HCIP-Datacom 分解实验 - RSTP

臧家林制作

RSTP 实验 1：STP 基础配置
RSTP 实验 2：RSTP 基础配置
RSTP 实验 3：RSTP 选举
RSTP 实验 4：RSTP 保护

==========

RSTP 实验 1：STP 基础配置

STP 是用来避免数据链路层出现逻辑环路的协议，使用 BPDU 传递网络信息计算出一根无环的树状网络结构，并阻塞特定端口。在网络出现故障时，STP 能快速发现链路故障，并尽快找出另外一条路径进行数据传输。

交换机上运行的 STP 通过 BPDU 信息的交互，选举根交换机，然后每台非根交换机选择用来与根交换机通信的根端口，之后每个网段选择用来转发数据至根交换机的指定端口，最后剩余端口则被阻塞。
每个网络只有一个根桥
每个非根桥都要选出一个根端口
每个 Segment 只有一个指定端口

非指定端口将被堵塞

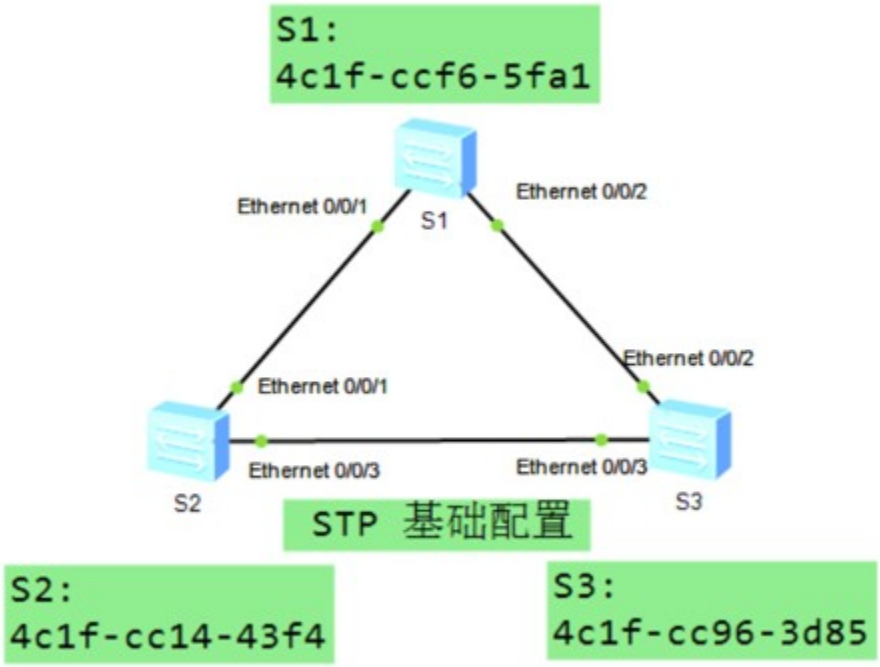
根端口选举：依据该端口的根路径开销、对端 BID（Bridge ID）、对端 PID（Port ID）和本端 PID。
指定端口选举：依据该端口的根路径开销、BID、PID

根交换机（Root）
在同一个三层网络中需要选举，即一个广播域内要选举，并且一个网络中只能选举一台根交换机。Birdge-ID 中优先级最高（即数字最小）的为根交换机，优先级范围为 0-65535，如果优先级相同，则 MAC 地址越小的为根交换机。

根端口（Root Port）
所有非根交换机都要选举，非根交换机上选举的根端口就是普通交换机去往根交换机的唯一链路，选举规则为 到根交换机的 Path Cost 值最小的链路，如果多条链路到达根交换机的 Path Cost 值相同，则选举上一跳交换机 Bridge-ID 最小的链路，如果是经过的同一台交换机，则上一跳交换机 Bridge-ID 也是相同的，再选举对端端口优先级最小的链路，如果到达对端的多个端口优先级相同，最后选举交换机对端端口号码最小的链路。

指定端口(Designated Port)
在每个二层网段都要选举，也就是在每个冲突域需要选举，简单地理解为每条连接交换机的物理线路的两个端口中，有一个要被选举为指定端口，每个网段选举指定端口后，就能保证每个网段都有链路能够到达根交换机，选举规则和选举根端口一样，即：到根交换机的 Path Cost 值最小的链路，如果多条链路到达根交换机的 Path Cost 值相同，则选举上一跳交换机 Bridge-ID 最小的链路，如果是经过的同一台交换机，则上一跳

交换机 Bridge-ID 也是相同的，再选举对端端口优先级最小的链路，如果到达对端的多个端口优先级相同，最后选举交换机对端端口号码最小的链路。



现在网络中的根桥为 SW2
修改为 stp 模式，修改优先级，让 SW1 成为网络中的根桥
SW1:
stp mode stp
stp priority 4096

