某局点t1000下联组播业务异常问题

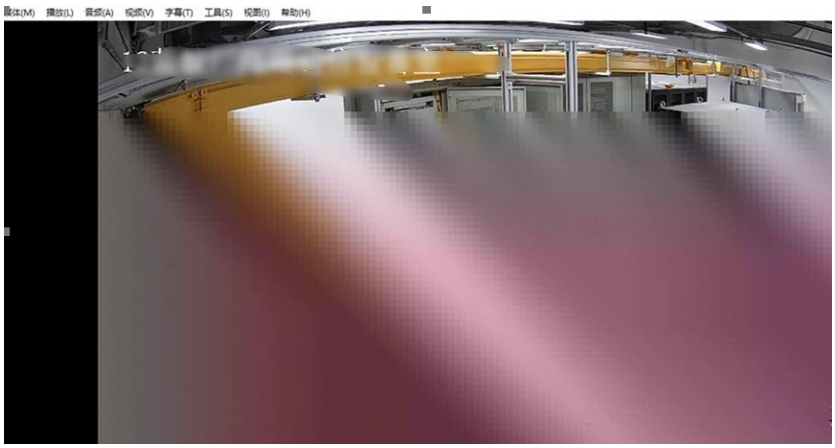
域间策略/安全域 ASPF 攻击防范 **陈泽勇** 2024-05-29 发表

组网及说明

t1000透明部署串联在核心交换机和防火墙之间，上下联都做的二层聚合。

问题描述

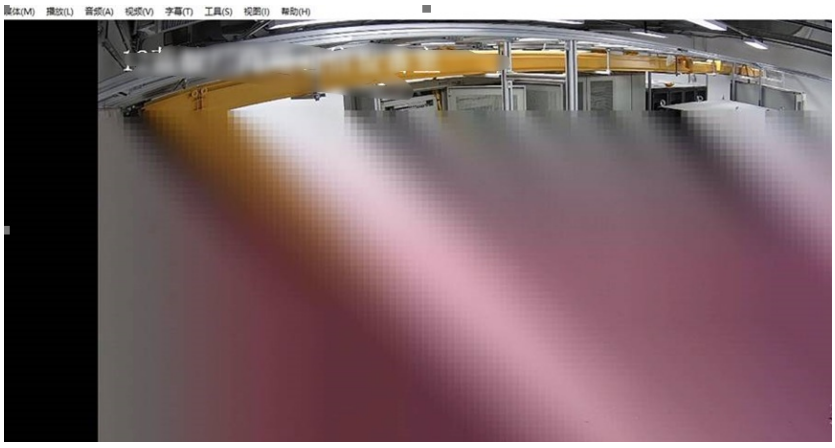
没有接入t1000设备的时候，组播业务正常；接入之后组播业务卡顿且花屏如下（为了方便测试该组播接收者直连在t1000 1/0/10口下）：



跳过设备直连核心交换机回显如下：

过程分析

1、没有接入t1000设备的时候，组播业务正常；接入之后组播业务卡顿且花屏如下：



2、查看配置安全策略全放通且没有开启dpi，查看cpu和内存都是正常的没有异常信息：

```
==============display cpu history==============
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|
 10%|
  5%|
    ------------------------------------------------------------
              10        20        30        40        50        60  (minutes)
               cpu-usage (Slot 1 CPU 0) last 60 minutes (SYSTEM)
==========================================================
```

```
#
security-policy ip
 rule 0 name any
  action pass
#
```

```
==============display memory==============
Memory statistics are measured in KB:
Slot 1:
             Total       Used       Free     Shared    Buffers     Cached  FreeRatio
Mem:       8210752    3027520    5183232          0      20160     586944       64.4%
-/+ Buffers/Cache:    2420416    5790336
```

3、后续将接电脑的接口的flow-intre改为5，查看display interface发现可能存在突发流量，敲了几次有一次达到了40%左右，其余都是1%左右。

一次40%：

```
[H3C_XY_IPSJdis interface g1/0/10
GigabitEthernet1/0/10
Current state: UP
Line protocol state: UP
IP packet frame type: Ethernet II, hardware address: 58b3-8fce-c4ac
Description: GigabitEthernet1/0/10 Interface
Bandwidth: 1000000 kbps
Loopback is not set
Media type is twisted pair, loopback not set, promiscuous mode set
1000Mb/s, Full-duplex, link type is autonegotiation
Output flow-control is disabled, input flow-control is disabled
1000Mbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
Maximum frame length: 9216
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
PVID: 100
MDI type: Automdix
Port link-type: Access
 Tagged VLANs:   None
 Untagged VLANs: 100
Last link flapping: 1 hours 6 minutes 7 seconds
Last clearing of counters: Never
Current system time:2024-05-28 14:30:59
Last time when physical state changed to up:2024-05-28 13:24:52
Last time when physical state changed to down:2024-05-28 11:42:09
 Peak input rate: 31315 bytes/sec, at 2024-05-28 11:34:13
 Peak output rate: 2010447 bytes/sec, at 2024-05-28 14:11:03
 Last 5 second input: 3 packets/sec 620 bytes/sec 0%
 Last 5 second output: 39813 packets/sec 48659035 bytes/sec 40%
 Input (total):  17071 packets, 2531663 bytes
         12039 unicasts, 1133 broadcasts, 3899 multicasts, 0 pauses
 Input (normal):  17071 packets, 2531663 bytes
         12039 unicasts, 1133 broadcasts, 3899 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, - throttles
         0 CRC, 0 frame, 0 overruns, 0 aborts
         0 ignored, - parity errors
 Output (total): 8503557 packets, 10392435976 bytes
         16055 unicasts, 5841 broadcasts, 8481661 multicasts, 0 pauses
 Output (normal): 8503557 packets, 10392435976 bytes
         16055 unicasts, 5841 broadcasts, 8481661 multicasts, 0 pauses
 Output: 0 output errors, 0 underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
```

