

# 目 录

<b>1 生成树协议概述</b>	<b>1-1</b>
1.1 STP简介	1-1
1.1.1 STP的协议报文	1-1
1.1.2 STP的基本概念	1-3
1.1.3 STP的拓扑计算过程	1-4
1.1.4 STP算法实现举例	1-6
1.1.5 STP的BPDU传递机制	1-8
1.1.6 STP的时间参数	1-9
1.2 RSTP简介	1-10
1.2.1 RSTP的协议报文	1-10
1.2.2 RSTP的基本概念	1-10
1.2.3 RSTP的工作原理	1-11
1.2.4 RSTP中的BPDU处理	1-11
1.3 PVST简介	1-12
1.3.1 PVST的协议报文	1-12
1.3.2 PVST的工作原理	1-12
1.4 MSTP简介	1-13
1.4.1 MSTP的优点	1-13
1.4.2 MSTP的协议报文	1-13
1.4.3 MSTP的基本概念	1-14
1.4.4 MSTP的工作原理	1-18
1.4.5 MSTP在设备上的实现	1-18
1.5 快速收敛机制	1-19
1.5.1 边缘端口机制	1-19
1.5.2 根端口快速切换机制	1-19
1.5.3 P/A机制	1-20
1.6 协议规范	1-21
<b>2 配置生成树协议</b>	<b>2-1</b>
2.1 生成树协议配置限制和指导	2-1
2.1.1 与其他功能之间的配置限制和指导	2-1
2.1.2 接口相关配置限制和指导	2-1
2.2 生成树协议配置任务简介	2-1

2.2.1 STP配置任务简介 .....	2-1
2.2.2 RSTP配置任务简介 .....	2-2
2.2.3 PVST配置任务简介 .....	2-3
2.2.4 MSTP配置任务简介 .....	2-4
2.3 配置生成树的工作模式 .....	2-6
2.4 配置MST域 .....	2-7
2.5 配置根桥和备份根桥 .....	2-8
2.5.1 配置限制和指导 .....	2-8
2.5.2 配置根桥 .....	2-8
2.5.3 配置备份根桥 .....	2-8
2.6 配置设备的优先级 .....	2-9
2.7 配置MST域的最大跳数 .....	2-9
2.8 配置交换网络的网络直径 .....	2-10
2.9 配置生成树的时间参数 .....	2-10
2.10 配置超时时间因子 .....	2-12
2.11 配置端口发送BPDU的速率 .....	2-12
2.12 配置端口为边缘端口 .....	2-13
2.13 配置端口的路径开销 .....	2-13
2.13.1 功能简介 .....	2-13
2.13.2 配置缺省路径开销的计算标准 .....	2-13
2.13.3 配置端口的路径开销 .....	2-15
2.14 配置端口的优先级 .....	2-15
2.15 配置端口的链路类型 .....	2-16
2.16 配置端口收发的MSTP报文格式 .....	2-17
2.17 打开端口状态变化信息显示开关 .....	2-17
2.18 开启生成树协议 .....	2-18
2.18.1 配置限制和指导 .....	2-18
2.18.2 开启生成树协议（STP/RSTP/MSTP模式） .....	2-18
2.18.3 开启生成树协议（PVST模式） .....	2-18
2.19 执行mCheck操作 .....	2-19
2.19.1 功能简介 .....	2-19
2.19.2 配置限制和指导 .....	2-19
2.19.3 全局执行mCheck操作 .....	2-19
2.19.4 在端口上执行mCheck操作 .....	2-19
2.20 关闭PVST的PVID不一致保护功能 .....	2-20
2.21 配置摘要侦听功能 .....	2-20

2.22 配置No Agreement Check功能 .....	2-21
2.23 配置TC Snooping功能 .....	2-23
2.24 配置生成树保护功能 .....	2-24
2.24.1 生成树保护功能配置任务简介 .....	2-24
2.24.2 配置BPDU保护功能 .....	2-25
2.24.3 配置根保护功能 .....	2-25
2.24.4 配置环路保护功能 .....	2-26
2.24.5 配置端口角色限制功能 .....	2-27
2.24.6 配置TC-BPDU传播限制功能 .....	2-27
2.24.7 配置防TC-BPDU攻击保护功能 .....	2-28
2.24.8 配置BPDU拦截功能 .....	2-28
2.24.9 配置MSTP的PVST报文保护功能 .....	2-29
2.24.10 关闭Dispute保护功能 .....	2-29
2.25 配置在PVST模式下设备检测或接收到TC报文时打印日志信息 .....	2-31
2.26 配置被BPDU保护功能关闭的端口不再自动恢复 .....	2-31
2.27 配置生成树的网管功能 .....	2-32
2.28 生成树显示和维护 .....	2-32
2.29 生成树典型配置举例 .....	2-33
2.29.1 MSTP配置举例 .....	2-33
2.29.2 PVST配置举例 .....	2-37

# 1 生成树协议概述

生成树协议是一种二层管理协议，它通过选择性地阻塞网络中的冗余链路来消除二层环路，同时还具备链路备份的功能。最初的生成树协议为 STP（Spanning Tree Protocol，生成树协议），之后又发展出 RSTP（Rapid Spanning Tree Protocol，快速生成树协议）、PVST（Per-VLAN Spanning Tree，每 VLAN 生成树）和 MSTP（Multiple Spanning Tree Protocol，多生成树协议）。

## 1.1 STP简介

STP 由 IEEE 制定的 802.1D 标准定义，用于在局域网中消除数据链路层物理环路的协议。运行该协议的设备通过彼此交互信息发现网络中的环路，并有选择的对某些端口进行阻塞，最终将环路网络结构修剪成无环路的树型网络结构，从而防止报文在环路网络中不断增生和无限循环，避免设备由于重复接收相同的报文造成的报文处理能力下降的问题发生。

STP 包含了两个含义，狭义的 STP 是指 IEEE 802.1D 中定义的 STP 协议，广义的 STP 是指包括 IEEE 802.1D 定义的 STP 协议以及各种在它的基础上经过改进的生成树协议。

### 1.1.1 STP的协议报文

STP 采用的协议报文是 BPDU（Bridge Protocol Data Unit，网桥协议数据单元），也称为配置消息。本文中把生成树协议的协议报文均简称为 BPDU。

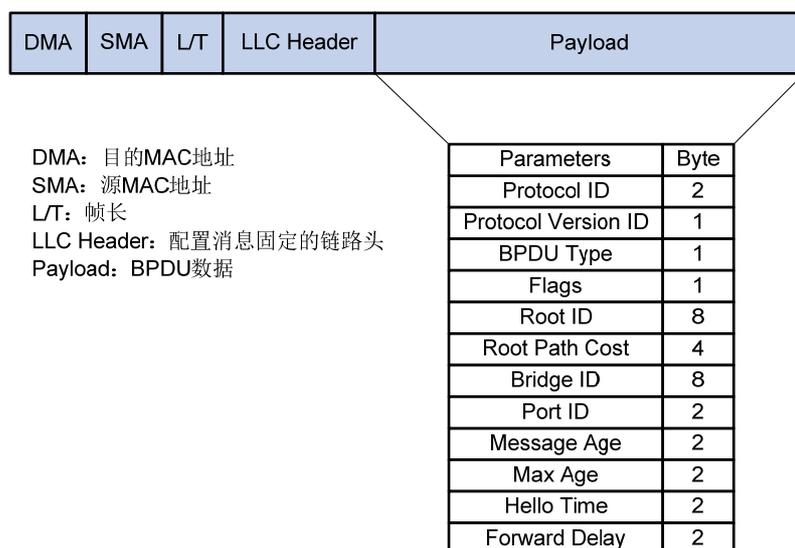
STP 通过在设备之间传递 BPDU 来确定网络的拓扑结构。BPDU 中包含了足够的信息来保证设备完成生成树的计算过程。STP 协议的 BPDU 分为以下两类：

- 配置 BPDU（Configuration BPDU）：用来进行生成树计算和维护生成树拓扑的报文。
- TCN BPDU（Topology Change Notification BPDU，拓扑变化通知 BPDU）：当拓扑结构发生变化时，用来通知相关设备网络拓扑结构发生变化的报文。

#### 1. 配置BPDU

网桥之间通过交互配置BPDU来进行根桥的选举以及端口角色的确定。配置BPDU的格式如 [图 1-1](#) 所示。

图1-1 配置 BPDU 格式



配置 BPDU 中 BPDU 数据的信息包括:

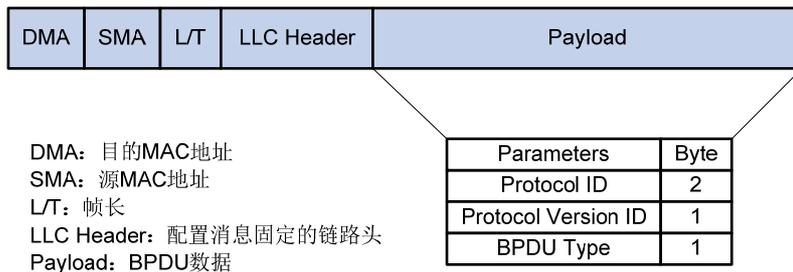
- 协议类型 (Protocol ID): 固定为 0x0000, 表示生成树协议。
- 协议版本号 (Protocol Version ID): 目前生成树有三个版本, STP 的协议版本号为 0x00。
- BPDU 类型: 配置 BPDU 类型为 0x00。
- BPDU Flags 位: BPDU 标志位, 表示是哪种 BPDU。由 8 位组成, 最低位 (0 位) 为 TC (Topology Change, 拓扑改变) 标志位; 最高位 (7 位) 为 TCA (Topology Change Acknowledge, 拓扑改变确认) 标志位; 其他 6 位保留。
- 根桥 (Root Bridge) ID: 由根桥的优先级和 MAC 地址组成。
- 根路径开销: 到根桥的路径开销。
- 指定桥 ID: 由指定桥的优先级和 MAC 地址组成。
- 指定端口 ID: 由指定端口的优先级和该端口的全局编号组成。
- Message Age: BPDU 在网络中传播的生存期。
- Max Age: BPDU 在设备中的最大生存期。
- Hello Time: BPDU 的发送周期。
- Forward Delay: 端口状态迁移的延迟时间。

其中通过根桥 ID、路径开销、指定桥 ID、指定端口 ID、Message Age、Max Age、Hello Time 和 Forward Delay 信息来保证设备完成生成树的计算过程。

## 2. TCN BPDU

如 图 1-2 所示, TCN BPDU 和配置 BPDU 在结构上基本相同, 也是由源/目的 MAC 地址、L/T 位、逻辑链路头和 BPDU 数据组成。但是 TCN BPDU 的 BPDU 数据组成非常简单, 只包含三部分信息: 协议类型、协议版本号和 BPDU 类型。协议类型和协议版本号字段和配置 BPDU 相同, BPDU 类型字段的值为 0x80, 表示该 BPDU 为 TCN BPDU。

图1-2 TCN BPDU 格式



TCN BPDU 有两个产生条件:

- 网桥上有端口转变为 **Forwarding** 状态，且该网桥至少包含一个指定端口。
- 网桥上有端口从 **Forwarding** 状态或 **Learning** 状态转变为 **Blocking** 状态。

当上述两个条件之一满足时，说明网络拓扑发生了变化，网桥需要使用 TCN BPDU 通知根桥。根桥可以通过将配置 BPDU 中对应标志位置位来通知所有网桥网络拓扑发生了变化，需要使用较短的 MAC 地址老化时间，保证拓扑的快速收敛。

## 1.1.2 STP的基本概念

### 1. 根桥

树形的网络结构必须有树根，于是 STP 引入了根桥的概念。根桥在全网中有且只有一个，其他设备则称为叶子节点。根桥会根据网络拓扑的变化而改变，因此根桥并不是固定的。

在网络初始化过程中，所有设备都视自己为根桥，生成各自的配置 BPDU 并周期性地向外发送；但当网络拓扑稳定以后，只有根桥设备才会向外发送配置 BPDU，其他设备则对其进行转发。

### 2. 根端口

所谓根端口，是指非根桥设备上离根桥最近的端口。根端口负责与根桥进行通信。非根桥设备上有且只有一个根端口，根桥上没有根端口。

### 3. 指定桥与指定端口

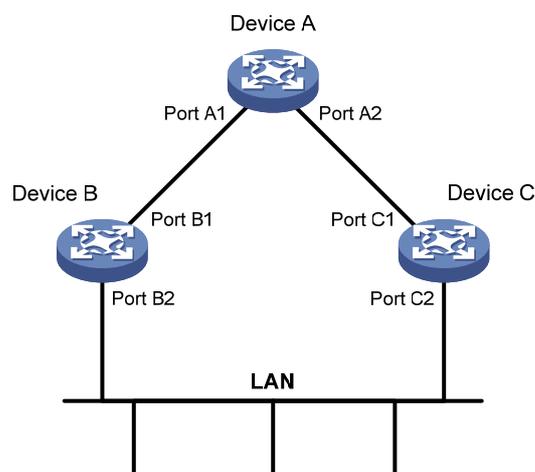
有关指定桥与指定端口的含义，请参见 [表 1-1](#) 的说明。

表1-1 指定桥与指定端口的含义

分类	指定桥	指定端口
对于一台设备而言	与本机直接相连并且负责向本机转发 BPDU 的设备	指定桥向本机转发 BPDU 的端口
对于一个局域网而言	负责向本网段转发 BPDU 的设备	指定桥向本网段转发 BPDU 的端口

如 [图 1-3](#) 所示，Device B 和 Device C 与 LAN 直接相连。如果 Device A 通过 Port A1 向 Device B 转发 BPDU，则 Device B 的指定桥就是 Device A，指定端口就是 Device A 上的 Port A1；如果 Device B 负责向 LAN 转发 BPDU，则 LAN 的指定桥就是 Device B，指定端口就是 Device B 上的 Port B2。

图1-3 指定桥与指定端口示意图



#### 4. 端口状态

STP的端口有 5 种工作状态。如 [表 1-2](#) 所示。

表1-2 STP 的端口状态

状态	描述
Disabled	该状态下的端口没有激活，不参与STP的任何动作，不转发用户流量
Listening	该状态下的端口可以接收和发送BPDU，但不转发用户流量
Learning	该状态下建立无环的转发表，不转发用户流量
Forwarding	该状态下的端口可以接收和发送BPDU，也转发用户流量
Blocking	该状态下的端口可以接收BPDU，但不转发用户流量

#### 5. 路径开销

路径开销是 STP 协议用于选择链路的参考值。STP 协议通过计算路径开销，选择较为“强壮”的链路，阻塞多余的链路，将网络修剪成无环路的树型网络结构。

### 1.1.3 STP的拓扑计算过程

STP 的拓扑计算过程如下：设备通过比较不同端口收到的 BPDU 报文的优先级高低，选举出根桥、根端口、指定端口，完成生成树的计算，建立对应的树形拓扑。

#### 1. 初始状态

各设备的各端口在初始时会生成以本设备为根桥的 BPDU，根路径开销为 0，指定桥 ID 为自身设备 ID，指定端口为本端口。

#### 2. 选择根桥

网络初始化时，需要在网络中所有的 STP 设备中选择一个根桥，根桥的选择方式有以下两种：

- 自动选举：网络初始化时，网络中所有的 STP 设备都认为自己是“根桥”，根桥 ID 为自身的设备 ID。通过交换 BPDU，设备之间比较根桥 ID，网络中根桥 ID 最小的设备被选为根桥。
- 手工指定：用户手工将设备配置为指定生成树的根桥或备份根桥。
  - 在一棵生成树中，生效的根桥只有一个，当两台或两台以上的设备被指定为同一棵生成树的根桥时，系统将选择 MAC 地址最小的设备作为根桥。
  - 用户可以在每棵生成树中指定一个或多个备份根桥。当根桥出现故障或被关机时，如果配置了一个备份根桥，则该备份根桥可以取代根桥成为指定生成树的根桥；如果配置了多个备份根桥，则 MAC 地址最小的备份根桥将成为指定生成树的根桥。但此时若配置了新的根桥，则备份根桥将不会成为根桥。

### 3. 选择根端口和指定端口

根端口和指定端口的选择过程如 [表 1-3](#) 所示。

表1-3 根端口和指定端口的选择过程

步骤	内容
1	非根桥设备将接收最优BPDU（最优BPDU的选择过程如 <a href="#">表1-4</a> 所示）的那个端口定为根端口
2	设备根据根端口的BPDU和根端口的路径开销，为每个端口计算一个指定端口BPDU： <ul style="list-style-type: none"> <li>● 根桥 ID 替换为根端口的 BPDU 的根桥 ID；</li> <li>● 根路径开销替换为根端口 BPDU 的根路径开销加上根端口对应的路径开销；</li> <li>● 指定桥 ID 替换为自身设备的 ID；</li> <li>● 指定端口 ID 替换为自身端口 ID。</li> </ul>
3	设备将计算出的BPDU与角色待定端口自己的BPDU进行比较： <ul style="list-style-type: none"> <li>● 如果计算出的 BPDU 更优，则该端口被确定为指定端口，其 BPDU 也被计算出的 BPDU 替换，并周期性地向外发送；</li> <li>● 如果该端口自己的 BPDU 更优，则不更新该端口的 BPDU 并将该端口阻塞。该端口将不再转发数据，且只接收不发送 BPDU。</li> </ul>



#### 说明

当拓扑处于稳定状态时，只有根端口和指定端口在转发用户流量。其他端口都处于阻塞状态，只接收 STP 协议报文而不转发用户流量。

表1-4 最优 BPDU 的选择过程

步骤	内容
1	每个端口将收到的BPDU与自己的BPDU进行比较： <ul style="list-style-type: none"> <li>● 如果收到的 BPDU 优先级较低，则将其直接丢弃，对自己的 BPDU 不进行任何处理；</li> <li>● 如果收到的 BPDU 优先级较高，则用该 BPDU 的内容将自己 BPDU 的内容替换掉。</li> </ul>
2	设备将所有端口的BPDU进行比较，选出最优的BPDU



说明

BPDU 优先级的比较规则如下:

根桥 ID 较小的 BPDU 优先级较高;

若根桥 ID 相同, 则比较根路径开销: 将 BPDU 中的根路径开销与本端口对应的路径开销相加, 二者之和较小的 BPDU 优先级较高;

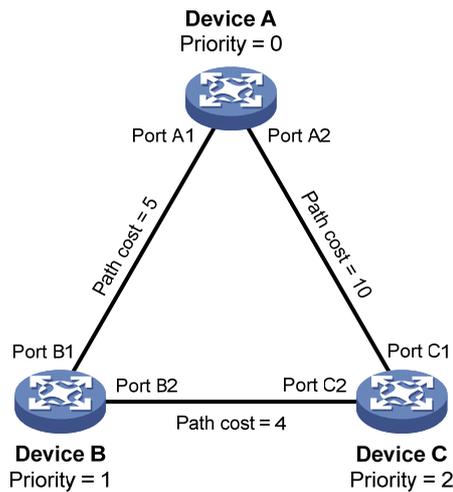
若根路径开销也相同, 则依次比较指定桥 ID、指定端口 ID、接收该 BPDU 的端口 ID 等, 上述值较小的 BPDU 优先级较高。

