

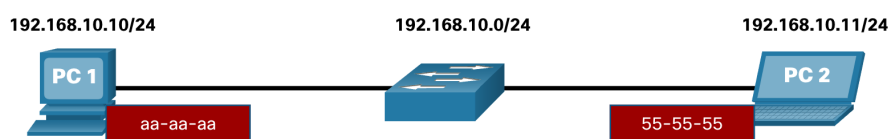
Unit 9

位址解析



MAC 和 IP

- 乙太網路 LAN 上的裝置有兩個主要位址
 - 實體位址 (MAC 位址) — 用於相同乙太網路上的 NIC 與 NIC 通訊
 - 邏輯位址 (IP 位址) — 用於將封包從來源裝置傳送至目的裝置
 - 目的 IP 位址可能與來源位於相同的 IP 網路上，也可能位於遠端網路上

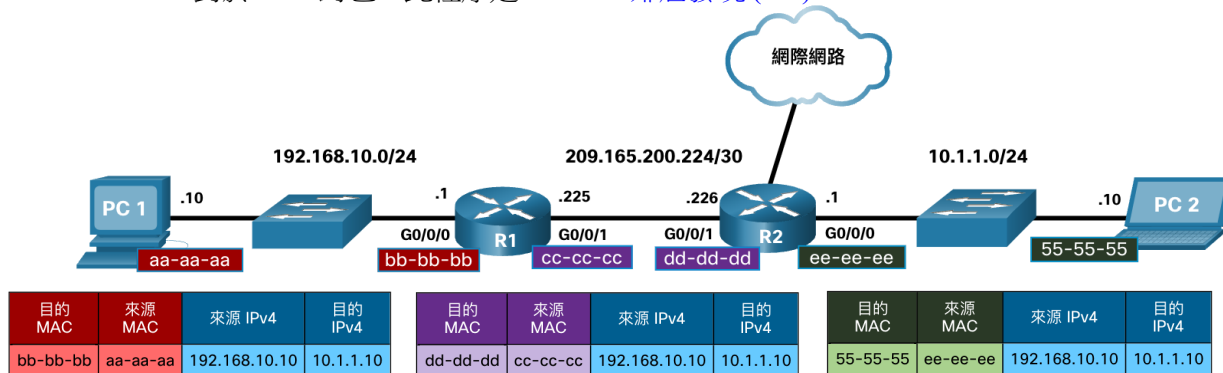


目的 MAC	來源 MAC	來源 IPv4	目的 IPv4
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11



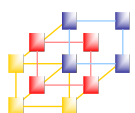
目的位於遠端網路

- 當目的 IP 位址 (IPv4 或 IPv6) 位於遠端網路上時，目的 MAC 位址將會是主機**預設閘道** (即路由器介面) 的位址
- 路由器會檢查**目的 IPv4 位址**，以判斷轉送 IPv4 封包的最佳路徑
- 資料流中 IP 封包的 IP 位址如何與通往目的路徑上的每個連結的 MAC 位址相關聯？
 - 對於 IPv4 封包，這是透過稱為**位址解析協定 (ARP)** 的程序完成
 - 對於 IPv6 封包，此程序是 ICMPv6 **鄰居發現 (ND)**



