

## 第 14 章 STP

为了减少网络的故障时间，我们经常会采用冗余拓扑。STP 可以让具有冗余结构的网络在故障时自动调整网络的数据转发路径。STP 重新收敛时间较长，通常需要 30—50 秒，为了减少这个时间，引入了一些补充技术，例如 uplinkfast、backbonefast 等。RSTP 则在协议上对 STP 作了根本的改进形成新的协议，从而减少收敛时间。STP 还有许多改进，例如 PVST、MST 协议，以及安全措施，本章将介绍这些常用的配置。

### 14.1 STP 简介

#### 14.1.1 基本 STP

为了增加局域网的冗余性，我们常常会在网络中引入冗余链路，然而这样却会引起交换环路。交换环路会带来三个问题：广播风暴、同一帧的多个拷贝、交换机 CAM 表不稳定。STP(STP, Spanning Tree Protocol)可以解决这些问题，STP 基本思路是阻断一些交换机接口，构建一棵没有环路的转发树。STP 利用 BPDU(Bridge Protocol Data Unit)和其他交换机进行通信，从而确定哪个交换机该阻断哪个接口。在 BPDU 中有几个关键的字段，例如：根桥 ID、路径代价、端口 ID 等。

为了在网络中形成一个没有环路的拓扑，网络中的交换机要进行以下三个步骤：(1) 选举根桥、(2) 选取根口、(3) 选取指定口。这些步骤中，哪个交换机能获胜将取决于以下因素（按顺序进行）：

- (1) 最低的根桥 ID；
- (2) 最低的根路径代价；
- (3) 最低发送者桥 ID；
- (4) 最低发送者端口 ID。

每个交换机都具有一个唯一的桥 ID，这个 ID 由两部分组成：网桥优先级+MAC 地址。网桥优先级是一个 2 个字节的数，交换机的默认优先级为 32768；MAC 地址就是交换机的 MAC 地址。具有最低桥 ID 的交换机就是根桥。根桥上的接口都是指定口，会转发数据包。

选举了根桥后，其他的交换机就成为非根桥了。每台非根桥要选举一条到根桥的根路径。STP 使用路径 Cost 来决定到达根桥的最佳路径（Cost 是累加的，带宽大的链路 Cost 低），最低 Cost 值的路径就是根路径，该接口就是根口；如果 Cost 一样，就根据选举顺序选举根口。根口是转发数据包的。

交换机的其他接口还要决定是否是指定口还是阻断口，交换机之间将进一步根据上面的四个因素来竞争。指定口是转发数据帧的。剩下的其它的接口将被阻断，不转发数据包。这样网络就构建出一棵没有环路的转发树。

当网络的拓扑发生变化时，网络会从一个状态向另一个状态过渡，重新打开或阻断某些接口。交换机的端口要经过几种状态：禁用 (Disable)、阻塞 (Blocking)、监听状态 (Listening)、学习状态 (Learning)、最后是转发状态 (Forwarding)。

#### 14.1.2 PVST

当网络上有多个 VLAN 时，PVST(Per Vlan STP)会为每个 VLAN 构建一棵 STP 树。这样的好处是可以独立地为每个 VLAN 控制哪些接口要转发数据，从而实现负载平衡。缺点是如果 VLAN 数量很多，会给交换机带来沉重的负担。Cisco 交换机默认的模式就是 PVST。

## 14.1.3 portfast、uplinkfast、backbonefast

STP 的收敛时间通常需要 30—50 秒。为了减少收敛时间，有一些改善措施。Portfast 特性使得以太网接口一旦有设备接入，就立即进入转发状态，如果接口上连接的只是计算机或者其他不运行 STP 的设备，这是非常合适的。

Uplinkfast 则经常用在接入层交换机上，当它连接到主干交换机上的主链路上故障时，能立即切换到备份链路上，而不需要经过 30 秒或者 50 秒。Uplinkfast 只需要在接入层交换机上配置即可。

Backbonefast 则主要用在主干交换机之间，当主干交换机之间的链路上故障时，可以比原有的 50 秒少 20 秒就切换到备份链路上。Backbonefast 需要在全部交换机上配置。

## 14.1.4 RSTP

RSTP 实际上是把减少 STP 收敛时间的一些措施融合在 STP 协议中形成新的协议。RSTP 中，接口的角色有：根接口、指定接口、备份接口 (Backup Interface)、替代接口 (Alternate Interface)。接口的状态有：丢弃 (Discarding)、学习状态 (Learning)、转发状态 (Forwarding)。接口还分为边界接口 (Edge Port)、点到点接口 (Point-to-Point Port)、共享接口 (Share Port)。

