

# ZXR10 6900 系列万兆路由交换机 用户手册以太网交换分册

产品版本: 2.8.02.B

中兴通讯股份有限公司 地址: 深圳市高新技术产业园科技南路中兴通讯大厦 邮编: 518057 电话: (86) 755 26770800 800-830-1118 传真: (86) 755 26770801 技术支持网站: http://support.zte.com.cn 电子邮件: 800@zte.com.cn

### 法律声明

本资料著作权属中兴通讯股份有限公司所有。未经著作权人书面许可,任何单位或个人不得以任何方式摘录、复制或翻译。

侵权必究。

"ZTE"和"ZTE中兴"是中兴通讯股份有限公司的注册商标。中兴通讯产品的名称和标志是中兴通 讯的专有标志或注册商标。在本手册中提及的其他产品或公司的名称可能是其各自所有者的商标或商 名。在未经中兴通讯或第三方商标或商名所有者事先书面同意的情况下,本手册不以任何方式授予阅 读者任何使用本手册上出现的任何标记的许可或权利。

本产品符合关于环境保护和人身安全方面的设计要求,产品的存放、使用和弃置应遵照产品手册、相关合同或相关国法律、法规的要求进行。

如果本产品进行改进或技术变更, 恕不另行专门通知。

当出现产品改进或者技术变更时,您可以通过中兴通讯技术支持网站http://support.zte.com.cn查询有关信息。

#### 修订历史

资料版本	修订日期	修订原因
R1.0	20081205	手册第1次发布

资料编号: sjzl20086161

发布日期: 20081205

1	VLAN配置1−1
	1.1 VLAN简介1-1
	1.1.1 VLAN类型1-1
	1.1.2 VLAN标签1-2
	1.1.3 VLAN链路类型1-2
	1.1.4 缺省VLAN1-3
	1.1.5 PVLAN
	1.1.6 QinQ1-3
	1.1.7 子网VLAN1-4
	1.1.8 协议VLAN1-4
	1.1.9 VLAN翻译1-4
	1.1.10 SuperVLAN1-5
	1.1.11 SVLAN
	1.2 配置VLAN
	1.2.1 创建VLAN1-5
	1.2.2 设置端口的VLAN链路类型1-6
	1.2.3 添加VLAN成员端口1-6
	1.2.4 设置端口的本地VLAN1-7
	1.2.5 设置端口的VLAN过滤1-8
	1.2.6 设置端口帧类型过滤1-8
	1.2.7 创建VLAN三层接口1-8
	1.2.8 VLAN配置实例1-8
	1.3 配置PVLAN1-9
	1.4 配置QinQ1-10
	1.5 配置子网VLAN
	1.6 配置协议VLAN
	1.7 配置VLAN翻译1-14
	1.8 配置SuperVLAN

	1.9 配置SVLAN1-17
	1.10 VLAN的维护与诊断1-21
2	STP配置2-1
	2.1 STP简介2-1
	2.1.1 SSTP模式2-1
	2.1.2 RSTP模式2-2
	2.1.3 MSTP模式2-2
	2.1.4 BPDU保护2-3
	2.2 配置STP2-7
	2.2.1 启用STP2-7
	2.2.2 配置STP模式2-8
	2.2.3 配置STP参数2-8
	2.2.4 创建实例
	2.2.5 设置MST名称和版本号2-9
	2.2.6 配置交换机的优先级2-9
	2.3 配置BPDU保护2-9
	2.3.1 配置边缘端口的BPDU保护2-9
	2.3.2 配置端口环回保护
	2.3.3 配置端口根保护2-10
	2.4 STP配置实例2-10
	2.5 STP的维护与诊断
3	MAC地址表操作3-1
	3.1 MAC地址表简介3-1
	3.1.1 MAC地址表的构成及意义3-1
	3.1.2 MAC地址的分类3-2
	3.1.3 MAC地址表的建立与删除3-2
	3.2 配置MAC地址表3-3
	3.2.1 设置MAC地址老化时间3-3
	3.2.2 设置MAC地址固化3-3
	3.2.3 设置端口绑定MAC地址3-4
	3.2.4 设置端口MAC地址学习3-4
	3.2.5限制端口或全局的MAC地址数目3-4

	3.2.6 设置端口MAC地址学习保护3-5
	3.2.7 设置MAC地址过滤
	3.2.8 配置MAC地址表的256K模式3-5
	3.2.9 查看MAC地址表3-6
	3.3 MAC地址表配置实例3-7
4	链路聚合配置4-1
	4.1 链路聚合简介4-1
	4.2 配置链路聚合
	4.3 链路聚合配置实例
	4.4 链路聚合的维护与诊断4-4
5	IGMP Snooping配置5-1
	5.1 IGMP Snooping简介5-1
	5.1.1 加入组播组5-2
	5.1.2 离开组播组5-2
	5.1.3 快速离开
	5.2 配置IGMP Snooping5-2
	5.2.1 启用IGMP Snooping5-2
	5.2.2 配置代理查询器5-3
	5.2.3 限制组播组5-4
	5.2.4 配置静态IGMP Snooping5
	5.2.5 设置IGMP Snooping时间参数5-4
	5.3 IGMP Snooping配置实例5-5
	5.4 IGMP Snooping的维护与诊断5-5
6	链路保护配置
	6.1 ZESR配置6-2
	6.1.1 ZESR简介6-1
	6.1.2 配置ZESR6-3
	6.1.3 ZESR配置实例6-4
	6.2 ZESS配置6-e
	6.2.1 ZESS简介6-e
	6.2.2 配置ZESS
	6.3 双上行链路保护6-7

	6.3.1 双上行链路保护简介6	7
	6.3.2 双上行链路保护配置实例6-8	8
7	以太网OAM配置7	1
	7.1 以太网OAM简介	1
	7.2 配置以太网OAM	3
	7.3 配置CFM	5
	7.4 OAM链路控制事件配置实例7	9
	7.5 以太网OAM的维护与诊断7-1	1
	7.6 CFM的维护与诊断	4
8	EPON OLT配置8-2	1
	8.1 EPON OLT简介8-	1
	8.2 配置EPON OLT	3
	8.2.1 配置OLT接口8	3
	8.2.2 配置EPON全局参数8	5
	8.2.3 配置ONU本地管理8-8-8-8-8-8-8-8-8-8-8-8-8-8-8-8-8	8
	8.2.4 配置OLT光路保护功能8	9
	8.2.5 配置QoS	1
	8.2.6 配置OLT告警功能	1
	8.2.7 配置ONU远程管理8-1	3
	8.3 EPON OLT配置实例	C
	8.4 EPON OLT的维护与诊断8-22	2
	图目录	I
	表目录	I
	缩略语	1

# 前言

# 手册说明

本手册为《ZXR10 6900系列(V2.8.02.B)万兆路由交换机用户手册以太网交换分册》, 适用于ZXR10 6902/6905/6908万兆路由交换机的V2.8.02.B版本。

ZXR10 6900系列万兆路由交换机的配套手册有:

手册名称	手册内容	
《ZXR10 6900系列(V2.8.02.B)万兆路由交换机硬 件安装手册》	介绍安装工程准备、19英寸机柜安装、主 设备安装、电源线安装、线缆安装和硬件 安装检查	
《ZXR10 6900系列(V2.8.02.B)万兆路由交换机硬 件手册》	介绍设备的功能、技术特性和参数、工作原 理、硬件结构、控制交换板、线路接口板、 电源模块和风扇插箱	
《ZXR10 6900系列(V2.8.02.B)万兆路由交换机用户 手册基本配置分册》	介绍设备的使用和操作、系统管理、CLI权限分级配置、端口配置、网络协议配置、 DHCP配置、VRRP配置、ACL配置、QoS 配置、DOT1X配置、集群管理配置、网络 管理配置、IPTV配置、VBAS配置、CPU攻 击保护、URPF配置和UDLD配置	
《ZXR10 6900系列(V2.8.02.B)万兆路由交换机用 户手册以太网交换分册》	介绍设备的VLAN配置、STP配置、MAC地 址表操作、链路聚合配置、IGMP Snooping 配置、链路保护配置、以太网OAM配置和 EPON OLT配置	
《ZXR10 6900系列(V2.8.02.B)万兆路由交换机用户 手册IPv4路由分册》	介绍设备的静态路由配置、RIP配置、OSPF 配置、IS-IS配置、BGP配置、负荷分担配 置、组播路由配置、IP/LDP FRR配置和 BFD配置	
《ZXR10 6900系列(V2.8.02.B)万兆路由交换机用 户手册MPLS分册》	介绍设备的MPLS配置、MPLS L3VPN配置 和MPLS L2VPN配置	

手册名称	手册内容	
《ZXR10 6900系列(V2.8.02.B)万兆路由交换机用户 手册IPv6分册》	介绍设备的IPv6地址配置、IPv6邻居发现协 议配置、IPv6隧道配置、IPv6静态路由配 置、RIPng配置、OSPFv3配置、IS-ISv6配 置和BGP4+配置	
《ZXR10路由器/以太网交换机命令手册(V4.8.22)	介绍ZXR10路由器/以太网交换机每条命	
命令索引分册》	令对应的分册、章节	
《ZXR10路由器/以太网交换机命令手册(V4.8.22)	介绍ZXR10路由器/以太网交换机与IPv6相	
IPv6分册》	关的命令	
《ZXR10路由器/以太网交换机命令手册(V4.8.22)	介绍ZXR10路由器/以太网交换机与RIP、	
IP路由分册一》	OSPF和IS-IS路由协议相关的命令	
《ZXR10路由器/以太网交换机命令手册(V4.8.22)	介绍ZXR10路由器/以太网交换机与BGP路	
IP路由分册二》	由协议、路由映射和路由策略相关的命令	
《ZXR10路由器/以太网交换机命令手册(V4.8.22)	介绍ZXR10路由器/以太网交换机与MPLS	
MPLS分册》	相关的命令	
《ZXR10路由器/以太网交换机命令手册(V4.8.22)	介绍ZXR10路由器/以太网交换机与QoS相	
QoS分册》	关的命令	
《ZXR10路由器/以太网交换机命令手册(V4.8.22)	介绍ZXR10路由器/以太网交换机与网络	
安全分册》	安全相关的命令	
《ZXR10路由器/以太网交换机命令手册(V4.8.22) 基本配置分册一》	介绍ZXR10路由器/以太网交换机与系统 管理、文件管理、用户界面、日志统计、 FTP/TFTP服务器和IPv4基础协议相关的命 令	
《ZXR10路由器/以太网交换机命令手册(V4.8.22) 基本配置分册二》	介绍ZXR10路由器/以太网交换机与接口配置、DHCP和VRRP相关的命令	
《ZXR10路由器/以太网交换机命令手册(V4.8.22) 基本配置分册三》	介绍ZXR10路由器/以太网交换机与NAT、 Time Range、堆叠和DEBUG调试相关的命 令	
《ZXR10路由器/以太网交换机命令手册(V4.8.22)	介绍ZXR10路由器/以太网交换机与网络	
网络管理分册》	管理相关的命令	
《ZXR10路由器/以太网交换机命令手册(V4.8.22) 以太网交换分册》	介绍ZXR10路由器/以太网交换机与MAC、 VLAN、SuperVLAN、STP、链路聚合、 VBAS、MAC PING和UDLD相关的命令	

手册名称	手册内容
《ZXR10路由器/以太网交换机命令手册(V4.8.22)	介绍ZXR10路由器/以太网交换机与VOIP和
语音视频分册》	IPTV相关的命令
《ZXR10路由器/以太网交换机命令手册(V4.8.22)	介绍ZXR10路由器/以太网交换机与远程
远程接入分册》	接入相关的命令
《ZXR10路由器/以太网交换机命令手册(V4.8.22)	介绍ZXR10路由器/以太网交换机与组播
组播分册》	协议相关的命令

ZXR10 6900系列(V2.8.02.B)万兆路由交换机支持的命令是基于统一平台ZXROS V4.8.22版本。

# 内容介绍

ZXR10 6900系列(V2.8.02.B)万兆路由交换机用户手册以太网交换分册的章节及其概要 如下所示:

章名	概要
第1章 VLAN配置	介绍VLAN、PVLAN、QinQ、子网VLAN、协议VLAN、VLAN
	翻译、SuperVLAN、SVLAN的原理、配置和配置实例
第2章 STP配置	介绍STP、BPDU保护的原理、配置和配置实例
第3章 MAC地址表操作	介绍MAC地址表的基本概念和相关操作
第4章 链路聚合配置	介绍链路聚合的原理、配置和配置实例
第5章 IGMP Snooping配置	介绍IGMP Snooping的原理、配置和配置实例
第6章 链路保护配置	介绍ZESR和ZESS的原理、配置和配置实例
第7章 以太网OAM配置	介绍以太网OAM的原理、配置和配置实例
第8章 EPON OLT配置	介绍EPON OLT的原理、配置和配置实例
缩略语	列举了本手册中常见的缩略语

# ┛ VLAN配置

本章包含如下主题:

- VLAN简介 1-1
   配置VLAN 1-5
- 配置PVLAN 1-9
- 配置QinQ 1-10
- 配置子网VLAN 1-11
- 配置协议VLAN 1-13
- 配置VLAN翻译 1-14
- 配置SuperVLAN 1-14
- 配置SVLAN 1-17
- VLAN的维护与诊断 1-21

# 1.1 VLAN简介

使用VLAN技术,网络管理者能够根据实际应用需要,将物理局域网逻辑划分成不同的广播域(每个广播域即一个VLAN),使具有相同需求的用户处于同一广播域,不同需求的用户处于不同的广播域。同一个VLAN中的所有广播和单播流量都被限制在该VLAN中,不会转发到其它VLAN。当不同VLAN的设备要进行通信时,必须经过三层的路由转发。

VLAN的优点主要有:

- 减少网络上的广播流量
- 增强网络的安全性
- 简化网络的管理控制

# 1.1.1 VLAN类型

交换机目前支持基于端口的VLAN、子网VLAN和协议VLAN。基于端口的VLAN是划分 VLAN的最简单也是最有效的方法,它将交换设备的各个端口分配给不同的VLAN。 例如,端口1、2和3属于同一个VLAN,其他端口属于别的VLAN,那么端口1所接收的帧 就只在端口2和3上传送而不会在其他端口上传送。如果VLAN中的用户移动到一个新位 置,就不再属于原来的VLAN,除非重新配置VLAN。

# 1.1.2 VLAN标签

帧在网络中传输时,如果能用某种方法表示出该帧所属的VLAN,就可以在一条链路上 传输多个VLAN的业务。IEEE 802.1Q通过在以太网帧结构中插入一个VLAN标签实现了 这一功能。

VLAN标签的长度为4个字节,在以太网帧中位于源MAC地址之后,长度/类型字段之前。 VLAN标签的格式如图1-1所示。

图1-1 VLAN标签格式



VLAN标签最常应用在跨交换机创建VLAN的情况,此时交换机之间的连接通常称为中继 (Trunk)。使用标签后,可以通过一个或多个中继创建跨多个交换机的VLAN。当连接 这些交换机的端口收到一个打标签(tagged)的帧时,端口能够根据VLAN标签判断该帧 属于哪一个VLAN。

每个802.1Q的端口都被分配了一个缺省的VLAN ID,称为PVID。当端口收到不打标签 (untagged)的帧时,该帧被认为属于端口缺省VLAN,并在该VLAN中进行转发。

# 1.1.3 VLAN链路类型

ZXR10 6900系列交换机的端口支持以下三种连接方式:

• 接入链路(Access Link)

接入链路用于将不能识别VLAN标签的设备(如工作站)连接到VLAN交换机端口。 它只传送不打VLAN标签的帧,且只与一个VLAN关联。

• 中继链路(Trunk Link)

中继链路用于连接两个能够识别VLAN标签的设备,传输多个VLAN的业务。它只传送打VLAN标签的帧,可承载多个VLAN。最常见的中继链路就是连接两个交换机的链路。

• 混合链路(Hybrid Link)

混合链路可以同时传送打标签的和不打标签的帧。但是对于一个特定的VLAN,混 合链路传送的所有帧必须是同一种类型的。

# 1.1.4 缺省VLAN

ZXR10 6900系列交换机初始情况下有一个缺省VLAN,该VLAN有以下特性:

- 缺省VLAN的VLAN ID为1。
- 缺省VLAN的名称为VLAN0001。
- 缺省VLAN包含所有端口。
- 缺省VLAN的所有端口默认都是untagged的。

### 1.1.5 PVLAN

为了提高网络的安全性,要将用户之间的报文隔离开,传统的解决办法是给每个用户分配一个VLAN。这种方法具有明显的局限性,主要表现在以下几个方面:

- 目前IEEE 802.1Q标准中所支持的VLAN数目最多为4094个,用户数量受到限制,且 不利于网络的扩展。
- 每个VLAN对应一个IP子网,划分大量的子网会造成IP地址的浪费。
- 大量VLAN和IP子网的规划使网络管理变得非常复杂。

PVLAN技术的出现解决了这些问题。

PVLAN将VLAN中的端口分为两类:与用户相连的端口为隔离端口(Isolate Port),上行 与路由器相连的端口为混合端口(Promiscuous Port)。隔离端口只能与混合端口通信,相互之间不能通信。这样就将同一个VLAN下的端口隔离开来,用户只能与自己的默认 网关通信,网络的安全性得到保障。

# 1.1.6 QinQ

QinQ是对基于IEEE 802.1Q封装的隧道协议的形象称呼,又称VLAN堆叠。QinQ技术是 在原有VLAN标签(内层标签)之外再增加一个VLAN标签(外层标签),外层标签可以 将内层标签屏蔽起来。

QinQ不需要协议的支持,通过它可以实现简单的L2VPN(二层虚拟专用网),特别适合 以三层交换机为骨干的小型局域网。

QinQ技术的典型组网如图1-2所示,连接用户网络的端口称为Customer端口,连接服务提供商网络的端口称为Uplink端口,服务提供商网络边缘接入设备称为PE(Provider Edge)。



#### 图1-2 QinQ典型组网

用户网络一般通过VLAN Trunk方式接入PE。

当报文从用户网络1到达交换机A的customer端口时,无论报文是tagged还是untagged的,交换机A都强行插入外层标签(VLAN ID为10)。在服务提供商网络内部,报文沿着VLAN 10的端口传播,直至到达交换机B。交换机B发现与用户网络2相连的端口为customer端口,于是按照传统的802.1Q协议剥离外层标签,恢复成用户的原始报文,发送到用户网络2。

这样,用户网络1和2之间的数据可以通过服务提供商网络进行透明传输,用户网络可以自由规划自己的私网VLAN ID,而不会和服务提供商网络中的VLAN ID冲突。

# 1.1.7 子网VLAN

基于子网的VLAN应用于二层VLAN网络环境,实现数据帧转发的灵活配置。基于子网的 VLAN是根据数据帧的源IP地址来决定转发到相应的VLAN中。这种按源IP地址来组成的 VLAN,可使不同网段用户跨越多个VLAN转发,但其VLAN成员身份仍然保留不变。

子网VLAN将不同源IP地址的数据帧隔开,用户只能得到属于同一网段的数据。UNTAG 帧转发子网VLAN的优先级高于协议VLAN,也高于PVID,TAG帧按照TAG模式转发,其优先级高于子网VLAN。

### 1.1.8 协议VLAN

基于协议的VLAN比较灵活,适合三层或者协议丰富的网络环境。基于协议的VLAN是根据数据包的网络层封装协议来划分的,可使广播域跨越多个VLAN交换机,用户可以在网络内部自由移动,但其VLAN成员身份仍然保留不变。这种方法的优点是用户的物理位置改变后不需要重新配置所属的VLAN。

### 1.1.9 VLAN翻译

VLAN翻译又叫VLAN映射,它允许用于边缘接入的不同以太网交换机的VLAN ID设置互相重叠。通过以太网交换机的VLAN翻译功能,将不同交换机的重复VLAN ID修改为不同的VLAN ID,并从上连端口发送出去。

### 1.1.10 SuperVLAN

传统的ISP网络给每个用户分配一个IP子网。每分配一个子网,就有三个IP地址被占用, 分别作为子网的网络号、广播地址和缺省网关。如果一些用户的子网中有大量未分配的 IP地址,也无法给其他用户使用,因此这种方法会造成IP地址的浪费。

SuperVLAN有效的解决了这个问题,它把多个VLAN(称为子VLAN)聚合成一个Super-VLAN,这些子VLAN使用同一个IP子网和缺省网关。

利用SuperVLAN技术, ISP只需为SuperVLAN分配一个IP子网,并为每个用户建立一个子VLAN,所有子VLAN可以灵活分配SuperVLAN中的IP地址,使用SuperVLAN的缺省网关。每个子VLAN都是一个独立的广播域,保证不同用户之间的隔离,子VLAN之间的通信通过SuperVLAN进行路由。

### 1.1.11 SVLAN

SVLAN是一种VLAN隧道技术,通过在原有802.1Q标签的之外再增加一个VLAN标签,将 内层VLAN标签屏蔽起来,在经过运营商网络到达边缘交换机时,再去除外层的VLAN标 签,从而构成多点到多点的透明传输服务,为用户提供一种较为简单的二层VPN隧道。 由于报文中可以携带双层标签,这有效的扩展了VLAN的数目,使VLAN的数目最多可达 4094\*4094个。通常外层VLAN标签称为运营商VLAN(SPVLAN),内层VLAN标签称为 客户VLAN(CVLAN)。

