常用STP保护功能

H3C交换机基础维护篇

STP保护功能

咖哥，上次你教的STP Dispute保护功能，我懂了！感谢咖哥！

很好。

STP还有其他保护功能吗？我也想学

边缘端口配合BPDU保护功能

当交换机端口直接与用户终端相连，而没有连接到其他网桥或局域网网段上时，该端口为边缘端口。边缘端口不会产生临时环路，所以可以略过两个Forward Delay时间，直接进入转发状态。由于交换机无法自动判断端口是否直接与终端相连，所以用户需要手工通过命令stp edged-port将与终端连接的端口配置为边缘端口。

由于终端不会发出BPDU，所以当边缘端口收到BPDU时，交换机自动将此端口设置为非边缘端口，重新计算生成树，引起网络拓扑结构的变化。如果有人伪造BPDU向边缘端口发起恶意攻击，就会引起网络震荡。

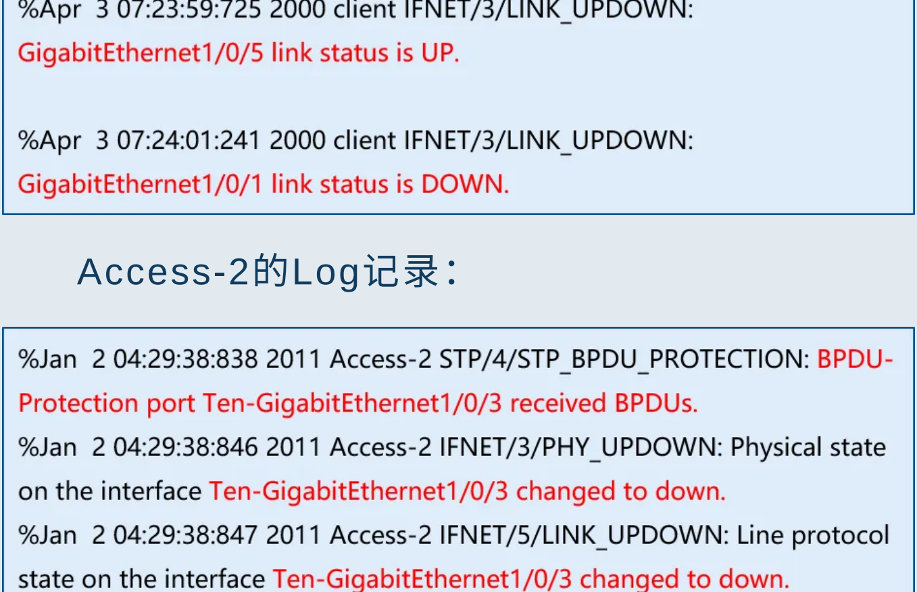
生成树协议提供了BPDU保护功能来防止这种攻击：开启了BPDU保护功能后，如果边缘端口收到了BPDU，交换机将关闭该端口以防止攻击或环路。

下面通过实验来说明BPDU保护功能。

实验过程及分析：

实验拓扑如下图所示，所有设备和接口开启STP，Access-1、Access-2与终端互联接口配置为边缘端口，并开启BPDU保护。实验通过三种不同场景下的环路连接测试BPDU保护情况。

场景一：接入设备单端口下联设备存在环路



观察Access-2和Access-3两台设备上的日志发现，Access-2上STP边缘端口G1/0/3收到BPDU后BPDU保护功能生效，G1/0/3被关闭从而防止了环路。

Access-3的Log记录：

```
%Apr  3 07:23:59:603 2000 client IFNET/3/LINK_UPDOWN:
GigabitEthernet1/0/3 link status is UP.
%Apr  3 07:23:59:725 2000 client IFNET/3/LINK_UPDOWN:
GigabitEthernet1/0/5 link status is UP.

%Apr  3 07:24:01:241 2000 client IFNET/3/LINK_UPDOWN:
GigabitEthernet1/0/1 link status is DOWN.
```

