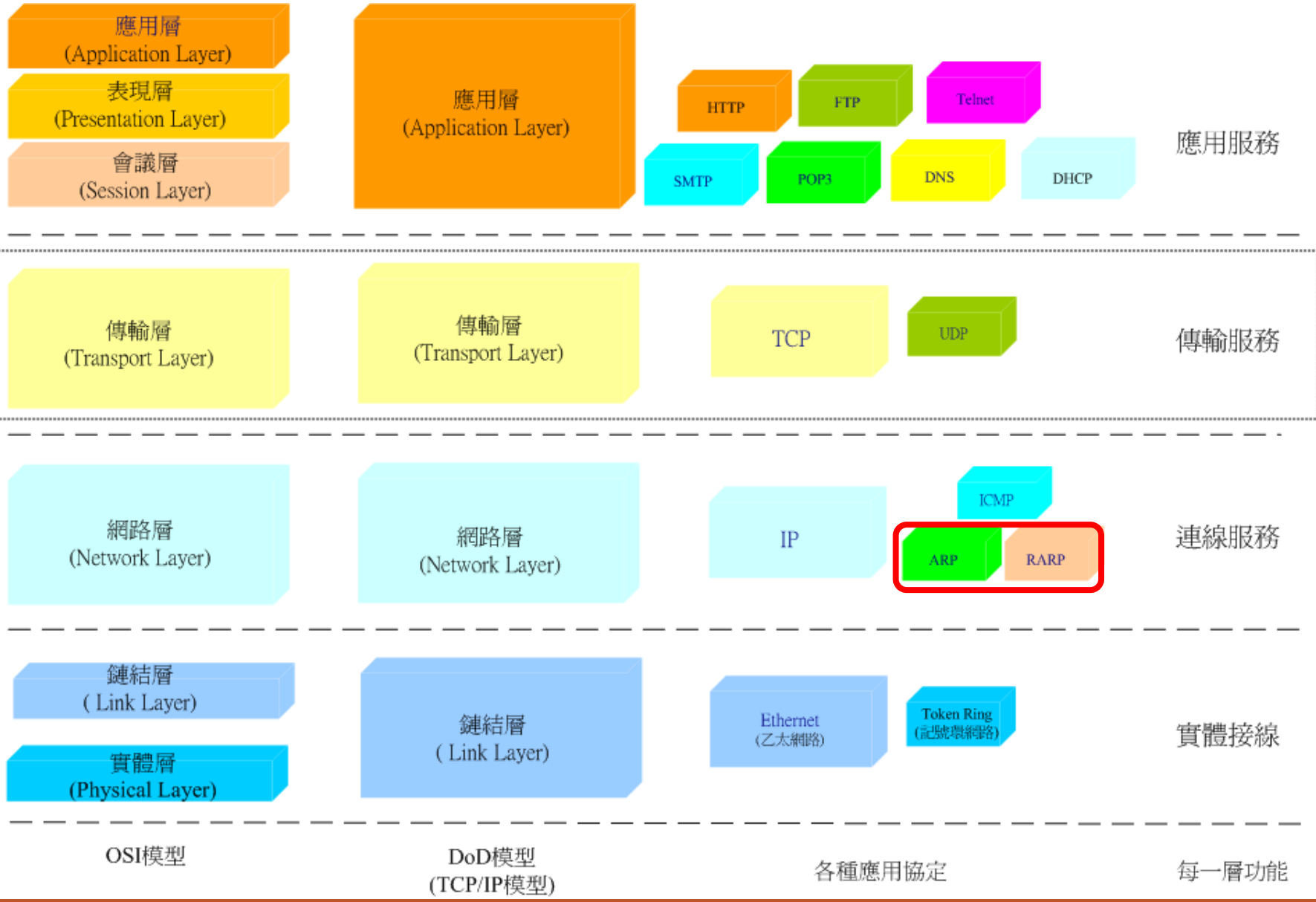
ARP 協定、RARP協定

位址解析協定 (知IP求MAC)

(ADDRESS RESOLUTION PROTOCOL)

反向位址解析協定 (知MAC求IP)

(REVERSE ADDRESS RESOLUTION PROTOCOL, RARP)


