二层模块配置

目 录

第 1 章 端口物理特性 1
1.1 配置速率 1
1.2 配置接口流量控制 1
第 2 章 端口保护、安全 2
2.1 端口保护配置任务列表 2
2.2 端口保护配置任务 2
2.2.1 配置/取消端口隔离 2
2.3 端口安全配置任务列表 2
2.4 端口安全配置任务 2
2.4.1 端口绑定 MAC/IP 地址 2
2.4.2 端口过滤 MAC/IP 地址 3
2.4.3 端口静态 MAC 地址允许/拒绝 3
2.4.4 端口动态 MAC 地址限制 4
第 3 章 端口阻塞、风暴控制 5
3.1 端口阻塞配置任务列表 5
3.2 端口阻塞配置任务 5
3.2.1 报文抑制 5
3.3 风暴控制配置任务列表 5
3.4 风暴控制配置任务 5
3.4.1 配置报文流量门限 5
第 4 章 端口镜像 7
4.1 配置端口镜像任务列表 7
4.1.1 配置端口镜像任务 7
第 5 章 配置 MAC 地址 8
5.1 MAC 地址配置任务列表 8
5.2 MAC 地址配置任务 8
5.2.1 配置静态 MAC 地址 8
5.2.2 配置 MAC 地址老化时间 8
5.2.3 显示 MAC 地址表 9
5.2.4 清除动态 MAC 地址 9
第 6 章 配置二层协议隧道 10
6.1 概述 10
6.2 配置二层协议隧道 10
6.3 二层协议隧道配置示例 10
第 7 章 VLAN 配置 11
7.1 VLAN 概述 11

7.2 VLAN 配置任务列表 11
7.3 VLAN 配置任务 12
7.3.1 添加/删除 VLAN 12
7.3.2 配置交换机端口 12
7.3.3 监控 VLAN 的配置和状态 13
第 8 章 配置生成树协议（STP） 14
8.1 STP 概述 14
8.2 SSTP 配置任务列表 15
8.3 SSTP 配置任务 15
8.3.1 选择 STP 模式 15
8.3.2 禁止/启动 STP 15
8.3.3 禁止/启动端口的 STP 16
8.3.4 配置网桥优先级 16
8.3.5 配置 Hello Time 16
8.3.6 配置 Max Age 17
8.3.7 配置 Forward Delay 17
8.3.8 配置端口优先级 17
8.3.9 配置端口路径开销 17
8.3.10 监控 STP 状态 18
8.3.11 配置 SNMP Trap 18
8.4 配置 VLAN 的生成树 18
8.4.1 概述 18
8.4.2 VLAN STP 配置任务 19
8.5 RSTP 配置任务列表 19
8.6 RSTP 配置任务 20
8.6.1 开启/关闭 RSTP 20
8.6.2 配置网桥优先级 20
8.6.3 配置 Forward Time 21
8.6.4 配置 Hello Time 21
8.6.5 配置 Max Age 21
8.6.6 配置端口路径开销 22
8.6.7 配置端口优先级 22
8.6.8 配置边缘端口 23
8.6.9 配置端口连接类型 23
8.6.10 重启协议转换检查 23
8.7 MSTP 简介 24
8.7.1 概述 24
8.7.2 多生成树区域 24
8.7.3 IST, CST, CIST 和 MSTI 24
8.7.4 端口的角色 26
8.7.5 MSTP BPDU 29

8.7.6 稳定状态 30
8.7.7 跳数 31
8.7.8 STP 兼容性 31
8.8 MSTP 配置任务列表 31
8.9 MSTP 配置任务 32
8.9.1 MSTP 默认配置 32
8.9.2 启动和停止多生成树协议 33
8.9.3 配置多生成树区域 33
8.9.4 配置网络根桥 34
8.9.5 配置次要根桥 35
8.9.6 配置网桥优先级 35
8.9.7 配置生成树协议的时间参数 36
8.9.8 配置网络直径 37
8.9.9 配置最大跳数 37
8.9.10 配置端口优先级 37
8.9.11 配置端口路径开销 38
8.9.12 配置边缘端口 38
8.9.13 配置端口连接类型 39
8.9.14 激活多生成树兼容模式 39
8.9.15 重启协议转换检查 40
8.9.16 查看多生成树协议信息 40
8.10 STP 可选特性介绍 41
8.10.1 Port Fast 41
8.10.2 BPDU Guard 42
8.10.3 BPDU Filter 42
8.10.4 Uplink Fast 43
8.10.5 Backbone Fast 44
8.10.6 Root Guard 45
8.10.7 Loop Guard 46
8.11 配置 STP 可选特性 46
8.11.1 STP 可选特性配置任务 46
8.11.2 配置 Port Fast 47
8.11.3 配置 BPDU Guard 47
8.11.4 配置 BPDU Filter 48
8.11.5 配置 Uplink Fast 49
8.11.6 配置 Backbone Fast 49
8.11.7 配置 Root Guard 49
8.11.8 配置 Loop Guard 50
8.11.9 配置 Loop Fast 50
8.11.10 配置地址表老化保护 51
8.11.11 配置 FDB-Flush 51
第 9 章 配置 802.1x 53

9.1 配置 802.1x 任务列表 53
9.2 配置 802.1x 任务 53
9.2.1 配置端口的 802.1x 认证 53
9.2.2 配置 802.1x 多主机端口认证 54
9.2.3 配置 802.1x 身份认证请求的最大次数 54
9.2.4 配置 802.1x 的重认证 55
9.2.5 控制 802.1x 发送频率 55
9.2.6 配置 802.1x 用户绑定 55
9.2.7 配置 802.1x 端口的认证方法 55
9.2.8 选择 802.1x 端口的认证类型 56
9.2.9 802.1x 恢复默认配置 56
9.2.10 监控 802.1x 认证配置和状态 56
9.3 配置 802.1x 示例 56

第 1 章 端口物理特性

1.1 配置速率

以太网的速率既可以通过自协商实现，也可以通过在 interface 下进行配置实现。

命令	作用
Speed {10|100|auto}	设置快速以太网的速率为 10M,100M 或自协商。
No speed	恢复缺省设置，速率为自协商。

缺省时，以太网接口可以自动协商是半双工还是全双工。

命令	作用
duplex {full|half|auto}	设置以太网的双工模式。
No duplex	恢复缺省设置，双工模式为自协商。

1.2 配置接口流量控制

在接口为全双工模式时，流量控制通过 802.3X 定义的 PAUSE 帧实现；在接口为半双工模式时，通过背压实现。

命令	作用
flow-control [on|off]	打开/关闭接口流控。
no flow-control	恢复缺省设置，接口无流控。

第 2 章 端口保护、安全

2.1 端口保护配置任务列表

* 配置/取消端口隔离

2.2 端口保护配置任务

2.2.1 配置/取消端口隔离

在正常情况下，交换机的不同端口间的数据包能够自由的转发。在某些情况下，需要禁止端口之间的数据流，端口隔离功能就是提供这种控制的，设置隔离功能的端口之间不能够再有数据包通信，其它没有隔离的端口之间以及隔离端口和未隔离端口之间的数据包仍然能够正常转发。

命令	目的
configure	进入全局配置模式。
[no] switchport protected	在二层端口的配置模式下配置/取消端口隔离
exit	退回到管理模式。
write	保存配置 。

2.3 端口安全配置任务列表

* 端口绑定 MAC/IP 地址
* 端口过滤 MAC/IP 地址
* 端口静态 MAC 地址允许/拒绝
* 端口动态 MAC 地址限制

2.4 端口安全配置任务

2.4.1 端口绑定 MAC/IP 地址

进入二层端口的配置模式，配置端口绑定 MAC 或 IP 地址，限制只有源地址是指定 MAC 地址或 IP 地址的报文才能通过该端口。

命令	目的

[no] switchport port-security bind mac *mac-addr*	绑定 MAC 地址 mac-addr 为指定的 MAC 地址
[no] switchport port-security bind ip *ip-addr*	绑定 IP 地址 ip-addr 为指定的 IP 地址
[no] switchport port-security bind ip *ip-addr* **mac** *mac-addr*	同时绑定 MAC 地址和 IP 地址 ip-addr 为指定的 IP 地址 mac-addr 为指定的 MAC 地址

2.4.2 端口过滤 MAC/IP 地址

进入二层端口的配置模式，配置端口过滤 MAC 或 IP 地址，限制源地址是指定 MAC 地址或 IP 地址的报文不能通过该端口。

命令	目的
[no] switchport port-security block mac *mac-addr*	过滤 MAC 地址 mac-addr 为指定的 MAC 地址
[no] switchport port-security block ip *ip-addr*	过滤 IP 地址 ip-addr 为指定的 IP 地址
[no] switchport port-security block ip *ip-addr* **mac** *mac-addr*	同时过滤 MAC 地址和 IP 地址 ip-addr 为指定的 IP 地址 mac-addr 为指定的 MAC 地址

2.4.3 端口静态 MAC 地址允许/拒绝

进入二层端口的配置模式，配置安全端口的静态 MAC 地址表，并配置允许或拒绝源 MAC 地址匹配的报文通过该端口。

命令	目的
[no] switchport port-security static mac-address *mac-addr*	配置安全端口的静态 MAC 地址表。 mac-addr 为指定的 MAC 地址
[no] switchport port-security mode static *[accept | reject]*	配置模式为允许或拒绝。 accept 只有源 MAC 地址存在于静态表中的报 文才能通过该端口 reject 源 MAC 地址存在于静态表中的报文拒绝 通过该端口

2.4.4 端口动态 MAC 地址限制

进入二层端口的配置模式，配置安全端口的模式为动态 MAC 地址模式，以及动态 MAC 地址最大数目，则该端口学习到最大数目 MAC 地址后，其余 MAC 的报文将不能通过该端口。安全端口动态模式默认只允许 1 个动态 mac 地址。

命令	目的
[no] switchport port-security dynamic maximum <*number*>	配置安全端口的动态 MAC 地址最大数目。 number 为动态 MAC 地址最大数目
[no] switchport port-security mode dynamic	配置模式为动态模式。

第 3 章 端口阻塞、风暴控制

3.1 端口阻塞配置任务列表

* 抑制广播报文
* 抑制组播报文
* 抑制未知单播报文

3.2 端口阻塞配置任务

3.2.1 报文抑制

在二层端口上启用端口阻塞，可以限制指定类型的报文通过该端口。

命令	目的
[no] switchport block [broadcast | multicast | unicast]	在二层端口的配置模式下配置/取消端口阻塞模式 broadcast 限制广播报文通过该端口 multicast 限制组播报文通过该端口 unicast 限制未知单播报文通过该端口

3.3 风暴控制配置任务列表

* 限制广播报文的流量
* 限制组播报文的流量
* 限制未知单播报文的流量

3.4 风暴控制配置任务

3.4.1 配置报文流量门限

在二层端口上配置风暴控制，限制指定类型的报文通过该端口的最大门限。

命令	目的

[no] storm-control [broadcast | multicast | unicast] **threshold** <number>	在二层端口的配置模式下配置/取消指定类型报文的流量门限 broadcast 配置广播报文的流量门限 multicast 配置组播报文的流量门限 unicast 配置未知单播报文的流量门限 number 流量门限数值

第 4 章 端口镜像

4.1 配置端口镜像任务列表

* 配置端口镜像
* 显示端口镜像信息

4.1.1 配置端口镜像任务

1. 配置端口镜像

为了方便对交换机进行管理，可以通过配置端口镜像，使用交换机某一个端口来对流经一组端口的流量进行观察。

进入特权模式下按下列步骤来配置端口镜像：

命令	目的
configure	进入全局配置模式。
mirror session *session_number* **{destination {interface** *interface-id***} | source {interface** *interface-id* **[, | -] [both | rx | tx] }**	配置端口镜像。 session-number 为端口镜像编号 。 destination 为镜像目的端口 。 source 为镜像源端口 。 both | rx | tx 为要镜像的数据流。rx 表示只镜像输 入数据，tx 表示镜像输出数据，both 表示输入输 出数据。
exit	退回到管理模式。
write	保存配置 。

2. 显示端口镜像信息

通过 show 命令可以显示端口镜像的配置信息。

命令	目的
show mirror [**session** *session_number]*	显示端口镜像信息。session-number 为端口镜像编号。

第 5 章 配置 MAC 地址

5.1 MAC 地址配置任务列表

* 配置静态 MAC 地址
* 配置 MAC 地址老化时间
* 显示 MAC 地址表
* 清除动态 MAC 地址

5.2 MAC 地址配置任务

5.2.1 配置静态 MAC 地址

静态 MAC 地址表项指的是那些不能够被交换机老化掉的 MAC 地址表项，它只能被人工的删除掉。根据交换机使用过程中的实际需要，可以添加和删除静态 MAC 地址。 进入特权模式下按下列步骤来添加和删除一个静态 MAC 地址。

命令	目的
configure	进入全局配置模式
[no] mac address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*	添加/删除一个静态 MAC 地址表项。 mac-addr 为 MAC 地址 ； vlan-id 为 VLAN 号，有效范围 1~4094 ； interface-id 为端口名称。
exit	退回到管理模式。
write	保存配置 。

5.2.2 配置 MAC 地址老化时间

当一个动态的 MAC 地址在指定的老化时间内没有被使用时，交换机将把该 MAC 地址从 MAC 地址表中删除。交换机 MAC 地址的老化时间可以根据需要进行配置，默认的老化时间为 300 秒。

进入特权模式下按下列步骤来配置 MAC 地址的老化时间：

命令	目的
configure	进入全局配置模式。

mac address-table aging-time [**0** | **10-1000000**]	配置 MAC 地址的老化时间。 0 表示 MAC 地址不老化 ； 10－1000000 以秒为单位的 MAC地址老化时间。
exit	退回到管理模式。
write	保存配置 。

5.2.3 显示 MAC 地址表

在使用交换机的过程中，由于调试或管理的需要，我们想要知道交换机 MAC 地址表的内容。通过 show 命令可以把交换机 MAC 地址表的内容显示出来。

命令	目的
show mac address-table {**dynamic** [**interface** interface-id **| vlan** vlan-id] **| static**}	显示 MAC 地址表内容。 dynamic 为动态学习的 MAC 地址； vlan-id 为 VLAN 号，有效范围 1~4094 ； interface-id 为端口名称 ； static 为静态 MAC 地址表；

