7.8 LACP配置

7.8.1 LACP概述

LACP（Link Aggregation Control Protocol）即链路聚合控制协议，是IEEE 802.3ad描述的标准协议。

链路聚合（Link Aggregation）是指将具有相同传输介质类型、相同传输速率的物理链路段“捆绑”在一起，在逻辑上看起来好像是一条链路。链路聚合又称中继（Trunking），它允许交换机之间或交换机和服务器之间的对等的物理链路同时成倍地增加带宽。因此，它在增加链路的带宽、创建链路的传输弹性和冗余等方面是一种很重要的技术。

聚合的链路又称干线（Trunk）。如果Trunk中的一个端口发生堵塞或故障，那么数据包会被分配到该Trunk中的其他端口上进行传输。如果这个端口恢复正常，那么数据包将被重新分配到该Trunk中所有正常工作的端口上进行传输。

除ZXR10 2850-52TC最多支持16个聚合组外，其他型号交换机最多支持8个聚合组，每个聚合组参与聚合的端口不超过8个。参与聚合的端口应具有相同的传输介质类型、相同的传输速率。

NOTE **说明：**

此功能在ZXR10 2850-52TCLE交换机中最多支持8个聚合组。

7.8.2 LACP基本配置

在交换机上配置LACP包括以下内容。

命令	功能
zte(cfg)#**set lacp** { **enable**| **disable**}	使能/关闭LACP，LACP功能的缺省状态是关闭的
zte(cfg)#**set lacp aggregator** < *trunkid*> **add port** < *portlist*>	在LACP聚合组中加入指定端口
zte(cfg)#**set lacp aggregator** < *trunkid*> **delete port** < *portlist*>	在LACP聚合组中删除指定端口 端口处于自动协商模式时允许聚合；否则如果端口处于双工模式则允许聚合，处于半双工模式则不允许聚合

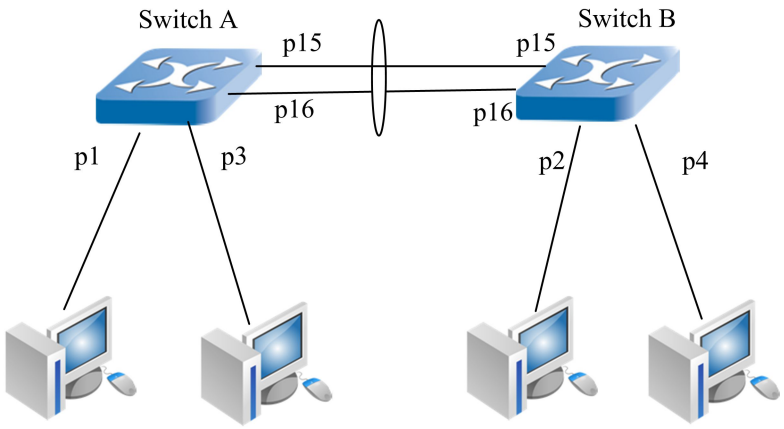
命令	功能
zte(cfg)#**set lacp aggregator** < *trunkid*> **mode** { **dynamic**| **static**| **mixed**}	设置聚合组聚合模式 当聚合组配置成动态模式时，则只能与运行LACP的设备对接。当配置成静态模式时，如果对端是静态的Trunk（不运行LACP协议），则进行静态聚合；当聚合组配置成混合模式时，如果对端是静态的Trunk（不运行LACP协议），则进行静态聚合；当对端同时存在静态Trunk和LACP时，优先考虑LACP聚合
zte(cfg)#**set lacp port** < *portlist*> **timeout** { **long**| **short**}	设置参与聚合的端口的超时情况 超时情况是指处于聚合状态的端口没有收到对端的LACP协议包时，经过多长时间退出聚合，短超时是3秒，长超时是90秒
zte(cfg)#**set lacp port** < *portlist*> **mode** { **active**| **passive**}	设置端口参与聚合的模式 端口参与聚合的模式是指在聚合组非静态模式下，聚合组内端口以主动或被动方式发送LACP协议包来更新状态信息的方式。当本端端口配置为主动协商模式时，对端端口可配置为主动或被动协商模式；当本端端口配置为被动协商模式时，对端端口只能配置为主动协商模式，否则不能成功参与聚合（运行LACP协议时）
zte(cfg)#**set lacp priority** < *1-65535*>	设置LACP的优先级
zte(cfg)#**show lacp**	显示LACP的配置信息
zte(cfg)#**show lacp aggregator** [< *trunkid*>]	显示LACP聚合组聚合信息
zte(cfg)#**show lacp port** [< *portlist*>]	显示LACP参与聚合的端口信息

