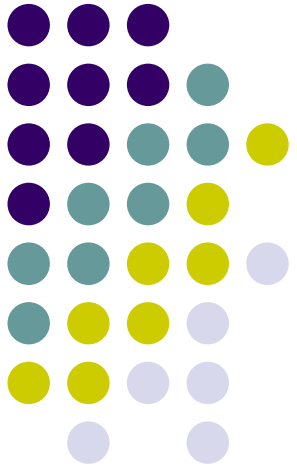
實驗五 ARP協定分析

實驗目的：

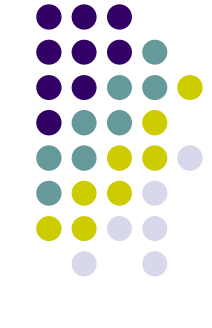
- 明瞭ARP（Address Resolution Protocol；位址解析協定）的工作原理
- 解析ARP協定下封包資料傳送的格式



背景資料

- 在網際網路中只有網路區段的分別，並無區域網路、網域網路、無線網路的分別，而網路區段在邏輯上的定義為網路號相同，在實際上則為ARP封包可以廣播的到。
- ARP負責的是由IP位址尋找網路卡實體位址（MAC），因為真正的網路連線發生在資料鏈結層需要雙方的實體位址，而更高層的連線均為虛擬連線。

ARP原理



- ARP並非網際網路專屬協定，且除非有ARP Proxy機制（代替其它機器的IP位址做出回應）存在，否則ARP僅在網路第二層用廣播方式傳遞，所以ARP會限制在區域網路內操作。
- 區域網路內的所有裝置大多有一個ARP表格（ARP Table）存放於ARP快取記憶區（ARP Cache）之中，記錄著同一區域網路中各裝置的IP位址和MAC位址的對應，加速ARP的處理。

ARP原理

- 裝置送出一個IP封包時，利用網路遮罩逐一確認出目的地址是否屬於相同網路區段以此類推。
- 如屬於相同網路區段，則檢查ARP表格中是否有目的地址的IP位址和MAC位址對，如有就直接將封包傳到該MAC位址。
- 如果沒有，則向區域網路送出一個ARP Request廣播封包查詢目的地址的MAC位址，所有區域網路上的裝置都會處理該請求，檢查IP欄位是自己的，如果是，將發送端的IP位址和MAC位址對更新到自己的ARP表格，然後回應一個ARP Reply封包給發送端，如果不是則忽略。

