

使用 Sniffer Pro 监控网络流量

硬件环境:

100M 网络环境下, 92 台终端数量, 主交换采用 D-LINK (友讯) DES-3226S 二层交换机 (支持端口镜像功能), 级联普通傻瓜型交换机。光纤 10M 接入, 华为 2620 做为接入网关。

软件环境:

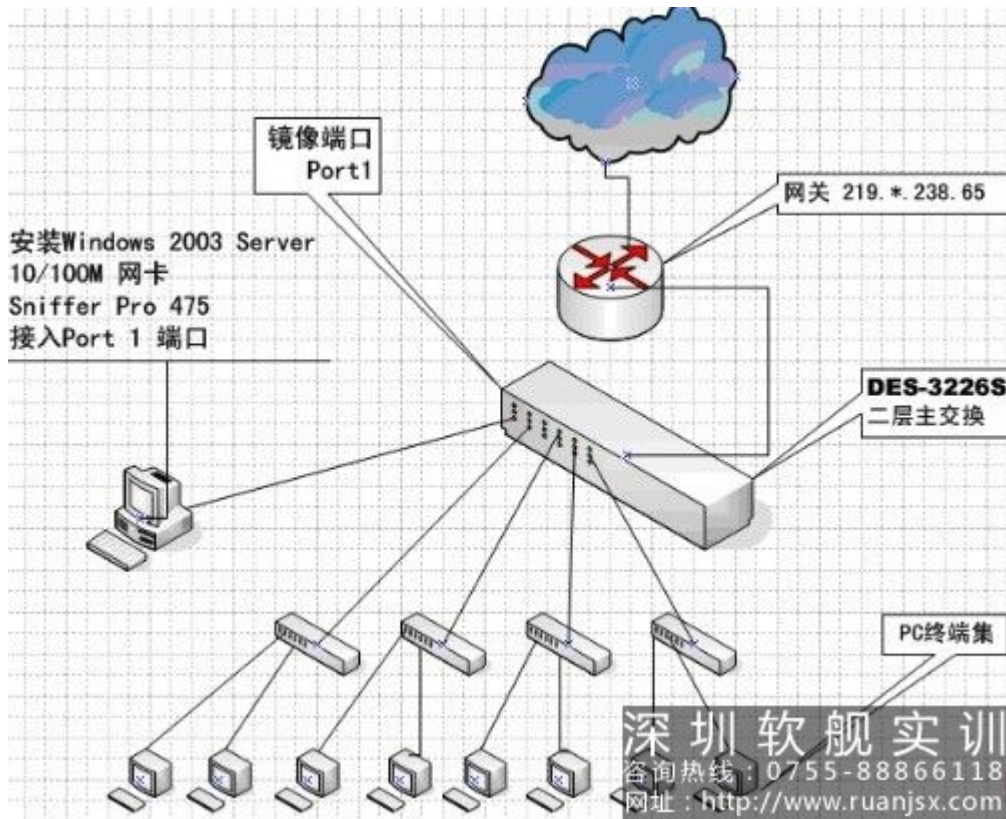
操作系统 Windows2003 Server 企业标准版 (Sniffer Pro 4.6 及以上版本均支持 Windows2000 Windows-xp Windows2003)、NAI 协议分析软件-Sniffer Portable 4.75 (本文选用网络上较容易下载到的版本做为测试)

环境要求:

1、如果需要监控全网流量, 安装有 Sniffer Portable 4.7.5 (以下简称 Sniffer Pro) 的终端计算机, 网卡接入端需要位于主交换镜像端口位置。(监控所有流经此网卡的数据)

2、Sniffer pro 4.75 仅支持 10M、100M、10/100M 网卡, 对于千兆网卡, 请安装 SP5 补丁, 或 4.8 及更高的版本

网络拓扑:



监控目的:

通过 Sniffer Pro 实时监控, 及时发现网络环境中的故障(例如病毒、攻击、流量超限等非正常行为)。对于很多企业、网吧网络环境中, 网关(路由、代理等)自身不具备流量监控、查询功能, 本文将是一个很好的解决方案。Sniffer Pro 强大的实用功能还包括: 网内任意终端流量实时查询、网内终端与终端之间流量实时查询、终端流量 TOP 排行、异常告警等。同时, 我们将数据包捕获后, 通过 Sniffer Pro 的专家分析系统帮助我们更进一步分析数据包, 以助更好的分析、解决网络异常问题。