## 14.1.5 MST

在 PVST 中，交换机为每个 VLAN 都构建一棵 STP 树，不仅会带来 CPU 的很大负载，也会占用大量的带宽。MST 则是把多个 VLAN 映射到一个 STP 实例上，从而减少了 STP 实例。MST 可以和 STP、PVST 配合使用。对于运行 STP、PVST 的交换机来说，一个 MST 域看起来就像一台交换机。

## 14.1.6 STP 防护

STP 协议并没有什么措施对交换机的身份进行认证。在稳定的网络中如果接入非法的交换机将可能给网络中的 STP 树带来灾难性的破坏。有一些简单的措施来保护网络，虽然这些措施显得软弱无力。Root Guard 特性将使得交换机的接口拒绝接收比原有根桥优先级更高的 BPDU。而 BPDU Guard 主要是和 portfast 特性配合使用，portfast 使得接口一有计算机接入就立即进入转发状态，然而万一这个接口接入的是交换机很可能造成环路。BPDU Guard 可以使得 portfast 接口一旦接收到 BPDU，就关闭该接口。

## 14.2 实验 1：STP、PVST

### 1. 实验目的

通过本实验，读者可以掌握如下技能：

- (1) 理解 STP 的工作原理
- (2) 掌握 STP 树的控制
- (3) 利用 PVST 进行负载平衡

### 2. 实验拓扑

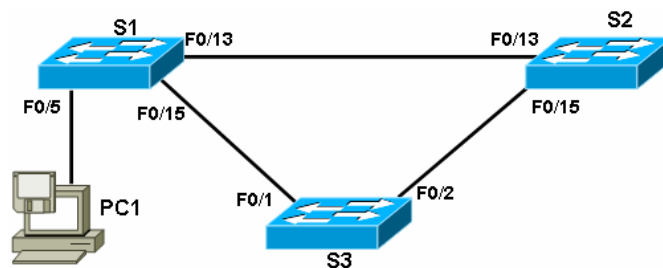


图 14-1 实验 1、实验 2、实验 4 拓扑图

图 14-1 中，S1 和 S2 模拟为核心层的交换机，而 S3 为接入的交换机。S1 和 S2 实际上是三层交换机，我们这里并不利用其三层功能，所以它们也采用二层交换机的图标。

### 3. 实验步骤

我们要在网络中配置 2 个 VLAN，不同 VLAN 的 STP 具有不同的根桥，实现负载平衡。

(1) 步骤 1: 利用 VTP 在交换机上创建 VLAN2，在 S1 和 S2 之间的链路配置 Trunk

S1(config)#vtp domain VTP-TEST

Changing VTP domain name from NULL to VTP-TEST

S1(config)#vlan 2

//在 S1 上配置 VTP 的域名，并创建 VLAN 2。由于默认时 S2 和 S3 的 VTP 域名为空，它们将自动学习到 S1 的 VTP 域名，同时 S2、S3 也将自动学习到 VLAN 2，请确认是否成功。

S1(config)#int f0/14

S1(config-if)#shutdown

//关闭该接口，以免影响我们的实验

S1(config)#int f0/13

S1(config-if)#switchport trunk encapsulation dot1q

S1(config-if)#switchport mode trunk

//S1 的 f0/13 改为 negotiate 后，由于默认时 S2 的 f0/13 为 auto 模式，S1 和 S2 将自动协商成功 Trunk。而默认时 S3 的以太网接口就是 desirable 模式，所以 S3 和 S1、S2 的链路也自动协商成功 Trunk。请确认三条链路的 Trunk 是否成功。

(2) 步骤 2: 检查初始的 STP 树

S1#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

//以上表明运行的 STP 协议是 IEEE 的 802.1D

Root ID Priority 32768

Address 0009.b7a4.b181

Cost 19

Port 17 (FastEthernet0/15)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

//以上显示 VLAN 1 的 STP 树的根桥信息，通过根桥的 MAC 地址可以确定 S3 是根桥。这是因为 S3 是较早的交换机，具有较低的 MAC 地址。由于 S3 是一台低端的交换机，成为根桥显然是不合理的。

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 0018.ba11.f500

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

//以上显示该交换机的桥 ID

Interface	Role	Sts	Cost	Prio.	Nbr	Type
-----------	------	-----	------	-------	-----	------

Fa0/13	Altn	BLK	19	128.	15	P2p
--------	------	-----	----	------	----	-----

Fa0/15	Root	FWD	19	128.	17	P2p
--------	------	-----	----	------	----	-----

//以上显示该交换机各个接口的状态，f0/13 为阻断状态，f0/15 为根口

VLAN0002

Spanning tree enabled protocol ieee

Root ID Priority 32768

Address 0009.b7a4.b182

Cost 19

Port 17 (FastEthernet0/15)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32770 (priority 32768 sys-id-ext 2)