應用層
(Application Layer)
表現層
(Presentation Layer)
會議層
(Session Layer)
應用層
(Application Layer)
HTTP
FTP
Telnet
SMTP
POP3
DNS
DHCP
應用服務
傳輸層
(Transport Layer)
傳輸層
(Transport Layer)
TCP
UDP
傳輸服務
網路層
(Network Layer)
網路層
(Network Layer)
IP
ICMP
ARP
RARP
連線服務
鏈結層
(Link Layer)
實體層
(Physical Layer)
鏈結層
(Link Layer)
Ethernet
(乙太網路)
Token Ring
(記號環網路)
實體接線
OSI模型
DoD模型
(TCP/IP模型)
各種應用協定
每一層功能

ARP快取

ARP快取

- ARP快取的紀錄：靜態、動態
  - 由於 ARP 快取儲存在電腦的記憶體中,無論是動態或靜態紀錄, 只要重新開機, 全部都會消失。
- 快取的動態解析紀錄不是永遠有效
  - IP位址變更(例如動態取得IP)
  - 主機已經不在區域網路上(例如關機)
  - 硬體變更(更換網路卡)
- 非詢問對象在收到ARP廣播封包時
  - 可以將發送端的對映紀錄加入自己的快取？
  - 縮短快取紀錄的有效期限解決紀錄快速擴增的問題
- 快取的容量
  - 最佳狀況是能容納區域網路內所有主機的紀錄
  - 容量過小時須定期刪除不常使用到的紀錄
- 定期內部整理(Housekeeping)達到最佳使用效能

ARP 快取

由於 ARP 要求為鏈結層的廣播封包, 如果經常出現, 勢必造成區域網路的沉重負擔。為了避免此項問題, 在實作 ARP 時, 通常會加入 ARP 快取的設計。

快取的英文為 Cache, 意思是將常用 (或是預期將用到) 的資料暫存在讀寫效率較佳的儲存區域, 以加速存取的過程。ARP 快取可將網路裝置的 IP/MAC 位址記錄在本機電腦上 (通常是儲存在記憶體中)。

系統每次要解析 MAC 位址前, 便先在ARP 快取中查看是否有符合的紀錄。若ARP 快取中有符合的紀錄, 便直接使用；若 ARP 快取中找不到符合的紀錄, 才需要發出 ARP 要求的廣播封包。如此, 不僅加快位址解析的過程, 也可避免過多的ARP 要求廣播封包。

。

動態紀錄

當 ARP 完成每筆 IP/MAC 位址的解析後, 便會將結果儲存在 ARP 快取中, 供後續使用, 以避免重覆向同一對象要求位址解析。這些由 ARP 自動產生的紀錄即為動態紀錄。

以先前A、B 電腦為例, 當 A 電腦經由ARP 要求和 ARP 答覆取得 B 電腦的MAC 位址後, 便將 B 電腦的 IP 位址與MAC 位址儲存在 A 電腦的 ARP 快取中。

