EE110300 電機資訊工程實習 實驗手冊

個人電腦系統

資訊工程系 金仲達 教授

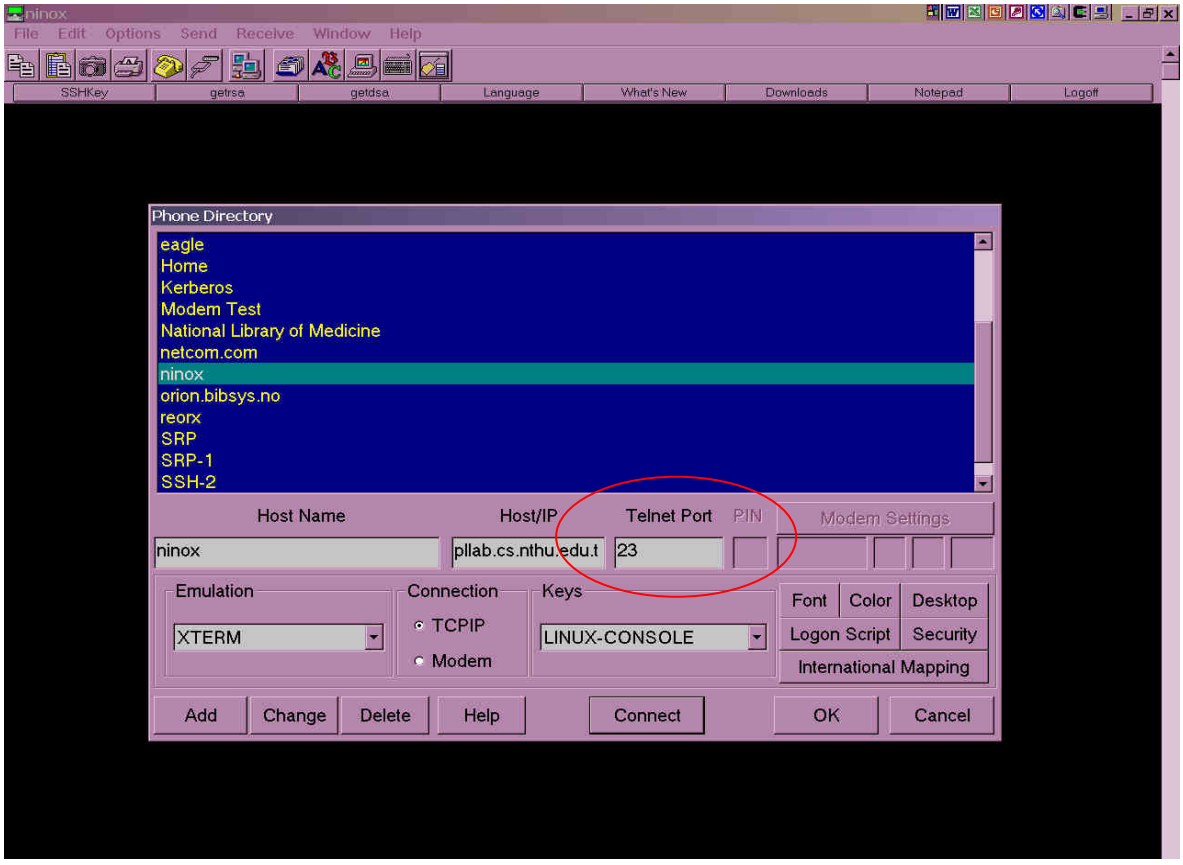
實驗二：封包解譯及追踪

實驗目的：本實驗旨在使同學能瞭解網際網路上的通訊協定，其封包的運送實際流程，對於 TCP/IP 的網路架構能有更深入一層的瞭解，並針對每一種網路應用程式，能實際瞭解其背後的運作模式。

實驗內容規畫：

1.網路應用程式範例-NetTerm

常用的 Telnet Client 程式 NetTerm,其外觀如下:



針對這樣一個應用程式,我們所要探討的是,這個應用程式用了 TCP/IP Architecture 的那些 protocol,其 packet 傳送的方式爲何，什麼是 TCP Port, 如何從 RFC 文件之中,找出你所需要的資訊。

