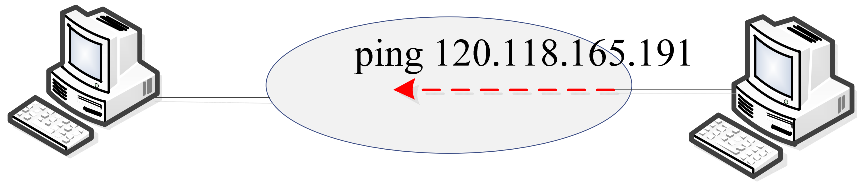
4-2-2 ARP 擷取與分析 - Wireshark (一)

系統分析

- Ping 命令，產生 ARP 封包(> ping 120.118.165.254)

擷取封包步驟

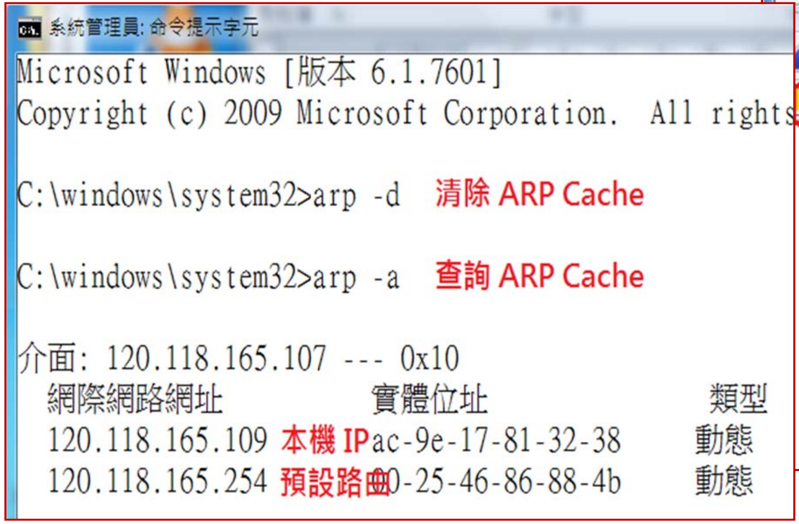
- 清除 ARP Cache



120.118.165.191

120.118.165.107

0806	ARP 封包	PAD

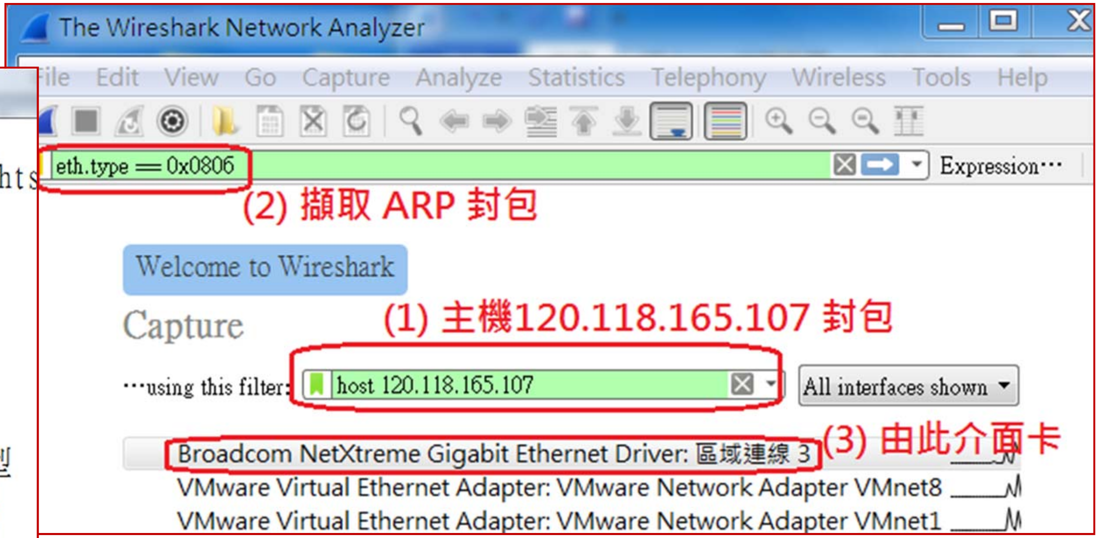


```
Microsoft Windows [版本 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights

C:\windows\system32>arp -d   清除 ARP Cache

C:\windows\system32>arp -a   查詢 ARP Cache

介面: 120.118.165.107 --- 0x10
  網際網路網址           實體位址               類型
  120.118.165.109 本機 IPac-9e-17-81-32-38      動態
  120.118.165.254 預設路由0-25-46-86-88-4b      動態
```


