甲信三层以太网交换机 可靠性通用配置手册

（链路聚合 G.8031 G.8032 STP/RSTP MSTP 环路检测 接口隔离 L2CP BFD 链路震荡保护）

配置指南(CLI)

(Rel_01)

北京甲信技术有限公司（以下简称“甲信”）为客户提供全方位的技术支持和服务。直接向甲信购买产品的用户，如果在使用过程中有任何问题，可与甲信各地办事处或用户服务中心联系，也可直接与公司总部联系。

读者如有任何关于甲信产品的问题，或者有意进一步了解公司其他相关产品，可通过下列方式与我们联系：

公司网址：　　www.jiaxinnet.com.cn

技术支持邮箱：　jxhelp@bjjx.cc

技术支持热线：　400-179-1180

公司总部地址：　北京市海淀区丹棱 SOHO 7 层 728 室

邮政编码:　　100080

声　明

目录

1 可靠性

本章介绍了网络可靠性的基本原理和配置过程，并提供相关的配置案例。

- 链路聚合
- G.8031
- G.8032
- STP/RSTP
- MSTP
- 环路检测
- 接口隔离
- L2CP
- BFD
- 链路震荡保护

1.1 链路聚合

1.1.1 简介

链路聚合通过将多个物理以太网接口聚合在一起形成一个逻辑上的聚合组，并把同一聚合组内的多条物理链路视为一条逻辑链路。链路聚合可以实现流量在聚合组各成员接口之间负载分担，在有效提高设备之间链路可靠性的同时，还在不进行硬件升级的条件下增大了带宽。

按照聚合方式的不同，设备支持以下四种链路聚合方式：

- 手工聚合方式

聚合组中所有接口都参与数据转发，平均分担负载流量，适用于两个直连设备，且一端设备无法使用 LACP 协议的情况。

- 手工主备方式链路聚合方式

聚合组中共有 2 个接口，2 个接口之间形成备份，一个处于 Active 状态，另外一个处于 Shutdown 状态。适用于一端设备无法使用 LACP 协议的情况。

- 静态 LACP 聚合方式

聚合组通过 LACP 协议来选择主动端和活动接口。活动接口用于转发数据，而非活动接口用于备份链路。适用于两端设备均支持 LACP 协议的情况。

- 静态 LACP 主备方式链路聚合方式

聚合组中共有 2 个接口，2 个接口之间形成备份，一个处于 Active 状态，另外一个处于 Shutdown 状态。适用于两端设备均支持 LACP 协议的情况。

1.1.2 配置准备

场景

当需要为 2 台设备之间的链路提供更高的通讯带宽和更高的可靠性时，可以配置选择手工模式或者静态 LACP 链路聚合功能。

前提

- 在配置链路聚合之前，需配置接口的物理参数，使接口的物理层状态为 Up。
- 在同一个链路聚合组中，参与负载分担的成员接口必须有一致的配置，否则数据转发存在问题。这些配置主要包括 QoS、QinQ、VLAN、接口属性、MAC 地址学习几个方面：
  - QoS 配置一致：流量监管、流量整形、拥塞避免、接口限速、SP 队列、WRR 队列调度、WFQ 队列、接口优先级、接口信任模式。
  - QinQ 配置一致：接口的 QinQ 功能使能/禁用状态、添加的外层 VLAN Tag、不同内层 VLAN ID 添加外层 VLAN Tag 的策略。
  - VLAN 配置一致：接口上允许通过的 VLAN、接口缺省 VLAN ID、接口的链路类型（即 Trunk、Hybrid、Access 类型）、子网 VLAN 配置、协议 VLAN 配置、VLAN 报文是否带 Tag 配置。
  - 接口属性配置一致：接口是否加入隔离组、接口速率、双工模式、链路 up/down 状态。
  - MAC 地址学习配置一致：是否使能 MAC 地址学习功能、接口是否具有最大学习 MAC 地址个数的限制。

1.1.3 缺省配置

设备上链路聚合的缺省配置如下。

功能	缺省值
负载均衡模式	**src-dst-mac** 模式
LACP 系统优先级	32768
LACP 接口优先级	32768
LACP 接口模式	**active**
LACP 超时模式	**slow**
最小活动接口数	1

功能	缺省值
最大活动接口数	8

1.1.4 配置手工链路聚合

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**int eth-trunk** *trunk-number*	进入聚合组配置模式。
3	JX(config-eth-trunk-*)#**mode manual**	配置链路聚合组的工作模式为手工链路聚合。
4	JX(config-eth-trunk-*)#**active-linknumber** { **max** | **min** } {*<1-8>* | *default* }	配置 LACP 链路聚合组最大或最小的活跃链路数量。 缺省情况下，最大活跃链路数为 8，最小活跃链路数为 1。
5	JX(config-eth-trunk-*)#**add interface** *interface-type interface-number*	将接口接入聚合
6	JX(config-eth-trunk-*)#**exit**	返回全局配置模式。

1.1.5 配置静态 LACP 链路聚合

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**lacp system-priority** *system-priority*	配置 LACP 协议优先级，优先级高的一端为主动端，LACP 按主动端的配置情况选择活动接口和备份接口。数值越小优先级越高，系统 LACP 优先级相同时，选择系统 MAC 地址小的作为主动端。 缺省情况下，系统的 LACP 优先级为 32768。
3	JX(config)#**interface eth-trunk** *trunk-number*	进入聚合组配置模式。
4	JX(config-eth-trunk-*)#**mode lacp-static**	配置链路聚合组的工作模式为静态 LACP 链路聚合。
5	JX(config-eth-trunk-*)#**lacp timeout** { **fast** | **slow** }	配置 LACP 超时模式。 缺省情况下，LACP 超时模式为慢速模式。

步骤	配置	说明
6	JX(config-eth-trunk-*)#**active-linknumber** { **max** | **min** } { *number* | **default** }	配置 LACP 链路聚合组最大或最小的活跃链路数量。 缺省情况下，最大活跃链路数为 8，最小活跃链路数为 1。
7	JX(config-eth-trunk-*)#**lacp preempt enable**	使能链路聚合组的优先级抢占功能。
8	JX(config-eth-trunk-*)#**lacp preempt delay** *time*	配置端口延时抢占。
9	JX(config-eth-trunk-*)#**add interface** *interface-type interface-number*	将接口接入聚合
10	JX(config-ge-1/0/*)#**lacp priority** *priority*	配置接口的 LACP 协议优先级，接口协议优先级影响 LACP 协议的缺省接口的选举，数值越小优先级越高。 缺省情况下，系统的 LACP 优先级为 32768。
11	JX(config-ge-1/0/*)#**exit**	返回全局配置模式。

说明

- 在静态 LACP 链路聚合组中，成员接口可以处于 Active 或 Standby 两种状态。Active 接口和 Standby 接口都能收发 LACP 协议报文，但 Standby 接口不能转发用户报文。
- 系统按照是否发现邻居、接口速率最大、接口 LACP 协议优先级最高、接口号最小的顺序选择缺省接口，缺省接口处于 Active 状态，与缺省接口具有相同速率、相同对端设备和对端设备操作 key 的接口也处于 Active 状态，其他接口则处于 Standby 状态。

1.1.6 配置主备方式链路聚合

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**int eth-trunk** *trunk-number*	进入聚合组配置模式。
3	JX(config-eth-trunk-*)#**mode** { **manual** | **lacp-static** } **active-standby**	配置链路聚合组的工作模式为手工主备或静态 LACP 主备方式链路聚合。
4	JX(config-eth-trunk-*)#**add primary interface** *interface-type interface-number*	配置链路聚合的主接口。

步骤	配置	说明
4	JX(config-eth-trunk-*)#**add secondary interface** *interface-type interface-number*	配置链路聚合的备接口。
5	JX(config-eth-trunk-*)#**revert enable** JX(config-eth-trunk-*)#**wait-to-store** *time*	配置链路聚合组恢复模式及延迟恢复时间。 缺省情况下，聚合组恢复模式为非返回模式。
6	JX(config-eth-trunk-*)#**exit**	返回全局配置模式。

说明

在配置链路聚合组故障返回模式为非返回模式时，必须先通过 **master-port** 命令进行主接口的配置。

1.1.7 配置聚合组负载分担算法

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**int eth-trunk** *trunk-number*	进入聚合组配置模式。
3	JX(config-eth-trunk-*)#**load-balance** { **src-mac** | **dst-mac** | **srcdst-mac** | **src-ip** | **dst-ip** | **srcdst-ip** | **default** }	基于全局配置链路聚合组的负载均衡模式。 缺省情况下，系统采用 **src-dst-mac** 模式，即依据源和目的 MAC 地址逻辑或的结果选择转发接口。

1.1.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show lacp eth-trunk** *trunk-number*	查看本端系统 LACP 协议接口状态、标志、接口优先级、管理 key、操作 key 和接口状态机状态。邻居 LACP 协议信息，包括标志、接口优先级、设备 ID、Age、操作键值、接口号、接口状态机状态。
2	JX#**show lacp statistics interface eth-trunk** *trunk-number*	查看接口 LACP 协议统计信息，包括 LACP 报文的总收发数、Marker 报文的收发数、Marker Response 报文的收发数和错误报文数。
3	JX#**show lacp information**	查看本端系统的 LACP 系统优先级，MAC 地址，各定时器时间

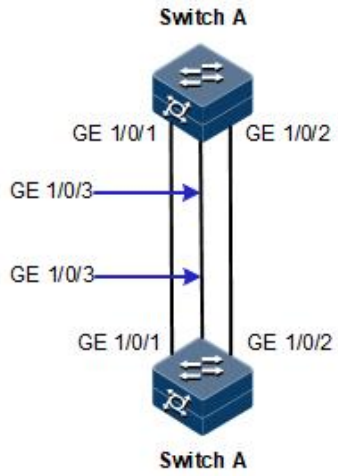
序号	检查项	说明
4	JX#**show** interface **eth-trunk** *trunk-number*	查看当前系统是否使能聚合链路、链路聚合负载均衡模式、当前所有聚合组设置的组成员接口列表和当前生效的成员接口列表等信息。 **说明** 当前生效的成员接口是指组成员接口中接口状态为 Up 的接口列表。

1.1.9 配置静态 LACP 方式的链路聚合示例

组网需求

如下图所示，为提高 Switch A 与 Switch B 之间链路的可靠性，在 Switch A 与 Switch B 之间配置静态 LACP 方式的链路聚合，将 GE 1/0/1、GE 1/0/2 和 GE 1/0/3 加入链路聚合组。

图 1-1 静态 LACP 方式链路聚合应用组网示意图



配置步骤

步骤 1 在 Switch A 上配置静态 LACP 链路聚合组，并将 Switch A 配置成主动端。

```
JX#hostname SwitchA
SwitchA#config
SwitchA(config)#lacp system-priority 1000
SwitchA(config)#int eth-trunk 1
SwitchA(config-eth-trunk-1)#mode lacp-static
SwitchA(config-eth-trunk-1)#add interface ge 1/0/1
SwitchA(config-eth-trunk-1)#add interface ge 1/0/2
SwitchA(config-eth-trunk-1)#add interface ge 1/0/3
SwitchA(config-eth-trunk-1)#exit
```

步骤 2 在 Switch B 上配置静态 LACP 链路聚合组。

```
JX#hostname SwitchB
SwitchB#config
SwitchB(config)#int eth-trunk 1
SwitchB(config-eth-trunk-1)#mode lacp-static
SwitchB(config-eth-trunk-1)#add interface ge 1/0/1
SwitchB(config-eth-trunk-1)#add interface ge 1/0/2
SwitchB(config-eth-trunk-1)#add interface ge 1/0/3
SwitchB(config-eth-trunk-1)#exit
```

检查结果

在 Switch A 上通过 **show lacp eth-trunk 1** 查看静态 LACP 方式链路聚合全局配置是否正确。

```
SwitchA#show lacp eth-trunk 1
------------------------------------------------------------------
------------------------
  LACP Status                 : master
  System Priority             : 1000
  System Mac Address          : f0:f1:f2:f3:01:01
  Member ports number         : 3
  Max Active ports number      : 8
  LACP timeout                : slow
  Preempt state               : disable
  Preempt delay               : 30(s)

 ge-1/0/1 :
   Port Status  : Up and bind
   Local information:
     Mode     Flags   PortPri   AdminKey  OperKey   PortId
State   Status
     active   slow    32768    1        1        449    0x3d
selected
   Partner information:
     SysPri    Flags   PortPri   AdminKey  OperKey   PortId
State   DeviceID
     32768    slow    32768    0        1        449    0x3d
0xf0f1f2f30201

 ge-1/0/2 :
   Port Status  : Up and bind
   Local information:
     Mode     Flags   PortPri   AdminKey  OperKey   PortId
State   Status
     active   slow    32768    1        1        450    0x3d
selected
   Partner information:
     SysPri    Flags   PortPri   AdminKey  OperKey   PortId
State   DeviceID
     32768    slow    32768    0        1        450    0x3d
0xf0f1f2f30201

 ge-1/0/3 :
   Port Status  : Up and bind
   Local information:
```

```
     Mode     Flags   PortPri   AdminKey  OperKey   PortId
State   Status
     active    slow    32768    1         1         451     0x3d
selected
   Partner information:
     SysPri    Flags   PortPri   AdminKey  OperKey   PortId
State   DeviceID
     32768     slow    32768    0         1         451     0x3d
0xf0f1f2f30201
------------------------------------------------------------
------------------------
```

1.2 G.8031

1.2.1 简介

G.8031 是 ITU-T 基于 VLAN 的以太网技术定义的线性保护倒换标准。在保护切换机制中，对工作资源都分配相应的保护资源，如路径和带宽等。相对于 IEEE 定义的生成树保护技术，G.8031 定义的保护技术简单快速，以一种可预测的方式实现网络资源切换，更易于运营商有效地规划网络及明了网络的活动状态，实现电信级的运营。

G.8031 定义了 1+1 和 1:1 两种保护结构，在 1+1 结构中每一个保护资源都对应着一个工作资源，在保护域内，1+1 结构采用双发单收的保护机制；1:1 结构采用保护资源与工作资源彼此切换的机制。

相关概念

- 故障检测机制

G.8031 采用 Y.1731 或 IEEE 802.1ag 中定义的连续性检测(CC)进行链路双向转发检测，能够定位故障点并检测故障是单向还是双向的，并且用于保护转换时，CC 帧默认的传输周期是 3.33 ms（即每秒 300 帧的传输速率）。

两个相邻节点间周期性的从物理端口发送连续性检测(CC)帧以检测故障，当一个节点在特定的时间内检测到 CC 帧丢失，即检测到了一个故障。

节点从检测到故障的端口发送 RDI(Remote Defect Indication)帧，如果是单向故障，链路下行的节点将检测到该 RDI 帧。

- 1+1 保护结构

在 1+1 结构中，保护连接是每条工作连接专用的，工作连接与保护连接在保护域的源端进行桥接。业务在工作和保护连接上同时发向保护域的宿端，在宿端，选择器基于缺陷指示来选择接收来自工作或保护连接上的业务。

1+1 以太网线性保护的倒换类型包括单向倒换和双向倒换。单向倒换时只有受影响的连接方向倒换至保护路径，两端的选择器是独立的，不需要

APS 信令支持。双向倒换的机制与单向类似，通常需要 APS 信令在两端协调。单向保护可以防止在两个独立方向上的单通故障。

1+1 以太网线性保护的操作类型可以是不可恢复或可恢复的。在可恢复模式下，故障链路恢复时，启动 WTR 定时器，WTR 超时后，选择器切换到工作链路；在不可恢复模式下，即使故障链路恢复，选择器仍然连接到保护链路。

- 1:1 保护结构

在 1:1 结构中，保护连接是每条工作连接专用的，被保护的工作业务由工作或保护连接进行传送。工作和保护连接的选择方法基于缺陷指示机制。

1:1 以太网线性保护的倒换类型也包括单向倒换和双向倒换，操作类型可以是可恢复的，也可以是不可恢复的，双向倒换时受影响的和未受影响的连接方向均倒换至保护路径，而单向倒换仅受影响的的连接方向均倒换至保护路径。倒换时源端和宿端连接器需要切换到同一个连接，因此需要自动保护倒换协议 APS 用于协调连接的两端。

在 1:1 保护倒换模式下，基于本地或近端信息和来自另一端或远端的 APS 协议信息，保护倒换由保护域源端选择器桥接和宿端选择器共同来完成。

使用连接性检查包检测工作和保护连接故障，当工作连接故障时，检测到故障的一端选择器切换到保护连接上，同时发送 APS 通知对端，源端收到 APS 同步倒换。

1.2.2 配置准备

场景

无

前提

在配置 G.8031 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up；
- 创建 VLAN；
- 将接口加入 VLAN。

