

Exp 8: IP 绕送路径之追踪

目的：介绍TTL的延伸应用，即使用传送ICMP报文，找出绕送路径的方法。

摘要：本实验将引用 trace routing 的算法，并通过MDDL语言让学生了解如何应用这些算法来发现数据包的路径。

时间：3 hrs。

一、网络拓扑

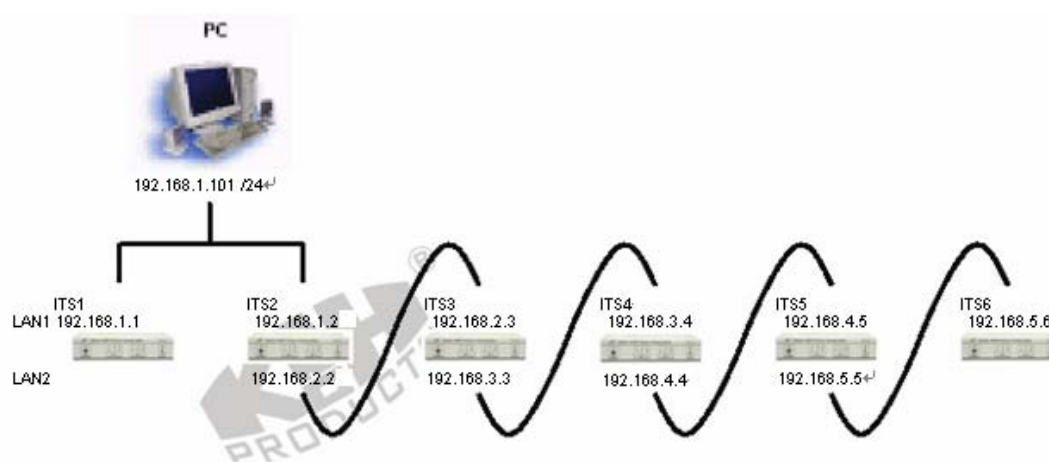


图8.1

二、技术背景

实验4中我们提到了ICMP协议，使用MDDL设计ICMP程序，并了解了ping指令的功能，不但可以验证网络上的点对点联机是否正常，同时也能收集一些联机效能的信息。实验7中我们则学到了TTL的机制，而追踪IP绕送路径(trace routing)，即是结合这些技术并加以运用的最佳例子。计算机指令tracert主要是使用相同于ping指令的功能透过TTL=0时会回传报文溢时(time, exceeded)的机制，首先发出TTL=X(起始值为1)的ICMP Echo Request给目的端，当回传溢时后再发出TTL=X+1的ICMP Echo Request，直到成功得到ICMP Echo Reply为止，如此一来便得知绕送过程中的所有节点。

而ICMP回传溢时的报文格式如表8.1所示：当一gateway 试着将一目的地址不为本身的IP报文绕送出去时，如果TTL值减1后变为0，此gateway 将会停止绕送并回发一个ICMP错误讯息“Time Exceeded” (type = 11) 给发送端。

0	8	16	31
TYPE (11)	CODE (0)	CHECKSUM	
UNUSED (0)			
INTERNET HEADER + 64 BITS OF ORIGINAL DATAGRAM DATA.			