配置聚合组后，可以对它进行各种设置，如设置PVID、加入VLAN、静态绑定MAC地址等。

7.8.3 LACP配置实例

如 图7-5所示，交换机A和交换机B通过聚合端口相连（将端口15和16捆绑而成），交换机A的端口1与交换机B的端口2属于VLAN2，交换机A的端口3与交换机B的端口4属于VLAN3，相同VLAN的成员之间能够互相通信。

图7-5 LACP配置实例



交换机A的配置：

```
zte(cfg)#set lacp enable
zte(cfg)#set lacp aggregator 3 add port 15-16
zte(cfg)#set lacp aggregator 3 mode dynamic
zte(cfg)#set vlan 2 add trunk 3 tag
zte(cfg)#set vlan 2 add port 1 untag
zte(cfg)#set vlan 3 add trunk 3 tag
zte(cfg)#set vlan 3 add port 3 untag
zte(cfg)#set port 1 pvid 2
zte(cfg)#set port 3 pvid 3
zte(cfg)#set vlan 2-3 enable
```

交换机B的配置：

```
zte(cfg)#set lacp enable
zte(cfg)#set lacp aggregator 3 add port 15-16
zte(cfg)#set lacp aggregator 3 mode dynamic
zte(cfg)#set vlan 2 add trunk 3 tag
zte(cfg)#set vlan 2 add port 2 untag
zte(cfg)#set vlan 3 add trunk 3 tag
zte(cfg)#set vlan 3 add port 4 untag
zte(cfg)#set port 2 pvid 2
zte(cfg)#set port 4 pvid 3
zte(cfg)#set vlan 2-3 enable
```

7.9 STP配置

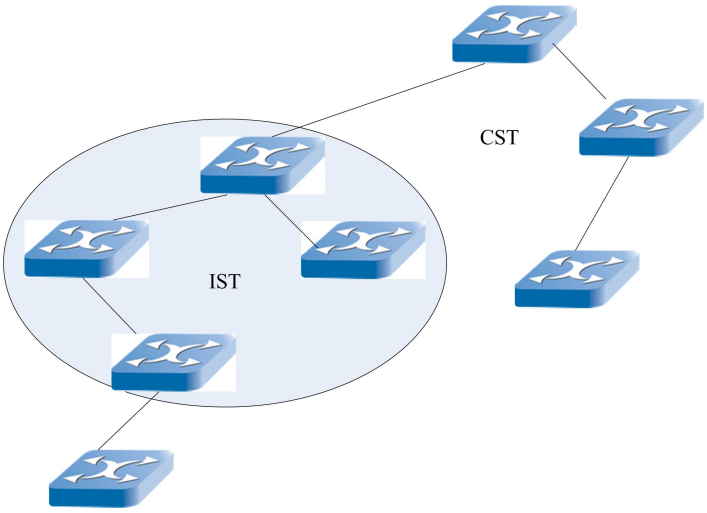
7.9.1 STP概述

STP（生成树协议）应用于有环路的网络，通过一定的算法得到一条通路，并阻断冗余路径，将环路网络修剪成无环路的树型网络，从而避免报文在环路网络中的增生和无限循环。当这条通路正常工作时，其余路径是关闭的；当这条通路出现故障时，将重新进行计算得到一条新的通路。

RSTP（快速生成树协议）在普通STP协议的基础上增加了端口可以快速由Blocking状态转变为Forwarding状态的机制，加快了拓扑的收敛速度。

MSTP（多生成树协议）是在快速和普通生成树协议基础上，增加对带有VLAN ID的帧转发的处理。整个网络拓扑结构可以规划为总生成树CIST，分为CST（主干生成树）和IST（区域生成树），如图7-6所示。

图7-6 多生成树的拓扑结构



在整个多生成树的拓扑结构中，可以把一个IST看作一个单个的网桥（交换机），这样就可以把CST作为一个RSTP生成树来进行配置信息（BPDU）的交互。在一个IST区域内可以创建多个实例，这些实例只在本区域内有效。可以把每一个实例等同于一个RSTP生成树，不同的是还要与区域外的网桥进行BPDU的交互。

用户在创建某个实例时，必须将一个或多个VLAN ID划入此实例中。IST区域内的网桥上属于这些VLAN的端口通过BPDU的交互，最终构成一个生成树结构（每个实例对应一个生成树结构）。

这样，该区域内的网桥在转发带有这些VLAN ID的数据帧时，将根据对应实例的生成树结构进行转发。对于要转发到该区域外的数据帧，无论它带有何种VLAN ID，均按照CST的RSTP生成树结构进行转发。

