第六章 中小企业安全路由器警示及监控

中小企业的网管，背负着整个企业网络的责任，网络若是发生问题时，往往大家第一个找的是网管。因此对于网管而言，如何能第一时间了解网络情况，或者于发生事件时第一时间了解发生什么情况。在老总询问时，网管若能很快地明白发生了什么事，或者是还没有接到询问，就先了解情况，事先因应了。

由于企业网络对外主要由路由器控制，因此可以给网管比较大的帮助。Qno 侠诺路由器提供了多种功能，协助网管快速了解网络运作。以下针对中小企业常见的网络警示及监控相关问题，及对应的产品，具体说明如下：

项次	问题	功能
1	如何进行网络状态的了解？如何针对特定应用或用户了解带宽使用情况？	系统状态实时监控、流量统计
2	如何选择日志记录的内容？	系统日志配置
3	如何在特定时间通知网管？如何进行语音告警功能配置？如何保存完整日志？如何架设日志服务器？	语音告警功能、电子邮件告警功能、
4	如何测试网络质量？	在线联机测试

6．1 系统状态实时监控

侠诺路由器的管理功能可以快速于一个页面提供系统目前运作信息，这个功能可帮助网管快速了解不同广域网端口的运作情况，是网管必须用到的重要工具。这个页面在接受厂商进行技术支持时也是挺重要的，其中的广域网 IP 可帮助外部用户登入路由器，进行管理。

这个页面提供信息包括局域或广域端口名称，目前端口联机状态 、IP 地址、网络实体位置、子网掩码、默认网关、域名解析服务器、网络侦测、收到的封包数量、传送的封包数量、全部的进出封包数量统计、收到的封包 Byte 流量统计、传送的封包 Byte 流量统计 、

全部进出的封包 Byte 流量统计、收到的错误封包统计以及端口丢弃的封包统计、联机数 、新联机数、上传带宽使用率、下载带宽使用率等信息。

系统状态

接口位置	局域网接口	广域网1接口	广域网2接口
机器名称	ixp0	ixp1	ixp2
目前端口连线状态	联机	联机	掉线
IP地址	192.168.1.1	60.248.80.100	0.0.0.0
网路实体位置	10-2f-d4-76-14-5d	26-0c-35-3c-74-b4	00-db-78-d2-79-a9
子网掩码	255.255.255.0	255.255.255.0	0.0.0.0
预设网关	---	60.248.80.254	0.0.0.0
域名解析服务地址	192.168.1.1	168.95.1.1 0.0.0.0	0.0.0.0
线路侦测机制	---	测试成功	测试失败
收到的封包数量	5579	0	0
传送的封包数量	5049	0	0
全部的封包数量	10628	0	0
统计收到的封包Byte数量	674266	0	0
统计传送的封包Byte数量	1629421	0	0
统计全部的封包Byte数量	2303687	0	0
接收Bytes/秒	0	0	0
传送Bytes/秒	0	0	0
统计收到的错误封包统计	0	0	0
统计收到的错误封包统计	0	0	0
联机数	---	0	2
新联机数/秒	---	0	0
上传带宽使用率(%)	---	0	0
下载带宽使用率(%)	---	0	0

刷新

图一：系统状态实时监控于一个页面提供整体广域端的运作情况，可协助网管于第一眼了解整体情况。

6．2 流量统计

当网管发现网络中某些部份出现异状时，可能需要更详细地查看不同的信息，以找出具体的问题所在。Qno 侠诺路由器中提供六种显示流量统计的信息，来提供管理者对于流量有更好的管理与控制。这六个信息分别为对外对内 IP 地址流量的置、对外对内不同服务端口的流量、对外对内不同 IP 地址的联机数。

网络流量显示状态：对内流量IP联机数

来源IP地址	通讯协议	来源端口	目的IP地址	目的端口	bytes/sec	%
192.168.1.100	TCP	1678	202.108.15.42	80	51	76
192.168.1.100	TCP	1672	202.108.9.30	80	4	5

图二：流量统计功能可显示较详细的不同 IP 地址或是服务端口的流量，协助作细部的除错工作。

另外特定 IP 及端口状态功能则能让网管人员可以针对某一 IP 或某一特定端口去查询此 IP 去访问的目的地址，或是有哪些人使用这个服务端口。其目的可以方便找出某些需要认证的网站无法走多 WAN 端口而必须走单一个 WAN 端口，网管人员可以查询出此目的地的 IP 做协议绑定来解决此登入问题。另外，若想查询何人在使用 BT 或 P2P 软件，也可选择端口做使用者查询。

6．3 系统日志配置

网管可以选择不同的方法保存系统日志：较详细的日志于日后进行检查时，方便找出问题所在，但是记录内容会很多，保存不方便；简化的日志适用于有问题需要告警时，能通知网管特殊事件的发生。

Qno 侠诺路由器提供三种日志相关设定：系统日志(Syslog)是把日志记录存放到日志服务器中、电子邮件通知则是把日志事件以电子邮件寄发给网管、日志类别则是需要记录的内容及格式。

系统日志(Syslog)服务器是专门用来保存不同设备日志的服务器，好处是可以完整地保持所有的日志，对于要求程度较高的企业，是必须配置的。常见的日志服务器软件为 MRTG 及 Mt_Syslog， 可以在 Unix/Linux 或是窗口操作系统平台上运作。

电子邮件通知则是将日志内容寄发到特定电邮中，在配置画面中可以设定一个信件最大的日志数量及发信时间，方便处理。电子邮件通知功能也可与短讯网关配合，变成发送短讯到网管的手机或是行动设备上。

