your future life

侠诺神捕 QnoSniff
专业版 2.0

简体中文使用手册

目 录

产品功能说明手册使用许可协议

《产品功能说明手册（以下称”手册”）使用许可协议》（以下称”协议”）是用户与侠诺科技股份有限公司（以下称”侠诺”）关于手册许可使用及相关方面的权利义务、以及免除或者限制侠诺责任的免责条款。直接或间接取得本手册档案以及享有相关服务的用户，都必须遵守此协议。

重要须知：侠诺在此提醒用户在下载、阅读手册前阅读本《协议》中各条款。请您审阅并选择接受或不接受本《协议》。除非您接受本《协议》条款，否则请您退回本手册及其相关服务。您的下载、阅读等使用行为将视为对本《协议》的接受，并同意接受本《协议》各项条款的约束。

【1】知识产权声明

手册内任何文字表述及其组合、图标、界面设计、印刷材料、或电子文件等均受我国著作权法和国际著作权条约以及其它知识产权法律法规的保护。当用户复制"手册"时，也必须复制并标示此知识产权声明。否则，侠诺视其为侵权行为，将适时予以依法追究。

【2】"手册"授权范围：

用户可以在配套使用的计算机上安装、使用、显示、阅读本"手册"。

【3】用户使用须知

用户在遵守法律及本协议的前提下可依本《协议》使用本"手册"。用户若是违反本《协议》，侠诺将中止其使用权力并立即销毁此"手册"的复本。本手册"纸质或电子档案"，仅限于为信息和非商业或个人之目的使用，并且不得在任何网络计算机上复制或公布，也不得在任何媒体上传播;及不得对任何"档案"作任何修改。为任何其它目的之使用,均被法律明确禁止,并可导致严重的民事及刑事处罚。违反者将在可能的最大程度上受到指控。

【4】法律责任与免责声明

【4-1】侠诺将全力检查文字及图片中的错误，但对于可能出现的疏漏，用户或相关人士因此而遭受的直接或间接的经济损失、数据损毁或其它连带的商业损失，侠诺及其经销商与供货商不承担任何责任。

【4-2】侠诺为了保障公司业务发展和调整的自主权，侠诺拥有随时自行修改或中断软件 / 手册授权而不需通知用户的权利，产品升级或技术规格如有变化，恕不另行通知，如有必要，修改或中断会以通告形式公布于侠诺网站的相关版块。

【4-3】所有设置参数均为范例，仅供参考，您也可以对本手册提出意见或建议，我们会参考并在下一版本作出修正。

【4-4】本手册为解说同系列产品所有的功能设置方式，产品功能会按实际机种型号不同而有部份差异，因此部分功能可能不会出现在您所购买的产品上。

【4-5】侠诺保留此手册档案内容的修改权利，并且可能不会实时更新手册内容，欲进一步了解产品相关更新

讯息，请至侠诺官方网站浏览。

【4-6】侠诺（和/或）其各供货商特此声明，对所有与该信息有关的保证和条件不负任何责任，该保证和条件包括关于适销性、符合特定用途、所有权和非侵权的所有默示保证和条件。所提到的真实公司和产品的名称可能是其各自所有者的商标，侠诺（和/或）其各供货商不提供其它公司之产品或软件等。在任何情况下,在由于使用或档案上的信息所引起的或与该使用或运行有关的诉讼中，侠诺和/或其各供货商就因丧失使用、数据或利润所导致的任何特别的、间接的或衍生性的损失或任何种类的损失，均不负任何责任，无论该诉讼是合同之诉、疏忽或其它侵权行为之诉。

【5】其它条款

【5-1】本协议高于任何其它口头的说明或书面纪录，所定的任何条款的部分或全部无效者，不影响其它条款的效力。

【5-2】本协议的解释、效力及纠纷的解决，适用于台湾法律。若用户和侠诺之间发生任何纠纷或争议，首先应友好协商解决。若协商未果，用户在完全同意将纠纷或争议提交侠诺所在地法院管辖。中国则以「中国国际经济贸易仲裁委员会」为仲裁机构。

一、简介

QnoSniff 专业版 2.0 是一款工作于 PC 上的网络信息记录软件，透过和侠诺系列路由器的整合，对网络数据进行记录、过滤、分析，从中将用户关注的内容提取出来，并呈现出易于检视与阅读的数据格式，并生成统计图表与报表，提供企业或网络管理人员参考。

企业或网络管理人员经常遇到以下困扰－员工上网都在作什么?

员工上网不外乎用收发电子邮件 E-mail、浏览网页或搜寻网页信息、用 MSN/Skype 等即时通讯（IM）跟朋友闲聊、用 BT 等点对点传输（P2P）下载资料。其中，Email 与 IM 是泄密与病毒入侵的管道，而 P2P 更是频宽的杀手与间谍软件的温床。不但如此，IM 浪费上班人力在聊天，耗损的生产力更难以估计。然而 IM 可以节省通信成本，甚至增加沟通效率，许多企业已不得不开放。

QnoSniff 专业版针对企业用户的这些问题量身定制，其首要任务就是解决企业的网络问题。通过对网络信息的监控与记录，QnoSniff 专业版可以有效帮助企业管理人员解决由网络应用衍生出的各种问题。无论是上网记录，邮件记录还是聊天记录，下载文件，QnoSniff 专业版都可以分析整理的井井有条，检查起来非常方便。

QnoSniff 专业版不仅仅是为了管理而管理，它同时为企业用户带来了全新的【主动管理】的理念。传统的管理模式是被动管理，员工总是到被管理人员关注并通知甚至警告之后，才会约束自己的行为，由此容易让员工产生抵触情绪，而且会带来一些管理问题。

而 QnoSniff 专业版针对此情况，通过提供流量统计排名功能，让员工可以随时自己去查看各种网络应用的使用流量排名，例如聊天、下载等，当“榜上有名”时，员工看到就会进行自我约束，从而形成一种自我管理的概念。

流量统计排名同样也会将服务类型进行排序，以协助网管人员找到本地网络中用户的网络使用习惯，进而指导网络的设计和规划，更好的管理网络，实现企业工作效率的最大化。值得一提的是，QnoSniff 专业版还提供了 PDF 转文件以及电子邮件寄送功能，可以随时生成离线档案，发送给相关人员进行查看。

二、QnoSniff 专业版系统安装与配置

本章节介绍用户在安装之前的准备，以及整体的安装过程与 QnoSniff 的基本系统设置。

2.1 开始之前的准备

安装 QnoSniff 专业版的 PC，建议的最低系统需求：

1、 Intel P4 2.0GHz 以上 / AMD 同等级以上 CPU。

2、 操作系统：Windows 平台 (不包含 Windows 2000 以下版本)。

3、 空闲的硬盘空间 100G 以上。

4、 系统内存 RAM 2GB 以上。

必要的搭配布署

1、 需与侠诺路由器一同搭配运作。

2、 侠诺路由器需要有 Mirror Port 镜像端口功能。

3、 安装 QnoSniff 专业版软件的 PC 需要透过网卡与网线，连接侠诺路由器的镜像端口。

4、 必须将路由器的镜像端口 (Mirror Port) 功能启用。

5、 必须要将路由器的 SNMP 网络管理功能启用。

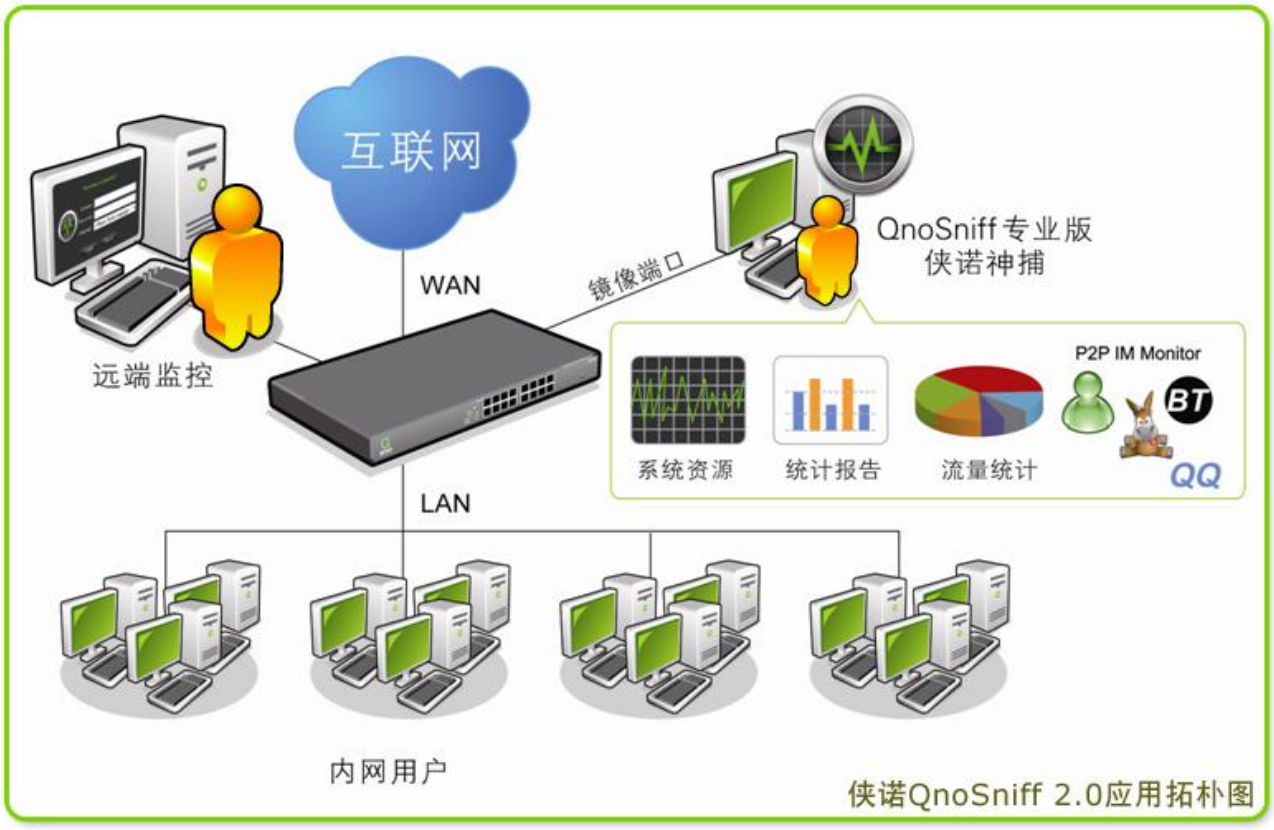
6、 必须将路由器许可证密钥功能的 QnoSniff 选项开启 (不论是试用还是正式版)。

2.2 QnoSniff 专业版安装过程中所需组件

QnoSniff 安装包内会有以下 QnoSniff 运作所需用的所有组件，但是若您的计算机已经有安装过这些组件，可能会需要移除 PC 内原本的原件版本，或是重新安装 / 升级成新的组件版本。

* Apache Server
* WinPcap
* .Net Framework
* PHP

2.3 布署连接范例拓朴图



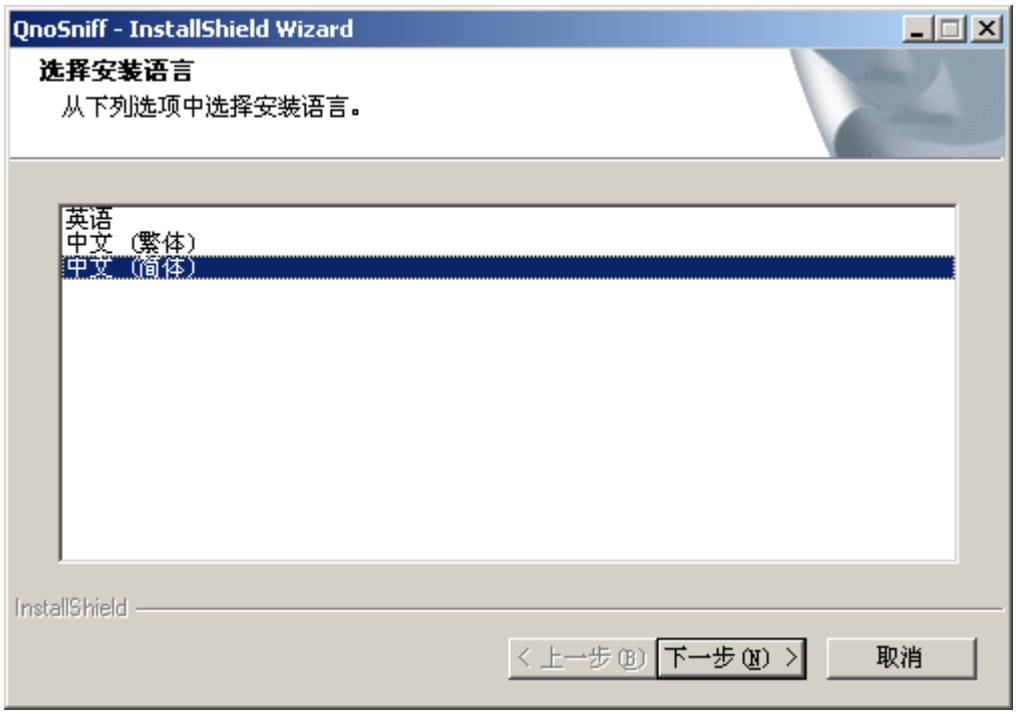
2.4 开始安装

请参照以下步骤安装到您的 PC 上

1.将 QnoSniff 专业版软件的光盘，放入您计算机的 CD 或 DVD 的读取装置中。

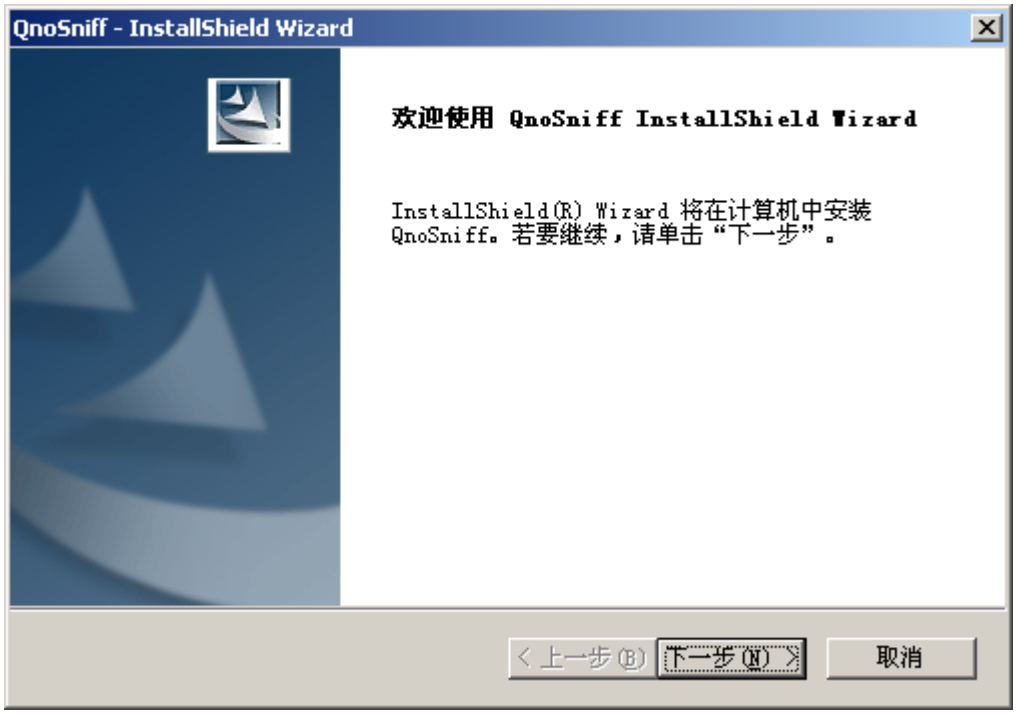
2.用鼠标点选安装档案  进行安装。(注：系统需要以最高权限管理用户身分进行安装)

3.【语系选择】开始安装程序后，首先会跳出选择语系页面，请选择您所使用的语系

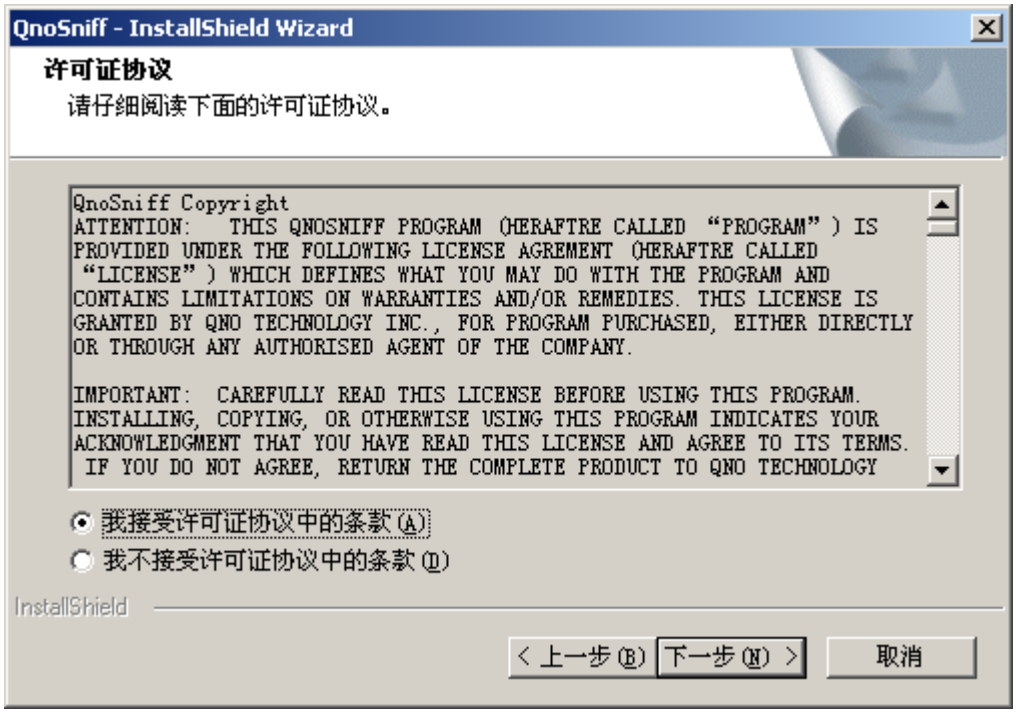


选择「下一步」继续安装，选择「取消」则取消安装程序。

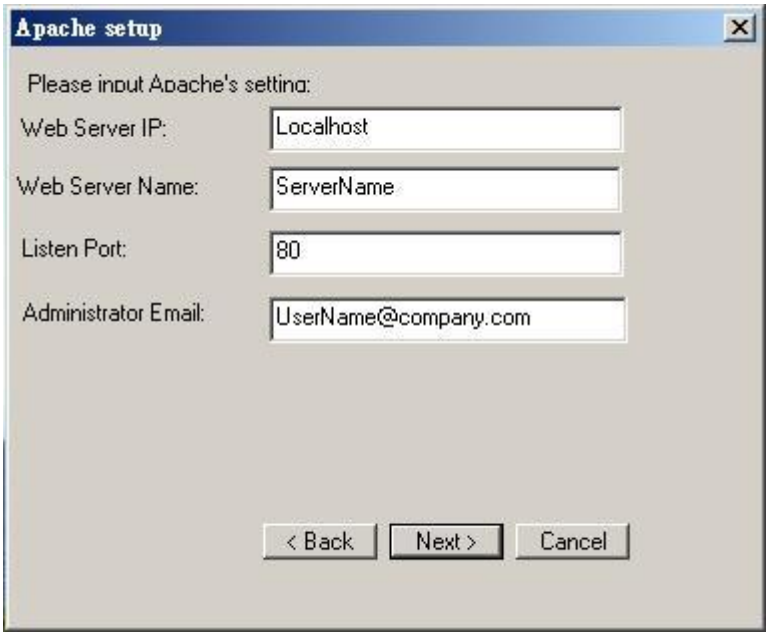
4.【欢迎页面】进入到欢迎安装页面，选择「下一步」继续安装，选择「取消」则取消安装程序。



5.【许可证协议】出现授权合约，请在仔细阅读后，点选「我接受许可证协议中的条款」，才能按「下一步」继续进行安装。



6.【Apache Server 安装】出现 Apache 服务器的安装设定页面，安装此服务器是用来让安装 QnoSniff 专业版的 PC 能够开启 Web 服务，使管理者或用户能够进行远程监控与存取，按「Next」继续进行安装程序



Web Server IP：表示 Web 服务器的 IP 地址，安装程序默认值会填写 Localhost，即 127.0.0.1

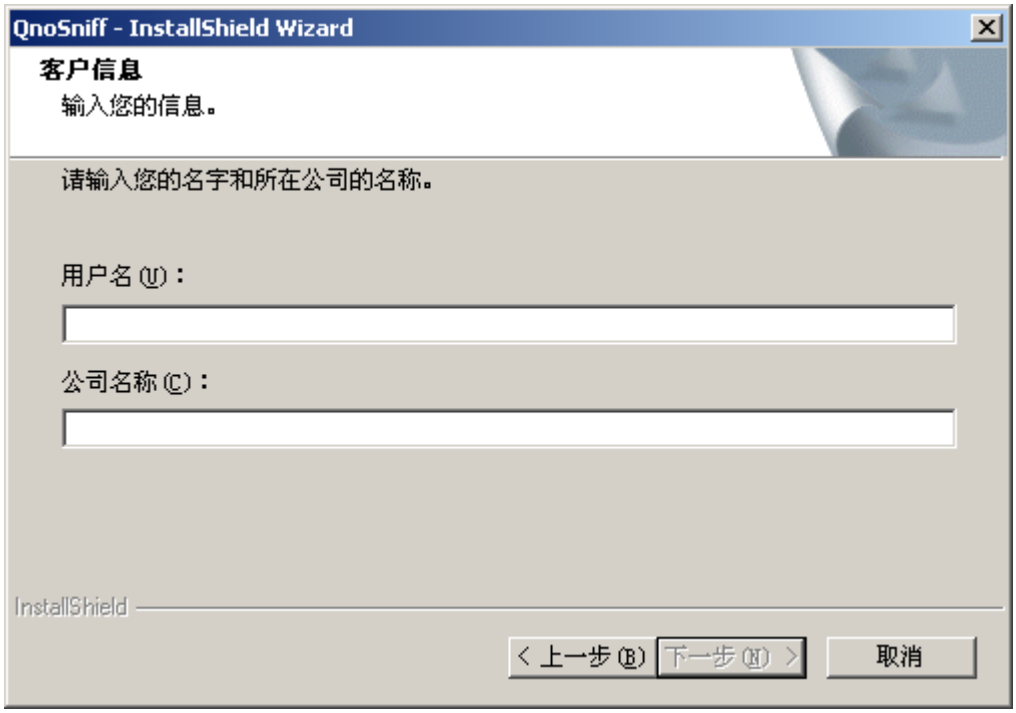
Web Server Name：表示 Web 服务器的名称

Listen Port：表示 Apache 服务器收送的通讯端口口，安装程序默认值填写 80 Port

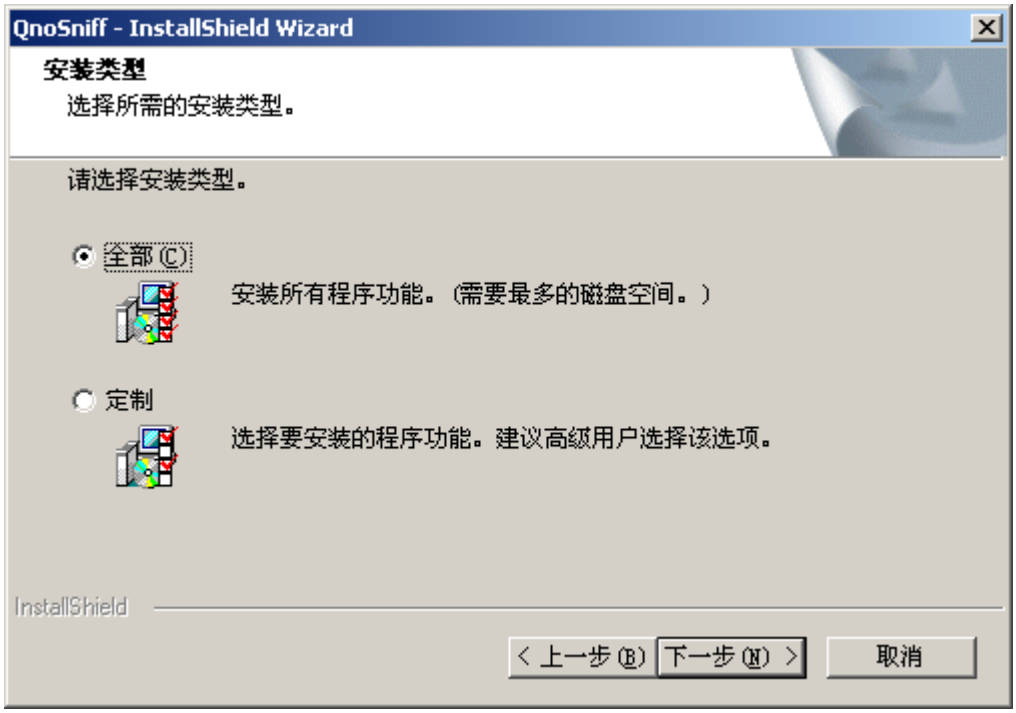
Administrator Email：表示 Administrator 权限的 Email，方便告知使用者重要讯息