SW2:
stp mode stp

SW3:
stp mode stp

==========

RSTP 实验 2：RSTP 基础配置

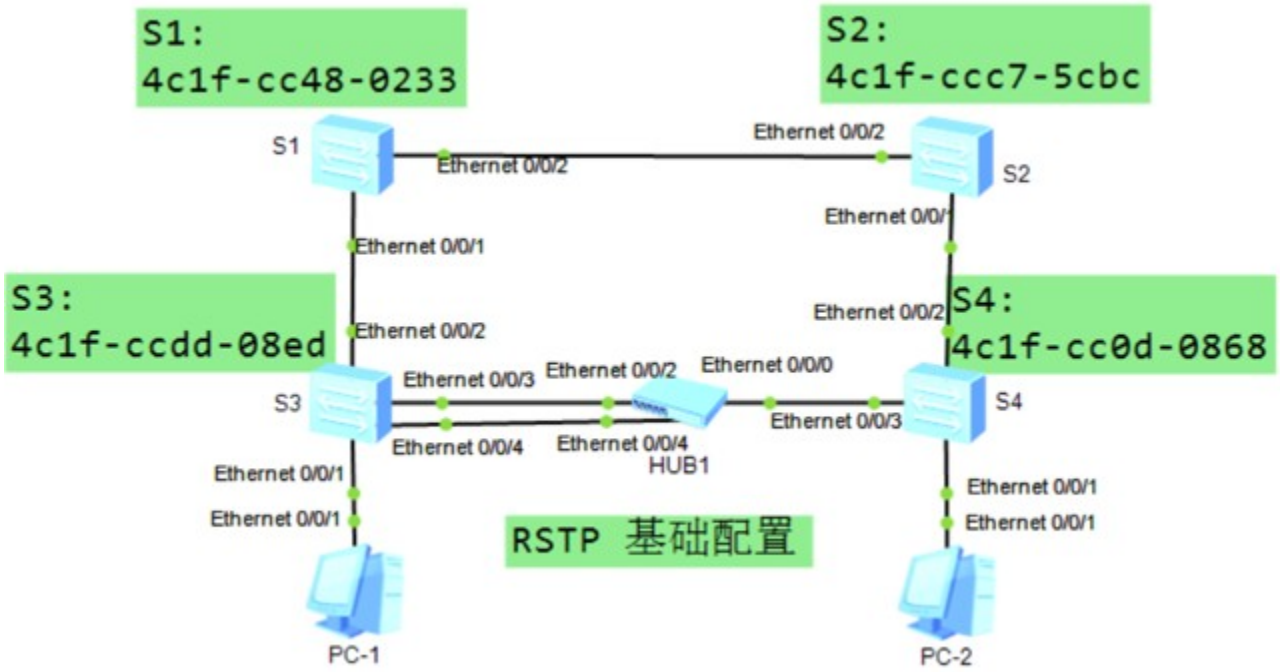
IEEE 于 2001 发布了 802.1 w 标准定义了 RSTP（Rapid Spanning-Tree Protocol 快速生成树协议），该协议基于 STP 协议，对原有的 STP 协议进行了更加细致的修改和补充。

STP 协议虽然能够解决环路问题，但是也存在一些不足。比如 STP 没有细致区分端口状态和端口角色，其次，STP 端口状态共有 5 种，即 discarding ,blocking,listening,learning 和 forwarding ，收敛较慢。而且，对于用户来说 blocking, listening 和 learning 状态并没有区别，都不转发流量 。根据 STP 的不足， RSTP 做出了改进。
RSTP 新增加了 2 种端口角色，其端口角色共有 4 种，根端口，指定端口，Alternate 端口 Backup 端口。
RSTP 把原来的 5 种状态缩减为 3 种。根据端口是否转发用户流量和学习 MAC 地址来划分，如果不转发用户流量也不学习 MAC 地址，那么端口状态就是 discarding 状态，如果不转发用户流量但是学习 MAC 地址，那么端口状态就是 learning 状态，如果既转发用户流量又学习 MAC 地址，那么端口状态就是 forwarding 状态。

RSTP 的快速收敛机制可以分为以下 3 种：
Proposal/Agreement 机制：
当一个端口被选举成为指定端口之后，在 STP 中，该端口至少要等一个 forward delay(learning) 时间才会迁移到 forwarding 状态。而在 RSTP 中，此端口会先进入 discarding 状态，再通过 Proposal/Agreement 机制，简称 P/A 机制，快速进入 forwarding 状态。这种机制必须在点到点的全双工链路上使用
根端口快速切换机制：
如果网络中一个根端口失效，那么网络中最优的 Alternate 端口将成为根端口，进入 forwarding 状态。因为通过这个 Alternate 端口连接的网段上必然有个指定端口可以通往根桥。

边缘端口的引入：

在 RSTP 里面，如果某一个指定端口位于整个网络的边缘，即不再与其他交换设备连接，而是直接与终端设备直连，这种端口叫做边缘端口。边缘端口不接收处理配置 BPDU，不参与 RSTP 运算，可以由 disable 直接转到 forwarding 状态，且不经历进延，就像在端口上将 STP 禁用。但是一旦边缘端口收到配置 BPDU，就失去了边缘端口属性，成为普通 STP 端口，并重新进行生成树计算，从而引起网络震荡。