5.2.4 清除动态 MAC 地址

某些情况下需要清除掉交换机已经学习到的 MAC 地址。

进入特权模式下使用下面的命令删除一个动态 MAC 地址：

命令	目的
clear mac address-table dynamic [address *mac-addr* | **interface** *interface-id* | **vlan** *vlan-id*]	删除一个动态 MAC 地址表项。 dynamic 为动态学习的 MAC 地 址 ； mac-addr 为 MAC 地址 ； interface-id 为端口名称 ； vlan-id 为 VLAN 号，有效范围 1~4094。

第 6 章 配置二层协议隧道

6.1 概述

二层协议隧道允许连接在交换机两端的用户通过交换机透明地在自己的网络中传输指定的二层协议报文，而不受交换机上相应二层协议模块的影响。交换机对用户来说只是一个透明的传输介质。

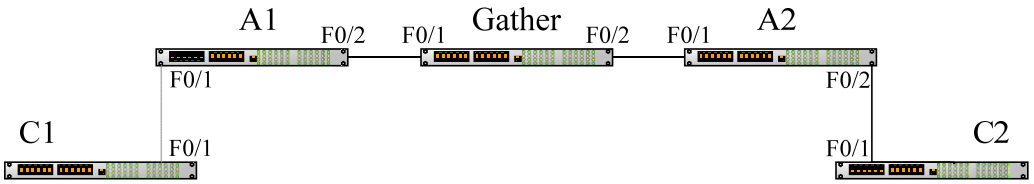
6.2 配置二层协议隧道

可以通过命令行在交换端口下配置某二层协议的隧道功能；配置步骤如下：

命令	说明
configure	进入全局配置模式。
interface *<intf_name>*	进入该某交换端口的接口配置模式。只有交换端口支持二层协议隧道（包括物理端口和聚合端口）。
[**no**] **l2protocol-tunnel** *[stp]*	配置该端口下启用隧道功能的二层协议。 目前只支持 stp 协议的隧道功能。
[CTRL] + Z	退回到管理模式。
write	保存配置。

6.3 二层协议隧道配置示例

有如下网络环境：



A1/A2/Gather 属于核心网络，C1/C2 是某客户分布在两地的分支机构交换机，客户想要将自己的两处网络作为一个单独的网络进行管理，即核心网络对于客户来说只是一条透明的传输通道。如果客户需要实现 STP 的透传，则需要在各交换机上作如下配置：

1. 交换机 A1 的 f0/2 端口、Gather 的 f0/1, f0/2 端口、A2 的 f0/1 端口设置为 trunk 模式；

2. 交换机 A1 的 f0/1 端口、A2 的 f0/2 端口设置为 Access，并在这两个端口上启动 STP 协议的隧道功能。

第 7 章 VLAN 配置

7.1 VLAN 概述

VLAN(Virtual Local Area Network)，即虚拟局域网，是一种通过将局域网内的设备逻辑地而不是物理地划分的交换网络。IEEE 于 1999 年颁布了用以标准化 VLAN 实现方案的 IEEE 802.1Q 协议标准草案。VLAN 技术允许将一个物理的 LAN 逻辑地划分成不同的广播域（VLAN），每一个 VLAN 都包含一组有着相同需求的设备，与物理上形成的 LAN 有着相同的属性，但由于它是逻辑地而不是物理地划分，所以同一个 VLAN 内的各个设备无须被放置在同一个物理空间，即，这些设备不一定属于同一个物理 LAN 网段，一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，从而有助于控制流量、减少设备投资、简化网络管理、提高网络安全。

* 支持基于端口的 VLAN

* 端口支持 802.1Q 的中继模式

* 支持访问型端口

  基于端口的 VLAN，就是将端口归属到交换机支持的 VLAN 的一个子集中。如果这个 VLAN 子集只有一个 VLAN，那么该端口就是访问模式（access）端口；如果这个 VLAN 子集中有多个 VLAN，该端口为中继（trunk）端口，其中有一个默认的 VLAN，它是该端口的 native VLAN，该 VLAN ID 就是 Port VLAN ID（PVID）。

* 支持端口 VLAN 的范围控制

  vlan-allowed 参数用于控制端口所归属的 VLAN 范围；vlan-untagged 参数用于控制端口发送不加上 VLAN 标签的报文到相应的 VLAN。

7.2 VLAN 配置任务列表

* 添加/删除 VLAN

* 配置交换机端口

* 监控 VLAN 的配置和状态

7.3 VLAN 配置任务

7.3.1 添加/删除 VLAN

VLAN 是一个按不同功能、不同项目组或不同的应用进行逻辑划分的交换网络，不区分这些用户的物理位置。 VLAN 拥有与物理局域网相类似的属性，利用 VLAN 可以将不在同一物理局域网的终端划分到一个 VLAN 组中。一个 VLAN 可以拥有多个端口，而所有的单播、组播、广播数据报文只能在同一个 vlan 中进行转发、扩散到终端。每一个 VLAN 就是一个逻辑上的网络，一个数据报文要到达另外一个 VLAN，则必须通过路由或桥转发。

使用下面的命令进行 vlan 的配置：

命令	目的
vlan *vlan-id*	进入到 VLAN 的配置模式。
name *str*	VLAN 配置模式下的命名。
Exit	退出 VLAN 配置模式，同时创建该 VLAN。
vlan *vlan-range*	同时创建多个 VLAN
no vlan *vlan-id* | *vlan-range*	删除一个或多个 VLAN

Vlan 也可以通过 VLAN 管理协议 GVRP 进行动态的添加删除。

7.3.2 配置交换机端口

交换机端口支持以下几种模式：访问模式、中继模式、VLAN 隧道模式、VLAN 翻译型隧道模式和 VLAN 隧道上连口模式。

* 访问模式表示该端口只从属于一个 VLAN，并且只发送和接收无标签的以太网帧。

* 中继模式表示该端口与其它交换机相连，可以发送和接收带标签的以太网帧。

* VLAN 隧道模式是基于访问模式的子模式。该端口收到的报文无论是否带有 VLAN tag，都认为其不带 tag，并由交换芯片自动加上该端口的 pvid 作为新 tag，有的机型还支持在下连口修改新 tag 的 TPID 值。交换机从而能够忽略接入网络中的不同 vlan 划分，而将报文原样传递到同一客户在另外一个端口的另一个子网络中，实现透明传输。

* VLAN 翻译型隧道模式是基于中继模式的子模式。该端口根据收到报文的 VLAN tag，查找 VLAN 翻译表得到对应的 SPVLAN，并由交换芯片用 SPVLAN 替换原 tag 或者在原 tag 外层添加 SPVLAN tag。报文从该端口出来时，会将 SPVLAN 替换为原 tag 或者强制除去 SPVLAN tag。交换机从而能够忽略接入网络中的不同 vlan 划分，而将报文原样传递到同一客户在另外一个端口的另一个子网络中，实现透明传输。

* VLAN 隧道上连口模式是基于中继模式的子模式。报文从该端口出去时，应该配置 SPVLAN 不在 untagged 的范围，保证所有报文原封不动的出去。报文从该端口进

来时，会对报文的 TPID 进行检查，如果发现不符，或者是 untagged 的报文，则会强制加上包含自己的 TPID 的 SPVLAN tag 作为报文的外层标签。

每一个端口都有一个默认的 VLAN 及 PVID，端口下接收到的所有的没有 VLAN 标签的数据都是属于该 VLAN 的数据报文。

中继模式可以将端口归属于多个 VLAN，同时也可以配置转发何种报文和所属的 VLAN 的数量，即端口发送的报文是 Tagged 还是 unTagged，以及端口所属的 VLAN list。

使用如下的命令可以配置交换机端口：

命令	目的
switchport pvid *vlan-id*	配置交换机端口的 PVID。
switchport mode {access | trunk}	配置交换机端口的端口模式。
switchport trunk vlan-allowed …	配置交换机端口的 VLAN 归属范围。
switchport trunk vlan-untagged …	配置交换机端口的 unTagged 的 VLAN 范围。

7.3.3 监控 VLAN 的配置和状态

为了监控 VLAN 状态，可以在管理模式下使用下面的命令：

命令	目的
show vlan [id *x* **| interface** *intf* **]**	显示 VLAN 状态。

第 8 章 配置生成树协议（STP）

8.1 STP 概述

标准的生成树协议（Spanning-Tree Protocol，STP）定义于 IEEE 802.1D，它将一个由若干网桥连接组成的局域网拓扑简化为一棵单独的生成树，防止网络环路的产生，保证网络的稳定工作。

生成树算法和协议将任意的桥接局域网配置为简单连接的活动拓扑结构。在活动拓扑中，有些网桥端口可以转发帧，有些端口则处在阻塞状态而不能转发。处在阻塞状态的端口也可能被包含在活动拓扑中，当网络中出现设备失效、添加或移出时，它就会转入转发状态。

在生成树拓扑中，一个网桥被认为是根或者根桥（Root）。对每一个局域网段，都有一个网桥端口负责该网段到根桥的数据转发，该端口被认为是该局域网段的指派端口，而端口所在的网桥被认为是该局域网的指派网桥（Designated Bridge）。根桥是所有与之连接的局域网段的指派网桥。在每个网桥的端口中，到根桥最近的端口为该桥的根端口，且只有根端口和指派端口（如果存在）处于转发状态；还有一类端口并没有被关闭掉但是也不是根端口或指派端口，这一类端口为备用端口。

以下参数决定了稳定后的活动拓扑的结构：

(1) 每个网桥的唯一标识。

(2) 每个端口的路径开销。

(3) 网桥每个端口的端口标识。 优先级最高（标识符值最小）的网桥将被选为根桥。网

络中每个网桥的端口都有一个根
路径开销属性（Root Path Cost），即从根桥到该网桥经历的所有端口的路径开销的和的最小值。每个局域网段的指派端口就是指连接到该网段的且根路径开销最小的端口；如果若干个端口（连接到同一局域网段的不同网桥上）具有相同的根路径开销，则会首先比较它们所在网桥的标识，然后比较端口标识。按照这种方法，每个局域网段都只有一个指派端口（Designated Port），每个网桥上也只有一个根端口（Root Port）。

生成树拓扑使网络中不存在环路，保证网络的稳定性并具有故障恢复的能力。 快速生成

树协议（Rapid Spanning-Tree Protocol，RSTP）是对 802.1D STP 的一项重要
更新。在网络中的网桥、网桥端口或者局域网段出现故障时，快速生成树协议实现了网络拓扑的快速收敛。网桥上新的根端口可以立即进入转发状态工作，同时，网桥之间的直接认可使指派端口也可以马上进行转发。RSTP 协议的配置请参见配置快速生成树协议（RSTP）。

请注意：
802.1D STP 和 802.1w RSTP 在本文中被简称为 SSTP 和 RSTP。其中“SSTP”意为“Single Spanning-tree”。

8.2 SSTP 配置任务列表

* 选择 STP 模式
* 禁止/启动 STP
* 禁止/启动端口的 STP
* 配置网桥优先级
* 配置 Hello Time
* 配置 Max Age
* 配置 Forward Delay
* 配置端口优先级
* 配置端口路径开销
* 配置自动指派端口
* 监控 STP 状态
* 配置 SNMP Trap

8.3 SSTP 配置任务

8.3.1 选择 STP 模式

使用下面的命令进行生成树协议模式配置：

命令	目的
spanning-tree mode {sstp | rstp | mstp | pvst}	进行的 STP 模式配置选择。

8.3.2 禁止/启动 STP

默认情况下 STP 启动，运行模式为 RSTP，当不需要运行 STP 时可以禁止其运行。

使用下面的命令禁止 STP：

命令	目的
no spanning-tree	禁止运行 STP。

使用下面的命令启动 STP：

命令	目的。

spanning-tree	启动默认模式的 STP（RSTP）。
spanning-tree mode {sstp | rstp | mstp | pvst}	启动某种模式的 STP。

8.3.3 禁止/启动端口的 STP

默认情况下 STP 协议在所有交换端口上运行，在端口配置模式通过下面的命令禁止 STP 运行：

命令	目的
no spanning-tree	禁止端口运行 STP。

禁止端口运行 STP 后，端口将保持指派端口角色和转发状态，也将不再发送 BPDU。但各 STP 模式仍会对端口收到的 BPDU 进行类型检查、计数，并更新边界信息和拓扑信息。

请注意：
进行"no spanning-tree"配置时，若端口已经具有"RootPort"、"AlternatePort"、"MasterPort"或"BackupPort"角色，在 RSTP/MSTP 模式中，端口收到的协议信息会立即老化而转为"DesignatedPort"；在 SSTP/PVST 模式中，端口将保持原角色一段时间，等待定时器超时后信息才会老化。

请注意：
各 STP 模式都支持"no spanning-tree"端口上的 BpduGuard 功能。

8.3.4 配置网桥优先级

可以通过更改交换机的网桥优先机值来选择网络拓扑的生成树根。

使用下面的命令可以配置 SSTP 的网桥优先级：

命令	目的
spanning-tree sstp priority *value*	更改 SSTP 模式的网桥优先级值。
no spanning-tree sstp priority	恢复 SSTP 的网桥优先级为默认值（32768）。

8.3.5 配置 Hello Time

通过配置 SSTP 的 Hello Time 可以决定当作为根桥时发送报文的时间间隔。

使用下面的命令可以配置 SSTP 的 Hello Time：

命令	目的
spanning-tree sstp hello-time *value*	更改 SSTP 模式的 Hello Time。
no spanning-tree sstp hello-time	恢复 SSTP 模式的 Hello Time 为默认值(4s)。

8.3.6 配置 Max Age

通过配置 SSTP 的 Max Age 可以决定当作为根桥时生成树中报文的最大生存时间。

使用下面的命令可以配置 SSTP 的 Max Age：

命令	目的
spanning-tree sstp max-age *value*	更改 SSTP 模式的最大生存时间。
no spanning-tree sstp max-age	恢复最大生存期为默认值（20s）。

