MSR系列路由器针对ARP防攻击的问题处理方法

纪合宝 2009-03-12 发表

MSR系列路由器

针对ARP防攻击的问题处理方法

一、 问题描述

前方使用MSR3040发现上网速率比较慢，同时查看CPU发现ARP进程比较高.

```
<MSR>dis  cpu-usage task
      TaskName       CPU       Runtime(CPU Tick High/CPU Tick Low)
                vt0          0%            0/  72ee7b
              VIDL         25%            0/158767a9
              TICK          0%            0/   d875b
              SOCK          3%            0/ 2e9727a
               ACL          0%            0/   257e8
             MSTP           0%            0/    a736
               ARP         68%            0/39b9f079
                IP          0%            0/   927fe
             NTPT           0%            0/   589a9
```

二、过程分析：

通过display ip interface gi 0/1可以看到收到的ARP报文很多，速率大概是400pps，打开debug arp packet可以看到攻击报文是大量仿冒网关的免费ARP报文攻击，源MAC有001d-0f85-be76、0019-e03d-51bc、0021-2750-e996三台PC，仿冒的IP为192.168.1.1，由于这三台PC的攻击ARP报文交替发送，导致MSR上192.168.1.1对应的ARP表项不断刷新，引起CPU利用率高。

在R17xx版本可以通过配置192.168.1.1的静态ARP规避该问题，可一旦出现其他ARP攻击可能会再出问题。升级R17xx SI版本后，配置arp anti-attack active-ack enable可以解决这类攻击，为了避免出现其他问题，同时使能了其余的防ARP攻击特性：

arp anti-attack valid-check enable
arp anti-attack source-mac filter
arp anti-attack source-mac threshold 10

debug arp packet的信息如下：

```
<msr-router>
*Jan 16 10:14:03:679 2009 fgw-router ARP/7/arp_rcv:Receive an ARP Packet, operation : 1, sender_eth_addr : 001d-0f85-be76, sender_ip_addr : 192.168.1.1, target_eth_addr : ffff-ffff-ffff, target_ip_addr : 192.168.1.1
*Jan 16 10:14:03:680 2009 fgw-router ARP/7/arp_rcv:Receive an ARP Packet, operation : 1, sender_eth_addr : 001d-0f85-be76, sender_ip_addr : 192.168.1.1, target_eth_addr : 0000-0000-0000, target_ip_addr : 192.168.1.1
*Jan 16 10:14:03:680 2009 fgw-router ARP/7/arp_rcv:Receive an ARP Packet, operation : 1, sender_eth_addr : 001d-0f85-be76, sender_ip_addr : 192.168.1.1, target_eth_addr : ffff-ffff-ffff, target_ip_addr : 192.168.1.1
*Jan 16 10:14:03:680 2009 fgw-router ARP/7/arp_rcv:Receive an ARP Packet, operation : 1, sender_eth_addr : 001d-0f85-be76, sender_ip_addr : 192.168.1.1, target_eth_addr : ffff-ffff-ffff, target_ip_addr : 192.168.1.1
*Jan 16 10:14:03:681 2009 fgw-router ARP/7/arp_rcv:Receive an ARP Packet, operation : 1, sender_eth_addr : 0019-e03d-51bc,
```

三、解决方案：

升级到1718SI版本，配置下面命令：

arp anti-attack valid-check enable
arp anti-attack source-mac filter
arp anti-attack source-mac threshold 10

注意：目前只有17XX-SI 版本支持,BI版本不支持