第三章 中小企业安全路由器用户管理

对于中小企业的网络管理，用户的管理是一个很常见的问题。例如有限的 IP 如何分配？如何管制不同员工上网权限？如何阻挡访客使用企业网络？如何分派较多带宽给高管或是老总？这些问题，都在影响企业网络的安全，因此网管要保证网络的安全，就必须从基本把用户管理的工作做好。这些问题都可经由路由器的用户管理功能来达成。以下 Qno 侠诺科技就中小企业常遇到的用户管理问题，作全面性的介绍。

内部局域网上网用户的管理，可分为企业局域网内地址合理分配、内部新增上网用户管制、及内部上网用户有效管制三个方面。如果没有一套合理有效的管理机制，会在后面的网络管理及安全方面带来很多负面影响及经济损失。

总括来说，常见的用户管理问题及对应路由器功能如下：

用户管理	常见问题	对应产品功能
地址合理分配	如何分配 IP 地址给用户？公网 IP 及虚拟 IP 如何共存？	动态/静态 IP 地址分配、One-to-one NAT
新增用户管制	如何阻挡非公司计算机上网？	IP/MAC 绑定功能
上网用户管制	如何管理不同用户？如何保留带宽给重要人员？	IP 群组管理、QoS 带宽管理

以上这些内部网络的管理都可以通过 Qno 侠诺路由器的相关功能来实现，达到确保网络安全的目的。Qno 侠诺路由器提供动态 IP 地址分配和静态 IP 地址分配的功能，满足内部上网用户 IP 地址分配的不同需要。路由器还提供了 IP 组管理功能，解决不同部门需要不同上网权限的群组设置，方便统一管理。配合 IP/MAC 绑定功能避免内部网络滥用 IP 地址造成网络管理的困难，同时可以通过 QoS 的设定给内网用户上网一定的带宽管理，保证企业领导希望联网速度能够保持畅通不塞车，确保公司重要业务信息不致延迟、确保公司重要应用服务联机顺畅等。

3．1 IP 地址分配

企业首先考虑的就是 IP 地址的分配管理，动态 IP 地址分配使用 DHCP 服务器，优点是客户端不需进行配置，只需配置服务器，配置简单。静态 IP 则必须在客户端进行 IP 配置，相对较严谨，管制较完全。

Qno 侠诺路由器提供动态 IP 地址分配和静态 IP 地址分配的功能，满足内部上网用户 IP 地址分配的不同需要。Qno 路由器提供动态 IP 地址分配机制（DHCP 功能），支持 C 类 IP 地址，可设置其 IP 地址分配的范围以及地址租约时间。进入“DHCP 功能”的“DHCP 配置”。

图一：DHCP 配置显示发放范围在 192.168.1.100~192.168.1.49 间共 50 台电脑，地址租约时间为 1440 分钟。

通过“DHCP 服务器状态显示”了解到内部网络 IP 地址分配情况，我们可以了解到 DHCP 服务器的相关情况以及内部网络用户的“主机名称”、“IP 地址”、网卡“MAC 地址”、“目前租约时间”。

