H3C网络学院参考书系列

H3C

H3C以太网交换机典型配置指导

杭州华三通信技术有限公司　编著

清华大学出版社

H3C网络学院参考书系列

H3C

H3C以太网交换机典型配置指导

杭州华三通信技术有限公司　编著

清华大学出版社
北京

内 容 简 介

本书从简到难，通过贴近实际应用的场景，给出大量的交换机配置实例，包括交换机基本配置、以太网接口配置、以太网交换配置、生成树协议配置、堆叠技术配置、IP 业务配置、IP 路由配置、IPv6 配置、IP 组播配置、ACL 与 QoS 配置、安全特性配置、可靠性配置、网络管理与监控配置、MPLS 与 MCE 配置、EPON-OLT 配置等。

本书的最大特点是将配置实例与实际应用场景紧密结合，通过给定场景与相应的配置实例，能够使读者更快、更直观地掌握交换机特性的应用和配置，增强读者的动手技能。

本书是为具备一定 IP 网络基础知识的人员编写的，尤其适合于学习了 H3C 网络学院系列教程的读者。对于网络工程技术人员，本书是简单易用的 H3C 交换机配置工具书。另外，本书还可以作为 H3C 网络学院系列教程的补充教材。

图书在版编目(CIP)数据

H3C 以太网交换机典型配置指导/杭州华三通信技术有限公司编著. —北京：清华大学出版社，2012.6

（H3C 网络学院参考书系列）

ISBN 978-7-302-28415-4

Ⅰ. ①H…　Ⅱ. ①杭…　Ⅲ. ①以太网－数据交换机－配置　Ⅳ. ①TP393.11

中国版本图书馆 CIP 数据核字(2012)第 056193 号

责任编辑：刘　青
封面设计：傅瑞学
责任校对：袁　芳
责任印制：张雪娇

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn

印 刷 者：清华大学印刷厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：29.5　　**字　　数**：715 千字
版　　次：2012 年 6 月第 1 版　　**印　　次**：2012 年 6 月第1 次印刷
印　　数：1～4000
定　　价：60.00 元

产品编号：045711-01

认证培训开发委员会

路由交换编委会

本书编审人员

原　稿　宋吉超　陈伯超　刘　芳　刘全永　郜　雾

改　编　张东亮　彭天付　汪　军　王　京　王　晨

张盛楠　赵国卫　陈小坤　杨逢君　赵治东

管祥杰

审　稿　张东亮

出版说明

PUBLICATION ELUCIDATION

伴随着互联网上各项业务的快速发展，作为信息化技术一个分支的网络技术与人们的日常生活已密不可分，在越来越多的人依托网络进行沟通的同时，网络本身也演变成了服务、需求的创造和消费平台，这种新的平台逐渐创造了一种新的生产力，一股新的力量。

如同人类民族之间语言的多样性一样，最初的计算机网络通信技术也呈现出多样化发展。不过伴随着互联网应用的成功，IP 作为新的力量逐渐消除了这种多样性趋势。在大量开放式、自由的创新和讨论中，基于 IP 的网络通信技术逐渐被积累完善起来；在业务易于实现、易于扩展、灵活方便性的选择中，IP 标准逐渐成为唯一的选择。

杭州华三通信技术有限公司(H3C)作为国际领先的 IP 网络技术解决方案提供商，一直专注于 IP 网络通信设备的研发和制造。H3C 的研发投入从成立伊始，一直高达公司营业收入的 15%以上，而这些研发投入又都集中在一个领域，就是 IP 网络技术，包括软件、硬件和测试。2010 年授权专利数量位列第六，对于仅仅拥有 4800 名员工的 H3C 平均每个研发人员拥有 1.2 个专利。

另外，为了使广大网络产品使用者和网络技术爱好者能够更好地掌握 H3C 产品的使用方法与 IP 网络技术，H3C 相关部门人员开发了大量的技术资料，详细而简明地介绍了相关知识。这些技术资料大部分是公开的，在 H3C 的官方网站(www.h3c.com.cn)上都能看到并可以下载。

但是，在传统的纸质媒介仍占重要地位的今天，许多合作伙伴和学校、机构、网络技术爱好者多次表达，希望 H3C 能够正式出版其技术资料，包括网络学院教材、产品配置手册、典型配置案例、行业解决方案等。作为国内 IP 领域技术和通信设备制造的领导者，华三公司深感自身责任重大、责无旁贷。

2004 年 10 月，华三公司的前身——华为 3Com 公司出版了自己的第一本网络学院教材，开创了华三公司网络学院教材正式出版的先河。在后续的几年间，华三公司陆续出版了《IPv6 技术》(第 2 版)、《路由交换技术第 1 卷》、《路由交换技术第 2 卷》、《路由交换技术第 3 卷》、《路由交换技术第 4 卷》等网络学院教材系列书籍，极大地推动了 IP 技术在网络学院和业界的普及。