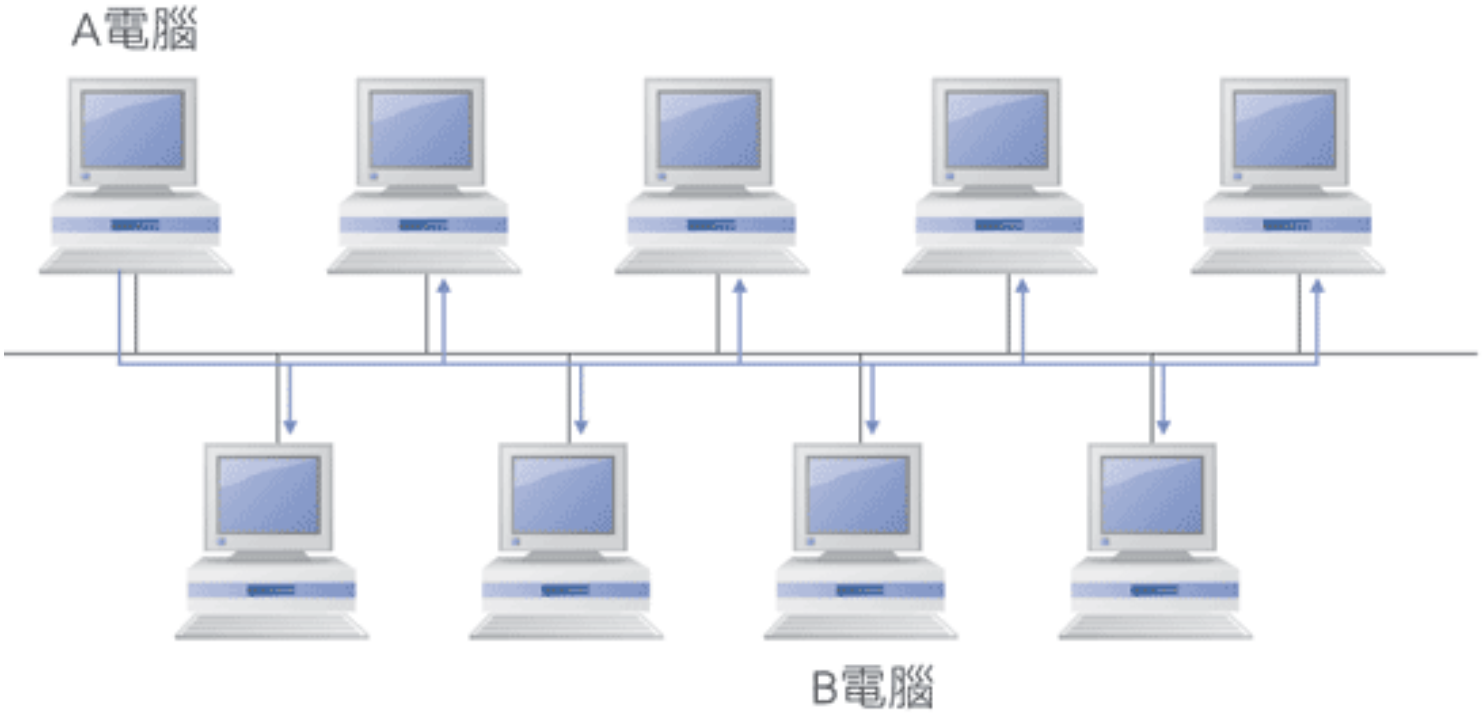
ARP原理

- 當發送端接到ARP Reply封包後更新自己的ARP表格，日後就可以用此記錄來進行傳送，否則宣告傳送失敗。
- 至於不同網路區段的IP位址傳送，由於最後一條紀錄為透過網路遮罩0.0.0.0的運算結果一定是0.0.0.0，所以會透過適當的介面轉發向預設路由器IP位址。
- 一般而言我們也可以說網路的連線是透過許多部路由器，進行多次 ARP解析的結果。

ARP Request與ARP Reply

- ARP運作僅由ARP request（ARP 查詢）與ARP reply（ARP 回應）兩種封包所組成。
- 假設A裝置要傳送IP封包給B裝置，雖然A裝置知道B裝置的IP位址，但是不知道B裝置的MAC位址，因此必須先利用ARP取得B裝置的MAC 位址。
- ARP request封包在資料連結層是封裝成廣播封包，所以區域網路上的每一裝置都會處理此一封包。
- ARP request除了包含A裝置本身的IP位址與MAC位址外，也會記錄所要解析對象的IP位址，即B裝置的IP位址。