一旦根桥、根端口和指定端口选举成功, 整个树形拓扑就建立完毕了。

### 1.1.4 STP算法实现举例

下面结合例子说明 STP 算法实现的具体过程。

图1-4 STP 算法实现过程组网图



如 图 1-4 所示, Device A、Device B和Device C的优先级分别为 0、1 和 2, Device A与Device B 之间、Device A与Device C之间以及Device B与Device C之间链路的路径开销分别为 5、10 和 4。

#### 1. 各设备的初始状态

各设备的初始状态如 表 1-5 所示。

表1-5 各设备的初始状态

设备	端口名称	端口的 BPDU
Device A	Port A1	{0, 0, 0, Port A1}
	Port A2	{0, 0, 0, Port A2}
Device B	Port B1	{1, 0, 1, Port B1}
	Port B2	{1, 0, 1, Port B2}
Device C	Port C1	{2, 0, 2, Port C1}

设备	端口名称	端口的 BPDU
	Port C2	{2, 0, 2, Port C2}



说明

表 1-5 中 BPDU 各项的具体含义为：{根桥ID，根路径开销，指定桥ID，指定端口ID}。

## 2. 各设备的比较过程及结果

各设备的比较过程及结果如 表 1-6 所示。

表1-6 各设备的比较过程及结果

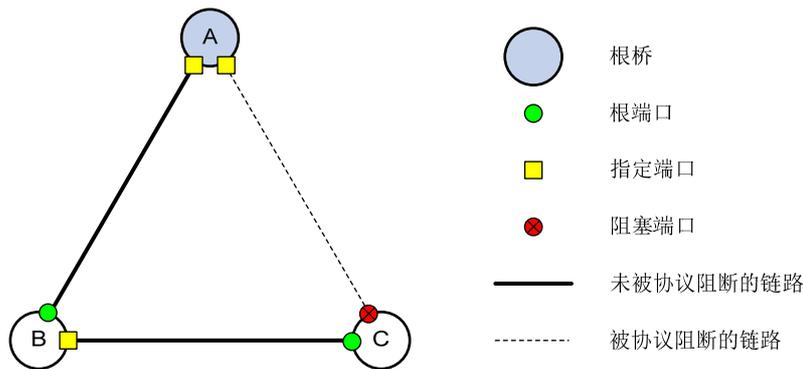
设备	比较过程	比较后端口的 BPDU
Device A	<ul style="list-style-type: none"> <li>Port A1 收到 Port B1 的 BPDU {1, 0, 1, Port B1}，发现自己的 BPDU {0, 0, 0, Port A1} 更优，于是将其丢弃。</li> <li>Port A2 收到 Port C1 的 BPDU {2, 0, 2, Port C1}，发现自己的 BPDU {0, 0, 0, Port A2} 更优，于是将其丢弃。</li> <li>Device A 发现自己各端口的 BPDU 中的根桥和指定桥都是自己，于是认为自己就是根桥，各端口的 BPDU 都不作任何修改，此后便周期性地向外发送 BPDU。</li> </ul>	<ul style="list-style-type: none"> <li>Port A1: {0, 0, 0, Port A1}</li> <li>Port A2: {0, 0, 0, Port A2}</li> </ul>
Device B	<ul style="list-style-type: none"> <li>Port B1 收到 Port A1 的 BPDU {0, 0, 0, Port A1}，发现其比自己的 BPDU {1, 0, 1, Port B1} 更优，于是更新自己的 BPDU。</li> <li>Port B2 收到 Port C2 的 BPDU {2, 0, 2, Port C2}，发现自己的 BPDU {1, 0, 1, Port B2} 更优，于是将其丢弃。</li> </ul>	<ul style="list-style-type: none"> <li>Port B1: {0, 0, 0, Port A1}</li> <li>Port B2: {1, 0, 1, Port B2}</li> </ul>
	<ul style="list-style-type: none"> <li>Device B 比较自己各端口的 BPDU，发现 Port B1 的 BPDU 最优，于是该端口被确定为根端口，其 BPDU 不变。</li> <li>Device B 根据根端口的 BPDU 和路径开销，为 Port B2 计算出指定端口的 BPDU {0, 5, 1, Port B2}，然后与 Port B2 本身的 BPDU {1, 0, 1, Port B2} 进行比较，发现计算出的 BPDU 更优，于是 Port B2 被确定为指定端口，其 BPDU 也被替换为计算出的 BPDU，并周期性地向外发送。</li> </ul>	<ul style="list-style-type: none"> <li>根端口 Port B1: {0, 0, 0, Port A1}</li> <li>指定端口 Port B2: {0, 5, 1, Port B2}</li> </ul>
Device C	<ul style="list-style-type: none"> <li>Port C1 收到 Port A2 的 BPDU {0, 0, 0, Port A2}，发现其比自己的 BPDU {2, 0, 2, Port C1} 更优，于是更新自己的 BPDU。</li> <li>Port C2 收到 Port B2 更新前的 BPDU {1, 0, 1, Port B2}，发现其比自己的 BPDU {2, 0, 2, Port C2} 更优，于是更新自己的 BPDU。</li> </ul>	<ul style="list-style-type: none"> <li>Port C1: {0, 0, 0, Port A2}</li> <li>Port C2: {1, 0, 1, Port B2}</li> </ul>
	<ul style="list-style-type: none"> <li>Device C 比较自己各端口的 BPDU，发现 Port C1 的 BPDU 最优，于是该端口被确定为根端口，其 BPDU 不变。</li> <li>Device C 根据根端口的 BPDU 和路径开销，为 Port C2 计算出指定端口的 BPDU {0, 10, 2, Port C2}，然后与 Port C2 本身的 BPDU {1, 0, 1, Port B2} 进行比较，发现计算出的 BPDU 更优，于是 Port C2 被确定为指定端口，其 BPDU 也被替换为计算出的 BPDU。</li> </ul>	<ul style="list-style-type: none"> <li>根端口 Port C1: {0, 0, 0, Port A2}</li> <li>指定端口 Port C2: {0, 10, 2, Port C2}</li> </ul>

设备	比较过程	比较后端口的 BPDU
	<ul style="list-style-type: none"> <li>Port C2 收到 Port B2 更新后的 BPDU {0, 5, 1, Port B2}, 发现其比自己的 BPDU {0, 10, 2, Port C2} 更优, 于是更新自己的 BPDU。</li> <li>Port C1 收到 Port A2 周期性发来的 BPDU {0, 0, 0, Port A2}, 发现其与自己的 BPDU 一样, 于是将其丢弃。</li> </ul>	<ul style="list-style-type: none"> <li>Port C1: {0, 0, 0, Port A2}</li> <li>Port C2: {0, 5, 1, Port B2}</li> </ul>
	<ul style="list-style-type: none"> <li>Device C 比较 Port C1 的根路径开销 10 (收到的 BPDU 中的根路径开销 0 + 本端口所在链路的路径开销 10) 与 Port C2 的根路径开销 9 (收到的 BPDU 中的根路径开销 5 + 本端口所在链路的路径开销 4), 发现后者更小, 因此 Port C2 的 BPDU 更优, 于是 Port C2 被确定为根端口, 其 BPDU 不变。</li> <li>Device C 根据根端口的 BPDU 和路径开销, 为 Port C1 计算出指定端口的 BPDU {0, 9, 2, Port C1}, 然后与 Port C1 本身的 BPDU {0, 0, 0, Port A2} 进行比较, 发现本身的 BPDU 更优, 于是 Port C1 被阻塞, 其 BPDU 不变。从此, Port C1 不再转发数据, 直至有触发生成树计算的新情况出现, 譬如 Device B 与 Device C 之间的链路 down 掉。</li> </ul>	<ul style="list-style-type: none"> <li>阻塞端口 Port C1: {0, 0, 0, Port A2}</li> <li>根端口 Port C2: {0, 5, 1, Port B2}</li> </ul>

### 3. 计算出的生成树

经过上述比较过程之后, 以 Device A 为根桥的生成树就确定下来了, 其拓扑如 [图 1-5](#) 所示。

图1-5 计算后得到的拓扑



#### 说明

为了便于描述, 本例简化了生成树的计算过程, 实际的过程要更加复杂。

## 1.1.5 STP的BPDU传递机制

STP 的 BPDU 传递机制如下:

- 当网络初始化时, 所有的设备都将自己作为根桥, 生成以自己为根的 BPDU, 并以 Hello Time 为周期定时向外发送。

- 接收到 BPDU 的端口如果是根端口，且接收的 BPDU 比该端口的 BPDU 优，则设备将 BPDU 中携带的 Message Age 按照一定的原则递增，并启动定时器为这条 BPDU 计时，同时将此 BPDU 从设备的指定端口转发出去。
- 如果指定端口收到的 BPDU 比本端口的 BPDU 优先级低时，会立刻发出自己的更好的 BPDU 进行回应。
- 如果某条路径发生故障，则这条路径上的根端口不会再收到新的 BPDU，旧的 BPDU 将会因为超时而被丢弃，设备重新生成以自己为根的 BPDU 并对外发送，从而引发生成树的重新计算，得到一条新的通路替代发生故障的链路，恢复网络连通性。

不过，重新计算得到的新 BPDU 不会立刻就传遍整个网络，因此旧的根端口和指定端口由于没有发现网络拓扑变化，将仍按原来的路径继续转发数据。如果新选出的根端口和指定端口立刻就开始数据转发的话，可能会造成暂时性的环路。

### 1.1.6 STP的时间参数

在 STP 的计算过程中，用到了以下三个重要的时间参数：

- **Forward Delay:** 用于确定状态迁移的延迟时间。缺省情况下 Forward Delay 时间为 15 秒。链路故障会引发网络重新进行生成树的计算，生成树的结构将发生相应的变化。不过重新计算得到的新 BPDU 无法立刻传遍整个网络，如果新选出的根端口和指定端口立刻就开始数据转发的话，可能会造成暂时性的环路。为此，生成树协议在端口由 Blocking 状态向 Forwarding 状态迁移的过程中设置了 Listening 和 Learning 状态作为过渡（Listening 和 Learning 状态都会持续 Forward Delay 时间），并规定状态迁移需要等待 Forward Delay 时间，以保持与远端的设备状态切换同步。新选出的根端口和指定端口要经过 2 倍的 Forward Delay 延时后才能进入转发状态，这个延时保证了新的 BPDU 已经传遍整个网络。
- **Hello Time:** 用于设备检测链路是否存在故障。缺省情况下 Hello Time 为 2 秒。生成树协议每隔 Hello Time 时间会发送 BPDU，以确认链路是否存在故障。如果设备在超时时间（超时时间 = 超时时间因子 × 3 × Hello Time）内没有收到 BPDU，则会由于消息超时而重新计算生成树。
- **Max Age:** 用于判断 BPDU 在设备内的保存时间是否“过时”，设备会将过时的 BPDU 丢弃。缺省情况下 Max Age 时间为 20 秒。在 MSTP 的 CIST 上，设备根据 Max Age 时间来确定端口收到的 BPDU 是否超时。如果端口收到的 BPDU 超时，则需要对该 MSTI 重新计算。Max Age 时间对 MSTP 的 MSTI 无效。

STP 每隔一个 Hello Time 发送一个 BPDU，并且引入 Keepalive 机制。Hello 包的发送可以避免最大失效定时器溢出。如果最大失效定时器溢出，通常表明有连接错误发生。此时，STP 会进入 Listening 状态。STP 要从连接错误中恢复过来，一般需要 50 秒的时间。其中 BPDU 最长的失效时间 20 秒；Listening 状态持续 15 秒；Learning 状态持续 15 秒。

为保证网络拓扑的快速收敛，需要配置合适的时间参数。上述三个时间参数之间应满足以下关系，否则会引起网络的频繁震荡：

- $2 \times (\text{Forward Delay} - 1 \text{ 秒}) \geq \text{Max Age}$
- $\text{Max Age} \geq 2 \times (\text{Hello Time} + 1 \text{ 秒})$

## 1.2 RSTP简介

RSTP 由 IEEE 制定的 802.1w 标准定义，它在 STP 基础上进行了改进，实现了网络拓扑的快速收敛。其“快速”体现在，当一个端口被选为根端口和指定端口后，其进入转发状态的延时将大大缩短，从而缩短了网络最终达到拓扑稳定所需要的时间。

### 1.2.1 RSTP的协议报文

RSTP 也是通过在设备之间传递 BPDU 来确定网络的拓扑结构。RSTP 的 BPDU 格式和 STP 的配置 BPDU 格式非常相似，仅在以下几个信息有所不同：

- BPDU 类型变为 0x02，表示为 RSTP 的 BPDU。
- BPDU 协议版本号为 0x02，表示为 RSTP 协议。
- Flags 位字段使用了全 8 位。
- RSTP 在 BPDU 报文的最后增加了 Version1 Length 字段。该字段的值为 0x00，表示本 BPDU 中不包含 Version 1 内容。

在拓扑改变时，RSTP 的拓扑改变处理过程不再使用 TCN BPDU，而使用 Flags 位中 TC 置位的 RST BPDU 取代 TCN BPDU，并通过泛洪方式快速的通知到整个网络。

### 1.2.2 RSTP的基本概念

#### 1. 端口角色

RSTP 中根端口和指定端口角色的定义和 STP 相同。与 STP 相比，RSTP 增加了三种端口角色替换端口（Alternate Port）、备份端口（Backup Port）和边缘端口（Edge Port）。

- 替换端口为网桥提供一条到达根桥的备用路径，当根端口或主端口被阻塞后，替换端口将成为新的根端口或主端口。
- 备份端口为网桥提供了到达同一个物理网段的冗余路径，当指定端口失效后，备份端口将转换为新的指定端口。当开启了生成树协议的同一天设备上的两个端口互相连接而形成环路时，设备会将其中一个端口阻塞，该端口就是备份端口。
- 边缘端口是不与其他设备或网段连接的端口，边缘端口一般与用户终端设备直接相连。

#### 2. 端口状态

RSTP 将端口状态缩减为三个，分别为 Discarding、Learning 和 Forwarding 状态。STP 中的 Disabled、Blocking 和 Listening 状态在 RSTP 中都对应为 Discarding 状态，如 [表 1-7](#) 所示。

表1-7 RSTP 的端口状态

STP 端口状态	RSTP 端口状态	是否发送 BPDU	是否进行 MAC 地址学习	是否收发用户流量
Disabled	Discarding	否	否	否
Blocking	Discarding	否	否	否
Listening	Discarding	是	否	否
Learning	Learning	是	是	否
Forwarding	Forwarding	是	是	是

### 1.2.3 RSTP的工作原理

进行RSTP计算时,端口会在 Discarding 状态完成角色的确定,当端口确定为根端口和指定端口后,经过 Forward Delay 端口会进入 Learning 状态;当端口确定为替换端口,端口会维持在 Discarding 状态。

处于 Learning 状态的端口其处理方式和 STP 相同,开始学习 MAC 地址并在 Forward Delay 后进入 Forwarding 状态开始收发用户流量。

在 RSTP 中,根端口的端口状态快速迁移的条件是:本设备上旧的根端口已经停止转发数据,而且上游指定端口已经开始转发数据。

在 RSTP 中,指定端口的端口状态快速迁移的条件是:指定端口是边缘端口(即该端口直接与用户终端相连,而没有连接到其他设备或共享网段上)或者指定端口与点对点链路(即两台设备直接相连的链路)相连。如果指定端口是边缘端口,则指定端口可以直接进入转发状态;如果指定端口连接着点对点链路,则设备可以通过与下游设备握手,得到响应后即刻进入转发状态。

### 1.2.4 RSTP中的BPDU处理

相比于 STP, RSTP 对 BPDU 的发送方式做了改进, RSTP 中网桥可以自行从指定端口发送 RST BPDU, 不需要等待来自根桥的 RST BPDU, BPDU 的发送周期为 Hello Time。

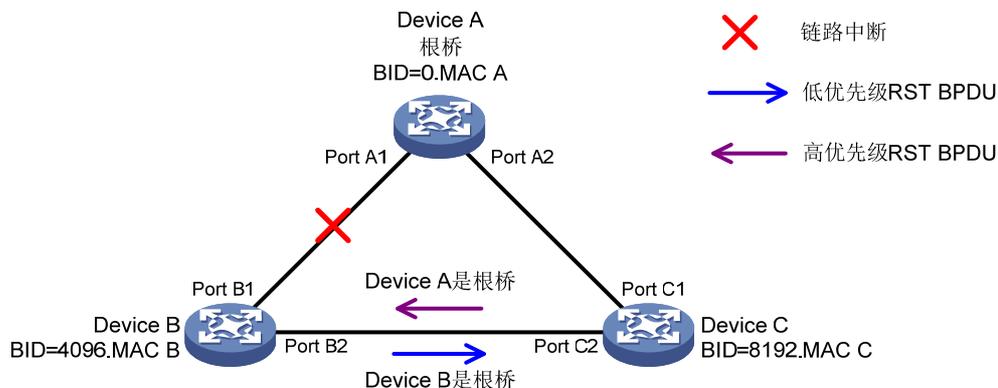
由于 RSTP 中网桥可以自行从指定端口发送 RST BPDU,所以在网桥之间可以提供一种保活机制,即在一定时间内网桥没有收到对端网桥发送的 RST BPDU,即可认为和对端网桥的连接中断。

RSTP 规定,若在三个连续的 Hello Time 时间内网桥没有收到对端指定桥发送的 RST BPDU,则网桥端口保存的 RST BPDU 老化,认为与对端网桥连接中断。新的老化机制大大加快了拓扑变化的感知,从而可以实现快速收敛。

在 RSTP 中,如果阻塞状态的端口收到低优先级的 RST BPDU,也可以立即对其做出回应。

如 图 1-6, 网络中 Device A 为根桥, Device C 阻塞和 Device B 相连的端口。当 Device B 和根桥之间的链路中断时, Device B 会发送以自己为根桥的 RST BPDU。Device C 收到 Device B 发送的 RST BPDU 后,经过比较, Device B 的值 RST BPDU 为低优先级的 RST BPDU, 所以 Device C 的端口会立即对该 RST BPDU 做出回应, 发送优先级更高的 RST BPDU。Device B 收到 Device C 发送的 RST BPDU 后,将会停止发送 RST BPDU, 并将和 Device C 连接的端口确定为根端口。

图1-6 RSTP 对低优先级 RST BPDU 的处理



## 1.3 PVST简介

STP 和 RSTP 在局域网内的所有网桥都共享一棵生成树，不能按 VLAN 阻塞冗余链路，所有 VLAN 的报文都沿着一棵生成树进行转发。而 PVST 则可以在每个 VLAN 内都拥有一棵生成树，能够有效地提高链路带宽的利用率。PVST 可以简单理解为在每个 VLAN 上运行一个 RSTP 协议，不同 VLAN 之间的生成树完全独立。

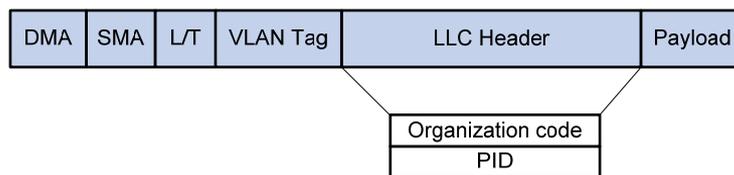
运行 PVST 的 H3C 设备可以与运行 Rapid PVST 或 PVST 的第三方设备互通。当运行 PVST 的 H3C 设备之间互联，或运行 PVST 的 H3C 设备与运行 Rapid PVST 的第三方设备互通时，H3C 设备支持像 RSTP 一样的快速收敛。