步骤二: Sniffer Pro 安装、启动、配置

Sniffer Pro 安装过程与其它应用软件没有什么太大的区别, 在安装过程中需要注意的是:

①Sniffer Pro 安装大约占用 70M 左右的硬盘空间。

②安装完毕 Sniffer Pro 后, 会自动在网卡上加载 Sniffer Pro 特殊的驱动程序(如图 5)。

③安装的最后将提示填入相关信息及序列号, 正确填写完毕, 安装程序需要重新启动计算机。

④对于英文不好的管理员可以下载网上的汉化补丁。



我们来启动 Sniffer Pro。第一次启动 Sniffer Pro 时, 需要选择程序从一个网络适配器接收数据, 我们指定位于端口镜像所在位置的网卡。

具体位于: File->Select Settings->New



名称自定义、选择所在网卡下拉菜单, 点击确定即可。(如图 6)

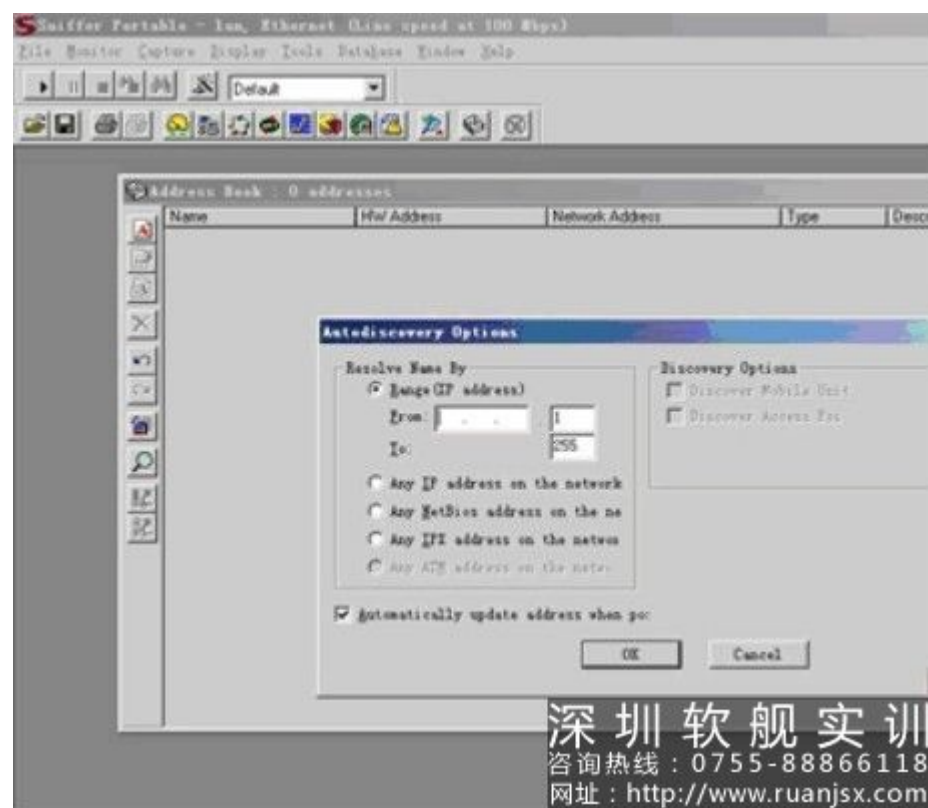
这样我们就进入了 Sniffer Pro 的主界面。

步骤三: 新手上路, 查询网关流量

下面以图文的方式介绍，如何查询网关(路由、代理：219.*.238.65)流量，这也是最为常用、重要的查询之一。

1. 扫描 IP-MAC 对应关系。这样做是为了在查询流量时，方便判断具体流量终端的位置，MAC 地址不如 IP 地址方便。

选择菜单栏中 Tools->Address Book 点击左边的放大镜(autodiscovery 扫描)在弹出的窗口中输入您所扫描的 IP 地址段，本例输入：219.*.238.64-219.*.238.159 点击 OK，系统会自动扫描 IP- MAC 对应关系。扫描完毕后，点击 DataBase->Save Address Book 系统会自动保存对应关系，以备以后使用。(如图 7)