其余几次都只有1%：

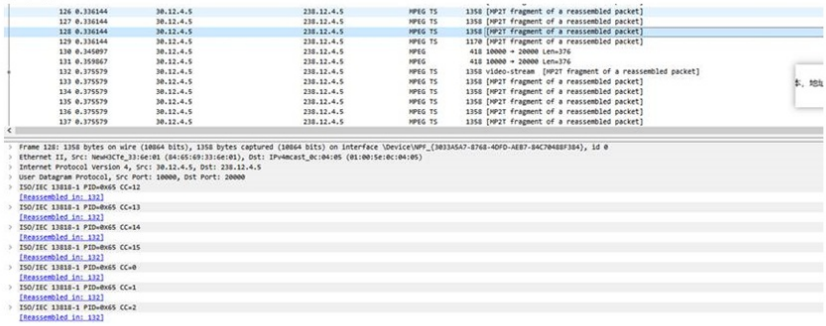
```
[H3C_XY_IPS]dis interface g1/0/10
GigabitEthernet1/0/10
Current state: UP
Line protocol state: UP
IP packet frame type: Ethernet II, hardware address: 58b3-8fce-c4ac
Description: GigabitEthernet1/0/10 Interface
Bandwidth: 1000000 kbps
Loopback is not set
Media type is twisted pair, loopback not set, promiscuous mode set
1000Mb/s, Full-duplex, link type is autonegotiation
Output flow-control is disabled, input flow-control is disabled
1000Mbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
Maximum frame length: 9216
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
PVID: 100
MDI type: Automdix
Port link-type: Access
 Tagged VLANs:   None
 Untagged VLANs: 100
Last link flapping: 1 hours 6 minutes 19 seconds
Last clearing of counters: Never
Current system time:2024-05-28 14:31:11
Last time when physical state changed to up:2024-05-28 13:24:52
Last time when physical state changed to down:2024-05-28 11:42:09
 Peak input rate: 31315 bytes/sec, at 2024-05-28 11:34:13
 Peak output rate: 201044? bytes/sec, at 2024-05-28 14:11:03
 Last 5 second input: 0 packets/sec 0 bytes/sec 0%
 Last 5 second output: 1356 packets/sec 1651393 bytes/sec 1%
 Input (total):  17074 packets, 2534053 bytes
         12039 unicasts, 1133 broadcasts, 3902 multicasts, 0 pauses
 Input (normal):  17074 packets, 2534053 bytes
         12039 unicasts, 1133 broadcasts, 3902 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, - throttles
         0 CRC, 0 frame, 0 overruns, 0 aborts
         0 ignored, - parity errors
 Output (total): 8523904 packets, 10417262223 bytes
         16059 unicasts, 5916 broadcasts, 8501929 multicasts, 0 pauses
 Output (normal): 8523904 packets, 10417262223 bytes
         16059 unicasts, 5916 broadcasts, 8501929 multicasts, 0 pauses
 Output: 0 output errors, 0 underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, 0 no carrier
```

4、后续display packet dorp interface去看丢包情况发现是没有记录的都是空，且开启burst-mode enable之后故障依旧：

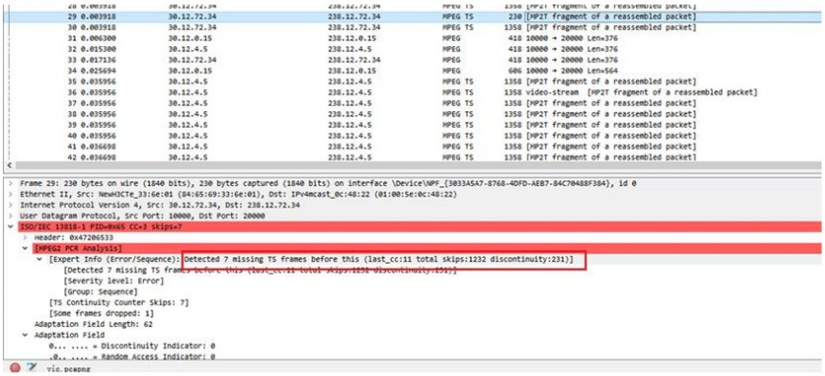
```
Packets dropped due to create mbuf: 0

GigabitEthernet1/0/10:
Packets dropped due to runt frame: 0
Packets dropped due to packet too long: 0
Packets dropped due to align: 0
Packets dropped due to under run: 0
Packets dropped due to over run: 0
Packets dropped due to CRC: 0
Packets dropped due to no buffer: 0
Packets dropped due to dribble: 0
Packets dropped due to lost carriers: 0
Packets dropped due to tx collision: 0
Packets dropped due to defered: 0
Packets dropped due to MAC fileter: 0
Packets dropped due to cpu receive: 0
Packets dropped due to create mbuf: 0

GigabitEthernet1/0/11:
Packets dropped due to runt frame: 0
```

5、让现场直接跳过t1000接上联的核心交换机发现监控画面恢复正常，于是在终端侧异常和正常的时候都抓了对应的报文发现异常时候的报文是每一份丢失7-8个tc帧，还是丢在t1000上了。

正常抓包：



异常抓包：



解决方法

后续和产线确认，目前版本都是组播逐包转发，可能会引入乱序。后续关闭组播逐包后测试正常。

probe

undo hardware cavium-chip mcast-per-packet enable