1.2.3 G.8031 的缺省配置

设备上 G.8031 的缺省配置如下。

功能	缺省值
G.8031 模式	返回模式
WTR 定时器	5min
HOLDOFF 定时器	0

1.2.4 创建 G.8031 保护组

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**g8031 instance** *instance-id*	创建 G8031 实例并进入配置节点
3	JX(config-g8031-instance-*)#**control-vlan** *vlan-id*	指定控制 vlan，如果配置了 **revertive dsiable**，则保护组变为非返回模式。非返回模式与返回模式的区别在于，返回模式下工作链路故障恢复时，流量由保护链路切换回工作链路，非返回模式下不切换。缺省情况下，保护组处于返回模式。
4	JX(config-g8031-instance-*)#**data-vlan** *vlan-id*	指定数据 vlan
5	JX(config-g8031-instance-*)# **working-port interface** *interface-type interface-number*	配置端口并指定为工作端口
6	JX(config-g8031-instance-*)# **protection-port interface** *interface-type interface-number*	配置端口并指定为保护端口
7	JX(config-g8032-instance-*)#**wtr-timer** *wtr-time*	配置 WTR 定时器。在返回模式下当工作链路故障恢复时，等待 WTR 定时器超时之后，才会恢复到工作链路上工作。
8	JX(config-g8032-instance-*)#**holdoff-timer** *holdoff-time*	配置环 HOLDOFF 定时器后，当工作链路故障时，系统会延时上报故障，即延时一段时间后再倒换到保护链路，可以防止工作链路震荡引起的频繁倒换。 **说明** HOLDOFF 定时器配置值较大时会影响 50ms 倒换性能，所以推荐使用缺省值 0。

1.2.5 配置 G.8031 倒换控制

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config-g8031-instance-*)#**protection-switch force-switch**	配置流量强制倒换。 强制倒换可配置在多个环节点的多个接口上。

步骤	配置	说明
3	JX(config-g8031-instance-*)#**protection-switch manual-switch**	配置流量手工倒换，优先级低于强制倒换和工作链路故障时产生的自动倒换。 手工倒换只能配置在同一个环节点的一个接口上。
4	JX(config-g8031-instance-*)#**protection-switch clear**	配置流量倒换清除。

1.2.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show g8031 interface**	查看 G.8031 接口状态信息。
2	JX#**show g8031 instance [** ***instanceid*** **]**	查看 G.8031 状态信息。

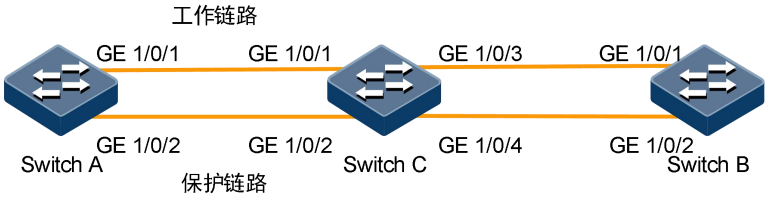
1.2.7 配置 G.8031 保护示例

组网需求

如图 9-2 所示，为提高以太网络的可靠性，Switch A、Switch B、Switch C 三台设备组成 G.8031 保护链路。

协议控制 VLAN 为 2，阻塞的 VLAN 范围为缺省值 2～10。

图 1-2 G.8031 组网示意图



配置步骤

步骤 1 配置接口加入 VLAN 2～VLAN 10。

配置 Switch A。

```
JX#hostname SwitchA
SwitchA#configure
SwitchA(config)#interface ge 1/0/1 to ge 1/0/2
SwitchA(config-ge-1/0/1->ge-1/0/2)#port link-type trunk
SwitchA(config-ge-1/0/1->ge-1/0/2)#port trunk allow-pass vlan
2-10
SwitchA(config-ge-1/0/1->ge-1/0/2)#exit
```

Switch B 配置同 Switch A

配置 Switch C。

```
JX#hostname SwitchC
SwitchC#config
SwitchC(config)#interface ge 1/0/1 to ge 1/0/4
SwitchC(config-ge-1/0/1->ge-1/0/4)#port link-type trunk
SwitchC(config-ge-1/0/1->ge-1/0/4)#port trunk allow-pass vlan
2-10
SwitchC(config-ge-1/0/1->ge-1/0/4)#exit
```

步骤 2 创建保护组。

配置 Switch A。

```
SwitchA(config)#g8031 instance 1
SwitchA(config-g8031-instance-1)#control-vlan 2
SwitchA(config-g8031-instance-1)#data-vlan 2-10
SwitchA(config-g8031-instance-1)#working-port interface ge
1/0/1
SwitchA(config-g8031-instance-1)#protection-port interface ge
1/0/2
```

配置 Switch B。

```
SwitchC(config)#g8031 instance 1
SwitchC(config-g8031-instance-1)#control-vlan 2
SwitchC(config-g8031-instance-1)#data-vlan 2-10
SwitchC(config-g8031-instance-1)#working-port interface ge
1/0/1
SwitchC(config-g8031-instance-1)#protection-port interface ge
1/0/2
```

检查结果

在设备上通过 **show g8031 interface** 查看 G.8031 保护是否生效。

以 Switch A 为例，状态信息如下：

```
SwitchA#show g8031 interface
Instance Interface      Role        Active  Operate   Forward
RxCount   TxCount
-------------------------------------------------------------
---------------------------------------
1       ge-1/0/1       working      active  working
forwarding  0        0
1       ge-1/0/2       protection    standby working   blocking
0        6
-------------------------------------------------------------
---------------------------------------
```

手动断开链路模拟故障，在 Switch A 上再次使用命令查看 G.8031 保护状态

```
SwitchA#show g8031 interface
Instance Interface      Role        Active  Operate   Forward
RxCount   TxCount
```

```
------------------------------------------------------------
--------------------------------------
1       ge-1/0/1       working      standby failed    blocking
0        0
1       ge-1/0/2       protection    active  working
forwarding   0      6
------------------------------------------------------------
--------------------------------------
```

1.3 G.8032

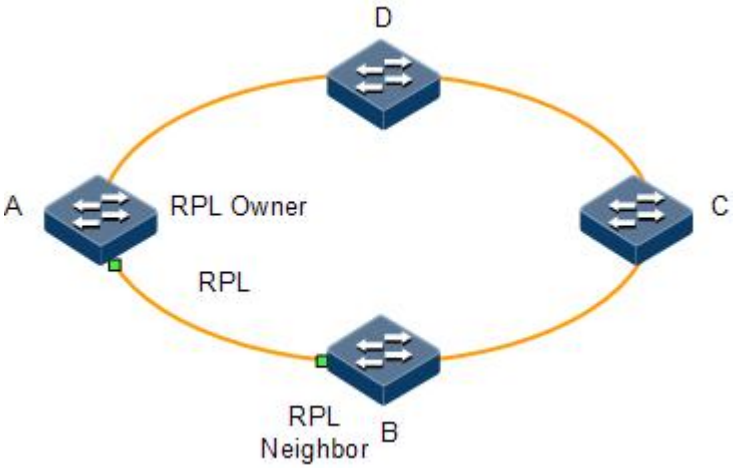
1.3.1 简介

G.8032 以太网环网保护倒换（Ethernet Ring Protection Switching，ERPS）是基于 ITU-T G.8032 标准的 APS 协议，是一种专门应用于以太网环的 链路层协议。正常情况下，它在以太网环中能够防止数据环路引起的广播风暴。当以太网环上链路或设备故障时，能迅速切换到备份链路，保证业务快速恢复。

G.8032 利用环网内专用的控制 VLAN 传递环网控制信息，同时结合环网本身的拓扑特点，在网络发生故障时快速发现，并启用备份链路从而做到快速恢复。

相关概念

图 1-3 G.8032 环网示意图



如图 9-3 所示，G.8032 环网的一些基本概念如下。

- RPL：RPL（Ring Protection Link，环网保护链路）是 RPL 节点间的链路，正常状态下阻塞该链路的相应接口以避免形成环路。一个环网只有一条 RPL。

- RPL Owner：与 RPL 相连的一个环网节点称为 RPL Owner，由用户指定，用于控制 RPL 接口的阻塞或解除阻塞。在正常状态下，RPL Owner 阻塞其 RPL 接口以防止业务形成环路。
- RPL Neighbor：与 RPL 相连的另一个环网节点称为 RPL Neighbor，配合 RPL Owner 完成保护倒换。
- 协议 VLAN：协议 VLAN 是 G.8032 采用的用于承载 R-APS 报文的独立 VLAN 通道。
- 阻塞 VLAN：业务 VLAN，不同于协议 VLAN 承载 R-APS 报文，是进行业务信息传递的 VLAN。
- R-APS 消息：定义在 G.8032 标准中的快速倒换协议报文。包括如下消息类型：
  - FS（Forced Switching）：FS 节点定期发送的消息用于执行强制倒换。
  - SF（Signal Failed）：故障节点定期发送的消息用于上报故障消息。
  - MS（Manual Switching）：MS 节点定期发送的消息用于执行手工倒换。
  - NR，RB（No Request Request Block）：RPL Owner 节点在无故障和无手动命令情况下定期发送通知环上其他节点的消息；用于 RPL Owner 节点阻塞 RPL 后定期发送此消息。
  - NR（No Request）：用于故障或管理命令清除时发送的消息。

在环网保护过程中，会使用 Guard Timer、WTR（Wait To Restore，等待恢复） Timer、WTB（Wait To Block，等待阻塞）Timer 和 Holdoff Timer 四个定时器。

- Guard Timer：用于过滤掉无效的 R-APS 报文，避免环上接收到无效的 R-APS 报文而产生的环上节点的错误保护倒换动作。尤其是在较大的环网络中，节点故障后如果立即恢复，可能会收到从环上传来的邻居节点发送的故障通知，从而再次陷于 Down 状态，而这个通知却是由本节点引起的。配置环 Guard Timer 可以解决这个问题。
- WTR Timer：当工作路径恢复正常时，RPL Owner 上的 WTR Timer 开始计时。当 WTR Timer 计时器超时才恢复业务到工作路径。WTR Timer 用于避免工作路径不稳定而引起频繁倒换。
- WTB Timer：在返回模式下，当手动命令被清除时用于 RPL Owner 上延迟 RPL 端口阻塞的定时器，避免重复阻塞端口带来的震荡。
- Holdoff Timer：当检测到一个或多个新的故障后，如果设置的 Holdoff Timer 值不为 0，则启动 Holdoff Timer。在 Holdoff Timer 未超时时间内，系统会延时发送故障消息，即延时一段时间后再倒换到保护链路，可以防止链路震荡引起的频繁倒换。当 Holdoff Timer 超时，不论触发该定时器启动的这个故障是否仍然存在，都将检查链路状态，若存在故障则发送故障消息至保护倒换。

环状态

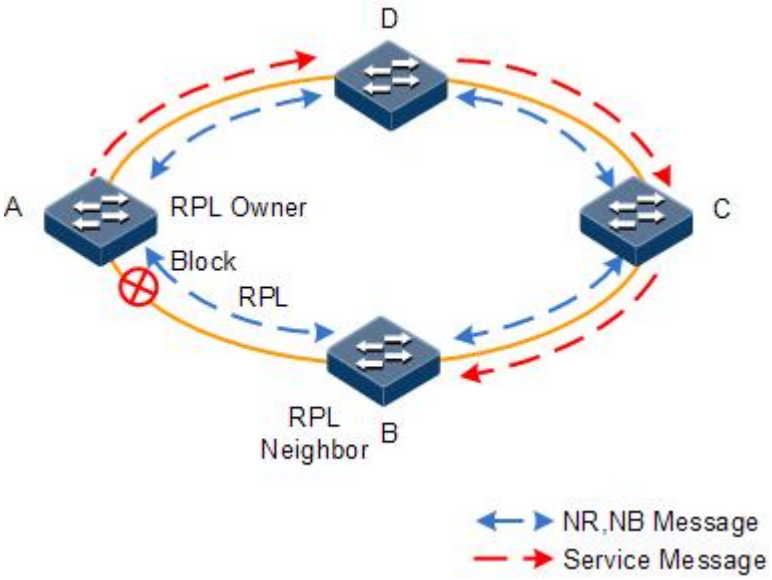
G.8032 定义了环网节点的 5 种状态。

- 空闲状态（Idle State）：无故障时的正常工作状态。

- 保护状态（Protecting State）：检测到链路故障后切换到的保护状态，该自动倒换过程由以太网 OAM（Operation, Administration and Maintenance，操作、管理与维护）的 CCM（Continuity Check Message，故障检测报文）检测到故障而触发。
- 挂起状态（Pending State）：故障修复前的悬而未决状态。
- 强制倒换状态（FS State）：下发强制倒换命令时的状态。
- 手工倒换状态（MS State）：下发手工倒换命令时的状态。

当系统无故障或故障恢复时，G.8032 以太网环处于空闲状态，空闲状态示意图如图 9-4 所示。

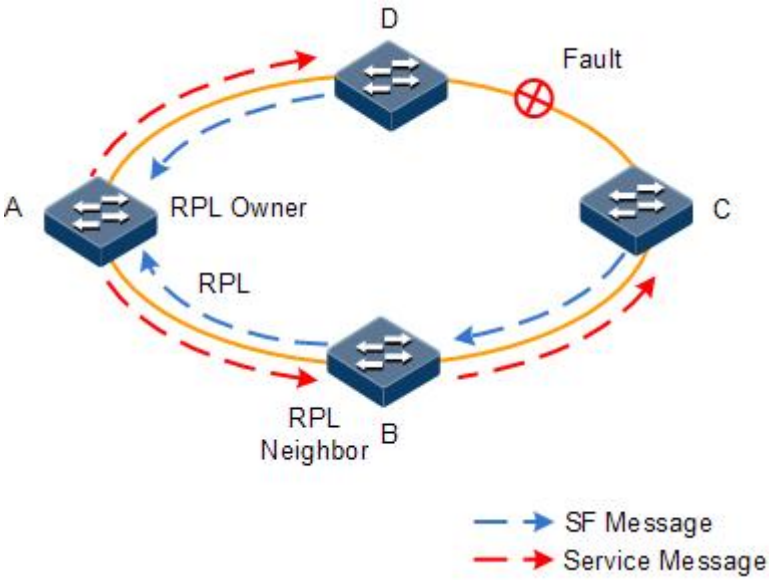
图 1-4 环网空闲状态



如图 9-4 所示，当环网处于空闲状态时，链路有如下的特征：

- 所有的节点在物理拓扑上以环的方式连接。
- G.8032 协议通过 RPL Owner 不断发送（NR，RB）信号，表示无故障，阻塞 RPL 链路，以确保不会成环。
- 相邻节点对每条链路使用以太网 OAM 中的 CCM 报文对链路进行监测。
- 当环路中出现故障时，G.8032 协议采用信号故障（SF）类型触发环路保护倒换。

图 1-5 环网保护状态



如图 9-5 所示当检测到环网故障时，启动自动保护倒换，进入保护状态：

- 在 Holdoff Timer 超时后，RPL Owner 触发与故障链路相邻的节点对故障链路进行阻塞，并发送 SF 信号向链路中其它节点报告该故障。如图 9-5 中的 C、D 节点间的故障发生后，D 节点和 C 节点分别向其它节点发送 SF 信号。
- SF 信号触发 RPL Owner 打开阻塞接口，并触发所有节点进行 FDB（Forwarding Database，转发数据库）清空，进入保护状态。

当故障恢复时，链路进行故障恢复倒换：

- 故障相邻的节点继续保持阻塞状态，Guard Timer 超时后，C、D 节点向其它节点发送 R-APS 的 NR 信号，表示没有本地故障请求。
- 当 RPL Owner 收到第一个 NR 信号后，立即启动 WTR Timer。
- 当 WTR 超时后，RPL Owner 阻塞 RPL，并发送 R-APS 的（NR，RB）信号，表示无本地故障请求，RPL 链路为阻塞状态。
- 其他节点收到该信号后，刷新 MAC 地址转发 FDB，发送 NR 信号的节点停止周期性发送报文，并打开原因故障阻塞的接口。
- 链路中各节点返回空闲状态。

子环

G.8032 的修订版增加了以太网多环的保护方案。子环是现存环网的附属环，通过互联节点（连接多个环的节点）与其它环或网络连接构成环。子环并不闭合，互联节点也不属于子环。

图 1-6 子环模型

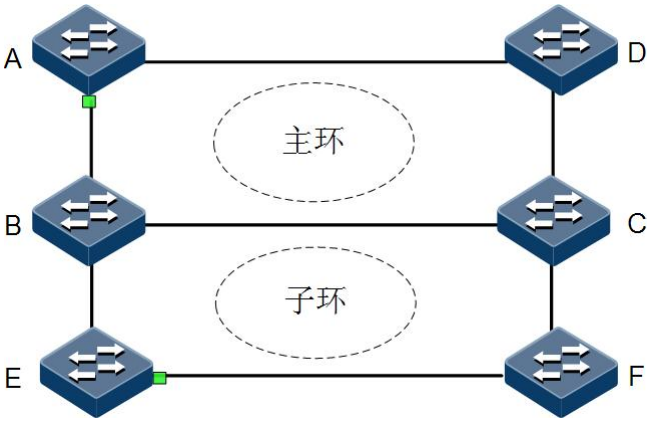


图 9-6 中，B 和 C 为互联节点，连接两个互联节点之间的通道称为 R-APS 虚通道，R-APS 虚通道用于相交环拓扑中的相交节点，如果相交环带有 R-APS 虚通道，则主环为子环 APS 报文提供虚拟通路，即子环 APS 报文会被传送到主环；如果不带，则主环不为子环提供虚拟通路，即子环 APS 报文在相交节点处被终结。主环和子环各自成环，每个环设定自己的 RPL Owner。多环的保护和单环类似，各自处理自己环内的故障。当互联节点间的共享链路出现故障时，主环切换到保护状态，子环不做处理。

