Exp 20：Telnet

目的：了解TELNET 协议的运作模式及如何执行。

摘要：本实验将介绍TCP/IP协定群内的一种远程终端协定，名为TELNET。TELNET 允许使用者透过局域网络或因特网登入远程计算机进行指令操控，本实验借着ITS 里的GUI 接口工具TCP Session教导学生TELNET 控制指令及 TELNET 协议运作模式。除此之外，学生更可藉此学习TELNET client 及 server 间的互动。

时间：4.5 hrs。

一、网络拓扑

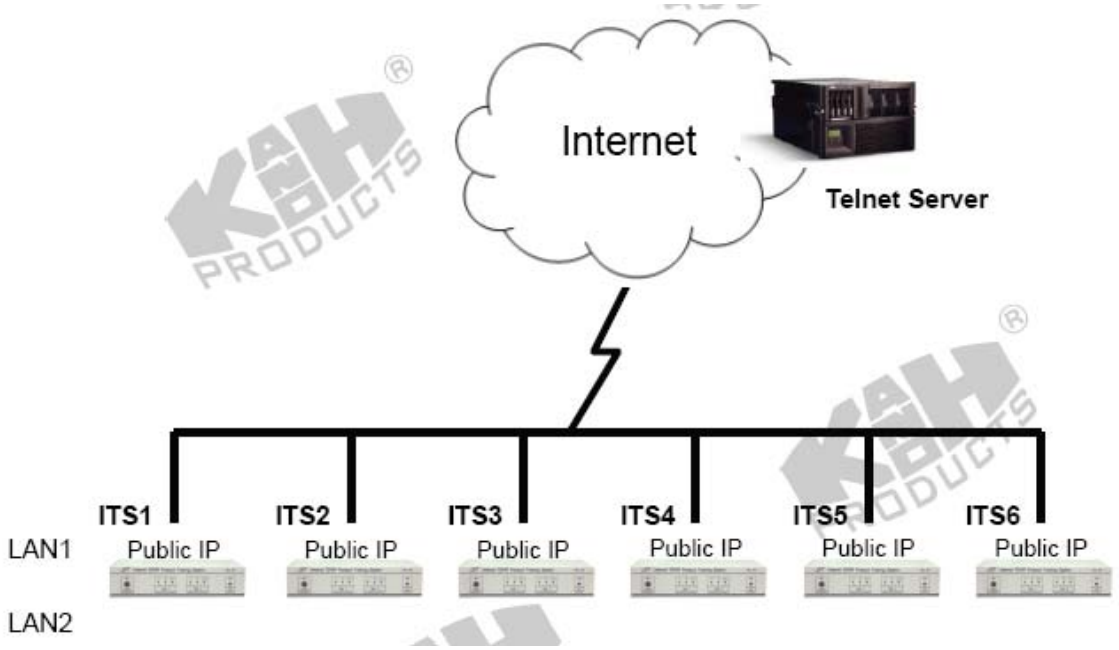


图 20.1

二、技术背景

协议数据：

Protocol suite:	TCP/IP
Port:	23: TCP server.

表 20.1

报文封装图：

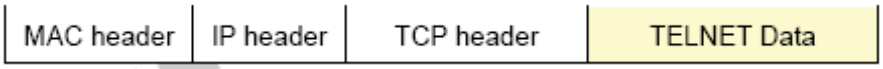


表 20.2

1、TELNET

TELNET 此名源自于telephone network 一词，为一种简单的远距终端协议，允许使用者透过局域网络或因特网登陆远程计算机进行指令操控。TELNET协议靠TCP协议建立联机后，使用者可通过本机的键盘控制远程计算机，彷佛使用者就在远程计算机前操作一样。当然要办到这一点，TELNET也要从远程计算机将输出送回给本地使用者才行。

当client端，也就是本地使用者要与远程计算机做沟通时，必须要先靠TCP建立起联机，联机建立之后，client端计算机就可以将本地使用者从键盘输入的句柄传送给远程计算机，同一时间也会接受从远程计算机传送回来的句柄，再经由本地的机器翻译这些句柄，从使用者的屏幕适当地显示出来。