设定完成后，请按「Next」继续进行安装程序

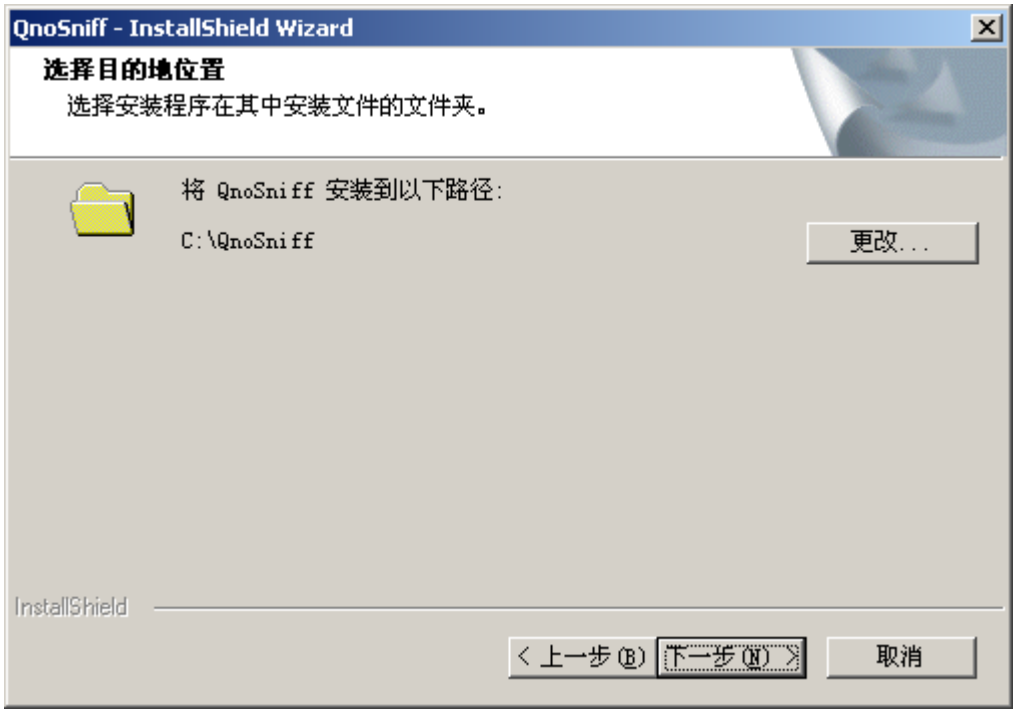
7.【客户信息】接着出现客户信息页面，麻烦请输入您的使用者名称以及公司名称，此两者皆须输入内容才能够按「下一步」继续进行安装程序



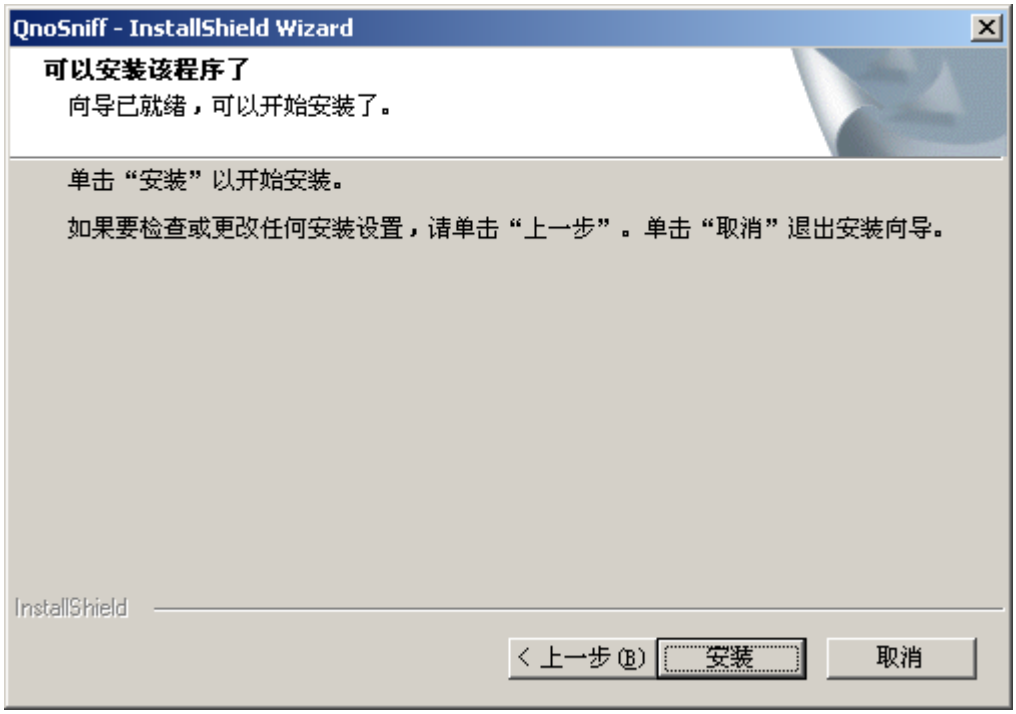
8.【安装类型】选择安装类型，选择全部是指安装所有程序的功能；选择自订是指可以选择程序的部分功能安装，以下显示图例选择安装类型为全部为例，目前在 QnoSniff 专业版 2.0 版本并没有其它全部安装与自订安装部分组件的差异，所以选择其中一个类型皆可。



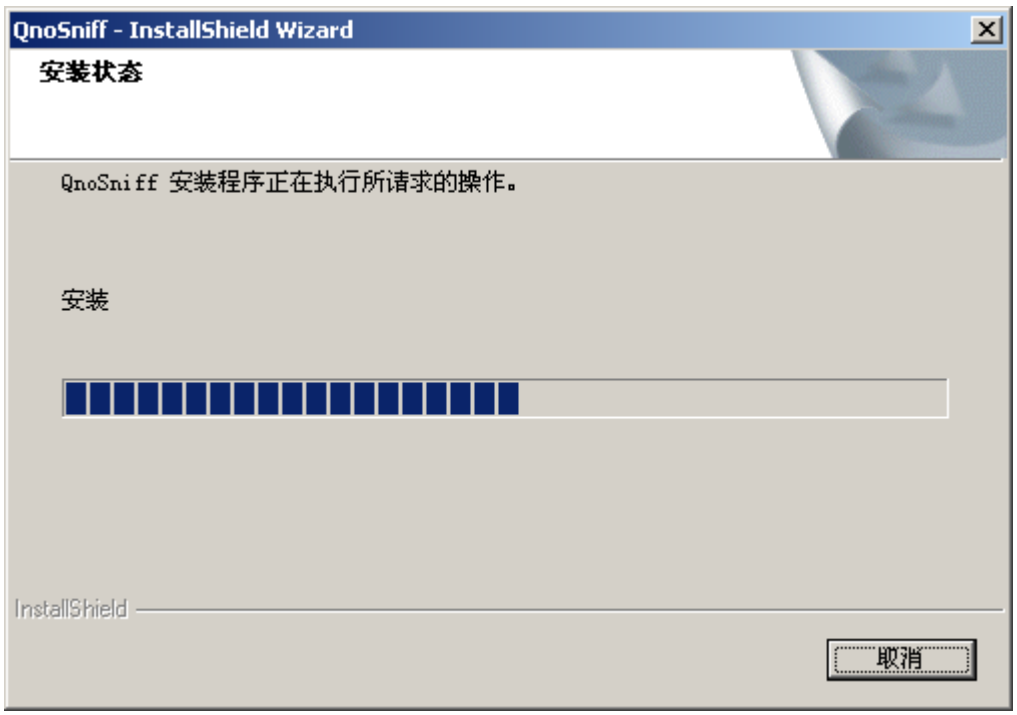
9.【程序安装路径】程序预设安装路径为 C:\QnoSniff，您可以按下「变更」按钮更改安装的档案夹路径，完成后按「下一步」进入开始安装页面。



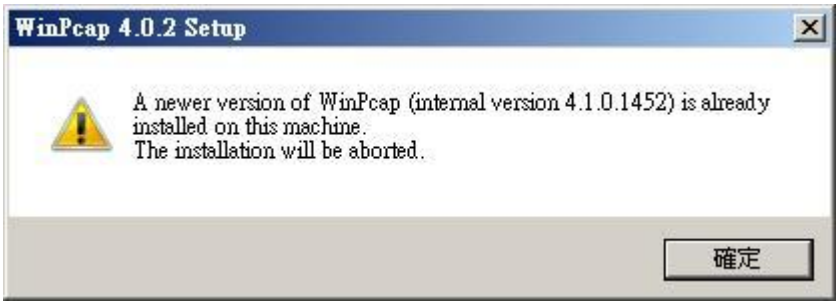
10.【开始安装】进入 QnoSniff 远程监控 (Web)本体程序安装程序，请按下「安装」开始。



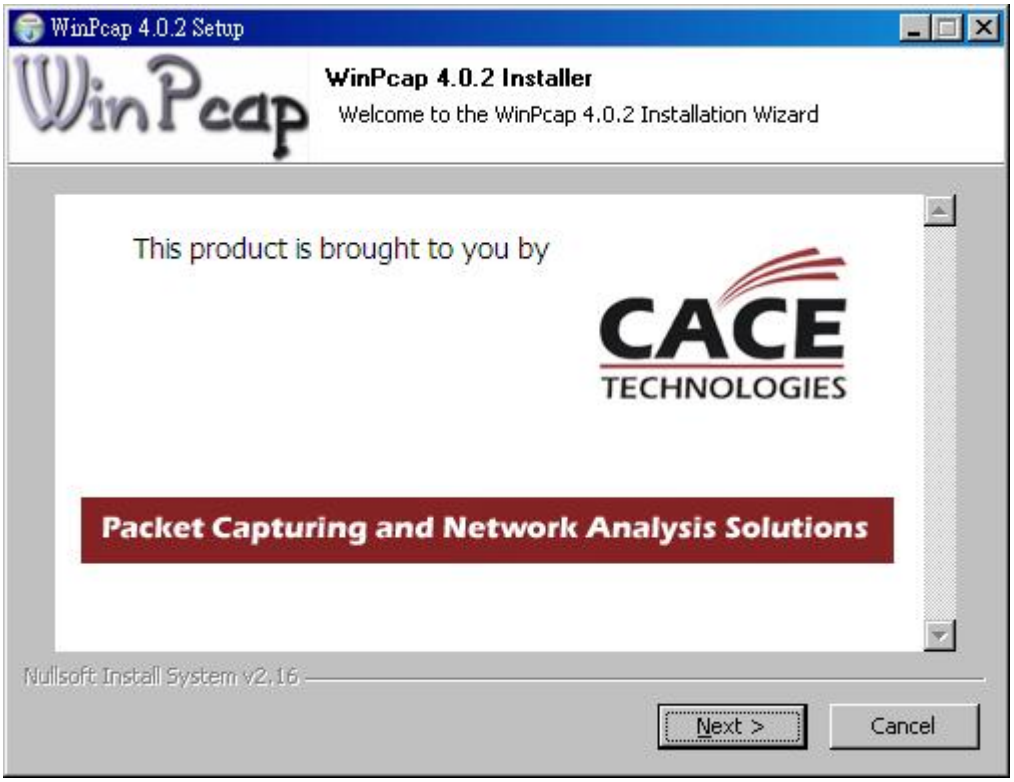
安装程序中



11.【安装 WinPcap】在以上的程序结束后，会接着安装 WinPcap 组件，若您的 PC 上已经有安装 WinPcap，并且比 QnoSniff 专业版安装包内的 WinPcap 版本更新的话，会出现警告讯息表示不用再安装并中断 WinPcap 的安装程序

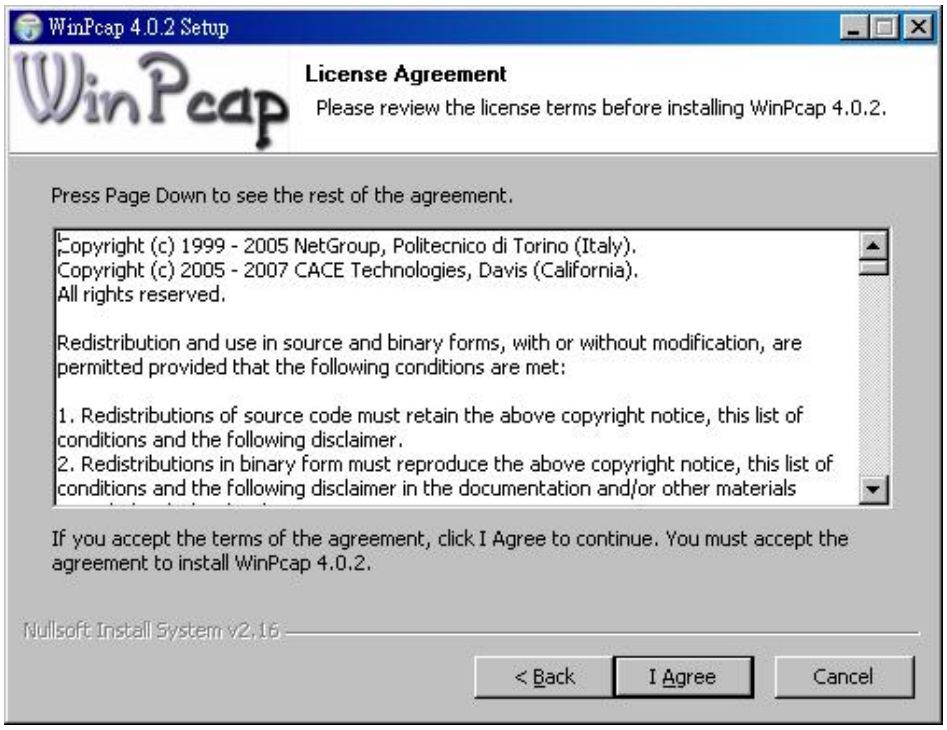


若您的 PC 没有安装过 WinPcap 的话，会进行 WinPcap 的安装程序；若您的 PC 所安装的版本是较旧的，则安装程序会要求您先移除旧的 WinPcap 版本在安装较新的版本。



请按下「Next」进行 WinPcap 安装程序

请在仔细检视完 WinPcap 的许可证协议之后，按下「I Agree」进行 WinPacp 安装



安装结束后几秒会出现 Completing Winpcap (安装完成) 画面

按下「Finish」继续安装其它组件

12.【注册 Apache 组件成功】在完成 WinPcap 安装后，会进行 Apahce 组件的注册并跳出注册成功讯息

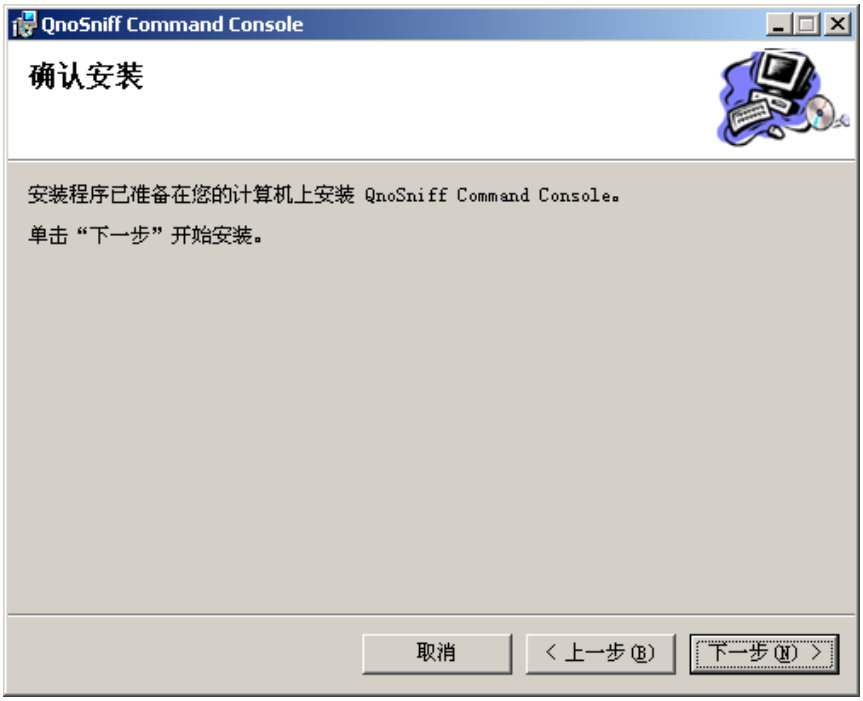
请按下确定继续其它组件的安装程序

13.【Apache 服务启动】当已注册完组件，Apahce 会启动服务，此时若您的 PC 有开启内建防火墙或是防毒软件的防火墙，应该会询问您是否需要开启此服务可以通过防火墙，请您在此时要选择「允许」或是「解除阻止」，如果您的防毒软件或防火墙已经预先将此服务阻挡，麻烦请在例外条例中开启允许此服务启动

14.【安装 .Net Framework 2.0】若您的 PC 已经有安装.Net Framework，则安装程序会直接跳过这一段的安装，如果没有，则会进行.Net Framework 2.0 的安装

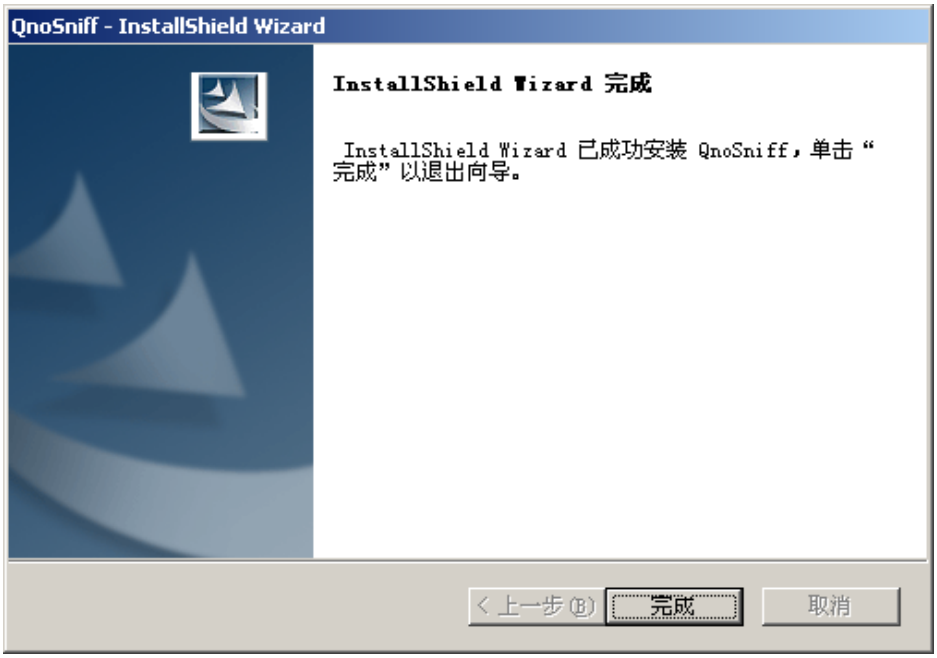
15.【安装 QnoSniff 专业版-应用程序版本】接着安装 QnoSniff 专业版 本地监控的程序安装

按下一步进行安装程序



确认安装 QnoSniff Command Console，按下一步进行

16.【QnoSniff 本地监控版本安装完成】当所有安装组件与程序完成后，会到安装完成页面，请按下「关闭」至结束整体安装页面



请按下完成离开 QnoSniff 专业版整体安装程序。

三、启用 QnoSniff 专业版

本章介绍如何开始启用 QnoSniff 专业版，以及搭配路由器的相关设定。

3.1 启用 QnoSniff 软件之前路由器的设定

在启用 QnoSniff 专业版软件之前，需要与连接监控 PC 的路由器上，「启动」QnoSniff 专业版的功能，所以请您先登入路由器的设定页面

选择「系统工具」=>「许可证密钥」

会有两个选择

【1】试用：按下「试用」按钮，会开启为期 15 天的试用，当超过 15 天后，QnoSniff 专业版会停止运作，您无法再继续使用，此时您若确实对 QnoSniff 专业版有所需求，就需要进行购买正式版产品密钥（License Key)，再输入密钥按下「提交」之后，若您的密钥是合法正确的，就能够继续使用 QnoSniff 专业版（正式版)。

【2】直接购买正式版产品密钥：若您觉得不需要进行试用，想直接使用正式版 QnoSniff 专业版功能，就需要进行购买正式版产品密钥（License Key)，再输入密钥按下「提交」之后，若您的密钥是合法正确的，就能够马上使用 QnoSniff 专业版的正式版本。(如下图)

※请注意：

1.开启 QnoSniff 专业版功能试用后，不能暂停试用，试用时间会一直倒数。

2.若您的产品密钥（License Key）输入错误超过三次，License Key 的输入页面会整个锁住无法再进行任何设定与输入动作，此时要请您与购买产品的代理商联络由侠诺原厂技术人员帮忙处理。

开启 Mirror Port 功能：

到实体端口口管理

启用镜像端口(Port1) (须先确认此端口没有被关闭)，按下确认按钮使设定生效

并且确定路由器的 Mirror Port 有用网线，连接至有安装 QnoSniff 专业版软件的 PC 网卡

3.2 启用 QnoSniff 专业版软件

完成路由器启用 QnoSniff 专业版功能动作之后，请您到安装完 QnoSniff 专业版软件的 PC，在桌面上会出现 QnoSniff 专业版的 Icon 图示 

，请用鼠标点选开启

若您的防火墙或是防毒软件有开启，在 QnoSniff 专业版启用时，会需要您将 QnoSniff 应用程序设定在防火墙或是防毒软件的防火墙例外条例中 (解除阻止)，QnoSniff 专业版才能够正常联机使用。

启用后会跳出以下登入画面

预设的账号是 administrator (须全部小写)

预设的密码是 admin (须全部小写)

