实验三 分组嗅探器的使用

【实验目的】

1. 了解协议分析仪的使用方法和基本特点，掌握使用协议分析仪分析协议的方法；
2. 了解 Ping 命令的工作过程；
3. 了解 FTP 协议的工作过程。

【预备知识】

1. 熟悉 Ping 命令，FTP 协议；
2. 了解协议分析仪的功能和工作原理；
3. 了解 Sniffer pro 分析仪的使用方法；
4. 阅读本实验的阅读文献；

【实验内容】

1. 使用 Sniffer 分析仪捕获一段 Ping 命令的数据流,并分析其工作过程。
2. 登录 ftp://networklab: networklab @210.26.100.188，并下载一个小文件，使用 sniffer 分析仪分析其工作过程。
3. 设置显示过滤器，以显示所选部分的捕获数据。

【实验要求】

1. 完成上述实验内容；
2. 记录捕获的关键数据，并分析协议工作过程。

【实验内容】

Sniffer 是 NAI 公司推出的协议分析软件，它可以利用计算机的网络接口截获目的地为其他计算机的数据报文，并迎合了网络管理所需的基本要求，支持丰富的协议，能够进行快速解码分析，而且 Sniffer 可以运行在各种 Windows 平台。

1、网络适配器的选择

在使用 Sniffer 软件之前必须要做的一件工作是为计算机选择合适的网络适配器，确定数据的接收渠道。用户可以通过命令 File/Select Setting…来实现（如图 1）。*如果系统只有一个网卡，则在软件初始化安装的时候就已经安装选择，并非每次启动都会选择。*

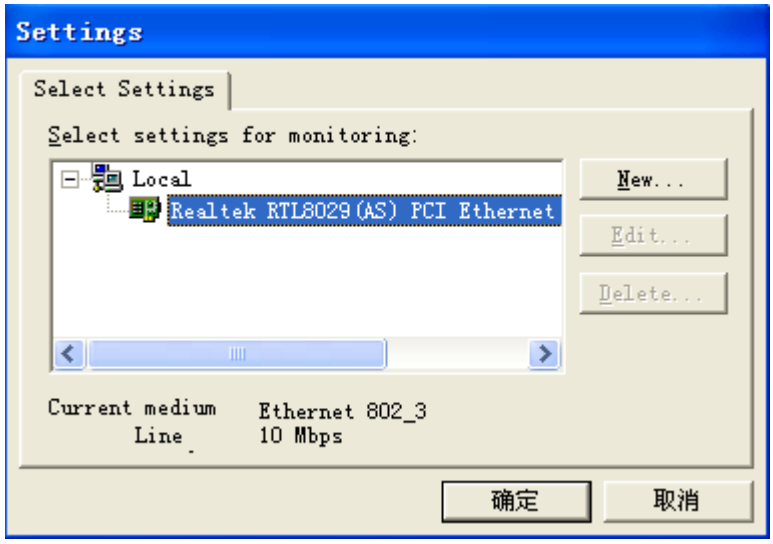

图 1

2、捕获报文

Sniffer 软件提供了两种最基本的网络分析操作，即报文捕获和网络性能监视（如图 2）。在这里我们首先对报文的捕获加以分析，然后再去了解如何对网络性能进行监视。

图 2

- 捕获面板

报文捕获可以在报文捕获面板中进行，如图 2 中蓝色标注区所示即为开始状态的报文捕获面板，其中各按钮功能如图 3 所示

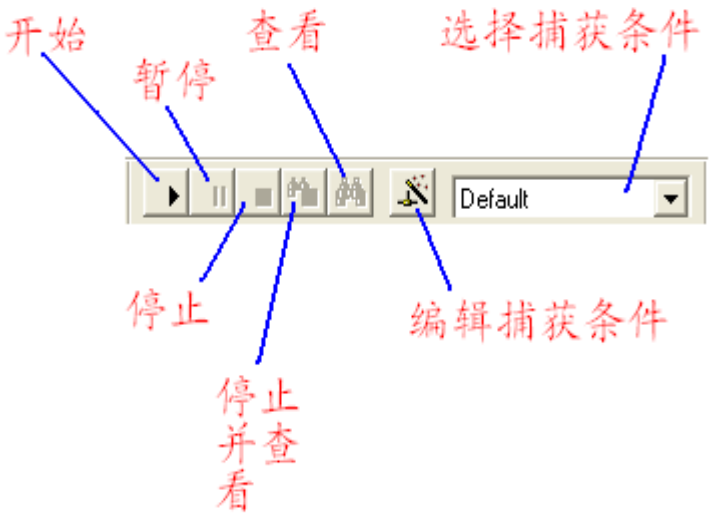

图 3

- 捕获过程的报文统计

在报文统计过程中可以通过单击 Capture Panel  按钮来查看捕获报文的数量和缓冲区的利用率（如图 4、5）。

图 4

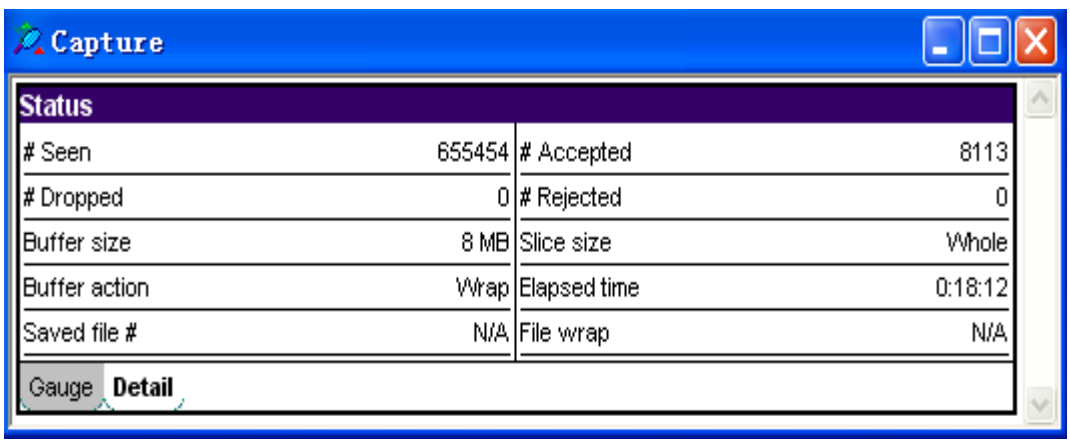

图 5

- 捕获报文的查看

如图 6 所示，Sniffer 软件提供了强大的分析和解码功能。对于捕获的报文可以通过 Expert、Decode、Matrix、Host Table、Protocol Dist 和 Statistics 来进行全方位的综合分析。由于 Matrix、Host Table、Protocol Dist 和 Statistics 将在网络性能监视部分详细介绍，所以本部分仅以 Expert 和 Decode 为重点作详细介绍。

a) Expert（专家分析）

专家分析系统平台只能对网络上的流量进行一些分析，对于分析的结果可以查看在线帮助获得。如图 6 所示即显示了在网络中 WINS 查询失败的次数及 TCP 重传的次数统计等内容，这样可以方便地了解网络中高层协议出现故障的可能节点。对于某项统计分析可以通过用鼠标双击此条记录来查看详细统计信息，且对于每一项都可以通过查看帮助来了解产生的原因。

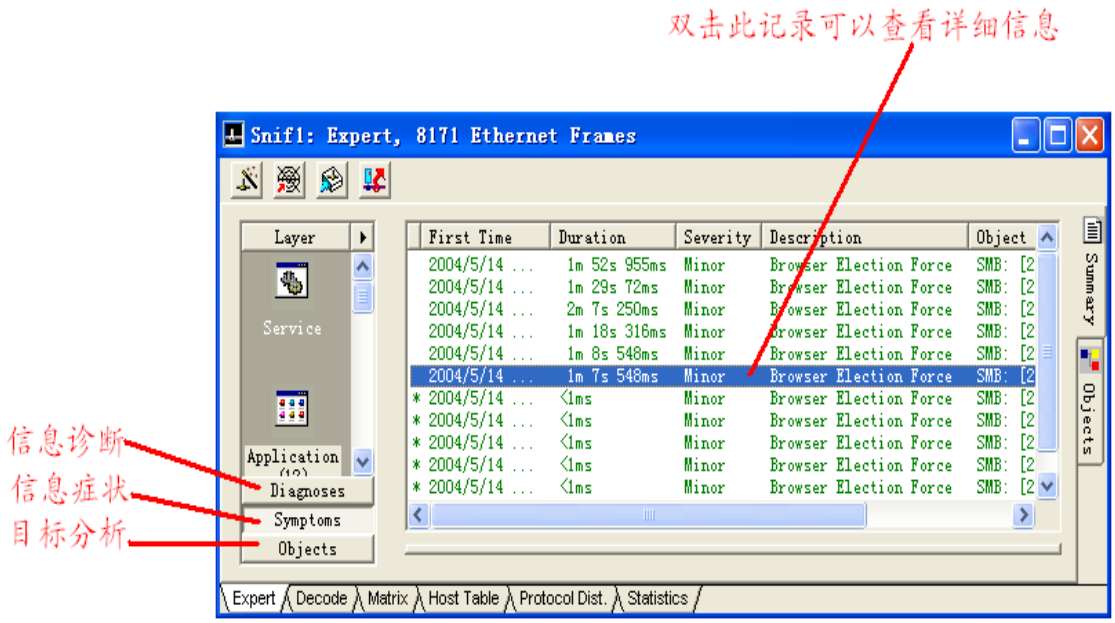

图 6

b) Decode（解码分析）

如图 7 所示为对捕获的报文进行解码分析，界面分为三个部分，分别显示捕获的报文、相应报文的解码和对应的二进制码。对于解码部分，要求分析人员对协议比较熟悉，而我们正通过协议课程学习，所以暂时没办法看懂解析出来的报文，要通过后继课程的学习不断积累和理解。

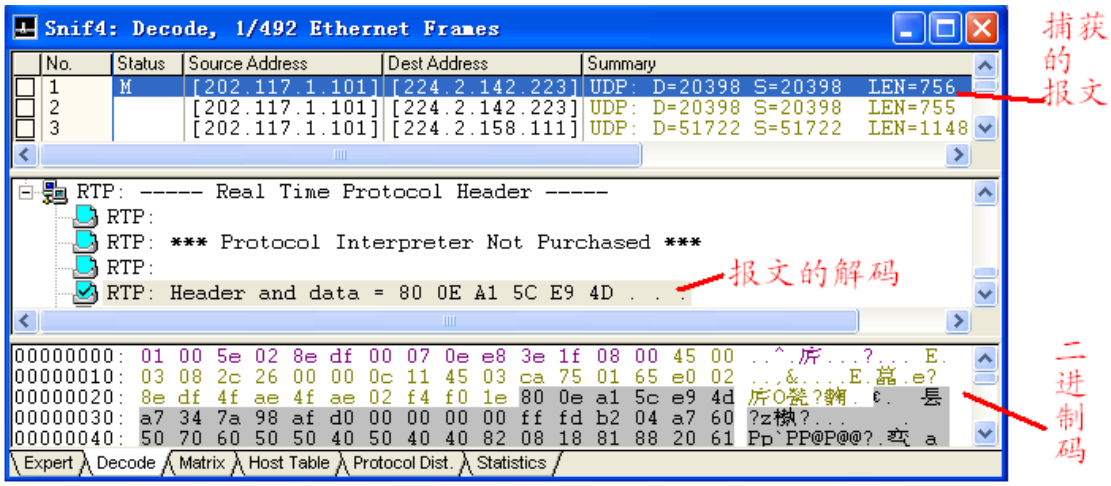

图 7

- 设置捕获条件

捕获功能是按照过滤设置的过滤规则进行数据的捕获和显示的。单击 Define Filter 按钮（Capture/Define Filter 或 Display/Define Filter）则可在弹出的过滤设置对话框中根据物理地址或 IP 地址和协议选择进行组合筛选。