表8.1

ICMP 协议里定义的错误回报讯息种类则如图 8.2 所示：

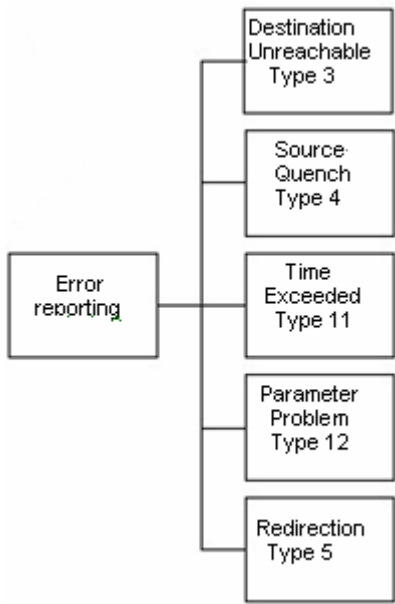


图8.2

三、实验步骤

1、网络拓扑连线

1) 在Hubox上的拓扑连线如图8.3所示。本实验设计让6台ITS连接成一个完整的实验网络。

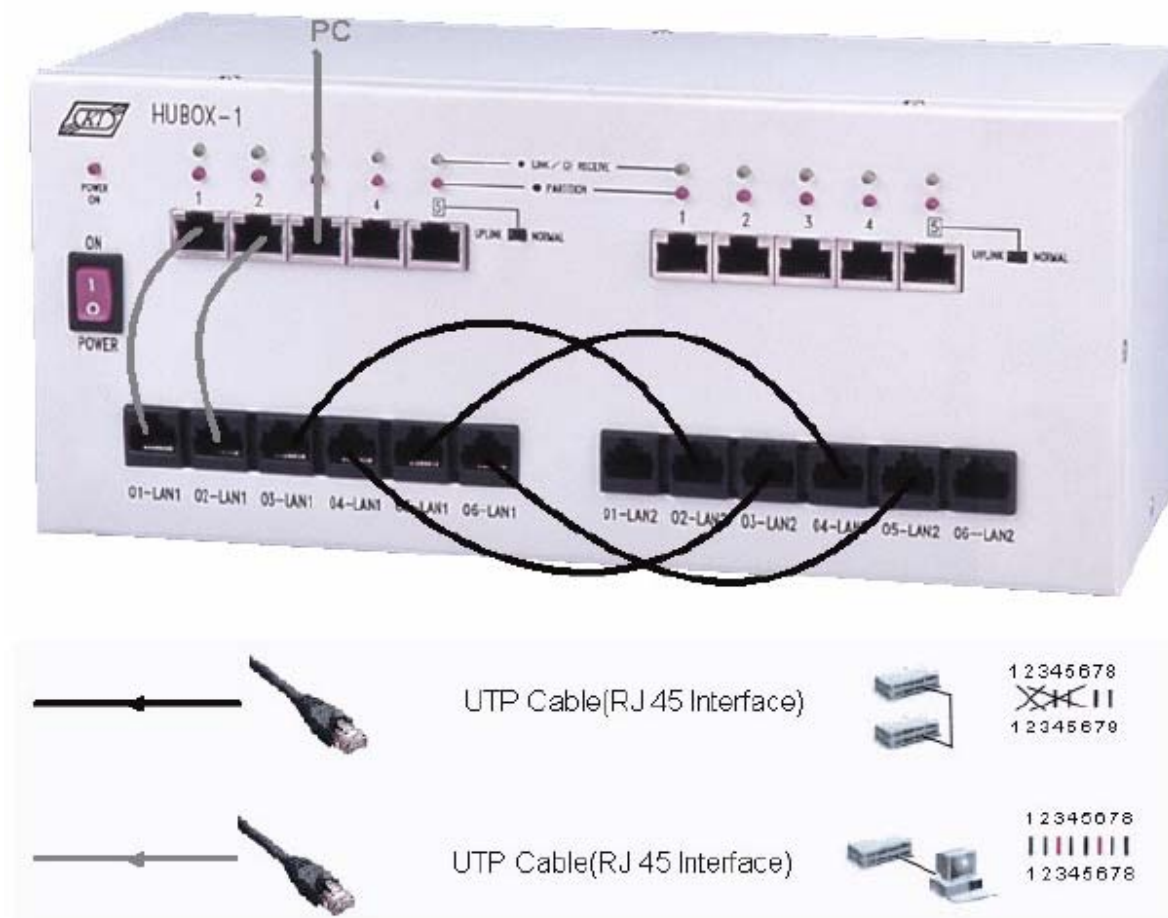


图8.3

2、路进追踪

A. 路由表的设定

所有ITS

- 2) 从Tool menu 里选择Network Configuration, 参考网络拓扑图, 在网络属性配置界面里输入每台ITS的IP地址, 并且设定ITS1和ITS6为“Host”模式, 其他ITS均设为“Gateway”模式。
- 3) 参考实验7里表7.1的路由表配置每台ITS, 然后点击Set&Close 按钮。此时, ITS1至ITS6可以相互通信。
- 4) 打开网络信息浏览器 (Network Message Browser), 勾选Listening On。