运行 RSTP

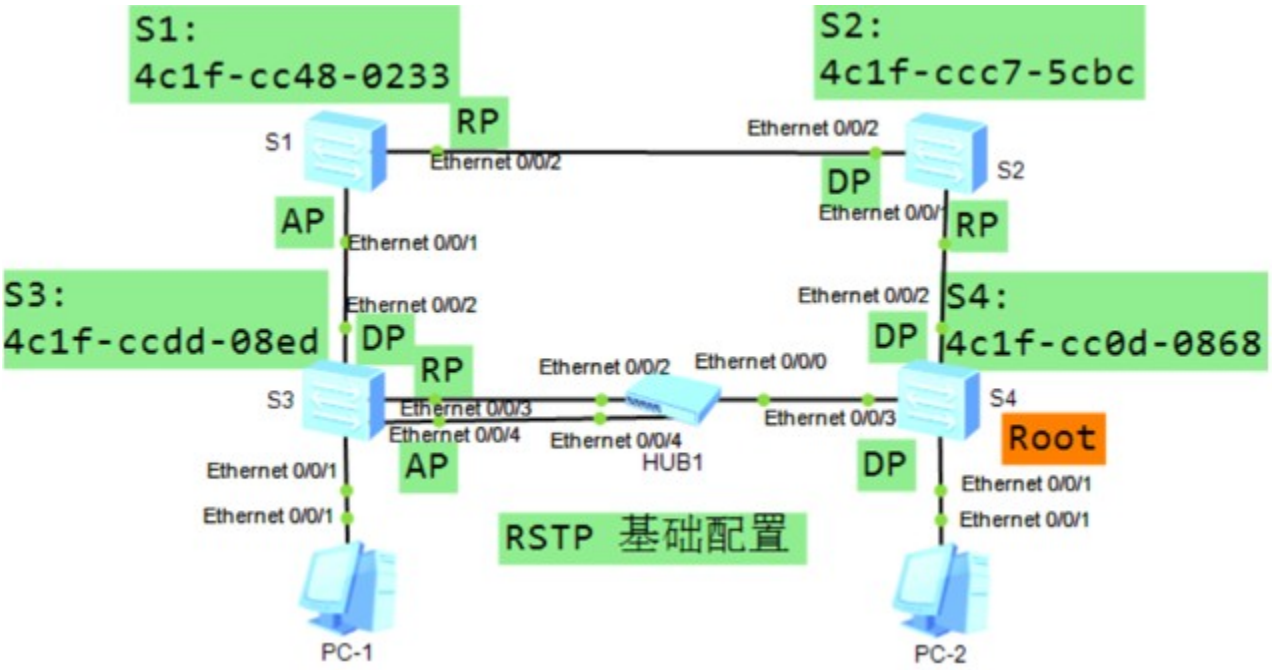
S1: stp mode rstp

S2: stp mode rstp

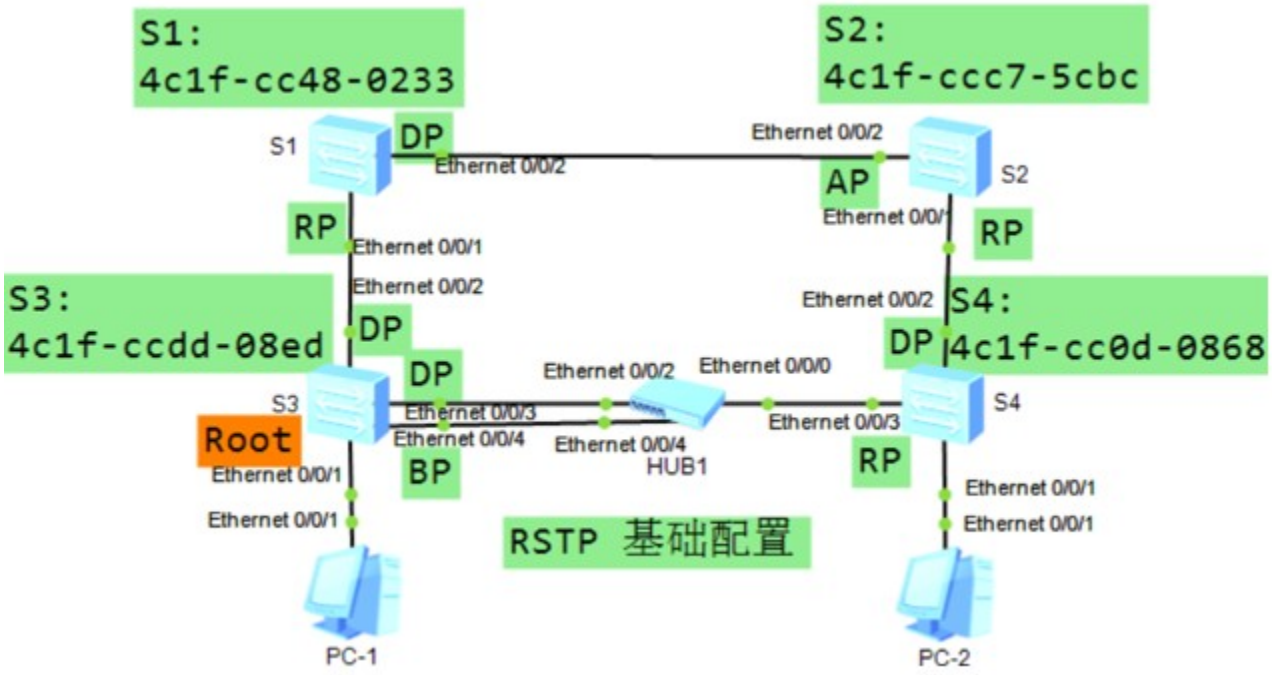
S3: stp mode rstp

S4: stp mode rstp

根桥为 S4 ，确定各个端口角色



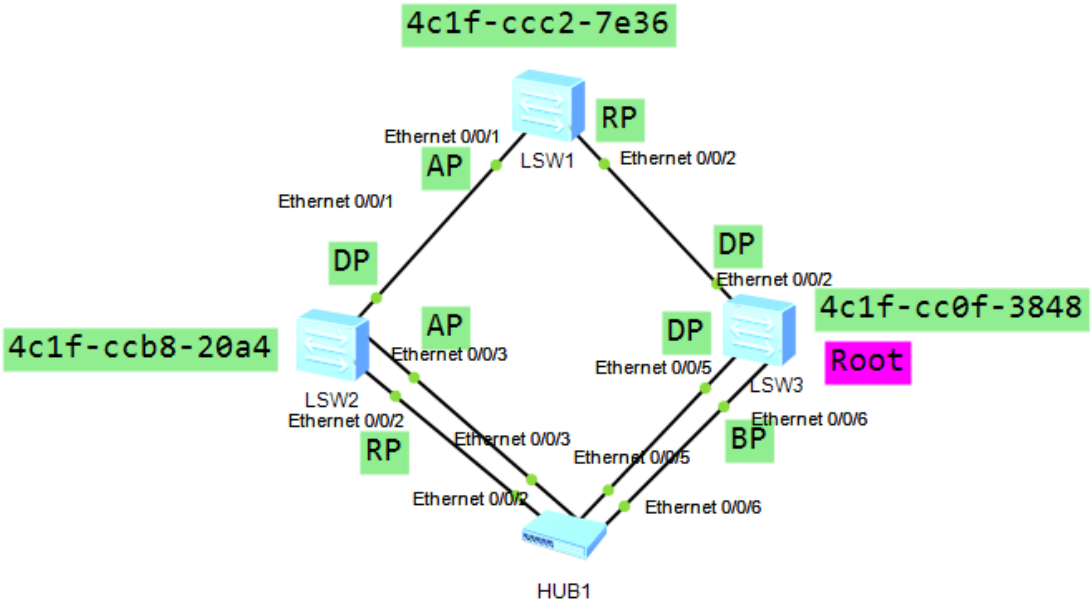
修改优先级，让 S3 做为根桥，再次确定各个端口角色



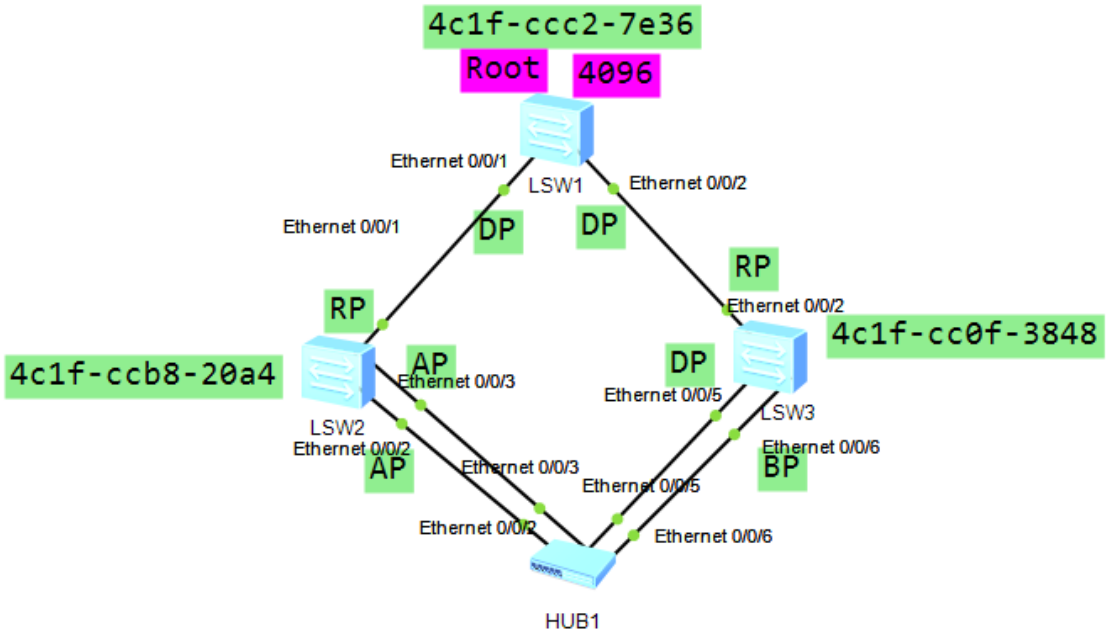