TELNET协议最一开始，也是最主要的目的，是提供给所有终端设备在网络上一个标准接口，和一个以终端为导向(terminal-oriented)的处理方式，在联机上它可以建立一个8bit的通用双向联机通道。在这里我们还可以说说TELNET协议的两个特色，又或者说TELNET协议就是建立在这两个概念之下：网络虚拟终端机(NVT，Network Virtual Terminal) 与交涉选择(negotiated options)原理。

1）网络虚拟终端机

网络虚拟终端机(NVT，Network Virtual Terminal) 是一个想象的装置，它可以连接网络上的两台终端机，并且互相映像至两端，也就是说，两端的操作系统都不需要管对方终端机的真正型态是什么，只要将本身映像至NVT 即可进行沟通。

2）交涉选择原理

TELNET 和TCP、IP等协议不同，它并没有定义自己封包header的格式，在TELNET协议中，它是将其句柄和数据一起送出，进行选择码序列(option code sequences)的交换动作(见EX20 实验讨论)。句柄和数据一起送出的方式，我们称为：in-band signaling。TELNET 定义了一个特殊字符0xFF ,称为命令直译(IAC，Interpret As Command)，当收到IAC时，其后的资料就会被判断为句柄。下表列出了所有被定义在RFC 854 的指令。

2、TELNET Commands

Code	HEX	Name	Description
240	F0	SE	End of subnegotiation parameters.
241	F1	NOP	No operation.
242	F2	Data Mark	The data stream portion of a Synch. This should always be accompanied by a TCP Urgent notification.
243	F3	Break	NVT character BRK.
244	F4	Interrupt Process	The function IP.
245	F5	Abort output	The function AO.
246	F6	Are You There	The function AYT.
247	F7	Erase character	The function EC.
248	F8	Erase Line	The function EL.
249	F9	Go ahead	The GA signal.
250	FA	SB	Indicates that what follows is subnegotiation of the indicated option.
251	FB	WILL (option code)	Indicates the desire to begin performing, or confirmation that you are now performing, the indicated option.
252	FC	WON'T (option code)	Indicates the refusal to perform, or continue performing, the indicated option.
253	FD	DO (option code)	Indicates the request that the other party perform, or confirmation that you are expecting the other party to perform, the indicated option.
254	FE	DON'T (option code)	Indicates the demand that the other party stop performing, or confirmation that you are no longer expecting the other party to perform, the indicated option.
255	FF	IAC	Data Byte 255.

表 20.3

3、TELNET options

Code	HEX	Option	References
0	0	TRANSMIT-BINARY, Binary Transmission.	RFC 856
1	1	ECHO, Echo.	RFC 857
2	2	Reconnection.	
3	3	SUPPRESS-GO-AHEAD, Suppress Go Ahead.	RFC 858
4	4	Approx Message Size Negotiation.	
5	5	STATUS.	RFC 859
6	6	TIMING-MARK, Timing Mark	RFC 860
7	7	RCTE, Remote Controlled Trans and Echo.	RFC 563, RFC 726
8	8	Output Line Width.	
9	9	Output Page Size.	
10	A	NAOCRD, Negotiate About Output Carriage-Return Disposition.	RFC 652
11	B	NAOHTS, Negotiate About Output Horizontal Tabstops.	RFC 653
12	C	NAOHTD, Negotiate About Output Horizontal Tab Disposition.	RFC 654
13	D	NAOFFD, Negotiate About Output Formfeed Disposition.	RFC 655
14	E	NAOVTS, Negotiate About Vertical Tabstops.	RFC 656
15	F	NAOVTD, Negotiate About Output Vertcial Tab Disposition.	RFC 657
16	10	NAOLFD, Negotiate About Output Linefeed Disposition.	RFC 658
17	11	Extended ASCII.	RFC 698
18	12	LOGOUT, Logout.	RFC 727
19	13	BM, Byte Macro.	RFC 735
20	14	Data Entry Terminal.	RFC 732, RFC 1043
21	15	SUPDUP.	RFC 734, RFC 736
22	16	SUPDUP-OUTPUT, SUPDUP Output.	RFC 749
23	17	SEND-LOCATION, Send Location.	RFC 779
24	18	TERMINAL-TYPE, Terminal Type.	RFC 1091
25	19	END-OF-RECORD, End of Record.	RFC 885
26	1A	TUID, TACACS User Identification.	RFC 927
27	1B	OUTMRK, Output Marking.	RFC 933
28	1C	TTYLOC, Terminal Location Number.	RFC 946
29	1D	Telnet 3270 Regime.	RFC 1041
30	1E	X.3 PAD.	RFC 1053
31	1F	NAWS, Negotiate About Window Size.	RFC 1073
32	20	Terminal Speed.	RFC 1079
33	21	Remote Flow Control.	RFC 1372
34	22	Line mode.	RFC 1184
35	23	X Display Location.	RFC 1096