华三公司希望通过这种形式，探索出一条理论与实践相结合的教育方法，顺应国家提倡的“学以致用、工学结合”教育方向，培养更多实用型的网络工程技术人员。

目前，华三公司正在计划推出“H3C 网络学院参考书系列”教辅教材，主要是作为网络

学院教材系列的有益补充，在提升学员动手能力、拓展学员的技术深度方面做一些有益的尝试。《H3C 以太网交换机典型配置指导》正是“H3C 网络学院参考书系列”中的第一本。华三公司还将规划、组织产品技术开发专家陆续推出有关行业解决方案、产品配置手册等相关书籍。

希望在 IP 技术领域，这一系列教材能成为一股新的力量，回馈广大网络技术爱好者，为推进中国 IP 技术发展尽绵薄之力，同时也希望读者对我们提出宝贵的意见。

H3C 客户服务热线：400-810-0504

H3C 客户服务邮箱：service@h3c.com

杭州华三通信技术有限公司全球技术服务部

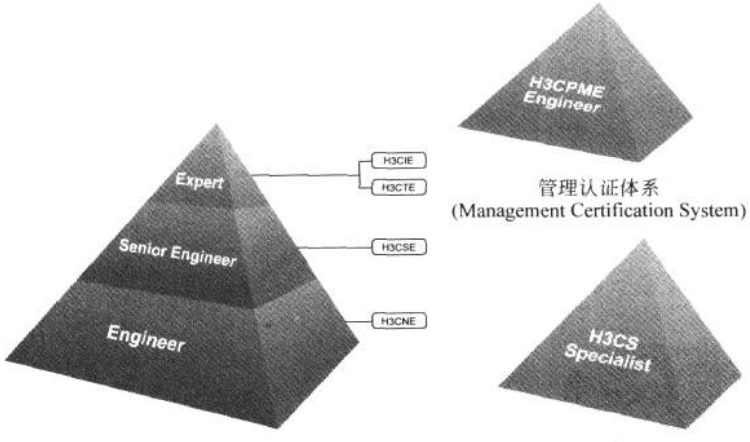
认证培训开发委员会路由交换编委会

2012 年 1 月

H3C认证简介

H3C 认证培训是国内最早建立的完善的网络产品技术认证，也是中国第一个走向国际市场的 IT 厂商认证，已成为当前权威的 IT 认证品牌之一，通过专业考试机构向全球提供认证考试，确保公平、公正、权威、规范。截至 2011 年年底，已有 40 多个国家和地区的 16 万余人次接受过培训，逾 9 万人次获得认证证书。H3C 认证将秉承“专业务实，学以致用”的理念，快速响应客户需求的变化，提供丰富的标准化培训认证方案及定制化培训解决方案，帮助学员实现梦想、制胜未来。

按照技术应用场合的不同，同时充分考虑客户不同层次的需求，H3C 公司为客户提供了从网络工程师到网络专家的三级技术认证体系、突出专业技术特色的专题认证体系和管理认证体系，构成了全方位的网络技术认证体系。



管理认证体系
(Management Certification System)

技术认证体系
(Technology Certification System)

专题认证体系
(Special Certification System)

要全面了解 H3C 认证培训相关信息，请访问 H3C 网站培训认证栏目(http://www.h3c.com.cn/Training/)。要了解 H3C 认证培训最新动态，请关注 H3C 培训认证官方微博(http://weibo.com/pxrzh3c)。

H3C 认证将秉承“专业务实，学以致用”的理念，与各行各业建立更紧密的合作关系，认真研究各类客户不同层次的需求，不断完善认证体系，提升认证的含金量，使 H3C 认证能有效证明学员所具备的网络技术知识和实践技能，帮助学员在竞争激烈的职业生涯中保持强有力的竞争实力。

FOREWORD

前 言

随着互联网技术的广泛普及和应用，通信及电子信息产业在全球迅猛发展起来，从而也带来了网络技术人才需求量的不断增加，网络技术教育和人才培养成为高等院校一项重要的战略任务。

H3C 网络学院(HNC)主要面向高校在校学生开展网络技术培训，培训使用 H3C 网络学院培训教程。HNC 教程分 4 卷，第 1 卷课程涵盖 H3CNE 认证课程内容，第 2～4 卷课程涵盖 H3CSE Routing & Switching 认证课程内容。培训课程高度强调实用性和提高学生动手操作的能力。

作为 H3C 网络学院课程的参考书，本书内含大量的特性配置实例与应用场景，使读者能够快速地对 H3C 交换机的大多数常见特性进行配置。本书适合以下几类读者。

大专院校在校生：本书可作为 H3C 网络学院课程的实验辅导教材，也可作为计算机通信相关专业学生的自学参考书。

公司职员：本书能够使员工快速配置 H3C 交换机，帮助员工理解和熟悉 H3C 交换机相关网络应用和设置，提升工作效率。

一般用户：本书可以作为所有对网络技术感兴趣的爱好者学习网络技术的自学参考书籍。

本书内容涵盖了目前主流的交换机特性配置与应用场景，内容由浅入深。这充分凸显了 H3C 网络学院系列教程的特点——专业务实，学以致用。本书经过精心设计，便于知识的连贯和理解，学员可以在较短的学时内完成全部内容的学习。书中内容遵循国际标准，从而保证了良好的开放性和兼容性。