### 1.3.1 PVST的协议报文

如 [图 1-7](#)，从报文结构对上看，PVST的BPDU和RSTP的BPDU不同在于以下几点：

- 报文的目的地 MAC 地址改变，变为私有 MAC 地址 01-00-0c-cc-cc-cd。
- 报文携带 VLAN 标签，确定该协议报文归属的 VLAN。
- 报文配置消息固定链路头字段添加 Organization code 和 PID 字段。

图1-7 PVST 报文格式



根据端口类型的不同，PVST 所发送的 BPDU 格式也有所差别：

- 对于 Access 端口，PVST 将根据该 VLAN 的状态发送 RSTP 格式的 BPDU。
- 对于 Trunk 端口和 Hybrid 端口，PVST 将在缺省 VLAN 内根据该 VLAN 的状态发送 RSTP 格式的 BPDU，而对于其他本端口允许通过的 VLAN，则发送 PVST 格式的 BPDU。

### 1.3.2 PVST的工作原理

PVST 借助 MSTP 的实例和 VLAN 映射关系模型，将 MSTP 每个实例映射一个 VLAN。PVST 中每个 VLAN 独立运行 RSTP，独立运算，并允许以每个 VLAN 为基础开启或关闭生成树。每个 VLAN 内的生成树实例都有单独的网络拓扑结构，相互之间没有影响。这样既可以消除了 VLAN 内的冗余环路，还可以实现不同 VLAN 间负载分担。

PVST 在缺省 VLAN 上通过 RSTP 报文进行拓扑运算；在其他 VLAN 上通过带 VLAN Tag 的 PVST 报文进行拓扑运算。

PVST 的端口角色和端口状态和 RSTP 相同，能够实现快速收敛，请参见“[1.2.2 RSTP的基本概念](#)”。

## 1.4 MSTP简介

### 1.4.1 MSTP的优点

MSTP 由 IEEE 制定的 802.1s 标准定义，相比于 STP、RSTP 和 PVST MSTP 的优点如下：

- MSTP 把一个交换网络划分成多个域，每个域内形成多棵生成树，生成树之间彼此独立。生成树间独立计算，实现快速收敛。
- MSTP 通过设置 VLAN 与生成树的对应关系表（即 VLAN 映射表），将 VLAN 与生成树联系起来。并通过“实例”的概念，将多个 VLAN 捆绑到一个实例中，从而达到了节省通信开销和降低资源占用率的目的。
- MSTP 将环路网络修剪成为一个无环的树型网络，避免报文在环路网络中的增生和无限循环，同时还提供了数据转发的多个冗余路径，不同 VLAN 的流量沿各自的路径转发，实现 VLAN 数据的负载分担。
- MSTP 兼容 STP 和 RSTP，部分兼容 PVST。

### 1.4.2 MSTP的协议报文

如 图 1-8，MST BPDU和RST BPDU的前 36 个字节格式是相同的，其中BPDU协议版本号为 0x03，表示MSTP协议，BPDU类型为 0x02，表示为RST/MST BPDU。

图1-8 MSTP 的 BPDU 格式

Parameters	Byte
Protocol ID	2
Protocol Version ID	1
BPDU Type	1
Flags	1
Root ID	8
Root Path Cost	4
Bridge ID	8
Port ID	2
Message Age	2
Max Age	2
Hello Time	2
Forward Delay	2
Version1 Length=0	1
Version3 Length	2
MST Configuration ID	51
CIST IRPC	4
CIST Bridge ID	8
CIST Remaining ID	1
MSTI Configuration Messages	LEN

MSTP专有字段

RST BPDU 中的 Root ID 字段在 MSTP 中表示 CIST（Common and Internal Spanning Tree，公共和内部生成树）总根 ID，Root Path Cost 字段在 MSTP 中表示 CIST 外部路径开销（External Path Cost, EPC），Bridge ID 字段在 MSTP 中表示 CIST 域根 ID，Port ID 字段在 MSTP 中表示 CIST 指定端口 ID。

从第 37 字节开始是 MSTP 的专有字段：

- **Version3 Length:** 表示 MSTP 专有字段长度，该字段用于接收到 BPDU 后进行校验。
- **MST 配置标识(Configuration ID):** 包含格式选择符(Format Selector)、域名(Configuration Name)、修订级别(Revision Level)和配置摘要(Configuration Digest)四个字段。其中格式选择符字段固定为 0x00，其余三个字段用来判断网桥是否属于某 MST 域。
- **CIST 内部路径开销 (Internal Root Path Cost, IRPC):** 表示发送此 BPDU 的网桥到达 CIST 域根的路径开销。
- **CIST Bridge ID:** 表示发送此 BPDU 的网桥 ID。
- **CIST 剩余跳数:** 用来限制 MST 域的规模。从 CIST 域根开始, BPDU 每经过一个网桥的转发, 跳数就被减 1; 网桥将丢弃收到的跳数为 0 的 BPDU, 使出于最大跳数外的网桥无法参与生成树的计算, 从而限制了 MST 域的规模。CIST 剩余跳数默认值为 20。
- **MSTI Configuration Messages:** 包含 0 个或最多 64 个 MSTI(Multiple Spanning Tree Instance, 多生成树实例)配置信息, MSTI 配置信息数量由域内 MST 实例数决定, 每一个 MSTI 配置信息长度为 16 字节。

### 1.4.3 MSTP的基本概念

图1-9 MSTP 的基本概念示意图

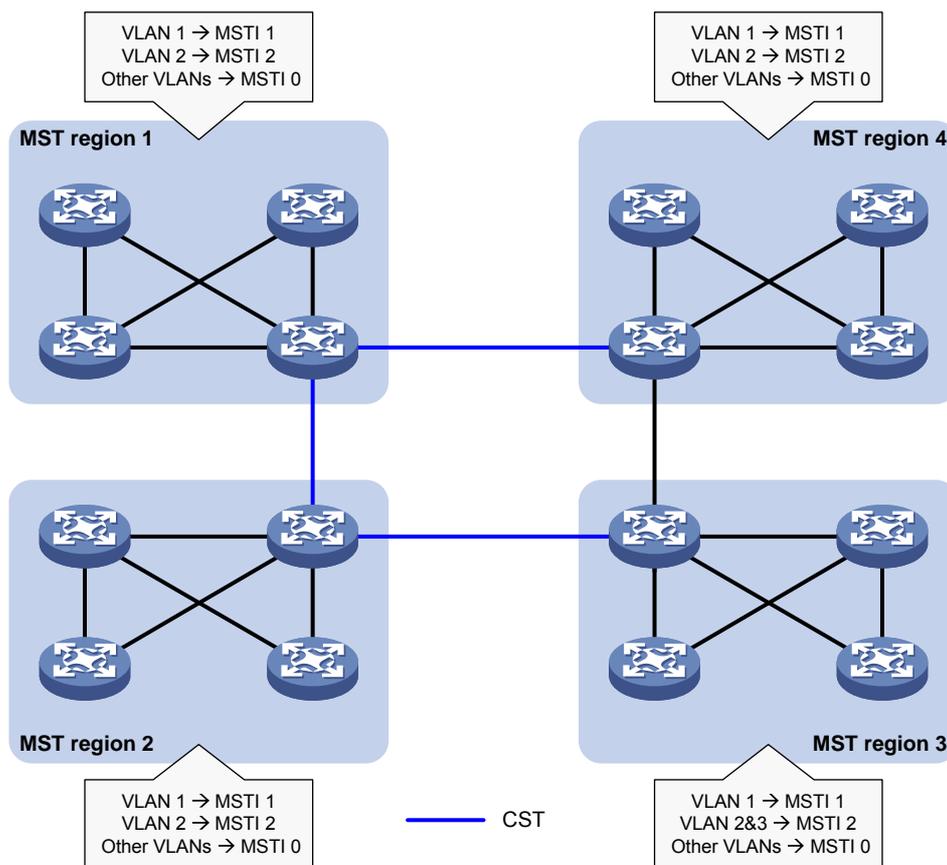
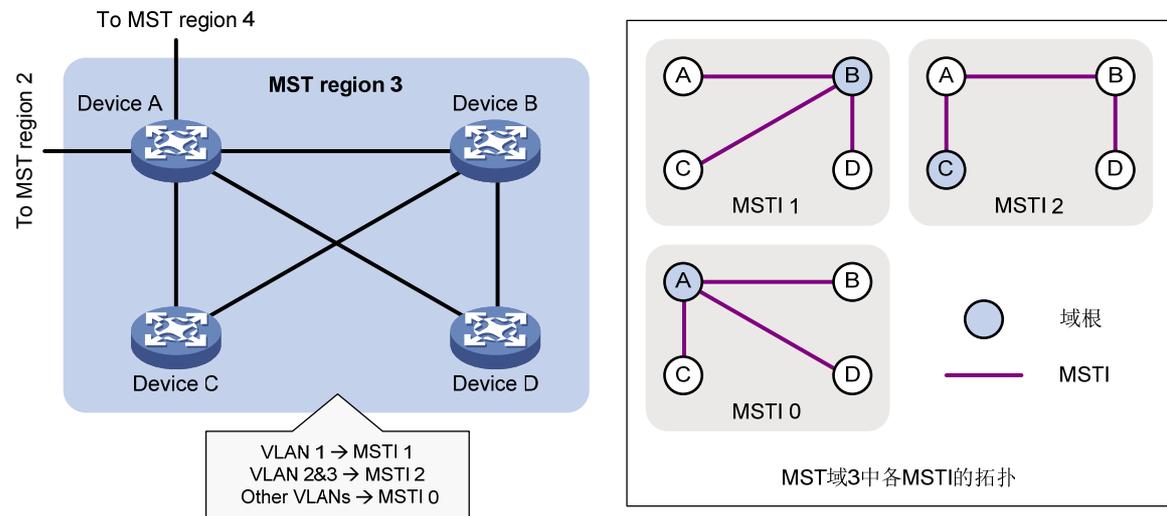


图1-10 MST 域 3 详图



在如 [图 1-9](#) 所示的交换网络中有四个MST域，每个MST域都由四台设备构成，所有设备都运行MSTP；为了看清MST域内的情形，我们以MST域 3 为例放大来看，如 [图 1-10](#) 所示。下面就结合这两张图来介绍一些MSTP中的基本概念：

### 1. MST域

MST 域（Multiple Spanning Tree Regions，多生成树域）是由交换网络中的多台设备以及它们之间的网段所构成。这些设备具有下列特点：

- 都开启了生成树协议。
- 域名相同。
- VLAN 与 MSTI 间映射关系的配置相同。
- MSTP 修订级别的配置相同。
- 这些设备之间有物理链路连通。

一个交换网络中可以存在多个MST域，用户可以通过配置将多台设备划分在一个MST域内。如在 [图 1-9](#) 所示的网络中就有MST域 1~MST域 4 这四个MST域，每个域内的所有设备都具有相同的MST域配置。

### 2. MSTI

一个MST域内可以通过MSTP生成多棵生成树，各生成树之间彼此独立并分别与相应的VLAN对应，每棵生成树都称为一个MSTI（Multiple Spanning Tree Instance，多生成树实例）。如在 [图 1-10](#) 所示的MST域 3 中，包含有三个MSTI：MSTI 1、MSTI 2 和MSTI 0。

### 3. VLAN映射表

VLAN映射表是MST域的一个属性，用来描述VLAN与MSTI间的映射关系。如 [图 1-10](#) 中MST域 3 的VLAN映射表就是：VLAN 1 映射到MSTI 1，VLAN 2 和VLAN 3 映射到MSTI 2，其余VLAN映射到MSTI 0。MSTP就是根据VLAN映射表来实现负载分担的。

#### 4. CST

CST（Common Spanning Tree，公共生成树）是一棵连接交换网络中所有MST域的单生成树。如果把每个MST域都看作一台“设备”，CST就是这些“设备”通过STP协议、RSTP协议计算生成的一棵生成树。如 [图 1-9](#) 中的蓝色线条描绘的就是CST。

#### 5. IST

IST（Internal Spanning Tree，内部生成树）是MST域内的一棵生成树，它是一个特殊的MSTI，通常也称为MSTI 0，所有VLAN缺省都映射到MSTI 0上。如 [图 1-10](#) 中的MSTI 0就是MST域 3 内的IST。

#### 6. CIST

CIST（Common and Internal Spanning Tree，公共和内部生成树）是一棵连接交换网络内所有设备的单生成树，所有MST域的IST再加上CST就共同构成了整个交换网络的一棵完整的单生成树，即CIST。如 [图 1-9](#) 中各MST域内的IST（即MSTI 0）再加上MST域间的CST就构成了整个网络的CIST。

#### 7. 域根

域根（Regional Root）就是MST域内IST或MSTI的根桥。MST域内各生成树的拓扑不同，域根也可能不同。如在 [图 1-10](#) 所示的MST域 3 中，MSTI 1 的域根为Device B，MSTI 2 的域根为Device C，而MSTI 0（即IST）的域根则为Device A。

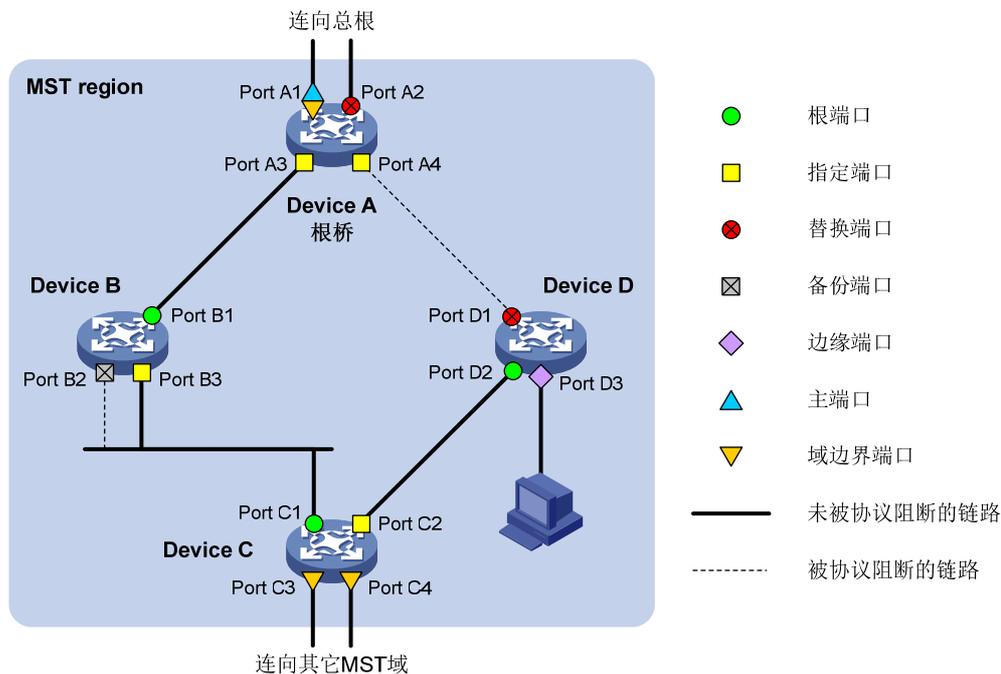
#### 8. 总根

总根（Common Root Bridge）就是CIST的根桥。如 [图 1-9](#) 中CIST的总根就是MST域 1 中的某台设备。

#### 9. 端口角色

端口在不同的MSTI中可以担任不同的角色。如 [图 1-11](#) 所示，在由Device A、Device B、Device C和Device D共同构成的MST域中，Device A的端口Port A1 和Port A2 连向总根方向，Device B的端口Port B2 和Port B3 相连而构成环路，Device C的端口Port C3 和Port C4 连向其他MST域，Device D的端口Port D3 直接连接用户主机。

图1-11 端口角色示意图



如 图 1-11 所示，MSTP 计算过程中涉及到的主要端口角色有以下几种：

- 根端口（Root Port）：在非根桥上负责向根桥方向转发数据的端口就称为根端口，根桥上没有根端口。
- 指定端口（Designated Port）：负责向下游网段或设备转发数据的端口就称为指定端口。
- 替换端口（Alternate Port）：是根端口和主端口的备份端口。当根端口或主端口被阻塞后，替换端口将成为新的根端口或主端口。
- 备份端口（Backup Port）：是指定端口的备份端口。当指定端口失效后，备份端口将转换为新的指定端口。当开启了生成树协议的同一台设备上的两个端口互相连接而形成环路时，设备会将其中一个端口阻塞，该端口就是备份端口。
- 边缘端口（Edge Port）：不与其他设备或网段连接的端口就称为边缘端口，边缘端口一般与用户终端设备直接相连。
- 主端口（Master Port）：是将 MST 域连接到总根的端口（主端口不一定在域根上），位于整个域到总根的最短路径上。主端口是 MST 域中的报文去往总根的必经之路。主端口在 IST/CIST 上的角色是根端口，而在其他 MSTI 上的角色则是主端口。
- 域边界端口（Boundary Port）：是位于 MST 域的边缘、并连接其他 MST 域或 MST 域与运行 STP/RSTP 的区域的端口。主端口同时也是域边界端口。在进行 MSTP 计算时，域边界端口在 MSTI 上的角色与 CIST 的角色一致，但主端口除外——主端口在 CIST 上的角色为根端口，在其他 MSTI 上的角色才是主端口。

## 10. 端口状态

MSTP 中的端口状态可分为三种，如 表 1-8 所示。同一端口在不同的 MSTI 中的端口状态可以不同。

表1-8 MSTP 的端口状态

状态	描述
Forwarding	该状态下的端口可以接收和发送BPDU，也转发用户流量
Learning	是一种过渡状态，该状态下的端口可以接收和发送BPDU，但不转发用户流量
Discarding	该状态下的端口可以接收和发送BPDU，但不转发用户流量

端口状态和端口角色是没有必然联系的，[表 1-9](#) 给出了各种端口角色能够具有的端口状态（“√”表示此端口角色能够具有此端口状态；“-”表示此端口角色不能具有此端口状态）。

表1-9 各种端口角色具有的端口状态

端口角色（右） 端口状态（下）	根端口/主端口	指定端口	替换端口	备份端口
Forwarding	√	√	-	-
Learning	√	√	-	-
Discarding	√	√	√	√

#### 1.4.4 MSTP的工作原理

MSTP 将整个二层网络划分为多个 MST 域，各域之间通过计算生成 CST；域内则通过计算生成多棵生成树，每棵生成树都被称为是一个 MSTI，其中的 MSTI 0 也称为 IST。MSTP 同 STP 一样，使用 BPDU 进行生成树的计算，只是 BPDU 中携带的是设备上 MSTP 的配置信息。

##### 1. CIST生成树的计算

通过比较 BPDU 后，在整个网络中选择一个优先级最高的设备作为 CIST 的根桥。在每个 MST 域内 MSTP 通过计算生成 IST；同时 MSTP 将每个 MST 域作为单台设备对待，通过计算在域间生成 CST。CST 和 IST 构成了整个网络的 CIST。

##### 2. MSTI的计算

在MST域内，MSTP根据VLAN与MSTI的映射关系，针对不同的VLAN生成不同的MSTI。每棵生成树独立进行计算，计算过程与STP计算生成树的过程类似，请参见“[1.1.3 STP的拓扑计算过程](#)”。