与RSTP相比，MSTP的优点在于：在某个IST区域中，可以按照用户设定的生成树结构对带有某个VLAN ID的数据帧进行转发，并保证不会造成环路。

7.9.2 STP基本配置

默认配置中，MSTP只有实例为0的实例，并且此实例永远存在，用户无法通过手工删除。此实例映射的VLAN为1~4094。

命令	功能
zte(cfg)#**set stp** { **enable**| **disable**}	使能/关闭STP
zte(cfg)#**set stp forceversion** { **mstp**| **rstp**| **stp**}	设置STP的强制类型
zte(cfg)#**set stp instance** < *0-15*> [**add**| **delete**] **vlan** < *vlanlist*>	设置VLAN和instance的映射关系 该命令新建一个实例，并设置VLAN与该实例的映射关系。这些VLAN将自动从instance 0的VLAN映射表中删除，加入新建实例的VLAN映射表中
zte(cfg)#**set stp instance** < *0-15*> **bridgeprio** < *0-61440*>	设置网桥优先级
zte(cfg)#**set stp instance** < *0-15*> **port** < *portname*> **priority** < *0-255*>	设置实例端口优先级
zte(cfg)#**set stp instance** < *0-15*> **trunk** < *trunkid* > **priority** < *0-255*>	设置实例trunk的优先级
zte(cfg)#**set stp instance** < *0-15*> **port** < *portname*> **cost** < *1-200000000*>	设置实例端口费用
zte(cfg)#**set stp instance** < *0-15*> **port** < *portname*> **root-guard** { **enable**| **disable**}	使能/关闭实例端口root保护
zte(cfg)#**set stp instance** < *0-15*> **port** < *portname*> **loop-guard**{ **enable**| **disable**}	使能/关闭实例端口loop保护
zte(cfg)#**set stp instance** < *0-15*> **trunk** < *trunkname*> **cost** < *1-200000000*>	设置实例trunk费用
zte(cfg)#**set stp instance** < *0-15*> **trunk** < *trunkname*> **root-guard** { **enable**| **disable**}	使能/关闭实例trunk root保护
zte(cfg)#**set stp instance** < *0-15*> **trunk** < *trunkname*> **loop-guard**{ **enable**| **disable**}	使能/关闭实例trunk loop保护
zte(cfg)#**set stp port** < *portlist*> { **enable**| **disable**}	使能/关闭端口STP功能
zte(cfg)#**set stp trunk** < *trunklist*> { **enable**| **disable**}	使能/关闭trunk的STP功能
zte(cfg)#**set stp port** < *portlist*> **bpdu-guard**{ **enable**| **disable**}	使能/BPDU 保护
zte(cfg)#**set stp port** < *portlist*> **pcheck**	设置端口STP类型检查

命令	功能
zte(cfg)#**set stp bpdu_interval** < *10-65535*>	设置BPDU保护端口linkdown的时间间隔
zte(cfg)#**set stp port** < *portlist*> **linktype** { **point-point**| **shared**}	设置实例端口的Linktype类型
zte(cfg)#**set stp trunk** < *trunklist*> **linktype** { **point-point**| **shared**}	设置实例trunk的Linktype类型
zte(cfg)#**set stp port** < *portlist*> **packettype** { **IEEE**| **CISCO**| **HUAWEI**| **HAMMER**| **extend**}	设置实例端口的包类型
zte(cfg)#**set stp trunk** < *trunkid*> **packettype** { **IEEE**| **CISCO**| **HUAWEI**| **HAMMER**| **extend** }	设置实例trunk的包类型
zte(cfg)#**set stp hellotime** < *1-10*>	设置STP的通告间隔时间
zte(cfg)#**set stp forwarddelay** < *4-30*>	设置STP的转发延迟时间
zte(cfg)#**set stp agemax** < *6-40*>	设置STP的老化时间
zte(cfg)#**set stp hopmax** < *1-40*>	设置MST的任意两终端间的最大跳数
zte(cfg)#**set stp name** < *name*>	设置MST的区域名称
zte(cfg)#**set stp revision** < *0-65535*>	设置MST的版本号 同一区域内MST的版本号必须相同
zte(cfg)#**set stp relay** { **enable**| **disable**}	使能/关闭STP Relay
zte(cfg)#**set stp edge-port** { **add**| **delete**} **port** < *portlist*>	设置边缘端口
zte(cfg)#**set stp hmd5-digest** { **CISCO**| **HUAWEI**} < *0,0x00..0-0xff..f*>	设置STP的hmd5摘要
zte(cfg)#**set stp hmd5-key** { **CISCO**| **HUAWEI**} < *0,0x00..0-0xff..f*>	设置STP的hmd5关键字
zte(cfg)#**show stp**	显示STP的信息
zte(cfg)#**show stp instance** [< *0-15*>]	显示STP实例的信息
zte(cfg)#**show stp port** [< *portlist*>]	显示STP端口的信息
zte(cfg)#**show stp trunk** < *trunklist*>	显示STP trunk的信息
zte(cfg)#**show stp relay**	显示STP Relay的信息