因为子环的数据需要通过主环转发，所以主环设备上会存在子环的 MAC 地址列表，在子环出现故障时需要通过 Propagate 开关及时通知主环刷新 FDB，避免流量丢失。

环模式

返回模式与非返回模式的区别如下：

- 返回模式：等待 WTR 定时器超时后，流量切换到未发生故障前的链路进行转发。
- 非返回模式：等待 WTR 定时器超时后，流量不切换到未发生故障前的链路。缺省情况下，保护环处于返回模式。

子环的虚通路模式如下：

- **with** 模式：子环使用 R-APS 虚通道。主环为子环 APS 报文提供通路，子环相交节点收到子环 APS 报文会传送到主环，利用主环完成子环相交节点间的通信。
- **without** 模式：子环不使用 R-APS 虚通道。相交节点上子环 APS 报文要求终结，不会传送到主环。这种方式要求子环不能阻塞子环协议 VLAN（以保证子环报文可以通过 Owner）。

1.3.2 配置准备

场景

随着以太网向电信级网络的发展，语音、视频组播业务对以太网的冗余保护和故障恢复时间提出了更高的要求。现有的 STP 机制对故障恢复的收敛时间都在秒级，远远达不到要求。G.8032 技术通过定义环上节点的不同角色，在正常情况下阻断环路防止产生广播风暴，在环上链路或节点故障的情况下迅速切换到备份链路，从而实现消除环路、故障保护倒换和自动故障恢复等功能，并且故障保护倒换时间低于 50ms，支持单环、相交环和相切环三种组网方式。

G.8032 提供基于物理接口状态来检测故障，能够快速获知链路故障达到快速倒换的目的，适用于相邻设备之间。

前提

在配置 G.8032 之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up；
- 创建 VLAN；
- 将接口加入 VLAN。

1.3.3 G.8032 的缺省配置

设备上 G.8032 的缺省配置如下。

功能	缺省值
保护环模式	返回模式
环 WTR 定时器	5min
环协议版本	2
Guard 定时器	500ms
环 HOLDOFF 定时器	0
相交节点上子环虚通路模式	with 模式
相交节点上环 Propagate 开关	禁止

1.3.4 创建 G.8032 保护环

注意

环上只允许一台设备配置为 RPL（Ring Protection Link，环保护链路）Owner，一台设备配置为 RPL Neighbour，其他设备只能配置为环转发节点。

相切环实际为两个独立的单环，配置与普通单环相同；相交环分为主环和子环，主环与单环配置相同，子环配置请参见“9.3.5 创建 G.8032 保护子环”。

ERPS 环接口需要工作在 switch 交换模式。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**g8032 instance** *instance-id*	创建 G8032 实例并进入配置节点
3	JX(config-g8032-instance-*)#**control-vlan** *vlan-id*	指定控制 vlan，如果配置了 **revertive dsiable**，则保护环变为非返回模式。非返回模式与返回模式的区别在于，返回模式下工作链路故障恢复时，流量由环保护链路切换回工作链路，非返回模式下不切换。缺省情况下，保护环处于返回模式。
4	JX(config-g8032-instance-*)#**data-vlan** *vlan-id*	指定数据 vlan
5	JX(config-g8032-instance-*)# **add interface** *interface-type interface-number* [**rpl** { **owner** | **neighbor** }]	配置端口并指定 rpl 角色
6	JX(config-g8032-instance-*)#**version** { **v1** | **v2** }	配置协议版本。同一个环上所有节点协议版本应一致，版本 1 通过协议 VLAN 区分不同环，因此不同环需配置不同的协议 VLAN，即使使用协议版本 2 也建议不同环配置不同的协议 VLAN。
7	JX(config-g8032-instance-*)#**guard-timer** *guard-time*	配置环 Guard 定时器后，到时之前的时间内不转发收到的任何协议报文。在节点发生恢复事件时 guard 定时器启动。在较大的环网络中，节点故障后如果立即恢复，可能会收到从环上传来的邻居节点发送的过时的故障通知，从而再次陷于 Down 状态，而这个通知却是由本节点引起的。
8	JX(config-g8032-instance-*)#**wtr-timer** *wtr-time*	配置环 WTR 定时器。在返回模式下当工作链路故障恢复时，等待 WTR 定时器超时之后，才会恢复到工作链路上工作。

步骤	配置	说明
9	JX(config-g8032-instance-*)#**holdoff-timer** *holdoff-time*	配置环 HOLDOFF 定时器后，当工作链路故障时，系统会延时上报故障，即延时一段时间后再倒换到保护链路，可以防止工作链路震荡引起的频繁倒换。 **说明** HOLDOFF 定时器配置值较大时会影响 50ms 倒换性能，所以推荐使用缺省值 0。

1.3.5 创建 G.8032 保护子环

注意

- 只有相交环存在主环和子环之分。
- 相交环主环的配置与单环或相切环相同，具体配置请参见“创建 G.8032 保护环”。
- 配置相交环时应先配置主环，再配置子环，否则子环找不到主环接口，将无法建立子环虚通路。
- 子环的实例号必须大于主环的实例号。
- 相交环子环上的非相交节点配置与单环或相切环相同，具体配置请参见“9.3.4 创建 G.8032 保护环”。
- ERPS 环接口需要工作在 switch 交换模式。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)# **g8032 instance** *instance-id*	创建实例

步骤	配置	说明
3	JX(config-g8032-instance-*)#**control-vlan** *vlan-id*	指定控制 vlan，如果配置了 **revertive dsiable**，则保护环变为非返回模式。非返回模式与返回模式的区别在于，返回模式下工作链路故障恢复时，流量由环保护链路切换回工作链路，非返回模式下不切换。缺省情况下，保护环处于返回模式。 **说明** 相交环两个相交节点之间的链路属于主环，所以在相交节点上配置子环时只能配置 port1 或 port2，不能同时配置。
4	JX(config-g8032-instance-*)#**data-vlan** *vlan-id*	指定数据 vlan
5	JX(config-g8032-instance-*)#**virtual-control-vlan** *vlan-id*	指定虚通道 vlan
5	JX(config-g8032-instance-*)# **add interface** *interface-type interface-number* [**rpl** { **owner** | **neighbor** }]	配置端口并指定 rpl 角色
6	JX(config-g8032-instance-*)# **add interface** *interface-type interface-number* **vc-mep**	配置端口并指定为 vc-mep

1.3.6 配置 G.8032 倒换控制

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config-g8032-instance-*)#**force-switch** *interface-type interface-number*	配置环上的流量强制倒换。 强制倒换可配置在多个环节点的多个接口上。
3	JX(config-g8032-instance-*)#**manual-switch** *interface-type interface-number*	配置环上的流量手工倒换，优先级低于强制倒换和工作链路故障时产生的自动倒换。 手工倒换只能配置在同一个环节点的一个接口上。

说明

缺省情况下，工作链路故障时流量会自动倒换到保护链路。所以只在某些特殊情况下才需要配置 ERPS 倒换控制。

1.3.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show g8032 interface**	查看 G.8032 环接口状态信息。
2	JX#**show g8032 instance**	查看 G.8032 环状态信息。

1.3.8 维护

用户可以通过以下命令，维护设备 ERPS 特性的运行情况和配置情况。

命令	描述
JX(config-g8032-instance-*)#**clear**	清除环倒换控制命令（force-switch、manual-switch、WTR 定时器超时和 WTB 定时器超时）的作用。

1.3.9 配置单环 G.8032 保护示例

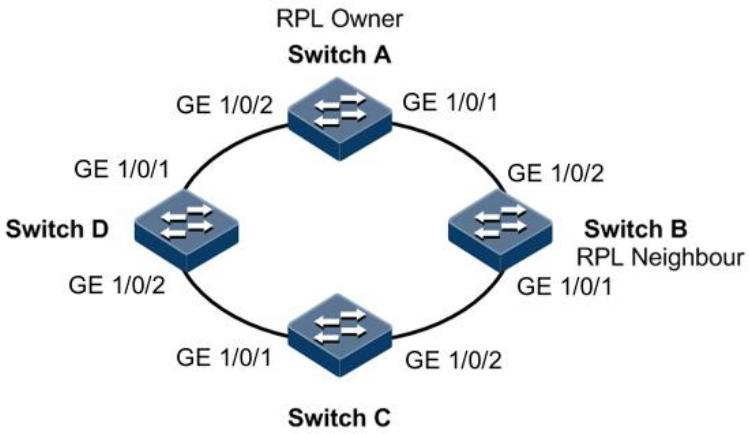
组网需求

如所示，为提高以太网络的可靠性，Switch A、Switch B、Switch C 和 Switch D 四台设备组成 G.8032 单环。

Switch A 设备作为 RPLOwner，Switch B 为 RPL Neighbour，Switch A 和 Switch B 之间的 RPL 链路阻塞。

协议控制 VLAN 为 1，阻塞的 VLAN 范围为缺省值 2～10。

图 1-7 单环 G.8032 应用组网示意图



配置步骤

步骤 1 配置接口加入 VLAN 2～VLAN 10。

配置 Switch A。

```
JX#hostname SwitchA
SwitchA#config
SwitchA(config)#interface ge 1/0/1 to ge 1/0/2
SwitchA(config-ge-1/0/1->ge-1/0/2)#port link-type trunk
SwitchA(config-ge-1/0/1->ge-1/0/2)#port trunk allow-pass vlan
2-10
SwitchA(config-ge-1/0/1->ge-1/0/2)#exit
```

Switch B，Switch C，Switch D 配置同 Switch A

步骤 2 创建 ERPS 保护环。

配置 Switch A。

```
SwitchA(config)#g8032 instance 1
SwitchA(config-g8032-instance-1)#control-vlan 1
SwitchA(config-g8032-instance-1)#data-vlan 2-10
SwitchA(config-g8032-instance-1)#add interface ge 1/0/1 rpl
owner
SwitchA(config-g8032-instance-1)#add interface ge 1/0/2
```

配置 Switch B。

```
SwitchB(config)#g8032 instance 1
SwitchB(config-g8032-instance-1)#control-vlan 1
SwitchB(config-g8032-instance-1)#data-vlan 2-10
SwitchA(config-g8032-instance-1)#add interface ge 1/0/1 rpl
neighbor
SwitchA(config-g8032-instance-1)#add interface ge 1/0/2
```

配置 Switch C。

```
SwitchC(config)#g8032 instance 1
SwitchC(config-g8032-instance-1)#control-vlan 1
SwitchC(config-g8032-instance-1)#data-vlan 2-10
SwitchC(config-g8032-instance-1)#add interface ge 1/0/1
SwitchC(config-g8032-instance-1)#add interface ge 1/0/2
```

配置 Switch D。

```
SwitchD(config)#g8032 instance 1
SwitchD(config-g8032-instance-1)#control-vlan 1
SwitchD(config-g8032-instance-1)#data-vlan 2-10
SwitchD(config-g8032-instance-1)#add interface ge 1/0/1
SwitchD(config-g8032-instance-1)#add interface ge 1/0/2
```

检查结果

在设备上通过 **show g8032 interface** 查看 G.8032 保护环是否生效。

以 Switch A 为例，RPL 链路被阻断防止环路产生，WTR 定时器超时后环状态信息如下：

```
SwitchA#show g8032 interface

Instance Interface      Role    Type    Operate   Forward
Rx-Count  Tx-Count

-------------------------------------------------------------
---------------------------------------
1       ge 1/0/1       port1   rpl     working   blocking    0
15
1       ge 1/0/2       port2   normal  working   forwarding  0
11
-------------------------------------------------------------
---------------------------------------
```

手动断开 Switch B 和 Switch C 之间的链路模拟故障，在 Switch A 上再次使用命令查看 G.8032 保护环状态，RPL 链路切换为转发状态。

```
SwitchA#show g8032 interface
Instance Interface      Role    Type    Operate   Forward
Rx-Count  Tx-Count
-------------------------------------------------------------
---------------------------------------
1       ge 1/0/1       port1   rpl     working   forwarding  16
41
1       ge 1/0/2       port2   normal  failed    blocking    18
42
-------------------------------------------------------------
---------------------------------------
```

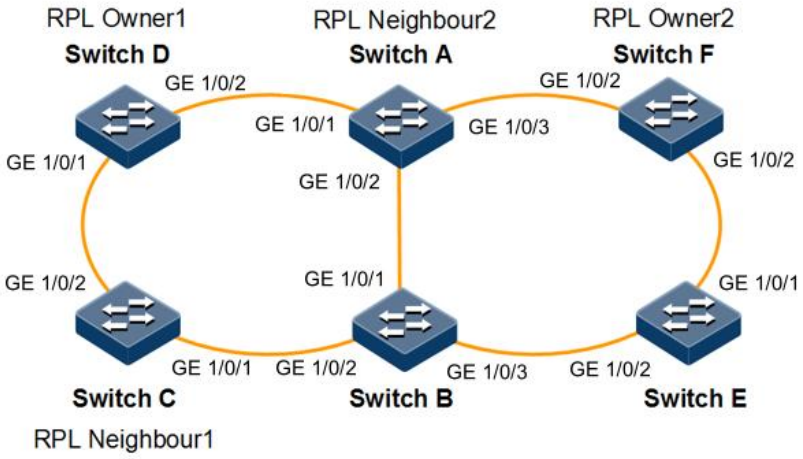
1.3.10 配置相交环 G.8032 保护示例

组网需求

如图 9-8 所示，为提高以太网络的可靠性，Switch A、Switch B、Switch C、Switch D、Switch E 和 Switch F 六台设备以 ERPS 相交环的形式组网。

- Switch A、Switch B、Switch C 和 Switch D 组成主环，Switch D 为主环 RPL Owner，Switch C 为主环 RPL Neighbour，阻断端口为 Switch D 的 GE 1/0/1，协议控制 VLAN 采用 VLAN 1。
- Switch A、Switch B、Switch E 和 Switch F 组成子环，Switch F 为子环 RPL Owner，Switch A 为子环 RPL Neighbour，阻断端口为 Switch F 的 GE 1/0/1，协议控制 VLAN 为 VLAN 4094。
- 主环和子环的阻塞 VLAN 范围均为缺省的 1～4094。

图 1-8 相交环 G.8032 应用组网示意图



配置步骤

步骤 1 创建 VLAN，并配置接口加入 VLAN。

配置 Switch A & B。

```
Switch#configure
Switch(config)#vlan 1-4094
Switch(config)#interface ge 1/0/1 to ge 1/0/3
Switch(config-ge-1/0/1->ge-1/0/3)#port link-type trunk
Switch(config-ge-1/0/1->ge-1/0/3)#port trunk allow-pass vlan
all
Switch(config-ge-1/0/1->ge-1/0/3)#exit
```

配置 Switch C & D & E & F。

```
Switch#config
Switch(config)#vlan 1-4094
Switch(config)#interface ge 1/0/1 to GE 1/0/2
Switch(config-ge-1/0/1->ge-1/0/2)#port link-type trunk
Switch(config-ge-1/0/1->ge-1/0/2)#port trunk allow-pass vlan
all
```

```
Switch(config-ge-1/0/1->ge-1/0/2)#exit
```

步骤 2 创建 G.8032 保护环主环。

配置 Switch A & B。

```
Switch(config)#g8032 instance 1
Switch(config-g8032-instance-1)#control-vlan 1
Switch(config-g8032-instance-1)#data-vlan 1-4094
Switch(config-g8032-instance-1)#add interface ge 1/0/1
Switch(config-g8032-instance-1)#add interface ge 1/0/2
```

配置 Switch C。

```
Switch(config)#g8032 instance 1
Switch(config-g8032-instance-1)#control-vlan 1
Switch(config-g8032-instance-1)#data-vlan 1-4094
Switch(config-g8032-instance-1)#add interface ge 1/0/1
Switch(config-g8032-instance-1)#add interface ge 1/0/2 rpl
neighbour
```

配置 Switch D。

```
Switch(config)#g8032 instance 1
Switch(config-g8032-instance-1)#control-vlan 1
Switch(config-g8032-instance-1)#data-vlan 1-4094
Switch(config-g8032-instance-1)#add interface ge 1/0/1 rpl owner
Switch(config-g8032-instance-1)#add interface ge 1/0/2
```

步骤 3 配置 G.8032 保护环子环。

配置 Switch A。

```
Switch(config)#g8032 instance 2
Switch(config-g8032-instance-2)#control-vlan 4094
Switch(config-g8032-instance-2)#data-vlan 1-4094
Switch(config-g8032-instance-2)#add interface ge 1/0/3 rpl owner
Switch(config-g8032-instance-2)#virtual-control-vlan 3
```

配置 Switch B。

```
Switch(config)#g8032 instance 2
Switch(config-g8032-instance-2)#control-vlan 4094
Switch(config-g8032-instance-2)#data-vlan 1-4094
Switch(config-g8032-instance-2)#add interface ge 1/0/3
Switch(config-g8032-instance-2)virtual-control-vlan 3
```

配置 Switch E。

```
Switch(config)#g8032 instance 2
Switch(config-g8032-instance-2)#control-vlan 4094
Switch(config-g8032-instance-2)#data-vlan 1-4094
Switch(config-g8032-instance-2)#add interface ge 1/0/1
Switch(config-g8032-instance-2)#add interface ge 1/0/2
```