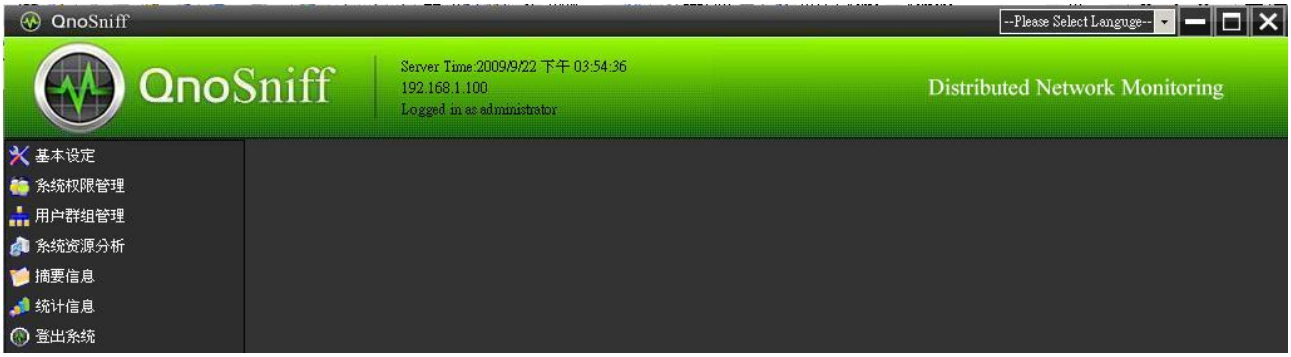
语系选择：

繁体中文请选择 Traditional Chinese

简体中文请选择 Simplified Chinese

英文请选择 English

选择完后按下确定进入 QnoSniff 专业版 本地监控版主控台



左上方会有现在的系统时间、登入 IP、登入身分，右上方可以直接做语系的切换

在左方选单共有 7 个主要选单项目

要能够正常启用 QnoSniff 功能，须先至基本设定中进行设置

【1】监听来源设定：设定要进行接受监听封包 / 流量的网卡，QnoSniff 专业版会预先抓取在您计算机上的网络接口信息，您可以从下拉式选单中做挑选，此网卡也必须确认有用网络线连接到 路由器 Mirror Port 端口。

【2】选择正确的监听设备之后，下面的接口信息 IP 与 MAC 会自动显示您选择的设备所带的值

【3】设备登入账号 / 密码：输入您连接 PC 的前方路由器账号密码名称，输入完毕后按下储存会进行联机作认证动作

【4】如果您按下储存后，会跳出「操作失败」讯息，可能会有以下原因

1.输入的路由器账号密码错误，请再确认一次。

2.与路由器之间的网络联机可能有问题（需确认连接至 Mirror Port)。

3.路由器上的 QnoSniff 专业版功能并没有正常启动，请再依前一章节确认一次。

【5】在输入完路由器账号密码按下储存后，会进行 QnoSniff 专业版与路由器之间的联机认证，联机成功会显示联机成功讯息，并且会显示 QnoSniff 专业版版本为试用版还是正式版本 (如下图)。

【6】远程访问设定：QnoSniff 有提供 Web 远程访问功能，所以若有需要用到远程访问，必须要设定远程访问所使用的通讯端口，系统预设为 80 Port，您可以依自己不同需求自更改，修改完后按下确认使设定生效，除了软件本身所设定的通讯端口外，您 PC 上的防火墙与防毒软件等，也必须将此通讯端口开放出来，才能使远程访问生效，另外在路由器上，也必须将您指定的远程访问通讯端口做设定，内容如下：

1.进入道路由器设定页面中，并选择「进阶功能配置」=>「DMZ / 虚拟服务器」=>「虚拟服务器」

2.在虚拟服务器功能中，将您已经设定成 QnoSniff 专业版远程访问的通讯端口，指定到安装 QnoSniff 专业版的 PC，举例来说若您安装 QnoSniff 软件的 PC IP 为 192.168.1.100，远程访问的通讯端口为 80 Port，就必须选择通讯端口为 HTTP [TCP/80 ~ 80]，内部 IP 地址为 192.168.1.100，接口位置选择 Any，选择启用后加入到对应列表，并按下确定键使设定生效。

※请注意！

1.若您所指定的远程访问通讯端口不在路由器既定的通讯端口列表 / 下拉式选单中，您需要在通讯部设定中增加此通讯端口内容。

2.若您有指定要从那个 WAN IP 做远程访问，而不是所有的 WAN，接口位置的部分就不用选择 Any，而是选择您所指定的 WAN IP 界面是那一个。

3.若 QnoSniff 专业版的远程访问通讯端口，已经有被路由器使用 (例如路由器的远程管理通讯端口也是 80 Port)，在设定上需要把这两个 Port 再做修改不能相同。

当您已经将远程访问端口从软件本身、PC 防火墙或防毒软件、路由器都已设定完成，可以试着从远程登入检视 QnoSniff 专业版的 Web 接口做测试

先至路由器首页确认您的广域网（WAN) IP

接口位置	廣域網1
IP位址	61.222.81.77
預設閘道	61.222.81.65
DNS 伺服器	168.95.1.1 0.0.0.0
連線數	2
下載頻寬使用率(%)	0
上傳頻寬使用率(%)	0
動態網域解析服務	Dyndns Disabled 3322 Disabled Dtdns Disabled Qnoddns Disabled
QoS頻寬管理	0 條規則
手動連線	

以上述为例，在浏览器的连接网址上打 http://61.222.81.77:80 (冒号后面是所设定的远程访问端口)

若您的设定与联机皆正常的话，一样会跳出登入页面

预设的账号是 administrator (须全部小写)

预设的密码是 admin (须全部小写)

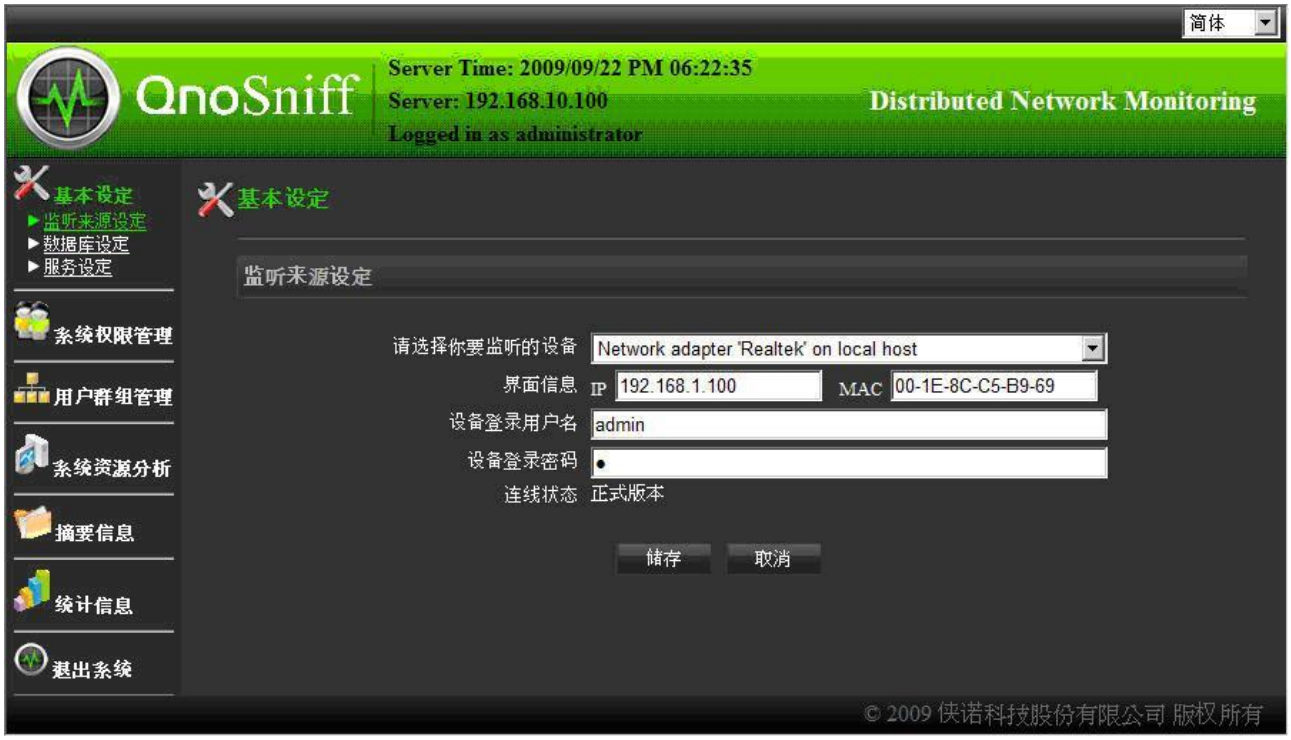
语系选择：

繁体中文请选择 Traditional Chinese

简体中文请选择 Simplified Chinese

英文请选择 English

选择完后按下确定进入 QnoSniff 专业版 Web 版主控台 远程监控 (Web)



※请注意！

1.若您的虚拟服务器设定有特别指定某一个 WAN 接口，请在输入网址连接的时候，参照首页该 WAN 界面的 IP 地址，若您的接口是选择 Any，则是使用任何一个 WAN IP 皆可

2.QnoSniff 专业版 PC 本地应用程序版（AP）与远程监控（Web）版本所表现的数据内容相同，设定部分只在基本设定上有差异，Ap 版本可以进行远程访问端口更改，远程监控（Web)版不行；Ap 版本可以进行数据库硬盘储存路径更改，远程监控（Web)版不行；Ap 版本可以将部分数据直接转成 PDF 档案，远程监控（Web)版不行（不过 E-mail 功能可以直接将数据转成 PDF 檔寄送出去)

四、基本设定

本章主要是在正常启用 QnoSniff 软件功能之后，对于软件一些基本的设置包括数据库的储存路径，以及储存方式与限制条件等进行设定。

基本设定主要分成三个子功能选单：

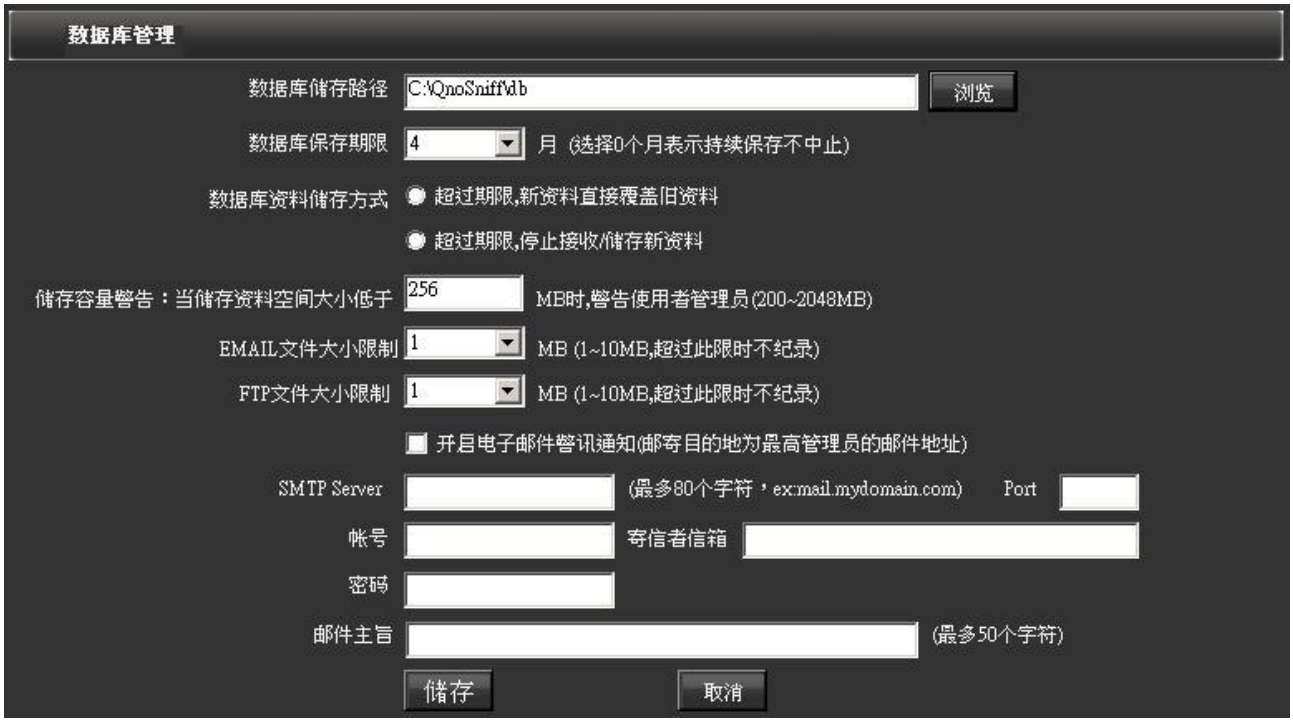
1.监听来源设定

2.数据库设定

3.服务设定

监听来源设定在前一章节已经说明过，便不再重复

数据库设定：



项目	说明
数据库储存路径	预设是在您安装 QnoSniff 专业版软件的硬盘分割中，若您需要变更数据库的储存路径，请按下右方的「浏览」按钮，在新跳出的窗口寻找合适正确的数据库储存路径。  ※数据库大小会因为随着时间一直累积数据量而增大，所以请特别注意您的硬盘盛余空间的使用状况
数据库保存期限	设定数据库的数据储存动作期限 1 至 6 个月，超过此期限，可以选择以下两种处理方式 1. 超过期限,新资料直接覆盖旧资料 当超过限制的时间条件时，新的数据会从最旧的数据陆续把旧数据覆盖掉，旧数据不会保存，占用硬盘空间也不会再持续变大。 2. 超过期限,停止接收/储存新资料 当超过限制的时间条件时，会停止接收、储存新数据，旧的数据不会被删除，但是也不会有新的数据产生，并须将期限做调整或是重置计算期限时间，才能够再开始收集新数据与储存新数据 3. (选择0个月表示持续保存不中止)

	若您不想中断数据持续储存，也不想删除旧数据，在选择时间期限时就必须要选择成「0 个月」表示持续保存资料不中断
储存容量警告	1.硬盘剩余储存空间大小侦测与预警： 设定当储存数据库的该硬盘剩余空间低于____MB 时 (200~2048MB)，警告使用者管理员 2.E-mail 文件大小限制：为避免过多的 E-mail 数据储存迅速占用甚至浪费硬盘空间，可设定 E-mail 记录大小 1~10 MB 的限制，若 E-mail 整体大小 (包含附件) 超过所设定限制，该封 E-mail 的纪录仍然会保留，但是由于最多就只有保留您所设定的大小，所以可能会产生附件档案超过的部分被截取掉，导致无法正常开启档案的现象，但是文件名称的纪录还是会保留住。 3.FTP 文件大小限制：为避免过大的 FTP 文件数据储存迅速占用甚至浪费硬盘空间，可设定 FTP 传输文件大小 1~10MB 的限制，若 FTP 文件大小 (不论上传下载) 超过所设定限制，该笔 FTP 传输记录仍然会保留，但是由于最多就只有保留您所设定的大小，所以可能会产生附件档案超过的部分被截取掉，导致无法正常开启档案的现象，但是文件名称的纪录还是会保留住。
开启电子邮件警讯通知：	启用此功能之后，当数据储存剩余空间低于您所设定的大小，系统就会发送 E-mail 电子邮件通知您，提醒您的剩余储存空间已经低于您所设定的警戒值。 并且此 SMTP 服务器也会成为之后各通讯协议类别清单上，E-mail 数据报表功能所必需的转发信件服务器，如果您没有正确设定此功能，E-mail 数据报表功能是无法正常使用的。 SMTP Server：请填入 SMTP 服务器的网域名称 (例：ms12.hinet.net) Port：发送电子邮件所使用的通讯端口 Port (例：25) 帐号：发送电子邮件的账号 (例：tony.chen) 密码：发送电子邮件所使用的密码 寄信者信箱：发送电子邮件使用的电子邮件信箱 (例：tony.chen@ms12.hinet.net) 邮件主旨：所发送电子邮件的主旨

服务设定：针对 Http (网页访问) 纪录的模式，与所需进行 QQ IM 通讯监控的账号进行设置。

HTTP 特定网站设定，需要详细记录的网站与 IP：

QnoSniff 专业版针对于 HTTP / 网页 / 网站访问的记录，预设只会记录在主要网域 (Domain) 「/」 以前的网址，例如 http://tw.yahoo.com/，若有去其它子页的记录，则不会显示出来，也会记录成 tw.yaoo.com，除非是把您需要特别将整个网站连结的细节都记录下来的网站名称，加入到「需要详细记录的网站 / IP」，才会将完整的网址细节连结记录下来，例如 http://tw.news.yahoo.com/article/url/d/a/090911/17/1qwgx.html。

将想详细记录网址的主要网域名称输入网站/IP 空白字段中，按下「新增」按钮，并按下「储存」后才会生效。

IM QQ 号码设定：

QnoSniff 专业版针对 IM 类别中的 QQ 监控，「必须」要将须监控的 QQ 账号与密码收集起来并且输入，才能进行监控与记录 QQ 活动。

将想监控的 QQ 账号、密码以及识别此账号的使用者名称输入在相对应的空白字段中，按下「新增」按钮，并按下「储存」后才会生效。

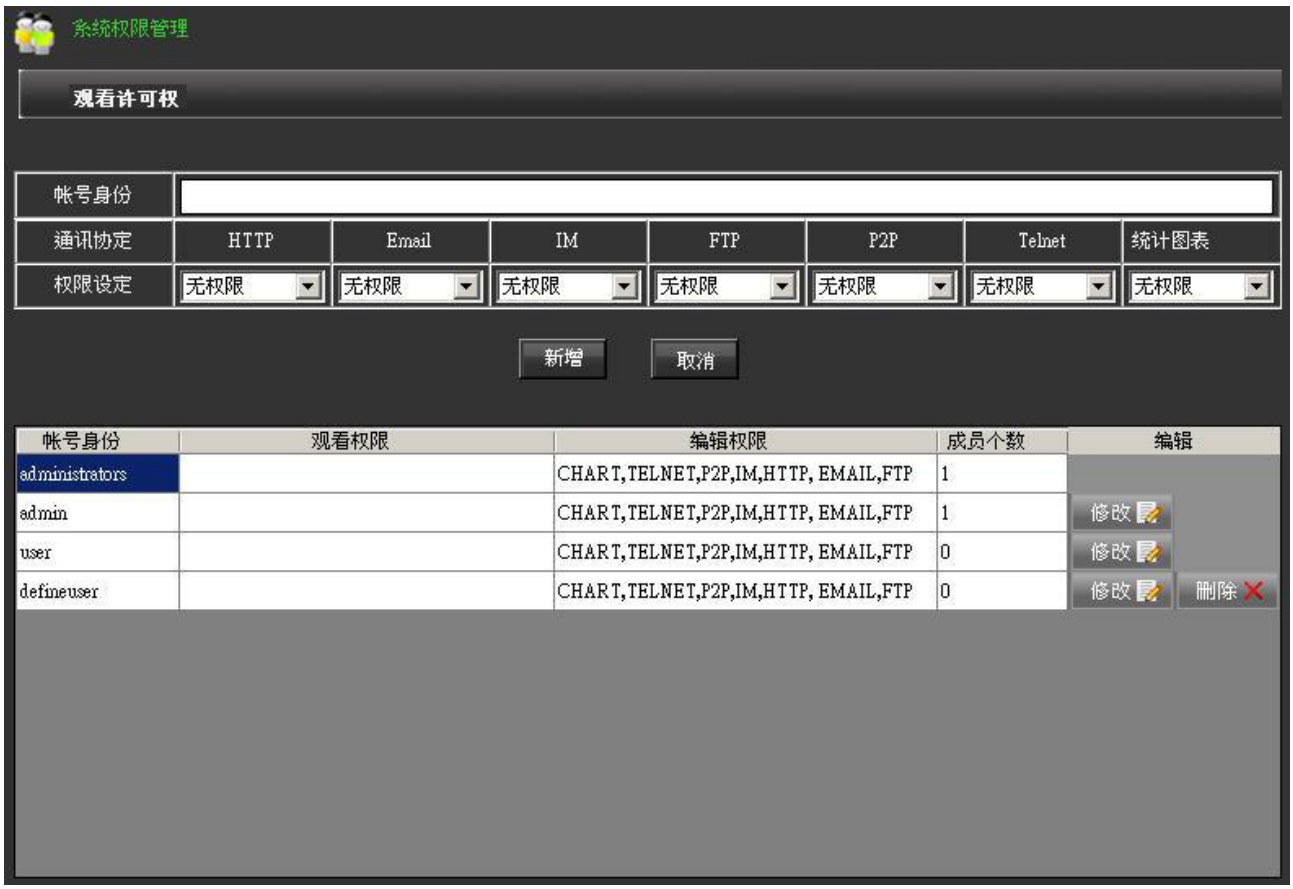
例如想要监控的 QQ 账号是 1xxxxxxx， 1xxxxxxx 此账号的密码是 34568989，使用者识别为 Sales1，就依序填入空白字段中，按下「新增」按钮，并按下「储存」后才会生效。

五、系统权限管理

本章介绍 QnoSniff 专业版系统管者与系统使用者登入账号的权限与系统相关操作的日志记录。

5.1 观看权限

观看权限主要在设置某一个「账号身分」在登入 QnoSniff 专业版系统之后，是否能观看甚至编辑各类通讯协议所记录的数据与统计图表。



账号身分：

此空白字段请输入您预归类为某类账号身分的命名，例如 Common User，administrator 账号身分为最高权限管理者与使用者，预设是对所有通讯协议类别以及统计图表等数据皆有观看及编辑权限，并且无法进行修改与删除。

※请注意！

系统的权限有五种，由高到低为：administrator、admin、user、

defineuser 和自定义用户。新增的身份账号都为自定义用户，权限比其它四种低。修改账号身份时，使用者只能修改自己的，以及比自己权限低的身份账号。

通讯协议：

由于 QnoSniff 专业版的记录数据最主要是以通讯协议为主，所以是以各类通讯协议所记录的数据，各别进行观看与编辑的权限设定，以及最后的统计图表等。

※请注意！

这边设定各类通讯协议的观看与编辑权限，是在摘要讯息内的限制(该类通讯协议细部列表)，在统计图表中，也会有各位通讯协议的分类，但是目前并无法从中再做权限设定，只是针对「所有的」统计数据及图表做观看或编辑的限制设定。