如图 8 所示为捕获条件基本情况的显示，而在图 9 所示对话框中则可以为捕获所需报文的缓冲区做参数和行为上的设定。

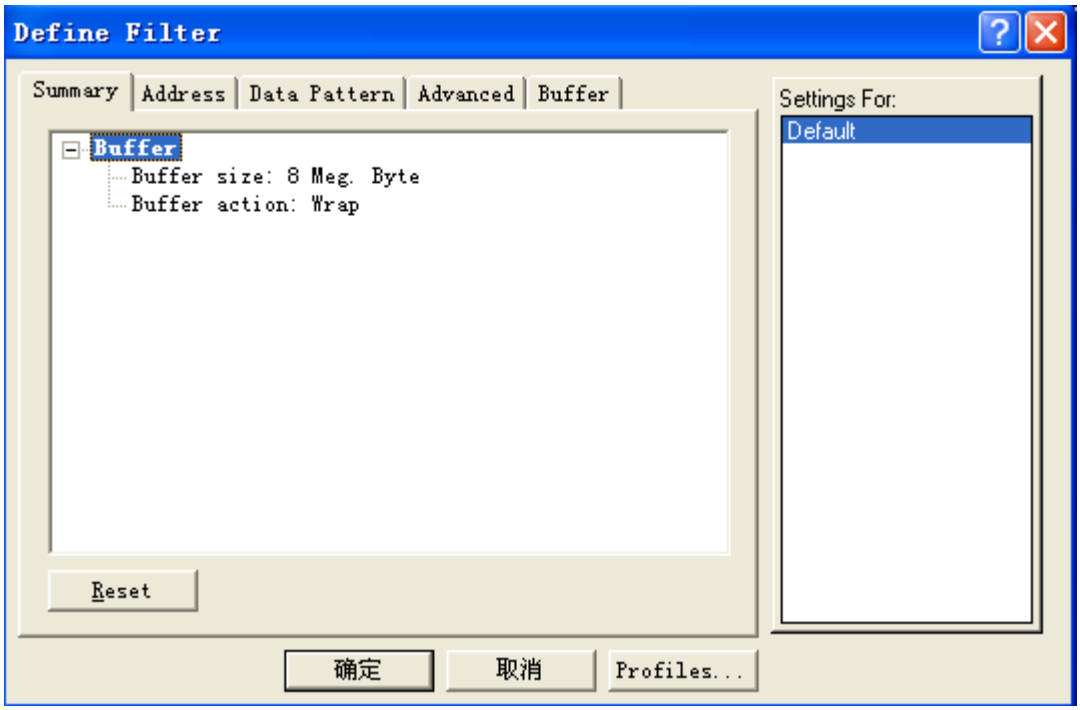

图 8

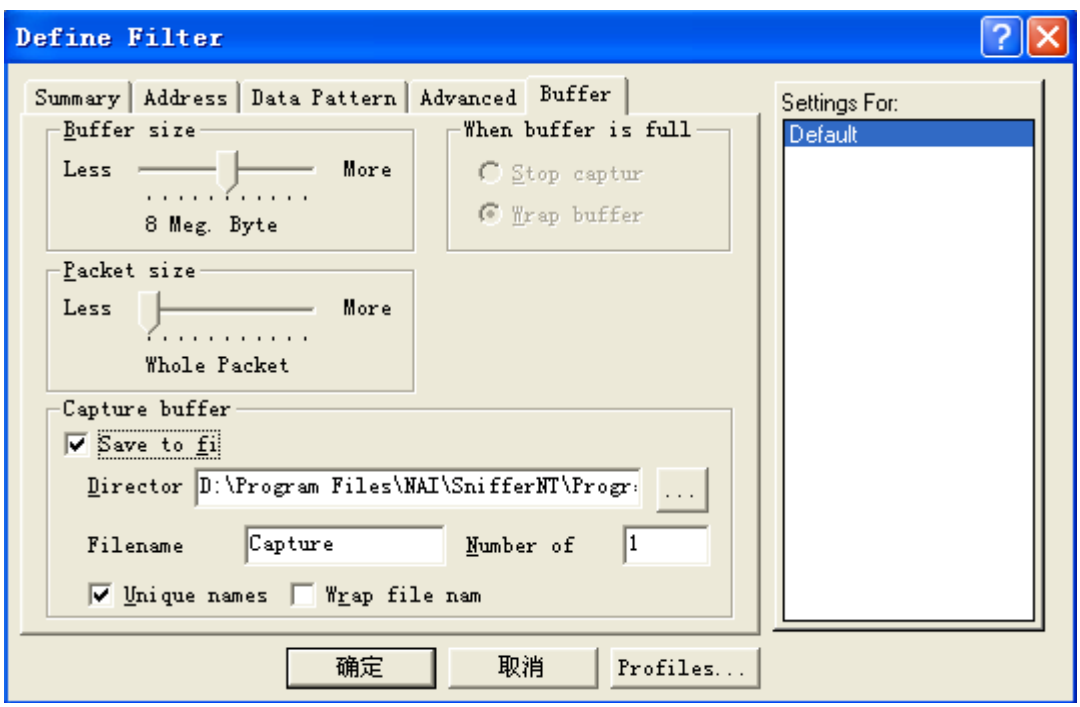

图 9

基本捕获条件

1）连路层捕获，按源 MAC 和目的 MAC 地址进行捕获，输入方式为十六进制连续

输入，如：00E0FC123456

2）IP 层捕获，按源 IP 和目的 IP 进行捕获。输入方式为点间隔方式，如：10.107.1.1。如果选择 IP 层捕获条件则 ARP 等报文将被过滤掉（如图 10）。

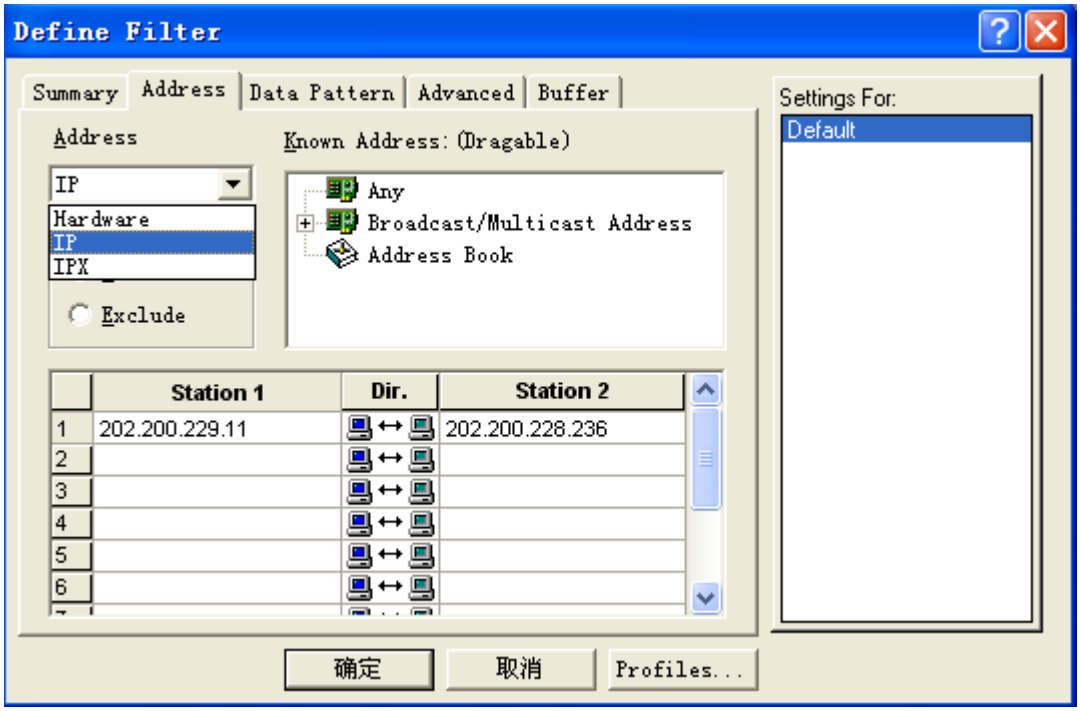

图 10

高级捕获条件

单击 Advance 按钮，用户可以编辑自己的协议捕获条件（如图 11）。

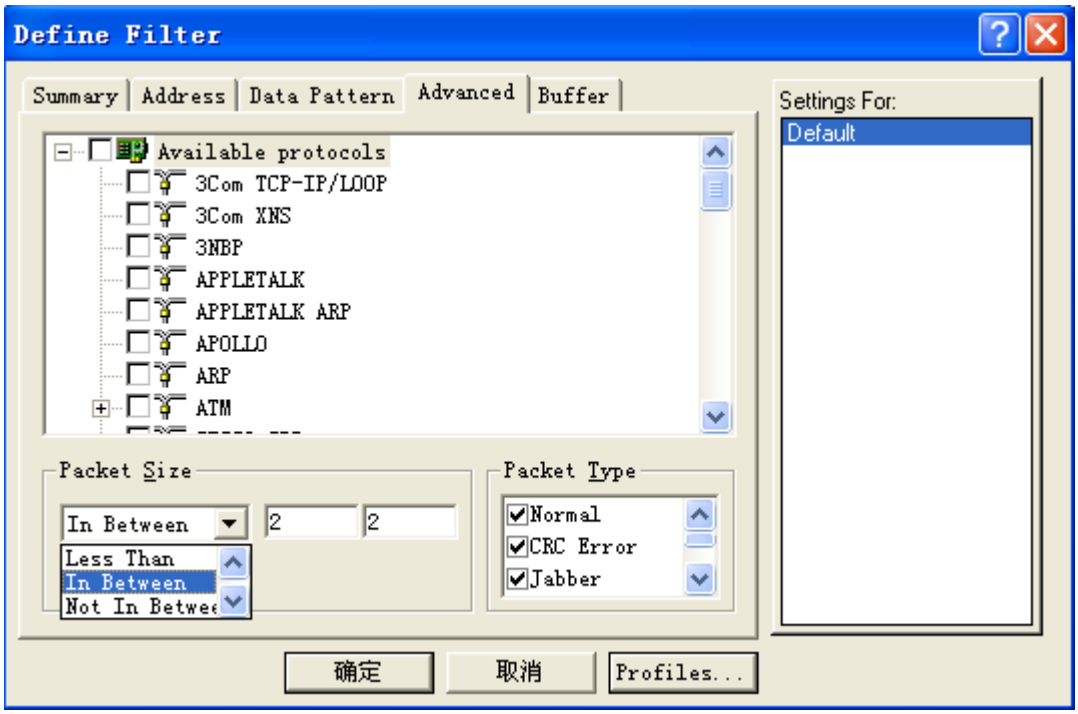

图 11

在协议选择树 Available protocols 中，用户可以选择自己需要的捕获条件，如果是么都不选，则表示忽略该条件，捕获所有的协议。

在捕获帧长度条件 Packer Size 下，用户可以捕获小于、等于、大于某个值的报文，也可以捕获介于两个值之间或不介于两个值之间的报文。

在帧类型栏 Packet Type 中，用户自然就可以选择希望捕获的帧的类型。比如，用户可以选择当网络上有相关错误时是否捕获。

在保存过滤规则条件按钮 Profiles……中，用户可以将当前设置的过滤规则进行保存。当然，用户可以设置多条过滤规则。这样一来，在捕获主面板中，用户可以单击按钮 

来选择所需要应用的捕获条件。（如图 12、13）

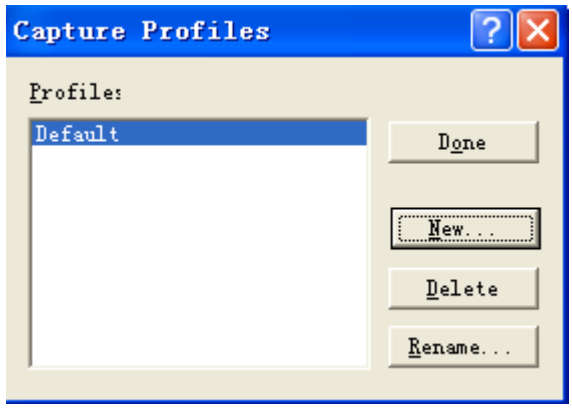

图 12

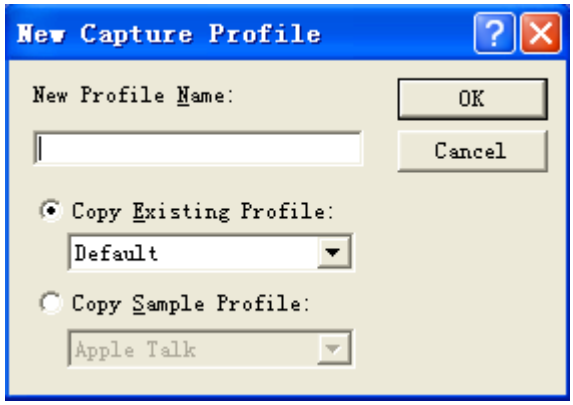

图 13

任意捕获条件

在 Data Pattern 下，用户可以编辑任意捕获条件（如图 14）。用这种方法就可以实现复杂的报文过滤，但很多时候会得不偿失，因为有时截获的报文本就不多，还不如自己看来得快。

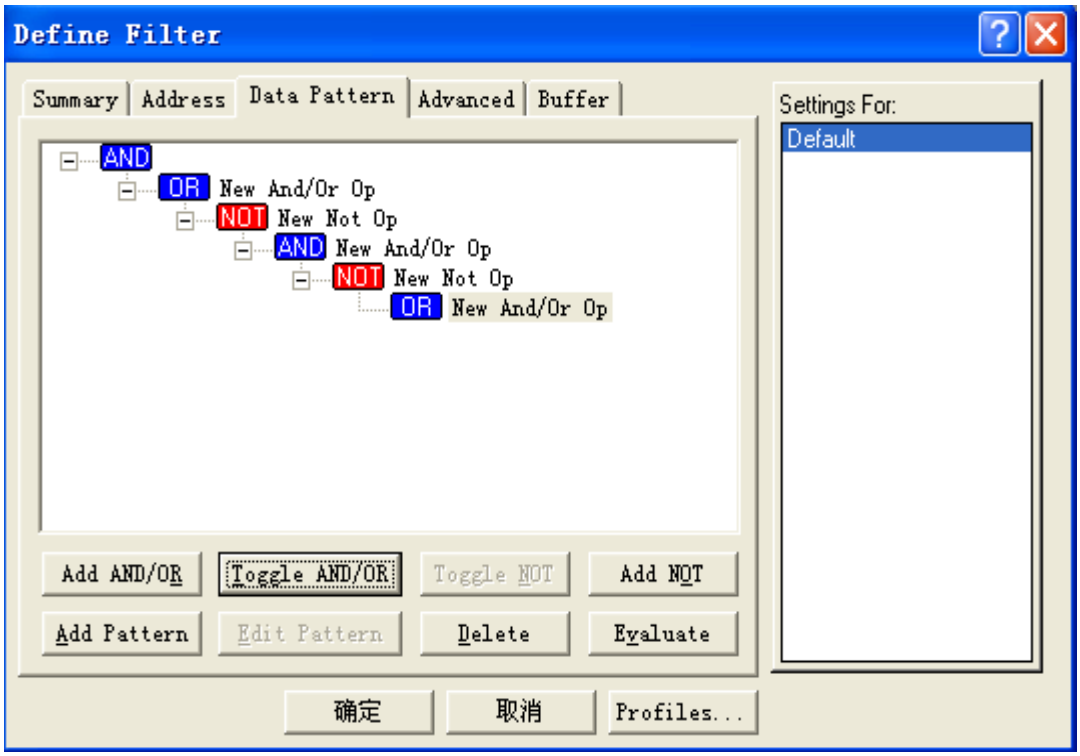

图 14

- 报文放送

a) 编辑报文放送

Sniffer 软件的报文放送功能相对而言比较弱，它的发送主面板如图 15 所示，用菜单命令 Tools/Packet Generator 即可打开。但是在发送之前，用户需要先编辑报文发送的内容，可以单击按钮  ，然后在图 16 所示界面下作相关选择后单击确定。