ARP Request與ARP Reply

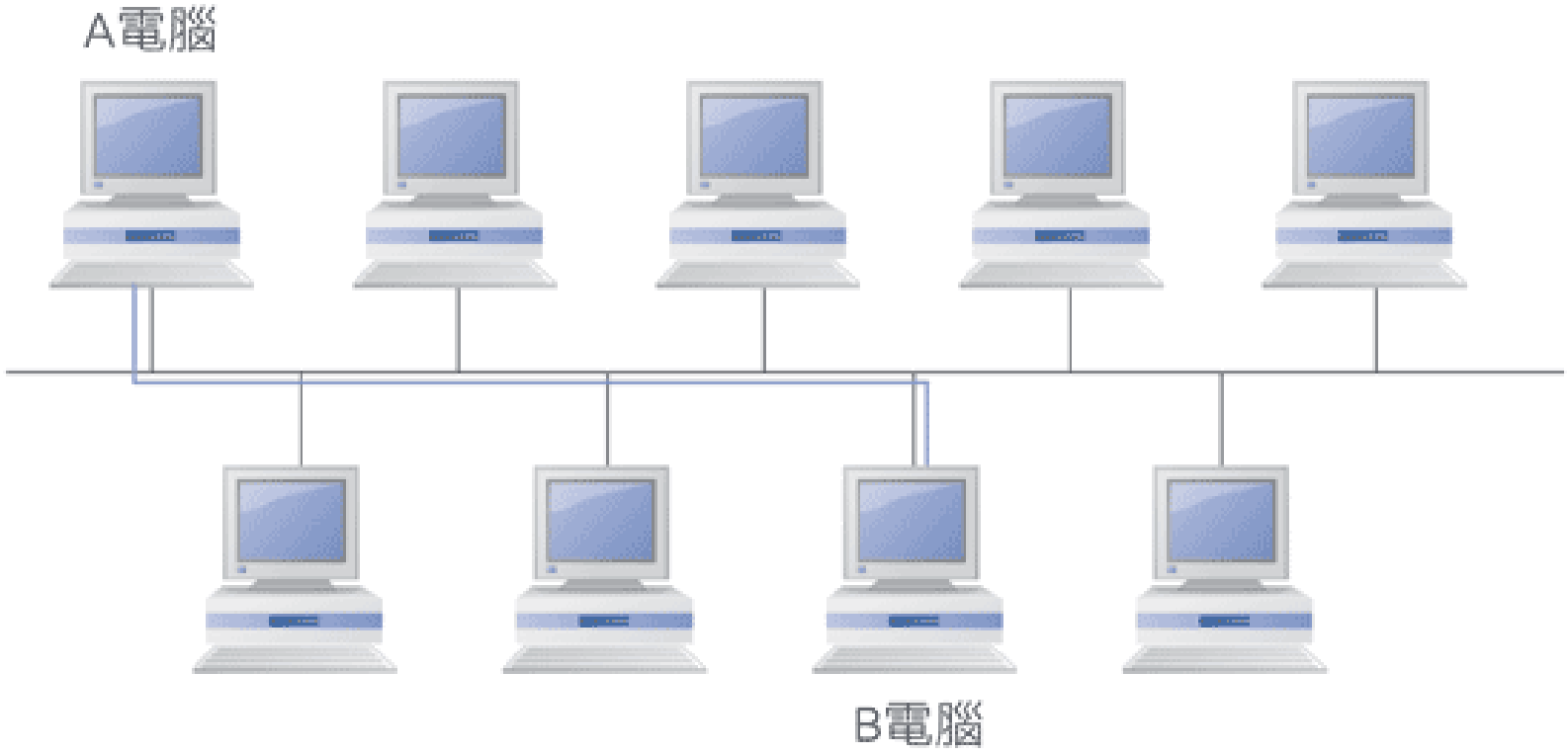


A電腦傳送ARPrequest封包給區域網路上
的所有電腦(雖然只有要詢問電腦B而已)

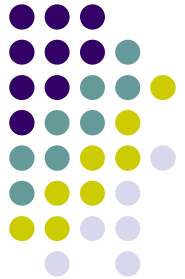
ARP Request與ARP Reply

- 區域網路內的所有裝置都會處理ARP request的封包，並與本身的IP位址比對，判斷出自己是否為此request所要解析的對象，B裝置為ARP request的解析對象，因此只有B 裝置會產生回應的ARP reply封包。

ARP Request與ARP Reply

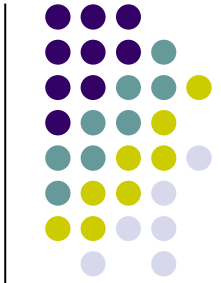


查看ARP記錄



- 在Windows XP中，我們可以利用C:\>arp –a命令來查詢ARP表格，之後可以看到看IP位址和MAC位址的對應，有些系統會用主機名稱和MAC對應，但如果在IP網路中最後是要轉換成IP位址才知道如何傳遞封包。