ARP 快取的動態紀錄雖然可提高位址解析的效能, 但也可能產生問題。

動態紀錄

這些封包傳送出去後不會有任何裝置加以處理, 就好像是丟到黑洞一樣有去無回, 此種現象稱為**網路黑洞**。

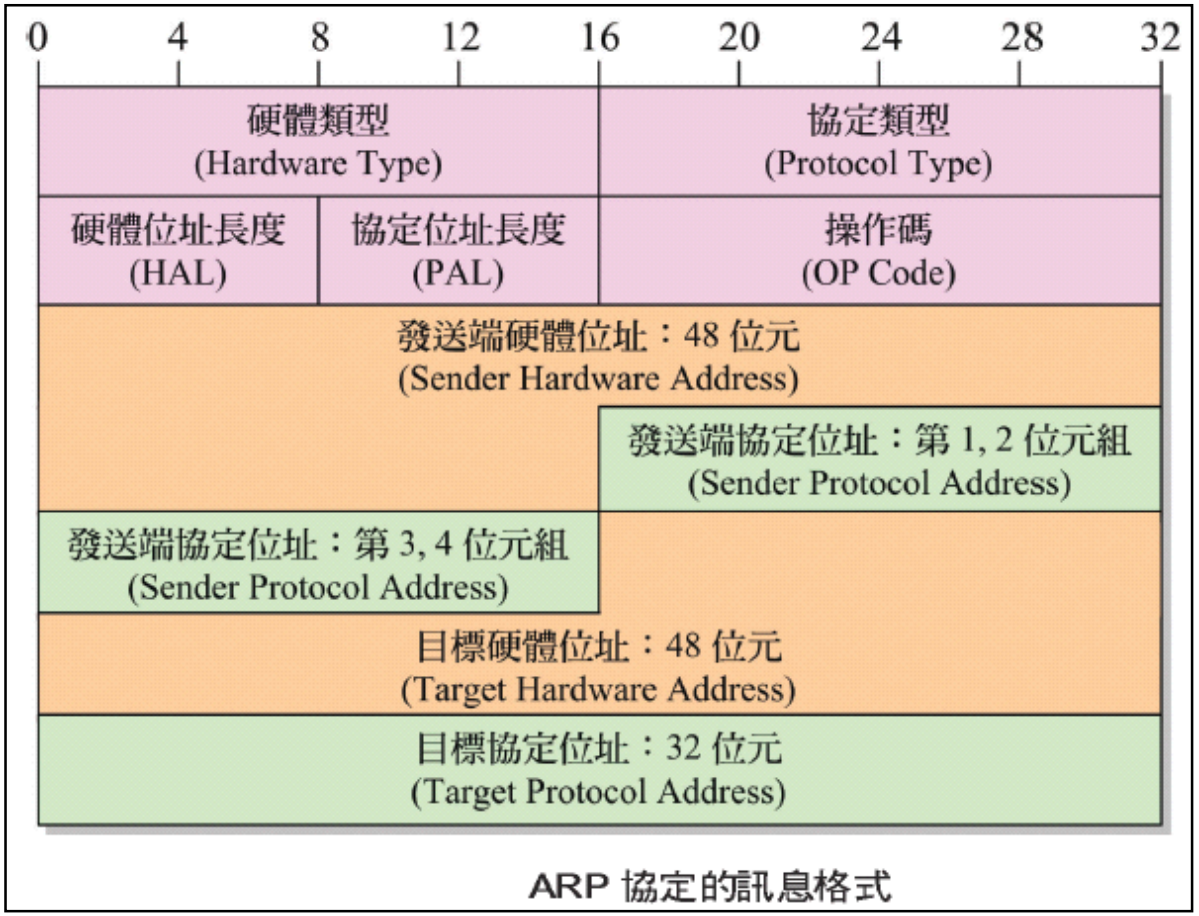
為了避免此種情形發生, ARP 快取中的動態紀錄必須有一定的壽命時間, 超過時間的紀錄便會被刪除。

