**實驗日期：**

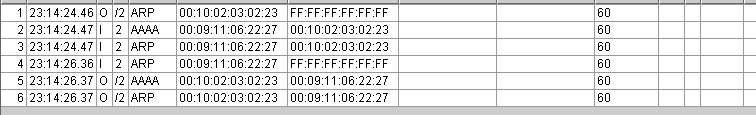
March 16, 2023

**實驗名稱：**

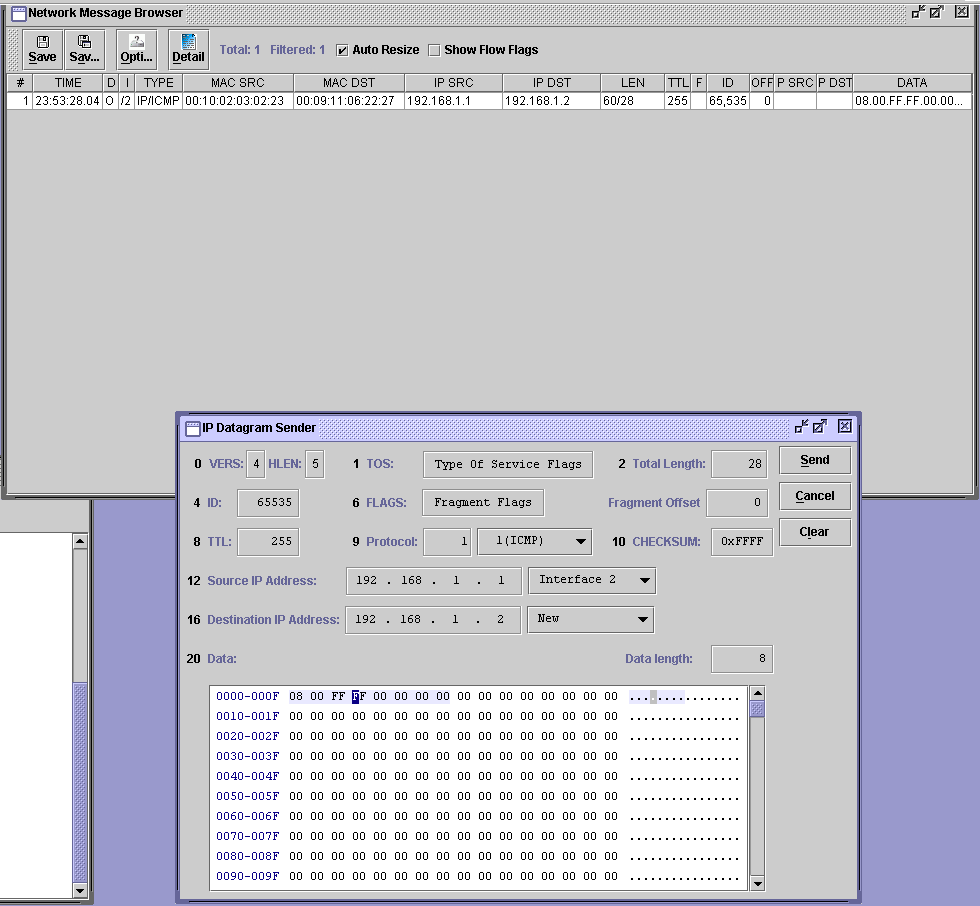