全书共 16 章。

第 1 章　H3C 以太网交换机产品介绍

本章介绍了以太网交换机发展历程、性能指标，H3C 系列以太网交换机的命名规则、特性和应用场合；最后，通过典型的 H3C 以太网交换机的解决方案，展示了如何在园区网内应用以太网交换机。

第 2 章　基本配置指导

本章给出了如何通过 Console 口、Telnet、Web 网管等登录交换机的配置示例，并给出了如何通过 FTP、TFTP 对交换机进行升级的配置示例，最后给出了如何对交换机的文件系统和配置文件进行管理的配置示例。

第 3 章　以太网接口配置指导

本章首先给出了二层以太网接口的配置示例，包括如何配置 Combo 端口、接口双工、速率、MDI、接口风暴抑制比等，然后又给出了三层以太网接口的 MTU 典型配置示例。

第 4 章　以太网交换配置指导

本章给出了以太网二层技术相关特性的配置示例，主要包括 MAC 地址表管理、链路聚合、端口隔离、VLAN、GVRP、Voice VLAN、QinQ、BPDU Tunnel、VLAN 映射等特性的配置示例。

第 5 章　生成树协议配置指导

本章首先给出了 RSTP 的配置示例，然后给出了 MSTP 的配置示例。

第 6 章　堆叠技术配置指导

本章首先给出了 HGMP 的配置示例，然后根据不同场景，给出了 IRF 堆叠技术的配置示例。

第 7 章　三层技术——IP 业务配置指导

本章给出了有关 IP 业务的相关特性配置示例，主要包括 IP 地址与 IP 性能、ARP、DHCP、域名解析、UDP Helper 等特性的典型配置示例。

第 8 章　三层技术——IP 路由配置指导

本章给出了 IP 路由相关的配置示例，包括静态路由、RIP 协议、OSPF 协议、IS-IS 协议、BGP 协议、路由策略等。其中 OSPF 和 BGP 配置内容丰富，示例数量众多。

第 9 章　IPv6 配置指导

本章给出了 IPv6 相关的配置示例，主要包括 IPv6 地址配置、IPv6 隧道配置、IPv6 路由协议配置等。

第 10 章　IP 组播配置指导

本章给出了 IGMP 和 PIM 协议的配置示例。其中，PIM 又包含 PIM-DM、PIM-SM、PIM-SSM 等配置示例。

第 11 章　ACL 与 QoS 配置指导

本章首先给出了 IPv4 ACL 的配置示例，主要包括基本 ACL、高级 ACL、二层 ACL 等。然后给出了 IPv6 ACL 的配置示例，包括基本和高级 IPv6 ACL。为了使学员快速掌握典型 ACL 应用，本章还给出了 ACL 在报文过滤中的应用示例，最后给出了 QoS 配置示例，包括端口限速、队列调度、流量监管、流镜像、重定向等示例。

第 12 章　安全特性配置指导

本章首先给出了 AAA 的典型配置示例，然后给出了 802.1x 和 EAD 的配置示例。另外，本章还给出了 MAC 地址认证、Portal 认证、端口安全，以及 SSH 等众多安全特性的配置示例。

第 13 章　可靠性配置指导

本章给出了交换机上众多可靠性特性的配置示例，包括 DLDP、VRRP、RRPP、Smart Link、Track 等特性的配置示例。

第 14 章　网络管理与监控配置指导

本章给出了网络管理和监控特性的配置示例，主要包括信息中心的配置，SNMP 和 RMON 的配置，端口镜像、NTP、LLDP 等配置示例。

第 15 章　MPLS 与 MCE 配置指导

本章给出了 MPLS 相关特性的配置示例，主要包括 MPLS、VPLS、MPLS L3VPN 以及 MCE 特性的配置示例。

第 16 章　EPON-OLT 配置指导

本章给出了 EPON-OLT 相关接入特性的配置示例，主要包括 OLT 端口隔离、ONU、可控组播等特性的配置示例。

由于编者水平有限，加之时间仓促，书中错漏之处在所难免，欢迎读者批评指正。来函可发到本书主编处(E-mail：zhangdongliang@h3c.com)。

H3C 培训中心
2012 年 1 月

目 录

CONTETNS

第1章

H3C以太网交换机产品介绍

1.1 以太网交换机发展历程

1. 以太网标准的发展

以太网技术从1973年诞生以来，经历了很多的变化和演进。但为了向前兼容，以太网的发展都遵循了相同的实现机制和基本结构，在链路层采用LLC和MAC子层的结构，而在物理层则采用PCS、PMA和PMD的层次结构，从而很好地保证了新的以太网技术对前以太网技术的兼容。到目前为止，以太网技术的发展经历如下标准更新。

