**Homework 1 ARP**

班級: 資網三A 座號： 16 學號： D1094181017 姓名： 張育丞

**網路實驗名稱：ARP**

說明：檔名為Hw1\_座號.docx，請更改為你座號，請由提供之Hw1\_ARP & ICMP\_學生IP.ppt，修改成自己之IP （圖形及內容之”座號”部分，皆改成自己之IP及自己之MAC）

**註：請同學注意：保留中括符號 【 】，但不輸入Terminal內。截圖紅色方框標記的時候，圖片須清楚 紅色框需框好，如附圖大小，大小和清晰度盡量如附圖(這個很重要： 圖片須清楚 紅色框需框好)**

**（1） ARP實驗之學習動機**

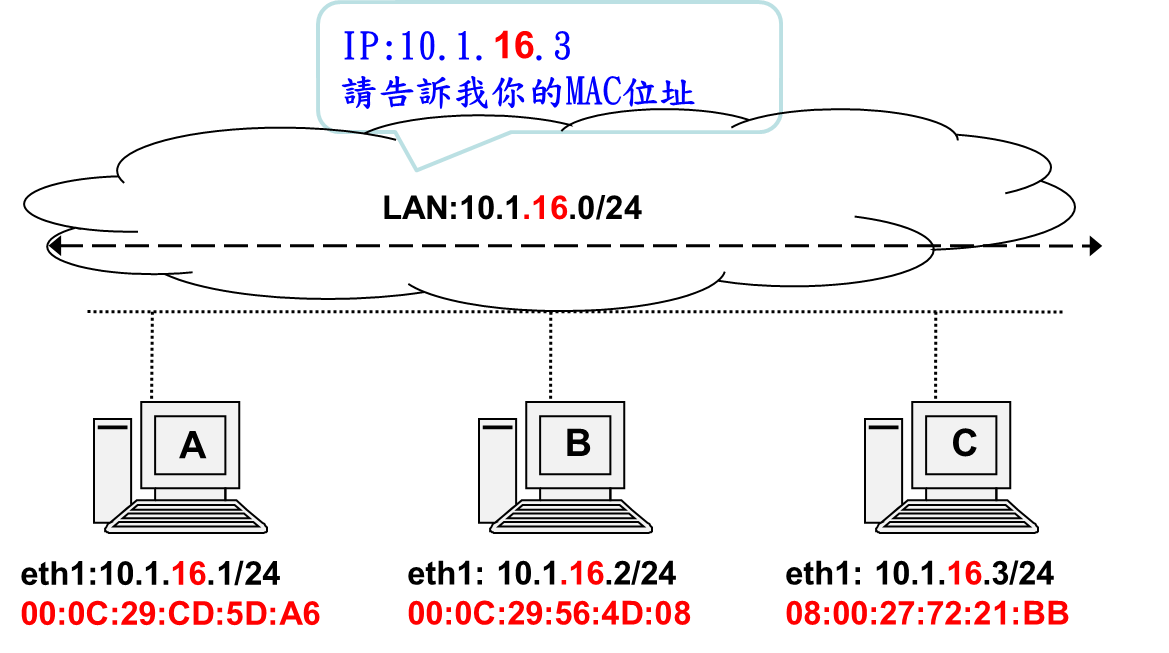
※ 認識ARP協定

※ 了解網路設備之網路層（Network Layer）『IP Address』，轉換或對應成鏈結層中的網路介面卡（Network Interface Card，簡稱NIC）上的實體位址『MAC Address』的過程