Access-2的Log记录：

```
%Jan  2 04:29:38:838 2011 Access-2 STP/4/STP_BPDU_PROTECTION: BPDU-
Protection port Ten-GigabitEthernet1/0/3 received BPDUs.
%Jan  2 04:29:38:846 2011 Access-2 IFNET/3/PHY_UPDOWN: Physical state
on the interface Ten-GigabitEthernet1/0/3 changed to down.
%Jan  2 04:29:38:847 2011 Access-2 IFNET/5/LINK_UPDOWN: Line protocol
state on the interface Ten-GigabitEthernet1/0/3 changed to down.
```

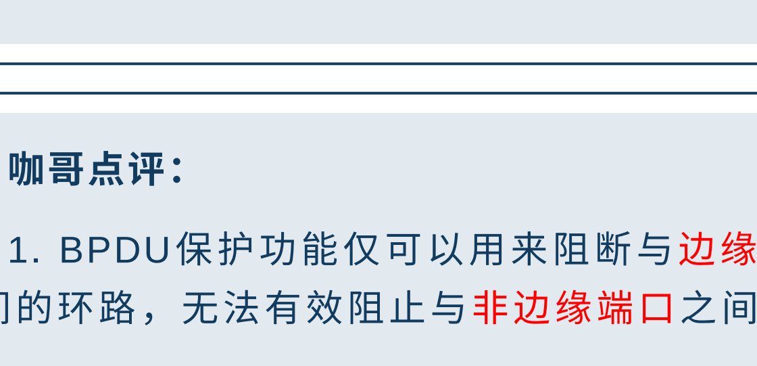
场景二：接入设备自身端口环路

Access-2的G1/0/3和G1/0/17接口互联，形成环路。观察Access-2上的日志发现边缘端口G1/0/3收到BPDU后BPDU保护功能生效，G1/0/3被关闭从而防止了环路。

Access-2的Log记录：

```
%Jan  2 04:31:34:362 2011 Access-2 STP/4/STP_BPDU_PROTECTION: BPDU-
Protection port Ten-GigabitEthernet1/0/3 received BPDUs.
%Jan  2 04:31:34:371 2011 Access-2 IFNET/3/PHY_UPDOWN: Physical state
on the interface Ten-GigabitEthernet1/0/3 changed to down.
%Jan  2 04:31:34:372 2011 Access-2 IFNET/5/LINK_UPDOWN: Line protocol
state on the interface Ten-GigabitEthernet1/0/3 changed to down.
%Jan  2 04:31:34:378 2011 Access-2 IFNET/3/PHY_UPDOWN: Physical state
on the interface Ten-GigabitEthernet1/0/17 changed to down.
%Jan  2 04:31:34:381 2011 Access-2 IFNET/5/LINK_UPDOWN: Line protocol
state on the interface Ten-GigabitEthernet1/0/17 changed to down.
```

场景三：接入设备间环路



Access-1的G1/0/15和Access-2的G1/0/3端口互联，形成环路。观察Access-2的日志发现STP边缘端口G1/0/3收到BPDU后BPDU保护功能生效，G1/0/3被关闭从而防止了环路。

Access-2的Log记录：

```
%Jan  2 04:33:15:950 2011 Access-2 STP/4/STP_BPDU_PROTECTION: BPDU-
Protection port Ten-GigabitEthernet1/0/3 received BPDUs.
%Jan  2 04:33:15:956 2011 Access-2 IFNET/3/PHY_UPDOWN: Physical state
on the interface Ten-GigabitEthernet1/0/3 changed to down.
%Jan  2 04:33:15:956 2011 Access-2 IFNET/5/LINK_UPDOWN: Line protocol
state on the interface Ten-GigabitEthernet1/0/3 changed to down.
```