(1) 1973年，以太网之父罗伯·梅特卡夫博士(Dr. Robert Metcalfe)在Xerox的巴罗阿尔托研究中心发明了以太网。

(2) 1985年，IEEE正式推出标准以太网802.3 10Base-5的标准。

(3) 1988年，IEEE正式推出标准以太网802.3a 10Base-2的标准。

(4) 1990年，IEEE正式推出标准以太网802.3i 10Base-T的标准。

(5) 1993年，IEEE正式推出标准以太网802.3j 10Base-F的标准。

(6) 1995年，IEEE正式推出快速以太网802.3u 100Base-T的标准。

(7) 1998年，IEEE正式推出千兆位以太网802.3z 1000Base-X的标准。

(8) 1999年，IEEE正式推出千兆位以太网802.3ab 1000Base-T的标准。

(9) 2002年，IEEE正式推出万兆位以太网802.3ae 10GBase-R、10GBase-W和10GBase-X的标准。

(10) 2006年，IEEE正式推出万兆位以太网802.3an 10GBase-T的标准。

(11) 2010年，IEEE正式推出40Gbps/100Gbps以太网802.3ba 40GBase-R和100GBase-R的标准。

2. 以太网交换机的发展

就像人类对知识的渴求无止境一样，信息技术对传输带宽的需求也越来越高，这种需求推动网络设备不断地向前发展。作为最重要的网络设备，以太网交换机负责终端设备间的数据传输，其转发性能直接受限于其交换架构。

(1) 共享总线或共享内存架构

从另一个角度来看，实现上述以太网标准的技术在不同的时期采取了不同的交换结构。早期采用最基本的总线交换结构，多个连接在总线上的以太网实体之间通过交换总线交换数据，共享总线带宽，如图1-1所示。

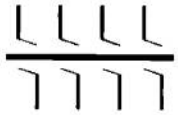


图 1-1 共享总线带宽架构示意图

在共享总线架构的交换机中，某一端口向另一端口转发数据时需要发出指令，表明需要占用总线资源，然后通过总线在端口间进行数据交换；在数据交换期间，其他端口不能交换数据。所以，共享总线架构的交换机其多端口间存在转发资源竞争关系，转发性能不高。

随着端口交换速率的提升，交换带宽的需求日益增加，总线式的交换架构已经无法满足需求，这时出现了新一代的共享内存交换。共享内存交换使用内存来取代交换总线。每个分支总线需要进行数据交换时，首先将其需要交换的数据写入这个内存中，并将内存地址（实际上是指针）告知引擎，引擎再通知另一个分支总线按照给定的指针信息进行数据的读取，从而完成两个分支总线的数据交换。共享内存交换通过高速的内存读/写操作，可以很大程度上提高交换带宽和交换速率。

但是，无论是共享总线交换还是共享内存交换，所有交换单元都共享同一交换资源，导致整体交换性能存在瓶颈。所以，采用共享总线交换或共享内存交换的以太网交换机具有天生的缺陷，其转发能力受到一定的限制。

大多数盒式交换机是共享总线或共享内存架构的。

（2）CrossBar 交换架构

因共享总线交换或共享内存交换架构的天生限制，开发者继而寻求一种新的交换架构，架构中的交换实体之间独享转发资源，交换性能更加强大。

CrossBar 交换架构采用输入/输出矩阵结构，实现任何两个交换实体都可以通过矩阵中的交叉连接点互连交换，而不影响其他交换实体间的数据交换，因此整个交换单元可以实现更大的交换容量，如图 1-2 所示。目前，单个 CrossBar 交换芯片可以实现从几百 Gbps 到 Tbps 级的交换容量。

在 CrossBar 交换架构中，任意两个端口之间想进行数据交换，只需要在矩阵中闭合两个交叉连接开关即可。图 1-2 中的端口 1 与端口 3 进行数据交换时，只需要闭合两个黑色圆点对应的连接开关即可，并且不影响其他端口之间的数据交换。如果多个端口同时交换数据，只需要同时闭合矩阵中的多个交叉连接开关。如此一来，每个端口的交换带宽可以得到大幅提升，同时整机的性能也得以大幅扩展，并且在这种矩阵内部，所有端口的转发没有任何阻塞。当然这种交换架构的实现原理相对复杂，硬件生产成本较高，一般只在高性能的高端设备上采用。

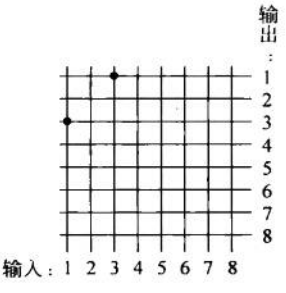


图 1-2 CrossBar 交换架构示意图

由于成本原因，通常在框式交换机中会采用 CrossBar 交换架构。

（3）CLOS 多级多平面交换架构

CrossBar 交换架构具有简单、高效的特点。但是，受限于芯片工艺和生产成本，采用 CrossBar 交换架构的交换机无法再快速扩大交换容量。在生产工艺没有突破的情况下，想达到更高级别的交换容量，需要从交换体系上创新。CLOS 多级多平面交换架构采用了全新的设计思想，在提升交换容量方面取得了新的突破。

CLOS 多级多平面交换架构中，包含有多级交换单元。每个下一级交换单元通过多个

上一级交换单元负载分担实现无阻塞交换，并且级数理论上可以无限延伸。实际应用常采用三级结构或者五级结构实现大容量无阻塞交换，从而突破单个 CrossBar 交换芯片的容量限制。