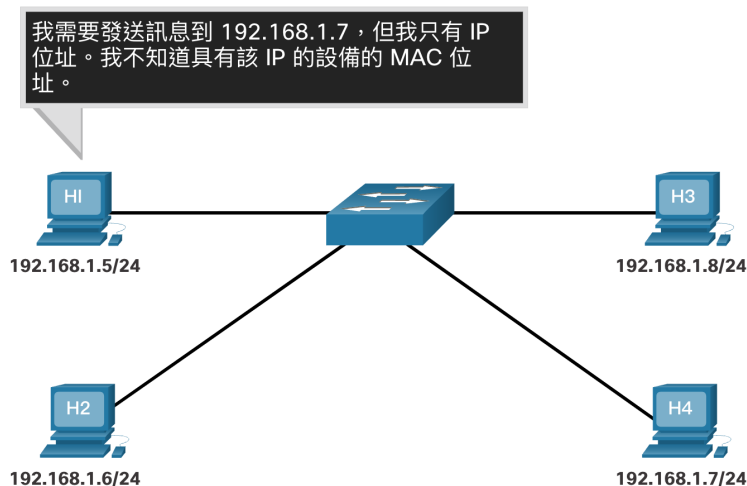
通訊與網路概論

3



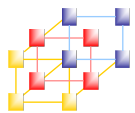
ARP 簡介

- ARP 提供兩個基本功能
 - 將 IPv4 位址解析為 MAC 位址
 - 維護 IPv4 到 MAC 位址的對映表



通訊與網路概論

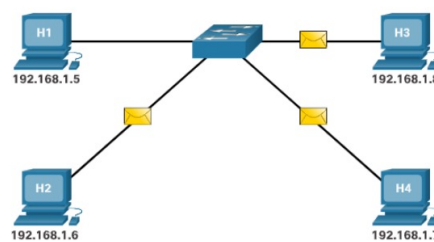
4



ARP 功能

- 當封包被發送到資料連結層封裝成乙太網路訊框時，設備會參考 **ARP 表** 或 **ARP 快取**，找到對映 IPv4 位址的 MAC 位址
 - ARP 表的每個條目或行，將一個 IP 位址與一個 MAC 位址繫結
 - 如果封包的目的 IPv4 位址與來源 IPv4 位址位於相同的網路上，裝置會在 ARP 表中搜尋 **目的 IPv4 位址**
 - 如果目的 IPv4 位址與來源 IPv4 位址位於不同的網路上，裝置將在 ARP 表中搜尋 **預設閘道的 IPv4 位址**

