

## CHAPTER 09



# ARP/RARP/ICMP協定

- ▶ 9-1 ARP操作原理
- ▶ 9-2 ARP cache(快取)
- ▶ 9-3 RARP操作原理
- ▶ 9-4 ARP/RARP封包格式
- ▶ 9-5 ARP工具程式
- ▶ 9-6 ARP封包的擷取分析
- ▶ 9-7 ICMP簡介
- ▶ 9-8 ICMP訊息格式
- ▶ 9-9 ICMP工具程式測試
- ▶ 9-10 ICMP封包的擷取分析

## 9-1 ARP操作原理

- ▶ ARP是Address Resolution Protocol的縮寫，中文稱之為位址解析協定。
- ▶ ARP定義在RFC 826標準，在Internet協定中屬於網路層的協定，主要是用來解析IP位址或是主機名稱所對應的實體位址(MAC位址)。
- ▶ 如果IP工作於網路層，而數據鏈路層使用乙太網路時，則利用ARP可取得對應的MAC位址。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-1 ARP操作原理

- ▶ 假設圖9-1的主機為本地網路主機，其中所示主機A要傳送IP封包給主機B，因此必須先利用ARP取得主機B的MAC位址，其位址為「00:1d:92:a2:d7:3c」，它的工作原理如下面步驟說明。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-1 ARP操作原理

- **步驟1**：每一部主機(或稱電腦)都會在ARP快取(ARP cache)緩衝區中建立一個ARP表格，主要用來記錄IP位址和實體位址的對應關係，亦即將IP/MAC位址對應關係記錄在本機電腦上的記憶體內。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-1 ARP操作原理

► **步驟2**：當主機A在已知道主機B的IP位址情況下要將封包傳送給主機B時，主機A會先檢查自己的ARP表格中是否有該IP位址的MAC位址對應。如果有，就直接使用此位址來傳送封包；反之，則主機A會廣播ARP request封包給區域網路上所有的主機，以便查詢目的主機B的MAC位址。這個廣播封包會包含主機A本身的IP位址和實體位址，以及目的主機B的IP位址。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-1 ARP操作原理

► **步驟3**：此時網路上所有的主機都會收到此廣播封包，每部主機會檢查自己的IP位址是否和廣播封包中的IP位址（指主機B的IP位址「192.168.1.3」）一致。如果不是則忽略；如果是，則會先將主機A的實體位址和IP位址資ARP request封包，並與本身的IP位址比對，判斷出自己是否為此ARPrequest所要解析的對象。結果只有主機B會產生回應的ARP reply封包。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-1 ARP操作原理

- **步驟4**：主機B可從ARP request封包中得知主機A的IP位址「192.168.1.8」與MAC位址「00:0c:f1:0a:4b:f8」，因而ARP reply封包不再用廣播方式送出，而是讓ARP reply封包以單向方式回傳，告知主機A關於自己的實體位址，為「00:1d:92:a2:d7:3c」。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-1 ARP操作原理

- ▶ **步驟5**：當主機A收到ARP reply後會更新自己的ARP表格；也代表完成IP/MAC位址解析。反之，如果主機A沒有得到ARP reply，代表ARP操作過程失敗。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

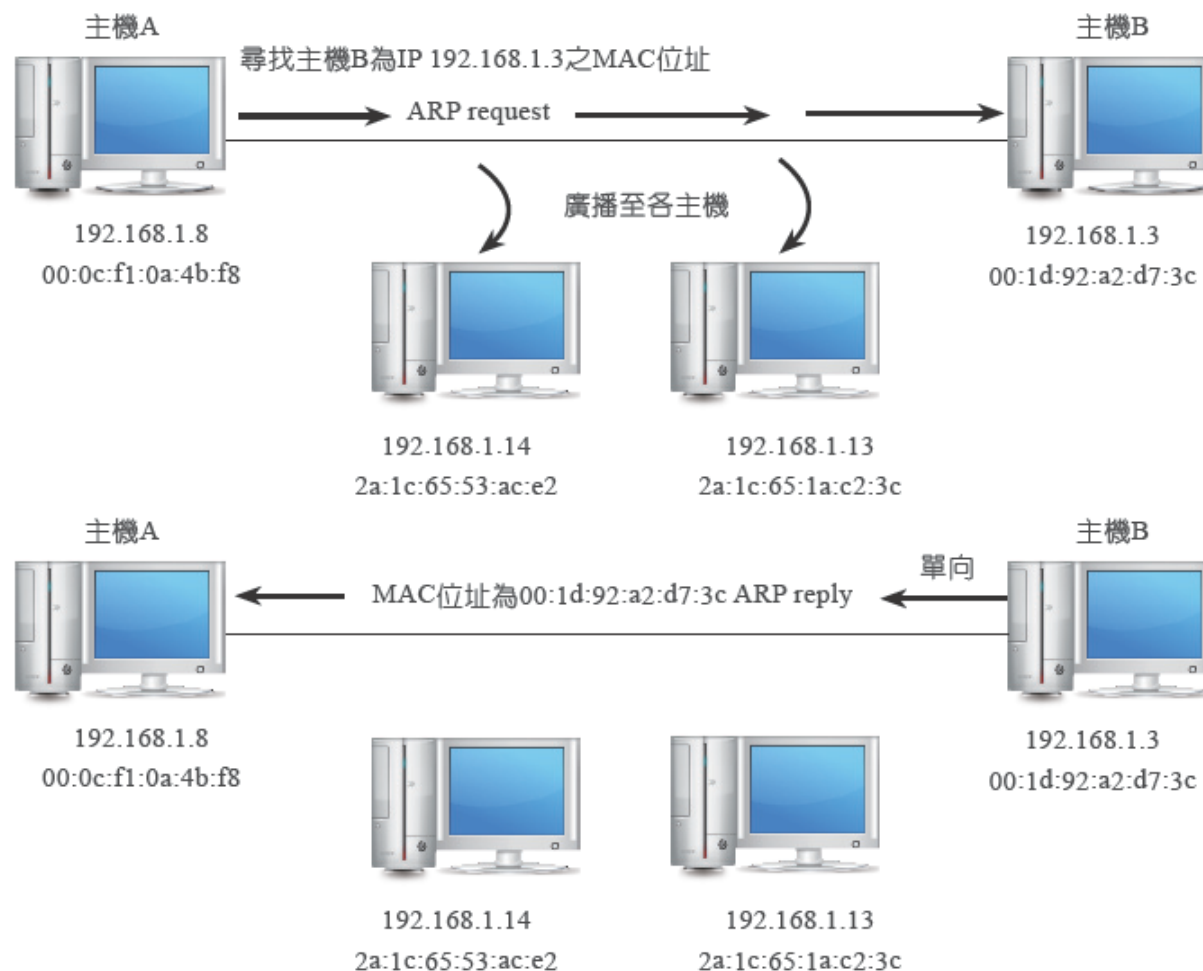
9-9

9-10

習題



# 9-1 ARP操作原理



●圖9-1 本地網路主機的ARP操作過程(request/reply)

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-2 ARP cache(快取)

- ▶ ARP cache記錄，可分為動態與靜態兩種。
  - ▶ 當主機A經由ARP request/reply過程取得主機B的MAC位址後，便將主機B的IP位址與MAC位址資料儲存在主機A的ARP cache中記錄下來。這些記錄由ARP自動產生，稱為動態記錄。
  - ▶ 反之，經由手動的方式將某主機的IP/MAC位址對應關係加入至ARP快取記錄下來，則稱為靜態記錄。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-2 ARP cache(快取)

▶ 靜態記錄被刪除的時機有下列情形：

- ▶ 重新開機。
- ▶ 以手動的方式刪除。
- ▶ 與動態記錄互相衝突。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-3 RARP操作原理

- ▶ RARP (Reverse ARP)協定是來源端已知自己的MAC位址，但不知自己的IP位址時，則可藉由RARP request封包向RARP伺服器查詢自己的IP位址。

9-1

9-2

9-3

9-4

9-5

9-6

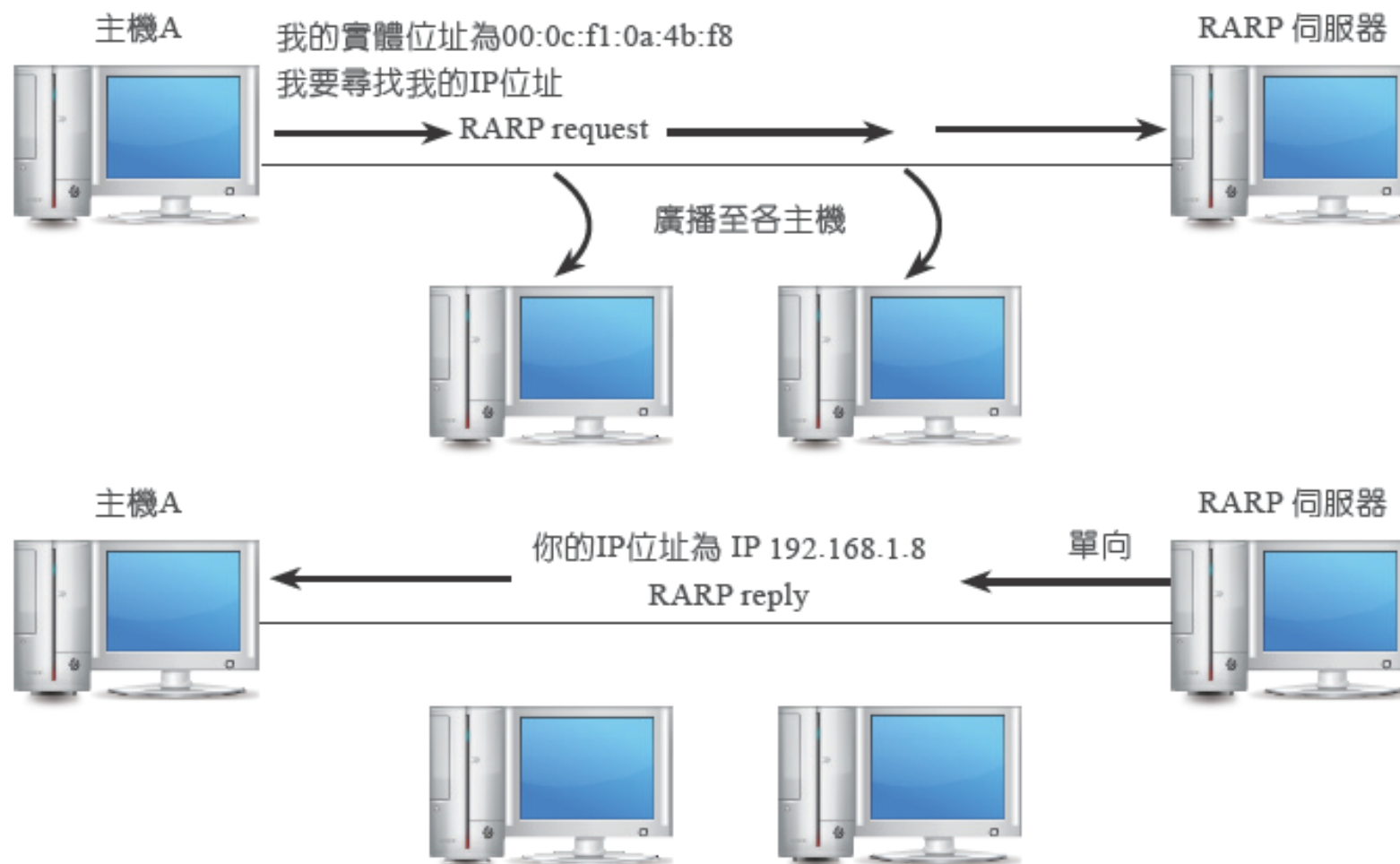
9-7

9-8

9-9

9-10

習題



9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

●圖9-2 RARP操作過程

## 9-4 ARP/RARP封包格式

### ► 硬體類型(hardware type)佔16bits

- 指出數據鏈路層所用的網路類型，如果值為1，表示為乙太網路；Token Ring值為6；Frame Relay值為15；ATM值為16。

硬體類型(16)		通訊協定類型(16)
硬體位址長度(8)	通訊協定位址長度(8)	操作(16)
送端硬體位址(長度不定)		
送端硬體位址		送端通訊協定位址(長度不定)
送端通訊協定位址		收端硬體位址
收端硬體位址(長度不定)		
收端通訊協定位址(長度不定)		