7.9.3 STP配置实例

下面的例子介绍了MSTP的具体配置。

1. 新建instance 1，与VLAN 10−20建立映射，并设置名称为zte，MST版本号为10。

```
zte(cfg)#set stp instance 1 add vlan 10-20
zte(cfg)#set stp name zte
```

```
zte(cfg)#set stp revision 10

zte(cfg)#show stp
  The spanning_tree protocol is enabled!

  The STP ForceVersion is MSTP !
  Revision: 10     Name: zte
  Cisco key:     0x13ac06a62e47fd51f95d2ba243cd0346
  Cisco digest:  0x00000000000000000000000000000000
  Huawei key:    0x13ac06a62e47fd51f95d2ba243cd0346
  Huawei digest: 0x00000000000000000000000000000000
  Instance VlanMap
  -------- --------------------
  0        1-9,21-4094
  1        10-20
zte(cfg)#
```

2. 设置实例的网桥优先级和实例端口的优先级。

```
zte(cfg)#set vlan 10 add port 2 untag
zte(cfg)#set stp instance 1 bridgeprio 7
zte(cfg)#set stp instance 1 port 2 priority 112

zte(cfg)#show stp instance 0
  RootID:
  Priority       : 32768       Address     : 00.d0.d0.ff.ff.0a
  HelloTime(s)   : 2           MaxAge(s)   : 20
  ForwardDelay(s): 15

  Reg  RootID:
  Priority       : 32768       Address     : 00.d0.d0.ff.ff.0a
  RemainHops     : 20

  BridgeID:
  Priority       : 32768       Address     : 00.d0.d0.ff.ff.0a
  HelloTime(s)   : 2           MaxAge(s)   : 20
  ForwardDelay(s): 15          MaxHops     : 20

  Interface PortId Cost      Status  Role       Bound GuardStatus
```

```
  --------- ------ --------- ------- ---------- ----- -----------
  2         128.2  200000    Forward Designated RSTP  None
zte(cfg)#show stp instance 1
  RootID:
  Priority       : 1           Address     : 00.d0.d0.ff.ff.0a
  HelloTime(s)   : 2           MaxAge(s)   : 20
  ForwardDelay(s): 15          RemainHops  : 20
  BridgeID:
  Priority       : 1           Address     : 00.d0.d0.ff.ff.0a
  HelloTime(s)   : 2           MaxAge(s)   : 20
  ForwardDelay(s): 15          MaxHops     : 20

  Interface PortId Cost      Status  Role       GuardStatus
  --------- ------ --------- ------- ---------- -----------
  2         112.2  200000    Discard Designated None

zte(cfg)#show stp port 2
The following ports are active!
  PortId      : 2             MSTI        : 00
    Priority    : 128           Cost        : 200000
    Status      : Forward       Role        : Designated
EdgePort    : Disabled      GuardType   : None

    LinkType    : P2P           PacketType  : IEEE

  PortId      : 2             MSTI        : 01
    Priority    : 112           Cost        : 200000
    Status      : Forward       Role        : Designated
    EdgePort    : Disabled      GuardType   : None
    LinkType    : P2P           PacketType  : IEEE
```

7.10 IGMP Snooping配置

本节主要介绍如何配置Internet Group Management Protocol(IGMP) Snooping功能，对应支持此功能的v1、v2和v3版本，同时为用户提供配置IGMP Snooping、组播过滤、静态组播等功能的详细说明和参考。

7.10.1 IGMP Snooping概述

由于组播地址不可能出现在报文的源地址中，所以交换机无法学习到组播地址。当交换机收到组播信息时，会向同一个VLAN中的所有端口广播。如果不采取措施，就会出现不想要的组播信息扩散到网络中每一点的严重问题，浪费网络带宽资源。

IGMP Snooping通过对主机和路由器之间的IGMP协议通信的“监听”，使组播包只发送给在组播转发表中的端口，而不是所有端口，从而限制了局域网交换机上的组播信息扩散，减少了不必要的网络带宽的浪费，提高了交换机的利用率。