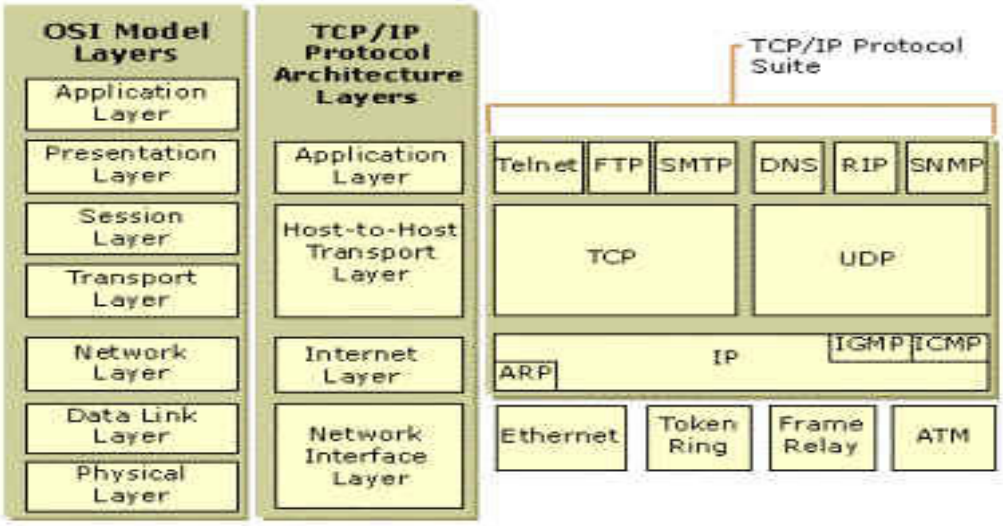
2.預備知識，文件導讀-RFC 1700,RFC 854

TCP Port Number	Description
20	FTP (Data Channel).
21	FTP (Control Channel).
23	Telnet.
80	HyperText Transfer Protocol (HTTP), used for the World Wide Web.
139	NetBIOS session service.

Well-known TCP ports

UDP Port Number	Description
53	Domain Name System (DNS) Name Queries.
69	Trivial File Transfer Protocol (TFTP).
137	NetBIOS name service.
138	NetBIOS datagram service.
161	Simple Network Management Protocol (SNMP).

Well-known UDP ports



the TCP/IP protocol architecture

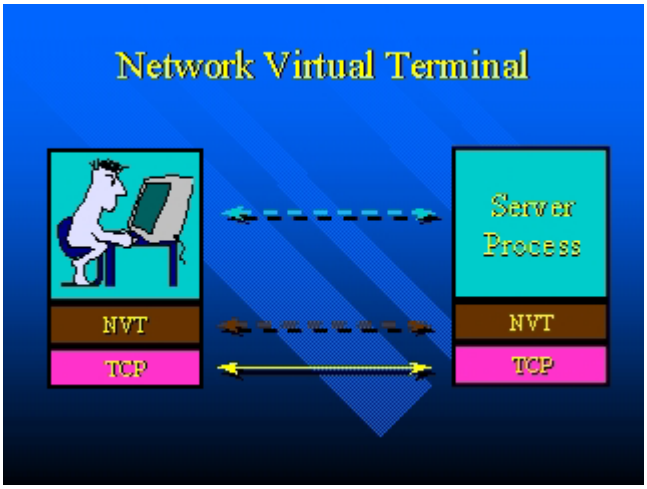
RFC 是許多持續進行及改進的一系列網路通訊協定的規範及報告，也規範了網際網路的標準協定。Windows 2000 所支援的 RFC 規範如下：(節錄部分)

RFC	**Title**
768	User Datagram Protocol (UDP)
783	Trivial File Transfer Protocol (TFTP)
791	Internet Protocol (IP)
792	Internet Control Message Protocol (ICMP)
793	Transmission Control Protocol (TCP)
816	Fault Isolation and Recovery
826	Address Resolution Protocol (ARP)
854	Telnet Protocol (Telnet)
862	Echo Protocol (ECHO)
863	Discard Protocol (DISCARD)
864	Character Generator Protocol (CHARGEN)
865	Quote of the Day Protocol (QUOTE)
867	Daytime Protocol (DAYTIME)
894	IP over Ethernet
919, 922	IP Broadcast Datagrams (broadcasting with subnets)
950	Internet Standard Subnetting Procedure
959	File Transfer Protocol (FTP)

1001, 1002	NetBIOS Service Protocols
1009	Requirements for Internet Gateways
1034, 1035	Domain Name System (DNS)
1042	A Standard for the Transmission of IP Datagrams over IEEE 802 Networks
1055	Transmission of IP over Serial Lines (IP-SLIP)
1112	Internet Group Management Protocol (IGMP)
1122, 1123	Host Requirements (communications and applications)
1144	Compressing TCP/IP Headers for Low-Speed Serial Links

