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：

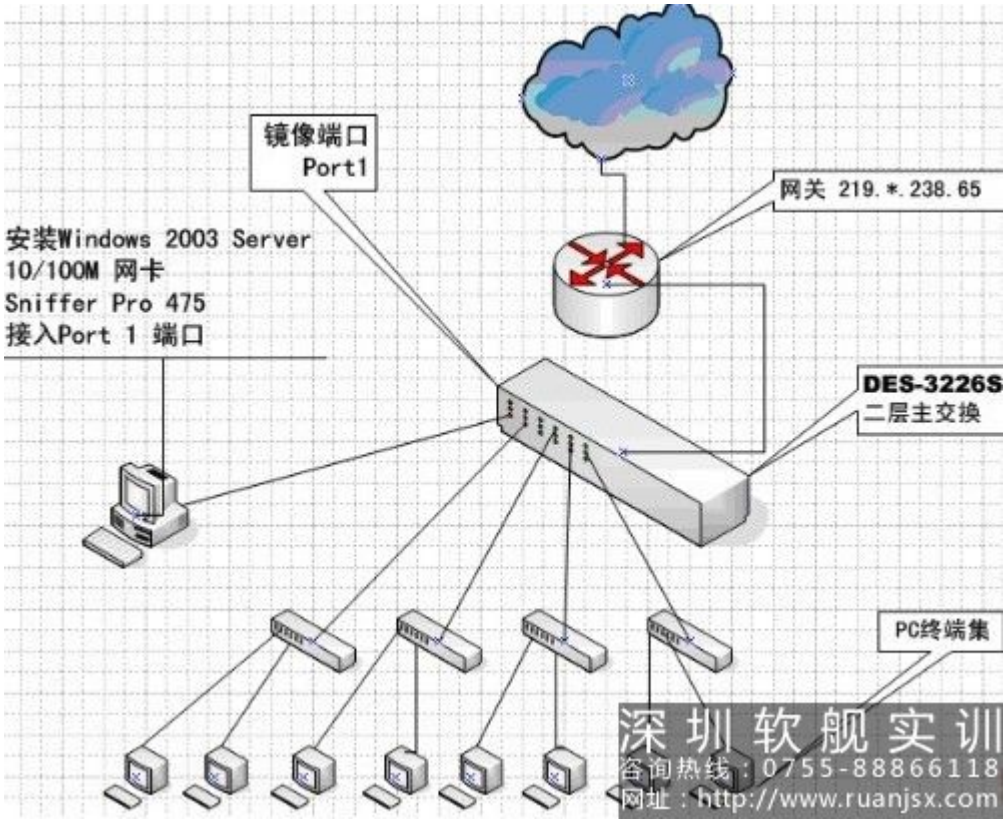
操作系统 Windows2003 Server 企业标准版(Sniffer Pro4.6 及以上版本均支持 Windows2000 Windows-xp Windows2003)、NAI 协议分析软件-Sniffer Portable 4.75(本文选用网络上较容易下载到的版本做为测试)

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、Snffier pro 475 仅支持 10M、100M、10/100M 网卡，对于千 M 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。

