交换机拥塞丢包问题排查云图



一、 开始

在现网运行中,当交换机端口接收到的报文超过最大转发能力时,此时端口会出现拥塞 丢包,影响到业务,如组播花屏马赛克,tcp重传,业务大量丢包等。拥塞丢包的具体排查 思路如下:

步骤1:收集相关信息,确定是否有拥塞丢包

步骤 2: 确认端口下是否有配置限速或者整形

步骤 3: 确认组网是否有端口高速打低速或端口多打一的情况

步骤 4: 确认是否有瞬间突发流量

步骤 5: 解决方案

二、 流程图相关操作说明

当交换机端口接收到的报文超过最大转发能力时,此时端口会出现拥塞丢包。 拥塞丢包产生条件可以分为以下几类:

- 1) 端口多打一,多个端口向一个端口同时发送数据
- 2) 端口高速打低速,高速端口向低速端口转发数据
- 3) 端口的出方向配置限速或者整形,发送的流量超过限速或者整形的阈值
- 4) 瞬间突发大流量:网络流量存在突发,在某个时刻端口流量超过端口的带宽

1、确定是否有拥塞丢包

先收集一下以下信息:

| display interface XXX XXX 为 拥塞丢包的物理端口 |
|---|
| display qos queue-statistics interface XXX outbound <mark>XXX 为 拥塞丢包的物理端口</mark> |
| display buffer usage slot XXX <mark>XXX 为 拥塞丢包的物理端口所槽位</mark> |
| 如 以 端口 interface Ten-GigabitEthernet 1/0/1 为例,收集信息为 |
| display interface Ten-GigabitEthernet 1/0/1 |
| display qos queue-statistics interface Ten-GigabitEthernet 1/0/1 outbound |
| displav buffer usage slot <mark>1</mark> |

通过命令 display qos queue-statistics interface Ten-GigabitEthernet 1/0/1 (需要查看的出

接口)outbound 来查看接口在出方向在各队列转发的时候是否丢包,如果出现拥塞丢包,

对应的队列会在下方标红部分 Dropped 部分有计数。

```
<H3C>dis qos queue-statistics interface Ten-GigabitEthernet 1/0/1 outbound
Interface: Ten-GigabitEthernet1/0/1
Direction: outbound
Queue 0
 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
 Queue 1
 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
 Queue 2
 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
 Queue 3
 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
 Queue 4
 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 5
 Forwarded: 5953 packets, 2076790 bytes, 0 pps, 0 bps
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 6
 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
```

| 5sec 1min 5min |
|------------------------------------|
| Ten-GigabitEthernet $1/0/1$ 0% 0% |
| |
| Ten-GigabitEthernet1/0/2 0% 0% 0% |
| Ten-GigabitEthernet1/0/3 0% 0% 0% |
| Ten-GigabitEthernet1/0/4 0% 0% 0% |
| Ten-GigabitEthernet1/0/5 0% 0% 0% |
| Ten-GigabitEthernet1/0/6 0% 0% 0% |
| Ten-GigabitEthernet1/0/7 0% 0% 0% |
| Ten-GigabitEthernet1/0/8 0% 0% 0% |
| Ten-GigabitEthernet1/0/9 0% 0% 0% |
| Ten-GigabitEthernet1/0/10 0% 0% 0% |
| Ten-GigabitEthernet1/0/11 0% 0% 0% |
| Ten-GigabitEthernet1/0/12 0% 0% 0% |
| Ten-GigabitEthernet1/0/13 0% 0% 0% |
| Ten-GigabitEthernet1/0/14 0% 0% 0% |
| Ten-GigabitEthernet1/0/15 0% 0% 0% |
| Ten-GigabitEthernet1/0/16 0% 0% 0% |
| Ten-GigabitEthernet1/0/17 0% 0% 0% |
| Ten-GigabitEthernet1/0/18 0% 0% 0% |
| Ten-GigabitEthernet1/0/19 0% 0% 0% |
| Ten-GigabitEthernet1/0/20 0% 0% 0% |
| Ten-GigabitEthernet1/0/21 0% 0% 0% |
| Ten-GigabitEthernet1/0/22 0% 0% 0% |
| Ten-GigabitEthernet1/0/23 0% 0% 0% |
| Ten-GigabitEthernet1/0/24 0% 0% 0% |

buffer 不足导致持续丢包的情况,主要关注 buffer 的使用率是否持续高或者达到 100%。

通过命令 display buffer usage slot 1 查看 buffer 的使用情况,该命令适用于

2、确认端口下是否有配置限速或者流量整形

如果端口下配置有限速或者流量整形,那丢包是因为配置原因导致丢弃,可以暂时取消 相关配置后,观察一下

3、确认组网是否有端口高速打低速或端口多打一的情况

可以配置流量统计确认丢包位置,并分析组网是否有端口高速打低速或端口多打一的情况

4、确认是否有瞬间突发流量

交换机转发流量可以分为平均速率和瞬时速率2个层面分析:

1) 平均速率:

display interface 看到的接口流量,这个是一段时间内的平均流量,默认 300 秒。 [H3C]display interface GigabitEthernet1/0/1 GigabitEthernet1/0/1 current state: UP Peak value of input: 174 bytes/sec, at 2000-05-30 17:49:11 Peak value of output: 5415 bytes/sec, at 2000-05-29 13:17:05 //端口输入输出流量的峰值速率大小,单位为 bytes/sec Last 300 seconds input: 0 packets/sec 4 bytes/sec 0% Last 300 seconds output: 0 packets/sec 22 bytes/sec 0% //接口在最近 300 秒接收/发送报文的平均速率 可以配置 flow-interval 5, 查看 5s 内接收/发送报文的平均速虑

