

# 第八章 ARP 與 ICMP

# 前言

- ◆ 8-1 ARP 簡介
- ◆ 實作練習1：ARP 工具程式
- ◆ 8-2 ICMP 簡介
- ◆ 實作練習2：ICMP 工具：PING

Networking  
Essentials

15th Edition

# 8-1 ARP 簡介

鏈結層與網路層位址的特性：

- ◆ 鏈結層在傳遞封包時, 必須利用鏈結層位址
- ◆ 網路層在傳遞封包時, 必須利用網路層位址
- ◆ 當網路層封包要封裝為鏈結層封包之前, 必須先取得目的裝置的 **MAC** 位址
- ◆ **ARP** 的功能, 便是利用網路層位址來取得對應的鏈結層位址

# ARP 簡介

- ◆ 8-1-1 ARP 運作方式
- ◆ 8-1-2 ARP 快取

*Networking  
Essentials*

15th Edition



## 8-1-1 ARP 運作方式

- ◆ 網路上每部裝置的 IP 位址與 MAC 位址的對應關係並未集中記錄, 因此, 當 ARP 欲取得某裝置的 MAC 位址時, 必須直接向該裝置詢問。
- ◆ ARP 運作過程是由『ARP 要求』(ARP Request) 與『ARP 答覆』(ARP Reply) 兩種封包所組成。

# 8-1-1 ARP 運作方式

## ◆ ARP 要求

A 電腦廣播 ARP 要求封包給區域網路上所有的電腦

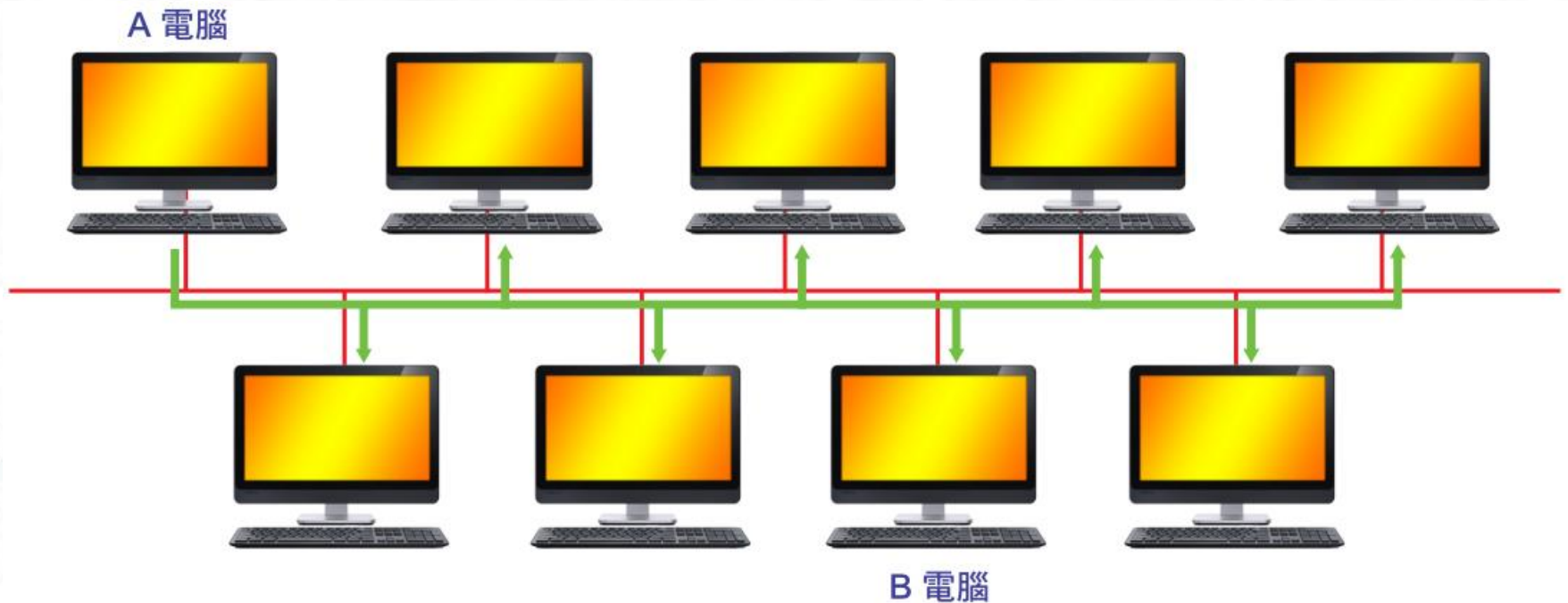


圖 8-1 『ARP 要求』封包會以廣播方式, 送至區域網路上的所有電腦

ARP 要求封包在鏈結層是屬於廣播封包, 因此區域網路上的每一部電腦都會處理此一封包

## ◆ ARP 答覆

B 電腦為 ARP 要求的解析對象, 因此只有 B 電腦會送出回應的 ARP 答覆封包。ARP 答覆封包中最重要內容是 B 電腦的 MAC 位址。A 電腦收到此封包後, 即完成 MAC 位址解析的工作。

