Ethernet與ARP封包之觀察與分析

資工三甲 408261292 丁柏瑋

問題與討論

⚠️本處因瀏覽器禁止http連線，故使用指令>> curl GET http://www.fju.edu.tw

1. 根據第一個帶有HTTP GET訊息的封包回答下列問題：
   a. 封包中來源端的Ethernet位址為何？是哪台電腦的位址？

      Source: MegaWell_05:1a:27 (10:5b:ad:05:1:27)

      為本機位置。

   b. 封包中目的地Ethernet位址為何？是否確實為fju.edu.tw主機的Ethernet位址，還是其他電腦？ 請解釋。

      Destination: HitronTe_63:5c:82 (bc:3e:07:63:5c:82)

      為本機連至路由器的位置。

   c. 請寫出「封包類別」欄位的值（用十六進位）。
      Type: IPv4 (0x0800)

   d. 封包的data部分長度為何？
      Data (118 bytes)

2. 根據ARP Request的封包回答下列問題：
   a. 封包中來源端的Ethernet位址為何？是哪台電腦的位址？
      Source: MegaWell_05:1a:27 (10:5b:ad:05:1a:27)
      為本機位置。

b. 封包中目的地Ethernet位址為何？是哪台電腦的位址？請解釋。

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

透過Broadcast通知給所有電腦。

c. 請寫出封包類別欄位的值（用十六進位）。
Type: ARP (0x0806)

d. 請寫出封包Opcode的值（用十六進位）。
Opcode: request (1)

e. 從封包的data欄位部分，寫出下列項目的值：Sender MAC address, Sender IP address, Target MAC address, Target IP address。

```
Sender MAC address: MegaWell_05:1a:27 (10:5b:ad:05:1a:27)
Sender IP address: 192.168.168.14
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.168.1
```

3. 根據ARP Reply的封包回答下列問題：

a. 封包中來源端的Ethernet位址為何？是哪台電腦的位址？
Source: HitronTe_63:5c:82 (bc:3e:07:63:5c:82)
為本機位置。

b. 封包中目的地Ethernet位址為何？是哪台電腦的位址？
Destination: MegaWell_05:1a:27 (10:5b:ad:05:1a:27)
為本機連至路由器的位置。

c. 請寫出封包類別欄位的值（用十六進位）。
Type: ARP (0x0806)

d. 請寫出封包Opcode的值（用十六進位）。
Opcode: reply (2)

e. 從封包的data欄位部分，寫出下列項目的值：Sender MAC address, Sender IP address, Target MAC address, Target IP address。

```
Sender MAC address: HitronTe_63:5c:82 (bc:3e:07:63:5c:82)
Sender IP address: 192.168.168.1
Target MAC address: MegaWell_05:1a:27 (10:5b:ad:05:1a:27)
Target IP address: 192.168.168.14
```

4. 寫出實驗步驟2顯示之arp cache的內容，並簡短解釋每一行代表之意義。

```
>>arp -a

介面: 140.136.20.229 --- 0x9
(在此介面的ARP快取表)    (類型)
  網際網路網址           實體位址                類型
  (IP位置)               (MAC位置)               (該位置使用何種記錄方式)
  140.136.1.254          00-78-88-32-ec-00       動態
  140.136.52.194         80-a5-89-23-43-47       動態
  140.136.63.255         ff-ff-ff-ff-ff-ff       靜態
  224.0.0.2              01-00-5e-00-00-02       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
  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
```

5. 你的電腦中的arp cache裡的紀錄大概經過多久就會被清除？
進入命令列後使用 netsh 進入 interface ipv4。
執行命令 show interface

```
netsh interface ipv4>show interface

Idx     Met         MTU          狀態                名稱
---  ----------  ----------  ------------  ---------------------------
  1          75  4294967295  connected     Loopback Pseudo-Interface 1
  9          50        1500  connected     Wi-Fi
 12          25        1500  disconnected  區域連線* 1
 19           5        1500  disconnected  乙太網路
  4          25        1500  disconnected  區域連線* 10
 10          25        1500  connected     VirtualBox Host-Only Network
```

找到目標 [Wi-Fi] 記下 Idx : 9

執行命令 show interface 9

觀察 " 公告的路由器存留期 : 1800 seconds " 得 (1800s)=30分鐘。