如图 1-3 所示，高速接口作为 CLOS 交换架构的输入/输出级，可以选择大容量交换芯片提供外部业务接口和上连交换矩阵的内部接口。为了尽可能地扩大交换矩阵的交换容量，交换矩阵采用多个交换平面共同为高速接口单元提供高速交换通道。如高速接口单元有 N 个上行链路，即可采用 N 个交换单元形成的交换矩阵，每个交换单元都与高速接口单元有 1 个甚至多个转发通道。由此在高速接口单元之间形成 $N\times N$ 条转发通道，通过智能调度实现 $N\times N$ 通道的负载分担以及冗余备份。理论上交换矩阵还可以继续采用三级结构实现容量扩展，依此类推实现多级延伸。

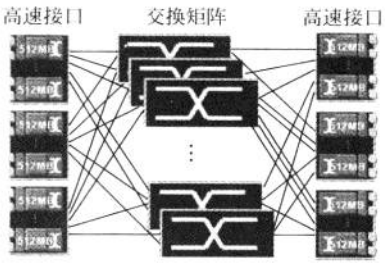


图 1-3 CLOS 多级多平面交换架构示意图

因 CLOS 多级多平面交换架构具有的这种多级层、大容量特性，通常只在核心网络设备中采用。

3. 以太网交换机的性能指标

以太网交换机作为局域网和城域网的主体设备，主要目标是实现终端主机的接入以及将接入流量汇聚后再高速交换到骨干网络。典型的园区网络层级结构中也明确介绍了接入层、汇聚层和核心层交换机的分工，为此人们在网络建设时需要根据不同的需求按照相应的设备性能指标进行准确选型。当前常用于衡量以太网交换机的性能指标有整机交换容量、包转发率、可靠性，对于机框式设备还有背板带宽。

(1) 交换容量

交换容量是衡量交换机转发能力的重要指标之一，它从设备能够提供的最大带宽来衡量交换机的转发性能。交换容量一般是指整机能够提供的所有业务端口的带宽之和，单位为 bps(比特/秒)。如 S5500-52C-EI 交换机可以提供 48GE+4×10GE，其交换容量(双向)为 48×2+4×10×2=176Gbps，单向则为 88Gbps。

(2) 包转发率

包转发率也是衡量交换机转发能力的重要指标之一，它从设备能够在单位时间内最大转发的报文数来衡量交换机的转发性能。包转发率一般是指整机能够在单位时间内转发 64B 报文的数量，单位为 pps(包/秒)。如果交换机支持线速转发，则可以通过交换容量换算。1Gbps 的线速交换容量换算为 64B 报文转发率为 1488.09Kpps，由此可以计算 S5500-52C-EI 交换机的包转发率为 130.94Mpps。

(3) 可靠性

交换机的可靠性通常包含有 MTBF(Mean Time Between Failure，平均无故障时间)和 MTTR(Mean Time To Repair，平均修复时间)等指标。

MTBF 是指设备在发生相邻两次故障之间正常可靠运行的时间间隔，MTBF 以小时为单位，时间间隔越大表明设备可靠性越高。

MTTR 是指设备发生故障后设备恢复正常运行需要花费的时间。MTTR 以小时为单

位，时间越短表明设备恢复性越好。

（4）背板带宽

背板带宽是指机框式或者机架式设备为各个业务单板之间提供的转发通道的带宽。为了满足设备的后期升级改造，产品设计初期都会参考整机交换容量考虑一定的余量，所以大多数情况背板带宽会高于整机交换容量。如 S7506E 交换机整机交换容量为 768Gbps，而背板带宽则大于等于 1.6Tbps。

1.2 H3C 以太网交换机产品系列介绍

杭州华三通信技术有限公司提供全系列以太网交换机，涵盖高端、中端和低端共计十几个系列产品。分别应用于网络的核心层、汇聚层和接入层，在企业网、运营商以及各大数据中心都有广泛应用。

1. H3C 以太网交换机命名规则

（1）机框式设备命名规则

H3C 中、高端以太网交换机都是机框式设备，且都属于三层交换机。其产品命名中最后两位数字表示设备支持的业务单板槽位数，前面的数字则表示系列名，其中系列名的末尾数字表示三层交换的含义，可能为 5 及以上的数字。如 S12518 高端核心路由交换机表示设备提供 18 个业务插槽，属于 S12500 系列且具有三层路由交换功能。

（2）盒式设备命名规则

H3C 低端以太网交换机都是盒式设备，分为二层交换机或三层交换机。为了便于描述，使用此类格式表示低端交换机的产品型号：S-AB-CC-DD-EE-PWR-FF。

① S 代表设备类型为交换机。

② AB 表示交换机系列。目前 A 为 5 表示千兆位或万兆位交换机，A 为 3 表示百兆位接入交换机；B 为大于等于 5 的数字则表示三层交换机，B 为小于 5 的数字则表示二层交换机。

③ CC 用于区分同等网络地位的不同系列。

④ DD 用于表示设备端口数量。

⑤ EE 用于表示设备的端口类型或者上行链路类型。如全光口交换机用 F 表示，如果上行链路灵活可配则用 C 表示，如果上行链路采用 SFP 光口则用 P 表示，如果同时提供千兆位电口和千兆位 SFP 光口则用 TP 表示，如果上行链路提供万兆位 SFP+端口则用 S 表示。