8.3.7 配置 Forward Delay

通过配置 SSTP 的 Forward Delay 可以决定当作为根桥时网络中节点的状态跳转的时间间隔。

使用下面的命令可以配置 SSTP 的 Forward Delay：

命令	目的
spanning-tree sstp *forward-time*	更改 SSTP 模式的 Forward time。
no spanning-tree sstp forward-time	恢复 Forward time 为默认值（15s）。

8.3.8 配置端口优先级

当有环路形成时，STP 会将一些端口的状态跳转为 Blocking 状态，以断开环路。通过配置端口优先级和端口路径开销可以控制端口是否被阻塞。

使用下面的命令可以配置 SSTP 的端口优先级：

命令	目的
spanning-tree port-priority *value*	配置所有模式下端口的优先级。
spanning-tree sstp port-priority *value*	更改 SSTP 模式的端口优先级。
no spanning-tree sstp port-priority	恢复端口优先级为默认值（128）。

8.3.9 配置端口路径开销

使用下面的命令可以配置 SSTP 的端口路径开销：

命令	目的
spanning-tree cost *value*	配置所有模式下端口的路径开销。
spanning-tree sstp cost *value*	更改 SSTP 模式的端口路径开销。
no spanning-tree sstp cost	恢复端口路径开销为默认值。

8.3.10 监控 STP 状态

为了监控 STP 配置和状态，可以在管理模式下使用下面的命令：

命令	目的
show spanning-tree	显示当前模式下生成树协议的状态。
show spanning-tree detail	显示当前模式 STP 的详细信息。
show spanning-tree interface	显示当前模式 STP 下的端口信息。

8.3.11 配置 SNMP Trap

通过配置生成树协议的 Trap 功能，可以从主机的网管软件远程监测交换机生成树协议的变化。STP 系列协议支持两种类型的 Trap：newRoot 和 topologyChange。当从非根转换为根时，发送 newRoot Trap 消息；当检查到拓扑变化时，比如一个非边缘端口从非转发态变为转发态，会发送 topologyChange Trap 消息。

请注意：
需使用支持 Trap 接收的网管软件方可接收 STP Trap。网管软件需要导入 Bridge-MIB 集合，OID 为 1.3.6.1.2.1.17。

在全局配置模式下，通过下面的命令启用 STP Trap。

命令	目的
spanning-tree management trap **[newroot | topologychange]**	启用 STP Trap。 不指定 Trap 类型将同时启用两种 Trap。
no spanning-tree management trap	关闭 STP Trap。

8.4 配置 VLAN 的生成树

8.4.1 概述

SSTP 模式下，整个网络仅有一个生成树实例，端口在生成树中的状态将决定它在所有 VLAN 中的状态。在网络中存在多个 VLAN 的情况下，单生成树协议与 VLAN 拓扑的这种隔离状态可能导致部分网络的正常通信被阻塞。

PVST 支持在一定数目的 VLAN 上运行独立的 SSTP，保证端口可以在不同的 VLAN 中具有不同的状态。同时也可以实现 VLAN 之间的流量均衡。

需要注意的是，目前设定最多支持在 64 个 VLAN 上运行独立的生成树协议，其它 VLAN 拓扑将不受 STP 控制。

8.4.2 VLAN STP 配置任务

在全局配置态下，使用下面的命令配置 VLAN 中 SSTP 的属性：

命令	目的
spanning-tree mode pvst	启动按 VLAN 分配 STP 的模式。
spanning-tree vlan *vlan-list*	为指定 VLAN 分配 STP 实例。 vlan-list：VLAN 列表（下同）。
no spanning-tree vlan *vlan-list*	删除指定 VLAN 上的生成树实例。
spanning-tree vlan *vlan-list* **priority** *value*	配置指定 VLAN 中生成树的优先级。
no spanning-tree *vlan-list* **priority**	恢复 VLAN 中生成树优先级为默认。
spanning-tree vlan *vlan-list* **forward-time** *value*	配置指定 VLAN 的 Forward Delay。
no spanning-tree vlan *vlan-list* **forward-time**	恢复指定 VLAN 的 Forward Delay 为默认。
spanning-tree vlan *vlan-list* **max-age** *value*	配置指定 VLAN 的 Max-age。
no spanning-tree vlan *vlan-list* **max-age**	恢复指定 VLAN 的 Max-age 为默认。
spanning-tree vlan *vlan-list* **hello-time** *value*	配置指定 VLAN 的 Hello-time。
no spanning-tree vlan *vlan-list* **hello-time**	恢复指定 VLAN 的 Hello-time 为默认。

在交换端口配置态下，使用下面的命令配置端口的属性：

命令	目的
spanning-tree vlan *vlan-list* **cost**	配置端口在指定 VLAN 的路径开销。
no spanning-tree vlan *vlan-list* **cost**	恢复端口在 VLAN 中的路径开销为默认。
spanning-tree vlan *vlan-list* **port-priority**	配置端口在 VLAN 中的优先级。
no spanning-tree vlan *vlan-list* **port-priority**	恢复端口在 VLAN 中的优先级为默认。

在监控或配置态下，使用下面的命令查看指定 VLAN 中生成树的状态：

命令	目的
show spanning-tree vlan *vlan-list*	查看 VLAN 中生成树状态。

8.5 RSTP 配置任务列表

* 开启/关闭 RSTP

* 配置网桥优先级

* 配置 Forward Time
* 配置 Hello Time
* 配置 Max Age
* 配置端口路径开销
* 配置端口优先级
* 配置边缘端口
* 配置端口连接类型
* 重启协议转换检查

8.6 RSTP 配置任务

8.6.1 开启/关闭 RSTP

在全局配置模式下进行下列配置

命令	目的
spanning-tree mode rstp	开启 RSTP。
no spanning-tree mode	关闭 stp 功能。

8.6.2 配置网桥优先级

网桥优先级的大小决定了这个网桥是否能够被选择为整个生成树的根网桥，通过配置较小的优先级可以使某个网桥成为生成树的根网桥。

在全局配置模式下进行下列配置

命令	目的
spanning-tree rstp priority *value*	配置网桥优先级。
no spanning-tree rstp priority	恢复优先级为默认 。

需要注意的是如果整个交换网络中所有网桥的优先级采用相同的值的话，那么 MAC 地址最小的那个网桥将被选择为根网桥，在 RSTP 协议开启的情况下如果网桥的优先级被改变则会引起生成树的重新计算。

缺省情况下网桥的优先级被配置为 32768。

8.6.3 配置 Forward Time

链路故障会引发网络重新进行生成树结构的计算，不过重新计算得到的新配置消息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路径回环，为此协议采用了一种状态迁移的机制。根端口和指定端口重新开始数据转发之前要经历一个中间状态，中间状态经过 Forward Delay 延时后才能进入转发状态，这个延时保证了新的配置消息已经传遍整个网络。网桥的 Forward Delay 特性与交换网络的网络直径有关，一般来说网络直径越大 Forward Delay 的时间就应该配置得越长。

在全局配置模式下进行下列配置：

命令	目的
spanning-tree rstp forward-time *value*	配置 Forward Delay 。
no spanning-tree rstp forward-time	恢复 Forward Delay 为默认值（15s）。

需要注意的是如果 Forward Delay 配置的过小可能会使网络出现暂时的冗余路径，如果 Forward Delay 配置的过大网络则可能会较长时间不能恢复连通，建议用户采用缺省值。

缺省情况下网桥的 Forward Delay 为 15 秒。

8.6.4 配置 Hello Time

合适的 Hello Time 时间值可以保证网桥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。

在全局配置模式下进行下列配置

命令	目的
spanning-tree rstp hello-time *value*	配置 Hello Time 。
no spanning-tree rstp hello-time	恢复 Hello Time 为默认值 。

需要注意的是过长的 Hello Time 值会因为链路丢包而导致网桥长时间收不到 Hello 报文，那么网桥会认为链路发生了故障并且开始重新计算生成树，如果 Hello Time 过短则会导致网桥频繁发送配置消息占用网络带宽，增加了网络负担和 CPU 负担，建议用户采用缺省值。

缺省情况下网桥的 Hello Time 为 4 秒。

8.6.5 配置 Max Age

Max Age 是用来判断配置消息是否过时的参数，用户可以根据实际的网络情况对其进行配置。

在全局配置模式下进行下列配置：

命令	目的

spanning-tree rstp max-age *value*	配置 Max Age。
no spanning-tree rstp max-age	恢复 Max Age 为默认值（20s）。

链路故障，降低网络自适应能力。建议用户采用缺省值。 需要注意的是如果 Max Age 配置的过小，生成树计算就会比较频繁，而且有可能将网络拥塞误认为链路故障，如果 Max Age 配置的过大则很可能不能及时发现。

缺省情况下网桥的 Max Age 为 20 秒。

8.6.6 配置端口路径开销

路径开销与端口的链路速率有关,链路速率越大应该将该参数配置的越小,当该参数被配置为缺省值时，RSTP 协议可以自动检测当前以太网端口的链路速率并换算成相应的路径开销。

请在端口配置模式下进行下列配置：

命令	目的
spanning-tree rstp cost *value*	配置端口的 Path Cost 值。
no spanning-tree rstp cost	恢复端口的 Path Cost 为默认值。

需要注意的是配置以太网端口的路径开销会引起生成树重新计算，建议用户采用缺省值，让 RSTP 协议自己来计算当前以太网端口的路径开销。

缺省情况下网桥所有以太网端口的 Path Cost 在端口速率为 10Mbps 时为 2000000，在端口速率为 100Mbps 时为 200000。

8.6.7 配置端口优先级

通过设定端口的优先级可以指定特定的以太网端口包含在生成树内，一般情况下配置的值越小端口的优先级就越高，该以太网端口就越有可能包含在生成树内，如果网桥所有的以太网端口采用相同的优先级参数值，则以太网端口的优先级高低就取决于该以太网端口的索引号。

请在端口配置模式下进行下列配置：

命令	目的
spanning-tree rstp port-priority *value*	配置端口的优先值。
no spanning-tree rstp port-priority	恢复端口的优先值为默认值。

需要注意的是改变以太网端口的优先级会引起生成树重新计算。

缺省情况下网桥所有以太网端口的优先级为 128。

8.6.8 配置边缘端口

边缘端口表示该端口连接着网络上的终端设备，一个强制的边缘端口在 Link Up 之后会立刻进入转发状态。在端口配置模式下，通过下面的命令配置 RSTP 的边缘端口：

命令	目的
spanning-tree rstp edge [**force-true** | **force-false** | **auto**]	配置边缘端口。 force-true：强制边缘端口生效。 force-false：强制边缘端口无效。 auto：协议自动检测边缘端口。

在协议自动检测模式下，如果端口在一定时间内没有收到过 BPDU，则认为该端口是边缘端口。

8.6.9 配置端口连接类型

运行 RSTP 协议的网络节点之间如果是点到点的直接连接，它们可以通过握手机制快速建立拓扑。配置端口连接类型功能允许将端口的连接设置为点到点。

在默认情况下，协议会根据端口的双工属性决定其是不是使用了点到点的连接。如果端口工作在全双工模式，协议就会认为它是点到点的连接；如果端口工作在半双工模式，协议会认为它的连接是共享的。

如果确认端口所连的网络节点运行着 RSTP 或者 MSTP 协议，可以将端口的连接类型设置为点到点，保证快速握手的进行。

在端口配置模式下，使用下面的命令设置端口的连接类型：

命令	目的
spanning-tree rstp point-to-point [**force-true** | **force-false** | **auto**]	配置边缘端口。 force-true：强制为点到点类型。 force-false：强制为共享链路类型。 auto：协议自动检测端口类型。

8.6.10 重启协议转换检查

RSTP 协议允许交换机通过一种协议转换机制与传统的 802.1D STP 交换机协同工作。如果交换机的一个端口接收到 STP 的配置信息，那么该端口就会转为仅发送 STP 报文。

一个端口进入 STP 兼容状态之后，即使该端口不再收到 802.1D STP BPDU，该端口也不会恢复为 RSTP 状态。这时，可以使用 **spanning-tree rstp migration-check** 命令，启动端口的协议转换检查过程，将端口恢复为 RSTP 模式。

在全局配置模式下，使用下面的命令重启 RSTP 协议转换检查：

命令	目的
spanning-tree rstp migration-check	重启所有端口的协议转换检查过程。

在交换端口配置模式下，使用下面的命令对该端口进行协议转换检查：

命令	目的
spanning-tree rstp migration-check	重启当前端口的协议转换检查过程。

8.7 MSTP 简介

8.7.1 概述

MSTP（Multiple Spanning Tree Protocol）多生成树协议，用来在桥接局域网中建立简单而完整的拓扑结构。MSTP 可以与早期的 STP（Spanning Tree Protocol）和 RSTP（Rapid Spanning Tree Protocol）相兼容。

STP 和 RSTP 都只能在网络中建立单独的生成树拓扑，所有 VLAN 的报文沿着唯一的生成树进行转发。STP 收敛过慢，RSTP 通过握手机制保证网络拓扑快速稳定。

MSTP 继承了 RSTP 的快速握手机制，同时，在保证网络拓扑快速建立的基础上，MSTP 允许将不同的 VLAN 划分到不同的生成树中去，从而在网络中建立多个树状拓扑。在 MSTP 建立的网络中，属于不同 VLAN 的帧可以在不同的路径上转发，实现了 VLAN 数据的负载均衡。

与按 VLAN 划分 STP（per-VLAN Spanning Tree，PVST）不同的是，MSTP 还允许将多个 VLAN 划分到同一个生成树拓扑中去，这样可以有效减少支持大量 VLAN 所需的生成树的数目。

8.7.2 多生成树区域

MSTP 中，VLAN 与生成树的对应关系是通过一个多生成树配置表来描述的。多生成树配置表，连同一个配置名称和一个配置修订号，共同构成了多生成树配置标识（MST Configuration Identifier）。

在网络上，相互连接且具有相同多生成树配置标识的网桥被认为是在同一个多生成树区域（MST Region）中。同一个多生成树区域中的网桥通常也具有相同的 VLAN 配置，从而保证这些 VLAN 的帧只在区域内部流动。