36	24	Environment Option.	RFC 1408
37	25	AUTHENTICATION, Authentication Option.	RFC 1416, RFC 2941, RFC 2942, RFC 2943, RFC 2951
38	26	Encryption Option.	RFC 2946
39	27	New Environment Option.	RFC 1572
40	28	TN3270E.	RFC 2355
41	29	XAUTH.	
42	2A	CHARSET.	RFC 2066
43	2B	RSP, Telnet Remote Serial Port.	
44	2C	Com Port Control Option	RFC 2217
45	2D	Telnet Suppress Local Echo	
46	2E	Telnet Start TLS	
47	2F	KERMIT	RFC 2840
48	30	SEND-URL	
49	31	FORWARD_X	
50 - 137	32 - 89		
138	8A	TELOPT PRAGMA LOGON	
139	8B	TELOPT SSPI LOGON	
140	8C	TELOPT PRAGMA HEARTBEAT	
141 - 254	8D - FD		
255	FF	EXOPL, Extended-Options-List.	RFC 861

表 20.4

三、实验步骤

1、了解网络拓扑结构

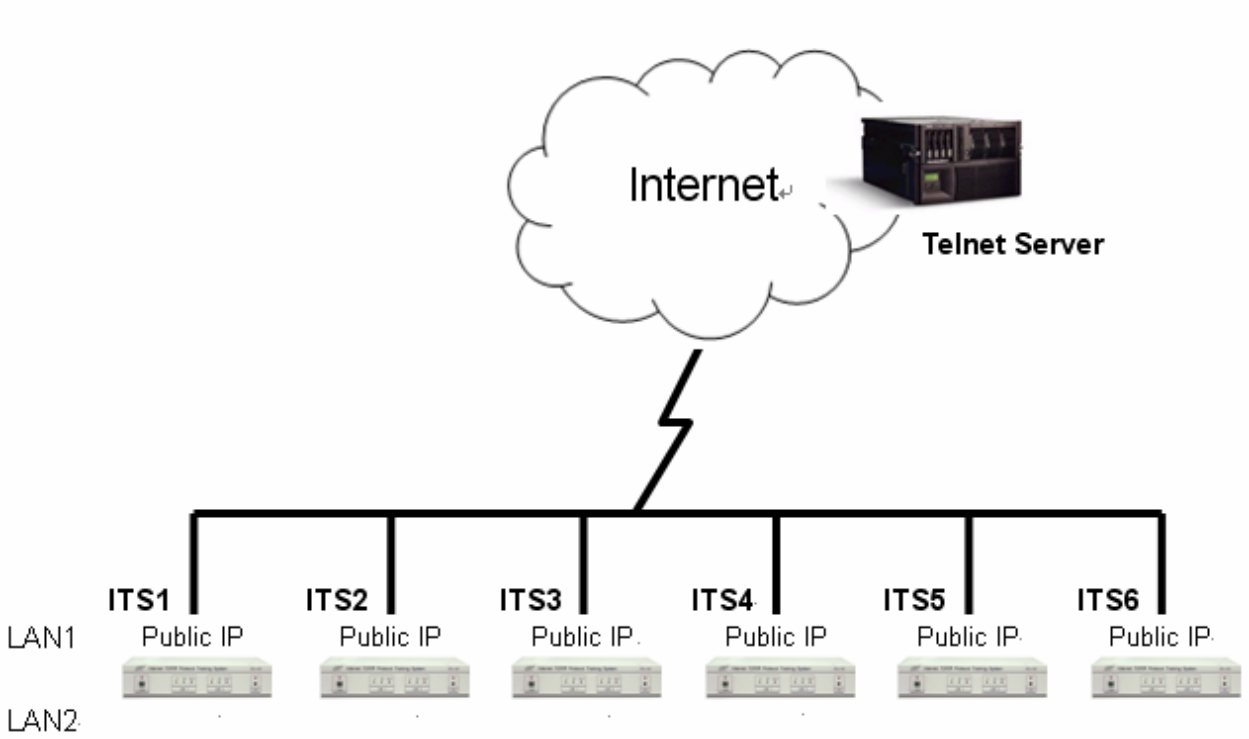


图 20.2

1）Complete the network connections on HUBOX by referring to Figure20.3。

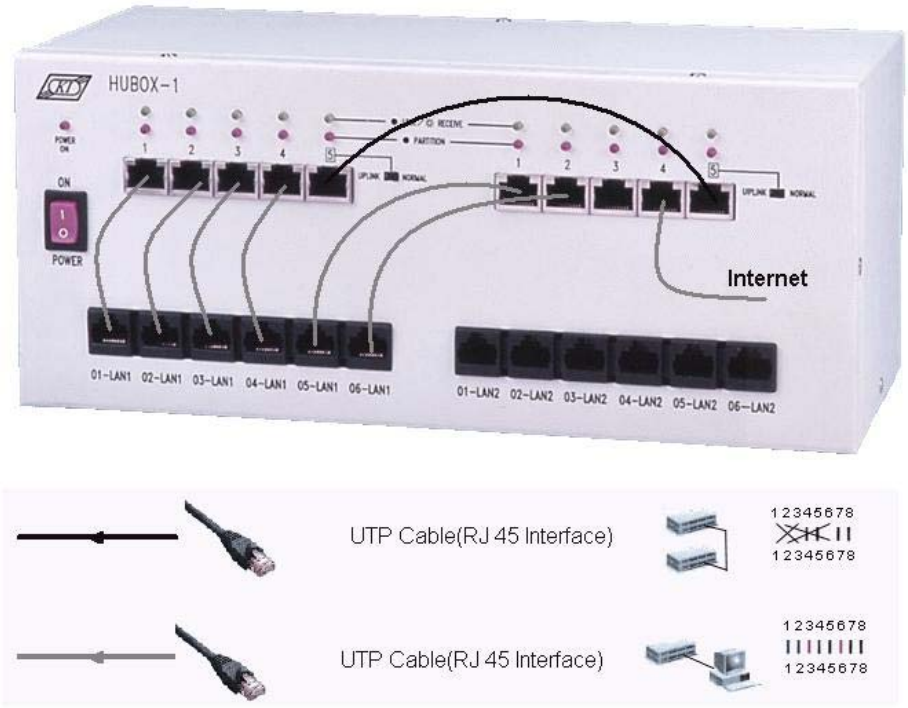


图 20.3

2、TELNET 登陆

A. 初始设置

2）执行 **XCLIENT.BAT，**打开 ITS 应用软件 KCodes Network Explorer。

3）打开网络封包浏览器 Network Message Browser。

4）在网络封包浏览器 Network Message Browser 界面中，选择“**Option”打开“ Set Message Range**”对话框。

5）点击“**Add new rule”按钮**.你需要设定两个参数用于观察封包。首先，在 Remote Port 中定义“23”,然后点击“ **Apply”按钮**。接着在 Local Port 中定义“**23**” ，然后再次点击 **Apply 按钮** (见图 20.4)。