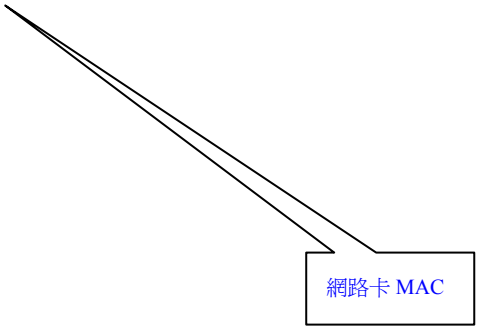
TELNET Protocol 的特性

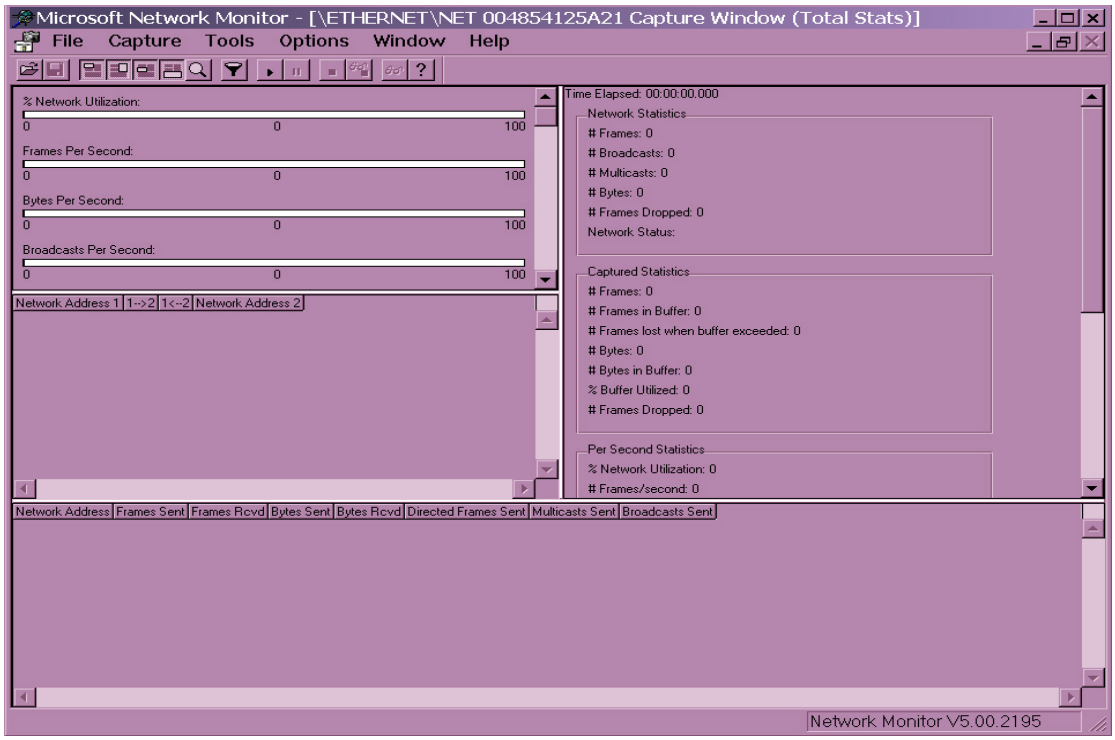
- TCP connection
- data and control over the same connection.
- Network Virtual Terminal
- negotiated options



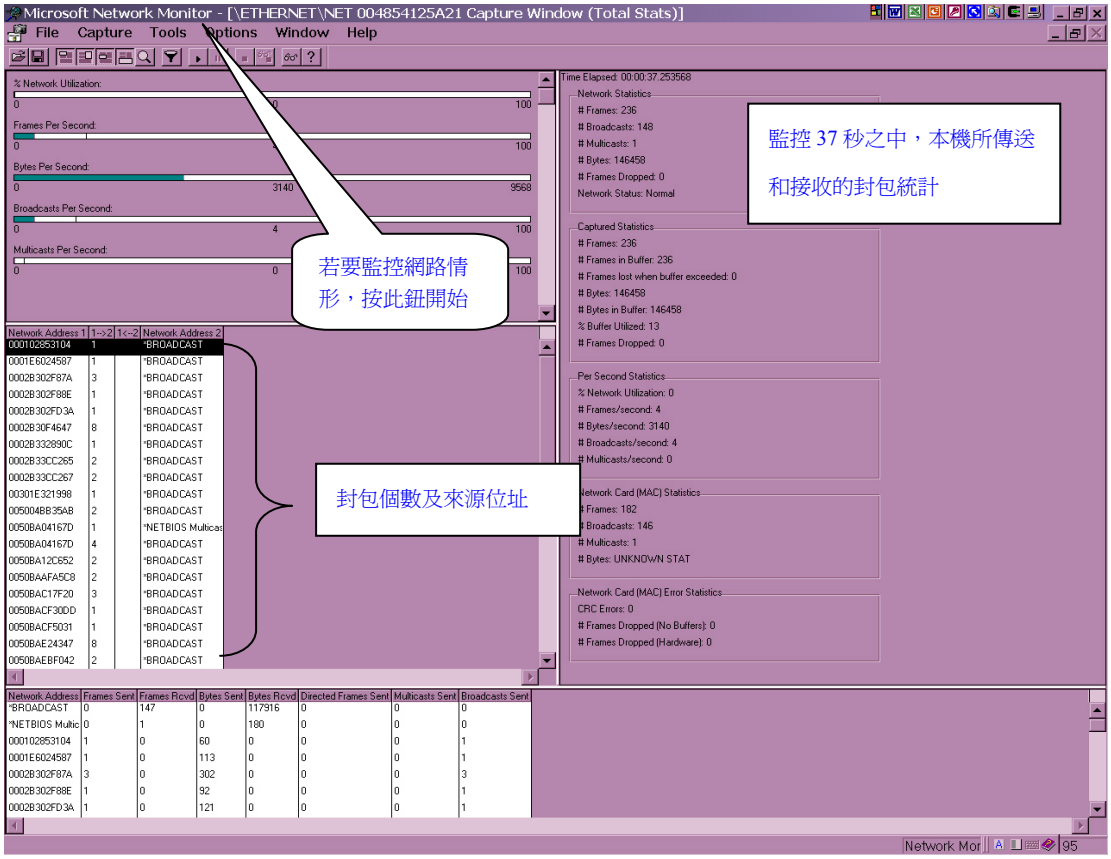
3.封包的追踪(使用 Microsoft Network Monitor)