## ◆ ARP 的解析範圍

路由器會阻擋乙太網路廣播封包, ARP 僅能解析同一網路內的 MAC 位址, 無法解析其他網路的 MAC 位址

Networking  
Essentials

15th Edition



## 8-1-2 ARP 快取

- ◆ 由於「ARP 要求」為鏈結層的廣播封包, 會造成區域網路的沉重負擔。在實作 ARP 時, 會加入 ARP 快取。
- ◆ ARP 快取可將網路裝置的 IP/MAC 位址記錄在本機電腦上
- ◆ ARP 快取所包含的紀錄, 依產生的方式, 可分為動態與靜態等兩種紀錄。
  - ◆ 動態紀錄
  - ◆ 靜態紀錄

## 8-1-2 ARP 快取

- ◆ 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，以避免重複向同一對象要求答覆 MAC 位址。動態紀錄必須有一定的保存期限，超過此期限的紀錄便會被自動刪除。
- ◆ 靜態紀錄：若已知某裝置的 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。
- ◆ 無論是動態或靜態紀錄，只要重新開機，全部都會消失

# 實作練習1：ARP 工具程式

## ◆ 檢視 ARP 快取中的紀錄

```
arp -a
```

```
C:\>arp -a
```

```
介面: 192.168.0.140 --- 0x9
```

| 網址            | 實體位址              | 類型 |
|---------------|-------------------|----|
| 192.168.0.3   | 00-13-48-60-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 |

這是系統自動加入的靜態記錄，  
對應到廣播位址

# ARP 工具程式

## ◆ 刪除 ARP 快取中的紀錄

```
arp -d [IP 位址]
```

```
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   | 00-13-48-60-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 |

目前有 4 筆紀錄

```
C:\>arp -d 192.168.0.3
```

← 刪除 192.168.0.3 這個 IP 位址的紀錄

```
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 |
| 192.168.0.255 | ff-ff-ff-ff-ff-ff | 靜態 |