6）最后点击 **Set & Close** 按钮。

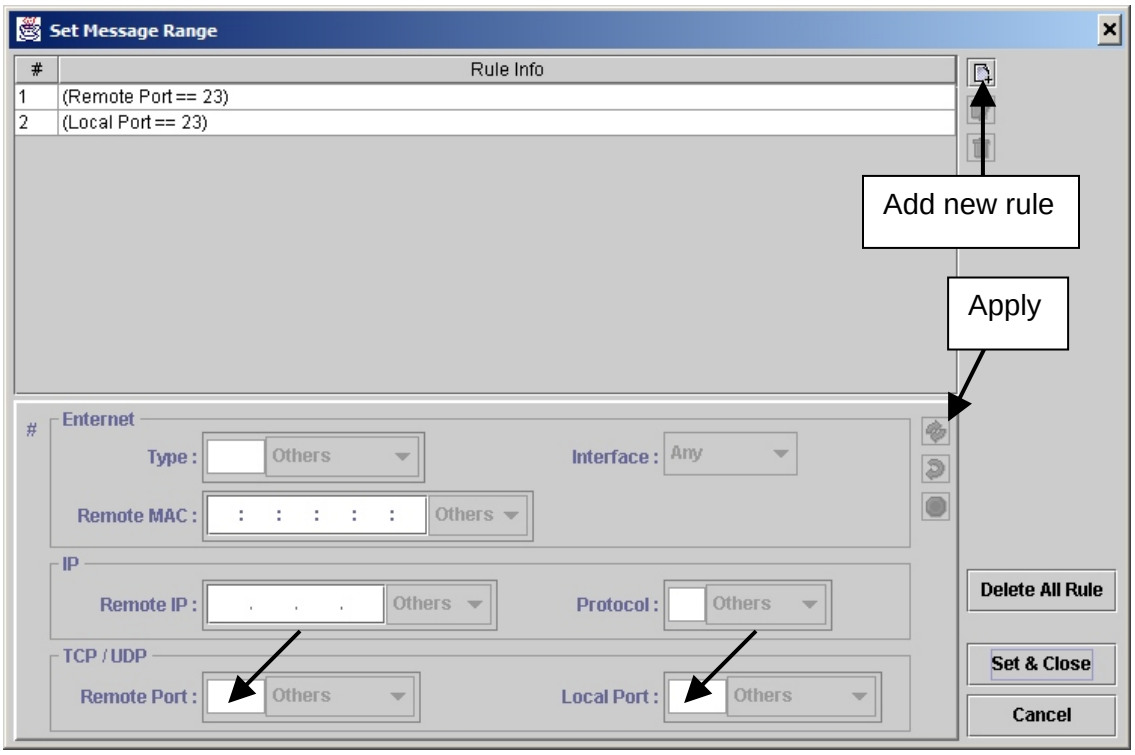


图 20.4

7）从主菜单打开 Network Configuration 设置界面。

8）在 Interface 1 中输入您实验室内分配的 IP 地址，设置您 Internet 网络的网关至路由表中。例如，定义 Interface 1 的 IP 地址为“**192.168.253.1**”， 然后输入“**192.168.253.254**” 至 “Gateway” 并且在 “Destination”and“Mask” 中输入