● 圖9-3 ARP與RARP有相同的封包格式

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-4 ARP/RARP封包格式

- ▶ 通訊協定類型(protocol type)佔16bits
  - ▶ 指出網路層所使用的協定，若為IP，則欄位值為2048，以16進位表示為0x0800。
- ▶ 硬體位址長度(hardware address length)佔8bits
  - ▶ 指出MAC位址的長度。以乙太網路為例，其MAC位址長度(以8bits為單位，共48bits)為6bytes，因此，硬體位址長度欄位值為6(代表8bits\*6=48bits)。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-4 ARP/RARP封包格式

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

- ▶ 通訊協定位址長度(protocol address length)佔8bits

- ▶ 指出網路層協定所用的位址長度。若通訊協定類型為0x0800(IP)，則長度欄位值為4(代表 $8\text{bits} \times 4 = 32\text{bits}$ )。

- ▶ 操作(operation)佔16bits

- ▶ 指出ARP封包類別，一共有4種，即：ARP request(欄位值為1)與ARP reply(欄位值為2)；RARP request(欄位值為3)與RARP reply(欄位值為4)。



## 9-4 ARP/RARP封包格式

### ▶ 送端硬體位址(sender HA)

- ▶ 長度不定，表示來源端的實體位址，若是乙太網路，此欄位值為6 (代表48bits)。

### ▶ 送端協定位址(sender protocol address)

- ▶ 長度不定，表示ARP封包來源端使用的協定位址。以IP為例，其長度為32bits的IP位址。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-4 ARP/RARP封包格式

### ► 收端硬體位址(target HA)

- 長度不定，表示目的端的實體位址，若是乙太網路，此欄位值為6 (48bits)。當傳送ARP request封包時，由於目的端的MAC位址還不知道，因此此欄位內容為000000000000。

### ► 收端協定位址(target protocol address)

- 長度不定，表示ARP封包目的端使用的協定位址，以IP為例，其長度為32bits的IP位址。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-4 ARP/RARP封包格式

- ▶ 當網路層是使用IP協定，數據鏈路層使用乙太網路時，則從圖9-3可計算ARP封包的長度為28bytes (4+4+6+4+6+4)。
- ▶ 根據Ethernet II的封包格式，規定資料欄位長度最短必須是46bytes，因此，ARP封包在封裝成乙太網路封包時必須再填補 $(46-28) = 18\text{bytes}$ 。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-4 ARP/RARP封包格式

- ▶ 從圖9-4得知，Ethernet II標準的乙太網路訊框，其資料欄位可從長度46至1500bytes，如果這是一個ARP request封包時，那該資料欄位就用來封裝整個ARP request封包。
- ▶ 注意：此時ARP request封包的訊息類型(佔2bytes) Etype欄位值為0x0806；如果為RARP封包，則Etype欄位值為0x0835

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

Ethernet II

前置位元 (8bytes)	DA (6bytes)	SA (6bytes)	Etype (2bytes)	ARP request封包	FCS (4bytes)
------------------	----------------	----------------	-------------------	------------------	-----------------

● 圖9-4 ARP request封包之封裝

## 9-5 ARP工具程式

- ▶ 作業系統如Windows 7都有提供ARP.EXE工具程式，現在您可以在C:\Users\ASUS> 敲入arp -a以便檢視ARP cache的內容為何，如圖9-5(a)紅框所示由左到右代表被解析主機的IP位址為192.168.1.1及指出經ARP解析後得到的MAC位址30-5a-3a-a8-4d-60，類型指出屬動態記錄。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-5 ARP工具程式

- ▶ 若要刪除ARP cache中的某一筆記錄可敲入  
arp -d IP 位址；若要全部刪除，則敲入arp -d  
\*。若要新增一筆靜態記錄，則敲入arp -s IP 位  
址 MAC位址後，再敲入arp -a看出結果，如圖  
9-5(b)指出新增一筆靜態記錄；並指出經ARP解  
析後得到的這一筆靜態記錄，其IP位址為  
192.168.1.17，MAC位址為11-22-33-44-55-  
66。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

```

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

C:\Users\ASUS>arp -a

介面: 192.168.1.161 --- 0xb
網際網路網址      實體位址      類型
192.168.1.1        30-5a-3a-a8-4d-60 動態
192.168.1.255      ff-ff-ff-ff-ff-ff 靜態
224.0.0.252        01-00-5e-00-00-fc 靜態
239.255.255.250    01-00-5e-7f-ff-fa 靜態

介面: 192.168.50.1 --- 0xf
網際網路網址      實體位址      類型
192.168.50.255     ff-ff-ff-ff-ff-ff 靜態
224.0.0.252        01-00-5e-00-00-fc 靜態
239.255.255.250    01-00-5e-7f-ff-fa 靜態

介面: 192.168.138.1 --- 0x10
網際網路網址      實體位址      類型
192.168.138.255     ff-ff-ff-ff-ff-ff 靜態
224.0.0.252        01-00-5e-00-00-fc 靜態
239.255.255.250    01-00-5e-7f-ff-fa 靜態

C:\Users\ASUS>
    
```

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

圖9-5(a) arp -a (動態記錄)



```

C:\Windows\system32\cmd.exe

239.255.255.250      01-00-5e-7f-ff-fa  靜態
介面: 192.168.138.1 --- 0x10
網際網路網址      實體位址      類型
192.168.138.255    ff-ff-ff-ff-ff-ff  靜態
224.0.0.252        01-00-5e-00-00-fc  靜態
239.255.255.250    01-00-5e-7f-ff-fa  靜態

C:\Users\ASUS>arp -s 192.168.1.17 11-22-33-44-55-66

C:\Users\ASUS>arp -a

介面: 192.168.1.161 --- 0xb
網際網路網址      實體位址      類型
192.168.1.1        30-5a-3a-a8-4d-60  動態
192.168.1.17       11-22-33-44-55-66  靜態
192.168.1.255      ff-ff-ff-ff-ff-ff  靜態
224.0.0.252        01-00-5e-00-00-fc  靜態
239.255.255.250    01-00-5e-7f-ff-fa  靜態
255.255.255.255    ff-ff-ff-ff-ff-ff  靜態

介面: 192.168.50.1 --- 0xf
網際網路網址      實體位址      類型
192.168.50.255     ff-ff-ff-ff-ff-ff  靜態
224.0.0.252        01-00-5e-00-00-fc  靜態
    
```

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

圖9-5(b) arp -s (新增一筆靜態記錄)

## 9-5 ARP工具程式-範例1

- ▶ 當主機A與主機B分別為兩個不同的網路如圖9-6(a)、(b)所示，依序分別為192.168.0.0/24與172.16.0.0/16，中介含一個路由器(Router)，請說明主機A敲入ping 主機B時的連線通訊整個過程。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

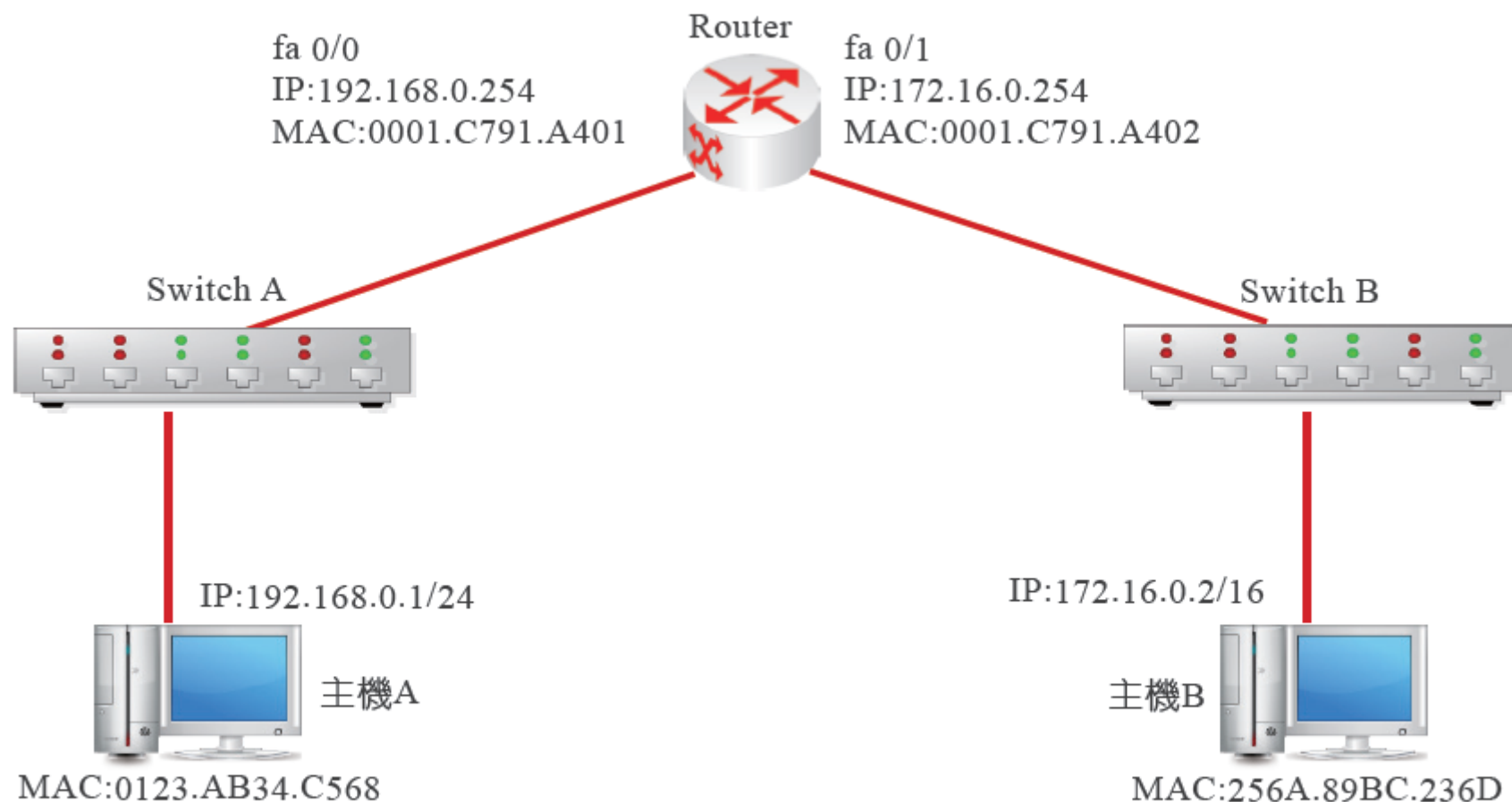


圖9-6(a) 範例1的網路架構

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-5 ARP工具程式-範例1

解：

- 如圖9-6(a)所示，主機A先透過ping172.16.0.2，再透過arp -a指令查知ARPCache內的資訊，其可得知IP位址與MAC位址對照表。
- ARPCache內(如圖9-6(b)所示)的資訊只有主機A的預設閘道IP 192.168.0.254，及其MAC位址0001.c791.a401(此實驗是由Cisco packet tracer實現出來)，並無主機B的MAC位址，這也證實了，ARP只操作於LAN之內。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-5 ARP工具程式-範例1

更詳細的說明如下：

- ▶ 主機 A(192.168.0.1) 想傳送 IP 資料包給主機 B(172.16.0.2)，但因ARP的範圍限制在LAN區域，所以發送端會將IP資料包送至Router的fa 0/0介面(它的MAC位址0001.C791.A401)，一旦發送端利用ARP取得IP 192.168.0.254的MAC位址，它便會建立訊框，並將此訊框送入至192.168.0.0這個子網路LAN1

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-5 ARP工具程式-範例1

- ▶ 當LAN1的Router的轉接卡看到這個鏈路層的訊框是對它定址，就會將此訊框交給Router的網路層，這也代表主機A的IP資料包已成功到達Router。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-5 ARP工具程式-範例1

- ▶ 此時Router也開始接手，透過路由表知道IP資料包應該由fa 0/1介面的IP 172.16.0.254轉送出去。注意，此時Router的來源MAC位址變成0001.C791.A402(亦即ping的封包離開Router的fa 0/1時，該封包的來源位址)，這也說明資料經過Router轉送時必須改變MAC位址，但目的IP位址不會改變