普通的QinQ仅仅是将到某个端口的数据包打上一个外层标签,这大大限制了组网灵活性;而SVLAN对同一个端口收到的流可以选择性地对不同的内层标签打上不同的外层标签。

有些业务流需要保证其报文在通过交换机时不受干扰,即其标签的数目和数值仍然保持 原有状态。SVLAN同样支持这种透传VLAN业务。SVLAN也可以实现外层标签和内层标 签的802.1P cos优先级映射。

# 1.2 配置VLAN

### 1.2.1 创建VLAN

1. 创建指定VLAN,并进入VLAN配置模式

命令	功能
ZXR10(config)# <b>vlan</b> < <i>vlan-id</i> >	交换机上缺省只有VLAN1,使用该命 令可以创建其他VLAN
ZXR10(config-vlan)# <b>name</b> < <i>vlan-name</i> >	设置VLAN的别名

1-5

在有些命令中可以使用别名代替VLAN号,VLAN别名用于区分各个VLAN,可以是小组名称、部门、地区等。缺省情况下,VLAN的别名为"VLAN"+VLAN ID,其中VLAN ID部分为4位数字,不足4位用0补足,如ID为4的VLAN别名缺省为VLAN0004。

2. 批量创建VLAN

命令	功能
ZXR10#vlan database	进入VLAN数据库
ZXR10(vlan)# <b>vlan</b> < <i>vlan-list</i> >	可以在数据库中批量创建VLAN
ZXR10(config-vlan)# <b>name</b> < <i>vlan-name</i> >	设置VLAN的别名

在有些命令中可以使用别名代替VLAN号,VLAN别名用于区分各个VLAN,可以是小组名称、部门、地区等。缺省情况下,VLAN的别名为"VLAN"+VLAN ID,其中 VLAN ID部分为4位数字,不足4位用0补足,如ID为4的VLAN别名缺省为VLAN0004。

# 1.2.2 设置端口的VLAN链路类型

步骤	命令	功能	
1	<pre>ZXR10(config) #interface &lt; interface-name&gt;</pre>	进入交换机上的二层接口	
2	<pre>ZXR10(config-if) #switchport mode { access  trunk  hybrid}</pre>	设置以太网端口的VLAN链路类型	

以太网端口的VLAN链路类型有三种: Access模式、Trunk模式和Hybrid模式,默认为Access 模式。

- Access模式的端口只能属于一个VLAN,端口不能打标签(untagged),一般是连接 主机的端口。
- Trunk模式的端口可以属于多个VLAN,端口必须打标签(tagged),可以接收和发送多个VLAN的报文,一般作为交换机之间连接的Trunk端口。
- Hybrid模式的端口可以属于多个VLAN,是否打标签由用户自由指定,可以接收和发送多个VLAN报文,可以用于交换机之间的连接,也可以连接用户计算机。

Hybrid端口和Trunk端口的不同之处在于: Hybrid端口可以发送带标签或不带标签的帧, 而Trunk端口一般只在发送缺省VLAN的报文时不打标签。

# 1.2.3 添加VLAN成员端口

Access端口只能加入到一个VLAN中,而Trunk端口和Hybrid端口可以加入到多个VLAN中。

● 将Access端口加入到指定VLAN

步骤	命令	功能	
1	ZXR10(config)#interface < interface-name>	进入交换机上的二层接口	
2	<pre>ZXR10(config-if)#switchport access vlan { &lt; vlan-id&gt;   &lt;</pre>	设置端口所属VLAN	
	<pre>vlan-name&gt; }</pre>		

### 将Trunk端口加入到指定VLAN

步骤	命令	功能
1	<pre>ZXR10(config) #interface &lt; interface-name&gt;</pre>	进入交换机上的二层接口
2	ZXR10(config-if) <b>#switchport trunk vlan</b> < <i>vlan-list</i> >	设置端口所属VLAN

### 将Hybrid端口加入到指定VLAN

步骤	命令	功能	
1	ZXR10(config) # <b>interface</b> < <i>interface-name</i> >	进入交换机上的二层接口	
2	ZXR10(config-if) #switchport hybrid vlan < vlan-list> [ tag   untag]	设置端口所属VLAN,并设置这些	
		VLAN的数据是否打标签	

### • 批量添加VLAN成员端口

命令	功能	
<pre>ZXR10(config-vlan) #switchport { pvid  tag  untag} &lt; port-list&gt;</pre>	在VLAN配置模式下,批量添加VLAN	
	成员端口	

# 1.2.4 设置端口的本地VLAN

Access端口只属于1个VLAN,所以它的本地VLAN就是它所在的VLAN,不用设置。

Trunk端口和Hybrid端口属于多个VLAN,需要设置本地VLAN。如果设置了端口的本地 VLAN,当端口接收到不带VLAN标签的帧时,则将该帧转发到属于本地VLAN的端口。 默认情况下Trunk端口和Hybrid端口的本地VLAN为VLAN 1。

步骤	命令	功能	
1	ZXR10(config)# <b>interface</b> < <i>interface-name</i> >	进入交换机上的二层接口	
2	ZXR10(config-if)#switchport { trunk   hybrid} native vlan { <	设置Trunk端口和Hybrid端口的native	
	vlan-id>   < vlan-name> }	VLAN	

# 1.2.5 设置端口的VLAN过滤

步骤	命令	功能		
1	<pre>ZXR10(config) #interface &lt; interface-name&gt;</pre>	进入交换机的二层接口		
2	<pre>ZXR10(config-if) # ingress filtering { enable   disable}</pre>	设置端口的VLAN过滤,默认情况下		
		VLAN入口过滤是打开的		

启用入口过滤后,如果端口接收到的帧所属VLAN的成员端口中并不包含该入口端口,则该帧将被丢弃。

# 1.2.6 设置端口帧类型过滤

步骤	命令	功能
1	<pre>ZXR10(config)# interface &lt; interface-name&gt;</pre>	进入交换机上的二层接口
2	<pre>ZXR10(config-if) #acceptable frame types { all   tag}</pre>	设置端口帧类型过滤

配置端口可接收的帧类型,可以选择接收所有的帧(包括untagged帧和tagged帧)或者只接收tagged帧。默认情况下接收所有的帧。

# 1.2.7 创建VLAN三层接口

步骤	命令	功能	
1	ZXR10(config)# <b>vlan</b> < <i>vlan-id</i> >	创建VLAN	
2	ZXR10(config-vlan)# <b>exit</b>	退出VLAN配置模式	
3	ZXR10 (config) # <b>interface vlan</b> < <i>vlan-id</i> >	创建VLAN三层接口	

可以使用shutdown命令关闭VLAN三层接口,使用no shutdown命令打开VLAN三层接口。

当VLAN中的所有以太网端口状态均为down时,该VLAN接口状态为down;当VLAN中有一个或多个以太网端口处于up状态时,该VLAN接口状态变为up。

# 1.2.8 VLAN配置实例

如图1-3所示,交换机A的端口gei\_3/1、gei\_3/2和交换机B的端口gei\_7/1、gei\_7/2属于 VLAN 10;交换机A的端口gei\_3/4、gei\_3/5和交换机B的端口gei\_7/4、gei\_7/5属于VLAN 20,均为Access端口。两台交换机通过端口gei\_3/24和gei\_7/24以Trunk方式连接,这两个 端口为Trunk端口。

#### 图1-3 VLAN典型组网



#### 交换机A的配置:

ZXR10\_A(config) #vlan 10 ZXR10\_A(config-vlan) #switchport pvid gei\_3/1-2 ZXR10\_A(config) #vlan 20 ZXR10\_A(config-vlan) #switchport pvid gei\_3/4-5 ZXR10\_A(config) #interface gei\_3/24 ZXR10\_A(config-if) #switchport mode trunk ZXR10\_A(config-if) #switchport trunk vlan 10 ZXR10\_A(config-if) #switchport trunk vlan 20

#### 交换机B的配置:

ZXR10_B(config)#vlan 10
ZXR10_B(config-vlan)#switchport pvid gei_7/1-2
ZXR10_B(config)#vlan 20
ZXR10_B(config-vlan)#switchport pvid gei_7/4-5
ZXR10_B(config)#interface gei_7/24
ZXR10_B(config-if)#switchport mode trunk
ZXR10_B(config-if)#switchport trunk vlan 10
ZXR10_B(config-if)#switchport trunk vlan 20

# 1.3 配置PVLAN

步骤	命令	功能	
1	ZXR10(config)#vlan private-map session-id < id> [ community <	配置PVLAN的隔离端口和混合端	
	<pre>port-list&gt; ] [ isolate &lt; port-list&gt; ] [ promis &lt; port-list&gt; ] [ vlan &lt; vlan-list&gt;</pre>	口。isolate表示隔离端口,promis表	
	]	示混合端口	
2	ZXR10(config) <b>#show vlan private-map</b> [ < <i>session-id</i> > ]	显示PVLAN的配置结果	

### 举例

需要配置了两个隔离组:

隔离组1: 端口gei\_3/1, gei\_3/2, fei\_7/4, fei\_7/5为隔离端口,端口gei\_5/10为混合端口。

隔离组2: 端口gei\_3/7, gei\_3/8, fei\_7/10, fei\_7/11为隔离端口, gei\_5/12为混合端口。

配置如下所示:

ZXR10(config)#vla	in private-map	session-id 1	l isola	te		
gei_3/1-2,fei_7/4	gei_3/1-2,fei_7/4-5 promis gei_5/10					
ZXR10(config)#vla	in private-map	session-id 2	2 isola	te		
gei_3/7-8,fei_7/1	.0-11 promis ge	ei_5/12				
ZXR10(config)#shc	w vlan private	e-map				
Session_id	Isolate_Por	rts		Promis_Ports		
1	gei_3/1-2,fei_	7/4-5,		gei_5/10		
2	gei_3/7-8,			gei_5/12		

# 1.4 配置QinQ

步骤	命令	功能
1	ZXR10(config)#interface < interface-name>	进入二层接口
2	ZXR10 (config-if) #switchport qinq { normal  uplink  customer	配置QinQ的端口属性, normal表示
	<b>tpid</b> < <i>tpid</i> > }	不进行QinQ操作,默认情况下端口
		处于normal状态; uplink表示上连运
		营商的端口; customer表示下连用户
		的端口
3	ZXR10(config-if)# <b>show qinq</b>	查看QinQ的配置结果

### 举例

如图1-4所示,假设交换机A的customer端口为gei\_3/1,uplink端口为gei\_3/24;交换机B的customer端口为gei\_7/1,uplink端口为gei\_7/24。配置QinQ时,SPVLAN的customer端口需设置为untagged,uplink端口需设置为tagged。

#### 图1-4 QinQ典型组网 **SPVLAN 10 Customer Port SPVLAN 10** SPVLAN 10 **Uplink Port Customer Port** 用户网络1 SwitchA **SPVLAN 10 CVLAN 1-100** PE **Uplink Port** SwitchB 用户网络2 PE **CVLAN 1-100** 运营商网络

#### 交换机A的配置:

ZXR10\_A(config) #vlan 10 ZXR10\_A(config) #interface gei\_3/1 ZXR10\_A(config-if) #switchport qinq customer ZXR10\_A(config-if) #switchport access vlan 10 ZXR10\_A(config) #interface gei\_3/24 ZXR10\_A(config-if) #switchport qinq uplink ZXR10\_A(config-if) #switchport mode trunk ZXR10\_A(config-if) #switchport trunk vlan 10

#### 交换机B的配置:

ZXR10\_B(config)#vlan 10 ZXR10\_B(config)#interface gei\_7/1 ZXR10\_B(config-if)#switchport qinq customer ZXR10\_B(config-if)#switchport access vlan 10 ZXR10\_B(config)#interface gei\_7/24 ZXR10\_B(config-if)#switchport qinq uplink ZXR10\_B(config-if)#switchport mode trunk ZXR10\_B(config-if)#switchport mode trunk

# 1.5 配置子网VLAN

步骤	命令	功能
1	ZXR10 (config) #vlan subnet-map session-no< session-no> < ipaddr>	配置子网VLAN,设备支持128个子
	< mask> vlan { < vlanid> < name> }	网VLAN
2	ZXR10 (config) # <b>show vlan subnet-map</b>	显示子网VLAN的配置结果

#### ZTE中兴

#### 举例

如图1-5所示,在交换机上配置子网VLAN数据,配置VLAN20和VLAN30,接口fei\_1/1 属于VLAN20,接口fei\_1/2属于VLAN30,接口fei\_1/10属于VLAN20和VLAN30,fei\_1/1、 fei\_1/2和fei\_1/10的Pvid不一样。源IP地址为20.20.20.0/24网段PC可访问服务器1,IP地址 为30.30.30.1的 PC可访问服务器2。

#### 图1-5 子网VLAN配置实例



交换机配置:

```
/*创建VLAN并将接口划分到VLAN中*/
ZXR10(config)#interface fei_1/1
ZXR10(config-int)#switch mode hybrid
ZXR10(config-int)#switchport hybrid native vlan 20
ZXR10(config-int)#switch hybrid vlan 20 untag
ZXR10(config-int)#exit
ZXR10(config)#interface fei_1/2
ZXR10(config-int)#switch mode hybrid
ZXR10(config-int)#switch port hybrid native vlan 30
ZXR10(config-int)#switch hybrid vlan 30 untag
ZXR10(config-int)#exit
ZXR10(config-int)#exit
ZXR10(config-int)#switch hybrid vlan 30 untag
ZXR10(config-int)#exit
```

```
ZXR10(config-int)#switch mode hybrid
ZXR10(config-int)#switch hybrid vlan 20,30 untag
ZXR10(config-int)#exit
/*创建子网vLAN数据*/
ZXR10(config)# vlan subnet-map session-no 1
20.20.20.0 255.255.255.0 vlan 20
ZXR10(config)# vlan subnet-map session-no 2
30.30.30.1 255.255.255.255 vlan 30
```

# 1.6 配置协议VLAN

命令	功能
ZXR10(config) #vlan protocol-map session-no < session-no> { ethernet2	配置协议VLAN
llc   snap} < 0xHHHH> vlan { < vlanId>   < name> }	
ZXR10#show vlan protocol-map	显示协议VLAN的配置结果

### 举例

交换机端口fei\_1/1收到两种协议的数据包,分别为0X800,0X7000,配置这两个数据包属于不同的VLAN。

```
交换机的配置:
```

```
ZXR10(config)#vlan protocol-map session-no 1
ethernet2 0x800 vlan 10
ZXR10(config)#vlan protocol-map session-no 2 ethernet2
0x7000 vlan 20
ZXR10(config)#int fei_1/1
ZXR10(config-if) #switchport mode trunk
ZXR10(config-if)#switchport trunk vlan 10,20
ZXR10(config)#exit
ZXR10(config)#int fei 1/2
ZXR10(config-if)#switchport mode trunk
ZXR10(config-if)#switchport trunk vlan 10
ZXR10(config)#exit
ZXR10(config)#int fei_1/3
ZXR10(config-if) #switchport mode trunk
ZXR10(config-if)#switchport trunk vlan 20
ZXR10(config)#exit
```

# 1.7 配置VLAN翻译

步骤	命令	功能
1	ZXR10 (config) <b>#vlan translate session-no</b> < <i>session_id</i> > { <b>ingress-port</b>	配置VLAN翻译
	egress-port} < interface-name> ingress-vlan < vlan-list> egress-vlan	
	< vlanId> [ uplink-port < interface-name> ]	
2	ZXR10#show vlan translate [ session-no < session_id> ]	显示VLAN翻译的配置结果

#### 举例

交换机端口gei\_1/1上来的数据包的VLAN标签是VLAN 100,但为了将数据包转发到本交换机的端口fei\_2/1,需要将该数据包的VLAN标签变为VLAN200,此时需要配置VLAN翻译。

交换机的配置:

```
ZXR10(config)#vlan translate session-no 1 ingress-port gei_1/1
ingress-vlan 100 egress-vlan 200
ZXR10(config)#int gei_1/1
ZXR10(config-if)#ingress filtering disable
ZXR10(config-if)#switchport access vlan 100
ZXR10(config)#exit
ZXR10(config)#int fei_2/1
ZXR10(config-if)#switchport access vlan 200
ZXR10(config-if)#switchport access vlan 200
```

# 1.8 配置SuperVLAN

步骤	命令	功能
1	ZXR10 (config) <b>#interface supervlan</b> < <i>supervlan-id</i> >	创建SuperVLAN, supervlan-id的范
		围是1-255
2	ZXR10(config)# <b>vlan</b> < <i>vlan-id</i> >	进入VLAN配置模式
3	ZXR10(config-vlan)# <b>supervlan</b> < <i>supervlan-id</i> >	添加子VLAN
4	ZXR10 (config) <b>#interface supervlan</b> < <i>supervlan-id</i> >	进入Supervlan接口配置模式,
		supervlan-id的范围是1-255

步骤	命令	功能
5	<pre>ZXR10(config-if)#inter-subvlan-routing { enable   disable}</pre>	启用/关闭子VLAN之间的路由功 能,缺省情况下该功能被启用
6	<pre>ZXR10(config-if)#arp-broadcast { enable  disable}</pre>	启用/关闭ARP广播功能,缺省情况 下该功能被关闭
7	ZXR10(config)# <b>vlan</b> < <i>vlan-id</i> >	进入VLAN配置模式
8	<pre>ZXR10(config-vlan) #ip supervlan pool &lt; ip address begin&gt; &lt; ip address end&gt;</pre>	创建SuperVLAN的IP地址池
9	ZXR10(config) #interface supervlan < supervlan-id>	进入SuperVLAN接口配置模式
10	<pre>ZXR10(config-if)#ip-pool-filter { enable   disable}</pre>	启用/关闭IP地址过滤功能,缺省情况下该功能被启用
11	<pre>ZXR10(config)#show supervlan [ { supervlan-id } ]</pre>	查看SuperVLAN的配置结果

### ARP广播功能说明如下:

缺省情况下ARP广播功能是关闭的,当子VLAN间路由功能开启时,SuperVLAN接口执行ARP代理功能,如果启用ARP广播功能,在本地ARP表中查不到ARP请求的目的地址时,会向子VLAN广播ARP请求,如果收到应答,则更新本地ARP表。如果关闭ARP广播功能则不向子VLAN发送ARP请求。

IP地址过滤功能说明如下:

当子VLAN间路由功能开启时,SueprVLAN接口执行ARP代理功能,如果此时IP地址过滤功能被启用,则对SueprVLAN收到的ARP请求进行过滤,如果源IP地址不在其所属VLAN的IP-POOL范围中,这样的ARP请求非法,直接抛弃。

如果源IP地址合法,在本地ARP表中查不到ARP请求的目的地址时,会向子VLAN广播 ARP请求,收到应答后更新本地ARP表。如果IP地址过滤功能被启用,则查看ARP请求 的目的地址属于哪个VLAN的IP-POOL,并向该VLAN发送ARP请求。

注意,如果IP地址过滤功能被启用,IP-POOL不可为空。如果IP地址过滤功能被关闭,则不会对源IP地址进行检查,也就不需要配置IP-POOL。

### 举例

如图1-6所示,在交换机A上配置SuperVLAN,分配子网10.1.1.0/24,网关为10.1.1.1。交换机B上配置两个子VLAN,VLAN 2和VLAN 3,属于SuperVLAN。交换机A和交换机B通过Trunk端口相连。



#### 交换机A的配置:

```
/*创建SuperVLAN并分配子网、指定网关*/
ZXR10_A(config)#interface supervlan 10
ZXR10_A(config-int)#ip address 10.1.1.1 255.255.255.0
/*把SubVLAN加入到SuperVLAN*/
ZXR10_A(config)#vlan 2
ZXR10_A(config-vlan)#supervlan 10
ZXR10_A(config)#vlan 3
ZXR10_A(config-vlan)#supervlan 10
/*设置vlan trunk端口*/
ZXR10_A(config)#interface gei_7/10
ZXR10_A(config-int)#switch mode trunk
ZXR10_A(config-int)#switch trunk vlan 2-3
```

#### 交换机B的配置:

```
ZXR10_B(config)#interface gei_3/1
ZXR10_B(config-int)#switch access vlan 2
ZXR10_B(config)#interface gei_3/10
ZXR10_B(config-int)#switch access vlan 2
ZXR10_B(config)#interface gei_5/1
ZXR10_B(config-int)#switch access vlan 3
ZXR10_B(config)#interface gei_5/10
```

```
ZXR10_B(config-int)#switch access vlan 3
ZXR10_B(config)#interface gei_8/10
ZXR10_B(config-int)#switch mode trunk
ZXR10_B(config-int)#switch trunk vlan 2-3
```

# 1.9 配置SVLAN

有两种方法可以配置SVLAN,分别是传统的SVLAN配置方法和基于VFP的SVLAN配置方法。

# 传统的SVLAN配置方法

步骤	命令	功能
1	ZXR10(config)#vlan qinq session-no < session-id> customer-port	配置SVLAN
	< port-id> uplink-port < port-id> { { in-vlan < vlan-id> { {	
	ovlan < vlan-id> }   { untag helper-vlan < vlan-id> } } }	
	<b>default-vlan-forwarding</b>   { <b>untag ovlan</b> < <i>vlan-id</i> > [ <b>undirect</b> ] } }	
2	<pre>ZXR10(config) #no vlan qinq { session-no &lt; session-id&gt;   all }</pre>	删除SVLAN

参数说明:

参数	描述
session-no < session-id>	会话标识,范围1~1000
<pre>customer-port&lt; port-id&gt;</pre>	客户端口
uplink-port< port-id>	上连端口
in-vlan< vlan-id>	内层标签
untag	透传,不打外层标签
ovlan< vlan-id>	外层标签

示例:

ZXR10(config)#vlan qinq session 1 customer-port fei\_1/1
uplink-port gei\_2/2 in-vlan 1-10 ovlan 20
ZXR10(config)#vlan qinq session 2 customer-port fei\_1/1
uplink-port gei\_2/2 in-vlan 30 untag helper-vlan 4094

### 基于VFP的SVLAN配置方法

步骤	命令	功能
1	<pre>ZXR10 (config) #vfp session &lt; session-no&gt; invlan { &lt; vlan range&gt;   any} in &lt; acl-number&gt; rule &lt; rule-id&gt; { { ovlan &lt; vlan id&gt; }   { untag {</pre>	配置基于VFP的SVLAN
	global   pinpoint} } }	
2	ZXR10(config) # <b>interface</b> < <i>interface-name</i> >	进入接口配置模式
3	ZXR10(config-if) # <b>ip access-group</b> < <i>acl-number</i> > <b>vfp</b>	应用基于VFP的SVLAN

VFP的全称是Vlan Filter Processor,它是交换机中的一个功能模块,可以实现基于流分类的SVLAN功能。

这种配置方法通过使用VFP模块,在配置中增加了访问控制列表,可以依据流量类别添加外层标签,优于第一种方法。

示例:

ZXR10(config)#vfp session 1 invlan 1-10 in 100 rule 1 ovlan 20 ZXR10(config)#vfp session 2 invlan 30 in 100 rule 2 untag pinpoint ZXR10(config)#interface fei\_1/1 ZXR10(config-if)#ip access-group 100 vfp

### 显示SVLAN的配置结果

命令	功能
<pre>ZXR10(config) #show vlan qinq [ session &lt; session-id&gt; ]</pre>	显示SVLAN的配置结果

示例:

```
ZXR10#show vlan qinq
Session Customer Uplink In_Vlan Out_Vlan Priority redirect
1 fei_1/1 fei_1/2 1-10 20 mapping
2 fei_1/1 gei_1/2 30 0
```

显示内容说明:

参数	描述
Session	会话标识

参数	描述
Customer	客户端口
Uplink	上连端口
In_Vlan	内层标签,如果为0,则表示入数据包是untag的
Out_Vlan	外层标签,如果为0,表示透传,不打外层标签
Priority	外层标签的优先级,mapping表示外层标签的QoS映射

### 举例

如图1-7所示,同一个custom端口,支持多个不同的外层标签和透传流,配置要求为:

- 从custom端口fei\_1/1收到的tag为10的报文,将在S1上打上双层tag,从uplink端口fei\_1/2 转发,外层tag为997,内层tag为10。
- 从custom端口fei\_1/1收到的tag为11的报文,将在S1上打双层tag,从uplink端口fei\_1/2 转发,外层tag为998,内层tag为11。
- 3. 从custom端口fei\_1/1收到的tag为999的报文,将通过uplink端口fei\_1/2透传。

### 图1-7 SVLAN 配置实例图



使用传统的SVLAN配置方法进行配置,如下所示。

S1的SVLAN配置:

ZTE中兴

```
ZXR10(config)#vlan qinq session-no 1 customer-port fei_1/1
uplink-port fei_1/2 in-vlan 10 ovlan 997
ZXR10(config)#vlan qinq session-no 2 customer-port fei_1/1
uplink-port fei_1/2 in-vlan 11 ovlan 998
ZXR10(config)#vlan qinq session-no 3 customer-port fei_1/1
uplink-port fei 1/2 in-vlan 999 untag helper-vlan 4094
```

#### S1的SVLAN相关端口配置:

```
ZXR10(config)#interface fei_1/1
ZXR10(config-if)# negotiation auto
ZXR10(config-if)# switchport mode hybrid
ZXR10(config-if)# switchport hybrid vlan 999 tag
ZXR10(config-if)# switchport hybrid vlan 997-998 untag
ZXR10(config-if)# switchport qinq customer
```

ZXR10(config)#interface fei\_1/2
ZXR10(config-if)# switchport mode hybrid
ZXR10(config-if)# switchport hybrid vlan 997-998 tag
ZXR10(config-if)# switchport hybrid vlan 999 tag
ZXR10(config-if)# switchport hybrid vlan 4094 untag
ZXR10(config-if)# switchport qinq uplink

#### 如果将配置要求改为:

- 从custom端口fei\_1/1收到的tag为10、源IP地址为192.168.0.1的报文,在S1上打上双层 tag,从uplink端口fei\_1/2转发,外层tag为997,内层tag为10。
- 从custom端口fei\_1/1收到的tag为10、源IP地址为192.168.0.2的报文,在S1上打上双层 tag,从uplink端口fei\_1/2转发,外层tag为998,内层tag为10。
- 从custom端口fei\_1/1收到的tag为11的报文,将在S1上打双层tag,从uplink端口fei\_1/2 转发,外层tag为998,内层tag为11。
- 4. 从custom端口fei\_1/1收到的tag为999的报文,将通过uplink端口fei\_1/2透传。

这时就要使用基于VFP的SVLAN配置方法进行配置,如下所示。

#### S1的SVLAN配置:

```
ZXR10(config)#vfp session 1 invlan 10 in 10
rule 1 ovlan 997
ZXR10(config)#vfp session 2 invlan 10 in 10 rule 2 ovlan 998
```

ZXR10(config)#vfp session 3 invlan 11 in 10 rule 3 ovlan 998 ZXR10(config)#vfp session 4 invlan 999 in 10 rule 3 untag pinpoint ZXR10(config)#acl standard number 10 ZXR10(config-std-acl)#rule 1 permit 192.168.0.1 0.0.0.0 ZXR10(config-std-acl)#rule 2 permit 192.168.0.2 0.0.0.0 ZXR10(config-std-acl)#rule 3 permit any

#### S1的SVLAN相关端口配置:

```
ZXR10(config)#interface fei_1/1
ZXR10(config-if)# negotiation auto
ZXR10(config-if)# switchport mode hybrid
ZXR10(config-if)# switchport hybrid vlan 999 tag
ZXR10(config-if)# switchport hybrid vlan 997-998 untag
ZXR10(config-if)# ip access-group 10 vfp
ZXR10(config-if)# switchport qinq customer
```

ZXR10(config)#interface fei\_1/2
ZXR10(config-if)# switchport mode hybrid
ZXR10(config-if)# switchport hybrid vlan 997-998 tag
ZXR10(config-if)# switchport hybrid vlan 999 tag
ZXR10(config-if)# switchport qinq uplink

# 1.10 VLAN的维护与诊断

为了方便VLAN的维护与诊断,交换机提供了如下命令:

命令	功能
ZXR10#show vlan [ brief  access  trunk  hybrid  id < vlan-id> [ ifindex]	查看VLAN信息
<pre>name &lt; vlan-name&gt; [ ifindex] ]</pre>	

举例

```
    查看所有VLAN的配置信息
    ZXR10(config)#show vlan
    VLAN Name PvidPorts UntagPorts TagPorts
    1 VLAN0001 gei_7/5-12
```

10	VLAN0010	gei_7/1-3	
100	VLAN0100		gei_7/3-4
130	VLAN0130	gei_7/4	gei_7/4
136	VLAN0136		gei_7/4
200	VLAN0200		gei_7/3

### 2. 查看端口为Trunk模式的所有VLAN信息

ZXR10(config	g)#show vlan tr	unk	
VLAN Name	PvidPorts	UntagPorts	TagPorts

V 117 71 V	ivanic	IVIGIOICS	Uncagrores	ragrores
1	VLAN0001			
10	VLAN0010	gei_7/3		
100	VLAN0100			gei_7/3
130	VLAN0130			
136	VLAN0136			
200	VLAN0200			gei_7/3



本章包含如下主题:

• STP简介	2-1
• 配置STP	2-7
• 配置BPDU保护	2-9
• STP配置实例	2-10
• STP的维护与诊断	2-12

# 2.1 STP简介

STP是生成树协议的英文缩写,该协议可应用于环路网络,通过一定的算法阻断某些冗余路径,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。

STP协议是通过在一个扩展的局域网中参与STP的所有交换机之间交换BPDU来实现的。 通过交换BPDU可以完成以下操作:

- 1. 在稳定的生成树拓扑结构中选择一个根网桥。
- 2. 在每个交换网段选择一台指定交换机。
- 3. 通过将冗余的交换机端口设置为阻塞状态来避免网络中的环路。

STP支持三种模式: SSTP、RSTP和MSTP, 它们分别遵循IEEE802.1d、IEEE802.1w、IEEE802.1s标准。

# 2.1.1 SSTP模式

SSTP模式被称为单生成树协议,在功能上完全遵照IEEE802.1d标准运行。运行SSTP模式的网桥可以与RSTP模式、MSTP模式的网桥实现互通。

# 2.1.2 RSTP模式

RSTP称为快速生成树协议,它比STP(即SSTP模式)提供了更快的收敛速度,即在网络 拓扑发生变化时,在点对点的连接条件下原来冗余的交换机端口状态可以迅速由阻塞到 转发。

# 2.1.3 MSTP模式

MSTP(Multiple Spanning Tree Protocol)即多生成树协议,它增加了实例和VLAN映射的概念,SSTP模式和RSTP模式均可以当作MSTP模式的特例,即只存在一个实例0的情况。MSTP模式还提供了VLAN环境的快速聚合和负载均衡。

在SSTP模式和RSTP模式下,没有VLAN的概念,每个端口的状态只有一种,即端口在不同VLAN中的转发状态是一致的。而在MSTP模式下,可以存在多个spanning-tree实例,端口在不同VLAN下的转发状态可以不同;在MST区域内部可以形成多个独立的子树实例,实现负载均衡。

下面详细介绍MSTP的几个基本概念。

1. 多生成树配置标识

多生成树配置标识(MST Config ID)是指带有不同VID的帧的转发方案,即在MST 区域中的所有网桥根据帧中的VID转发到特定的生成树(CIST或某一MST实例)。

MST Config ID由以下几部分组成:

- 配置名:长度为32字节的字符串。
- 版本级别:长度为2个字节的非负整数。
- 配置摘要:根据MST Config Table产生的经过MD5处理的签名,长度为16字节。

MST Config Table由4096个连续的两字节组成,第一个两字节和最后一个两字节均为0,其他两字节可表示一个二进制数。第二个两字节表示VID 1对应的MSTID数值,第三个两字节表示VID 2对应的MSTID数值,依次类推,倒数第二个两字节表示VID 4094对应的MSTID数值。配置摘要是将MST Config Table与一个固定KEY值经过HMAC-MD5 算法处理所获得的,它通过解析可以获得某个VID属于哪一个MST实例或CIST。

2. MST区域

每一个MST区域由一个或几个具有相同MST Config ID的相连网桥组成,它们启用相同的多个实例,此区域同时包括那些在CIST实例中指定网桥为这些网桥之一的LAN。

# NOTE **说明**:

一个MST区域内的网桥的MST Config ID肯定相同,但两个MST Config ID相同的网桥 不一定在同一个MST区域内。例如:两个相同MST Config ID的网桥通过属于另一个 MST区域的LAN进行相连,那么这两个网桥属于不同的MST区域。

在MST区域中,可以有不同的生成树结构: IST (Internal Spanning Tree)、MST1、MST2、…、MSTn。每一个MSTi都可以被称作MSTI(MST实例),网桥根据与VID对应的路径(MSTI的生成树结构)来转发特定VID的帧。VID与MSTI的对应关系在MST Config ID中得到体现,而MSTI的生成树结构则通过系统配置的优先级参数来决定。

#### 3. MST实例

MST桥必须支持两种实例(Instance)的实现:一个IST和多个MST实例。在一个区域中默认运行IST,所有VLAN都缺省地配置到IST中,IST连接了区域中的所有交换机,负责与区域外面的其他MST区域和SST区域通信。MST实例不单独发送BPDU报文,生成树信息被包含在M-record中,作为IST BPDU的一部分在区域内部传送。

4. CIST

各个MST区域内部的IST以及外部的CST共同组成CIST(Common and Internal Spanning Tree),即CIST在MST区域内部与IST相同,在MST区域外部和CST相同。

5. IST Region Root

每个MST区域中都有一个IST Region Root交换机,它是距CST Root路径开销最小的交换机。如果CIST Root在某个MST区域中,则CIST Root就是该MST区域的IST Region Root。选定了IST Region Root后,区域中其它指向CIST Root的端口将被堵塞。

6. MST BPDU

MST区域内的MSTI不与区域外通信,只有IST才和区域外交换BPDU报文。在区域内,MSTI也不单独发送BPDU报文,IST发送的MST BPDU报文包含了MSTI信息。 MSTI通过一个标志表示需要发送MST BPDU报文,具体的报文由IST发送。所有需要 发送BPDU的MSTI将自己的信息放在M-record结构中,M-record结构作为IST BPDU 的一部分发出。

# 2.1.4 BPDU保护

交换机根据BPDU协议包中的内容来进行生成树计算,网络只要发生拓扑变化就会引发 全网的重新计算,如果这样的计算太频繁,会占用大量的系统资源,严重影响数据包的 正常转发,同时根网桥的变换也会为网络管理者带来不便。应用BPDU保护就是为了把 拓扑变化的影响降低到最小,BPDU保护包括三个功能:

- 1. 边缘端口的BPDU保护
- 2. 端口环回保护
- 3. 端口根保护

下面分别介绍它们。

1. 边缘端口的BPDU保护

应用边缘端口的BPDU保护是为了防止边缘端口所接的设备影响整个网络的正常运行。

如图2-1所示,交换机A的优先级为8192,是网络中的根交换机,交换机B的优先级为16384,交换机A和B之间连接的是千兆链路。交换机C是一个接入层交换机,它的优先级是32768,交换机A和C、交换机B和C之间连接的是百兆链路,交换机C和交换机D连接的端口是边缘端口。

根据生成树计算方法,交换机C和交换机B相连的端口被阻塞,如图2-1中的1所示, 当设备D不参与生成树计算时,箭头的方向表示BPDU的流向。



图2-1 边缘端口的BPDU保护

如果交换机D开始参与生成树计算,而且它的优先级比交换机A(根交换机)低,那 么交换机D将成为根交换机,交换机B和A相连的端口被阻塞,如图2-1中的2所示, 网络流量通过AC和BC之间的百兆线路转发,降低了网络的使用效率。
为了防止这种情况的发生,可以在交换机C与D相连的端口上配置边缘端口的BPDU 保护功能。配置该功能后,当发现端口上收到来自交换机D的BPDU报文时,立刻关 闭和交换机D相连的端口,保证生成树协议不会重新计算。

2. 端口环回保护

导致生成树环路的情况有很多,有一种情况是由于阻塞端口停止接收或未能接收到 BPDU报文,导致该端口状态错误的由阻塞变为转发。如图2-2所示,交换机A是根 交换机。根据生成树的计算方法,交换机C和B相连的端口被阻塞,但是该端口继续 接收交换机B发送过来的BPDU包。

图2-2 端口环回保护功能1



当发生了单向链路故障后,该端口接收不到交换机B发送的BPDU报文,端口状态在 一定时间后会变为转发状态,从而形成了环路,如图2-3所示。





如果配置了端口环回保护功能,交换机C和B相连的阻塞端口在一定时间后转变为 LOOP\_INCONSISTENT状态,端口在该状态时不会转发用户的数据流,所以不会形 成环路,如图2-4所示。





3. 端口根保护

根端口保护功能保证当端口使能的情况下,是指定端口。如果网桥在配了ROOT GUARD的端口接收到了更优的BPDU报文,该端口会转变到ROOT\_INCONSISTENT 状态,而且用户的数据流量也不会从该端口转发。



图2-5 端口根保护功能

如图2-5中的1所示,交换机A是根交换机,交换机C是接入层交换机,交换机C和B 相连的端口被阻塞,交换机D未参加生成树计算。

如果交换机D开始参与生成树计算,而且它的优先级比交换机A(根交换机)的优先级低,交换机D将被选为根交换机,交换机B和A相连的端口被阻塞,如图2-5中的2所示。

为了防止这种情况发生,需要在交换机C和D相连的端口配置端口根保护功能。配置 了该功能后的端口始终保持在指定端口状态,不会成为根端口。如果该端口接收到 了更低优先级的BPDU报文,根保护功能会把该端口设置为ROOT\_INCONSISTENT 状态,不会重新计算生成树。当交换机D停止发送更优的BPDU报文时,该端口经过 一定的时间后重新转变为转发状态,恢复是自动的,不需要人为干预。

# 2.2 配置STP

## 2.2.1 启用STP

1. 在全局模式下启用STP

命令	功能
<pre>ZXR10(config) #spanning-tree { enable   disable}</pre>	启用或关闭STP协议

默认情况下,STP处于关闭状态。在交换机上关闭STP协议后,所有物理状态为up的 端口均设为转发状态。

2. 在接口配置模式下启用STP

命令	功能
<pre>ZXR10(config-if) #spanning-tree { enable   disable}</pre>	配置交换机的端口是否参与生成树计算

在一些特定的环境中,可能要求某端口不参与生成树的计算,比如交换机的上行口 或连接PC机的端口。

## 2.2.2 配置STP模式

命令	功能
ZXR10 (config) <b>#spanning-tree mode</b> { <b>sstp</b>   <b>rstp</b>   <b>mstp</b> }	配置STP模式,交换机默认的模式为
	MSTP,无论配置哪一种模式,都可以
	与其他两种模式完全兼容和互通

## 2.2.3 配置STP参数

步骤	命令	功能
1	ZXR10 (config) # <b>spanning-tree hello-time</b> < <i>time</i> >	设置BPDU数据包的发送时间间隔
2	ZXR10 (config) # <b>spanning-tree forward-delay</b> < <i>time</i> >	设置端口从阻塞状态进入转发状态
		需要经历的延时
3	ZXR10(config)# <b>spanning-tree max-age</b> < <i>time</i> >	设置BPDU数据包的最大有效时间
4	ZXR10 (config) # <b>spanning-tree mst max-hops</b> < <i>hop</i> >	设置BPDU数据包的最大有效跳数

# 2.2.4 创建实例

在MSTP模式中,用户可以通过创建实例使相连的交换机组成一个MST区域,这样可以 实现整个网络的快速收敛和负载均衡。

步骤	命令	功能
1	ZXR10 (config) <b>#spanning-tree mst configuration</b>	进入MSTP配置模式

步骤	命令	功能
2	ZXR10(config)#instance < instance > vlans < vlan-id>	创建实例

# 2.2.5 设置MST名称和版本号

相互连接的交换机属于同一个MST区域需要以下三个条件: MST名称相同、MST版本号相同和实例VLAN映射表相同。

步骤	命令	功能
1	ZXR10 (config) #spanning-tree mst configuration	进入MSTP配置模式
2	ZXR10(config)# <b>name</b> < <i>string</i> >	设置MST名称
3	<pre>ZXR10(config) #revision &lt; version&gt;</pre>	设置MST版本号

# 2.2.6 配置交换机的优先级

命令	功能
ZXR10 (config) <b>#spanning-tree mst instance</b> < <i>instance</i> > <b>priority</b> < <i>priority</i> >	配置交换机的优先级和端口优先级

NOTE 说明:

交换机优先级和端口优先级必须在实例已创建的条件下进行配置。

# 2.3 配置BPDU保护

# 2.3.1 配置边缘端口的BPDU保护

命令	功能
ZXR10 (config-if) # <b>spanning-tree edged-port enable</b>	激活边缘端口的BPDU保护
ZXR10(config-if) #spanning-tree bpduguard action { discard   shutdown}	配置BPDU保护开启后端口的状态。
	配置为discard时,端口收到BPDU报文
	后,只是丢弃BPDU报文,并不阻塞
	端口; 配置为shutdown时, 端口收到
	BPDU报文后,会阻塞端口

使用命令spanning-tree edged-port disable取消边缘端口的BPDU保护。

## 举例

在需要配置边缘端口BPDU保护的端口进行如下配置:

ZXR10(config-if)#spanning-tree bpduguard action shutdown

ZXR10(config-if)#spanning-tree edged-port enable

# 2.3.2 配置端口环回保护

命令	功能
ZXR10 (config-if) # <b>spanning-tree guard loop instance</b> < <i>instance-id</i> >	配置在实例中开启端口环回保护功能
ZXR10 (config-if) #no spanning-tree guard loop instance < instance-id>	取消端口环回保护功能

# 2.3.3 配置端口根保护

命令	功能
ZXR10 (config-if) # <b>spanning-tree guard root instance</b> < <i>instance-id</i> >	在实例中开启端口根保护功能
ZXR10 (config-if) <b>#no spanning-tree guard root instance</b> < <i>instance-id</i> >	取消端口根保护功能

# 2.4 STP配置实例

MSTP可以支持多个MST区域,但是建议只配置一个MST区域,通常是将MST区域运行 在骨干网上,作为整个CST的根,这样可以更好地实现整个网络的快速聚合,并实现负 载均衡。

如图2-6所示,在骨干网运行MSTP,MST域作为CST的根,即CST根交换机在MST区域内部。三台交换机A、B、C配置在同一个区域中,它们的初始优先级均为32768,根据MAC地址确定CST root和IST root。三台交换机的MAC地址分别为:

Switch A: 000d.0df0.0101

Switch B: 000d.0df0.0102

Switch C: 000d.0df0.0103

#### 图2-6 MSTP配置实例组网图1



SwitchA、B和C同属一个MST区域,并且此 区域在网络拓扑中的身份是CIST root

创建两个MST实例,将区域中的VLAN映射到这两个MST实例中。

交换机D上运行CST模式,它的MAC地址为:000d.0df0.0104,优先级为32768。本例的目的是要实现整个网络的快速聚合和区域内交换机A上两条链路的负载均衡。

交换机A的配置:

/\*配置MST区域\*/

ZXR10\_A(config) # spanning-tree enable ZXR10\_A(config) #spanning-tree mode mstp ZXR10\_A(config) #spanning-tree mst configuration ZXR10\_A(config-mstp) #name zte ZXR10\_A(config-mstp) #revision 2

/\*将VLAN 1~10映射到instance 1中, VLAN 11~20映射到instance 2 中\*/ ZXR10\_A(config-mstp)#instance 1 vlan 1-10 ZXR10 A(config-mstp)#instance 2 vlan 11-20

#### 交换机B的配置:

/\*配置MST区域\*/
ZXR10\_B(config)# spanning-tree enable
ZXR10\_B(config)#spanning-tree mode mstp
ZXR10\_B(config)#spanning-tree mst configuration
ZXR10\_B(config-mstp)#name zte
ZXR10\_B(config-mstp)#revision 2

```
/*将VLAN 1~10映射到instance 1中, VLAN 11~20映射到instance 2 中*/
ZXR10_B(config-mstp)#instance 1 vlan 1-10
ZXR10_B(config-mstp)#instance 2 vlan 11-20
```

/\*改变交换机B在instance 2中的优先级,使之成为Instance 2的Root\*/ ZXR10 B(config-mstp)#spanning-tree mst instance 2 priority 4096

交换机C的配置:

/\*配置MST区域\*/

ZXR10\_C(config)# spanning-tree enable ZXR10\_C(config)#spanning-tree mode mstp ZXR10\_C(config)#spanning-tree mst configuration ZXR10\_C(config-mstp)#name zte ZXR10\_C(config-mstp)#revision 2

/\*将VLAN 1~10映射到instance 1中, VLAN 11~20映射到instance 2 中\*/ ZXR10\_C(config-mstp)#instance 1 vlan 1-10 ZXR10 C(config-mstp)#instance 2 vlan 11-20

/\*改变交换机C在instance 1中的优先级,使之成为Instance 1的Root\*/ ZXR10 C(config-mstp)#spanning-tree mst instance 1 priority 4096

交换机D保留默认配置即可。

# 2.5 STP的维护与诊断

ZXR10 6900系列交换机提供show命令查看STP的相关信息,进行故障诊断。

命令	功能
ZXR10# <b>show spanning-tree instance</b> < <i>instance</i> >	显示基于实例的生成树详细信息
ZXR10#how spanning-tree interface < port-name>	显示指定端口的生成树信息
ZXR10# <b>show spanning-tree statistics</b> < <i>port-name</i> >	显示指定端口的BPDU包发送和接收
	的统计信息
ZXR10#show spanning-tree mst configuration	显示MSTP的配置信息
ZXR10#show spanning-tree inconsistentports	显示BPDU保护的配置结果

ZTE中兴



#### 本章包含如下主题:

• MAC地址表简介	3-1
• 配置MAC地址表	3-3
• MAC地址表配置实例	3-7

## 3.1 MAC地址表简介

MAC地址是网络设备的硬件标识,交换机根据MAC地址进行报文转发。MAC地址具有 唯一性,这保证了报文的正确转发。

每个交换机都维护着一张MAC地址表。在这张表中,MAC地址和交换机的端口相对应。 当交换机收到数据帧时,根据MAC地址表来决定对该数据帧进行过滤还是转发到交换机 的相应端口。

## 3.1.1 MAC地址表的构成及意义

MAC地址表的表项由MAC地址和VLAN ID唯一标识,只要MAC地址和VLAN ID部分相同,就认为是同一个表项。MAC地址表的表项包含以下部分:

- 1. MAC地址:如00D0.8756.95CA。
- 2. VLAN ID:如果某个端口被设置成属于多个VLAN,那么同一个MAC地址会对应多个VLAN ID。
- 3. 端口号:如gei\_2/3。
- 4. 其它相关标志:这些标志表示MAC地址的状态和操作,有以下五种:
  - static: 表示MAC地址是静态的。
  - permanent: 表示MAC地址是永久MAC地址。
  - to-static: 表示MAC地址是被固化的MAC地址。
  - src\_filter: 表示依据源MAC地址对数据帧进行过滤。
  - dst\_filter: 表示依据目的MAC地址对数据帧进行过滤。

交换机进行二层转发时,根据数据帧的目的MAC和VLAN查找MAC地址表,用来判断将 数据帧转发到哪个端口。

交换机进行三层快速转发时,当得到下一跳IP地址对应的MAC地址后,同样要通过查找 MAC地址表判断需要将数据包转发到哪个端口。

## 3.1.2 MAC地址的分类

MAC地址表中的MAC地址分为以下三种类型。

1. 动态MAC地址

动态MAC地址是交换机在网络中通过数据帧学习到的,当老化时间到来时会被删除。 当设备所连接的交换机的端口发生变化时,MAC地址表中相应的MAC地址和端口的 对应关系也会随之改变。动态MAC地址在交换机关电重启后会消失,需要重新学习。

2. 静态MAC地址

静态MAC地址是通过配置产生的,不会被老化掉。不管设备所连接的交换机的端口 发生怎样的变化,MAC地址表中MAC地址和端口的对应关系始终不会改变,特殊情 况是当端口不再属于原VLAN时,相应的静态MAC会被删除。静态MAC地址在交换 机关电重启后也会消失,需要重新进行配置。

3. 永久MAC地址

永久MAC地址也是通过配置产生的,不会被老化掉。不管设备所连接的交换机的端口发生怎样的变化,MAC地址表中MAC地址和端口的对应关系始终不会改变,特殊情况是当端口不再属于原VLAN时,相应的永久MAC会被删除。保存交换机配置后,永久MAC地址在交换机关电重启后不会消失。

## 3.1.3 MAC地址表的建立与删除

初始状态下,交换机的MAC地址表是空的,为了实现快速转发,必须建立MAC地址表。 同时,由于MAC地址表的容量有限,而网络上的设备变动比较频繁,交换机要及时删除 旧的MAC地址表项,更新发生了变化的MAC地址表项。

1. 动态学习

MAC地址表中的动态MAC地址是由交换机通过学习得来的。交换机学习MAC地址的过程如下:

当交换机的某端口收到一个数据帧时,交换机就会分析该数据帧的源MAC地址和 VLAN ID(假设为MAC1+VID1)。如果这个MAC地址合法,并且可以学习,就以 MAC1+VID1作为键值查找MAC地址表。如果MAC地址表中不存在该地址,就把该 地址添加到表中;如果MAC地址表中已经存在该地址,就对该表项进行更新。

NOTE ▶ 说明:

- a. MAC地址学习是对数据帧的源MAC地址进行学习,而不是目的MAC地址。
- b. MAC地址学习只学习单播地址,对于广播和组播地址不进行学习。
- 2. MAC地址老化

MAC地址表的容量是有限的,为了实现MAC地址表资源的有效利用,交换机提供了 MAC地址老化功能。

如果交换机在一段时间(设定的老化时间)内没有收到某个设备发出的数据帧,交换机就认为该设备已经离开网络。这时,交换机会将这个设备的MAC地址从MAC地址表中删除,这样就实现了交换机MAC地址表的及时更新。MAC地址老化只对动态MAC地址起作用。

3. 手动添加和删除

如果网络相对比较稳定,某个设备所连接的交换机端口始终是固定的,那么可以通 过配置命令,直接将MAC地址条目添加到交换机的MAC地址表中,可以将MAC地 址配置成静态、永久两种类型中的任何一种。通过添加静态或永久的MAC地址可以 防止MAC欺骗形式的网络攻击。

通过MAC地址删除命令可以删除添加的MAC地址。在交换机上使用删除命令还可以 强制删除动态学习到的MAC地址,让其重新进行学习。

## 3.2 配置MAC地址表

#### 3.2.1 设置MAC地址老化时间

MAC地址老化时间的设置会影响交换机的性能。如果设置的MAC地址老化时间过短, 交换机可能会删除许多有效的MAC地址表项,导致交换机大量广播找不到目的MAC地 址的报文,占用交换机的带宽。如果设置的MAC地址老化时间过长,交换机可能会保存 许多过时的MAC地址表项,从而耗尽MAC地址表资源,导致新的MAC地址无法添加到 MAC地址表中。

命令	功能
ZXR10(config)# <b>mac aging-time</b> < <i>time</i> >	设置MAC地址老化时间,默认为360秒

## 3.2.2 设置MAC地址固化

MAC地址固化是指将MAC地址表中所有的动态MAC地址转换成静态MAC地址。静态 MAC地址不会被永久保存,在交换机关电重启后会消失。

命令	功能	
<pre>ZXR10(config) #mac to-static [ interface &lt; port-name&gt; ] { enable   disable}</pre>	设置MAC地址固化	

## 3.2.3 设置端口绑定MAC地址

在交换机上通过添加静态或永久MAC地址,实现端口MAC地址绑定。绑定MAC地址后,MAC地址和端口的对应关系就按照配置的情况固定下来,该地址将不再被学习。

步骤	命令	功能
1	<pre>ZXR10(config) #mac add { permanet   static} &lt; mac-address&gt;</pre>	添加MAC地址
	interface < port-name> [ all-owner-vlans   vlan < vlan-id> ]	
2	<pre>ZXR10(config)#mac delete { interface &lt; port-name&gt;   vlan   &lt; maa addreas&gt; ) &lt; vlan id&gt;</pre>	删除MAC地址
	mac-address> } < vlan-id>	

## 3.2.4 设置端口MAC地址学习

默认情况下,交换机端口的MAC地址学习功能都是打开的,端口可以动态学习MAC地址。如果交换机某个端口连接的设备都是固定的,就可以进行MAC地址绑定,把该端口上所有可能出现的MAC地址都进行手动配置,然后关闭端口的MAC地址学习,使该端口不再动态学习MAC地址。

命令	功能
<pre>ZXR10(config) #mac learning [ interface &lt; port-name&gt; ] { enable   disable}</pre>	设置端口MAC地址学习

## 3.2.5 限制端口或全局的MAC地址数目

交换机MAC地址表的容量是有限的,当用户数量非常多,将要达到MAC地址表所能支持的容量时,可以对低优先级用户所处的端口所能学习的MAC地址数目进行限制。

通过限制端口MAC地址数目,还可以很好的防范利用MAC地址泛洪促使MAC地址表溢 出这类网络攻击。

命令	功能
ZXR10 (config) # <b>mac limit-num</b> [ <b>interface</b> < <i>port-name</i> > ] < <i>max-number</i> >	限制端口或全局的MAC地址数目

默认情况下交换机对MAC地址的数目没有限制。配置了MAC地址数目限制后,如果要取消限制,只要将MAC地址数目限制设置为0。

## 3.2.6 设置端口MAC地址学习保护

当检测到某个端口的MAC地址学习异常时,交换机会将该端口的MAC地址学习保护一段时间。一旦端口进入保护状态,将不进行新的地址学习,当保护时间到了以后,端口 才重新转入MAC学习状态。

设置端口MAC地址学习保护需要以下几个步骤:

- 1. 设置端口MAC地址学习数目限制。
- 2. 启用端口MAC地址学习保护功能。
- 3. 设置被保护端口的保护时间。

步骤	命令	功能
1	<pre>ZXR10(config)#mac protect [ interface &lt; port-name&gt; ] { enable  </pre>	设置端口MAC地址学习保护,默认
	disable}	情况下端口MAC地址学习保护功能
		是关闭的
2	ZXR10(config) #mac protect time < time>	设置端口MAC地址学习保护时间

## 3.2.7 设置MAC地址过滤

根据MAC地址进行数据帧的过滤,有以下三种形式:

- 只匹配数据帧的源MAC地址;
- 只匹配数据帧的目的MAC地址;
- 匹配数据帧的源和目的MAC地址。

命令	功能
<pre>ZXR10(config) #mac filter { source   both   destination } &lt; mac-address &gt; &lt;</pre>	设置MAC地址过滤
vlan-id>	

配置MAC地址过滤时,不需要输入端口名称,交换机对从任何一个端口进来的数据帧都 会进行过滤。

## 3.2.8 配置MAC地址表的256K模式

配置MAC地址表的256K模式后,需要保存配置并重启交换机才能生效。启用MAC地址 表的256K模式后,交换机上不能插入128M内存的线卡,交换机主控和大于128M内存的 线卡上会申请256K的地址表,128M内存的线卡仍然是64K的地址表。

步骤	命令	功能	
1	ZXR10 (config) # <b>mac learning-strategy micode</b>	配置MAC地址学习方式	
2	ZXR10 (config) # <b>mac learn special</b>	是关闭交换芯片内部接口上进行 MAC地址学习,默认是开启的,在 起用网络处理器业务的情况下要求	
3	<pre>ZXR10(config) #mac 256k { disable  enable}</pre>	交换机上MAC地址表的256K模式默 认为关闭	

# 3.2.9 查看MAC地址表

命令	功能
ZXR10#show mac [ dynamic  static  permanent   to-static  src-filter	查看MAC地址表
dst-filter   { < mac-address> [ vlan < vlan-id> ] }   interface < port-name>	
vlan < vlan-id> ]	

## 举例

ZXR10(config)#show mac						
Total mac addres	ss : 6					
Flags:vid -VLAN	id,stc -	stati	lc,per	-permar	nent,toS -to	o-static,
srF -sourc	ce filter	,dsF	-desti	nation	filter,	
time -day:	:hour:min	n:sec,	Frm -	-mac f	rom where:0	,drv;1,
config;2,V	/PN;3,802	2.1X;4	l,micro	;5,dhcp	)	
MAC_Address p	port	vid s	static	locked	<pre>src_filter</pre>	dst_filter
0000.0000.0018 f	fei_8/6	200	0	0	0	0
0000.0000.2222		1	1	1	1	0
0000.0000.0022 f	fei_8/14	888	0	0	0	0
0000.0000.1111 g	gei_3/3	888	1	0	0	0
0000.0000.3333 g	gei_3/3	888	1	1	0	0
0000.0000.0021 f	fei_8/12	888	0	0	0	0

# 3.3 MAC地址表配置实例

如图3-1所示,交换机A和交换机B通过聚合链路相连,交换机B连接了3台PC和1台ZXR10 2826E,具体数据如表3-1所示。

#### 图3-1 MAC地址表配置实例



表3-1 MAC地址表配置实例数据

设备	MAC地址	交换机端口	VLAN
PC1	0X00D0.8765.95CA	fei_2/1	1
PC2	0X00D0.8765.95CB	fei_2/3	2
PC3	0X00D0.8765.95CC	fei_2/5	3
ZXR10 2826E		fei_2/7	4

将PC1、PC2、PC3的MAC地址绑定到交换机B的端口。ZXR10 2826E下面连接的个人用 户较多,需要在交换机B的相应端口上设置端口MAC地址学习保护,保护数目为1000个, 保护时间120s。同时还需要设置交换机B的MAC地址老化时间为180s。

#### 交换机B的配置:

```
/*配置端口MAC地址绑定*/
ZXR10(config)#mac add permanent 00D0.8765.95CA interface
fei_2/1 vlan 1
ZXR10(config)#mac add permanent 00D0.8765.95CB interface
fei_2/3 vlan 2
ZXR10(config)#mac add permanent 00D0.8765.95CC interface
```

fei\_2/5 vlan 3

/\*配置端口MAC地址学习保护\*/ ZXR10(config)#mac limit-num interface fei\_2/7 1000 ZXR10(config)#mac protect interface fei\_2/7 enable ZXR10(config)#mac protect time 120

/\*配置MAC地址老化时间\*/

ZXR10(config)#mac aging-time 180



#### 本章包含如下主题:

• 链路聚合简介	4-1
• 配置链路聚合	4-2
• 链路聚合配置实例	4-2
• 链路聚合的维护与诊断	4-4

# 4.1 链路聚合简介

链路聚合(Link Aggregation)又称Trunk,是指将多个物理端口捆绑在一起,成为一个逻辑端口,以实现出/入流量在各成员端口中的负荷分担,交换机根据用户配置的端口负荷分担策略决定报文从哪一个成员端口发送到对端的交换机。

当交换机检测到其中一个成员端口的链路中断时,就停止在此端口上发送报文,直到这 个端口的链路恢复正常。链路聚合在增加链路带宽、实现链路传输弹性和冗余等方面是 一项很重要的技术。

ZXR10 6900系列交换机支持静态Trunk和LACP两种链路聚合方式。

- 1. 静态Trunk将多个物理端口直接加入Trunk组,形成一个逻辑端口。这种方式不利于 观察链路聚合端口的状态。
- 2. LACP即链路聚合控制协议,遵循IEEE 802.3ad标准。LACP通过协议将多个物理端口 动态聚合到Trunk组,形成一个逻辑端口。LACP自动产生聚合以获得最大的带宽。

在ZXR10 6900系列交换机上配置链路聚合功能需要遵循以下原则:

- 一共可以配置32个Trunk组,每个Trunk组最多包含8个成员端口。
- 支持跨接口板的聚合,成员端口可以分布在任何接口板上,但是所选择的端口必须 工作在全双工模式,工作速率必须一致。
- 成员端口的模式可以是access、trunk或hybrid,但是必须保持一致。

ZXR10 6900系列交换机上链路聚合形成的逻辑端口称为smartgroup,可以把smartgroup当 作普通端口使用。

# 4.2 配置链路聚合

步骤	命令	功能
1	ZXR10(config) #interface smartgroup < smartgroup-id>	创建链路聚合组
2	ZXR10 (config-if) # <b>smartgroup load-balance</b> < <i>mode</i> >	设置链路聚合负荷分担方式
3	ZXR10(config-if)# <b>exit</b>	离开链路聚合组
4	<pre>ZXR10(config) #interface &lt; interface-name&gt;</pre>	进入交换机二层接口
5	<pre>ZXR10 (config-if) #smartgroup &lt; smartgroup-id&gt; mode { passive  </pre>	在Trunk组中添加成员端口,并设置
	active   on }	端口聚合模式
6	ZXR10(config-if)# <b>exit</b>	离开交换机二层接口
7	ZXR10 (config) #smartgroup nonucast { load-balance	(可选)设置非单播包的负载均衡
	non-load-balance}	模式

端口链路聚合支持6种负荷分担方式,分别基于源IP、目的IP、源和目的IP、源MAC、目的MAC、源和目的MAC。默认情况下是基于源和目的MAC。

聚合模式设置为on时端口运行静态trunk,参与聚合的两端都需要设置为on模式。

聚合模式设置为active或passive时端口运行LACP, active指端口为主动协商模式, passive指端口为被动协商模式。配置动态链路聚合时,应当将一端端口的聚合模式设置为active, 另一端设置为passive,或者两端都设置为active。

NOTE 说明:

成员端口的VLAN链路类型配置必须和smartgroup的VLAN链路类型配置一致,否则不允许 加入此Trunk组。

# 4.3 链路聚合配置实例

如图4-1所示,交换机A和交换机B通过smartgroup端口相连,它们分别由4个物理端口聚 合而成。smartgroup的端口模式为trunk,承载VLAN10和VLAN20。

#### 图4-1 链路聚合配置实例



#### 交换机A的配置如下所示:

ZXR10\_A(config)#interface smartgroup10 ZXR10\_A(config)#interface gei\_5/1 ZXR10\_A(config-if)#smartgroup 10 mode active ZXR10\_A(config)#interface gei\_5/2 ZXR10\_A(config-if)#smartgroup 10 mode active ZXR10\_A(config)#interface gei\_5/3 ZXR10\_A(config)#interface gei\_5/4 ZXR10\_A(config)#interface gei\_5/4 ZXR10\_A(config-if)#smartgroup 10 mode active ZXR10\_A(config-if)#smartgroup 10 mode active ZXR10\_A(config-if)#smartgroup 10 mode active ZXR10\_A(config-if)#switchport mode trunk ZXR10\_A(config-if)#switchport trunk vlan 10 ZXR10\_A(config-if)#switchport trunk vlan 20 ZXR10\_A(config-if)#switchport trunk native vlan 10

#### 交换机B的配置如下所示:

ZXR10\_B(config) #interface smartgroup11 ZXR10\_B(config) #interface gei\_3/5 ZXR10\_B(config-if) #smartgroup 11 mode passive ZXR10\_B(config) #interface gei\_3/6 ZXR10\_B(config-if) #smartgroup 11 mode passive ZXR10\_B(config) #interface gei\_3/7 ZXR10\_B(config-if) #smartgroup 11 mode passive ZXR10\_B(config) #interface gei\_3/8 ZXR10\_B(config-if) #smartgroup 11 mode passive ZXR10\_B(config-if) #smartgroup 11 mode passive ZXR10\_B(config-if) #smartgroup 11 mode passive

```
ZTE中兴
```

```
ZXR10_B(config-if)#switchport mode trunk
ZXR10_B(config-if)#switchport trunk vlan 10
ZXR10_B(config-if)#switchport trunk vlan 20
ZXR10_B(config-if)#switchport trunk native vlan 10
```