基于源或目的地址的组播过滤，能够按照用户在监听VLAN添加的过滤条目对主机向路由器发送的IGMP协议报文进行过滤处理，增强交换机对组播监听的控制。

7.10.2 IGMP Snooping基本配置

在交换机上配置IGMP Snooping包括以下内容。

步骤	命令	功能
1	zte(cfg)#**set igmp snooping** { **enable**| **disable**}	使能或关闭IGMP Snooping功能，缺省为**disable**
2	zte(cfg)#**set igmp snooping add vlan** < *vlanlist*>	添加对指定VLAN的IGMP Snooping功能
3	zte(cfg)#**set igmp snooping delete vlan** < *vlanlist*>	删除对指定VLAN的IGMP Snooping功能 只有添加对指定的VLAN进行组播监听的功能，才能监听到相应的组播转发表。本交换机最多支持同时监听256个VLAN
4	zte(cfg)#**set igmp snooping query vlan** < *vlanlist*> { **enable**| **disable**}	使能或关闭对指定VLAN的IGMP Query功能
5	zte(cfg)#**set igmp snooping vlan** < *vlanname*> **add group** < *A.B.C.D*>	添加基于VLAN的静态组播组
6	zte(cfg)#**set igmp snooping vlan** < *vlanname*> **delete group** < *A.B.C.D*>	删除基于VLAN的静态组播组
7	zte(cfg)#**set igmp snooping vlan** < *1-4094*> **add group** < *A.B.C.D*> [**port** < *portlist*> | **trunk** < *trunklist*>]	在指定VLAN中添加基于端口或聚合口的静态组播组
8	zte(cfg)#**set igmp snooping vlan** < *1-4094*> **delete group** < *A.B.C.D*> [**port** < *portlist*> | **trunk** < *trunklist*>]	在指定组播监听VLAN中删除基于端口或聚合口的静态组播组
9	zte(cfg)#**set igmp snooping vlan** < *1-4094*> **add smr** [**port** < *portlist*> | **trunk** < *trunklist*>]	在指定组播监听VLAN中加入静态路由端口或静态路由聚合口

步骤	命令	功能
10	zte(cfg)#**set igmp snooping vlan** < *1-4094*> **delete smr** [**port** < *portlist*> | **trunk** < *trunklist*>]	在指定组播监听VLAN中删除静态路由端口或静态路由聚合口 当为某个监听VLAN添加了静态路由端口或聚合口后，能够将此端口或聚合口添加到此监听VLAN对应的所有组播组中，并且组播组中成员端口的加入、离开等报文将同时向路由端口和此静态路由端口转发
11	zte(cfg)#**set igmp snooping add maxnum** < *1-256*> **vlan** < *vlanlist*>	设置指定组播监听VLAN的最大组播组数目限制
12	zte(cfg)#**set igmp snooping delete maxnum vlan** < *vlanlist*>	清除指定组播监听VLAN的最大组播组数目限制
13	zte(cfg)#**set igmp snooping timeout** < *100-2147483647*> { **host**| **router**}	设置组播成员/路由超时
14	zte(cfg)#**set igmp snooping query-interval** < *10-2147483647*>	设置查询周期
15	zte(cfg)#**set igmp snooping response-interval** < *10-250*>	设置查询响应周期
16	zte(cfg)#**set igmp snooping last-member-query** < *10-250*>	设置最后的成员查询周期
17	zte(cfg)#**set igmp snooping fastleave** { **enable**| **disable**}	允许/禁止快速离开，缺省为**disable**
18	zte(cfg)#**set igmp snooping crossvlan** { **enable**| **disable**}	允许/禁止跨VLAN组播监听，缺省为**disable**
19	zte(cfg)#**set igmp filter** { **enable**| **disable**}	使能或关闭组播过滤功能，组播过滤功能的缺省状态是关闭的
20	zte(cfg)#**set igmp filter add groupip** < *A.B.C.D*> **vlan** < *vlanlist*>	添加基于VLAN的组播组地址过滤
21	zte(cfg)#**set igmp filter delete groupip** < *A.B.C.D*> **vlan** < *vlanlist*>	删除基于VLAN的组播组地址过滤
22	zte(cfg)#**set igmp filter add sourceip** < *A.B.C.D*> **vlan** < *vlanlist*>	添加基于VLAN的组播源地址过滤
23	zte(cfg)#**set igmp filter delete sourceip** < *A.B.C.D*> **vlan** < *vlanlist*>	删除基于VLAN的组播源地址过滤
24	zte(cfg)#**set igmp snooping query version** { **v2**| **v3**}	设置组播查询器版本
25	zte(cfg)#**set igmp snooping proxy version** { **v2**| **auto**}	设置组播代理版本
26	zte(cfg)#**set igmp snooping v3** { **enable**| **disable**}	设置IGMPv3版本组播功能
27	zte(cfg)#**show igmp snooping**	显示组播监听的配置

步骤	命令	功能
28	zte(cfg)#**show igmp snooping vlan** [< *vlanname*> [**host**| **router**]]	显示组播监听结果
29	zte(cfg)#**show igmp filter**	显示组播过滤状态
30	zte(cfg)#**show igmp filter vlan** < *1-4094*>	显示某监听VLAN的组播地址过滤条目
31	zte(cfg)#**show igmp snooping v3 port** < *num*>	显示端口上监听到的v3组播组信息
32	zte(cfg)#**show igmp snooping v3 trunk** < *num*>	显示聚合口上监听到的v3组播组信息

步骤2中：

当IGMP Snooping功能关闭时，对于组播流根据set port multicast命令的配置进行处理，如果选择参数forward则对相应端口进行转发，如果选择discard则对相应端口丢弃。

