75交换机查看上CPU报文的方法

杨超 2007-12-26 发表

> **75交换机查看上CPU报文的方法**

在处理75交换机CPU利用率高、ARP攻击、网络环路等问题时，经常需要抓取上CPU的报文，以判断从哪里来的什么报文导致了该问题，确定导致问题的源，从而采取进一步措施使网络恢复正常。本文就75交换机上如何查看上CPU的报文做一介绍。

一、 进入诊断模式

本文中的命令多是在诊断模式下使用的。在系统模式下使用en命令即可进入诊断模式：

```
<S6506R-Right>
<S6506R-Right>system-view
System View: return to User View with Ctrl+Z.
[S6506R-Right]en
NOTICE: Commands under this mode may influence the machine's configuration data,so you need to ensure that your configure has been saved to flash before executing them and reset the machine afte
r executing them.
[S6506R-Right-testdiag]
```

二、 对上CPU的报文分类统计

```
[S6506R-Right-testdiag]catch rxtx by ?
  da      Dest packet mac
  dip     Dest IP
  etype   Packet type
  iptype  Packet IP type
  sa      Source packet mac
  sip     Source IP
  vlan    VLAN
```

使用如上命令可以根据源mac、目的mac、源IP、目的IP、帧类型、报文类型、VLAN等对报文进行统计。

该命令还可以统计不同单板的报文信息进行统计。如果不输入槽位号则默认统计0槽位的主控板上CPU的报文。

```
[S6506R-Right-testdiag]catch rxtx by sip ?
  slot  Set Slot Number
  <cr>
```

执行完之后，等待一定时间，再使用下面的命令停止统计，需要制定相应的槽位号，如果不指定则默认为0号槽位的主控板：

```
[S6506R-Right-testdiag]catch rxtx end ?
  slot  Set Slot Number
  <cr>
```

如按照etype统计上2号槽位单板的报文：

```
[S6506R-Right-testdiag]catch rxtx by etype slot 2
```

等待一分钟后

```
[S6506R-Right-testdiag]catch rxtx end slot 2
Slot 2: information of Module RxTx
 The Catch Result of etype is :
        806 -------- 150666
        ffee -------- 700
        cdef -------- 950
        800 -------- 230
        6a -------- 88
        88a7 -------- 3
        8809 -------- 12
```

该统计表明在我们等的时间间隔（一分钟）内，etype为806，即arp报文有150666个上送到CPU。该数目远远超过正常值，因此初步判断设备遭到了ARP攻击。顺便提一下，ffee和cdef类型的报文为我们设备板间交互报文。

按照源IP对2号槽位上CPU的报文进行统计：

```
[S6506R-Right-testdiag]catch rxtx by sip slot 2
```

等待一分钟后

```
[S6506R-Right-testdiag]catch rxtx end slot 2
```

```
Slot 2: information of Module RxTx
 The Catch Result of sip is :
        192.168.1.1 -------- 88631
        10.141.51.63 -------- 3
        192.168.0.1 -------- 3
        10.3.40.5 -------- 14
        192.168.1.89 -------- 7
        10.0.1.1 -------- 6
```

该统计信息表明一分钟内从192.168.1.1上来的报文有88631之多，因此怀疑该IP对应的设备存在问题，可以让用户排查该IP对应的设备。

三、 抓取上CPU的报文

有时候我们需要查看上CPU的报文，可以通过开关控制我们需要抓取的报文。通过下面的命令可以查看可以打开哪些开关，与前面的catch命令一样，该命令也可以查看不同单板的相关信息：

```
[S6506R-Right-testdiag]dis rxtx ?
  all         All packet
  broadcast   Broadcast packet
  chip        Chip
  cos         COS
  dest_mac    Dest packet mac
  dip         Dest IP
  etype       Packet type
  iptype      Packet IP type
  multicast   Multicast packet
  port        Port
  reason      Receive packet reason
  receive     Receive packet
  remote      Display packet to memory
  send        Send packet
  sip         Source IP
  source_mac  Source packet mac
  switchflag  Set Slot Number
  unicast     Unicast packet
  vlan        VLAN
  vp          VP packet
```

设置开关，如在slot2抓取源地址为192.168.1.1的报文

```
[S6506R-Right-testdiag]dis rxtx sip 192.168.1.1 slot 2
Slot 2: information of Module RxTxSlot 2: information of Module RxTx
```