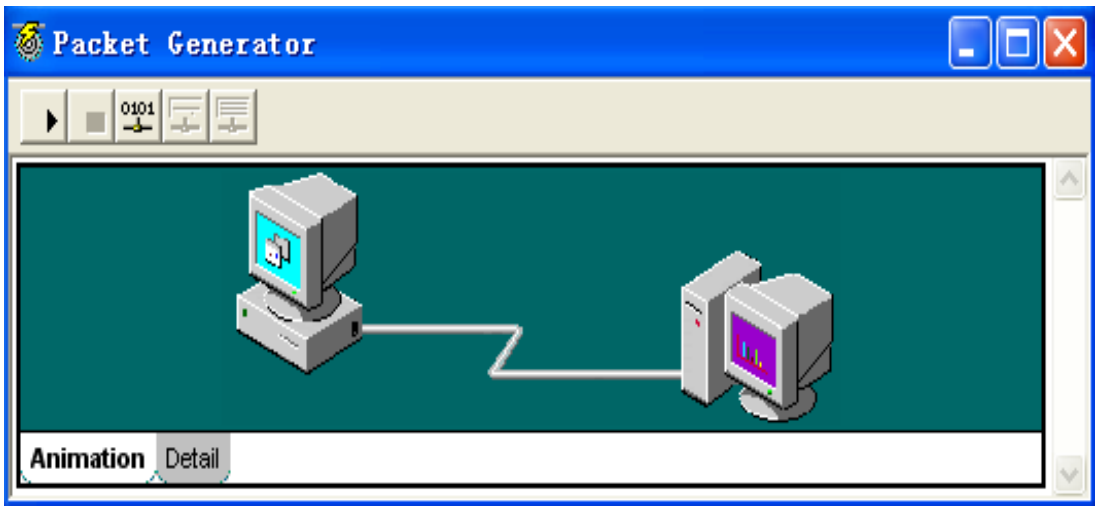

图 15

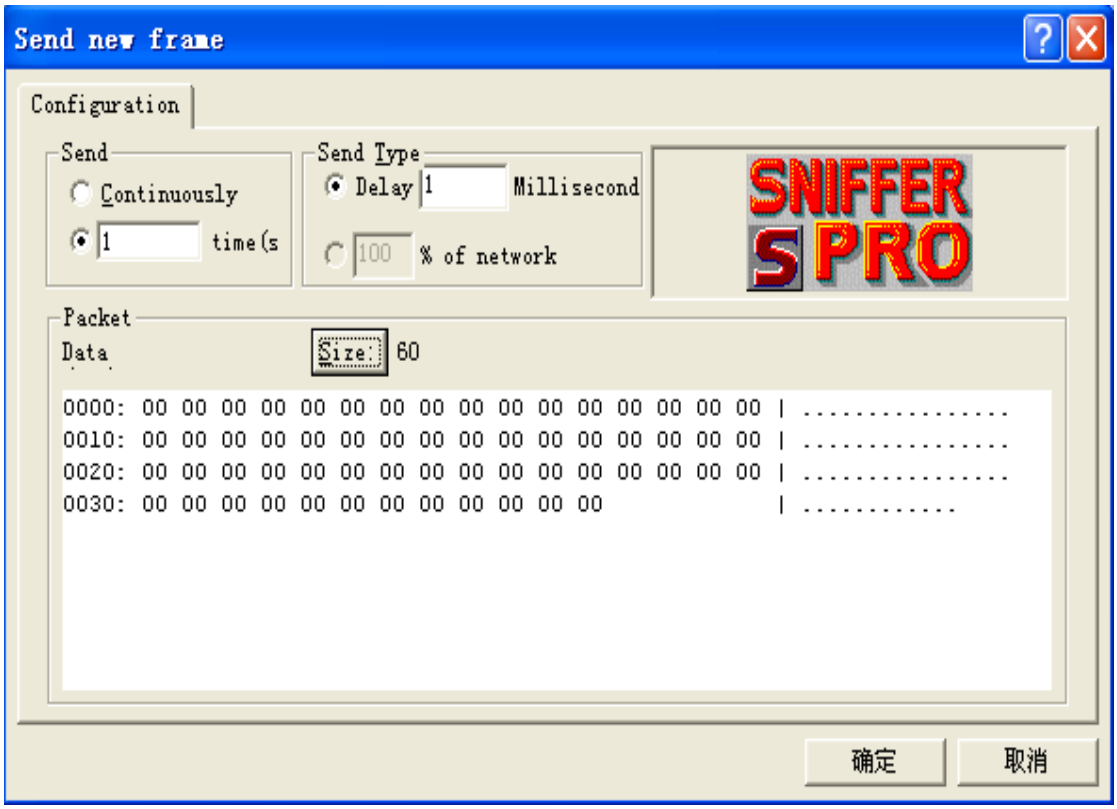

图 16

回到图 15 所示界面，此时，用户可首先查看 Detail 所显示的将要发送的信息，然后选择 Animation 界面，单击发送按钮 ▶ 就可以形象地看到捕获的报文被发送到指定地点。

b) 捕获报文的直接编辑发送

当然也可以将捕获到的报文直接转换成发送包文，然后做一些修改也是可以的。操作如图 17 所示。

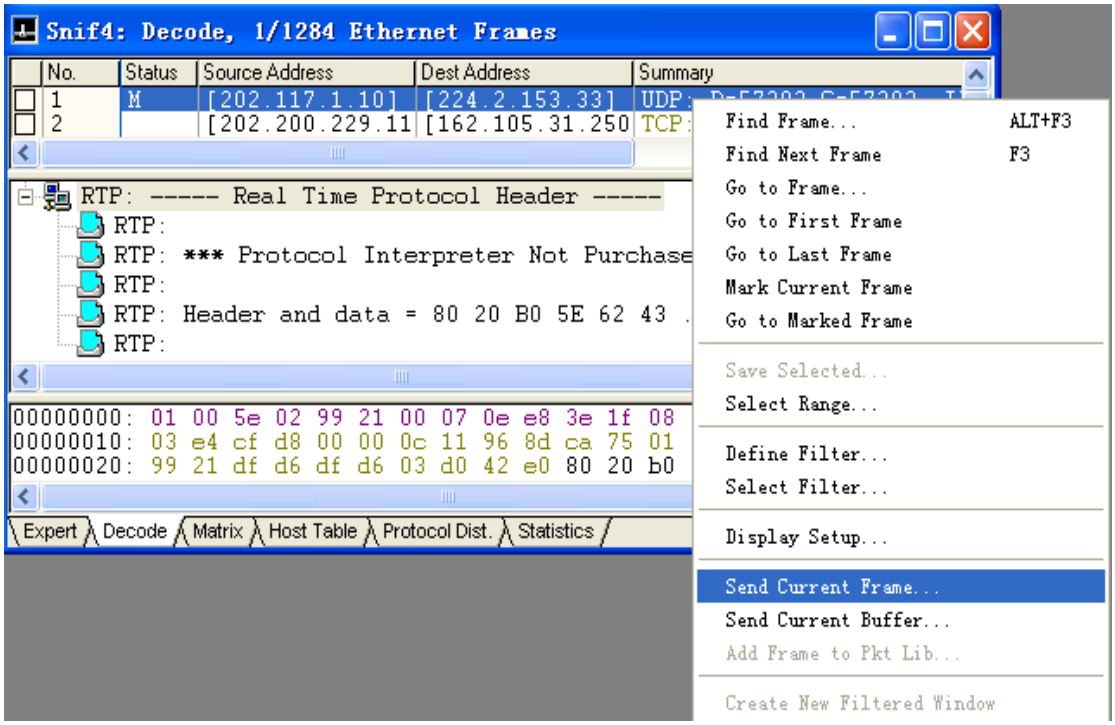

图 17

可以选中某个捕获的报文，用鼠标右键激活菜单，选择 Send Current Packet，这是，该报文的内容已经被原封不动地送到“发送编辑窗口”了。这是在做一些修改就比全部填充报文省事多了。

3、网络监视功能

网络监视功能能够时刻监视网络统计、网络上资源利用率以及网络流量的异常情况，并且能够以多种直观的方式显示。

除了我们在报文捕获中已经介绍过的 Capture Panel 之外，这部分内容还有 Dashbord、Host Table、Matrix、Application Response Time、History、Protocol Distribution、Global Statistics、Alarm Log以及 Address Book，按照其功能作用的重要性，我们在这里首先以 Dashbord和 ART 为主要分析对象做详细阐述，然后对其他功能一一作介绍。

- Dashbord

Dashbord 可以监控网络的利用率、流量以及错误报文等多种内容。单击 Dashbord  按钮（Monitor/Dashbord）即可打开 Dashbord 面板运行操作（如图 18）。

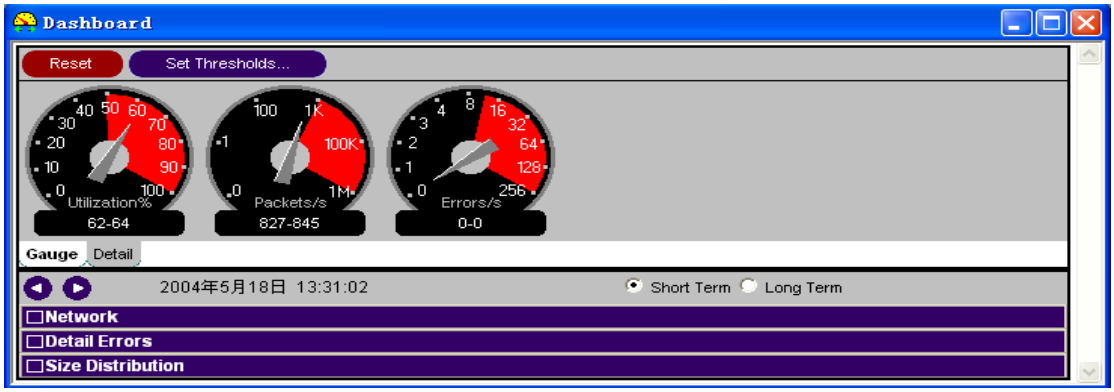

图 18

通常我们可以首先单击 Reset  按钮来开始一次新的网络监控，但是在此之前往往需要用户首先做一些相关参数的设定，这时可以单击 Set Thresholds…  按钮，于是便可以在如图 19 所示对话框中做符合用户需要的参数设置。除了一些常用的测量与控制（MAC）参数（如 Packets）之外，用户还可以在 Monitor sampling 中选择监听采样时间。当选择完相关参数之后，单击“确定”即可完成参数的保存。

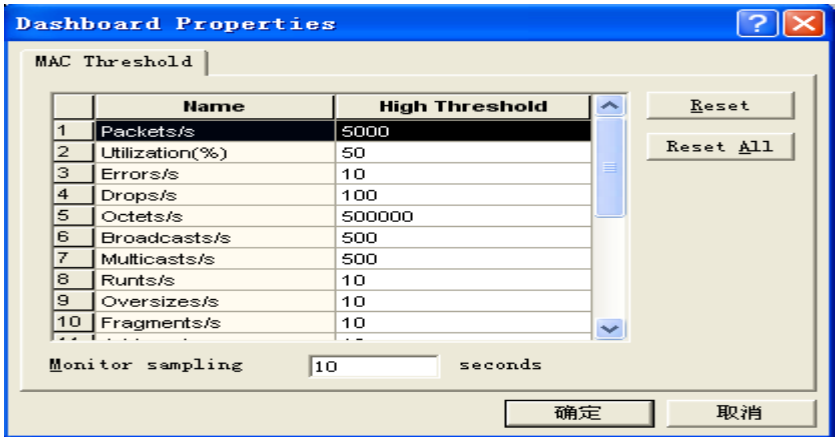

图 19

在开始网络监控之后，我们就可以进行相关参数的分析。**Gauge** 按钮为用户提供了形象直观但相对粗略的参数分析方法（如图 20），而 Detail 按钮适用于对参数的深入分析（如图 21）。