8.7.3 IST, CST, CIST 和 MSTI

如图 2.1 所示为一个示例 MSTP 网络，其中包括三个多生成树区域以及一个运行 802.1D STP 协议的节点。

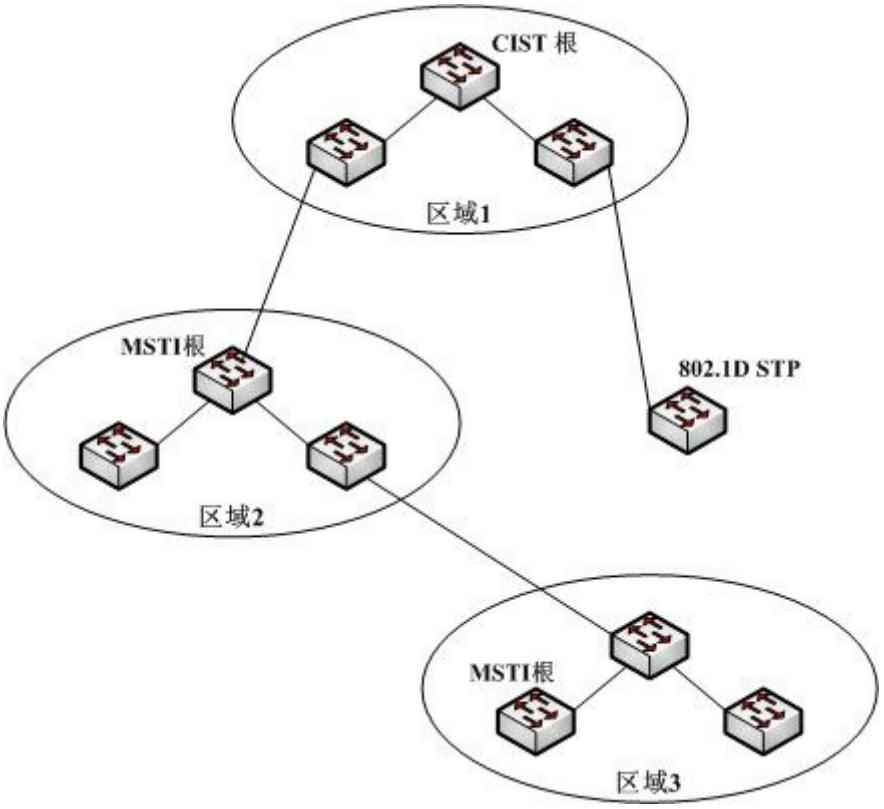


图 2.1 MSTP 拓扑示例

1. CIST

Common and Internal Spanning Tree，公共与内部生成树。是指网络中所有单个交换机及其连接的局域网构成的生成树。这些交换机可能分属不同的多生成树区域，也可能是运行传统 STP 或者 RSTP 协议的交换机，运行这两种协议的交换机在多生成树网络中被认为是处在仅由其自身组成的区域中。

网络拓扑稳定后，整个 CIST 会选出一个 CIST 根桥。每个区域内部也会选出 CIST 区域内根桥，作为从区域内部到达 CIST 根的最短路径。

2. CST

Common Spanning Tree，公共生成树。如果把每个多生成树区域看作是一个单独的交换机，CST 就是连接着所有这些“单独交换机”的生成树。如图 2.1 所示，区域 1, 2, 3 以及 STP 交换机共同构成了网络的 CST。

3. IST

Internal Spanning Tree，内部生成树。是指 CIST 在某个多生成树区域以内的部分。也可以理解为 IST 与 CST 共同构成了 CIST。

4. MSTI

Multiple Spanning Tree Instance，多生成树实例。MSTP 协议允许将不同的 VLAN 划分到不同的生成树中，从而就建立起多个生成树实例。通常情况下，编号为 0 的生成树实例是指 CIST，它可以扩展到整个网络，而从 1 开始所指的生成树实例，都处在某个区域的内部。每个生成树实例中都可以被分配多个 VLAN，初始情况下，所有的 VLAN 都被分配在 CIST 中。

多生成树区域中所有的 MSTI 都是相互独立的，它们可以选出不同的交换机作为各自的根。比如图 2.1 的区域 3 中，MSTI01 的根桥可能是处在左下角的交换机，而 MSTI00，也就是 CIST 的区域内根桥则可能是处在中间位置的交换机。

8.7.4 端口的角色

MSTP 协议具有与 RSTP 相似的端口角色分配。

1. 根端口（Root Port）

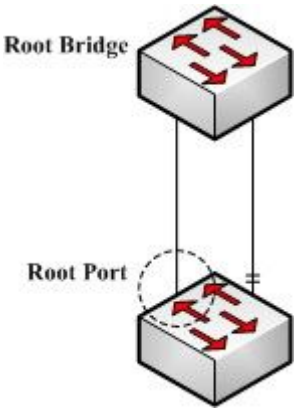


图 2.2 根端口

根端口表示当前交换机到网络根桥的路径，该路径具有最小的根路径开销。

2. 预备端口（Alternate Port）

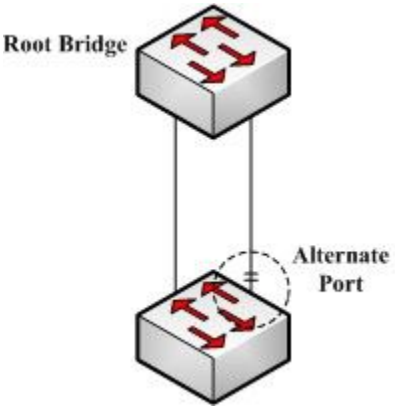


图 2.3 预备端口

预备端口作为当前交换机到网络根桥路径的备份，当根端口连接失效时，预备端口可以立即转为新的根端口开始工作。

3. 指派端口（Designated Port）

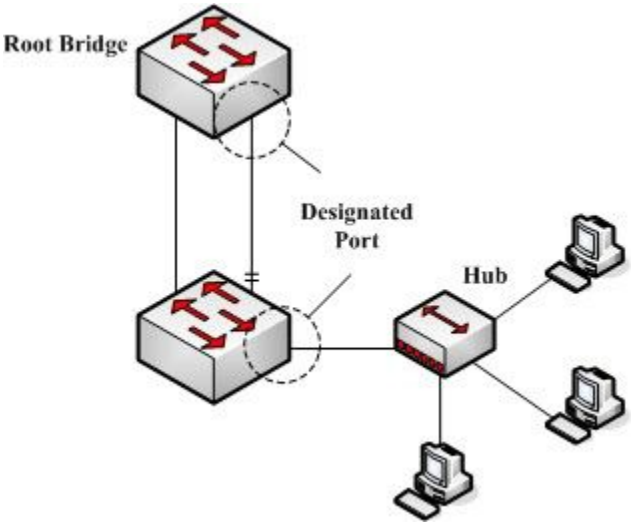


图 2.4 指派端口

指派端口可以连接着下游的交换机或者局域网，作为该局域网到达网络根桥的路径。

4. 备份端口（Backup Port）

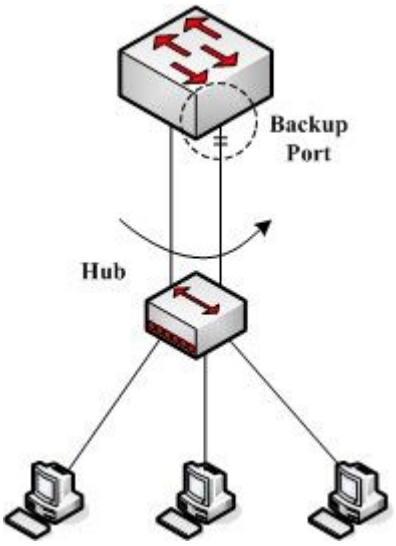


图 2.5 备份端口

当交换机的两个端口直接相连或者连接到同一个局域网时，优先级较低的端口会成为备份端口（较高的成为指派端口）。如果指派端口失效，则备份端口转为指派端口开始工作。

5. Master 端口

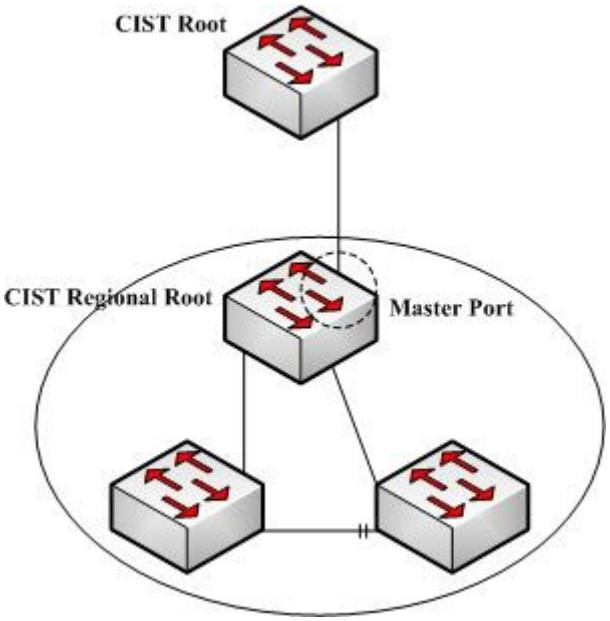


图 2.6 Master 端口

Master 端口作为多生成树区域连接 CIST 根桥的最短路径。Master 端口也就是 CIST 区域内根桥的根端口。

6. 边界端口（Boundary Port）

边界端口的概念在 CIST 中与在每个 MSTI 中稍有不同。在 CIST 中，边界端口表示连接着另一个多生成树区域的端口；而在 MSTI 中，边界端口角色表示该生成树实例在这个端口处不再扩展。

7. 边缘端口（Edge Port）

在 RSTP 和 MSTP 协议中，边缘端口表示直接连接到网络主机的端口，这些端口不需要经过等待既可以进入转发状态，且不会在网络上造成环路。

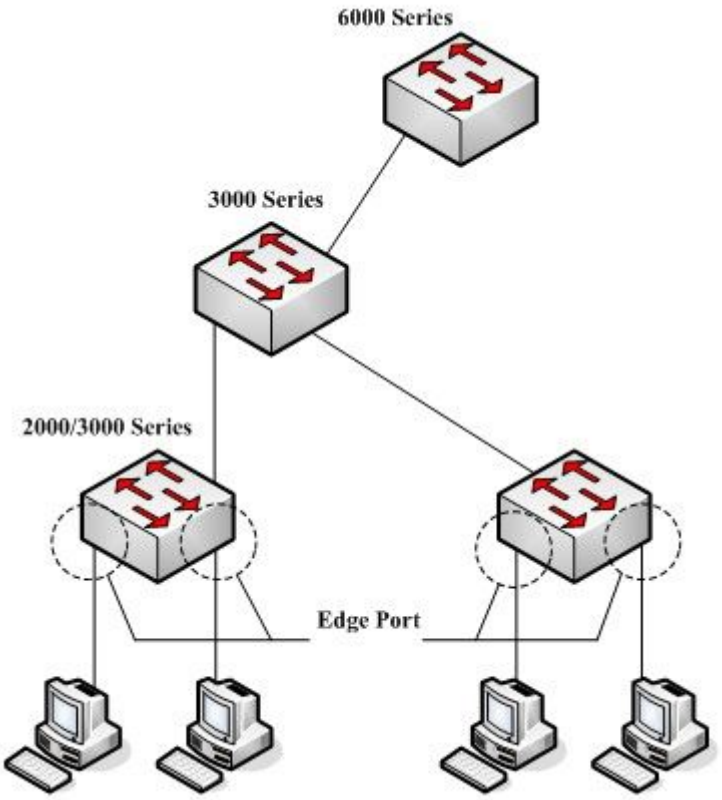


图 2.7 边缘端口

在初始情况下，MSTP（包括 RSTP）协议会认为所有的端口都是边缘端口，从而可以保证网络拓扑的快速建立。此时如果一个端口收到了来自其它交换机的 BPDU，该端口就会从边缘状态恢复为普通状态，如果收到的是 802.1D STP BPDU，那么该端口需要等待 2 倍的 Forward Delay 时间才能进入转发。

8.7.5 MSTP BPDU

与 STP 和 RSTP 协议相同，运行 MSTP 协议的交换机之间通过 BPDU（Bridge Protocol Data Unit）交互信息，CIST 以及所有 MSTI 中的配置信息都可以由 BPDU 携带。表 2.1 和表 2.2 列出了 MSTP 协议使用的 BPDU 结构。

表 2.1 MSTP BPDU

字段名	字节数
Protocol Identifier	1 – 2
Protocol Version Identifier	3
BPDU Type	4
CIST Flags	5
CIST Root Identifier	6 – 13
CIST External Root Path Cost	14 – 17

CIST Regional Root Identifier	18 – 25
CIST Port Identifier	26 – 27
Message Age	28 – 29
Max Age	30 – 31
Hello Time	32 – 33
Forward Delay	34 – 35
Version 1 Length	36
Version 3 Length	37 – 38
Format Selector	39
Configuration Name	40 – 71
Revision	72 – 73
Configuration Digest	74 – 89
CIST Internal Root Path Cost	90 – 93
CIST Bridge Identifier	94 – 101
CIST Remaining Hops	102
MSTI Configuration Messages	103 ~

表 2.2 MST 配置消息

字段名	字节数
MSTI FLAGS	1
MSTI Regional Root Identifier	2 – 9
MSTI Internal Root Path Cost	10 – 13
MSTI Bridge Priority	14
MSTI Port Priority	15
MSTI Remaining Hops	16

8.7.6 稳定状态

MSTP 交换机根据接收到的 BPDU 执行计算和比较操作，最终可以使网络达到如下的稳定状态：

(1) 一台交换机被选为整个网络的 CIST 根（CIST Root）；

(2) 每个交换机和局域网段都会决定出到 CIST 根的具有最小开销的路径，以保证连接的完整性并防止环路；

(3) 每个区域内部都会选出一台交换机作为 CIST 区域内根（CIST Regional Root），该交换机具有到达 CIST 根的开销最小的路径；

(4) 每个 MSTI 都会独立的选择出一台交换机作为 MSTI 区域内根；

(5) 区域内部的每台交换机和局域网段都会确定出到达所在MSTI的根的开销最小的路径；

(6) CIST 根端口（Root Port）提供经过 CIST 区域内根（如果该交换机不是 CIST 区域内根）到达 CIST 根（如果该交换机不是 CIST 根）的具有最小开销的路径；