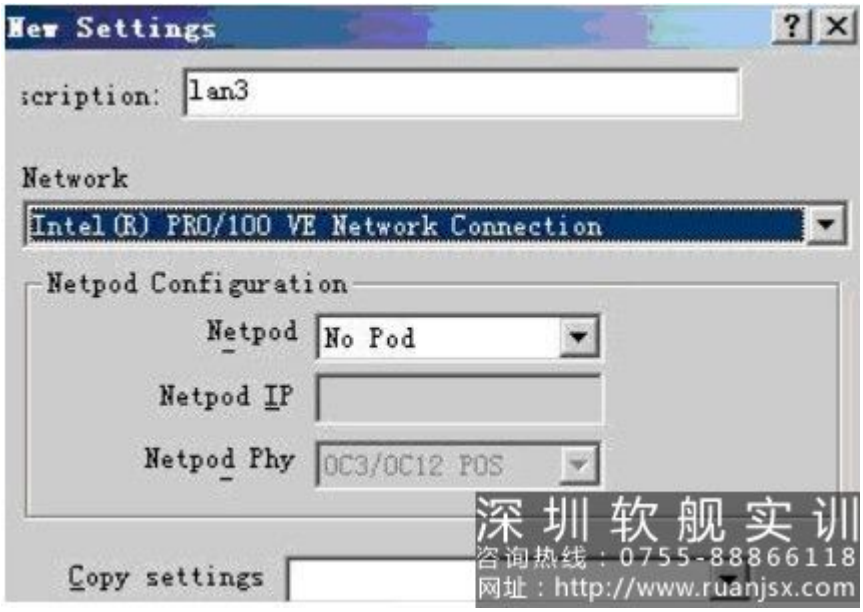
②安装完毕 Sniffer Pro 后，会自动在网卡上加载 Sniffer Pro 特殊的驱动程序(如图 5)。

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,需要选择程序从那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。

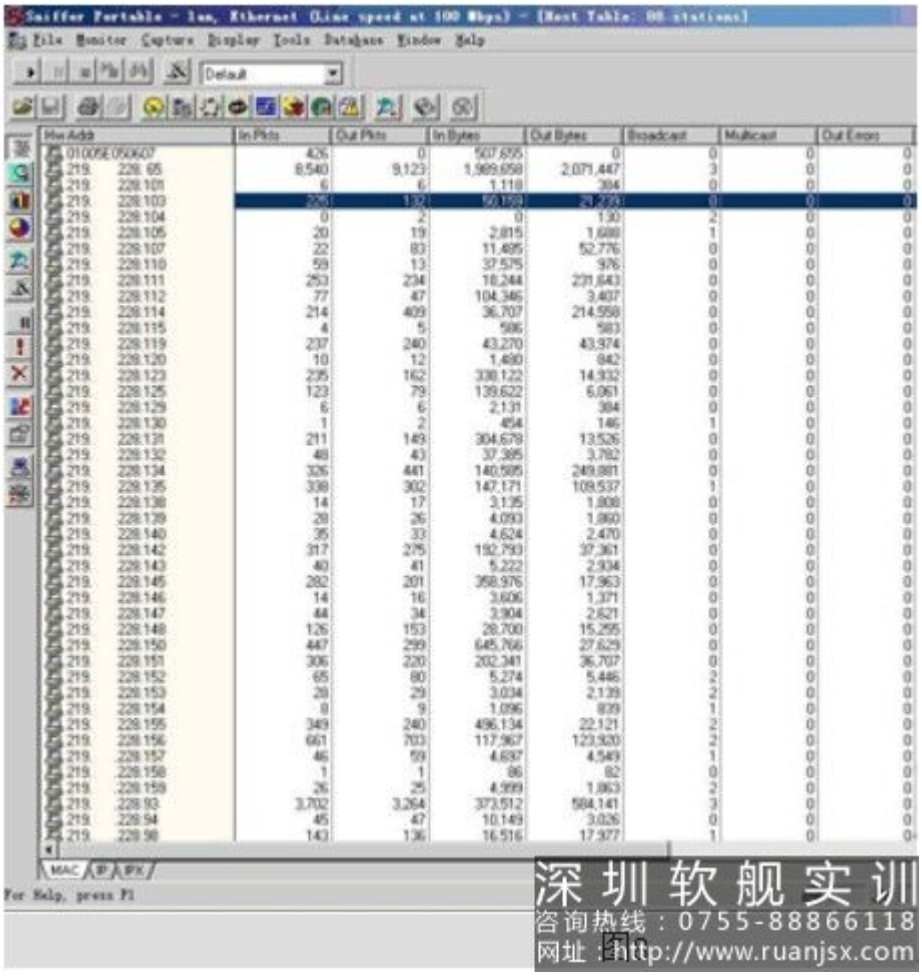
步骤三：新手上路，查询网关流量

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要扫描的 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)