“**0.0.0.0**”(见图 20.5)。

9）模式选择“ **Host”**，然后点击“ **Set & Close”按钮**。

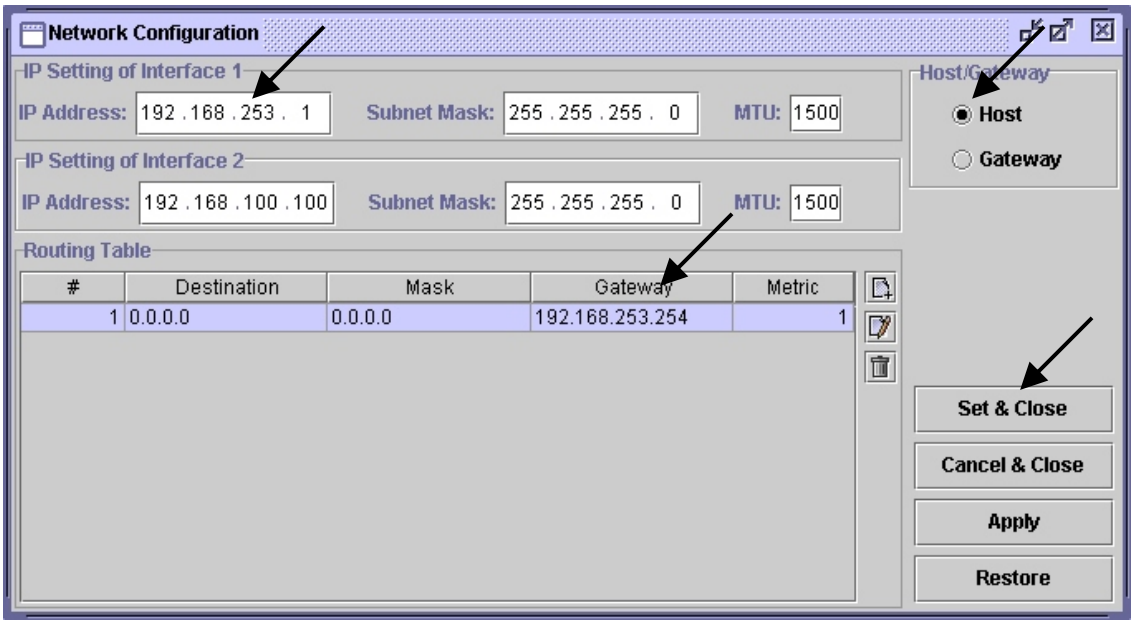


图 20.5

B. 登入 TELNET

10）从 TCP 菜单中点击“ **New TCP Session”** 打开“New TCP Session”对话框。

11）选择“**System Default TCP”**. 