组合一（EP）

2020年3月14日 15:07

组合一：
理论：MPLS-VPN、双点双向
项目：EP

EP边缘端口---------通常部署在连接终端的接口
特点或优化
1、立刻进入转发状态，跳过两倍转发延时（Discarding-Learning-forwarding）,节省30s
2、不参与STP计算，不受TC影响（TC清空MAC地址表不会清空EP对应的表项），不受P/A影响（P/A同步过程不影响EP）
3、边缘端口的状态迁移不会触发TC（RSTP中非边缘端口进入转发状态才会触发TC）
4、边缘端口收到BPDU会成为普通端口，参与STP计算
应用场景
1、企业网接入层连接终端的接口，不会因为大量TC造成网络不稳定
2、连接关键业务服务器的接口，比如DHCP服务器，立刻进入转发状态
问题
1、如果交换机两个EP互联（或者连接HUB），短暂环路--------通过BPDU-protection解决，收到BPDU将接口shutdown，可以设置自动恢复

在配置了BPDU保护功能后关闭端口的情况下，被关闭的端口默认不会自动恢复，只能由网管先执行shutdown命令再执行undo shutdown命令手动恢复，也可以在接口视图下执行restart命令重启端口。
如果用户希望被关闭的端口可以自动恢复，则可以通过在系统视图下执行error-down auto-recovery cause bpdu-protection interval *interval-value*命令使能端口状态自动恢复为Up的功能并设置端口自动恢复为Up的延时时间，使被关闭的端口经过延时时间后能够自动恢复。

2、如果配置EP，确保连接终端，可以配置BPDU-filter，不收不发BPDU，节省资源，但出现环路无法检测
3、如果配置EP，下游连接交换机关闭STP（关闭STP的交换机不透传BPDU），出现环路无法检测
追问
P/A协商问题
RSTP改进-----BPDU转发机制、收到次级BPDU处理方式、 BPDU老化时间、端口角色、端口状态、 P/A协商、 TC机制变化
其他保护------TC防护、根防护、环路防护

配置后，在stp tc-protection interval指定的时间内，设备只会处理stp tc-protection threshold指定数量的拓扑变化报文，对于其他的报文会延迟处理，所以可能会影响生成树的收敛速度。例如，时间设定为10秒，阈值设定为5，则设备收到拓扑变化报文后，在10秒内只会处理最开始收到的5个拓扑变化报文，对于后面收到的报文则会等10秒超时后再统一处理。

当端口的角色是指定端口时，配置的Root保护功能才生效。
配置了根保护的端口，不可以配置环路保护。

由于Alternate端口是根端口的备份端口，如果交换设备上有Alternate端口，需要在根端口和Alternate端口上同时配置环路保护。
配置了根保护的端口，不可以配置环路保护。

BPDU透传问题？

二层协议透明传输功能一般配置在PE设备连接CE的接口上，使能后接收到来自用户网络的二层协议报文需要上送CPU进行目的MAC地址替换，在运营商网络中二层协议报文不会上送CPU处理，而是直接被转发，穿越运营商网络。
一般情况下，l2protocol-tunnel命令配置在PE设备的用户侧接口上。
l2protocol-tunnel vlan命令用来透传VLAN匹配的报文，l2protocol-tunnel命令用来透传所有的报文。
不能把l2protocol-tunnel vlan命令和l2protocol-tunnel命令在同一个接口下配置相同协议类型，否则会提示配置冲突。
如果需要使用l2protocol-tunnel enable命令，在接口上使能用户自定义协议的透明传输功能，请先使用l2protocol-tunnel user-defined-protocol命令，定义用户的二层透明传输协议的特征信息。
此外，除STP协议报文在全局有默认的group-mac外，在接口下对其他协议报文使能透明传输功能时，全局都必须先配置group-mac，具体请参见l2protocol-tunnel group-mac命令。

