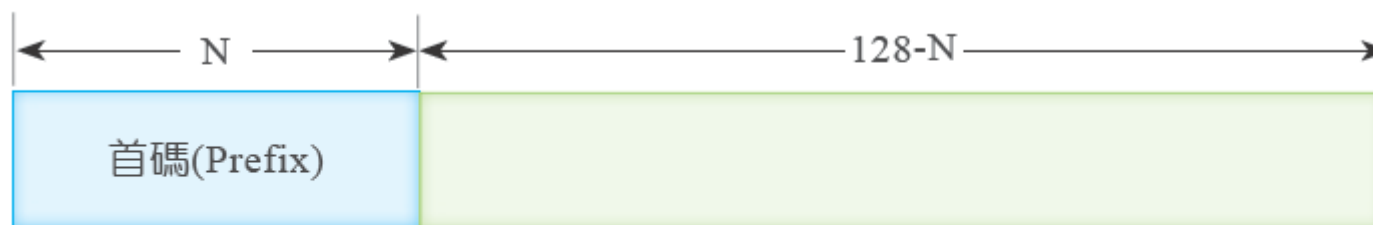
8-12

8-13

習題

8-11 IPv6簡介

- ▶ 另一種IPv6位址表示為「IPv6位址/首碼長度」，如圖8-18所示，在128位元的IPv6長度中，首碼(prefix)佔有Nbits，首碼長度依位址的類型分為Unicast、Multicast和Anycast三種類型，例如1234::2ADC:9A1B/8，首碼長度佔8bits。



●圖8-18 另一種IPv6 位址格式表示

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11 IPv6簡介

- ▶ 在圖8-18中的前置碼N可以看成Net ID，128-N 可以看成 Host ID。在 IPv4 若為 192.168.1.0/24 中的 /24 代表 Net ID 為 192.168.1.0，net mask為255.255.255.0
- ▶ 但在IPv6因結構關係只使用前置碼來表示。例如2001 : 0CA2 : 65DB : 7DAC :: 1/64其中Net ID(網路位元部分)為2001 : 0CA2 : 65DB : 7DAC，及Host ID主機位元部份為0000 : 0000 : 0000 : 0001。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11 IPv6簡介

- ▶ IPv6不同前置碼的網路位元部分與主機位元部份將依下列原則可決定出來：
- ▶ 1. 網路位元是16的倍數，網路位元部分與主機位元部份是以組(16位元為一組)數決定長度。
- ▶ 2. 網路位元是4的倍數，網路位元部分與主機位元部份是以16位元決定長度。
- ▶ 3. 網路位元非4的倍數，網路位元部分與主機位元部份是以2進位位元決定長度。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11 IPv6簡介-範例7

- ▶ 寫出下列IPv6的網路位元部分與主機位元部份。
- ▶ 解：
- ▶ 1. 2001::1/96 表示網路位元佔96 bits及主機位元佔32 bits。例如網路部分佔6組($96 \div 16$)為2001:0:0:0:0:0及主機部份為0:1。
- ▶ 2. 2001:1/80 表示網路位元佔80 bits及主機位元佔48 bits。例如網路部分佔5組($80 \div 16$)為2001:0:0:0:0及主機部份為0:0:1。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11 IPv6簡介-範例7

▶ 解：

- ▶ 3. 2001:1/8 表示網路位元佔8 bits及主機位元佔120 bits。例如網路部分佔16 bits的一半為20(即)及主機部份為NN01:0:0:0:0:0:0:1，其中N表示空值。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11 IPv6簡介-範例7

- ▶ 4. 2001:1/4 表示網路位元佔4 bits及主機位元佔124 bits。例如網路部分佔16 bits的四分之一為2及主機部份為N001:0:0:0:0:0:0:1，其中N表示空值。
- ▶ 5. 2001:1/3 表示網路位元佔3 bits及主機位元佔125 bits。此部份要先將2001轉換成二進位0010 0000 0000 0001，所以網路部分佔3 bits為001，其他佔125 bits則為主機部份。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11 IPv6簡介

► IPv6位址的分類如下說明：

- Unicast(單播位址)：適用於單一節點間的資料傳送。
- Multicast(群播位址)：適用於單一節點對多個節點間的資料傳送。
- Anycast(任播位址)：它是IPv4的Unicast與Broadcast(多點廣播)的綜合。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11-1 IPv6封包的標頭欄位