⑥ PWR 专指提供 PoE 供电的交换机，如果不提供 PoE 供电则无此区段。

⑦ FF 用于区分功能和性能不同的子系列。如 S5120 系列交换机分为超级型的 HI、增强型的 EI、标准型的 SI 以及轻量级的 LI 这 4 个子系列。

如 S5120-52C-PWR-EI 交换机表示属于二层千兆位交换机，整机提供 52 个业务端口，且上行端口可灵活选配，可以提供 PoE 供电，属于增强型系列交换机。

2. 核心路由交换机

（1）S12500 系列核心路由交换机

S12500 是面向下一代数据中心设计的核心交换产品，采用 CLOS 多级多平面交换架

构，可以提供持续的带宽升级能力。

S12500是一款100Gbps平台交换机，支持40GE和100GE以太网标准，整机可以提供576个万兆位端口，提供高密度的万兆位接入能力；面对数据中心突发流量，采用了“分布式入口缓存”技术，可以实现数据200ms缓存，满足数据中心、高性能计算等网络突发流量的要求；为了满足数据中心级网络高可靠、高可用、虚拟化的要求，S12500采用IRF2(Intelligent Resilient Framework 2，第二代智能弹性架构)设计，可将多台高端设备虚拟化为一台逻辑设备，同时支持独立的控制引擎、检测引擎、维护引擎，为系统提供强大的控制能力和50ms的高可靠保障。

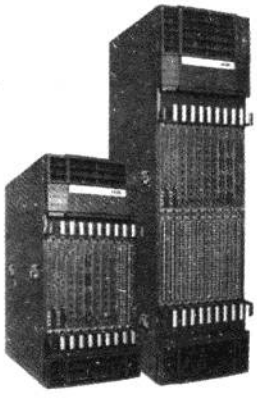


图1-4 S12500系列核心路由交换机

S12500产品包括S12508、S12518等型号，能够适应不同网络规模的端口密度和性能要求，结合H3C系列路由器、交换机、安全、存储以及iMC智能管理平台，可以为数据中心网络提供全系列的解决方案，如图1-4所示。

(2) S10500系列核心多业务交换机

H3C S10500系列交换机产品是面向园区网核心和城域网汇聚的核心交换产品，采用CLOS多级多平面交换架构，可以提供持续的带宽升级能力，支持40GE和100GE以太网标准。该产品基于H3C自主知识产权的Comware V5操作系统，以IRF2技术为系统基石的虚拟化软件系统，进一步融合MPLS VPN、IPv6、应用安全、应用优化、无线等多种网络业务，提供不间断转发、不间断升级、优雅重启、环网保护等多种高可靠技术，在提高用户生产效率的同时，保证了网络最大正常运行时间，从而降低了客户的总拥有成本(TCO)。S10500产品包括S10504、S10508、S10508-V这3个型号，能够适应不同网络规模的端口密度和性能要求，如图1-5所示。

3. 中、高端多业务路由交换机

(1) S9500E系列高端路由交换机

S9500E系列高端路由交换机是面向园区网和数据中心的核心高端交换机。S9500E在提供大容量、高性能L2/L3交换服务基础上，融合了硬件IPv6、硬件MPLS、安全、业务分析等智能特性，可为园区网、数据中心构建融合业务的基础网络平台。

S9500E采用高可靠、分布式的硬件设计，通过独立的控制引擎、检测引擎、维护引擎为系统提供统一的控制能力和50ms的高可靠保障；通过基于分布式的高性能硬件转发和大容量CrossBar无阻塞交换技术，确保系统具有高性能和高扩展能力；通过H3C的OAA开放架构，可以实现网络和安全、无线的融合。

H3C S9500E系列核心路由交换机包含如下型号，如图1-6所示。

① S9505E：5个业务板插槽，2个主控板插槽。

② S9508E/S9508E-V：8个业务板插槽，2个主控板插槽。

③ S9512E：12个业务板插槽，2个主控板插槽。

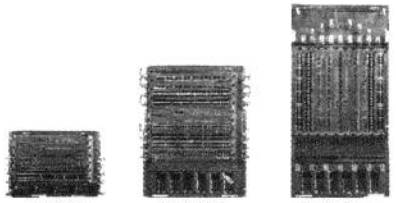


图 1-5 S10500 系列核心多业务交换机

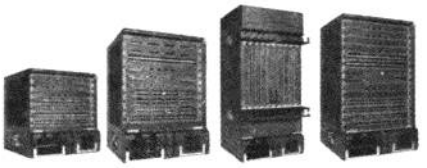


图 1-6 S9500E 系列高端交换机

(2) S7500E 系列中端多业务路由交换机

S7500E 系列产品是面向融合业务网络的机框式多业务路由交换机，基于 H3C 的 Comware V5 操作系统，以 IRF2 技术为系统基石的虚拟化软件系统，进一步融合 MPLS VPN、IPv6、网络安全、无线、无源光网络等多种网络业务，提供不间断转发、不间断升级、优雅重启、环网保护等多种高可靠技术。S7500E 符合“限制电子设备有害物质标准(RoHS)”，是绿色环保的路由交换机。