权限设定：

对每一个通讯协议项目与统计图表的存取权限设定

无权限－代表不能观看与不能编辑，该类用户登入后该选项会消失

观看权限－代表仅能观看该项讯息数据内容，无法进行数据删除修改并且只能无法使用邮寄、PDF 按钮功能

编辑权限－代表可以对该项讯息数据观看、删除与使用邮寄与 PDF 功能

新增：

输入完账号内容后按下新增，会跳出「新增使用者成功」，并将该笔数据增加至下方列表

修改：

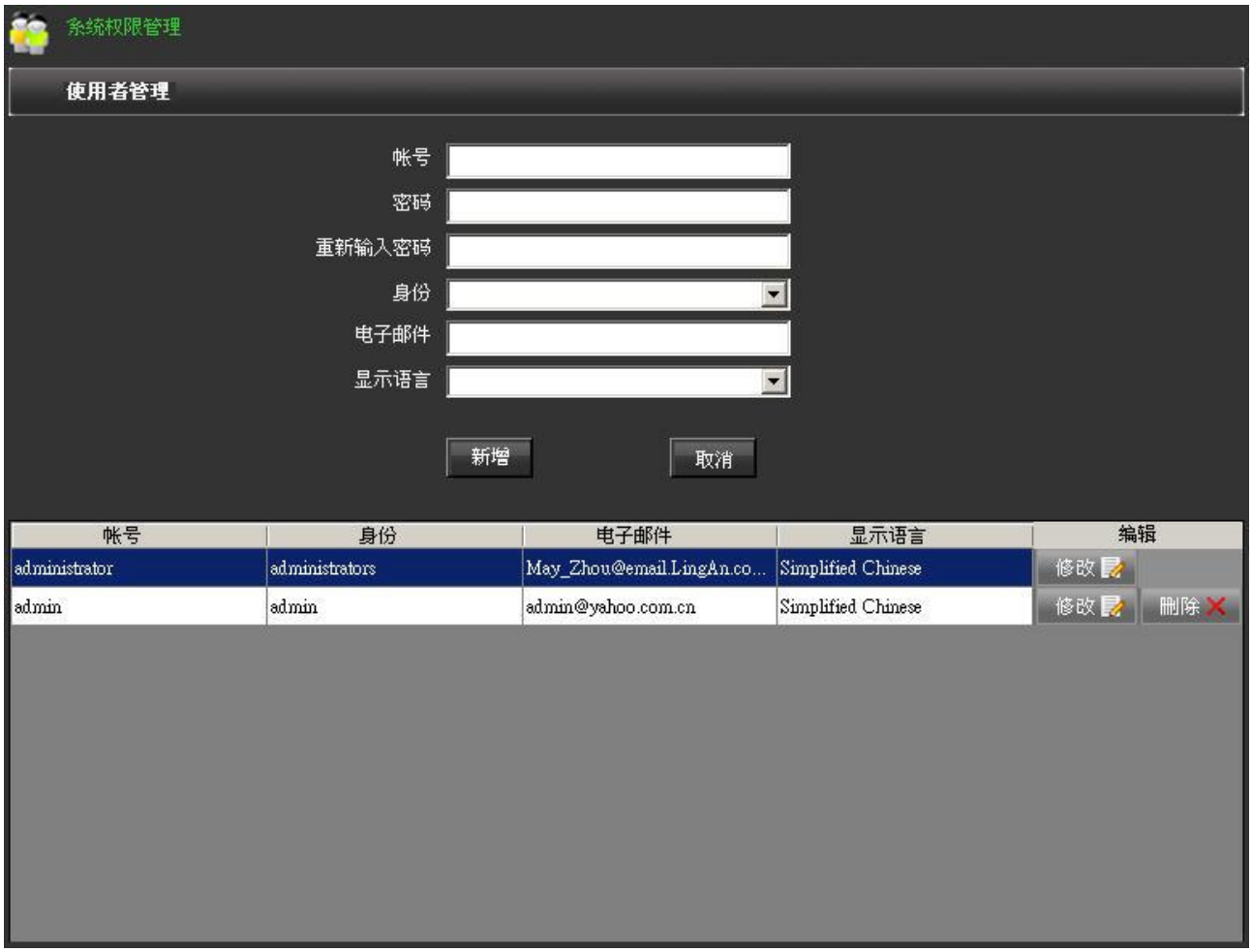
若您需要进行修改已有的账号内容，请按下下方列表中该笔数据右方的「修改」按钮，该笔数据会内容会出现在上方各个对应字段内，您就可以依此进行修改，修改完成后请按下「修改」按钮 (原本新增按钮在修改状态下会变成修改)，系统会询问您是否确认修改该笔数据，再按下是修改数据动作即完成。

取消：

取消会将您正在设定账号过程中已输入的数据清空，或是取消修改动作。

5.2 使用者管理

当您设定完您想分类的账号身分类别后，就要在每个身分类别下增加账号，所以在「观看权限」所设定的账号身分是一种在权限逻辑上的账号分类，至于在「使用者管理」所设定的账号，则是登入系统所使用的真实账号、密码以及该账号的使用语系等设定，同样地，根据使用者登录账号身份的不同，使用者只能修改自己的，以及新增或修改比自己权限低的账号身份。最高管理员 administrator 可以增加 administrator 身份的账号，其它身份的用户则不能做此操作。



账号：	输入登入的账号名称
密码：	输入此账号登入的密码
重新输入密码：	须再输入相同密码再确认一次
身分：	从下拉式选单中挑选属于何种身分账号，预设会有 administrator、admin、user、defineuser，您所新增或修改的身分账号也会出现在下拉式选单中提供选择。

电子邮件：	输入该账号的电子邮件信箱内容，在使用者使用「邮寄」功能时，数据会寄到所设定电子邮件信箱当中。
显示语言：	设定此用户在登入页面后，预设的系统显是语系为繁中、简中或英文。
新增：	输入完账号内容后按下新增，会跳出「新增使用者成功」，并将该笔数据增加至下方列表
修改：	若您需要进行修改已有的账号内容，请按下下方列表中该笔数据右方的「修改」按钮，该笔数据会内容会出现在上方各个对应字段内，您就可以依此进行修改，修改完成后请按下「修改」按钮（原本新增按钮在修改状态下会变成修改)，系统会询问您是否确认修改该笔数据，再按下是修改数据动作即完成。
取消：	取消会将您正在设定账号过程中已输入的数据清空，或是取消修改动作。

※请注意！

administrator 与 admin 身分账号在预设的时候，系统会各别预先设定一个「administrator」与「admin」的「登入账号」，而且这两个账号下的电子邮件信箱（E-amil）预设也是虚拟、不正确的，请您务必记得修改成该账号所对应的正确电子邮件信箱内容，数据列表的 E-mail 功能才能将报表档案，正确发送至您所设定的电子邮件信箱。

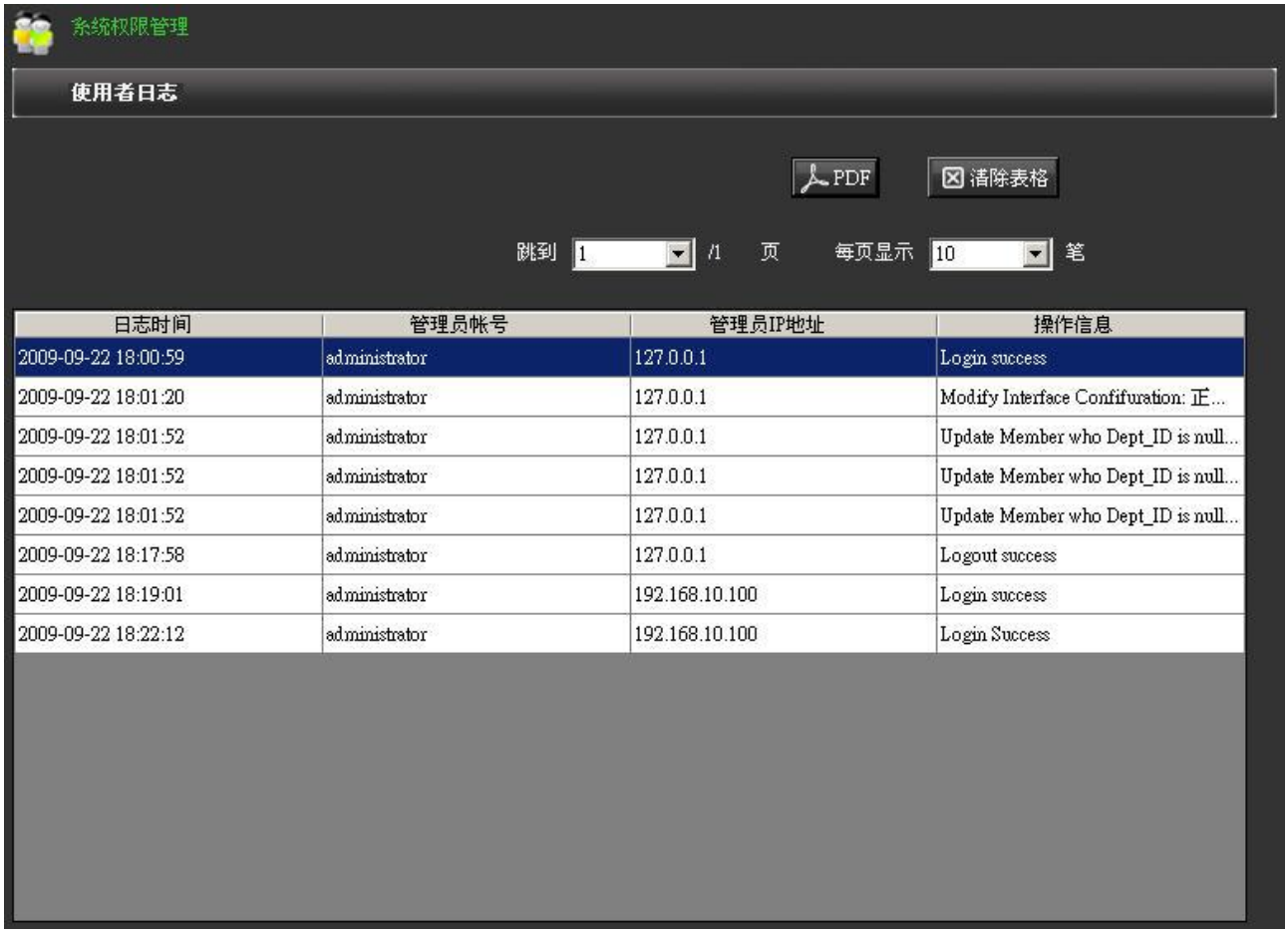
5.3 使用者日志

使用者日志会显示所有使用者登入、注销、编辑与修改数据等信息，QnoSniff 专业版只有 administrator 与 admin 两种身分账号的使用者，登入后才会看到使用者日志列表，其它的身分账号得使用者是看不到的。

PDF：若有需要将日志转换成 PDF 文件做保存或参考，请按下 PDF 按钮做汇出动作。

清除表格：若记录已经过多并且多半是旧有记录不需再保留，可以按下清除表格按钮清除所有日志记录

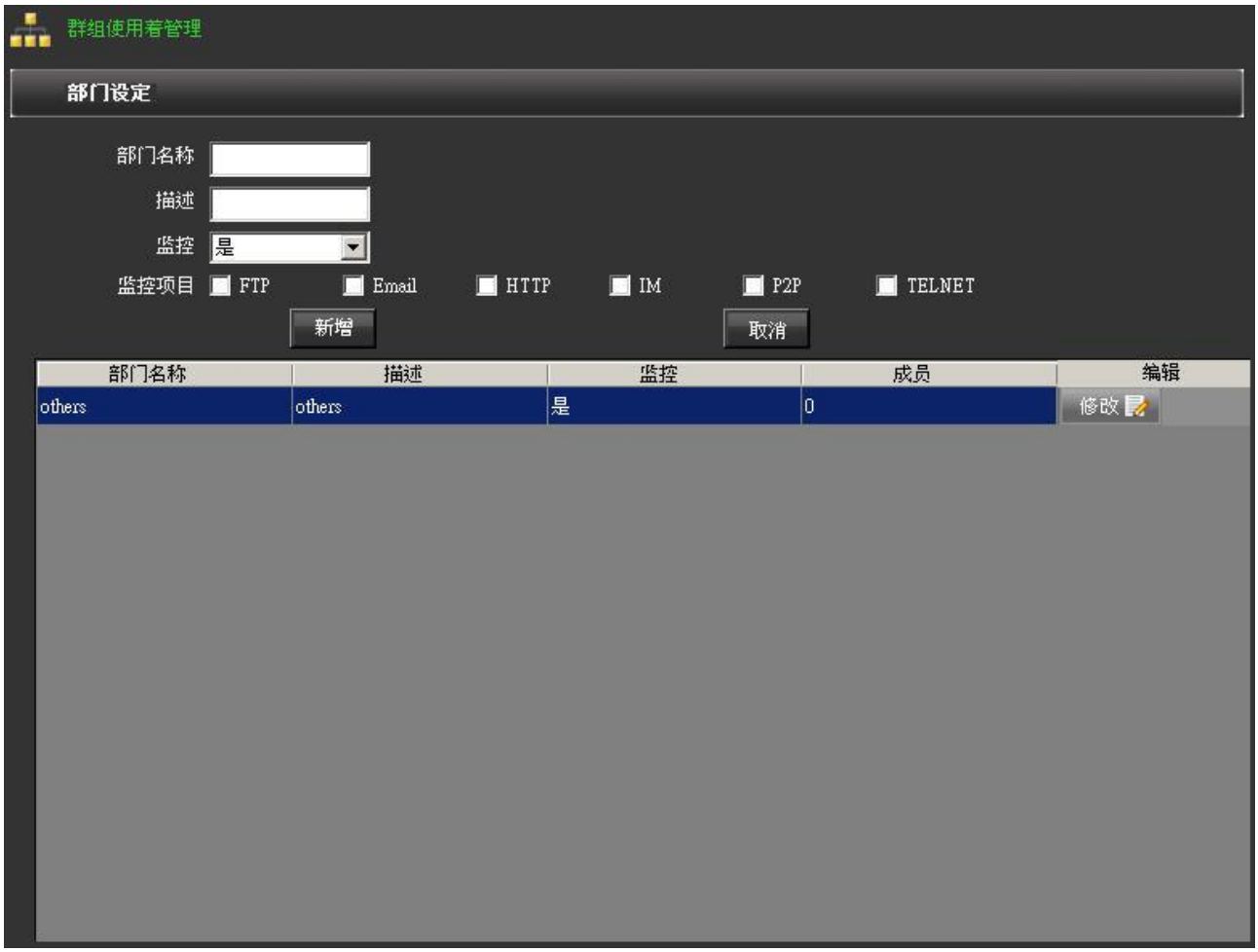
每页显示____笔，跳到____页：您可以自定义日志列表一页可显示几笔数据，并可以直接跳到另外一页观看。



六、群组使用者管理

本章节讲述 QnoSniff 专业版中的群组架构设定，使用群组的好处是方便统一管理，该群组下的成员不需一一进行设置与调整，可以将设定一次套用该群组所有成员，并且您可以依网络真实的使用状况进行群组划分，使 QnoSniff 专业版所记录分析的数据，更符合您内网用户的网络使用现况。

6.1 部门设定



部门名称：　　将您预分类出来的部门命名名称，例如 Sales、RD。

描述：　　针对该部门做简单的注释与叙述以识别。

监控：　　选择是否针对此部门进行监控记录。

监控项目：	选择该部门会受 QnoSniff 专业版监控并记录的通讯协议类别，若您的某些部门是不方便进行监控或具机密性质的，例如总经理或董事长的 E-mail 或 IM 实时通讯，您就可以在此做不监控的选择设定。
新增：	输入完账号内容后按下新增，会跳出「新增使用者成功」，并将该笔数据增加至下方列表
修改：	若您需要进行修改已有的账号内容，请按下下方列表中该笔数据右方的「修改」按钮，该笔数据会内容会出现在上方各个对应字段内，您就可以依此进行修改，修改完成后请按下「修改」按钮 (原本新增按钮在修改状态下会变成修改)，系统会询问您是否确认修改该笔数据，再按下是修改数据动作即完成。
取消：	取消会将您正在设定账号过程中已输入的数据清空，或是取消修改动作。

6.2 用户树状列表

用户树状列表是用来便于展开您所设定的所有群组与使用者，QnoSniff 专业版必须要将受监控的用户加入树状列表与其下方的用户列表才有办法进行监控动作。

用户名称：　输入用户的名称，例如 SalesPC1。

IP 地址：　输入用户的 IP 地址，例如 192.168.3.100。
可以手动输入，也可以用下拉式选单选择自动学习到的 IP。

MAC 地址：　输入用户的 MAC 地址，例如 00-1A-B6-02-3F-9A。(请注意格式必须以”-“相隔)

部门名称：　从下拉式选单中挑选您已经设定完成并且欲加入的群组。

监控：　针对此单一用户是否进行监控。

请注意，即使该用户所归属的群组已经纳入要监控范围，但是在单一用户的监控选项是选择「否」 (不监控)，则此单一用户就不会纳入监控范围，监控的动作选项会以单一用户的选择决定。

IP－MAC 学习：

若您的手边已经有建立好的内网用户对照表，自然可以一一将这些资料依序输入，但是这仍然会花费不少时间，QnoSniff 专业版有提供一个更方便的工具让您使用，就是 IP-MAC 自动学习。

当您按下 IP-MAC 学习按钮后，会跳出另一个窗口画面，是 QnoSniff 专业版帮您学习到的内网用户数据，包含计算机名称 (如果没有学习到计算机名称会显示 MAC)、IP 地址、MAC 地址，用户名称是您可以自己填写的，部门则是用下拉式选从现有设定好的部门群组做选择，最后选择该用户是否监控，当列表的用户都设定好之后，就可以勾选「全选」并按下「保存」，就可以一次就将众多的内网用户分好群组、设定是否监控、以及用户名称等设定完成，相较于一个个输入会方便许多。

若您发觉某些用户数据，在进入窗口画面当时并没有学习到，您可以再按下「重新整理」按钮来更新学习到用户列表内容。

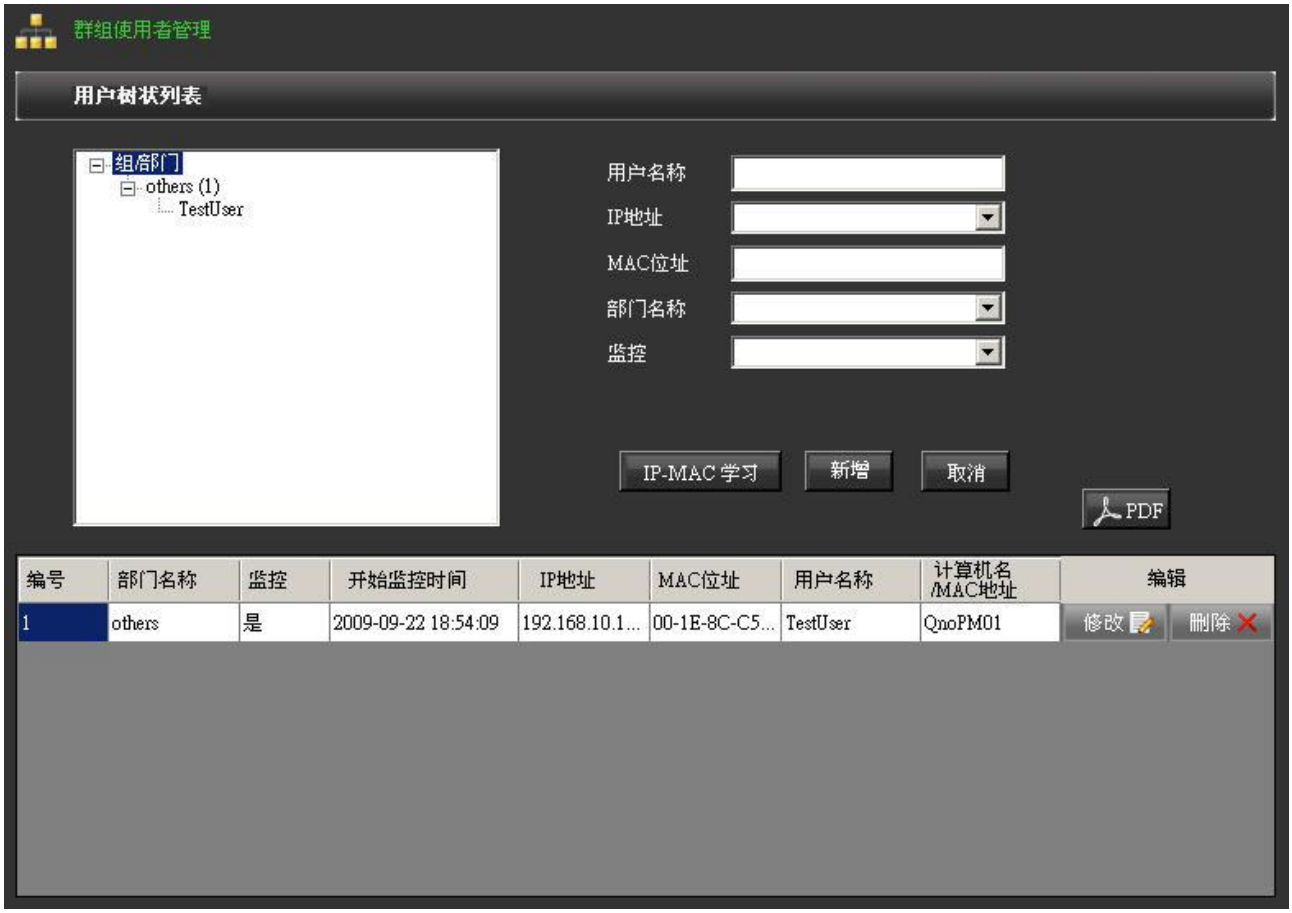
请注意，已经设定好并加入用户以及树状列表的用户，不会再出现在 IP-MAC 学习清单当中，若您的用户在设定加入列表完成后更改 IP，则已经设定好数据仍然会以原本的 MAC 为主，并自动更新成目前最新的 IP 地址为该用户的 IP 数据。

全选	序号	计算机名称/MAC地址	IP地址	MAC地址	用户名称	部门名称	监控
☐	1	00-00-74-65-4B-E3	192.168.0.123	00-00-74-65-4B-E3		others	是
☐	2	00-00-E8-7C-89-42	192.168.0.163	00-00-E8-7C-89-42		others	是
☐	3	00-01-29-4C-16-E5	192.168.2.180	00-01-29-4C-16-E5		others	是
☐	4	00-01-4A-CC-1C-FF	192.168.2.92	00-01-4A-CC-1C-FF		others	是
☐	5	00-02-3F-B7-E0-EC	192.168.2.70	00-02-3F-B7-E0-EC		others	是
☐	6	00-02-DD-50-E1-28	192.168.2.160	00-02-DD-50-E1-28		others	是
☐	7	00-03-9D-73-40-7C	192.168.1.133	00-03-9D-73-40-7C		others	是
☐	8	00-04-61-4A-87-87	192.168.2.110	00-04-61-4A-87-87		others	是
☐	9	00-05-5D-69-6B-6E	192.168.0.237	00-05-5D-69-6B-6E		others	是
☐	10	00-08-54-A7-05-91	192.168.0.9	00-08-54-A7-05-91		others	是
☐	11	00-08-A1-8D-0D-B9	192.168.2.108	00-08-A1-8D-0D-B9		others	是
☐	12	00-09-6B-47-72-48	192.168.1.214	00-09-6B-47-72-48		others	是
☐	13	00-0A-48-05-7D-E6	192.168.2.124	00-0A-48-05-7D-E6		others	是
☐	14	00-0A-48-13-95-44	192.168.2.10	00-0A-48-13-95-44		others	是
☐	15	00-0A-79-BD-96-4C	192.168.0.198	00-0A-79-BD-96-4C		others	是
☐	16	00-0A-E4-30-29-91	192.168.2.164	00-0A-E4-30-29-91		others	是
☐	17	00-0A-E4-E6-16-C1	192.168.1.156	00-0A-E4-E6-16-C1		others	是
☐	18	00-0A-E4-FE-A7-FF	192.168.1.55	00-0A-E4-FE-A7-FF		others	是
☐	19	00-0C-6E-36-8E-1A	192.168.2.7	00-0C-6E-36-8E-1A		others	是
☐	20	00-0C-6E-94-F9-5A	192.168.2.53	00-0C-6E-94-F9-5A		others	是

完成加入的用户列表

※请注意！

IP-MAC 自动学习方法，是当按下 IP-MAC 学习按钮，会针对内网 LAN 端所有子网 (Subnet) 用户计算机发出 ARP 询问并且进行学习，所以若您的内网 PC 若是放在防火墙里面，很有可能会学习不到该用户数据。



※用户成功加入列表的时间，并且必须选择监控选项为「是」的时间，就是开始监控时间。

七、系统资源分析

本章节是介绍以 QnoSniff 专业版，抓取监控 PC 所连接路由器的路由器系统信息，其中包括路由器的 CPU 使用率、内存（Memory）使用率、以及每个广域网（WAN）的上传及下载流量。