# 4.4 链路聚合的维护与诊断

为了方便链路聚合的维护与诊断,ZXR10 6900系列交换机提供了以下命令。

步骤	命令	功能
1	<pre>ZXR10#show lacp [ &lt; smartgroup-id&gt; ] internal</pre>	查看成员端口的聚合状态
2	<pre>ZXR10#show lacp [ &lt; smartgroup-id&gt; ] counters</pre>	查看成员端口的协议收发包计数
3	<pre>ZXR10#show lacp [ &lt; smartgroup-id&gt; ] neighbors</pre>	查看对端的成员端口

示例:

1. 查看trunk组2中成员端口的聚合状态

当Agg State为selected, Port State为0x3d时,表示端口聚合成功。如果聚合不成功则Agg State显示为unselected。

2. 查看Trunk组2中成员端口的收发包计数

```
ZXR10(config)#show lacp 2 counters
Smartgroup:2
      LACPDUS Marker LACPDUS
Actor
                             Marker
Port
      Τx
           Rx
              Tx Rx
                      Err
                              Err
_____
fei 3/17 11
           5 0 0
                      0
                              0
```

fei\_3/18 10 6 0 0 0 0 ZXR10(config)#

当每个成员端口的协议发包Tx与协议收包Rx都有计数时,才可能聚合成功,否则聚 合失败。

3. 查看Trunk组2对端的成员端口

ZXR10(config)#show lacp 2 neighbors Smartgroup 2 neighbors Actor Partner Partner Port Oper Port Port System ID Port No. Priority Key State -----fei\_3/18 8000,00d0.d0c0.0f60 513 0x8000 0x202 0x3d fei\_3/17 8000,00d0.d0c0.0f60 514 0x8000 0x202 0x3d ZXR10(config)#

其中Partner Port No.代表邻居的端口号,当Port State为0x3d时表示两端聚合成功。

# 5 IGMP Snooping配置

#### 本章包含如下主题:

• IGMP Snooping简介	5-1
• 配置IGMP Snooping	5-2
• IGMP Snooping配置实例	5-5

• IGMP Snooping的维护与诊断 5-5

# 5.1 IGMP Snooping简介

IGMP是Internet组管理协议,运行在主机和组播路由器之间,如图5-1所示。IGMP Snooping对主机和路由器之间的IGMP协议通信进行监听,使交换机在转发组播数据包前学习 到哪些端口属于组播成员,得到组播转发表。这样,组播包只会发送给组播转发表中的 端口,限制了交换机上组播包的扩散,避免了不必要的网络带宽浪费,提高了交换机的 利用率。





## 5.1.1 加入组播组

主机通过主动发送IGMP加入消息加入相应的组播组。当交换机监听到主机发送的IGMP 报文时,转发模块就为收到请求报文的端口所在的VLAN创建一个二层组播转发条目。 当同一VLAN中的其他主机对这个组播流量感兴趣,并发出一个加入该组的请求时,交 换机就把它们加入到已存在的转发条目中。

交换机在同一个VLAN中对每个组播组只创建一个转发条目,在收到请求报文的所有端 口转发相应的组播流量。

## 5.1.2 离开组播组

加入组播组的主机必须回应由路由器定期发出的IIGMP查询报文。只要一个VLAN中至少 有一台主机回应IGMP查询,路由器就必须继续向该VLAN转发主机所属组播组的流量。

当主机想要离开一个组播组时,它可以忽略路由器定期发出的IGMP查询报文(称为"静离开"),也可以发送一个指定组的IGMPv2离开消息。

当IGMP Snooping监听到指定组的IGMPv2离开消息时,交换机向收到该消息的端口发送特定组查询消息,查询该端口上是否还有其他属于该组播组的主机。如果经过多次查询后,IGMP Snooping仍然收不到任何回应消息,则表明该端口上已经没有属于该组播组的主机,IGMP Snooping就会删除二层转发条目中相应的端口;如果收到回应消息,则不修改转发表。

## 5.1.3 快速离开

IGMP Snooping的快速离开功能是指:当交换机监听到指定组的IGMPv2离开消息时,不 发送查询消息,直接删除二层转发条目中相应的端口。

当要在某个VLAN中使能快速离开功能时必须注意,如果一个端口上有多台主机,其中一 台主机离开组播组时,该端口上同一组播组的其他主机将无法收到该组播组的组播流量。

# 5.2 配置IGMP Snooping

## 5.2.1 启用IGMP Snooping

步骤	命令	功能
1	ZXR10(config)# <b>ip igmp snooping</b>	全局启用IGMP Snooping
2	ZXR10(config-vlan)# <b>igmp snooping</b>	启用VLAN下的IGMP Snooping功能
3	ZXR10 (config) # <b>ip igmp snooping mode proxy vlan</b> < <i>vlan-id</i> >	启用IGMP Snooping代理
4	ZXR10(config-vlan)# <b>igmp snooping drop</b> < <i>group-address</i> > [ <b>num</b>	配置没有组播用户时IGMP Snooping
	< group-number > ]	是否广播组播数据

步骤	命令	功能
5	ZXR10(config-vlan)#igmp snooping fast-leave	配置组快速离开功能
6	ZXR10(config-vlan)#igmp snooping max-host-in-group <	配置组中最大用户数
	ip-address> [ <b>num</b> < num> ]	
7	ZXR10(config-vlan)#igmp snooping mode{ proxy   route	选择配置IGMP SNOOPING的功能
	transparent}	模式:代理模式、路由模式、透传
		模式
8	<pre>ZXR10(config-vlan) #igmp snooping fast-leave</pre>	配置VLAN下的组快速离开功能

# 5.2.2 配置代理查询器

通常情况下,组播网络中至少有一个组播路由器,定期发送IGMP查询报文。如果网络中没有组播路由器,可以配置代理查询器,用于发送IGMP查询报文。

步骤	命令	功能
1	ZXR10(config) # <b>ip igmp snooping querier</b> [ <b>vlan</b> < <i>vlan-id</i> > ]	启用代理查询器
2	ZXR10 (config) # <b>ip igmp snooping query-interval</b> < 30-65535>	配置代理查询器的查询间隔时间, 单位为秒
3	ZXR10 (config) # <b>ip igmp snooping query-response-interval</b> < 1-255>	配置代理查询器的最大查询响应时间,单位为100毫秒
4	ZXR10(config)# <b>igmp snooping prejoin</b> < <i>ip-address</i> > [ <b>num</b> < <i>number</i> > ]	配置IGMP SNOOPING的组预加入 功能,缺省不启用IGMP SNOOPING 组预加入功能
5	ZXR10(config)# <b>igmp snooping proxy-ip</b> < <i>ip-address</i> >	配置IGMP SNOOPING的代理主机IP 功能,缺省不启用IGMP SNOOPING 代理主机IP
6	ZXR10(config)# <b>igmp snooping querier</b>	配置IGMP SNOOPING的代理查询 器功能,当网络中没有组播路由器 时,代理组播路由器发送IGMP查询 报文。不设置代理查询功能

步骤	命令	功能
7	ZXR10(config)# <b>ip igmp snooping mode</b> { <b>proxy</b>   <b>route</b>   <b>transparent</b> }	批量选择配置VLAN下IGMP
	vlan< vlan-id>	SNOOPING的工作模式:代理模
		式、路由模式、透传模式。缺省
		VLAN下启用IGMP SNOOPING代
		理功能
8	ZXR10(config)#ip igmp snooping packet-manage { igmpv1   igmpv2	配置IGMP 报文的的v1、v2、v3版本
	igmpv3} { accept   discard   ignore}	的accept、discard、ignore功能

# 5.2.3 限制组播组

步骤	命令	功能
1	ZXR10(config-vlan)# <b>igmp snooping acl</b> < <i>1-99</i> >	对VLAN下的组进行ACL过滤
2	ZXR10(config-vlan)# <b>igmp snooping max-group-num</b> < 1-1024>	配置VLAN允许接入的最大组数
3	ZXR10(config)#multicast-limit { 256   512   1024}	配置二层组播条目数

# 5.2.4 配置静态IGMP Snooping

命令	功能
ZXR10(config-vlan) # <b>igmp snooping static</b> < <i>ip-address</i> > <b>interface</b> <	配置VLAN下的静态用户
port-name>	如果一个用户需要加入一个组播组,但
	没有运行IGMP, IGMP Snooping无法监
	听到,此时就可以进行静态配置
<pre>ZXR10 (config-vlan) #igmp snooping mrouter interface &lt; port-name&gt;</pre>	配置VLAN下的组播路由端口
	当没有配置PIM-Snooping或与不发送查
	询报文的组播路由器相连时使用
ZXR10 (config-vlan) #igmp snooping dynamic-learn-closedown [ interface	关闭VLAN下的组播学习路由端口
< port-name> ]	

# 5.2.5 设置IGMP Snooping时间参数

步骤	命令	功能
1	ZXR10(config-vlan)# <b>igmp snooping host-time-out</b> < 30-65535>	设置用户的老化时间,单位为秒

步骤	命令	功能
2	<pre>ZXR10(config-vlan) #igmp snooping last-member-query-interval &lt; 1-25&gt;</pre>	设置最后成员查询间隔,单位为秒
3	ZXR10(config-vlan) # <b>igmp snooping mrouter-time-out</b> < 30-65535>	设置路由端口老化时间,单位为秒

# 5.3 IGMP Snooping配置实例

如图5-2所示,端口fei\_1/1,fei\_1/3,fei\_1/5连接主机,端口fei\_3/1连接组播路由器,这些端口同属于VLAN 10。在交换机上启动IGMP Snooping功能。





# 5.4 IGMP Snooping的维护与诊断

步骤	命令	功能
1	ZXR10# <b>show ip igmp snooping vlan</b> < <i>vlan-id</i> >	显示指定VLAN的IGMP Snooping配
		置信息

步骤	命令	功能
2	ZXR10# <b>show ip igmp snooping mr-port-info</b>	显示与IGMP Snooping有关的路由端 口信息
3	<pre>ZXR10#show ip igmp snooping statistic { interface&lt; portname&gt;   np&lt; id&gt; ] }</pre>	显示IGMP报文的统计信息
4	<pre>ZXR10#clear igmp-snooping { all np &lt; id&gt;   interface { &lt; port-name&gt;   smartgroup &lt; smartgroup-id&gt; } }</pre>	清除IGMP报文的统计信息
5	ZXR10# <b>debug ip igmp-snooping</b>	对IGMP Snooping进行调试,跟踪相 关信息
6	ZXR10# <b>show ip igmp snooping</b>	显示相关的IGMP SNOOPING配置 信息
7	ZXR10# <b>show ip igmp snooping group</b> < <i>ip-address</i> > <b>vlan</b> < <i>vlan-id</i> >	显示某一组的配置和运行信息
8	ZXR10# <b>show ip igmp snooping iptv port-info</b> < <i>ip-address</i> > <b>vlan</b> < <i>vlan-id</i> >	显示某一可控组播用户信息
9	ZXR10# <b>show ip igmp snooping port-info vlan</b> < <i>vlan-id</i> >	显示与IGMP SNOOPING相关的 VLAN端口信息
10	ZXR10#show ip igmp snooping query	显示相关的IGMP SNOOPING查询 信息
11	ZXR10#show ip igmp snooping statistic [ clear] [ < port-name> ]	显示IGMP报文的统计信息

当需要显示所有统计数据时,使用**show ip igmp snooping statistic**命令,显示的统计信息 是累加的。当需要显示收到报文的相对速率时,使用**show ip igmp snooping statistic clear** 显示清零后的统计信息。

当需要显示指定端口收到的所有IGMP报文的统计信息时,使用show ip igmp snooping statistic < *port-name*> 命令。当需要显示某个端口收到报文的相对速率时,使用show ip igmp snooping statistic clear < *port-name*> 命令显示清零后的统计信息。

举例

跟踪IGMP Snooping数据包的收发过程。

```
ZXR10#debug ip igmp-snooping
ZXR10#
IGMP SNOOPING Rcv 224.1.1.1 Group Report Msg: From Vlan 1, Port fei_4/10
IGMP SNOOPING Rcv 224.1.1.1 Group Report Msg: From Vlan 1, Port fei_4/11
...
```



#### 本章包含如下主题:

• ]	ZESR配置	6-1
• ]	ZESS配置	6-6
• ]	双上行链路保护	6-7

# 6.1 ZESR配置

## 6.1.1 ZESR简介

ZESR是基于EAPS(RFC3619)协议的以太环网技术。ZESR技术允许网络管理员创建以 太网环,其方式类似于光纤分布式数据接口(FDDI)或SONET/SDH环。ZESR可以在 不到50毫秒时间内,从任何链路或节点故障中恢复过来。

如图6-1所示, S1被配置为"主节点",其他交换机被配置为"传输节点"。在主节点的两个端口中,一个为"主端口",另一个为"从端口"。初始时,从端口被阻塞,以避免环路。当某个传输节点发现自己相邻的某段链路出现问题时,将给主节点发送链路中断消息。主节点收到链路中断消息后,清空桥接表,将从端口打开,并给传输节点发送控制帧,通知它们清空自己的桥接表,此后的地址学习过程按普通方式重新开始。



主节点判断环故障的条件为收到LINK-DOWN帧或者检测到端口down(取消了HELLO超时机制)。Master节点收到LINK-DOWN帧后,认为环故障,进入Failed state,打开从端口,发送FLUSH-DOWN帧,更新FDB,其他节点收到FLUSH-DOWN帧后刷新FDB,进入Failed state。

- Master节点在Failed state时,收到LINK-DOWN帧无动作;
- Transit节点在Failed state时,收到FLUSH-DOWN帧无动作。

主节点判断环恢复的条件为超时未收到LINK-DOWN帧(取消了收到HELLO认为环恢复的机制),Master节点收到LINK-DOWN帧后,认为环故障,进入Failed state,打开从端口,发送FLUSH-DOWN帧,更新FDB,其他节点收到FLUSH-DOWN帧后刷新FDB,进入Failed state。

- Master节点在Failed state时,收到LINK-DOWN帧无动作;
- Transit节点在Failed state时,收到FLUSH-DOWN帧无动作。

Master节点检测到LINK-DOWN超时后,认为环恢复,进入Complete state,重新阻塞从端口,发送FLUSH-UP帧,更新FDB,其他节点收到FLUSH-UP帧后刷新FDB,进入Complete state,节点收到FLUSH-UP帧后打开阻塞端口。

Transit节点在Complete state时,收到FLUSH-UP帧无动作。

相邻节点之间增加了LINK-HELLO交互协议,用来检测相邻链路之间的链路单通、链路降质、链路跨传输设备等链路故障。

# 6.1.2 配置ZESR

步骤	命令	功能
1	ZXR10(config) # <b>zesr ctrl-vlan</b> < <i>vlan-id</i> > <b>protect-instance</b> < 0-16>	配置ZESR控制VLAN,将控制VLAN 与需要保护的生成树实例绑定
2	<pre>ZXR10(config) #zesr ctrl-vlan &lt; vlan-id&gt; major-level role { master   transit} &lt; port1&gt; &lt; port2&gt;</pre>	配置ZESR主环的节点角色,对于 主节点,配置的第一个端口为主端 口,第二个端口为从端口,对于传 输节点,两个端口的角色相同
3	ZXR10 (config) #zesr ctrl-vlan < vlan-id> level < 1-2> seg < 1-4> role master < port1> < port2>	配置ZESR从环的主节点,配置的第 一个端口为主端口,第二个端口为 从端口,负责发送hello包并诊断链 路完整
4	ZXR10 (config) #zesr ctrl-vlan < vlan-id> level < 1-2> seg < 1-4> role transit < port1> < port2>	配置ZESR从环的传输节点,两个端 口的角色相同,负责转发hello包
5	<pre>ZXR10(config) #zesr ctrl-vlan &lt; vlan-id&gt; level &lt; 1-2&gt; seg &lt; 1-4&gt; role edge=assistant &lt; port1&gt;</pre>	配置ZESR从环的edge-assistant节 点,edge-assistant标识该节点为边缘 辅助节点,负责将hello包进行回送
6	ZXR10 (config) #zesr ctrl-vlan < vlan-id> level < 1-2> seg < 1-4> role edge-control < port1>	配置ZESR从环的edge-control节点, edge-control标识该节点为边缘控制 节点,负责发送hello并检测链路完整
7	ZXR10(config)#zesr ctrl-vlan < vlanid> major—level preforward < 1-600> preup < 0-500>	配置节点的preforward和preup参数, 同一域的preforward应设置一致, preup值只在控制节点有效,规则要 求preforward – preup >=1
8	ZXR10(config)#zesr ctrl-vlan < vlanid> major—level hello < 1-6> fail < 3-18>	配置节点的hello和fail参数,分别 作为hello报文的发送周期和超时时 间,只在控制节点有效,规则要求 hello*3 <=fail
9	ZXR10(config) # <b>zesr restart-time</b> < 30-600>	配置节点的restart-time参数,表示 单板或设备重启后在参数时间内 将ZESR端口阻塞,对传输节点和 edge-assistant节点有效
10	ZXR10(config)# <b>show zesr</b>	查看ZESR配置信息

#### 6.1.3 ZESR配置实例

如图6-2所示,由三台交换机组成环网,各交换机上端口均在vlan10-20中;要求断开环 网时,S1的端口gei\_1/1为主用,gei\_1/2为备用。

#### 图6-2 ZESR配置实例



```
8908-1(config)#zesr ctrl-vlan 4000 major-level role master
gei_1/1 gei_1/2
```

#### S2的配置如下所示:

8908-2#vlan databale 8908-2(vlan)#vlan 10-20 8908-2(vlan)#vlan 4000 8908-2(vlan)#exit 8908-2(config)#interface gei 1/1 8908-2(config-if)#switchport mode trunk 8908-2(config-if)#switchport trunk vlan 10-20 8908-2(config-if)#switchport trunk vlan 4000 8908-2(config-if)#exit 8908-2(config)#interface gei 1/2 8908-2(config-if)#switchport mode trunk 8908-2(config-if)#switchport trunk vlan 10-20 8908-2(config-if)#switchport trunk vlan 4000 8908-2(config-if)#exit 8908-2(config)#spanning enable 8908-2(config) #spanning-tree mst configuration 8908-2(config-mstp)#instance 1 vlans 10-20 8908-2(config)#zesr ctrl-vlan 4000 protect-instance 1 8908-2(config)#zesr ctrl-vlan 4000 major-level role transit gei\_1/1 gei\_1/2

```
S3的配置与S2相同。
```

#### S1和S2上查看配置结果,如下所示:

```
8908-1(config)#show zesr
ZESR domain:
ctrl vlan
           4000
           gei_1/1(Primary) gei_1/2(Secondary)
ports
node type
           MASTER
                         //MAC地址学习方式
mode
            standard
                   //环的当前工作状态,
ring
            Up
如果配置错误可能导致环不能正常up。
switch times 5
                     //环网切换次数,
```

```
链路发生故障并恢复算两次
                   //health帧发送时间间隔
healthtime: 1ms
failtime: 3ms
                   //health帧超时时间
8908-1(config)#show zesr brief
ctrl-vlan: 4000 protectinstance: 1
level seg role port
                      port level-state switch-times
        master gei 1/1(P) gei 1/2(S) up
major
                                               1
8908-2(config)#show zesr brief
ctrl-vlan: 4000 protectinstance: 1
level seg role port port level-state switch-times
major transit gei_1/1(P) gei_1/2(S) up
                                          1
```

# 6.2 ZESS配置

## 6.2.1 ZESS简介

ZESS是ZTE以太网智能切换技术,功能描述如下。

如图6-3所示,节点1支持ZESS功能,其中端口1为主端口,端口2为从端口。当节点1检测到主端口、从端口都为UP时,阻塞从端口的数据转发功能;当节点1检测到主端口发生DOWN时,阻塞主端口的数据转发功能,打开从端口的数据转发功能;当节点1检测到主端口恢复为UP时,有反转和非反转模式,在反转模式时,打开主端口,重新阻塞从端口,在非反转模式时,保持主端口为阻塞,从端口为放开状态。另外,ZESS在切换时,要更新被阻塞端口的FDB。





## 6.2.2 配置ZESS

步骤	命令	功能
1	ZXR10 (config) #zess domain < 1-4> member primary < port-name>	创建ZESS域
	secondary < port-name>	
2	ZXR10 (config) #zess domain < 1-4> protect-instance < 0-16>	绑定ZESS域和生成树实例
3	ZXR10 (config) # <b>zess domain</b> < <i>1-4</i> > <b>preup</b> < <i>0-600</i> >	设置preup时间
4	ZXR10(config) #zess domain < 1-4> mode { revertive	设置ZESS模式
	non_revertive}	
5	ZXR10#show zess { brief   domain < 1-4> }	查看ZESS配置结果
6	ZXR10#clear zesr-switchtimes all	清除ZESS切换时间

# 6.3 双上行链路保护

# 6.3.1 双上行链路保护简介

在城域网的核心网与骨干网连接的上行链路中,一般一台交换机有两个上行端口连接至两台BRAS或者SR,这样可以通过ZESS来实现双上行保护。这种连接方式实现了上行链路、SR或者BRAS的保护,但存在上行到BRAS或者SR的交换机单点故障风险。在实际组网中出于安全的考虑,两个连接到相同SR或BRAS设备的上行出口分别分布在两台交换机上,这样即实现双上行链路保护功能。