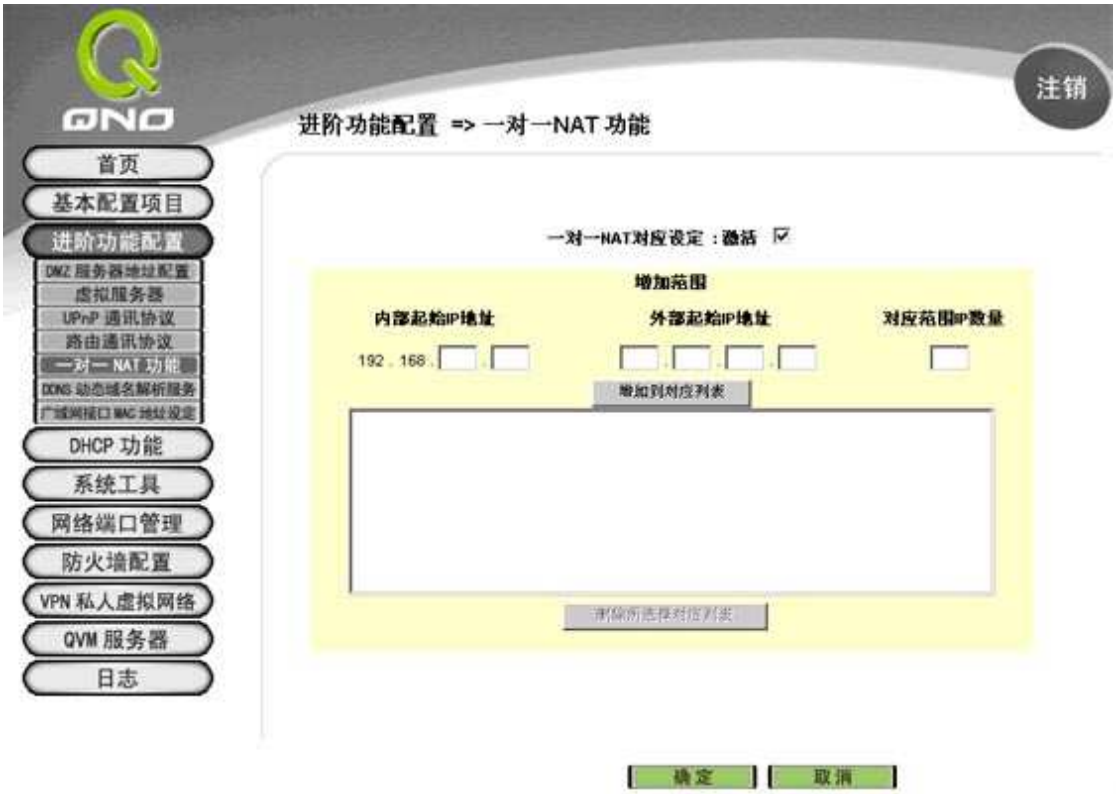
图二：DHCP 服务器状态显示。同时路由器还支持静态的 IP 分配功能，只要保证其 IP 地址不和 DHCP 范围冲突就好。

静态的 IP 分配，只要不激活 DHCP 功能即可。但是客户端配置的 IP 地址和路由器配置的范围必须相符。也可将 DHCP 功能与静态 IP 配合使用，即在整个路由器配置的 IP 范围中，部份使用 DHCP 发放，部份使用静态 IP。例如厂内使用的计算机不常移动，可使用静态 IP；业务人员计算机时常移动，则采用动态 IP。

适当的 IP 地址分配，是后续安全管理的基础，适当地在安全性及便利性间取得平衡，这是必须达成的。

3．2 One-to-one NAT

有些企业具备几个公网 IP，用来作特别的用途，例如总部服务器只能和固定公网 IP 联系，以加强安全性。在这种情况，往往发生公网 IP 不够办公室所有的计算机使用，这时就可以进行一对一 NAT 的配置，把几个公网 IP 对应到内部计算机，这时就可以达到公网 IP 与虚拟 IP 共同在局域网共存的目的了。