Address 0018.ba11.f500

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface	Role	Sts	Cost	Prio.	Nbr	Type
-----------	------	-----	------	-------	-----	------

Fa0/13	Altn	BLK	19	128.	15	P2p
--------	------	-----	----	------	----	-----

Fa0/15	Root	FWD	19	128.	17	P2p
--------	------	-----	----	------	----	-----

//以上是 VLAN 2 的 STP 树情况，VLAN 2 的 STP 树和 VLAN 1 的类似。默认时，Cisco 交换机会为每个 VLAN 都生成一个单独的 STP 树，称为 PVST(Per VLAN Spanning Tree)。

**【技术要点】**需要仔细分析为什么 STP 会是目前这种情况。三个交换机的默认优先级都是 32768，而 S3 的 MAC 较低，所以成为了根桥，则 S3 上的 f0/1 和 f0/2 是指定口，处于 Forward 状态。S1 有两个接口可以到达 S3，一个接口是 f0/13，到达 S3 的 Cost 为  $19+19=38$ ，另一个接口是 f0/15，到达 S1 的 Cost 为 19，因此 f0/15 是根口，处于 Forward 状态。同样 S2 上，f0/15 也是根口，处于 Forward 状态。在 S1 和 S2 之间的链路上，要选举出一个指定口。根据选举的要素，根桥的 ID 是一样的，不能决出胜负；到达根桥的 Cost 值也是一样的，都为 19，不能决出胜负；但是发送者桥 ID 不一样，S1 的 MAC 地址高，S2 的 MAC 地址低，S2 获胜，所以 S2 的 f0/13 是指定口，处于 Forward 状态，S1 的 f0/13 就处于 Block 状态了。

(3) 步骤 3: 控制 S1 为 VLAN1 的根桥，S2 为 VLAN2 的根桥

S1(config)#spanning-tree vlan 1 priority 4096

S2(config)#spanning-tree vlan 2 priority 4096

//对于 VLAN 1 来说，S1 的优先级为 4096，而 S2 和 S3 保持默认值 32768，这样 S1 就成为了 VLAN 1 的根桥。同样我们控制 S2 成为了 VLAN 2 的根桥。优先级通常要是 4096 的倍数。

S1#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID      Priority      4097

Address      0018.ba11.f500

**This bridge is the root**

Hello Time    2 sec    Max Age 20 sec    Forward Delay 15 sec

//S1 成为了 VLAN 1 的根桥了

Bridge ID    Priority      4097    (priority 4096 sys-id-ext 1)

Address      0018.ba11.f500

Hello Time    2 sec    Max Age 20 sec    Forward Delay 15 sec

Aging Time 15

Interface	Role	Sts	Cost	Prio.	Nbr	Type
-----------	------	-----	------	-------	-----	------

Fa0/13	Desg	FWD	19	128.	15	P2p
--------	------	-----	----	------	----	-----

Fa0/15	Desg	FWD	19	128.	17	P2p
--------	------	-----	----	------	----	-----

//对于 VLAN 1 来说，f0/13 和 f0/15 是指定口，都处于转发状态了

VLAN0002

Spanning tree enabled protocol ieee

Root ID      Priority      4098

Address      0018.ba11.eb80

Cost          19

Port          15 (FastEthernet0/13)

Hello Time    2 sec    Max Age 20 sec    Forward Delay 15 sec

//S2 成为了 VLAN 2 的根桥了

Bridge ID    Priority      32770    (priority 32768 sys-id-ext 2)

Address      0018.ba11.f500

Hello Time    2 sec    Max Age 20 sec    Forward Delay 15 sec

Aging Time 15

Interface	Role	Sts	Cost	Prio.	Nbr	Type
-----------	------	-----	------	-------	-----	------

Fa0/13	Root	FWD	19	128.	15	P2p
--------	------	-----	----	------	----	-----

Fa0/15	Altn	BLK	19	128.	17	P2p
--------	------	-----	----	------	----	-----

//对于 VLAN 2 来说，f0/13 是根口，处于转发状态，而 f0/15 却是阻断状态

S3#show spanning-tree brief

VLAN1

Spanning tree enabled protocol ieee

Root ID      Priority      4097

Address      0018.ba11.f500

Cost          19

Port          1 (FastEthernet0/1)

# 国内资料最多的网络技术论坛 bbs.hh010.com

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768  
Address 0009.b7a4.b181  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  
Aging Time 300

Interface	Designated						
Name	Port ID	Prio	Cost	Sts	Cost	Bridge ID	Port ID
FastEthernet0/1	128.1	128	19	FWD	0	4097 0018.ba11.f500	128.17
FastEthernet0/2	128.2	128	19	FWD	19	32768 0009.b7a4.b181	128.2