2. 查看网关流量。点击 Monitor->Host Table，选择 Host table 界面左下角的 MAC-IP-IPX 中的 MAC。(为什么选择 MAC?在网络中，所有终端的对外数据，例如使用 QQ、浏览网站、上传、下载等行为，都是各终端与网关在数据链路层中进行的)(如图 8)

Sniffer Portable - lan, Ethernet (Link speed at 100 Mbps) - [Host Table: 98 stations]

File Monitor Capture Display Tools Database Window Help

Default

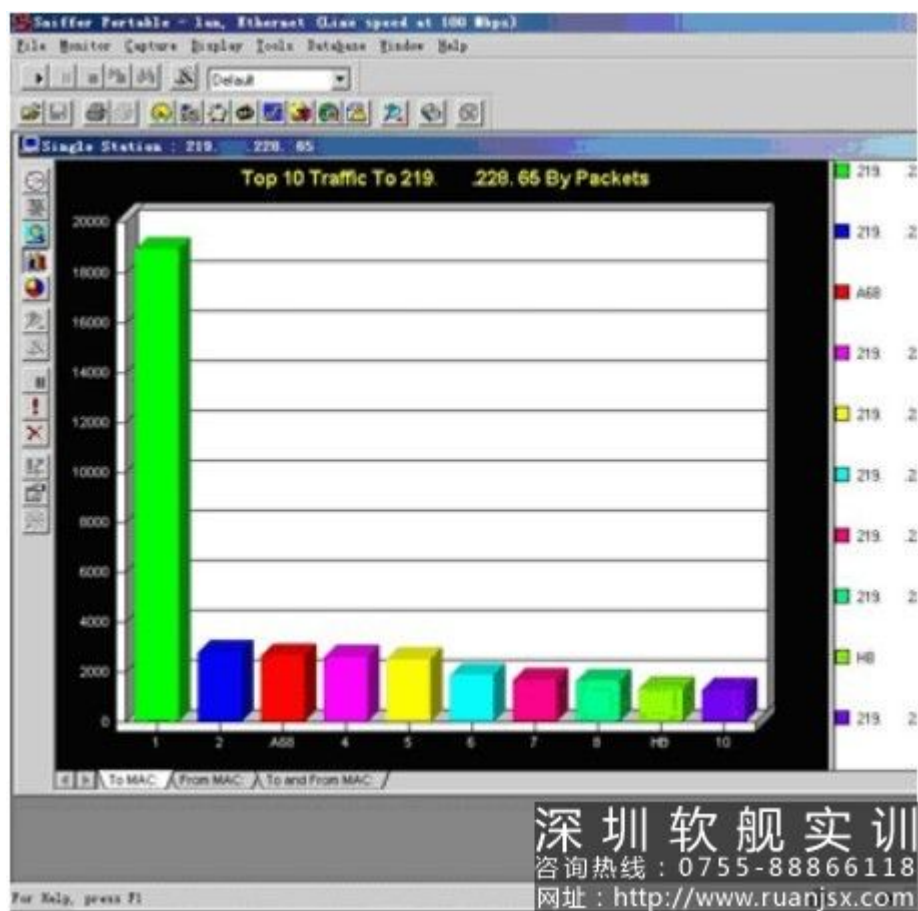
HostAdd	In Pkts	Out Pkts	In Bytes	Out Bytes	Broadcast	Multicast	Out Errors
01005E050607	425	0	507,895	0	0	0	0
219.228.65	8,540	9,123	1,989,658	2,071,447	3	0	0
219.228.101	6	6	1,118	204	0	0	0
219.228.103	206	132	50,159	21,250	0	0	0
219.228.104	0	2	0	130	2	0	0
219.228.105	20	19	2,815	1,680	1	0	0
219.228.107	22	83	11,485	52,776	0	0	0
219.228.110	59	13	37,575	976	0	0	0
219.228.111	253	234	18,244	231,843	0	0	0
219.228.112	77	47	104,346	3,407	0	0	0
219.228.114	214	409	36,707	214,558	0	0	0
219.228.115	4	5	586	583	0	0	0
219.228.119	237	240	43,270	43,374	0	0	0
219.228.120	10	12	1,480	842	0	0	0
219.228.123	235	162	338,122	14,332	0	0	0
219.228.125	123	79	139,622	5,061	0	0	0
219.228.129	6	6	2,131	384	0	0	0
219.228.130	1	2	454	146	1	0	0
219.228.131	211	143	304,678	13,526	0	0	0
219.228.132	48	43	37,385	3,782	0	0	0
219.228.134	336	441	140,589	249,881	1	0	0
219.228.135	338	302	147,171	108,537	0	0	0
219.228.138	14	17	3,125	1,888	0	0	0
219.228.139	28	26	4,083	1,860	0	0	0
219.228.140	35	33	4,624	2,470	0	0	0
219.228.142	317	275	192,793	37,361	0	0	0
219.228.143	40	41	5,222	2,334	0	0	0
219.228.145	282	201	358,976	17,963	0	0	0
219.228.146	14	16	3,606	1,371	0	0	0
219.228.147	44	34	3,904	2,521	0	0	0
219.228.148	126	153	28,700	15,295	0	0	0
219.228.150	447	299	645,766	27,629	0	0	0
219.228.151	306	220	202,241	36,707	0	0	0
219.228.152	65	80	5,274	5,446	2	0	0
219.228.153	28	29	3,034	2,139	2	0	0
219.228.154	8	9	1,096	939	1	0	0
219.228.155	349	240	496,134	22,121	2	0	0
219.228.156	661	703	117,967	123,520	2	0	0
219.228.157	46	59	4,697	4,549	1	0	0
219.228.158	1	1	86	82	0	0	0
219.228.159	26	25	4,999	1,863	2	0	0
219.228.93	3,702	3,264	373,512	584,141	3	0	0
219.228.94	45	47	10,149	3,026	0	0	0
219.228.98	143	136	16,516	17,377	1	0	0