- IPv6封包如同IPv4封包，也是由標頭(長度為40bytes)和資料欄兩部分所組成，如圖8-19所示（參考RFC 2460）。

Version (4)	Traffic Class (8)	Flow Label (20)
Payload Length (16)	Next Header (8)	Hop Limit (8)
Source Address (128)		
Destination Address (128)		
資料		

●圖8-19 IPv6的封包格式

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11-1 IPv6封包的標頭欄位

- ▶ Version佔4bits：表示Internet Protocol的版本號碼。
- ▶ 訊務等級(Traffic Class)佔8bits：表示封包的類別或優先權，如同IPv4的TOS的功能。
- ▶ 資料流標記(Flow Label)佔20bits：用來識別資料封包的資料流。
- ▶ 酬載長度(Payload Length)佔16bits：記錄資料封包的長度。注意，IPv4封包總長度有包含標頭的長度。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11-1 IPv6封包的標頭欄位

- ▶ 內層標頭(Next Header)佔8 bits：此欄位能識別在IPv6標頭之後，是哪一種型態的標頭，也如同IPv4標頭中的PROT欄位的功能。另一功能是作為擴充標頭，可以存放IPv6通訊所需的擴充資料。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11-1 IPv6封包的標頭欄位

- ▶ 躍程限制(Hop Limit)佔8bits：每一路由器轉送一個資料封包時，欄位內容就減1，直到0時，封包就會被丟棄。
- ▶ 來源端位址佔128bits：是用來記錄來源主機的IP位址。
- ▶ 目的端位址佔128bits：用來記錄目的端主機的IP位址。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11-1 IPv6封包的標頭欄位

- ▶ 原存在於IPv4封包中的欄位，像分割 / 重組 (Fragmentation/Reassembly)、標頭檢查和及 Options(選項)欄位已不再存在於IPv6 的封包中，簡述如下：

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11-1 IPv6封包的標頭欄位

- ▶ (1) 分段 / 重組 (Fragmentation/Reassembly)
- ▶ IPv6 並不允許路由器進行分割跟重組；這些操作只能由來源端與目的端來進行。如果路由器收到進來的IPv6的封包太大，而無法轉送時，路由器會丟棄封包，然後送出「封包太大」的ICMP 錯誤訊息回送給發送端。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11-1 IPv6封包的標頭欄位

- ▶ (2) 標頭檢查和(header checksum)
- ▶ 因為IPv4標頭包含TTL欄位(類似IPv6的躍程限制欄位)，所以每台路由器都必須重新計算IPv4的標頭檢查和，這也是IPv4其中一項付出的代價。IPv6設計者認為傳輸層與數據鏈路層都有執行檢查和計算，所以刪除標頭檢查和的計算以能快速處理封包。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11-1 IPv6封包的標頭欄位

- ▶ (3) Options欄位
- ▶ Options欄位不再是標準IP標頭的一部分，然而，它並沒有消失。取而代之的是，Options欄位變成了IPv6標頭的內層標頭欄位可能指向的欄位之一。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11-2 IPv4和IPv6間的轉換

- ▶ IETF提出3種IPv4與IPv6轉換技術，分別是
 - ▶ 雙重堆疊架構(dual-stack)
 - ▶ 隧道(tunneling)技術
 - ▶ 網路位址與協定轉換 (Network Address Translation-Protocol Translation ; NAT-PT)。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11-2 IPv4和IPv6間的轉換-雙重堆疊架構

- ▶ 在RFC 4213規定，節點同時能傳送與接收IPv4/IPv6兩種封包；即IPv4/IPv6與IPv4節點互動時，可以使用IPv4協定；若與IPv6節點互動時，IPv4/IPv6節點可以使用IPv6協定。
- ▶ 然而，若送收其中一方只能使用IPv4，則這類型的架構即使中間某兩節點是使用IPv6，最後得到的依然還是IPv4資料包，如圖8-20所示。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

