ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.7, No.35, December 2011.
E-mail: info@cccc.net.cn
http://www.dnzs.net.cn
Tel:+86-551-5690963 5690964

# 共享检测的防范技术与实现

赵丙秀

（武汉软件职业学院，湖北 武汉 430205）

**摘要：**随着互联网带宽的发展，运营商为了保护自己的利益而不让用户几家合用路由上网，于是普遍采用IPID、时间戳、User-Agent头等技术来检测技术来判定路由器后面有多少台计算机在共享上网。该文深入剖析这些技术的基础上，提出如何防范运营商的共享检测，着重分析了IPID解决方案。

**关键词：**共享神盾；共享神矛；网络尖兵；IPID

**中图分类号：TP393　　文献标识码：A　　文章编号：1009-3044(2011)35-9061-02**

## 1 检测原理简析

现在电信运营商的带宽越来越大，Internet技术的发展和高昂的接入价格，使得越来越多的用户采取合租方式通过路由上网。但是有线宽带由于没有无线宽带那种SIM防复制，防止破解等技术，因此控制路由器上网一直是他们研究的重点。

原来电信运营商常用SMTP检测技术来判定是否路由，但是随着时代的发展和设备的更新，现在运营商很难从设备层来控制用户，于是更新的检测技术，采用IPID判定法、TTL判定法、时间戳判定法、User-Agent判定法等方法来检测路由后面的用户数。

1）IPID判定法：根据Windows协议栈的特性，一台计算机IPID值是连续的。通过分析IPID值的跳跃我们可以得出计算机的台数。Windows网络协议栈实现时，ID字段的值随着发送IP报文数的增加而增加，IPID的初始值是随机值，一般说来，不同主机的初始值有较大差距。由于Linux、Unix的IPID是随机值，故此判定方法对Linux、Unix无效。

2）TTL判定法：TTL指生存时间，指定数据报被路由器丢弃之前允许通过的网段数量。TTL是由发送主机设置的，以防止数据包不断在IP互联网络上永不终止地循环。转发IP数据包时，要求路由器至少将TTL减小1。不同的操作系统其TTL不同：LINUX为64，WIN2K/NT为128，WINDOWS9X系列为32，UNIX系列为255。如果检测到有多个TTL的值则可以断定有多台主机。

3）时间戳判定法：由于不同主机的物理时钟一般存在偏移，且网络协议栈时钟与物理时钟存在对应关系，同时不同主机发送报文的频率与时钟存在统计关系，因此可以分析发现不同的网络时钟偏移数目来确定主机的台数。

4）User-Agent头判定法：HTTP头分为HTTP请求头和HTTP应答头。HTTP请求头为HTTP客户在浏览服务器上的主页时，向服务器发送请求的时候必须指明请求类型。请求类型是指HTTP-GET或HTTP-POST，每个HTTP-GET和HTTP-POST都由一系列HTTP请求头组成，这些请求头定义了客户端从服务器请求了什么，而响应则是由一系列HTTP应答头和应答数据组成，如果请求成功则返回应答。在HTTP头中有一个User - Agent头标明了浏览器类型。不同操作系统、不同IE版本、不同补丁的User-Agent字段不同。由此可以根据user-Agent头的不同来判定主机的数量。

## 2 分析WindowsTCPIP协议栈数据处理过程

在众多检测原理中，IPID判定法判定准确，用得较多，其他再作为辅助判定方法。下面我们主要分析一下WindowsTCPIP协议栈数据处理过程。

1）WinSock的数据包形成后，Tcpip.sys会将其传递给防火墙驱动程序(Ipnat.sys)进行处理。防火墙检查该数据包是否属于所要阻止的Internet控制消息协议(ICMP)消息类型。如果ICMP消息被阻止，防火墙就将丢弃该数据包。

处理完后，防火墙会将该数据包传回给Tcpip.sys，

2）Tcpip.sys将数据包传递给筛选器驱动程序(Ipfltdrv.sys)进行处理。

Ipfltdrv.sys根据下一跃点接口，将该数据包与已配置的出站IP数据包筛选器格式进行对比。

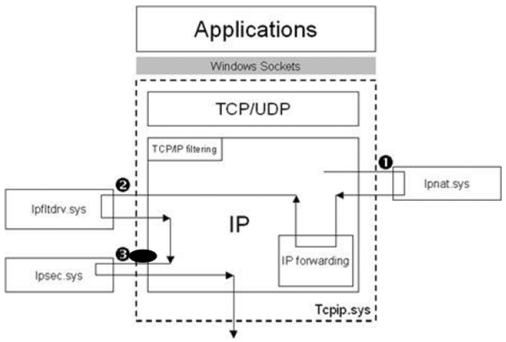


图1　数据包处理的TCP/IP体系结构

若出站数据包筛选器不允许该数据包通过，Ipfltdrv.sys就会直接下，丢弃该数据包。若出站数据包筛选器允许该数据包，Ipfltdrv.sys就会将该数据包传回给Tcpip.sys。