※了解ARP協定的重要性

※了解ARP協定的應用

**（2） ARP實驗架構圖**



**（3） ARP實驗導引**

* 設定網卡IP以及子網路遮罩
* Wireshark啟動與設定
* 測試連接並觀察封包形態

**（4） ARP實驗目的**

* 瞭解網卡IP位址設定指令
* 檢測連線狀態
* 瞭解ARP運作流程

**（5） ARP實驗步驟**

**Step1. 設定網路卡IP及子網路遮罩 (保留中括符號【 】但不輸入Terminal內)**

▲HostA: ifconfig eth1 [10.1.16.1] netmask 255.255.255.0

▲HostB: ifconfig eth1 [10.1.16.2] netmask 255.255.255.0

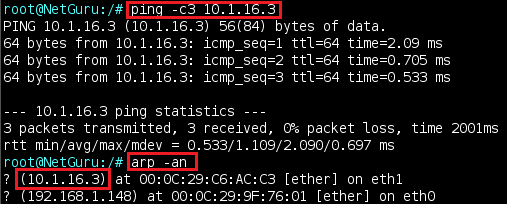
▲HostC: ifconfig eth1 [10.1.16.3] netmask 255.255.255.0

**Step2.**

**HostA eth1: [10.1.16.1/24] ping HostC eth1: [ 10.1.16.3/24] 三次**

**[10.1.16.1] ping [10.1.16.3] 三次**

1. Host A, C之Wireshark皆打開，Host A之Terminal打開
2. 在Host A之Terminal 打[**ping -c3 10.1.**16**.3]**



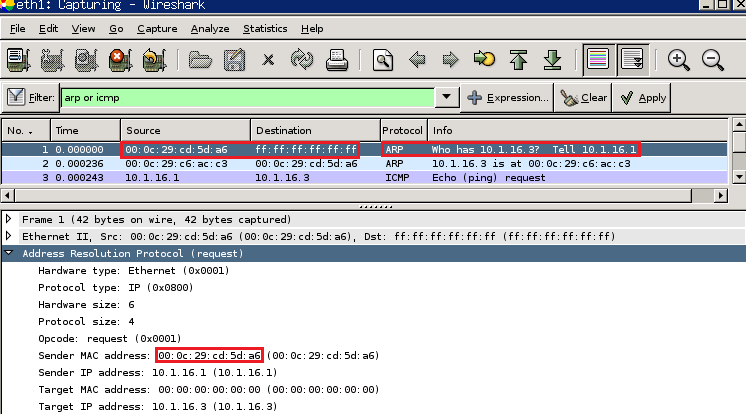
1. 請先畫出ARP之格式，再寫出ARP Broadcast（ARP Request） 和ARP Reply之格式，並比較其差異

**Step3. ARP 封包格式**

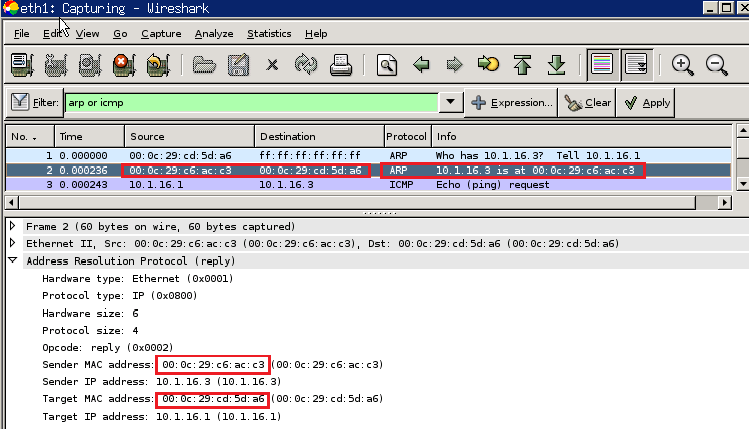
|  |  |  |
| --- | --- | --- |
| **Hardware Type（16 Bits）** | | **Protocol Type（16 Bits）** |
| **Hardware Address Length（8 Bits）** | **Protocol Address Length（8Bits）** | **Operation （16 Bits）** |
| **Sender Hardware Address （48 Bits）** | | |
| **Sender Protocol Address （32 Bits）** | | |
| **Target Hardware Address （48 Bits）** | | |
| **Target Protocol Address （32 Bits）** | | |