PC

- 5) 确定您的PC安装的是Windows XP操作系统。
- 6) 从XP系统中找到“控制面板”, 再找到“网络连接”, 如图 8.4

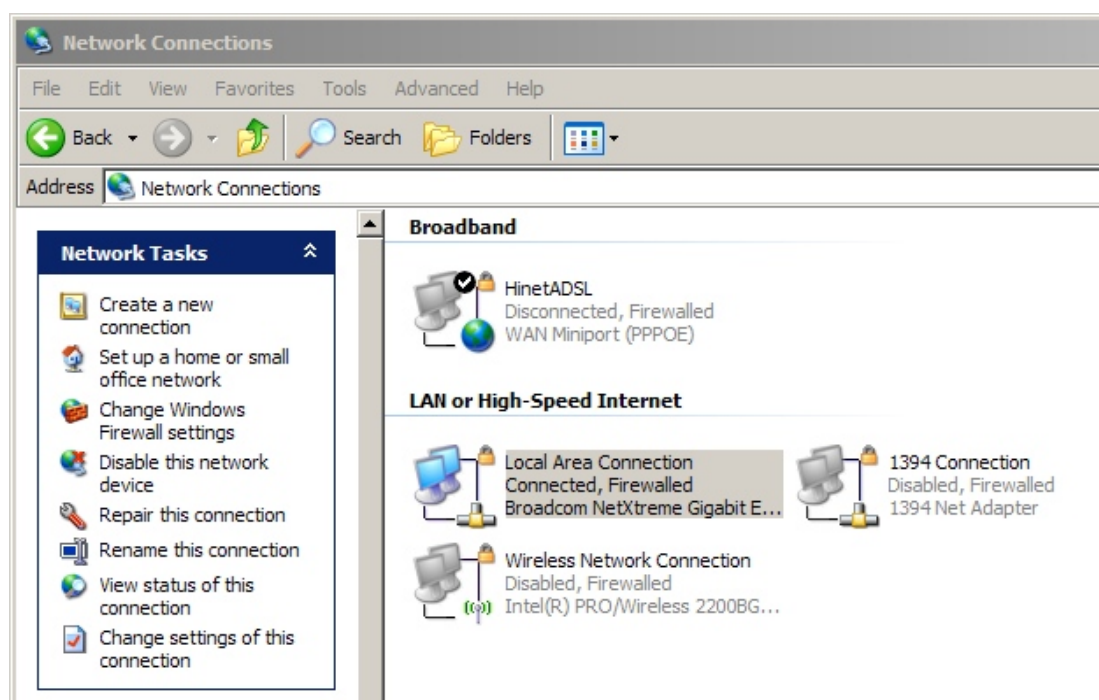


图8.4

7) 打开其中的本地连接界面，进入本地连接属性对话框，如图8.5。

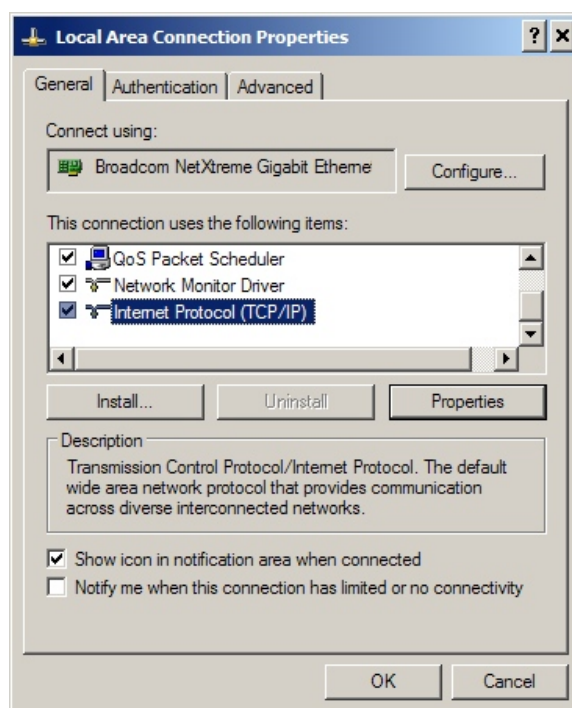


图8.5

8) 在众多选项里找到 Internet Protocol (TCP/IP)，并点击属性按钮。此时，将会打开一个视窗界面如图 8.6 所示。选择“使用下面的 IP 地址”自定义 IP 地址和子网掩码。在本范例中，我们可以输入 “192.168.1.101”到 IP 地址栏，输入“255.255.255.0”到子网掩码栏，输入“192.168.1.2”到默认网关，设定完成后点击确定按钮。

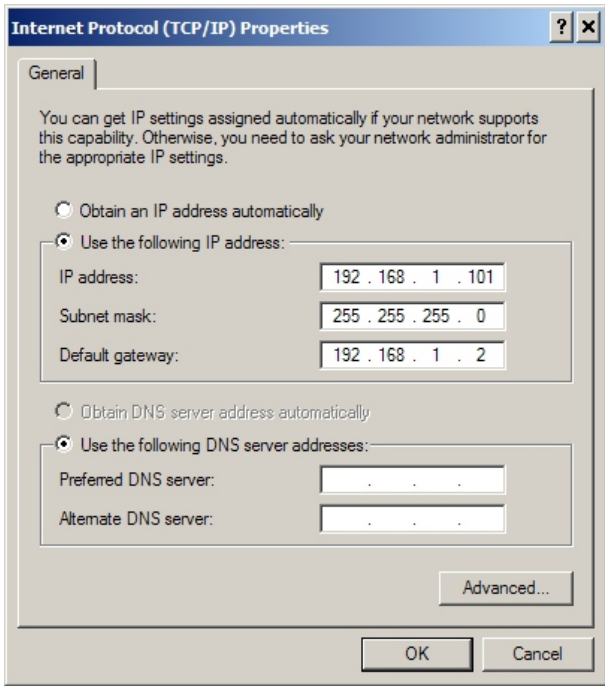


图 8.6

B. 追踪 ITS6 的绕送路径

PC

9) 再从 Windows XP 的附属应用程序中，打开一个新的命令提示符（Command Prompt），然后输入指令 `tracert -d 192.168.5.6`。如图 8.7 所示，我们即开始从 PC 追踪 ITS6 的绕送路径。