图三：一对一 NAT 功能可允许公网 IP 和虚拟 IP 共同存在局域网，可适用于注重信息安全的通讯应用。

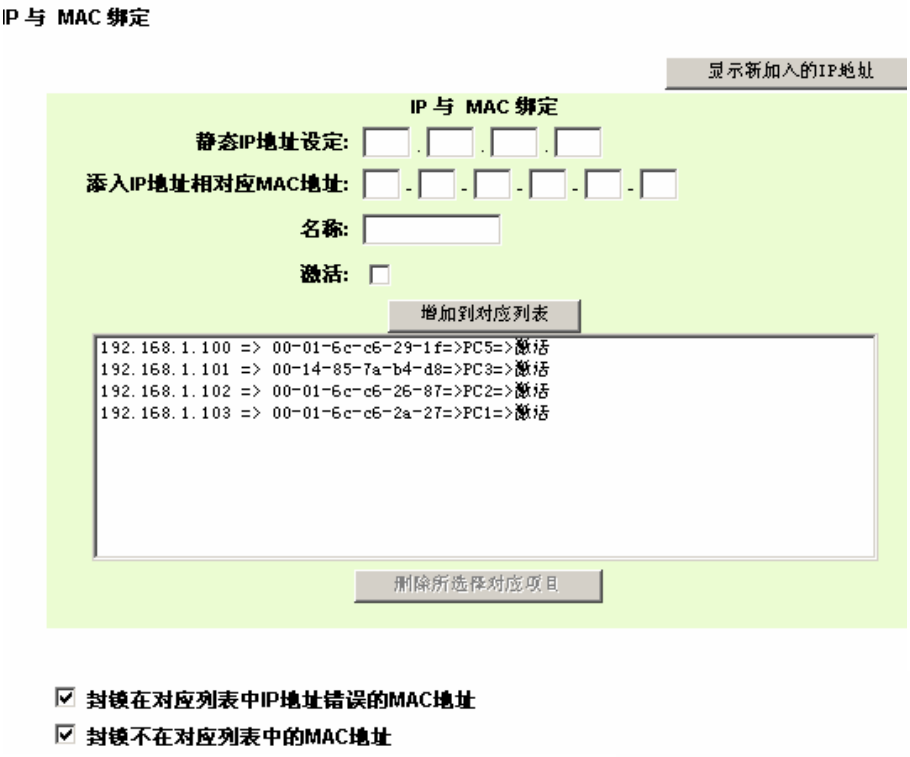
适当地利用这个功能，分隔不同的 IP，可避免内部网络的数据外流。

3．3 IP/MAC 绑定功能

DHCP 服务器自动分配内部网络用户的 IP 地址，用户可以不用手动设置 IP 地址。但是 DHCP 是不容易管理，内部网络随意加入一个用户通过自动获得 IP 地址都能在 DHCP 范围里获得一个合法的 IP 地址。有些攻击者，会通过无线网络进入企业局域网。或是在静态的 IP 分配情况下，有些员工会自行修改成高管或领导的 IP 地址，以逃避管制。这些都是可以通过 Qno 侠诺路由器产品提供的 IP/MAC 绑定功能来因应，并达到安全管理的功能。

企业网管进行 IP/MAC 绑定，必须把企业内网计算机的 MAC 地址都键入到路由器，并与 IP 地址建立对照表。如果路由器发现来向 DHCP 服务器索取 IP 的计算机的 MAC 不在表列中，那么就不会予以响应。因此网管可把企业内的计算机 MAC 都进行绑定，那么外部的计算机就无法进入企业网络，也可避免内部员工自行修改 IP 以逃避管制的措施。

IP 绑定的功能很简单，侠诺路由器“DHCP 功能”的“DHCP 配置”页面的“IP 与 MAC 绑定”，点击“显示新加入的 IP 地址”将内部网络的 IP 地址/MAC 对应加入到 IP 与 MAC 绑定列表中，同时也可以通过手动的模式加入。



图四：IP 与 MAC 绑定画面。您可以勾选“封锁在对应列表中 IP 地址，错误的 MAC 地址”防止内部网络用户修改 IP 地址逃避网络管理，如勾选“封锁不在对应列表中的 MAC 地址”，可以阻止内部网络中并没经过网管人员同意而加入的上网用户。

IP/MAC 绑定功能为我们解决了其内网用户逃避管理以及管理可能加入的新上网用户等问题，也是安全管理一个必要的手段。

3．4 IP 群组管理

企业网管大多希望给不同部门的人不同的权限，例如业务单位的需要较多对外联络，相对的制造单位或事务单位对外联络的需要较少。但是针对内部上网用户 IP 地址上网权限配置，工作量很大，输入过程中也容易出现错误，甚至有时出现遗漏的事情，这种情况下侠诺路由器的 IP 群组管理功能，可将多个用户，例如一个部门所有 IP 地址，组成一个群组解决这个问题。

比如一个企业的 A 部门分得的 IP 地址是 192.168.1.100~192.168.1.110，B 部门分到的 IP 地址是 192.168.1.111~192.168.1.120，我们可以将这些连续的 IP 地址群组到一起，方便做统一的设置。减少网管人员的工作量，同时也避免繁多的 IP 地址输入容易出错。同时内部网络需要同时大量的 IP 地址需要做同样管理的时候就将这些连续的 IP 群组到一个组做相同设置。