使能IGMP Snooping功能后，对于组播流首先根据监听到的组播转发表来转发，如果没有查找到该组播转发表，则按照上述的配置针对端口决定转发或丢弃。

当IGMP Snooping关闭时，对于非路由端口，最好关闭端口的组播转发功能；而对于路由端口，最好开启端口的组播转发功能。

步骤4：

使能了IGMP Snooping功能后，如果没有IGMP Query路由器存在，则无法完成正常的IGMP Snooping的功能，这时可以开启交换机的IGMP Query的功能。

如果所监听的VLAN存在IGMP Query路由器，最好关闭本交换机的IGMP Query功能。交换机运行的IGMP Query版本是V2.0，遵循V2.0 IGMP Query路由器选举功能。当配置了三层端口的IP和MAC地址，则IGMP Query的源IP和源MAC使用三层配置；否则使用223.255.255.255和交换机的MAC地址作为IGMP Query的源。

步骤6：

当已添加了基于此VLAN和某些端口的静态组播组后，则不再允许添加仅基于此VLAN的静态组播组；同时，当删除基于VLAN的静态组播组时，则已添加了基于此VLAN和某些端口的静态组播组也被同时清除。

步骤8：

当运行了IGMP Snooping的功能，允许以本交换机的名义注册基于VLAN或基于VLAN+端口的静态组播组，本交换机支持最多对64个静态组播组的注册。

注册的静态组播组只能是用户组播地址224.x.x.x~239.x.x.x，不能是保留的组播地址。224.0.0.x的组播地址不允许注册。

步骤12：

缺省状态下，每个被监听的VLAN所能建立的组播组数目为256，当设置了此VLAN的组播组数目后，此VLAN上所能建立的组播组条目不会大于此VLAN限制的组播组数目。

设置IGMP过滤最大组数的VLAN必须是监听的VLAN。

步骤17：

运行了IGMP Snooping功能，并正确地监听到了主机加入的端口后，当该端口收到IGMP离开报文时，如果关闭了IGMP的快速离开功能，则交换机将向该端口发送两次特定组查询，以确认是否在组播转发表中删除该端口；如果使能了IGMP的快速离开功能，则不进行特定组查询，直接从组播转发表中删除该端口。

当跨VLAN的组播监听从使能状态变为关闭状态时，经过跨VLAN组播监听的某些监听结果要经过相应的超时时长才能正确删除掉。

步骤18：

当运行了IGMP Snooping功能，并利用PVID（default vlan_id）正确地配置一对多的端口转发形式后，可以利用本交换机跨VLAN的IGMP Snooping功能对不同VLAN之间的IGMP信息进行监听并进行跨VLAN的组播转发。

步骤19：

当使能组播过滤功能后，对于组播加入请求的处理，将按照添加的组播过滤条目对其进行过滤后再进行处理；如果组播过滤功能关闭，对于端口的加入请求，将不作任何基于源地址或组地址的过滤操作。

步骤20：

在组播过滤使能后，设置了基于VLAN的组播组地址过滤条目后，此VLAN内的端口如果收到组地址为此过滤地址的组播加入请求时，本端交换机不对此端口的加入请求进行处理。

步骤22：

在组播过滤使能后，设置了基于VLAN的组播源地址过滤条目后，此VLAN内的端口如果收到源地址为此过滤地址的组播加入请求时，本端交换机不对此端口的加入请求进行处理。

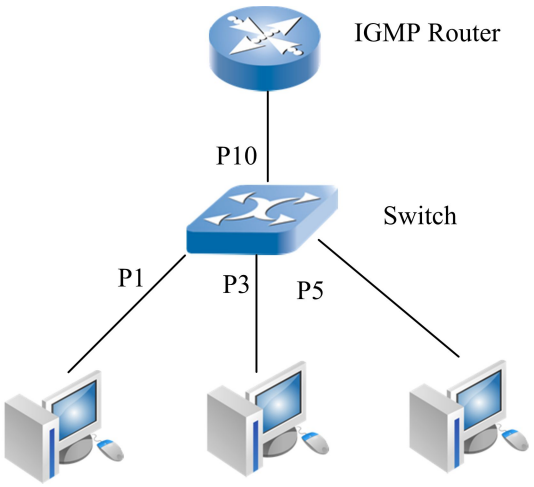
7.10.3 IGMP Snooping配置实例

实例一：

如图7-7所示，端口1，3，5接主机，端口10接路由器，将端口10，1，3，5加入到VLAN200，端口1、3，5上的用户分别发送组地址为230.44.45.167、230.44.45.157的组播加

