

网 路 岗 七 代

用 户 手 册



研制单位：深圳市德尔软件技术有限公司

编写时间：二〇一〇年一月一日

产品网站：<http://www.softbar.com>

关键词：网络监控软件，网络管理软件，内网管理，上网管理软件，网络岗，邮件监控软件，聊天监控

目 录

第一章：产品安装 / 卸载/重装.....	3
产品安装.....	3
配置要求.....	3
开始安装.....	3
注册产品.....	3
卸载产品.....	4
重装产品.....	4
第二章：初始化工作.....	4
快速启动（针对单网段）.....	4
了解已有的网络结构，确定监控方案.....	6
选择捕包网卡 / 过滤网卡.....	7
启动监控服务.....	7
检验“监视 / 过滤”效果.....	7
第三章：基于MAC的跨VLAN监控.....	8
最常见的跨VLAN结构及安装图.....	8
跨VLAN监控常用俗语.....	9
跨VLAN监控时的软件配置.....	10
第四章：监控模式：基于MAC/帐户/IP.....	11
“基于网卡”的监控模式.....	11
MAC地址及其获取方法.....	11
基于网卡监控的含义.....	11
管理电脑列表.....	11
跨VLAN.....	12
“基于帐户”的监控模式.....	12
“基于IP”的监控模式.....	13
监控方式的选择.....	14
第五章：过滤规则.....	14
第六章：上网评价.....	15
第七章：报警.....	17
GSM短信报警.....	18
邮件报警.....	20
声音报警.....	21
第八章：网路岗NAT及网桥.....	22
NAT基本知识.....	22
启用网路岗NAT.....	22
网桥和虚拟网桥.....	23
第九章：常见问题解答.....	24

第一章：产品安装 / 卸载/重装

产品安装

配置要求

运行平台：Windows XP/2K/2003；

最低配置：奔 4 处理器，40G 硬盘，256M 内存。如果用户监控电脑数量较多，可适当提高系统基本配置。

开始安装

如果您的电脑上已安装过《网路岗》早期版本，那么请停止相关的后台服务，但不用卸载，因为最新产品安装目录不一样，对于老版本的监控日志，第七代是兼容的，您只需要把以前的日志目录拷贝到第七代的日志目录下即可。

运行安装包(或 CD)中的 Sentry7_Setup.exe 文件，根据安装提示操作即可完成安装。

(网路岗以后的版本不再需要 Winpcap 的支持)

注册产品

打开“帮助”菜单，选择“产品信息”项，在弹出的窗口的中点击“注册”按钮，填写相关内容，进行注册，见下图。

<图 1>

如果您没有注册码，那么可以进入《网路岗》产品网站“下载中心”获取一个免费试用

关键词：网络监控软件，网络管理软件，内网管理，上网管理软件，网络岗，邮件监控软件，聊天监控

码。如果免费注册码的“试用期限/监控点数/功能”等不符您的要求，您可以直接联系销售人员，以获取其他的试用码。

注册码可分为几个不同版本：校园版、企业版、城域网版、网络审计专版。

卸载产品

进入系统“菜单”，选择“卸载产品”，或进入“控制面板”——“添加/删除程序”，开始卸载。

卸载时，主要考虑两个选项：删除“配置文件”，删除“日志文件”，配置文件存放在安装目录下的 ETC 子目录下，缺省日志文件目录在安装目录的 CAPLOG 子目录下。

如果卸载时选择了保留以前的配置文件和日志文件，则以后重新安装的时候，这两个目录不会被覆盖。

重装产品

如果您需要更换操作系统，或对系统盘进行格式化处理，那么需要重装本系统，我们建议：

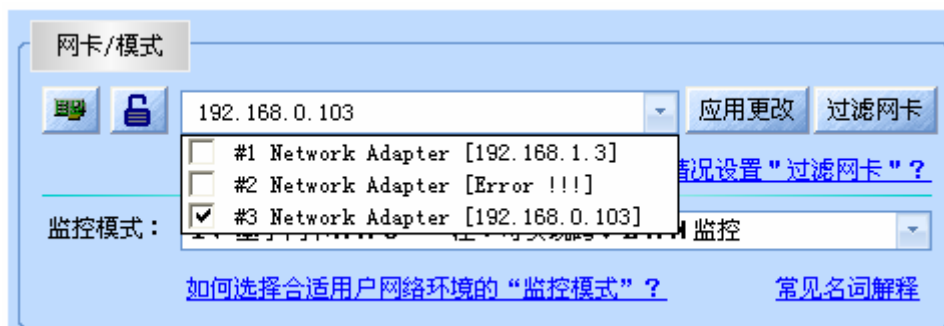
- 1、 停止“网路岗”监控服务，关闭网路岗相关程序，然后备份“配置文件”和“日志文件”到其他盘中，
- 2、 等系统处理完成后，那么再安装“网路岗”，在没有打开“网路岗”的情况下，把备份的日志和配置文件覆盖回去。