MSTP 中，一个 VLAN 报文将沿着如下路径进行转发：

- 在 MST 域内，沿着其对应的 MSTI 转发；
- 在 MST 域间，沿着 CST 转发。

#### 1.4.5 MSTP在设备上的实现

MSTP 同时兼容 STP 和 RSTP。STP 和 RSTP 的协议报文都可以被运行 MSTP 协议的设备识别并应用于生成树计算。设备除了提供 MSTP 的基本功能外，还从用户的角度出发，提供了如下便于管理的特殊功能：

- 根桥保持。
- 根桥备份。

- 根保护功能。
- BPDU 保护功能。
- 环路保护功能。
- 防 TC-BPDU 攻击保护功能。
- 端口角色限制功能。
- TC-BPDU 传播限制功能。

## 1.5 快速收敛机制

在 STP 中，为避免临时环路，端口从开启到进入转发状态需要等待默认 30 秒的时间，如果想要缩短这个时间，只能手工方式将 **Forward Delay** 设置为较小值。但是 **Forward Delay** 是由 **Hello Time** 和网络直径共同决定的一个参数，如果将 **Forward Delay** 设置太小，可能会导致临时环路的产生，影响网络的稳定性。

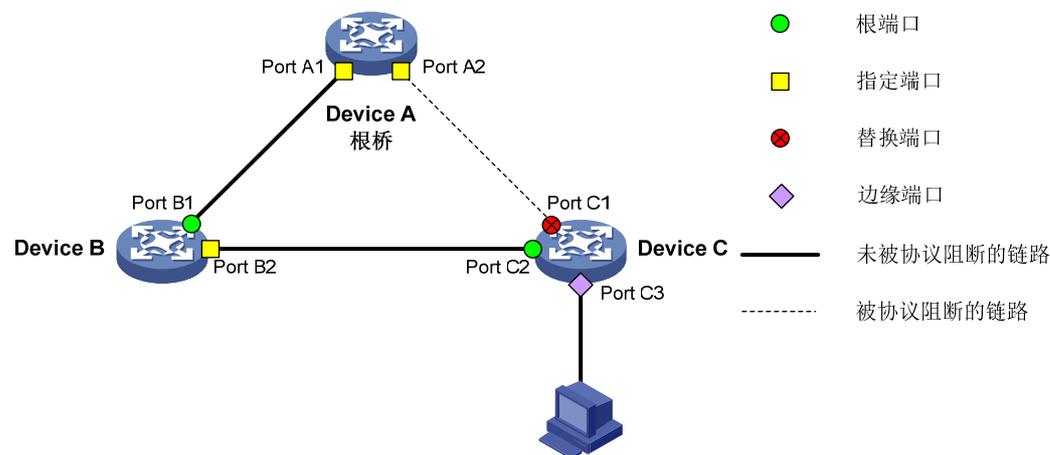
目前，RSTP/PVST/MSTP 都支持快速收敛机制。快速收敛机制包括边缘端口机制、根端口快速切换机制、指定端口快速切换机制。其中指定端口快速切换机制也称为 P/A（Proposal/Agreement，请求/回应）机制。

### 1.5.1 边缘端口机制

当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，该端口即为边缘端口。边缘端口连接的是终端，当网络拓扑变化时，边缘端口不会产生临时环路，所以边缘端口可以略过两个 **Forward Delay** 的时间，直接进入 **Forwarding** 状态，无需任何延时。

由于网桥无法自动判断端口是否直接与终端相连，所以用户需要手工将与端口连接的端口配置为边缘端口。

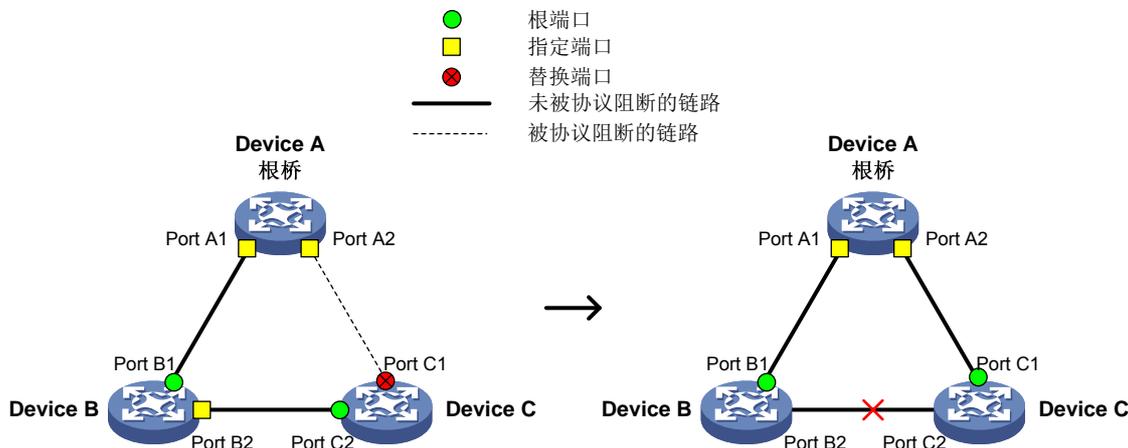
图1-12 边缘端口示意图



### 1.5.2 根端口快速切换机制

当旧的根端口进入阻塞状态，网桥会选择优先级最高的替换端口作为新的根端口，如果当前新根端口连接的对端网桥的指定端口处于 **Forwarding** 状态，则新根端口可以立刻进入 **Forwarding** 状态。

图1-13 根端口快速切换示意图



如 图 1-13，Device C有两个端口，一个为根端口另一个为替换端口，当根端口链路中断时，替换端口会立刻成为新的根端口并进入Forwarding状态，期间不需要延时。

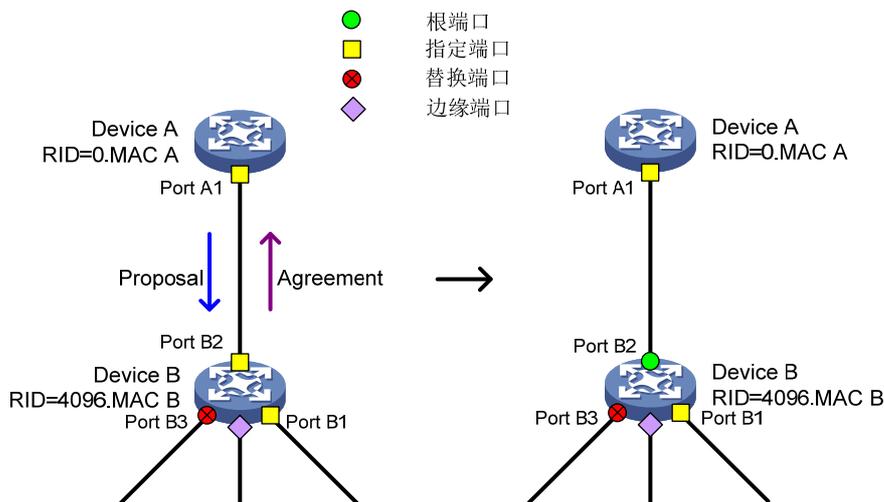
### 1.5.3 P/A机制

P/A 机制是指指定端口可以通过与对端网桥进行一次握手，即可快速进入转发状态，期间不需要任何定时器。P/A 机制的前提条件是：握手必须在点到点链路上进行。有点到点链路作为前提，P/A 机制可以实现网络拓扑的逐链路收敛，而不必像 STP，需要被动等待 30 秒的时间以确保全网实现收敛。

#### 1. RSTP/PVST的P/A机制

当新链路连接或故障链路恢复时，链路两端的端口初始都为指定端口并处于阻塞状态。当指定端口处于 Discarding 状态和 Learning 状态，其所发送的 BPDU 中 Proposal 位将被置位，端口角色为指定端口。收到 Proposal 置位的 BPDU 后，网桥会判断接收端口是否为根端口，如果是，网桥会启动同步过程。同步过程指网桥阻塞除边缘端口之外的所有端口，在本网桥层面消除环路产生的可能。

图1-14 RSTP/PVST 的 P/A 机制实现快速收敛



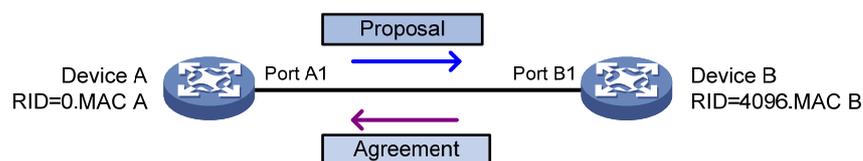
如 图 1-14，当 Device A 和 Device B 之间的链路连接后，P/A 机制处理过程如下：

- Device A 从端口 Port A1 发送 Proposal 置位的 BPDUs 给 Device B。
- Device B 收到 Proposal BPDUs 后，判断端口 Port B2 为根端口，启动同步过程阻塞指定端口 Port B1 和替换端口 Port B3 避免环路产生，然后将根端口 Port B2 设置为转发状态，并向 Device A 回复 Agreement BPDUs。
- Device A 收到 Agreement BPDUs 后，指定端口 Port A1 立即进入转发状态。
- Device A 的端口 Port A1 和 Device B 的端口 Port B2 均进入转发状态，P/A 收敛过程结束。

## 2. MSTP 的 P/A 机制

在 MSTP 中，上游网桥发送的 Proposal BPDUs 中的 Proposal 位和 Agreement 位均置位，下游网桥收到 Proposal 位和 Agreement 位均置位的 BPDUs 后，执行同步操作然后回应 Agreement 置位的 BPDUs，使得上游指定端口快速进入转发状态。

图 1-15 MSTP 的 P/A 机制实现快速收敛



如 图 1-15，Device A 和 Device B 之间的 P/A 机制处理过程如下：

- Device A 从端口 Port A1 发送 Proposal 位和 Agreement 位均置位的 BPDUs 给 Device B。
- Device B 收到 Proposal 位和 Agreement 位均置位的 BPDUs 后，判断端口 Port B1 为根端口，执行同步操作然后将根端口 Port B1 设置为转发状态，并向 Device A 回复 Agreement BPDUs。
- Device A 收到 Agreement BPDUs 后，指定端口 Port A1 立即进入转发状态。
- Device A 的端口 Port A1 和 Device B 的端口 Port B1 均进入转发状态，P/A 收敛过程结束。

从 RSTP/PVST 和 MSTP 的 P/A 机制处理过程可以看到，P/A 机制没有依赖任何定时器，可以实现快速的收敛。

需要注意的是，如果指定端口发出的 Proposal BPDUs 后没有收到 Agreement BPDUs，则该端口将切换到 STP 方式，需要等待 30 秒时间才能进入转发状态。

## 1.6 协议规范

与生成树相关的协议规范有：

- IEEE 802.1D: Media Access Control (MAC) Bridges
- IEEE 802.1w: Part 3: Media Access Control (MAC) Bridges—Amendment 2: Rapid Reconfiguration
- IEEE 802.1s: Virtual Bridged Local Area Networks—Amendment 3: Multiple Spanning Trees
- IEEE 802.1Q-REV/D1.3: Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks—Clause 13: Spanning tree Protocols

# 2 配置生成树协议

## 2.1 生成树协议配置限制和指导

### 2.1.1 与其他功能之间的配置限制和指导

当同时开启 MVRP（Multiple VLAN Registration Protocol，多 VLAN 注册协议）和生成树协议时，MVRP 报文将沿 MSTI 传播。因此当同时开启了 MVRP 和生成树协议时，如果希望通过 MVRP 在网络中发布某个 VLAN，则配置生成树协议的 VLAN 映射表时要保证将该 VLAN 映射到 MSTI 上。有关 MVRP 的详细介绍，请参见“二层技术-以太网交换配置指导”中的“MVRP”。

生成树协议与以下功能互斥：RRPP 功能、Smart Link 功能和 L2PT 功能。

### 2.1.2 接口相关配置限制和指导

生成树的部分功能支持在二层以太网接口视图和二层聚合接口视图配置，本文后续将概括称为接口视图。BPDU 拦截功能只支持在二层以太网接口视图下配置。

系统视图下的配置全局生效；二层以太网接口视图下的配置只对当前端口生效；二层聚合接口视图下的配置只对当前接口生效；聚合成员端口上的配置，只有当成员端口退出聚合组后才能生效。

在二层聚合接口上开启生成树协议后，生成树的相关计算只在二层聚合接口上进行，聚合成员端口不再参与生成树计算。二层聚合接口的所有选中成员端口上生成树协议的开启/关闭状态以及端口转发状态与二层聚合接口保持一致。尽管聚合成员端口不参与生成树计算，但端口上的生成树相关配置仍然保留，当端口退出聚合组时，该端口将采用这些配置参与生成树计算。

## 2.2 生成树协议配置任务简介

### 2.2.1 STP配置任务简介

#### 1. 配置根桥

STP 模式下，根桥上的配置任务如下：

- (1) [配置生成树的工作模式](#)  
通过本配置将生成树的工作模式配置为 STP 模式。
- (2) （可选）[配置根桥和备份根桥](#)
- (3) （可选）[配置设备的优先级](#)
- (4) （可选）配置影响 STP 拓扑收敛的参数
  - [配置交换网络的网络直径](#)
  - [配置生成树的时间参数](#)
  - [配置超时时间因子](#)
  - [配置端口发送BPDU的速率](#)
- (5) （可选）[打开端口状态变化信息显示开关](#)
- (6) [开启生成树协议](#)

- (7) (可选) 配置生成树高级功能
  - [配置TC Snooping功能](#)
  - [配置生成树保护功能](#)
  - [配置被BPDU保护功能关闭的端口不再自动恢复](#)
  - [配置生成树的网管功能](#)

## 2. 配置叶子节点

STP 模式下，叶子节点上的配置任务如下：

- (1) [配置生成树的工作模式](#)

通过本配置将生成树的工作模式配置为 STP 模式。
- (2) (可选) [配置设备的优先级](#)
- (3) (可选) 配置影响 STP 拓扑收敛的参数
  - [配置超时时间因子](#)
  - [配置端口发送BPDU的速率](#)
  - [配置端口的路径开销](#)
  - [配置端口的优先级](#)
- (4) (可选) [打开端口状态变化信息显示开关](#)
- (5) [开启生成树协议](#)
- (6) (可选) 配置生成树高级功能
  - [配置TC Snooping功能](#)
  - [配置生成树保护功能](#)
  - [配置被BPDU保护功能关闭的端口不再自动恢复](#)
  - [配置生成树的网管功能](#)

## 2.2.2 RSTP配置任务简介

### 1. 配置根桥

RSTP 模式下，根桥上的配置任务如下：

- (1) [配置生成树的工作模式](#)

通过本配置将生成树的工作模式配置为 RSTP 模式。
- (2) (可选) [配置根桥和备份根桥](#)
- (3) (可选) [配置设备的优先级](#)
- (4) (可选) 配置影响 RSTP 拓扑收敛的参数
  - [配置交换网络的网络直径](#)
  - [配置生成树的时间参数](#)
  - [配置超时时间因子](#)
  - [配置端口发送BPDU的速率](#)
  - [配置端口为边缘端口](#)
  - [配置端口的链路类型](#)
- (5) (可选) [打开端口状态变化信息显示开关](#)

- (6) [开启生成树协议](#)
- (7) (可选) 配置生成树高级功能
  - [执行mCheck操作](#)
  - [配置TC Snooping功能](#)
  - [配置生成树保护功能](#)
  - [配置被BPDU保护功能关闭的端口不再自动恢复](#)
  - [配置生成树的网管功能](#)

## 2. 配置叶子节点

RSTP 模式下，叶子节点上的配置任务如下：

- (1) [配置生成树的工作模式](#)

通过本配置将生成树的工作模式配置为 RSTP 模式。
- (2) (可选) [配置设备的优先级](#)
- (3) (可选) 配置影响 RSTP 拓扑收敛的参数
  - [配置超时时间因子](#)
  - [配置端口发送BPDU的速率](#)
  - [配置端口为边缘端口](#)
  - [配置端口的路径开销](#)
  - [配置端口的优先级](#)
  - [配置端口的链路类型](#)
- (4) (可选) [打开端口状态变化信息显示开关](#)
- (5) [开启生成树协议](#)
- (6) (可选) 配置生成树高级功能
  - [执行mCheck操作](#)
  - [配置TC Snooping功能](#)
  - [配置生成树保护功能](#)
  - [配置被BPDU保护功能关闭的端口不再自动恢复](#)
  - [配置生成树的网管功能](#)

### 2.2.3 PVST配置任务简介

#### 1. 配置根桥

PVST 模式下，根桥上的配置任务如下：

- (1) [配置生成树的工作模式](#)

通过本配置将生成树的工作模式配置为 PVST 模式。
- (2) (可选) [配置根桥和备份根桥](#)
- (3) (可选) [配置设备的优先级](#)
- (4) (可选) 配置影响 PVST 拓扑收敛的参数
  - [配置交换网络的网络直径](#)
  - [配置生成树的时间参数](#)

- [配置超时时间因子](#)
- [配置端口发送BPDU的速率](#)
- [配置端口为边缘端口](#)
- [配置端口的链路类型](#)
- (5) (可选) [打开端口状态变化信息显示开关](#)
- (6) [开启生成树协议](#)
- (7) (可选) 配置生成树高级功能
  - [执行mCheck操作](#)
  - [关闭PVST的PVID不一致保护功能](#)
  - [配置生成树保护功能](#)
  - [配置在PVST模式下设备检测或接收到TC报文时打印日志信息](#)
  - [配置被BPDU保护功能关闭的端口不再自动恢复](#)
  - [配置生成树的网管功能](#)

## 2. 配置叶子节点

PVST 模式下，叶子节点上的配置任务如下：

- (1) [配置生成树的工作模式](#)  
通过本配置将生成树的工作模式配置为 PVST 模式。
- (2) (可选) [配置设备的优先级](#)
- (3) (可选) 配置影响 PVST 拓扑收敛的参数
  - [配置超时时间因子](#)
  - [配置端口发送BPDU的速率](#)
  - [配置端口为边缘端口](#)
  - [配置端口的路径开销](#)
  - [配置端口的优先级](#)
  - [配置端口的链路类型](#)
- (4) (可选) [打开端口状态变化信息显示开关](#)
- (5) [开启生成树协议](#)
- (6) (可选) 配置生成树高级功能
  - [执行mCheck操作](#)
  - [关闭PVST的PVID不一致保护功能](#)
  - [配置生成树保护功能](#)
  - [配置在PVST模式下设备检测或接收到TC报文时打印日志信息](#)
  - [配置被BPDU保护功能关闭的端口不再自动恢复](#)
  - [配置生成树的网管功能](#)