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-5 ARP工具程式-範例1

- ▶ 因此介面會將IP資料包交給它的轉接卡，轉接卡再將此資料包封裝到新的訊框，然後訊框才送入LAN2:172.16.0.0子網路上，此時訊框的目的端MAC位址256A.89BC.236D終於被找到；接著，Router再透過ARP取得此MAC位址。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

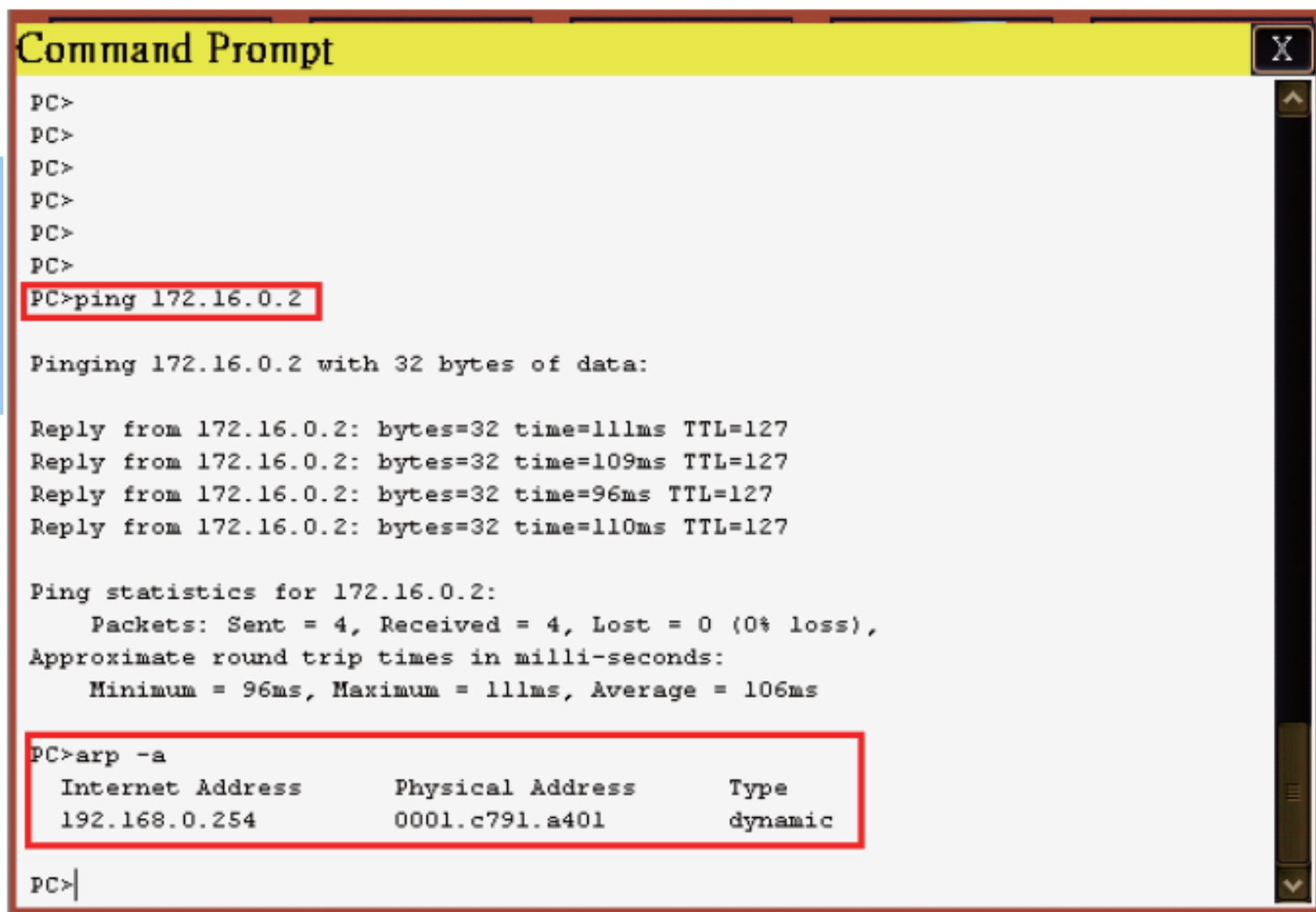
9-8

9-9

9-10

習題





The screenshot shows a Windows Command Prompt window with a yellow title bar labeled "Command Prompt". The window contains the following text:

```
PC>
PC>
PC>
PC>
PC>
PC>
PC>ping 172.16.0.2

Pinging 172.16.0.2 with 32 bytes of data:

Reply from 172.16.0.2: bytes=32 time=111ms TTL=127
Reply from 172.16.0.2: bytes=32 time=109ms TTL=127
Reply from 172.16.0.2: bytes=32 time=96ms TTL=127
Reply from 172.16.0.2: bytes=32 time=110ms TTL=127

Ping statistics for 172.16.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 96ms, Maximum = 111ms, Average = 106ms

PC>arp -a

Internet Address      Physical Address      Type
192.168.0.254         0001.c791.a401        dynamic

PC>|
```

The command `PC>ping 172.16.0.2` and the output of `arp -a` are highlighted with red boxes in the original image.

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

圖9-6(b) 範例1得到ARP Cache內的資訊

## 9-6 ARP封包的擷取分析

- ▶ 首先，我們在Windows 7環境下(如下註解說明區域網路的環境設定)由2部電腦建立一LAN，其中一台書房的電腦(主機A)擔任發送端，其IP位址為192.168.1.8，MAC位址為00:0c:f1:0a:4b:f8；另一台客廳的電腦(主機B)擔任接收端，其IP位址為192.168.1.3，MAC位址為00:1d:92:a2:d7:3c。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-6 ARP封包的擷取分析

- ▶ 現在你可以先開啟Wireshark，然後在主機A的C:\Documents and Settings\yunlung> 敲入 ping 192.168.1.3，利用 Wireshark 對 ARP request與ARP reply做封包的擷取分析。
- ▶ 注意：我們在「Filter」欄位敲入小寫的arp，可以加速找到ARP request與ARPreply的封包，如圖9-7(a)與圖9-7(b)所示，圖中數據代表意義可參考9-4節。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-6 ARP封包的擷取分析

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

- ▶ 2部電腦可直接連接或透過Hub連接。首先，必須把連接在此LAN內的主機A設定好，順序如下：
  - ▶ 在「我的電腦」按滑鼠右鍵→「內容」→在「變更設定」中的「電腦描述」輸入「書房的電腦」→「變更」→「電腦名稱」輸入MARRY→「工作群組」輸入TTI。
  - ▶ 同樣地，主機B的「電腦名稱」中的「電腦描述」輸入「客廳的電腦」後，選取「變更」，接著同上述，在「電腦名稱」輸入JOHN，「工作群組」的設定要特別注意，由於同一LAN其群組一定要相同，所以也輸入TTI。

## 9-6 ARP封包的擷取分析

- ▶ 一旦兩台電腦的相關設定完畢，不要忘掉網路卡也要設定。首先打開主機A，進入「開始」→「控制台」→「變更介面卡設定」→在「區域連線」按滑鼠右鍵→「內容」→在「連線使用下列項目」選擇「網際網路通訊協定第4版 (TCP/IP)」→「內容」→選取「使用下列IP位址」→在IP位址欄位輸入192.168.1.8，子網路遮罩 255.255.0.0，DNS網路位址為168.95.1.1→「確定」。主機B的不同處在於只有輸入IP 192.168.1.3，其他完全一樣。一切大功告成。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-6 ARP封包的擷取分析

- ▶ 再來就是確認所設定的LAN沒有問題，其步驟為：在主機A進入「電腦」→「網路」，「Enter」此時就可看到兩台電腦 MARRY 及 JOHN 出現，若您在「JOHN」點兩下，就可以讀取主機B所共享出來的資料夾。
- ▶ 注意，共享資料夾必須事先被勾選，其步驟為：在所選取的資料夾按右鍵→「內容」→「共用」→勾選「共用此資料夾」→「確定」。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-6 ARP封包的擷取分析