系统日志配置则是日志的细节，包括内容及格式。内容的方面，包括不同的警告事件，是否要记录，应该视需要开启，因为持续的日志发送，也会影响路由器的效能，这对于高负载的应用情况，也是必须避免的。网管很直接的配置记录所有的事件，会造成系统工作的负担，这点是需要注意的。

图三：Qno 侠诺路由器提供三种日志相关设定：系统日志(Syslog)是把日志记录存放到日志服务器中、电子邮件通知则是把日志事件以电子邮件寄发给网管、日志类别则是需要记录的内容及格式。

6．4 语音告警功能

部份侠诺路由器提供了语音报警功能，方便管理人员通过语音提示来及时发现路由器的不正常工作状态，解决网络最常面临的网络掉线、拥塞、及攻击问题，快速调节路由器的相关设置来满足网络提供连续的上网服务。

语音告警提示功能，需要先连接小音箱与路由器指定的接口，然后在路由器 Web 管理页面语音告警栏目做点选激活，再点开高级设定对需要做报警提示的相关选项做勾选择，有参数要求的按照要求添入相关参数，当路由器工作过程中出现你所选择的内容的不正常工作情况的时候，连接路由器的小音箱就会发出报警语音提示来提醒管理人员及时解决问题。

图四：Qno 侠诺路由器的语音告警功能，可配合路由器内部发音线路，发出声音通知。

下表为 Qno 侠诺路由器中所提供的语音警示及处理方法对照参考表，对于技术能力不足的网管，可以起到直观方便的作用。

警示语音 / 现象	可能原因	处理程序 / 解决方式
"广域网 1 断线" / 全网掉线	运营商线路问题或是光纤盒或 ADSL 猫故障	• 检查是否为实体线路不小心被扯掉 • 电话联系 WAN1 运营商，提出线路报修 • 了解故障排除时间，向网吧客人说明 • 确认线路备援功能自动将流量送往另一运营商线路（使用两家运营商线路时）
"广域网 1 断线" 及"广域网 1 联机 "间断发出 / 广域网 1 联机不稳定	运营商线路问题或是光纤盒或 ADSL 猫故障	• 检查是否为实体线路被碰到 • 联系所属运营商进行检修 了解故障排除时间，向网吧客人说明
"内网窜改 IP，IP 地址 192.168.1.100" / 没有异常现象	内网出现不正常用户自行修改 IP	• 网吧管理者或网管可立即依照 IP 对照表，找出窜改 IP 的用户，规劝阻止该用户

"ARP 攻击，IP 地址 192.168.1.100" ／内网掉线	内网遭受 ARP 攻击	• 确定已作路由器及内网计算机端双向绑定 IP/MAC 地址 • 网吧管理者或网管可立即依照 IP 对照表，找出内网攻击源头的中毒机器，予以隔离 • 进行杀毒或重新安装系统
"内网 DoS 攻击，IP 地址 192.168.1.100" ／内网掉线	内网遭受 DoS 攻击	• 网吧管理者或网管可立即依照 IP 对照表，找出内网攻击源头的中毒机器 • 第一时间先拔除计算机网络线，阻止 DoS 攻击影响扩大 • 进行杀毒或重新安装系统
"广域网 1 DoS 攻击，IP 地址 220.112.44.69" ／内网掉线	广域网埠一遭受外部黑客攻击	• 直接联系对应的运营商，请求更换 WAN IP
"冲击波攻击" ／内网掉线	内网机器中毒，发动波击波攻击引起掉线	• 针对特定服务埠(TCP/UDP 135~139，445)设置网络存取条例 • 从被启动的防火墙日志中，查找到内网攻击源头的中毒机器 • 先拔除计算机网络线，阻止冲击波攻击影响扩大 • 进行杀毒或重新安装系统
"广域网 1 上(下)行拥塞" ／短暂上网卡	网吧内突发的带宽高峰	• 持续关注状况 • 若有需要可配置带宽管理规则
"广域网 1 上(下)行拥塞" 连续发出告警／上网卡	网吧根本带宽不足，线路带宽过小，不足以提供目前在线众多人数使用	• 查看是否有用户使用 BT、P2P 软件做大量上传，占用大量带宽。若有应设置 QoS 流量管理规范内网用户最大使用带宽 • 考虑于内网安装电影服务器供用户 • 若持续发生则应考虑进行带宽的升级

6．5 在线联机测试(Diagnostic)

在线测试机制提供简易及方便的方法，协助网管测试线路质量，不必再开启计算器上的软件，直接在路由器的配置界面即可，让网管方便除错。这个功能包含 DNS Lookup 以及 Ping 二种工具。

其中网域名称查询测试(DNS Name Lookup)是网管可于测试画面输入想查询的网域主机位置名称，如 www.abc.com 然后按下开始的按钮开始测试。测试结果会显示于此画面上。Ping-封包传送/接收测试则是提供管理者了解对外联机的实际状况，可以藉由此功能了解网络上的计算机是否存在！这二个贴心的应用软件，也是网管在除错时不可少的帮手。

图五：在线测试机制提供简易及方便的方法，协助网管测试线路质量，包含 DNS Lookup 以及 Ping 二种工具。

小结

对网管而言，完整的日志、实时的告警、及使用方便的小工具，是在进行问题侦测时一个很重要的环境。网管越快把问题找出来，企业受到的安全威胁就越少，因此这方面的功能，值得企业用户了解应用。