咖哥点评：

1. BPDU保护功能仅可以用来阻断与边缘端口之间的环路，无法有效阻止与非边缘端口之间的环路。

2. 被阻断的边缘端口默认30S被重新激活，可以通过命令undo shutdown手动恢复，也可以通过命令stp port shutdown permanent配置被BPDU保护功能关闭的边缘端口不再自动恢复。

根保护功能

各位小学徒是否遇到过新上线一台接入设备导致核心网络异常中断？是否听说过将核心设备配置为根桥但并未生效？

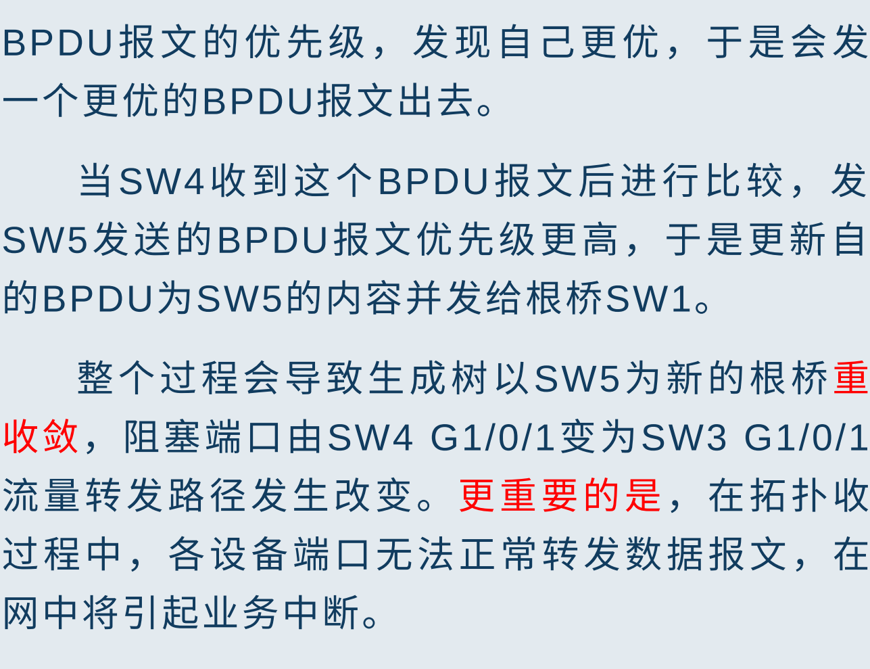
由于错误配置或网络恶意攻击等原因，STP合法根桥有可能会收到优先级更高的BPDU，这样合法根桥会失去根桥的地位，STP拓扑将重新收敛，收敛过程中各设备端口无法正常转发报文，从而引起业务中断。

为了防止这种情况发生，生成树协议提供了根保护功能：对于开启了根保护功能的端口，其端口角色只能为指定端口。一旦该端口收到优先级更高的BPDU，该端口将被置为侦听状态，不再转发报文。当在2倍的Forward Delay时间内没有收到更优的BPDU时，端口恢复原来的正常状态。

下面通过实验来说明根保护功能。

实验过程及分析：

实验拓扑如下图所示，所有设备及端口均开启STP，SW1被选举为根桥，各个端口的STP角色如图所示，其中SW4的G1/0/1处于阻塞状态。



更改SW5的STP优先级为0，模拟高优先级BPDU报文攻击，此时SW5会重新计算生成自己的BPDU报文。SW5比较收到BPDU报文与自身生成BPDU报文的优先级，发现自己更优，于是会发送一个更优的BPDU报文出去。