9-1

9-2

9-3

9-4

9-5

9-6

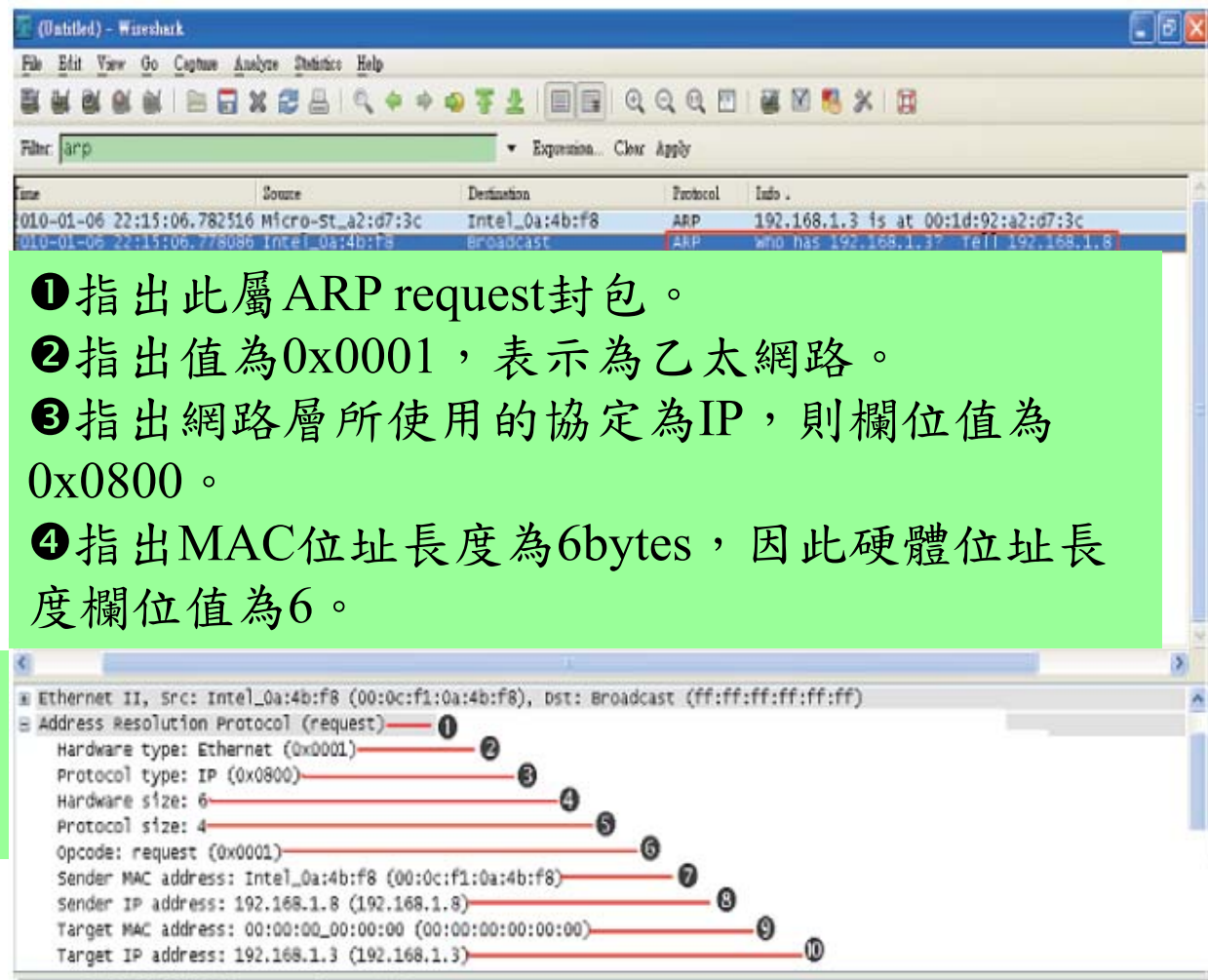
9-7

9-8

9-9

9-10

習題



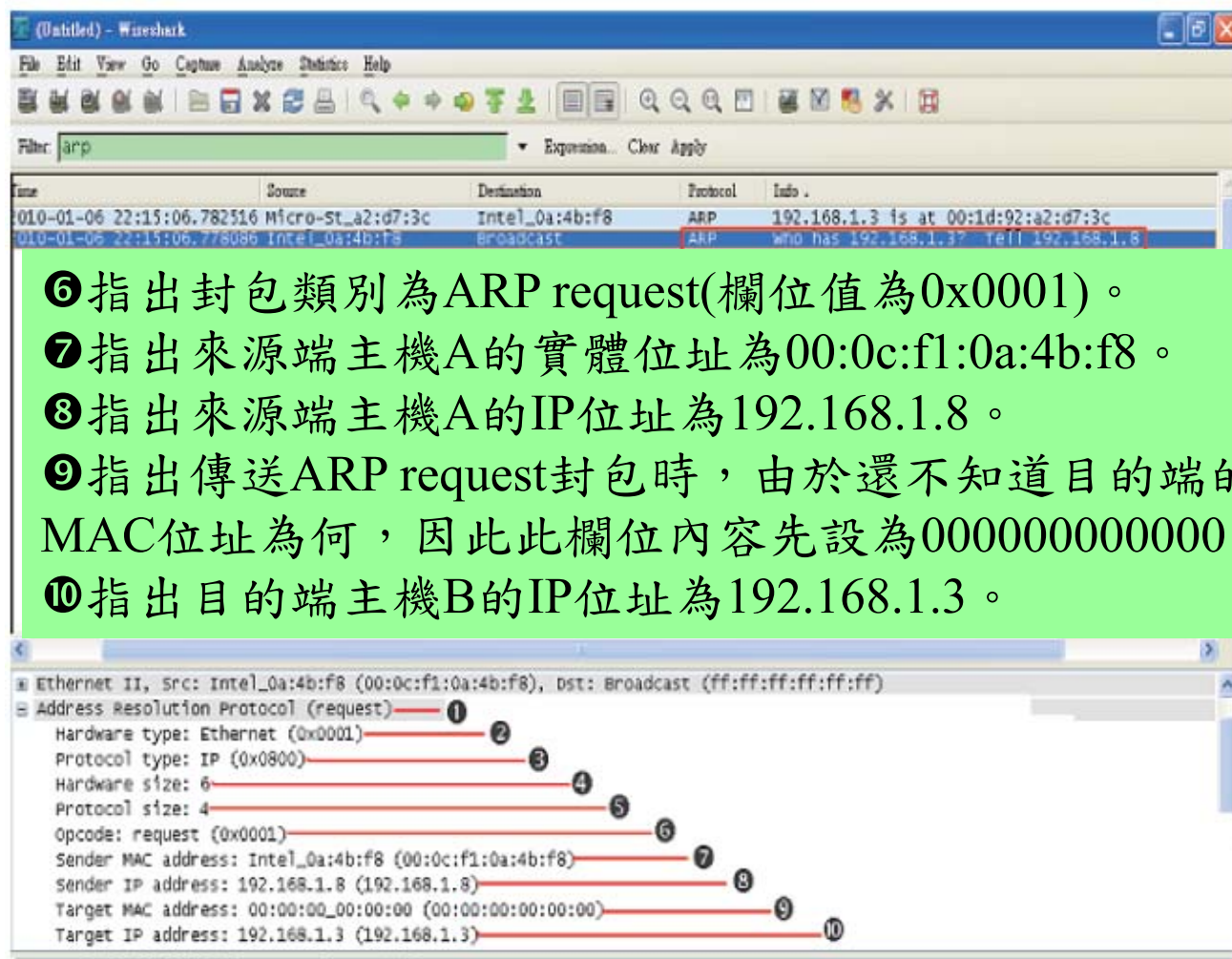
- ①指出此屬ARP request封包。
- ②指出值為0x0001，表示為乙太網路。
- ③指出網路層所使用的協定為IP，則欄位值為0x0800。
- ④指出MAC位址長度為6bytes，因此硬體位址長度欄位值為6。

⑤指出IP協定所用的位址長度，因此長度欄位值為4。

●圖9-7(a) ARP request封包的擷取分析



## 9-6 ARP封包的擷取分析



●圖9-7(a) ARP request封包的擷取分析

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題



## 9-6 ARP封包的擷取分析

9-1

9-2

9-3

9-4

9-5

9-6

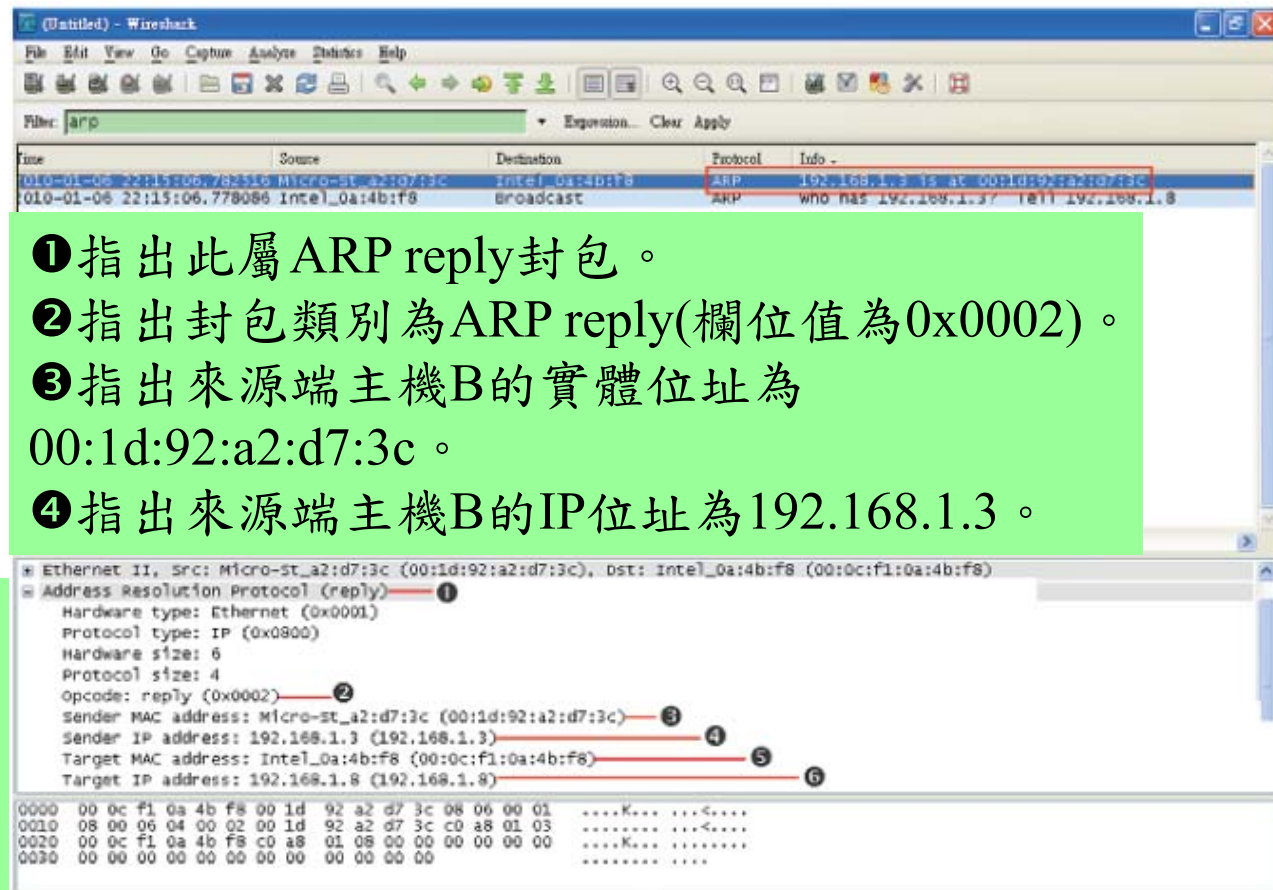
9-7

9-8

9-9

9-10

習題



- ①指出此屬ARP reply封包。
- ②指出封包類別為ARP reply(欄位值為0x0002)。
- ③指出來源端主機B的實體位址為00:1d:92:a2:d7:3c。
- ④指出來源端主機B的IP位址為192.168.1.3。

- ⑤指出目的端主機A的實體位址為00:0c:f1:0a:4b:f8。
- ⑥指出目的端主機A的IP位址為192.168.1.8。

圖9-7(b) ARP reply封包的擷取分析

## 9-7 ICMP簡介

- ▶ ICMP稱為「網際網路控制訊息協定」，英文全名是Internet Control Message Protocol。
- ▶ ICMP其實就是一個錯誤偵測與回報機制，主要包括能檢測網路的連線情況、偵測遠端主機是否存在，以及建立和維護IP路由資料等功能。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-7 ICMP簡介

- ▶ ICMP同ARP屬網路層協定，一旦IP路由出現問題，就需利用此協定傳送並報告相關的資訊。ICMP無法獨立操作，它必須與IP協定標頭一起搭配使用，此時IP協定標頭內的PROT的值為1(即0x01)，如圖9-8(a)。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-7 ICMP簡介

- ▶ 注意：ICMP標頭的位置是位於IP標頭的後面。  
像ping、tracert或pathping命令，都是用來測試網路連線的情況，而所用的協定正是ICMP。  
ICMP封包在網路上是如何傳送的呢？

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-7 ICMP簡介

- 其實 ICMP 封包 ( 即 ICMP 標頭 加上 ICMP Payload)是封裝在IP封包中儲存資料的地方，稱為IP Payload，並經IP路由傳送到目的端。值得一提的是，ICMP Payload(也是ICMP封包存放資料的部分)隨著ICMP封包的類型而有所不同。雖然ICMP封包是位於IP標頭的後面，但仍屬於網路層，如圖9-8(b)所示。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

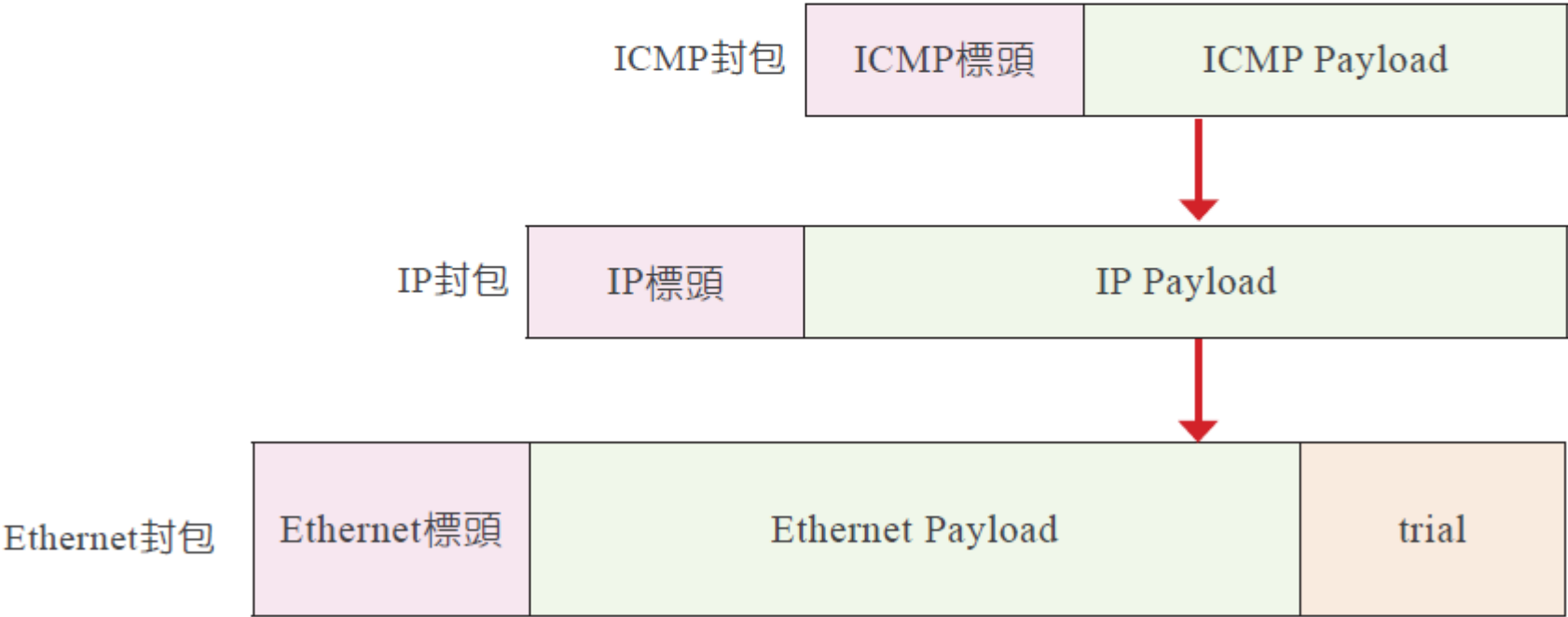
9-9

9-10

習題



●圖9-8(a) 代表ICMP 封包時IP標頭內的PROT



●圖9-8(b) ICMP封包的封裝方式

9-1
9-2
9-3
9-4
9-5
9-6
9-7
9-8
9-9
9-10
習題

## 9-8 ICMP訊息格式

- ▶ ICMP訊息（亦稱為ICMP封包）分成兩部分，即ICMP標頭及ICMP資料(或稱ICMP Payload)，前者包含1個8位元組的標頭，雖然不同的訊息有不同的標頭格式，但前4個位元組都是一樣的；後者則是一個非固定長度的ICMP資料
- ▶ 換言之，隨著ICMP訊息類型的不同，每一個封包欄位的長度與內容也會跟著不同，如圖9-9所示