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
Welcome to Wireshark
Capture
All interfaces shown

eth.type == 0x0806

(2) 擷取 ARP 封包

(1) 主機120.118.165.107 封包

…using this filter: host 120.118.165.107

Broadcom NetXtreme Gigabit Ethernet Driver: 區域連線 3

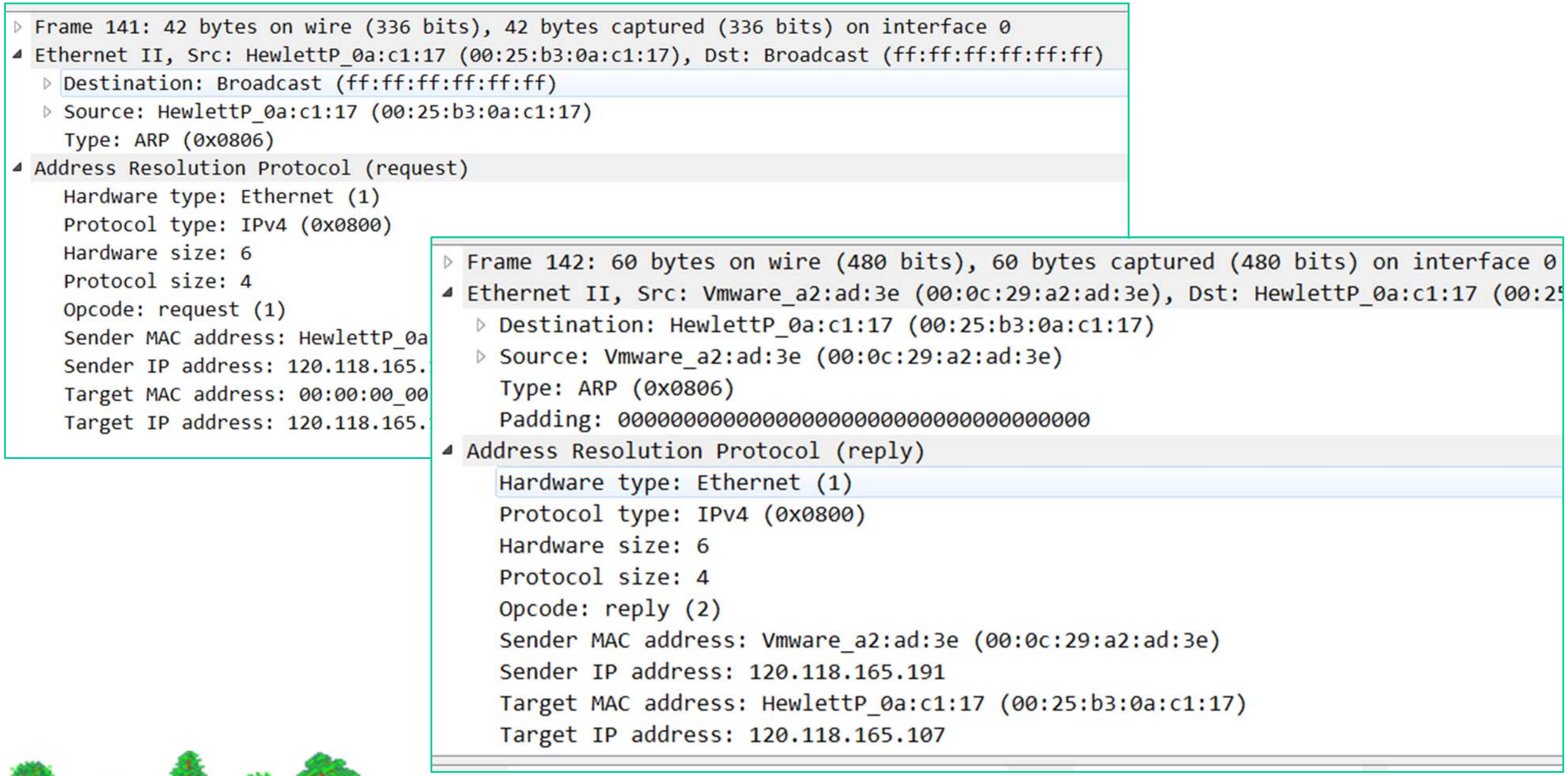
(3) 由此介面卡

VMware Virtual Ethernet Adapter: VMware Network Adapter VMnet8

VMware Virtual Ethernet Adapter: VMware Network Adapter VMnet1

4-2-2 ARP 擷取與分析 - Wireshark (一)

- ARP 協定分析
  - ARP Request 封包標頭、
  - ARP Replay 封包標頭



```
▷ Frame 141: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
◢ Ethernet II, Src: HewlettP_0a:c1:17 (00:25:b3:0a:c1:17), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▷ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▷ Source: HewlettP_0a:c1:17 (00:25:b3:0a:c1:17)
    Type: ARP (0x0806)
◢ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: HewlettP_0a
    Sender IP address: 120.118.165.
    Target MAC address: 00:00:00_00
    Target IP address: 120.118.165.
```

```
▷ Frame 142: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
◢ Ethernet II, Src: Vmware_a2:ad:3e (00:0c:29:a2:ad:3e), Dst: HewlettP_0a:c1:17 (00:25
  ▷ Destination: HewlettP_0a:c1:17 (00:25:b3:0a:c1:17)
  ▷ Source: Vmware_a2:ad:3e (00:0c:29:a2:ad:3e)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
◢ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Vmware_a2:ad:3e (00:0c:29:a2:ad:3e)
    Sender IP address: 120.118.165.191
    Target MAC address: HewlettP_0a:c1:17 (00:25:b3:0a:c1:17)
    Target IP address: 120.118.165.107
```