靜態紀錄

當使用者已知某裝置的 IP/MAC 位址的對應關係後, 可經由手動的方式將之加入ARP 快取中, 此即為靜態紀錄。

ARP訊息格式

ARP訊息格式



ARP 協定的訊息格式

例子：ARP 封包

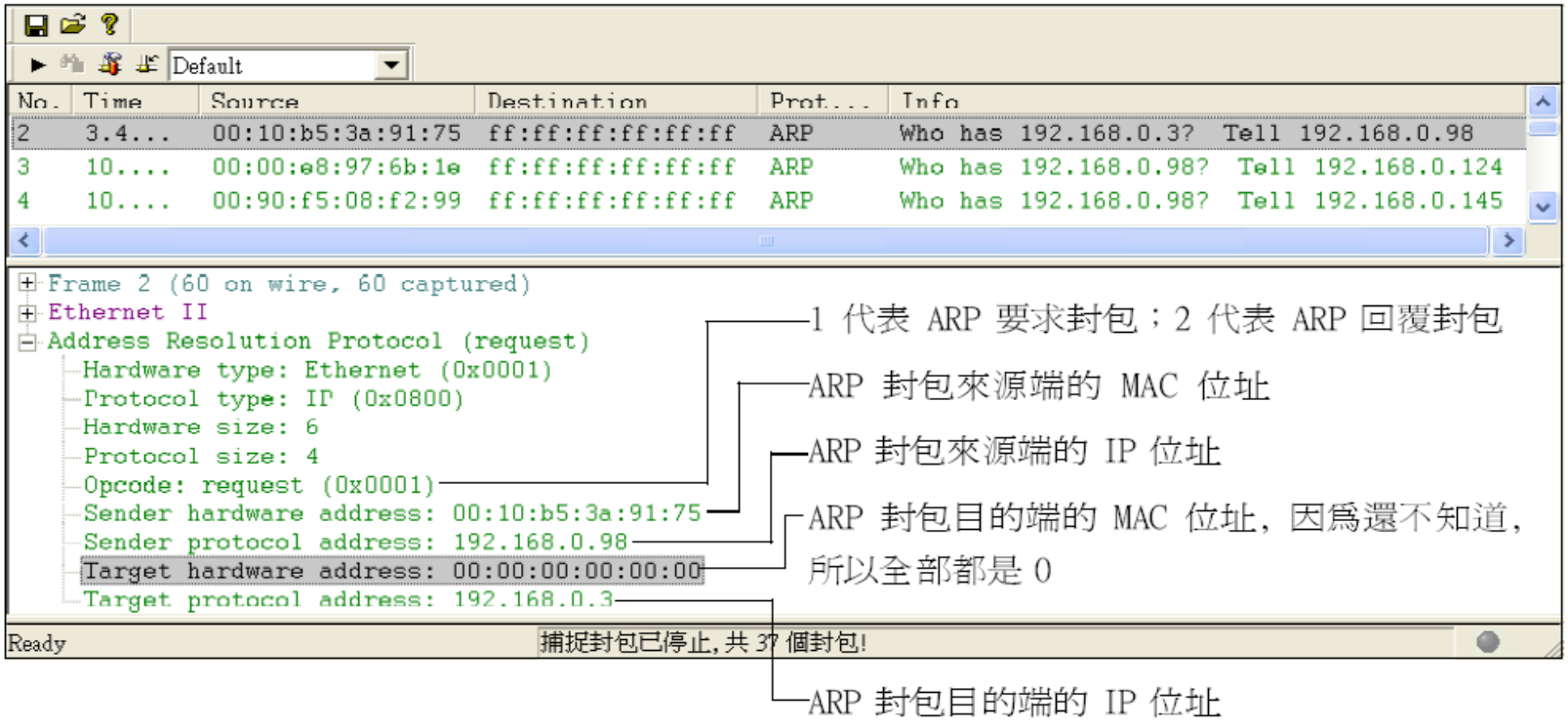


圖 10-04 ARP 要求封包的檔頭內容

ARP 工具程式

ARP 工具程式

提供了 ARP.EXE 這個工具程式, 方便使用者檢視與編輯 ARP快取的內容, 它主要提供了『檢視紀錄』、『刪除紀錄』和『新增紀錄』等 3 種功能。說明如下。

檢視 ARP 快取中的紀錄

檢視目前 ARP 快取紀錄的語法如下：

```
arp -a
```

請參考以下範例：

```
C:\arp -a
介面: 192.168.0.140 --- 0x9
網址          實體位址          類型
192.168.0.3       00-13-49-60-a4-67     動態
192.168.0.4       00-00-e8-97-73-69     動態
192.168.0.7       00-11-d8-f3-d0-7b     動態
192.168.0.32      00-01-80-0f-24-4d     動態
192.168.0.255     ff-ff-ff-ff-ff-ff     靜態
```

由於中文化的關係，使得欄位名稱無法對齊內容(在 9x/XP 用英文欄位名稱，便能對齊內容)

這是系統自動加入的靜態記錄，對應到廣播位址

刪除 ARP 快取中的紀錄

刪除 ARP 快取紀錄的語法如下：

```
arp -d [IP 位址]
```

請參考以下範例。

```
C:\arp -a
介面: 192.168.0.140 --- 0x9
網址實體位址  類型
192.168.0.1   00-50-18-00-0f-01      動態
192.168.0.3   00-13-49-60-a4-67      動態
192.168.0.40  00-01-80-0d-a5-a5      動態
192.168.0.255 ff-ff-ff-ff-ff-ff      靜態

C:\arp -d 192.168.0.3

介面: 192.168.0.140 --- 0x9
網址      實體位址    類型
192.168.0.1   00-50-18-00-0f-01      動態
192.168.0.40  00-01-80-0d-a5-a5      動態
192.168.0.255 ff-ff-ff-ff-ff-ff      靜態
```