(7) CIST 指派端口（Designated Port）为所连接的局域网提供到达 CIST 根的最小开销路径；

(8) Alternate 和 Backup 端口在交换机、端口或局域网失效或被移除时提供连接；

(9) MSTI 根端口（Root Port）提供到达 MSTI 区域内根的最小开销路径（如果该交换机不是 MSTI 区域内根桥）；

(10) MSTI 指派端口（Designated Port）为所连接局域网提供到达 MSTI 区域内根的最小开销路径；

(11) 一个主端口（Master Port）提供区域与区域外 CIST 根桥的连接。在区域内部，CIST 区域内根桥的 CIST 根端口会作为区域内所有 MSTI 的 Master 端口。

8.7.7 跳数

与 STP 和 RSTP 不同，MSTP 协议不使用 BPDU 配置消息中的消息生存期（Message Age）和最大生存期（Max Age）来计算网络拓扑，而是使用了跳数属性（Hop Count）。

为了防止旧的信息在网络中无休止的循环而影响新信息的传输，MSTP 使传输的信息在每个生成树中都与一个跳数属性相关联。BPDU 的跳数属性由 CIST 区域内根桥或者 MSTI 区域内根桥指定，并在每个接收端口处被减小。如果跳数在端口处变为了 0，该信息会被丢弃同时该端口会成为一个指派端口。

8.7.8 STP 兼容性

MSTP 协议允许交换机通过一种协议转换机制与传统的 STP 交换机协同工作。如果交换机的一个端口接收到 STP 的配置信息，那么该端口就会转为仅发送 STP 报文。同时，接受到 STP 信息的端口也会被认为是一个边界端口。

请注意：
一个端口转入 STP 兼容状态之后，即使不再接受到 STP 报文，该端口也不会自动恢复为 MSTP 状态。这种情况下，可以使用 **spanning-tree mstp migration-check** 命令清除端口学习到的生成树协议信息，使之恢复为 MSTP 状态。

运行 RSTP 协议的交换机可以识别并处理 MSTP 报文，因此与 RSTP 交换机协同工作时 MSTP 交换机不需要发生协议转换。

8.8 MSTP 配置任务列表

* MSTP 默认配置

* 启动和停止多生成树协议
* 配置多生成树区域
* 配置网络根桥
* 配置次要根桥
* 配置网桥优先级
* 配置生成树协议的时间参数
* 配置网络直径
* 配置最大跳数
* 配置端口优先级
* 配置端口路径开销
* 配置边缘端口
* 配置端口连接类型
* 激活多生成树兼容模式
* 重启协议转换检查
* 查看多生成树协议信息

8.9 MSTP 配置任务

8.9.1 MSTP 默认配置

属性	默认设置
生成树协议模式	RSTP（PVST，SSTP 和 MSTP 没有启动）。
区域名称	交换机 MAC 地址的字符串形式。
区域修订级别	0
多生成树配置表	所有 VLAN 都映射在 CIST（MST00）中。
生成树优先级（CIST 和所有 MSTI）	32768
生成树端口优先级（CIST 和所有 MSTI）	128
生成树端口路径开销（CIST 和所有 MSTI）	1000 Mbps：20000 100 Mbps：200000 10 Mbps：2000000

Hello Time	2 秒
Forward Delay	15 秒
Maximum-aging Time	20 秒
最大跳数	20

8.9.2 启动和停止多生成树协议

生成树协议在默认情况下会以 RSTP（或 SSTP）模式启动，当不需要运行 spanning-tree 时可以停止其运行。

使用下面的命令将生成树协议设置为 MSTP 模式：

命令	目的
spanning-tree	启动默认模式的生成树协议。
spanning-tree mode mstp	启动 MSTP 多生成树协议。

使用下面的命令停止生成树协议运行：

命令	目的
no spanning-tree	禁止生成树协议运行。

8.9.3 配置多生成树区域

交换机所处的多生成树区域，由配置名称、修订号以及 VLAN 与 MSTI 映射关系这三项属性决定，通过区域配置命令可以分别对其进行设置。需要注意的是，三项属性中任何一项的变化都会导致交换机所处区域的变化。

在初始情况下，多生成树配置名称等于交换机 MAC 地址的字符串形式，修订号为 0，并且所有的 VLAN 都被映射在 CIST（MST00）中。由于不同交换机的 MAC 地址都是不同的，因此初始情况下所有运行多生成树协议的交换机都是处在不同的区域中。通过执行 **spanning-tree mstp instance** *instance-id* **vlan** *vlan-list* 命令，可以创建一个新的 MSTI，并将指定的 VLAN 映射给它；如果该 MSTI 被删除，这些 VLAN 会被重新映射到 CIST 中。

使用下面的命令设置多生成树的区域信息：

命令	目的
spanning-tree mstp name *string*	设置多生成树配置名称。 string 表示配置名称字符串，最多可包含 32 个字符，大小写敏 感。默认值为交换机 MAC 地址的字符串形式。
no spanning-tree mstp name	设置多生成树配置名称为默认值。
spanning-tree mstp revision *value*	设置多生成树配置修订号。 value 表示修订号，范围：0 – 65535，默认值 0。

no spanning-tree mstp revision	设置多生成树修订号为默认值。
spanning-tree mstp instance *instance-id* **vlan** *vlan-list*	将 VLAN 映射到 MSTI。 instance-id：生成树实例号，表示一个 MSTI。范围 1 – 15。 vlan-list：映射到该生成树的 VLAN 列表。范围 1 – 4094。 instance-id 为单独的值，仅表示一个生成树实例；vlan-list 可以表示一组 VLAN，比如：”1,2,3”、”1-5”、“1,2,5-10”等。
no spanning-tree mstp instance *instance-id*	取消 MSTI 的 VLAN 映射，停止生成树实例。 instance-id：生成树实例号，表示一个 MSTI。范围 1 – 15。

使用下面的命令查看多生成树协议的区域设置：

命令	目的
show spanning-tree mstp region	显示多生成树协议的区域设置。

8.9.4 配置网络根桥

在 MSTP 协议中，每个生成树实例都有一个网桥标识属性（Bridge ID），网桥标识中包含有该交换机的优先级值以及 MAC 地址。在网络生成树拓扑建立过程中，网桥标识较小的交换机会被选为网络（或区域）的根。

多生成树协议允许通过配置将交换机设为网络的根。**Spanning-tree mstp** *instance-id* **root** 配置命令可以将交换机在某个生成树实例中的优先级从默认的 32768 设置为一个足够小的值，保证交换机在该生成树实例中成为根。

通常情况下，当执行上述命令后，协议会自动检查当前网络根桥的网桥标识，然后把网桥标识的优先级字段设置为 24576，如果这个值可以保证当前交换机成为生成树实例的根。

如果网络根桥的优先级比 24576 更小，那么协议会自动把当前网桥的生成树优先级设置为比根桥优先级小 4096 的一个值。需要注意的是，4096 是网桥优先级值的步长。

设置根桥时，可以通过 **diameter** 子命令设置多生成树网络的网络直径，该关键字仅在生成树实例号为 0 时有效。设定网络直径以后，为了保证网络收敛的稳定，协议会自动根据这个值来计算合适的生成树协议时间参数，包括：Hello Time，Forward Delay 以及 Maximum Age。**Hello-time** 子命令可以用来设置新的 Hello Time 时间，以取代默认设置。

使用下面的命令设置交换机为网络的根：

命令	目的
spanning-tree mstp *instance-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	设置交换机在指定生成树实例中为根。 instance-id：生成树实例号，范围：0 – 15； net-diameter：可选参数，网络直径，当 instance-id 为 0 时有效， 范围：2 – 7；

	seconds：可选参数没，Hello Time，范围：1 – 10 秒。
no spanning-tree mstp *instance-id* **root**	取消交换机在生成树中的根桥设置。 instance-id：生成树实例号，范围：0 – 15。

使用下面的命令查看多生成树协议信息：

命令	目的
show spanning-tree mstp [**instance** *instance-id*]	查看多生成树实例的信息。

8.9.5 配置次要根桥

为网络配置根桥以后，可以通过 **spanning-tree mstp** *instance-id* **root secondary** 命令设置一台或多台交换机成为网络的次要根桥（或称备份根桥）。如果根桥因为某些原因不能工作，次要根桥会接替成为网络的根。

与配置主要根桥不同，执行配置次要根桥的命令后，协议会将交换机的生成树优先级直接设置为 28672，这样，在网络中其它交换机的优先级都为默认的 32768 的情况下，当前交换机就可以成为次要根桥。

配置次要根桥时，仍然可以通过 **diameter** 和 **hello-time** 子命令来更新生成树协议的时间参数。当次要根桥成为主要根桥开始工作后，这些参数将会开始起作用。

使用下面的命令设置交换机为网络的次要根桥：

命令	目的
spanning-tree mstp *instance-id* **root secondary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	设置交换机在指定生成树实例中为次要根桥。 instance-id：生成树实例号，范围：0 – 15； net-diameter：可选参数，网络直径，当 instance-id 为 0 时有效， 范围：2 – 7； seconds：可选参数没，Hello Time，范围：1 – 10 秒。
no spanning-tree mstp *instance-id* **root**	取消交换机在生成树中的根桥设置。 instance-id：生成树实例号，范围：0 – 15。

使用下面的命令查看多生成树协议信息：

命令	目的
show spanning-tree mstp [**instance** *instance-id*]	查看多生成树实例的信息。

8.9.6 配置网桥优先级

配置网桥优先级在某些情况下可以更直接的将交换机设置为网络的根，而不需通过 root 子命令。交换机在每个生成树实例中的优先级值是相互独立的，可以独立配置。

使用下面的命令设置生成树的优先级：

命令	目的
spanning-tree mstp *instance-id* **priority** *value*	设置交换机的优先级值。 instance-id：生成树实例号，范围：0 – 15； value：网桥优先级，可为下列值之一： 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440。
no spanning-tree mstp *instance-id* **priority**	恢复交换机的网桥优先级为默认值。 instance-id：生成树实例号，范围：0 – 15。

8.9.7 配置生成树协议的时间参数

生成树协议的时间参数包括下列几项：

* **Hello Time**： 交换机作为网络根桥时向指派端口发送配置信息的时间间隔；
* **Forward Delay**：STP 模式下，端口从 Blocking 状态到 Learning 状态，以及从 Learning 状态到 Forwarding 状态经历的时间；
* **Max Age**： 生成树配置信息的最大生存期。

为了减少网络拓扑震荡，时间参数之间应该符合以下条件的要求：

* 2 x (fwd_delay - 1.0) >= max_age
* max_age >= (hello_time + 1) x 2

使用下面的命令配置多生成树协议的时间参数：

命令	目的
spanning-tree mstp hello-time *seconds*	设置 Hello Time 参数。 seconds：范围：1 – 10 秒，默认值 2 秒。
no spanning-tree mstp hello-time	恢复 Hello Time 参数为默认值。
spanning-tree mstp forward-time *seconds*	设置 Forward Delay 参数。 seconds：范围：4 – 30 秒，默认值 15 秒。
no spanning-tree mstp forward-time	恢复 Forward Delay 参数为默认值。
spanning-tree mstp max-age *seconds*	设置 Max Age 参数。

	seconds：范围：6 – 40 秒，默认值 20 秒。
no spanning-tree mstp max-age	恢复 Max Age 参数为默认值。

建议通过设置根桥或者设置网络直径的方法来修改生成树协议的时间参数，以保证其合理性。

即使新设置的时间参数不符合上述公式的要求，仍然会在协议中生效。配置时请注意控制台的提示。

8.9.8 配置网络直径

网络直径表示网络上两台主机之间跨越交换机的最大数目，它反映了网络的规模。 可以

通过 **spanning-tree mstp diameter** *net-diameter* 命令设置多生成树协议的网络直径。网络直径参数仅对 CIST 有效，设置后，生成树协议的三个时间参数会被自动更新为较优的值。

使用下面的命令配置网络直径参数：

命令	目的
spanning-tree mstp diameter *net-diameter*	设置网络直径参数。 net-diameter：范围：2 – 7，默认值为 7。
no spanning-tree mstp diameter	恢复网络直径为默认值。

网络直径参数在交换机中并没有作为一项单独的设置而被保存，只有通过设置网络直径而修改的时间参数才会被保存。

8.9.9 配置最大跳数

使用下面的命令配置最大跳数：

命令	目的
spanning-tree mstp max-hops *hop-count*	设置最大跳数。 hop-count：范围：1 – 40，默认值为 20。
no spanning-tree mstp *hop-count*	恢复最大跳数为默认值。

8.9.10 配置端口优先级

如果交换机的两个端口之间形成环路，优先级较高的端口会进入 Forwarding 状态，较低的则被阻塞。如果所有端口的优先级都相同，那么端口号较小的端口将优先进入 Forwarding 状态。

在端口配置模式下，使用下面的命令设置多生成树协议端口的优先级：

命令	目的

spanning-tree mstp *instance-id* **port-priority** *priority*	设置端口优先级。 instance-id：生成树实例号，范围 0 – 15； priority：端口优先级，为下列值之一： 0, 16, 32, 48, 64, 80, 96, 112 128, 144, 160, 176, 192, 208, 224, 240。
spanning-tree port-priority *value*	设置端口在所有生成树实例中的优先级。 value：端口优先级值，为下列值之一： 0, 16, 32, 48, 64, 80, 96, 112 128, 144, 160, 176, 192, 208, 224, 240。
no spanning-tree mstp *instance-id* **port-priority**	恢复端口优先级为默认值。
no spanning-tree port-priority	恢复端口在所有生成树实例中的优先级为默认值。

使用下面的命令查看多生成树协议的端口信息：

命令	目的
show spanning-tree mstp interface *interface-id*	查看多生成树协议下的端口信息。 interface-id：端口名称，比如“F0/1”、“FastEtnernet0/3”等。