配置 Switch F。

```
Switch(config)#g8032 instance 2
Switch(config-g8032-instance-2)#control-vlan 4094
Switch(config-g8032-instance-2)#data-vlan 1-4094
Switch(config-g8032-instance-2)#add interface ge 1/0/1 rpl
neighbour
Switch(config-g8032-instance-2)#add interface ge 1/0/2
```

检查结果

在设备上通过 **show g8032 interface** 查看 G.8032 保护环是否生效。

分别在 Switch A、Switch D 和 Switch F 上检查，等待 WTR 定时器超时后，结果如下。

```
SwitchD#show g8032 interface

Instance Interface      Role    Type    Operate   Forward
Rx-Count  Tx-Count

-----------------------------------------------------------------
---------------------------------------
1       ge 1/0/1       port1   rpl     working   blocking    0
15
1       ge 1/0/2       port2   normal  working   forwarding  0
11
-----------------------------------------------------------------
---------------------------------------
```

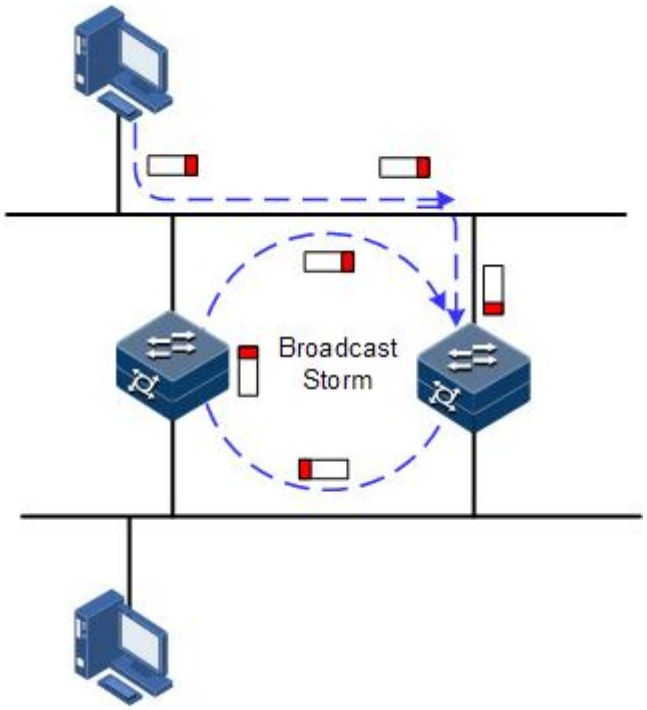
1.4 STP/RSTP

1.4.1 简介

STP

随着网络结构的日益复杂和网络中交换机数量的增多，网络环路成为以太网中最突出的问题。由于交换机对报文的广播机制，网络环路会使得网络中产生网络风暴，耗尽网络资源，对正常的数据转发产生严重的影响。由于网络环路产生的网络风暴示意图如下图所示。

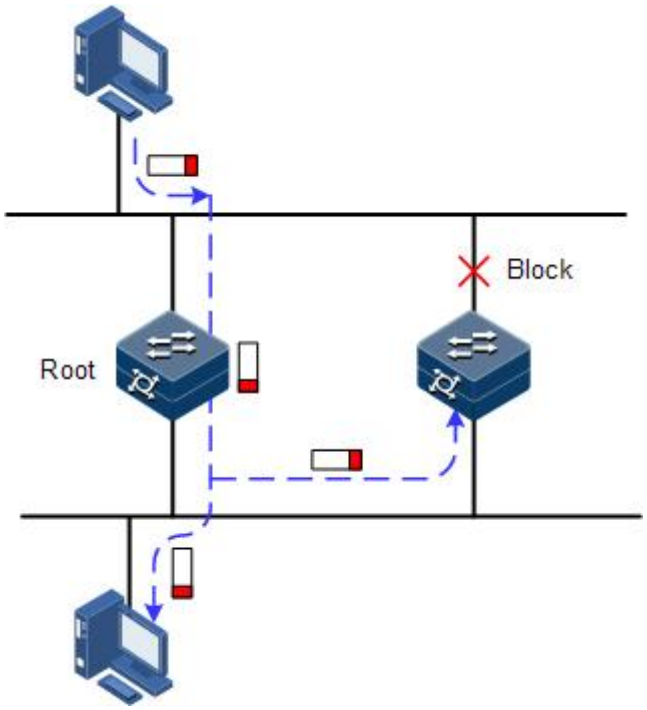
图 1-9 网络环路造成网络风暴示意图



STP（Spanning Tree Protocol，生成树协议）是根据 IEEE 802.1d 标准建立的，用于在局域网中消除数据链路层物理环路的协议。

运行 STP 的设备可以通过彼此交互 BPDU（Bridge Protocol Data Unit，桥协议数据单元）报文进行根交换机的选举、根端口和指定端口的选择，并根据选择结果对设备中存在环路的接口进行逻辑上的阻塞，最终将环路网络结构修剪成以某一台设备为根（Root）的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而导致广播风暴，并避免主机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。运行了 STP 协议的环网示意图如下图所示。

图 1-10 运行 STP 协议的环网示意图



虽然 STP 协议能够很好的消除环网，防止广播风暴的产生，但是随着应用的深入和网络技术的发展，STP 协议的缺点也逐渐暴露了出来。

STP 协议的主要缺点表现在收敛速度较慢。

RSTP

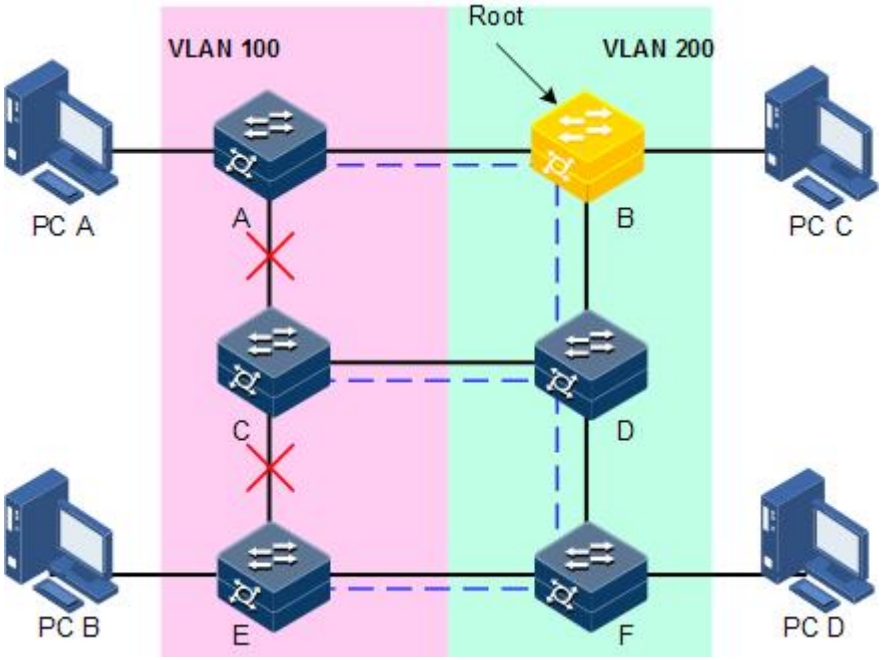
为了弥补 STP 协议收敛速度较慢的不足，IEEE 802.1w 制定了 RSTP（Rapid Spanning Tree Protocol，快速生成树协议）。在普通 STP 协议的基础上，增加了接口可以快速由阻塞状态转变为转发状态的机制，加快了拓扑的收敛速度。

STP/RSTP 协议的目的都是将一个桥接的局域网，修剪成为逻辑拓扑上的一棵单一的生成树，从而避免广播风暴的产生。

由于 VLAN 技术快速发展，STP/RSTP 的局限性逐渐暴露出来。STP/RSTP 协议将网络拓扑修剪为单一生成树，会导致以下问题：

- 整个交换网络只有一个生成树，在网络规模比较大的时候会导致较长的收敛时间。
- 链路被阻塞后将不承载任何流量，造成带宽的浪费。
- 在网络结构不对称时，可能造成部分 VLAN 的报文无法转发。如下图所示，由于 RSTP 协议，选举 Switch B 为根交换机，且逻辑上阻断了 Switch A 和 Switch C 之间的链路，造成 VLAN 100 中的 VLAN 报文无法转发，Switch A 和 Switch C 无法通信。

图 1-11 RSTP 协议造成 VLAN 报文无法转发示意图



1.4.2 配置准备

场景

在较大型的局域网中，有多台设备进行级连满足多主机相互访问的需求，为防止设备之间组成环路造成 MAC 地址学习错误，并导致数据帧快速在环路中进行复制转发造成广播风暴、网络瘫痪，需要在这些设备上开启 STP。通过 STP 协议计算，阻塞掉环路当中的其中一个接口，保证每一个数据流去往目的主机的路径只有一条，并且被 STP 协议计算为最优路径。

前提

无

1.4.3 STP 的缺省配置

设备上 STP 的缺省配置如下。

功能	缺省值
全局 STP 功能状态	禁止
接口 STP 功能状态	使能
设备的 STP 优先级	32768
接口的 STP 优先级	128
接口的路径开销	0

功能	缺省值
Max Age 定时器	20s
Hello Time 定时器	2s
Forward Delay 定时器	15s

1.4.4 使能 STP 功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**stp mode** { **stp** | **rstp** | **mstp** | **default** }	配置生成树的运行模式。
3	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
4	JX(config-ge-1/0/*)#**stp enable**	使能接口生成树协议。

1.4.5 配置 STP 参数

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**stp priority** *priority-value*	配置设备优先级。
3	JX(config)#**interface** *interface-type interface-number* JX(config-ge-1/0/*)#stp **priority** *priority-value*	配置设备接口优先级。
4	JX(config-ge-1/0/*)#**stp path-cost** *cost-value*	配置设备接口路径开销。
5	JX(config)#**stp hello-time** *value*	配置 Hello Time 的值。
6	JX(config)#**stp forward-delay** *value*	配置 Forward Delay 的值。
7	JX(config)#**stp max-age** *value*	配置 Max Age 的值。
8	JX(config)#**stp pathcost-standard** { **dot1d-1998** | **dot1t** }	配置生成树路径开销计算标准。

1.4.6 配置 RSTP 边缘接口

边缘接口是指不直接与任何设备连接，也不通过接口所连接的网络间接与任何设备相连的接口。

设置为边缘接口能够使该接口的状态迅速转变为转发状态，而不需要时间等待，对于直接与用户终端相连的以太网接口，为能使其快速迁移到转发状态，应将其设置为边缘接口。

当某个接口设置为边缘接口（enable）时，当接口收到 BPDU 后实际运行值会变为非边缘接口。当某个接口设置为非边缘接口（disable）时，同样，无论其实际情况下为边缘或非边缘接口，此接口会保持为非边缘接口，直到配置改变。

缺省情况下，以太网设备中所有接口的均设置为 disable。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**stp edge-port** { **enable** | **disable** }	配置 RSTP 边缘接口属性。

1.4.7 配置 RSTP 链路类型

点对点链路相连的两个接口可以通过传送同步报文快速迁移到转发状态，减少了不必要的转发延迟时间。缺省情况下，根据双工状态设定接口的链路类型。全双工接口被认为是点到点链路，半双工被认作共享链路。

用户可以手工强行配置当前以太网接口与点对点链路相连，但是如果该链路不是点到点链路会使系统出现问题，一般情况下建议用户将此配置项设为自动状态，由系统自动发现接口是否与点到点链路相连。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**stp point-to-point** { **force-true** | **force-false** | **auto** }	配置接口的链路类型。

1.4.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

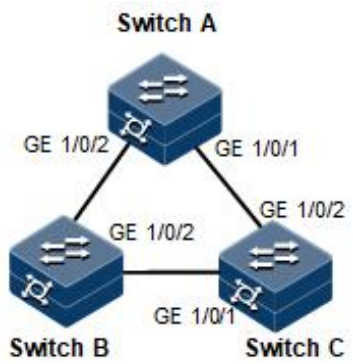
序号	检查项	说明
1	JX#show stp infomation	查看 STP 基本配置信息。
2	JX#show stp interface	查看接口下生成树配置信息。
3	JX#show stp bridge	查看 stp 根桥信息

1.4.9 配置 STP 示例

组网需求

如下图所示，三台设备 Switch A、Switch B 和 Switch C 组网成一个环，需在物理链路成环情况下解决环路问题，三台设备上需开启 STP，并设置 Switch A 的优先级为 0，Switch B 到 Switch A 的开销改为 10。

图 1-12 STP 应用组网示意图



配置步骤

步骤 1 在三台设备上均开启 STP 功能。

配置 Switch A。

```
JX#hostname SwitchA
SwitchA#configure
SwitchA(config)#stp mode stp
```

配置 Switch B。

```
JX#hostname SwitchB
SwitchB#configure
SwitchB(config)#stp mode stp
```

配置 Switch C。

```
JX#hostname SwitchC
SwitchC#configure
```

```
SwitchC(config)#stp mode stp
```

步骤 2 配置三台设备的接口模式。

配置 Switch A。

```
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#port link-type trunk
SwitchA(config-ge-1/0/1)#stp enable
SwitchA(config-ge-1/0/1)#exit
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#port link-type trunk
SwitchA(config-ge-1/0/2)#stp enable
SwitchA(config-ge-1/0/2)#exit
```

配置 Switch B。

```
SwitchB(config)#interface ge 1/0/1
SwitchB(config-ge-1/0/1)#port link-type trunk
SwitchB(config-ge-1/0/1)#stp enable
SwitchB(config-ge-1/0/1)#exit
SwitchB(config)#interface ge 1/0/2
SwitchB(config-ge-1/0/2)#port link-type trunk
SwitchB(config-ge-1/0/2)#stp enable
SwitchB(config-ge-1/0/2)#exit
```

配置 Switch C。

```
SwitchC(config)#interface ge 1/0/1
SwitchC(config-ge-1/0/1)#port link-type trunk
SwitchC(config-ge-1/0/1)#stp enable
SwitchC(config-ge-1/0/1)#exit
SwitchC(config)#interface ge 1/0/2
SwitchC(config-ge-1/0/2)#port link-type trunk
SwitchC(config-ge-1/0/2)#stp enable
SwitchC(config-ge-1/0/2)#exit
```

步骤 3 配置生成树优先级及接口路径开销。

配置 Switch A。

```
SwitchA(config)#stp priority 0
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#stp path-cost 10
```

配置 Switch B。

```
SwitchB(config)#interface ge 1/0/1
SwitchB(config-ge-1/0/1)#stp path-cost 10
```

检查结果

通过 **show stp** 命令查看桥状态，以 Switch A 为例。

```
SwitchA#show stp infomation
------------------------------------------------------------
------------------
  Mode                              : stp
  Trap state                         : disable
  Bridge type                        : customer
```

```
  BPDU Guard state                    : disable
  TC protection state                 : disable
  TC protection threshold              : 2
  Hello time                         : 2
  Max age                            : 20
  Forward delay                       : 15
  Max hops                           : 20
  Time factor                        : 6
  Format selector                     : 0
  Revision level                      : 0
  Config name                        : region
  TC flush arp state                  : disable
  Migration time                     : 3
  Pathcost standard                   : dot1t
  TC holdoff time                    : 10
  Transmit limit                     : 6 (packets/s)
  Link detection state                : enable
  Edge default state                  : disable
-------------------------------------------------------------
-------------------
```

通过 **show stp interface** 查看接口状态，以 Switch A 为例。

```
SwitchA#show stp interface
  MSTID Port         Role         State        Protection
Region
-------------------------------------------------------------
------------------------
  0     ge-1/0/1     designated    forward       --
different
  0     ge-1/0/2     designated    forward       --
different
```

1.5 MSTP

1.5.1 简介

IEEE 802.1s 标准定义了 MSTP（Multiple Spanning Tree Protocol，多生成树协议）。MSTP 可以弥补 STP 和 RSTP 的缺陷，既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径分发，从而提供了很好的负荷分担机制。