=========

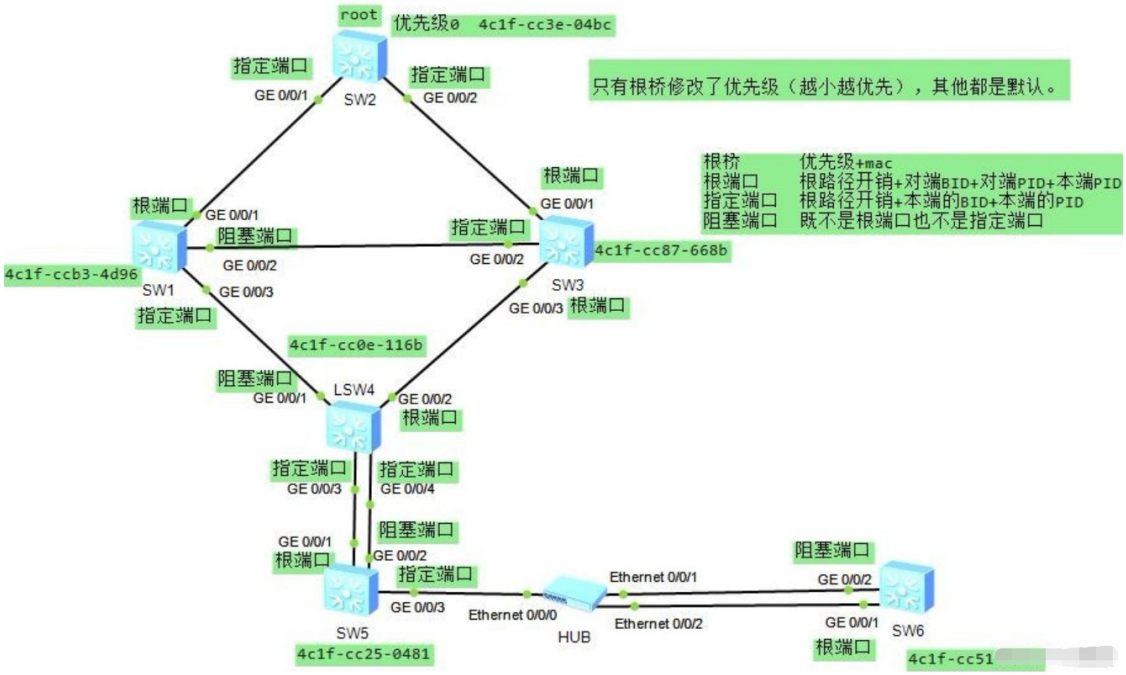
RSTP 实验 3：RSTP 选举

RSTP 生成树的选举，有 HUB 的情况



改变 Root 的位置





==========

RSTP 实验 4：RSTP 保护

在 RSTP 或 MSTP 交换网络中，为了防止恶意或临时环路的产生，可配置保护功能来增强网络的健壮性和安全性。

- BPDU 保护
- 根保护
- 环路保护
- 防止 TC-BPDU 攻击

BPDU 保护（有边缘端口的交接机，全局配置）

