secpath1000f发送畸形arp报文引起的地址冲突问题分析案例

魏文立 2006-06-11 发表

华为三康技术有限公司 Huawei-3Com Technologies Co., Ltd.	文档编号 Document ID	**密级 Confidentiality level**
		内部公开Confidential
	文档状态 Document Status	共13页 Total 13 pages

secpath1000f发送畸形arp报文引起的地址冲突问题分析案例

拟制 Prepared by	**魏文立 03742**	**Date 日期**	**2006-05-25**
评审人 Reviewed by		**Date 日期**	**yyyy-mm-dd**
批准 Approved by		**Date 日期**	**yyyy-mm-dd**

一、问题描述：

抚顺社保客户反映使用我司secpath1000F后，IBM小型机提示有地址冲突，而且出现冲突没有时间规律，更换其他厂商的防火墙设备无此问题，并且不挂防火墙时也无此问题，怀疑是secpath1000F有问题。

二、组网配置：

1、组网拓扑：

2、cisco3600配置及版本：

```
Router#show run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
logging buffered 4096 errors
enable secret 5 $1$PPjo$3//3wL7kwOQv0n.mBqpit/
!
!
!
!
!
ip subnet-zero
no ip domain-lookup
!
!
!
process-max-time 200
!
interface FastEthernet0/0
 ip address 172.17.0.254 255.255.0.0
 no ip directed-broadcast
 no ip mroute-cache
 tx-queue-limit 128
 full-duplex
 no cdp enable
!
interface FastEthernet2/0
 ip address 10.58.34.254 255.255.192.0
 no ip directed-broadcast
 full-duplex
 no cdp enable
!
ip classless
ip route 10.56.50.0 255.255.255.0 10.58.34.99
ip route 21.0.0.0 255.255.0.0 10.58.34.107
ip route 128.0.0.0 255.0.0.0 172.17.0.253
ip route 172.16.0.0 255.255.0.0 10.58.34.99
ip route 172.18.0.0 255.255.0.0 10.58.34.105
no ip http server
!
no cdp run
!
line con 0
 transport input none
line 33 48
line aux 0
line vty 0 4
 password fssi_h7~!
 login
!
end
```

Router# show ver
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-I-M), Version 12.0(5)XK1, EARLY DEPLOYMENT RELEASE SOFT
WARE
(fc1)
TAC:Home:SW:IOS:Specials for info
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 14-Sep-99 21:43 by jjgreen
Image text-base: 0x600088F0, data-base: 0x607E4000

ROM: System Bootstrap, Version 11.1(20)AA2, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
ROM: 3600 Software (C3640-I-M), Version 12.0(5)XK1, EARLY DEPLOYMENT RELEASE SOFTWA
RE (fc1)

Router uptime is 2 days, 21 hours, 44 minutes
System returned to ROM by power-on
System image file is "flash:c3640-i-mz.120-5.XK1"

cisco 3640 (R4700) processor (revision 0x00) with 24576K/8192K bytes of memory.
Processor board ID 18693000
R4700 CPU at 100Mhz, Implementation 33, Rev 1.0
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
16 terminal line(s)
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