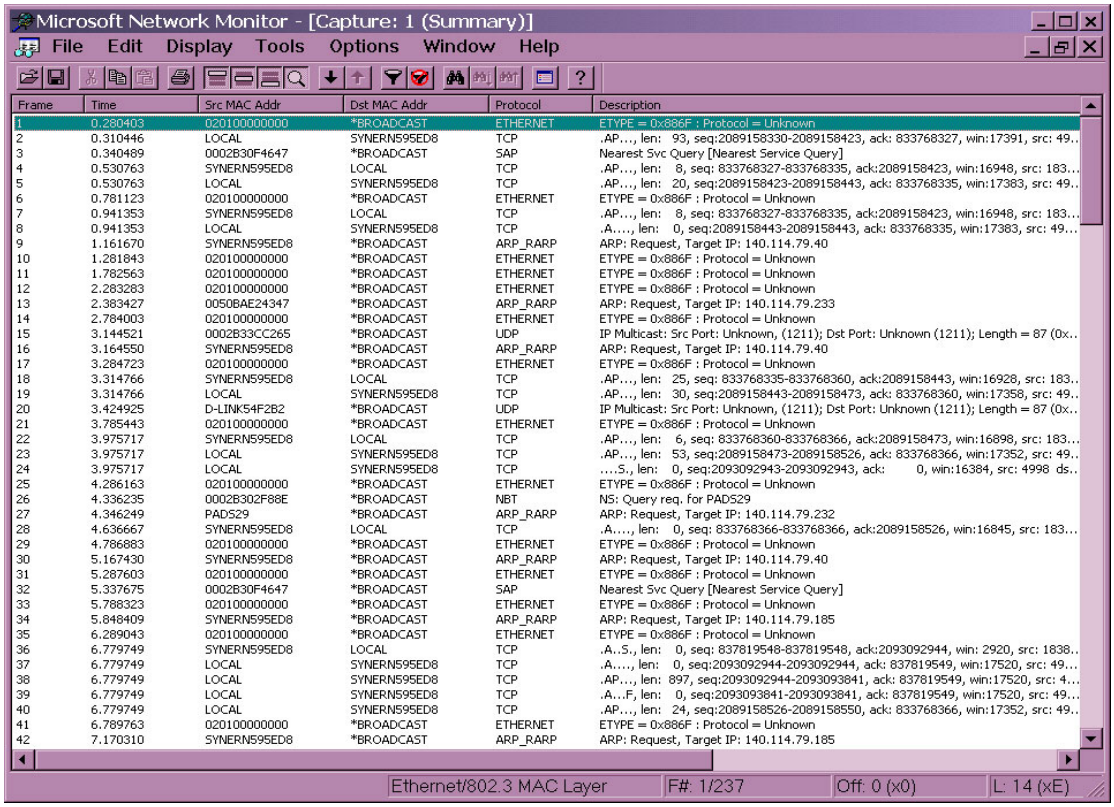
Network Monitor存在於windows 2000 server版之中，使用者可以在command line 執行 netmon.exe 開啓此網路監控程式(sniffer)。