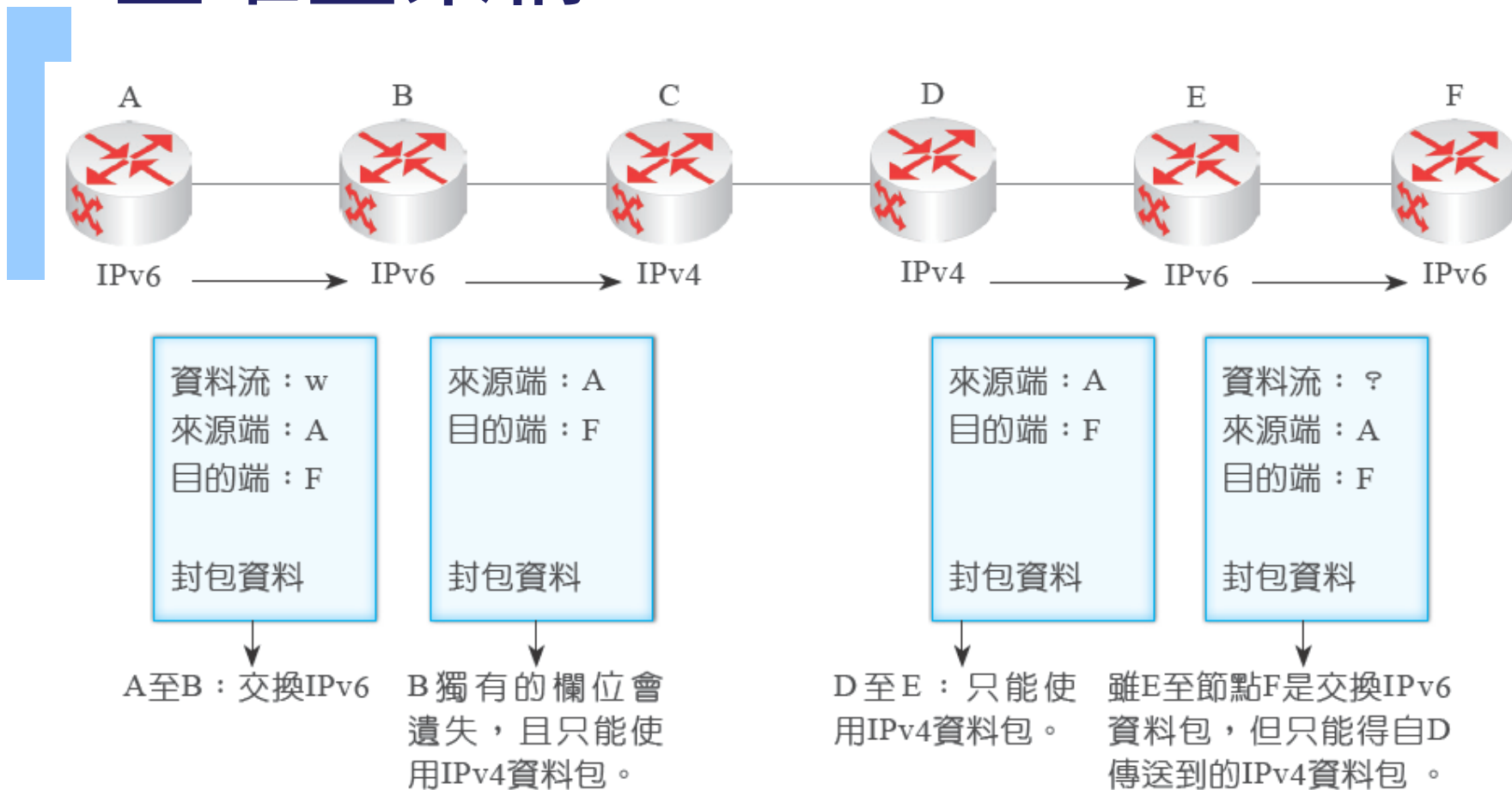
8-11

8-12

8-13

習題

8-11-2 IPv4和IPv6間的轉換-雙重堆疊架構



●圖8-20 雙重堆疊架構

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11-2 IPv4和IPv6間的轉換-隧道技術

- ▶ 圖8-20的問題可利用隧道技術解決。即當節點B的IPv6封包進入節點C時(即IPv4協定的網域時)，將IPv6封包當作資料，並在前面加上IPv4標頭，再送入節點D的IPv4網域。
- ▶ 當資料包由節點D的IPv4網域離開，進入節點E的IPv6網域時，再將IPv4的標頭移除，並還原為原來的IPv6封包，像這樣的情形稱為隧道技術，即網路的兩端是IPv6協定網域，而中間節點(節點C與節點D)都是IPv4協定的網域，正是所謂的隧道。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