//在 S3 上, 对于 VLAN1, S3 的 f0/1 和 f0/2 都处于转发状态。

VLAN2

Spanning tree enabled protocol ieee

Root ID Priority 4098  
Address 0018.ba11.eb80  
Cost 19  
Port 2 (FastEthernet0/2)  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768  
Address 0009.b7a4.b182  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  
Aging Time 300

Interface	Designated						
Name	Port ID	Prio	Cost	Sts	Cost	Bridge ID	Port ID
FastEthernet0/1	128.1	128	19	FWD	19	32768 0009.b7a4.b182	128.1
FastEthernet0/2	128.2	128	19	FWD	0	4098 0018.ba11.eb80	128.17

//S3 上, 对于 VLAN2, S3 的 f0/1 和 f0/2 也都处于转发状态。

(4) 步骤 4: 控制指定口

在步骤 3 中可以看到对于 VLAN 1, S1 成为了根桥, S1 的 f0/13 和 f0/15 处于转发状态; S2 的 f0/13 是根口, 也处于转发状态; S3 的 f0/1 是根口, 也处于转发状态; 然而 S2 和 S3 之间的链路上, 却是低端交换机 S3 的 f0/2 在转发数据, 原因在于 S2 和 S3 在竞争指定口时, 由于 S3 的 MAC 较低而获胜了, 这是不合理的。VLAN 2 的情况类似。

我们要控制指定口, 这可以通过改变优先级实现, 如下:

S2(config)#spanning-tree vlan 1 priority 8192

S1(config)#spanning-tree vlan 2 priority 8192

//对于 VLAN 1 来说, S2 的优先级为 8192, 比 S1 的 4096 低, 不至于成为根桥, 但是比 S3 的 32768 低, 所以在竞争指定口时会获胜。VLAN 2 的情况类似。

S3#show spanning-tree brief

VLAN1

(此处省略)

Interface				Designated			
Name	Port ID	Prio	Cost	Sts	Cost	Bridge ID	Port ID
FastEthernet0/1	128.1	128	19	FWD	0	4097 0018.ba11.f500	128.17
FastEthernet0/2	128.2	128	19	BLK	19	8193 0018.ba11.eb80	128.17

//S3 上，对于 VLAN1，S3 的 f0/1 处于转发状态，而 f0/2 处于阻断状态。

VLAN2

(此处省略)

Interface				Designated			
Name	Port ID	Prio	Cost	Sts	Cost	Bridge ID	Port ID
FastEthernet0/1	128.1	128	19	BLK	19	8194 0018.ba11.f500	128.17
FastEthernet0/2	128.2	128	19	FWD	0	4098 0018.ba11.eb80	128.17

// S3 上，对于 VLAN 2，S3 的 f0/1 处于阻断状态，而 f0/2 处于转发状态，这样起到了负载均衡的作用。

## 14.3 实验 2: portfast、uplinkfast、backbonefast

### 1. 实验目的

通过本实验，读者可以掌握如下技能：

- (1) 理解 portfast 的工作场合和配置
- (2) 理解 uplinkfast 的工作场合和配置
- (3) 理解 backbonefast 的工作场合和配置

### 2. 实验拓扑

如图 14-1。

### 3. 实验步骤

在实验 1 的基础上继续本实验，我们将只关心 VLAN 1 的 STP 树。

- (1) 步骤 1: 配置 portfast

图 14-1 中，S1 的 f0/5 是用于接入计算机。当计算机接入时，f0/5 接口立即进入 Listening 状态，随后经过 Learning，最后才成为 Forwarding，这期间需要 30 秒的时间。这对于有些场合是不可忍受的，可以配置 portfast 特性，使得计算机一接入，接口立即进入 Forwarding。

```
S1(config)#int f0/5
```

```
S1(config-if)#spanning-tree portfast
```

```
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
```

%Portfast has been configured on FastEthernet0/5 but will only have effect when the interface is in a non-trunking mode.