第二章：初始化工作

快速启动（针对单网段）

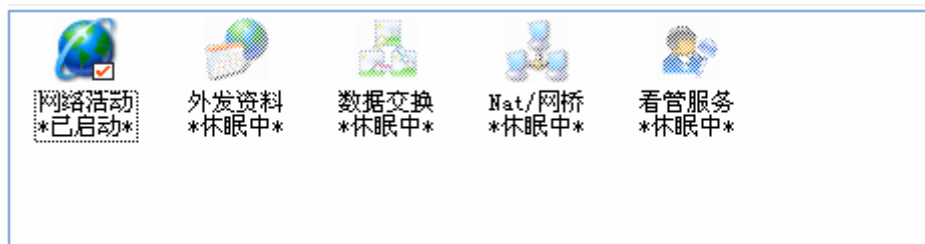
执行下面步骤之前，请确保该产品已经注册，注册方法见“安装”部分。

第一步：打开桌面“网路岗”主程序，选择捕包网卡，通常情况选一块，如下图：



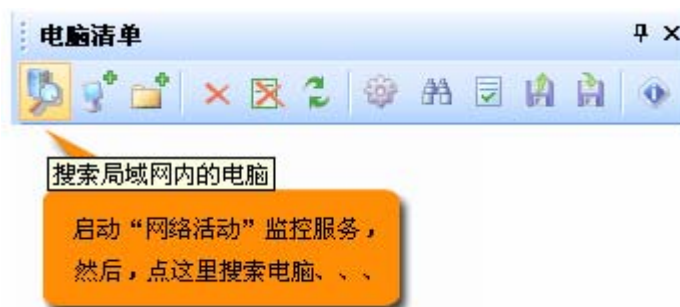
<图 2>

第二步：启动“网络活动”监控服务（双击启动），如下图：



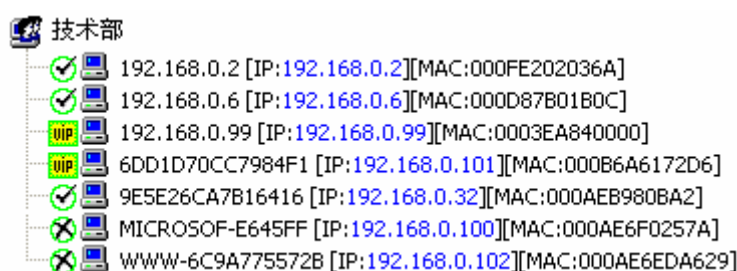
<图 3>

第三步：搜索目标电脑，如下图：






<图 4>

如果搜索成功，会出现类似下面的列表，

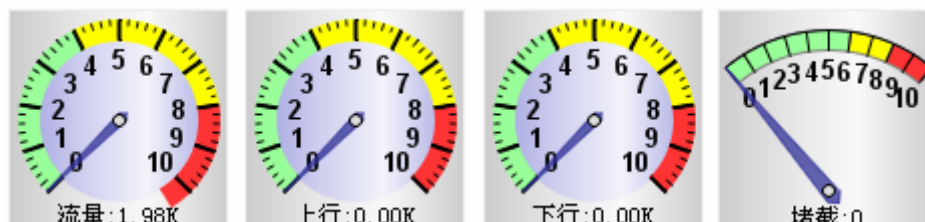


<图 5>


电脑前面的小图标分别代表不同的状态：监控、不监控、封杀，用鼠标点击后可改变其状态。

第四步：观看效果。

如果网络有流量出现，则下面图中的指针会摆离 0 的位置；出现摆动，说明所绑定的网卡的确有通讯流量。



<图 6>

打开“现场观察”窗口，让搜索出来的电脑上网，观察上网情况。

如果在“现场观察”窗口中能观察到客户机的上网活动，则表明监控已初见成效。相反，

如果没有任何监控内容出现，那么，请继续阅读下面的介绍。

了解已有的网络结构，确定监控方案

常见的网络情形：

1. 单网段结构，所有电脑以一个硬件路由器(或防火墙)作为上网出口。
2. 单网段结构，所有电脑通过其中某一台电脑上网，该电脑安装了代理服务器软件（或启用了系统本身自带的 Internet 共享）。
3. 多网段结构，核心交换机上划分 VLAN，所有电脑通过一台(或多台)连接核心交换机的路由器(或防火墙)上网。
4. 多局域网结构，整个网络由多个互不相连局域网组成，各自通过单独的路由器(或防火墙)上网。

针对上述几种常见网络结构，这里分别给出各自的应对方案：

针对<情形 1>有三种可能的方案。

第一方案：在路由器和内部交换机之间添加共享 HUB，路由器和交换机分别连线到 HUB，监控机也连接到该 HUB 上。这是惯用的老式监控方案，该方案要求 HUB 性能稳定，最好是 100M 的。

第二方案：在安装“网路岗”的电脑上安装两块网卡，一进一出，分别接交换机和路由器，在“网路岗”软件中启用“网络桥”功能。该类方案需要较高的电脑配置，控制方面非常有效，可有效针对 UDP 类型通讯包进行拦截。

第三方案：如果和路由器相连的交换机是网管型交换机，支持“端口镜像”功能，那么，直接在该交换机上找出一个空闲口，设置为“镜像端口 / 监控端口”，和路由器相连的交换机口，设置为“被镜像端口 / 被监控端口”。

针对<情形 2>，安装非常简单，只需要将《网路岗》和代理服务器软件安装在同一电脑。

针对<情形 3>，监控相对复杂一些。

首先，因为网络通讯包在跨 VLAN 后发生改变（这种变化还因交换机型号不同而不同），造成监控和封堵上的困难，尽管如此，大多数用户仍希望以网卡地址来作为监控依据。

但是，“网路岗七代”仍然有较为满意的解决方案：

通常情况下，用户需要在核心交换机上设置“端口镜像”功能，将连接路由器（或防火墙）的网线的交换机口全部镜像到位于某一同级 VLAN 的口（监控口）。监控口连入安装“网路岗”软件的电脑，这样所有电脑的上网信息包汇总到“监控电脑”上，于是达到监控的目的。要正常监控，用户还必须做相关设置，包括“汇聚 MAC”，“MAC 采集点”等，具体见《第三章》。

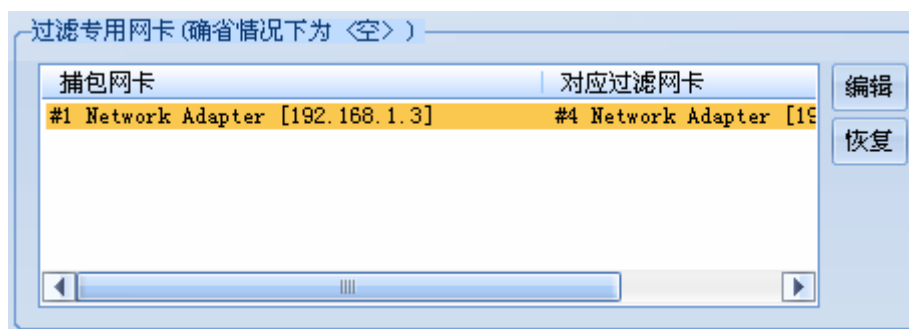
如果交换机设置“端口镜像”功能后，监控口变成“单向接受”状态，具体表现为：不能和其他内网电脑发生通讯。那么用户需要添加另外一块网卡，用来作为专门的过滤网卡，具体见《第三章》。

针对<情形 4>，需要在监控机上安装多块网卡，每块网卡对应一个网络，通过设置“端口镜”或加 HUB 等方式将通讯数据搜集过来，关于设置端口镜像和过滤网卡部分请参考<情形 3>。

选择捕包网卡 / 过滤网卡

见<图 2>，用户可以同时选择多块网卡作为“捕包网卡”；绝大多数情况下，捕包网卡只有一块，但可能存在特殊情况，需要通过多块网卡才能捕获到需要的网络通讯，这时，就需要选多块捕包网卡，如上面提到的网络结构<情形 4>。