ARP Cache



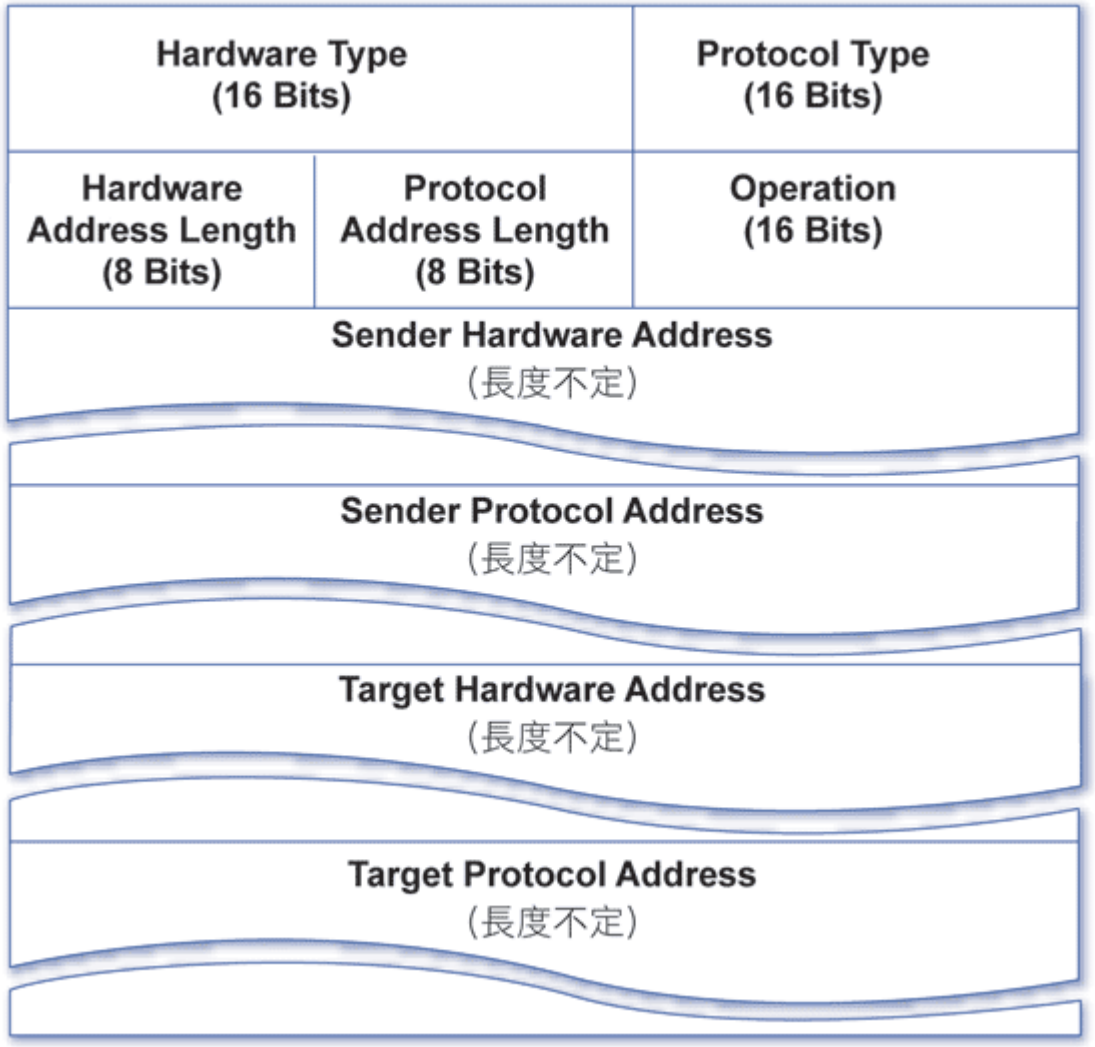
- ARP快取記憶區（ARP Cache）之中，記錄著同一區域網路中各裝置的IP位址和MAC位址的對應，期以加速ARP的處理，因此，只有在cache中找不到符合的記錄時，才會發出ARP request的廣播封包。ARP Cache中所包含的記錄，可分為下列二種：
  - 動態記錄：當ARP完成每筆IP/MAC位址的解析後，便會將結果儲存在ARP Cache中，供後續使用，以避免重複向同一對象要求位址解析，而這些由ARP自動產生的紀錄即為動態記錄。同時為了避免「網路黑洞」的發生，動態紀錄必須有一定的壽命時間，超過此時間的記錄便會被刪除。預設值是紀錄如果在2分鐘內沒有再使用，系統就會將它刪除；如果有被使用到，檢查的時期則會變成10分鐘。

ARP Cache

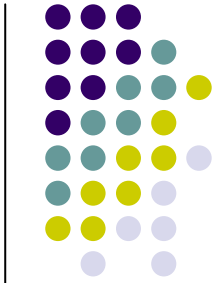
- 靜態記錄：當使用者已知某裝置的IP/MAC位址的對應關係後，可經由手動的方式將某裝置的IP/MAC位址加入ARP Cache中，此即為靜態紀錄。靜態紀錄的壽命限制與動態紀錄不同，只有在下列情況下才會被刪除：
  - 重新開機：由於ARP Cache儲存在電腦的RAM中，因此只要重新開機，不管動態或靜態都會全部消失。
  - 以手動的方式刪除：靜態紀錄是由手動方式加入ARP Cache中，當然也可以由手動的方式刪除。
  - 與動態紀錄衝突：當動態與靜態紀錄出現不一致的情況時，會以動態紀錄為準，刪除靜態紀錄。
- 設置靜態紀錄可以用以下命令：
- arp -s IP MAC