在交换设备上，通常将直接与用户终端或文件服务器等非交换设备相连的端口配置为边缘端口，边缘端口一般不会收到 BPDU。如果有人伪造 BPDU 恶意攻击交换机，边缘端口接收到 BPDU 后，交换机会自动将边缘端口设置为非边缘端口，并重新进行生成树计算，从而引起网络震荡。交换机上启动了 BPDU 保护 功能后，如果边缘端口收到了 BPDU，那么边缘端口将被关闭，但是边缘端口属性不变，同时通知网管系统。被关

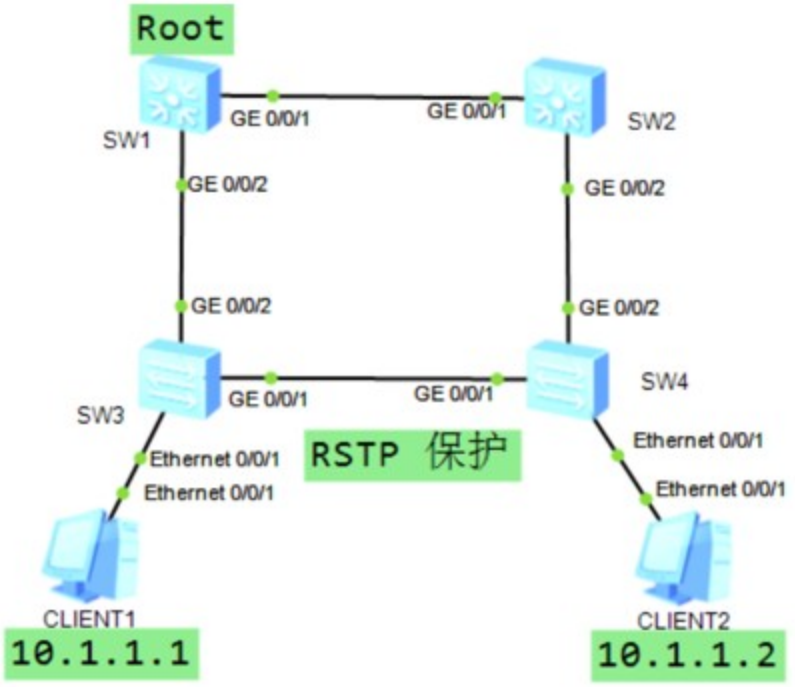
闭的边缘端口只能由网络管理员手动恢复，如果需要被关闭的边缘端口自动恢复，可以配置端口自动恢复功能，并设置延迟时间。