7.1 CPU 使用记录

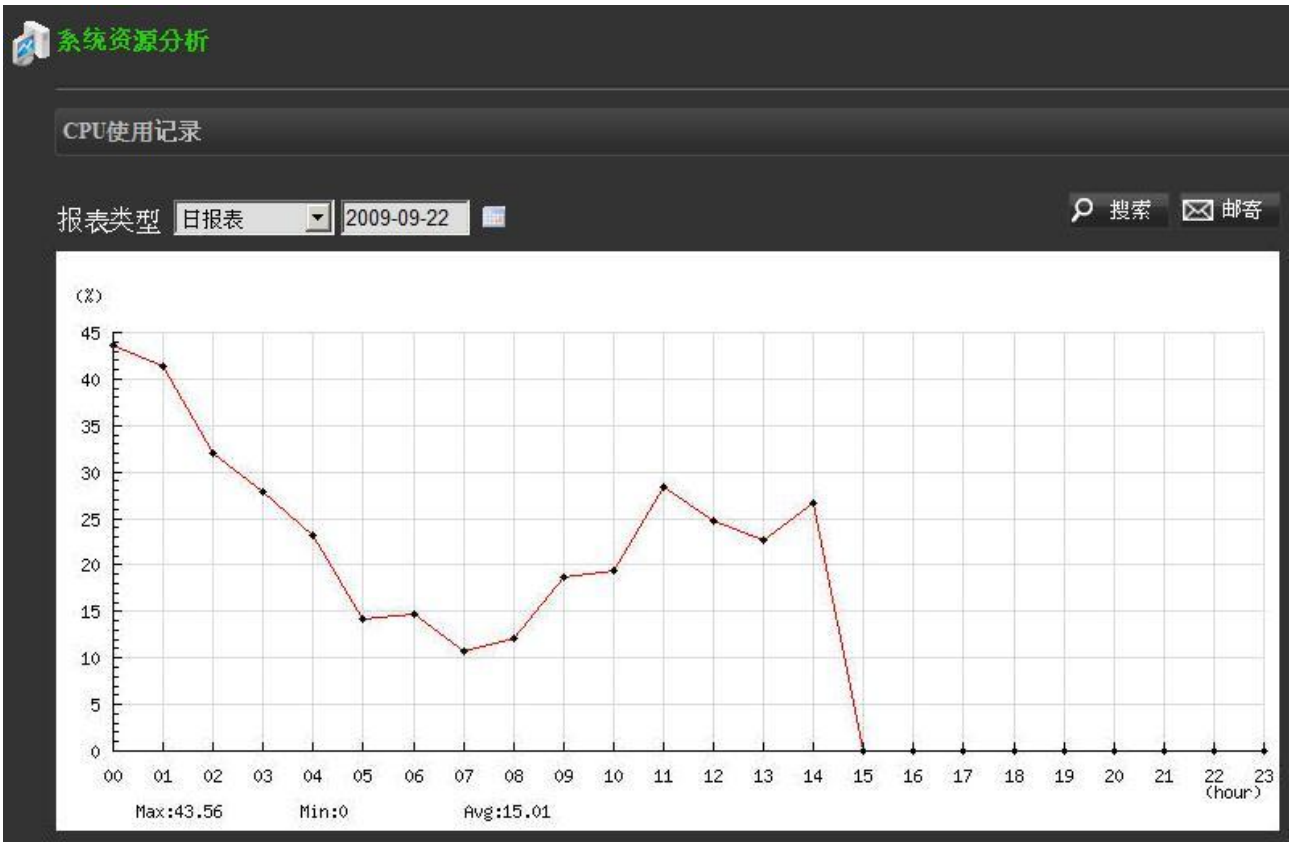
不论是路由器的 CPU 使用记录，还是内存使用率或广域网（WAN）的流量，QnoSniff 专业版要能正常抓到正确的数值，必须确认路由器有开启 SNMP 功能，所以先进入路由器的管理页面「系统工具」=>「SNMP 网络管理」，确认有将 SNMP 网络管理功能启用。

回到 QnoSniff 专业版系统资源分析的 CPU 使用记录页面，左方的时间选择会有日报表、周报表、月报表

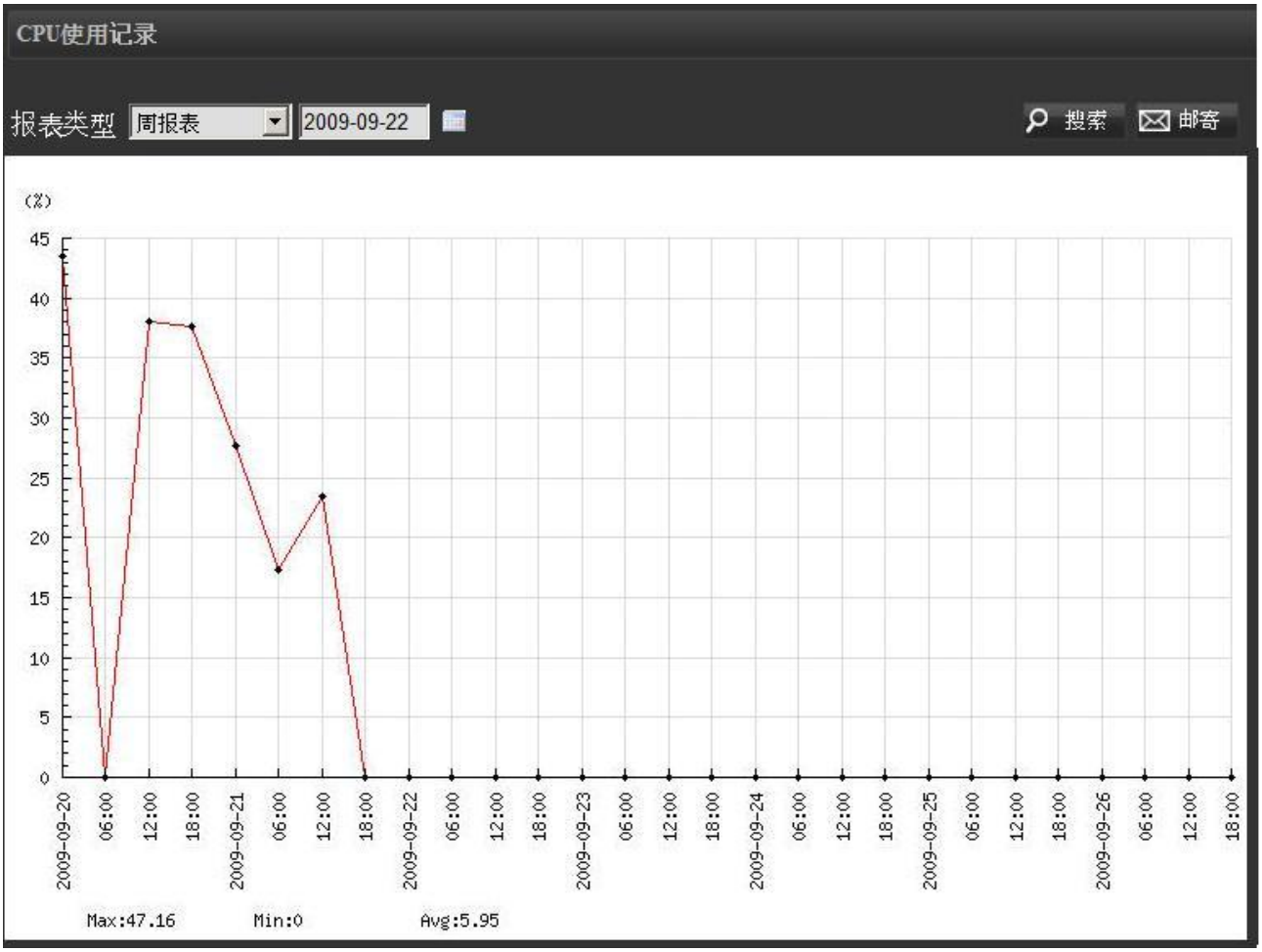
及自订日期，右方有电子月历 

可以直接点选，出现的图表除了折线图外，还会在图表下方显示这段时间内的最大值、最小值、平均值，另外报表与月历点选的时间关系如下：

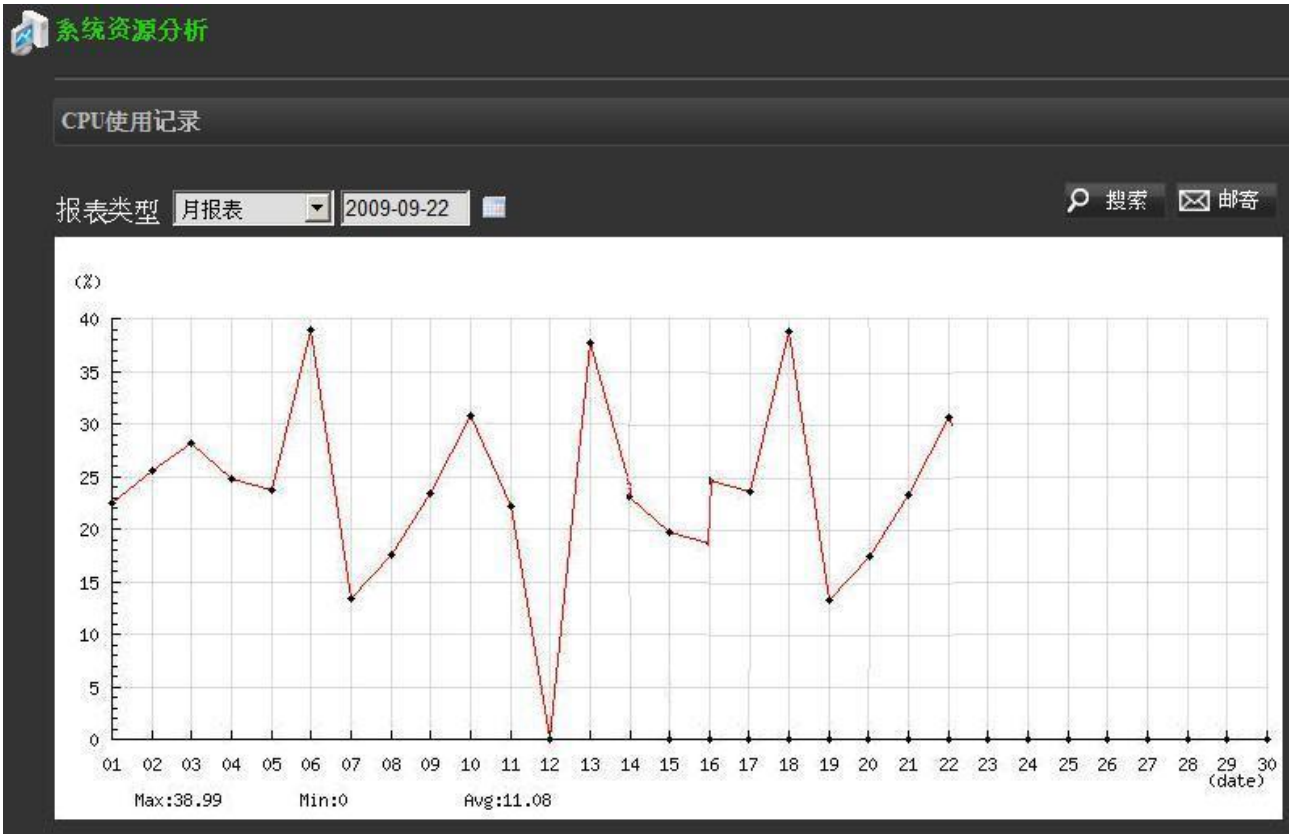
【1】选择日报表：月历日期选择到那一天，就是指那一天的 CPU 使用率状况（0 ~ 24 小时），例如选择到 2009/9/22 表示数据图标是显示 2009/9/22 当天的 CPU 使用记录



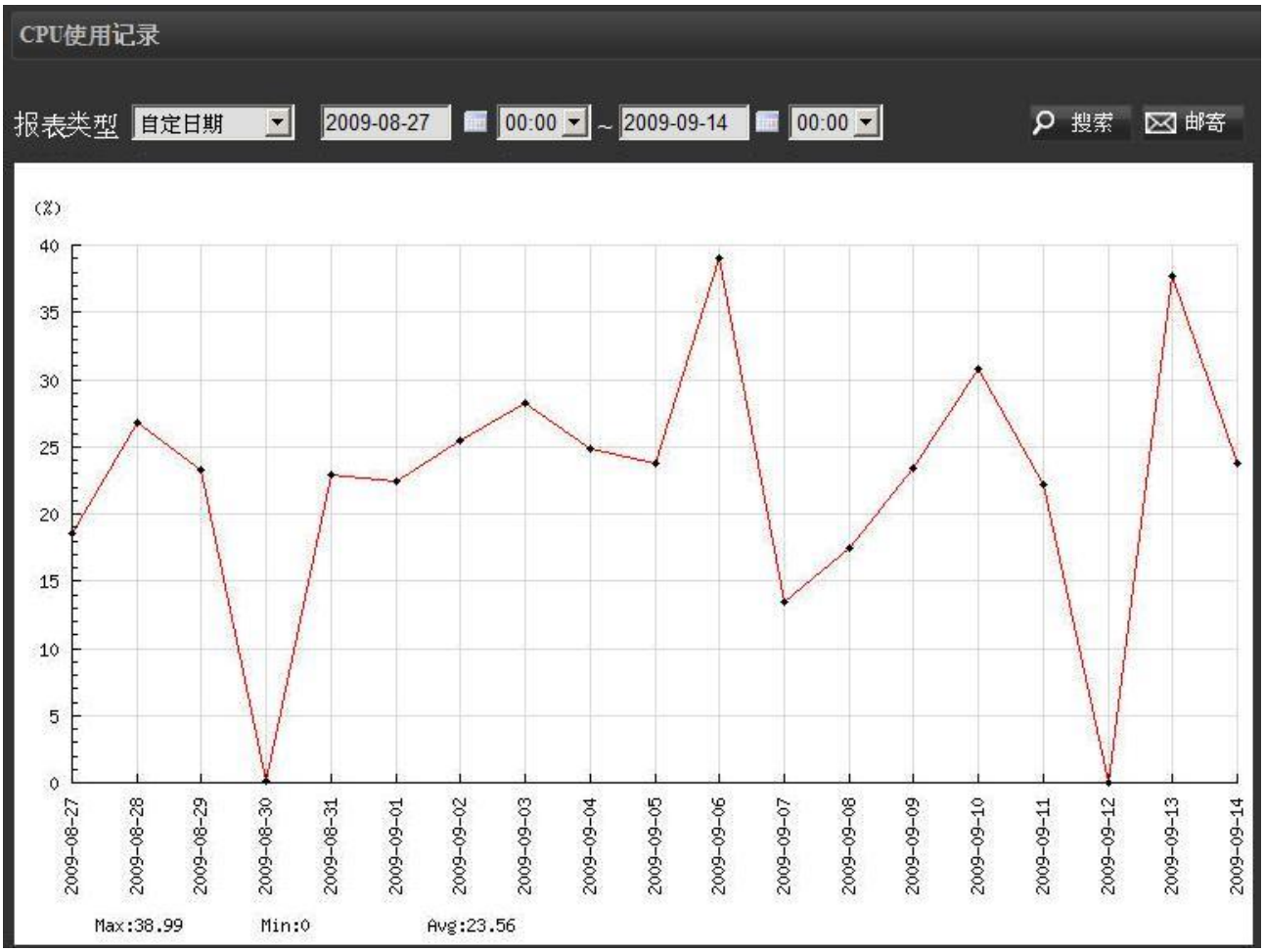
【2】选择周报表：月历日期选择到那一天，就是指那一天所在的那周 CPU 使用率状况，例如选择到 2009/9/22，就表示数据图标是显示 2009/9/14 到 2009/9/20 这一周的 CPU 使用记录



【3】选择月报表：月历日期选择到那一天，就是指那一天所在的那一个月 CPU 使用率状况，例如选择到 2009/9/22，就表示数据图标是显示 2009 年 9 月份整个月的 CPU 使用记录



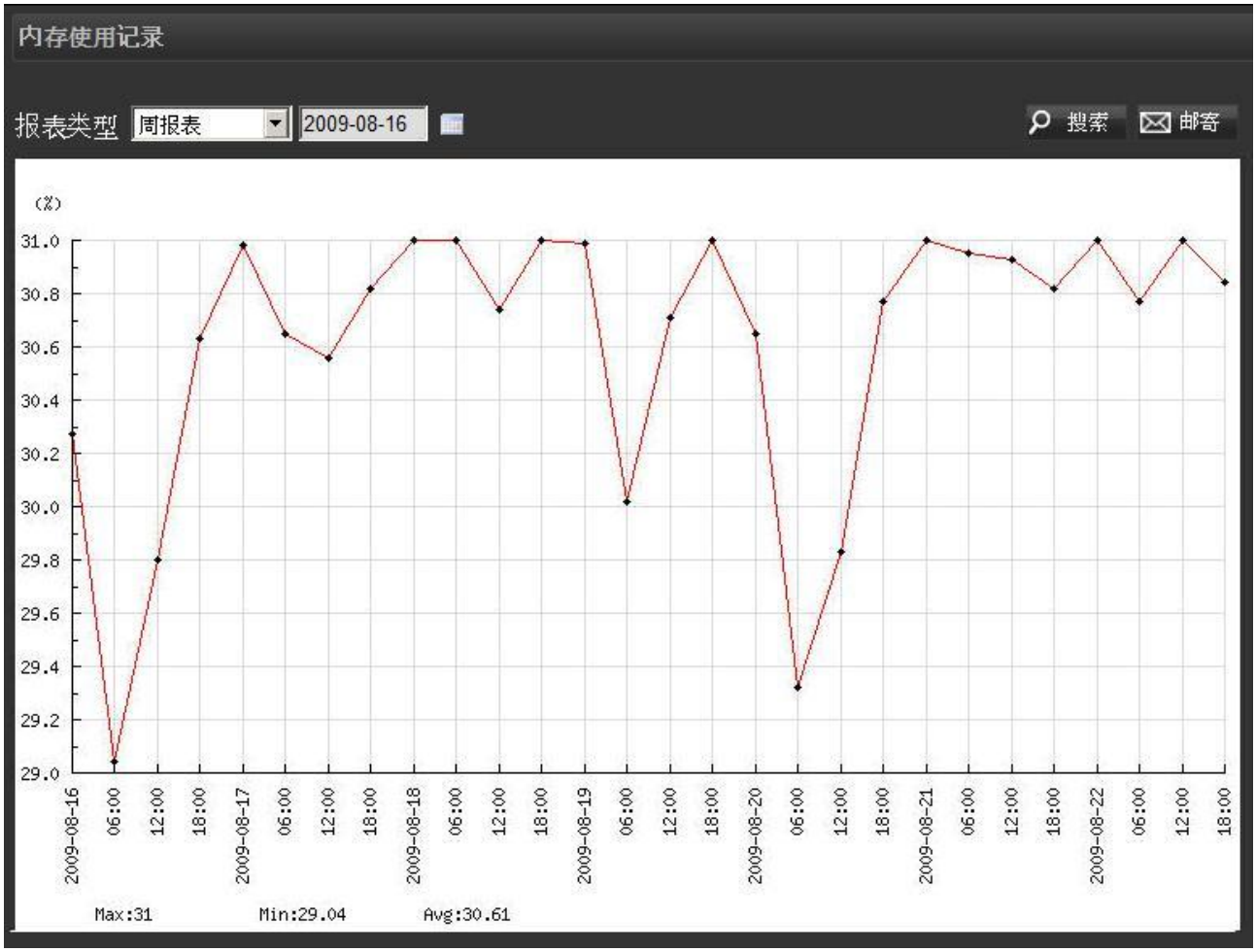
【4】选择自订日期：可以跨月自己选择一段时间做资料查询，当选择到这个选项时，会跳出两个月历以及 24 小时制时间，时间间隔最多不能超过 32 天，并且由于是自定义查询条件 (非默认值)，所以在呈现资料的时间上会相对比较久。



请注意：以上查询时间区段确认后，请记得按下「搜索」按钮，因为该画面数据数据只会在从别的页面首次跳到此页时会更新，当您查询的时间区段有变动，麻烦请再按下「搜索」按钮以让数据可以更新到符合您新定义的时间区段，另外 Aplication 版会有 PDF 与邮寄功能，远程监控 (Web)版会有邮寄功能，有需要亦可善加利用。

7.2 内存（Memory）使用记录

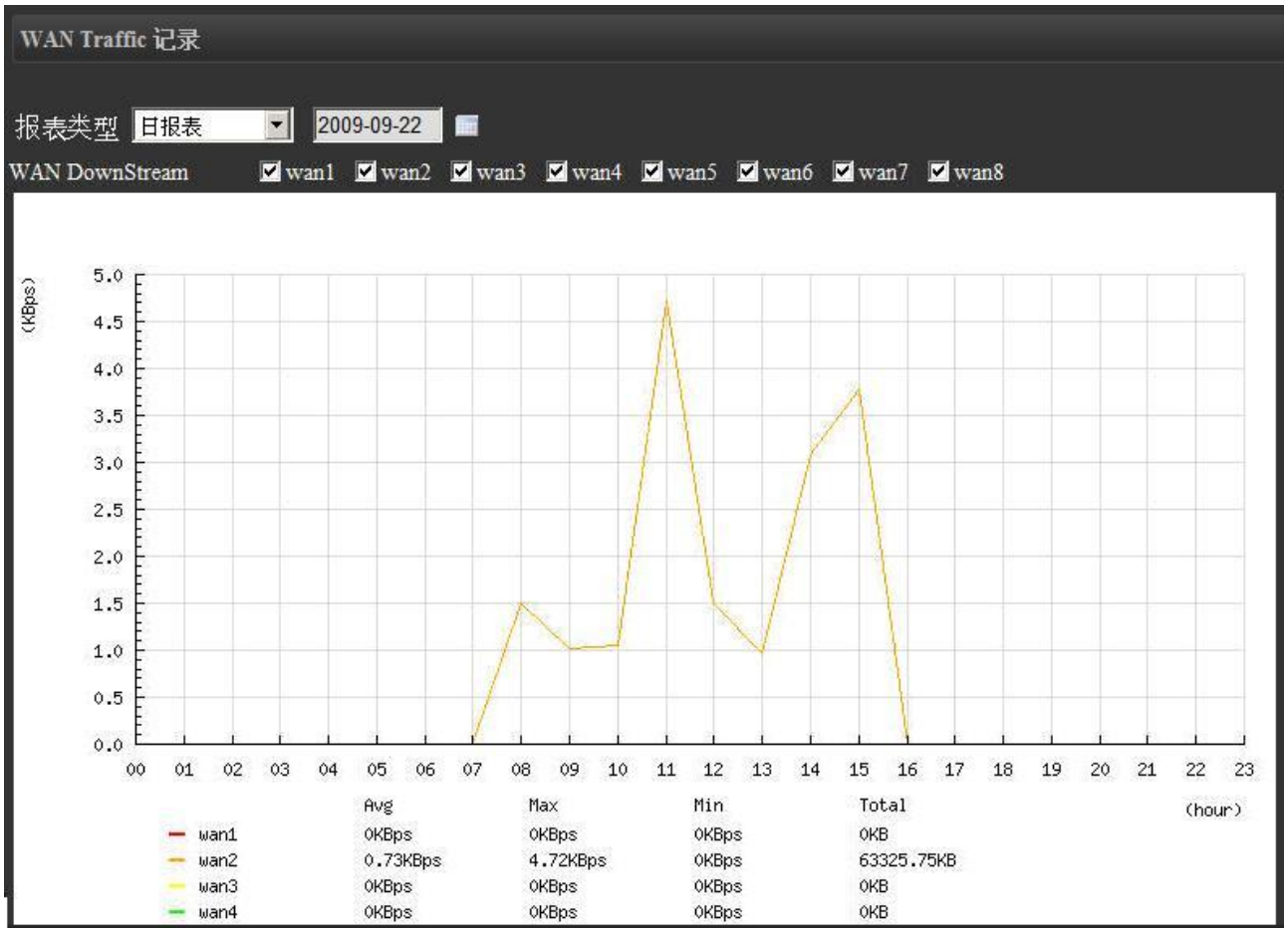
这部分的的列表图示，是指路由器的系统内存使用状况，是以使用了多少百分比来显示。



时间区段的选择与上述 CPU 使用记录的方式相同，您可以依您的需要切换不同时间区段，来检视不同时间区段的路由器系统内存使用状况。

7.3 WAN Traffic(广域网流量) 记录

WAN 的流量有分 Upstream (上传) 与 Downstream (下载)，您可以选择您想观察的某个 WAN 端口，进行流量使用状况显示。



最下方仍然会出现您所选择 WAN 口的流量平均值、最大值、最小值数据 (在您所定义的时间区段之内)。

八、摘要信息

接下来进入 QnoSniff 专业版的核心功能－各类通讯协议流量监控与记录。

QnoSniff 专业版目前可监控的通讯协议最主要分为以下几大类：

（1）网页浏览（HTTP)