当SW4收到这个BPDU报文后进行比较，发现SW5发送的BPDU报文优先级更高，于是更新自己的BPDU为SW5的内容并发给根桥SW1。

整个过程会导致生成树以SW5为新的根桥重新收敛，阻塞端口由SW4 G1/0/1变为SW3 G1/0/1，流量转发路径发生改变。更重要的是，在拓扑收敛过程中，各设备端口无法正常转发数据报文，在现网中将引起业务中断。

```
SW5:（变为根桥）
[SW5]stp priority 0
[SW5]dis stp brief
 MST ID   Port                          Role  STP State   Protection
 0        GigabitEthernet1/0/1          DESI  FORWARDING  NONE

SW1:  （被抢根）
[SW1]dis stp brief
 MST ID   Port                          Role  STP State   Protection
 0        GigabitEthernet1/0/1          DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/2          DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/3          ROOT  FORWARDING  NONE

SW2:
[SW2]dis stp brief
 MST ID   Port                          Role  STP State   Protection
 0        GigabitEthernet1/0/1          ROOT  FORWARDING  NONE

SW3:
[SW3]dis stp brief
 MST ID   Port                          Role  STP State   Protection
 0        GigabitEthernet1/0/1          ALTE  DISCARDING  NONE
 0        GigabitEthernet1/0/2          ROOT  FORWARDING  NONE

SW4:
[SW4]dis stp brief
 MST ID   Port                          Role  STP State   Protection
 0        GigabitEthernet1/0/1          DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/3          DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/4          ROOT  FORWARDING  NONE
```

在SW4的G1/0/4配置根保护功能后，当SW4收到SW5发出的更高优先级BPDU报文后，会强制保持G1/0/4为指定端口并设为侦听状态，从而保证SW5发出的高优先级报文不会继续向上传播，维持SW1的根桥地位不变。

此时查看各端口的STP角色和状态，SW4的G1/0/4触发根保护功能被阻塞，从而保证了核心SW1和其他设备的拓扑稳定：

```
[SW4-GigabitEthernet1/0/4]stp root-protection

%Jan 22 02:26:05:597 2021 SW4 STP/4/STP_ROOT_PROTECTION: Instance
0's ROOT-Protection port GigabitEthernet1/0/4 received superior BPDUs.

SW4:
[SW4]dis stp brief
 MST ID   Port                          Role  STP State   Protection
 0        GigabitEthernet1/0/1          ALTE  DISCARDING  NONE
 0        GigabitEthernet1/0/3          ROOT  FORWARDING  NONE
 0        GigabitEthernet1/0/4          DESI  DISCARDING  ROOT （根保护）
```

咖哥点评：

1. 根保护功能的本质是通过阻塞收到高优先级BPDU的指定端口来达到保护根桥的目的。如果一个端口一直收到高优先级BPDU报文，那么这个端口就会一直处于阻塞状态，在没有备份链路的情况下，这个端口下的业务就会受到持续影响。

2. 在现网应用中，建议通过命令指定根桥，设备上线之前检查网络中相关设备的STP配置，避免出现抢根的情况。

环路保护功能

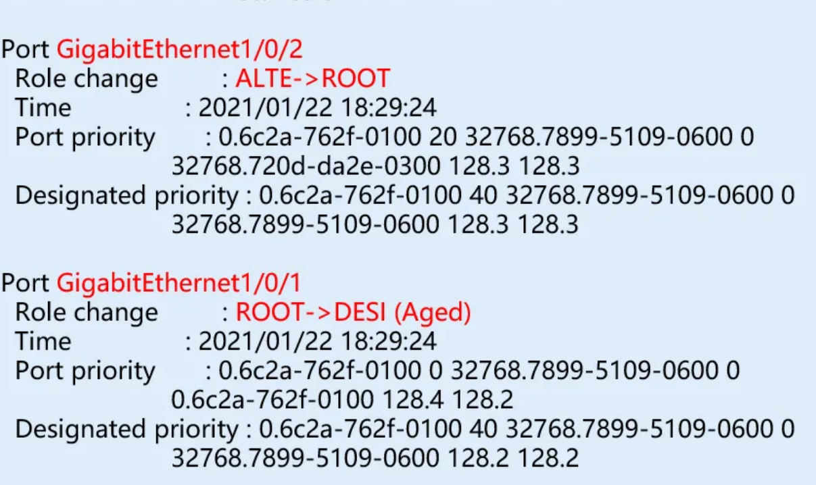
由于链路拥塞或者单向链路故障等问题，下游设备的端口收不到上游设备的BPDU时，会重新选择端口角色。收不到BPDU的下游设备端口会转变为指定端口，阻塞端口会迁移到转发状态，从而产生环路。