## 2.2.4 MSTP配置任务简介

### 1. 配置根桥

MSTP 模式下，根桥上的配置任务如下：

- (1) [配置生成树的工作模式](#)  
通过本配置将生成树的工作模式配置为 MSTP 模式。
- (2) [配置MST域](#)
- (3) (可选) [配置根桥和备份根桥](#)
- (4) (可选) [配置设备的优先级](#)
- (5) (可选) 配置影响 MSTP 拓扑收敛的参数
  - [配置MST域的最大跳数](#)
  - [配置交换网络的网络直径](#)
  - [配置生成树的时间参数](#)
  - [配置超时时间因子](#)
  - [配置端口发送BPDU的速率](#)
  - [配置端口为边缘端口](#)
  - [配置端口的链路类型](#)
- (6) (可选) [配置端口收发的MSTP报文格式](#)
- (7) (可选) [打开端口状态变化信息显示开关](#)
- (8) [开启生成树协议](#)
- (9) (可选) 配置生成树高级功能
  - [执行mCheck操作](#)
  - [配置摘要侦听功能](#)
  - [配置No Agreement Check功能](#)
  - [配置TC Snooping功能](#)
  - [配置生成树保护功能](#)
  - [配置被BPDU保护功能关闭的端口不再自动恢复](#)
  - [配置生成树的网管功能](#)

## 2. 配置叶子节点

MSTP 模式下，叶子节点上的配置任务如下：

- (1) [配置生成树的工作模式](#)  
通过本配置将生成树的工作模式配置为 MSTP 模式。
- (2) [配置MST域](#)
- (3) (可选) [配置设备的优先级](#)
- (4) (可选) 配置影响 MSTP 拓扑收敛的参数
  - [配置超时时间因子](#)
  - [配置端口发送BPDU的速率](#)
  - [配置端口为边缘端口](#)
  - [配置端口的路径开销](#)
  - [配置端口的优先级](#)
  - [配置端口的链路类型](#)
- (5) (可选) [配置端口收发的MSTP报文格式](#)

- (6) (可选) [打开端口状态变化信息显示开关](#)
- (7) [开启生成树协议](#)
- (8) (可选) 配置生成树高级功能
  - [执行mCheck操作](#)
  - [配置摘要侦听功能](#)
  - [配置No Agreement Check功能](#)
  - [配置TC Snooping功能](#)
  - [配置生成树保护功能](#)
  - [配置被BPDU保护功能关闭的端口不再自动恢复](#)
  - [配置生成树的网管功能](#)

## 2.3 配置生成树的工作模式

### 1. 功能简介

生成树的工作模式有以下几种：

- STP 模式：设备的所有端口都将向外发送 STP BPDU。如果端口的对端设备只支持 STP，可选择此模式。
- RSTP 模式：设备的所有端口都向外发送 RSTP BPDU。当端口收到对端设备发来的 STP BPDU 时，会自动迁移到 STP 模式；如果收到的是 MSTP BPDU，则不会进行迁移。
- PVST 模式：设备的所有端口都向外发送 PVST BPDU，每个 VLAN 对应一棵生成树。进行 PVST 组网时，若网络中所有设备的生成树维护量（开启生成树协议的 VLAN 数×开启生成树协议的端口数）达到一定数量，会导致 CPU 负荷过重，不能正常处理报文，引起网络震荡。本系列设备支持的使能生成树协议的 VLAN 数为 128。
- MSTP 模式：设备的所有端口都向外发送 MSTP BPDU。当端口收到对端设备发来的 STP BPDU 时，会自动迁移到 STP 模式；如果收到的是 RSTP BPDU，则不会进行迁移。

### 2. 配置限制和指导

MSTP 模式兼容 RSTP 模式，RSTP 模式兼容 STP 模式，PVST 模式与其他模式的兼容性如下：

- 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. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置生成树的工作模式。

```
stp mode { mstp | pvst | rstp | stp }
```

缺省情况下，生成树的工作模式为 MSTP 模式。

## 2.4 配置MST域

### 1. 功能简介

两台或多台开启了生成树协议的设备若要属于同一个 MST 域，必须同时满足以下两个条件：第一是选择因子（取值为 0，不可配）、域名、修订级别和 VLAN 映射表的配置都相同；第二是这些设备之间的链路相通。

在配置 MST 域的相关参数（特别是 VLAN 映射表）时，会引发生成树的重新计算，从而引起网络拓扑的振荡。为了减少网络振荡，新配置的 MST 域参数并不会马上生效，而是在使用 **active region-configuration** 命令激活，或使用命令 **stp global enable** 全局开启生成树协议后才会生效。

### 2. 配置限制和指导

在 STP/RSTP/PVST 模式下，MST 域的相关配置不会生效。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 MST 域视图。

```
stp region-configuration
```

- (3) 配置 MST 域的域名。

```
region-name name
```

缺省情况下，MST 域的域名为设备的 MAC 地址。

- (4) 配置 VLAN 映射表。请选择其中一项进行配置。

- 将指定 VLAN 映射到指定的 MSTI 上。

```
instance instance-id vlan vlan-id-list
```

- 快速配置 VLAN 映射表。

```
vlan-mapping modulo modulo
```

缺省情况下，所有 VLAN 都映射到 CIST（即 MSTI 0）上。

- (5) 配置 MSTP 的修订级别。

```
revision-level level
```

缺省情况下，MSTP 的修订级别为 0。

- (6) （可选）显示 MST 域的预配置信息。

```
check region-configuration
```

- (7) 激活 MST 域的配置。

```
active region-configuration
```

## 2.5 配置根桥和备份根桥

### 2.5.1 配置限制和指导

生成树协议可以根据桥 ID 自动计算确定生成树的根桥，也可以手工将设备配置为指定生成树的根桥或备份根桥。手工指定时，需要注意：

- 设备在各生成树中的角色互相独立，在作为一棵生成树的根桥或备份根桥的同时，也可以作为其他生成树的根桥或备份根桥；但在同一棵生成树中，一台设备不能既作为根桥，又作为备份根桥。
- 用户指定根桥后不会再根据设备的优先级选举根桥。当设备一旦被配置为根桥或者备份根桥之后，便不能再修改该设备的优先级。也可以通过配置设备的优先级为 0 来实现将当前设备指定为根桥的目的。有关设备优先级的配置，请参见“[2.6 配置设备的优先级](#)”。

### 2.5.2 配置根桥

(1) 进入系统视图。

```
system-view
```

(2) 配置设备为根桥。

○ STP/RSTP 模式：

```
stp root primary
```

○ PVST 模式：

```
stp vlan vlan-id-list root primary
```

○ MSTP 模式：

```
stp [ instance instance-list ] root primary
```

缺省情况下，设备不是根桥。

### 2.5.3 配置备份根桥

(1) 进入系统视图。

```
system-view
```

(2) 配置设备为备份根桥。

○ STP/RSTP 模式：

```
stp root secondary
```

○ PVST 模式：

```
stp vlan vlan-id-list root secondary
```

○ MSTP 模式：

```
stp [ instance instance-list ] root secondary
```

缺省情况下，设备不是备份根桥。

## 2.6 配置设备的优先级

### 1. 功能简介

设备的优先级参与生成树计算，其大小决定了该设备是否能够被选作生成树的根桥。数值越小表示优先级越高，通过配置较小的优先级，可以达到指定某台设备成为生成树根桥的目的。可以在不同的生成树中为设备配置不同的优先级。如果设备的优先级相同，则 MAC 地址最小的设备将被选择为根。当指定设备为根桥或者备份根桥之后，不允许再修改该设备的优先级。

### 2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 配置设备的优先级。

○ STP/RSTP 模式：

```
stp priority priority
```

○ PVST 模式：

```
stp vlan vlan-id-list priority priority
```

○ MSTP 模式：

```
stp [ instance instance-list ] priority priority
```

缺省情况下，设备的优先级为 32768。

## 2.7 配置MST域的最大跳数

### 1. 功能简介

MST 域的最大跳数限制了 MST 域的规模，在域根上配置的最大跳数将作为该 MST 域的最大跳数。

从 MST 域内的生成树的根桥开始，域内的 BPDU 每经过一台设备的转发，跳数就被减 1；设备将丢弃跳数为 0 的 BPDU，以使处于最大跳数外的设备无法参与生成树的计算，从而限制了 MST 域的规模。

### 2. 配置限制和指导

本配置只需在根桥设备上进行，非根桥设备将采用根桥设备的配置值。

用户可以根据设计的 MST 域内拓扑的层数来配置 MST 域的最大跳数，MST 域的最大跳数要大于 MST 域内拓扑的最大层数。

### 3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 配置 MST 域的最大跳数。

```
stp max-hops hops
```

缺省情况下，MST 域的最大跳数为 20。

## 2.8 配置交换网络的网络直径

### 1. 功能简介

交换网络中任意两台终端设备都通过特定路径彼此相连，这些路径由一系列的设备构成。网络直径就是指对于交换网络中的任意两台网络边缘设备，其中一台经过根桥到达另一台所经过的最大设备数。网络直径越大，说明网络的规模越大。

在 STP/RSTP/MSTP 模式下，每个 MST 域将被视为一台设备，且网络直径配置只对 CIST 有效（即只能在总根上生效），而对 MSTI 无效。在 PVST 模式下，网络直径的配置只能在指定 VLAN 的根桥上生效。

通过本配置，可以根据网络直径调整设备的 Hello Time、Forward Delay 和 Max Age 三个时间参数到合适的值。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置交换网络的网络直径。

- o STP/RSTP/MSTP 模式：

```
stp bridge-diameter diameter
```

- o PVST 模式：

```
stp vlan vlan-id-list bridge-diameter diameter
```

缺省情况下，交换网络的网络直径为 7。

## 2.9 配置生成树的时间参数

### 1. 功能简介

在生成树的计算过程中，用到了以下三个时间参数：

- (1) **Forward Delay**：用于确定状态迁移的延迟时间。为了防止产生临时环路，生成树协议在端口由 Discarding 状态向 Forwarding 状态迁移的过程中设置了 Learning 状态作为过渡，并规定状态迁移需要等待 Forward Delay 时间，以保持与远端的设备状态切换同步。
- (2) **Hello Time**：用于检测链路是否存在故障。生成树协议每隔 Hello Time 时间会发送 BPDU，以确认链路是否存在故障。如果设备在超时时间（超时时间=超时时间因子×3×Hello Time）内没有收到 BPDU，则会由于消息超时而重新计算生成树。
- (3) **Max Age**：用于确定 BPDU 是否超时。在 MSTP 的 CIST 上，设备根据 Max Age 时间来确定端口收到的 BPDU 是否超时。如果端口收到的 BPDU 超时，则需要对该 MSTI 重新计算。Max Age 时间对 MSTP 的 MSTI 无效。

为保证网络拓扑的快速收敛，需要配置合适的时间参数。上述三个时间参数之间应满足以下关系，否则会引起网络的频繁震荡：

- $2 \times (\text{Forward Delay} - 1 \text{ 秒}) \geq \text{Max Age}$
- $\text{Max Age} \geq 2 \times (\text{Hello Time} + 1 \text{ 秒})$

### 2. 配置限制和指导

配置生成树时间参数时，需要注意：

- Forward Delay 的长短与交换网络的网络直径有关。一般来说，网络直径越大，Forward Delay 就应该越长。如果 Forward Delay 过短，可能引入临时的冗余路径；如果 Forward Delay 过长，网络可能较长时间不能恢复连通。建议用户采用自动计算值。
- 合适的 Hello Time 可以保证设备能够及时发现网络中的链路故障，又不会占用过多的网络资源。如果 Hello Time 过长，在链路发生丢包时，设备会误以为链路出现了故障，从而引发设备重新计算生成树；如果 Hello Time 过短，设备将频繁发送重复的 BPDU，增加了设备的负担，浪费了网络资源。建议用户采用自动计算值。
- 如果 Max Age 过短，设备会频繁地计算生成树，而且有可能将网络拥塞误认成链路故障；如果 Max Age 过长，设备很可能不能及时发现链路故障，不能及时重新计算生成树，从而降低网络的自适应能力。建议用户采用自动计算值。

通常情况下，不建议通过手工配置直接调整上述三个时间参数。由于这三个时间参数的取值与网络规模有关，生成树协议会自动根据网络直径计算出这三个时间参数的最优值，因此在网络拓扑变化时，建议在设备上通过执行 **stp bridge-diameter** 命令调整网络直径，使设备自动调整这三个时间参数的值。当网络直径取缺省值时，这三个时间参数也分别取其各自的缺省值。

本配置只需在根桥设备上进行，整个交换网络中的所有设备都将采用根桥设备的配置值。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 Forward Delay 时间参数。

- STP/RSTP/MSTP 模式：

```
stp timer forward-delay time
```

- PVST 模式：

```
stp vlan vlan-id-list timer forward-delay time
```

缺省情况下，Forward Delay 为 15 秒。

- (3) 配置 Hello Time 时间参数。

- STP/RSTP/MSTP 模式：

```
stp timer hello time
```

- PVST 模式：

```
stp vlan vlan-id-list timer hello time
```

缺省情况下，Hello Time 为 2 秒。

- (4) 配置 Max Age 时间参数。

- STP/RSTP/MSTP 模式：

```
stp timer max-age time
```

- PVST 模式：

```
stp vlan vlan-id-list timer max-age time
```

缺省情况下，Max Age 为 20 秒。

## 2.10 配置超时时间因子

### 1. 功能简介

超时时间因子用来确定设备的超时时间： $\text{超时时间} = \text{超时时间因子} \times 3 \times \text{Hello Time}$ 。

当网络拓扑结构稳定后，非根桥设备会每隔 **Hello Time** 时间向周围相连设备转发根桥发出的 **BPDU** 以确认链路是否存在故障。通常如果设备在 9 倍的 **Hello Time** 时间内没有收到上游设备发来的 **BPDU**，就会认为上游设备已经故障，从而重新进行生成树的计算。

### 2. 配置限制和指导

对于以下情况，建议将设备的超时时间因子配置为 5~7。

- 有时本端设备在较长时间内收不到对端设备发来的 **BPDU**，可能是由于对端设备的繁忙导致的（例如，对端设备配置了大量二层接口时），在这种情况下一般不应重新进行生成树的计算，需要延长本端设备的超时时间。
- 稳定的网络中，可以通过延长超时时间来减少网络资源的浪费。

### 3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 配置设备的超时时间因子。

```
stp timer-factor factor
```

缺省情况下，设备的超时时间因子为 3。

## 2.11 配置端口发送BPDU的速率

### 1. 功能简介

每 **Hello Time** 时间内端口能够发送的 **BPDU** 的最大数目 = 端口发送 **BPDU** 的速率 + **Hello Time** 时间值。端口发送 **BPDU** 的速率越高，每个 **Hello Time** 内可发送的 **BPDU** 数量就越多，占用的系统资源也越多。适当配置发送速率一方面可以限制端口发送 **BPDU** 的速度，另一方面还可以防止在网络拓扑动荡时，生成树协议占用过多的带宽资源。

### 2. 配置限制和指导

端口发送 **BPDU** 的速率与端口的物理状态和网络结构有关，建议用户采用缺省配置。

### 3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入接口视图。

```
interface interface-type interface-number
```

(3) 配置端口的发送 **BPDU** 的速率。

```
stp transmit-limit limit
```

缺省情况下，端口发送 **BPDU** 的速率为 10。

## 2.12 配置端口为边缘端口

### 1. 功能简介

当端口直接与用户终端相连，而没有连接到其他设备或共享网段上，则该端口被认为是边缘端口。网络拓扑变化时，边缘端口不会产生临时环路。

由于设备无法知道端口是否直接与终端相连，所以需要用户手工将端口配置为边缘端口。如果用户将某个端口配置为边缘端口，那么当该端口由阻塞状态向转发状态迁移时，这个端口可以实现快速迁移，而无需等待延迟时间。

### 2. 配置限制和指导

对于直接与终端相连的端口，请将该端口设置为边缘端口，同时开启 BPDU 保护功能。这样既能够使该端口快速迁移到转发状态，也可以保证网络的安全。

在同一个端口上，不允许同时配置边缘端口和环路保护功能。

在端口没有开启 BPDU 保护的情况下，如果被设置为边缘端口的端口上收到来自其他端口的 BPDU，则该端口会重新变为非边缘端口。此时，只有重启端口才能将该端口恢复为边缘端口。

### 3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入接口视图。

```
interface interface-type interface-number
```

(3) 配置当前端口为边缘端口。

```
stp edged-port
```

缺省情况下，端口为非边缘端口。

## 2.13 配置端口的路径开销

### 2.13.1 功能简介

路径开销 (Path Cost) 是与端口相连的链路速率相关的参数。在支持生成树协议的设备上，端口在不同的 MSTI 中可以拥有不同的路径开销。设置合适的路径开销可以使不同 VLAN 的流量沿不同的物理链路转发，从而实现按 VLAN 负载分担的功能。

设备可以自动计算端口的缺省路径开销，用户也可以直接配置端口的路径开销。

### 2.13.2 配置缺省路径开销的计算标准

#### 1. 功能简介

缺省路径开销的计算标准有以下三种，用户可以通过本配置来改变设备自动计算端口的缺省路径开销时所采用的计算标准：

- **dot1d-1998**：表示按照 IEEE 802.1D-1998 标准来计算缺省路径开销。
- **dot1t**：表示按照 IEEE 802.1t 标准来计算缺省路径开销。
- **legacy**：表示按照私有标准来计算缺省路径开销。

不同速率链路的路径开销值请参见下列各表。

表2-1 100M 及以下链路速率与端口路径开销值的对应关系表

链路速率	端口类型	端口的路径开销值		
		IEEE 802.1D-1998	IEEE 802.1t	私有标准
0	-	65535	200,000,000	200,000
10Mbps	单个端口	100	2,000,000	2,000
	聚合接口（含两个选中端口）		1,000,000	1,800
	聚合接口（含三个选中端口）		666,666	1,600
	聚合接口（含四个选中端口）		500,000	1,400
100Mbps	单个端口	19	200,000	200
	聚合接口（含两个选中端口）		100,000	180
	聚合接口（含三个选中端口）		66,666	160
	聚合接口（含四个选中端口）		50,000	140

表2-2 1000M 链路速率与端口路径开销值的对应关系表

链路速率	端口类型	端口的路径开销值		
		IEEE 802.1D-1998	IEEE 802.1t	私有标准
1000Mbps	单个端口	4	20,000	20
	聚合接口（含两个选中端口）		10,000	18
	聚合接口（含三个选中端口）		6,666	16
	聚合接口（含四个选中端口）		5,000	14

表2-3 10G 链路速率与端口路径开销值的对应关系表

链路速率	端口类型	端口的路径开销值		
		IEEE 802.1D-1998	IEEE 802.1t	私有标准
10Gbps	单个端口	2	2,000	2
	聚合接口（含两个选中端口）		1,000	1
	聚合接口（含三个选中端口）		666	1
	聚合接口（含四个选中端口）		500	1

## 2. 配置限制和指导

改变缺省路径开销的计算标准，将使端口的路径开销值恢复为缺省值。

在计算聚合接口的路径开销时，IEEE 802.1D-1998 标准不考虑聚合接口所对应聚合组内选中端口的数量；而 IEEE 802.1t 标准则对此予以考虑，其计算公式为：端口的路径开销 =  $200000000 \div$  链路速率（单位为 100Kbps），其中链路速率为聚合接口所对应聚合组内选中端口的速率之和。

### 3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 配置缺省路径开销的计算标准。

```
stp pathcost-standard { dot1d-1998 | dot1t | legacy }
```