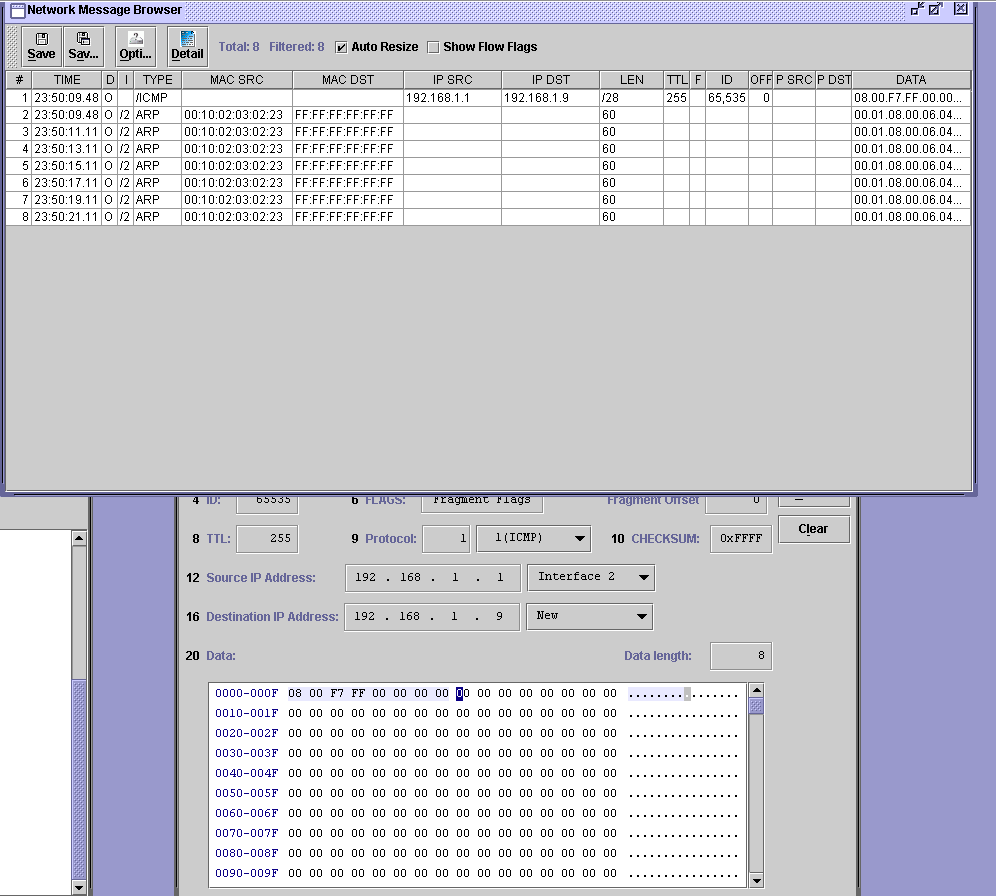
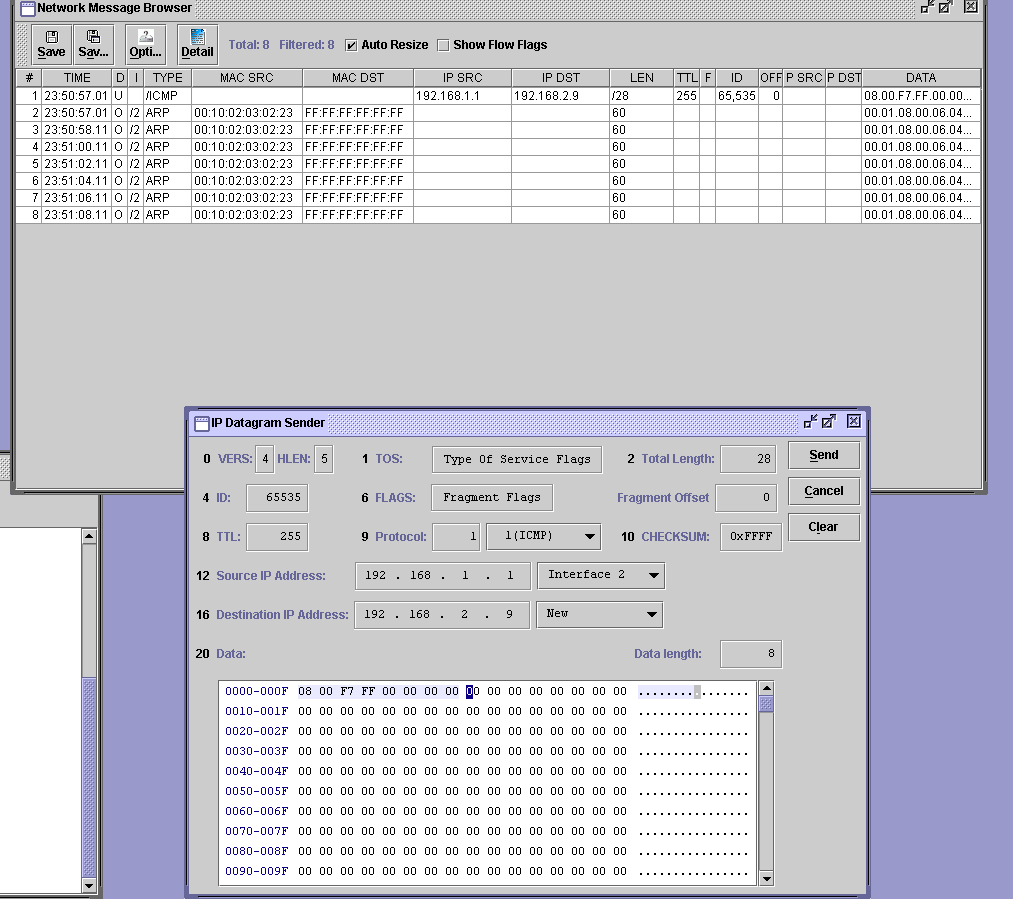