ARP封包格式

ARP封包主要是紀錄IP與MAC位址的相關資料

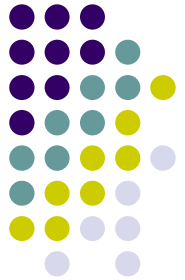


ARP封包格式



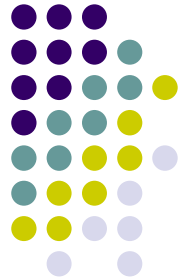
- Hardware Type：長度為2 Bytes，代表發送端主機網路卡的類型，若硬體類型為乙太網路，則此欄位值為1。
- Protocol Type：長度為2 Bytes，說明網路層所使用的協定，若欄位值為0800（16進位），則表示協定採用IP位址進行定址。
- Hardware Address Length（HLEN）：長度為1 Byte，對硬體位址的長度作定義，欄位值以BYTE為單位。例如乙太網路的MAC位址長度為6 Bytes，此欄欄位值即為6。
  Protocol Address Length（PLEN）：長度為1 Byte，網路層協定所使用的位址長度，以BYTE為單位。若ProtocolType為2048（IP），由於IP位址長度為4 Bytes, 因此本欄位值為4。

ARP封包格式



- Operation：長度為2 Bytes，指定ARP封包的類型，最常見的即是Request與Reply兩種類型，欄位值分別為1、2。
- Sender Hardware Address：ARP封包來源端的MAC位址。以乙太網路為例，即為6 Bytes的MAC位址。
- Sender Protocol Address：ARP封包來源端所用協定的位址。以IP為例，即為4 Bytes的IP位址。