先測試目前網路的流量，此範例爲 37 秒。





4.追踪應用程式 Netterm 的封包

NetTerm 常用來連上各 bbs 站，或 remote login。我們的實驗過程如下：

a.使用 NetTerm 連上楓橋 bbs

先使用 nslookup 指令找出 bbs.cs.nthu.edu.tw 的 IP Address,如下

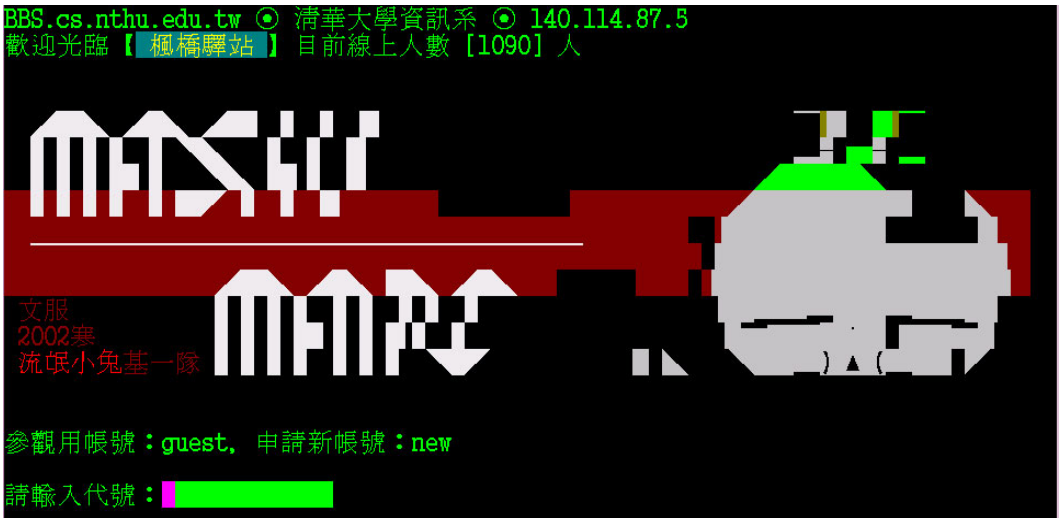
```
C:\Documents and Settings\Administrator>nslookup
Default Server:  nthu.edu.tw
Address:  140.114.64.10

> bbs.cs.nthu.edu.tw
Server:  nthu.edu.tw
Address:  140.114.64.10

Non-authoritative answer:
Name:    bbs.cs.nthu.edu.tw
Address:  140.114.87.5
```

按F12用來查看所有攔截到的封包

b.使用 NetTerm 連上此 bbs



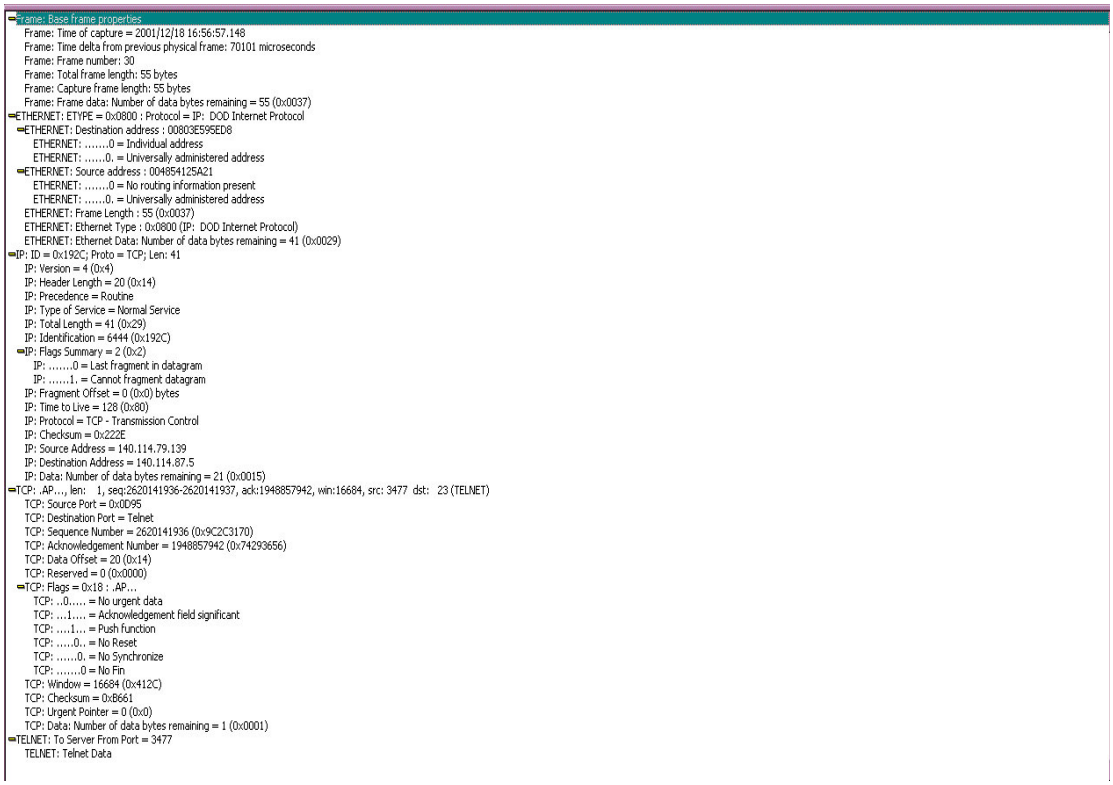
a. 開啓\winnt\system32\netmon\netmon.exe(執行 Microsoft Network Monitor)

