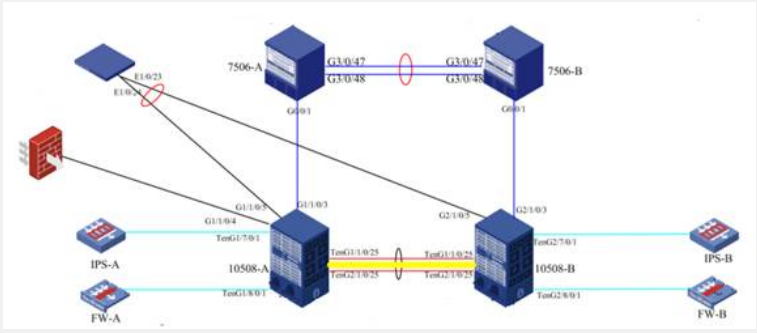
S10500 交换机OSPF Router ID冲突问题排查案例

OSPF 赵国卫 2012-07-15 发表

S10500交换机OSPF Router ID冲突问题排查案例

一、 组网：



两台S10500做IRF，分别插一块IPS、FW插卡，作为核心设备采用OSPF与网络内其他设备交互路由协议。

二、 问题描述：

S10500的设备上不断打印类似于下面的信息：

*Jun 19 14:25:58:436 2012 S10508 RM/6/RMDEBUG:

OSPF 10 :OSPF received packet having conflicted Router ID :10.255.0.1 from interface Vlan-interface806.

#Jun 18 15:14:35:495 2012 S10508 OSPF/4/IF_BAD_RX: OSPF TrapID1.3.6.1.2.1.14.16.2.8: Non-virtual Interface 10.254.0.41 index 0 Router 10.255.0.1 received error packet from 10.254.0.41 PacketType 1.

#Jun 18 15:14:35:495 2012 S10508 OSPF/4/IF_BAD_RX: OSPF TrapID1.3.6.1.2.1.14.16.2.8: Non-virtual Interface 10.254.0.57 index 0 Router 10.255.0.1 received error packet from 10.254.0.57 PacketType 1.

#Jun 18 15:14:35:496 2012 S10508 OSPF/4/IF_BAD_RX: OSPF TrapID1.3.6.1.2.1.14.16.2.8: Non-virtual Interface 10.254.0.73 index 0 Router 10.255.0.1 received error packet from 10.254.0.73 PacketType 1.

三、 过程分析：

从打印的信息来看，故障现象比较明显，网络内存在Router ID冲突，冲突的Router ID就是S10500的Router ID 10.255.0.1。

通过display ospf error 也可以清楚的看到OSPF Router ID confusion错误在不断增长。

display ospf error

OSPF Process 10 with Router ID 10.255.0.1

OSPF Packet Error Statistics

576978 : OSPF Router ID confusion 0: OSPF bad packet

0 : OSPF bad version 0: OSPF bad checksum

0 : OSPF bad area ID 0: OSPF drop on unnumbered interface

0 : OSPF bad virtual link 0: OSPF bad authentication type

0 : OSPF bad authentication key 0: OSPF packet too small

0 : OSPF Neighbor state low 0: OSPF transmit error

0 : OSPF interface down 2: OSPF unknown neighbor

0 : HELLO: Netmask mismatch 0: HELLO: Hello timer mismatch

0 : HELLO: Dead timer mismatch 0: HELLO: Extern option mismatch

0 : HELLO: Neighbor unknown 0: DD: MTU option mismatch

0 : DD: Unknown LSA type 0: DD: Extern option mismatch

0 : LS ACK: Bad ack 0: LS ACK: Unknown LSA type

0 : LS REQ: Empty request 0: LS REQ: Bad request

0 : LS UPD: LSA checksum bad 0: LS UPD: Received less recent LSA

0 : LS UPD: Unknown LSA type

display ospf error

OSPF Process 10 with Router ID 10.255.0.1

OSPF Packet Error Statistics

576994 : OSPF Router ID confusion 0: OSPF bad packet

0 : OSPF bad version 0: OSPF bad checksum

0 : OSPF bad area ID 0: OSPF drop on unnumbered interface

0 : OSPF bad virtual link 0: OSPF bad authentication type

0 : OSPF bad authentication key 0: OSPF packet too small

0 : OSPF Neighbor state low 0: OSPF transmit error

0 : OSPF interface down 0: OSPF unknown neighbor

0 : HELLO: Netmask mismatch 0 : HELLO: Hello timer mismatch

0 : HELLO: Dead timer mismatch 0: HELLO: Extern option mismatch

0 : HELLO: Neighbor unknown 0: DD: MTU option mismatch

0 : DD: Unknown LSA type 0: DD: Extern option mismatch

0 : LS ACK: Bad ack 0: LS ACK: Unknown LSA type

0 : LS REQ: Empty request 0 : LS REQ: Bad request

0 : LS UPD: LSA checksum bad 0: LS UPD: Received less recent LSA

0 : LS UPD: Unknown LSA type

且现场S10500设备上每一个VLAN虚接口都提示收到了错包。

现场组网中OSPF设备较多，逐一排查比较困难，要找到哪台设备和S10500的Router ID冲突了就存在一个很大的困难，问题的焦点就集中在如何找出这台冲突的设备。这里介绍一个相对简单的方法，在S10500上配置一个ACL来匹配OSPF报文。

acl number 3333

rule permint ip ospf

然后设备上开启debug引用此ACL，这样就可以只打印OSPF相关的协议报文：debug ip packet acl 3333

打开debug开关之后，发现了下面的debug信息：

*Jun 19 14:25:58:433 2012 S10508 IPTRAP/7/debug_case:

Delivering, interface = Vlan-interface806, version = 4, headlen = 20, tos = 192,

pktlen = 68, pktid = 26772, offset = 0, ttl = 1, protocol = 89,

checksum = 25785, s = 10.254.0.81, d = 224.0.0.5

prompt: IP packet is delivering up!

*Jun 19 14:25:58:433 2012 S10508 IPFWD/7/debug_case: -Chassis=2-Slot=7;

Receiving, interface = Vlan-interface806, version = 4, headlen = 20, tos = 192,

pktlen = 68, pktid = 26772, offset = 0, ttl = 1, protocol = 89,

checksum = 25785, s = 10.254.0.81, d = 224.0.0.5

prompt: Receiving IP packet

从debug信息，我们发现，设备从VLAN interface 806发出去一个OSPF报文，紧接着报文又从这个VLAN interface 806收到，收到报文的源IP10.254.0.81恰好就是S10500设备自己的VLAN 806虚接口地址。这样就报了router ID 冲突以及收到错包的提示。

接下来的疑问就是为何设备会从这个虚接口收到自己发送的OSPF报文呢？通过查看配置，我们发现S10500上报此错误是因为IPS将OSPF组播报文弹回导致， OSPF报文为何会被弹回呢？我们想到此设备上配置了IPS插卡，检查IPS插卡配置发现，原来是S10500上插卡的接口Ten-GigabitEthernet1/7/0/1和Ten-GigabitEthernet2/7/0/1的配置存在问题， 导致IPS插卡 deny广播、组播、arp的策略没有生效导致，下面是错误的

配置。红色部分错误配置导致设备实际上并没有deny掉ACL 4000中定义的报文。

```
acl number 4000
 description Match-MultiCast-Broadcast-ARP
 rule 0 permit dest-mac 0100-0000-0000 ff00-0000-0000
 rule 5 permit dest-mac ffff-ffff-ffff ffff-ffff-ffff
 rule 10 permit type 0806 ffff
#
traffic classifier Multicast-Broadcast-ARP operator or
 if-match acl 4000
#
traffic behavior Deny-Multicast-Broadcast-ARP
 filter deny
qos policy Deny-Multicast-Broadcast-ARP
 classifier Multicast-Broadcast-ARP behavior Deny-Multicast-Broadcast-ARP
#
interface Ten-GigabitEthernet1/7/0/1
 port link-mode bridge
 description Link_To_IPS-01
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 800 802 805 807 809 to 810
 flow-interval 5
 stp disable
packet-filter 4000 inbound
qos apply policy Deny-Multicast-Broadcast-ARP inbound
mac-address mac-learning disable
#
interface Ten-GigabitEthernet2/7/0/1
 port link-mode bridge
 description Link_To_IPS-02
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 801 803 806 808 to 810
 flow-interval 5
 stp disable
packet-filter 4000 inbound
qos apply policy Deny-Multicast-Broadcast-ARP inbound
mac-address mac-learning disable
```

四、 解决方法：

问题原因清楚了之后。只有修改配置将ACL 4000中定义的报文deny掉即可。修改后的配置如下：

```
interface Ten-GigabitEthernet1/7/0/1
 port link-mode bridge
 description Link_To_IPS-01
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 800 802 805 807 809 to 810
```

flow-interval 5

stp disable

qos apply policy Deny-Multicast-Broadcast-ARP outbound

mac-address mac-learning disable

interface Ten-GigabitEthernet2/7/0/1

port link-mode bridge

description Link_To_IPS-02

port link-type trunk

undo port trunk permit vlan 1

port trunk permit vlan 801 803 806 808 to 810

flow-interval 5

stp disable

qos apply policy Deny-Multicast-Broadcast-ARP outbound

mac-address mac-learning disable

修改配置之后不再报此OSPF Router ID冲突错误。

这个案例重点在于三点：

1. 这个OSPF Router ID冲突故障相对比较少见，在配置IPS插卡时，一定要注意deny掉组播、arp、广播等报文防止其被环回。
2. 在排查OSPF Router ID冲突的问题时，大家可以使用ACL来匹配OSPF报文，开启debug ip packet时引用此ACL，这样可以只debug到OSPF报文，并且可以看到报文的源IP，就不需要逐台设备检查配置去排查冲突源了。
3. 下发策略时需要在S10500与IPS插卡的outbound方向下发，如果在inbound方向下发只能deny掉部分报文，因为协议报文会被系统ACL抓上CPU，因此inbound方向下发时不能deny掉OSPF这样的协议报文。

   qos apply policy Deny-Multicast-Broadcast-ARP outbound