ARP封包格式

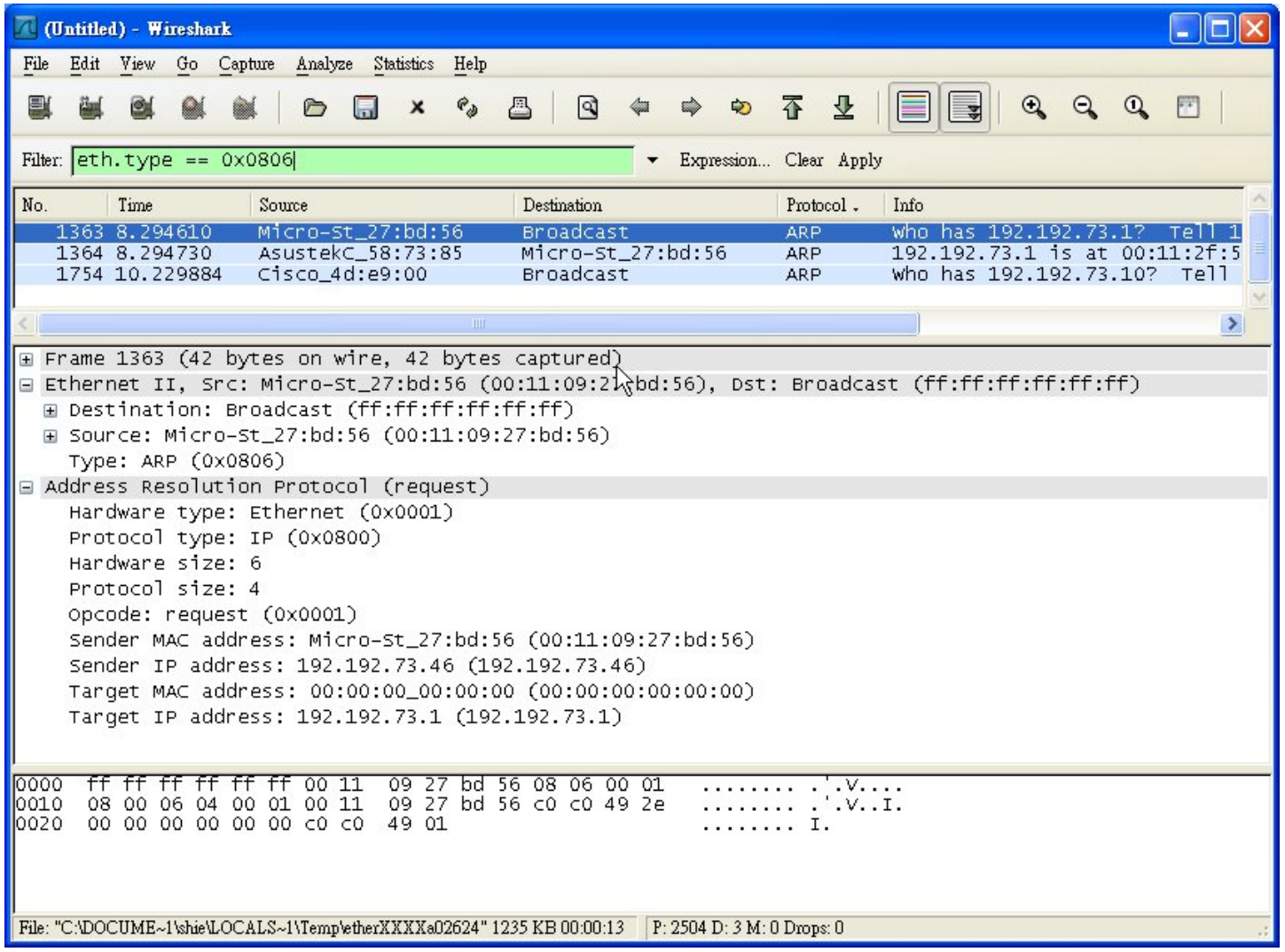


- Target Hardware Address：ARP封包目的端的MAC位址。以乙太網路為例，即為6 Bytes的MAC位址。若是ARP request封包，則本欄位址為00-00-00-00-00-00。
- Target Protocol Address：ARP封包目的端所用協定的位址。以IP為例，即為4 Bytes的IP位址。
- ARP封包的長度：ARP封包的長度並不固定，要視網路層與資料連結層的位址長度。

實驗方法：擷取ARP封包

- 用三個步驟來實驗：
  1. arp -a顯示目前系統中ARP Cache。
  2. Ping 相同網路區段位址。
  3. 用arp -a顯示最新系統中ARP Cache。