進行封包擷取，所得到的封包如下：

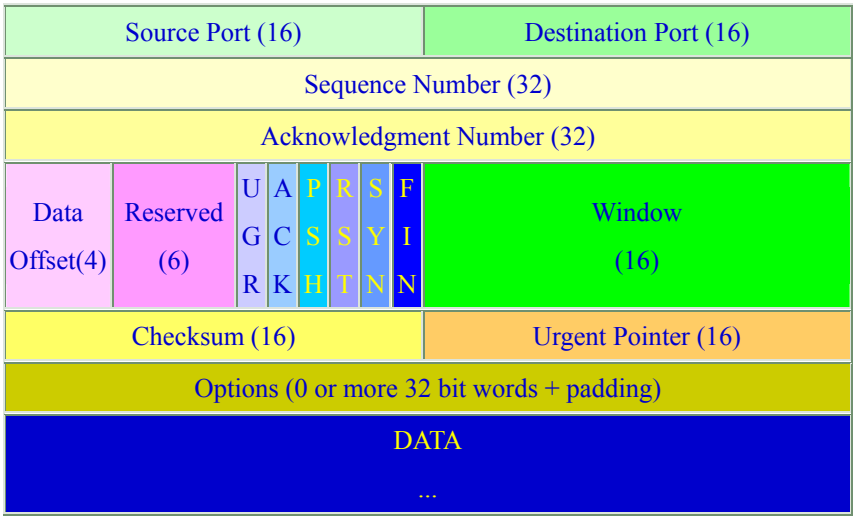
Src MAC Addr	Dst MAC Addr	Protocol	Description	Src Other Addr	Dst Other Addr	Type O
SYNERN595ED8	LOCAL	TCP	.A...., len: 0, seq: 843596491-843596491...	211.79.242.25	BLUETOOTH	IP
020100000000	*BROADCAST	ETHERNET	ETYPE = 0x886F : Protocol = Unknown			
OLDWAYNE	*BROADCAST	SMB	C transact, File = \MAILSLOT\BROWSE	OLDWAYNE	140.114.79.255	IP
OLDWAYNE	*BROADCAST	SMB	C transact, File = \MAILSLOT\BROWSE	OLDWAYNE	140.114.79.255	IP
ANTSLAB	*BROADCAST	SMB	C transact, File = \MAILSLOT\BROWSE	ANTSLAB	140.114.79.255	IP
SYNERN595ED8	LOCAL	TCP	.A...., len: 0, seq: 843596491-843596491...	211.79.242.25	BLUETOOTH	IP
MIR	*BROADCAST	SMB	C transact, File = \MAILSLOT\BROWSE	MIR	140.114.79.255	IP
SONGBOR	*BROADCAST	SMB	C transact, File = \MAILSLOT\BROWSE	SONGBOR	0.FFFFFFFFFFFF	IPX/XNS
SONGBOR	*BROADCAST	SMB	C transact, File = \MAILSLOT\BROWSE	SONGBOR	140.114.79.255	IP
MIR	*BROADCAST	SMB	C transact, File = \MAILSLOT\BROWSE	MIR	140.114.79.255	IP
020100000000	*BROADCAST	ETHERNET	ETYPE = 0x886F : Protocol = Unknown			
SYNERN595ED8	LOCAL	TCP	.A...., len: 0, seq: 843596491-843596491...	211.79.242.25	BLUETOOTH	IP
0050BAEBF042	*BROADCAST	UDP	IP Multicast: Src Port: Unknown, (1211); Dst...	140.114.79.12	255.255.255.255	IP
SYNERN595ED8	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 140.114.79.152			
SYNERN595ED8	LOCAL	TCP	.A...., len: 0, seq: 843596491-843596491...	211.79.242.25	BLUETOOTH	IP
020100000000	*BROADCAST	ETHERNET	ETYPE = 0x886F : Protocol = Unknown			
005004BB35AB	*BROADCAST	UDP	IP Multicast: Src Port: Unknown, (1211); Dst...	140.114.79.16	255.255.255.255	IP
MIR	*BROADCAST	SMB	C transact, File = \MAILSLOT\BROWSE	MIR	140.114.79.255	IP
020100000000	*BROADCAST	ETHERNET	ETYPE = 0x886F : Protocol = Unknown			
0050BAAFA5C8	*BROADCAST	UDP	IP Multicast: Src Port: Unknown, (1211); Dst...	140.114.79.22	255.255.255.255	IP
LOCAL	SYNERN595ED8	TCP	.A...., len: 1460, seq:2101115647-2101117...	BLUETOOTH	211.79.242.25	IP
020100000000	*BROADCAST	ETHERNET	ETYPE = 0x886F : Protocol = Unknown			
ALPHA22	*NETBIOS Multicast	NetBIOS	Name Query (0x0A), ALPHA22 <00> -...			
SYNERN595ED8	LOCAL	TCP	.A...., len: 0, seq: 843596491-843596491...	211.79.242.25	BLUETOOTH	IP
LOCAL	SYNERN595ED8	TCP	.A...., len: 1460, seq:2101121487-2101122...	BLUETOOTH	211.79.242.25	IP
LOCAL	SYNERN595ED8	TCP	.A...., len: 1460, seq:2101122947-2101124...	BLUETOOTH	211.79.242.25	IP
ALPHA22	*BROADCAST	NBT	NS: Query req. for ALPHA30	140.114.79.222	140.114.79.255	IP
00D0B7BE4DE4	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 140.114.79.222			
MIR	*BROADCAST	SMB	C transact, File = \MAILSLOT\BROWSE	MIR	140.114.79.255	IP
LOCAL	SYNERN595ED8	TELNET	To Server From Port = 3477	BLUETOOTH	140.114.87.5	IP
SYNERN595ED8	LOCAL	TELNET	To Client With Port = 3477	140.114.87.5	BLUETOOTH	IP
LOCAL	SYNERN595ED8	TELNET	To Server From Port = 3477	BLUETOOTH	140.114.87.5	IP
SYNERN595ED8	LOCAL	TELNET	To Client With Port = 3477	140.114.87.5	BLUETOOTH	IP
020100000000	*BROADCAST	ETHERNET	ETYPE = 0x886F : Protocol = Unknown			
SYNERN595ED8	LOCAL	TCP	.A...., len: 0, seq: 843596491-843596491...	211.79.242.25	BLUETOOTH	IP
LOCAL	SYNERN595ED8	TCP	.A...., len: 1460, seq:2101124407-2101125...	BLUETOOTH	211.79.242.25	IP
SYNERN595ED8	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 140.114.79.152			
LOCAL	SYNERN595ED8	TELNET	To Server From Port = 3477	BLUETOOTH	140.114.87.5	IP
SYNERN595ED8	LOCAL	TELNET	To Client With Port = 3477	140.114.87.5	BLUETOOTH	IP
LOCAL	SYNERN595ED8	TCP	.A...., len: 0, seq:2620141939-26201419...	BLUETOOTH	140.114.87.5	IP
LOCAL	SYNERN595ED8	TELNET	To Server From Port = 3477	BLUETOOTH	140.114.87.5	IP
SYNERN595ED8	LOCAL	TELNET	To Client With Port = 3477	140.114.87.5	BLUETOOTH	IP