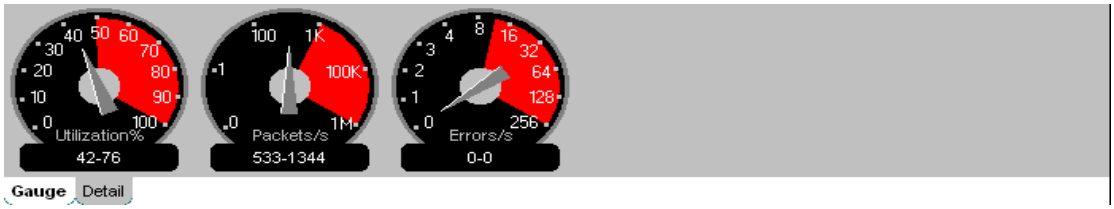

图 20

Network		Size Distribution		Detail Errors	
Packets	1,593,025	64s	121,879	CRCs	0
Drops	0	65-127s	153,617	Runts	0
Broadcasts	40,910	128-255s	32,777	Oversizes	0
Multicasts	1,128,200	256-511s	44,147	Fragments	0
Bytes	1,479,187,369	512-1023s	441,315	Jabbers	0
Utilization	41	1024-1518s	799,290	Alignments	0
Errors	0			Collisions	0

Gauge **Detail**

图 21

无论哪种分析方式，Dashbord 都提供了短时间 Short Term 和长期 Long Term 两种分析选择。而且用户可以通过分别选择 Network、Detail Errors 或 Size Distribution，从而对自己最关心的问题作最细致地分析（如图 22、23、24），并且当用户将鼠标移动到相关选项上时，如 Network 中的 Error 选项，分析图中的对应曲线会突出显示。

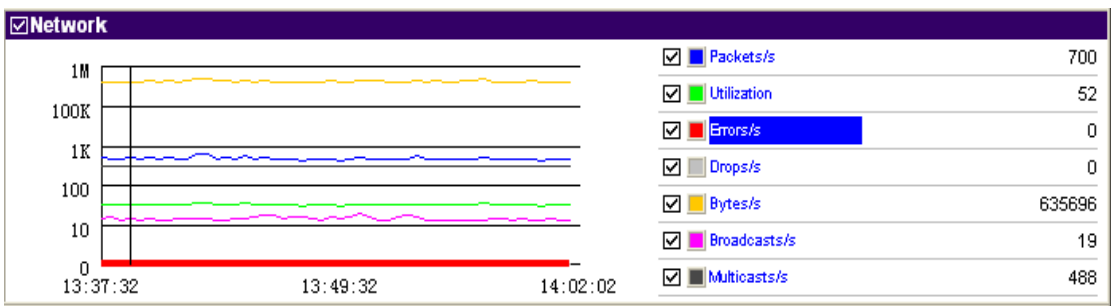

图 22

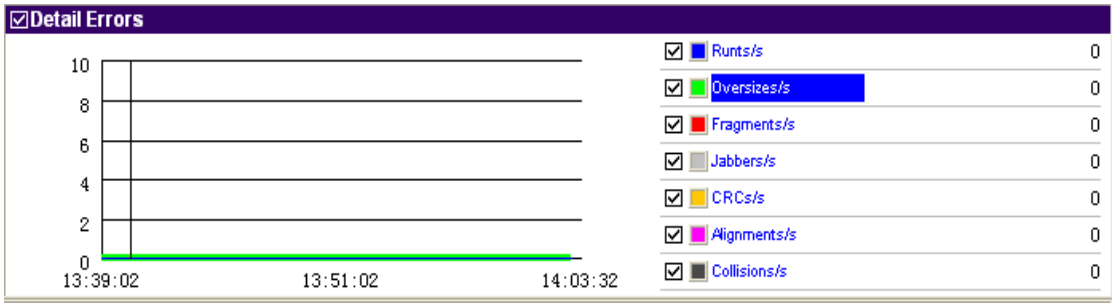

图 23

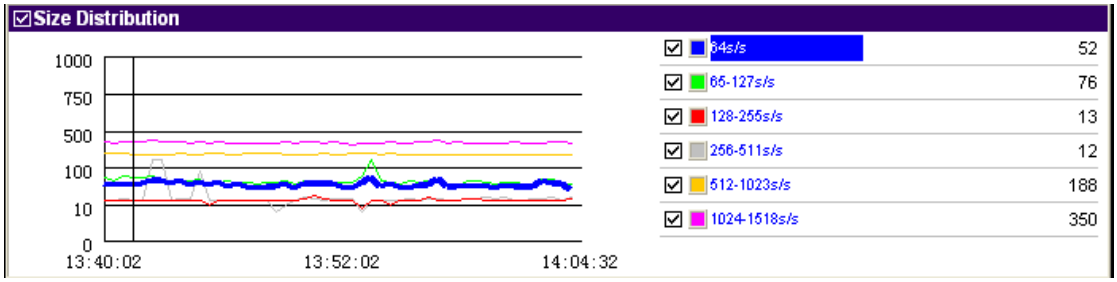

图 24

- Application Response Time(ART)

Application Response Time(ART)可以监视 TCP/UDP 应用层程序在客户端和服务器的响应时间，如 HTTP，FTP，DNS 等的应用。单击 Application Response Time 按钮（Monitor/Application Response Time）即可打开 ART 操作界面（如图 25）。

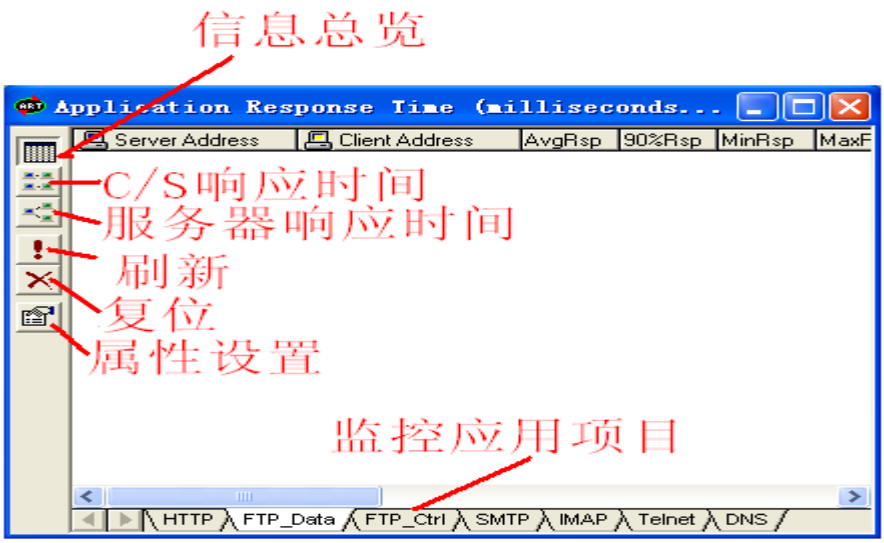

图 25

当然，在正式开始监视 TCP/UDP 应用层程序在客户端和服务器的响应时间之前用户可以根据自己的需要首先做一些相关的配置，如图 25 所示，单击 properties  便可进入属性

设置对话框（如图 26）。在这里，用户可以在 General 页面下首先选择数据更新的时间间隔。然后用户可以打开 Display Protocols 页面，在对应于 Name 栏的 Shoe ART 栏选择需要应用的协议（如图 27）。最后用户可以打开 Server-Client 和 Server Only 页面选择具体需要监视的参数(如图 28、29)。在做完全部属性设置后，单击“确定”按钮，此时系统会提示监视功能将按照新的参数设置重新启动（如图 30）。此后，每次执行复位操作  时便给系统设定义选的属性参数。

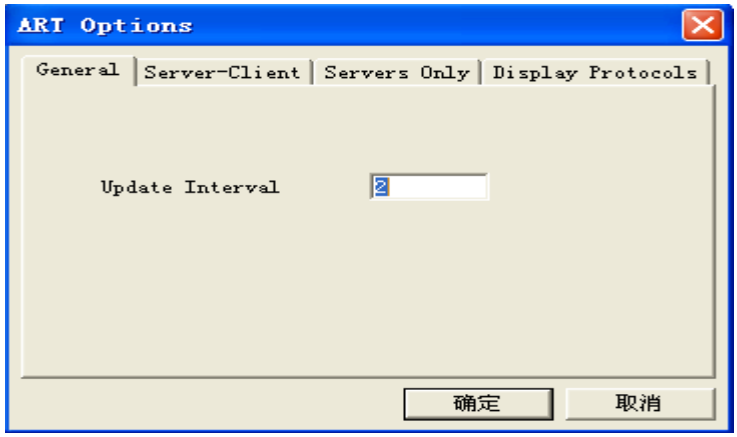

图 26

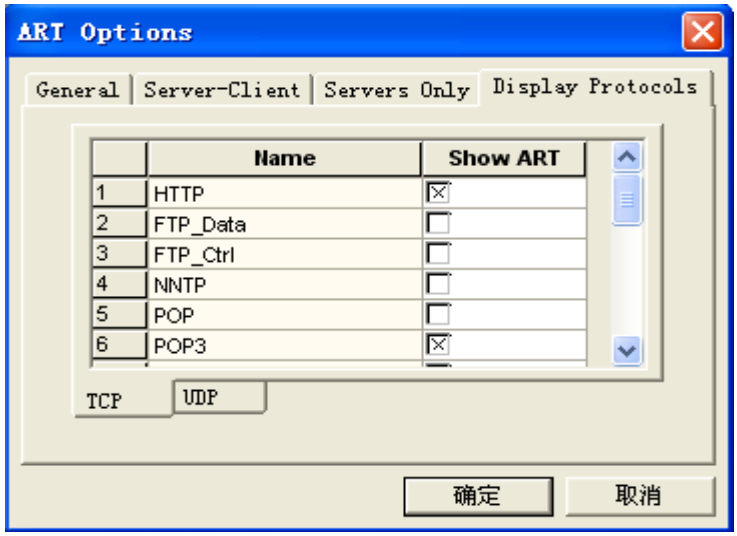
ART Options
General
Server-Client
Servers Only
Display Protocols
Name
Show ART
1
HTTP
2
FTP_Data
3
FTP_Ctrl
4
NNTP
5
POP
6
POP3
TCP
UDP
确定
取消

图 27

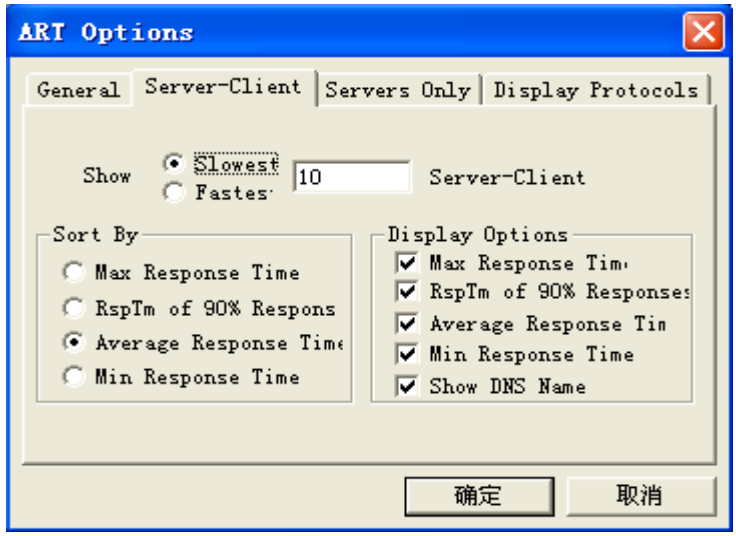
ART Options
General
Server-Client
Servers Only
Display Protocols
Show
Slowest
Fastes
10
Server-Client
Sort By
Max Response Time
RspTm of 90% Respons
Average Response Time
Min Response Time
Display Options
Max Response Tim
RspTm of 90% Responses
Average Response Tin
Min Response Time
Show DNS Name
确定
取消

图 28

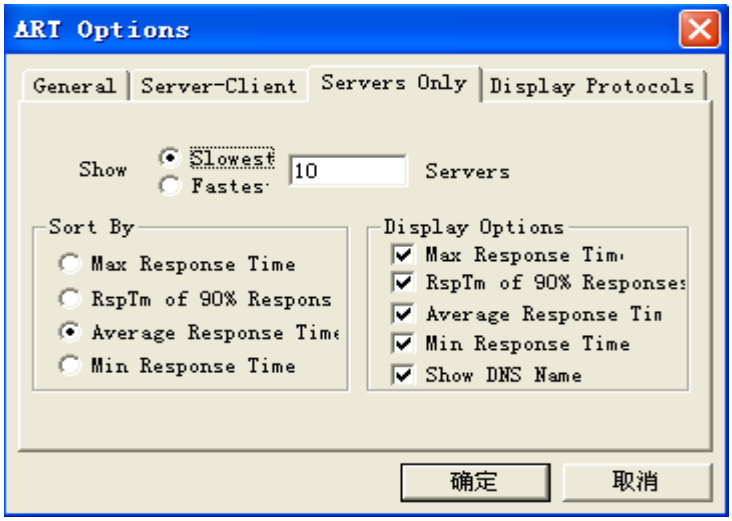

图 29

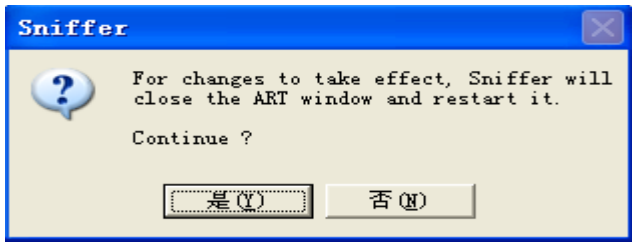

图 30

接下来用户便可以在 Table View、Client-Server Response Time、Server Response Time 几个网络参数观察方式之间切换观察获取需要的信息了，当然也需要使用刷新功能来帮助获取最新最有效的信息（如图 31、32、33）。