2) 瞬时速率

假设产生的是瞬时突发,端口在非常短的时间(毫秒级别)内收到非常多的突发数据, 以至于瞬时突发速率达到平均速率的数十倍、数百倍,甚至超过端口带宽的现象,而上述接 口下速率因为是数秒或者数分钟时间的平均数率,通常无法体现这种微突发,因此当看到接 口下统计的速率没有出现很高的情况,并不能说明没有出现过瞬时突发。

极端瞬时突发的例子:假设一个 10GE 链路上有平均 1Gbps 速率的流量,极端情况下可 以是:前 100 毫秒有 10Gbps 的流量,后面 900 毫秒的流量为 0。这时前 100 毫秒的 10Gbps 的流量对于设备而言就是瞬时突发。突发流量的瞬时速率超过交换机的转发能力,交换机会 将突发的数据进行缓存以便稍后发送。如果交换机没有足够的缓存,那么超出的数据只能丢 弃,这就产生了拥塞丢包。一般缓存都很小,只能缓存几毫秒的流量

可以借助捕获报文软件和 Wireshark 软件来检测网络中是否存在瞬时突发。使用 Wireshark 软件打开捕获报文软件记录的捕获到的报文文件,选择"统计 > 1/0 图表", 就可以看到流量图。在 I0 图表中,可以将 Y 轴单位改为 Bits,间隔改为秒或者 1 毫秒, 这样就能看到秒级或毫秒级流量的突发。

下图是导出图表过程示例:

| He Edit Yiew Go Capture Analyze Statistics Tele; | hony Ioos Internals Help |
|--|---|
| 🛛 🛞 📕 🚊 📄 🗎 💥 💕 🖻 Summary | j q q q 🗉 🕷 X 🧕 🕷 🕅 |
| Filter: Comments S Show addres | ummary s resolution ression Clear Apply Save |
| Vo. Time Protocol Hier | archy ination Protocol Length Info |
| 1 2019-11-27 16:54:04.938 B Conversation | 6 e1:ad:13:26:c1 ARP 56 100.118.116.212 is at 00:00:00:00:0 |
| 2 2019-11-27 16:54:04.9621 @ Endpoints | tegro_79:0c:2e ARP 56 100.118.117.11 is at 00:00:00:00:00 |
| 3 2019-11-27 16:54:04,996 Backet Land | 9c:23:2e:55:4b ARP 56 100.118.117.23 /s at 00:00:00:00:00 |
| 4 2019-11-27 16:54:05.089 | 39:09:3f:fc:af ARP 56 100.118.118.160 is at 00:00:00:00:0 |
| 5 2019-11-27 16:54:05.136 | 62:e5:12:06:1f ARP 56 100.118.116.254 is at 00:00:00:00:00:0 |
| 6 2019-11-27 16:54:05.3371 Conversation | List tegro_7a:97:06 ARP 56 100.118.118.116 is at 00:00:00:00:00:0 |
| 7 2019-11-27 16:54:05.3490 Enderset 14 | cc:6a:c9:c3:98 ARP 56 100.118.119.38 is at 00:00:00:00:00 |
| 8 2019-11-27 16:54:05.3491 groupown Lis | 39:09:3f:02:85 ARP 56 100.118.116.153 is at 00:00:00:00:0 |
| 9 2019-11-27 16:54:05.359(Service Mesp | onse ime /versa_3e:65:eb ARP 56 100.118.116.254 is at 00:00:00:00:0 |
| 10 2019-11-27 16:54:05.376 29WAR | 16:45:2a:b9:cc ARP 56 100.118.119.33 is at 00:00:00:00:00 |
| 11 2019-11-27 16:54:05.3804 ANCD | tegro_1d:3a:58 ARP 56 100.118.118.160 is at 00:00:00:00:00: |
| 12 2019-11-27 16:54:05.391 | 62:e5:13:5f:a4 ARP 56 100,118,78,1 15 at 00:00:00:00:00:00 |
| 13 2019-11-27 16:54:05.437 | versa_51:ae:82 ARP 56 100.118,117.218 is at 00:00:00:00:0 |
| 14 2019-11-27 16:54:05.468(Collecte | 4b:90:c7:c1:55 ARP 56 100,118,116,200 is at 00:00:00:00:0 |
| 15 2019-11-27 16:54:05.471 Compare | e1:ad:7c:8d:6d ARP 56 100.118.116.174 is at 00:00:00:00:00 |
| 16 2019-11-27 16:54:05. 517 14 Row Graph. | + control-true-(for-OxBAA) 174 Ethernet II |
| 17 2019-11-27 16:54:05.5841 HART-IP | 60:24:98:d3:c2 ARP 56 100.118.116.182 is at 00:00:00:00:00: |
| 18 2019-11-27 16:54:05.690 UTT | 62:e5:06:97:c6 ARP 56 100.118.116.208 is at 00:00:00:00:0 |
| | The second |



5、解决方案

1) 突发来源及场景排查:

- 从流量来源和组网上着手,寻找突发的源头,使源头不会过度、过快、突发过强地发包, 尽量从根源上减少瞬时突发。
- ▶ 在网络业务流量规划时,尽量避免多打一场景,避免收敛比过高的场景。

2) 硬件能力提升:

进行出端口扩容,增加出口带宽,出端口做聚合或者更换成高速链路。网络中重要节点替换 为缓存更大的设备。

3) 配置增强模式提高抗突发能力

开启 burst-mode enable 命令,在同一时刻并发突发的端口不多的情况下能够优化现网的

拥塞丢包问题

开启该命令后,对于网络中少量突发的情况,可以提供更好的报文缓存功能和流量转发性能,缓解接口下因突发流量造成的丢包。

但同一芯片多个端口同时瞬时突发,则可能无法完全解决丢包,且会影响其他正常端口的转发性能,该功默认关闭。