3、Secpath1000F配置及版本

```
dis cu
#
 sysname Quidway
#
 super password level 3 simple huawei
#
 dvpn service enable
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
 firewall mode transparent
 firewall system-ip 10.58.33.252 255.255.255.0
#
 firewall statistic system enable
#
radius scheme system
#
domain system
#
local-user admin
 password simple huawei
 service-type telnet
 level 3
local-user huawei
 password simple huawei
 service-type telnet
 level 3
#
acl number 3000
```

```
 rule 0 permit ip
#
interface Aux0
 async mode flow
#
interface GigabitEthernet0/0
 promiscuous
#
interface GigabitEthernet0/1
 promiscuous
#
interface Encrypt2/0
 mtu 0
#
interface NULL0
#
interface LoopBack0
 ip address 10.58.33.252 255.255.255.0
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface GigabitEthernet0/1
 set priority 85
 statistic enable ip inzone
 statistic enable ip outzone
#
firewall zone untrust
 add interface GigabitEthernet0/0
 set priority 5
 statistic enable ip inzone
 statistic enable ip outzone
#
firewall zone DMZ
 set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local DMZ
#
firewall interzone trust untrust
#
firewall interzone trust DMZ
#
firewall interzone DMZ untrust
#
 acl accelerate enable
#
 firewall defend land
 firewall defend smurf
 firewall defend fraggle
 firewall defend winnuke
 firewall defend source-route
 firewall defend route-record
 firewall defend ping-of-death
 firewall defend tcp-flag
 firewall defend ip-fragment
 firewall defend large-icmp
 firewall defend teardrop
 firewall defend ip-sweep
 firewall defend port-scan
```

```
 firewall defend syn-flood enable
 firewall defend udp-flood enable
#
user-inton 0
user-interface aux 0
user-interface vty 0 4
 authentication-mode scheme
#
return

<Quidway>
<Quidway>dis ver
 Copyright Notice:
 All rights reserved (Nov 29 2005).
 Without the owner's prior written consent, no decompiling
 nor reverse-engineering shall be allowed.
 Huawei Versatile Routing Platform Software
 VRP(R) software, Version 3.40, Release 0006
 Copyright (c) 1998-2005 Huawei Tech. Co., Ltd. All rights reserved.
 Quidway SecPath 1000F uptime is 0 week, 0 day, 23 hours, 58 minutes
  CPU type: Mips BCM1125H 600MHz
  512M bytes DDR SDRAM Memory
  16M bytes Flash Memory
  Pcb      Version:4.0
  Logic    Version:2.0
  BootROM  Version:1.12
  [SLOT 0] 2GBE     (Hardware)4.0, (Driver)1.0, (Cpld)2.0
  [SLOT 2] NDEC     (Hardware)3.0, (Driver)3.3, (Cpld)1.0
<Quidway>
<Quidway>
<Quidway>vrbd
Routing Platform Software
Version SecPath 1000F 8042V100R002B02D009SP03 (COMWAREV300R002B40D002), RELEASE
SOFTWARE
Compiled Nov 29 2005 10:59:00 by xiedong
<Quidway>
<Quidway>
<Quidway>
```

三、处理过程：

1、到达客户处，了解网络情况，发现所有的小型机以及PC机的网关全部指向CISCO3600，通过在CISCO3600配置静态路由到达其他网段，这必然造成通过1000F，到达CISCO3600出入流量非常巨大，同时会产生大量重定向报文。

2、经过分析，必然是因为小型机收到源MAC非自己，源IP为自己，也就是10.58.34.112的arp报文导致的。

3、通过在交换机上抓包发现如下arp报文：

4、这种arp报文非常异常，
首先，源MAC为CISCO端口地址，而sender ip 为IBM小型机的IP地址，这必然会引起小型机报地址冲突，然后我们通过在网络中发送该报文，得到证实，引起小型机报地址冲突的原因就是收到类似报文；
其次，该arp请求报文的sender ip 和target ip并不在同一网段，就这一点并不象一般网络设备发出来的arp请求报文，有点象是篡改的；
最后，该arp请求报文的target ip网段是在172.16.0.0/16网段，并且真实存在，然后抓包发现引起报地址冲突的这类报文target ip都是在172.16.0.0/16网段和172.18.0.0/16网段，难道是因为网络结构引起的。

5、既然确认了引起报地址冲突的报文，我们就要确认什么原因引起的，存在两种可能：
1}由人恶意篡改，但这需要三个条件：
a：知道cisco端口mac；

b：对网络协议比较了解；
c：会构造报文。
从客户实际环境来看，这种可能性比较低。

2）由网络设备发出的，但又有三种可能：
a：由CISCO3600发出，secpath1000F由于是透明模式未更改广播到网络中引起小型机地址冲突；
b：由CISCO3600发出某种报文，经过secpath 1000F更改后成为这种畸形arp报文，导致小型机报错；
c：网络结构导致由secpath 1000F 自己发出的这种畸形arp报文，导致小型机报错。

6、通过在CISCO3600和SECPATH1000F之间和交换机上同时抓包，当出现报错时，我们抓获报文如下：
CISCO3600和SECPATH1000F之间：

交换机上：

7、经过分析发现在CISCO3600和SECPATH1000F之间的报文并没有类似的畸形arp报文出现，而在交换机上有，这就排除了是由a引起的（由CISCO3600发出，secpath1000F由于是透明模式未更改广播到网络中引起小型机地址冲突）看来还是问题还是在我们secpath1000F上面，那么是b还是c呢！？仔细分析了CISCO3600和SECPATH1000F之间抓获的报文，b并不存在，可以确定是C引起的。

8、那么既然已经定位是1000F的问题，是由C引起的，那么怎样解决呢！？是不是因为开了的某种firewall defend引起的！？于是，我关掉所有的firewall defend，发现问题依旧，排除这种可能性。