如果因为设置“端口镜像”导致不能对目标机进行封堵，则用户还必须通过“添加网卡”来达到封堵的目的。这时，请针对“捕包网卡”设置对应的过滤网卡，见下图：



<图 7>

启动监控服务

见前面的<图 3>，双击选中的后台服务程序，以启动或停止它。针对不同的服务，对其功能做个介绍：

《监控服务》功能：监视/控制常见的网络活动和外发资料，更新机器列表。

《数据通讯服务》功能：负责处理远程客户机查阅监控日志的请求。

《NAT/网桥服务》功能：实现 NAT/或网络桥/或虚拟网桥等功能。

《看管服务》功能：监视其他服务运行情况，处理报警信息。

检验“监视 / 过滤”效果

严格按照前面提到的方式安装并配置完成后，这时用户就可以体验监控效果了：

1、监视功能

前面<快速启动>部分已经提到。


2、过滤功能

用鼠标选中某一台要测试的电脑，确认其状态为监控状态[✔]，检查其“过滤规则”，缺省为<空>状态，选择已有过滤规则：“只允许访问 Google”，如下图，按下“保存设置”按钮。保存后，在电脑列表中出现已经设置好的规则。



这时，规则只允许当前电脑访问 google 网站，而其他网站则被过滤掉。

<图 8>

让被控电脑上网，检验预期效果，另外，为了确认系统是否做过封堵操作，同样可打开

“现场观察”窗口，进入“过滤”显示栏目，并观察是否有封堵记录。

当设置过滤规则后，电脑会显示规则名：

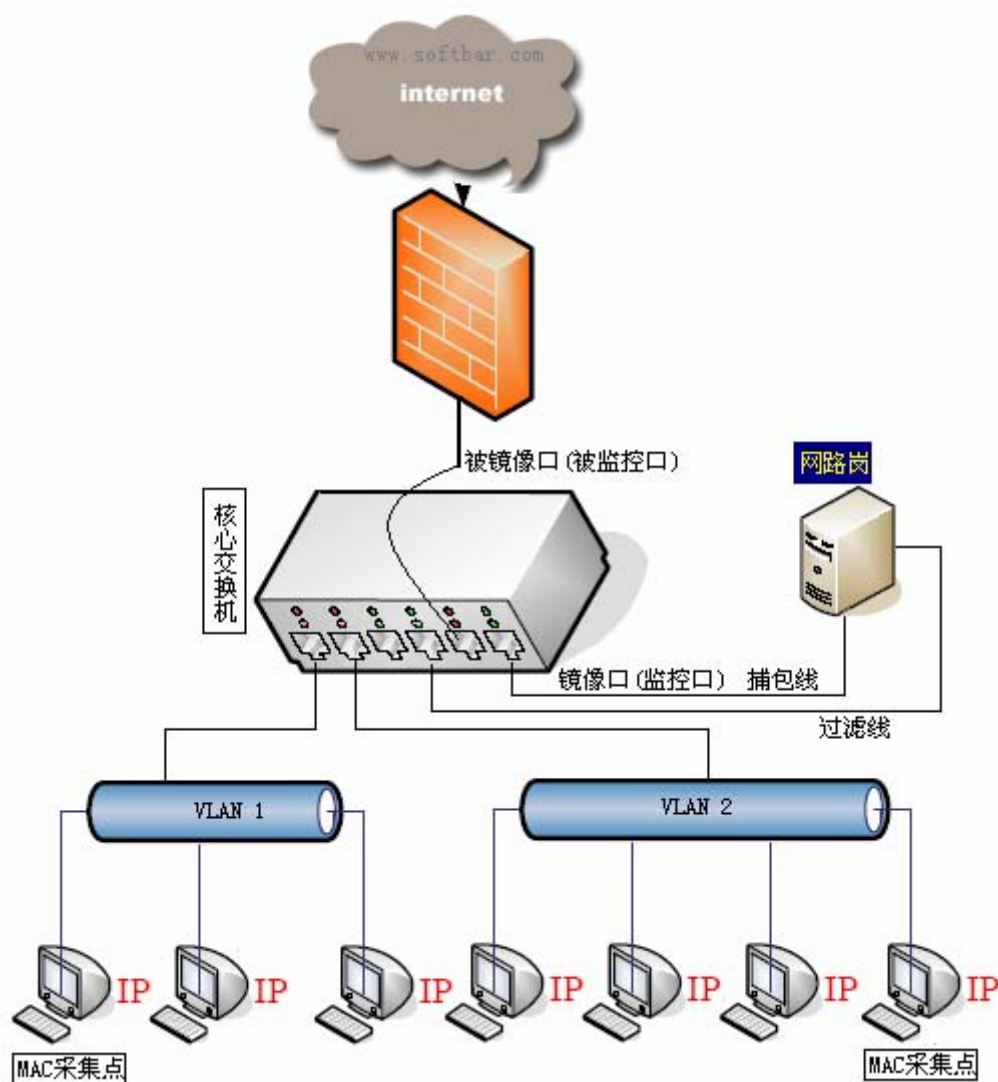
  dbfan [IP:192.168.0.103][MAC:00174208E856]{只允许上google(测试用)}

第三章：基于 MAC 的跨 VLAN 监控

最常见的跨 VLAN 结构及安装图。

如下图：被控目标机器位于 VLAN1 VLAN2 VLAN3... ..中。

镜像口/被镜像口/过滤网络线口位于 VLAN0 中，VLAN0 被当作“管理 VLAN”，最高级别，最靠近 Internet。



<图 9>

跨 VLAN 监控常用俗语

端口镜像：将交换机的某一网口网络通讯数据拷贝到另一个端口，源网口称为“镜像端口/监控口”，目的网口称为“被镜像端口/被监控口”。如果设置“端口镜像”后，电脑无法通过监控网口和网络内其他电脑发生通讯，这种情况通常被称为“单向接受模式”。CISCO 交换机属于这类情况，但也有做了“端口镜像”后，仍可以通讯的，如 TPLINK-SF2008 等。

MAC 采集点：是一个用以采集其所在 VLAN 内其他电脑网卡地址信息的小程序，不需要做任何配置，能和监控机主动通讯，及时上报 VLAN 内的 MAC 地址信息。

该程序并非必不可少，只不过有了它，监控机对信息的采集更及时、准确。MAC 采集程序一般在每个 VLAN 投放一个，如果被投放的电脑经常关机，则也可同时投放多个采集程序到同一 VLAN。

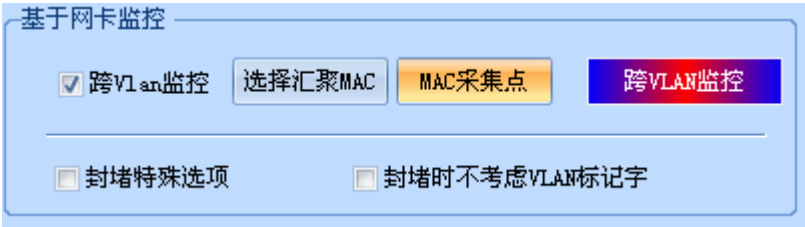
过滤专用网卡：为了将过滤信息包发送到交换机，网路岗需要一块能和其他电脑正常通讯的网卡，这块网卡就是“过滤专用网卡”。过滤网卡必须和被监控口位于同一 VLAN 中。