由上圖可看出，frame30 其 Protocol 即爲 Telnet，其 source address 爲 BLUETOOTH(即爲 local host)，而 destination address 爲 140.114.87.5，即爲我們所要連上楓橋的 IP 。

對於上面的 frame 30 packet，我們再進行更詳細的剖析，如下



由於我們關心的是應用及傳送層的封包格式，因此，對於 IP 封包我們不加以解釋，而對於 TCP 封包的格式，詳列如下：



今次我不再爲每一個 TCP 封包部件擷取樣板了，只打算略略討論一下它們的名稱和定義：

Source Port & Destination Port

如果我們將 IP 比喻成地址,那麼 Port 可以說是門口了，試想一下：一座大樓有前門、後門、側門、那麼，一個 IP 地址也有著好多個各種功能的 port，而每一個 port

都被不同的服務傾聽著，就好比看門人一樣。

其實 port 號碼可以隨您喜歡任意指定給哪些服務使用，但爲了避免“找錯門口”的情形出現(除非您故意想躲起來)，人們將一些比較常用的服務(Well known services)的 port 號碼固定下來了。但是，在 TCP 資料傳送過程中，可能同時要處理一個以上的封包，程式也會建立多個 port 來避免衝突。在兩台主機進行資料傳送的時候，來源地的 port 和目的地的 port 都必須讓 TCP 知道才行。

Sequence Number

發送序號。當資料要從一台主機傳送去另一台主機的時候，發送端會爲封包建立起一個初始號碼，然後按照所傳送的位元組數，依次的遞增上去；那麼下一個封包的序號就會使用遞增之後的值來作爲它的序號了。這樣，接收端就可以根據序號來檢測資料是否接收完整了。

Acknowledgement Number

回應序號。當接收端接收到 TCP 封包之後，通過檢驗確認之後，然後會依照發送序號產生一個回應序號，發出一個回應封包給發送端，這樣接收端就知道剛才的封包已經被成功接收到了。

可是，如果由於網路狀況或其它原因，當封包的 TTL 值達到期限時，接收端還沒接收到回應序號，就會重發該個被以爲丟失了的封包。但如果剛好重發封包之後才接收到回應呢？這時候接收端就會根據序號來判斷該封包是否被重複發送，如果是的話，很簡單，將之丟棄不做任何處理就是了。