入请求，在VLAN200上添加组播过滤组地址230.44.45.167。在交换机上开启IGMP Snooping和IGMP Filter功能并显示监听结果。

图7-7 一对多通信方式的网络拓扑结构示意图



具体配置如下：

```
zte(cfg)#set vlan 200 add port 1,3,5,10 untag
zte(cfg)#set vlan 210 add port 1,10 untag
zte(cfg)#set vlan 230 add port 3,10 untag
zte(cfg)#set vlan 250 add port 5,10 untag
zte(cfg)#set port 10 pvid 200
zte(cfg)#set port 1 pvid 210
zte(cfg)#set port 3 pvid 230
zte(cfg)#set port 5 pvid 250
zte(cfg)#set vlan 200,210,230,250 fid 200
zte(cfg)#set vlan 200,210,230,250 enable
zte(cfg)#set igmp snooping enable
zte(cfg)#set igmp snooping add vlan 200,210,230,250
zte(cfg)#set igmp snooping crossvlan disable
```

显示组播监听结果：

```
zte(cfg)#show igmp snooping vlan

Num  VlanId  Group             Last_Report      PortMember
1    210      224.1.1.1         192.168.1.1      1
2    230      224.1.1.1         192.168.1.2      3
3    250      224.1.1.1         192.168.1.3      5
```

在交换机上开启跨VLAN组播监听，经过组播监听的显示结果：

```
zte(cfg)#set igmp snooping crossvlan enable
zte(cfg)#show igmp snooping vlan
Num  VlanId  Group             Last_Report      PortMember
1    210     224.1.1.1         192.168.1.1      1,10
2    230     224.1.1.1         192.168.1.2      3,10
3    250     224.1.1.1         192.168.1.3      5,10
4    200     224.1.1.1         192.168.1.3      1,3,5,10
```

实例二：

如图7-7所示，端口1，3，5接主机，端口10接路由器，将端口10，1，3，5加入到vlan 200，端口1、3，5上的用户分别发送组地址为230.44.45.167、230.44.45.157组播加入请求，在vlan200上添加组播过滤组地址230.44.45.167。在交换机上开启IGMP Snooping和IGMP Filter功能并显示监听结果。

具体配置如下：

```
zte(cfg)#set vlan 200 add port 1,3,5,10 untag
zte(cfg)#set port 1,3,5,10 pvid 200
zte(cfg)#set vlan 200 enable
zte(cfg)#set igmp snooping enable
zte(cfg)#set igmp snooping add vlan 200
zte(cfg)#set igmp filter enable
zte(cfg)#set igmp filter add groupip 230.44.45.167 vlan 200
```

显示组播监听及过滤结果：

```
zte(cfg)#show igmp snooping vlan
Num  VlanId  Group             Last_Report      PortMember
1    200     230.44.45.157     192.168.1.1      1,3,5,10


zte(cfg)#sho igmp filter
  IGMP Filter: enabled
  Index Type       IpAddress        VlanList
  ----- ---------- -------------- -------------- ---------
  1     Groupip    230.44.45.167    200
zte(cfg)#show igmp filter vlan 200
  The filter address list of this vlan:
  Index FilterIpAddress  Vlan   Type
  ----- ---------- -----  ------
  1      230.44.45.167     200    Groupip
```

7.11 IPTV配置

7.11.1 IPTV概述

IPTV又称交互式网络电视，是由运营商基于宽带基础推出的，利用IP宽带网络，集互联网、多媒体、通信等多种技术于一体，向用户提供直播电视、视频点播、上网浏览等多种交互式服务的业务，用户可以通过PC或“IP机顶盒＋电视”的方式使用的业务。

7.11.2 IPTV基本配置

交换机上IPTV的配置包括以下内容。

1. 配置IPTV全局参数

命令	功能
zte(cfg-nas)#**iptv control** { **enable**| **disable**}	开启或关闭IPTV控制功能
zte(cfg-nas)#**iptv control login-time** < *1-65534*>	设置用户的最小识别时间
zte(cfg-nas)#**iptv control prvcount count** < *0-65535*>	设置全局最大预览次数
zte(cfg-nas)#**iptv control prvinterval** < *2-65535*>	设置全局最小预览间隔
zte(cfg-nas)#**iptv control prvtime** < *1-65535*>	设置全局最大预览时间
zte(cfg-nas)#**iptv control prvcount reset-period** < *1-4294967295*>	设置全局复位预览次数的周期

2. IPTV频道

命令	功能
zte(cfg-nas)#**create iptv channel** { **general**< *256-263*> | **special**< *0-255*> }	创建IPTV的频道
zte(cfg-nas)#**iptv channel** < *channellist*> **name** < *channelname*>	设置频道名
zte(cfg-nas)#**iptv channel** < *channellist*> **mvlan** < *vlanid*>	设置频道所属组播VLAN
zte(cfg-nas)#**clear iptv channel** < *channellist*>	删除频道