H3C S7500E 系列包括 S7510E(12 槽)、S7506E(8 槽)、S7506E-V(垂直 8 槽)、S7506E-S(8 槽)、S7503E(5 槽)、7503E-S(3 槽)和 S7502E(4 槽)7 款产品，如图 1-7 所示。除了 7503E-S 外，所有产品均支持冗余主控。S7500E 可应用于城域网、数据中心、园区网核心和汇聚等多种网络环境，为用户提供了有线无线一体化、有源无源一体化的行业解决方案。

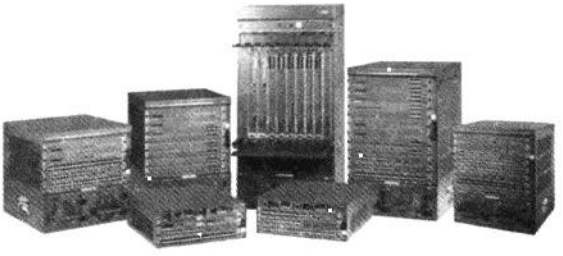


图 1-7 S7500E 系列中端多业务路由交换机

4. 数据中心级万兆位以太网交换机系列产品

(1) S5830 系列交换机

S5830 是数据中心级万兆位以太网交换机系列产品，采用业界先进的硬件结构设计，提供高密度接入端口，强大的端口报文缓存能力，而内置模块化双电源插槽设计双倍提升了设备的可用性。S5830 系列主要包括 S5830-52SC 和 S5830-106S，如图 1-8 所示。

图 1-8 S5830 系列交换机

(2) S5820X 系列交换机

S5820X 系列交换机是数据中心级万兆位以太网交换产品，为数据中心提供丰富的服务器接入方案，也可以用于园区网的汇聚层或接入层以及中小企业核心。

S5820X 系列交换机是业内最高性能的交换机之一，可同时提供最多 24 个全线速万兆位接口，使万兆位服务器高密度接入和园区网高密度万兆位汇聚成为可能。S5820X 系列交换机包括 S5820X-28S、S5820X-26S、S5820X-28C，如图 1-9 所示。

图 1-9 S5820X 系列交换机

(3) S5810 系列交换机

S5810 系列交换机是数据中心级万兆位以太网交换产品，为数据中心提供丰富的服务器接入方案，也可以用于园区网的汇聚层或接入层以及中小企业核心。

S5810 系列交换机提供超大的入口/出口缓存能力和高密度端口，内置模块化双电源插槽设计以提升设备可用性，完全适用于数据中心 Top of Rack 的应用要求。S5810 系列交换机包括 S5810-50S，如图 1-10 所示。

图 1-10 S5810 系列交换机

(4) S5800 系列交换机

S5800 系列交换机是另一款数据中心级万兆位以太网交换产品，为数据中心提供丰富的服务器接入方案，也可以用于园区网的汇聚层或接入层以及中小企业核心。

S5800 系列交换机支持 IRF2 技术，用户可以将多台 S5800 交换机连接，形成一个逻辑上的独立实体，从而构建具备高可靠性、易扩展性和易管理的新型智能网络。S5800 系列交换机包括 S5800-60C-PWR、S5800-56C-PWR、S5800-56C、S5800-32C-PWR、S5800-32C、S5800-32F、S5800-54S 等，如图 1-11 所示。

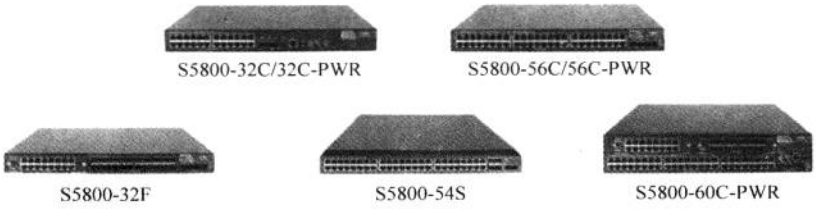


图 1-11 S5800 系列交换机

5. 三层千兆位及万兆位以太网交换机系列产品

三层千兆位及万兆位以太网交换机产品主要是 S5500 系列，包含 S5500-HI、S5500-EI 和 S5500-SI 共 3 个子系列产品。

(1) S5500-HI 系列交换机

S5500-HI 系列交换机是增强型 IPv6 三层万兆位以太网交换机产品，具备先进的硬件处理能力和丰富的业务特性，支持最多 6 个万兆位接口，在 1U 设备上实现高端口密度和灵活端口扩展能力，支持 IPv4/IPv6 硬件双栈及线速转发。另外，其出色的安全性、可靠性和多业务支持能力使其成为大型企业网络和园区网的汇聚，中、小企业网核心以及城域网边缘设备的选择。它包含 S5500-34C-HI 和 S5500-58C-HI，如图 1-12 所示。

图 1-12 S5500-HI 系列交换机

(2) S5500-EI 系列交换机

S5500-EI 系列交换机是增强型 IPv6 三层万兆位以太网交换机产品，支持最多 4 个万兆位扩展接口，支持 IPv4/IPv6 硬件双栈及线速转发。除此以外，其出色的安全性、可靠性和多业务支持能力使其成为大型企业网络和园区网的汇聚，中、小企业网核心以及城域网边缘设备的选择。