MAC / IP / Fx

For help, press F1

深圳软舰实训
咨询热线：0755-88866118
网址：<http://www.ruangj.com>

3. 找到网关的 IP 地址->选择 single station->bar (本例中网关 IP 为 219.*.238.65)

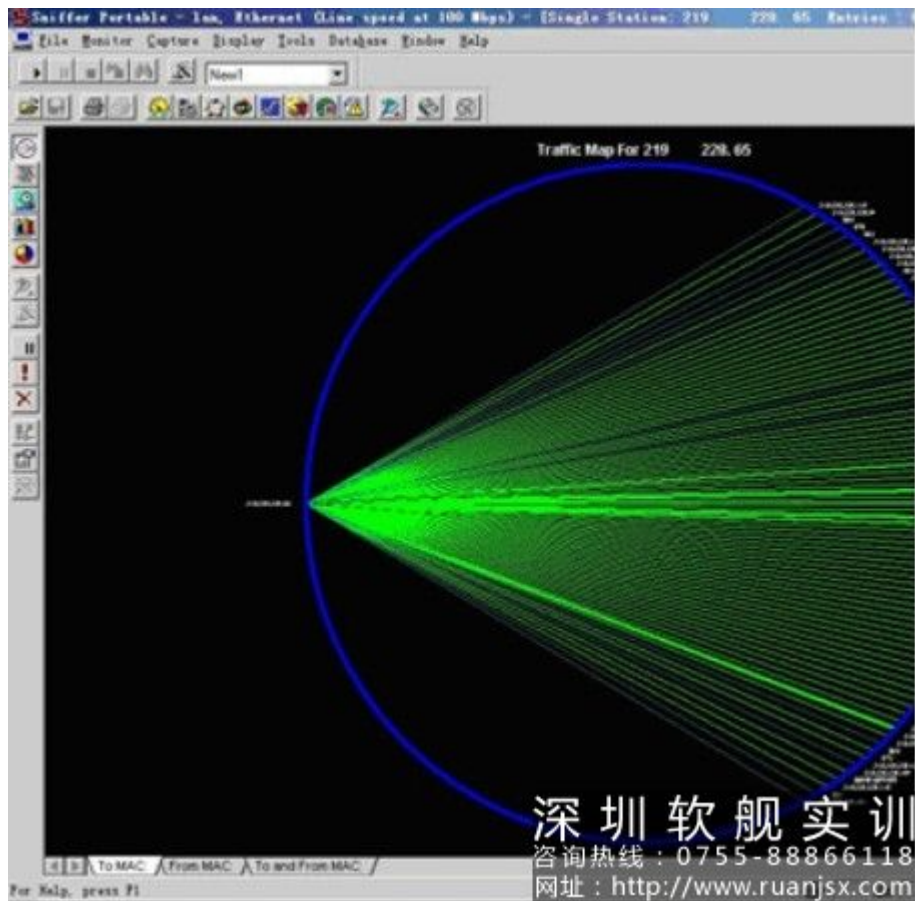


如图(9)所示：

219.*.238.65(网关)流量 TOP-10 此图为实时流量图。在此之前如果我们没有做扫描 IP(Address Book)的工作，右边将会以网卡物理地址-MAC 地址的方式显示，现在转换为 IP 地址形式(或计算机名)，现在很容易定位终端所在位置。流量以 3D 柱形图的方式动态显示，其中最左边绿色柱形图与网关流量最大，其它依次减小。本图中 219.*.238.93 与网关流量最大，且与其它终端流量差距悬殊，如果 这个时候网络出现问题，可以重点检查此 IP 是否有大流量相关的操作。

如果要查看 219.*.238.65(网关)与内部所有流量通信图，我们可以点击左边菜单中，排列第一位的->MAP 按钮

如图(10)所示，网关与内网间的所有流量都在这里动态的显示。