8.9.11 配置端口路径开销

MSTP 协议中端口路径开销的默认值是根据端口的连接速率计算出来的。如果两台交换机之间形成环路，路径开销较小的端口会进入 Forwarding 状态，路径开销越小表示端口的速率越高。如果所有端口的路径开销都相同，端口号较小的端口会优先进入转发状态。

在端口配置模式下，使用下面的命令设置端口的路径开销：

命令	目的
spanning-tree mstp *instance-id* **cost** *cost*	设置端口路径开销。 instance-id：生成树实例号，范围 0 – 15； cost：路径开销值，范围 1 – 200000000。
spanning-tree cost *value*	设置端口在所有生成树实例中的路径开销。 value：端口路径开销，范围 1 – 200000000。
no spanning-tree mstp *instance-id* **cost**	恢复端口路径开销为默认值。
no spanning-tree cost	恢复端口在所有生成树实例中的路径开销为默认值。

8.9.12 配置边缘端口

边缘端口表示该端口连接着网络上的终端设备，一个强制的边缘端口在 Link Up 之后会立刻进入转发状态。在端口配置模式下，通过下面的命令配置 MSTP 的边缘端口：

命令	目的
spanning-tree mstp edge force-true	强制端口为边缘端口。
spanning-tree mstp edge force-false	强制端口为非边缘端口。
spanning-tree mstp edge auto	自动检测边缘端口（默认）。
no spanning-tree mstp edge	恢复默认。

8.9.13 配置端口连接类型

运行 MSTP 协议的交换机之间如果是点到点的直接连接，它们可以通过握手机制快速建立拓扑。配置端口连接类型功能允许将端口的连接设置为点到点。

在默认情况下，协议会根据端口的双工属性决定其是不是使用了点到点的连接。如果端口工作在全双工模式，协议就会认为它是点到点的连接；如果端口工作在半双工模式，协议会认为它的连接是共享的。

如果确认端口所连的交换机运行着 RSTP 或者 MSTP 协议，可以将端口的连接类型设置为点到点，保证快速握手的进行。

在端口配置模式下，使用下面的命令设置端口的连接类型：

命令	目的
spanning-tree mstp point-to-point force-true	设置端口连接方式为点到点。
spanning-tree mstp point-to-point force-false	设置端口连接方式为共享。
spanning-tree mstp point-to-point auto	自动检测端口的连接方式（默认）。
no spanning-tree mstp point-to-point	将端口的连接方式恢复为默认设置。

8.9.14 激活多生成树兼容模式

本公司交换机支持的 MSTP 协议是基于 IEEE 802.1s 标准实现的，为了与某些其它的 MSTP 实现兼容--主要是 Cisco 交换机在早期支持的 MSTP--协议可以工作在多生成树兼容模式。工作在 MST 兼容模式的交换机可以识别其它多生成树协议的报文结构，检查其中包含的多生成树区域标识信息，并与之建立多生成树区域。

MST 兼容模式的工作方式与 STP 兼容模式相同，都是依赖 MSTP 的协议转换机制实现的：如果交换机的一个端口收到兼容模式的 BPDU，该端口就会自动迁移到该模式运行，发送兼容模式的 BPDU。如果希望将端口恢复为标准的多生成树模式，请使用 **spanning-tree mstp migration-check** 命令。

在全局配置模式下，使用下面的命令激活或关闭 MSTP 的兼容模式：

命令	目的
spanning-tree mstp mst-compatible	激活交换机的 MST 兼容模式。
no spanning-tree mstp mst-compatible	关闭交换机的 MST 兼容模式。

请注意：

兼容模式的主要作用是使交换机可以与运行其它 MSTP 协议的交换机建立多生成树区域，在实际组网时，请确保交换机具有相同的配置名称和修订号，并建议将运行其它 MSTP 协议的交换机配置为 CIST 的根，以保证交换机可以通过接收报文而进入兼容模式。

如果没有激活 MST 兼容模式，交换机将不会解析兼容 BPDU 的全部内容，而是仅将其当作普通的RSTP BPDU对待,这样交换机就不能与相连的兼容MSTP交换机处在同一区域中。

对一个已经处在兼容模式的端口，即使通过全局命令关闭交换机的兼容模式，该端口也不会自动恢复到发送标准的 MST BPDU，这时，请使用 **migration-check** 命令。

8.9.15 重启协议转换检查

MSTP 协议允许交换机通过一种协议转换机制与传统的 STP 交换机或不同类型的 MST 交换机协同工作。如果交换机的一个端口接收到 STP 的配置信息，那么该端口就会转为仅发送 STP 报文。接受到 STP 信息的端口也会被认为是一个边界端口。同样，在 MST 兼容模式下，如果一个端口接收到兼容模式的 BPDU，该端口也会转为发送兼容模式的 BPDU。

请注意：
一个端口转入 STP 兼容状态或 MST 兼容状态之后，即使不再接收到相应模式的报文，该端口也不会自动恢复为 MSTP 状态。这种情况下，可以使用 **spanning-tree mstp migration-check** 命令清除端口学习到的生成树协议信息，使之恢复为 MSTP 状态。

运行 RSTP 协议的交换机可以识别并处理 MSTP 报文，因此与 RSTP 交换机协同工作时 MSTP 交换机不需要发生协议转换。

在全局配置模式下，使用下面的命令清除交换机所有端口检测到的生成树协议信息：

命令	目的
spanning-tree mstp migration-check	清除交换机所有端口检测到的生成树协议信息。

在端口配置模式下，使用下面的命令清除端口检测到的生成树协议信息：

命令	目的
spanning-tree mstp migration-check	清除端口检测到的生成树协议信息。

8.9.16 查看多生成树协议信息

在监控模式、全局配置模式以及端口配置模式下，使用下面的命令查看多生成树协议的各种信息：

命令	目的
show spanning-tree	查看生成树协议信息。 （SSTP, PVST, RSTP, MSTP 通用）
show spanning-tree detail	查看生成树协议详细信息。

	（SSTP, PVST, RSTP, MSTP 通用）
show spanning-tree interface *interface-id*	查看生成树协议端口信息。 （SSTP, PVST, RSTP, MSTP 通用）
show spanning-tree mstp	查看所有多生成树实例。
show spanning-tree mstp region	查看多生成树区域配置。
show spanning-tree mstp instance *instance-id*	查看某一个多生成树实例信息。
show spanning-tree mstp detail	查看多生成树详细信息。
show spanning-tree mstp interface *interface-id*	查看多生成树端口配置。
show spanning-tree mstp protocol-migration	查看端口的协议转换状态。

8.10 STP 可选特性介绍

本公司交换机的生成树协议模块支持七种额外的附加功能（下称为“可选特性”），这些功能在缺省情况下是没有配置的，各种生成树协议模式对可选特性的支持情况如下表所示。

可选特性	Single STP	PVST	RSTP	MSTP
Port Fast	Yes	Yes	No	No
BPDU Guard	Yes	Yes	Yes	Yes
BPDU Filter	Yes	Yes	No	No
Uplink Fast	Yes	Yes	No	No
Backbone Fast	Yes	Yes	No	No
Root Guard	Yes	Yes	Yes	Yes
Loop Guard	Yes	Yes	Yes	Yes

8.10.1 Port Fast

Port Fast 特性可以使一个端口立刻进入 Forwarding 状态而不需经过从 Listening 到 Learning 的状态等待。在 SSTP 和 PVST 模式下，可以在直接连接主机或服务器的端口启用 Port Fast 功能，使主机或服务器可以快速的连接到网络。

Prot Fast 特性适用于直连主机的端口，这些端口不会收到 BPDU，也就不会对网络拓扑造成影响，因此可以不经等待而进入转发状态。如果在一个连接交换机的端口上配置了 Port Fast 功能，就有可能造成环路。

Port Fast 特性可以在全局或端口配置模式下进行设置，如果在全局模式下配置，所有的端口都会被认为是 Port Fast 端口而快速进入 Forwarding 状态。这样也更容易产生环路。为了防止因为配置 Port Fast 功能而造成网络环路，可以使用 BPDU Guard 或 BPDU Filter 特性对端口进行保护。

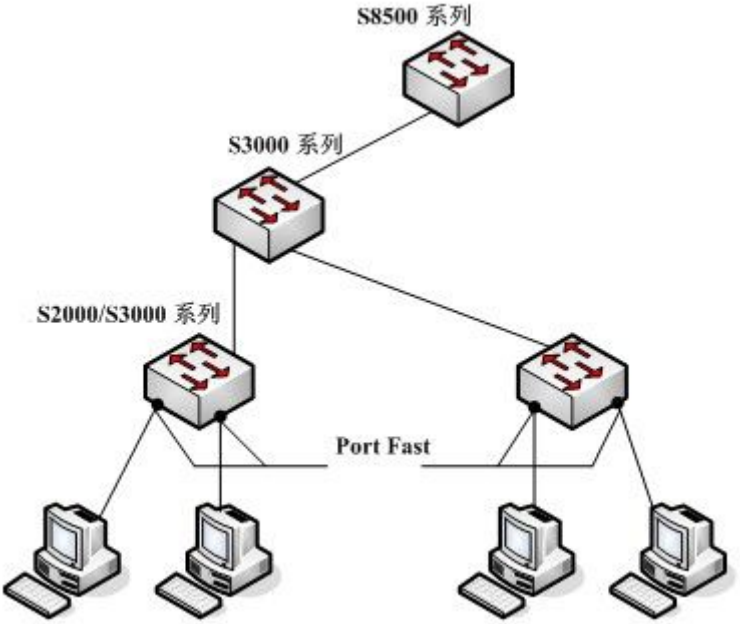


图 1.1 Port Fast 端口

请注意：
快速收敛的生成树协议，RSTP 和 MSTP，在缺省情况下已经支持端口快速进入 Forwarding 状态，因此不需要使用 Port Fast 功能。

8.10.2 BPDU Guard

一个 Port Fast 端口如果会收到 BPDU，可以认为是由于错误的网络配置造成的，BPDU Guard 特性在一个 Port Fast 端口收到 BPDU 之后，被动的对其进行保护。

在不同的生成树协议模式下，BPDU Guard 的行为有所不同。在 SSTP/PVST 模式下，一个同时配置了 BPDU Guard 的 Port Fast 端口如果收到 BPDU，该端口会被强制 shutdown，此后用户只能通过手动配置将其恢复。在 RSTP/MSTP 模式下，一个配置了 BPDU Guard 的端口如果收到 BPDU，该端口的会在一段时间内被设置为 Blocking 状态。

BPDU Guard 特性可以独立于 Port Fast 进行配置。在所有的生成树协议模式下，配置了 BPDU Guard 特性的端口都不会发送 BPDU，但是该端口可以接收 BPDU，并对其进行处理。在 RSTP/MSTP 模式下，可以通过在连接主机的端口上配置 BPDU Guard 来使这些连接到交换机的设备不会收到 BPDU。

BPDU Guard 特性可以在全局或端口模式下进行配置，在全局配置模式下，使用 **spanning-tree portfast bpduguard** 命令可以阻止所有端口发送 BPDU。需要注意的是，在一个较复杂的网络中，不恰当的使用 BPDU Guard 功能可能导致环路。

8.10.3 BPDU Filter

BPDU Filter 特性可以在 SSTP/PVST 模式下使交换机的端口不向外发送 BPDU，同时也是对 Port Fast 端口的另一种保护手段。

在 SSTP/PVST 模式下，一个配置了 BPDU Filter 特性的 Port Fast 端口如果收到 BPDU，该端口的 BPDU Filter 和 Port Fast 特性都会被自动关闭，从而使该端口恢复为一个普通端口，必须经过从 Listening 到 Learning 的等待才能进入 Forwarding 状态。

与 BPDU Guard 特性相同，BPDU Filter 特性也可以在全局或端口下进行配置。在全局配置模式下，**spanning-tree portfast bpdufilter** 命令可以使所有端口都不向外发送BPDU，但是端口仍然可以接收和处理 BPDU。

8.10.4 Uplink Fast

Uplink Fast 特性在交换机到网络根桥的连接中断的情况下，使新的根端口快速进入 Forwarding 状态。

一个较复杂的网络中通常包含多层的设备分布，如图 1.2 所示。其中汇聚层和接入层的交换机都有到上一层的冗余线路连接，并且正常情况下这些冗余连接都被生成树阻塞，以防止环路。

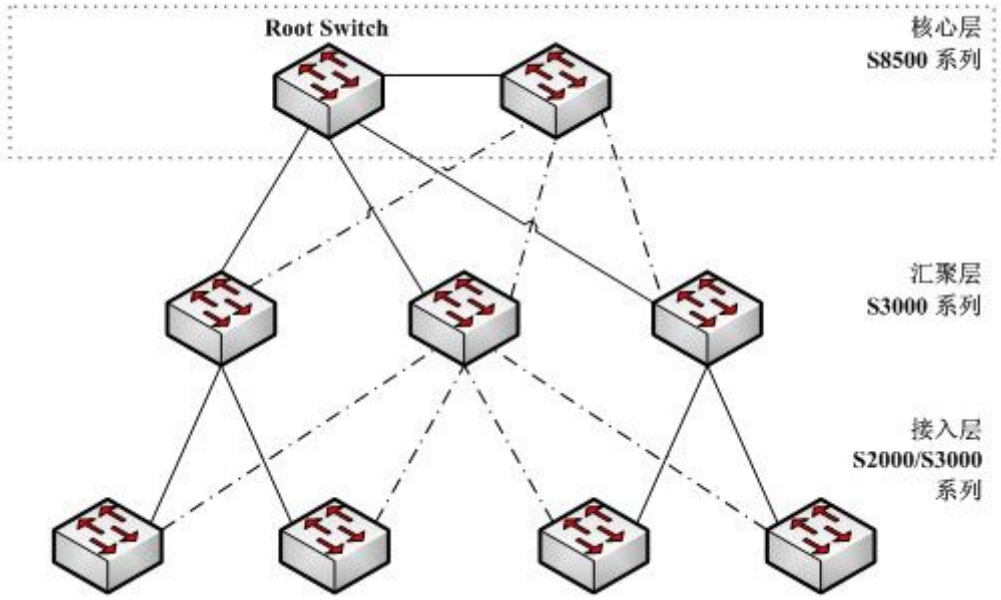


图 1.2 层次化的交换网络示例

假如一台交换机到上层的连接中断（称为 Direct Link Failure），STP 会选择冗余线路上的 Alternate 端口成为新的 Root 端口，该端口在经过从 Listening 到 Learning 的状态变化之后进入 Forwarding 状态。如果通过全局命令 **spanning-tree uplinkfast** 配置了 Uplink Fast 特性，新的 Root 端口可以不经过状态等待而直接进入 Forwarding 状态，使交换机到上层的连接立刻恢复。