我必須發出 ARP 請求來了解 IP 位址為 192.168.1.7 的主機的 MAC 位址。



通訊與網路概論

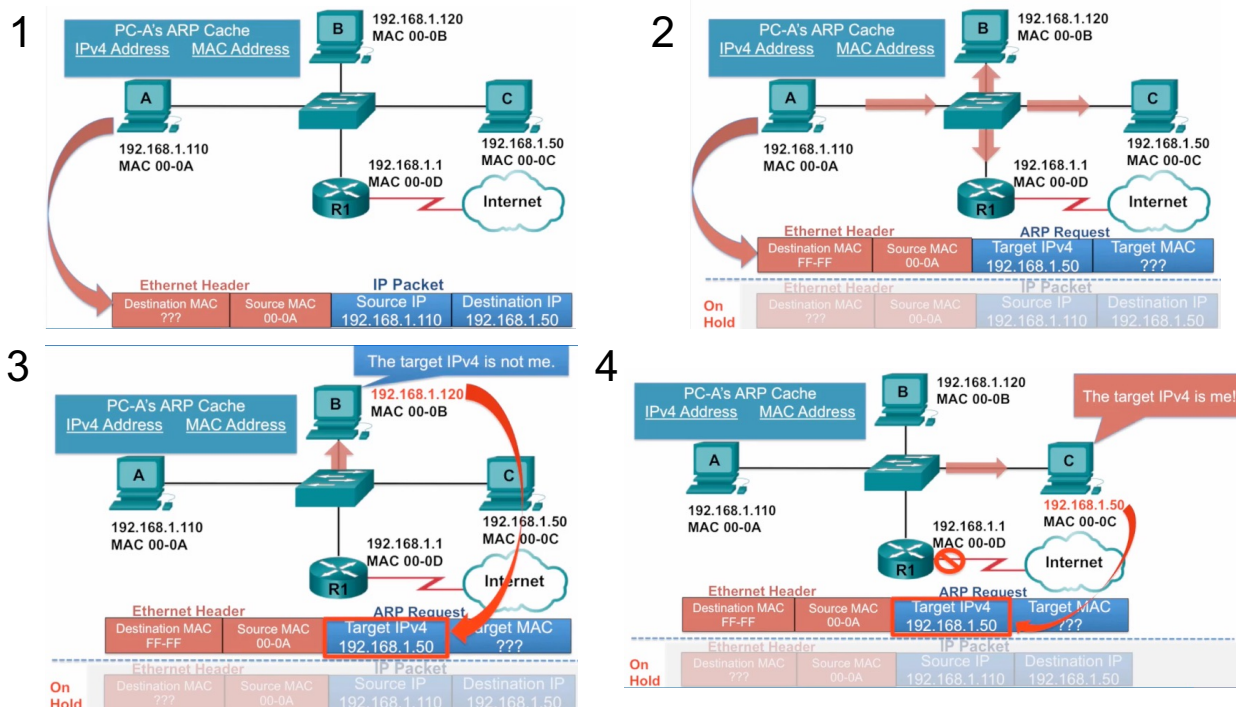


ARP 請求 (1/2)

- 當裝置需要確定與 IPv4 位址相關聯的 MAC 位址，而且其 ARP 表中沒有該 IPv4 位址的條目時，會發送 ARP 請求
 - ARP 請求為廣播
 - 每個裝置都必須處理 ARP 請求，以查看目的 IPv4 位址是否與自己的位址相符
- ARP 請求使用下列標頭資訊封裝在乙太網路訊框中
 - 目的 MAC 位址 — 這是一個廣播位址 FF-FF-FF-FF-FF-FF，要求區域網路上的所有乙太網路 NIC 接受和處理 ARP 請求
 - 來源 MAC 位址 -這是 ARP 請求發送者的 MAC 位址
 - 類型 -ARP 訊息的類型欄位為 0x806。這會通知接收的 NIC 需要將訊框的資料部分傳遞給 ARP 處理程序



ARP 請求 (2/2)

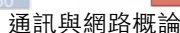


7



ARP 回覆 (1/2)

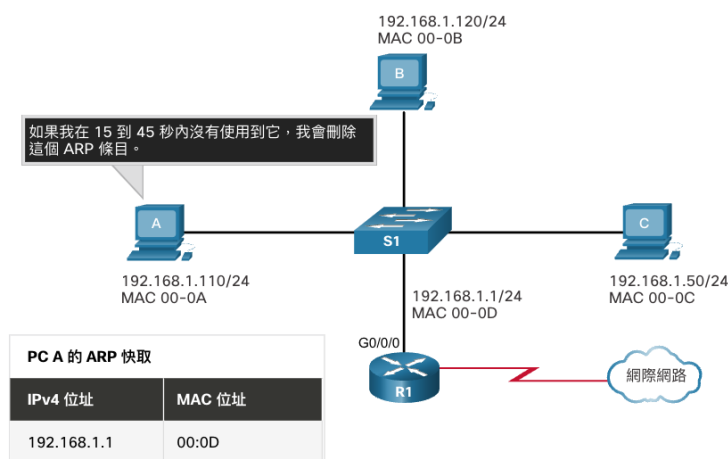
- 只有具有與 ARP 請求相關聯的目的 IPv4 位址的裝置才會以 ARP 回覆作出回應
- ARP 回覆使用下列標頭資訊封裝在乙太網路訊框中
 - 目的 MAC 位址 — 這是 ARP 請求發送者的 MAC 位址
 - 來源 MAC 位址 -這是 ARP 回覆的發送者的 MAC 位址
 - 類型 -ARP 訊息的類型欄位為 0x806。這會通知接收的 NIC 需要將訊框的資料部分傳遞給 ARP 處理程序



C



- ARP 快取計時器將會刪除在指定時間內未使用的 ARP 條目。具體時間取決於裝置的作業系統
 - 例如，較新的 Windows 作業系統會儲存介於 15 到 45 秒之間的 ARP 表條目



注意：MAC 位址縮短以供示範之用。



網路裝置上的 ARP 表

■ 在 Cisco 路由器上

```
R1# show ip arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.10.1 - a0e0.af0d.e140 ARPA GigabitEthernet0/0/0
Internet 209.165.200.225 - a0e0.af0d.e141 ARPA GigabitEthernet0/0/1
Internet 209.165.200.226 1 a03d.6fe1.9d91 ARPA GigabitEthernet0/0/1
R1#
```