（2）电子邮件（SMTP 与 POP3)

（3）文件传输（FTP)

（4）点对点下载（P2P)

（5）TELNET

（6）即时通讯（IM)

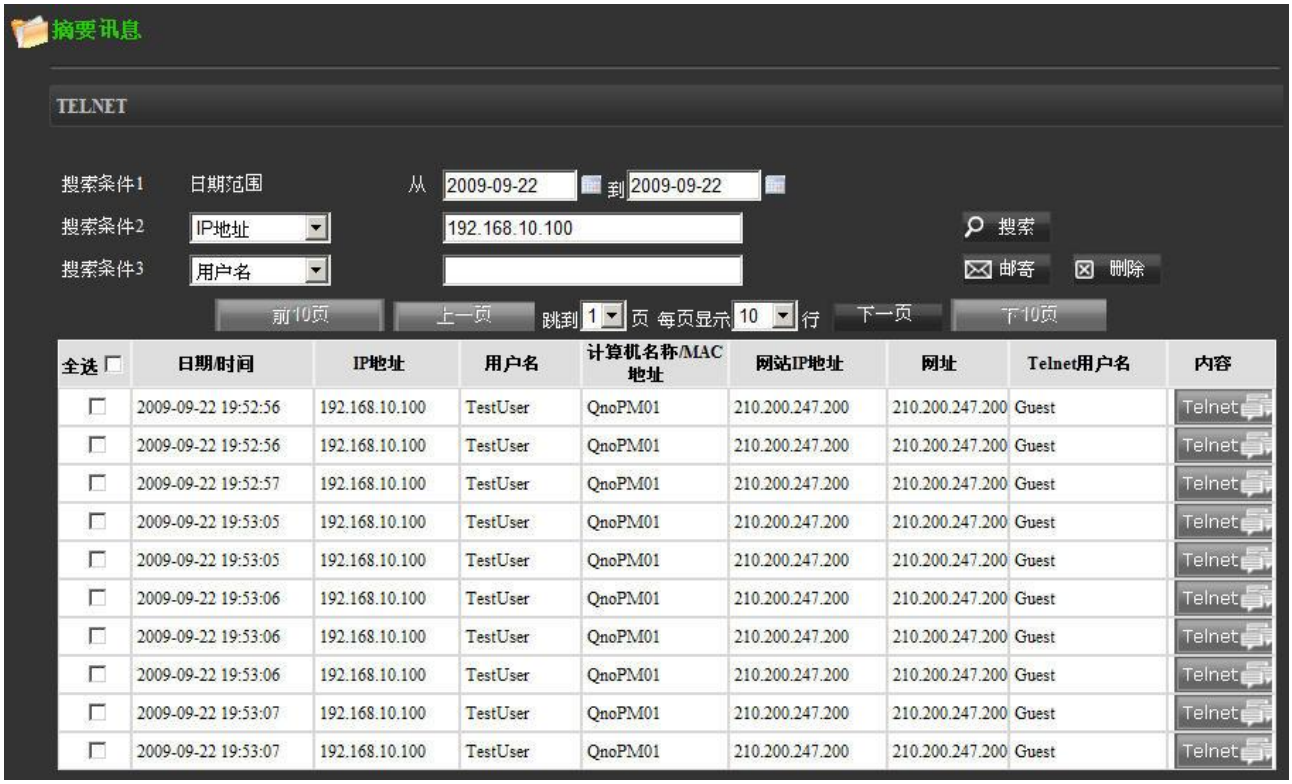
针对不同的服务与流量内容各别进行监控与记录，接下来我们来一一介绍。

8.1 即时服务总表

实时服务总表用途，是用来显示在您浏览当天，内网所有用户的网络流量状况，**所以数据量的累积只有一天**，当您在隔天登入检视此页，所检视的就是隔天的内网用户使用状况。

序号	用户名	计算机名称/MAC地址	部门名称	聊天记录	网页浏览	文件传输	收发邮件	TELNET	所占频宽(KB)	IP地址	开始监控时间
1	TestUser	QnoPM01	others	0	0	0	0	17	11872.84	192.168.10.100	2009-09-22 18:54:09

在这个列表当中会列出当下用户各个网络通讯协议类别的流量使用情形，包括聊天记录 (IM)、网页浏览、文件传输、收发邮件、Telnet 的记录数量与流量大小 (所占频宽)，每个用户记录在各个通讯协议类别的数量都有超级链接，可以直接用鼠标点选进入该用户的该项通协议记录查询细部的记录内容如下图 (以鼠标点选 Telnet 为例)。



全选	日期/时间	IP地址	用户名	计算机名称/MAC地址	网站IP地址	网址	Telnet用户名	内容
	2009-09-22 19:52:56	192.168.10.100	TestUser	QnoPM01	210.200.247.200	210.200.247.200	Guest	Telnet
	2009-09-22 19:52:56	192.168.10.100	TestUser	QnoPM01	210.200.247.200	210.200.247.200	Guest	Telnet
	2009-09-22 19:52:57	192.168.10.100	TestUser	QnoPM01	210.200.247.200	210.200.247.200	Guest	Telnet
	2009-09-22 19:53:05	192.168.10.100	TestUser	QnoPM01	210.200.247.200	210.200.247.200	Guest	Telnet
	2009-09-22 19:53:05	192.168.10.100	TestUser	QnoPM01	210.200.247.200	210.200.247.200	Guest	Telnet
	2009-09-22 19:53:06	192.168.10.100	TestUser	QnoPM01	210.200.247.200	210.200.247.200	Guest	Telnet
	2009-09-22 19:53:06	192.168.10.100	TestUser	QnoPM01	210.200.247.200	210.200.247.200	Guest	Telnet
	2009-09-22 19:53:06	192.168.10.100	TestUser	QnoPM01	210.200.247.200	210.200.247.200	Guest	Telnet
	2009-09-22 19:53:07	192.168.10.100	TestUser	QnoPM01	210.200.247.200	210.200.247.200	Guest	Telnet
	2009-09-22 19:53:07	192.168.10.100	TestUser	QnoPM01	210.200.247.200	210.200.247.200	Guest	Telnet

8.2 网页浏览

网页浏览指的是用户的网页访问记录，在网络通讯协议方面监控的是 HTTP。

全选	日期/时间	IP地址	用户名	计算机名称/MAC地址	Website	Website IP Address	数量
☐	2009-09-22 00:00:01	192.168.1.165		USER-3C1A75A06B	HTTP://CO121W.COL121.MAIL.LIVE.COM/	65.55.15.123	1
☐	2009-09-22 00:00:07	192.168.0.174		00-16-E6-37-BE-FE	HTTP://APPS.FACEBOOK.COM/	203.69.113.56	1
☐	2009-09-22 00:00:07	192.168.1.76		00-1D-92-E4-3F-9E	HTTP://174.133.30.162/	174.133.30.162	1
☐	2009-09-22 00:00:08	192.168.0.101		00-1F-16-AE-81-79	HTTP://WWW.FACEBOOK.COM/	203.69.113.26	1
☐	2009-09-22 00:00:08	192.168.1.165		USER-3C1A75A06B	HTTP://WWW.FACEBOOK.COM/	203.69.113.48	1
☐	2009-09-22 00:00:10	192.168.2.23		00-1F-C6-25-58-2E	HTTP://0173054056.CHANNEL04.FACEBOOK.COM/	69.63.176.164	1
☐	2009-09-22 00:00:10	192.168.2.89		00-22-15-6E-E4-C6	HTTP://OPTIMIZED-BY.RUBICONPROJECT.COM/	203.190.124.21	2

搜索条件 1 日期范围：选择您想要查询数据所在的日期时间范围。

搜索条件 2、搜索条件 3：您可以依照以下条件进行筛选查询

IP 地址、用户名、计算机名称/MAC 地址、WebSite 网址名称

※请注意！

包括实时服务总表以及之后的其它通讯协议类别数据列表，搜索的条件若是三个都有设定，则搜寻结果必须三个条件都要符合；若是设定两个，则两个条件都要符合；如果只有设定一个，那么只要符合所设定的一个条件即可。

搜索：定义好筛选搜寻条件后，须按下此「搜索」按钮更新数据列表

邮寄：每个登入账号都会有属于该账号的电子邮件信箱 (在「系统权限管理」=>「使用者管理中设定」)，邮寄功能是可以将您目前所检视的页面画面，直接以 PDF 档案格式呈现并邮寄到您目前登入账号所归属的电子邮件信箱当中。

删除：选择删除列表中的记录，选择的方式则是用列表左方的方格勾选

PDF (本地监控版本才有)：若您是在安装 QnoSniff 专业版软件的 PC 上，可以按下 PDF 按钮将所呈现的画面数据转变成 PDF 档案，储存在别的硬盘空间或位置上。

前 10 页：	按此按钮数据列表会直接跳到前 10 页的数据，举例来说，若您现在是在第 201 笔数据列表画面，而您所选择是每页显示 10 笔数据，在按下前 10 页的按钮之后，会跳到第 101 笔资料列表画面。
上一页：	选择您现在正在浏览页面本页的前一页数据列表。
下一页：	选择您现在正在浏览页面本页的后一页数据列表。
下 10 页：	按此按钮数据列表会直接跳到后 10 页的数据，举例来说，若您现在是在第 1 笔数据列表画面，而您所选择是每页显示 10 笔数据，在按下下 10 页的按钮之后，会跳到第 101 笔资料列表画面。
跳到____页 每页显示____笔	您可以自己定义每页所显示的数据笔数，10 笔、30 笔、50 笔、100 笔；也可以透过下拉式选单，直接跳选想检视的页数。

数据列表字段

日期 / 时间：	用户访问该笔数据网站的时间
IP 地址：	用户的 IP
用户名：	用户的名称
计算机名称或 MAC 地址：	用户的计算机名称或 MAC 地址（解析不到计算机名称会直接显示成 MAC）
Website：	用户所访问的网站名称
Website IP Address：	用户所访问的网站 IP 地址
数量：	访问该网站的次数（每 15 分钟累加一次）

请注意！

有时候网站的网域名称虽然相同（例如：tw.yahoo.com），但是所对应的 IP 地址是的不同的，这种状况会将数据显示成另一笔数据；而用户访问同一网站的次数，每隔 15 分钟才会再累加一次，也就是说在这 15 分钟以内，不论访问该网站几次（包括主要网域名称「/」之后的网址），都只会算成一次。

8.3 电子邮件

电子邮件指的是用户收送电子邮件的流量记录，在网络通讯协议上所监控的是标准 SMTP 与 POP3。

搜索条件 1 日期范围：　选择您想要查询数据所在的日期时间范围。

搜索条件 2、搜索条件 3：　您可以依照以下条件进行筛选查询 IP 地址、用户名、计算机名称/MAC 地址、寄件者电子邮件信箱、收件者电子邮件信箱、电子邮件主题

搜索：　定义好筛选搜寻条件后，须按下此「搜索」按钮更新数据列表

邮寄：　每个登入账号都会有属于该账号的电子邮件信箱 (在「系统权限管理」=>「使用者管理中设定」)，邮寄功能是可以将您目前所检视的页面画面，直接以 PDF 档案格式呈现并邮寄到您目前登入账号所归属的电子邮件信箱当中。

删除：　选择删除列表中的记录，选择的方式则是用列表左方的方格勾选

PDF (本地监控版本才有)：　若您是在安装 QnoSniff 专业版软件的 PC 上，可以按下 PDF 按钮将所呈现的画面数据转变成 PDF 档案，储存在别的硬盘空间或位置上。

前 10 页：　按此按钮数据列表会直接跳到前 10 页的数据，举例来说，若您现在是在第 201 笔数据列表画面，而您所选择是每页显示 10 笔数据，在按下前 10 页的按钮之后，会跳到第 101 笔资料列表画面。

上一页：　选择您现在正在浏览页面本页的前一页数据列表。

下一页： 选择您现在正在浏览页面本页的后一页数据列表。

下 10 页： 按此按钮数据列表会直接跳到后 10 页的数据，举例来说，若您现在是在第 1 笔数据列表画面，而您所选择是每页显示 10 笔数据，在按下下 10 页的按钮之后，会跳到第 101 笔资料列表画面。

跳到____页
每页显示____笔 您可以自己定义每页所显示的数据笔数，10 笔、30 笔、50 笔、100 笔；也可以透过下拉式选单，直接跳选想检视的页数。

数据列表字段

日期 / 时间： 该笔电子邮件收送的时间。

IP 地址： 收送该笔电子邮件的用户 IP 地址

用户名： 收送电子邮件的用户名称

计算机名称或 MAC 地址： 收送电子邮件的计算机名称或是 MAC 地址（当计算机名称解析不到时会直接显示 MAC 地址信息

寄件者： 该封电子邮件的寄件者

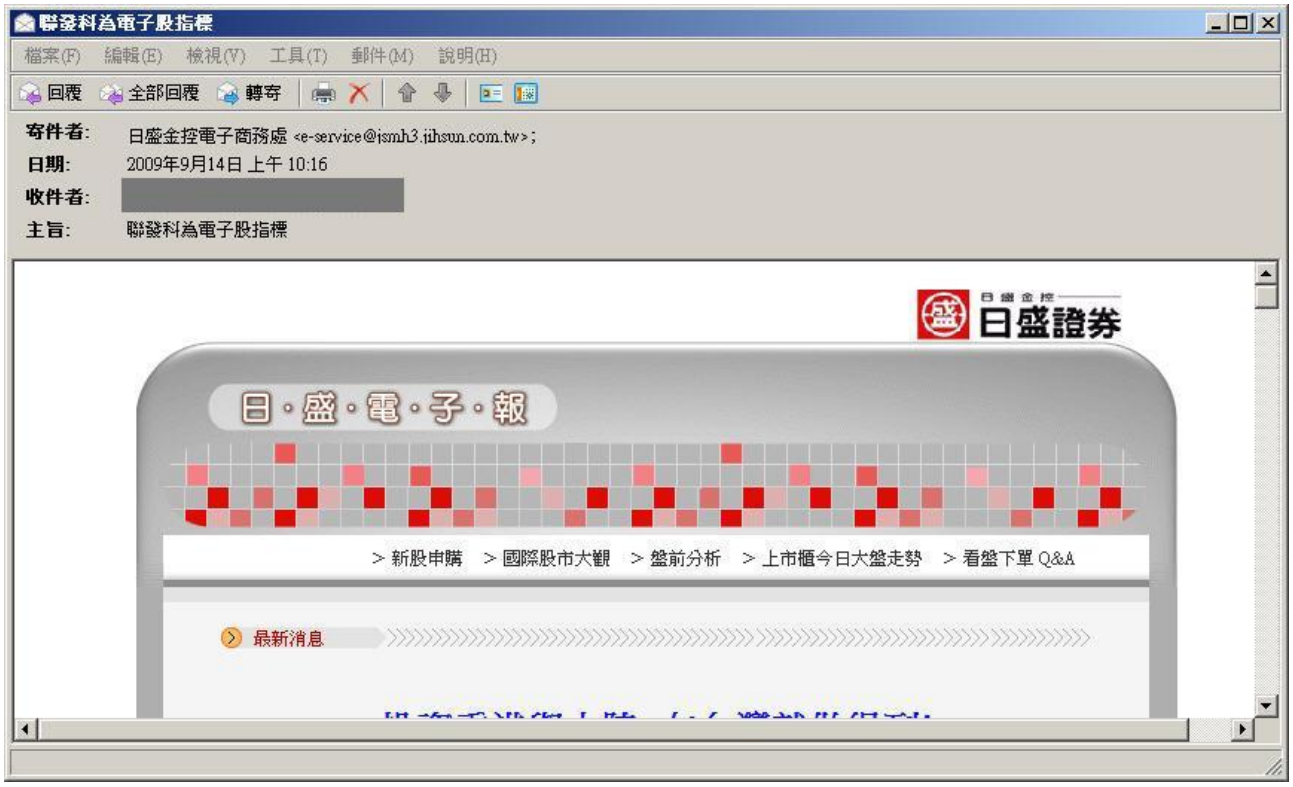
收件者： 该封电子邮件的收件者

主题： 该封电子邮件的主题

大小： 该封电子邮件的大小（整封邮件包含内文与附件)

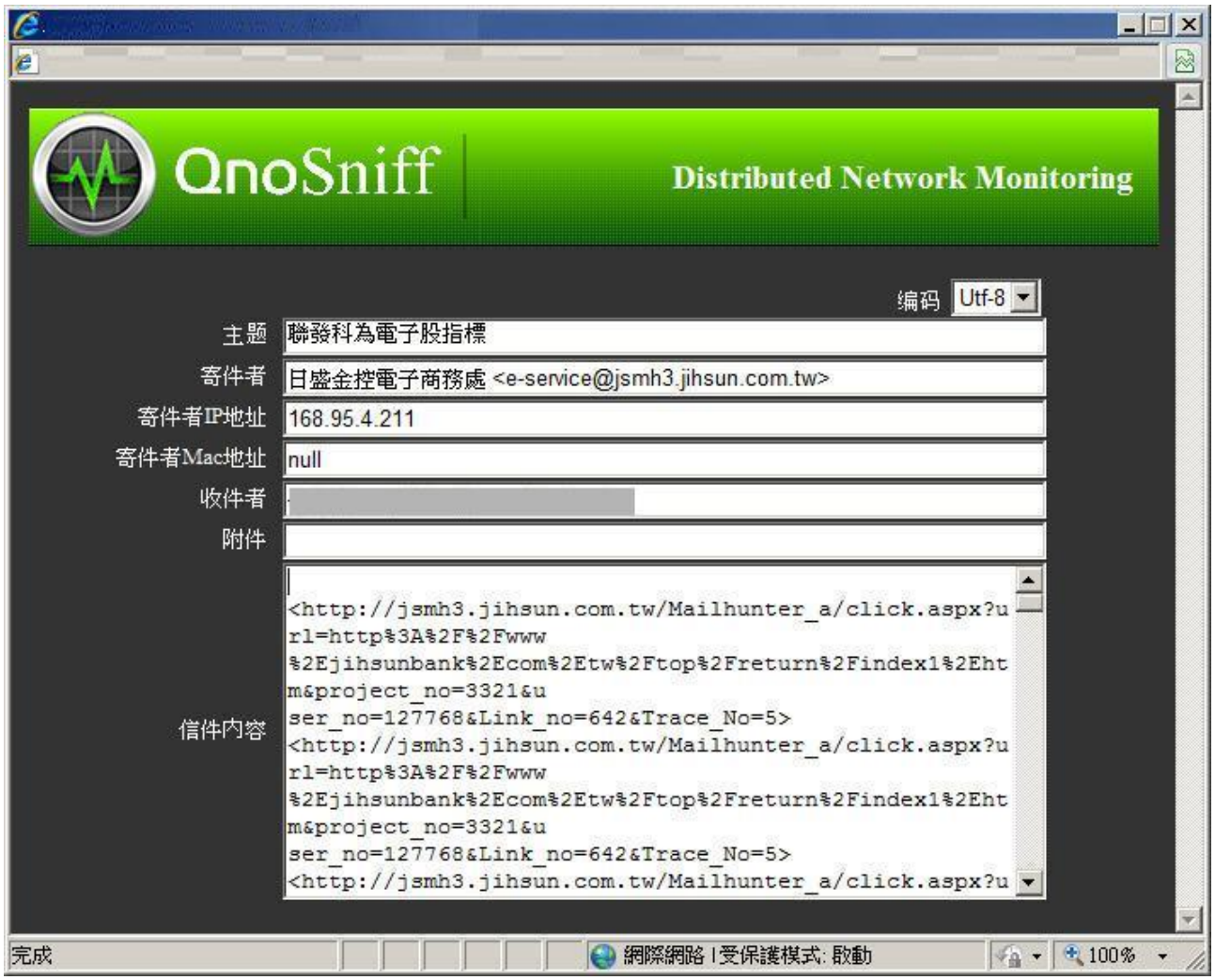
下载附件： 「Outlook Open」按钮是用来以 Outlook 或 Windows Mail 程序来打开邮件，在按下「Outlook Open」按钮之后，您可以先储存整个邮件，再用到储存邮件的地方用 Outlook 程序打开，或是直接以 Outlook 程序执行开启，附件档案此时便会在该程序中正常显示，所以此时就可以针对附件进行开启或储存动作。

请注意，若您是用远程登入远程监控（Web)版本，若是按下「Outlook Open」并选择直接开启邮件，邮件会以您预设浏览网页格式（HTML）的程序直接开启，或是您的系统内建开启 .eml 格式的执行程序，以下图为例就是直接用 Firefox 直接开启邮件内容。(右上方仍可选择以那种语系解析信件内容，共有 English 英文、Tradtional Chinese 繁体中文、Simplified Chinese 简体中文)



信件内容：　「Content」按钮是以 QnoSniff 专业版内建的程序开启，所以信件内文只能呈现纯文字内容，附件档案部分指会显示文件名称，并无法针对附件进行开启或储存动作，这是用来让使用者快速浏览某些只有文字叙述的电子邮件内容。

另外右上方目前可以选择繁体中文、简体中文与 UTF-8 编码来解析信件内容，若您的信件因为语系不同而出现乱码，您可以试着调整看看语系来看内容是否能正常显示。


QnoSniff
Distributed Network Monitoring
编码
Utf-8
主题
聯發科為電子股指標
寄件者
日盛金控電子商務處 <e-service@jsmh3.jihsun.com.tw>
寄件者IP地址
168.95.4.211
寄件者Mac地址
null
收件者
附件
信件內容
<http://jsmh3.jihsun.com.tw/Mailhunter_a/click.aspx?url=http%3A%2F%2Fwww%2Ejihsunbank%2Ecom%2Etw%2Ftop%2Freturn%2Findex1%2Ehtm&project_no=3321&user_no=127768&Link_no=642&Trace_No=5>
<http://jsmh3.jihsun.com.tw/Mailhunter_a/click.aspx?url=http%3A%2F%2Fwww%2Ejihsunbank%2Ecom%2Etw%2Ftop%2Freturn%2Findex1%2Ehtm&project_no=3321&user_no=127768&Link_no=642&Trace_No=5>
<http://jsmh3.jihsun.com.tw/Mailhunter_a/click.aspx?u
完成
網際網路 | 受保護模式: 啟動
100%

8.4 文件传输（FTP）

QnoSniff 专业版的档案传输目前指的是标准 FTP 通讯协议，包括主动模式与被动模式，若是采取其它加密型态的档案传输（如 SFTP、FTPS、FTPES 等），是不在 QnoSniff 专业版的监控范围内。