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-8 ICMP訊息格式

- ▶ ICMP標頭前4個位元組包含3個固定長度的欄位：類型(Type)佔1 byte，代碼(Code)佔1 byte，與檢查和(Checksum)佔2 bytes。
- ▶ Type定義出各類的ICMP訊息類型，如表9-1所示，ICMP可分為兩大訊息類型，分別為「查詢」(Query)與「錯誤回報」(Error-Reporting)。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題



## 9-8 ICMP訊息格式

- ▶ 「查詢」訊息類型的Type值有4組，分別為8/0、10/9、13/14和17/18，每組分別代表request/reply，查詢的主要功能是協助一部主機或網路管理者取得另一部主機或路由器的相關訊息，查詢訊息可由一部主機送出，目的端主機再以各自獨特格式回應。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-8 ICMP訊息格式

- ▶ 錯誤回報訊息共5種，它的Type值分別為3、4、5、11和12，主要功能是回報路由器或目的端主機在處理IP封包時可能遭遇到的一些問題。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

表9-1 ICMP訊息的類型與說明

類型	訊息功能
0	Echo reply
3	Destination unreachable
4	Source quench
5	Redirection
8	Echo request
9	Router advertisement
10	Router solicitation
11	Time exceeded
12	Parameter problem
13	Timestamp request
14	Timestamp reply
17	Address mask request
18	Address mask reply

9-1

9-2

9-3

9-4

9-5

9-6

9-7

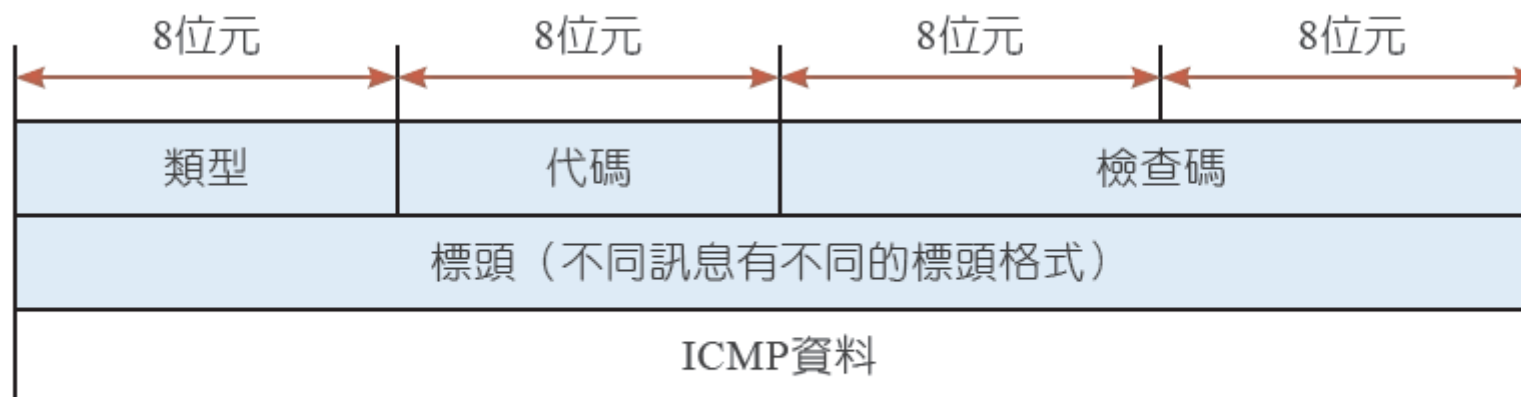
9-8

9-9

9-10

習題

## 9-8 ICMP訊息格式



●圖9-9 ICMP訊息格式

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-8-1 ICMP的查詢訊息

### ► Echo request / Echo reply

- 它們的Code欄位值為0。Echo request / Echo reply封包常用來偵測兩主機間是否可以通訊。
- 因為ICMP訊息是封裝在IP資料包內，所以當某主機一旦接收到Echo request封包並送出Echo reply封包後，這樣也就驗證，送收兩端的IP資料包可開始進行通訊，則路徑上的路由器也可接收、處理及轉送IP資料包。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-8-1 ICMP的查詢訊息

- ▶ 一個Echo request封包(類型號碼為8)可由主機或路由器送出，收到Echo request封包的主機或路由器會送出Echo reply封包(類型號碼為0)。
- ▶ 網路管理者也可以用Echo request封包及Echo reply封包檢查IP協定的運作。
- ▶ 有關Echo request封包及Echo reply封包格式如圖9-10所示。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-8-1 ICMP的查詢訊息



●圖9-10(a) Echo request及Echo reply封包格式

9-1

9-2

9-3

9-4

9-5

9-6

9-7

**9-8**

9-9

9-10

習題

## 9-8-1 ICMP的查詢訊息-範例2

請利用圖9-10(a)的ICMP Echo request封包訊息內容來計算檢查和(或稱錯誤檢查和)。注意，ICMP資料的內容為ABCD。

**解：**ICMP檢查和是以整個訊息(包括標頭與資料)來計算。其過程先將整個訊息分成很多組16 bits，再將它們加總起來，然後求1的補數得出檢查和。注意，一開始的檢查和填入0。A&B&C&D的值可由ASCII表查知。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題



# 9-8-1 ICMP的查詢訊息-範例2

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

8	0	0
5		1
測試		

```

8&0  —————> 00001000 00000000
0     —————> 00000000 00000000
8     —————> 00000000 00000101
1     —————> 00000000 00000001
A&B  —————> 01000001 01000010
C&D  —————> 01000011 01000100
      —————> 10001100 10001100
檢查和 —————> 01110011 01110011
    
```

圖9-10(b) ICMP Echo request封包的檢查和計算

## 9-8-1 ICMP的查詢訊息

- ▶ 時間戳記要求(Timestamp request) / 時間戳記回覆(Timestamp reply)
  - ▶ 它們的Code欄位值為0。
  - ▶ 主要功能是在兩部主機間進行系統時間同步的調整，即使兩部主機的時間不同步，時間戳記要求訊息與時間戳記回覆訊息仍可以計算資料包在來源端與目的端主機間的傳輸延遲，是以格林威治時間(Universal Time ; UT)為基準，由格林威治時間午夜零時零分起算。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-8-1 ICMP的查詢訊息

- ▶ 時間戳記欄位佔32 bits，時戳訊息以ms為單位。
- ▶ Timestamp request(類型號碼為13)與Timestamp reply(類型號碼為14)訊息格式如圖9-11所示。
- ▶ 來源端建立Timestamp request訊息，並以送出訊息時的格林威治時間作為開始時間戳記，其他兩個欄位填0。
- ▶ 目的端會將接收到的Timestamp request訊息中的開始時間戳記拷貝到其所建立Timestamp reply訊息的相同欄位內

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-8-1 ICMP的查詢訊息

13：要求  
14：回覆

類型：13或14	代碼：0	檢查和
識別碼		序號
開始時間戳記		
接收時間戳記		
送出時間戳記		

●圖9-11 Timestamp request / Timestamp reply訊息格式

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-8-1 ICMP的查詢訊息-範例3

當Timestamp request訊息開始時間戳記、接收時間戳記及送出時間戳記欄位值依序為50 ms、58 ms及71 ms；而封包到達時間值為75 ms，則來回時間為何？假設單程時間為去程時間與回程時間的平均值，則兩部主機間進行系統時間同步的時間差值為何？

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-8-1 ICMP的查詢訊息-範例3

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

解：

去程時間為 $58-50=8$  ms；回程時間為 $75-71=4$  ms；所以來回時間為 $8+4=12$  ms。

因單程時間為 $(8+4)\div 2=6$  ms，由於同步雙方主機的時間，必須計算時間差值以便調整，所以時間差值 $=58-(50+6)=2$  ms。

利用這2ms，可以讓Timestamp request訊息與Timestamp reply訊息同步雙方主機的時間。

## 9-8-1 ICMP的查詢訊息

- ▶ 位址遮罩要求(Address mask request) / 位址遮罩回覆(Address mask reply)
  - ▶ 它們的Code欄位值為0。
  - ▶ 若已知路由器的位址，為取得網路遮罩訊息，主機可送出Address mask request(類型號碼為17)訊息給LAN上的路由器；反之，就將Address mask request訊息廣播出去，路由器收到此訊息就回應Address maskreply(類型號碼為18)訊息，以提供網路遮罩訊息給要求的主機如圖9-12所示。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-8-1 ICMP的查詢訊息

17 : Address mask request  
18 : Address mask reply

類型：17或18	代碼：0	檢查和
識別碼		序號
位址遮罩		

●圖9-12 Address mask request / Address mask reply訊息格式

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題



## 9-8-1 ICMP的查詢訊息

- ▶ 路由器要求(Router solicitation) / 路由器通知(Router advertisement)
  - ▶ 它們的Code欄位值為0。
  - ▶ ICMP路由器發現訊息(Router Discovery Messages)是使用Router solicitation(類型號碼為10)及Router advertisement(類型號碼為11)兩訊息，以便找出子網路上的路由器操作位址。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-8-1 ICMP的查詢訊息

- ▶ 不管是否有主機詢問，每一個路由器會由它的群播介面定期送出Router advertisement訊息，通知該介面的 IP 位址。主機也可以透過 Router advertisement訊息得知鄰居路由器的位址。
- ▶ 當一個群播鏈路的主機啟動時，它可將Router solicitation群播出去，並要求立即通知，而不是等待下一個週期的出現

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-8-1 ICMP的查詢訊息

- ▶ 換言之，為瞭解路由器相關的資訊，主機以群播或廣播送出一個Router solicitation訊息如圖9-13所示，所有路由器收到此詢問訊息時就用Router advertisement訊息(如圖9-14所示)廣播它們的路徑訊息出去，這不但代表自己存在，並提供該主機周邊相關路由器設定訊息。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

# 9-8-1 ICMP的查詢訊息

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

類型：10	代碼：0	檢查和
保留		

●圖9-13 Router solicitation訊息格式

類型：9	代碼：0	檢查和
位址數目	位址項目大小	存活期間
路由器位址1		
位址優先權1		
路由器位址1		
位址優先權2		
⋮		

●圖9-14 Router advertisement訊息格式

## 9-8-2 錯誤回報訊息

► 圖9-15指出錯誤訊息發生時，ICMP封包如何構成，說明如下：

- 首先，某主機接收到的資料包是由原始的(original)IP資料包標頭及原始的IP資料欄位構成，一旦資料包有錯誤發生，所有錯誤訊息放資料的地方稱為ICMP資料，它是由原始的(original)IP資料包標頭及原始的IP資料欄位最前面64 bits的資料所形成
- 接著，ICMP標頭會加進原始的IP資料包標頭前面，形成ICMP封包。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