根保护（交接机的 DP 端口，接口配置-DP）
由于维护人员的错误配置或网络中的恶意攻击，网络中的合法根交换机有可能会收到优先级更高的 BPDU，使得合法根交换机失去根交换机的地位，从而引起网络拓扑结构的错误变动。这种不合法的拓扑变化，可能会导致原来应该通过高速链路的流量被牵引到低速链路上，造成网络拥塞。对于启用了根保护功能的端口，其端口角色不能成为根端口，一旦启用根保护功能的指定端口收到了优先级更高的 BPDU 时，端口将进入 Discarding 状态，不再转发报文。在经过一段时间（通常为 2 倍的 Forward Delya， 30s）后，如果端口一直没有再收到优先级更高的 BPDU，端口会自动恢复到正常的 Forwarding 状态。

环路保护（有阻塞端口的交接机，接口配置-RP 或 AP）
在运行 RSTP 或 MSTP 的协议网络中，根端口和其他阻塞端口的状态是依靠上游交换机发来的 BPDU 进行维持的。当由于链路拥塞或者单向链路故障导致这些端口收不到来自上游交换机的 BPDU 时，交换机就会重新选择根端口。原先的根端口会转变为指定端口，而原先的阻塞端口会迁移到转发状态，从而造成交换机中可能产生环路。在启动了环路保护功能后，如果根端口或 Alternate 端口长时间收不到来自上游的 BPDU，则会向网络管理员发送通知信息，如果是根端口则进入 Discarding 状态，阻塞端口则会一直保持在阻塞状态，不转发报文，从而不会在网络中形成环路。直到根端口或 Alternate 端口收到 BPDU 后，端口状态才恢复到 Forwarding 状态。

防止 TC-BPDU 攻击（所有交接机，全局配置）

交换机在接收到 TC BPDU 后，会执行 MAC 地址表项和 ARP 表项的删除操作。如果有人伪造了 TC BPDU 报文恶意攻击交换机，交换机在短时间内会收到很多 TC BPDU 报文，频繁的删除操作会给设备造成很大的负担，给网络的稳定性带来很大隐患。启用防 TC BPDU 报文攻击功能后，可以配置交换机在单位时间内处理 TC BPDU 报文的次数。如果在单位时间内，交换机收到的 TC BPDU 报文数量大于配置的阈值，交换机只会处理阈值指定的次数。对于其他超出阈值的 TC BPDU 报文，定时器到期后设备只对其统一处理一次。这样可以避免频繁地删除 MAC 地址表项和 ARP 表项，从而达到保护设备的目的。



SW1 为主根交换机，SW2 为备份交换机

SW1:
undo ter mo
sy

sys SW1
stp mode rstp
stp priority 4096

SW2:
undo ter mo
sy
sys SW2
stp mode rstp
stp priority 8192

SW3:
undo ter mo
sy
sys SW3
stp mode rstp

SW4:
undo ter mo
sy
sys SW4
stp mode rstp

使用<SW1>display stp brief，查看交换机的端口状态
可以看到 S1 为根交换机，SW1 的接口为 DP ,S4 的 g0/0/1 端口状态为 Discarding

```
[SW1]dis stp brief
 MSTID    Port
Role    STP State          Protection
```

```
      0         GigabitEthernet0/0/1
DESI    FORWARDING              NONE
         0               GigabitEthernet0/0/2
DESI    FORWARDING              NONE

[SW4]dis stp bri
 MSTID    Port
Role    STP State           Protection
      0         Ethernet0/0/1
DESI    FORWARDING              NONE
      0         GigabitEthernet0/0/1
ALTE    DISCARDING              NONE
      0         GigabitEthernet0/0/2
ROOT    FORWARDING              NONE
```

配置 S3 S4 的 e0/0/1 端口为边缘端口

SW3:
int e0/0/1
stp edged-port enable

SW4:
int e0/0/1
stp edged-port enable

两台 PC 相互 ping 一下，是可以通的

= = = = = = = =

配置 BPDU 保护

为防止边缘端口收到不合法的 BPDU 后网络重新收敛，在 SW3 SW4 上配置 BPDU 保护功能。
在系统视图下使用命令 stp bpdu-protection 启用交换机边缘端口的 BPDU 保护功能。默认，交换机的 BPDU 保护功能处于禁用状态

```
[SW3]dis stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge                  :32768.4c1f-
cc0b-6f81
Config Times                 :Hello 2s
MaxAge 20s FwDly 15s MaxHop 20
Active Times                 :Hello 2s
MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC             :4096 .4c1f-cc13-
66cd / 20000
CIST RegRoot/IRPC       :32768.4c1f-cc0b-
6f81 / 0
CIST RootPortId           :128.24
BPDU-Protection           :Disabled
TC or TCN received    :22
```