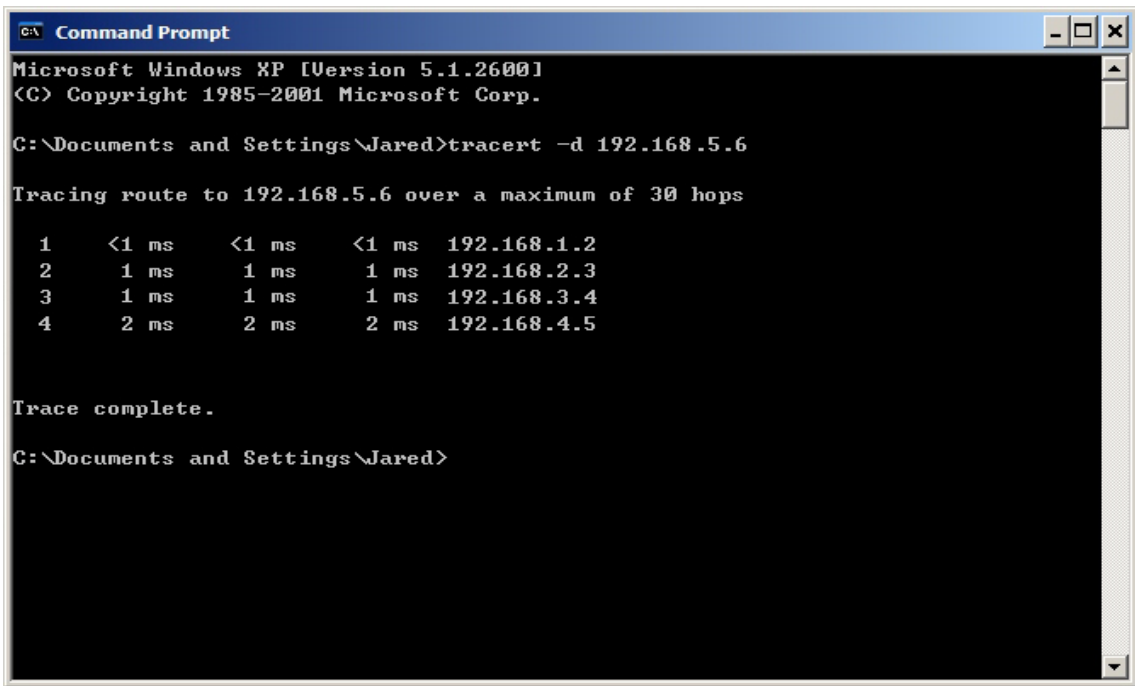


图 8.7

所有 ITS

- 10) 在 PC 成功追踪 ITS6 的绕送路径后, 接下来我们可以尝试用 ITS1 追踪 ITS6。
- 11) 打开一个新的网络信息浏览器 (Network Message Browser), 同时确定 Listening level 中 IP Packets 和 Interface Frames 的选项均打勾。

ITS1

- 12) 从 Send 菜单中选择 Send IP Packet, ITS 