//交换机会警告该接口只能用于接入计算机或者路由器，不要接入其他的交换机

## (2) 步骤 2: 配置 uplinkfast

先确认实验 1 的 STP 树已经正确。在图 14-1 中的 S1 上，关闭 f0/15 接口，在 S3 上反复执行 “**show spanning-tree vlan 1 brief**” 观察 f0/2 接口的状态变化：

```
FastEthernet0/2      128.2      128    3019 LIS      19    8193 0018.ba11.eb80 128.17
```

大约 15 秒后变为：

```
FastEthernet0/2      128.2      128    3019 LRN      19    8193 0018.ba11.eb80 128.17
```

大约 15 秒后变为：

```
FastEthernet0/2      128.2      128    3019 FWD      19    8193 0018.ba11.eb80 128.17
```

合计大约 15+15=30 秒，f0/2 变为转发状态。

```
S3(config)#spanning-tree uplinkfast
```

```
S1(config)#int f0/15
```

```
S1(config-if)#no shutdown
```

```
S1(config-if)#shutdown //等 STP 重新稳定后，才执行该语句
```

在 S3 上重复执行 “**show spanning-tree vlan 1 brief**”，可以看到 f0/2 很快就进入了 Forwarding 状态。

**【技术要点】**没有配置 uplinkfast 时，交换机 S3 如果能直接检测到 f0/1 接口上的链路故障，f0/2 会立即进入 Listen 状态，这样 30 秒就能进入 Forward 状态。然而如果 S1 和 S3 之间存在一个 Hub，S1 上的 f0/15 接口故障了，S3 将无法直接检测到故障，S3 只能等待 10 个周期没有收到 S1 的 BPDU（每个周期 2 秒），20 秒中后，S3 的 f0/2 才进入 Listen 状态，这样总共 50 秒才能进入 Forward 状态。所以 STP 重新收敛的时间通常需要 30—50 秒。

## (3) 步骤 3: 配置 backbonefast

打开 S1 上 f0/15 接口，确认 STP 树已经正确。在图 14-1 中的 S1 上，关闭 f0/13 接口，在 S3 上反复执行 “**show spanning-tree vlan 1 brief**” 观察 f0/2 接口的状态变化：

```
FastEthernet0/2      128.2      128    3019 BLK      19    8193 0018.ba11.eb80 128.17
```

大约 20 秒后变为：

```
FastEthernet0/2      128.2      128    3019 LIS      19    8193 0018.ba11.eb80 128.17
```

大约 15 秒后变为：

```
FastEthernet0/2      128.2      128    3019 LRN      19    8193 0018.ba11.eb80 128.17
```

大约 15 秒后变为：

```
FastEthernet0/2      128.2      128    3019 FWD      19    8193 0018.ba11.eb80 128.17
```

合计大约 20+15+15=50 秒，f0/2 变为转发状态。

```
S1(config)#spanning-tree backbonefast
```

```
S2(config)#spanning-tree backbonefast
```

```
S3(config)#spanning-tree backbonefast
```

```
S1(config)#int f0/13
```

```
S1(config-if)#no shutdown
```

```
S1(config-if)#shutdown //等 STP 重新稳定后，才执行该语句
```



在 S3 上重复执行 “`show spanning-tree vlan 1 brief`”，可以看到 f0/2 很快就进入了 Listening 状态，合计大约  $15+15=30$  秒后，f0/2 就变为转发状态，比之前的 50 秒少了 20 秒。

**【提示】**uplinkfast 命令只需要在 S3 配置即可，而 backbonefast 命令需要在 S1、S2、S3 三台交换机上都配置。

## 14.4 实验 3:RSTP

### 1. 实验目的

通过本实验，读者可以掌握如下技能：

- (1) 熟悉 RSTP 的配置

### 2. 实验拓扑

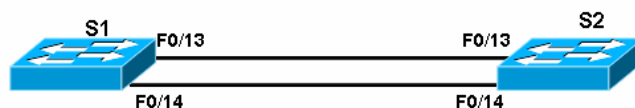


图 14-2 实验 3 拓扑图

### 3. 实验步骤

- (1) 步骤 1：请把两台交换机的配置清除干净，重启交换机

```
S1#delete flash:vlan.dat
```

```
S1#erase startup-config
```

```
S1#reload
```

```
S2#delete flash:vlan.dat
```

```
S2#erase startup-config
```

```
S2#reload
```

- (2) 步骤 2：配置 S1 和 S2 之间的 Trunk

```
S1(config)#int f0/13
```

```
S1(config-if)#switchport trunk encapsulation dot1q
```

```
S1(config-if)#switchport mode trunk
```

```
S1(config)#int f0/14
```

```
S1(config-if)#switchport trunk encapsulation dot1q
```

```
S1(config-if)#switchport mode trunk
```

- (3) 步骤 3：配置 S1 成为根桥

```
S1(config)#spanning-tree vlan 1 priority 4096
```

在 S1 和 S2 上用 “`show spanning-tree`” 命令检查 STP 的情况，S2 的 f0/14 应该处于阻断状态。

**【技术要点】**S1 是根桥，S2 要选取到达 S1 的根路径，有两条路径，Cost 都为 19。这时由于 S2 在 f0/13 接口上收到的 BPDU 中，发送者（S1）端口号为 13；在 f0/14 接口上收到的 BPDU 中，发送者端口号为 14。所以 f0/13 被选举为根口了，f0/14 则只能被阻断了。