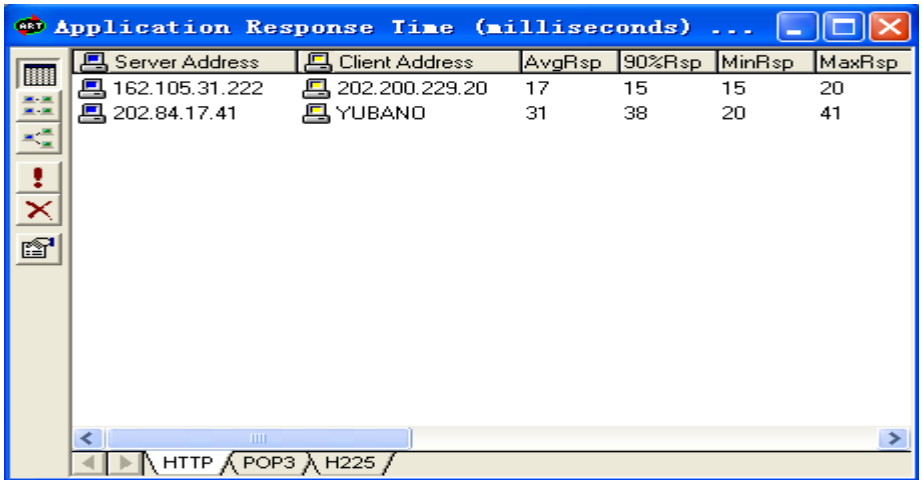

图 31

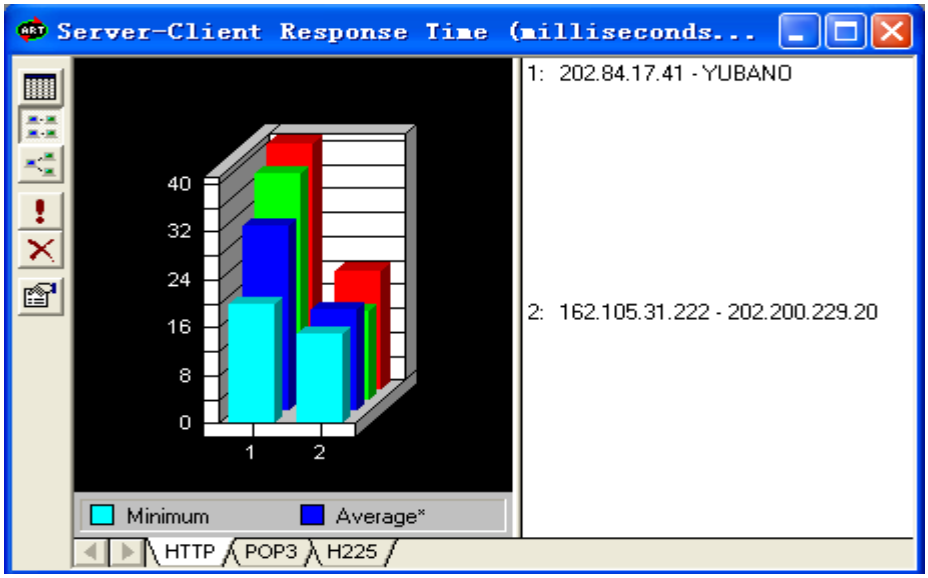

图 32

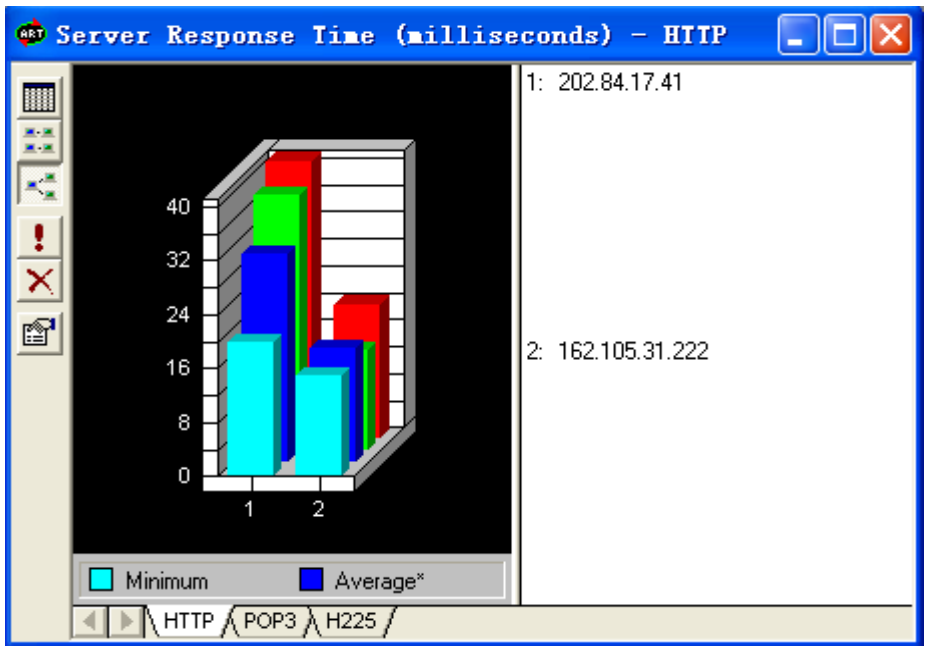

图 33

- Host Table

Host Table  提供了被监视到的所有主机正在与网络的通信情况，在其操作界面下，单击 Outline  按钮便可获知各主机的 IP 地址、出入信包和信包大小等信息（如图 34）。

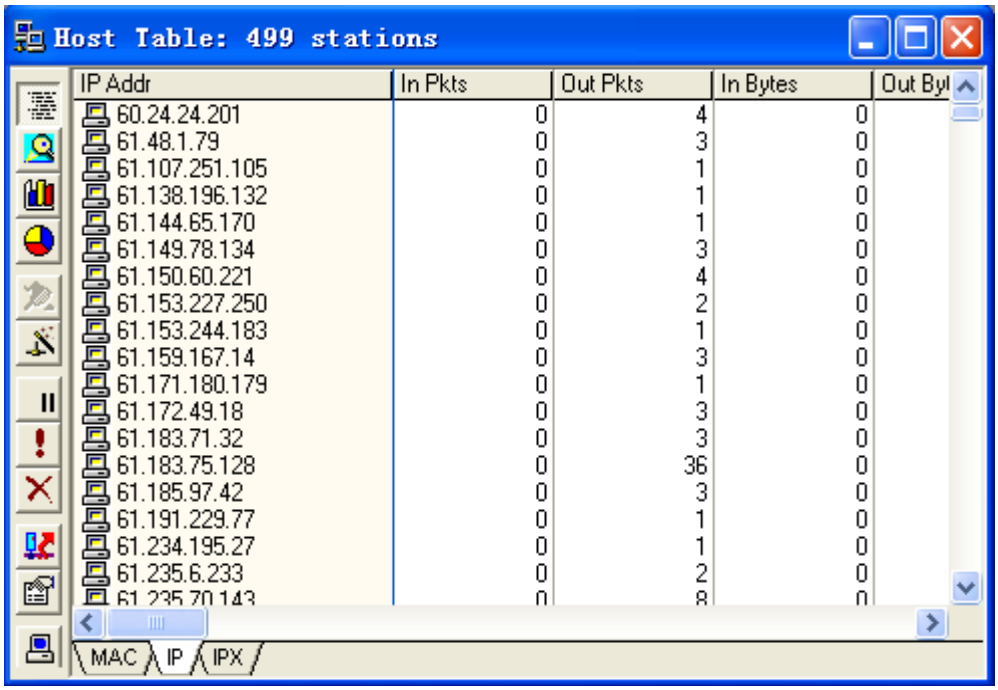

图 34

单击 Detail  按钮，可以进一步获知各主机正在使用的网络应用层协议（如图 35）

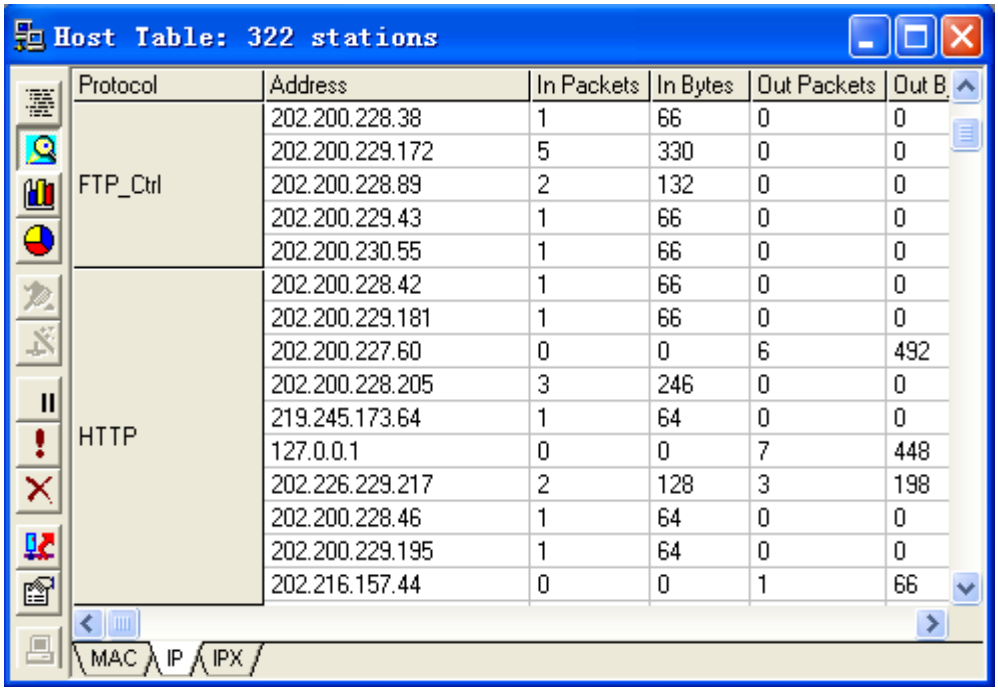

图 35

如果用户对当前信息流量前十名的主机 IP 地址有兴趣，单击 Bar 或 Pie 按钮即可获得相关信息（如图 36、37）。

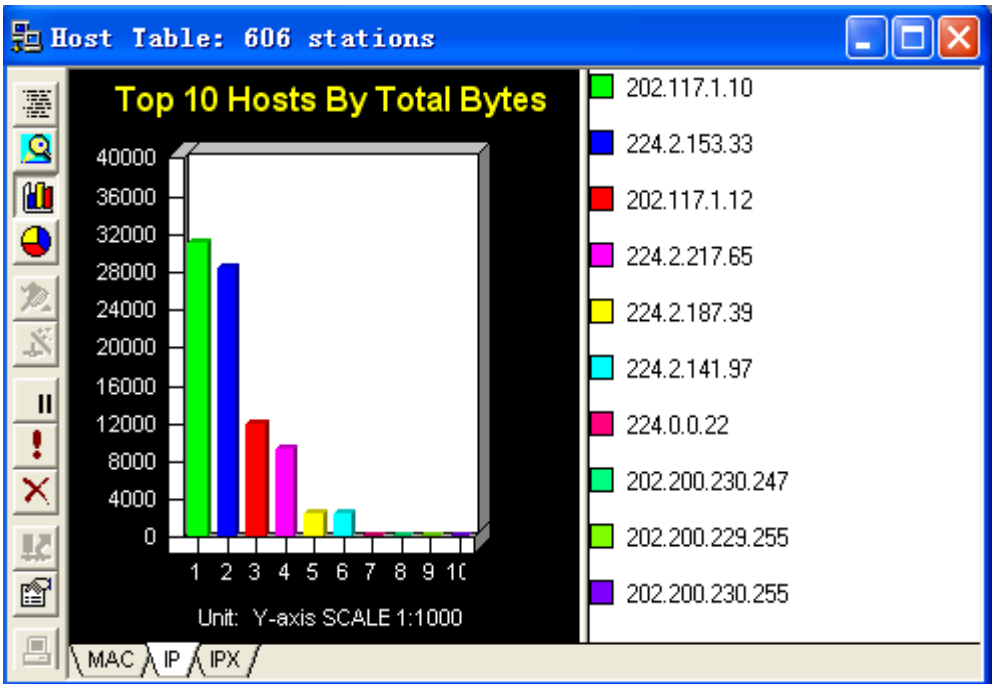

图 36

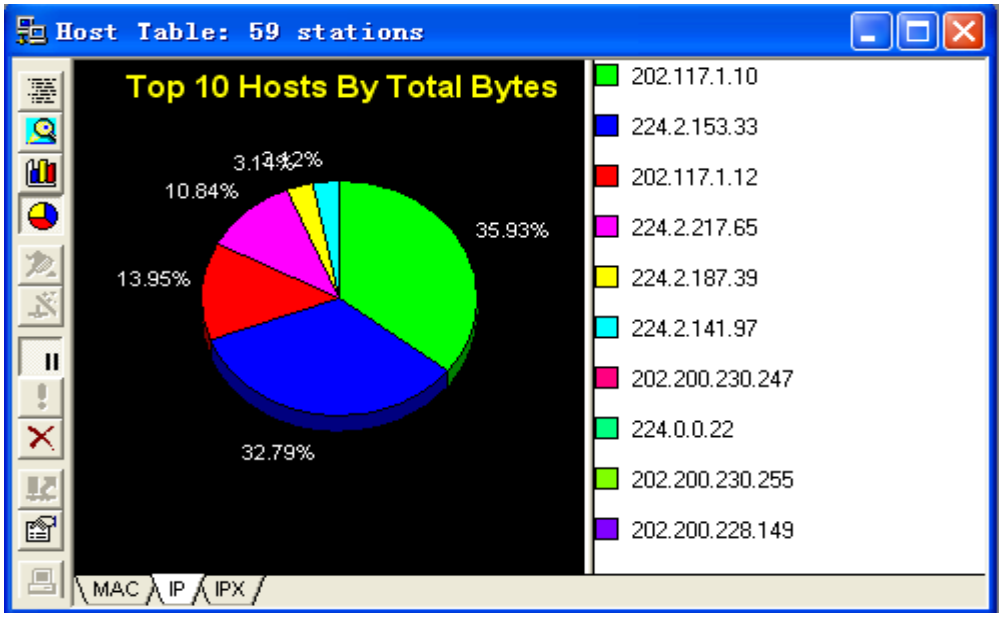

图 37

正如我们在 Dashbord 和 ART 中介绍过的那样，用户所需要的信息可以由用户自己

设定，在这里和以下的介绍中我们将不再多说。

- Matrix

如果说 Host Table 提供了单台主机与网络的通信情况，那么 Matrix向用户提供的是被监视到的主机对之间的网络通信情况，而两者的操作界面和功能信息是完全类似的。