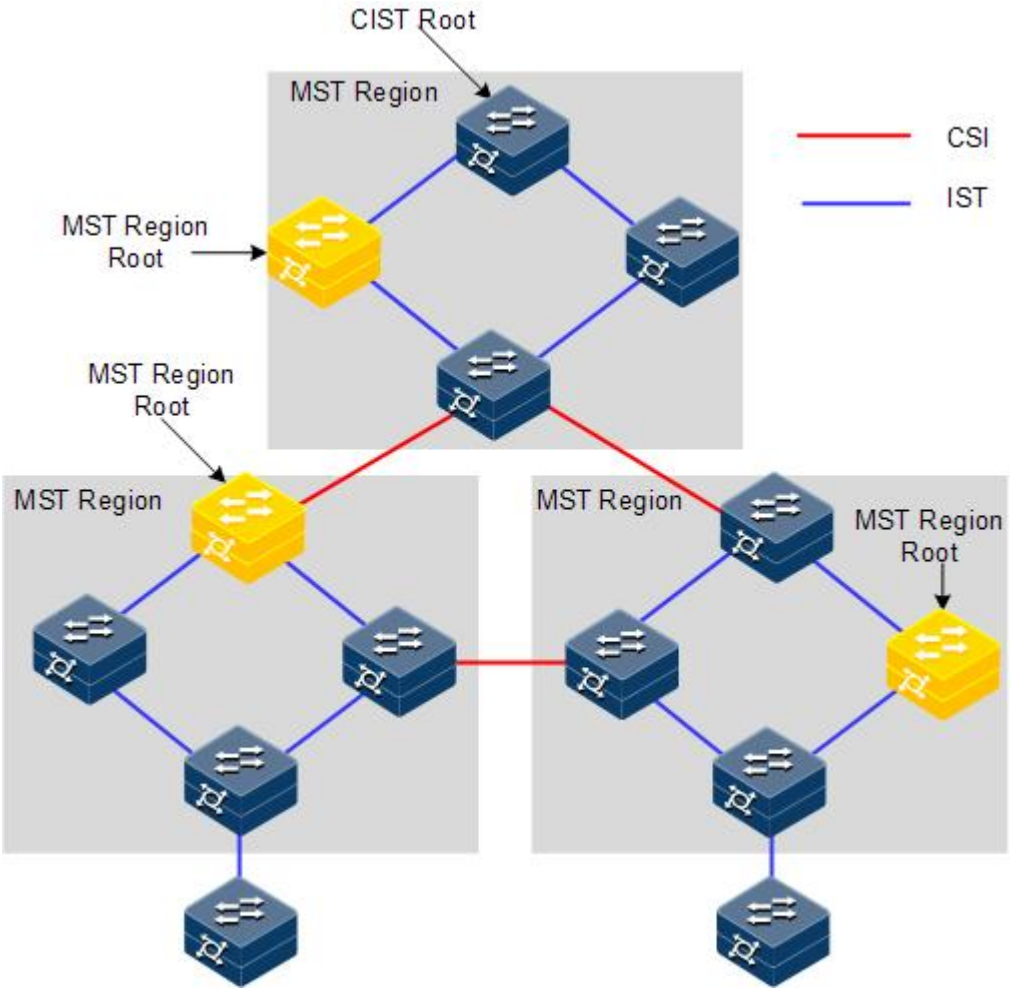
MSTP 把一个交换网络划分成多个域，每个域叫做一个 MST 域。每个域内形成多棵生成树，生成树之间彼此独立。每棵生成树叫做一个 MSTI（Multiple Spanning Tree Instance，多生成树实例）。

MSTP 协议引入了 CST（Common Spanning Tree，公共生成树）和 IST（Internal Spanning Tree，内部生成树）的概念。其中 CST 是指把 MST 域当成一个整体时，计算生成的一棵生成树。而 IST 是指在 MST 域内部生成的生成树。

与 STP 和 RSTP 相比，MSTP 中还引入了总根（CIST Root）和域根（MST Region Root）的概念。总根是一个全局概念，对于所有运行的 STP/RSTP/MSTP 的交换机只能有 1 个总根，也即是 CIST 的根。而域根

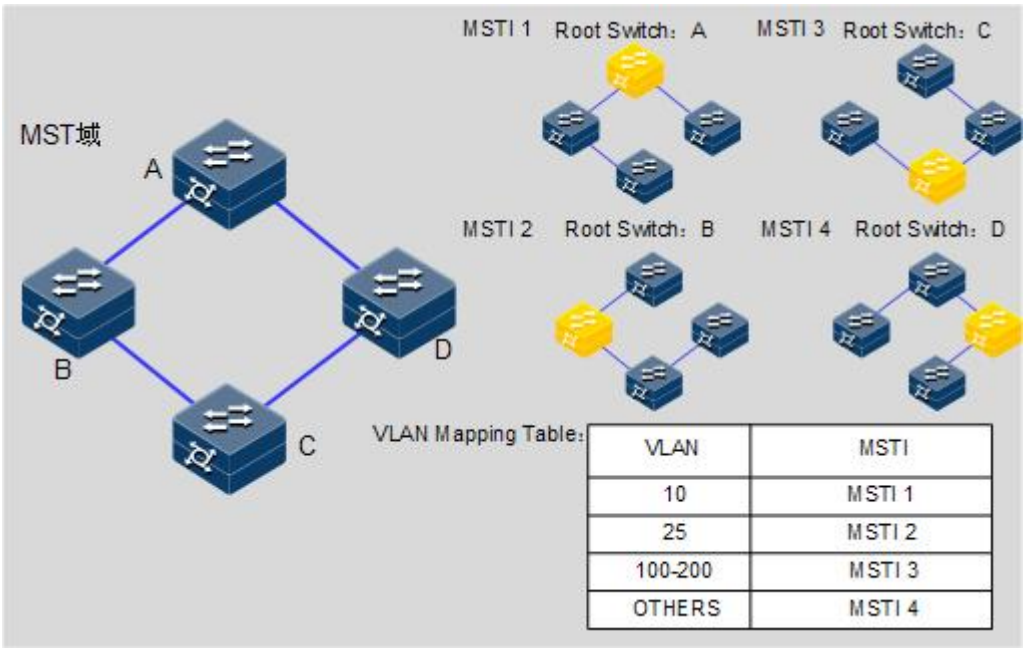
是一个局部概念，是相对于某个域的某个实例而言。如下图所示，所有相连的设备，总根只有 1 个，而每个域包含的域根数目与实例个数相关。

图 1-13 MSTP 网络基本概念示意图



在每个 MST 域中，可以有不同的 MST 实例，通过设置 VLAN 映射表（即 VLAN 和 MSTI 的对应关系表），把 VLAN 和 MSTI 联系起来。MSTI 概念示意图如下图所示。

图 1-14 MSTI 概念示意图

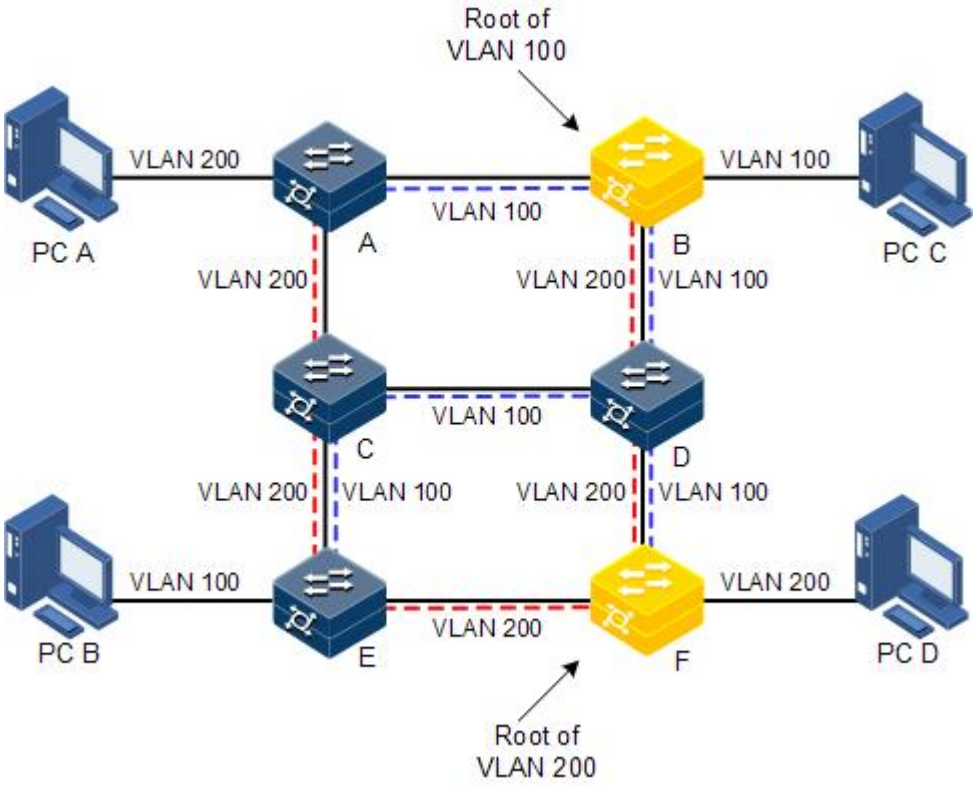


说明

每个 VLAN 只能对应一个 MSTI，即同一 VLAN 的数据只能在一个 MSTI 中传输；而一个 MSTI 可能对应多个 VLAN。

MSTP 协议相对于之前的 STP 协议和 RSTP 协议，优势非常明显。MSTP 具有 VLAN 认知能力，可以实现负载均衡分担，可以实现类似 RSTP 的端口状态快速切换，可以捆绑多个 VLAN 到一个 MST 实例中，以降低资源占用率。此外，网络中运行 MSTP 协议的设备可以很好的与运行 STP 协议和 RSTP 协议的设备兼容。

图 1-15 MST 域内多生成树实例组网示意图



将 MSTP 应用于如上图所示的网络，经计算最终生成两棵生成树（也即 2 个 MST 实例）：

- MSTI1 以 B 为根交换设备，转发 VLAN100 的报文；
- MSTI2 以 F 为根交换设备，转发 VLAN200 的报文。

这样所有 VLAN 内部可以互通，同时不同 VLAN 的报文沿不同的路径转发，实现了负荷分担。

1.5.2 配置准备

场景

大型局域网或小区汇聚时，汇聚设备之间组成一个环作为线路的备份，在实现线路备份的同时，需要防止环路以及实现业务的负载分担，MSTP 协议可以为每一个或一组 VLAN 选择不同且唯一的转发路径。

前提

无

1.5.3 MSTP 的缺省配置

设备上 MSTP 的缺省配置如下。

功能	缺省值
全局 MSTP 功能状态	禁止
接口 MSTP 功能状态	使能
MST 域的最大跳数	20
设备的 MSTP 优先级	32768
接口的 MSTP 优先级	128
接口的路径开销	0
每个 Hello time 内的最大发送报文数量	3
Max Age 定时器	20s
Hello Time 定时器	2s
Forward Delay 定时器	15s
MST 域的修订级别	0
TC 保护	禁用
TC 保护功能的阈值	1

1.5.4 使能 MSTP 功能

请在设备上进行以下配置。

步骤	配置	说明
1	`JX#config`	进入全局配置模式。
2	`JX(config)#stp mode mstp`	配置生成树模式为 MSTP。
3	`JX(config)#interface` *`interface-type interface-number`*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
4	`JX(config-ge-1/0/*)#stp enable`	使能接口生成树协议。

1.5.5 配置 MST 域和 MST 域最大跳数

当设备的运行模式为 MSTP 时，可为设备设置其归属的域信息。设备属于哪个 MST 域，是由域名，VLAN 映射表，MSTP 修订级别配置决定的。用户可以通过下面的配置过程将当前设备划分在一个特定的 MST 域内。

MST 域的最大跳数限制了 MST 域的规模。从域内的生成树的根桥开始，域内的配置消息（BPDU）每经过一台设备的转发跳数就被减 1，设备将丢弃收到的跳数为 0 的配置消息。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。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**stp instance** *instance-id* **vlan** *vlan-list*	配置 MST 域的 VLAN 到实例映射关系。
3	JX(config)#**stp config-name** *name*	配置 MST 域名。
4	JX(config)#**stp revision-level** *level-value*	配置 MST 域的修订级别。
6	JX(config)#**stp max-hops** *hops-value*	配置设备 MST 域最大跳数。

说明

当且仅当配置的设备为域根时，配置的最大跳数才作为 MST 域的最大跳数，其他非域根桥配置此项无效。

1.5.6 配置根桥/备份根桥

MSTP 根桥的选举，一方面可以通过配置设备的优先级，然后经过生成树计算，来确定生成树的根桥或备份根桥；另一方面，用户也可以通过此命令来直接指定。当根桥出现故障或被关机时，备份根桥可以取代根桥成为相应实例的根桥。此时如果用户设置了新的根桥，则备份根桥将不会成为根桥。如果用户为一棵生成树实例配置了多个备份根桥，当根桥失效时，MSTP 将选择 MAC 地址最小的那个备份根桥作为根桥。

注意

如果采用这种直接指定根桥的方式，建议用户不要再修改网络中任何设备的优先级，否则，可能会造成指定根桥或备份根桥无效。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**spanning-tree** [**instance** *instance-id*] **root** { **primary** | **secondary** }	为某个生成树实例，设置设备为根桥或备份根桥。

说明

- 用户可以通过参数 **instance** *instance-id* 确定根桥或备份根桥生效的实例。如果 *instance-id* 取值为 0，或者省去参数 **instance** *instance-id* 时，当前设备将被指定为 CIST 的根桥或备份根桥。
- 设备在各实例中的根类型是互相独立的，即它既可以作为一个实例的根桥或备份根桥，同时又可以作为其他生成树实例的根桥或备份根桥。但在同一棵生成树实例中，同一台设备不能既作为根桥，又作为备份根桥。
- 用户不能同时为一棵生成树实例指定两个或两个以上的根桥。相反，用户可以给同一棵生成树指定多个备份树根。一般情况下，建议用户给一棵生成树指定一个树根和多个备份树根。

1.5.7 配置设备接口和系统的优先级

接口是否被选为根接口需要根据接口优先级进行判断。同等条件下，接口优先级值越小，接口越优先被选为根接口。接口可在不同的实例中具有不同的接口优先级，也可以在不同实例中充当不同的角色。

设备 Bridge ID 的大小决定了这台设备是否能够被选作生成树的根。通过配置较小的优先级，可以得到较小的设备 Bridge ID，达到指定某台设备成为生成树树根的目的。优先级相同的情况下，MAC 地址小的为树根。

与配置根与备份根相同，优先级在不同实例中的配置相互独立。用户可以通过参数 **instance** *instance-id* 确定的配置优先级的实例。如果 *instance-id* 取值为 0，或者省去参数 **instance** *instance-id* 时，则是为 CIST 配置的桥优先级。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**stp** [**instance** *instance-id*] **priority** *priority-value* JX(config-ge-1/0/*)#**exit**	配置某个生成树实例的接口优先级。
4	JX(config)#**stp** [**instance** *instance-id*] **priority** *priority-value*	配置某个生成树实例的系统优先级。

说明

优先级取值必须为 4096 的倍数，如 0、4096、8192 等，缺省值为 32768。

1.5.8 配置接口的路径开销

在选举根接口（root port）和指定接口（designated port）时，路径开销越小的接口越容易被选举为根接口或者指定接口。接口的路径开销在不同实例中的配置相互独立。用户可以通过参数 **instance** *instance-id* 确定的配置接口的内部路径开销的实例。如果 *instance-id* 取值为 0，或者省去参数 **instance** *instance-id* 时，则是为 CIST 配置的接口内部路径开销。

接口的开销一般依据其物理特性，缺省情况如下：

- 10Mbit/s 为 2000000
- 100Mbit/s 为 200000
- 1000Mbit/s 为 20000
- 10Gbit/s 为 2000

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**stp** [**instance** *instance-id*] **path-cost** *cost-value*	配置接口的路径开销。

1.5.9 配置接口最大发送速率

MSTP 每 Hello Time 时间内允许发送的最大 BPDU 数量。此参数是一个相对值，没有单位，该参数被配置得越大，则每个 Hello Time 内允许发送的报文个数就越多，同时也会占用会更多的设备资源。与时间参数相同，只有根设备的此项配置生效。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**stp transmit-limit** *value*	配置接口最大发送速率。

1.5.10 配置 MSTP 定时器

- Hello Time：设备定期发送桥配置信息（BPDU）的时间间隔，用于设备检测链路是否存在故障。设备每隔 Hello Time 时间，会向周围的设备发送 Hello 报文，以确认链路是否存在故障。缺省值为 2s，用户可以根据网络情况对此值进行调整。当网络中链路出现频繁变化

时，可以适当缩短该值，来增强生成树协议的健壮性。相反，增大此值则可以降低生成树协议对系统 CPU 资源的占用率。

- Forward Delay：保证设备状态安全迁移的时间参数。链路故障会引发网络重新进行生成树的计算，不过重新计算得到的新配置消息无法立刻传遍整个网络。如果新选出的根接口和指定接口立刻开始数据转发，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：根接口和指定接口重新开始数据转发之前，要经历一个中间状态（学习状态），中间状态经过 Forward Delay 时间的延时后，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。用户可以根据实际情况调整该值，当网络拓扑不频繁变化时可以将该值减小，反之增大。
- Max Age：生成树协议所使用的桥配置信息有生存周期，用来判断配置消息是否过时。设备会将过时的配置消息丢弃。当桥配置信息过期后，生成树协议将重新计算生成树。缺省值为 20s，该值过小会导致生成树重计算过于频繁，过大则会导致生成树协议不能及时适应网络拓扑结构的变化。

整个交换网络中所有的设备采用 CIST 根设备上的三个时间参数，因此只有在根设备上的配置生效。

请在设备上进行以下配置。

步骤	配置	说明
1	`JX#config`	进入全局配置模式。
2	`JX(config)#stp hello-time value`	配置 HelloTime 的值。
3	`JX(config)#stp forward-delay value`	配置 Forward Delay 的值。
4	`JX(config)#stp max-age value`	配置 MaxAge 的值。

