侠诺科技股份有限公司
Qno Technology Inc.
http://www.Qno.cn

Qno 侠诺酒店用户 ARP 病毒防制攻略

在酒店的网络管理中，通常的作法，都会把客房的上网和内部办公放在同一台路由器下面。这就面临着安全问题，特别是 ARP 病毒的攻击。Qno 侠诺工程师在实际工作中，总结出一套专门针对酒店行业用户的解决办法，下面我们就向读者介绍Qno侠诺在酒店行业ARP病毒防制的攻略手段。

由于 ARP 病毒变种太多，传播速度太快，国内外的反病毒厂商都没有很好的办法来解决ARP病毒问题。一般都是在内网主机和路由器之间建立双向的ARP绑定来解决这个问题，这也是目前看来最行之有效的解决方案。但酒店不同于网吧，随着住宿客人的不断更换，酒店客房里的主机也是不断变化的，这就意味着遭遇 ARP 病毒风暴时，不可能通过 IP 与 MAC 地址绑定的传统方法解决此问题。同时，也很难让住店的客人操作对路由器的 ARP 绑定，从而导致酒店会经常接到客户对上网速度慢或上不去网的一些投诉。由于不能够耽误酒店的正常使用，所以整个网络也不能有太大改动。鉴于酒店的特殊性，针对 Qno 侠诺路由器酒店用户，提出以下解决方案：

1、激活防止 ARP 病毒攻击功能，防止病毒的侵入；
2、利用 Qno 侠诺路由器多子网功能，加划 VLAN 的方法，减少攻击损害的影响；
3、办公区做 MAC 绑定，设置访问规则，更完整保护办公区计算机。

首先，酒店客房通常是客人自备电脑入网，大多数酒店采用 DHCP 技术给上网用户动态分配 IP 地址。在防火墙里面开启防止 ARP 病毒攻击，这样可以防止病毒的侵入。

激活防止 ARP 病毒攻击功能。输入路由器 IP 地址登陆路由器的 Web 管理页面，进入“防火墙配置”的“基本页面”，再在右边找到“防止 ARP 病毒攻击”，在进行“激活”。系统默认“防 ARP 攻击每秒发送 20 笔”，建议设置为“2—5”笔，以防止发送广播包过多而造成网络堵塞。如图 1。

基本设定

防火墙功能：	◉ 激活 ○ 关闭
SPI封包主动侦测检验功能：	◉ 激活 ○ 关闭
DoS侦测功能：	◉ 激活 ○ 关闭 高级设定
关闭对外的封包回应：	◉ 激活 ○ 关闭
远程配置管理功能：	◉ 激活 ○ 关闭 Port: 80
允许Multicast封包穿透格式：	○ 激活 ◉ 关闭
防止ARP病毒攻击：	◉ 激活 ○ 关闭 防ARP攻击每秒发送 2 笔.