Map，如图 38 所示为主机对链接图

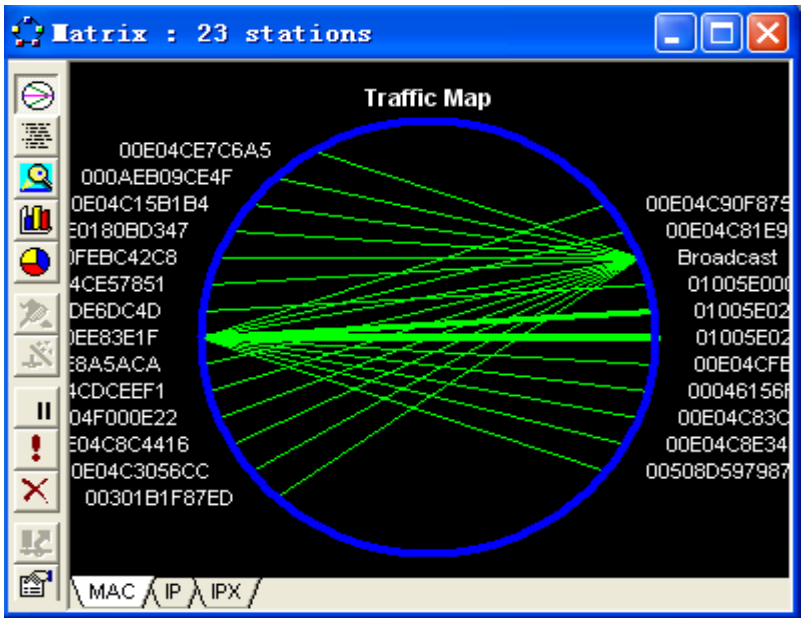

图 38

而图 39、40、41、42 所示信息与我们在 Host Table 中的介绍基本相同（只需将一台主机换成两台主机即可）。

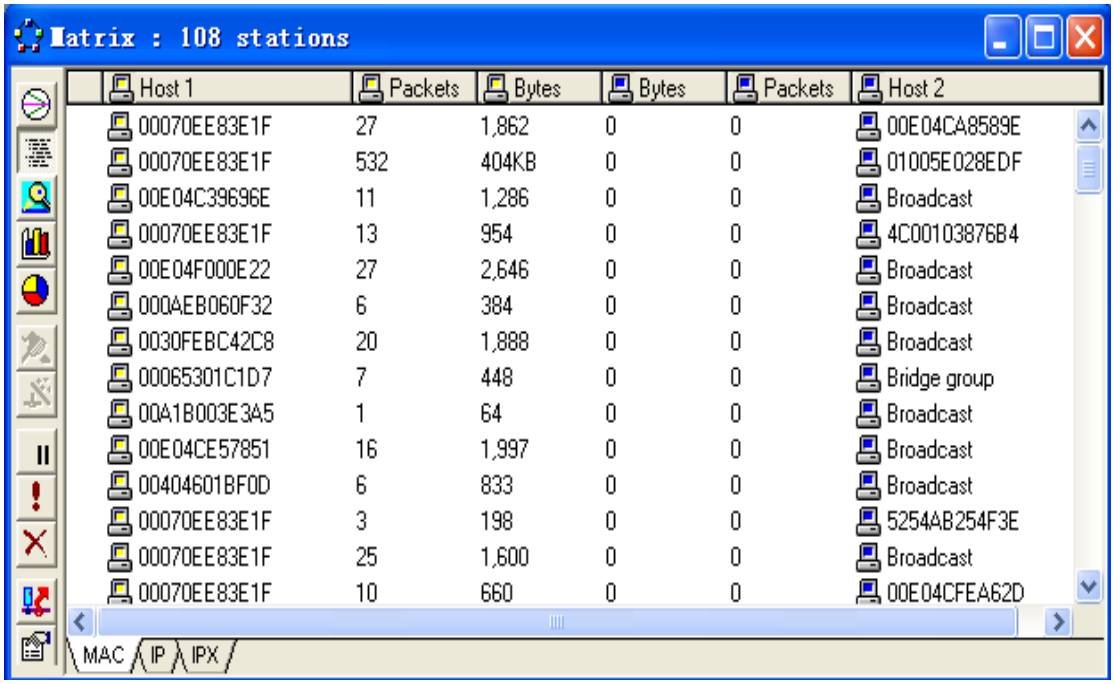
Matrix : 108 stations
Host 1 | Packets | Bytes | Bytes | Packets | Host 2
00070EE83E1F | 27 | 1,862 | 0 | 0 | 00E04CA8589E
00070EE83E1F | 532 | 404KB | 0 | 0 | 01005E028EDF
00E04C39696E | 11 | 1,286 | 0 | 0 | Broadcast
00070EE83E1F | 13 | 954 | 0 | 0 | 4C00103876B4
00E04F000E22 | 27 | 2,646 | 0 | 0 | Broadcast
000AEB060F32 | 6 | 384 | 0 | 0 | Broadcast
0030FEBC42C8 | 20 | 1,888 | 0 | 0 | Broadcast
00065301C1D7 | 7 | 448 | 0 | 0 | Bridge group
00A1B003E3A5 | 1 | 64 | 0 | 0 | Broadcast
00E04CE57851 | 16 | 1,997 | 0 | 0 | Broadcast
00404601BF0D | 6 | 833 | 0 | 0 | Broadcast
00070EE83E1F | 3 | 198 | 0 | 0 | 5254AB254F3E
00070EE83E1F | 25 | 1,600 | 0 | 0 | Broadcast
00070EE83E1F | 10 | 660 | 0 | 0 | 00E04CFEA62D
MAC IP IPX

图 39

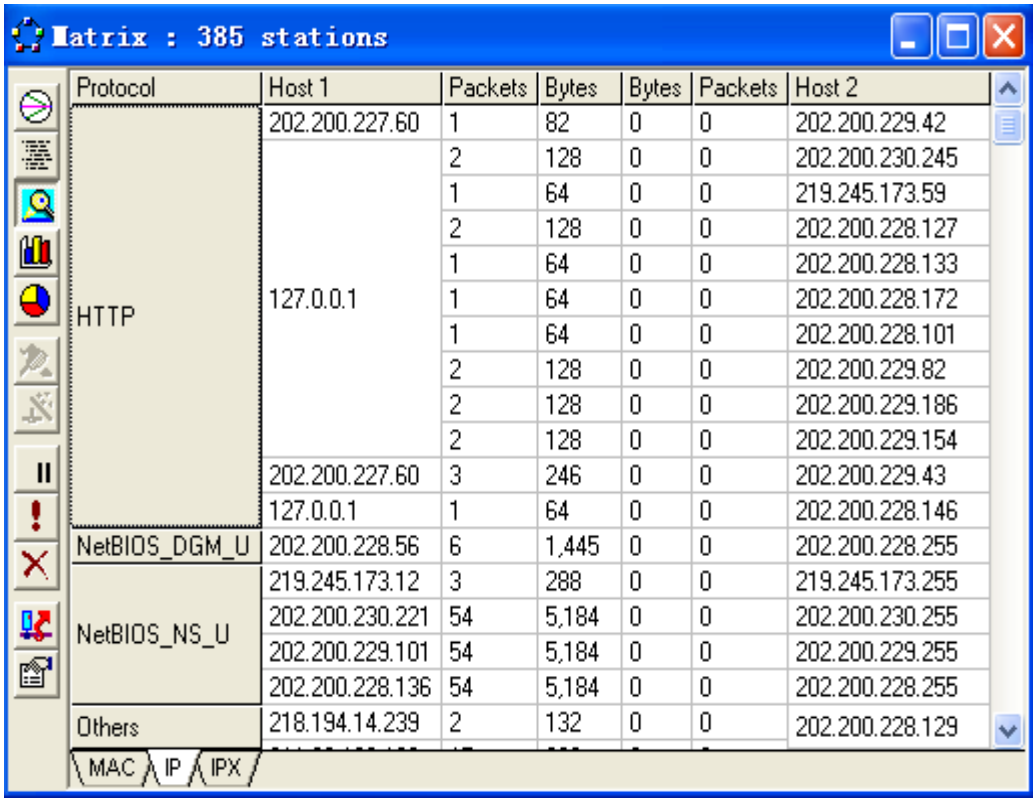
Matrix : 385 stations
Protocol | Host 1 | Packets | Bytes | Bytes | Packets | Host 2
HTTP | 202.200.227.60 | 1 | 82 | 0 | 0 | 202.200.229.42
HTTP | 127.0.0.1 | 2 | 128 | 0 | 0 | 202.200.230.245
HTTP | 127.0.0.1 | 1 | 64 | 0 | 0 | 219.245.173.59
HTTP | 127.0.0.1 | 2 | 128 | 0 | 0 | 202.200.228.127
HTTP | 127.0.0.1 | 1 | 64 | 0 | 0 | 202.200.228.133
HTTP | 127.0.0.1 | 1 | 64 | 0 | 0 | 202.200.228.172
HTTP | 127.0.0.1 | 1 | 64 | 0 | 0 | 202.200.228.101
HTTP | 127.0.0.1 | 2 | 128 | 0 | 0 | 202.200.229.82
HTTP | 127.0.0.1 | 2 | 128 | 0 | 0 | 202.200.229.186
HTTP | 127.0.0.1 | 2 | 128 | 0 | 0 | 202.200.229.154
HTTP | 202.200.227.60 | 3 | 246 | 0 | 0 | 202.200.229.43
HTTP | 127.0.0.1 | 1 | 64 | 0 | 0 | 202.200.228.146
NetBIOS_DGM_U | 202.200.228.56 | 6 | 1,445 | 0 | 0 | 202.200.228.255
NetBIOS_NS_U | 219.245.173.12 | 3 | 288 | 0 | 0 | 219.245.173.255
NetBIOS_NS_U | 202.200.230.221 | 54 | 5,184 | 0 | 0 | 202.200.230.255
NetBIOS_NS_U | 202.200.229.101 | 54 | 5,184 | 0 | 0 | 202.200.229.255
NetBIOS_NS_U | 202.200.228.136 | 54 | 5,184 | 0 | 0 | 202.200.228.255
Others | 218.194.14.239 | 2 | 132 | 0 | 0 | 202.200.228.129
MAC IP IPX

图 40

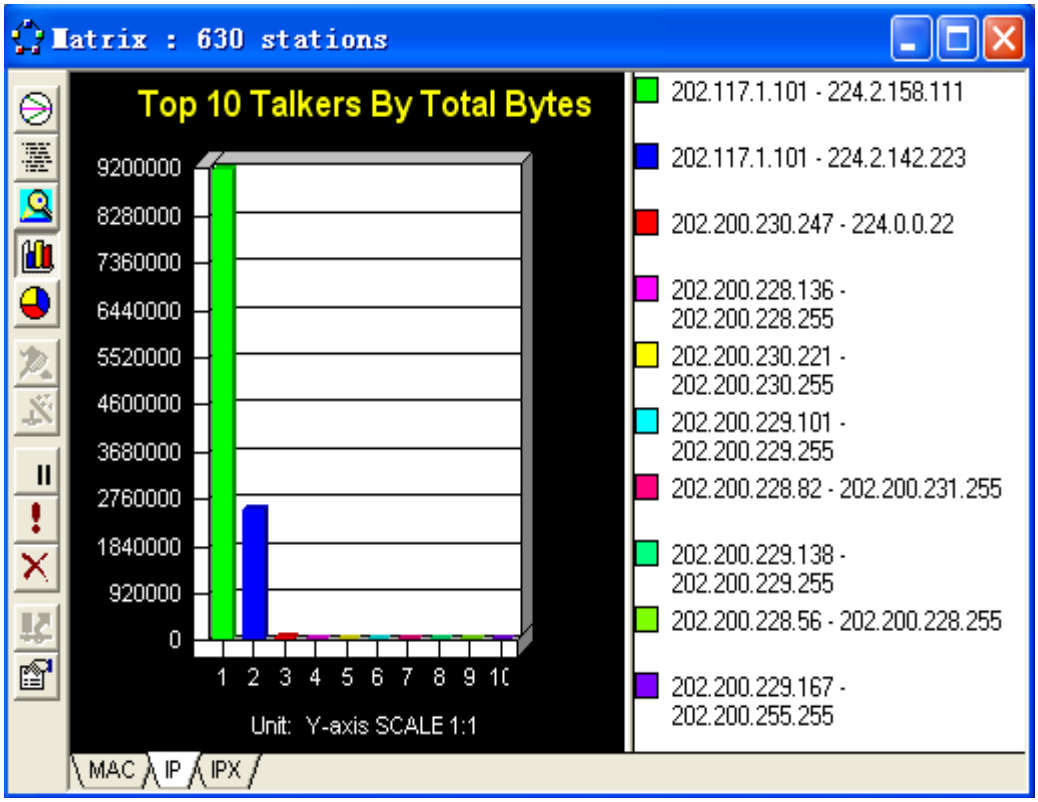
Matrix : 630 stations
Top 10 Talkers By Total Bytes
9200000
8280000
7360000
6440000
5520000
4600000
3680000
2760000
1840000
920000
0
1 2 3 4 5 6 7 8 9 10
Unit: Y-axis SCALE 1:1
MAC
IP
IPX
202.117.1.101 - 224.2.158.111
202.117.1.101 - 224.2.142.223
202.200.230.247 - 224.0.0.22
202.200.228.136 - 202.200.228.255
202.200.230.221 - 202.200.230.255
202.200.229.101 - 202.200.229.255
202.200.228.82 - 202.200.231.255
202.200.229.138 - 202.200.229.255
202.200.228.56 - 202.200.228.255
202.200.229.167 - 202.200.255.255