- (4) 步骤 4：在 S2 上关闭 f0/13 接口，观察 STP 树的重新生成

在 S2 上关闭 f0/13 接口，重复执行 “show spanning-tree”，可以看到 f0/14 经过 30 秒后才进入了 Forwarding 状态。

(5) 步骤 5: 配置 RSTP

```
S1(config)#spanning-tree mode rapid-pvst
```

```
S2(config)#spanning-tree mode rapid-pvst
```

(6) 步骤 6: 在 S2 上关闭 f0/13 接口，观察 STP 树的重新生成

在 S2 上重新打开 f0/13 接口，确认 STP 稳定后，在 S2 上关闭 f0/13 接口，重复执行 “show spanning-tree”，可以看到 f0/14 立即进入了 Forwarding 状态。说明 RSTP 的收敛比普通 STP 有了很大的改善。

(7) 步骤 7: 配置链路类型

```
S1(config)#int range f0/13 -14
```

```
S1(config-if-range)#duplex full
```

```
S1(config-if-range)#spanning-tree link-type point-to-point
```

```
S2(config)#int range f0/13 -14
```

```
S2(config-if-range)#duplex full
```

```
S2(config-if-range)#spanning-tree link-type point-to-point
```

//S1 和 S2 之间的链路是 Trunk 链路，自动协商为全双工，RSTP 会自动把它们的链路类型标识为点到点。我们这里强制配置了一遍。

**【技术要点】**RSTP 中接口分为边界接口 (Edge Port)、点到点接口 (Point-to-Point Port)、共享接口 (Share Port)。如果接口上配置了 spanning portfast，接口就为边界接口；如果接口是半双工，接口就为共享接口；如果接口是全双工，接口就为点到点接口。在接口上指明类型有利于 RSTP 的运行。

## 14.5 实验 4: MST

### 1. 实验目的

通过本实验，读者可以掌握如下技能：

- (1) 理解 MST 的工作原理
- (2) 掌握 MST 的配置

### 2. 实验拓扑

如图 14-1。

### 3. 实验步骤

我们要在网络中创建 4 个 VLAN，VLAN 1 和 VLAN 2 使用 MST 实例 1，VLAN 3 和 VLAN 4 使用 MST 实例 2。

(1) 步骤 1: 利用 VTP 在交换机上创建 VLAN，在 S1 和 S2 之间的链路配置 Trunk

```
S1(config)#vtp domain VTP-TEST
```

```
Changing VTP domain name from NULL to VTP-TEST
```

```
S1(config)#vlan 2
```

```
S1(config)#vlan 3
```

```
S1(config)#vlan 4
```

```
S1(config)#int f0/14
S1(config-if)#shutdown
//关闭该接口，以免影响我们的实验
S1(config)#int f0/13
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S2(config)#int f0/13
S2(config-if)#switchport trunk encapsulation dot1q
S2(config-if)#switchport mode trunk
```

## (2) 步骤 2: 配置 MST

只有 S1 和 S2 才能支持 MST。

```
S1(config)#spanning-tree mode mst
//以上把生成树的模式改为 MST，默认时是 PVST。
S1(config)#spanning-tree mst configuration
//以上是进入 MST 的配置模式下
S1(config-mst)#name TEST-MST
//以上命名 MST 的名字
S1(config-mst)#revision 1
//以上配置 MST 的 revision 号，只有名字和 revision 号相同的交换机才是在同一个 MST
区域
S1(config-mst)#instance 1 vlan 1-2
//以上是把 VLAN 1 和 VLAN 2 的生成树映射到实例 1
S1(config-mst)#instance 2 vlan 3-4
//以上是把 VLAN 3 和 VLAN 4 的生成树映射到实例 2，我们这里一共有三个 MST 实例，实例
0 是系统要使用的
S1(config-mst)#exit
//要退出，配置才能生效
S1(config)#spanning-tree mst 1 priority 8192
S1(config)#spanning-tree mst 2 priority 12288
//以上配置 S1 为 MST 实例 1 的根桥
```

```
S2(config)#spanning-tree mode mst
S2(config)#spanning-tree mst configuration
S2(config-mst)#name TEST-MST
S2(config-mst)#revision 1
S2(config-mst)#instance 1 vlan 1-2
S2(config-mst)#instance 2 vlan 3-4
S2(config-mst)#exit
S2(config)#spanning-tree mst 1 priority 12288
S2(config)#spanning-tree mst 2 priority 8192
//以上配置 S2 为 MST 实例 2 的根桥
```