**（6） ARP實驗結果**

**第一筆ARP Broadcast（ARP Request）圖 （更換成自己IP之圖）**



**第一筆ARP Reply圖 （更換成自己IP之圖）**



**ARP封包格式之內容 (顏色不可更改，尤其紅色部分)**

|  |  |  |  |
| --- | --- | --- | --- |
| **ARP封包格式** | **ARP Broadcast（ARP Request）** | **ARP Reply** | **差異（一樣：O、不一樣：X）** |
| **Hardware Type（16 bits）** | **[Ethernet (0x0001) ]** | **[Ethernet (0x0001) ]** | **[ O ]** |
| **Protocol Type（16 bits）** | **[IP (0x0800) ]** | **[IP (0x0800) ]** | **[ O ]** |
| **Hardware Address Length（8 bits）** | **[ 6 ]** | **[ 6 ]** | **[ O ]** |
| **Protocol Address Length（8 bits）** | **[ 4 ]** | **[ 4 ]** | **[ O ]** |
| **Operation（16 bits）** | **[request (0x0001) ]** | **[reply (0x0002)]** | **[ X ]** |
| **Sender Hardware Address（48 bits）** | **[ 00:0C:29:CD:5D:A6 ]** | **[ 00:0C:29:C6:AC:C3 ]** | **[ X ]** |
| **Sender Protocol Address（32 bits）** | **[ 10.1.16.1 ]** | **[ 10.1.16.3 ]** | **[ X ]** |
| **Target Hardware Address（48 bits）** | **[ 00:00:00:00:00:00 ]** | **[ 00:0C:29:CD:5D:A6 ]** | **[ X ]** |
| **Target Protocol Address（32 bits）** | **[ 10.1.16.3 ]** | **[ 10.1.16.1 ]** | **[ X ]** |

**（7） 心得與討論：**包括這次實驗，我聽到什麼？我學到什麼？我遇到什麼問題？或其他（至少200字）

本次實驗以ARP為主軸，首先我們透過Terminal終端機執行”ifconfig”指令，透過該指令進行網卡資訊的確認，接下來將上周實驗的內容之網卡與子遮罩設定”ifconfig eth1 10.1.16.x netmask 255.255.255.0”指令加入，其中在ip的結尾有之x變數分別表示HostA、HostB與HostC三台虛擬機代碼，而指令中的eth1表示為網卡代號，此外netmask直翻就是網路面罩，也就是子遮罩的意思，那要如知道該參數呢！依據網路原理課程ip後面有/24那就表示有24個1，而對應的就是255.255.255.0此子遮罩，由於本實驗為ARP實驗，需進行封包捕捉並解析，因此在陳永輝教授的指導下，他告訴我們從HostA的Terminal中運用Ping指令針對HostC進行連線，並且傳送為三次，因此才有上述指示中的ping -c3，若要五次僅需要將指令改為-c5以此類推，在本次實驗中也有另一個協助我們進行封包捕捉與解析的工具，也就是WireShark，我們利用Control+K以快速鍵方式跳轉至設定，將Interface選定本次實驗使用的eth1之網卡，並且將Capture packets in promiscuous mode的**打勾取消**以免收到其他實驗不需要的數據，並且將Display Options**全數打勾**，反之Name Resolution的打勾**全數拿掉**，以便後續實驗的參數為我們所需要的部分，經歷這些設定我們還要運用Wireshark的Filter(過濾器)，使實驗的參數僅剩下ARP和ICMP，既單純又能快速觀察，是相當實用的操作功能，經歷以上我們可以完成實驗並將上述題組內的圖完成。回歸本次實驗內容為兩大主軸為敝人之印象深刻，ARP中運用Terminal進行網卡與子遮罩設定，以及Wireshark的各項設定與操作，從網路原理的紙上談兵，運用實作達成做中學，學中做的概念，會期待往後課程與實作，期盼這門課也能成為大學生涯中印象極深，且適性學習的代表性課程之一。

**註：請同學注意：保留中括符號 【 】，但不輸入Terminal內。截圖紅色方框標記的時候，圖片須清楚 紅色框需框好，如附圖大小，大小和清晰度盡量如附圖(這個很重要： 圖片須清楚 紅色框需框好)**