汇聚 MAC：被监控目标电脑发出的通讯包跨 VLAN 后，数据包发生改变，网卡地址被统

一修改为某个特殊的 MAC，这个 MAC 称为“汇聚 MAC”，“汇聚 MAC”地址由系统自动探测，但需要用户手动选取。

跨 VLAN 监控时的软件配置

选好捕包网卡，启动<网络活动监控服务>，进入系统“设置”栏目，打开“杂项”设置，如下图：



<图 10>

选择跨 VLAN 监控，系统自动打开“汇聚 MAC”的设置部分，保持该窗口处于打开状态，定期按下“刷新”按钮，如果系统探测出“汇聚 MAC”，会自动显示出来；用户将显示的汇聚 MAC 加入到汇聚 MAC 列表中；如果网内电脑上网活跃，则很快能搜集出所有的汇聚 MAC，首次进行设置时，建议保持该窗口打开 10 分钟以保证搜集出所有汇聚 MAC。

如果用户在网内其他电脑上安装有“MAC 采集点”，则很快就能被系统探测出来，并列出来采集点的 IP 地址。

另外，某些交换机 VLAN 通讯比较特殊，需要选中“封堵特殊选项”和“封堵时不考虑 VLAN 标记”。

至此，跨 VLAN 监控的配置基本完成。

最后，考虑到涉及到跨 VLAN 的用户，通常其监控目标也较多，电脑列表中会出现非常多的电脑，如果电脑全部搜集到一个“群组”下面，管理起来比较困难，所以，第七代提供了专门的“新电脑自动归类”处理机智，如下图：



<图 11>

第四章：监控模式：基于 MAC/帐户/IP

“基于网卡”的监控模式

MAC 地址及其获取方法

网卡地址也称 MAC 地址，就是在媒体接入层上使用的地址，通俗点说就是网卡的物理地址，现在的 Mac 地址一般都采用 6 字节 48bit（在早期还有 2 字节 16bit 的 Mac 地址），MAC 地址被习惯地用 12 位数字和字母组成，如：00E018D3C239。

获取网卡 MAC 方法比较多，在 Win9x 可用 WinIPcfg 获得，在 2000、XP 可用命令：IPconfig -all 获得。

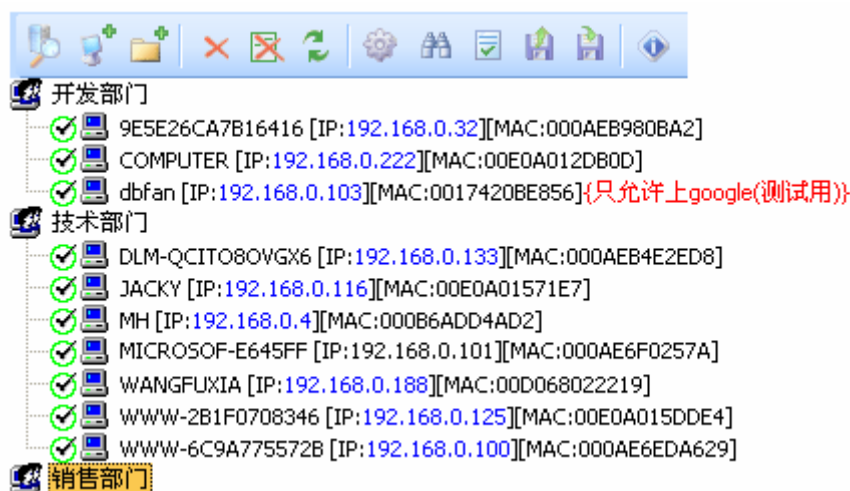
基于网卡监控的含义

“基于网卡”监控就是以网卡 MAC 为依据，根据网卡 MAC 地址确定被监控的信息内容的身份。由于每台机器的网卡 MAC 相对固定，用户不易修改，因此我们建议用户将该网络监控模式列为首选。

在这种网络监控模式下，用户更换新的网卡后，网路岗会重新检测到新的 MAC，因此，新网卡将被当作新加入的机器来处理。

管理电脑列表

见下图：



<图 12>

隐藏操作提示：

点鼠标右键，可弹出菜单。

选中电脑并拖动，可改变其所在群组。

关键词：网络监控软件，网络管理软件，内网管理，上网管理软件，网络岗，邮件监控软件，聊天监控

点击电脑前面的状态小图标，可直接改变其监控状态。

双击单台电脑，会弹出电脑信息编辑窗口。

对列表的操作不需要按下“保存设置”按钮，每次改动立即生效。

跨 VLAN

基于 MAC 的跨 VLAN 监控被很多客户采用，新产品也有较大的改进。这类监控相对比较复杂（捕包难、过滤难），但网路岗新版比较完美地解决了该问题。具体实施请参考前面第三章。

这里补充说明以下几点：

1. 电脑列表中可能会出现类似“?00192168011”这样的 MAC 地址，用户不必担心，这个 MAC 只是临时 MAC，是系统没有真正获取到 MAC 地址前临时分配的，一旦找到系统会自动更改过来。

2. 有效利用 MAC 采集点程序（MacDetect.exe），投放 MAC 采集程序到选定监控的 VLAN 中某台电脑。这个程序只是辅助获取所在 VLAN 所有电脑的 MAC 地址，也并非必须安装。此程序设计巧妙，体积小且不占用 CPU，也不需进行任何设置，点击运行即可。

3. 建议设置“新电脑自动归类处理”机制，如上面的<图 11>：

“基于帐户”的监控模式

“基于帐户”启用后，被控电脑浏览网页时，会弹出身份认证窗口，如下图：



<图 13>

基于帐户的客户端如何修改密码？

基于帐户功能需要用户打开“上网评价”功能，上网评价客户端可以修改上网密码。

当一台电脑重启后，该账户自动注销；也可手动注销：



上网评价客户端

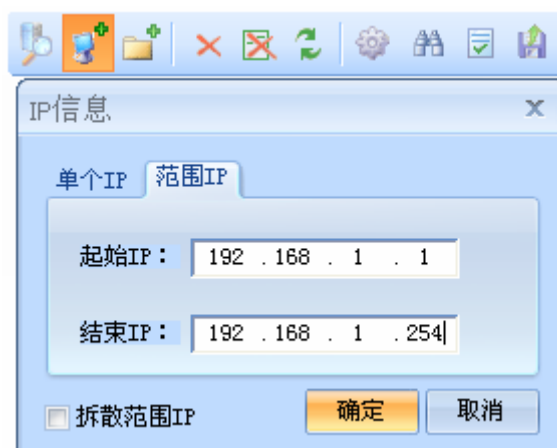
用户必须通过身份验证才可以正常上网，这类方式特别适合酒店行业。比如：客人来后，临时分配一个密码给它，而帐户名称就是其“房间编号”。