会自动打开 IP Datagram Sender 发送界面, 如图 8.8 所示, 注意黑色箭头所指的区域: TTL 处输入“1”; Protocol 处选择“1 (ICMP)”; Destination IP Address 处输入“192.168.5.6”, 并在 Data 处输入 “08:00:F7:FF:00:00:00:00”, 最后点击 Send 按钮。

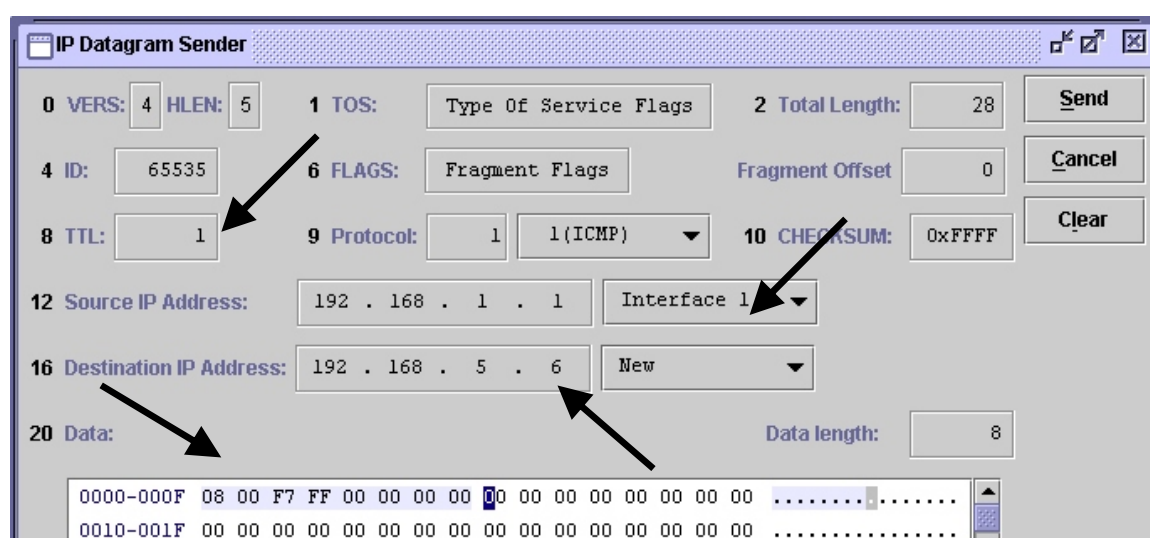
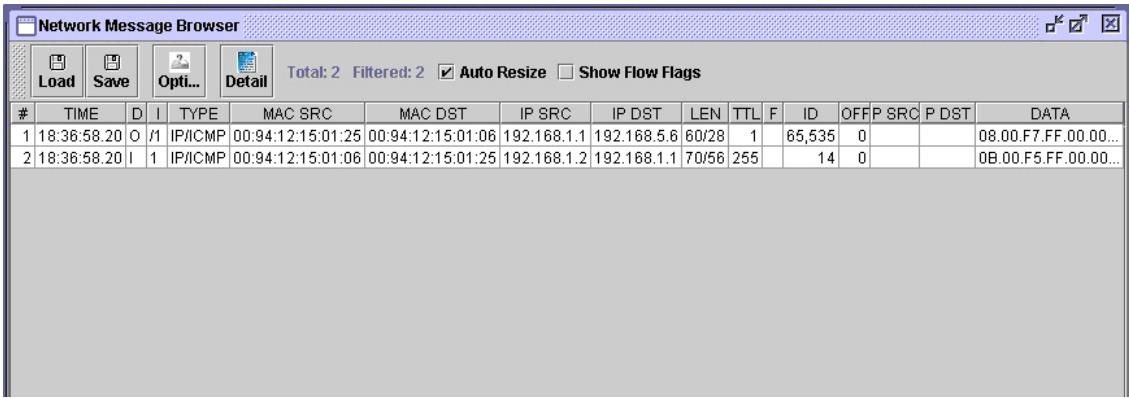