如图6-4所示的网络中,环网上两台交换机(S1,S4)各出一条上行链路到SR和BRAS, 实现到SR和BRAS的上行链路保护。假设交换机S1到SR的链路中断,此时该链路的流量 会自动经交换机S4到SR。实现双上行链路保护后,当某条上行链路故障时,系统可以在 50ms以内完成切换。



#### 图6-4 双上行链路故障保护拓扑图

# 6.3.2 双上行链路保护配置实例

图6-5为典型的双上行拓扑图,其中节点ZXR10-1、ZXR10-2和ZXR10-3虚拟一个主环;节点ZXR10-2、ZXR10-3和ZXR10-4组成一个level 1 seg 1的从环。


节点ZXR10-1为一个普通交换机,主用功能为透传数据包,只需要配置VLAN信息,以及关闭端口的广播和未知单播抑制。

节点ZXR10-2为上行控制节点普通交换机,配置如下:

```
zesr ctrl-vlan 4001 protect-instance 1
zesr ctrl-vlan 4001 major-level role zess-master gei_2/2 gei_2/1
/*配置zess-master角色,需要注意的是Secondary端口决定了阻塞位置,因此Secondary端口不能
配置在ZXR10-2和ZXR10-3之间链路对应端口上,否则阻塞端口错误*/
zesr ctrl-vlan 4001 level 1 seg 1 role edge-assistant gei_2/3
/*配置普通ZESR的边界节点角色*/
```

节点ZXR10-3为上行协助控制节点普通交换机,配置如下:

zesr ctrl-vlan 4001 protect-instance 1 zesr ctrl-vlan 4001 major-level role zess-transit gei\_3/2 gei\_3/1 /\*配置zess-transit角色,需要注意的是Primary端口决定了节点发送hello帧的方向,因此 Primary端口一定要配置在zxR10-2和zxR10-3之间链路对应端口上,否则配置错误\*/ zesr ctrl-vlan 4001 level 1 seg 1 role edge-assistant gei 3/3 /\*配置普通ZESR的边界节点角色\*/

节点ZXR10-4为ZESR低层次节点,配置如下:

zesr ctrl-vlan 4001 protect-instance 1 zesr ctrl-vlan 4001 level 1 seg 1 role master gei\_4/2 gei\_4/1 /\*配置普通ZESR的低层次主节点角色\*/

# 了 以太网OAM配置

## 本章包含如下主题:

• 以太网OAM简介	7-1
• 配置以太网OAM	7-3
• 配置CFM	7-5
• OAM链路控制事件配置实例	7-9
• 以太网OAM的维护与诊断	7-11
• CFM的维护与诊断	7-14

# 7.1 以太网OAM简介

## Ethernet OAM的发展

随着近年来以太网技术的快速开展,以太网组网在网络建设中的比重逐渐增加,以太网的网络规模也不断的增多,从接入、汇聚到骨干网中都大量使用了以太网来代替ATM等网络设备。

同时IP承载网络向着多业务、宽带化方向的发展,传统的以太网没有电信级管理能力, 不能检测、通告或隔离二层网络故障,而采用SNMP协议的网管也只能管理链路与设备 状态,不能检测用户业务的端到端连接性能和状态,当网络发生故障时,无法定位或者 定位不够迅速。而且网络设备的大量应用,网络设备管理者更加关注以太网设备的OAM 功能。在此背景下产生了一系列已标准的或出于草案阶段的技术,其中几个主要的关于 以太网OAM的文献有:

- IEEE 802.3ah ( Operations, Administration, and Maintenance-OAM )
- IEEE 802.1ag ( Connectivity Fault Management-CFM )
- ITU-T Y.1731 ( OAM functions and mechanisms for Ethernet based networks )

# 主要协议介绍

IEEE 802.3ah,操作、管理及维护标准是IEEE的正式标准,它主要针对"链路"级别的管理,可以对网络中的点到点(或虚拟点到点)以太网链路进行监控和故障处理。该协议在故障比较容易发生的地方,如网络用户最后一公里,对于这些点的连接管理有重要的意义。

IEEE 802.1ag, 连接故障管理(CFM)功能,该标准目前是IEEE的草案。它是主要针对 "服务"级别的管理,为网络提供容易和快捷的故障发现、检测和管理的功能。可以有 效的对虚拟桥局域网进行检查、隔离和连接性故障报告。

ITU-Y 1731,操作、管理及维护是ITU的建议草案,主要是对IEEE 802.3ah、IEEE 802.1ag 进行了一定的增强,全面的扩充了在链路的故障检测、监控和隔离的方法。本草案只提 出了一些要求,具体的实现还是要依靠其他的标准实体的功能。

#### 功能列表

ZXR10 6900系列交换机支持IEEE 802.3ah与IEEE 802.1ag协议,主要支持功能如表7-1所示。

协议	功能
IEEE 802.3ah	Ethernet OAM对象管理
	Ethernet OAM发现
	Ethernet OAM包收发
	Ethernet OAM远端失效指示
	Ethernet OAM链路监控
	Ethernet OAM诊断信息的事件通知机制
	Ethernet OAM厂家扩展功能
	Ethernet OAM SNMP网管
	Ethernet OAM告警和日志

	田栄
- 6- 1	T/\

协议	功能
	CFM对象管理
	CFM组播包发送与接收
	CFM单播包发送与接收
IEEE 802.1ag	CFM协议报文的透传
	CFM故障探测
	CFM链路跟踪
	CFM环回功能
	CFM故障通知机制
	CFM厂家扩展功能
	CFM SNMP网管
	CFM告警和日志
	CFM与ITU-T Y1731兼容

# 7.2 配置以太网OAM

# 1. 开启/关闭全局链路OAM功能

命令	功能
ZXR10 (config) #set ethernet-oam { enable   disable}	在全局配置模式下,开启/关闭全局链
	路OAM功能

# 2. 开启/关闭指定端口链路的OAM功能

命令	功能
ZXR10(config)#interface < portname>	进入端口配置模式
ZXR10(config-if) #set ethernet-oam { enable   disable}	开启/关闭该端口链路的OAM功能

# 3. 配置链路以太网OAM的OUI信息

命令	功能
ZXR10 (config) <b>#set ethernet-oam oui</b> < <i>list</i> >	在全局配置模式下,设置链路以太网
	OAM的OUI信息

命令	功能
ZXR10 (config) # <b>interface</b> < <i>portname</i> >	进入端口配置模式
ZXR10 (config-if) #set ethernet-oam remote-loopback { start   stop}	开启/关闭该端口链路以太网OAM的
	远端环回功能

# 5. 配置链路以太网OAM的环回超时时间

命令	功能
ZXR10 (config) #set ethernet-oam remote-loopback timeout < 1-10>	在全局配置模式下,设置远端环回的超
	时时间,单位秒,默认时间为3秒

## 6. 配置端口普通属性

命令	功能
ZXR10 (config) # <b>interface</b> < <i>portname</i> >	进入端口配置模式
<pre>ZXR10(config-if) #set ethernet-oam period &lt; level-value&gt; timeout &lt; time&gt;</pre>	配置端口普通属性
mode { active   passive}	

## 7. 开启/关闭端口链路的以太网OAM链路检测功能

命令	功能
ZXR10 (config) # <b>interface</b> < <i>portname</i> >	进入端口配置模式
ZXR10 (config-if) #et ethernet-oam link-monitor { enable   disable}	开启/关闭该端口链路的以太网OAM
	链路检测功能

# 8. 配置端口错误符号链路事件参数

命令	功能
ZXR10 (config) #set ethernet-oam link-monitor symbol-period threshold <	配置端口错误符号链路事件参数
1-65535> window < 1-65535>	

## 9. 配置端口错误帧链路事件参数

命令	功能
ZXR10 (config-if) set ethernet-oam link-monitor frame threshold <	配置端口错误帧链路事件参数
1-65535> window < 1-60>	

ZTE中兴

### 10. 配置端口错误帧周期链路事件参数

命令	功能
ZXR10(config)#interface < portname>	进入端口配置模式
ZXR10 (config-if) #set ethernet-oam link-monitor frame-period threshold	配置端口错误帧周期链路事件参数
< 1-65535> window < 1-600000>	

### 11. 配置端口错误帧秒统计链路事件参数

命令	功能
ZXR10(config-if)#set ethernet-oam link-monitor frame-seconds	配置端口错误帧秒统计链路事件参数
threshold < 1-900> window < 10-900>	

# 7.3 配置CFM

# 1. 开启/关闭全局CFM功能

命令	功能
<pre>ZXR10(config) #cfm &lt; enable   disable&gt;</pre>	在全局配置模式下,开启/关闭全局
	CFM功能,默认关闭该功能

#### 2. 创建/删除维护域

命令	功能
<pre>ZXR10(config)#cfm { create   delete} MD session &lt; session-id&gt; name &lt;</pre>	在全局配置模式下,创建/配置一个维
<i>md-name&gt;</i> <b>level</b> < <i>level-value&gt;</i>	护域

# 3. 进入维护域

命令	功能
<pre>ZXR10(config) #cfm MD session &lt; session-id&gt;</pre>	在全局配置模式下,进入维护域

## 4. 创建/删除维护联合

命令	功能
ZXR10(config-md)#MA { create   delete} session < MA-session-id> name	在MD配置模式下,创建/删除维护联合
< MA-name>	

5. 进入维护联合配置模式

命令	功能
ZXR10(config-md)# <b>MA session</b> < <i>MA-session-id</i> >	在MD配置模式下,进入维护联合配置
	模式

## 6. 配置MA的主VLAN

命令	功能
ZXR10(config-ma)# <b>primary VLAN</b> < <i>vlan-id</i> >	在MA配置模式下,配置MA的主VLAN

## 7. 配置MA CCM报文的快速/慢速标识

命令	功能
ZXR10(config-ma)# <b>speed</b> < fast/slow>	在MA配置模式下,配置MA CCM报文
	的快速/慢速标识

# 8. 配置MA中CCM发送的时间间隔

命令	功能
ZXR10(config-ma)# <b>CCM timer interval</b> < <i>integer</i> >	在MA配置模式下,配置MA中CCM发
	送的时间间隔

### 9. 创建/删除MEP

命令	功能
ZXR10(config-ma)#{ create   delete} [ < mep-id>   < session-id>   all]	在MA配置模式下,创建/删除MEP

## 10. 创建/删除MIP

命令	功能
<pre>ZXR10(config-ma)#{ create   delete} MIP session &lt; session-id&gt; name &lt;</pre>	在MA配置模式下,创建/删除MIP
string>	

#### 11. MEP管理状态设置

命令	功能
<pre>ZXR10(config-ma)#MEP &lt; med-id&gt; state { enable   disable}</pre>	在MA配置模式下,设置MEP管理状态

## 12. MEP发送CCM功能设置

命令	功能
<pre>ZXR10(config-ma)#MEP &lt; mep-id &gt; CCM-send { enable   disable}</pre>	在MA配置模式下,设置MEP发送CCM
	功能

# 13. 配置MEP的优先级

命令	功能
ZXR10(config-ma)# <b>MEP</b> < mep-id> priority < value>	在MA配置模式下,配置MEP的优先级

## 14. 定义MEP错误检测的优先级

命令	功能
ZXR10(config-ma)# <b>MEP</b> < mep-id> alarm-lowest-pri < value>	在MA配置模式下,定义MEP错误检测
	的优先级

# 15. 清除所有的CFM配置

命令	功能
ZXR10(config)#clear pbt-cfm	在全局配置模式下,清除所有的CFM
	配置

# 16. 触发LTM

命令	功能
ZXR10#cfm ltm md < md-session-id> ma < ma-session-id > smep-id <	在特权模式下,在本地的一个MEP上发
$smep-id > \{ dmep-id < dmep-id >   dmep-mac < dmep-mac >   dmip-mac < dmep-mac >   dmip-mac < dmep-mac >   dmip-mac < dmep-mac >   dmip-mac >   dmi$	起另外一个MP的链路检测消息。
$dmip-mac> \} [-t   -w]$	

# 17. 触发LBM

命令	功能
ZXR10#cfm lbm md < md-session-id> ma < ma-session-id> smep-id <	在特权模式下,在本地的一个MEP上发
$smep-id> \{ dmep-id < dmep-id>   dmep-mac < dmep-mac>   dmip-mac < dmep-mac>   dmip-mac < dmep-mac>   dmip-mac < dmep-mac>   dmip-mac < dmep-mac>   dmip-mac>   d$	起另外一个MP的环回消息。
$dmip-mac> \} [-c   -d   -t]$	

# 18. 读LTR(Linktrace Reply)的命令

命令	功能
ZXR10(config)#cfm ltr-read trans-id < <i>ltm-trans-id</i> >	显示某个LTM的响应的路径树

## 19. 配置MA的保护模式

命令	功能
ZXR10(config-ma) #protect type { vlan   link}	在MA配置模式下,配置MA的保护模式。

## 20. 配置MEP检测功能的开启/关闭

命令	功能
<pre>ZXR10(config-ma)#mep &lt; mep-id&gt; ccm-check { enable   disable}</pre>	在MA配置模式下,配置MEP检测功能
	的开启/关闭

# 21. 配置MEP复杂处理标记

命令	功能
<pre>ZXR10(config-ma)#mep &lt; mep-id&gt; complex-flag { enable   disable}</pre>	在MA配置模式下,配置MEP复杂处理
	标记

## 22. CFM接口MAC地址设置

命令	功能
ZXR10(config-if)# <b>cfm-mac</b> < <i>mac-address</i> >	在接口配置模式下,设置CFM接口
	MAC地址

# 23. 将一个MEP与端口或隧道相关联

命令	功能
<pre>ZXR10(config-ma) #assign MEP &lt; mep-id &gt; to { interface &lt; port-name &gt; }</pre>	在MA配置模式下,将一个MEP与端口
	或隧道相关联

# 24. 将一个MIP和端口相关联

命令	功能
ZXR10(config-ma)#assign MIP < session-id> interface < port-name>	在MA配置模式下,将一个MIP和端口
	相关联

## 25. 调试CFM功能模块

命令	功能
ZXR10# <b>Debug cfm pkt [ megid   all   { md</b> < md-index> ma < ma-index>	在特权模式模式下,调试CFM功能模块
mep < <i>mep-id</i> > } ] [ direction { send   rcv   all} > ] { pkt-nums < <i>inter</i> > }	

# 7.4 0AM链路控制事件配置实例

# 实例描述及组网图

OAM监视功能能够对链路接收端的异常帧按照特定方式通告给本地。该功能是基于OAM 发现成功的基础上实现的。用户通过console口登录交换机,配置OAM功能,并使能对接端口的OAM功能后,再使能对接端口的链路监视,可以检测到链路中的错误符号和错误 帧,并通告给本地交换机。

#### 图7-1 链路控制事件组网



### 交换机配置

#### • 交换机A的配置

```
ZXR10(config)#set ethernet-oam enable
ZXR10(config)#interface gei_1/2
ZXR10(config-if)#set Ethernet-oam enable
```

### • 交换机B的配置

```
ZXR10(config)#set ethernet-oam enable
ZXR10(config)#interface gei_1/1
ZXR10(config-if)#set ethernet-oam enable
ZXR10(config-if)#set ethernet-oam link-monitor enable
ZXR10(config-if)#set ethernet-oam link-monitor symbol-period
threshold 10 window 10
ZXR10(config-if)#set ethernet-oam link-monitor frame threshold
10 window 20
```

```
ZTE中兴
```

```
ZXR10(config-if)#set ethernet-oam link-monitor frame-period
threshold 5 window 1000
ZXR10(config-if)#set ethernet-oam link-monitor frame-seconds
threshold 10 window 30
ZXR10(config-if)#show ethernet-oam gei_1/1 link-monitor
 Link Monitoring of Port: 1
 Errored Symbol Period Event:
   Symbol Window : 10 (million symbols)
   Errored Symbol Threshold : 10
   Total Errored Symbols : 0
   Local Total Errored Events : 0
   Remote Total Errored Events : 0
  Errored Frame Event:
   Period Window : 20(s)
   Errored Frame Threshold : 10
   Total Errored Frames : 0
   Local Total Errored Events : 0
   Remote Total Errored Events : 0
  Errored Frame Period Event:
   Frame Window : 1000(ten thousand frames)
   Errored Frame Threshold : 5
   Total Errored Frames
                         : 0
   Local Total Errored Events : 0
   Remote Total Errored Events : 0
  Errored Frame Seconds Event:
   Errored Seconds Window : 30(s)
   Errored Seconds Threshold : 10(s)
   Total Errored Frame Seconds : 0(s)
   Local Total Errored Frame Seconds Events : 0
```

Remote Total Errored Frame Seconds Events :  $\ensuremath{\texttt{0}}$ 

## 配置关键点

链路监视事件分四类:错误符号监视事件、错误帧监视事件、错误帧周期监视事件以及 错误帧秒统计监视事件。查看端口的链路监视情况时,每类事件下都可以看到相应的错 误符号和错误帧的统计,以及本端和远端链路事件的统计。

# 7.5 以太网OAM的维护与诊断

命令	功能
ZXR10(config) # <b>show ethernet_oam</b>	显示链路以太网OAM的全局信息
ZXR10(config) # <b>show ethernet_oam</b> < <i>portname</i> > <b>discovery</b>	显示指定端口以太网OAM的发现状态
ZXR10(config) # <b>show ethernet_oam</b> < <i>portname</i> > <b>link-monitor</b>	显示指定端口以太网OAM的链路事件
	信息
<pre>ZXR10(config) #show ethernet_oam &lt; portname&gt; statistics</pre>	显示指定端口以太网OAM的管理帧信息

#### 举例

### 显示链路以太网OAM的全局信息,如下所示:

ZXR10(config)#show ethernet-oam

```
Ethernet Oam : disabled
Link Monitor : support
Mib Retrieval : nonsupport
Remote LoopBack : support
Event Time Stamp : 10*100(ms)
Remote LoopBack Timeout : 3(s)
Local OUI : 00-15-EB
```

## 显示指定端口以太网OAM的发现状态,如下所示:

```
ZXR10 (config)#show ethernet-oam gei_1/1 discovery
PortId 1: ethernet oam disabled
Local DTE
-----
Config:
Mode : active
Period : 10*100(ms)
Link TimeOut : 5(s)
Unidirection : nonsupport
```

```
PDU max size : 1518
Status:
 Parser : forward
 Multiplexer : forward
 Stable
           : no
 Discovery : undone
 Loopback
            : off
 PDU Revision : 0
Remote DTE
_____
Config:
 Mode : passive
 Link Monitor : nonsupport
 Unidirection : nonsupport
 Remote Loopback : nonsupport
 Mib Retrieval : nonsupport
 PDU max size : 0
Status:
 Parser : forward
 Multiplexer : forward
 Stable
           : no
 Mac Address : 00.00.00.00.00.00
 PDU Revision : 0
```

# 显示指定端口以太网OAM的链路事件信息,如下所示:

```
ZXR10 (config)#show ethernet-oam gei_1/1 link-monitor
Link Monitoring of Port: 1
Link Monitoring disabled
Errored Symbol Period Event:
Symbol Window : 1(million symbols)
Errored Symbol Threshold : 1
Total Errored Symbols : 0
Local Total Errored Events : 0
Remote Total Errored Events : 0
```

Errored Frame Event:

```
Period Window : 1(s)
 Errored Frame Threshold : 1
  Total Errored Frames : 0
 Local Total Errored Events : 0
  Remote Total Errored Events : 0
Errored Frame Period Event:
  Frame Window : 100(ten thousand frames)
 Errored Frame Threshold : 1
 Total Errored Frames : 0
 Local Total Errored Events : 0
 Remote Total Errored Events : 0
Errored Frame Seconds Event:
 Errored Seconds Window : 60(s)
 Errored Seconds Threshold : 1(s)
 Total Errored Frame Seconds : 0(s)
 Local Total Errored Frame Seconds Events : 0
  Remote Total Errored Frame Seconds Events : 0
```

## 显示指定端口以太网OAM的管理帧信息,如下所示:

```
ZXR10 (config)#show ethernet-oam gei_1/1 statistics
   OAMPDU Counters of Port: 1
   TransmitInformation : 0
   ReceiveInformation : 0
   TransmitLoopbackControl : 0
   ReceiveLoopbackControl : 0
    TransmitVariableRequest : 0
    ReceiveVariableRequest : 0
   TransmitVariableResponse : 0
    ReceiveVariableResponse : 0
    TransmitUniqueEventNotification
                                      : 0
    ReceiveUniqueEventNotification
                                   : 0
    TransmitDuplicateEventNotification : 0
    ReceiveDuplicateEventNotification : 0
    TransmitZTESpecific : 0
    ReceiveZTESpecific : 0
```

TransmitUnsupported : 0 ReceiveUnsupported : 0

# 7.6 CFM的维护与诊断

命令	功能
<pre>ZXR10(config) #show MD { all   session &lt; session-id&gt; }</pre>	显示设备上配置的MD
<pre>ZXR10(config) #show MA { all   session &lt; MA-session-id&gt; } MD &lt; MD-session-id&gt;</pre>	显示MA的配置
<pre>ZXR10(config) #show MEP { mep-id   all} MD &lt; MD-session-id&gt; MA &lt; MA-session-id&gt;</pre>	显示MEP的配置