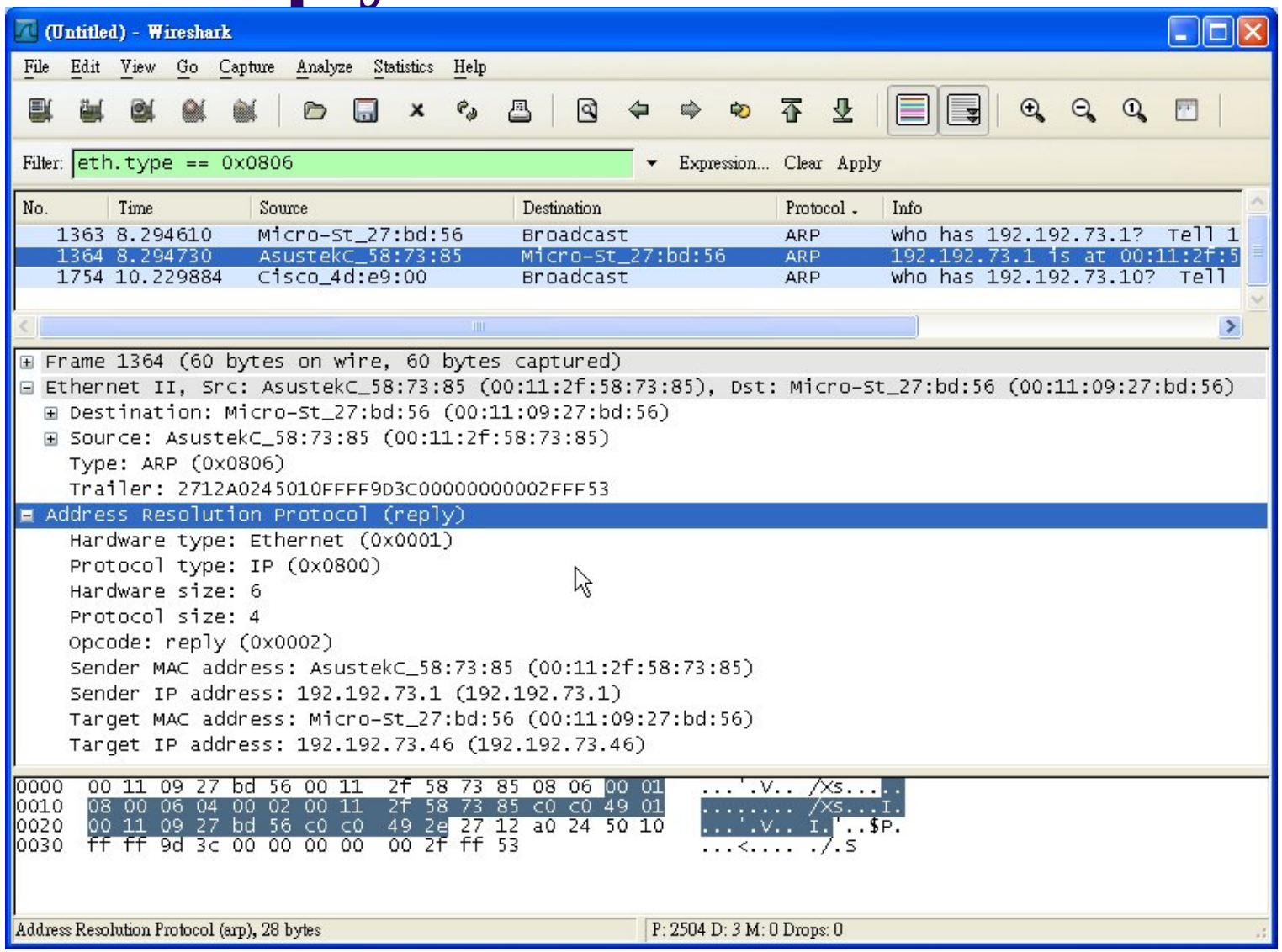
ARP Request


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: eth.type == 0x0806
Expression... Clear Apply
No. Time Source Destination Protocol Info
1363 8.294610 Micro-St_27:bd:56 Broadcast ARP Who has 192.192.73.1? Tell 1
1364 8.294730 AsustekC_58:73:85 Micro-St_27:bd:56 ARP 192.192.73.1 is at 00:11:2f:5
1754 10.229884 Cisco_4d:e9:00 Broadcast ARP Who has 192.192.73.10? Tell
Frame 1363 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: Micro-St_27:bd:56 (00:11:09:27:bd:56), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: Micro-St_27:bd:56 (00:11:09:27:bd:56)
Type: ARP (0x0806)
Address Resolution Protocol (request)
Hardware type: Ethernet (0x0001)
Protocol type: IP (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (0x0001)
Sender MAC address: Micro-St_27:bd:56 (00:11:09:27:bd:56)
Sender IP address: 192.192.73.46 (192.192.73.46)
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.192.73.1 (192.192.73.1)
0000 ff ff ff ff ff ff 00 11 09 27 bd 56 08 06 00 01 ..... .'.V....
0010 08 00 06 04 00 01 00 11 09 27 bd 56 c0 c0 49 2e ..... .'.V..I.
0020 00 00 00 00 00 00 c0 c0 49 01 ..... I.
File: "C:\DOCUME~1\shie\LOCALS~1\Temp\etherXXXXa02624" 1235 KB 00:00:13
P: 2504 D: 3 M: 0 Drops: 0

ARP Request

- 如圖中可觀察ARP Request封包(Filter設定eth. type == 0x0806)
  - Hardware Type = 1(Ethernet)，其十六進位為00 01。
  - Protocol Type = 0x0800 (IP)。
  - Hardware Addr Length = 6 bytes，其十六進位為06。
  - Protocol Addr Length = 4 bytes，其十六進位為04。
  - Operation = 1 (Request)，其十六進位為00 01。
  - Sender Ethernet Addr = 00 11 09 27 bd 56。
  - Sender IP Address = 192.192.73.46。
  - Target Ethernet Addr = 000000000000。
  - Target IP Address = 192.192.73.1。