侠诺路由器内“DHCP 功能”的“DHCP 配置”页面的“IP GROUP”,如图对应输入相关信息确定后就可完成 IP 群组的设置。

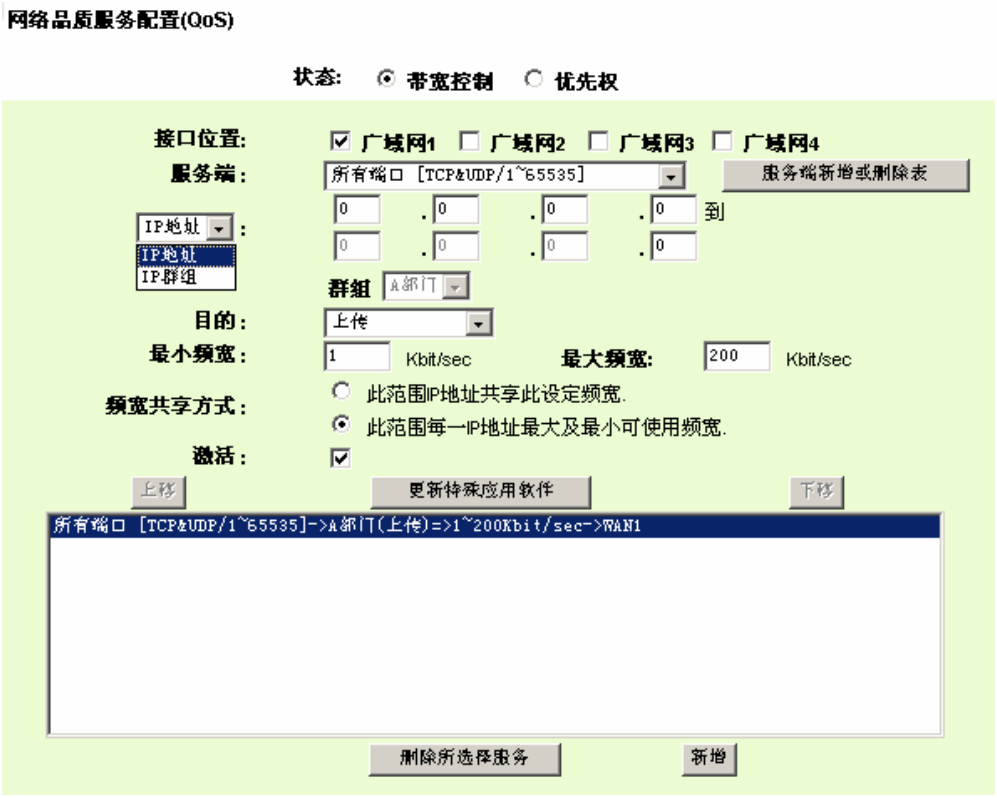
图五：IP 群组管理设置画面。

3．5 QoS 带宽管理功能

有些企业希望针对特定用户进行配置，例如内部网络特殊用户（比如经理、董事长等）

给予大的带宽、内部网络用户选择特定 WAN 访问外部网络、特定线路留给特定的用户等等。通过 QoS 带宽管理功能能达到以上的功能。

Qno 侠诺路由器可以允许选择设置内部网络的某一单个 IP 地址、一连串 IP 地址、或者某一 IP 群组，通过有效的管理上传与下载的速度来达到对带宽的管理功能，保证内网上网用户能够合理利用带宽，同时还可以确保特殊用户上网不受限制，保证足够的带宽使用。如可以为重要的高管设定较大的最小带宽，或是保留特定的广域网口给特定 IP 群组。



图六：带宽管理功能设置页面

小结

以上针对中小企业内部局域网用户的管理，以 Qno 侠诺安全路由器的功能，针对常遇到的一些问题，作了初步的介绍。相信对于企业网管在进行日常管理，有相当的帮助。用户管理是网络安全的最基本的工作，网管如能在一开始就把这方面的工作作到位，相信可以减少后续很多的问题。