**實驗日期:2020/3/26**

**實驗名稱:**

ITS Exp. 3: ARP位址解析協定

ITS Exp. 4: ICMP網控訊息協定與Checksum計算

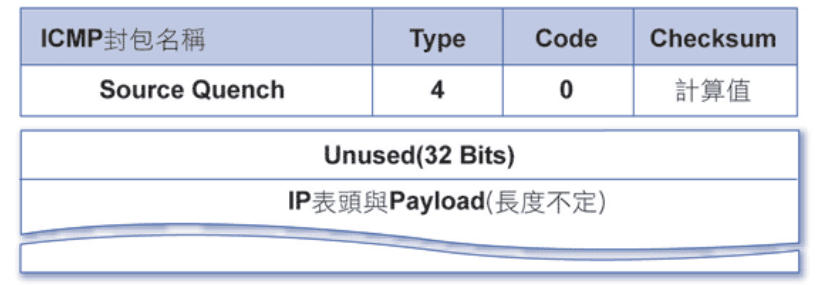
**實驗相關技術資訊:**

1. What is ARP? How does it work to achieve its goal?

Address Resolution Protocol (ARP) 是 TCP/IP 設計者利用乙太網路的廣播性質﹐設計出來的位址解釋協定。它的主要特性和優點是它的位址對應關係是動態的﹐它以查詢的方式來獲得 IP 位址和實體位址的對應。它的工作原理非常簡單﹕

1. 首先﹐每一台主機都會在 ARP 快取緩衝區 (ARP Cache)中建立一個 ARP 表格﹐用來記錄 IP 位址和實體位址的對應關係。這個 Table 的每一筆資料會根據自身的存活時間遞減而最終消失﹐以確保資料的真實性。
2. 當發送主機有一個封包要傳送給目的主機的時候﹐並且獲得目的主機的 IP 位址﹔那發送主機會先檢查自己的 ARP 表格中有沒有該 IP 位址的實體位址對應。如果有﹐就直接使用此位址來傳送框包﹔如果沒有﹐則向網路發出一個 ARP Request 廣播封包﹐查詢目的主機的實體位址。這個封包會包含發送端的 IP 位址和實體位址資料。
3. 這時﹐網路上所有的主機都會收到這個廣播封包﹐會檢查封包的 IP 欄位是否和自己的 IP 位址一致。如果不是則忽略﹔如果是則會先將發送端的實體位址和 IP 資料更新到自己的 ARP 表格去﹐如果已經有該 IP 的對應﹐則用新資料覆蓋原來的﹔然後再回應一個 ARP Reply 封包給對方﹐告知發送主機關於自己的實體位址﹔
4. 當發送端接到 ARP Reply 之後﹐也會更新自己的 ARP 表格﹔然後就可以用此紀錄進行傳送了。
5. 如果發送端沒有得到 ARP Reply ﹐則宣告查詢失敗。
6. What is ICMP? Please briefly describe its message format.

每個ICMP封包都會有ICMP表頭，其中包含了三個 固定長度的欄位：Type、Code與Checksum；至於 ICMP資料的部分，則會隨著ICMP封包的類型而異。



* TYPE：長度為1 Byte，定義ICMP封包的類型。
* CODE：長度為1 Byte，每種類型可再根據 Code欄位來定義各種不同用途。不過大部分 ICMP封包類型只定義了一種Code欄位值。
* Checksum：長度為2 Bytes，記錄ICMP封包的錯誤檢查碼。

1. The ICMP header contains a field called checksum. What is its function? How is it calculated?

將要計算的對象以 16 bits 為單位以一的補數作相加（計算前的 checksum 是設為零），最後相加的結果再取一的補數填入 checksum 這個欄位，觀念非常簡單容易， 不過 checksum 計算對象依照不同的協定仍然不太一樣 。 （以下以 IPv4 為準）

（一）IP

IP header 中的 checksum 計算對象只有 IP header，因此所保證的欄位也就只有 IP header

（二）ICMP

ICMP 的 header 也有 checksum，其計算對象除了 header 外，也包含了 ICMP data

（三）TCP/UDP

TCP/UDP header 中 checksum 的計算對象，除了直覺上的 header 和 data 外，還包含所謂的虛擬表頭（psuedo-header），此 psuedo-header 包含了 L3 的 SrcIP 、 DstIP 、 Packet Length 及 Protocol Num，之所以要增加 psuedo header，目的在於，封包在傳輸過程中，目的 IP 可能會被更改，而傳到錯誤的 host，不過 IP 的 checksum 隨時都在改變，因此可能會把被改過的 IP 當成是對的計算進去因而檢查不出來，但是 L4 的 checksum 在傳輸過程中並不會被更改，因此算進去的目的 IP 就是原本 sender 要送的對象，當 receiver 端拆解封包檢查 L4 的 checksum 即可知送錯對象，不過有一點要注意的是，UDP 的 checksum 是 optional 的，它可以被寫為 0 而被 disable 掉。

1. What can we do with the "ping" program?

* 當架設好一個TCP / IP網路時，最常利用Ping 這個命令來檢查網路是否連接成功，不過要注意的是有時為了安全起見，遠方機器或經過的 某些網路節點會過濾該ICMP封包。
* Ping回應的各個欄位所代表的意義分別如下：
  + Reply From：是從何處得到的回應。
  + Bytes：是該次Ping執行的數據大小。
  + TTL：Round Trip時間（毫秒）生存期限（毫秒）

補充資料:

<http://pcnet.idv.tw/pcnet/network/network_ip_arp.htm>