缺省情况下，缺省路径开销的计算标准为 legacy。

## 2.13.3 配置端口的路径开销

### 1. 配置限制和指导

当端口的路径开销值改变时，系统将重新计算端口的角色并进行状态迁移。

### 2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入接口视图。

```
interface interface-type interface-number
```

(3) 配置端口的路径开销。

○ STP/RSTP 模式：

```
stp cost cost-value
```

○ PVST 模式：

```
stp vlan vlan-id-list cost cost-value
```

○ MSTP 模式：

```
stp [ instance instance-list ] cost cost-value
```

缺省情况下，自动按照相应的标准计算各生成树上的路径开销。

## 2.14 配置端口的优先级

### 1. 功能简介

端口优先级是确定该端口是否会被选为根端口的重要依据，同等条件下优先级高的端口将被选为根端口。在支持生成树协议的设备上，端口可以在不同的生成树中拥有不同的优先级，同一端口可以在不同的生成树中担任不同的角色，从而使不同 VLAN 的数据沿不同的物理路径传播，实现按 VLAN 进行负载分担的功能。用户可以根据组网的实际需要来设置端口的优先级。

### 2. 配置限制和指导

当端口的优先级改变时，系统将重新计算端口的角色并进行状态迁移，引起网络拓扑变化，请用户做好相关准备工作。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置端口的优先级。

- STP/RSTP 模式:

```
stp port priority priority
```

- PVST 模式:

```
stp vlan vlan-id-list port priority priority
```

- MSTP 模式:

```
stp [ instance instance-list ] port priority priority
```

缺省情况下，端口的优先级为 128。

## 2.15 配置端口的链路类型

### 1. 功能简介

点对点链路是两台设备之间直接连接的链路。与点对点链路相连的两个端口如果为根端口或者指定端口，则端口可以通过传送同步报文（Proposal 报文和 Agreement 报文）快速迁移到转发状态，减少了不必要的转发延迟时间。

### 2. 配置限制和指导

如果某端口是二层聚合接口或其工作在全双工模式下，则可以将该端口配置为与点对点链路相连。通常建议使用缺省配置，由系统进行自动检测。

在 PVST 或 MSTP 模式下，如果某端口被配置为与点对点链路（或非点对点链路）相连，那么该配置对该端口所属的所有 VLAN 或 MSTI 都有效。

如果某端口被配置为与点对点链路相连，但与该端口实际相连的物理链路不是点对点链路，则有可能引入临时环路。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置端口的链路类型。

```
stp point-to-point { auto | force-false | force-true }
```

缺省情况下，端口的链路类型为 **auto**，即由系统自动检测与本端口相连的链路是否为点对点链路。

## 2.16 配置端口收发的MSTP报文格式

### 1. 功能简介

端口可以收发的 MSTP 报文格式有两种：

- **dot1s**：符合 802.1s 协议的标准格式；
- **legacy**：与非标准格式兼容的格式。

端口默认配置为自动识别方式（**auto**），即可以自动识别这两种格式的 MSTP 报文，并根据识别结果确定发送报文的格式，从而实现与对端设备的互通。

用户也可以通过配置改变端口发送的 MSTP 报文格式，使端口只发送与所配格式相符的 MSTP 报文，实现与对端只识别特定格式报文的设备互通。

当端口处于 **auto** 模式时，默认发送 802.1s 标准的报文。在此模式下，为避免因收到不同格式的 MSTP 报文而导致端口发送的报文格式频繁变化，端口一旦收到私有格式报文就将一直以该格式发送报文。若想使该端口恢复发送 802.1s 标准的报文，可对其依次执行关闭/开启操作。

### 2. 配置限制和指导

如果当前配置的 MSTI 大于 48，端口将只发送 802.1s 标准的 MSTP 报文。

### 3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入接口视图。

```
interface interface-type interface-number
```

(3) 配置端口收发的 MSTP 报文格式。

```
stp compliance { auto | dot1s | legacy }
```

缺省情况下，端口会自动识别收到的 MSTP 报文格式并根据识别结果确定发送的报文格式。

## 2.17 打开端口状态变化信息显示开关

### 1. 功能简介

在开启了生成树协议的大型网络中，用户可以通过打开端口状态变化信息显示开关，使系统输出端口状态变化的相关信息，方便用户对端口状态进行实时监控。

### 2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 打开端口状态变化信息显示开关。

○ STP/RSTP 模式：

```
stp port-log instance 0
```

○ PVST 模式：

```
stp port-log vlan vlan-id-list
```

○ MSTP 模式：

```
stp port-log { all | instance instance-list }
```

缺省情况下，端口状态变化信息显示开关处于关闭状态。

## 2.18 开启生成树协议

### 2.18.1 配置限制和指导

只有开启了生成树协议，生成树的其他配置才会生效。在 STP/RSTP/MSTP 模式下，必须保证全局和端口上的生成树协议均处于开启状态；在 PVST 模式下，必须保证全局、VLAN 和端口上的生成树协议均处于开启状态。

可以通过 `undo stp enable` 命令关闭指定端口的生成树协议，使其不参与生成树计算，以节省设备的 CPU 资源。但必须保证指定的端口关闭生成树协议后，网络中不能出现环路。

### 2.18.2 开启生成树协议（STP/RSTP/MSTP模式）

- (1) 进入系统视图。

```
system-view
```

- (2) 全局开启生成树协议。

```
stp global enable
```

空配置启动时，使用软件功能缺省值，全局生成树协议处于关闭状态。

出厂配置启动时，使用软件功能出厂值，全局生成树协议处于开启状态。

关于空配置启动和出厂配置启动的详细介绍，请参见“基础配置指导”中的“配置文件管理”。

- (3) 进入接口视图。

```
interface interface-type interface-number
```

- (4) 在端口上开启生成树协议。

```
stp enable
```

缺省情况下，所有端口上的生成树协议均处于开启状态。

### 2.18.3 开启生成树协议（PVST模式）

- (1) 进入系统视图。

```
system-view
```

- (2) 全局开启生成树协议。

```
stp global enable
```

空配置启动时，使用软件功能缺省值，全局生成树协议处于关闭状态。

出厂配置启动时，使用软件功能出厂值，全局生成树协议处于开启状态。

关于空配置启动和出厂配置启动的详细介绍，请参见“基础配置指导”中的“配置文件管理”。

- (3) 在 VLAN 中开启生成树协议。

```
stp vlan vlan-id-list enable
```

缺省情况下，生成树协议在 VLAN 中处于开启状态。

- (4) 进入接口视图。

```
interface interface-type interface-number
```

- (5) 在端口上开启生成树协议。

```
stp enable
```

缺省情况下，所有端口上的生成树协议均处于开启状态。

## 2.19 执行mCheck操作

### 2.19.1 功能简介

生成树的工作模式有 STP 模式、RSTP 模式、PVST 模式和 MSTP 模式四种。在运行 RSTP、PVST 或 MSTP 的设备上，若某端口连接着运行 STP 协议的设备，该端口收到 STP 报文后会自动迁移到 STP 模式；但当对端运行 STP 协议的设备关机或撤走，而该端口又无法感知的情况下，该端口将无法自动迁移回原有模式，此时需要通过执行 mCheck 操作将其手工迁移回原有模式。

当运行 STP 的设备 A、未开启生成树协议的设备 B 和运行 RSTP/PVST/MSTP 的设备 C 三者顺次相连时，设备 B 将透传 STP 报文，设备 C 上连接设备 B 的端口将迁移到 STP 模式。在设备 B 上开启生成树协议后，若想使设备 B 与设备 C 之间运行 RSTP/PVST/MSTP 协议，除了要在设备 B 上配置生成树的工作模式为 RSTP/PVST/MSTP 外，还要在设备 B 与设备 C 相连的端口上都执行 mCheck 操作。

可以在全局或在端口上执行 mCheck 操作。

### 2.19.2 配置限制和指导

只有当生成树的工作模式为 RSTP 模式、PVST 模式或 MSTP 模式时执行 mCheck 操作才有效。

### 2.19.3 全局执行mCheck操作

- (1) 进入系统视图。

```
system-view
```

- (2) 全局执行 mCheck 操作。

```
stp global mcheck
```

### 2.19.4 在端口上执行mCheck操作

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 在端口上执行 mCheck 操作。

```
stp mcheck
```

## 2.20 关闭PVST的PVID不一致保护功能

### 1. 功能简介

在当链路相连的两端 PVID 不一致时，PVST 的计算可能出现错误，为了防止这样的错误，系统默认会开启 PVID 不一致保护功能，即做 PVID 不一致的检查。若端口 PVID 不一致保护功能触发后，端口在 PVID 不一致的 VLAN 中，会变为阻塞状态。

在某些特定的组网场景中，比如网络中的接入层设备采用同样的配置，其接口 PVID 一致，而网络管理员在汇聚层设备的下行口（即连接接入层设备的接口）上做了不同的 PVID 配置，该配置与接入层设备的上行口（即连接汇聚层设备的接口）的 PVID 配置不一致时，有可能引起生成树的阻塞，为避免这种情况的发生，保持流量的转发，可以关闭 PVID 不一致保护功能。

### 2. 配置限制和指导

关闭 PVST 的 PVID 不一致保护功能后，如果链路两端端口 PVID 不一致，为了避免生成树的计算错误，需要注意：

- 除了缺省 VLAN，本端所在设备不能创建对端 PVID 对应的 VLAN，同样，对端也不能创建本端 PVID 对应的 VLAN。
- 本端端口的链路类型是 Hybrid 时，建议本端所在设备不创建以 Untagged 方式允许通过的 VLAN，同样，对端也不创建本端 Untagged 方式允许通过的 VLAN。
- 建议链路对端设备也关闭 PVST 的 PVID 不一致保护功能。
- 本配置在 PVST 工作模式下才能生效。

### 3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 关闭 PVST 的 PVID 不一致保护功能。

```
stp ignore-pvid-inconsistency
```

缺省情况下，PVST 的 PVID 不一致保护功能处于开启状态。

## 2.21 配置摘要侦听功能

### 1. 功能简介

根据 IEEE 802.1s 规定，只有在 MST 域配置（包括域名、修订级别和 VLAN 映射关系）完全一致的情况下，相连的设备才被认为是在同一个域内。当设备开启了生成树协议以后，设备之间通过识别 BPDU 数据报文内的配置 ID 来判断相连的设备是否与自己处于相同的 MST 域内；配置 ID 包含域名、修订级别、配置摘要等内容，其中配置摘要长 16 字节，是由 HMAC-MD5 算法将 VLAN 与 MSTI 的映射关系加密计算而成。

在网络中，由于一些厂商的设备在对生成树协议的实现上存在差异，即用加密算法计算配置摘要时采用私有的密钥，从而导致即使 MST 域配置相同，不同厂商的设备之间也不能实现在 MST 域内的互通。

通过在我方设备与对生成树协议的实现存在差异的第三方厂商设备相连的端口上开启摘要侦听功能，可以实现我方设备与这些厂商设备在 MST 域内的完全互通。

## 2. 配置限制和指导

摘要侦听功能在端口生效后，由于不再通过配置摘要的比较计算来判断是否在同一个域内，因此需要保证互连设备的域配置中 VLAN 与 MSTI 映射关系的配置相同。

全局开启摘要侦听功能后，如果要修改 VLAN 与 MSTI 间的映射关系，或执行 **undo stp region-configuration** 命令取消当前域配置，均可能因与邻接设备的 VLAN 和 MSTI 映射关系不一致而导致环路或流量中断，因此请谨慎操作。

只有当全局和端口上都开启了摘要侦听功能后，该功能才能生效。开启摘要侦听功能时，建议先在所有与第三方厂商设备相连的端口上开启该功能，再全局开启该功能，以一次性让所有端口的配置生效，从而减少对网络的冲击。

请不要在 MST 域的边界端口上开启摘要侦听功能，否则可能会导致环路。

建议配置完摘要侦听功能后再开启生成树协议。在网络稳定的情况下不要进行摘要侦听功能的配置，以免造成临时的流量中断。

## 3. 配置准备

配置本任务前，请确保生成树协议在我方设备与第三方厂商设备上均正常运行。

## 4. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入接口视图。

```
interface interface-type interface-number
```

(3) 在端口上开启摘要侦听功能。

```
stp config-digest-snooping
```

缺省情况下，端口上的摘要侦听功能处于关闭状态。

(4) 退回系统视图。

```
quit
```

(5) 全局开启摘要侦听功能。

```
stp global config-digest-snooping
```

缺省情况下，摘要侦听功能处于全局关闭状态。

## 2.22 配置No Agreement Check功能

### 1. 功能简介

RSTP 和 MSTP 的指定端口快速迁移机制使用两种协议报文：

- Proposal 报文：指定端口请求快速迁移的报文。
- Agreement 报文：同意对端进行快速迁移的报文。

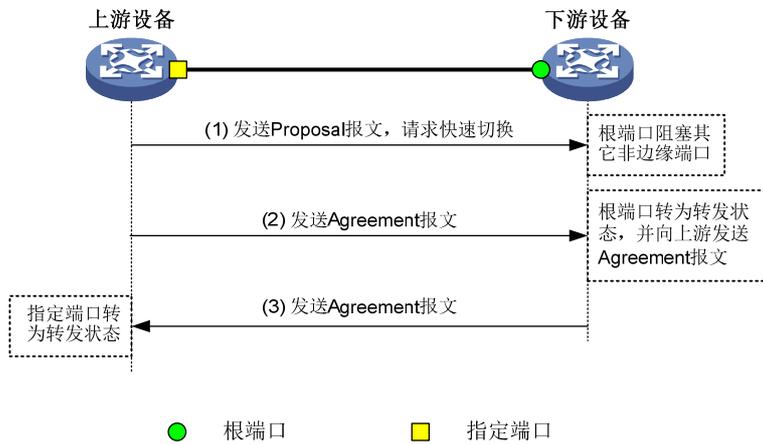
RSTP 和 MSTP 均要求上游设备的指定端口在接收到下游设备的 Agreement 报文后才能进行快速迁移。不同之处如下：

- 对于 MSTP，上游设备先向下游设备发送 Agreement 报文，而下游设备的根端口只有在收到了上游设备的 Agreement 报文后才会向上游设备回应 Agreement 报文。

- 对于 RSTP，下游设备无需等待上游设备发送 Agreement 报文就可向上游设备发送 Agreement 报文。

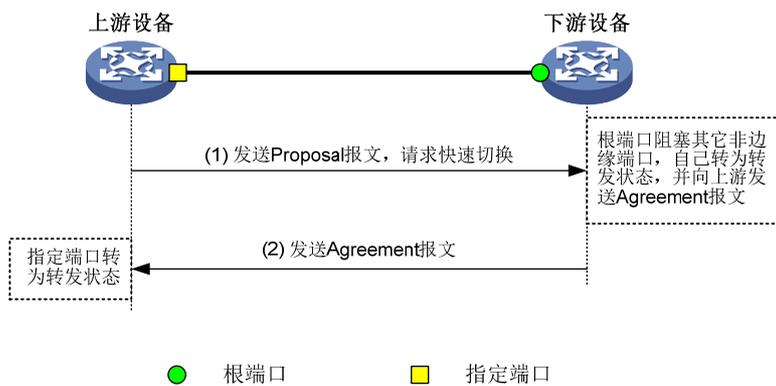
如 图 2-1 所示，是MSTP的指定端口快速迁移机制。

图2-1 MSTP 指定端口快速迁移机制



如 图 2-2 所示，是RSTP的指定端口快速迁移机制。

图2-2 RSTP 指定端口快速迁移机制



当我方设备与作为上游设备且与对生成树协议的实现存在差异的第三方厂商设备互联时，二者在快速迁移的配合上可能会存在一定的限制。例如：上游设备指定端口的状态迁移实现机制与 RSTP 类似；而下游设备运行 MSTP 并且不工作在 RSTP 模式时，由于下游设备的根端口接收不到上游设备的 Agreement 报文，它不会向上游设备发 Agreement 报文，所以上游设备的指定端口无法实现状态的快速迁移，只能在 2 倍的 Forward Delay 延时后变成转发状态。

通过在我方设备与对生成树协议的实现存在私有性差异的上游第三方厂商设备相连的端口上开启 No Agreement Check 功能，可避免这种情况的出现，使得上游的第三方厂商设备的指定端口能够进行状态的快速迁移。

## 2. 配置限制和指导

请在设备的根端口上进行如下配置，且本功能只有在根端口上配置才会生效。

### 3. 配置准备

设备与作为上游设备且支持生成树协议的第三方厂商设备互连，并且端口之间为点对点链路。

为我方设备与第三方厂商设备配置相同的域名、域配置修订级别和 VLAN 与 MSTI 的映射关系，以确保它们在同一个域内。

### 4. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入接口视图。

```
interface interface-type interface-number
```

(3) 开启 No Agreement Check 功能。

```
stp no-agreement-check
```

缺省情况下，No Agreement Check 功能处于关闭状态。

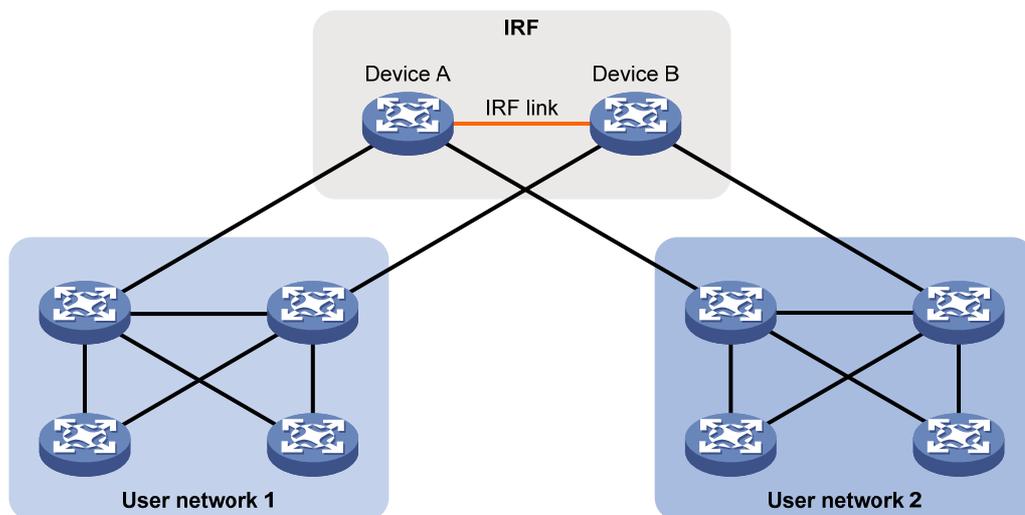
## 2.23 配置TC Snooping功能

### 1. 功能简介

TC Snooping功能的典型应用环境如 [图 2-3](#) 所示。在该组网中，由Device A和Device B组成的IRF设备未开启生成树协议，而用户网络 1 和用户网络 2 中的所有设备均开启了生成树协议。用户网络 1 和用户网络 2 均通过双上行链路与IRF设备相连以提高链路可靠性，IRF设备可以透明传输每个用户网络中的BPDU。

在该组网中，当用户网络的拓扑结构发生改变时，由于 IRF 设备对 BPDU 进行了透明传输而不参与生成树计算，因而其本身可能需经过较长时间才能重新学到正确的 MAC 地址表项和 ARP 表项，在此期间可能导致网络中断。

图2-3 TC Snooping 功能典型应用组网图



为了避免这种情况，可以通过在 IRF 设备上开启 TC Snooping 功能，使其在收到 TC-BPDU（网络拓扑发生变化的通知报文）后，主动更新接收该报文的端口所属的 VLAN 所对应的 MAC 地址表和