Data Offset

這是用來記錄標頭固定長度用的，和 IP 封包的 IHL 差不多：如果 options 沒設定的話，其長度就是 20byte，用十六進位表示就是 0x14 了。

Reserved

這是保留區間，暫時還沒被使用。

Contral Flag

控制標記。一個有六個，它們分別是：

Urgent data

當 URG 被設定爲 1 的時候，就表示這是一個攜有緊急資料的封包。

Acknowledgment field significant

當 ACK 爲 1 的時候，表示此封包屬於一個要回應的封包，一般都會爲 1。

Push function

如果 PSH 爲 1 的時候，此封包所攜帶的資料就會被直接上遞給上層的應用程式，而無需經過 TCP 處理了。

Reset

如果 RST 爲 1 的時候，表示要求重新設定封包，再重新傳遞。

Synchronize sequence number

如果 SYN 爲 1 時，表示要求雙方進行同步溝通。

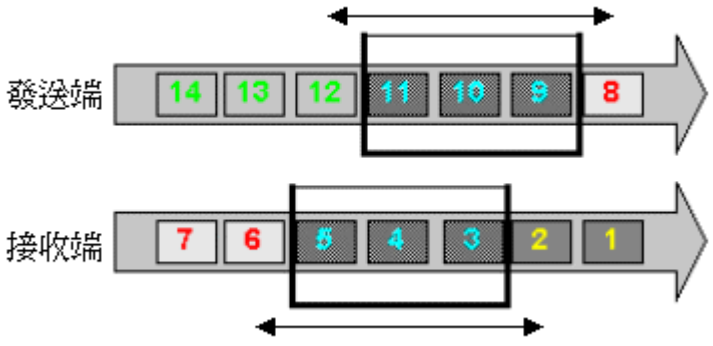
No more data fro sender (Finish)

如果封包的 FIN 爲 1 的時候，就表示傳送結束，然後雙方發出結束回應，進而正式終止一個 TCP 傳送過程。

Window

我們都知道 MS Windows 是什麼東西，但這裡的 Window 卻非作業系統的“視窗”哦，我們稱這裡的視窗爲“滑動視窗(Sliding Window)”。爲什麼我們需要使用視窗呢?

正如您剛才看到的，TCP 封包會通過 SQN 和 ACK 序號來確保傳送的正確性，但如果每一個封包都要等上一個封包的回應才被發送出去的話，實在是太慢和難以接受的。這樣，我們可以利用 Sliding Window 在傳送兩端劃分出一個緩衝範圍，規定出可以一次性發送的最大封包數目：



當 TCP 傳送建立起來之後，兩端都會將 window 的設定值還原到初始值，比方說：每次傳送 3 個封包。然後發送端就一次過發送三個封包出去，然後視窗則會往後移動三個封包，填補發送出去之封包的空缺。如果接收端夠順利，也能一次處理接收下來的三個封包的話，就會告訴發送端的 window 值爲 3；但如果接收端太忙，或是其它因素影響，暫時只能處理兩個封包，那麼，在視窗裡面就剩下一個封包，然後就會告訴發送端 window 值爲 2。這個時候，發送端就只送出兩個封包，而視窗就會往後移動兩個封包，填補發送出去的空缺。

Chechsum

當資料要傳送出去的時候，發送端會計算好封包資料大小，然後得出這個檢驗值封包一起發送；當接收端收到封包之後，會再對資料大小進行計算，看看是否和檢驗值一致，如果結果不相稱則被視爲殘缺封包，會要求對方重發該個封包。

Urgent Pointer

還記得剛才講到 Control Flag 的時候我們提到一個 URG 的標記嗎？如果 URG 被設定爲一的時候，這裡就會指示出緊急資料所在位置。不過這種情形非常少見，例如當資料流量超出頻寬的時候，系統要求網路主機暫緩發送資料，所有主機收到這樣的信息，都需要優先處理。

Option

這個選項也比較少用。當那些需要使用同步動作的程式，如 Telnet，要處理好終端的交互模式，就會使用到 option 來指定資料封包的大小，因爲 telnet 使用的資料封包都很少，但又需要即時回應。

Option 的長度要麼是 0，要麼就是 32bit 的整倍數，即使資料不足數，也要使用標頭中沒有的資料來填夠。

5.結果要求

1.對於 TCP/IP Architecture 能有更深的瞭解

2.對於每一種 Network Application 所使用的 protocol 能清楚認知

6.Reference:

1.Microsoft MSDN Library 2000 Oct.

2.http://www.theweb.org.tw/nelson/study_area/network/network_tcp.htm
3.Windows 2000 Server 建構徹底研究，旗標出版社，2000