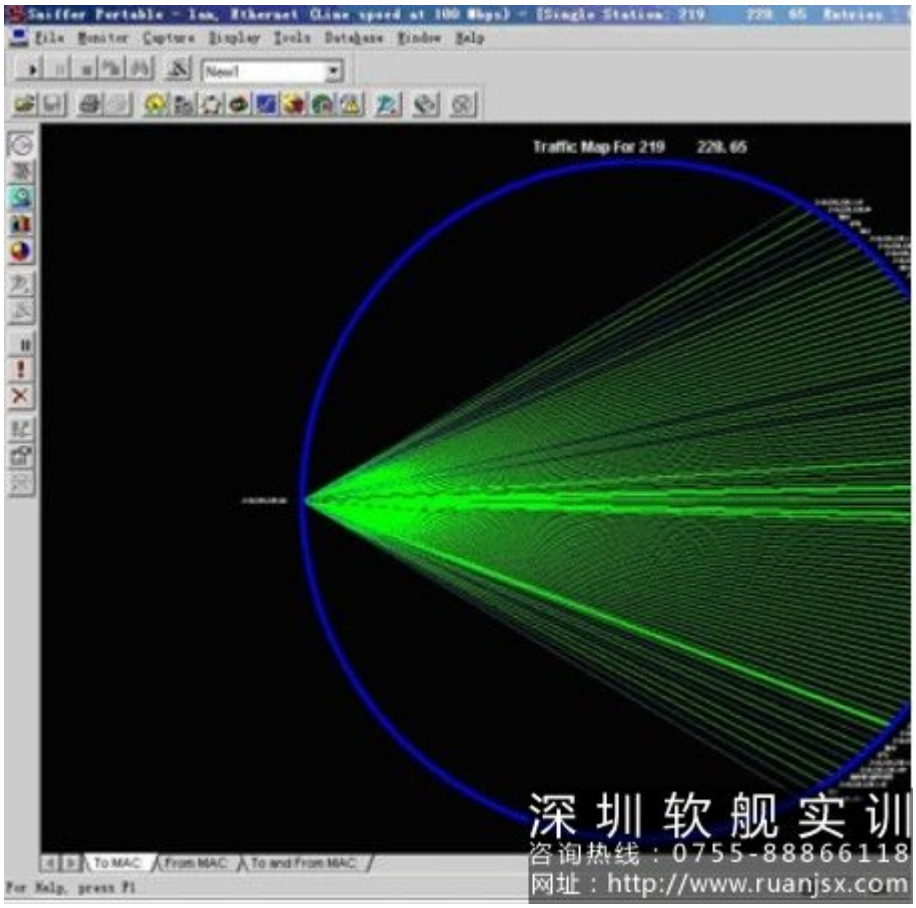
3.找到网关的 IP 地址->选择 single station->bar（本例中网关 IP 为 219.*.238.65）