## (3) 步骤 3: 检查生成树

```
S1#show spanning-tree
MST00
```

Spanning tree enabled protocol mstp

//以上表明运行的是 MST 协议

```
Root ID    Priority    32768
          Address    0009.b7a4.b181
          Cost        200000
          Port        15 (FastEthernet0/13)
          Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Bridge ID  Priority    32768 (priority 32768 sys-id-ext 0)
          Address    0018.ba11.f500
          Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface    Role Sts Cost        Prio.Nbr Type
-----
Fa0/13       Root FWD 200000      128.15  P2p
Fa0/15       Altn BLK 200000      128.17  P2p Bound(PVST)
```

//以上的 MST00 是系统要使用的实例，BPDU 是通过它来发送的

MST01

Spanning tree enabled protocol mstp

```
Root ID    Priority    8193
          Address    0018.ba11.f500
          This bridge is the root
          Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Bridge ID  Priority    8193 (priority 8192 sys-id-ext 1)
          Address    0018.ba11.f500
          Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface    Role Sts Cost        Prio.Nbr Type
-----
Fa0/13       Desg FWD 200000      128.15  P2p
Fa0/15       Boun BLK 200000      128.17  P2p Bound(PVST)
```

MST02

Spanning tree enabled protocol mstp

```
Root ID    Priority    8194
          Address    0018.ba11.eb80
          Cost        200000
          Port        15 (FastEthernet0/13)
          Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Bridge ID  Priority    12290 (priority 12288 sys-id-ext 2)
          Address    0018.ba11.f500
          Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface    Role Sts Cost        Prio.Nbr Type
-----
Fa0/13       Root FWD 200000      128.15  P2p
Fa0/15       Boun BLK 200000      128.17  P2p Bound(PVST)
```

//以上显示的是 S1 上的 MST 实例情况。

S3#show spanning-tree brie

VLAN1

Spanning tree enabled protocol ieee

Root ID Priority 32768

Address 0009.b7a4.b181

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768

Address 0009.b7a4.b181

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 15

Interface		Designated					
Name	Port ID	Prio	Cost	Sts	Cost	Bridge ID	Port ID
FastEthernet0/1	128.1	128	19	FWD	0	32768 0009.b7a4.b181	128.1
FastEthernet0/2	128.2	128	19	FWD	0	32768 0009.b7a4.b181	128.2

(此处省略)

//以上表明 S3 成为了所有 VLAN 的根桥，f0/1 和 f0/2 都处于转发状态，这不是我们想要的。

(4) 步骤 4: 控制 S1 成为根桥

S1(config)#spanning-tree mst 0 priority 4096

//注意这里应该配置 MST 0 的优先级，只有 MST 0 才发送 BPDU。

S3#show spanning-tree brief

VLAN1

Spanning tree enabled protocol ieee

Root ID Priority 4096

Address 0018.ba11.f500

Cost 19

Port 1 (FastEthernet0/1)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

//以上表明 S1 是 VLAN 1 的根桥了

Bridge ID Priority 32768

Address 0009.b7a4.b181

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface		Designated					
Name	Port ID	Prio	Cost	Sts	Cost	Bridge ID	Port ID
FastEthernet0/1	128.1	128	19	FWD	0	4096 0018.ba11.f500	128.17
FastEthernet0/2	128.2	128	19	BLK	0	32768 0018.ba11.eb80	128.17

(此处省略)

//对于 S3 上所有的 VLAN 来说，f0/2 都是阻断的，无法取得负载平衡。

(5) 步骤 5: 控制负载平衡

```
S3(config)#int f0/2
```

```
S3(config-if)#spanning-tree vlan 3 cost 10
```

```
S3(config-if)#spanning-tree vlan 4 cost 10
```

//以上改变 VLAN 3 和 VLAN 4 在 f0/2 接口上的 Cost 值。这样对于 VLAN 3 和 VLAN 4，S3 的 f0/2 接口就处于转发状态了。

## 14.6 实验 5: STP 保护

### 1. 实验目的

通过本实验，读者可以掌握如下技能：

- (1) ROOT GUARD 的使用
- (2) BPDU GUARD 的使用

### 2. 实验拓扑

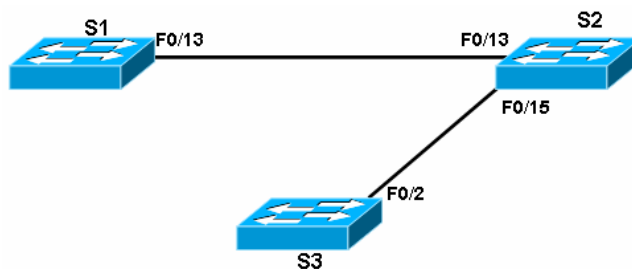


图 14-3 实验 6 拓扑图

### 3. 实验步骤

(1) 步骤 1: 关闭不需要的接口，配置 S1 和 S2 之间的 Trunk，

```
S1(config)#int f0/14
```

```
S1(config-if)#shutdown
```

```
S1(config)#int f0/15
```

```
S1(config-if)#shutdown
```

```
S1(config)#int f0/13
```

```
S1(config-if)#switchport trunk encapsulation dot1q
```

```
S1(config-if)#switchport mode trunk
```