“基于帐户”监控时,建议用“非旁路”安装方式，如：“网络桥（双网卡）”，即“一进一出”的方式；或选用“网路岗 NAT”方式。之所以建议采用这两类方式，主要是考虑到这两类方式对数据包的控制非常有效，而“旁路”的模式对 UDP 封包很困难。

“基于 IP”的监控模式

“基于 IP”的监控主要应用在大型网络，比如 5000 台电脑以上；这类客户网络的特点是：网络复杂、电脑数量多、可能有多级 NAT，客户监控目的主要是留下监控日志，并做简单过滤规则。

因为电脑数量巨大，在电脑列表中如果列出所有电脑的 IP，则管理十分繁琐，所以，我们建议用户手动输入“IP 范围”作为监控目标，如下图：



<图 14>

“基于 IP”也可以启用“新电脑自动归类”机制，见前<图 11>。

在监控电脑数量比较大时，除了要求监控机配置相对较高外，还需要根据实际情况调整捕包缓冲区的大小，如下图：



<图 15>

监控方式的选择

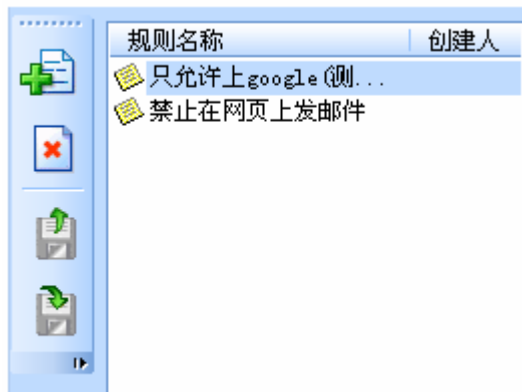
“基于网卡”是我们主要推荐的一种监控方式，适合网络规模在 5000 台电脑以下。

“基于 IP”监控主要用于电脑规模大、控制要求不高的网络；基于 IP 监控时，用户可以定义范围 IP，以简化对监控目标的管理。

“基于帐户”主要针对一些特殊行业，比如酒店、宾馆等。

第五章：过滤规则

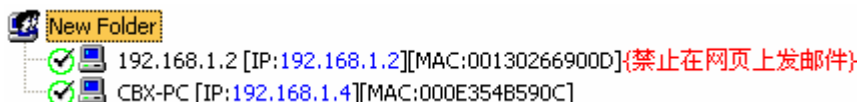
选中某台电脑，打开“过滤规则”，如下图：



<图 16>

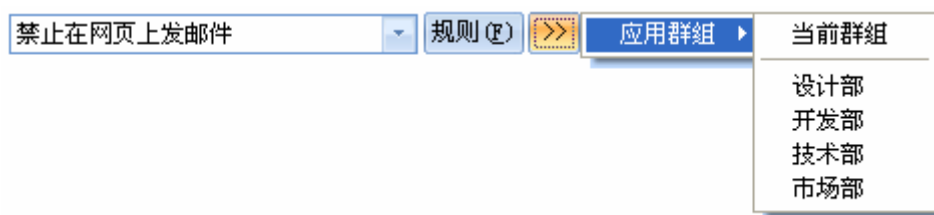
见上图，用户可一次性定义多个“不同上网级别”的过滤规则，以便分配给被控电脑。建议用系统提供的“导出”“导入”功能来备份或恢复设置好的过滤规则，以减轻重装电脑或系统时带来的麻烦。

分配了过滤规则的电脑，过滤规则名称会以红色标记出来，如下图：



<图 17>

如果电脑比较多，针对单个电脑进行分配过滤规则时可能会很麻烦，为较少工作量，用户可一次性将某个规则应用到一个群组，如下图：



<图 18>

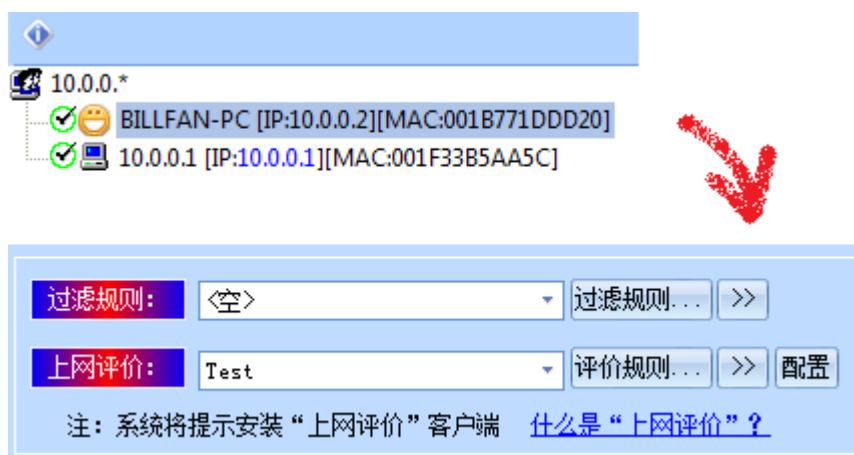
第六章：上网评价

“上网评价”是网路岗第七代产品新功能，上网评价内容由系统自动给出或由管理者给出；评价的内容会实时通知被监控者，因而启动该功能后，单位内的上网人员可能随时收到一份来自服务器的评价；比如：访问了黄色网站、上了开心农场、访问财经网站等等。

“上网评价”让被监控者随时知道自己的上网行为被关注，使管理更具人性化。

如何设置才能启动上网评价功能？

选中电脑，设置上网评价规则；



设置完成后，当客户电脑浏览网页时，会自动转到下载“上网评价”客户端的页面；缺省情况下，该下载页面位于 <http://www.softbar.com/pj> 目录，用户也可以把该页面转到用户自己的网页服务器上，这样就避免客