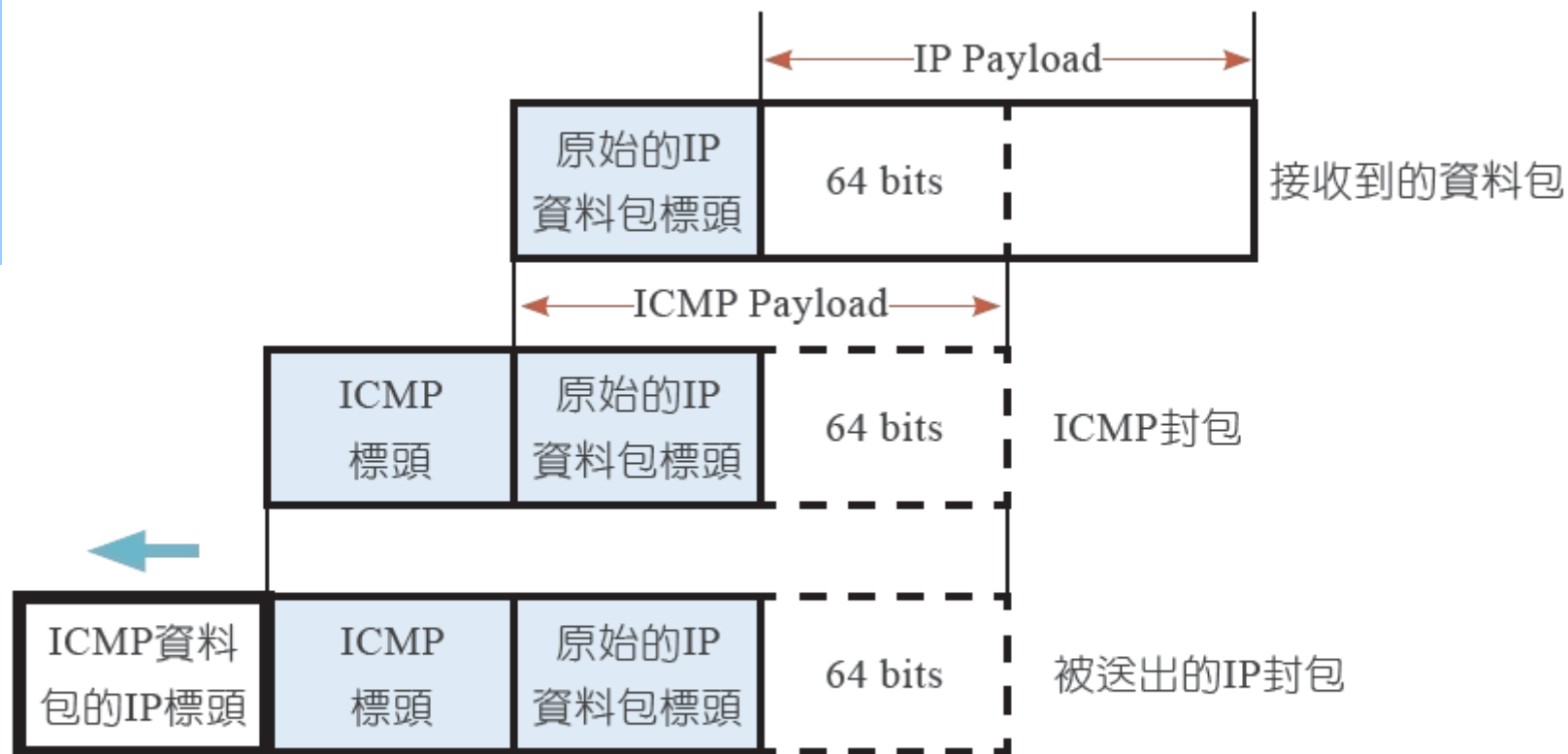
9-8

9-9

9-10

習題

## 9-8-2 錯誤回報訊息



●圖9-15 錯誤訊息發生時的ICMP封包構成

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-8-2 錯誤回報訊息

- ▶ 目的端無法到達(Destination Unreachable)
  - ▶ 它的Code欄位值為0 ~ 15。當IP資料包無法到達目的端時，主機或路由器將根據ICMP的錯誤訊息發送Destination unreachable訊息(類型號碼為3)給來源端。

類型：3	代碼：0到15	檢查和
未使用（全部為0）		
原始的IP資料包標頭及原始的IP資料欄位最前面的64 bits		

●圖9-16 Destination unreachable訊息格式

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題



表9-2 在不同代碼分別出不同的「目的端無法到達」原因說明

Code	原因說明	補充敘述
0	網路無法到達 (Network unreachable)	可能硬體發生問題，此訊息由路由器產生。注意，路由器知道目的端網路存在。
1	主機無法到達 (Host unreachable)	可能硬體發生問題，此訊息由路由器產生。注意，路由器知道目的端主機存在。
2	協定無法到達 (Protocol unreachable)	發生在被指定的傳輸協定不支援時，此訊息由目的端主機產生。
3	埠無法到達 (Port unreachable)	發生在被指定的傳輸層(例如UDP)，無法將IP資料包解多工，也沒有協定機制能通知發送端。
4	資料包太大 (The datagram is too big)	IP封包太大必須分割，但是在IP封包內的DF位元又被設定為不可以分割(即DF=1)。
5	來源路徑失敗 (Source route failed)	來源端路徑選項中的某些路由器無法經過。
6	目的端網路不明 (Destination network unknown)	路由器根本不知道目的端網路的相關資料。
7	目的端主機不明 (Destination host unknown)	路由器根本不知道目的端主機存在。
8	來源端主機被隔離 (Source host isolated)	ICMP發送端(路由器)因配置設定而無法轉送來源封包。
9	與目的端網路的連線被禁止 (Communication with destination network is administratively prohibited)	ICMP發送端(路由器)因配置設定而無法對期望的網路做存取。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題



## 9-8-2 錯誤回報訊息

Code	原因說明	補充敘述
10	與目的端主機的通訊被禁止 (Communication with destination host is administratively prohibited)	ICMP發送端(路由器)因配置設定而無法對期望的主機做存取。
11	網路無法到達所指定的服務型態 (The network is unreachable for Type Of Service)	TOS及Precedence欄位在現今網路都採用Differserv欄位。
12	主機無法到達所指定的服務型態 (The host is unreachable for Type Of Service)	同Code 11之說明。
13	通訊因管理而被禁止 (Communication Administratively Prohibited)	當一個路由器因管理需要而過濾資料包，導致無法轉送被過濾掉的資料包造成通訊禁止。
14	違反主機優先權的設定 (Host precedence violation)	因違反主機優先權的設定，而使主機無法到達，此訊息由路由器送出，表示到達此目的端的資料包其要求的優先權不被允許。
15	優先權被中止 (Precedence cutoff in effect)	資料包優先等級低於管理者設定的優先等級。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-8-2 錯誤回報訊息

### ▶ 來源放慢(Source quench)

- ▶ 它的Code欄位值為0。
- ▶ IP協定為免接式連接(Connectionless ; CL)，由於沒有TCP具有的流量控制的機制，主機必須依賴佇列儲存等待要被處理的封包。
- ▶ 當路由器過載，無法處理太多的IP封包(即資料包)時，必須丟棄某一個資料包，就會送出Source quench訊息(類型號碼為4)給資料包發送者，通知它網路已發生壅塞，應該降低發送資料包的速度。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-8-2 錯誤回報訊息

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

類型：4	代碼：0	檢查和
未使用（全部為0）		
原始的IP資料包標頭及原始的IP資料欄位最前面的64 bits		

●圖9-17 Source quench訊息格式

## 9-8-2 錯誤回報訊息

### ► 重新導向(Redirection)

- 它的Code欄位值為0 ~ 3。
- 當主機A透過閘道器1要傳送資料包給主機B時，閘道器1由本身的路由表發現有更佳路徑時，便會發送Redirection訊息(類型號碼為5)給來源端主機A，此訊息將透過另一個閘道器2轉送至另一個路徑，訊息格式如圖9-18所示。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-8-2 錯誤回報訊息

- ▶ 至於Redirection代碼0 ~ 3代表意義如下：
- ▶ 代碼0：特定網路路徑的重新導向。
- ▶ 代碼1：特定主機路徑的重新導向。
- ▶ 代碼2：指定服務種類的特定網路路徑的重新導向。
- ▶ 代碼3：指定服務種類的特定主機路徑的重新導向。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-8-2 錯誤回報訊息

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

類型：5	代碼：0～3	檢查和
目的端路由器的IP位址		
原始的IP資料包標頭及原始的IP資料欄位最前面的64 bits		

●圖9-18 Redirection訊息格式

## 9-8-2 錯誤回報訊息

### ▶ 時間逾時(Time exceeded)

- ▶ 它的Code欄位值為0或1。
- ▶ 為避免網路因壅塞或其他因素造成IP資料包(即IP封包)無法到達目的端，並可能無窮盡地在網路中傳送造成負擔。因此，在IP封包每經過一個路由器，IP封包內TTL值減1；直到TTL=0時，路由器立刻放棄該IP封包，並送出Time exceeded訊息(類型號碼為11)給來源端主機。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-8-2 錯誤回報訊息

類型：11	代碼：0或1	檢查和
未使用（全部為0）		
原始的IP資料包標頭及原始的IP資料欄位最前面的64 bits		

●圖9-19 Time exceeded訊息格式

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題



## 9-8-2 錯誤回報訊息

### ▶ 參數錯誤(Parameter problem)

- ▶ 它的Code欄位值為0。
- ▶ 當目的端主機收到的IP封包欄位內的值不正確時，Parameter problem訊息(類型號碼為12)會被送給來源端主機。

類型：12	代碼：0	檢查和
指標	未使用（全部為0）	
原始的IP資料包標頭及原始的IP資料欄位最前面的64 bits		

●圖9-20 Parameter problem訊息格式

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-9 ICMP工具程式測試

- ▶ 一般網路使用者可透過ping工具程式來測試網路連線是否正常。ping的語法與參數可寫成：

ping [參數] [網址或IP位址]

- ▶ 要查詢ping命令所使用的相關參數種類，可在命令提示字元，例如C:\Users\ASUS>敲入單一命令ping，可得出表9-3說明。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

# 9-9 ICMP工具程式測試

表9-3 ping的參數種類說明

-t	ping到指定的主機，會連續送出Echo request封包，直到按「Ctrl+C」才停止；按「Ctrl+Break」則出現統計結果並繼續下去。
-a	將位址解析為主機名稱。
-n count	傳送Echo request封包數，預設值為4。
-l size	使用緩衝器的大小。
-f	傳送封包中的Don't Fragment旗標。
-i TTL	設定TTL所指定的值。
-v TOS	將服務類型欄位設定為TOS所指定的值。
-r count	記錄封包的路由。
-s count	指定count所指定的跳躍數(hops)的時間戳記。
-j host-list	host-list所指定的主機清單的路徑(使用鬆散路由來源)來傳送封包(僅IPv4)。
-k host-list	host-list所指定的主機清單的路徑(使用嚴密路由來源)來傳送封包(僅IPv4)。
-w timeout	每個回覆的等待逾時(毫秒)。
-R	也使用路由器標頭測試反向路由(僅IPv6)。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-9 ICMP工具程式測試

```
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 -n 2 -w 5000 www.yahoo.com.tw

Ping src.003.vahoodns.net [106.10.212.150] <使用 32 位元組的資料>:
回覆自 106.10.212.150: 位元組=32 時間=199ms TTL=49
回覆自 106.10.212.150: 位元組=32 時間=199ms TTL=49

106.10.212.150 的 Ping 統計資料:
    封包: 已傳送 = 2, 已收到 = 2, 已遺失 = 0 (0% 遺失)
    大約的來回時間 (毫秒):
        最小值 = 199ms, 最大值 = 199ms, 平均 = 199ms

C:\Users\ASUS>
```

- ①指出-n 2表示發出Echo request封包只設定2次。
- ②指出-w 5000表示等待時間延長5秒。
- ③指出回覆自106.10.212.150：位元組=32 時間=199ms TTL=49。
- ④指出Echo request封包送出2個，收到也是2個。