全选	日期/时间	IP地址	用户名	计算机名称/MAC地址	FTP主机	FTP用户名	方向	文件名称	文件大小(KB)
☐	2009-09-24 00:11:11	192.168.2.59		888TIGER-8CEAE2	210.64.12.133	Anonymous	DownLoad	god_crc.txtZ	10.597
☐	2009-09-24 00:14:03	192.168.0.229		00-1A-4D-FF-2E-4D	60.199.214.43	Anonymous	DownLoad	update.ini	0.313
☐	2009-09-24 00:14:03	192.168.0.229		00-1A-4D-FF-2E-4D	60.199.214.43	Anonymous	DownLoad	welcome.txt	0.135
☐	2009-09-24 00:21:01	192.168.2.59		888TIGER-8CEAE2	210.64.12.133	Anonymous	DownLoad	god_crc.txtZ	10.597
☐	2009-09-24 00:47:54	192.168.2.61		00-26-18-40-7A-79	210.64.12.133	Anonymous	DownLoad	god_crc.txtZ	10.597
☐	2009-09-24 00:47:57	192.168.2.61		00-26-18-40-7A-79	210.64.12.133	Anonymous	DownLoad	ExchangeDLL.dll	129.024
☐	2009-09-24 00:47:59	192.168.2.61		00-26-18-40-7A-79	210.64.12.133	Anonymous	DownLoad	Guild.rom	0.537

搜索条件 1 日期范围：　选择您想要查询数据所在的日期时间范围。

搜索条件 2、搜选条件 3：　您可以依照以下条件进行筛选查询

IP 地址、用户名、计算机名称/MAC 地址、FTP 主机、FTP 账号名称、方向、文件名称

搜索：　定义好筛选搜寻条件后，须按下此「搜索」按钮更新数据列表

邮寄：　每个登入账号都会有属于该账号的电子邮件信箱（在「系统权限管理」=>「使用者管理中设定」），邮寄功能是可以将您目前所检视的页面画面，直接以 PDF 档案格式呈现并邮寄到您目前登入账号所归属的电子邮件信箱当中。

删除：　选择删除列表中的记录，选择的方式则是用列表左方的方格勾选

PDF (本地监控版本才有)：　若您是在安装 QnoSniff 专业版软件的 PC 上，可以按下 PDF 按钮将所呈现的画面数据转变成 PDF 档案，储存在别的硬盘空间或位置上。

前 10 页：　按此按钮数据列表会直接跳到前 10 页的数据，举例来说，若您现在是在第 201 笔数据列表画面，而您所选择是每页显示 10 笔数据，在按下前 10 页的按钮之后，会跳到第 101 笔资料列表画面。

上一页：　选择您现在正在浏览页面本页的前一页数据列表。

下一页：	选择您现在正在浏览页面本页的后一页数据列表。
下 10 页：	按此按钮数据列表会直接跳到后 10 页的数据，举例来说，若您现在是在第 1 笔数据列表画面，而您所选择是每页显示 10 笔数据，在按下下 10 页的按钮之后，会跳到第 101 笔资料列表画面。
跳到___页 每页显示___笔	您可以自己定义每页所显示的数据笔数，10 笔、30 笔、50 笔、100 笔；也可以透过下拉式选单，直接跳选想检视的页数。

数据列表字段

全选：	可以透过勾选此方格，将此页面多笔数据一起做勾选，进行删除动作。
日期 / 时间：	该笔 FTP 上传下载动作记录的时间与日期。
IP 地址：	该笔 FTP 上传下载动作记录的内网 IP 地址。
用户名：	该笔 FTP 上传下载动作记录的内网用户名称。
计算机名称 / MAC 地址：	该笔 FTP 上传下载动作记录的内网计算机名称或 MAC 地址。
FTP 主机：	该笔 FTP 上传下载动作记录的 FTP 主机 IP 地址。
FTP 账号名：	该笔 FTP 上传下载动作记录的 FTP 登入账号名称。
方向：	该笔 FTP 上传下载动作记录的方向，是属于上传 (UpLoad) 还是下载 (Download)。
文件名称：	该笔 FTP 上传下载动作记录的目标文件名称，点选超级链接可以储存或是直接用相关程序开启档案内容。 **※请注意** 若您已经有在「基本设定」=>「数据库设定」=>「文件大小限制」有做设定 (例如 10MB)，FTP 上传/下载动作的目标档案若是超过此大小，是无法将完整档案收集至数据库当中的，数据库只会收集至您所设定的大小限制 (但是档案大小字段的数据显示，还是会显示真实的传输大小)，所以您在开启档案若是发生错误，很有可能就是因为有此限制，造成档案不完整而无法开启。
文件大小(KB)：	该笔 FTP 上传下载动作记录的目标档案大小。 ※数据库只会储存您所设定 FTP 文件大小限制，超过此大小的部分不会储存，但是文件大小会显示完整的档案数据大小，所以不会造成流量大小误判

8.5 点对点下载 (P2P)

QnoSniff 专业版可以针对某些现在热门的 P2P 下载软件行为，进行监控记录，目前可以判断这些流量为 P2P 的流量模式以及流量大小是多少，QnoSniff 专业版未来规划有可能会陆续加上 P2P 软件种类的流量识别。

全选	日期时间	IP地址	用户名	计算机名称/MAC地址	上传速度 (KB/S)	下载速度 (KB/S)	上传大小 (KB)	下载大小 (KB)
☐	2009-09-24 00:06:14	192.168.0.4		F1	0.0	0.0	0.21	0.29
☐	2009-09-24 00:06:15	192.168.0.101		00-1F-16-AE-81-79	2.88	2.14	2594.21	1926.94
☐	2009-09-24 00:06:15	192.168.0.113		00-16-E6-DC-15-19	0.0	0.0	3.83	3.19
☐	2009-09-24 00:06:15	192.168.0.125		00-1F-1F-47-C3-41	0.0	0.0	4.49	2.0
☐	2009-09-24 00:06:15	192.168.0.132		CAT-01	15.63	54.11	14070.21	48698.41
☐	2009-09-24 00:06:15	192.168.0.132		CAT-01	24.17	13.96	21751.15	12568.22
☐	2009-09-24 00:06:15	192.168.0.132		CAT-01	0.01	0.01	5.27	8.55
☐	2009-09-24 00:06:15	192.168.0.162		00-23-F8-2C-39-F9	0.0	0.01	3.1	4.93
☐	2009-09-24 00:06:15	192.168.0.163		00-00-E8-7C-89-42	0.06	1.51	50.74	1361.39
☐	2009-09-24 00:06:15	192.168.0.167		HOME	0.01	0.01	5.59	6.61

搜索条件 1 日期范围：　选择您想要查询数据所在的日期时间范围。

搜索条件 2：　您可以依照以下条件进行筛选查询
IP 地址、用户名、计算机名称/MAC 地址

搜索：　定义好筛选搜寻条件后，须按下此「搜索」按钮更新数据列表

邮寄：　每个登入账号都会有属于该账号的电子邮件信箱 (在「系统权限管理」=>「使用者管理中设定」)，邮寄功能是可以将您目前所检视的页面画面，直接以 PDF 档案格式呈现并邮寄到您目前登入账号所归属的电子邮件信箱当中。

删除：　选择删除列表中的记录，选择的方式则是用列表左方的方格勾选

PDF (本地监控版本才有)：　若您是在安装 QnoSniff 专业版软件的 PC 上，可以按下 PDF 按钮将所呈现的画面数据转变成 PDF 档案，储存在别的硬盘空间或位置上。

前 10 页：　按此按钮数据列表会直接跳到前 10 页的数据，举例来说，若您现在是在第 201 笔数据列表画面，而您所选择是每页显示 10 笔数据，在按下前 10 页的按钮之后，会跳到第 101 笔资料列表画面。

上一页：　选择您现在正在浏览页面本页的前一页数据列表。

下一页：　选择您现在正在浏览页面本页的后一页数据列表。

下 10 页：	按此按钮数据列表会直接跳到后 10 页的数据，举例来说，若您现在是在第 1 笔数据列表画面，而您所选择是每页显示 10 笔数据，在按下下 10 页的按钮之后，会跳到第 101 笔资料列表画面。
跳到___页 每页显示___笔	您可以自己定义每页所显示的数据笔数，10 笔、30 笔、50 笔、100 笔；也可以透过下拉式选单，直接跳选想检视的页数。

数据列表字段

全选：	可以透过勾选此方格，将此页面多笔数据一起做勾选，进行删除动作。
日期 / 时间：	该笔被判断为 P2P 上传/下载行为动作的时间与日期。
IP 地址：	该笔被判断为 P2P 上传/下载行为动作的内网 IP 地址。
用户名：	该笔被判断为 P2P 上传/下载行为动作的内网用户名称。
计算机名称 / MAC 地址：	该笔被判断为 P2P 上传/下载行为动作的内网计算机名称或是 MAC 地址。
上传速率 (KB/S)：	该笔被判断为 P2P 上传/下载行为动作的平均上传流量速率。
下载速率 (KB/S)：	该笔被判断为 P2P 上传/下载行为动作的平均下载流量速率。
上传大小 (KB)：	该笔被判断为 P2P 上传/下载行为动作的目前上传档案大小。
下载大小 (KB)：	该笔被判断为 P2P 上传/下载行为动作的目前下载档案大小。

8.6 Telnet

QnoSniff 专业版所针对的是标准 Telnet 网络通讯协议标准，如果您的用户使用 Telnet 有改变用其它的通讯端口进行联机，或是加密型的 SSH，QnoSniff 专业版目前是不支持此类的非标准协议或加密协议。

搜索条件 1 日期范围：选择您想要查询数据所在的日期时间范围。

搜索条件 2、搜索条件 3：您可以依照以下条件进行筛选查询

IP 地址、用户名、计算机名称/MAC 地址、网站 IP 地址、网站名称、 Telnet 账号名称

搜索：定义好筛选搜寻条件后，须按下此「搜索」按钮更新数据列表

邮寄：每个登入账号都会有属于该账号的电子邮件信箱 (在「系统权限管理」=>「使用者管理中设定」)，邮寄功能是可以将您目前所检视的页面画面，直接以 PDF 档案格式呈现并邮寄到您目前登入账号所归属的电子邮件信箱当中。

删除：选择删除列表中的记录，选择的方式则是用列表左方的方格勾选

PDF (Application 版本才有)：若您是在安装 QnoSniff 专业版软件的 PC 上，可以按下 PDF 按钮将所呈现的画面数据转变成 PDF 档案，储存在别的硬盘空间或位置上。

前 10 页：按此按钮数据列表会直接跳到前 10 页的数据，举例来说，若您现在是在第 201 笔数据列表画面，而您所选择是每页显示 10 笔数据，在按下前 10 页的按钮之后，会跳到第 101 笔资料列表画面。

上一页：选择您现在正在浏览页面本页的前一页数据列表。

下一页：选择您现在正在浏览页面本页的后一页数据列表。

下 10 页：	按此按钮数据列表会直接跳到后 10 页的数据，举例来说，若您现在是在第 1 笔数据列表画面，而您所选择是每页显示 10 笔数据，在按下下 10 页的按钮之后，会跳到第 101 笔资料列表画面。
跳到___页 每页显示___笔	您可以自己定义每页所显示的数据笔数，10 笔、30 笔、50 笔、100 笔；也可以透过下拉式选单，直接跳选想检视的页数

数据列表字段

全选：	可以透过勾选此方格，将此页面多笔数据一起做勾选，进行删除动作。
日期 / 时间：	该笔 Telent 记录动作的时间
IP 地址：	该笔 Telnet 记录动作的内网 IP 地址
用户名：	该笔 Telnet 记录动作的内网用户名称
计算机名称 / MAC 地址：	该笔 Telnet 记录动作的内网计算机名称或 MAC 地址
网站 IP 地址：	该笔 Telnet 记录的目的地 IP 地址
网址：	该笔 Telnet 记录的目的地网址或网域名称
Telnet 账号名：	该笔 Telent 记录的登入账号名称
内容  ：	该笔 Telnet 记录的详细内容信息，按下此按钮后会出以下内容信息

网站 IP 地址：您 Telnet 远程登入的目的地 IP 地址

网址：您 Telnet 远程登入的目的地的网址或网域名称

日期 / 时间：该笔 Telnet 登入动作的时间与日期

内容页面：显示 Telnet 的登入信息内容

编码：有繁体编码、简体编码以及 UTF-8 编码可以做切换

8.7 聊天信息

QnoSniff 专业版目前可以进行监控与记录的应用程序如下：

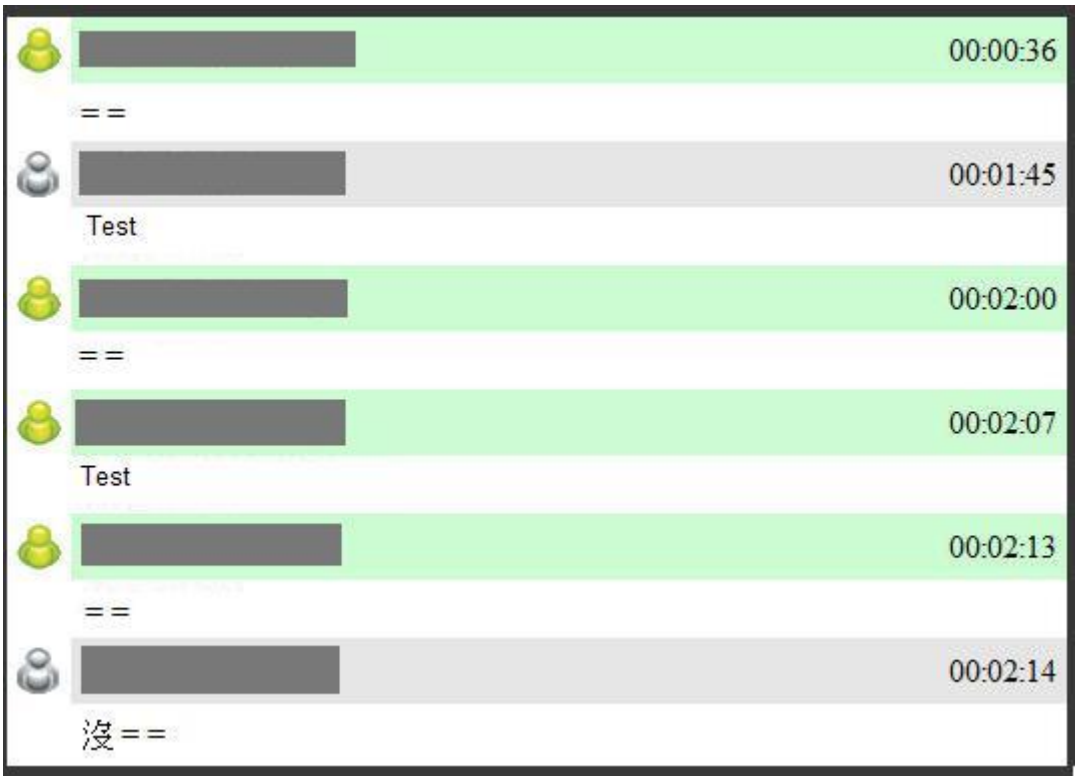
【1】MSN (Live Message / 8.5 / 8.0)
【2】QQ (并须将用户 QQ 账号、密码输入在「基本设定」=>「服务设定」内的「IM：QQ 号码设定才能够进行监控与记录」，并且目前无法对 QQ「所有 TM」版本进行监控与记录)
【3】Yahoo Message
【4】Google Talk

搜索条件 1 日期范围：	选择您想要查询数据所在的日期时间范围。
搜索条件 2、搜索条件 3：	您可以依照以下条件进行筛选查询 IP 地址、用户名、计算机名称/MAC 地址、本地账号、对方账号、IM 类别
搜索：	定义好筛选搜寻条件后，须按下此「搜索」按钮更新数据列表
邮寄：	每个登入账号都会有属于该账号的电子邮件信箱 (在「系统权限管理」=>「使用者管理中设定」)，邮寄功能是可以将您目前所检视的页面画面，直接以 PDF 档案格式呈现并邮寄到您目前登入账号所归属的电子邮件信箱当中。
删除：	选择删除列表中的记录，选择的方式则是用列表左方的方格勾选
PDF (本地监控版本才有)：	若您是在安装 QnoSniff 专业版软件的 PC 上，可以按下 PDF 按钮将所呈现的画面数据转变成 PDF 档案，储存在别的硬盘空间或位置上。

前 10 页：	按此按钮数据列表会直接跳到前 10 页的数据，举例来说，若您现在是在第 201 笔数据列表画面，而您所选择是每页显示 10 笔数据，在按下前 10 页的按钮之后，会跳到第 101 笔资料列表画面。
上一页：	选择您现在正在浏览页面本页的前一页数据列表。
下一页：	选择您现在正在浏览页面本页的后一页数据列表。
下 10 页：	按此按钮数据列表会直接跳到后 10 页的数据，举例来说，若您现在是在第 1 笔数据列表画面，而您所选择是每页显示 10 笔数据，在按下下 10 页的按钮之后，会跳到第 101 笔资料列表画面。
跳到____页 每页显示____笔	您可以自己定义每页所显示的数据笔数，10 笔、30 笔、50 笔、100 笔；也可以透过下拉式选单，直接跳选想检视的页数

数据列表字段

全选：	可以透过勾选此方格，将此页面多笔数据一起做勾选，进行删除动作。
日期 / 时间：	该笔实时通讯的通讯时间
IP 地址：	该笔实时通讯所使用的内网 IP 地址
用户名：	该笔实时通讯所使用的用户名称
计算机名称 / MAC 地址：	该笔实时通讯所使用的计算机名称
本地账号：	该笔实时通讯在上述所列 IP / 计算机上所使用的账号
对方账号：	该笔实时通讯交谈的另一个账号
IM 类别：	该笔实时通讯类别是属于 MSN、QQ、YahooMessage 或是 Google Talk。
记录：	该笔通讯记录来回的讯息总共有几笔数量，点选该数字的超级链接后，会另外跳出详细实时通讯记录内容 (如下图)。



※灰色遮蔽的部分在您的软件上会正常显示账号内容，以上图标只是范例。

日期/时间、IP 地址、用户名、计算机名称/MAC 地址、IM 类别、记录都可接点选该字段进行排序。

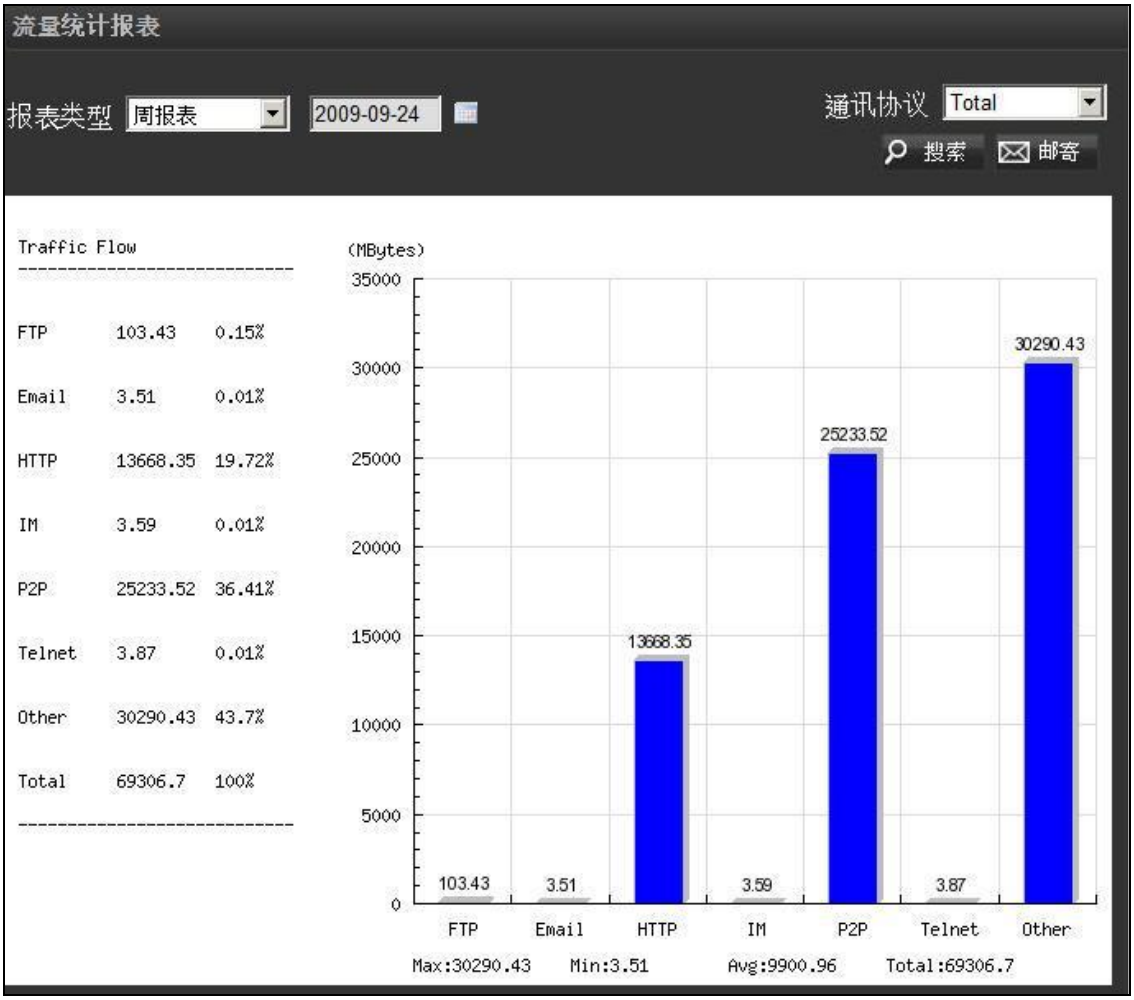
九、统计信息

本章节介绍 QnoSniff 专业版的流量统计功能，总共有流量统计报表、部门流量排名总表、使用者流量排名总表，可以依据部门别、网络通讯协议类别以及所自订的时间，充分的呈现内网用户网络流量以及应用程序使用各种情形，所有统计报表的数值与报表图标是**每 15 分钟**更新一次统计内容，所以 15 分钟以内的数值与图示并不会有变动。

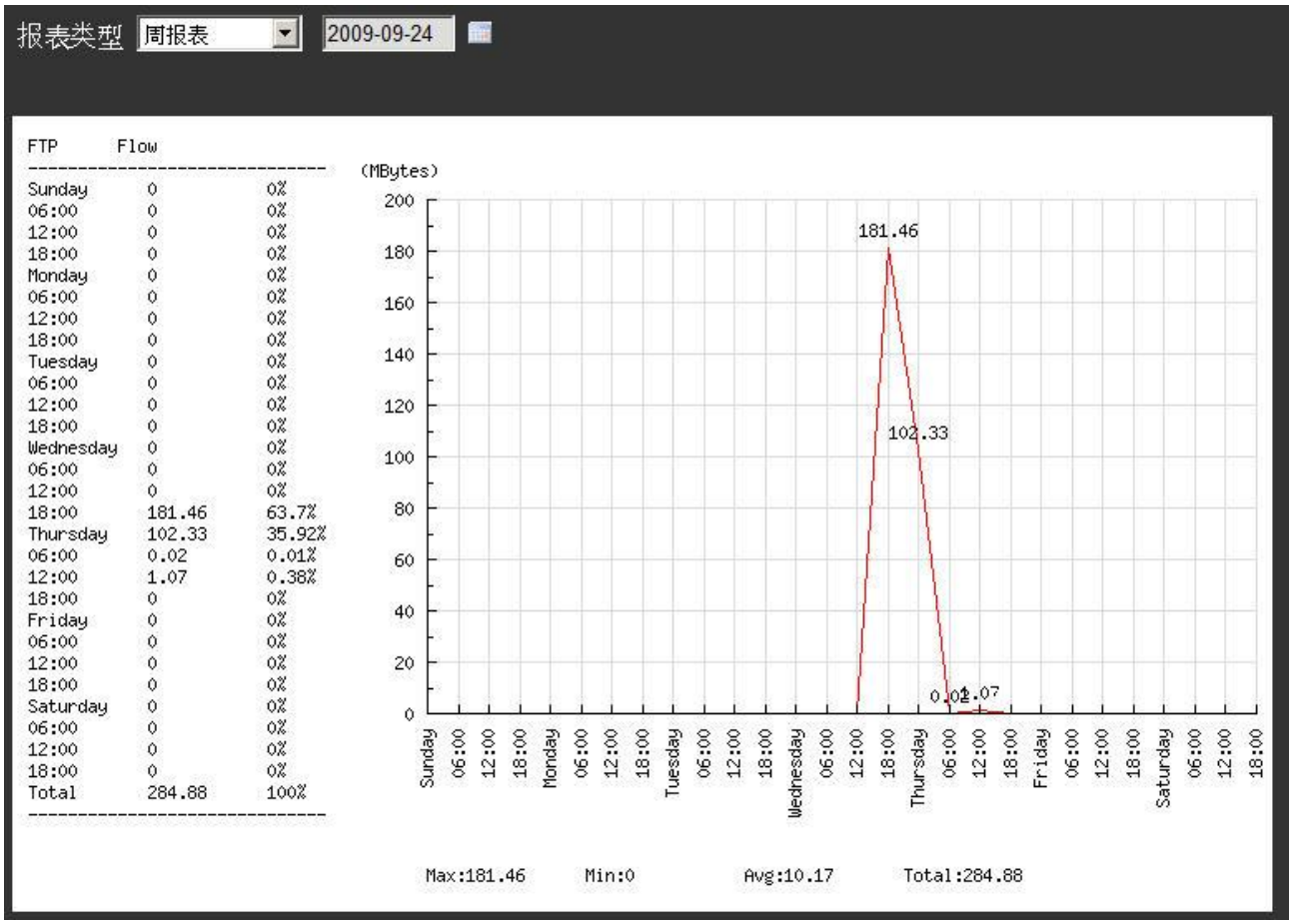
9.1 流量统计报表

这部分的报表主要是以图表与统计数字，来显示各个通讯协议下的流量统计信息。

左方有 Traffic Flow 列表，在通讯协议选择「Total」的时后，会显示各个通讯协议在您所选择的时间区段内的统计数值与所占总流量的百分比，右方则是图示，在选择时间区段以及选择通讯协议过后，需要再按一下「搜寻」按钮，以使数据数值能够更新到您所选择的时间区段，以及通讯协议所正确对应的数据内容。