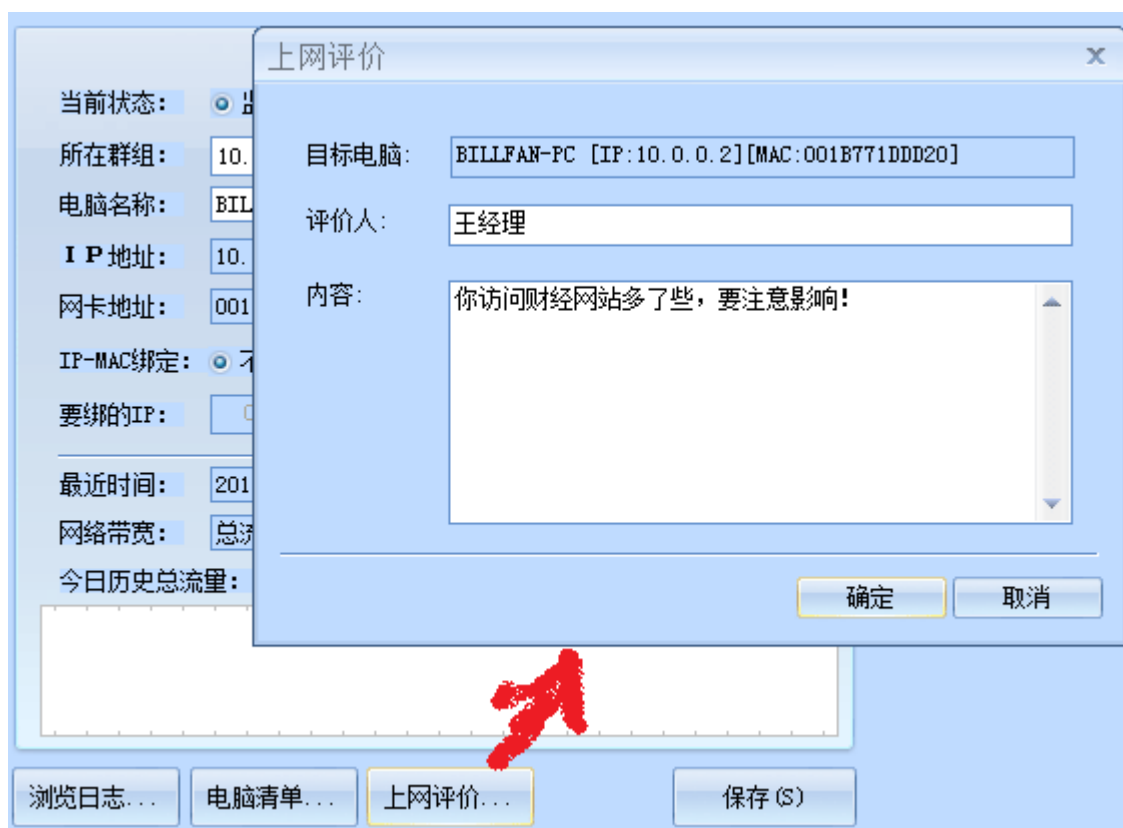
关键词：网络监控软件，网络管理软件，内网管理，上网管理软件，网络岗，邮件监控软件，聊天监控

户电脑访问我们的网站。

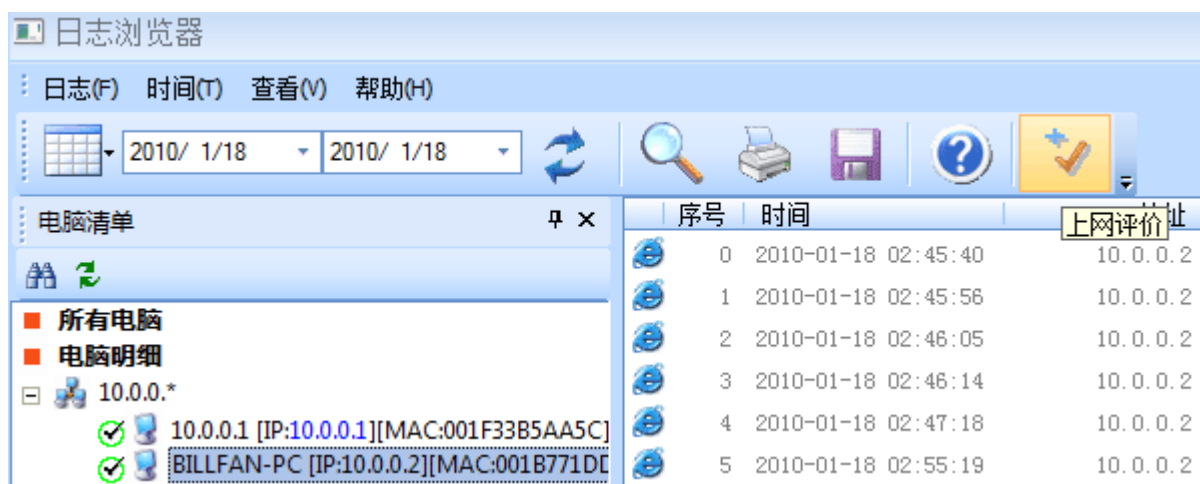
客户机安装“上网评价”客户端后，上网才能正常，且其桌面上会出现平价工具条，如下图：