图 1: 激活防止 ARP 病毒攻击

其次，利用 Qno 侠诺路由器多子网功能，加划 VLAN 的方法，对客房区和办公区进行防 ARP 设置。结构图如图 2 所示。

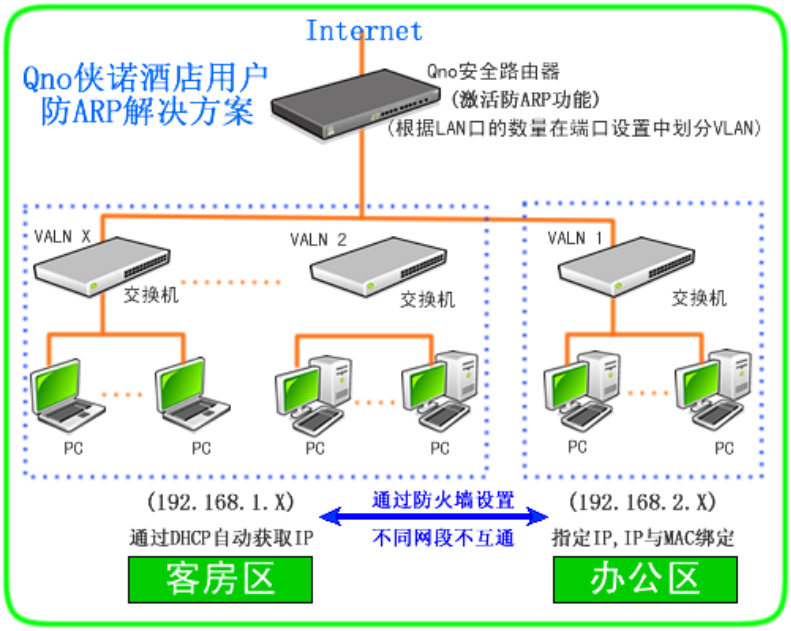

图 2: 划分 VLAN 结构图

把路由器设定两个网段，本身的网段给客房区客人用，再利用多子网功能，为办公区设另一个网段内部办公用。在路由器下面接出来两个交换机，分别利用路由器的虚拟局域网功能划出两个 VLAN，划分 VLAN 可根据 LAN 口的数量而定，客房区应该尽可能多的划分，以减少客房相互间的影响。如图 3 所示。

图 3: 端口设置

此功能可以让网管人员在自己的局域网内将每一个局域网端口设定 1 个或多个不同网段且无法互通的局域网端口，但都可以通过路由器上网。在同一个网段内的成员（在同一个 VLAN 局域网络内）可互相沟通并看得到对方，若不在同一个 VLAN 群组内的成员则无法得知其它成员的存在。

然后在防火墙设置里，添加一条新访问规则禁止客房区本身的网段访问办公区子网段。这样做是为了防止 ARP，使网络更加安全。如图 4 所示。如也需要限制办公区子网段不能访问客房区网段，则需激活前面一条规则。

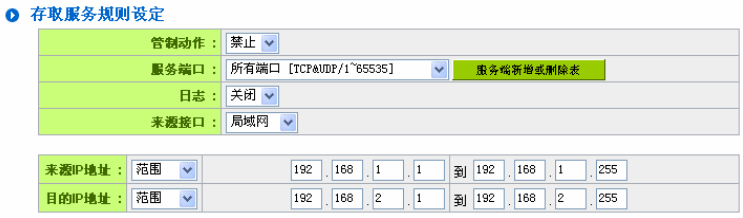

图 4:设置访问规则

Qno 侠诺路由器在 MAC 绑定功能页面下方有两个选项，一个是“封锁在对应列表中 IP 地址错误的 MAC 地址”，另一个是“封锁不在对应列表中的 MAC 地址”。 如图 5。

图 5: IP 及 MAC 地址绑定

大家知道要彻底的防止 ARP 病毒，需要做双向绑定，但是客房是不能做绑定的，因为客人天天变，所以，不勾选“封锁不在对应列表中的 MAC 地址”。但办公区的网段是固定的，我们可以绑定在路由器上，并勾上“封锁在对应列表中 IP 地址错误的 MAC 地址”， 那么设定为固定 IP 的计算机或通过此功能已发给特定 IP 的计算机擅自更改 IP 为非指定的 IP 地址时，则会无法上网。这样，一则可以防止其它人乱改 IP 跟内部冲突，二则 ARP 病毒不会对办公区产生影响。

如果内网发现 ARP 攻击，排除方法可参考 Qno 侠诺关于排除防制 ARP 攻击的技术文章“ARP 攻击防制进阶篇---侠诺科技 ARP 防制经验谈”。

以上方法基本可以解决ARP病毒攻击对网络造成相关问题，这样客人的又可以从DHCP分IP，又不影响到酒店内部办公。避免了因办公网络瘫痪，而造成大部分房客 check out 时，手拎大包小包无限时在等的情况。ARP 欺骗病毒在相当长的时间内还会继续存在，侠诺科技将不断的为用户提供各种解决方案，帮助用户打造一个安全稳定、高效的接入环境。

＃＃＃

- **什么是 ARP？**

ARP（Address Resolution Protocol，地址解析协议）是一个位于 TCP/IP 协议栈中的低层协议，负责将某个 IP 地址解析成对应的 MAC 地址。

- **什么是 ARP 欺骗?**

从影响网络连接通畅的方式来看，ARP 欺骗分为二种，一种是对路由器 ARP 表的欺骗；另一种是对内网 PC 的网关欺骗。

第一种 ARP 欺骗的原理是——截获网关数据。它通知路由器一系列错误的内网 MAC 地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的 MAC 地址，造成正常 PC 无法收到信息。第二种 ARP 欺骗的原理是——伪造网关。它的原理是建立假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的路由器途径上网。在 PC 看来，就是上不了网了，“网络掉线了”。