09 Wireshark分析流量最高的那台電腦

有時候MIS/IT只是想找出佔流量最高的那台電腦

方法如下

抓一段封包



先用Statistics

IO Graph



觀察流量最高的時間點



在Statistics

Conversations



可以看出Port的統計

左下有一個Name resolution可以把製造公司名稱拿掉



變成純MAC Address

這功能是分析Port的流量

可以點排序



如果是要知道IP對IP的流量

要點Statistics

Endpoints



統計完之後再點

Packets做排序

就可以回到剛剛的IO Graph



做Graph 1的Filter 的條件設定

就可以看出流量高的那台電腦的統計了