1.5.11 配置边缘接口

边缘接口是指不直接与任何设备连接，也不通过接口所连接的网络间接与任何设备相连的接口。

设置为边缘接口能够使该接口的状态迅速转变为转发状态，而不需要时间等待，对于直接与用户终端相连的以太网接口，为能使其快速迁移到转发状态，应将其设置为边缘接口。

当某个接口设置为边缘接口自动检测（auto）则边缘接口的属性是由实际情况决定的。当某个接口设置为边缘接口（force-true）时，当接口收到 BPDU 后实际运行值会变为非边缘接口。当某个接口设置为非边缘接口（force-false）时，同样，无论其实际情况下为边缘或非边缘接口，此接口会保持为非边缘接口，直到配置改变。

缺省情况下，以太网设备中所有接口的均设置为自动检测属性。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**stp edge-port** { **enable** | **disable** }	配置接口边缘接口属性。

1.5.12 配置 BPDU 过滤

用户使能边缘接口的 BPDU 过滤功能后，边缘接口不会发送 BPDU 报文，也不会处理收到的 BPDU 报文。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#config	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**stp bpdu-filter** { **enable** | **disable** }	配置边缘接口的 BPDU 过滤功能。

1.5.13 配置 BPDU 保护

在交换机上，通常将直接与用户终端（如 PC 机）或文件服务器等非交换机设备相连的接口配置为边缘接口，以实现这些接口的快速迁移。

正常情况下，这些边缘接口不会收到 BPDU。如果有人伪造 BPDU 恶意攻击交换机，当这些接口接收到 BPDU 时，会自动将这些接口设置为非边缘接口，并重新进行生成树计算，从而引起网络震荡。

MSTP 提供 BPDU 保护功能来防止这种攻击。启动 BPDU 保护功能后，可以防止伪造 BPDU 恶意攻击。

如果使能 BPDU 保护功能，则边缘接口收到了 BPDU，设备将关闭这些接口，同时通知网管系统。被关闭的接口只能由网络管理人员通过命令手动恢复。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**stp bpdu-protection** { **enable** | **disable** }	配置 BPDU 保护功能。

步骤	配置	说明
3	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
4	JX(config-ge-1/0/*)#**stp bpdu-protection error-down recovery-interval** *interval*	配置 BPDU 保护的恢复周期

说明

当边缘接口使能了 BPDU 过滤功能，同时设备使能了 BPDU 保护功能，则 BPDU 保护功能优先生效，即边缘接口接收到 BPDU 报文时，接口被关闭。

1.5.14 配置 STP/RSTP/MSTP 模式切换

当生成树协议开启时，支持三种生成树运行模式，分别为 STP 兼容模式、RSTP 模式和 MSTP 模式。

- STP 兼容模式：不执行替换接口到根接口的快速转换和指定接口快速 Forwarding。只发送 STP 配置报文（STP Configuration BPDU）和拓扑变化通知（STP TCN BPDU）。收到 MST BPDU 将丢弃不识别部分。
- RSTP 模式：执行替换接口到根接口的快速转换和指定接口快速 Forwarding。只发送 RST BPDU。收到 MST BPDU 将丢弃不识别部分；如果本交换机接口的对端运行 STP 协议，接口将转移到 STP 兼容模式下。
- MSTP 模式：发送 MST BPDU。如果本交换机接口的对端运行 STP 协议，接口将转移到 STP 兼容模式下。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**stp mode { stp | rstp | mstp }**	配置生成树的运行模式。
3	JX(config-ge-1/0/*)#**stp mcheck**	(可选)强制端口变为 MSTP 模式。

1.5.15 配置链路类型

点对点链路相连的两个接口可以通过传送同步报文快速迁移到转发状态，减少了不必要的转发延迟时间。缺省情况下，MSTP 根据双工状态设定接口的链路类型。全双工接口被认为是点到点链路，半双工被认作共享链路。

用户可以手工强行配置当前以太网接口与点对点链路相连，但是如果该链路不是点到点链路会使系统出现问题，一般情况下建议用户将此配置项设为自动状态，由系统自动发现接口是否与点到点链路相连。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-ge-1/0/*)#**stp point-to-point** { **force-true** | **force-false** | **auto** }	配置接口的链路类型。

1.5.16 配置根接口保护

当桥收到更高优先级的报文的时候就需要重新选举，重新选举一个是会影响网络的连通性，二来会消耗 CPU 资源。对于开启了 MSTP 功能的网络，如果有人发送高优先级的 BPDU 报文进行攻击，网络就会由于不断的选举而导致不稳定。而一般而言，各个桥的优先级是在网络规划阶段就已经配置好，越是靠近边缘的桥优先级越低，因此下行接口一般不会收到比桥优先级高的报文，除非有人恶意攻击。对于这些接口，可以通过开启根接口保护功能，拒绝处理比桥优先级高的报文，并在收到高优先级报文的时候阻塞接口一段时间，防止攻击源的其他攻击损害更上层的链路。

请在需要的设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/*)#**stp root-guard** { **enable** | **disable** }	配置接口的根接口保护功能。

1.5.17 配置接口环路保护

生成树主要作用有两个：防止环路和链路备份。防止环路就要求必须将拓扑裁剪成树状结构，而如果需要进行链路备份，拓扑中必须有冗余的链路。生成树就是通过阻塞冗余链路来达到防止环路的功能，而在链路发生故障的时候放开冗余链路从而达到链路备份的功能。

生成树模块会周期性交换报文，如果一定时间内没有收到报文即认为发生了链路故障。然后选举，放开备份接口。而在实际应用中，导致收不到报文的原因可能并不是链路故障，如果在这种情况下放开备份接口就有可能导致环路。

环路保护的目的是当接口在一定时间内收不到报文的时候，不进行重新选举，保持接口原来的状态不变。注意：环路保护的功能和链路备份的功能是对立的，也即环路保护是以失去链路备份功能的代价来实现环路避免。

请在设备上进行以下配置。

步骤	配置	说明
1	`JX#config`	进入全局配置模式。
2	`JX(config)#interface` *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	`JX(config-ge-1/0/*)#stp loop-guard { enable | disable }`	配置接口环路保护功能。

1.5.18 配置端口 TC 报文抑制功能

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，可以在端口上使能 TC 报文抑制功能，此后当该端口收到 TC 报文时，不会再向其他端口传播。

请在设备上进行以下配置。

步骤	配置	说明
1	`JX#config`	进入全局配置模式。
2	`JX(config)#interface` *interface-type interface-number*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	`JX(config-ge-1/0/*)#stp tc-restriction { enable | disable }`	配置端口 TC 抑制功能。

1.5.19 配置 TC 保护功能

TC 保护功能可避免拓扑变化相关的 BPDU 报文攻击，提高设备和网络的安全性。

- 使能 TC 保护功能后，在 STP 的 Hello Time 时间内，仅接收阈值数量以内的 TC 报文。该 Hello Time 时间内的、超过阈值数量的 TC 报文会被丢弃，直到下一个 Hello Time 时间再重新开始计算接收的 TC 报文数量。
- 禁用 TC 保护功能后，设备会处理所有 TC 报文。当设备受到 TC 报文攻击时，可能会导致业务中断、设备 CPU 利用率过高甚至无法正常工作。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**stp tc-protection threshold** *threshold-value*	配置 TC 保护功能的阈值。
3	JX(config)#**stp tc-protection { enable | disable }**	配置 TC 保护功能。

1.5.20 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show stp infomation**	查看 STP 基本配置信息。
2	JX#**show stp interface**	查看接口下生成树配置信息。
3	JX#**show stp bridge**	查看 STP 根桥信息
4	JX#**show stp instance**	查看 STP 实例与 VLAN 映射关系。

1.5.21 维护

用户可以通过以下命令维护 MSTP 特性。

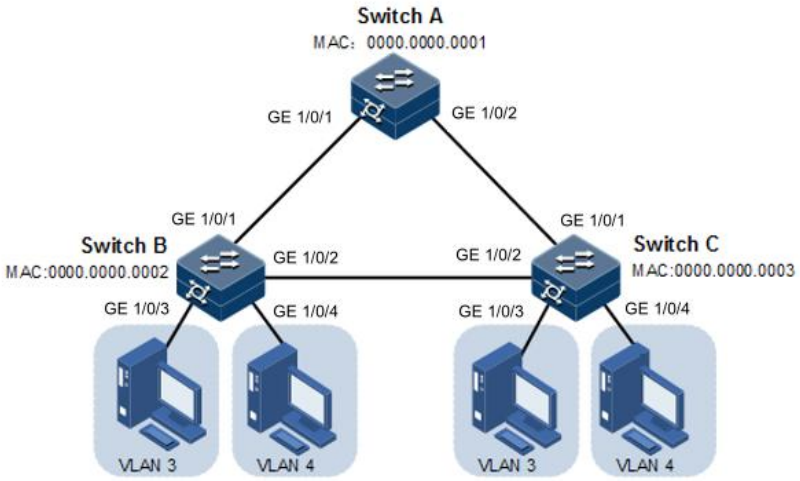
命令	描述
JX(config-ge-1/0/*)#**reset stp statistics**	清除接口生成树统计信息。

1.5.22 配置 MSTP 示例

组网需求

如下图所示，三台交换机设备组成环形网络运行 MSTP 协议，域名 aaa。Switch B 和 Switch C 上分别各连接两台 PC，分别属于 VLAN 3 和 VLAN 4。实例 3 关联 VLAN 3，实例 4 关联 VLAN 4。配置优先级，使得实例 3 的根桥为 Switch A，实例 4 的根桥为 SwicthB,这样可以使两个 VLAN 的报文分别在两条路径进行转发，消除了环路的同时实现了负载分担。

图 1-16 MSTP 应用组网示意图



配置步骤

步骤 1 在三台交换机上分别创建 VLAN 3 和 VLAN 4 并激活。

配置 Switch A。

```
JX#hostname SwitchA
SwitchA#config
SwitchA(config)#vlan 3,4
```

配置 Switch B。

```
JX#hostname SwitchB
SwitchB#config
SwitchB(config)#vlan 3,4
```

配置 Switch C。

```
JX#hostname SwitchC
SwitchC#config
SwitchC(config)#vlan 3,4
```

步骤 2 Switch A 的接口 GE 1/0/1、GE 1/0/2 以 Trunk 模式允许所有 VLAN 通过，Switch B 的接口 GE 1/0/1、GE 1/0/2 以 Trunk 模式允许所有 VLAN 通过，Switch C 的接口 GE 1/0/1、GE 1/0/2 以 Trunk 模式允许所有 VLAN 通过。Switch B、Switch C 的接口 GE 1/0/3、GE 1/0/4 以 Access 模式分别允许 VLAN 3、VLAN 4 通过。

配置 Switch A。

```
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#port link-type trunk
SwitchA(config-ge-1/0/1)#port trunk allow-pass vlan all
SwitchA(config-ge-1/0/1)#exit
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#port link-type trunk
SwitchA(config-ge-1/0/1)#port trunk allow-pass vlan all
SwitchA(config-ge-1/0/2)#exit
```

配置 Switch B。

```
SwitchB(config)#interface ge 1/0/1
SwitchB(config-ge-1/0/1)#port link-type trunk
SwitchB(config-ge-1/0/1)#port trunk allow-pass vlan all
SwitchB(config-ge-1/0/1)#exit
SwitchB(config)#interface ge 1/0/2
SwitchB(config-ge-1/0/2)#switchport mode trunk
SwitchB(config-ge-1/0/2)#port trunk allow-pass vlan all
SwitchB(config-ge-1/0/2)#exit
SwitchB(config)#interface ge 1/0/3
SwitchB(config-ge-1/0/3)#switchport access vlan 3
SwitchB(config-ge-1/0/3)#exit
SwitchB(config)#interface ge 1/0/4
SwitchB(config-ge-1/0/4)#switchport access vlan 4
SwitchB(config-ge-1/0/4)#exit
```

配置 Switch C。

```
SwitchC(config)#interface ge 1/0/1
SwitchC(config-ge-1/0/1)#port link-type trunk
SwitchC(config-ge-1/0/1)#port trunk allow-pass vlan all
SwitchC(config-ge-1/0/1)#exit
SwitchC(config)#interface ge t 1/0/2
SwitchC(config-ge-1/0/2)#switchport mode trunk
SwitchC(config-ge-1/0/2)#port trunk allow-pass vlan all
SwitchC(config-ge-1/0/2)#exit
SwitchC(config)#interface ge 1/0/3
SwitchC(config-ge-1/0/3)#switchport access vlan 3
SwitchC(config-ge-1/0/3)#exit
SwitchC(config)#interface ge 1/0/4
SwitchC(config-ge-1/0/4)#switchport access vlan 4
SwitchC(config-ge-1/0/4)#exit
```

步骤 3 Switch A、Switch B、Switch C 设置生成树模式为 MSTP，并开启生成树协议。进入 MSTP 配置模式设置域名为 aaa，修正版本为 0，instance 3 映射 VLAN 3、instance 4 映射 VLAN 4，退出 mst 配置模式。

配置 Switch A。

```
SwitchA(config)#stp mode mstp
SwitchA(config)#stp config-name aaa
SwitchA(config)#stp revision-level 0
SwitchA(config)#stp instance 3 vlan 3
SwitchA(config)#stp instance 4 vlan 4
SwitchA(config)#stp instance 3 priority 0
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#stp enable
SwitchA(config-ge-1/0/1)#exit
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#stp enable
```

配置 Switch B。

```
SwitchB(config)#stp mode mstp
SwitchB(config)#stp config-name aaa
SwitchB(config)#stp revision-level 0
SwitchB(config)#stp instance 3 vlan 3
```

```
SwitchB(config)#stp instance 4 vlan 4
SwitchA(config)#stp instance 4 priority 0
SwitchB(config)#interface ge 1/0/1
SwitchB(config-ge-1/0/1)#stp enable
SwitchB(config-ge-1/0/1)#exit
SwitchB(config)#interface ge 1/0/2
SwitchB(config-ge-1/0/2)#stp enable
```

配置 Switch C。

```
SwitchC(config)#stp mode mstp
SwitchC(config)#stp config-name aaa
SwitchC(config)#stp revision-level 0
SwitchC(config)#stp instance 3 vlan 3
SwitchC(config)#stp instance 4 vlan 4
SwitchC(config)#interface ge 1/0/1
SwitchC(config-ge-1/0/1)#stp enable
SwitchC(config-ge-1/0/1)#exit
SwitchC(config)#interface ge 1/0/2
SwitchC(config-ge-1/0/2)#stp enable
```

步骤 4 Switch B 修改生成树实例 3 接口 GE 1/0/1 的路径开销为 500000。

```
SwitchB(config)#interface ge 1/0/1
SwitchB(config-ge-1/0/1)#stp instance 3 path-cost 500000
```

检查结果

通过 **show stp interface** 命令查看 MST 域的接口状态信息，以 Switch C 为例。

```
SwitchA#show stp interface
  MSTID Port         Role         State        Protection
Region
-------------------------------------------------------------
------------------------
  0    ge-1/0/1      root         forward      --
same
  0    ge-1/0/2      alternate     discarding    --
same
  3    ge-1/0/1      root         forward      --
same
  3    ge-1/0/2      alternate     discarding    --
same
  4    ge-1/0/1      alternate     discarding    --
same
  4    ge-1/0/2      root         forward      --
same
-------------------------------------------------------------
-----------
------------------------------
```

1.6 环路检测

1.6.1 简介

环路检测功能可以消除因环路对网络造成的影响，提高网络的自检错性、容错性和健壮性。

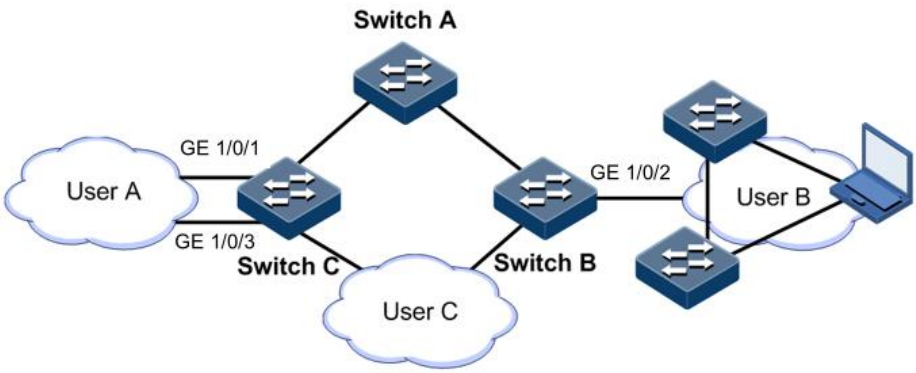
环路检测过程中每个开启环路检测功能的接口周期性地发送环路检测报文（Hello 报文），由于环路检测功能主要应用于网络边缘接口，因此，正常情况下边缘接口是不应该收到任何环路检测报文的。如果边缘设备接收到了环路检测报文，则认为网络出现了环路。接收环路检测报文分为两种情况：接收到了自身发送的报文和接收到了其他设备发送的报文，主要依据设备 MAC 地址和报文携带的 MAC 地址进行比较区分。