SW3:
stp bpdu-protection
SW4:
stp bpdu-protection

配置之后，就是 Enable 状态

为了演示边缘端口收到 BPDU 的效果，把 SW3 的 g0/0/2 端口配置为边缘端口
SW3:
int g0/0/2
stp edged-port enable

Jun 11 2020 14:48:36-08:00 SW3 %%01MSTP/4/BPDU_PROTECTION(l)[0]:This edged-port GigabitEthernet0/0/2 that enabled BPDU-Protection will be shutdown, because it received BPDU packet!

g0/0/2 端口收到交换机的 BPDU 后被关闭，并弹出日志提示

设置自动恢复为 up 延时为 30 s。当端口被关闭后，删掉 g0/0/2 端口的边缘端口配置，30 s 后端口会自动 up 并弹出日志提示
SW3:
int g0/0/2
undo stp edged-port
undo shut
q
error-down auto-recovery cause bpdu-protection interval 30

如果 SW3 上还是边缘端口，
int g0/0/2
stp edged-port

端口一直处于 up 和 down 的状态切换。撤消端口下的边缘端

口配置
int g0/0/2
undo stp edged-port

Jun 11202014:51:4708:00SW3ERRDOWN/4/ErrordownRecover:OID1.3.6.1.4.1.2011.5.25.257.2.2 Error-down recovered. (Ifindex=29,Ifname=GigabitEthernet0/0/2, Cause=bpdu-protection, RecoverType=auto recovery)
Jun 11 2020 14:51:49-08:00 SW3 %%01PHY/1/PHY(l)[9]: GigabitEthernet0/0/2: change status to up
Jun 11202014:51:4908:00SW3ERRDOWN/4/ErrordownOccur:OID1.3.6.1.4.1.2011.5.25.257.2.1 Error-down occured. (Ifindex=29, Ifname=GigabitEthernet0/0/2, Cause=bpdu-protection)
Jun 11 2020 14:51:49-08:00 SW3 %%01MSTP/4/BPDU_PROTECTION(l)[10]:This edged-portGigabitEthernet0/0/2 that enabled BPDU-Protection will be shutdown, because it received BPDU packet!

= = = = = = = =

配置根保护

根保护是指定端口上的特性。当端口角色是指定端口时，配置

根保护功能才能生效。若在其他类型的端口上配置根保护功能，根保护功能不会生效。

```
<SW1>dis stp brief
 MSTID    Port
Role    STP State           Protection
      0        GigabitEthernet0/0/1
DESI    FORWARDING             NONE
      0        GigabitEthernet0/0/2
DESI    FORWARDING             NONE
<SW1>

<SW2>dis stp bri
 MSTID    Port
Role    STP State           Protection
      0        GigabitEthernet0/0/1
ROOT    FORWARDING             NONE
        0              GigabitEthernet0/0/2
DESI    FORWARDING             NONE


[SW3]dis stp brief
 MSTID    Port
Role  STP State           Protection
      0        Ethernet0/0/1
DESI    FORWARDING             BPDU
      0        GigabitEthernet0/0/1
DESI    FORWARDING             NONE
      0        GigabitEthernet0/0/2
ROOT    FORWARDING             NONE
```

```
[SW3]


[SW4]dis stp bri
 MSTID    Port
Role    STP State           Protection
      0         Ethernet0/0/1
DESI    FORWARDING             BPDU
      0         GigabitEthernet0/0/1
ALTE    DISCARDING             NONE
        0               GigabitEthernet0/0/2
ROOT    FORWARDING             NONE
```

==========

在指定端口上配置根保护

SW1:
int g0/0/1
stp root-protection
int g0/0/2
stp root-protection

SW2:
int g0/0/2
stp root-protection

SW3:
int g0/0/1
stp root-protection

修改 S4 的优先级优于 S1
SW4:
stp priority 0
交换机的优先级的值越小，优先级越大，成为根交换机的可能性也就越大。

在 S4 上查看根交换机的信息，可以看到 S4 已经认为自己是根桥

```
[SW4]dis stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge                  :0
  .4c1f-cc49-36ba
Config Times                 :Hello 2s
MaxAge 20s FwDly 15s MaxHop 20
Active Times                 :Hello 2s
MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC               :0        .4c1f-
cc49-36ba / 0
CIST  RegRoot/IRPC           :0          .4c1f-
cc49-36ba / 0
```

但在 SW2 SW3 上却不是，还是 SW1 为根桥

```
[SW2]dis stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge                  :8192 .4c1f-
cc7d-4eb5
Config Times                 :Hello 2s
```

```
MaxAge 20s FwDly 15s MaxHop 20
Active Times                  :Hello 2s
MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC              :4096 .4c1f-cc13-
66cd / 20000
CIST  RegRoot/IRPC          :8192  .4c1f-cc7d-
4eb5 / 0
```