需要注意的是:

绿色线条状态为: 正在通讯中

暗蓝色线条状态为: 通信中断

线条的粗细与流量的大小成正比

如果将鼠标移动至线条处, 程序显示出流量双方位置、通讯流量的大小(包括接收、发送)、并自动计算流量占当前网络的百分比。

其它主要功能:

PIE: 饼图的方式显示 TOP 10 的流量占用百分比。

Detail: 将 Protocol(协议类型)、From Host(原主机)、in/out packets/bytes(接收、发送字节数、包数)等字段信息以二维表格的方式显示。

第四步: 基于 IP 层流量

1. 为了进一步分析 219.*.238.93 的异常情况, 我们切换至基于 IP 层的流量统计图中看看。点击菜单栏中的 Monitor->Host Table, 选择 Host Table 界面左下角的 MAC-IP-IPX 中的 IP。

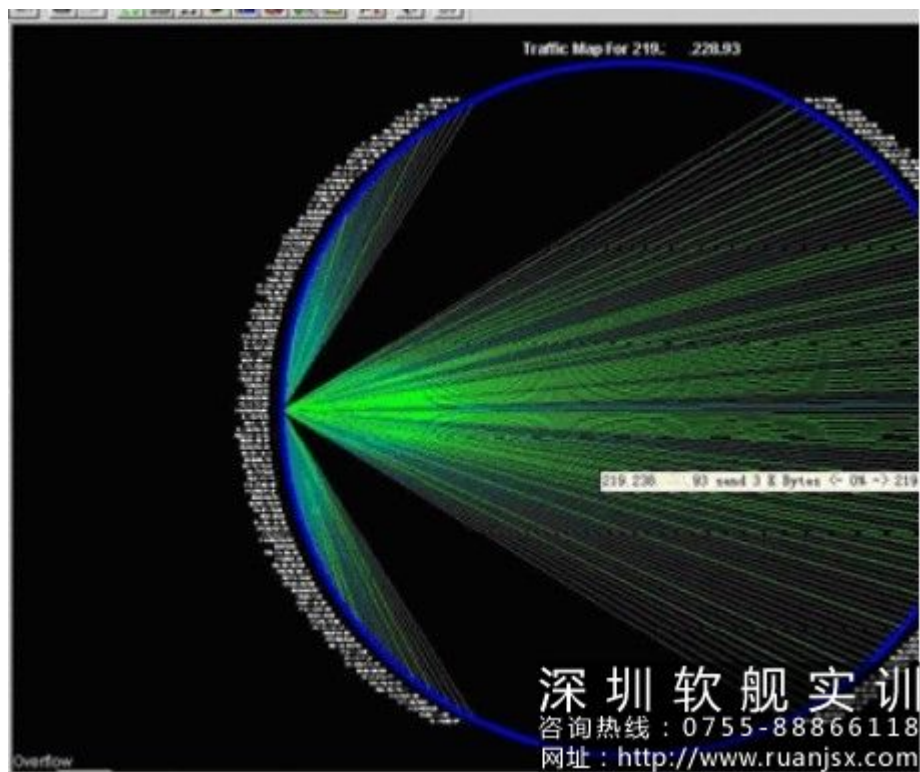
2. 找到 IP: 219.*.238.93 地址(可以用鼠标点击 IP Addr 排序, 以方便查找)->选择 single station->bar (如图 11 所示)