环路类型

常见的环路类型有自环、内环两种。如下图所示，Switch B 和 Switch C 是连接用户网络的边缘交换机。

- 自环：同一设备上同一以太网接口下存在的用户环路，例如用户网络 B 自身存在环路使 Switch B 的 GE 1/0/2 接口形成自环。
- 内环：同一设备上不同以太网接口之间形成的环路，例如 Switch C 的接口 GE 1/0/1 和接口 GE 1/0/3 与用户网络 A 形成内环。

图 1-17 环路类型示意图



环路处理机制

设备遵循如下原则进行环路处理：

- 如果接收和发送环路检测报文的设备是同一设备，但不是同一接口，则处理接口号小的接口消除环路（内环）。
- 如果接收和发送环路检测报文的设备是同一设备且是同一接口，则处理该接口消除环路（自环）。

在下图中，假设 Switch B 和 Switch C 连接用户网络的接口都使能了环路检测功能。环路检测针对不同环路类型的处理机制如下：

- 对于自环，Switch B 收发报文接口号相同，将在 GE 1/0/2 接口采取配置的环路检测动作来消除自环。
- 对于内环，Switch C 会收到自身发出的环路检测报文，而且收发报文接口号不同，因此会在接口号小的 GE 1/0/1 采取配置的环路检测动作来消除内环。

环路处理动作

环路处理动作即设备检测到接口出现环路时的处理方式，用户可以根据实际情况在指定接口上配置不同的环路处理动作。包括以下几种：

- Block：阻塞指定接口并发送 Trap 信息。
- Trap-only：只发送 Trap 信息。
- Shutdown：关闭指定接口并发送 Trap 信息。
- Shutdown-restore：发送 trap，关闭端口并等待恢复

环路检测模式

环路检测模式为 Port 模式。

Port 模式：出现环路时，若环路处理方式为 Block，则阻塞接口并发送 Trap；若环路处理方式为 Shutdown 方式，则关闭物理接口并发送 Trap。

若环路处理方式为 Trap-only，则只发送 Trap 信息。

环路恢复

接口由于环路被关闭之后，可以根据用户配置于指定时间后自动恢复。

1.6.2 配置准备

场景

在网络中，所有接入设备下连的主机或二层设备都可能存在有意、无意的连接而引起的环路，在每台接入设备上开启环路检测功能，可以避免网络环路造成数据流无限制复制而形成的网络拥塞状况。

前提

设备上环路检测、接口备份、STP、G.8032 功能之间可能会相互影响，建议不要同一接口上同时开启这些功能。

1.6.3 环路检测的缺省配置

设备上环路检测的缺省配置如下。

功能	缺省值
环路检测功能状态	禁止
接口阻塞后的自动恢复时间	30s

功能	缺省值
环路检测处理方式	block
环路检测报文发送周期	5s
环路检测模式	vlan 模式

1.6.4 配置环路检测功能

请在设备上进行以下配置。

说明

环路检测与生成树协议冲突，二者不能同时开启。

直连设备两端不能同时开启环路检测。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
3	JX(config-ge-1/0/*)#**loopback-detect mode vlan**	配置基于 VLAN 的环路检测功能。
4	JX(config-ge-1/0/*)#**loopback-detect vlan** *vlan-list*	配置发包 vlan
5	JX(config-ge-1/0/*)#**loopback-detect action block**	配置环路动作
6	JX(config)#**loopback-detect interval** *interval*	配置发包间隔，单位：秒
7	JX(config)#**loopback-detect recovery-interval** *interval*	配置恢复时间，单位：秒

1.6.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show loopback-detect interface**	查看接口环路检测配置。

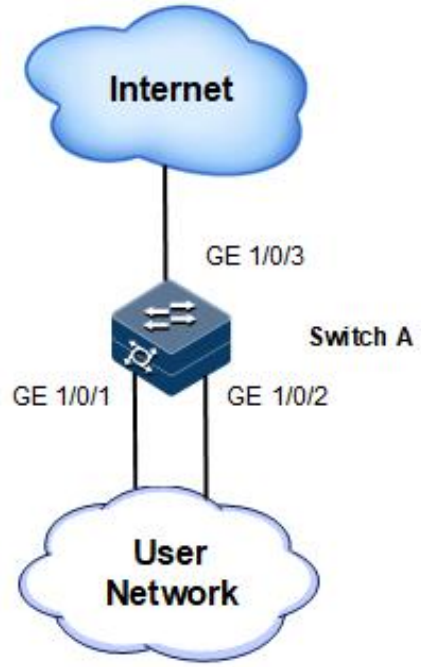
1.6.6 配置环路检测内环应用示例

组网需求

如下图所示，Switch A 通过 GE 1/0/1 和 GE 1/0/2 接口连接 VLAN 3 用户网络，为了避免用户网络中存在环路，需要在 Switch A 上开启环路检测功能，及时检测用户网络中的环路并进行处理。具体要求如下：

- 使能 GE 1/0/1 和 GE 1/0/2 接口的环路检测功能。
- 配置环路检测报文发送间隔为 3s。
- 配置环路检测模 VLAN 为 VLAN3。
- 配置 GE 1/0/2 接口的环路检测处理动作为 Block，发送告警信息并阻塞接口。

图 1-18 环路检测内环应用组网示意图



配置步骤

步骤 1 创建 VLAN，并将接口加入 VLAN。

```
JX#configure
JX(config)#vlan 3
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-type hybrid
JX(config-ge-1/0/1)#port hybrid vlan 3 untagged
JX(config-ge-1/0/1)#exit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/1)#port link-type hybrid
JX(config-ge-1/0/2)#port hybrid vlan 3 untagged
JX(config-ge-1/0/2)#exit
```

步骤 2 配置环路检测 VLAN、环路检测处理动作和环路检测报文发送周期。

```
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#loopback-detect enable
JX(config-ge-1/0/1)#loopback-detect action block
JX(config-ge-1/0/1)#loopback-detect vlan 3
JX(config-ge-1/0/1)#loopback-detect interval 3
JX(config-ge-1/0/1)#exit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#loopback-detect enable
JX(config-ge-1/0/2)#loopback-detect action block
JX(config-ge-1/0/2)#loopback-detect vlan 3
JX(config-ge-1/0/2)#loopback-detect interval 3
```

检查结果

通过 **show loopback-detect interface** 命令查看接口环路检测状态，此时没有环路。

```
JX#show loopback-detect interface
 Interface      Enable  Action        Loop-Status
------------------------------------------------------------
 ge-1/0/1       enable  block         none-loop
 ge-1/0/2       enable  block         none-loop
------------------------------------------------------------
```

1.7 接口备份

1.7.1 简介

双上行组网是目前常用的应用组网之一，该组网下常通过生成树协议（STP，Spanning Tree Protocol）阻塞冗余链路，起备份作用。虽然这种方案从功能上可以实现客户冗余备份的需求，但是在性能上却不能达到很多用户的要求，即使采用快速生成树协议的快速迁移，也只能是秒级的收敛速度。这对于应用于电信级网络核心的高端以太网交换机，是非常不利的一个性能参数。

接口备份解决方案针对双上行组网，实现主备链路冗余备份及快速迁移。该方案为双上行组网量身定做，既保证了性能，又简化了配置。

接口备份功能是 STP 协议的另一个解决方案，用户可以在关闭 STP 功能的情况下，通过手动设置接口实现基本的链路冗余。如果交换机已经开启 STP，就需要禁止接口备份功能，因为 STP 已经提供了类似的功能。

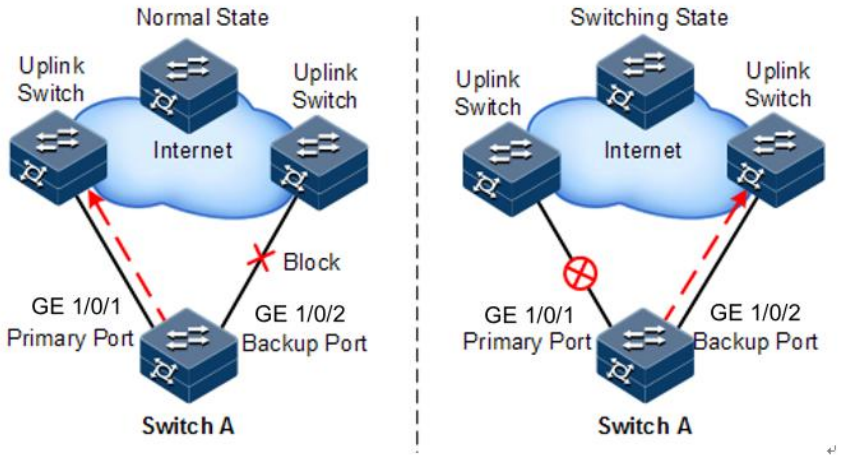
接口备份原理

接口备份功能需要设置接口备份组来实现。接口备份组包括一对接口，其中一个接口是主接口，另一个接口是备份接口。主接口所在的链路称为主链路，备份接口所在的链路称为备份链路。接口备份组的成员接口支持物理接口和链路聚合组，不支持三层接口。

在接口备份组中，当一个接口处于转发（Forward）状态时，另一个接口则处于阻塞状态（Block）。任何时刻，两个接口中只有一个接口处于转发

状态。当处于转发状态的接口发生链路故障时，处于待命状态的接口才会切换到转发状态，以保持链路正常。

图 1-19 接口备份原理示意图



接口备份原理如上图所示。Switch A 上的 GE 1/0/1、GE 1/0/2 分别与上行交换机相连，接口转发状态如下：

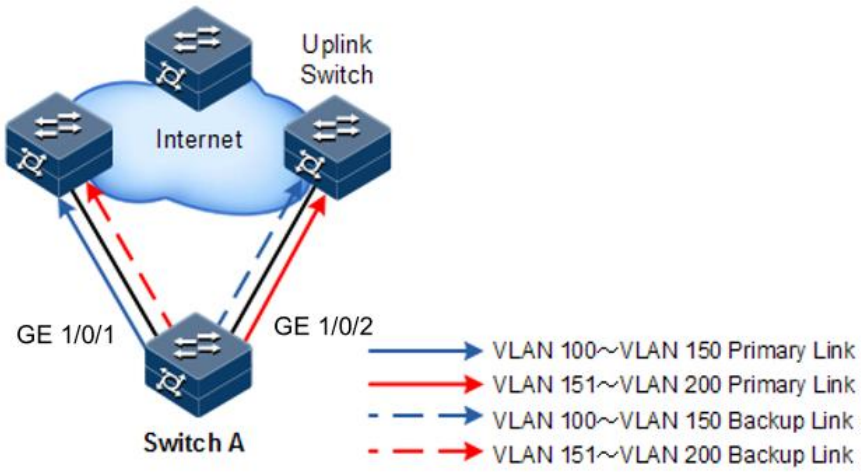
- 正常状态下，Switch A 的 GE 1/0/1 为主接口，GE 1/0/2 为备份接口，GE 1/0/1 和上行交换机之间转发报文，GE 1/0/2 和上行交换机之间不转发报文。
- 当 GE 1/0/1 与上行交换机之间出现链路故障时，备份接口 GE 1/0/2 和上行交换机之间转发报文。
- 当 GE 1/0/1 链路故障恢复并保持一段时间（恢复延时）后，GE 1/0/1 变为转发状态，GE 1/0/2 变为待命状态。

如果主接口和备份接口之间发生切换，交换机会发送一个 Trap 上报网管系统。

接口备份在不同 VLAN 上的应用

接口备份通过在 VLAN 上进行应用，还可以实现两个接口在不同 VLAN 上同时进行转发，如下图所示。

图 1-20 接口备份在不同 VLAN 上的应用原理示意图



在不同的 VLAN 上，接口的转发状态如下：

- 正常情况下，配置 Switch A 在 VLAN 100～VLAN 150 上，GE 1/0/1 为主接口，GE 1/0/2 为备份接口；在 VLAN 151～VLAN 200 上，GE 1/0/2 为主接口，GE 1/0/1 为备份接口。那么，GE 1/0/1 在 VLAN 100～VLAN 150 转发流量，GE 1/0/2 在 VLAN 151～VLAN 200 上转发流量。
- 当 GE 1/0/1 发生链路故障时，GE 1/0/2 负责转发 VLAN 100～VLAN 200 上的流量。
- 当 GE 1/0/1 恢复正常并保持一段时间（恢复延时）后，GE 1/0/1 在 VLAN 100～VLAN 150 上转发流量，GE 1/0/2 在 VLAN 151～VLAN 200 上转发流量。

利用这种方法，接口备份可以用于负载均衡。同时，这种应用不依赖于上联交换机的配置，便于用户操作。

1.7.2 配置准备

场景

在双上行网络中，通过配置端口备份功能，可以实现主备链路的冗余备份及其快速倒换。通过在不同 VLAN 中应用端口备份，还可以实现各端口之间的负载分担。

与 STP 功能相比，端口备份功能既保证了毫秒级的倒换性能，又简化了配置。

前提

无

1.7.3 接口备份的缺省配置

设备上接口备份的缺省配置如下。

功能	缺省值
接口备份组	无
故障恢复延时时间	15s
恢复模式	不返回模式

1.7.4 配置接口备份基本功能

注意

设备上接口备份与 STP、环路检测和 ERPS 功能之间可能会相互影响，建议不要在同一接口上同时开启这些功能。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**protect-link group** *group-id*	创建备份组
3	JX(config-protectlink-*)#**protect-vlan** *vlan-list*	配置指定的 VLAN 列表
4	JX(config-protectlink-*)#**add interface** *interface-type interface-number* **role master**	指定主接口
5	JX(config-protectlink-*)#**add interface** *interface-type interface-number* **role slave**	指定备份接口
6	JX(config-protectlink-*)#**port backup fault-detect lldp**	配置 LLDP 故障探测。
7	JX(config-protectlink-*)#**reverse** { **enable** | **disable** }	配置恢复模式。
8	JX(config-protectlink-*)#**reverse time** *interval*	配置恢复时间

说明

- 在一个接口备份组中，一个接口不能既是主接口，又是备份接口。
- 在同一 VLAN 上，一个接口/链路聚合组不能同时充当两个接口备份组的成员。

1.7.5 配置接口强制倒换

注意

- 配置强制倒换成功后，主备链路将进行倒换，工作链路被强制倒换到备份链路上。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**protect-link group** *group-id*	进入物理接口配置模式或聚合组配置模式。以下步骤以物理接口配置模式为例。
3	JX(config-protectlink-*)#**manual-switch**	配置接口强制倒换。

1.7.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show protect-link interface**	查看接口备份相关的状态信息。
2	JX#**show protect-link group**	查看接口备份组相关的配置信息。

1.7.7 配置接口备份示例

组网需求

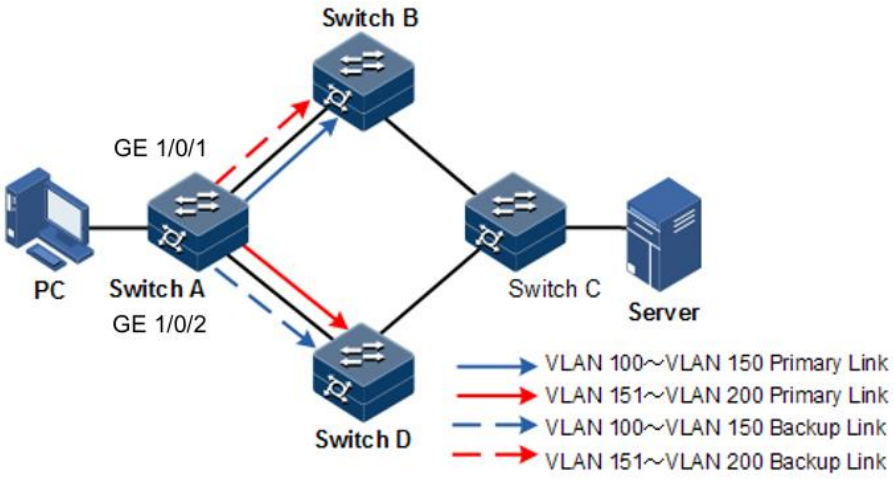
如下图所示，为实现远程 PC 到服务器的可靠访问，需要在 Switch A 上配置接口备份组，并指定 VLAN 列表，实现接口链路保护和负载分担。其要求如下：

- 配置 Switch A 在 VLAN 100～VLAN 150 上，GE 1/0/1 为主接口，GE 1/0/2 为备份接口；
- 配置 Switch A 在 VLAN 151～VLAN 200 上，GE 1/0/2 为主接口，GE 1/0/1 为备份接口。

当 GE 1/0/1 发生链路故障时，切换到备份接口 GE 1/0/2，以保持链路正常。

Switch A 需要支持接口备份功能，Switch B、Switch C、Switch D 无需支持接口备份功能。

图 1-21 接口备份应用组网示意图



配置步骤

步骤 1 创建 VLAN 100～VLAN 200，并将 GE 1/0/1 和 GE 1/0/2 加入到 VLAN 100～VLAN 200 中。

```
JX#configure
JX(config)#vlan 100-200
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-type trunk
JX(config-ge-1/0/1)#port trunk allow-pass vlan 100-200
JX(config-ge-1/0/1)#exit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#port link-type trunk
JX(config-ge-1/0/2)#port trunk allow-pass vlan 100-200
JX(config-ge-1/0/2)#exit
```