ARP 表，从而保证业务流量的正常转发。有关 MAC 地址表和 ARP 表的详细介绍，请分别参见“二层技术-以太网交换配置指导”中的“MAC 地址表”和“三层技术-IP 业务配置指导”中的“ARP”。

## 2. 配置限制和指导

配置 TC Snooping 功能时，需要注意：

- TC Snooping 功能与生成树协议互斥，因此在开启 TC Snooping 功能之前必须全局关闭生成树协议。
- L2PT 功能比 TC Snooping 功能的优先级高，因此若某端口开启了生成树协议的 L2PT 功能，TC Snooping 功能将不会在该端口上生效。
- TC Snooping 功能不支持 PVST 格式的 TC-BPDU，因此在 PVST 模式下不支持该功能。

## 3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 全局关闭生成树协议。

```
undo stp global enable
```

空配置启动时，使用软件功能缺省值，全局生成树协议处于关闭状态。

出厂配置启动时，使用软件功能出厂值，全局生成树协议处于开启状态。

关于空配置启动和出厂配置启动的详细介绍，请参见“基础配置指导”中的“配置文件管理”。

(3) 开启 TC Snooping 功能。

```
stp tc-snooping
```

缺省情况下，TC Snooping 功能处于关闭状态。

## 2.24 配置生成树保护功能

### 2.24.1 生成树保护功能配置任务简介

本节中的所有配置均为可选，请根据实际情况选择配置。

- [配置BPDU保护功能](#)
- [配置根保护功能](#)
- [配置环路保护功能](#)
- [配置端口角色限制功能](#)
- [配置TC-BPDU传播限制功能](#)
- [配置防TC-BPDU攻击保护功能](#)
- [配置BPDU拦截功能](#)
- [配置MSTP的PVST报文保护功能](#)
- [关闭Dispute保护功能](#)

## 2.24.2 配置BPDU保护功能

### 1. 功能简介

对于接入层设备，接入端口一般直接与用户终端（如 PC）或文件服务器相连，此时接入端口被设置为边缘端口以实现这些端口的快速迁移；当这些端口接收到 BPDU 时系统会自动将这些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。这些端口正常情况下应该不会收到 STP 的 BPDU。如果有人伪造 BPDU 恶意攻击设备，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：设备上开启了 BPDU 保护功能后，如果边缘端口收到了 BPDU，系统就将这些端口关闭，同时通知网管这些端口已被生成树协议关闭。被关闭的端口在经过一定时间间隔之后将被重新激活，这个时间间隔可通过 `shutdown-interval` 命令配置。有关该命令的详细介绍，请参见“基础配置命令参考”中的“设备管理”。

### 2. 配置限制和指导

BPDU 保护功能支持在系统视图下配置或在指定端口配置。对于一个端口来说，优先采用该端口的配置，只有该端口内未进行配置时，才采用全局的配置。

配置端口的 BPDU 保护功能时，请在直连用户终端的端口上配置，勿在连接其他设备或共享网段的端口上配置。

BPDU 保护功能对开启了环回测试功能的端口无效。有关环回测试功能的相关介绍，请参见“接口管理配置指导”中的“以太网接口”。

### 3. 系统视图下配置BPDU保护功能

- (1) 进入系统视图。

```
system-view
```

- (2) 开启全局的 BPDU 保护功能。

```
stp bpdu-protection
```

缺省情况下，全局的 BPDU 保护功能处于关闭状态。

### 4. 接口视图下配置BPDU保护功能

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置端口的 BPDU 保护功能。

```
stp port bpdu-protection { enable | disable }
```

缺省情况下，边缘端口的 BPDU 保护功能与全局的 BPDU 保护功能的开关状态保持一致。

## 2.24.3 配置根保护功能

### 1. 功能简介

请在设备的指定端口上配置本功能。

生成树的根桥和备份根桥应该处于同一个域内，特别是对于 CIST 的根桥和备份根桥，网络设计时一般会把 CIST 的根桥和备份根桥放在一个高带宽的核心域内。但是，由于维护人员的错误配置或网络中的恶意攻击，网络中的合法根桥有可能会收到优先级更高的 BPDU，这样当前合法根桥会失

去根桥的地位，引起网络拓扑结构的错误变动。这种不合法的变动，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，导致网络拥塞。

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，其在所有 MSTI 上的端口角色只能为指定端口。一旦该端口收到某 MSTI 优先级更高的 BPDU，立即将该 MSTI 端口设置为侦听状态，不再转发报文（相当于将此端口相连的链路断开）。当在 2 倍的 Forward Delay 时间内没有收到更优的 BPDU 时，端口会恢复原来的正常状态。

## 2. 配置限制和指导

在同一个端口上，不允许同时配置根保护功能和环路保护功能。

## 3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入接口视图。

```
interface interface-type interface-number
```

(3) 开启端口的根保护功能。

```
stp root-protection
```

缺省情况下，端口上的根保护功能处于关闭状态。

## 2.24.4 配置环路保护功能

### 1. 功能简介

请在设备的根端口和替换端口上配置本功能。

依靠不断接收上游设备发送的 BPDU，设备可以维持根端口和其他阻塞端口的状态。但是由于链路拥塞或者单向链路故障，这些端口会收不到上游设备的 BPDU，此时下游设备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，而阻塞端口会迁移到转发状态，从而交换网络中会产生环路。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，其所有 MSTI 的初始状态均为 Discarding 状态：如果该端口收到了 BPDU，这些 MSTI 可以进行正常的状态迁移；否则，这些 MSTI 将一直处于 Discarding 状态以避免环路的产生。

### 2. 配置限制和指导

请不要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 而导致其所有 MSTI 将一直处于 Discarding 状态。

在同一个端口上，不允许同时配置边缘端口和环路保护功能，或者同时配置根保护功能和环路保护功能。

以下端口配置环路保护功能后，该端口不会因收不到 BPDU 而导致其一直处于 Discarding 状态，而是进行端口状态迁移，经过两个 Forward Delay 时长后再次变为 Forwarding 状态：

- 端口状态从 down 变成 up。
- 处于 up 状态的端口，生成树功能状态从关闭变成开启。

### 3. 配置步骤

(1) 进入系统视图。

**system-view**

- (2) 进入接口视图。

**interface** *interface-type interface-number*

- (3) 开启端口的环路保护功能。

**stp loop-protection**

缺省情况下，端口的环路保护功能处于关闭状态。

## 2.24.5 配置端口角色限制功能

### 1. 功能简介

请在与用户接入网络相连的端口上配置本功能。

用户接入网络中设备桥 ID 的变化会引起核心网络生成树拓扑的改变。为了避免这种情况，可以在端口上开启端口角色限制功能，此后当该端口收到最优根消息时将不再当选为根端口，而是成为替换端口。

### 2. 配置限制和指导

开启端口角色限制功能后可能影响生成树拓扑的连通性，请慎重配置。

### 3. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 进入接口视图。

**interface** *interface-type interface-number*

- (3) 开启端口角色限制功能。

**stp role-restriction**

缺省情况下，端口角色限制功能处于关闭状态。

## 2.24.6 配置TC-BPDU传播限制功能

### 1. 功能简介

请在与用户接入网络相连的端口上配置本功能。

用户接入网络的拓扑改变会引起核心网络的转发地址更新，当用户接入网络的拓扑因某种原因而不稳定时，就会对核心网络形成冲击。为了避免这种情况，可以在端口上开启 TC-BPDU 传播限制功能，此后当该端口收到 TC-BPDU 时，不会再向其他端口传播。

### 2. 配置限制和指导

开启 TC-BPDU 传播限制功能后，当拓扑改变时原有转发地址表项可能无法更新，请慎重配置。

### 3. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 进入接口视图。

**interface** *interface-type interface-number*

- (3) 开启 TC-BPDU 传播限制功能。

```
stp tc-restriction
```

缺省情况下，TC-BPDU 传播限制功能处于关闭状态。

## 2.24.7 配置防TC-BPDU攻击保护功能

### 1. 功能简介

设备在收到 TC-BPDU 后，会执行转发地址表项的刷新操作。在有人伪造 TC-BPDU 恶意攻击设备时，设备短时间内会收到很多的 TC-BPDU，频繁的刷新操作给设备带来很大负担，给网络的稳定带来很大隐患。而通过在设备上开启防 TC-BPDU 攻击保护功能，就可以避免转发地址表项的频繁刷新。

当开启了防 TC-BPDU 攻击保护功能后，如果设备在单位时间（固定为十秒）内收到 TC-BPDU 的次数大于 **stp tc-protection threshold** 命令所指定的最高次数（假设为 N 次），那么该设备在这段时间之内将只进行 N 次刷新转发地址表项的操作，而对于超出 N 次的那些 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，这样就可以避免频繁地刷新转发地址表项。

### 2. 配置限制和指导

建议不要关闭防 TC-BPDU 攻击保护功能。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启防 TC-BPDU 攻击保护功能。

```
stp tc-protection
```

缺省情况下，防 TC-BPDU 攻击保护功能处于开启状态。

- (3) （可选）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。

```
stp tc-protection threshold number
```

缺省情况下，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为 6。

## 2.24.8 配置BPDU拦截功能

### 1. 功能简介

在开启了生成树协议的网络中，由于设备收到 BPDU 后会进行 STP 计算并向其他设备转发，因此恶意用户可借此进行 BPDU 攻击：通过不停地发送 BPDU，使网络中的所有设备都不停地进行 STP 计算，从而导致设备的 CPU 占用率过高或 BPDU 的协议状态错误等问题。

为了避免这种情况，用户可以在端口上配置 BPDU 拦截功能。开启了该功能的端口将不再接收任何 BPDU，从而能够防止设备遭受 BPDU 攻击，保证 STP 计算的正确性。

### 2. 配置步骤

- (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) 开启端口的 BPDU 拦截功能。

```
bpdu-drop any
```

缺省情况下，端口的 BPDU 拦截功能处于关闭状态。

## 2.24.9 配置MSTP的PVST报文保护功能

### 1. 功能简介

本配置在 MSTP 工作模式下才能生效。

对于开启 MSTP 的设备，并不识别 PVST 报文，所以开启 MSTP 的设备会将 PVST 报文当做数据报文转发。在另一个并不相干的网络中，开启 PVST 的设备收到该报文，处理后可能导致该网络的拓扑计算出现错误。

对于这个问题，可以通过配置 MSTP 的 PVST 报文保护功能来解决。在 MSTP 模式下，设备上开启了 PVST 报文保护功能后，如果端口收到了 PVST 报文，系统就将这些端口关闭。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 MSTP 的 PVST 报文保护功能。

```
stp pvst-bpdu-protection
```

缺省情况下，MSTP 的 PVST 报文保护功能处于关闭状态。

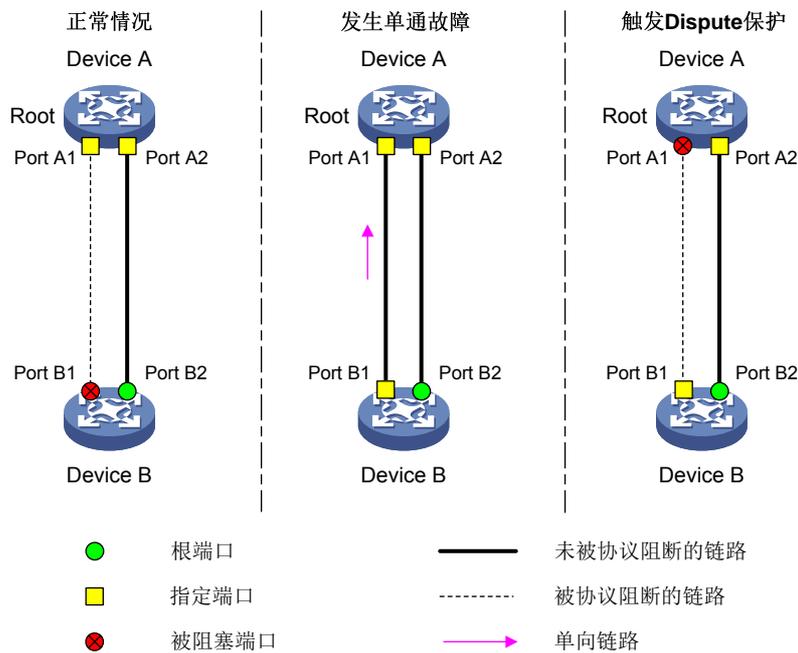
## 2.24.10 关闭Dispute保护功能

### 1. 功能简介

当端口收到指定端口发出的低优先级消息，且发送端口处于 Forwarding 或 Learning 状态时，会触发 Dispute 保护，阻塞端口以防止环路。

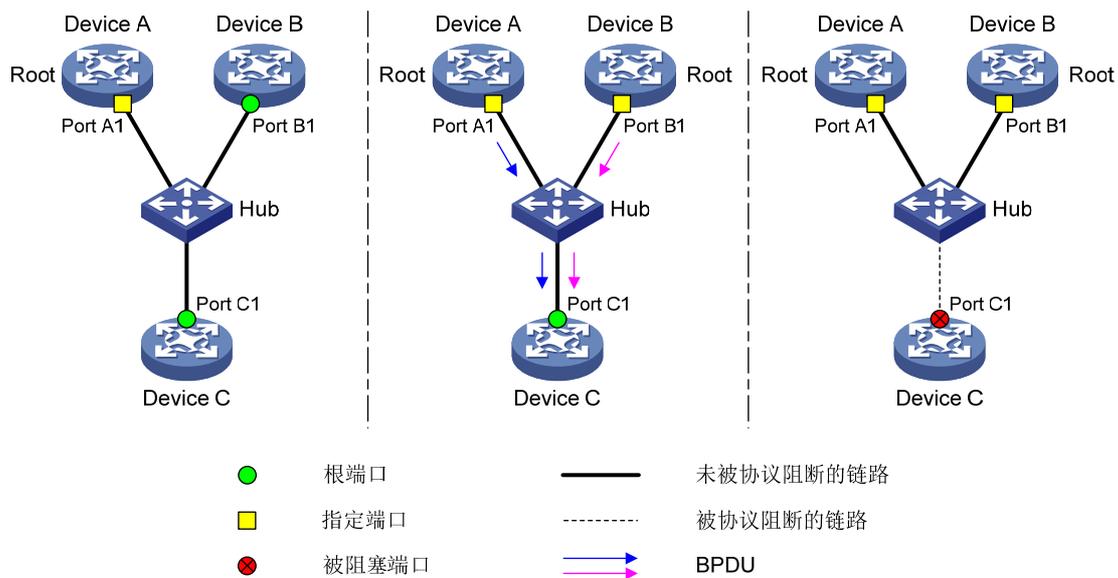
如 [图 2-4](#) 所示，正常情况下，Device A 是根桥，经过生成树计算后，Port B1 被阻塞。如果 Port A1 发生单通故障，即 Port A1 不能发送报文，只能接收报文。Port B1 在一定时间内未收到 Port A1 发送的 BPDU，则 Device B 认为自己是根桥，由 Port B1 发送低优先级 BPDU 到 Port A1。此时，Port A2 和 Port B2 之间链路正常，Device B 会接收到自己发送 BPDU，导致产生环路。因此当链路出现单通故障后，会触发 Dispute 保护功能，阻塞端口，防止环路。

图2-4 Dispute 保护触发场景（指定端口触发）



如 图 2-5 所示，正常情况下，Device A 是根桥，经过生成树计算后，Port B1 和 Port C1 为根端口。如果 Device A 和 Device B 之间出现单通故障，Device B 收不到 Device A 的 BPDUs，则 Device B 认为自己为根桥，Device B 以自己为根桥发送 BPDUs。此时 Device C 收到以 Device A 为根桥的 BPDUs 和以 Device B 为根桥的 BPDUs，则 Device C 认为网络中存在环路，Port C1 触发 Dispute 保护，Port C1 被阻塞。

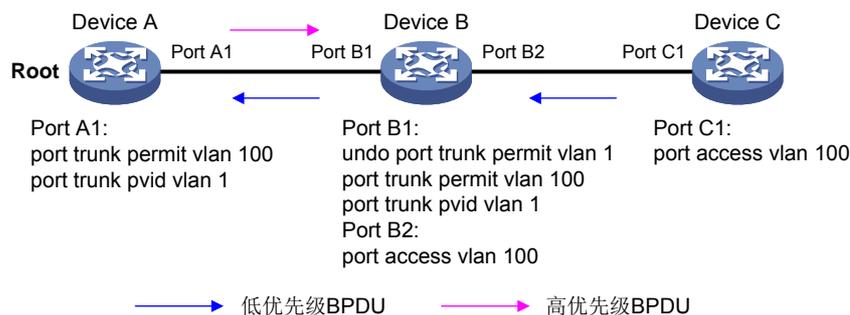
图2-5 Dispute 保护触发场景（根端口触发）



在如 图 2-6 所示的 VLAN 组网的场景中，需要关闭 Dispute 保护功能，防止链路被阻塞。Device A 和 Device C 开启生成树功能，Device B 关闭生成树功能，此时 Device B 会透传 BPDUs。由于 Device B

上Port B1 的配置，导致Device C不能收到根桥Device A发送的VLAN 1 的高优先级BPDU。Device C在一定时间内未收到根桥发送的BPDU，则Device C认为自己是根桥，由Port C1 发送VLAN 100 的低优先级BPDU到Device A。Device A收到低优先级BPDU后，会触发Dispute保护阻塞端口，导致用户业务流量中断。为了保证业务流量正常处理，用户可以关闭Dispute保护功能，避免链路被生成树阻塞而影响用户业务。

图2-6 关闭 Dispute 保护功能使用场景



## 2. 配置限制和指导

如果用户不需要检测链路单通故障，则可以关闭该功能。

## 3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 关闭 Dispute 保护功能。

```
undo stp dispute-protection
```

缺省情况下，Dispute 保护功能处于开启状态。

## 2.25 配置在PVST模式下设备检测或接收到TC报文时打印日志信息

### 1. 功能简介

配置在 PVST 模式下，设备检测或接收到 TC 报文时打印日志信息。

### 2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 配置在 PVST 模式下设备检测或接收到 TC 报文时打印日志信息。

```
stp log enable tc
```

缺省情况下，PVST 模式下设备检测或接收到 TC 报文后，不打印日志信息。

## 2.26 配置被BPDU保护功能关闭的端口不再自动恢复

### 1. 功能简介

设备上使能了 BPDU 保护功能后，如果边缘端口收到了 BPDU，系统就将这些端口关闭，同时通知网管这些端口已被生成树协议关闭。被关闭的端口在经过一定时间间隔之后将被重新激活，这个时

间间隔可通过 **shutdown-interval** 命令配置。有关该命令的详细介绍，请参见“基础配置命令参考”中的“设备管理”。

## 2. 配置限制和指导

配置 **stp port shutdown permanent** 命令后，端口被 BPDU 保护功能关闭，再执行 **undo stp port shutdown permanent** 命令，端口不会 UP，端口保持关闭状态，需要需要执行 **undo shutdown** 命令才能恢复。

端口被 BPDU 保护功能关闭，再配置 **stp port shutdown permanent** 命令，此时端口经过 **shutdown-interval** 命令配置的时间间隔后变为 UP 状态，当再次被生成树保护功能关闭时，端口才不会恢复，保持关闭状态。