管理人员手动评价



或在浏览日志的时候评价：



第七章：报警

“报警”是指对符合特定条件的网络行为，及时通过短信、邮件、声音三种方式实现的紧急通知功能。

报警的方式有三种：GSM 短信报警、邮件报警、声音报警。打开报警选项，如下图：



<图 19>

报警点：（保留项，为“报警中心管理系统”预留项）。

报警功能由后台“看管服务”实现，所以务必启用“看管服务”，出现新的报警信息时候，桌面系统工具条上“看管服务”小图标不停地闪烁。

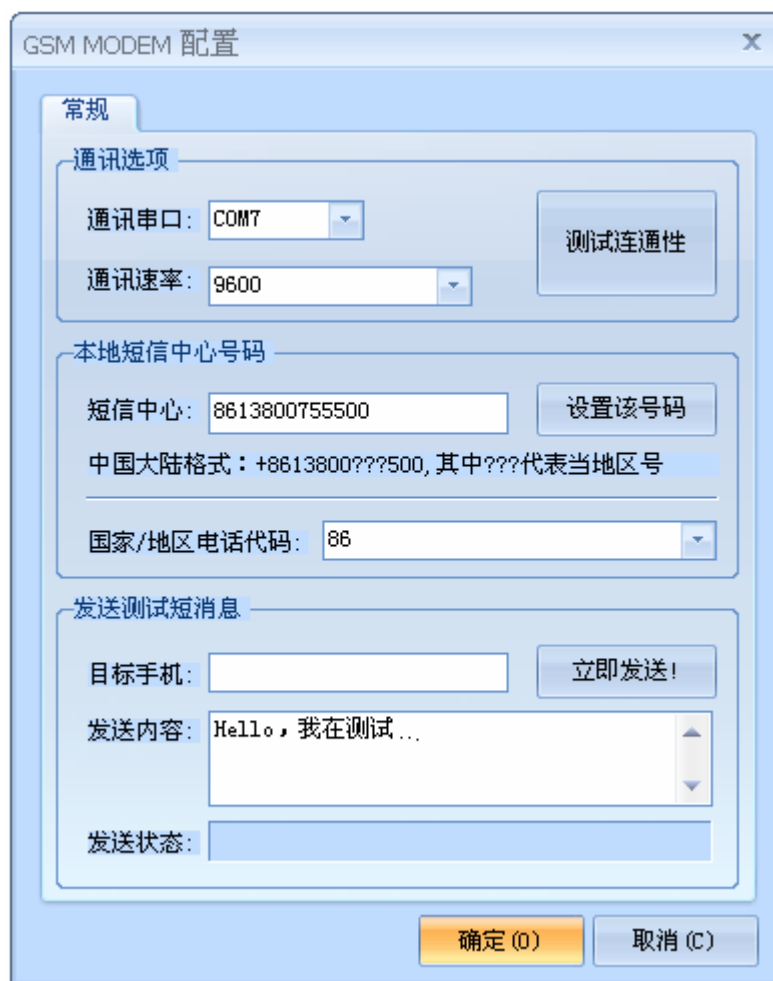
GSM 短信报警

短信报警需要专门的 GSM 报警设备，该配件由用户自行选购。除购买报警短信发送设备外，用户还需要在当地购买一手机卡。

连接报警设备的方式有两类，一种是 USB 接口，另一种是电脑串口，两种连线同时提供给客户选用。

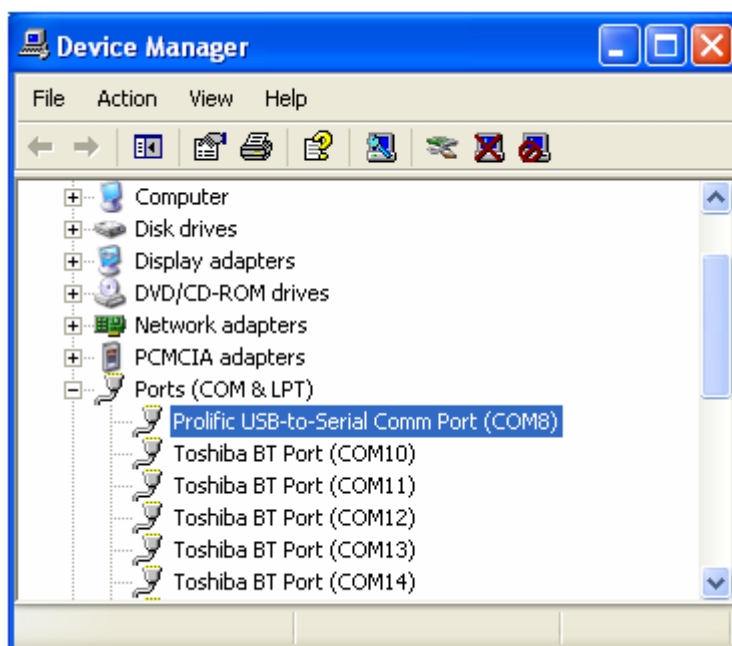
短信设备的具体安装详见产品包装盒中“GSM 报警设备”安装说明单页。

如果你选择用 USB 的接口方式，那么您还需要安装相应的“USB-串口”驱动程序，驱动程序位于安装 CD 的 USB Driver 目录下。当您成功安装报警设备之后，接下来的工作就是对报警设备进行配置。配置窗口如下：



<图 20>

见上图：通讯速率通常为 9600，通讯串口在不同的电脑上可能不一样，如果您用的是串口线，那么需要从 COM1 开始逐个进行测试；如果您用的是 USB 接线方式，那么建议您在桌面上的“我的电脑”上点鼠标右键，在弹出的菜单中选择“属性”－“硬件”－“设备管理”，见下面的窗口：



上图显示：USB 转串口的虚拟串口为 COM8，因此 COM8 就是我们要设的串口。

短信中心号码一般在用户“测试连通性”时由系统自动从手机卡中读取。在中国大陆，短信中心的号码有一定规律，+8613800XXX500，其中 XXX 为当地区号，如北京：010,深圳:755。

配置完毕，用户可以试着发一条消息，检查设置是否正确。

邮件报警

打开“邮件设置”窗口：



填写相应的邮件服务器及接受报警的邮箱等信息,因常用的邮件服务器均需要验证身份,故需要用户名称和用户密码。注:一些邮件服务器的用户名称为邮箱全名

设置完毕后,请进行“发送测试”,如果发送失败,建议参考邮件服务器的网上帮助进行设置。

声音报警

打开“报警声音设置”:



有新的报警信息,且启用了声音报警选项,则系统播放上面设置的音效。在桌面系统工具条上的“看管服务”小图标自动闪烁,在小图标上点鼠标右键,用户可以快速关闭声音报警功能。

关键词: 网络监控软件, 网络管理软件, 内网管理, 上网管理软件, 网络岗, 邮件监控软件, 聊天监控

第八章：网路岗 NAT 及网桥

NAT 基本知识

什么是 NAT？

网络地址转换 (NAT) 是一个 Internet 工程任务组 (Internet Engineering Task Force, IETF) 标准, 用于允许专用网络上的多台 PC (使用专用地址段, 例如 10.0.x.x、192.168.x.x、172.x.x.x) 共享单个、全局路由的 IPv4 地址。IPv4 地址日益不足是经常部署 NAT 的一个主要原因。Windows XP 和 Windows Me 中的“Internet 连接共享”及许多 Internet 网关设备都使用 NAT, 尤其是在通过 ADSL 或电缆调制解调器连接宽带网的情况下。

NAT 对于解决 IPv4 地址耗费问题 (在 IPv6 部署中却没必要) 尽管很有效, 但毕竟属于临时性的解决方案。这种 IPv4 地址占用问题在亚洲及世界其他一些地方已比较严重, 且日渐成为北美地区需要关注的问题。这就是人们为什么长久以来一直关注使用 IPv6 来克服这个问题的原因所在。

除了减少所需的 IPv4 地址外, 由于专用网络之外的所有主机都通过一个共享的 IP 地址来监控通信, 因此 NAT 还为专用网络提供了一个隐匿层。NAT 与防火墙或代理服务器不同, 但它确实有利于安全。

网路岗 NAT 适用环境:

- 1.双网卡:一个接 Internet, 一个接内网。
- 2.单网卡+电话线拨号。
- 3.单网卡+ADSL Modem。

网路岗 NAT 介绍

网路岗 NAT 的实现并非依赖于 Windows 已有的内部功能,而是完全自主开发,并参考了常见的 NAT 标准,在提高地址转化速度上做了比较理想的改进工作,使其最大限度地减少系统资源占用和提高运行效率,并能和网路岗有效地结合,真正实现并行监控与串行过滤的完美结合。

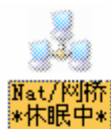
网路岗 NAT 配置十分简单,大部分工作由系统自动探测部分完成。

如果采用网路岗 NAT, 在不影响用户上网速度的前提下, 用户能很好地对聊天软件和 p2p 下载软件进行过滤。

启用网路岗 NAT

OS 系统要求: Windows 2000/XP/2003

用户安装《网路岗》产品后, 一定要重启机器, 否则 NAT 不会生效, 重启后, 见下图, 点击后台服务“NAT/网桥”, 弹出菜单, 请选择“启用共享上网 NAT”项, 然后进入 NAT 配置画面进行相关配置。



