常见问题答复集（二）

H3C交换机基础维护篇

精选Q&A

话不多说，《常见问题答复集》第二期来啦！

PS. 好多小伙伴在后台留言，希望将我们的文章内容保存成PDF形式，方便随时查看，这个有哒！

链接： https://zhiliao.h3c.com/ 记得用PC端打开哦！

指路： 知了社区-运维工具-资料中心-交换机-《交换那些事儿》系列维护资料，快去瞧瞧吧！

VLAN篇

Q1 为什么部分VLAN无法通过Trunk端口？

部分VLAN无法通过Trunk端口，可能是用户未将相应的VLAN加入到Trunk端口。此外，本端设备Trunk端口的缺省VLAN ID和相连对端设备Trunk端口的缺省VLAN ID必须一致，否则报文将不能转发。

出现该问题时，可以通过display vlan命令来查看相应的VLAN是否加入了Trunk端口。若未加入，可以在接口视图下通过port trunk permit vlan命令设置相应的VLAN加入Trunk口，同时通过port trunk pvid命令正确配置Trunk端口的PVID。

Q2 如何正确配置允许所有VLAN通过Trunk端口？

基于Trunk端口的VLAN只能在接口视图下配置，正确配置步骤如下：

```
(1) 进入系统视图。
system-view
(2) 进入二层以太网接口视图。
interface interface-type interface-number
(3) 配置端口的链路类型为Trunk类型。
port link-type trunk
缺省情况下，端口的链路类型为Access类型。
(4) 允许所有的VLAN通过当前Trunk端口。
port trunk permit vlan all
缺省情况下，Trunk端口只允许VLAN 1的报文通过。
(5) 配置Trunk端口的PVID。
port trunk pvid vlan vlan-id
缺省情况下，Trunk端口的PVID为VLAN 1。
```

建议用户谨慎使用port trunk permit vlan all命令，以防止未授权VLAN的用户通过该端口访问受限资源。

Q3 为什么设备获取不到IP Phone的MAC地址？

设备获取不到IP Phone的MAC地址，可能是该话机不在设备缺省的OUI地址中，请客户按以下配置步骤预先配置话机的OUI地址，然后执行display voice-vlan mac-address命令查看表项中是否存在该话机。配置步骤：

```
(1) 进入系统视图。
system-view
(2) 配置Voice VLAN识别的OUI地址。
voice-vlan mac-address oui mask oui-mask [ description text ]
Voice VLAN启动后将有缺省的OUI地址。
```

在配置Voice VLAN的OUI时,需要注意：

1. OUI地址不能是广播地址或者组播地址，也不能是全0的地址。

2. OUI地址是mac-address和oui-mask参数相与的结果。

3. 设备最多支持配置OUI地址个数以具体产品实际规格为准。

Q4 网络中存在流量泛洪导致断网，该如何处理？

可以通过划分设备所属VLAN，将广播报文限制在一个VLAN内，有效地限制广播域范围。交换机支持基于端口、MAC地址、IP子网、协议的方式来划分VLAN。

Q5 错误配置接口链路类型导致无法正常通信怎么办？

首先要正确区分三种端口的链路类型：

1. Access：端口只能发送一个VLAN的报文，发出去的报文不带VLAN Tag。一般用于和不能识别VLAN Tag的用户终端设备相连，或者不需要区分不同VLAN成员时使用。

2. Trunk：端口能发送多个VLAN的报文，发出去的端口缺省VLAN的报文不带VLAN Tag，其他VLAN的报文都必须带VLAN Tag。通常用于网络传输设备之间的互连。

3. Hybrid：端口能发送多个VLAN的报文，端口发出去的报文可根据需要配置某些VLAN的报文带VLAN Tag，某些VLAN的报文不带VLAN Tag。

然后根据接口转发报文时是否需要携带VLAN tag或是否允许转发多个VLAN的报文，使用port link-type命令将错误的接口类型切换为正确的接口类型。切换接口类型应注意：

1. Trunk端口不能直接切换为Hybrid端口，只能先将Trunk端口配置为Access端口，再配置为Hybrid端口。

2. Hybrid端口不能直接切换为Trunk端口，只能先将Hybrid端口配置为Access端口，再配置为Trunk端口。

Q6 在Voice VLAN中出现除语音数据之外的业务数据丢失情况怎么办？

在Voice VLAN中发生除语音数据之外的业务数据丢失情况时，请执行undo voice-vlan security enable命令关闭Voice VLAN的安全模式。在安全模式下，设备将对每一个要进入Voice VLAN传输的报文进行源MAC地址匹配检查，对于不能匹配OUI地址的报文，将其丢弃。

因此建议用户尽量不要在Voice VLAN中同时传输语音和业务数据。如确有此需要，请确认Voice VLAN的安全模式已关闭，否则业务数据会被丢弃。

STP篇

Q1 什么情况下需要配置生成树边缘端口？

与交换机连接的用户侧设备（如服务器等）无需运行生成树协议。若交换机上与这些设备相连的端口使能了生成树协议，当该端口频繁UP/DOWN，或当生成树拓扑变化端口角色需要重新计算时，该端口一段时间后才能进入转发状态。这对一些需要高链路稳定性或低转发延迟的业务是不可接受的。