●圖9-21 ping -n 2 -w 5000 www.yahoo.com.tw結果

9-1

9-2

9-3

9-4

9-5

9-6

9-7

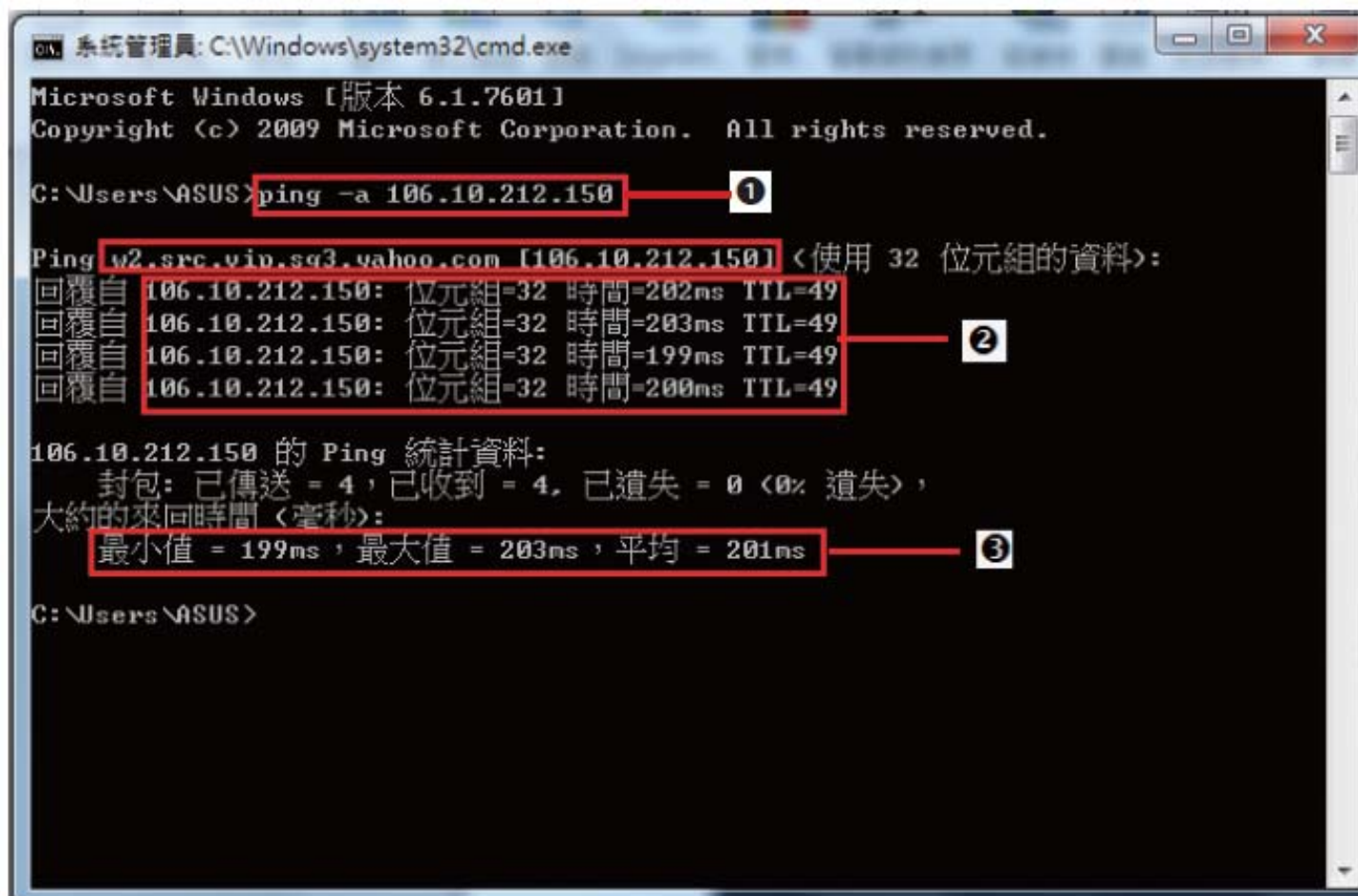
9-8

9-9

9-10

習題

## 9-9 ICMP工具程式測試



```
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 -a 106.10.212.150 ①

Ping w2.src.vip.sg3.yahoo.com [106.10.212.150] <使用 32 位元組的資料>:
回覆自 106.10.212.150: 位元組=32 時間=202ms TTL=49
回覆自 106.10.212.150: 位元組=32 時間=203ms TTL=49 ②
回覆自 106.10.212.150: 位元組=32 時間=199ms TTL=49
回覆自 106.10.212.150: 位元組=32 時間=200ms TTL=49

106.10.212.150 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 = 199ms, 最大值 = 203ms, 平均 = 201ms ③

C:\Users\ASUS>
```

●圖9-22 利用ping -a 203.66.88.89反向查詢

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題



## 9-9 ICMP工具程式測試

- ❶ 指出ping -a 106.10.212.150可反向查詢DNS，得知為[www.yahoo.com](http://www.yahoo.com)。
- ❷ 指出Echo request封包的基本設定為4次。這4次的回覆封包(即Echo reply封包)都來自目的端www.hinet.net主機所對應IP位址為106.10.212.150之回應。
- ❸ 指出發出4個Echo request封包，其中最大來回時間值是203ms，最小來回時間值是199ms，平均來回時間值是201ms。所謂來回時間(Round Trip Time)指發出Echo request封包至目的端的時間，加上回應Echo reply封包至發送端的時間。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

# 9-9 ICMP工具程式測試

表9-4 tracert的參數種類說明

-d	不執行位址至主機名稱的解析。
-h maximum_hops	搜尋目標最大限制的跳躍數。
-j host-list	用host-list所指定的主機清單的路徑(鬆散路由來源)來傳送封包(僅IPv4)。
-w timeout	等待Echo reply的時間(單位以毫秒計)。
-R	追蹤來回路徑(僅IPv6)。
-S srcaddr	要使用的來源位址(僅IPv6)。
-4	強制使用IPv4。
-6	強制使用IPv6。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

# 9-9 ICMP工具程式測試

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

```

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>tracert www.hinet.net

在上限 30 個躍點上
追蹤 hinet-hp.cdn.hinet.net [175.41.55.1] 的路由:

 1  1 ms    1 ms    1 ms    192.168.1.1
 2  28 ms   27 ms   29 ms   h254.s98.ts.hinet.net [168.95.98.254]
 3  27 ms   27 ms   27 ms   tpdb-3315.hinet.net [168.95.82.42]
 4  33 ms   35 ms   36 ms   sczs-3201.hinet.net [220.128.7.74]
 5  49 ms   44 ms   27 ms   220-128-10-89.HINET-IP.hinet.net [220.128.10.89]

 6  28 ms   27 ms   42 ms   tp-gs-c6r2.router.hinet.net [203.75.232.81]
 7  11 ms   147 ms  111 ms   203.78.181.197
 8  168 ms  136 ms  138 ms   218-60-41-175.TWGATE-IP.twgate.net [175.41.60.21]
 9  52 ms   51 ms   52 ms   174-226-160-203.TWGATE-IP.twgate.net [203.160.226.174]
10  50 ms   49 ms   53 ms   1-55-41-175.TWGATE-IP.twgate.net [175.41.55.1]

追蹤完成。
C:\Users\ASUS>
    
```

圖9-23 tracert www.hinet.net



## 9-9 ICMP工具程式測試

- ①指出追蹤www.hinet.net的路徑，最大hops值為30。
- ②指出每部路由器會回應3次，所以有3次回應時間，例如編號2的路由器3次回應時間分別為28ms、27ms和29ms；注意：從來源端主機至目的端主機www.hinet.net主機必須經過9部路由器，亦即編號10為目的端主機。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

# 9-9 ICMP工具程式測試

表9-5 pathping的參數種類說明

-g host-list	host-list所指定的主機清單的路徑(使用鬆散路由來源)來傳送封包。
-h maximum_hops	搜尋目標最大限制的跳躍數。
-i address	指定來源位址。
-n hostnames	不執行位址至主機名稱的解析。
-p period	Echo request封包之間的時間間隔(毫秒計)。
-q num_queries	每個跳躍點的查詢數。
-w time-out	等待Echo reply的時間(單位以毫秒計)。
-4	強制使用IPv4。
-6	強制使用IPv6。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

```

C:\Windows\system32\cmd.exe
C:\Users\ASUS>pathping www.hinet.net

在上限 30 個躍點上追蹤
hinet-hp.cdn.hinet.net [175.41.55.3] 的路由:
0  ASUS-PCpowerful [192.168.1.161]
1  192.168.1.1
2  h254.s98.ts.hinet.net [168.95.98.254]
3  tpdh-3315.hinet.net [168.95.82.42]
4  TPDT-3011.hinet.net [220.128.1.10]
5  220-128-10-89.HINET-IP.hinet.net [220.128.10.89]
6  tp-gs-c6r2.router.hinet.net [203.75.232.81]
7  203.78.181.197
8  218-60-41-175.TWGate-IP.twgate.net [175.41.60.218]
9  202-58-41-175.TWGate-IP.twgate.net [175.41.58.202]
10 3-55-41-175.TWGate-IP.twgate.net [175.41.55.3]

計算統計資料已經過 250 秒...
源自 此節點/連結
躍點 RTT 已遺失/已傳送 = Pct 已遺失/已傳送 = Pct 位址
0 ASUS-PCpowerful [192.168.1.161]
1 1ms 0/ 100 = 0% 0/ 100 = 0% 192.168.1.1
2 50ms 0/ 100 = 0% 0/ 100 = 0% h254.s98.ts.hinet.net [168.95.98.254]
3 45ms 0/ 100 = 0% 0/ 100 = 0% tpdh-3315.hinet.net [168.95.82.42]
4 53ms 2/ 100 = 2% 2/ 100 = 2% TPDT-3011.hinet.net [220.128.1.10]

```

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

●圖9-24 pathping www.hinet.net

## 9-10 ICMP封包的擷取分析

- ▶ ICMP查詢的訊息類型共4組，最常使用的查詢類型是Echo request/Echoreply，也就是來源端主機發送Echo request的ICMP封包給目的端主機，再由目的端主機回應Echo reply的ICMP封包給來源端主機。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-10 ICMP封包的擷取分析

- ▶ 圖 9-25(b) 則指出 Echo request 封包與 Echo reply封包中的ICMP Payload的架構，其包含了識別值(Identifier)、序號(Sequence Number)、選項資料(Option Data)3個欄位：

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-10 ICMP封包的擷取分析

### ► Identifier佔16 bits：

- 作為識別之用。Identifier欄位值可由主機A裝置的程式決定出來。以Windows 7的ping工具程式為例，它所送出Echo request的預設值為4。當主機B收到Echo request封包後，回送Echo reply封包的Identifier欄位值必須與收到的Echo request封包一樣。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

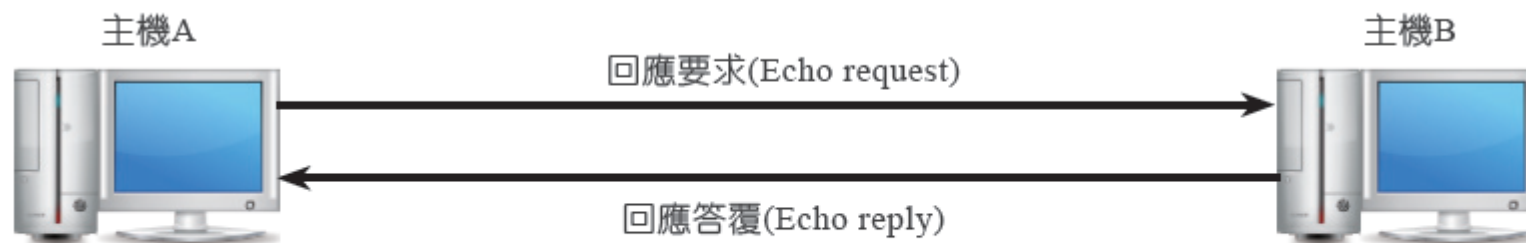
習題

## ► Sequence佔16 bits：

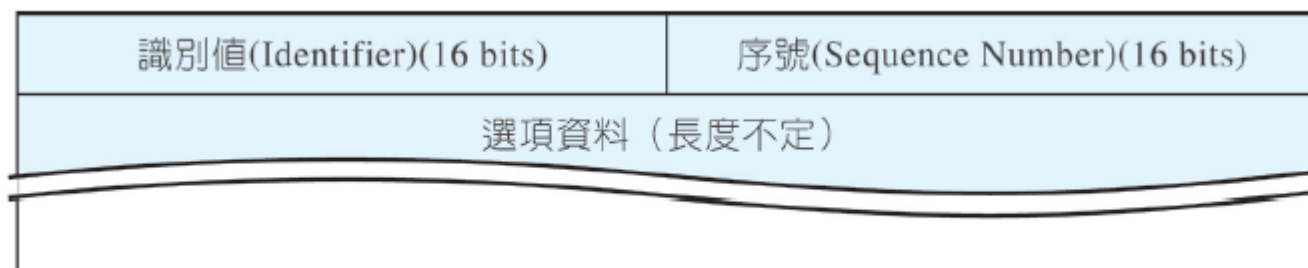
- 用來記錄ICMP封包的序號。Sequence Number欄位值由主機A裝置的程式所決定。它每送出1個Echo request封包，其Sequence Number值就會加1，依此類推。
- 當主機B收到Echo request封包後，回送的Echo reply封包其Sequence Number值必須與收到的Echo request封包一樣。透過Identifier與Sequence Number兩欄位，可識別出特定一組的Echo request與Echo reply封包。