← 果然少了 192.168.0.3 的紀錄



# ARP 工具程式

## ◆ 新增 ARP 快取中的紀錄

```
arp -s [IP 位址] [MAC 位址]
```

```
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 |
| 192.168.0.255 | ff-ff-ff-ff-ff-ff | 靜態 |

 ← 這就是我們新增的靜態記錄

## 8-2 ICMP 簡介

ICMP 屬於在網路層運作的協定, 當 IP 路由的過程中若發生問題, 用來通知 IP 封包的來源端。

- ◆ 8-2-1 回應要求與回應答覆
- ◆ 8-2-2 無法送達目的
- ◆ 8-2-3 降低來源端傳送速度
- ◆ 8-2-4 重新導向
- ◆ 8-2-5 傳送逾時

## 8-2-1 回應要求與回應答覆

- ◆ 回應要求與回應答覆 (Echo Request / Echo Reply) 可說是最常見的 ICMP 封包類型, 可用來排解網路問題



圖 8-2 回應要求與回應答覆的運作方式

# 回應要求與回應答覆

1. A 主動發出回應要求封包給 B。
2. B 收到回應要求後, 被動發出回應答覆封包給 A。
  - ◆ B 裝置存在, 且運作正常。
  - ◆ A、B 之間的 IP 路由正常。
  - ◆ A、B 之間的網路連線狀況正常。



## 8-2-2 無法送達目的

- ◆ 無法送達目的 (Destination Unreachable) 也是常見的 ICMP 封包類型
- ◆ 若出現下列問題, 路由器或目的裝置便會發出此類型的 ICMP 封包：
  - ◆ 路由器無法將 IP 封包傳送出去
  - ◆ 目的裝置無法處理收到的 IP 封包

## 8-2-3 降低來源端傳送速度

- ◆ 當路由器因為來往的 IP 封包太多, 以致於來不及處理時, 便會發出降低來源端傳送速度 (Source Quench) 的 ICMP 封包

Networking  
Essentials

15th Edition

## 8-2-4 重新導向

- ◆ 當路由器發現主機所選的路徑並非最佳路徑時, 會送出 ICMP 重新導向 (Redirect) 封包, 通知主機較佳的路徑

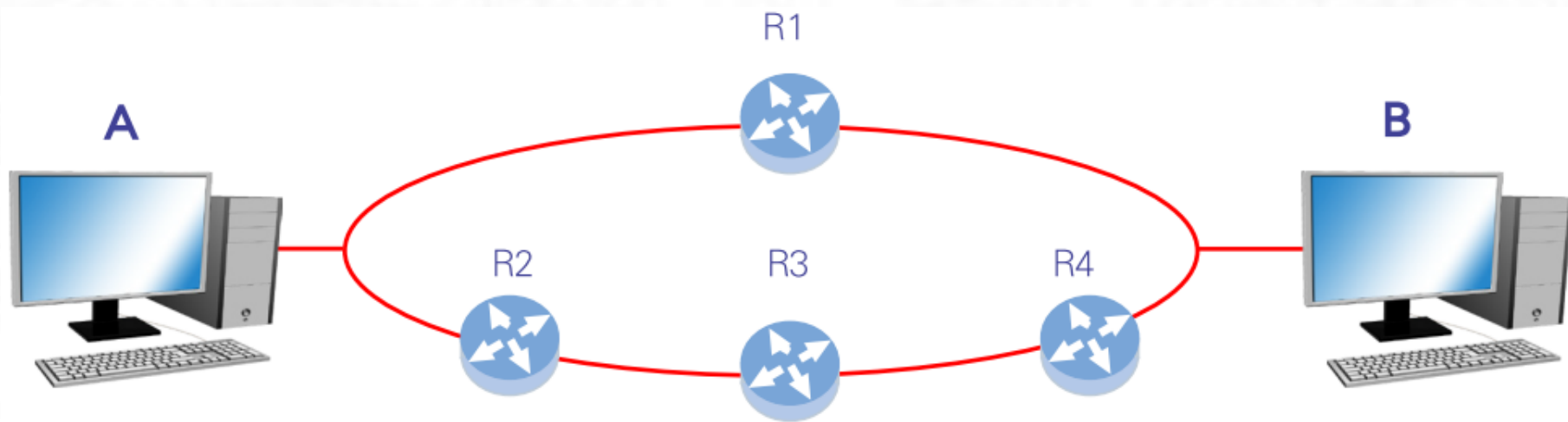


圖 8-3 可能產生 ICMP 重新導向的網路環境

## 8-2-5 傳送逾時

- ◆ 當路由器收到存活時間為 1 的 IP 封包時, 會將此 IP 封包丟棄, 然後送出傳送逾時 (Time Exceeded) 的 ICMP 封包給 IP 封包的來源裝置。
- ◆ 當 IP 封包在傳送過程中發生切割時, 若在指定的時間內未收到全部切割後的 IP 封包, 也會發出傳送逾時的 ICMP 封包



# 實作練習2：ICMP 工具程式： PING

## ◆ PING

1. ping 127.0.0.1
2. ping 本機 IP 位址
3. ping 對外連線的路由器
4. ping 網際網路上電腦的 IP 位址
5. ping 網際網路上電腦的網址

# ICMP 工具程式：PING

PING [參數] [網址或 IP 位址]

| 參數        | 意義   |
|-----------|--|
| -a        | 執行 DNS 反向查詢 (由 IP 位址查出 FQDN, 詳見第 12 章), 預設不會執行此查詢。 |
| -i <存活時間> | 設定 IP 封包的存活時間, 預設為 128。                            |
| -n <封包數量> | 每次執行時, 發出回應要求封包的數量, 預設為 4。                         |
| -t        | 持續發出回應要求封包, 直到按 <b>Ctrl</b> + <b>C</b> 才停止。        |
| -w <等待時間> | 等待回應答覆的時間。<等待時間> 的單位為千分之一秒, 預設值為 1000, 亦即 1 秒。     |

# ICMP 工具程式：PING

```
C:\>ping -a 168.95.192.1
```

從 IP 位址查出來的網域名稱  
(又稱 FQDN, 詳見第 12 章)

```
Ping hntpl.hinet.net [168.95.192.1] 具有 32 位元組的資料:
```

```
回覆自 168.95.192.1: 位元組=32 時間=1ms    TTL=128
```

```
回覆自 168.95.192.1: 位元組=32 time<1ms    TTL=128
```

```
要求等候逾時。
```

← 超過預設的等待時間未獲回應, 便會出現此種訊息

```
要求等候逾時。
```

```
168.95.192.1 的 Ping 統計資料:
```

```
封包: 已傳送 = 4, 已收到 = 2, 已遺失 = 2 (50% 遺失),
```

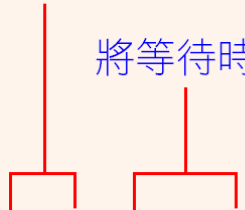
```
大約的來回時間 (毫秒):
```

```
最小值 = 0ms, 最大值 = 1ms, 平均 = 0ms
```

# ICMP 工具程式：PING

設定只發出 2 個回應要求封包

將等待時間延長為 5 秒



```
C:\>ping -n 2 -w 5000 192.168.0.52
```

Ping 192.168.0.52 具有 32 位元組的資料：

回覆自 192.168.0.52：位元組=32 時間 =1ms TTL=128

回覆自 192.168.0.52：位元組=32 time <1ms TTL=128

192.168.0.52 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 = 0ms，最大值 = 1ms，平均 = 0ms