1. **實驗日期:** 2017/6/8

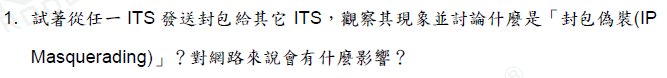
**2.**  **實驗名稱:**

1. ITS Exp. 22: NAT

2. ITS Exp. 23: Firewall

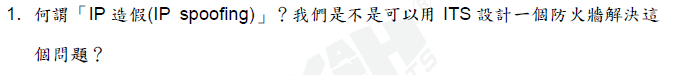
**3.  問題與答案:**

實驗一



安全的防火牆至少必須具有「NAT伺服器」，用來攔截網際網路進入私有網路的封包，阻擋怪客的攻擊，或是進行封包偽裝，將私有IP改變成真實IP再傳送到網際網路，使網際網路上的人無法得知私有網路的IP分配情形，而增加安全性。

實驗二



更改封包的source IP，使封包看起來是可信任的網域傳送過來，達到入侵電腦的任務。

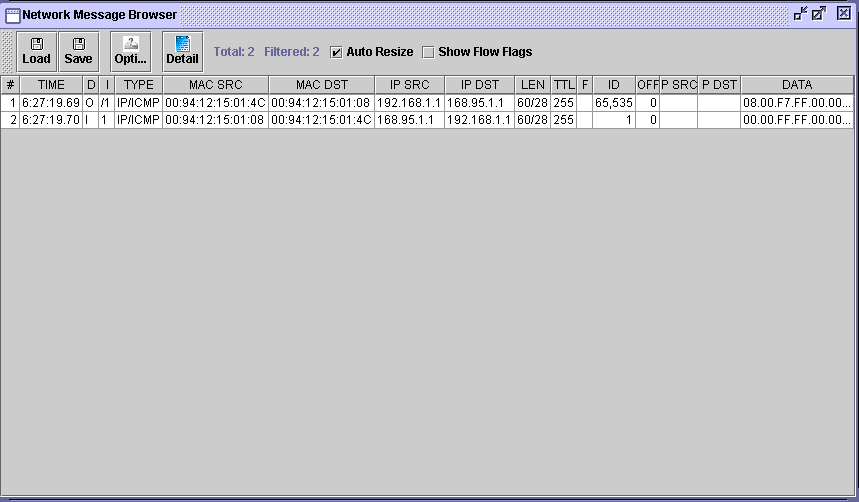
將防止來源IP位址偽造(Anti-Spoofing)功能列為網路架構必要的選項。網路端末(Edge)是唯一可以實施防止來源IP位址偽造的地方。如果網路端末處具備防止來源IP位址偽造功能而且具備自動化管理機制，在網路端末建構Anti-Spoofing 機能將是最理想的方向。

**4.  結果討論:**

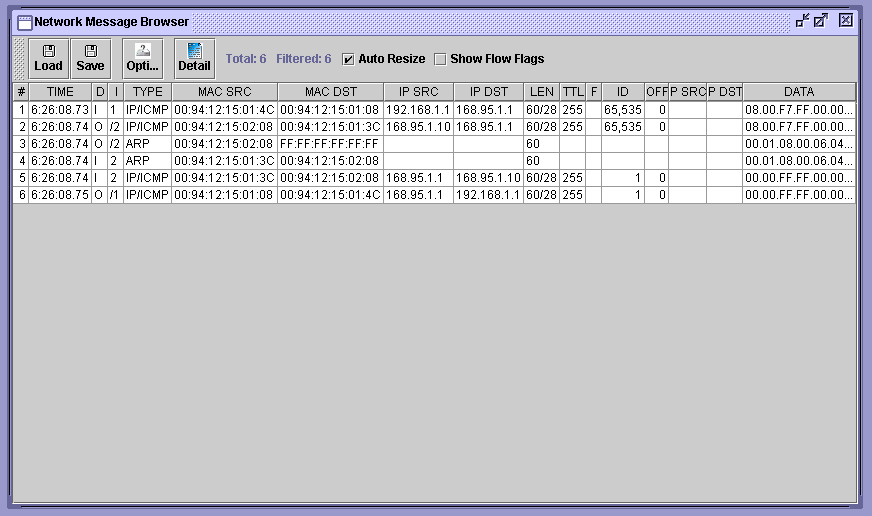
實驗一

ITS1傳送封包給ITS4

ITS1看到的情形



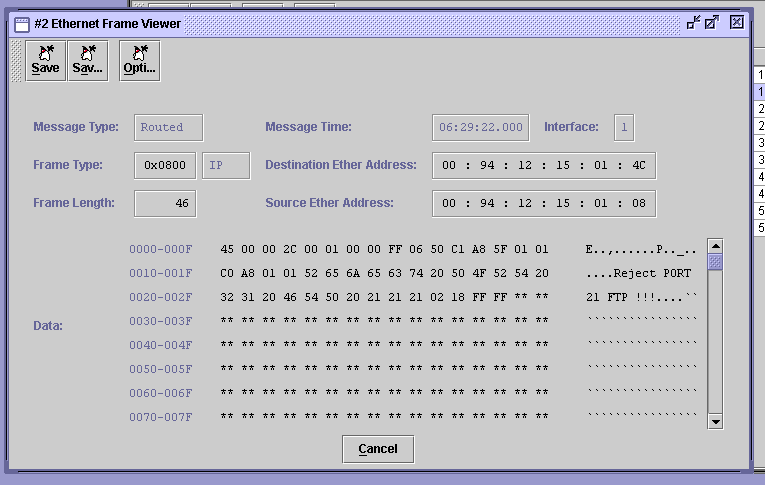
ITS3看到的情形



實驗二

ITS3阻擋所有port為21的封包通過

ITS1傳送封包給ITS4



ITS4傳送封包給ITS1