定义您的 ***TELNET*** 服务器的 IP 地址至“Destination IP Address”，从“Destination Port”中选择 **TELNET (23)** 例如，在“Destination IP Address”中定义为“**203.149.174.99**”（见图 20.6）。

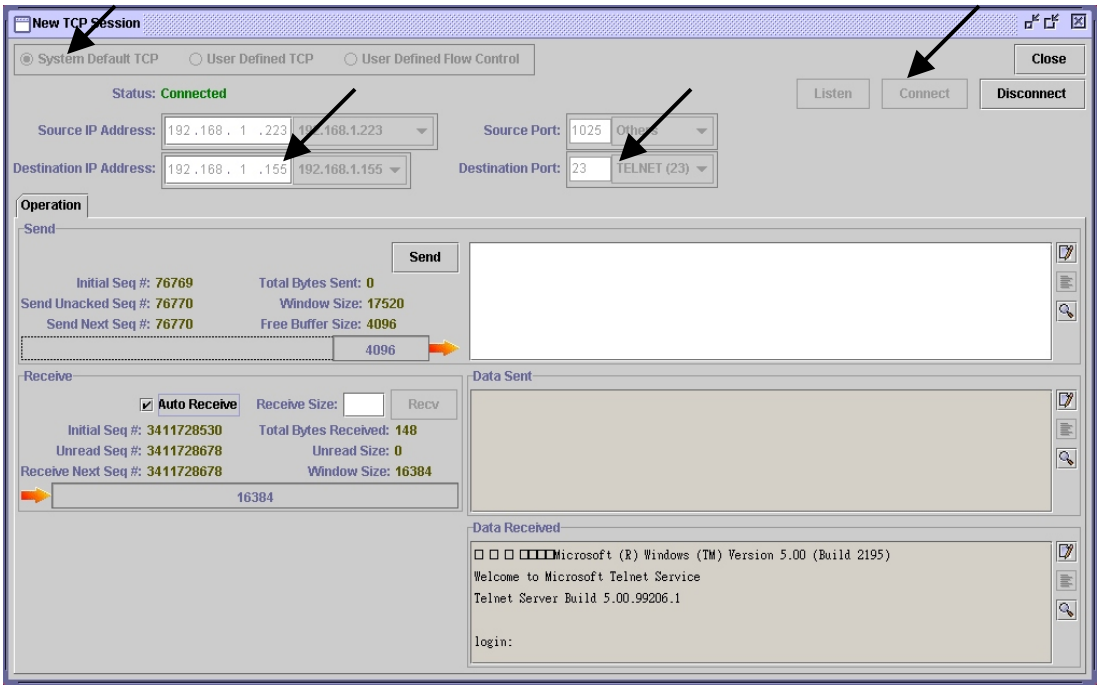
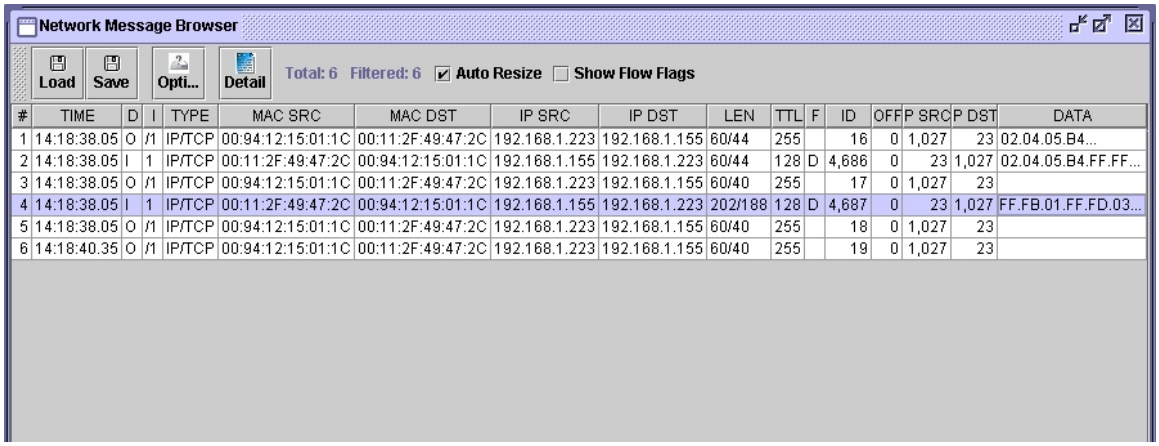