■ 在 Windows 10 電腦上

```
C:\Users\PC > ARP -a
介面: 192.168.1.124 --- 0x10
網際網路網址 實體位址 類型
192.168.1.1 c8-d7-19-cc-a0-86 動態
192.168.1.101 08-3e-0c-f5-f7-77 動態
192.168.1.110 08-3e-0c-f5-f7-56 動態
192.168.1.112 ac-b3-13-4a-bd-d0 動態
192.168.1.117 08-3e-0c-f5-f7-5c 動態
192.168.1.126 24-77-03-45-5d-c4 動態
192.168.1.146 94-57-a5-0c-5b-02 動態
192.168.1.255 ff-ff-ff-ff-ff-ff 靜態
224.0.0.22 01-00-5e-00-00-16 靜態
224.0.0.251 01-00-5e-00-00-fb 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
C:\Users\PC >
```

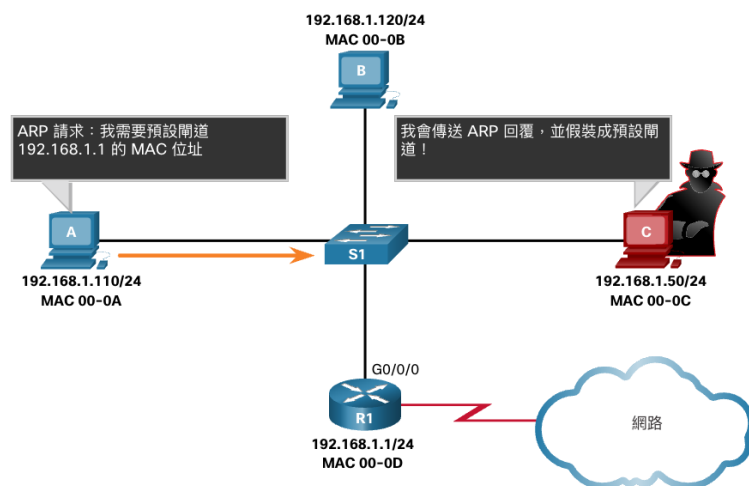
通訊與網路概論

11



ARP 欺騙 (ARP Spoofing)

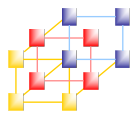
- 攻擊者可以使用 ARP 欺騙來執行 ARP 毒化攻擊
 - 這是威脅行動者用來回覆屬於另一個裝置 (例如預設閘道) 之 IPv4 位址的 ARP 請求的技術