安装后的配置：

进入配置画面，选择正确的内网网卡，外网卡由系统自己探测，如果用户机器只有一块网卡，那么系统会提示错误信息。

配置成功后，我们一般建议客户机将“网关”和“DNS”指向该安装 NAT 的机器。

1、选择本地网卡，也就是内网网卡。如果该网卡同时配置多个内部 IP，那么第一个 IP 地址及掩码所代表的网段就是能被共享的网段。

2、外网卡，系统自动探测，但用户必须首先保证该机器已能上网。

网桥和虚拟网桥

网络桥：

我们常见的是透明网桥，在 WINDOWS XP 和 2003 系统中自带该功能，需要两块网卡实现，“网路岗”同样提供“网络桥”功能，启用网路岗“网络桥”时候，请删除系统自带的网络桥。



虚拟网桥：

关键词：网络监控软件，网络管理软件，内网管理，上网管理软件，网络岗，邮件监控软件，聊天监控

“虚拟网桥”实际上是“网路岗”为一种“网络监控技术”而命名的一个技术名词。和实际“网桥”概念完全不同，仅仅因为其通迅过程类似“网桥”罢了。

通常意义上的“网桥”一般需要两块网卡来实现，而这里所谓的“虚拟网桥”只需要一块网卡。

要达到一台机器监控整个网络的目的，只需要启用“虚拟网桥”功能就可以了，这种监控技术可以在纯交换机环境下实现，不需要添加 HUB，也不需要设置镜像端口。行话称之为“装在任何一台电脑上就可以监控整个网络”。

而实际使用中，该技术的缺点非常明显，虽然“网路岗”已经加入该技术，但有必要向客户交代其中问题所在。

缺点 1：客户机盲目安装。

既然装在任何一台电脑就可以实现对整个网络的监控，员工或学生是否会随意下载、随意安装、随意监控？这是完全可能的，因为毕竟实现监控的门槛太低。不过，当同时多台机器启用这类监控方式后，网络会出现紊乱状况，很可能导致无法上网。

缺点 2：很容易逃避监控

所有采用类似监控技术的产品，均需要发送 ARP 欺骗包，以使正常上网路径发生改变。但是象瑞星等杀毒软件可以识别并抛弃 ARP 欺骗包，使对本机的监控不能得逞。另外用户也可以通过添加静态路由轻松避免被监控。

因此，在单网段环境下，我们建议客户仍然采用传统的“监控手段”。如果客户执意采用该监控手段，那么请注意：“网路岗”可以自动探测出网内其他机器是否启用过类似的监控手段(也许是其他监控产品)，并记录在历史记录中。

第九章：常见问题解答

一、《网路岗》分为哪些不同的版本？

按应用行业分：企业版/校园版/城域网版

按功能分：专业版/标准版/审计版

专业版具备所有功能，标准版不具备“外发资料监控”功能，不具备内网管控功能，网路审计专版只记录常见的网络日志，不能对电脑进行过滤控制。

二、《网路岗》，享有哪些服务？

您购买《网路岗》后，可以在工作时间通过邮件/电话等方式咨询相关技术问题，并享有一年内产品免费升级服务。

三、为什么选用《网路岗》，和同类网络监控产品相比，《网路岗》有什么优势？

“网路岗”一代产品于 2002 年问世，至今已是第七代产品；经过几次换代升级，产品已十分稳定成熟。

“网路岗”对 QQ 内容监控做的很好，该监控不需要客户端支持。

“网路岗”同时具备 Internet 管理和内网管理功能，还能截取目标电脑屏幕。

“网路岗”具有国内领先的邮件监控技术和国内领先的聊天监控技术；对各类复杂网络环境的适应能力也是首屈一指。不仅功能强大、界面友好、操作方便，其领先的监控技术和快速的产品升级能力使其在众多的监控产品中脱颖而出！

四、网络监控产品是用硬件好，还是用软件好？

网络监控类产品是用硬件还是用软件，主要取决于两点：

1、网络规模

2、功能要求

我们的建议是：网络规模大用软件，功能要求多用软件，小规模、少功能且不考虑产品价格的前提下，可以考虑硬件产品。

《网路岗》客户中，目前同一网络内,监控点最多的将近 1 万个点，处理能力是一般硬件产品无法做到的。

市面上硬件网络产品的确具有很广泛的应用，比如防火墙、路由器等，和软件相比，硬件产品的价格通常要高出很多，不过，细心的用户会发现：硬件产品在实际应用中，所用到的功能往往比较简单。就拿一些知名品牌防火墙的过滤功能来说，尽管其说明书上列出诸多规则设置，但如果用户真正启用这些功能时，当在线电脑稍多时，其上网速度会变得明显缓慢。硬件产品所采用的过滤模式为转发式过滤方式，当网络通讯量比较大时，普通硬件的 CPU 处理能力无法适应网络实时通讯的要求，造成通讯瓶颈现象。

功能完善的网络监控产品必然会分析大量的通讯数据包，同时也要求 CPU 应具备很强的处理能力，针对大型的网络（比如大学校园网），至少需要奔腾 4 以上 CPU 来处理；另外，硬盘的存储空间也很重要，就拿邮件监控的功能来说，如果有 100 台机器每天收发邮件，其日志量应该在 300M 左右，一个月的邮件日志量就应该在 10G 左右；可想而知，如果让一款硬件产品来实现该功能的话，的确有些捉襟见肘了。

我们这里提到的硬件产品指的是已将软件固化到芯片中的网络设备，市面上出现的一些“高配置硬件”是“能自动启动的无显示器的 PC 主机”，不能算是真正的硬件产品。

以“网路岗”为代表的软件产品，能及时追随新的监控/反监控技术，快速升级产品。并且，这些产品大都采用并行监控技术，对网络速度影响甚小，在监控类产品所发挥的作用是有目共睹的。

五、《网路岗》是黑客软件吗？它容易被人利用吗？

不是。该产品在监控网络活动的同时,已经将个人密码等关键信息严格过滤掉，另外我们提供的试用版也限制了一些功能：如不能查看别人的邮件内容等措施；我们决不会将该产品卖给个人或从事不法活动的团体组织等。所以本产品不容易被人利用。

六、以前产品的日志和配置文件七代可以用吗？两者可以共存吗？

两者可以同时运行在一台电脑上，其安装目录不同，后台服务程序也不一样。

早期产品产生的日志文件在七代产品中可以打开；但配置文件不能重用。

七、如何对《网路岗》进行远程管理？

建议客户使用 Windows 自带的“远程桌面管理”来远程操作《网路岗》。