#### 本章包含如下主题:

EPON OLT简介	8-1	
• 配置EPON OLT	8-3	
• EPON OLT配置实例	8-20	

• EPON OLT的维护与诊断 8-22

# 8.1 EPON OLT简介

## PON的发展

随着网络技术的发展,骨干网和局域网的速率均有大幅度的提高,因而作为骨干网和局 域网或家庭用户间桥梁的"最后一英里"成为限制网络发展的瓶颈。

原有的接入技术如T1/E1或SONET/SDH费用过高,Cable Modem等光接入技术的网络建设成本高昂,而无线接入技术受到环境和安全性制约,也不宜推广。

PON(Passive Optical Network)无源光网络,作为一种接入技术,可以保证用户获得较大接入带宽,并且有效的控制网络建设成本,因而发展迅速。

# PON介绍

光纤接入分为两大类:

- 有源光网络(AON, Active Optical Network)
- 无源光网络(PON, Passive Optical Network)

PON是单纯的物理介质网络,局端与终端之间不需要有源设备的支持。这样可以有效避免外部设备的电磁干扰,降低线路和设备的故障率,提高系统可靠性,同时可节省维护成本。

PON的业务透明性较好,适用于较多的制式和速率的信号。基于PON的技术主要有 APON/BPON、GPON、EPON/GEPON几种,它们的主要差异在于采用了不同的二层技术。

# EPON简介

为更好适应IP业务,第一英里以太网联盟(EFMA)在2001年初提出了在二层用以太网取 代ATM的EPON技术,IEEE 802.3ah工作小组对其进行了标准化。2004年6月,IEEE802.3 EFM工作组发布了EPON标准—IEEE 802.3ah(2005年并入IEEE 802.3-2005标准)。用于 解决网络接入的"最后一英里"问题。

EPON是承载在PON网络上的以太网,支持1.25Gbps对称速率,保留了PON易于部署和维护的特点。EPON无需复杂的协议,光信号就可以在局端与终端之间准确地传送。EPON继承了以太网的可扩展性强、对IP数据业务适配效率高等优点,同时支持高速Internet接入、语音、IPTV、TDM专线甚至CATV等多种业务综合接入,并具有很好的QoS保证和组播业务支持能力。

EPON采用成熟的全双工以太技术,上行采用TDMA(时分复用多址接入方式),下行使用TDM(Time Division Multiplex and Multiplexer,时分复用和复用器)。ONU在自己的分时内发送数据报,因此与其他ONU不发生碰撞,从而充分利用带宽。EPON系统如图8-1所示。



图8-1 EPON系统参考图

## EPON的特点

- EPON网络内所有的承载设备均为无源设备,不需要电力网络支持;
- 采用了波分复用技术,上下行流量均在同一光纤上传播,节省光缆;
- 基于以太网分层结构, EPON工作于物理层和逻辑链路层, 对上层业务和协议完全透明;
- 本身作为一种点到多点接入方式,可以有效的节省汇聚侧接口数目。

### EPON相关概念

- OLT: Optical Line Terminal, EPON中上行方向上的汇聚节点,是局侧的光线路终端;
- ONU: Optical Network Unit, 用户侧光网络单元接入节点。

### EPON的网络应用

按照ONU 在接入网中所处的位置不同, EPON 系统可以有几种网络应用类型:

- 光纤到交接箱(FTTCab)
- 光纤到楼宇/分线盒(FTTB/C)
- 光纤到家庭用户(FTTH)
- 光纤到公司/办公室(FTTO)

# 8.2 配置EPON OLT

# 8.2.1 配置0LT接口

1. 进入OLT接口配置模式

命令	功能
ZXR10(config) #interface epon-olt_< slot> /< oltid>	进入OLT接口配置模式

参数说明:

参数	描述
< slot>	EPON单板的槽位号
< oltid>	OLT接口号

# 2. 配置EPON OLT接口描述信息

命令	功能
<pre>ZXR10(config-if)#description &lt; LINE &gt;</pre>	配置接口描述信息

参数	描述
< LINE >	OLT名称,范围1~100个字符

# 3. 将指定ONU设备绑定到当前EPON OLT接口下

命令	功能
<pre>ZXR10(config-if)#onu &lt; onuid&gt; type &lt; type-name&gt; mac &lt; macAddr&gt;</pre>	将指定ONU设备绑定到当前EPON
	OLT接口下

使用no onu解除绑定。

参数说明:

参数	描述
< onuid>	ONU的设备号,范围1~32
< type-name>	ONU型号名称
< macAddr>	ONU MAC地址

ONU型号支持列表:

名称	ZTE-D400; ZTE-D402; ZTE-D420; ZTE-D421; ZTE-D422; ZTE-F401; ZTE-F425;
	ZTE-F429; ZTE-F430; ZTE-F435; ZTE-F500; ZTE-F820

### 4. 创建、删除ONU子接口

命令	功能
<pre>ZXR10(config) #interface epon-olt_&lt; slot&gt; /&lt; oltid&gt; .&lt; onuld&gt;</pre>	创建/进入ONU子接口配置模式

#### 使用no interface epon-olt\_< slot> /< oltid> .< onuId> 删除指定接口

参数说明:

参数	描述
< slot>	EPON单板的槽位号
< oltid>	OLT端口号
< onuId>	ONU子接口号,范围1-32

# 5. 配置EPON ONU接口描述信息

命令	功能
ZXR10(config-if)#description < LINE>	配置接口描述信息

参数	描述
< LINE>	ONU名称,范围1~100个字符

# 8.2.2 配置EPON全局参数

1. 进入EPON全局配置模式

命令	功能
ZXR10(config) #epon	进入EPON全局配置模式

2. 开启/关闭自动鉴权模式

命令	功能
<pre>ZXR10(config-epon) #auto-authentication card &lt; slot&gt; { enable   disable}</pre>	在EPON全局配置模式下,设置EPON
	单板是否需要执行自动鉴权模式, slot
	为槽位号,默认为关闭

如果采用的是自动鉴权模式,ONU上电后立即自动注册加入EPON系统,不需要进行ONU端口和ONU MAC地址绑定即可直接与OLT进行数据转输。

如果采用的是非自动鉴权模式,EPON系统需要手工对ONU端口和ONU MAC地址 绑定,绑定后方可与OLT进行数据传输。

3. 配置ONU软件认证方式

命令	功能
<pre>ZXR10(config-epon) #software-authentication card &lt; slot&gt; mode { mac}</pre>	配置ONU软件认证方式,基于MAC或
	根据序列号认证,默认基于MAC

# 4. 配置ONU硬件认证功能

命令	功能
ZXR10(config-epon)#hardware-authentication card < <i>slot</i> > { enable	开启/关闭ONU硬件认证功能,默认
disable}	为开启

使用**no hardware-authentication card** < *slot*> 取消硬件认证。

5. 配置OLT DBA

命令	功能
ZXR10(config-epon)# <b>dba epon-olt_</b> < <i>slot&gt; /&lt; oltid&gt;</i> [ .< <i>onuid&gt;</i> ] {	配置指定接口的动态带宽分配方法
Archimedes   thales   plato}	

为了实时地改变PON中各ONU上行带宽,根据带宽状态和ONU需求动态分配ONU 上行带宽,EPON系统的DBA算法支持公平性机制,能够保证剩余带宽按照三种方式 进行公平分配。

6. 配置OLT加密算法

命令	功能
ZXR10 (config-epon) #encrypt algorithm epon-olt_< slot> /< oltid>	配置ONU加密功能的属性,包括加密
[.< onuid>] { aes   triple-churning [ key-update-period < integer> [	方式、密钥更新时间、更新超时时间
<pre>churning-timer &lt; integer&gt; ] ] }</pre>	

使用no encrypt algorithm epon-olt\_< slot> /< oltid> 取消加密功能。

只有加密方式为三重搅动时,需要设置密钥更新时间和密钥更新无应答超时时间。 参数说明:

参数	描述
< slot>	槽位号, 1~12
< oltid>	OLT端口号
key-update-period < integer>	密钥更新时间,单位s,1~255,默认10
triple-churning	三重搅动加密方式
churning-timer < integer>	密钥更新无应答超时时间,单位s,
	1~255

## 7. 开启/关闭指定OLT端口的激光器控制开关

命令	功能
<pre>ZXR10 (config-epon) #laser { enable   disable} epon-olt_&lt; slot&gt; /&lt; oltid&gt;</pre>	开启/关闭指定OLT端口的激光器控制 开关

## 8. 配置ONU间桥接互通

命令	功能
ZXR10 (config) #interface epon-olt_< slot> /< oltid>	进入OLT端口配置模式

命令	功能
ZXR10(config-if)# <b>bridge-port</b> { <b>enable</b>   <b>disable</b> } <b>onu</b> < <i>onu_id</i> >	开启指定ONU间的桥接互通功能

#### 参数说明:

参数	描述
< slot>	槽位号, 1~12
< oltid>	OLT端口号
< onu_id>	ONU设备的编号,范围0~31个字符

## 9. 配置光路自动测量功能

命令	功能
ZXR10(config-if)# <b>optics measure low</b> < <i>lowdb</i> > <b>high</b> < <i>highdb</i> >	在OLT端口配置模式下,设置OLT接口
	测量和告警的下限功率和上限功率

OLT支持对其接收到的来自每个ONU的上行光功率的测量功能,测量精度±1dB。当OLT接受到的来自某个ONU的上行光功率过低(低于标准规定的OLT灵敏度上限) 或者过高(高于标准规定的OLT过载光功率下限),则OLT应产生相应的光功率越限告警。

参数说明:

参数	描述
< lowdb>	标准低功率(单位db)
< highdb>	标准高功率(单位db)

## 10. OLT诊断与预测功能

命令	功能
ZXR10(config-if) #optics diagnosis interval < seconds>	在OLT端口配置模式下, 配置诊断预测
	功能时间间隔,单位s

使用命令no optics diagnosis取消该功能。

OLT支持基于对PON接口下ONU的上行光功率的测量实现光链路的故障诊断和性能 预测功能:

故障诊断是指根据PON接口上接受到的各ONU的光功率分析光链路的衰减等指标是否正常,并提供一定的链路故障的判断功能;

- 性能预测是指通过对接受到的来自每个ONU的上行光功率进行定期的测量和分析,提供对光链路衰减或光模块性能的预测。
- 11. 配置OLT协议报文透传控制功能

命令	功能
ZXR10(config-if)#epon-protocol-protect mode { DHCP   IGMP	在OLT端口配置模式下,配置OLT协议
<b>BPDU</b> } { enable   disable}	报文透传控制功能

## 12. 配置LLID间的广播关闭功能

命令	功能
ZXR10(config-if)#packet-limit { broadcast-limit   unknowcast-limit} {	在OLT端口配置模式下,配置对广播
disable   enable}	包和未知组播包的抑制,可关闭LLID
	之间的广播

# 8.2.3 配置0NU本地管理

## 1. 配置ONU的最大RTT值

命令	功能
ZXR10 (config) # <b>interface epon-olt_</b> < <i>slot&gt; /&lt; oltid&gt;</i>	进入OLT端口配置模式
ZXR10(config-if)# <b>onu max-rtt</b> < 1000~25000>	配置ONU的最大RTT值,使各ONU
	都能成功进行注册

## 使用no onu max-rtt删除配置的最大值。

参数说明:

参数	描述
< 1000~25000>	往返时间

#### 2. 将ONU接口与指定类型的ONU的MAC地址绑定

命令	功能
ZXR10(config-if)# <b>onu bind onuid</b> < <i>onuid</i> > <b>type</b> < <i>type-name</i> > { <b>mac</b> <	在OLT端口配置模式下,将ONU端口
$macAddr >   \mathbf{sn} < \mathbf{sn} > \}$	与指定类型的ONU的MAC地址进行绑
	定,只有绑定之后OLT才能与ONU通
	信,并配置ONU

## 参数说明:

参数	描述
< onuid>	ONU设备号,范围1~64
< type-name>	ONU设备型号名称
< macAddr>	ONU设备的MAC地址
< <i>sn</i> >	ONU设备序列号

## 3. 配置ONU设备能学习到的最大MAC地址数目

命令	功能
ZXR10 (config) #interface epon-olt_< slot> /< oltid> .< onuld>	进入ONU子接口配置模式
ZXR10(config-if)# <b>onu mac limit-num</b> < max-number>	配置指定ONU设备的以太网端口所能
	学习到的最大MAC地址数目

使用no onu mac limit-num删除配置的最大MAC地址数目,并且恢复到默认值。

参数说明:

参数	描述
< max-number>	最大MAC地址数,范围0~8192,缺省
	是256

# 8.2.4 配置0LT光路保护功能

1. 创建光路保护组

命令	功能
ZXR10(config) #interface smartgroup< number>	进入smartgroup接口配置模式
ZXR10 (config-if) #epon protection-group enable	创建EPON的光路保护组,在需要时
	进行光路倒换

## 2. 保护倒换返回机制配置

命令	功能
ZXR10(config-if)# <b>epon protection-group revertive</b> < <i>1-65535</i> >	在smartgroup接口配置模式下,配置倒
	换保护时间

### 参数说明:

参数	描述
< 1-65535>	等待恢复时间间隔, 单位s

## 3. 保护接口和工作口的倒换

命令	功能
ZXR10(config-if)#epon protection-group switch { force   enable}	在smartgroup接口配置模式下, 配置保
	护组里的工作口和保护口的倒换方式,
	缺省为无倒换

使用no epon protection-group switch删除倒换配置。

光纤保护倒换可在以下两种方式下进行:

- a. 自动倒换:由故障发现触发,如信号丢失或信号劣化等;
- b. 强制倒换:由管理事件触发。

参数说明:

参数	描述
force	强制切换到另一个接口
enable	自动切换使能

## 4. 将OLT接口加入到保护组配置

命令	功能
ZXR10 (config) #interface epon-olt_< slot> /< oltid>	进入OLT端口配置模式
ZXR10(config-if)#smartgroup < groupid> mode on { master   backup}	将OLT端口加入到EPON的保护组中,
	允许没有主接口只有备接口的情况。

一个时刻,最多只能有一个接口处于激活状态。

参数	描述
master	接口为主接口
backup	接口为备接口

# 8.2.5 配置QoS

1. 配置QoS本地标记

命令	功能
ZXR10(config)#epon	进入EPON配置模式
ZXR10(config-epon)# <b>qos cos-map-local</b> < 0-7> < 0-7> < 0-7> < 0-7> <	配置QoS本地标记
0-7> < 0-7> < 0-7> < 0-7>	

# 2. 配置端口QoS

命令	功能
ZXR10(config) #interface epon-olt_< slot> /< oltid>	进入OLT端口配置模式
ZXR10(config-if)#trust-cos-local { enable  diable}	开启/关闭端口QOS

# 8.2.6 配置0LT告警功能

1. 开启/关闭OLT告警功能

命令	功能
ZXR10(config) #interface epon-olt_< slot> /< oltid>	进入EPON OLT接口配置模式
<pre>ZXR10(config-if)#alarm &lt; alarmType&gt; { disable   enable}</pre>	开启/关闭OLT告警功能

# 告警类型说明:

告警类型	描述
bit error rate	由于ONU和OLT间光路通道衰减不在一个正常的范围内或者ONU、OLT光参数配置不正确,导致光路异常,从而产生bit error rate告警
frame error rate	由于ONU和OLT间光路通道衰减不在一个正常的范围内或者ONU、OLT光参数配置不正确,导致光路异常,从而产生frame error rate告警
llid-mismatch	当时隙错乱,ONU不在自己的时隙内转发数据时,就会引起LLID匹配错误帧告警, 缺省情况下为关闭
localstable	当系统误用时,比如:把OAM1.2的ONU与OAM2.0的ONU混用时(因为同一系统下的ONU必须采用同一OAM版本),就会引起localstable告警(此告警是OLT侧产生的),缺省情况下为开启

告警类型	描述
remote stable	当系统误用时,比如:把OAM1.2的ONU与OAM2.0的ONU混用时(因为同一系统下的ONU必须采用同一OAM版本),就会引起remote stable告警(此告警是由ONU侧产生的,并且被反馈给OLT),缺省情况下为开启
bad encryption key	当ONU不应该改变加密键(加密键就是在ONU的发现过程中,ONU随机产生的密钥, 用于对ONU和OLT之间转发的数据进行加密和解密)时加密键改变了,就会引起bad encryption key告警,缺省情况下为开启
registration error	(可选)当ONU在注册过程中发生错误时,就会引起registration error告警,缺省情况下为开启
oamlink disconnection	(可选)当OAM链路中断时,就会引起oamlink disconnection告警,缺省情况下为开启
critical event	critical event告警包含local link fault与dying gasp两种
dying gasp	当遇到系统出错,数据加载错误或者其它无法恢复的错误时,就会引起dying gasp告警,缺省情况为开启
local link fault	当本地数据终端设备的接收方向出现故障时,就会引起local link fault告警,缺省情况为开启
onu over limitation	当OLT下所挂的ONU总数超过系统所支持的规格,就会引起onu over limitation告警, 缺省情况下为开启

## 2. 配置告警监控方向和阀值

命令	功能
ZXR10(config-if)#alarm < alarmType> direction < direction> threshold	配置告警监控方向和阀值
< threshold>	

## 参数说明:

参数	描述
< direction>	表示监控方向
< threshold>	表示告警阈值
< alarmType>	表示告警类型

监控方向包括:

- uplink: 只对ONU向OLT转发的上行通信数据进行监控
- downlink: 只对OLT向ONU转发的下行通信数据进行监控
- up-down-link: 对OLT和ONU之间的上下行通信数据进行监控

#### 缺省的方向是up-down-link。

3. 配置告警阀值

命令	功能
ZXR10(config-if)# <b>alarm</b> < <i>alarmType</i> > <b>threshold</b> < <i>threshold</i> >	配置告警阈值

参数说明:

参数	描述
< threshold>	表示LLID匹配错误帧,缺省为5000
< alarmType>	告警类型

# 8.2.7 配置ONU远程管理

#### 1. 进入EPON ONU远程管理模式

命令	功能
ZXR10 (config) # <b>epon-onu-mng epon-olt_</b> < <i>slot&gt; /&lt; oltid&gt; .&lt; onuid&gt;</i>	进入EPON ONU远程管理配置模式

## 参数说明:

参数	描述
< slot> /< oltid>	OLT单板槽位号和OLT端口号
< onuid>	ONU设备号,范围1~32

# 2. 配置EPON ONU的告警上报功能

命令	功能
ZXR10(epon-onu-mng)#alarm { enable   disable}	开启/关闭EPON ONU的告警上报功能

## 3. 配置EPON ONU端口隔离功能

命令	功能
<pre>ZXR10(epon-onu-mng) #isolation { enable  diable}</pre>	开启/关闭EPON ONU端口隔离功能

# 4. 配置EPON ONU上行FEC功能

命令	功能
ZXR10(epon-onu-mng)#fec { enable  diable}	开启/关闭EPON ONU上行FEC功能

### 5. 配置ONU加密报文的流向

命令	功能
ZXR10 (config) #interface epon-olt_< slot> /< oltid> .< onuid>	进入ONU子接口配置模式
ZXR10 (config-if) #encrypt direction { downstream   upstream   both} {	对上行/下行数据报文或两种报文同时
enable   disable}	进行加密

参数说明:

参数	描述
direction	加密报文的流向
downstream	下行报文
upstream	上行报文
both	上行和下行报文

# 6. 配置EPON ONU的队列门限值

命令	功能
<pre>ZXR10 (config) #epon-onu-mng epon-olt_&lt; slot&gt; /&lt; oltid&gt; .&lt; onuid&gt;</pre>	进入OLT端口配置模式下
ZXR10 (epon-onu-mng) # <b>dba queue-set</b> < <i>queuesetid</i> > { <b>queue1</b> < <i>value1</i> >	配置EPON ONU的队列门限值
queue2 < value2>   queue3 < value3>   queue4 < value4>   queue5 <	
<pre>value5&gt;   queue6 &lt; value6&gt;   queue7 &lt; value7&gt;   queue8 &lt; value8&gt; }</pre>	

## 参数说明:

参数	描述
< queuesetid>	队列组号码,范围1~3
{ queue1 < value1> queue8 < value8> }	各队列的门限值,范围1~65535

# 7. 激活EPON ONU队列的DBA功能

命令	功能
ZXR10 (epon-onu-mng) # <b>dba queue-set active</b> < <i>queueSetList</i> >	在EPON ONU远程管理配置模式下,
	激活EPON ONU队列的DBA功能

## 8. 配置EPON ONU的以太网端口属性

命令	功能
ZXR10(epon-onu-mng)#interface eth eth_slot/< portId> { phy-state	在EPON ONU远程管理配置模式下,
flow-control} { enable   disable}	配置EPON ONU的以太网端口属性
<pre>ZXR10 (epon-onu-mng) #interface eth eth_slot/&lt; portId&gt; auto-neg { enable   disable   restart}</pre>	
<pre>ZXR10 (epon-onu-mng) #interface eth eth_slot/&lt; portId&gt; policing { enable   disable} cir &lt; value1&gt; cbs &lt; value2&gt; ebs &lt; value3&gt;</pre>	

该命令可配置以太网端口开启/关闭,流控开启/关闭,自协商开启/关闭,强制自协 商,管制功能属性。

参数	描述
eth_slot/ < portId>	单板槽位,端口号
phy-state	以太网端口是否开启
flow-control	流量控制功能
auto-neg	自协商功能
policing	管制功能
cir value1	CIR值,范围0~16777215,单位: kbps
cbs value2	承诺突发值,范围0~16777215,单位: kbps
ebs value3	EBS值,范围0~16777215,单位:kbps