可以查看2号槽位打开了哪些开关，即抓取具有哪些特征的报文。如下面的例子表明抓取源地址为192.168.1.1的报文

```
[S6506R-Right-testdiag]dis rxtx switchflag slot 2
Slot 2: information of Module RxTx
 The switchflag of the packet printing
      Broadcast  : Yes
      Multicast  : Yes
      Unicast    : Yes
      Receive    : Yes
      Send       : Yes
      Vp         : No

      Dest mac   : All
      Source mac : All
      VlanID     : All
      ChipID     : All
      PortNumber : All
      EtherType  : All
      DestIP     : All
      SourceIP   : 192.168.1.1(I)
      IPType     : All
      Display    : Console
      Reason     : All
      Cos        : All

      ALL:No limitation (I):Include {E}:Exclude
```

之后就可以用下面的命令抓取报文了。在使用下面的命令之前，需要在用户视图下打开以下两个开关

:
<S6506R-Right>terminal debugging
% Current terminal debugging is on
<S6506R-Right>terminal monitor
% Current terminal monitor is on
在后在诊断模式下，使用下面的命令采集满足前面制定特征的100个上2号业务板的报文。
[S6506R-Right-testdiag]debug rxtx -c 100 pkt slot 2
Slot 2: information of Module RxTx
 Debug RxTx packet is on!
上来的报文可能为如下格式：
*0.47538967 Quidway S6506R RXTX/8/pkt: received packet from chip1,port2,reason=0x1000,cos=2,l
en=68
*0.47539089 Quidway S6506R RXTX/8/pkt:
----
00 e0 fc 0b e5 a9 00 e0 fc 0b 0c 62 81 00 00 67
08 00 45 00 00 30 4b f4 40 00 07 06 f5 21 50 0d
55 61 dc c0 b0 83 10 a0 00 50 6e 45 90 2f 00 00
00 00 70 02 40 00 01 08 00 00 02 04 05 b4 01 01

该报文为IP报文，chip1，port2表示从1号芯片的2号口上来，报文中的各项数据分别表示：
00 e0 fc 0b e5 a9   -->目的MAC
00 e0 fc 0b 0c 62   -->原MAC
00 67   --> VLAN为67（HEX）= 103
08 00   -->IP报文
06   -->协议类型：06为tcp报文，11为udp报文，01为icmp报文
50 0d 55 61   -->源IP地址：80.13.85.97
dc c0 b0 83   -->目的IP地址:220.192.176.131
经常见到的ARP报文格式如下：
----
        00 0f e2 3f d6 0c 00 11 09 03 d2 70 81 00 00 08
        08 06 00 01 08 00 06 04 00 02 00 11 09 03 d2 70
c0 a8 08 50 00 0f e2 3f d6 0c c0 a8 08 01 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0806表示为arp报文，之后第8个位置的数据，01为arp request报文，02表示为arp reply报文。由此判
断此报文为arp reply报文。之后的数据中，00 11 09 03 d2 70为源mac，c0 a8 08 50为源IP， 00 0f e
2 3f d6 0c c0 a8 08 01为目的mac和目的IP。
arp request报文0806之后的部分如下：
  00 01 08 00 06 04 00 01 00 e0 fc 20 1e 17 0a 99 5b 01 00 00
  00 00 00 00 0a 99 5b 17
在抓取报文之后，记得要关闭开关：
[S6506R-Right-testdiag]dis rxtx all ?
  slot Set Slot Number
  <cr>
打开了那个槽位的开关则关闭哪个槽位的开关。
[S6506R-Right-testdiag]dis rxtx switchflag
Slot 0: information of Module RxTx
 The switchflag of the packet printing
     Broadcast : Yes
     Multicast : Yes
     Unicast   : Yes
     Receive   : Yes
     Send   : Yes
     Vp   : No

     Dest mac   : All
     Source mac : All
     VlanID   : All
     ChipID   : All
     PortNumber : All
     EtherType : All
     DestIP   : All
     SourceIP   : All
     IPType   : All

Display : Console
Reason : All
Cos : All

ALL:No limitation (I):Include {E}:Exclude
[S6506R-Right-testdiag]
这种状态表明没有特殊的开关打开，为初始状态。
之后请在用户视图下关闭打开的开关：
<S6506R-Right>undo terminal debugging
% Current terminal debugging is off

<S6506R-Right>undo terminal monitor
% Current terminal monitor is off
通过以上方法，我们能够看到上送CPU的报文，根据实际情况和报文可以分析可能存在的问题。