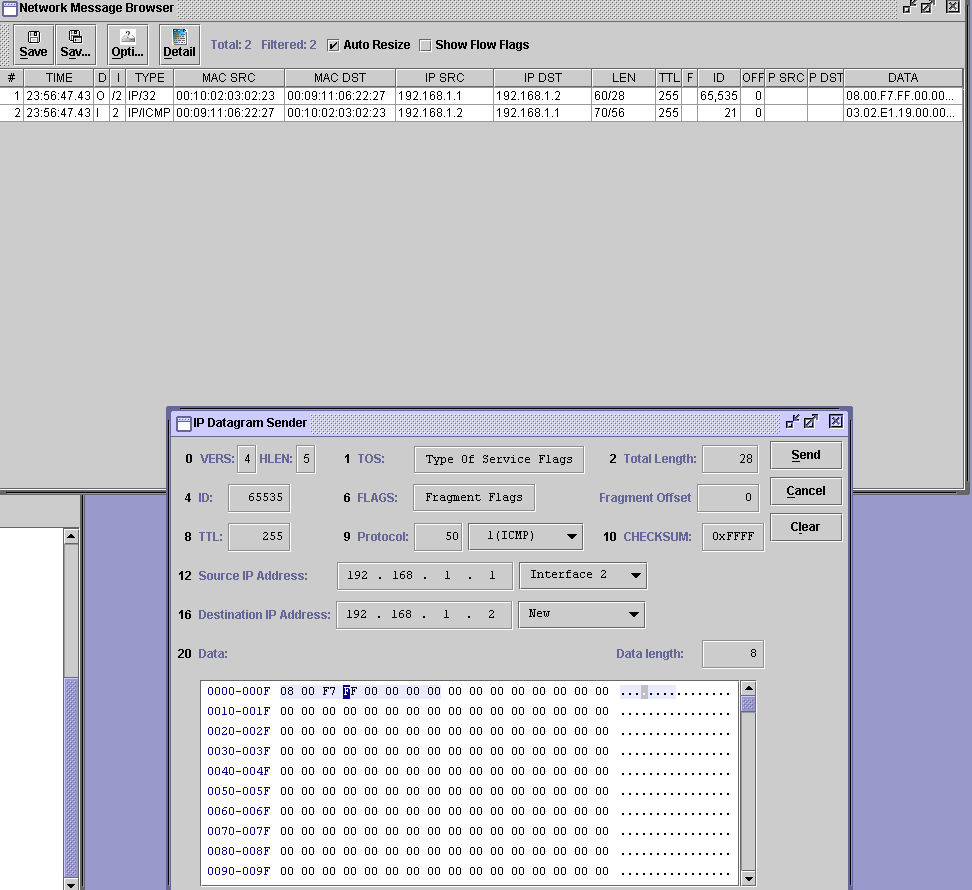
1. ITS Exp. 3: ARP位址解析協定
2. ITS Exp. 4: ICMP網控訊息協定與Checksum計算