图 1.3 通过一个简单网络中的示例显示了 Uplink Fast 特性的工作情况。C 连接 B 的端口在初始状态下为预备端口，当 C 到根桥 A 的连接断开之后，先前的 Alternate 端口被选为新的 Root 端口并且立刻开始转发。

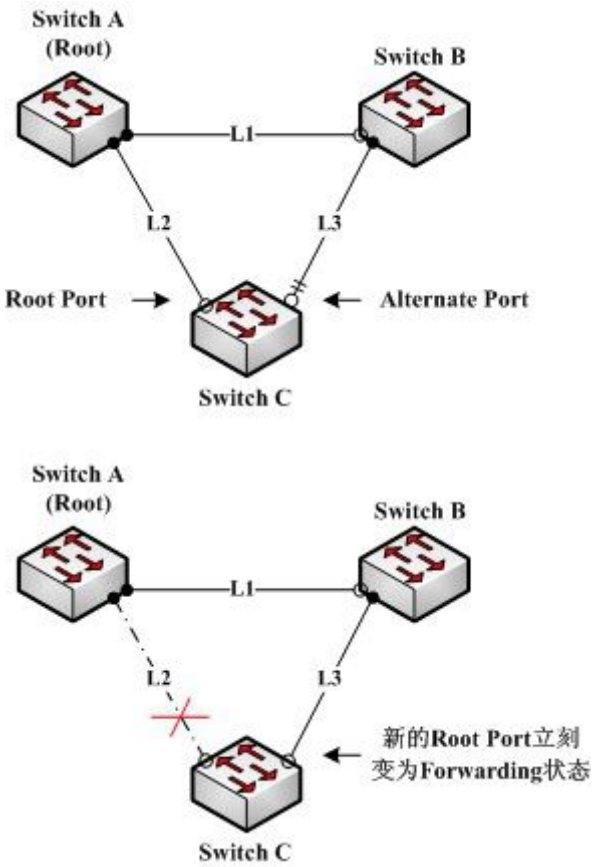


图 1.3 Uplink Fast 示例

请注意：
Uplink Fast 特性适用于慢速收敛的 SSTP 和 PVST。在 RSTP 和 MSTP 模式下，新的根端口总是可以快速进入 Forwarding 状态，而不需要此功能。

8.10.5 Backbone Fast

Backbone Fast 特性是对 Uplink Fast 技术的补充。Uplink Fast 在到达指派交换机的直接连接中断的情况下使冗余线路快速开始工作，而 Backbone Fast 则可以检测上一层网络中发生的、非直连的网络中断，并加速端口的状态变化。

以图 1.3 中的网络为例，交换机 C 到 A 的连接 L2 称为是 C 到根桥的直接连接（Direct Link），该连接的中断可以由 Uplink Fast 功能处理。而 B 到 A 的连接 L1 对 C 来讲是非直接的连接，而该处的连接中断（Indirect Failure）则由 Backbone Fast 特性处理。

Backbone Fast 的工作情况如图 1.4 所示。

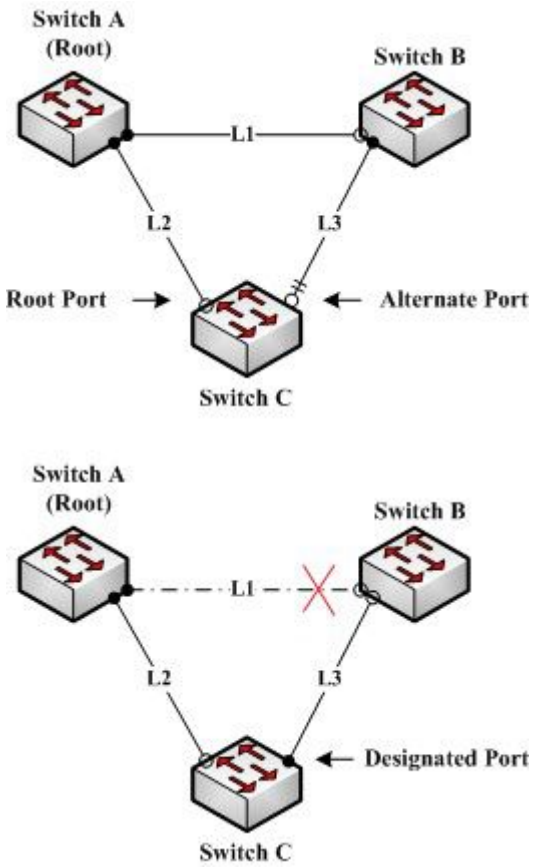


图 1.4 Backbone Fast 示例

假设交换机 C 的网桥优先级高于 B。当 L1 中断时，B 会以自身的网桥优先级作为根优先级发送 BPDU 到 C，对 C 而言，该 BPDU 包含的信息并不比自身更优先。在没有启动 Backbone Fast 的情况下，C 到 B 的端口由于不再收到根桥的 BPDU，该端口会在等待根桥信息老化之后变为指派端口，一般情况下，等待信息老化可能需要几秒钟的时间。如果用过 **spanning-tree backbonefast** 全局配置命令启动了该功能，一旦 C 的 Alternate 端口收到一个优先级较低的 BPDU，C 便可以认为在该端口上，一条非直连的、到达根桥的连接中断，然后立刻更新该端口为指派端口，而不需要等待端口信息老化。

启动 Backbone Fast 之后，不同角色的端口上收到低优先级 BPDU 会导致交换机不同的行为。如果是 Alternate 端口收到该报文，如上面的例子，该端口会被更新为指派端口；如果是在根端口上收到低优先级报文，并且没有其它的预备端口，交换机就会成为根。

需要注意的是，Backbone Fast 特性只是跳过了端口信息老化的时间，新的指派端口仍然需要经过从 Listening 到 Learning 的状态等待才能进入转发状态。

请注意：
与 Uplink Fast 相同，Backbone Fast 特性仅在 SSTP 和 PVST 模式中有效。

8.10.6 Root Guard

Root Guard 特性可以防止一个端口因为收到高优先级的 BPDU 而变为 Root 端口。

在一个较复杂的二层网络中，管理员可能希望某台核心层的交换机作为网络的根桥，但是他却无法对所有的接入层交换机进行管理（可能因为接入层交换机属于其它客户）。这样，其他交换机的不恰当配置会导致核心交换机无法成为根。

可以通过在边缘交换机上配置 Root Guard 功能来防止根桥角色被管理区域之外的交换机抢夺。如果一个配置了 Root Guard 的端口因为收到更高级的 BPDU 被选为 Root Port，Root Guard 会自动将该端口设置为阻塞状态，并将其恢复为一个指派端口。

在 PVST 和 MSTP 模式下，Root Guard 可以在各生成树实例中独立工作。在 MSTP 模式中，如果一个边界端口在 CIST 中因为 Root Guard 被阻塞，该端口在其它所有 MSTI 中都会被阻塞。边界端口是指连接到局域网主机、STP 交换机、RSTP 交换机或者区域之外 MSTP 交换机的端口。

在端口配置模式下，通过 **spanning-tree guard root** 命令在该端口上启动 Root Guard 特性。

请注意：
Root Guard 特性在 SSTP/PVST 和 RSTP/MSTP 中的行为有所不同。在 SSTP/PVST 模式下，Root 端口总是会被 Root Guard 阻塞；而在 RSTP/MSTP 中，端口只有在收到更高级的 BPDU 之后才会被 Root Guard 阻塞，一个原本就具有 Root 角色的端口是不会被阻塞的。

8.10.7 Loop Guard

Loop Guard 特性在一个 Root Port 或 Alternate Port 变为 Designated Port 之后对其进行保护，该功能可以防止因为端口无法持续收到 BPDU 而造成环路。

可以通过 **spanning-tree loopguard default** 全局配置命令启动交换机的 Loop Guard 功能。启动后，一个 Root 端口或 Alternate 端口如果变为 Designated 端口，会被设置为阻塞状态。如果该端口在一段时间之后重新收到高优先级 BPDU，会自动从 Loop Guard 中恢复。

在 PVST 和 MSTP 模式下，Loop Guard 可以在各生成树实例中独立工作。在 MSTP 模式中，如果一个边界端口在 CIST 中因为 Loop Guard 被阻塞，该端口在其它所有 MSTI 中都会被阻塞。

请注意：
Loop Guard 特性在 SSTP/PVST 和 RSTP/MSTP 中的行为有所不同。在 SSTP/PVST 模式下，Designated 端口总是会被 Loop Guard 阻塞；而在 RSTP/MSTP 中，端口只在因为不能收到 BPDU 而变为 Designated 端口之后才会被阻塞，一个因为收到低优先级 BPDU 而具有 Designated 角色的端口是不会被 Loop Guard 阻塞的。

8.11 配置 STP 可选特性

8.11.1 STP 可选特性配置任务

* 配置 Port Fast

* 配置 BPDU Guard
* 配置 BPDU Filter
* 配置 Uplink Fast
* 配置 Backbone Fast
* 配置 Root Guard
* 配置 Loop Guard
* 配置 Loop Fast
* 配置地址表老化保护
* 配置 FDB-Flush

8.11.2 配置 Port Fast

Port Fast 特性在 SSTP/PVST 模式下使一个端口立刻进入 Forwarding 状态而不需经过从 Listening 到 Learning 的状态等待。其它生成树模式下该功能无效。

在全局配置模式下，使用下面的命令配置 Port Fast 功能：

命令	目的
spanning-tree portfast default	全局启动 Port Fast 功能，对所有端口有效。
no spanning-tree portfast default	全局关闭 Port Fast 功能，不影响端口配置。

请注意：
Port Fast 功能仅适用于连接主机的端口，若在全局进行配置，请同时配置 BpduGuard 或 BpduFilter 功能进行保护。

在交换端口配置模式下，使用下面的命令配置 Port Fast 功能：

命令	目的
spanning-tree portfast	对当前端口启动 Port Fast 功能。
no spanning-tree portfast	关闭当前端口的 Port Fast 功能，不影响全局配置。

8.11.3 配置 BPDU Guard

BPDU Guard 特性在端口收到 BPDU 时执行保护动作，配置了该特性的端口不会再发送 BPDU。

在不同的生成树协议模式下，BPDU Guard 的行为有所不同。在 SSTP/PVST 模式下，一个配置了 BPDU Guard 和 Port Fast 特性的端口如果收到 BPDU，该端口会被强制

shutdown，此后用户只能通过手动配置将其恢复。在 RSTP/MSTP 模式下，一个配置了 BPDU Guard 的端口如果收到 BPDU，该端口的会在一段时间内被设置为 Blocking 状态。

在全局配置模式下，使用下面的命令配置 BPDU Guard 特性：

命令	目的
spanning-tree portfast bpduguard	全局启动 BPDU Guard 功能，对所有端口有效。
no spanning-tree portfast bpduguard	全局关闭 BPDU Guard 功能。

请注意：
全局配置 Port Fast 功能，可能导致产生广播风暴。应当同时配置 BPDU Guard 或 Filter 进行保护。

在交换端口配置模式下，使用下面的命令配置 BPDU Guard 特性：

命令	目的
spanning-tree bpduguard enable	启动端口的 BPDU Guard 功能。
spanning-tree bpduguard disable	关闭端口的 BPDU Guard 功能，不影响全局配置。
no spanning-tree bpduguard	关闭端口的 BPDU Guard 功能，不影响全局配置。

8.11.4 配置 BPDU Filter

BPDU Filter 特性可以在 SSTP/PVST 模式下使交换机的端口不向外发送 BPDU，同时也是对 Port Fast 端口的另一种保护手段。

在全局配置模式下，使用下面的命令配置 BPDU Filter 特性：

命令	目的
spanning-tree portfast bpdufilter	全局启动 BPDU Filter 功能，对所有端口有效。
no spanning-tree portfast bpdufilter	全局关闭 BPDU Filter 功能。

请注意：
全局配置 Port Fast 功能，可能导致产生广播风暴。应当同时配置 BPDU Guard 或 Filter 进行保护。

在交换端口配置模式下，使用下面的命令配置 BPDU Filter 特性：

命令	目的
spanning-tree bpdufilter enable	启动端口的 BPDU Filter 特性。
spanning-tree bpdufilter disable	关闭端口的 BPDU Filter 特性，不影响全局配置。
no spanning-tree bpdufilter	关闭端口的 BPDU Filter 特性，不影响全局配置。

8.11.5 配置 Uplink Fast

Uplink Fast 特性在交换机到网络根桥的连接中断的情况下，使新的根端口快速进入 Forwarding 状态。

Uplink Fast 特性仅在 SSTP/PVST 模式下有效。 在全局配置

模式下，使用下面的命令配置 Uplink Fast 特性：

命令	目的
spanning-tree uplinkfast	启动 Uplink Fast 特性。
no spanning-tree uplinkfast	关闭 Uplink Fast 特性。

8.11.6 配置 Backbone Fast

Backbone Fast 特性是对 Uplink Fast 技术的补充。Uplink Fast 在到达指派交换机的直接连接中断的情况下使冗余线路快速开始工作，而 Backbone Fast 则可以检测上一层网络中发生的、非直连的网络中断，并加速端口的状态变化。

Backbone Fast 特性仅在 SSTP/PVST 模式下有效。 在全局配置

模式下，使用下面的命令配置 Backbone Fast 特性：

命令	目的
spanning-tree backbonefast	启动 Backbone Fast 特性。
no spanning-tree backbonefast	关闭 Backbone Fast 特性。