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。

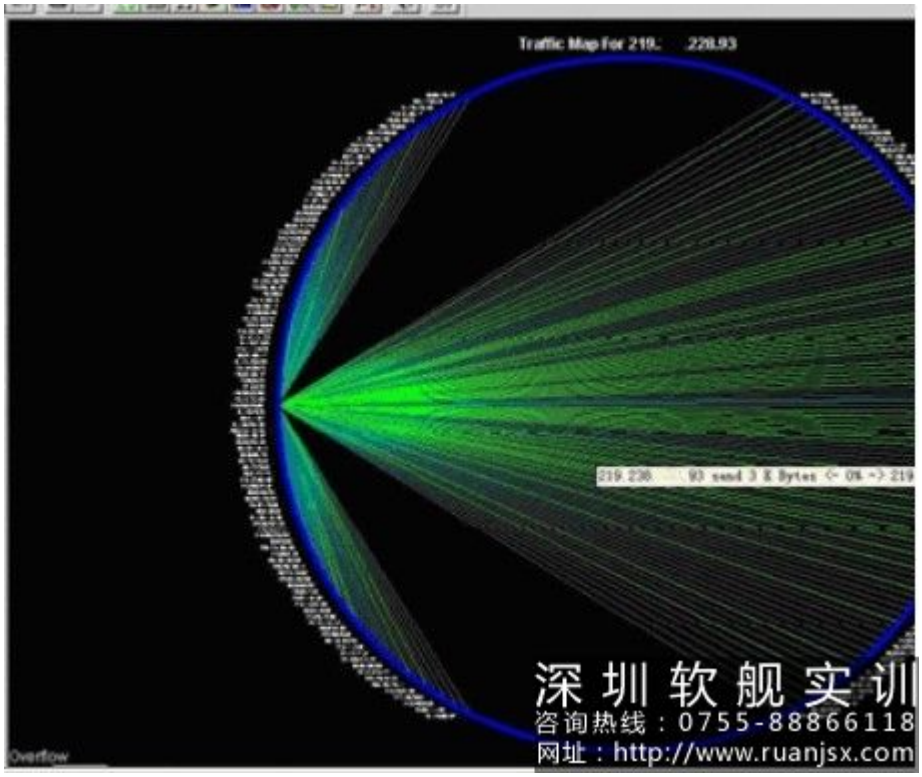
Detail：将 Protocol(协议类型)、From Host(原主机)、in/out packets/bytes(接收、发送字节数、包数)等字段信息以二维表格的方式显示。

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）

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

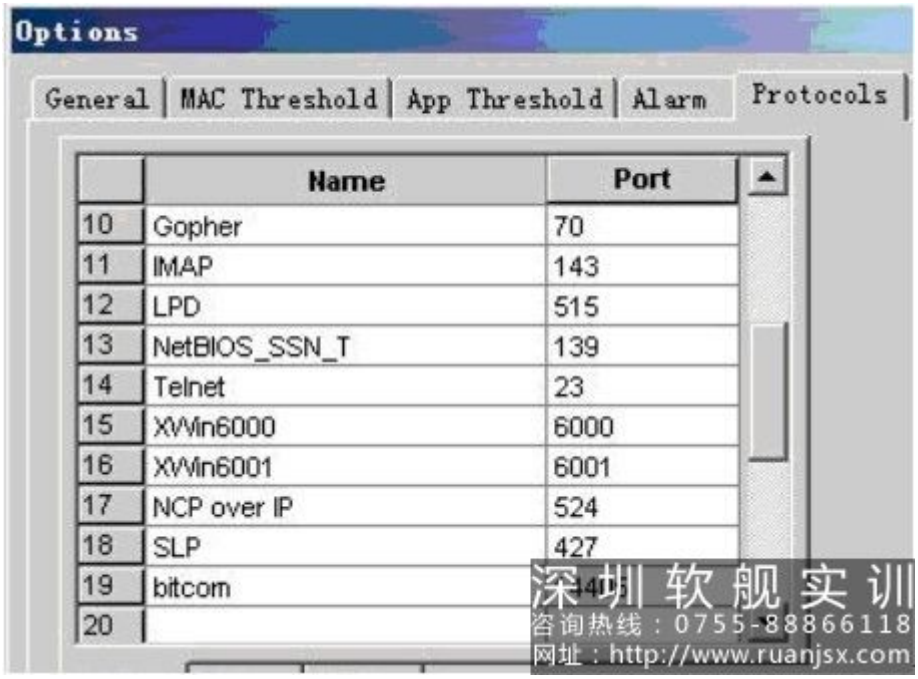


我们可以从 219.*.238.93 的通信图中看到，与它建立 IP 连接的情况。图中 IP 连接数目非常大，这对于普通应用终端来讲，显然不是一种正常的 业务连接。我们猜测，该终端可能正在进行有关 P2P 类的操作，比如正在使用 P2P 类软件进行 BT 下载、或者正在观看 P2P 类在线视频等。

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 Othen.我们知道在 Sniffer Pro 中 Othen 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。

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。



现在我们再次查看 219.*.238.93 协议分布情况.(如图 15)

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。