使用实例

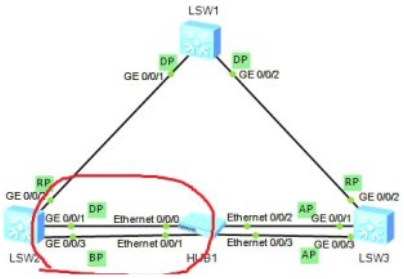
在接口GE0/0/1上使能对STP协议的透明传输功能。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp disable
[HUAWEI-GigabitEthernet0/0/1] l2protocol-tunnel stp enable
```

接口Error-down问题
MSTP、 RSTP、 STP兼容问题
其他二层类似防环技术----smart-link，RRPP（快速环网保护协议），SEP（智能以外网保护），VBST，堆叠等

追问5：为什么STP网络半径推荐值不大于7？
答：最初的生成树协议标准，默认定时2s发送一次配置BPDU，每一个交换机接收和处理报文耗时1s（CPU处理很快，不需要1s），最大支持20跳.
快速生成树协议，默认3个周期老化报文消息，即6s，按照1跳/s最多6跳就超时，也就是半径为7。
二层STP网络半径推荐不大于7，还考虑到网络带宽的利用率、风暴范围以及网络可运维管理。

如图，SW2的DP出故障，BP能不能立即变成DP？-----不能



答：如果DP故障，首先BP等待holdtime = 3*hello，华为还要乘以时间因子，默认为3 ，即为 holdtime=3*hello*时间因子3=18sec，
BP在等待18sec之后，还没有收到最优bpdu，那么端口角色会变为DP，准备收敛为forwarding。
角色变为DP之后，要等待2*forwarding Delay =30sec，收敛成为forwarding状态。
所以，如果在上述环境中，DP故障，BP一共等待48sec收敛为forwarding。

MPLS-VPN

控制层面---------区分重叠私网路由

1、VPN实例的创建，形成VRF

2、RD路由区分符，全局唯一，可以采用XX：YY的表示方式，RD+ipv4形成VPNv4路由

3、RT VPN-target，作为BGP扩展团队属性，可以定义多个值，实现VPNv4路由灵活引入和控制-------讲Hub-sopke模型RT应用

数据转发-----两层标签

1、外层---通过LDP或静态分配，去往目标下一跳的隧道

2、内层--MP-BGP分配，区分不同VPN实例的私网数据报文

追问：

1、 P设备执行路由汇总的问题

2、 PE和CE部署OSPF，其他拓展团体属性（OSPF RT / Domain ID / OSPF router-id ），Sham-link

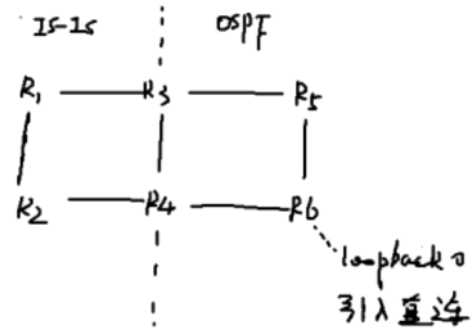
3、双宿主问题

4、 LSP和IGP联动问题

5、三层标签---跨域 Option-C

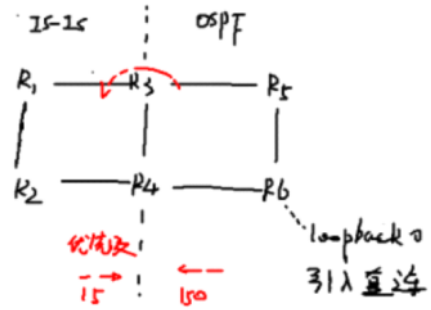
双点双向

3.0 LAB场景是这样的（画菱形拓扑也行）

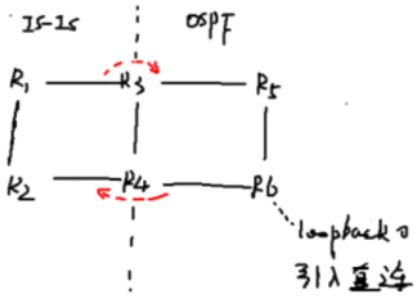


分析：

分析次优问题----------优先级问题



分析环路问题---------考虑域外路由选路问题，可能出现R3-R4之间的路由环路



解决方案：解决次优问题、解决环路问题（配置具有扩展性）

追问：

1、各协议优先级，OSPF为什么设置内部和外部？如何考虑

2、 OSPF和ISIS携带Tag的LSA和TLV

3、 OSPF的FA地址

4、各协议防环