## 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置被 BPDU 保护功能关闭的端口不再自动恢复。

```
stp port shutdown permanent
```

缺省情况下，被 BPDU 保护功能关闭的端口会自动恢复。

## 2.27 配置生成树的网管功能

### 1. 功能简介

开启生成树的告警功能之后，生成树会生成告警信息，用于报告本模块的重要事件。生成的告警信息将发送至 SNMP 模块，通过配置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启生成树的告警功能。

```
snmp-agent trap enable stp [ new-root | tc ]
```

缺省情况下，生成树的 new-root 告警功能处于关闭状态。在 MSTP 模式下，生成树的 TC 告警功能在 MSTI 0 中处于开启状态，在其他 MSTI 中处于关闭状态。在 PVST 模式下，生成树的 TC 告警功能在所有 VLAN 中处于关闭状态。

## 2.28 生成树显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令都可以显示配置后生成树的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除生成树的统计信息。

表2-4 生成树显示和维护

操作	命令
显示生成树的状态和统计信息	<code>display stp [ instance instance-list   vlan vlan-id-list ] [ interface interface-list   slot slot-number ] [ brief ]</code>
显示生成树端口角色计算的历史信息	<code>display stp [ instance instance-list   vlan vlan-id-list ] history [ slot slot-number ]</code>
显示生成树所有端口收发的TC或TCN报文数	<code>display stp [ instance instance-list   vlan vlan-id-list ] tc [ slot slot-number ]</code>
显示被生成树保护功能阻塞的端口历史信息	<code>display stp abnormal-port</code>
显示端口上的BPDU统计信息	<code>display stp bpdu-statistics [ interface interface-type interface-number [ instance instance-list ] ]</code>
显示被生成树保护功能down掉的端口信息	<code>display stp down-port</code>
显示生效的MST域配置信息	<code>display stp region-configuration</code>
显示所有生成树的根桥信息	<code>display stp root</code>
清除生成树的统计信息	<code>reset stp [ interface interface-list ]</code>

## 2.29 生成树典型配置举例

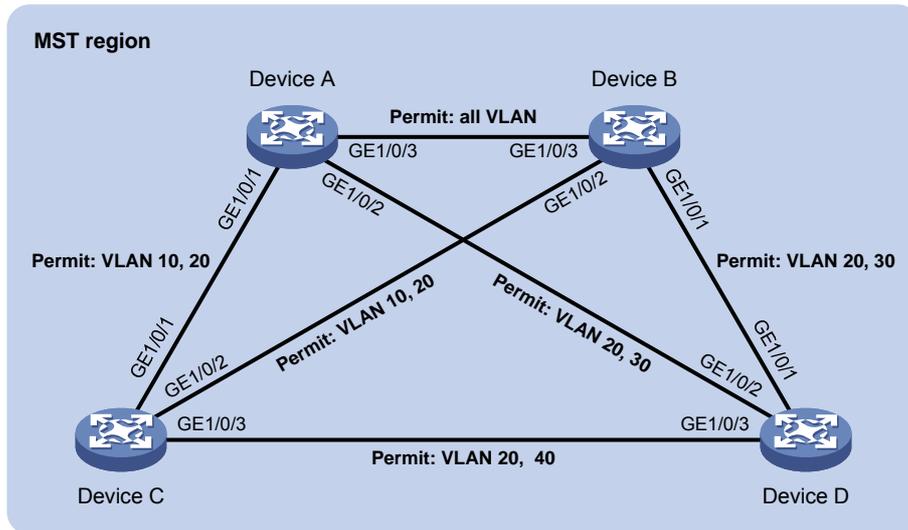
### 2.29.1 MSTP配置举例

#### 1. 组网需求

- 网络中所有设备都属于同一个 MST 域。Device A 和 Device B 为汇聚层设备，Device C 和 Device D 为接入层设备。
- 通过配置 MSTP，使不同 VLAN 的报文按照不同的 MSTI 转发：VLAN 10 的报文沿 MSTI 1 转发，VLAN 30 沿 MSTI 3 转发，VLAN 40 沿 MSTI 4 转发，VLAN 20 沿 MSTI 0 转发。
- 由于 VLAN 10 和 VLAN 30 在汇聚层设备终结、VLAN 40 在接入层设备终结，因此配置 MSTI 1 和 MSTI 3 的根桥分别为 Device A 和 Device B，MSTI 4 的根桥为 Device C。

## 2. 组网图

图2-7 MSTP 典型配置组网图



## 3. 配置步骤

### (1) 配置 VLAN 和端口

请按照 [图 2-7](#) 在 Device A 和 Device B 上分别创建 VLAN 10、20 和 30，在 Device C 上创建 VLAN 10、20 和 40，在 Device D 上创建 VLAN 20、30 和 40；将各设备的各端口配置为 Trunk 端口并允许相应的 VLAN 通过，具体配置过程略。

### (2) 配置 Device A

# 配置 MST 域的域名为 **example**，将 VLAN 10、30、40 分别映射到 MSTI 1、3、4 上，并配置 MSTP 的修订级别为 0。

```
<DeviceA> system-view
[DeviceA] stp region-configuration
[DeviceA-mst-region] region-name example
[DeviceA-mst-region] instance 1 vlan 10
[DeviceA-mst-region] instance 3 vlan 30
[DeviceA-mst-region] instance 4 vlan 40
[DeviceA-mst-region] revision-level 0
# 激活 MST 域的配置。
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
# 配置本设备为 MSTI 1 的根桥。
[DeviceA] stp instance 1 root primary
# 全局开启生成树协议。
[DeviceA] stp global enable
```

### (3) 配置 Device B

# 配置 MST 域的域名为 **example**，将 VLAN 10、30、40 分别映射到 MSTI 1、3、4 上，并配置 MSTP 的修订级别为 0。

```
<DeviceB> system-view
```

```

[DeviceB] stp region-configuration
[DeviceB-mst-region] region-name example
[DeviceB-mst-region] instance 1 vlan 10
[DeviceB-mst-region] instance 3 vlan 30
[DeviceB-mst-region] instance 4 vlan 40
[DeviceB-mst-region] revision-level 0
# 激活 MST 域的配置。
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
# 配置本设备为 MSTI 3 的根桥。
[DeviceB] stp instance 3 root primary
# 全局开启生成树协议。
[DeviceB] stp global enable

```

#### (4) 配置 Device C

# 配置 MST 域的域名为 **example**，将 VLAN 10、30、40 分别映射到 MSTI 1、3、4 上，并配置 MSTP 的修订级别为 0。

```

<DeviceC> system-view
[DeviceC] stp region-configuration
[DeviceC-mst-region] region-name example
[DeviceC-mst-region] instance 1 vlan 10
[DeviceC-mst-region] instance 3 vlan 30
[DeviceC-mst-region] instance 4 vlan 40
[DeviceC-mst-region] revision-level 0
# 激活 MST 域的配置。
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
# 配置本设备为 MSTI 4 的根桥。
[DeviceC] stp instance 4 root primary
# 全局开启生成树协议。
[DeviceC] stp global enable

```

#### (5) 配置 Device D

# 配置 MST 域的域名为 **example**，将 VLAN 10、30、40 分别映射到 MSTI 1、3、4 上，并配置 MSTP 的修订级别为 0。

```

<DeviceD> system-view
[DeviceD] stp region-configuration
[DeviceD-mst-region] region-name example
[DeviceD-mst-region] instance 1 vlan 10
[DeviceD-mst-region] instance 3 vlan 30
[DeviceD-mst-region] instance 4 vlan 40
[DeviceD-mst-region] revision-level 0
# 激活 MST 域的配置。
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
# 全局开启生成树协议。
[DeviceD] stp global enable

```

## 4. 验证配置



说明

在本例中，假定 Device B 的根桥 ID 最小，因此该设备将在 MSTI 0 中被选举为根桥。

当网络拓扑稳定后，通过使用 **display stp brief** 命令可以查看各设备上生成树的简要信息。例如：

# 查看 Device A 上生成树的简要信息。

```
[DeviceA] display stp brief
```

MST ID	Port	Role	STP State	Protection
0	GigabitEthernet1/0/1	ALTE	DISCARDING	NONE
0	GigabitEthernet1/0/2	DESI	FORWARDING	NONE
0	GigabitEthernet1/0/3	ROOT	FORWARDING	NONE
1	GigabitEthernet1/0/1	DESI	FORWARDING	NONE
1	GigabitEthernet1/0/3	DESI	FORWARDING	NONE
3	GigabitEthernet1/0/2	DESI	FORWARDING	NONE
3	GigabitEthernet1/0/3	ROOT	FORWARDING	NONE

# 查看 Device B 上生成树的简要信息。

```
[DeviceB] display 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	DESI	FORWARDING	NONE
1	GigabitEthernet1/0/2	DESI	FORWARDING	NONE
1	GigabitEthernet1/0/3	ROOT	FORWARDING	NONE
3	GigabitEthernet1/0/1	DESI	FORWARDING	NONE
3	GigabitEthernet1/0/3	DESI	FORWARDING	NONE

# 查看 Device C 上生成树的简要信息。

```
[DeviceC] display stp brief
```

MST ID	Port	Role	STP State	Protection
0	GigabitEthernet1/0/1	DESI	FORWARDING	NONE
0	GigabitEthernet1/0/2	ROOT	FORWARDING	NONE
0	GigabitEthernet1/0/3	DESI	FORWARDING	NONE
1	GigabitEthernet1/0/1	ROOT	FORWARDING	NONE
1	GigabitEthernet1/0/2	ALTE	DISCARDING	NONE
4	GigabitEthernet1/0/3	DESI	FORWARDING	NONE

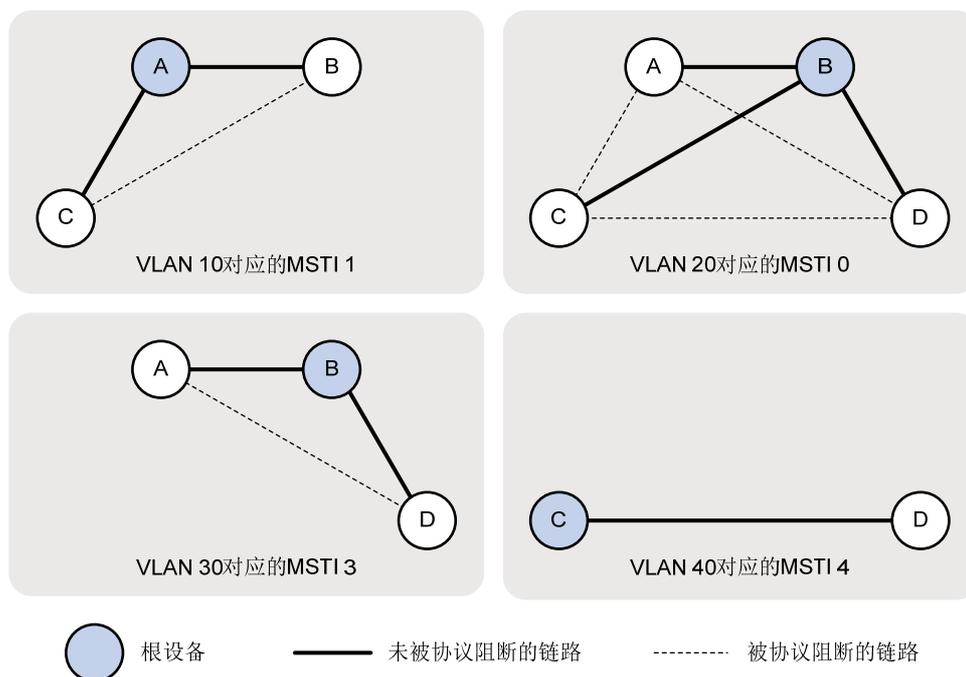
# 查看 Device D 上生成树的简要信息。

```
[DeviceD] display stp brief
```

MST ID	Port	Role	STP State	Protection
0	GigabitEthernet1/0/1	ROOT	FORWARDING	NONE
0	GigabitEthernet1/0/2	ALTE	DISCARDING	NONE
0	GigabitEthernet1/0/3	ALTE	DISCARDING	NONE
3	GigabitEthernet1/0/1	ROOT	FORWARDING	NONE
3	GigabitEthernet1/0/2	ALTE	DISCARDING	NONE

根据上述显示信息，可以绘出各VLAN所对应MSTI的拓扑，如 图 2-8 所示。

图2-8 各 VLAN 所对应 MSTI 的拓扑图



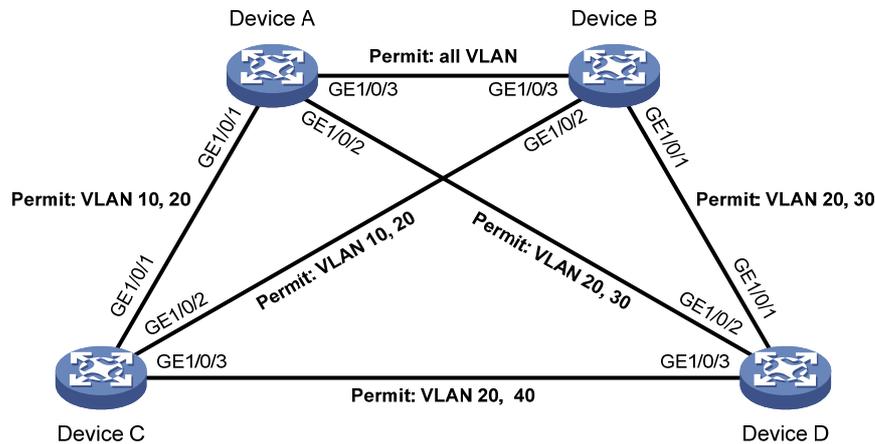
## 2.29.2 PVST配置举例

### 1. 组网需求

- Device A 和 Device B 为汇聚层设备，Device C 和 Device D 为接入层设备。
- 通过配置 PVST，使 VLAN 10、20、30 和 40 中的报文分别按照其各自 VLAN 所对应的生成树转发。
- 由于 VLAN 10、20 和 30 在汇聚层设备终结、VLAN 40 在接入层设备终结，因此配置 VLAN 10 和 20 的根桥为 Device A，VLAN 30 的根桥为 Device B，VLAN 40 的根桥为 Device C。

## 2. 组网图

图2-9 PVST 典型配置组网图



## 3. 配置步骤

### (1) 配置 VLAN 和端口

请按照 图 2-9 在 Device A 和 Device B 上分别创建 VLAN 10、20 和 30，在 Device C 上创建 VLAN 10、20 和 40，在 Device D 上创建 VLAN 20、30 和 40；将各设备的各端口配置为 Trunk 端口并允许相应的 VLAN 通过，具体配置过程略。

### (2) 配置 Device A

# 配置生成树的工作模式为 PVST 模式。

```
<DeviceA> system-view
[DeviceA] stp mode pvst
```

# 配置本设备为 VLAN 10 和 VLAN 20 的根桥。

```
[DeviceA] stp vlan 10 20 root primary
```

# 全局开启生成树协议，并开启 VLAN 10、20 和 30 中的生成树协议。

```
[DeviceA] stp global enable
[DeviceA] stp vlan 10 20 30 enable
```

### (3) 配置 Device B

# 配置生成树的工作模式为 PVST 模式。

```
<DeviceB> system-view
[DeviceB] stp mode pvst
```

# 配置本设备为 VLAN 30 的根桥。

```
[DeviceB] stp vlan 30 root primary
```

# 全局开启生成树协议，并开启 VLAN 10、20 和 30 中的生成树协议。

```
[DeviceB] stp global enable
[DeviceB] stp vlan 10 20 30 enable
```

### (4) 配置 Device C

# 配置生成树的工作模式为 PVST 模式。

```
<DeviceC> system-view
[DeviceC] stp mode pvst
```

# 配置本设备为生成树 VLAN 40 的根桥。

```
[DeviceC] stp vlan 40 root primary
```

# 全局开启生成树协议，并开启 VLAN 10、20 和 40 中的生成树协议。

```
[DeviceC] stp global enable
```

```
[DeviceC] stp vlan 10 20 40 enable
```

#### (5) 配置 Device D

# 配置生成树的工作模式为 PVST 模式。

```
<DeviceD> system-view
```

```
[DeviceD] stp mode pvst
```

# 全局开启生成树协议，并开启 VLAN 20、30 和 40 中的生成树协议。

```
[DeviceD] stp global enable
```

```
[DeviceD] stp vlan 20 30 40 enable
```

### 4. 验证配置

当网络拓扑稳定后，通过使用 **display stp brief** 命令可以查看各设备上生成树的简要信息。

例如：

# 查看 Device A 上生成树的简要信息。

```
[DeviceA] display stp brief
```

VLAN ID	Port	Role	STP State	Protection
10	GigabitEthernet1/0/1	DESI	FORWARDING	NONE
10	GigabitEthernet1/0/3	DESI	FORWARDING	NONE
20	GigabitEthernet1/0/1	DESI	FORWARDING	NONE
20	GigabitEthernet1/0/2	DESI	FORWARDING	NONE
20	GigabitEthernet1/0/3	DESI	FORWARDING	NONE
30	GigabitEthernet1/0/2	DESI	FORWARDING	NONE
30	GigabitEthernet1/0/3	ROOT	FORWARDING	NONE

# 查看 Device B 上生成树的简要信息。

```
[DeviceB] display stp brief
```

VLAN ID	Port	Role	STP State	Protection
10	GigabitEthernet1/0/2	DESI	FORWARDING	NONE
10	GigabitEthernet1/0/3	ROOT	FORWARDING	NONE
20	GigabitEthernet1/0/1	DESI	FORWARDING	NONE
20	GigabitEthernet1/0/2	DESI	FORWARDING	NONE
20	GigabitEthernet1/0/3	ROOT	FORWARDING	NONE
30	GigabitEthernet1/0/1	DESI	FORWARDING	NONE
30	GigabitEthernet1/0/3	DESI	FORWARDING	NONE

# 查看 Device C 上生成树的简要信息。

```
[DeviceC] display stp brief
```

VLAN ID	Port	Role	STP State	Protection
10	GigabitEthernet1/0/1	ROOT	FORWARDING	NONE
10	GigabitEthernet1/0/2	ALTE	DISCARDING	NONE
20	GigabitEthernet1/0/1	ROOT	FORWARDING	NONE
20	GigabitEthernet1/0/2	ALTE	DISCARDING	NONE
20	GigabitEthernet1/0/3	DESI	FORWARDING	NONE
40	GigabitEthernet1/0/3	DESI	FORWARDING	NONE

# 查看 Device D 上生成树的简要信息。

[DeviceD] display stp brief

VLAN ID	Port	Role	STP State	Protection
20	GigabitEthernet1/0/1	ALTE	DISCARDING	NONE
20	GigabitEthernet1/0/2	ROOT	FORWARDING	NONE
20	GigabitEthernet1/0/3	ALTE	DISCARDING	NONE
30	GigabitEthernet1/0/1	ROOT	FORWARDING	NONE
30	GigabitEthernet1/0/2	ALTE	DISCARDING	NONE
40	GigabitEthernet1/0/3	ROOT	FORWARDING	NONE

根据上述显示信息，可以绘出各VLAN所对应生成树的拓扑，如 [图 2-10](#) 所示。

图2-10 各 VLAN 所对应生成树的拓扑图