参数说明:

# 9. 配置EPON ONU的E1端口属性

命令	功能
ZXR10 (epon-onu-mng) #interface e1 < UniNo> { enable   disable}	在EPON ONU远程管理配置模式下,
	配置EPON ONU的E1端口属性

参数说明:

参数	描述
< UniNo>	E1端口UNI号,范围1~16

10. 配置EPON ONU的VoIP端口属性

命令	功能
ZXR10 (epon-onu-mng) #interface voip < UniNo> { enable   disable}	在EPON ONU远程管理配置模式下,
	配置EPON ONU的VoIP端口属性

# 参数说明:

参数	描述
< UniNo>	VoIP端口UNI号,范围1~64

#### 11. 配置EPON ONU以太网端口的MAC地址

命令	功能
ZXR10 (epon-onu-mng) #mac { add   delete   clear } eth_< slot> /< port> {	在EPON ONU远程管理配置模式下,配
filter   bind   static} [ mac-address]	置EPON ONU以太网端口的MAC地址

# 12. 配置EPON ONU以太网端口MAC地址的老化时间

命令	功能
ZXR10 (epon-onu-mng) # <b>mac aging-time</b> < <i>aging-time</i> >	在EPON ONU远程管理配置模式下,
	配置EPON ONU以太网端口MAC地址
	的老化时间

## 参数说明:

参数	描述
< aging-time>	MAC地址老化时间,范围15~86400,
	并且是15的倍数,单位s

## 13. 配置EPON ONU以太网端口所能学习的最大MAC地址数

命令	功能
ZXR10 (epon-onu-mng) # <b>mac limit-num eth_</b> < <i>slot&gt; /&lt; port&gt; &lt;</i>	在EPON ONU远程管理配置模式下,
max-number> [ no-limit]	配置EPON ONU以太网端口所能学习
	的最大MAC地址数目

参数	描述
< max-number>	最大MAC地址数,范围0~65534

参数	描述
[ no-limit]	无限制

# 14. 配置EPON ONU的管理IP地址

命令	功能
ZXR10 (epon-onu-mng) #mgmt-ip { onu-ip < ip-address> < ip-mask> < priority> < vlanID> } { mgm-ip < in-address> < in-mask> < gateway> } [	在EPON ONU远程管理配置模式下,
status { enable   disable} ]	

## 参数说明:

参数	描述
< ip-address>	ONU IP地址
< ip-mask>	ONU IP地址的掩码
< priority>	优先级,范围0~7
< vlanID>	VLAN ID,范围1~4094
< ip-address>	远程主机IP地址
< ip-mask>	远程主机IP地址的掩码
< gateway>	网关IP地址
status	管理状态

# 15. 配置EPON ONU以太网端口的VLAN属性

命令	功能
ZXR10 (epon-onu-mng) #vlan ethernet < UniNo> mode { transparent   tag < Vlan-Tag>   translation < default-vid> [ < delete-vid> < add-vid> ] }	在EPON ONU远程管理配置模式下,配置EPON ONU以太网端口的VLAN属性

参数	描述
< Vlan-Tag>	缺省VLAN tag,范围1~4094
< delete-vid> < add-vid>	删除和添加多个Tag对

## 16. 配置EPON ONU以太网端口的组播VLAN

命令	功能
ZXR10 (epon-onu-mng) # <b>multicast vlan ethernet</b> < <i>UniNo</i> > { add   delete	在EPON ONU远程管理配置模式下,配
clear} [ vlanlist < vlanlist> ]	置EPON ONU以太网端口的组播VLAN

#### 参数说明:

参数	描述
vlanlist < vlanlist>	VLAN ID列表,以逗号分隔,最多支持
	8个组播VLAN

## 17. 配置EPON ONU以太网端口的组播VLAN tag剥离功能

命令	功能
ZXR10 (epon-onu-mng) # <b>multicast vlan tag-stripe</b> < UniNo> { enable	在EPON ONU远程管理配置模式下,
disable}	配置EPON ONU以太网端口的组播
	VLAN tag剥离功能

## 18. 配置EPON ONU的组播模式

命令	功能
ZXR10 (epon-onu-mng) #multicast switch { igmpsnooping	在EPON ONU远程管理配置模式下,
control-multicast}	配置EPON ONU的组播模式,包括
	IGMP Snooping模式和可控组播模式

## 19. 配置EPON ONU以太网端口的最大组播组数目

命令	功能
ZXR10 (epon-onu-mng) #multicast group-max-number ethernet < UniNo>	在EPON ONU远程管理配置模式下,
< max-number>	配置EPON ONU以太网端口的最大组
	播组数目

参数	描述
< max-number>	最大组播组,范围1~255

# 20. 创建EPON ONU分类条件模版

命令	功能
ZXR10(epon-onu-mng)#lassification condition-profile < profileNo> { {	在EPON ONU远程管理配置模式下,
da-mac   sa-mac} < mac-address>   { destIp   sourceIp} < ip-address>	创建EPON ONU分类条件模版
priority < priority>   vlanId < vlanId>   dscp < dscp>   { SourcePort	
DestPort} < portno>   eth-type < match-value1>   ip-protocol-type	
<pre>&lt; match-value2&gt; } { never-match   equal   not-equal   less-equal  </pre>	
greater-equal   exists   not-exists   always-match} }	

## 参数说明:

参数	描述
< profileNo>	模版号,范围1~8
{ da-mac   sa-mac} < mac-address>	按照报文的源MAC地址/目的MAC地址
{ destIp   sourceIp} < <i>ip-address</i> >	按照报文的源IP地址/目的IP地址
< priority>	优先级,范围0~7
dscp < dscp >	DSCP值,范围1~64
{ SourcePort   DestPort} < portno>	端口号,范围1~65535
eth-type < match-value1>	以太网类型,十六进制数字,如0x8808
<pre>ip-protocol-type &lt; match-value2&gt;</pre>	IP协议类型,十六进制数字,如0x02
operator-type	该模板执行的操作类型

# 21. 创建EPON ONU映射规则模板

命令	功能
ZXR10(epon-onu-mng)# <b>classification rule-profile</b> < <i>profileNo</i> > <b>queue</b> <	在EPON ONU远程管理配置模式下,
<pre>vlaue1&gt; priority &lt; value2&gt;</pre>	创建EPON ONU映射规则模板

参数	描述
rule-profile< profileNo>	模板名称
queue < vlaue1>	队列优先级,范围0~7
<pre>priority &lt; value2&gt;</pre>	映射后的优先级值,范围0~7

#### 22. 增加或删除EPON ONU以太网端口上行业务流分类、映射控制规则

命令	功能
ZXR10 (epon-onu-mng) # <b>classification port</b> < <i>EthernetUniNo</i> >	在EPON ONU远程管理配置模式下,
<pre>rule-precedence &lt; precedence&gt; { add   delete} &lt; rule-profile-name&gt; &lt;</pre>	增加或删除EPON ONU以太网端口上
condition-profile-name-list>	行业务流分类、映射控制规则

#### 使用no classification port < portname> 删除某端口所有控制规则。

#### 23. 重启EPON ONU

命令	功能
ZXR10 (epon-onu-mng) # <b>reboot</b>	在EPON ONU远程管理配置模式下,
	重启远端ONU设备

# 8.3 EPON OLT配置实例

如图8-2所示,局端OLT设备为三层路由交换机,终端ONU设备为ZXR10 2928,OLT与ONU之间通过光分路器连接。





配置思路如下所示:

- 1. 配置ONU自动鉴权模式,让ONU自动注册到OLT;
- 2. 非自动鉴权模式注册;
- 3. 配置带宽动态分配;
- 4. 配置ONU MAC最大学习数目;
- 5. 配置ONU远程管理。

OLT设备配置:

```
ZXR10(config)#epon /*进入EPON配置模式*/
ZXR10(config-epon)#auto-authentication card 3 enable
/*使能EPON线卡自动鉴权模式*/
ZXR10#show epon onu authentication epon-olt_3/15
Port:epon-olt_3/15.1
```
```
RTT:42  /*状态UP*/
State:UP
MAC ADDR:0015.eba3.c500
                           /*ONU的MAC地址*/
                  Hard Ver:
OnuType:
OnuSoft Ver:V1.1.0b_D03 EEPROM Ver:3
Onu Host Type:
Port:epon-olt_3/15.2
                  RTT:44
State:UP
MAC ADDR:0015.eba3.c8b7
OnuType:
                  Hard Ver:
OnuSoft Ver:V1.1.0b D03 EEPROM Ver:3
Onu Host Type:
ZXR10#show interface b 3
Interface Portattribute Mode BW(Mbits) Admin Phy Prot Description
epon-olt 3/15 optical
                       Duplex/full 1000
                                         up up up
                                                      none
epon-olt 3/15.1 optical
                       Duplex/full 1000
                                         up up up
                                                      none
epon-olt_3/15.2 optical Duplex/full 1000 up up up
                                                      none
ZXR10#show epon onu mac epon-olt 3/15
                         Llid StaticFlag
Mac address
               Port
_____
0015.eba3.c500 epon-olt_3/15.1 1
                                        0
0015.eba3.c8b7
              epon-olt 3/15.2
                                2
                                        0
ZXR10(config)#epon
ZXR10 (config-epon)#auto-authentication card 2 disable /*关闭自动注册模式*/
ZXR10 (config-epon)#hardware-authentication card 2 enable /*开启硬件注册模式*/
ZXR10 (config-epon) #exit
ZXR10 (config)#int epon-olt_2/13 /*进入OLT接口配置模式,手工绑定ONU*/
ZXR10 (config-if)#onu 1 type 123 mac 0015.ebac.c87c
ZXR10 (config)#interface epon-olt 2/13.1
/*手工绑定ONU后,需要初始化ONU接口,直接进入子接口即可*/
ZXR10(config)#epon
ZXR10(config-epon)#dba epon-olt 2/13 ?
```

```
archimedes DBA archimedes type
```

/\*目前只支持plato算法\*/

plato

thales

```
ZXR10(config)#int epon-olt_2/13.1
/*进入ONU接口配置模式,限制ONU MAC最大学习数目*/
ZXR10(config-if)#onu mac limit-num ?
<0-8191> Limit number
```

DBA plato type DBA thales type

```
ZXR10(config)#epon-onu-mng epon-olt_2/13.1
/*进入ONU远程管理配置*/
```

## 8.4 EPON OLT的维护与诊断

### 全局配置管理维护与诊断

命令	功能	
ZXR10 (config) # <b>show epon olt</b>	显示OLT端口相关信息	
ZXR10 (config) # <b>show epon dba epon-olt_</b> < <i>slot&gt; /&lt; olt&gt;</i>	显示OLT接口的DBA算法信息	
ZXR10 (config) <b>#show epon optical-epon</b> { <b>npc</b> < <i>1-12</i> >   <b>interface</b>	显示OLT光模块信息,包括光模块型	
<b>epon-olt_</b> < <i>slot</i> > /< <i>olt</i> > }	号、光模块厂商信息,光模块的波长和	
	光模块设备ID	

## 0LT 0NU本地管理维护与诊断

命令	功能
<pre>ZXR10 (config) #show epon onu mac epon-olt_&lt; slot&gt; /&lt; oltid&gt;.[ &lt; onuid&gt; ]</pre>	显示指定OLT端口的ONU设备MAC地
	址
<pre>ZXR10 (config) #show epon onu authentication [ epon-olt_&lt; slot&gt; /&lt; oltid&gt;</pre>	查询指定OLT端口的ONU相关注册认
epon-olt_< slot> /< oltid> .< onuid> ]	证信息
ZXR10 (config) <b>#show epon onu information</b>	显示指定OLT端口下所有ONU信息

### 示例:

#### 显示指定OLT端口的ONU设备MAC地址,如下所示:

ZXR10(config)#show epon onu mac

显示各域说明:

域	描述
MAC_Address	MAC地址的点分形式
port	MAC地址所在的OLT端口或ONU端口
llid	逻辑链路标识
static	MAC地址静态标志,0为动态,1为静态,2为两种状态都有

## 光路保护功能维护与诊断

命令	功能
<pre>ZXR10(config) #show epon protection-group { groupid   all}</pre>	显示保护组的配置状态
<pre>ZXR10(config) #show epon switch-record { groupid   all}</pre>	显示保护组的发生光路切换的记录

#### 示例:

显示保护组的配置状态,如下所示:

ZXR10(config)#show epon protection-group 1 gId Master Backup Active bSw bReval itv 1 OLT 1/1 OLT 1/2 MASTER YES NO N/A

显示保护组的切换记录,如下所示:

ZXR10(config)#show eponswitch-record 2gIdnoswitchTimeswitchTypeMtoB2108-6-1014:30forceYES2208-6-1014:35ALARMNO

性能管理维护与诊断

命令	功能
ZXR10 (config) <b>#show protection request</b> [ <b>group</b> < groupid> ]	显示对于指定保护组所有的请求消息,
	包括告警请求和外部切换请求信息

#### 示例:

ZXR10#show protection reque	st group test
Groupid:	1
protect ponIf:	epon-olt_3/2
work ponIf:	epon-olt_3/1
Alarm request:	
WorkChannel:	No alarm request!
ProtectChannel:	OLTSF
External requset:	none
Highest local request:	protect-fail

## 0NU远程管理模块维护与诊断

命令	功能
ZXR10 (config) #show remote onu information	显示EPON ONU远程管理基本信息
ZXR10 (config) # <b>show remote onu dba</b>	显示EPON ONU远程管理的DBA队列 门限配置信息
<pre>ZXR10 (config) #show remote onu ethernet-uni epon-olt_&lt; slot&gt; /&lt; oltId&gt; .&lt; onuId&gt; [ &lt; UniNo&gt; ]</pre>	显示EPON ONU远程管理的以太网端 口配置信息
<pre>ZXR10 (config) #show remote onu mac epon-olt_&lt; slot&gt; /&lt; oltId&gt; .&lt; onuId&gt; eth_&lt; olt&gt; /&lt; portID&gt;</pre>	显示EPON ONU远程管理的MAC地址 配置信息
<pre>ZXR10 (config) #show remote onu mgmt-ip epon-olt_&lt; slot&gt; /&lt; oltId&gt; .&lt; onuId&gt;</pre>	显示EPON ONU远程管理的IP地址配 置信息
<pre>ZXR10(config) #show remote onu vlan epon-olt_&lt; slot&gt; /&lt; oltId&gt; .&lt; onuId&gt;</pre>	显示EPON ONU远程管理的VLAN配 置信息
<pre>ZXR10 (config) #show remote onu multicast epon-olt_&lt; slot&gt; /&lt; oltId&gt; .&lt; onuId&gt; [ &lt; 1-79&gt; ]</pre>	显示EPON ONU远程管理的组播配置 信息
<pre>ZXR10 (config) #show remote onu classification epon-olt_&lt; slot&gt; /&lt; oltId&gt; .&lt; onuId&gt; &lt; UniNo&gt;</pre>	显示EPON ONU远程管理的以太网端 口分流配置信息
<pre>ZXR10(config) #show remote onu { condition-profile   rule-profile} epon-olt_&lt; slot&gt; /&lt; oltId&gt; .&lt; onuId&gt;</pre>	显示EPON ONU远程管理的以太网端口分流模版信息

## 示例:

显示epon-onu\_3/1:1远程管理的基本信息,如下所示:

ZXR10#show remote onu information epon-olt 3/1.1 epon-onu\_3/1:1 PONU . OnuModel Onu vendorId 0xBEAC6301. OnuId 0003.0000.000A. PAS6301E. Hardware version Software version 299. 0x0135. Firmware version E6 . Chip vendorId ChipModel 0x6301. Chip revison ο. ChipDesignDate 06/09/27. Number of Ge port 1 . GePort 1. Number of Fe port Ο. FePort Number of POTS port 0. Number of El port Ο. Number of US Queues 4. Max queues per US port 4. Number of DS Queues 8. Max queues per DS port 8. BatteryBackup no.

#### 显示epon-onu\_3/1:1的DBA队列门限配置信息,如下所示:

ZXR10#show remote onu dba epon-onu\_3/1:1 Active queueSet 1.

#### SetId Threshold

 Queue1
 Queue2
 Queue3
 Queue4
 Queue5
 Queue6
 Queue7
 Queue8

 1
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 65,535
 <td

#### 显示epon-onu\_1/1:1的1号以太网端口配置信息以及运行状态信息,如下所示:

ZXR10(config-onu-mng)#show remote onu ethernet-uni epon-olt\_1/1.1 1
UNI Link-Status FlowControl US-CIR US-CBS US-EBS DS-CIR DS-PIR
1 Up Disable N/A N/A N/A 100

#### 显示epon-onu\_3/1:1的MAC地址配置信息,如下所示:

ZXR10#show remote onu mac epon-onu\_3/1:1 eth\_0/1

```
epon-onu_0/2/1:1;
MAC_Address info
Port Name:eth 0/1;
Limit num: no-limit;
Filter mac-address info
vlan
             mac
2
             9877.9878.4566
Bind mac-address info
vlan
             mac
3
             9877.9899.0988
Static mac-address info
vlan
             mac
    4557.3241.3423
1
```

#### 显示epon-onu\_3/1:1的远程管理IP地址配置信息,如下所示:

```
ZXR10# show remote onu mgmt-ip epon-onu_0/3/1:1
Status enable;
IP Address 172.168.1.122;
Mask 255.255.0.0;
Priority 3; vlan 300;
Mgmt-IP 172.168.1.10;
Mgmt-Mask 255.255.0.0;
```

Mgmt-Gateway 172.168.1.250.

#### 显示epon-onu\_3/1:1的VLAN配置信息,如下所示:

ZXR10(c	config-onu-mng	)#show re	mote onu vlan e	epon-olt_3/1.1
UNI	Mode	VlanTag	DeleteVlanTag	AddVlanTag
1	Translation	3	10	20

#### 显示epon-onu\_3/1:1的组播配置信息,如下所示:

ZXR10	\$show remote	onu multicast	epon-olt_3/1.1
UNI	TagStripe	MaxGroupNum	VlanList
1	Striped	20	N/A
2	Striped	10	1-8

```
显示epon-onu_3/1:1的以太网端口分流配置信息,如下所示:
ZXR10#show remote onu classification epon-olt_3/1.1 1
RulePrecedence RuleName ConditionNameList
1 1 1 1
```

## 显示epon-onu\_3/1:1的以太网端口分流模版信息,如下所示:

ZXR10#show remote onu class profile epon-onu\_3/1:1

---rule profile---

index	name	queuemap	priority
1	aaa	1	0
2	bbb	3	7

---condition profile---

index	name	filed	matchValue	operator
1	c1	vid	111	never-match
2	c2	priority	7	always-match

# 图目录

图1-1	VLAN标签格式1-2
图1-2	QinQ典型组网1-4
图1-3	VLAN典型组网1-9
图1-4	QinQ典型组网1-11
图1-5	子网VLAN配置实例1-12
图1-6	SuperVLAN配置实例1-16
图1-7	SVLAN 配置实例图1-19
图2-1	边缘端口的BPDU保护2-4
图2-2	端口环回保护功能12-5
图2-3	端口环回保护功能22-6
图2-4	端口环回保护功能32-6
图2-5	端口根保护功能2-7
图2-6	MSTP配置实例组网图12-11
图3-1	MAC地址表配置实例
图4-1	链路聚合配置实例4-3
图5-1	IGMP Snooping的应用5-1
图5-2	IGMP Snooping配置实例5-5
图6-1	ZESR拓扑示意图6-2
图6-2	ZESR配置实例6-4
图6-3	ZESS网络拓扑图6-6
图6-4	双上行链路故障保护拓扑图6-8
图6-5	双上行链路拓扑图6-9
图7-1	链路控制事件组网7-9
图8-1	EPON系统参考图8-2
图8-2	EPON OLT配置实例

# 表目录

表3-1	MAC地址表配置实例数据	3-7
表7-1	OAM功能列表	7-2

- BPDU Bridge Protocol Data Unit,网桥协议数据单元
- BRAS Broadband Remote Access Server, 宽带远程接入服务器
- CIST Common and Internal Spanning Tree, 公共和内部生成树
- CST Common Spanning Tree, 公共生成树
- FDDI Fiber Distributed Data Interface, 光纤分布式数据接口
- HMAC-MD5 Hashed Message Authentication Code with MD5, 基于MD5的消息验证编码
- IGMP Internet Group Management Protocol, Internet组管理协议
- ISP Internet Service Provider, Internet服务提供商
- IST Internal Spanning Tree, 内部生成树
- LACP Link Aggregation Control Protocol, 链路聚合控制协议
- MAC Media Access Control, 介质访问控制
- MD5 Message Digest 5, 信息摘要5
- MSTP Multiple Spanning Tree Protocol, 多生成树协议
- PE Provider Edge,运营商边缘
- PVID Port VLAN ID, 端口虚拟局域网标识
- PVLAN Private VLAN, 私有虚拟局域网
- RSTP Rapid Spanning Tree Protocol, 快速生成树协议
- SDH Synchronous Digital Hierarchy,同步数字系列
- STP Spanning Tree Protocol, 生成树协议
- SVLAN Selective VLAN, 可选择性VLAN
- VID VLAN Identifier, 虚拟局域网标识
- VLAN Virtual Local Area Network, 虚拟局域网
- ZESR ZTE Ethernet Switch Ring, 中兴以太网交换环
- ZESS ZTE Ethernet Smart Switch, 中兴以太网智能切换