IP Addr	In Pkts	Out Pkts	In Bytes	Out Bytes	Broadcast
219.138.31.158	77	100	5,733	130,388	0
219.140.80.154	13	15	1,689	6,153	0
219.140.178.162	258	260	44,737	45,107	0
219.140.194.219	9	11	995	1,063	0
219.141.136.10	66	66	5,312	12,319	0
219.148.141.250	1	2	66	130	0
219.149.47.100	648	644	116,915	116,151	0
219.149.141.157	0	5	0	370	0
219.151.35.200	13	11	3,446	2,328	0
219.151.36.117	180	315	12,679	256,957	0
219.153.155.222	619	744	289,752	866,856	0
219.153.239.92	13	11	1,447	1,343	0
219.155.167.174	246	235	148,632	243,797	0
219.155.177.136	685	1,171	45,586	941,392	0
219.157.96.110	623	621	114,514	114,112	0
219.197.72.9	38	47	3,811	36,784	0
219.233.95.127	325	206	365,282	30,717	0
219.235.207.2	9	9	1,410	652	0
219.237.42.148	61	44	32,267	3,986	0
219. .34.254	1	1	64	64	0
219. .227.2	50	36	49,620	2,793	0
219. .228.85	91	115	22,036	24,555	0
219. .228.93	59,817	55,786	47,300,885	29,031,584	0
219. .228.94	342	274	153,319	21,324	0
219. .228.98	8,066	14,787	878,480	17,878,505	0
219. .228.100	3,177	4,556	289,928	6,575,980	0
219. .228.106	109	127	14,204	8,920	0
219. .228.115	150	168	17,511	14,509	0
219. .228.117	4,570	3,185	6,576,880	290,462	0
219. .228.119	4	0	264	0	0
219. .228.121	14	12	1,132	1,004	0
219. .228.123	3	0	414	0	0
219. .228.132	70	79	8,775	8,482	0
219. .228.134	1	0	66	0	0
219. .228.140	3,105	3,285	54,566	54,566	0
219. .228.149	1	1	22	22	0

深圳软舰实训
咨询热线: 0755-88866118
网址: <http://www.ruansjx.com>

3. 我们切换至 Traffic Map 来看看它与所有 IP 的通信流量图。(图 12)



我们可以从 219.*.238.93 的通信图中看到，与它建立 IP 连接的情况。图中 IP 连接数目非常大，这对于普通应用终端来讲，显然不是一种正常的业务连接。我们猜测，该终端可能正在进行有关 P2P 类的操作，比如正在使用 P2P 类软件进行 BT 下载、或者正在观看 P2P 类在线视频等。

为了进一步的证明我们的猜测，我们去看看 219.*.228.93 的流量协议分布情况。

4. 如图(13)所示: Protocol 类型绝大部分为 Other. 我们知道在 Sniffer Pro 中 Other 表示未能识别出来协议，如果提前定义了协议类型，这里将会直接显现出来。

Protocol	From Host	Packets Out	Bytes Out	Output Usage
	60.46.203.162	621	504,967	
	60.242.92.241	561	593,780	
	221.206.109.229	542	512,643	0.02 %
	68.198.143.197	254	193,294	
	24.193.226.140	1,006	467,052	
	122.198.26.14	590	787,163	0.03 %
	61.141.231.198	439	217,877	
	220.253.72.90	775	542,154	0.02 %
	222.183.39.54	533	596,347	
	222.188.198.163	596	450,258	0.01 %
	60.48.93.51	227	194,649	
	219.195.167.174	453	495,751	
	222.71.151.60	426	467,130	0.02 %
	58.37.221.198	214	256,887	
	221.201.28.14	743	620,750	
	218.19.5.137	768	661,259	
	58.214.136.130	75	56,983	0.01 %
	218.88.212.157	796	756,939	
	218.66.91.26	741	996,252	
	211.142.212.3	1,327	1,006,397	
	125.238.89.202	1,308	947,545	
	82.21.16.65	798	876,174	
	218.111.221.137	703	962,181	
	218.82.232.219	1,277	866,532	
	59.42.238.73	745	817,774	
	219.128.2.17	891	643,624	
	219.153.155.222	1,025	933,836	0.03 %
	81.154.27.238	691	678,884	
	71.72.158.21	802	635,461	
	222.72.85.90	609	499,762	
	58.232.233.2	642	869,139	
	74.13.141.10	625	639,786	
	85.147.121.233	668	893,135	
	202.104.18.99	1,685	875,135	
	213.113.42.155	1,096	883,860	
	220.249.109.14	1,055	999,937	
	171.33.0.33.4	1,683	878,307	