9、在研发徐宋大哥的指导下，下发firewall unknown-mac flood后，问题解决。

四、问题分析
1、为什么下发firewall unknown-mac flood后，问题就得到了解决呢！？
首先我们来看看操作手册对firewall unknown-mac flood的描述：
配置对未知目的MAC地址的IP报文的处理方式
当工作在透明模式下的防火墙接收到未知目的MAC地址的IP报文时，即不能根据目的MAC地址找到出接口，则防火墙根据配置情况可以用三种方式进行处理：
直接丢弃该未知目的MAC地址的IP报文。
向除接收到该报文的接口外的其它所有接口（接口必须属于某一安全区域）广播ARP请求报文，并且丢弃原来的未知MAC地址的IP报文。收到ARP响应报文后，保存MAC地址和接口的对应关系。
将此未知目的MAC地址的IP报文从除接收接口外的其它所有接口（接口必须属于某一安全区域）发送出去，待收到响应报文后，将建立MAC地址与接口之间的对应关系。
请在系统视图下进行下列配置。
配置对未知目的MAC地址报文的处理方式

操作	命令
配置对未知目的MAC地址的单播IP报文的处理方式	firewall unknown-mac [unicast] { drop | arp | flood }
配置对组播和广播IP报文的处理方式	firewall unknown-mac { broadcast | multicast } { drop | flood }
恢复对未知目的MAC地址的IP报文的处理方式为缺省值	undo firewall unknown-mac [unicast | broadcast | multicast]

缺省情况下，防火墙对单播IP报文按照arp方式进行处理，而对广播和组播报文按照drop的方式进行处理。

3、Secpath 1000F在透明模式下，secpath 1000F也是根据MAC表转发的，它必然存在一个MAC学习过程，但当MAC没有该目的MAC的报文怎么转发呢！？上面作出了解释。当我们采用默认设置时，即：防火墙对单播IP报文按照arp方式进行处理，而对广播和组播报文按照drop的方式进行处理。也就是说，如果有一个源MAC为1-1-1，源IP为1.1.1.1，目的MAC为2-2-2，目的IP为2.2.2.2的IP报文经过SECPATH 1000F，此时正好mac表里没有2-2-2的表项，那么secpath会向除接收到该报文的接口外的其它所有接口（接口必须属于某一安全区域）广播ARP请求报文，
该arp报文结构如下：
smac dmac TYPE sender –mac sender-ip target-mac target-ip
1-1-1 FFFFFF 0X0806 1-1-1 1.1.1.1 000000 2.2.2.2
即sender-ip和target-ip不在同一网段的畸形arp，但它对网络是没有影响的，因为2.2.2.2在这个网段，也就不会收到这样一个arp请求；同时，因为该arp请求不会“向接收到该报文的接口”发送，所以1.1.1.1也不会收到，所以不会产生ip地址冲突。所以在一般的网络中是不会有影响的。

4、为什么在抚顺社保会存在ip地址冲突的问题呢！？

那是由客户网络结构决定的，因为所有的小型机以及PC机的网关全部指向CISCO3600，通过在CISCO3600配置静态路由到达其他网段。假设此时IBM小型机要访问172.18.0.0/16网段的一台pc，ip地址为172.18.1.1，IBM小型机首先查找路由表发现要先送到CISCO，所以会首先请求CISCO的arp，CISCO回应，那么SECPATH会学习到CISCO和IBM的mac，IP报文送到CISCO后，CISCO查找路由表，发现到172.18.0.0/16要先送到10.58.34.115,也会先请求10.58.34.115的arp，10.58.34.115回应，secpath又学到10.58.34.115的mac，这样都不会产生畸形arp报文，但是由于secpath mac表老化时间比CISCOarp表老化时间短，就存在这种情况，secpath学到的10.58.34.115的mac老化了，而此时CISCO上10.58.34.115的arp并没有老化，并且IBM此时要和172.18.1.1通信，这时，由于secpath没有172.18.1.1的mac，就会产生畸形arp，报文结构如下：

smac dmac TYPE sender –mac sender-ip target-mac target-ip

CISCOmac FFFFFF 0X0806 10.58.34.112 CISCOmac 000000 172.18.1.1

当IBM小型机收到这个arp报文后，就会提示ip地址冲突，到此真相大白。

五、总结

这次现象比较奇怪，特别是在抓到这种怪异的arp报文后。但好在思路比较清晰，处理得当，又有安全组师兄王思军和研发部的徐宋大哥悉心指导，问题得到了圆满解决。这次问题处理充分体现了我们的技术实力，得到了客户的认可和好评。

六、特别鸣谢

特别感谢安全组师兄王思军和研发部的徐宋大哥悉心指导以及办事处兄弟们的大力支持。