若您的通讯协议不是选择「Total」而是选择单一通讯协议例如「E-mail」(电子邮件)，左方的 Traffic Flow 列表转化成时间纵轴的方式，显示各个时间区段内的流量统计，若您选择日报表，则是 0-23 小时，每一个小时显示统计数据；若您选择周报表，则是七天并且每六个小时为一个时间区段显示统计数据若您选择月报表，则显示的是该月 1 日到 30 或 31 日，每一日显示统计数据。

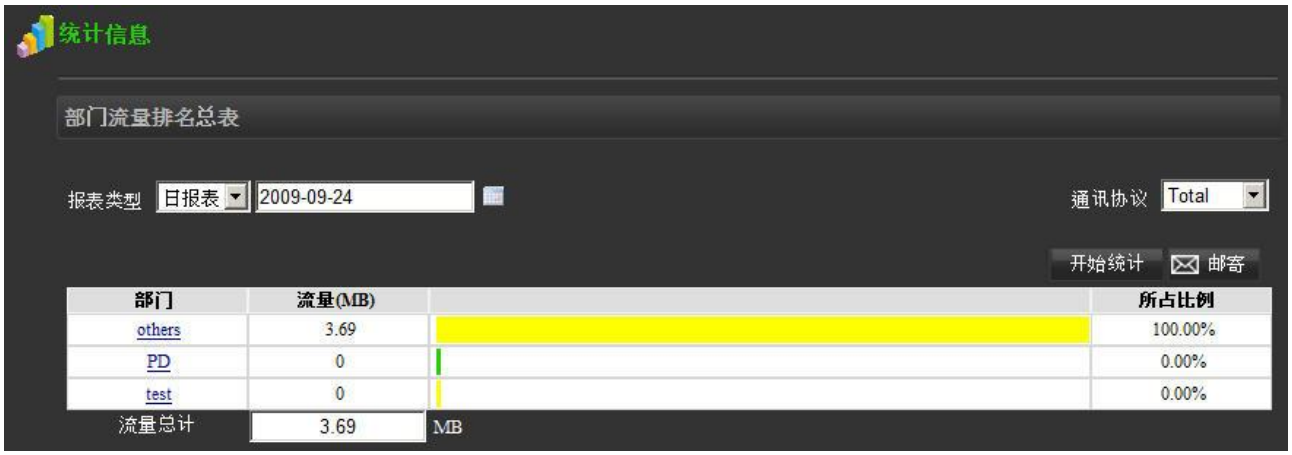


FTP	Flow	
Sunday	0	0%
06:00	0	0%
12:00	0	0%
18:00	0	0%
Monday	0	0%
06:00	0	0%
12:00	0	0%
18:00	0	0%
Tuesday	0	0%
06:00	0	0%
12:00	0	0%
18:00	0	0%
Wednesday	0	0%
06:00	0	0%
12:00	0	0%
18:00	181.46	63.7%
Thursday	102.33	35.92%
06:00	0.02	0.01%
12:00	1.07	0.38%
18:00	0	0%
Friday	0	0%
06:00	0	0%
12:00	0	0%
18:00	0	0%
Saturday	0	0%
06:00	0	0%
12:00	0	0%
18:00	0	0%
Total	284.88	100%

邮寄、PDF (只有本地监控版本)功能仍然可以在统计列表中使用，直接将查询的报表 / 图标数据转成 PDF 档案或是直接以 PDF 档案寄送电子邮件到管理者电子邮件信箱。

9.2 部门流量排名总表

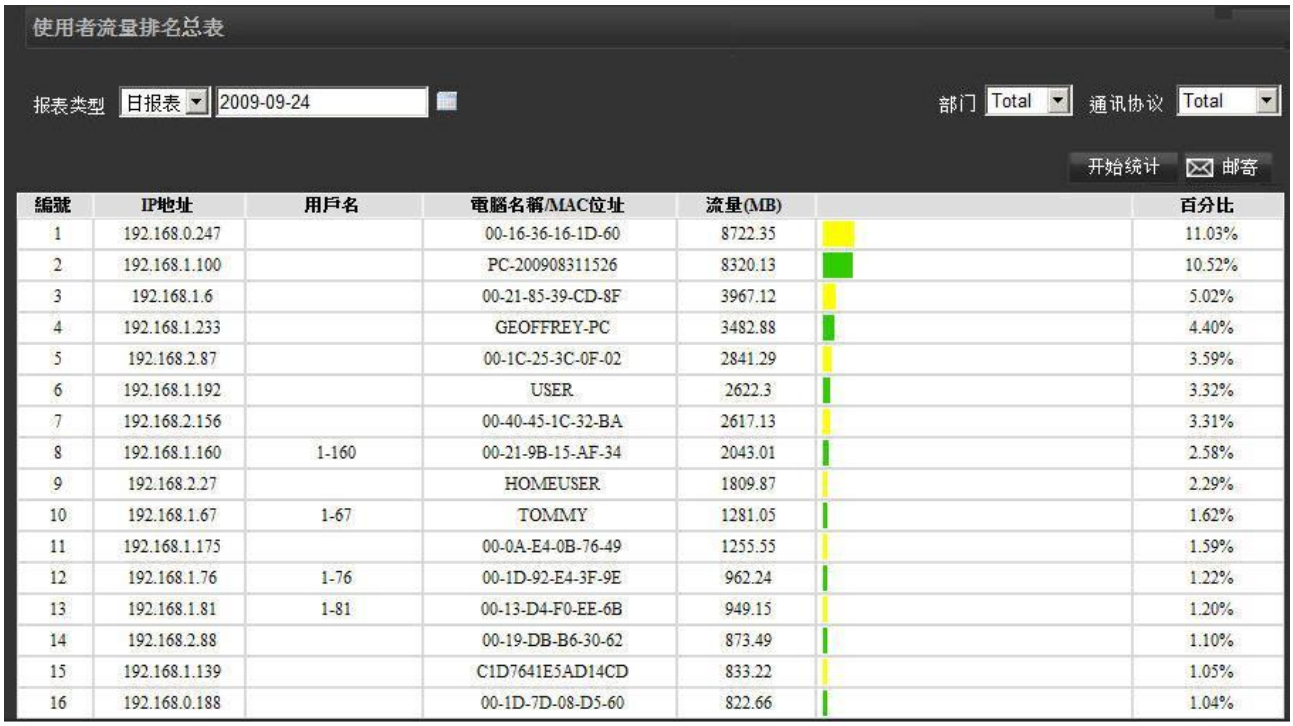
部门流量排名总表，主要是用部门所使用的流量来排序，并且可以针对不同通讯协议，来查询各个部门的使用流量状况，例如所有部门的实时通讯流量，从最多到最小的流量统计列表内容。



您可以依照您想检视的时间区段、网络通讯协议类别，来显示您所有部门的流量统计状况以及数值，若您想检视某个部门、在某个通讯协议下，该部门下的成员流量使用统计明细，可以直接按下部门名称的超级链接，就会显示出该部门（例如 Sales）以下成员，使用某种通讯协议（例如 E-mail）的流量统计排名与数值、百分比等（如下图例）。

9.3 使用者流量排名总表

使用者流量排名总表，是针对所有单一内网用户所做的流量统计与排序，也可以依不同时间区段、部门别以及网络通讯协议类别，选择流量统计内容与排序列表。



編號	IP地址	用戶名	電腦名稱/MAC位址	流量(MB)	百分比
1	192.168.0.247		00-16-36-16-1D-60	8722.35	11.03%
2	192.168.1.100		PC-200908311526	8320.13	10.52%
3	192.168.1.6		00-21-85-39-CD-8F	3967.12	5.02%
4	192.168.1.233		GEOFFREY-PC	3482.88	4.40%
5	192.168.2.87		00-1C-25-3C-0F-02	2841.29	3.59%
6	192.168.1.192		USER	2622.3	3.32%
7	192.168.2.156		00-40-45-1C-32-BA	2617.13	3.31%
8	192.168.1.160	1-160	00-21-9B-15-AF-34	2043.01	2.58%
9	192.168.2.27		HOMEUSER	1809.87	2.29%
10	192.168.1.67	1-67	TOMMY	1281.05	1.62%
11	192.168.1.175		00-0A-E4-0B-76-49	1255.55	1.59%
12	192.168.1.76	1-76	00-1D-92-E4-3F-9E	962.24	1.22%
13	192.168.1.81	1-81	00-13-D4-F0-EE-6B	949.15	1.20%
14	192.168.2.88		00-19-DB-B6-30-62	873.49	1.10%
15	192.168.1.139		C1D7641E5AD14CD	833.22	1.05%
16	192.168.0.188		00-1D-7D-08-D5-60	822.66	1.04%

一开始进入画面的时候，会以所有使用者、所有类型的流量统计做排序，包括实际流量统计(MB)以及所占百分比，若您要查询某部分，或是其它通讯协议，皆可以透过右方的下拉式选单做筛选，则选择新的查询条件之后，请您注意一定要再按下「开始统计」按钮，数据才会开始更新符合您的新筛选条件。

十、注销系统

当您不再使用 QnoSnif 专业版，可以按下「注销系统」选单离开 QnoSniff 专业版操作主页面。

在远程登入离开后自然是离开网页，若是在安装 QnoSniff 专业版的 PC 上，离开本地监控版本的主控页面后，右下角的系统列仍然会有 QnoSniff 专页版的 Icon，表示 QnoSniff 专页版仍然在后台运行抓取数据（绿色图标表示正常与路由器联机中，灰色的图示表示未与路由器正常联机)。

若您需要关闭整个 QnoSniff 专业版，包括收集数据功能，就需要在系统列的 Icon 上按鼠标右键，选择选单中的「Exit Minitor」离开系统，QnoSniff 专业版会再询问您一次是否要确认关闭整个 QnoSniff 专业版系统，按下确定后，QnoSniff 专业版系统会进行关闭程序，大约在 10~15 秒内，系统列的 Icon 会因为整个系统关闭完成而消失。

※请注意！

若关闭整个 QnoSniff 专业版，包括数据收集功能，这段关闭的时间之内是没有数据的，QnoSniff 专业版的数据库也不会有数据，所以在统计的数据中也不会出现这段时间的数据内容。

在系统列的 Icon 上按下鼠标右键会跳出以下选单：

1.Information：有 QnoSniff 专业版的版权信息、所使用的监听网卡设备、QnoSniff 专业版的软件版本，以及现在储存数据所占用的大小。

2.Login System：若您还未成功登入 QnoSniff 专业版主控台，可以点选此选项进行登入。

3.Enable/Disable Auto：可以启用（Enable）或是 关闭（Disable）开机后自动启用 QnoSniff 专业版于背景运行，您若是第一次选择自动运行，则在下次开机的时候就会生效随着开机后自动启用 QnoSniff 专业版。

4.Exit Monitror：离开并关闭整个 QnoSniff 专业版，包括数据收集的功能，按下后系统会跳出以下视

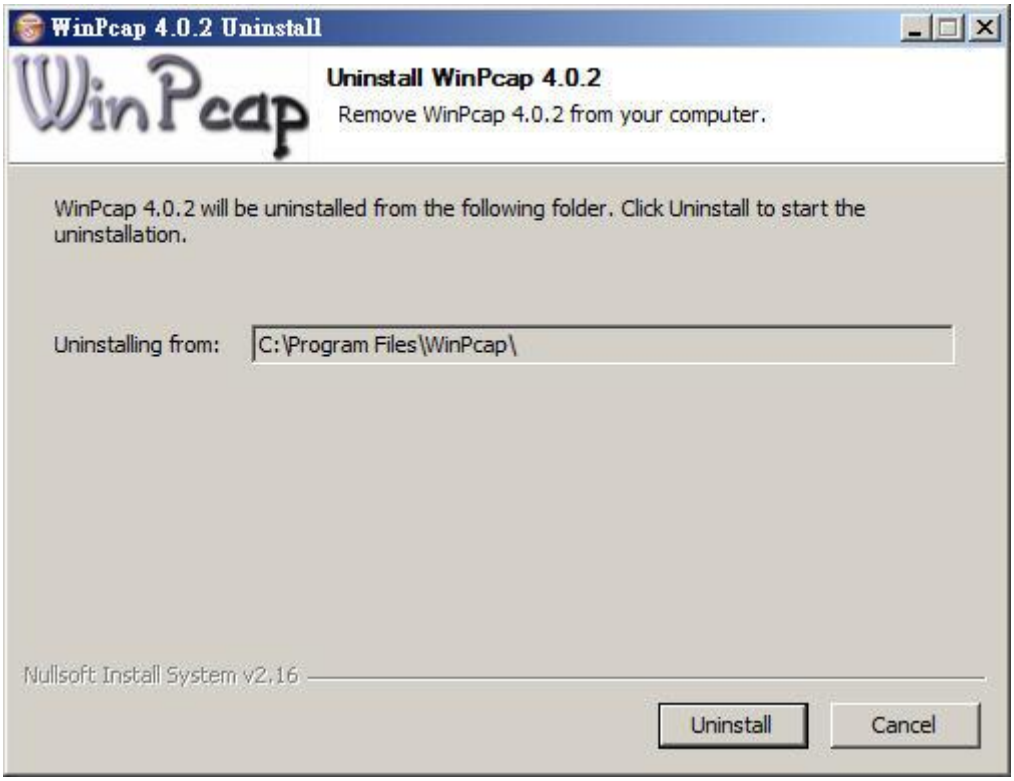
窗再次询问您是否确认离开并关闭整个系统，按下「是」后，QnoSniff 专业版系统会进行关闭程序，大约在 10~15 秒内系统拖盘的图标会因为整个系统关闭完成而消失。

十一、卸载 QnoSniff

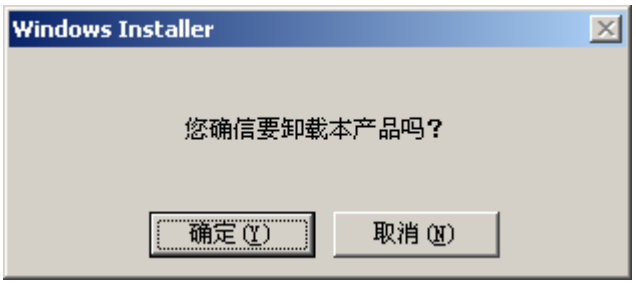
当您想要卸载 QnoSniff 专业版，请到系统程序集寻找 QnoSniff 数据夹，该数据夹下有会有「Uninstall」选项如右图 

选择 Uninstall 就会开始进行卸载程序，或是到「控制面板」的「更改或删除程序」，点选 QnoSniff 进行移除程序动作。

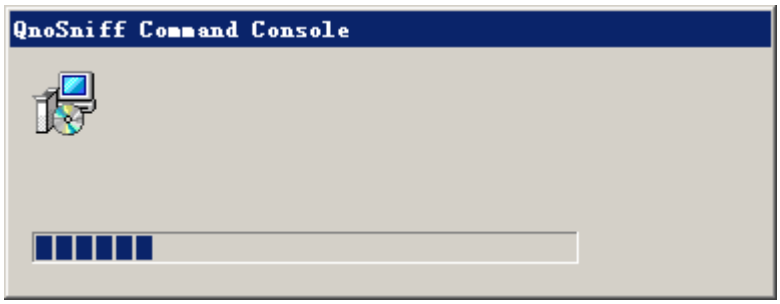
卸载程序首先会移除 WinPcap 如下图，若您是直接到控制面板选择卸载 QnoSniff 专业版，可能会跳过反安装 WinPcap 这部分，但是一样能达成完全删除的效果。



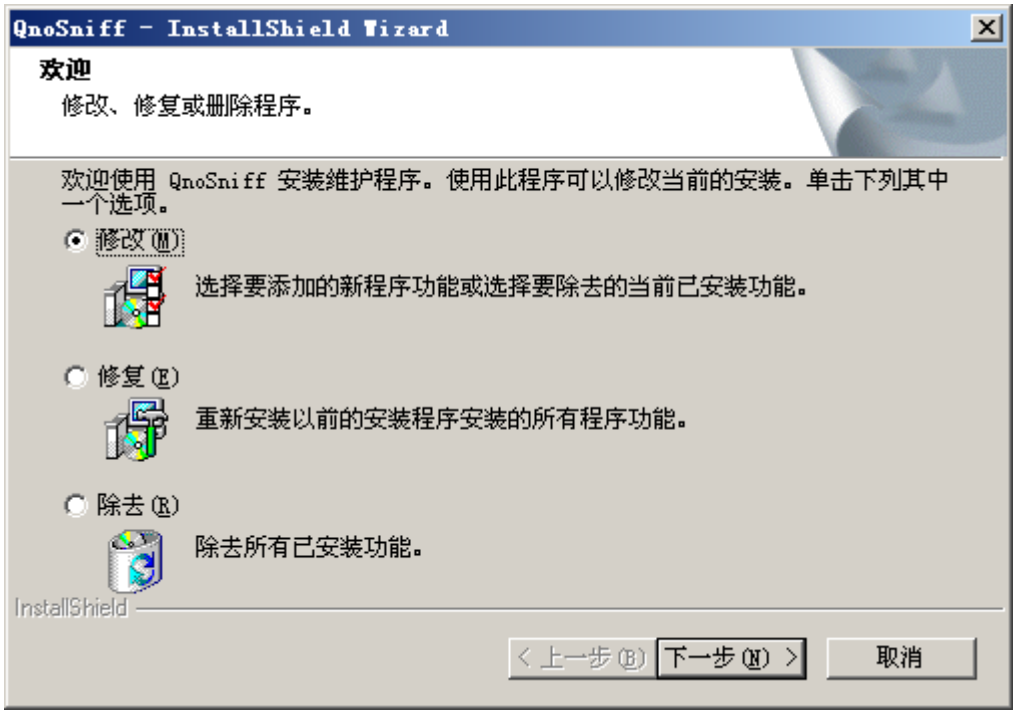
按下 Uninstall 进行移除 WinPcap 组件，移除完成画面如下，请按下 Finish 继续卸载程序，会跳出是否确认删除程序信息，请按下「是」



搜集解除安装相关资料中



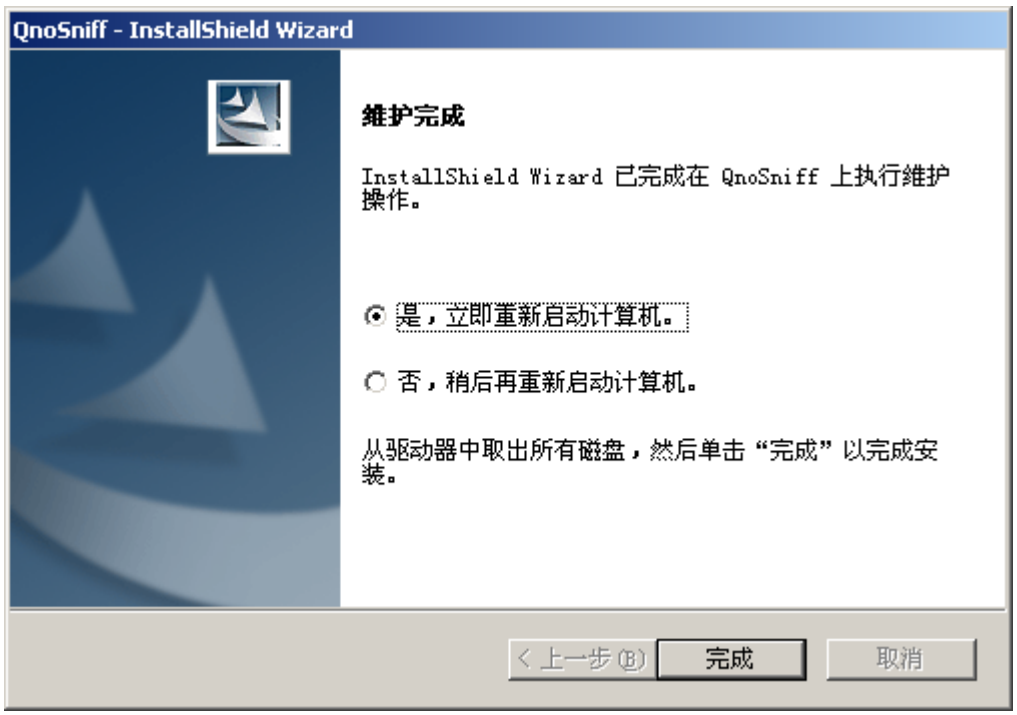
跳出软件维护画面如下，请选择「移除(R)」并按下一步继续



询问是否确认移除，请按「是」便会开始进行主程序解除安装程序

进行完解除安装后，会挑出要您重新开机的讯息，若您仍有其它作业尚未完成并且未做储存动作，可以选择稍后再自行重新启动计算机，若无其它疑虑，则可立刻重开机，请注意必须要将计算机重开机后，整个安装

程序才算完成。



重新开机后，请到您之前所安装 QnoSniff 专业版软件的硬盘位置（如 C:\QnoSniff 

），

您所收集到的数据库内容仍然会留在此档案夹中如下图

若您之后再重新安装 QnoSniff 专业版并且安装在相同的硬盘位置，这些数据仍可以与 QnoSniff 专业版主控台做连结，进行数据检视与筛选；若是您确认往后都使用不到这些数据库内容，便可将整个 QnoSniff 数据夹进行删除，已增加您硬盘的剩余可用空间。

附录：Qno 技术支持信息

更多有关侠诺产品技术信息，除了可以登录侠诺宽带讨论区、参照 FTP 服务器的相关实例；或是进一步联系侠诺各经销商技术部门、或侠诺大陆技术中心取得相关协助。

侠诺科技官方网站：http：//www.Qno.cn

各大经销商服务联系方式：

用户可以登录网站先上服务页面查询各大经销联系方法：

http://www.qno.cn/web/where_buy.asp

侠诺技术中心：

电子邮件信箱：service@mail.qno.cn