目前有 4 筆紀錄

刪除 192.168.0.3 這個 IP 位址的紀錄

果然少了 192.168.0.3 的紀錄

新增 ARP 快取中的紀錄

在 ARP 快取中新增一筆靜態紀錄的語法如下：

```
arp -s [IP 位址] [MAC 位址]
```

請參考以下範例。

```
C:\arp -s 192.168.0.133 00-80-c8-11-22-33      ←新增這一筆紀錄

介面: 192.168.0.140 --- 0x9
網址          實體位址          類型
192.168.0.1    00-50-18-00-0f-01      動態
192.168.0.40   00-01-80-0d-a5-a5      動態
192.168.0.133  00-80-c8-11-22-33      靜態    ←這就是我們新增的靜態記錄
192.168.0.255  ff-ff-ff-ff-ff-ff      靜態
```

RARP 協定

反向位址解析協定

(REVERSE ADDRESS RESOLUTION PROTOCOL, RARP)

RARP簡介

- RARP 用來解決一台只知道自己實體位址的機器，但不知道邏輯位址的問題。
- 每台電腦或路由器可被給予一個或一個以上的 IP 位址。
- IP位址通常可從存在硬碟的組態檔案中取得。

RARP

RARP 訊息是以廣播方式送到區域網路上，網路上的某台機器知道所有的 IP 位址，會回一個 RARP 的回應訊息，所以要求的機器要跑一個 RARP 用戶端程式，而回應的機器要跑 RARP 的伺服端程式。

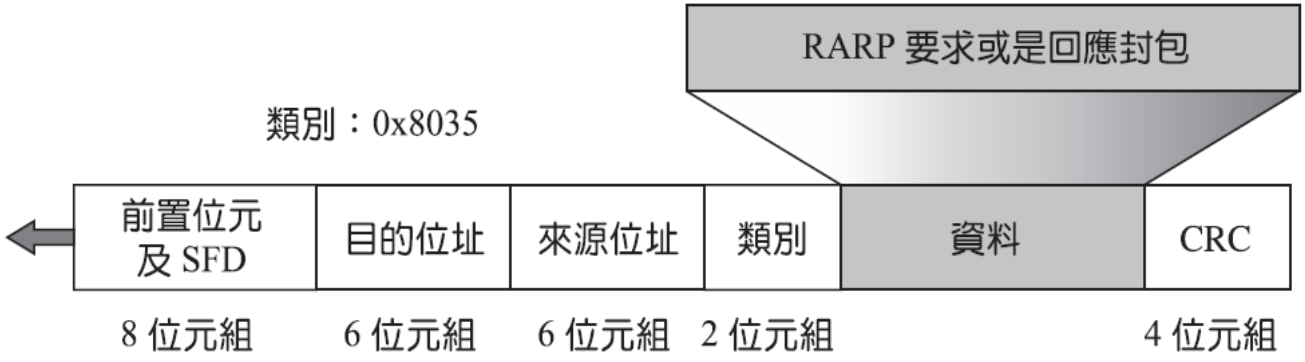
RARP要求封包以廣播的方式傳送；
RARP 回應封包以單點傳播的方式傳送。

RARP 封包的格式

硬體種類		通訊協定種類
硬體長度	通訊協定長度	運作 要求為 3，回應為 4
傳送者硬體位址 （例如：乙太網路為 6 個位元組）		
傳送者通訊協定位址 （例如：IP 為 4 個位元組） （若是要求封包則為空白）		
目標硬體位址 （例如：乙太網路為 6 個位元組） （若是要求封包則為空白）		
目標通訊協定位址 （例如：IP 為 4 個位元組） （若是要求封包則為空白）		

註：RARP 封包的欄位意義與 ARP 封包相同。

Rarp封裝


RARP 要求或是回應封包
類別：0x8035
前置位元及 SFD
目的位址
來源位址
類別
資料
CRC
8 位元組
6 位元組
6 位元組
2 位元組
4 位元組