步骤 2 在 VLAN 100～VLAN 150 上配置 GE 1/0/1 为主接口，GE 1/0/2 为备份接口。

```
JX(config)#protect-link group 1
JX(config-protectlink-1)#protect-vlan 100-150
JX(config-protectlink-1)#add interface ge 1/0/1 role master
JX(config-protectlink-1)#add interface ge 1/0/2 role slave
```

步骤 3 在 VLAN 151～VLAN 200 上配置 GE 1/0/2 为主接口，GE 1/0/1 为备份接口。

```
JX(config)#protect-link group 2
JX(config-protectlink-1)#protect-vlan 151-200
```

```
JX(config-protectlink-1)#add interface ge 1/0/2 role master
JX(config-protectlink-1)#add interface ge 1/0/1 role slave
```

检查结果

通过 **show protect-link interface** 命令，分别在正常状态和链路故障情况下查看接口备份相关的状态信息。

当 GE 1/0/1 和 GE 1/0/2 链路均为 Forward 时，GE 1/0/1 在 VLAN 100～VLAN 150 上转发流量，GE 1/0/2 在 VLAN 151～VLAN 200 上转发流量。

```
JX#show protect-link interface
 Interface         Group  Role    State     Status    Linkstate
------------------------------------------------------------------
------------------
 ge-1/0/1          1      master  forward   active    up/up
 ge-1/0/2          1      slave   block     active    up/up
 ge-1/0/1          2      slave   block     active    up/up
 ge-1/0/2          2      master  forward   active    up/up
------------------------------------------------------------------
------------------
```

手动断开 Switch A 和 Switch B 之间的链路来模拟故障，此时 GE 1/0/1 变为 Down，则 GE 1/0/2 负责转发 VLAN 100～VLAN 200 上的流量。

```
JX#show protect-link interface
  Interface         Group  Role    State     Status    Linkstate
------------------------------------------------------------------
------------------
 ge-1/0/1          1      master  block     active    up/down
 ge-1/0/2          1      slave   forward   active    up/up
 ge-1/0/1          2      slave   block     active    up/down
 ge-1/0/2          2      master  forward   active    up/up
------------------------------------------------------------------
------------------
```

1.8 接口隔离

1.8.1 简介

通过接口隔离特性，用户可以将需要进行控制的接口使能隔离特性，实现接口之间二层数据的隔离，达到类似于接口之间物理隔离效果，既增强了网络的安全性，也为用户提供了灵活的组网方案。

配置接口保护后，在使能接口保护的接口之间报文不能互通，使能接口保护的接口和未使能接口保护的接口之间的通信不会受影响。

1.8.2 配置准备

场景

通过配置接口隔离功能，可以实现接口之间互相隔离，能增强网络的安全性，也为用户提供了灵活的组网方案。

前提

无

1.8.3 接口隔离的缺省配置

设备上接口隔离的缺省配置如下。

功能	缺省值
各接口的接口隔离功能状态	禁止

1.8.4 配置接口隔离

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**port-isolate group** *group-id*	创建隔离组。
3	JX(config-isolate-group-1)#**add interface** *interface-type interface-number*	将接口加入隔离组

1.8.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

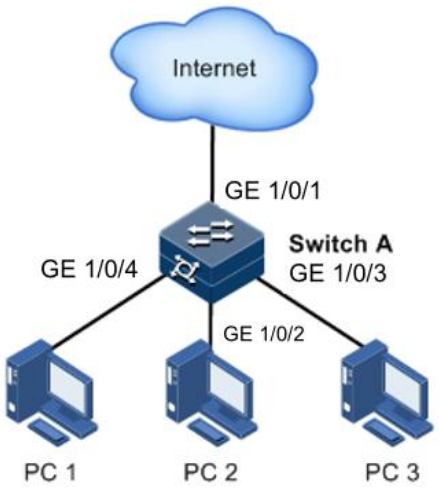
序号	检查项	说明
1	JX#**show port-isolate information**	查看接口保护配置。
2	JX#**show port-isolate group**	查看接口隔离配置信息。

1.8.6 配置接口保护示例

组网需求

如下图所示，为了使 PC1 和 PC2 之间不能互通，但 PC 1 和 PC 2 可以分别与 PC 3 通信，可以在 Switch A 的 GE 1/0/4 和 GE 1/0/2 接口上开启接口保护功能。

图 1-22 接口保护组网示意图



配置步骤

步骤 1 创建接口隔离组。

```
JX#configure
JX(config)#port-isolate group 1
```

步骤 2 将 GE 1/0/1 和 GE 1/0/2 加入隔离组。

```
JX(config-isolate-group-1)##add interface ge 1/0/4
JX(config-isolate-group-1)##add interface ge 1/0/2
```

检查结果

通过 **show port-isolate group** 查看接口保护配置是否正确。

```
JX#show port-isolate group
  GroupId       Ports
------------------------------------------------------------------
------------------
  1             ge-1/0/2 ge-1/0/4
------------------------------------------------------------------
------------------
```

通过 PC 1 ping PC 3、PC 2 ping PC 3 是否能够 ping 通。

- PC 1 ping PC 3，可以 ping 通。
- PC 2 ping PC 3，可以 ping 通。

通过 PC 1 ping PC 2 是否能够 ping 通，查看接口保护功能是否正确。

PC 1 ping PC 2，不能 ping 通，接口保护功能生效。

1.9 L2CP

1.9.1 简介

MEF（Metro Ethernet Forum，城域以太网论坛）引入了服务的概念，如EPL、EVPL、EP-LAN 和 EVP-LAN 等六种服务类型，每种服务对 L2CP（Layer 2 Control Protocol，二层控制协议）报文的处理方式不同。

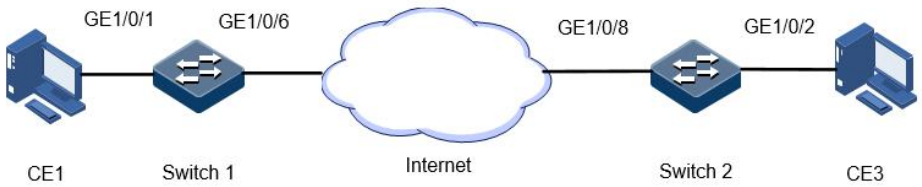
在 MEF6.1 中定义了 L2CP 报文的处理方式，分别为：

- discard：丢弃报文。
- peer：上交到 cpu。
- tunnel：传递到城域网，处理方式配置相比 discard 和 peer 较为复杂。需通过将用户网络侧接口的匹配规则和运营商侧接口 tunnel 终端的配合使用，才能使报文穿过运营商网络。

1.9.2 配置准备

场景

图 1-23 L2CP 拓扑图



switch1,switch2 交换机作为运营商网络接入设备，CE1，CE3 作为用户网络接入设备，CE1，CE3 分别与 switch1 的 ge 1/0/1,switch2 的 ge 1/0/2 相连。

通过配置不同用户网络的 L2PROTOCOL 报文透明传输，使得：

用户网络中的设备可以共同完成生成树功能

前提

无

1.9.3 缺省配置

功能	缺省值
L2CP 功能	未使能

1.9.4 配置 L2CP

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface interface-type** *interface-number*	进入接口配置模式。
3	JX(config-ge-1/0/1)#**l2cp { uni | nni | disable }**	使能 l2cp 功能 uni：用户侧接口 nni：网络侧接口 disable：去使能端口角色 缺省为没有角色
4	JX(config-ge-1/0/1)#**l2cp known-protocol {cdp|eoam3ah|gmrp |gvrp|hgmp|lacp|lldp|pagp|stp |udld|vtp|lamp|esmc |dot1x|elmi|pvst} [vlan** *vlan-id* **] action tunnel group-mac** *mac-address*	在 uni 接口上配置替换规则 known-protocol：匹配的协议名称 mac-address：替换的组播 mac 地址 vlan-id：匹配 vlan id
5	JX(config-ge-1/0/1)#**l2cp protocol-mac** *dst-mac-address* **[vlan** *vlan-id* **] action tunnel group-mac** *mac-address*	在 uni 接口上配置替换规则 dst-mac-address：匹配的目的 mac 地址 mac-address：替换的组播 mac 地址 vlan-id：匹配 vlan id
6	JX(config-ge-1/0/1)#**l2cp known-protocol {cdp|eoam3ah|gmrp |gvrp|hgmp|lacp|lldp|pagp|stp |udld|vtp|lamp|esmc |dot1x|elmi|pvst} action { peer | discard }**	在 uni 接口上配置上送或丢弃规则 known-protocol：匹配的协议名称 peer：上送 CPU discard：丢弃
7	JX(config-ge-1/0/1)#**l2cp protocol-mac** *dst-mac-address* **action { peer | discard }**	在 uni 接口上配置上送或丢弃规则 dst-mac-address：匹配的目的 mac 地址 peer：上送 CPU discard：丢弃

1.9.5 检查配置

步骤	配置	说明
1	JX#show l2cp	显示 l2cp 全局信息。
2	JX#show l2cp config	显示 l2cp 配置信息。
3	JX#show protocol statistics rx with-value	显示 l2cp 上送 CPU 的报文统计

1.9.6 配置 L2CP 示例

配置步骤

步骤 1 配置 CE-1：

```
JX(config)#stp enable
```

步骤 2 配置 CE-3：

```
JX(config)#stp enable
```

步骤 3 配置 switch1：

```
JX(config-ge-1/0/1)#l2cp uni
JX(config-ge-1/0/1)#l2cp known-protocol stp action tunnel
group-mac 01:00:0c:cd:cd:d0
JX(config-ge-1/0/6)#l2cp nni
```

步骤 4 配置 switch2：

```
JX(config-ge-1/0/2)#l2cp uni
JX(config-ge-1/0/2)#l2cp known-protocol stp action tunnel
group-mac 01:00:0c:cd:cd:d0
JX(config-ge-1/0/8)#l2cp nni
```

检查配置

CE1 和 CE3 上分别可以看到对方的生成树信息

1.10 BFD

1.10.1 简介

双向转发检测 BFD（Bidirectional Forwarding Detection）是一种全网统一的检测机制，用于快速检测、监控网络中链路或者 IP 路由的转发连通状况。

1.10.2 配置准备

场景

BFD 在两台网络设备上建立会话，用来检测网络设备间的双向转发路径，为上层应用服务。BFD 本身并没有邻居发现机制，而是靠被服务的上层应用通知其邻居信息以建立会话。会话建立后会周期性地快速发送 BFD 报文，如果在检测时间内没有收到 BFD 报文则认为该双向转发路径发生了故障，通知被服务的上层应用进行相应的处理。

前提

无

1.10.3 BFD 的缺省配置

设备上接口隔离的缺省配置如下。

功能	缺省值
全局 BFD 功能	未使能
发送间隔	1000 毫秒
接收间隔	1000 毫秒
本地检测倍数	3

1.10.4 配置 BFD 静态会话检测

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**bfd start**	全局使能 bfd。
3	JX(config)#bfd track 1 remote-ip 10.0.0.2 local-ip 10.0.0.1 interface vlan 1	配置 track，产生 bfd 静态会话。
4	JX(config)#bfd track 1 remote-ip6 2001::2 local-ip6 2001::1 interface vlan 1	配置 track，产生 ipv6 bfd 静态会话。

1.10.5 配置 BFD 单臂回声会话

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。

步骤	配置	说明
2	JX(config)#**bfd start**	全局使能 bfd。
3	JX(config)#bfd track 1 remote-ip 10.0.0.2 local-ip 10.0.0.1 interface vlan 1 one-arm-echo	配置单臂 ECHO 功能的 BFD 会话。
4	JX(config)#bfd track 1 remote-ip6 2001::2 local-ip6 2001::1 interface vlan 1 one-arm-echo	配置单臂 ECHO 功能的 BFD 会话。

1.10.6 配置 BFD 检测三层 eth-trunk

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**bfd start**	全局使能 bfd。
3	JX(config)#bfd track 1 link-bundle remote-ip 10.0.0.2 local-ip 10.0.0.1 interface eth-trunk 1	配置 track 绑定聚合口，产生主会话和子会话。
4	JX(config)#bfd track 1 link-bundle remote-ip6 2001::2 local-ip 2001::1 interface eth-trunk 1	配置 track 绑定聚合口，产生主会话和子会话。

1.10.7 配置 BFD 会话参数

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**bfd start**	全局使能 bfd。
3	JX(config)#bfd track 1 remote-ip 10.0.0.2 local-ip 10.0.0.1	创建会话。
4	JX(config)#bfd track 1 min-tx 1000 min-rx 1000 multiplier 3	配置会话参数。

1.10.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

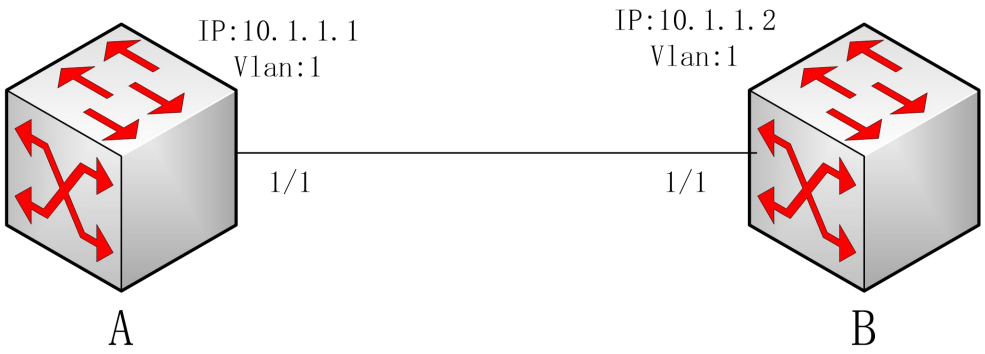
序号	检查项	说明
1	JX#**show bfd session**	查看 bfd 会话。
2	JX#**show bfd track**	查看 bfd track。
3	JX#**show bfd link-bundle session**	查看 bfd link-bundle 会话。

1.10.9 配置 BFD 单跳应用示例

组网需求

如下图所示，配置 BFD 单跳会话检测设备 A、B 之间的链路状态。

图 1-24 BFD 单跳应用



配置步骤

步骤 1 配置 A 设备 IP 和会话参数。

```
JX#config
JX(config)#interface vlan 1
JX(config)#ip address 10.1.1.1/24
JX(config)#bfd track 1 remote-ip 10.1.1.2 local-ip 10.1.1.1
interface vlan 1
JX(config)#bfd track 1 min-tx 500 min-rx 600 multiplier 3
```

步骤 2 配 A 设备 IP 和会话参数。

```
JX#config
JX(config)#interface vlan 1
JX(config)#ip address 10.1.1.1/24
JX(config)#bfd track 1 remote-ip 10.1.1.1 local-ip 10.1.1.2
interface vlan 1
JX(config)#bfd track 1 min-tx 500 min-rx 600 multiplier 4
```

检查结果

通过 **show bfd session** 查看会话状态

```
JX>show bfd session
  Interface       State Local-Discr Remote-Discr local-addr          remote-addr
```

```
------------------------------------------------------------------------------
------------

  vlan-1          up     1            1              10.1.1.1          10.1.1.2
------------------------------------------------------------------------------
----------------------------
```

1.11 链路震荡保护

1.11.1 简介

链路震荡保护（Link-flap Protection）是一种将物理状态频繁 Up/Down 变化的接口关闭，使之处于 Down 状态，防止网络拓扑结构频繁变化的技术。

1.11.2 配置准备

场景

网络抖动或者链路线路故障等原因会引起本端设备接口物理状态频繁 Up/Down 变化，导致链路震荡，致使网络拓扑结构频繁变化，影响用户通信。为了解决上述问题，用户可以配置链路震荡保护，将物理状态频繁 Up/Down 的接口关闭，使之处于 Down 状态，使网络拓扑结构停止频繁变化。

链路震荡次数：接口状态 Up/Down 切换一次，记为一次震荡。

链路震荡检测时间间隔：系统需要统计指定时间间隔内链路震荡的次数。

如果在链路震荡检测时间间隔内，链路震荡次数达到了门限值，则将该端口关闭。

前提

无

1.11.3 链路震荡保护的缺省配置

设备上接口隔离的缺省配置如下。

功能	缺省值
使能链路震荡保护	未使能
链路检测检测时间间隔	10 秒
链路震荡次数	5 次

1.11.4 配置链路震荡保护

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/*)#**port link-flap protection** { **enable** | **disable** }	配置链路震荡保护使能或去使能。
4	JX(config)#**port link-flap interval** { *60* | **default**}	配置链路震荡检测时间间隔。
5	JX(config)#**port link-flap threshold** { *7* | **default**}	配置链路震荡次数门限值。

1.11.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show link-flap config**	查看链路震荡保护相关配置。
2	JX#**show link-flap interface**	查看链路震荡保护相关接口信息。

1.11.6 配置链路震荡保护应用示例

配置步骤

步骤 1 配置 A 设备 IP 和会话参数。

```
JX#configure
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port link-flap protection enable
JX(config-ge-1/0/1)#port link-flap interval 60
JX(config-ge-1/0/1)#port link-flap threshold 7
```

检查结果

通过 **show link-flap interface** 查看链路震荡保护接口状态

```
JX#show link-flap interface
 Error-down recovery interval   : 0
 Interface          Status      Interval    Threshold
-------------------------------------------------------------
---------
 ge-1/0/1           enable      60          7
```