图 20.6

12）点击“**Connect** ”按钮。您将可以通过网络封包浏览器观察到 TELNET 登陆的过程（见图 20.6 and 20.7）。



#	TIME	D	I	TYPE	MAC SRC	MAC DST	IP SRC	IP DST	LEN	TTL	F	ID	OFF	P SRC	P DST	DATA
1	14:18:38.05	O	/1	IP/TCP	00:94:12:15:01:1C	00:11:2F:49:47:2C	192.168.1.223	192.168.1.155	60/44	255		16	0	1,027	23	02.04.05.B4...
2	14:18:38.05	I	1	IP/TCP	00:11:2F:49:47:2C	00:94:12:15:01:1C	192.168.1.155	192.168.1.223	60/44	128	D	4,686	0	23	1,027	02.04.05.B4.FF.FF...
3	14:18:38.05	O	/1	IP/TCP	00:94:12:15:01:1C	00:11:2F:49:47:2C	192.168.1.223	192.168.1.155	60/40	255		17	0	1,027	23	
4	14:18:38.05	I	1	IP/TCP	00:11:2F:49:47:2C	00:94:12:15:01:1C	192.168.1.155	192.168.1.223	202/188	128	D	4,687	0	23	1,027	FF.FB.01.FF.FD.03...
5	14:18:38.05	O	/1	IP/TCP	00:94:12:15:01:1C	00:11:2F:49:47:2C	192.168.1.223	192.168.1.155	60/40	255		18	0	1,027	23	
6	14:18:40.35	O	/1	IP/TCP	00:94:12:15:01:1C	00:11:2F:49:47:2C	192.168.1.223	192.168.1.155	60/40	255		19	0	1,027	23	