## 9-10 ICMP封包的擷取分析



●圖9-25(a) 主機A與主機B之間的Echo request / Echo reply封包



●圖9-25(b) ICMP Echo request/Echo reply封包中的識別值，序號及ICMP Payload

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題



# 9-10 ICMP封包的擷取分析- Echo request封包

9-1

9-2

9-3

9-4

9-5

9-6

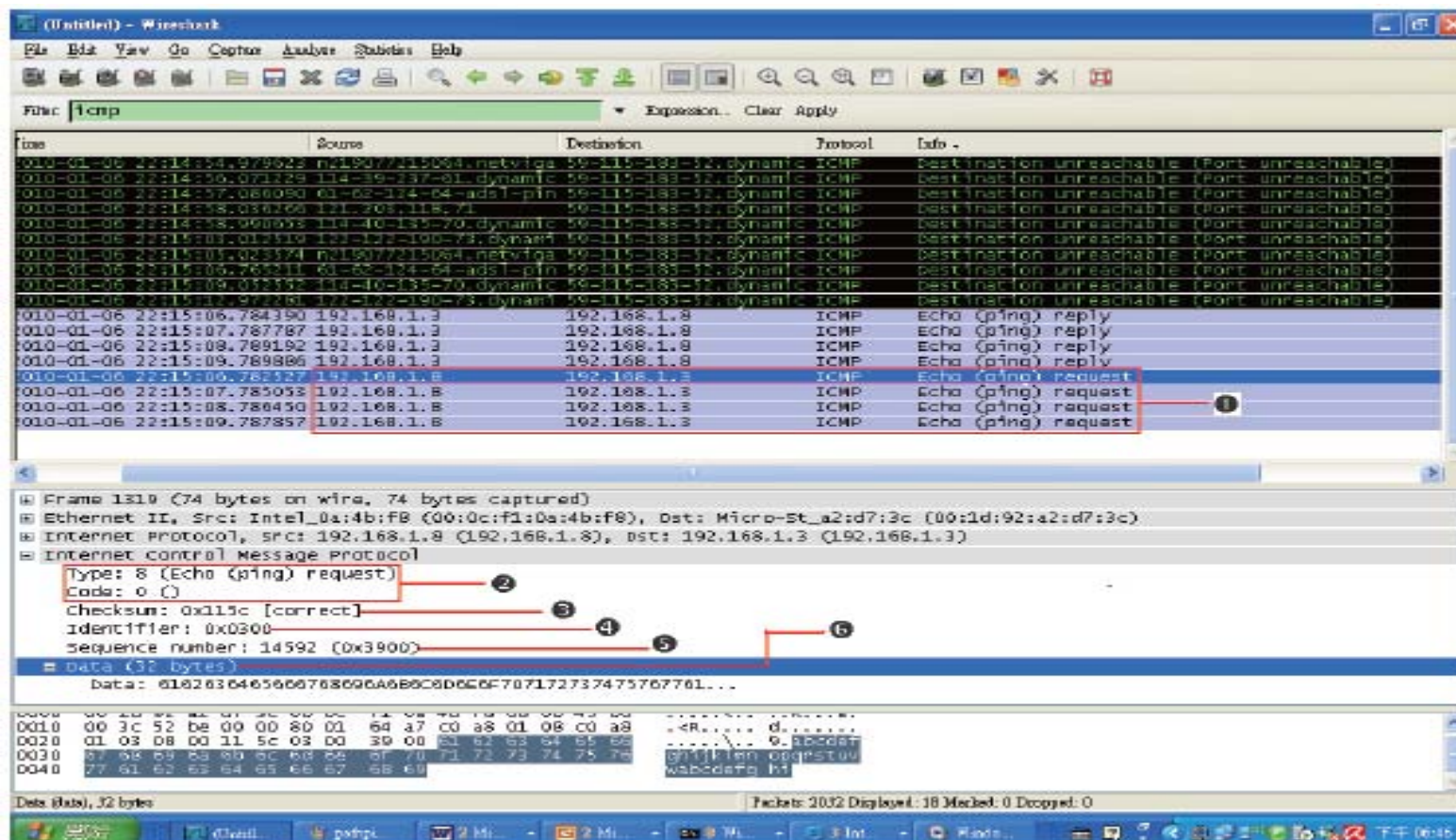
9-7

9-8

9-9

9-10

習題



● 圖9-26(a) ICMP Echo request封包

## 9-10 ICMP封包的擷取分析- Echo request封包

- ❶ 指出第1對的Echo request(預設值共4對Echo request) 封包。
- ❷ 指出Echo request封包的Type = 8，Code為0。
- ❸ 指出錯誤檢查和。注意主機B只要將主機A傳送過來的Echo request封包中的類型值改寫成Echo reply封包的類型值(即0x08改寫成0x00)，並計算出檢查和就可直接回覆封包給主機A。
- ❹ 指出Echo request封包的識別值。若採用Wireshark 1.8x以後的版本，將出現兩個識別值稱為BE(Big Endian)及LE(Little Endian)。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 9-10 ICMP封包的擷取分析- Echo request封包

⑤指出第1對的Echo request封包所記錄的序號是14592(0x3900)。注意每個Echo request封包(共有4個Echo request封包)的序號都不一樣，每送出1個Echo request封包序號就增加1，所以第2個Echo request封包的序號應是14593(0x3901)，第3個Echo request封包的序號應是14594(0x3902)，第4個Echo request封包的序號應是14595(0x3903)。

⑥指出欄位32 bytes所記錄的選項(option)資料。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題



# 9-10 ICMP封包的擷取分析- Echo reply封包

9-1

9-2

9-3

9-4

9-5

9-6

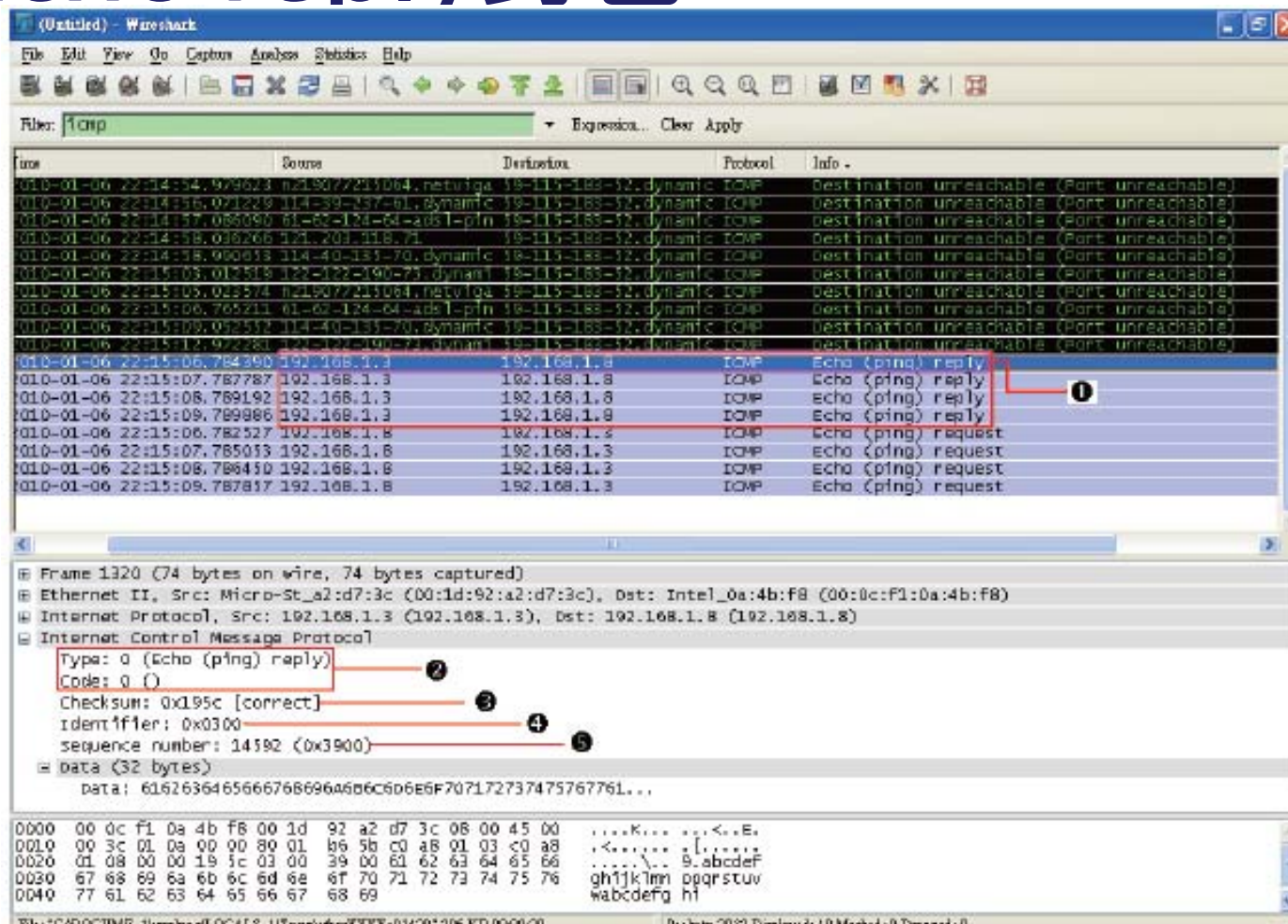
9-7

9-8

9-9

9-10

習題



●圖9-26 (b) Echo reply封包內容

# 9-10 ICMP封包的擷取分析- Echo reply封包

- ❶ 指出第1對的Echo reply(預設值共有4個Echo reply)封包。
- ❷ 指出Echo reply封包的Type = 0，Code為0。
- ❸ 指出錯誤檢查和。
- ❹ 指出Echo reply封包的識別值，由於它與第1個Echo request封包配成一對，故兩者的識別值全為0x0300。
- ❺ 指出如同圖9-26(a) ❺所述，第1個Echo request封包所記錄的序號值為14592(0x3900)，故Echo reply封包所記錄的序號值也為14592(0x3900)。換言之，第1對的Echo request/Echo reply封包所記錄的序號值必須一樣，其值均為14592(0x3900)。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 本章習題

- ▶ ( 2 ) 1. 網際網路的MAC位址長度為多少位元？ (1)32 (2)48 (3)64 (4)128。
- ▶ ( 1 ) 2. 如何得知該網路介面卡是何家製造商所生產？ (1)MAC位址的前3位元組 (2)MAC位址的後3位元組 (3)MAC位址的前後3位元組均可 (4)IP位址的32 bits。
- ▶ ( 1 ) 3. ARP協定在何種網路上操作？ (1)LAN (2)MAN (3)WAN (4)任何一種網路均可。
- ▶ ( 3 ) 4. ARP request是一種什麼樣的封包？ (1)unicast (2)multicast (3)broadcast (4)anycast。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 本章習題

- ▶ ( 1 ) 5. ARP reply是一種什麼樣的封包？ (1)unicast (2)multicast (3)broadcast (4)anycast。
- ▶ ( 2 ) 6. 什麼樣的協定會藉由查詢網路上其他主機而得到自己的IP位址？ (1)ARP (2)RARP (3)ICMP (4)DHCP。
- ▶ ( 4 ) 7. 在IP路由的過程中若發生問題，需將此狀況通知IP封包的來源端，此時會用到什麼樣的協定？ (1)ARP (2)RARP (3)DHCP (4)ICMP。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題

## 本章習題

- ▶ ( 4 ) 8. Echo request與Echo reply是屬什麼樣的封包？  
主要用來解決網路出現的一些問題 (1)ARP (2)RARP  
(3)DHCP (4)ICMP。
- ▶ ( 2 ) 9. ICMP的時間逾時封包會發生在何處？ (1)終端  
節點 (2)中間節點 (3)任何節點 (4)只發生最前端與  
終端節點。
- ▶ ( 2 ) 10. 什麼樣的工具程式可找出至目的端IP位址所經  
過的路由器？ (1)ping (2)tracert (3)DHCP (4)任  
何一種均可。

9-1

9-2

9-3

9-4

9-5

9-6

9-7

9-8

9-9

9-10

習題