深圳软舰实训
咨询热线：0755-88866118
网址：http://www.ruanjisx.com

如图(14)通过菜单栏下的 Tools->Options->Protocols, 在第 19 栏中定义 14405(bitcomet 的默认监听端口), 取名为 bitcom。

Options		
General MAC Threshold App Threshold Alarm Protocols		
	Name	Port
10	Gopher	70
11	IMAP	143
12	LPD	515
13	NetBIOS_SSN_T	139
14	Telnet	23
15	Xvln6000	6000
16	Xvln6001	6001
17	NCP over IP	524
18	SLP	427
19	bitcom	14405
20		

深圳软舰实训
咨询热线：0755-88866118
网址：http://www.ruanjisx.com

现在我们再次查看 219.*.238.93 协议分布情况。(如图 15)

Protocol	From Host	Packets Out	Bytes Out	Output Usage
bitcom	222.36.101.177	277	388,907	0.04 %
	218.249.214.130	130	10,576	0.00 %
Others	220.176.204.230	1,325	2,670,620	0.26 %
	211.142.212.9	5,018	4,155,481	0.40 %
	61.155.58.2	5,441	3,103,296	0.30 %
bitcom	125.31.194.124	267	147,736	0.01 %
	222.82.216.4	106	7,236	0.00 %
Others	221.130.56.14	299	371,189	0.04 %
bitcom	222.165.98.218	14	1,000	0.00 %
Others	124.116.206.10	1	64	0.00 %
bitcom	222.129.48.62	84	82,771	0.01 %
Others	222.241.118.86	1,242	1,434,342	0.14 %
Others	219.148.206.43	15	2,106	0.00 %
Others	219.148.206.43	168	170,730	0.02 %
bitcom	125.54.227.228	610	856,538	0.08 %
Others	221.239.189.236	36	13,506	0.00 %
Others	207.112.43.14	5	329	0.00 %
Others	220.203.1.11	571	687,303	0.06 %
Others	222.208.127.8	8	6,620	0.00 %
bitcom	219.137.23.164	53	58,617	0.01 %
	220.174.147.22	25	2,329	0.00 %
	219.132.68.221	19	9,430	0.00 %
	221.237.36.40	37	2,664	0.00 %
Others	218.13.25.149	105	129,492	0.01 %
	222.168.8.20	13	952	0.00 %
Others	218.66.109.67	47	51,329	0.01 %
bitcom	220.162.57.145	6	3,499	0.00 %
Others	61.145.233.66	80	95,620	0.01 %
Others	222.83.123.102	13	928	0.00 %
Others	61.147.153.99	5	384	0.00 %
bitcom	218.92.27.10	100	102,092	0.01 %
	222.86.53.84	12	2,972	0.00 %
	218.70.153.93	63	62,324	0.01 %
Others	211.92.96.55	11	1,290	0.00 %
	58.211.189.99	156	189,178	0.02 %
	61.144.109.149	17	1,806	0.00 %
To IP: From IP: To and From IP:		196.93.206.216	3	264

深圳软舰实训
咨询热线：0755-88866118
网址：http://www.ruanjx.com

现在，协议类型大部分都转换为 bitcom，这样我们就可以断定，此终端正在用 bitcomet 做大量上传、下载行为。

注意：很多 P2P 类软件并没有固定的使用端口，且端口也可以自定义，因此使用本方法虽然不失为一种检测 P2P 流量的好方法，但并不能完全保证其准确性。

好了，使用 Sniffer Pro 监控网关流量，就到这里结束了。实际上我们可以用同样的方法监控网络内的任何一台终端。