图 8.8

- 13) 这个发送出去的 IP 报文就是一个标准的 ICMP Echo Request 报文。如果一切无误, ITS1 将 ICMP Echo Request 发送出去后, 将会立即收到一个来自 ITS2 的 ICMP Echo Reply 报文, 并且 header 类型是“0B.00” (见图 8.9) 这是因为 ITS1 与 ITS6 中间要经过四个路由, 但我们只将 TTL 设为“1”。下面, 我们可以由 ITS1 再发送一个 TTL 为“2”的 ICMP Echo Request 报文, 此时, 会收到来自 ITS3 的 ICMP Echo Reply, 它的 header 类型同样是“0B.00”。

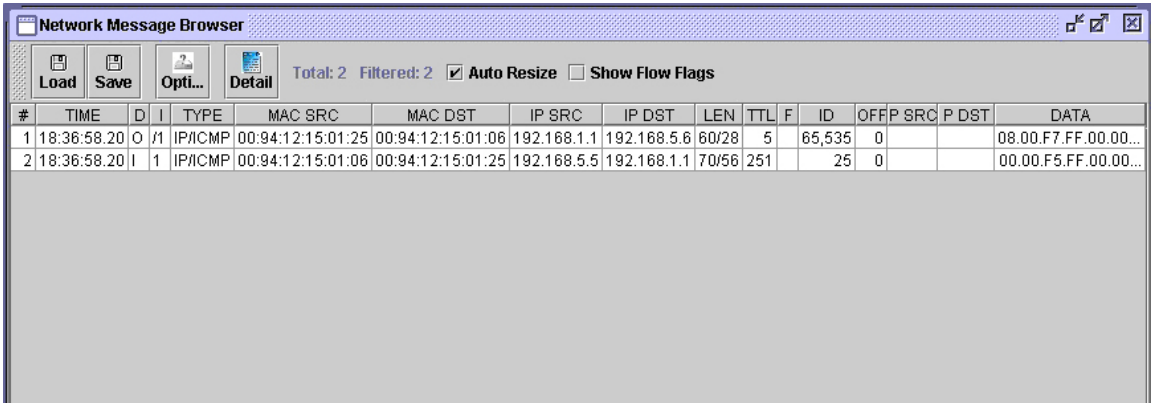


The screenshot shows the Network Message Browser window with two packets. The first packet is an ICMP Echo Request from 192.168.1.1 to 192.168.5.6 with TTL 1. The second packet is an ICMP Echo Request from 192.168.1.2 to 192.168.1.1 with TTL 255.