图 41

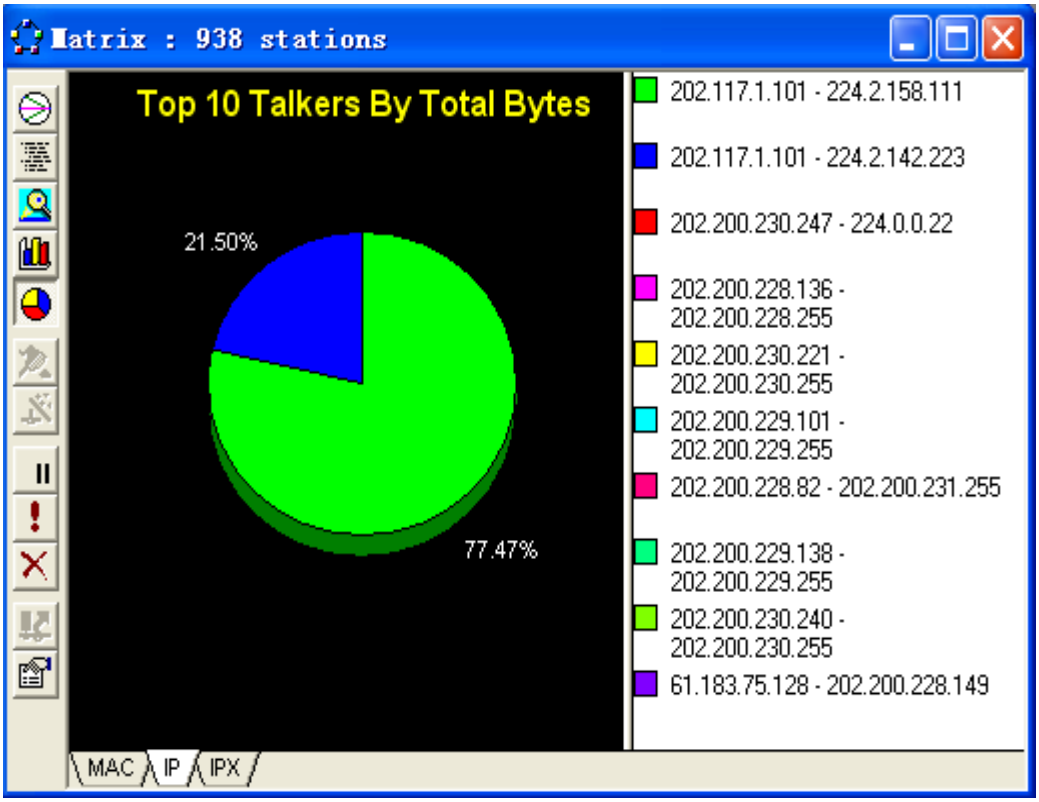

图 42

- History

History 为管理网络监视的历史信息提供了极大的方便，用户可以通过添加和删除历史数据来对网络信息做纵向比较分析。也可以调出某个特定的网络对象对其作跟踪分析。（如图 43）

图 43

- Protocol Distribution

Protocol Distribution  提供了观察网络协议使用情况的手段，用户可以通过 Protocol Distribution 来了解各种协议在网络中的应用情况（如图 44、45）。

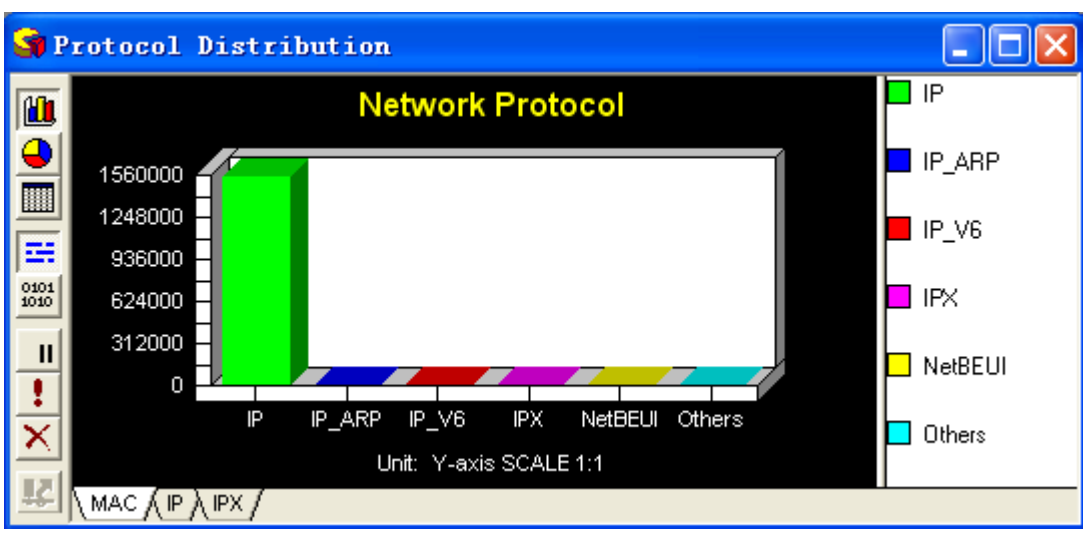

图 44

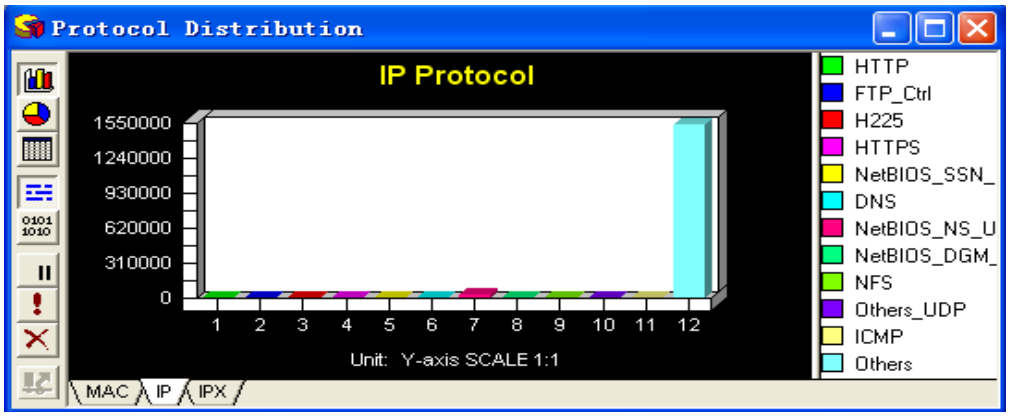

图 45

- Global Statistics

通过 Global Statistics，用户可以对网络上传输的数据包尺寸统计分布规律和相应的利用率有所了解（如图 46、47）。

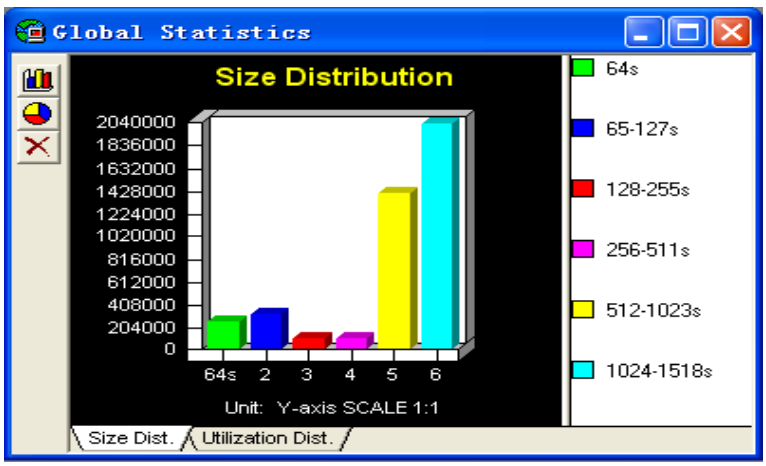

图 46

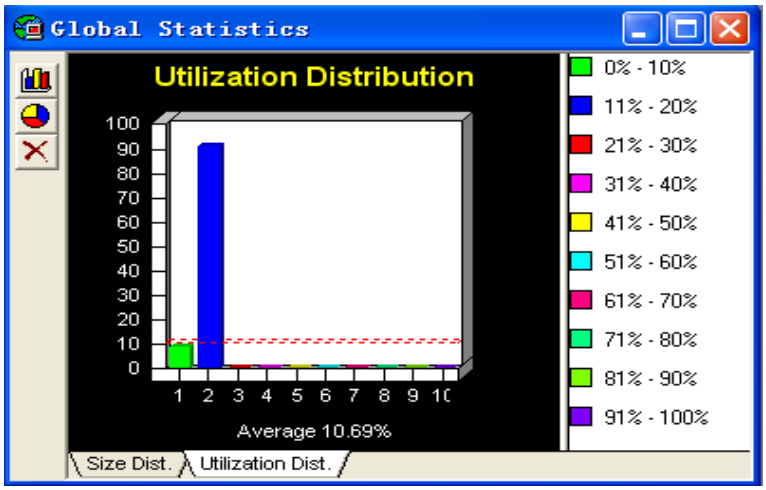

图 47

- Alarm Log

在 Alarm Log中，用户可以了解到本主机接收到的一些异常数据包，并且可以对这些异常数据包作出选择性的操作，只需在选中要操作的异常数据包后单击右键，便可进行 Acknowledge 应答，Remove 删除等操作（如图 48）。

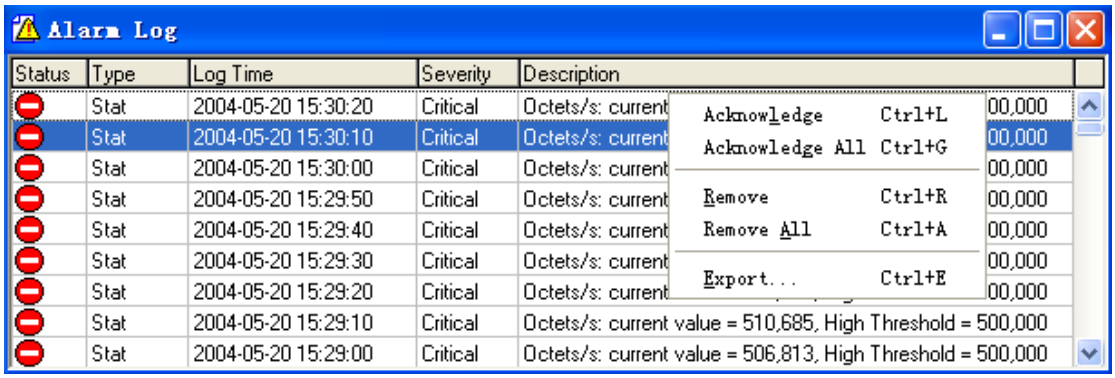

图 48

- Address Book

Address Book使用户的网络监视更具目的性，通过 New Address和 Autodiscovery两种操作，用户便可以对“满足自己设定的网络条件的主机”展开监视和跟踪（如图 49）。