(2) 步骤 2: 配置 S1 成为根桥

```
S1(config)#spanning-tree vlan 1 priority 8192
```

(3) 步骤 3: 在 S2 的 f0/15 上配置 guard root

```
S2(config)#int f0/15
```

```
S2(config-if)#spanning-tree guard root
```

(4) 步骤 4: 把 S3 改为根桥，观察 S2 的动作

```
S3(config)#spanning-tree vlan 1 priority 4096
```

```
S2#show spanning-tree inconsistentports
```

Name	Interface	Inconsistency
------	-----------	---------------

VLAN0001                      FastEthernet0/15                      Root Inconsistent

Number of inconsistent ports (segments) in the system : 1

//S2 将从 f0/15 收到 S3 发送的更优的 BPDU，然而由于该接口上配置 Root guard，S2 的接口进入阻断状态。

S2#show spanning-tree

VLAN0001

(此处省略)

Interface	Role	Sts	Cost	Prio.	Nbr	Type
-----------	------	-----	------	-------	-----	------

Fa0/13	Root	FWD	19	128.	15	P2p
--------	------	-----	----	------	----	-----

Fa0/15	Desg	BKN*19		128.	17	P2p *ROOT_Inc
--------	------	--------	--	------	----	---------------

(5) 步骤 5: 配置 BPDU Guard

S2(config)#int f0/15

S2(config-if)#shutdown

//关闭接口

S2(config-if)#no spanning-tree guard root

//去掉之前的配置

S2(config-if)#spanning-tree portfast

S2(config-if)#spanning-tree bpduguard enable

//以上配置 BPDU Guard

S2(config)#int f0/15

S2(config-if)#no shutdown

0:28:49: %SPANTREE-2-BLOCK\_BPDUGUARD: Received BPDU on port FastEthernet0/15 with BPDU Guard enabled. Disabling port.

00:28:49: %PM-4-ERR\_DISABLE: bpduguard error detected on Fa0/15, putting Fa0/15 in err-disable state

00:28:50: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/15, changed state to down

//交换机从 f0/15 接口收到 S3 的 BPDU，f0/15 被 disable 了

S2#show interfaces f0/15

FastEthernet0/15 is down, line protocol is down (err-disabled)

//可以看到 f0/15 接口关闭了。要重新开启，请先移除 BPDU 源，在接口下执行“shutdown”、“no shutdown”命令。

## 14.7 本章小结

本章首先介绍了 STP 的作用和基本工作原理，交换机通过 STP 协议有选择性地阻断了某些接口，从而构建无环路的转发路径，STP 需要选取根桥、根口、指定口。802.1D 的 STP 需要较长时间才收敛，通常为 30—50 秒。本章还介绍减少 STP 收敛的措施：uplinkfast、backbonefast 和 RSTP 协议。默认时 CISCO 交换机为每个 VLAN 构建一棵树，这样方便控制 STP 树，但导致 STP 树数量太多。MST 则可以为多个 VLAN 共同构建一棵树。本章最后介绍了

保护 STP 树的两个简单措施：Root Guard 和 BPDU Guard。表 14-1 是本章出现的命令。

表 14-1 本章命令汇总

命令	作用
show spanning-tree	查看 STP 树信息
spanning-tree vlan 1 priority 4096	配置 VLAN1 的桥优先级
spanning-tree portfast	配置接口为 portfast，当有设备接入时立即进入转发状态
spanning-tree uplinkfast	配置 uplinkfast 特性
spanning-tree backbonefast	配置 backbonefast 特性
spanning-tree mode rapid-pvst	把 STP 的运行模式设为 RSTP+PVST
spanning-tree link-type point-to-point	把接口的链路类型改为点对点
spanning-tree mode mst	把生成树的模式改为 MST
spanning-tree mst configuration	进入 MST 的配置模式
name TEST-MST	命名 MST 的名字
revision 1	配置 MST 的 revision 号
instance 1 vlan 1-2	把 VLAN 1 和 VLAN 2 的生成树映射到实例 1
spanning-tree guard root	在接口上配置 root guard 特性
spanning-tree bpduguard enable	在接口上配置 bpduguard 特性