3. 配置CAC（频道访问控制）

命令	功能
zte(cfg-nas)#**create iptv cac-rule** < *rule id*>	创建CAC规则
zte(cfg-nas)#**iptv cac-rule** < *rulelist*> **name** < *rulename*>	设置规则名
zte(cfg-nas)#**iptv cac-rule** < *rulelist*> **prvcount** < *0-65535*>	设置规则的最大预览次数，缺省为全局最大预览次数

命令	功能
zte(cfg-nas)#**iptv cac-rule** < *rulelist*> **prvtime** < *1-65535*>	设置规则的最大预览时间，缺省为全局最大预览时间
zte(cfg-nas)#**iptv cac-rule** < *rulelist*> **prvinterval** < *2-65535*>	设置规则的最小预览间隔，缺省为全局最小预览间隔
zte(cfg-nas)#**iptv cac-rule** < *rulelist*> **right** { **order**| **preview**| **query**} < *channellist*>	设置规则对频道的权限
zte(cfg-nas)#**clear iptv cac-rule** < *rulelist*> [**channel** < *channellist*>]	删除规则

4. IPTV用户的管理命令

命令	功能
zte(cfg-nas)#**clear iptv client**	删除在线的IPTV用户

7.11.3 IPTV配置实例

1. 如果端口1下的用户是组播组224.1.1.1的定购用户，组播组所在的vlan为100，配置如下：

```
ZXR10(config-nas)# iptv control enable
ZXR10(config-nas)# create iptv channel special 1 address 224.1.1.1
ZXR10(config-nas)# iptv channel 1 mvlan 100
ZXR10(config-nas)# iptv channel 1 name cctv1
ZXR10(config-nas)# create iptv cac-rule 1 port 1
ZXR10(config-nas)# iptv cac-rule 1 right order 1
```

2. 如果端口1，vlan1下的用户是组播组224.1.1.1的预览用户，最大预览时间为2分钟，最小预览间隔为20秒，最大预览次数为10，组播组所在的vlan为100，配置如下：

```
ZXR10(config-nas)# iptv control enable
ZXR10(config-nas)# create iptv channel special 1 address 224.1.1.1
ZXR10(config-nas)# iptv channel 1 mvlan 100
ZXR10(config-nas)# iptv channel 1 name cctv1
ZXR10(config-nas)# create iptv cac-rule 1 port 1 vlan 1
ZXR10(config-nas)# iptv cac-rule 1 prvcount 10
ZXR10(config-nas)# iptv cac-rule 1 prvtime 120
ZXR10(config-nas)# iptv cac-rule 1 prvinterval 20
ZXR10(config-nas)# iptv cac-rule 1 right preview 1
```

3. 如果端口1下的用户可以看vlan100中所有组播组，配置如下：

```
ZXR10(config-nas)# iptv control enable
```

```
ZXR10(config-nas)# create iptv channel general 256
ZXR10(config-nas)# iptv channel 256 mvlan 100
ZXR10(config-nas)# create iptv cac-rule 1 port 1
ZXR10(config-nas)# iptv cac-rule 1 right order 256
```

4. 如果端口1只允许接受组播组224.1.1.1的查询报文，组播组所在的vlan为100，配置如下：

```
ZXR10(config-nas)# iptv control enable
ZXR10(config-nas)#  create iptv channel special 1 address 224.1.1.1
ZXR10(config-nas)# iptv channel 1 mvlan 100
ZXR10(config-nas)# create iptv cac-rule 1 port 1
ZXR10(config-nas)# iptv cac-rule 1 right query 1
```

7.11.4 IPTV的维护与诊断

当IPTV遇到问题时，我们可以通过相关的调试命令来帮助定位故障，排除错误，其中用到的命令主要是与其相关的**show**命令。

命令	功能
zte(cfg)#**show iptv control**	显示IPTV的全局配置信息
zte(cfg)#**show iptv channel**	显示IPTV频道信息
zte(cfg)#**show iptv channel** [**id** < *0-263*> | **name**< *channelname*>]	显示特定频道号的频道统计信息
zte(cfg)#**show iptv cac-rule**	显示CAC规则
zte(cfg)#**show iptv cac-rule** [**id** < *1-64*> | **name**< *rulename*>]	显示CAC规则统计
zte(cfg)#**show iptv client**	显示在线的IPTV用户

7.12 QoS配置

7.12.1 QoS概述

交换机提供一定的QoS功能，提供优先级控制功能，可以基于数据包的源MAC地址优先级、VLAN优先级、802.1P用户优先级、三层DSCP优先级或端口默认优先级来决定数据包的优先级。一个数据包优先级决定顺序为（前面的优先）：

1. CPU发送的数据包优先级（由CPU决定）
2. MGMT数据包（管理数据包，如BPDU包）优先级（初始化决定管理包的优先级）
3. 静态源MAC地址优先级
4. VALN优先级