ARP Reply

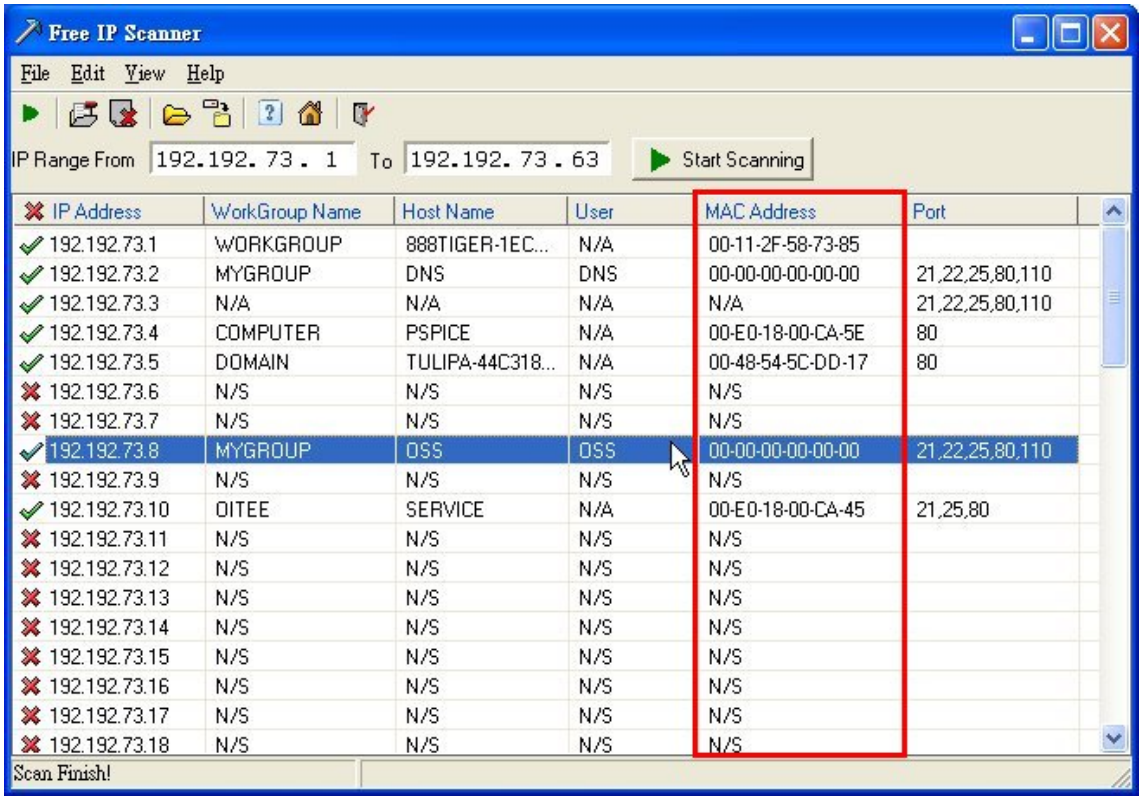

(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: eth.type == 0x0806
Expression... Clear Apply
No. Time Source Destination Protocol Info
1363 8.294610 Micro-St_27:bd:56 Broadcast ARP Who has 192.192.73.1? Tell 1
1364 8.294730 AsustekC_58:73:85 Micro-St_27:bd:56 ARP 192.192.73.1 is at 00:11:2f:5
1754 10.229884 Cisco_4d:e9:00 Broadcast ARP Who has 192.192.73.10? Tell
Frame 1364 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: AsustekC_58:73:85 (00:11:2f:58:73:85), Dst: Micro-St_27:bd:56 (00:11:09:27:bd:56)
Destination: Micro-St_27:bd:56 (00:11:09:27:bd:56)
Source: AsustekC_58:73:85 (00:11:2f:58:73:85)
Type: ARP (0x0806)
Trailer: 2712A0245010FFFF9D3C00000000002FFF53
Address Resolution Protocol (reply)
Hardware type: Ethernet (0x0001)
Protocol type: IP (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (0x0002)
Sender MAC address: AsustekC_58:73:85 (00:11:2f:58:73:85)
Sender IP address: 192.192.73.1 (192.192.73.1)
Target MAC address: Micro-St_27:bd:56 (00:11:09:27:bd:56)
Target IP address: 192.192.73.46 (192.192.73.46)
0000 00 11 09 27 bd 56 00 11 2f 58 73 85 08 06 00 01 ...'.V.. /Xs.....
0010 08 00 06 04 00 02 00 11 2f 58 73 85 c0 c0 49 01 .... /Xs...I.
0020 00 11 09 27 bd 56 c0 c0 49 2e 27 12 a0 24 50 10 ...'.V.. I.'..$P.
0030 ff ff 9d 3c 00 00 00 00 00 2f ff 53 ...<.... ./.S
Address Resolution Protocol (arp), 28 bytes
P: 2504 D: 3 M: 0 Drops: 0

ARP Reply

- 如圖中可觀察ARP Reply封包：
  - Hardware Type = 1(Ethernet)，其十六進位為00 01。
  - Protocol Type = 0x0800 (IP)。
  - Hardware Addr Length = 6 bytes，其十六進位為06。
  - Protocol Addr Length = 4 bytes，其十六進位為04。
  - Operation = 1 (Reply)，其十六進位為00 02。
  - Sender Ethernet Addr = 00 11 2f 58 73 85。
  - Sender IP Address = 192.192.73.1。
  - Target Ethernet Addr = 00 11 09 27 bd 56。
  - Target IP Address = 192.192.73.46。

Free IP scanner

- 使用Free IP scanner來檢視區域網路上所有的IP/MAC對。



學習評量

1. 請說明何謂RARP協定。
2. 如果不支援廣播的通訊協定如ATM，該如何對應IP位址？
3. 請說明ARP Cache的操作過程。
4. 如何將不同的兩個實體區域網路管理成一個單一網路？
5. 請說明ARP協定有無潛在風險？