环路保护功能会抑制这种环路的产生：在开启了环路保护功能的端口上，其初始状态为阻塞状态，如果该端口收到了BPDU，则进行正常的状态迁移；否则，该端口将一直处于阻塞状态以避免环路的产生。

下面通过实验来说明环路保护功能。

实验过程及分析：

实验拓扑如下图所示，所有设备及端口均开启STP，SW1被选举为根桥，各个端口的STP角色如图所示，其中SW4的G1/0/2处于阻塞状态。



关闭根桥SW1 G1/0/3的STP功能来模拟SW1和SW4之间BPDU报文单通的情况。此时SW4 G1/0/1由于收不到根桥的BPDU报文，从根端口变成指定端口并处于转发状态，G1/0/2变为了根端口也处于转发状态，整个拓扑每个端口都处于转发状态，产生环路。

SW4上产生如下STP历史记录：

```
[SW4]dis stp history
 -------------- STP slot 1 history trace --------------
 ------------------  Instance 0  ---------------------

 Port GigabitEthernet1/0/2
   Role change        : ALTE->ROOT
   Time              : 2021/01/22 18:29:24
   Port priority       : 0.6c2a-762f-0100 20 32768.7899-5109-0600 0
                       32768.720d-da2e-0300 128.3 128.3
   Designated priority : 0.6c2a-762f-0100 40 32768.7899-5109-0600 0
                       32768.7899-5109-0600 128.3 128.3

 Port GigabitEthernet1/0/1
   Role change        : ROOT->DESI (Aged)
   Time              : 2021/01/22 18:29:24
   Port priority       : 0.6c2a-762f-0100 0 32768.7899-5109-0600 0
                       0.6c2a-762f-0100 128.4 128.2
   Designated priority : 0.6c2a-762f-0100 40 32768.7899-5109-0600 0
                       32768.7899-5109-0600 128.2 128.2

[SW4]dis stp brief
 MST ID   Port                          Role  STP State   Protection
 0        GigabitEthernet1/0/1          DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/2          ROOT  FORWARDING  NONE
```

在SW4 G1/0/1开启环路保护功能后，继续模拟BPDU报文单通的情况。此时查看SW4的端口状态发现G1/0/1变成了指定端口并被置于阻塞状态，防止了环路的产生。

```
[SW4-GigabitEthernet1/0/1]stp loop-protection

%Jan 22 03:06:09:382 2021 SW4 STP/4/STP_LOOP_PROTECTION: Instance
0's LOOP-Protection port GigabitEthernet1/0/1 failed to receive
configuration BPDUs.

SW4:
[SW4]dis stp brief
 MST ID   Port                          Role  STP State   Protection
 0        GigabitEthernet1/0/1          DESI  DISCARDING  LOOP （触发环路保护）
 0        GigabitEthernet1/0/2          ROOT  FORWARDING  NONE
```

咖哥点评：

1. 不能在与用户终端相连的端口上开启环路保护功能，否则该端口会因收不到BPDU而一直处于阻塞状态。

2. 同一个端口上不能同时配置边缘端口和环路保护功能，或同时配置根保护功能和环路保护功能。

3. 在已经发生环路的情况下，再配置环路保护功能是没有效果的。

STP保护功能小节

1. 边缘端口开启了BPDU保护功能后，如果收到了BPDU，该端口将被关闭。

2. 端口开启了根保护功能后，如果收到了优先级更高的BPDU，该端口将被置为阻塞状态。

3. 端口开启了环路保护功能后，如果未收到BPDU，该端口将被置为阻塞状态。

—— end ——