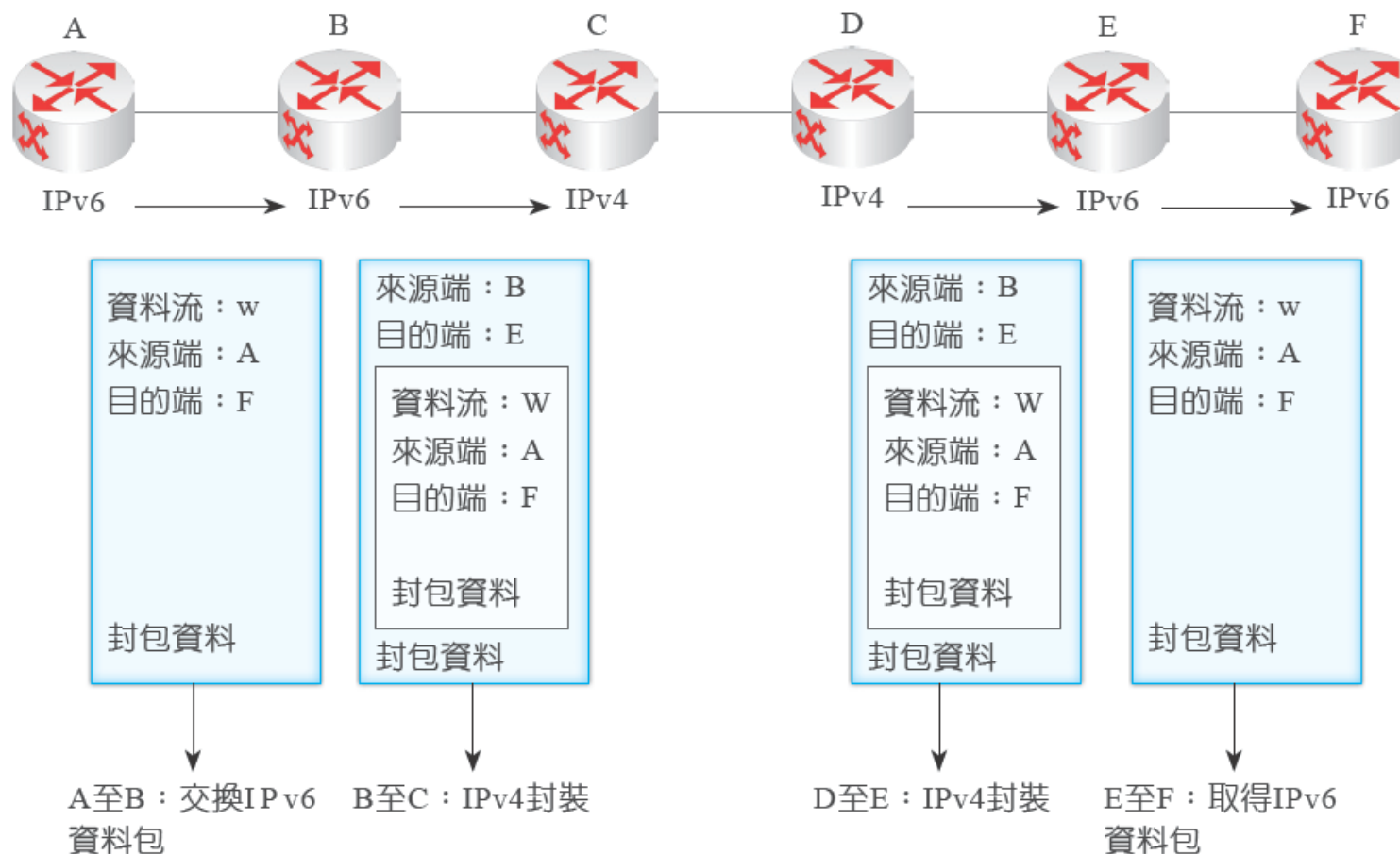
8-11

8-12

8-13

習題

8-11-2 IPv4和IPv6間的轉換-隧道技術



●圖8-21 隧道技術

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11-2 IPv4和IPv6間的轉換- NAT-PT

- ▶ 此技術必須將封包的欄位做相對應的轉換。例如：當資料包是IPv6協定時，其資料包的欄位會對應到IPv4資料包的欄位，並因而轉換成IPv4資料包。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-11-2 IPv4和IPv6間的轉換- NAT-PT

- ▶ 同樣的，IPv4的資料包要轉換成IPv6的資料包亦是透過欄位相對應的轉換方法。NAT-PT技術也可使用於純IPv6與純IPv4網域的連結，透過通訊協定的完全轉換，使得封包可以在完全的IPv4網域或IPv6網域傳送。有關NAT-PT可參考RFC 2766。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-12 IP Spoofing