图 20.7

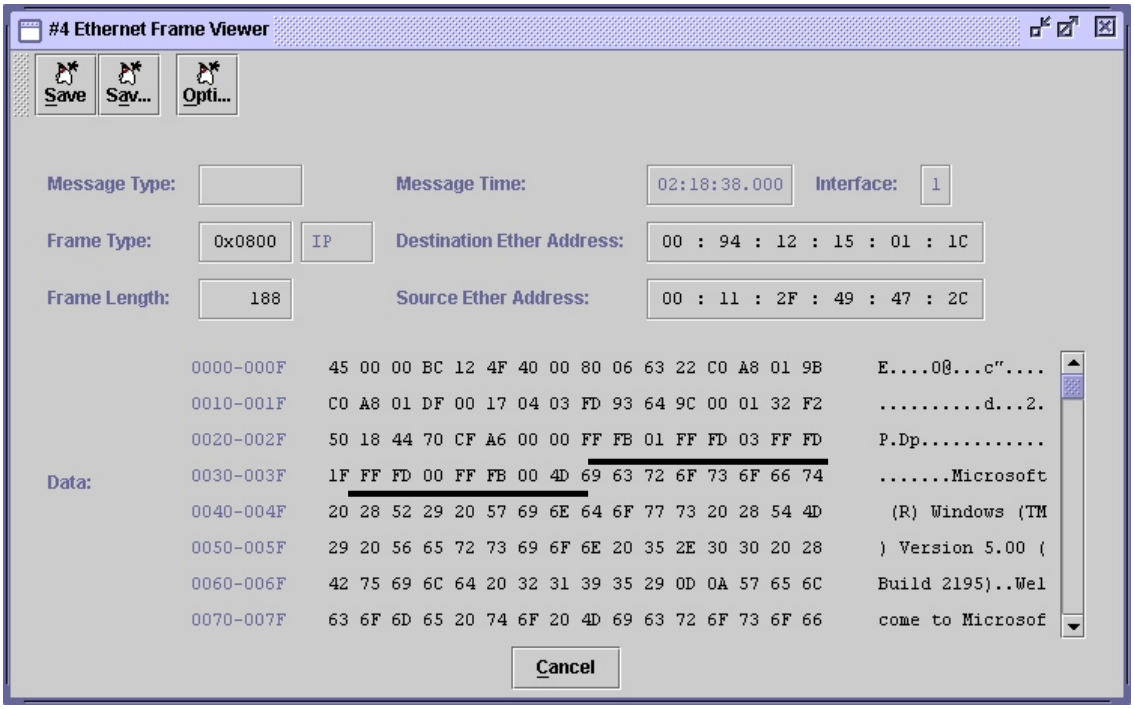


图 20.8

四、实验讨论

1、对建构在某些操作系统的TELNET server 而言，可以使用到完整TELNET进行选择码序列(option code sequences)的交换动作，此时可以依下表的顺序，从TCP Session按步输入client 端的指令，完成登入TELNET的动作。

Sequence	Direction (send)	Options in Text Mode	Options in Binary Mode
1	Server	DO TERMINAL TYPE	FF FD 18
2	Server	DO TERMINAL SPEED	FF FD 20
3	Server	DO X DISPLAY LOCATION	FF FD 23
4	Server	DO NEW ENVIRINMENT OPTION.	FF FD 27
5	Client	WILL TERMINAL TYPE	FF FB 18
6	Client	WONT TERMINAL SPEED	FF FC 20
7	Client	WONT X DISPLAY LOCATION	FF FC 23
8	Client	WILL NEW ENVIRINMENT OPTION.	FF FB 27
9	Client	WILL NAWS (Negotiate About Window Size)	FF FB 1F
10	Server	DO NAWS (Negotiate About Window Size)	FF FD 1F
11	Client	SB NAWS 80 x 25 SE	FF FA 1F 00 50 00 19 FF F0
12	Server	IAC SB NEW ENVIRINMENT SEND	FF FA 27 01 FF F0
9	Server	IAC SB TERMINAL TYPE SEND	FF FA 18 01 FF F0
10	Client	IAC SB NEW ENVIRINMENT IS	FF FA 27 00 FF F0
11	Client	IAC SB TERMINAL TYPE IS “ANSI”	FF FA 18 00 41 4E 53 49 FF F0
12	Server	WILL SUPPRESS GO AHEAD	FF FB 03
13	Server	DO ECHO	FF FD 01
14	Server	WILL STATUS	FF FB 05
15	Server	DO LFLOW	FF FD 21
16	Client	DO SUPPRESS GO AHEAD	FF FD 03
17	Client	WILL ECHO	FF FB 01
18	Client	DONT STATUS	FF FE 05
19	Client	WONT LFLOW	FF FC 21
20	Server	DONT ECHO	FF FE 01
21	Server	WILL ECHO	FF FB 01

表 20.5