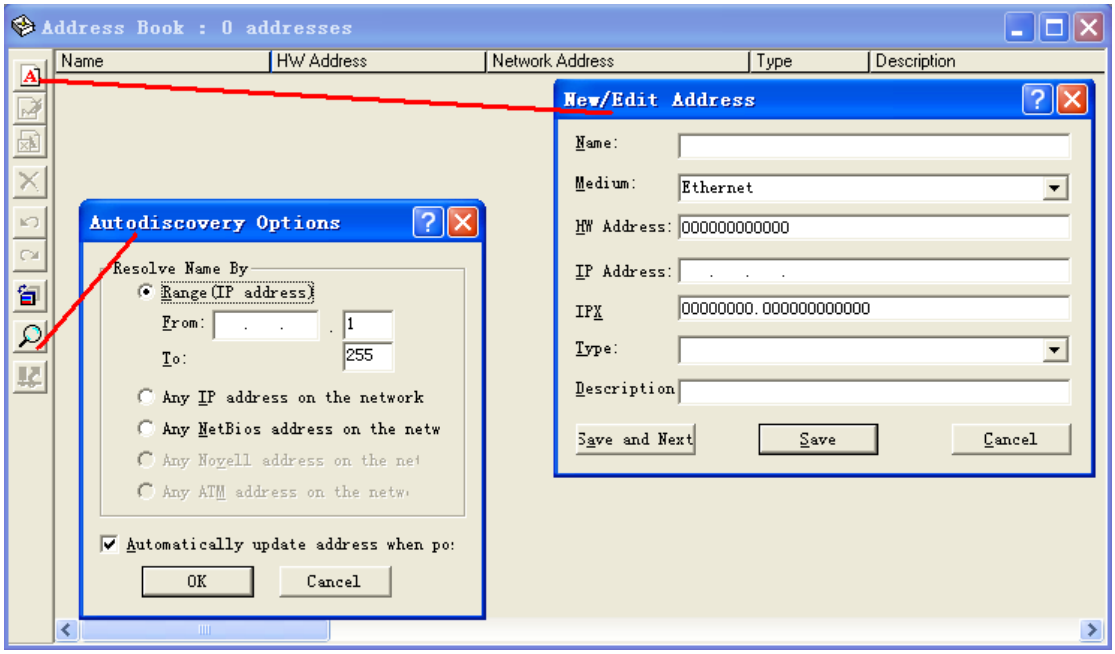

图 49

4、数据报文解码简析

（1）、数据报文分层

如下表所示为网络结构中的四层协议，不同层次完成不同的功能，每一层都有众多协议组成。

应用层----------Telnet、Ftp 和 Email 等
传输层----------TCP 和 UDP
网络层----------IP,ICMP 和 IGMP
链路层----------设备驱动程序和接口卡

于是，图 50 为 sniffer 解码表中分别对每一个层次协议的解码分析，DLC 对应链路层，IP 对应网络层，UDP 对应传输层，RTP 对应应用层高层协议。Sniffer 可以针对众多协议进行详细结构化解码分析，利用树型结构显示。

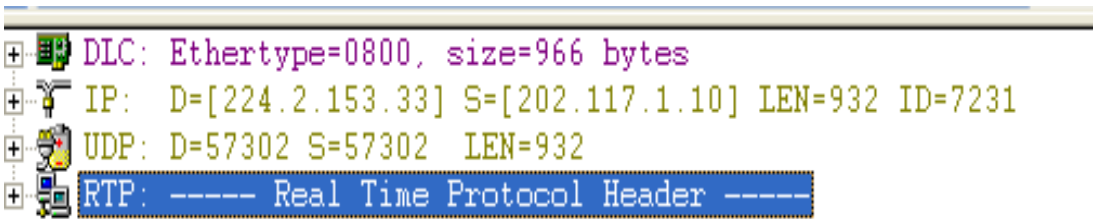

图 50

（2）、以太报文结构

如下表所示为 Ethernet 帧结构

DMAC	SMAC	TYPE	DATA/PAD	FCS

这种类型报文结构为：目的 MAC 地址（ 6 bytes）+源 MAC 地址（ 6 bytes）＋上层协议类型（2bytes）+数据字段（46-1500bytes）+校验（4bytes）

于是，如图 51 所示，解码表中分别显示各字段内容，若要查看 MAC 详细内容，鼠标点击上面解码框中地址，在下面的表格中回以黑色突出显示对应的 1 6 进制编码。

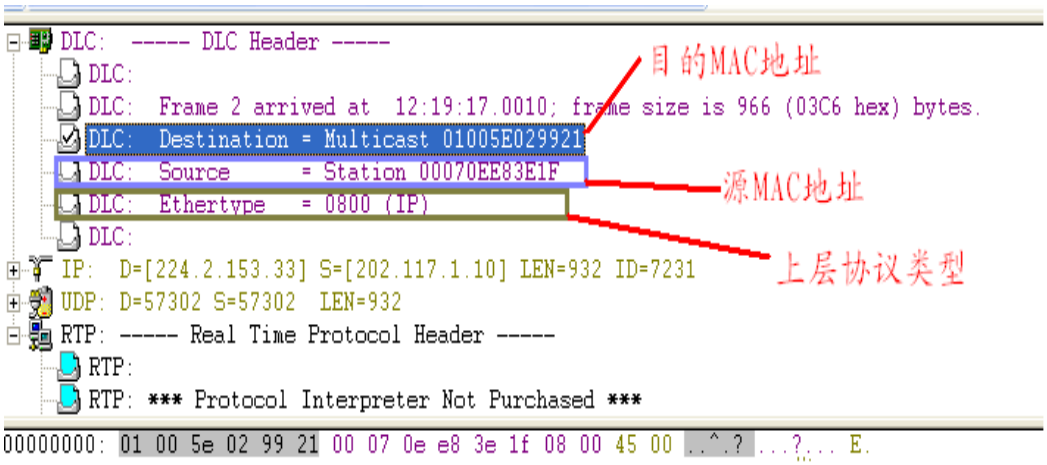

图 51

（3）、IP 协议

IP 报文结构为：IP 协议头+载荷，其中对 IP 协议头的分析是分析报文结构的主要内容之一，IP 协议头的一种结构如下：

- 版本： 4 －－－IPv4

- 首部长度：单位是 4 字节，最大 6 0 字节
- TOS: IP 优先级字段
- 总长度：单位为字节，最大长度 6 5 5 3 5 字节
- 标识： IP 报文标识字段
- 标志：占 3 比特，只用到低位的 2 比特
- MF(More Fragment)
- MF=1，后面还有分片的数据包
- MF=0,分片数据包的最后一个
- DF(Don’t Fragment)
- DF=1,不允许分片
- DF=0,允许分片
- 段偏移：分片后的分组在原分组中的相对位置，总共 1 3 比特，单位为 8 字节
- 寿命：TTL(Time to Live) 丢弃 TTL=0 的报文
- 协议：携带的是何种协议报文
- 1：ICMP
- 6 ：TCP
- 17：UDP
- 89：OSPF
- 头部检验和：对 IP 协议首部的校验和
- 源 IP 地址：IP 报文的源地址
- 目的 IP 地址：IP 报文的目的地址

于是我们理解图 52 既是 Sniffer 对 IP 协议首部解码分析的结构，和 IP 首部各个字段相对应，并给出了各个字段之所表示含义的英文解释。

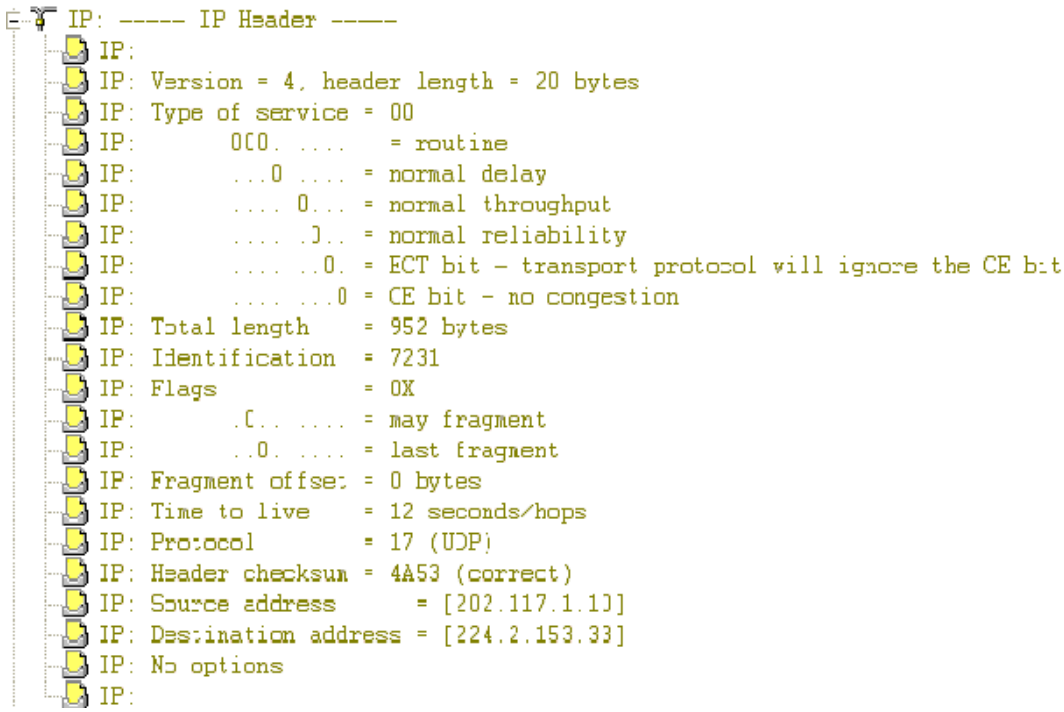

图 52

（4）、ARP 协议

如下表所示为 ARP 的报文结构

硬件类型		协议类型
硬件长度	协议长度	操作请求 1，回答 2
发送站硬件地址（例如，以太网是 6 字节）		
发送站协议地址（例如，对 ip 是 4 字节）		
目标硬件地址　（例如，对以太网是 6 字节）		
目标协议地址　（例如，对 IP 是 4 字节）		

ARP 分组具有以下一些字段：

- HYTPE(硬件类型)。这是一个 16 比特字段，用来定义运行 ARP 的网络的类型。每一个局域网基于其类型被指派给一个整数。例如，以太网是类型 1。ARP 可使用在任何网络上。

- PTYPE(协议类型)。这也是一个 16 比特字段，用来定义协议的类型，例如，对 IPv4 协议，这个字段的值是 0800。ARP 可用于任何高层协议。
- HLEN (硬件长度)。这是一个 8 比特字段，用来定义以字节为单位的物理地址的长度，例如，对以太网这个值是 6。
- PLEN（协议长度）。这是一个 8 比特字段，用来定义以字节为单位的逻辑地址的长度，例如，对 IPv4 这个值是 4。
- OPER（操作）。这是一个 16 比特的字段，用来定义分组的类型。已定义了两种类型：ARP 请求（1），ARP 回答（2）
- SHA（发送硬件地址）。这是一个可变长度的地段，用来定义发送站的物理地址的长度，例如，对以太网这个字段是 6 字节长。
- SPA（发送站协议地址）。这是一个可变长度的地段，用来定义发送站的逻辑（例如，IP）地址的长度，对于 IP 协议，这个字段是 4 字节长。
- THA（目标硬件地址）。这是一个可变长度的字段，用来定义目标的物理地址的长度，例如，对以太网这个字段是 6 字节长，对于 ARP 请求报文，这个字段是全 0，因为发送站不知道目标的物理地址。
- TPA（目标协议地址）。这是一个可变长度字段，用来定义目标的逻辑地址（例如，IP 地址）的长度，对于 IPV4 协议，这个字段是 4 字节长。

于是，通过 Sniffer 解码的 ARP 报文结构便如图 53 所示。

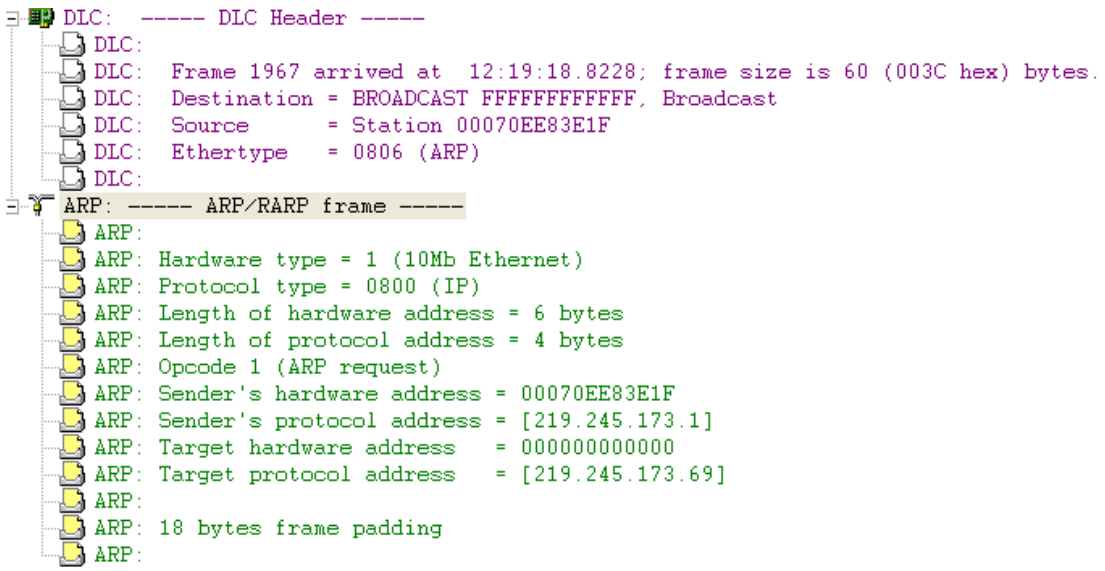
DLC: ----- DLC Header -----
DLC:
DLC: Frame 1967 arrived at 12:19:18.8228; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station 00070EE83E1F
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 1 (ARP request)
ARP: Sender's hardware address = 00070EE83E1F
ARP: Sender's protocol address = [219.245.173.1]
ARP: Target hardware address = 000000000000
ARP: Target protocol address = [219.245.173.69]
ARP:
ARP: 18 bytes frame padding
ARP:

图 53