查看端口状态信息<SW2>display stp brief

```
[SW2]dis stp bri
 MSTID    Port
Role    STP State           Protection
      0        GigabitEthernet0/0/1
ROOT    FORWARDING              NONE
         0               GigabitEthernet0/0/2
DESI    DISCARDING              ROOT
```

可以看到，与 SW4 相连的指定端口变成了 Discarding

删除 SW4 上的优先级配置
SW4:
undo stp priority

= = = = = = = =

配置环路保护

如果由于链路拥塞或者单向链路故障导致根端口收不到来自上游设备的 BPDU，交换机会重新选择根端口。原先的根端口会转变为指定端口，而原先的阻塞端口会迁移到转发状态，从而造成交换网络中环路的产生。

在 SW2 的 g0/0/2 端口下配置
SW2:
int g0/0/2
stp bpdu-filter enable

这样一来，SW4 由于收不到来自上游的 BPDU，就重新选择根端口，观察所有交换机的端口信息

```
<SW1>dis stp bri
 MSTID    Port
Role    STP State           Protection
      0        GigabitEthernet0/0/1
DESI    FORWARDING             NONE
      0        GigabitEthernet0/0/2
DESI    FORWARDING             NONE


<SW2>dis stp bri
 MSTID    Port
Role    STP State           Protection
      0        GigabitEthernet0/0/1
ROOT    FORWARDING             NONE
      0        GigabitEthernet0/0/2
DESI    FORWARDING             ROOT


<SW3>dis stp brief
 MSTID    Port
Role    STP State           Protection
     0        Ethernet0/0/1
DESI    FORWARDING             BPDU
```

```
      0         GigabitEthernet0/0/1
DESI    FORWARDING              ROOT
        0               GigabitEthernet0/0/2
ROOT    FORWARDING              NONE


<SW4>dis stp brief
 MSTID    Port
Role    STP State           Protection
      0         Ethernet0/0/1
DESI    FORWARDING              BPDU
      0         GigabitEthernet0/0/1
ROOT    FORWARDING              NONE
        0               GigabitEthernet0/0/2
DESI    FORWARDING              NONE
```

可以看到所有交换机端口都进入了转发状态

PC1 PC2 相互间 ping 不通，这是因为网络中已经产生了环路

```
PC>ping 192.168.1.2

Ping 192.168.1.2: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!
```

恢复 SW2 的 g0/0/2 端口，在 SW4 的 g0/0/1 和 g0/0/2 端口配置环路防护功能

SW2:

int g0/0/2

undo stp bpdu-filter

SW4:
int g0/0/1
stp loop-protection
int g0/0/2
stp loop-protection

```
[SW4]dis stp brief
 MSTID    Port
Role    STP State           Protection
      0        Ethernet0/0/1
DESI    FORWARDING             BPDU
      0        GigabitEthernet0/0/1
ALTE    DISCARDING             LOOP
        0              GigabitEthernet0/0/2
ROOT    FORWARDING             LOOP
```

在 SW2 上配置 BPDU 过滤
SW2:
int g0/0/2
stp bpdu-filter enable

在 SW4 上查看 STP 的状态信息

```
[SW4]dis stp brief
 MSTID    Port
Role    STP State           Protection
      0        Ethernet0/0/1
DESI    FORWARDING             BPDU
      0        GigabitEthernet0/0/1
ROOT    FORWARDING             LOOP
```

```
0                 GigabitEthernet0/0/2
DESI    DISCARDING                LOOP
```

可以看到 SW4 的 g0/0/1 端口成为了根端口，g0/0/2 端口虽然成为了指定端口，但是处于 Discarding 状态，不转发数据，这样就避免了环路。

没有了环路，两台 PC 之间是可以 ping 通的

```
PC>ping 10.1.1.2

Ping 10.1.1.2: 32 data bytes, Press Ctrl_C to break
From 10.1.1.2: bytes=32 seq=1 ttl=128 time=78 ms
From 10.1.1.2: bytes=32 seq=2 ttl=128 time=62 ms
From 10.1.1.2: bytes=32 seq=3 ttl=128 time=78 ms
From 10.1.1.2: bytes=32 seq=4 ttl=128 time=62 ms
From 10.1.1.2: bytes=32 seq=5 ttl=128 time=62 ms
```

= = = = = = = = =

配置 TC-BPDU 保护

启用了 TC-BPDU 保护功能后，可以配置交换机处理 TC 类型 BPDU 报文的最大速度，以避免频繁地删除 MAC 地址表项和 ARP 表项，从而达到保护交换机的目的。默认情况交换机的 TC 保护功能是处于关闭状态。

stp tc-protection interval 10
stp tc-protection threshold 5
配置的含义是：交换机在 10s 间隔内，默认是 hello 时间的 2 s , 处理 TC 报文的数量为 5, 默认为 1

SW1:
stp tc-protection
stp tc-protection threshold 5

SW2:
stp tc-protection
stp tc-protection threshold 5

SW3:
stp tc-protection
stp tc-protection threshold 5

SW4:
stp tc-protection
stp tc-protection threshold 5