#	TIME	D	I	TYPE	MAC SRC	MAC DST	IP SRC	IP DST	LEN	TTL	F	ID	OFF	P SRC	P DST	DATA
1	18:36:58.20	O	/1	IP/ICMP	00:94:12:15:01:25	00:94:12:15:01:06	192.168.1.1	192.168.5.6	60/28	1		65,535	0			08.00.F7.FF.00.00...
2	18:36:58.20	I	1	IP/ICMP	00:94:12:15:01:06	00:94:12:15:01:25	192.168.1.2	192.168.1.1	70/56	255		14	0			0B.00.F5.FF.00.00...

图 8.9

14) 重复发送 ICMP Echo Request 给 ITS6, 并且每次将 TTL 增加 1, 直到收到来自 ITS6 的 ICMP Echo Reply (header 类型为“00.00”.), 如图 8.10 所示, 这就表示 ITS1 已经成功的 Ping 到 ITS6, 并追踪处绕送路径上的所有路由。



The screenshot shows the Network Message Browser window with two packets. The first packet is an ICMP Echo Request from 192.168.1.1 to 192.168.5.6 with TTL 5. The second packet is an ICMP Echo Request from 192.168.5.5 to 192.168.1.1 with TTL 251.

#	TIME	D	I	TYPE	MAC SRC	MAC DST	IP SRC	IP DST	LEN	TTL	F	ID	OFF	P SRC	P DST	DATA
1	18:36:58.20	O	/1	IP/ICMP	00:94:12:15:01:25	00:94:12:15:01:06	192.168.1.1	192.168.5.6	60/28	5		65,535	0			08.00.F7.FF.00.00...
2	18:36:58.20	I	1	IP/ICMP	00:94:12:15:01:06	00:94:12:15:01:25	192.168.5.5	192.168.1.1	70/56	251		25	0			00.00.F5.FF.00.00...

图 8.10

2、用MDDL追踪绕送路径

所有 ITS

15) 打开一个新的网络信息浏览器(Network Message Browser.), 并勾选 **Listening On**。

ITS1

16) 从 Reactor menu 中运行 **MDDL Reactor Panel** 。打开 MDDL 编辑平台。

17) 点击 **Load** 按钮, 调用 RuleTraceroute.mddl 程序(路径为 C: \XClient \Data \Mddl \Tutorial \Ex08 \RuleTraceroute.mddl), 再点击 **Upld** 按钮。载入程序后, 我们从 ITS1 发送一个 TTL 值为 1 的 ICMP Echo Request 报文给 ITS6 时, ITS 会做类似 PC 的 tracert 指令一样的动作, 自动最终路径。

四、实验讨论

- 1、试想其它任何可行的方式，找到所有介于来源端和目的端间的所有节点。

REACTOR PROGRAM

1、RuleTraceroute.mddl

```

IP_RECEIVED_HANDLER
{
    IF(S.IP_PROT != CNST_IP_PROT_ICMP || S.IP_DATA.ICMP_TYPE != 11)
        RETURN;

    VAR1[0] = VAR1[0] + 1;
    IF(VAR1[0] < 128)
    {
        SEND_OUT_IP WITH_DATA
        {
            T.IP_TTL                = VAR1[0]                ,
            T.IP_PROT                = CNST_IP_PROT_UDP      ,
            T.IP_ADDR SRC            = S.[28, ].IP_ADDR SRC  ,
            T.IP_ADDR DST            = S.[28, ].IP_ADDR DST  ,
            T.[20, 21]               = S.[28, ].ICMP_TYPE_CODE ,
            T.[22, 23]               = S.[28, ].ICMP_CHKSUM  ,
            T.[24, 25]               = 12W                   ,
            T.[26, 27]               = 0W                    ,
            T.[28, 31]               = "TEST"                ,
            T.IP_LEN                 = LENGTH(T)              ,
            T.IP_HEADER_CHKSUM       = {0, 0}                 ,
            T.IP_HEADER_CHKSUM       = CHECKSUM(T.IP_HEADER)

        }
    }
}

```