为了避免上述问题，需要将与用户侧设备连接的端口配置为边缘端口。边缘端口状态变为UP后可以快速进入转发状态，并且不会发送TC报文，也不会对其他运行了生成树协议的网络造成影响。

Q2 在生成树拓扑中，不同的设备可以配置不同的生成树工作模式吗？

H3C设备在运行生成树协议时，设备间的不同生成树工作模式可以互相兼容。其中：

1. MSTP模式可以兼容RSTP模式和STP模式，RSTP模式可以兼容STP模式。

2. 对于Access端口，PVST模式在任意VLAN中都能与其他模式互相兼容；对于Trunk端口或Hybrid端口，PVST模式仅在缺省VLAN中能与其他模式互相兼容。

3. 若设备的对端为友商设备，建议对端设备与H3C设备使用同一种工作模式，以避免因厂商差异而出现不兼容问题。

Q3 开启生成树协议后，可通过哪些方法维持网络拓扑的稳定？

在使能了生成树协议的网络中，可通过下列方法维护生成树的拓扑稳定：

1. **根桥保护**：可参考《交换那些事儿 | 基础维护篇 - 常用STP保护功能》，在此不赘述。

2. **配置边缘端口和BPDU保护**：同上。

3. **配置环路保护**：同上。

4. **配置防TC-BPDU攻击保护功能**：在遭受到TC-BPDU恶意攻击时，设备会频繁刷新MAC地址表和ARP表。此类攻给设备带来了很大负担，随时威胁着网络的稳定性。此时可以通过开启防TC-BPDU攻击保护功能，避免频繁地刷新转发地址表项。该功能的描述如下：

(1) 在系统视图下执行stp tc-protection命令，可以开启防TC-BPDU攻击保护功能。

(2) 在系统视图下执行stp tc-protection threshold *number*命令，可以配置在单位时间（固定为十秒）内，设备收到TC-BPDU后立即刷新转发地址表项的最高次数。

(3) 如果设备在单位时间（固定为十秒）内收到TC-BPDU的次数大于number次，那么该设备在这段时间之内将只进行number次刷新转发地址表项的操作，而对于超出number次的TC-BPDU，设备会在这段时间过后再统一进行一次地址表项刷新的操作。

环路检测篇

Q1 如何选择环路检测时间间隔？

开启环路检测功能后，设备以一定的时间间隔发送环路检测报文来确定是否存在环路，这个时间间隔决定了在Block模式和No-learning模式下，端口恢复正常转发状态的速度：时间间隔越小，端口恢复速度越快，环路检测的灵敏度越高，占用设备的系统资源越多；时间间隔越大，端口恢复速度越慢，环路检测的灵敏度越低，占用设备的系统资源越少。用户需要根据设备实际情况及二层组网防环需求，灵活配置环路检测时间间隔。

同时需要注意的是，环路检测在Shutdown模式下，被关闭端口的恢复不受环路检测时间间隔的影响，而是在shutdown-interval命令配置的端口状态检测定时器超时后，自动恢复为UP状态。

Q2 环路检测和生成树功能可以同时配置吗？

不建议同时配置。因为环路检测和生成树都具有二层防环功能，如果两者同时配置，可能其中一者在另一者计算出环路之前就已经消除了环路，造成环路检测功能不生效或生成树功能不生效等问题。

镜像篇

Q1 希望为本地端口镜像组配置多于一个目的端口，但设备不支持加入第二个目的端口怎么办？

对于本地端口镜像组不支持配置多个目的端口的设备，可以使用远程镜像VLAN实现本地镜像组支持多个目的端口。

该方式利用二层远程端口镜像中镜像报文在远程镜像VLAN中广播发送的原理实现，具体实现方式为：

1. 在本地设备上创建远程源镜像组、远程镜像VLAN和反射端口，并将本设备上连接监测设备的多个端口加入该VLAN。

2. 镜像报文在远程镜像VLAN中广播时即可从这些端口中发送出去，实现将镜像报文发送到多个目的端口。

Q2 配置二层远程端口镜像后，为什么镜像无关的端口有异常的流量增加？

查看这些端口是否在远程镜像VLAN中，将镜像无关的端口从远程镜像VLAN中删除。

Q3 将端口配置为镜像源端口失败，有哪些可能原因？

最常见的原因为端口类型支持情况限制和一个端口允许加入的聚合组数量限制。

请确认该端口是否支持配置为镜像源端口，特别是聚合口、VLAN接口等虚接口。VLAN接口一般不支持作为镜像源端口，需配置VLAN中的物理端口作为镜像源端口。聚合口是否支持作为镜像源端口与设备型号有关，需查询产品配置指导或命令手册。

一个端口可以作为镜像源端口加入的镜像组数目受设备支持情况限制：

1. 部分设备上：一个端口仅支持作为一个镜像组的源端口，将该端口配置为第二个镜像组的源端口时输出类似如下提示信息，表示该端口已经配置为其他镜像组的源端口：

```
[sysname] mirroring-group 2 mirroring-port ten-gigabitethernet 1/0/1 both
Ten-gigabitethernet 1/0/1 is a mirroring port of mirroring group 1.
```

2. 部分设备上：一个端口作为单向源端口最多可以加入四个镜像组，作为双向源端口最多可以加入两个镜像组，或者以一个双向源端口和两个单向源端口的形式加入三个镜像组。

—— end ——

扫码关注我们哦