8.11.7 配置 Root Guard

Root Guard 特性可以防止一个端口因为收到高优先级的 BPDU 而变为 Root 端口。

Root Guard 特性在 SSTP/PVST 和 RSTP/MSTP 中的行为有所不同。在 SSTP/PVST 模式下，Root 端口总是会被 Root Guard 阻塞；而在 RSTP/MSTP 中，端口只有在收到更高级的 BPDU 之后才会被 Root Guard 阻塞，一个原本就具有 Root 角色的端口是不会被阻塞的。

在交换端口配置模式下，使用下面的命令配置 Root Guard 特性：

命令	目的
spanning-tree guard root	在端口启动 Root Guard。
no spanning-tree guard	关闭端口的 Root Guard 和 Loop Guard 特性。
spanning-tree guard none	关闭端口的 Root Guard 和 Loop Guard 特性。

8.11.8 配置 Loop Guard

Loop Guard 特性在一个 Root Port 或 Alternate Port 变为 Designated Port 之后对其进行保护，该功能可以防止因为端口无法持续收到 BPDU 而造成环路。

Loop Guard 特性在 SSTP/PVST 和 RSTP/MSTP 中的行为有所不同。在 SSTP/PVST 模式下，Designated 端口总是会被 Loop Guard 阻塞；而在 RSTP/MSTP 中，端口只在因为不能收到 BPDU 而变为 Designated 端口之后才会被阻塞，一个因为收到低优先级 BPDU 而具有 Designated 角色的端口是不会被 Loop Guard 阻塞的。

在全局配置模式下，使用下面的命令配置 Loop Guard 特性：

命令	目的
spanning-tree loopguard default	全局启动 Loop Guard 特性，对所有端口有效。
no spanning-tree loopguard default	全局关闭 Loop Guard。

在交换端口配置模式下，使用下面的命令配置 Loop Guard 特性：

命令	目的
spanning-tree guard loop	启动端口的 Loop Guard 特性。
no spanning-tree guard	关闭端口的 Root Guard 和 Loop Guard 特性。
spanning-tree guard none	关闭端口的 Root Guard 和 Loop Guard 特性。

8.11.9 配置 Loop Fast

注意： 请在技术人员的指导下使用本小节描述的配置命令。

请注意：
交换机软件 2.0.1M 及之前版本，高端交换机 4.0.1A 及之前版本，均不支持本小 节描述的功能。

Loop Fast 特性用于在特殊的网络环境下有限的提升网络的收敛性能。比如，在一个由数十台交换机组成的环网中为每个组成环网的端口启用该特性。

在全局配置模式下，使用下面的命令为所有端口配置 Loop Fast：

命令	目的
spanning-tree loopfast	全局启动 Loop Fast 特性，对所有端口有效。
no spanning-tree loopfast	全局关闭 Loop Fast。

在端口配置模式下，使用下面的命令配置 Loop Fast：

命令	目的

spanning-tree loopfast	启动端口的 Loop Fast 特性。
no spanning-tree loopfast	取消端口的 Loop Fast 配置。 若配置全局的 Loop Fast，特性在端口上仍然有效。
spanning-tree loopfast disable	禁止端口的 Loop Fast。

8.11.10 配置地址表老化保护

请注意：
交换机软件 2.0.1M 及之前版本，高端交换机 4.0.0O 及之前版本，均不支持地址 表老化保护功能。

在网络拓扑变化频繁的情况下，配置地址表老化保护功能可以避免生成树协议因频繁更新 MAC 地址表而影响通信。

快速收敛的生成树协议，比如 RSTP 和 MSTP，在检测到生成树拓扑发生变化时，会对交换机的 MAC 地址表执行清除操作，删除旧的 MAC 地址，加速 MAC 地址的更新，从而确保通信可以快速恢复。在缺省配置下，交换机通过 MAC 地址表快速老化的方式 完成清除操作。对于大多数型号的交换机，地址表的快速老化可以在 1 秒钟以内完成，并且对设备 CPU 的性能影响极小。

开启地址表老化保护功能之后，STP 协议会在执行第一次老化后启动保护定时器，定时器超时之前（缺省为 15 秒）不会再执行老化。若在 15 秒内又发生了网络拓扑变化，协议会在定时器超时之后自动执行第二次老化。

请注意：
通过命令 **no spanning-tree fast-aging** 可以完全禁止 STP 协议执行地址表的老化。在执行此项配置之前，请确保网络不存在环路。否则，网络拓扑变化之后终端设备之间可能需要 **5** 分钟或更长时间才能恢复通信。

在全局配置模式下，通过下面的命令配置地址表老化保护功能：

命令	目的
spanning-tree fast-aging	启动/关闭地址表老化功能。
spanning-tree fast-aging protection	启动/关闭地址表老化保护功能。
spanning-tree fast-aging protection time	配置地址表老化保护的时间。在此时间之内，生成树协议只能执行一次地址表老化。 缺省为 15 秒。

在上述命令之前增加 **no** 前缀可以取消对应的配置。

8.11.11 配置 FDB-Flush

注意：

请在技术人员的指导下使用本小节描述的配置命令。

请注意：
交换机软件 2.0.1M 及之前版本，高端交换机 4.0.0O 及之前版本，均不支持本小 节描述的功能。

交换机的快速生成树协议（RSTP 和 MSTP）在缺省配置下使用地址表快速老化的方 式清除旧的 MAC 地址，而非 FDB-Flush。对于部分机型，FDB-Flush 对地址表的操作比 老化方式更有效，但可能耗费较多的 CPU 资源。

在全局配置模式下，使用下面的命令配置 FDB-Flush：

命令	目的
spanning-tree fast-aging flush-fdb	开启 FDB-Flush。
no spanning-tree fast-aging flush-fdb	关闭 FDB-Flush。

需要注意的是，FDB-Flush 与快速老化功能相互独立，可以在配置 **no spanning-tree fast-aging** 的同时配置 FDB-Flush。但快速老化保护功能对 FDB-Flush 无效。

第 9 章 配置 802.1x

9.1 配置 802.1x 任务列表

* 配置端口的 802.1x 认证
* 配置 802.1x 多主机端口认证
* 配置 802.1x 身份认证请求的最大次数
* 配置 802.1x 的重认证
* 配置 802.1x 发送频率
* 配置 802.1x 用户绑定
* 配置 802.1x 端口的认证方法
* 选择 802.1x 端口的认证类型
* 配置 guest-vlan
* 802.1x 恢复默认配置
* 监控 802.1x 认证配置和状态

9.2 配置 802.1x 任务

9.2.1 配置端口的 802.1x 认证

802.1x 定义了三种端口的控制方式：强制认证通过、强制认证不通过和启动 802.1x 认证。

强制认证通过，表示端口已经认证通过，不需要在使用任何认证过程对端口进行认证，所有的用户都可以通过该端口进行数据访问控制；该模式是端口的默认模式。强制认证不通过，表示端口认证不通过，即使使用任何认证手段对端口进行认证，该端口都不会认证通过，所有的用户都无法通过该端口进行数据访问控制。

启动 802.1x 认证，即端口将运行 802.1x 认证协议，对访问该端口的用户进行 802.1x 认证，只有认证通过后用户都可以通过该端口进行数据访问控制。启动端口的 802.1x 的认证后还要配置 AAA 的认证方法。

在配置 802.1x 前，必须将 802.1x 功能使能，使用下面的命令可以使能 802.1x：

命令	目的

dot1x enable	使能 802.1x 功能 。

使用下面的命令可以启动 802.1x 认证：

命令	目的
dot1x port-control auto	配置端口为 802.1x 协议控制方式。
aaa authentication dot1x {default |list name} method	配置 802.1x 的 AAA 认证。

选择 802.1x 控制方式，可以在接口配置模式下使用下面的任意一个命令：

命令	目的
dot1x port-control auto	端口启动 802.1x 的认证方法。
dot1x port-control force-authorized	端口强制认证通过。
dot1x port-control force-unauthorized	端口强制认证不通过。

9.2.2 配置 802.1x 多主机端口认证

802.1x 的认证主要对单个主机用户进行认证，这时，交换机只允许一个用户进行认证、访问控制，其他用户是不能进行认证和访问的，除非前一个用户退出认证、访问过程；然而有时端口可能通过不支持 802.1x 的交换设备（例如 1108 交换机）与多个主机相连接，为了使这些主机用户都能访问，可以启动多主机端口访问功能。

将一个端口配置为 802.1x 的多主机认证后，交换机将对不同的台主机用户进行认证，当认证通过后，交换机将允许该主机通过交换机进行访问（使用主机的 MAC 进行控制），理论上 802.1x 对主机用户的数量是没有限制的，然而由于交换机对用户的认证控制是通过用户的 MAC 地址进行控制的，这时，主机用户的数量是就会受到交换机的 MAC 地址表大小的限制。

激活 802.1x 多主机端口认证，可以在接口配置模式下使用下面的任意一个命令：

命令	目的
dot1x multiple-hosts	设置 802.1x 多主机端口认证。

9.2.3 配置 802.1x 身份认证请求的最大次数

802.1x 开始认证时或重认证过程中，它会向客户主机发送身份认证请求，然而由于网络的原因造成报文的丢失或延时，这时就应该重新发送该请求报文，达到一定次数后，可以停止该认证请求，认为没有客户主机认证，认证失败。

根据不同的网络环境，更改身份认证请求的最大次数设置，以保证客户端与认证服务器间的认证通过。

配置身份认证请求的最大次数，可以在接口配置模式下使用下面一个或两个命令：

命令	目的
dot1x max-req *count*	配置身份认证请求的最大次数。

9.2.4 配置 802.1x 的重认证

在认证通过后，为了保证认证客户端的合法性，间隔一段时间后还会向客户端进行认证，这时就需要启动重认证功能。

启动重认证功能，当端口认证通过以后，将会周期性的向主机进行认证请求。

配置重认证功能，可以使用下面的命令：

命令	目的
dot1x re-authentication	启动重认证功能。
dot1x timeout re-authperiod *time*	配置重认证的周期。
dot1x reauth-max *time*	配置重认证失败后的重试次数。

9.2.5 控制 802.1x 发送频率

802.1x 认证过程中，它会向客户主机发送数据报文，通过控制 802.1x 发送频率可以调节数据发送以保证客户主机的响应。

配置发送频率，可以使用下面的命令：

命令	目的
dot1x timeout tx-period *time*	设定 802.1x 报文发送频率。

9.2.6 配置 802.1x 用户绑定

802.1x 认证时，可以将用户与某一个端口进行绑，保证端口访问的安全。启动 802.1x 用户绑定功能，可以在接口配置模式下使用下面的命令：

命令	目的
dot1x user-permit *xxxz*	配置端口下绑定的用户。

9.2.7 配置 802.1x 端口的认证方法

802.1x 认证时不同的端口可以使用不同的认证方法，缺省时，802.1x 认证使用 default 方法。

配置 802.1x 认证方法，可以在接口配置模式下使用下面的命令：

命令	目的
dot1x authentication method *yyy*	配置 802.1x 认证方法。

9.2.8 选择 802.1x 端口的认证类型

802.1x 认证时可以选择认证类型，该类型将决定 AAA 使用 Chap 或 Eap 认证(eap 认证支持 md5-challenge 和 eap-tls 方式)；使用 Chap 时 MD5 所需的 challenge 将在本地产生，而使用 Eap 时 challenge 将认证服务器上产生；每一个端口只使用一种认证类型，默认情况下该类型使用全局配置的认证类型，当端口配置了认证类型时就一直使用该认证类型，除非使用 No 命令恢复到默认值。

eap-tls 采用电子证书作为认证凭证，遵循 tls(Translation Layer Security)中 handshake 协议规范，具有更好的安全性。

配置认证类型，可以在全局配置模式下使用下面的命令：

命令	目的
dot1x authen-type {chap|eap}	选择 chap 或 eap。

也可以在接口配置模式下使用下面的命令：

命令	目的
dot1x authentication type {chap|eap}	选择 chap 或 eap 或使用全局下的配置类型。

9.2.9 802.1x 恢复默认配置

将所有的全局配置恢复到默认配置。可以在全局配置模式下使用下面的命令：

命令	目的
dot1x default	将所有的全局配置恢复到默认配置。

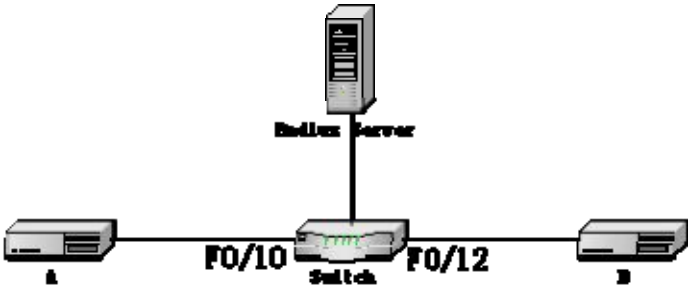
9.2.10 监控 802.1x 认证配置和状态

为了监控 802.1x 认证配置和状态，决定那个 802.1x 参数需要调整，可以在管理模式下使用下面的命令：

命令	目的
show dot1x {*interface ….*}	802.1x 认证配置和状态。

9.3 配置 802.1x 示例

连接如图：



Host A 与交换机的端口 F0/10 相连，Host B 与交换机的端口 F0/12 相连，radius-server host 的 ip 地址为 192.168.20.2，radius 的 key 为 TST；端口 F0/10 的认证使用远程的 radius 认证并且使用了用户绑定，端口 F0/12 的认证使用本地认证没使用用户绑定，但用 eap 类型，并且启用了 Multi-hosts。

全局的配置

```
username switch password 0 TST
username TST password 0 TST
aaa authentication dot1x TST-F0/10 radius
aaa authentication dot1x TST-F0/12 local
interface VLAN1
 ip address 192.168.20.24 255.255.255.0
radius-server host 192.168.20.2 auth-port 1812 acct-port 1813
radius-server key TST
```

端口 F0/10 的配置

```
interface FastEthernet0/10
 dot1x port-control auto
 dot1x authentication method TST-F0/10
 dot1x user-permit radius-TST
```

端口 F0/12 的配置

```
interface FastEthernet0/12
 dot1x multiple-hosts
 dot1x port-control auto
 dot1x authentication method TST-F0/12
 dot1x authentication type eap
```