**問題與答案：**

**Exp 3: ARP**

1. 將T.ETHER\_TYPE改成{0xAA,0xAA}或者其他非預設的type就可以在Network Message Browser上看到由mddl回傳的AAAA訊息。
2. 用來更新Arp table，判斷是否超過time period 200，如果超過就把表格刪掉，以免資料太久沒更新。
3. 動態形式代表MAC address是由網路設備自動學習和維護所產生的，會經過一段時間後被清除；而靜態形式是手動配置的，通常是需要長期保留的重要設備或伺服器的位置，不會被自動清除。

**Exp 4: ICMP**

1. 當發送錯誤的checksum時，不會收到有回傳封包，因為接收端判定它收到的封包有錯誤，所以不會回覆。
2. 當傳送端要傳送資料時，會先檢查自己的ARP table中是否有目標端的IP位址對應的MAC位址，如果有，傳送端就會將目標MAC位址寫入封包中，並直接發送資料；如果ARP table中沒有對應的IP位址，傳送端就會向同一個網域內的所有主機發出廣播詢問，其他主機不會回應此ARP詢問，只有目標端主機收到此詢問後，才會回應一個ARP回應，並將自己的MAC位址傳回給傳送端。同時，目標端主機還會更新自己的ARP cache，以便下次可以更快地尋找到對應的MAC位址，下次收到ARP request時，傳送端就可以從ARP table中找到目標端的MAC位址，直接發送資料。
   1. 由於不知道這個IP位置的MAC位置所以會發送廣播給網域中的所有裝置，因為timeout沒有收到回覆，所以一直重傳。
   2. 由於不知道這個IP位置的MAC位置所以會發送廣播給網域中的所有裝置，但是接收端不在同個網域內所以收不到，又因為timeout沒有收到回覆，所以一直重傳。
   3. Protocol Type設為50時，表示使用的是IPsec協議中的/，ESP協議提供對IP數據包的加密和身份驗證，可用於保護數據在網絡上的傳輸安全。 接收端收到 ESP 封包後，會先將資料解密，再組合回原封包格式。

**討論：**

這次的實驗完成得非常迅速，發送封包的方法和前幾次實驗大同小異，然而在修改IP的過程中遇到了一些挑戰，因為實驗手冊使用的是window XP，而修改IP的方法與現在的系統有些不同，不過最終還是透過一點年輕人的天賦完成了IP設置。在整個過程中，最讓我有點緊張的是要記住自己原本電腦的IP位置，雖然已經截圖存證還是感到很不安心，好險最後成功將其還原回去。

**補充資料：**

1. [ARP地址解析，動態ARP，靜態ARP，一分鐘了解下 - 每日頭條 (kknews.cc)](https://kknews.cc/zh-tw/code/9vm9boq.html)
2. [小蘿蔔工作室 Little Robot Studio: IPsec (lirobo.blogspot.com)](http://lirobo.blogspot.com/2010/10/ipsec.html)
3. [IPSec ESP 安全協定 (tsnien.idv.tw)](http://www.tsnien.idv.tw/Manager_WebBook/chap10/10-4%20IPSec%20ESP%20%E5%AE%89%E5%85%A8%E5%8D%94%E5%AE%9A.html)