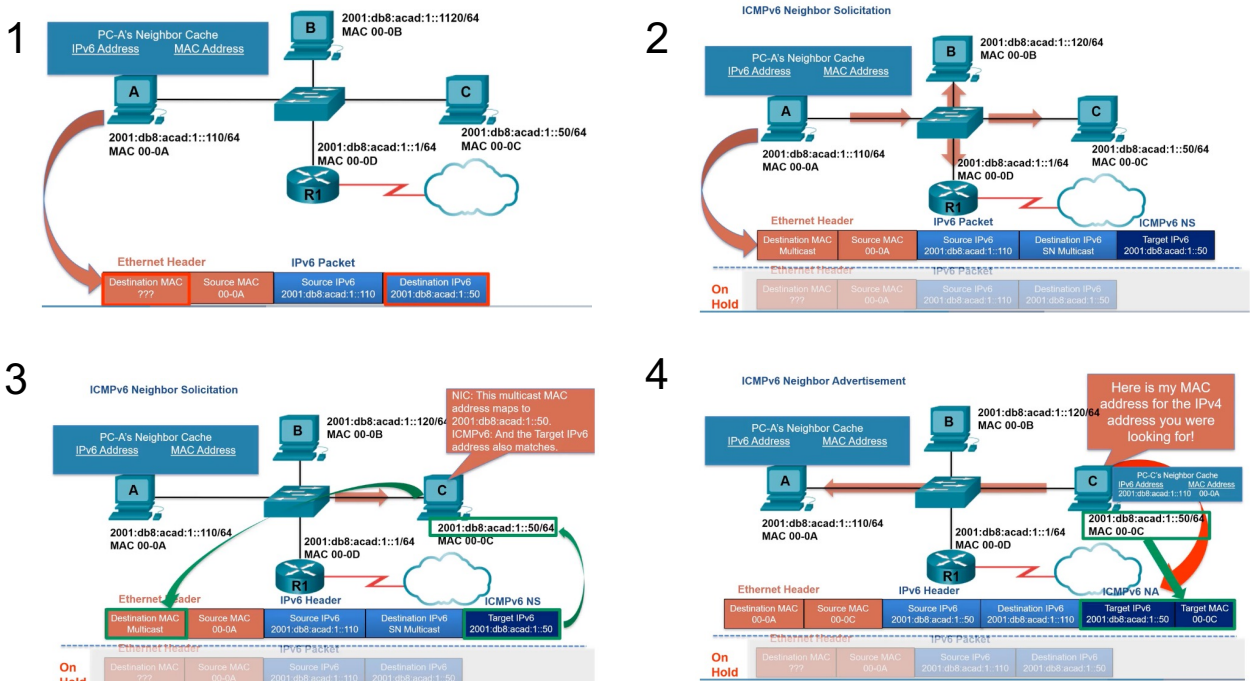
注意: MAC 位址縮短以供示範之用。

通訊與網路概論

12

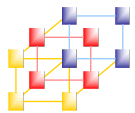


IPv6 鄰居發現 (Neighbor Discovery, ND)

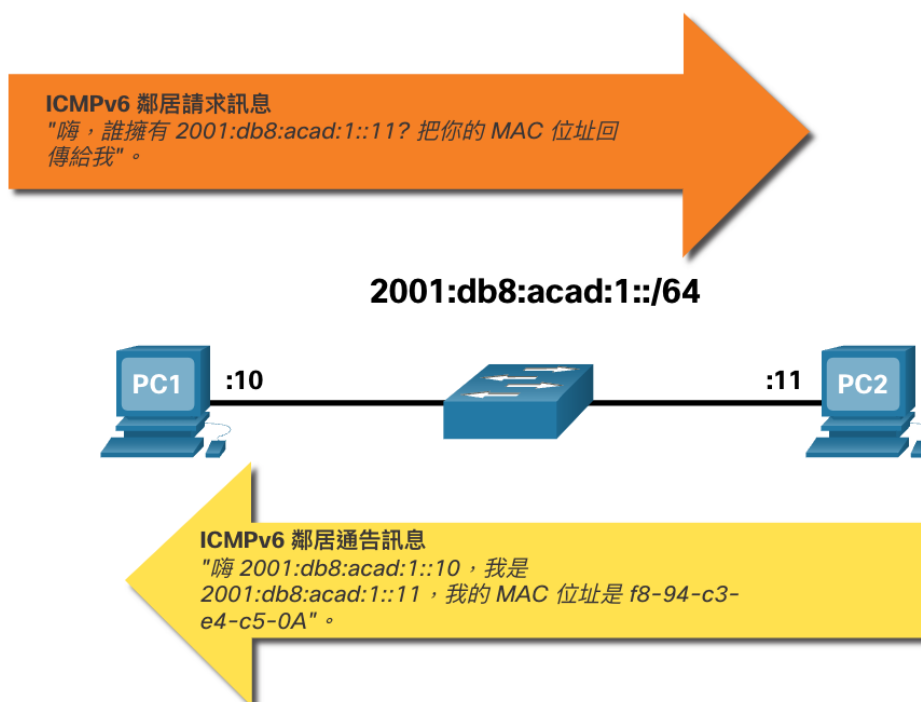


通訊與網路概論

13



IPv6 鄰居發現 - 位址解析



14