3）Tcpip.sys将该数据包传递给Ipsec.sys进行处理。

Ipsec.sys根据IPsec筛选器组，决定是否允许、阻止或保护该数据包。若允许的话，Ipsec.sys会在不修改该数据包的情况下，将其发回给Tcpip.sys。若阻止的话，Ipsec.sys会直接丢弃该数据包。若要进行保护的话，Ipsec.sys会在将数据包传回给Tcpip.sys之前，对其添加适当的IPsec保护。

收稿日期：2011-09-15
作者简介：赵丙秀(1976-)，女，副教授。

Tcpip.sys随后会通过下一跃点接口,将该数据包发送到下一跃点IP地址。完成数据包的出站。

## 3 解决方案

1)对于IPID检测的破解

因为各运营商破解时是采集其前置机上的数据包通过分析IPID来判定的其主机数目。由上面我们知道只需要我们出去的数据包在发出前我们修改其所有数据包的IPID头设定为一个统一的值或者随机值即可。因此我们只需在图1第2步黑色椭圆的位置添加驱动程序修改IPID头即可。

既然破解检测的核心在于修改Windows协议栈,我们选择修改开源驱动DrvFiltIp.sys来完成IPID头的修改,因为数据包通过ipfltdrv.sys以后,IP层的数据包结构都不会拦截或者修改,这个时候我们只要在他进入TCPIP.sys之前使用一个hook驱动,加载了DrvFiltIp.sys,将IPID改为固定值或者随机值,就可以解决所谓IPID检测问题。

修改FilterPackets过滤函数

```
if(RecvInterfaceIndex == INVALID_PF_IF_INDEX &&(pIPHdr->ipProtocol ==6 || pIPHdr->ipProtocol ==17 || pIPHdr->ipProtocol == 1))//表示是本机发出去的包
{//固定模式
ipp->ipID= htohl(456);
//随机模式
#else
IPID = rand();
ipp->ipID= htohl(IPID);
#endif }
```

2)对于TTL的检测,我们有多种解决办法:

① 修改注册表办法,在windows下我们可以直接修改注册表让TTL同一为一个固定值。

在“HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\ Parameters”,找到“DefaultTTL”,将该值修改为十进制的固定值,重新启动服务器系统后即可。

② 修改驱动的办法:在上面ipid改动代码中加入ipp->ipTTL=111(111为固定值)

③ Linux下修改方法:

命令行#sysctl -w net.ipv4.ip_default_ttl=N,(N=0~255),若N>255,则ttl=0,重启服务器即可生效。

3)统一时间戳,这个可以通过服务程序在内网建立一个动态的UDP的时钟服务器,将每台计算机启动后时钟进行同步,保证内网的计算机的时间都是一致的,这样就解决了时间戳的检查问题。

4)User-Agent头判定法 同样可以通过修改注册表修改User - Agent头。 这个办法网上介绍了很多,就不再阐述。

## 4 改进和建议

上述办法虽然比较完美的解决了网络尖兵的检测问题,但是随着时间的推移,电信商又通过Windows的TCP连接数不超过255个来做文章,判定后台端口使用数量等问题,这些问题虽然可以通过路由器编程直接解决,但是也可以通过一个服务来统计连接数解决,总之未来将会有更新的检测技术产生,研究检测原理的办法也将不断的更新。

## 参考文献:

[1] 赵丙秀.ADSL共享上网检测原理与实现[J].电脑学习,2009(2).
[2] 安志锋.破解网络尖兵初探[J].电脑知识与技术,2006(22).
[3] 吴县植.让您的宽带继续共享[J].办公自动化,2007(6).

(上接第9060页)

## 3 结束语

面对即将到来的IPv6过渡,作为中小型网络的管理者,不应该再去逃避或者拖延网络的过渡,应该积极的投入其中,核算成本,选择合适的过渡技术,勇于探索不同组合的IPv6过渡机制,只有这样才能推动占网络大多数的中小网络积极向IPv6过渡,也才能更好的推广IPv6的技术和应用,为整个网络的发展提供推动力。

## 参考文献:

[1] 徐朝晖.IPv6:当前过渡情况综述[J].数字通信世界,2011,5(77):72-75.
[2] 张伟.IPv6过渡技术发展历程分析[J].电信网技术,2011,6(204):25-27
[3] 卢媛媛.校园网IPv4向IPv6过渡方法研究与探讨[J].黄冈师范学院学报,2011,6(134):63-65.