- ▶ 所謂的IP Spoofing主要是讓攻擊封包看起來會讓人誤以為它來自可信任的網域，而允許其進入路由器或防火牆(firewall)，最後達成直接攻擊受害者主機的目的。
- ▶ IP Spoofing亦稱為IP欺騙，其原理是攻擊者使用偽造的來源位址來傳送IP封包，由於這不存在的來源IP位址向受害者發送SYN封包，要求建立TCP連線。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-13 IPv6 安全性

- ▶ 新的網路層協定將提供各式各樣的安全性服務。這些協定的其中一種是IPsec(Internet Protocol Security)
- ▶ 這是種較常用的安全網路層協定，它也被廣為部署在虛擬私人網路(Virtual Private Network, VPN)中。
- ▶ (IPSec)原本是為IPv6開發，但是在IPv4中已被大量部署使用。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-13 IPv6 安全性

- ▶ 安全問題始終是Internet的一個重要話題。由於IP協定在設計之初沒有考慮安全性，因而常發生網路遭到攻擊，為了加強Internet的安全性，1995年開始IETF著手研究制定了一套用於保護IP通訊的IP安全協定稱為IPSec。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-13 IPv6 安全性

- ▶ IPSec是IPv4的一個可備選的擴展協定，也是IPv6組成的一部分。
- ▶ IPSec的主要功能是在網路層對資料分組提供加密和鑒別等安全服務，它提供了兩種安全機制：認證和加密。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-13 IPv6 安全性

- ▶ 認證機制使IP通訊的資料接收方能夠確認資料發送端的真實身份以及資料在傳輸過程中是否遭到更動。加密機制是通過對資料進行編碼來保證資料的機密性，以防止資料在傳輸過程中被他人竊取而失密。
- ▶ IPsec會談所提供的服務包括：密碼協商、IP資料報內容的加密、來源認證與資料完整性。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

本章習題

- ▶ (1) 1. IP位址23. 22. 17. 34，可判斷此IP位址為分級網路中的 (1)Class A (2)Class B (3)Class C (4)Class D。
- ▶ (1) 2. 有一個網路的IP位址為196.165.11.25/24，其中的24代表該網路有 (1)24部電腦 (2)24個1 (3)24個0 (4)24部伺服器。
- ▶ (2) 3. 有一個網路的IP位址為196.165.11.25/26，代表可切割成 (1)2 (2)3 (3)4 (4)8 個子網路。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

本章習題

- ▶ (3) 4. Class C最左邊的最高位元固定為何？ (1)0
(2)10 (3)110 (4)1110。
- ▶ (3) 5. Class B最左邊的最高位元及次位元固定為何？
(1)0 (2)10 (3)110 (4)1110。
- ▶ (2) 6. 196.165.11.25/24的主機數目為何？ (1)126
(2)254 (3)510 (4)1022。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

本章習題

- ▶ (4) 7. 一個網路的IP位址為196.165.11.25/X，表示有510個主機位址，請問X的數值為何？ (1)20 (2)21 (3)22 (4)23。
- ▶ (3) 8. 一個網路位址為176.16.0.0，在一個B級中切割子網路有2048個，請問子網路遮罩為何？
(1)255.255.0.0 (2)255.255.255.0
(3)255.255.255.224 (4)255.255.255.240。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

本章習題

- ▶ (1)9. 一個網路位址為176.16.0.0，在一個B級中切割子網路有4096個，請問有幾個主機位址？ (1)14 (2)30 (3)62 (4)126。
- ▶ (2)10. 一個公司有192.170.22.0/24、192.170.23.0/24、192.170.24.0/24及192.170.25.0/24共4個網路，下列何值透過Supernet可以將這4個網路合併為一個較大網路？ (1)192.170.22.0/21 (2)192.170.22.0/22 (3)192.170.22.0/23 (4)192.170.22.0/24。

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

8-1

8-2

8-3

8-4

8-5

8-6

8-7

8-8

8-9

8-10

8-11

8-12

8-13

習題

- ▶ (3)11.IPv6的位址是由多少 bits所組成
(1) 32 bits (2)64bits (3) 128bits (4)
256bits
- ▶ (3)12.IPv6封包的標頭長度為
(1) 20bytes (2)32bytes (3)40bytes (4)
48byres