S5500-EI 系列以太网交换机目前包含 S5500-28C-EI、S5500-52C-EI、S5500-28C-PWR-EI、S5500-52C-PWR-EI、S5500-28F-EI，如图 1-13 所示。

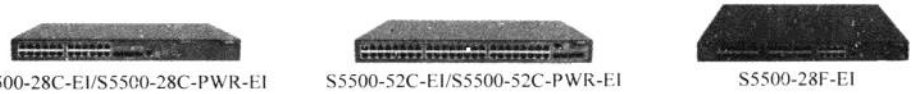


图 1-13 S5500-EI 系列交换机

(3) S5500-SI 系列交换机

S5500-SI 系列交换机是全千兆位三层以太网交换机产品，具备丰富的业务特性，提供 IPv6 转发功能以及最多 4 个 10GE 扩展接口。通过 H3C 特有的集群管理功能，用户能够简化对网络的管理。

S5500-SI 系列千兆位以太网交换机定位为企业网和城域网的汇聚或接入，同时还可以用于数据中心服务器群的连接。

S5500-SI 系列以太网交换机目前包含 S5500-28C-SI、S5500-52C-SI、S5500-28C-PWR-SI、S5500-52C-PWR-SI、S5500-24P-SI、S5500-48P-SI、S5500-20TP-SI，如图 1-14 所示。

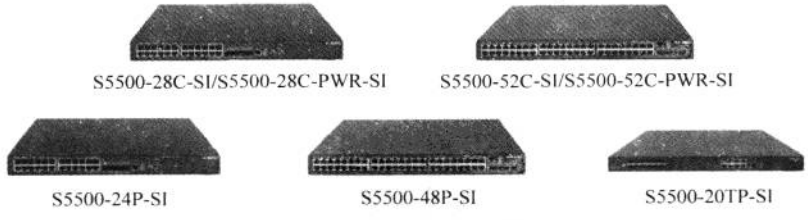


图 1-14 S5500-SI 系列交换机

6. 二层千兆位以太网交换机系列产品

二层千兆位以太网交换机主要是 S5120 系列，包含 S5120-HI、S5120-EI、S5120-SI 和 S5120-LI 共 4 个子系列。

(1) S5120-HI 系列交换机

S5120-HI 系列交换机是全千兆位以太网交换机产品，具备丰富的业务特性，提供 IPv6 转发功能以及最多 4 个 10GE 扩展接口，通过 H3C IRF2 功能，简化对网络的管理。S5120-HI 系列交换机采用前后风道，模块化电源、模块化风扇设计，是专门为 IDC 数据中心量身定制的接入交换机，如图 1-15 所示。

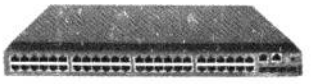


图 1-15 S5120-HI 系列交换机

(2) S5120-EI 系列交换机

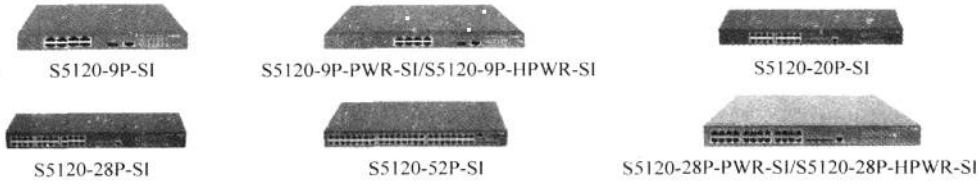
S5120-EI 系列交换机是全千兆位以太网交换机产品，具备丰富的业务特性，提供 IPv6 转发功能以及最多 4 个 10GE 扩展接口，通过 H3C IRF2 功能，简化对网络的管理。S5120-EI 系列千兆位以太网交换机定位为企业网千兆位接入，同时还可以用于数据中心服务器群的连接。S5120-EI 系列交换机包括 S5120-28C-EI、S5120-52C-EI、S5120-28C-PWR-EI、S5120-52C-PWR-EI、S5120-24P-EI 和 S5120-48P-EI，如图 1-16 所示。

S5120-24P-EI　S5120-48P-EI　S5120-28C-EI/S5120-28C-PWR-EI　S5120-52C-EI/S5120-52C-PWR-EI

图 1-16 S5120-EI 系列交换机

(3) S5120-SI 系列交换机

S5120-SI 系列以太网交换机是全千兆位以太网交换机，广泛应用于企业网和园区网的接入层，提供灵活的全千兆位以太网端口的接入密度、丰富的业务特性，支持 IRF 技术。S5120-SI 系列交换机包括 S5120-9P-SI、S5120-9P-PWR-SI、S5120-9P-HPWR-SI、S5120-20P-SI、S5120-28P-SI、S5120-52P-SI、S5120-28P-PWR-SI 和 S5120-28P-HPWR-SI，如图 1-17 所示。



S5120-9P-SI　S5120-9P-PWR-SI/S5120-9P-HPWR-SI　S5120-20P-SI

S5120-28P-SI　S5120-52P-SI　S5120-28P-PWR-SI/S5120-28P-HPWR-SI

图 1-17 S5120-SI 系列交换机

(4) S5120-LI 系列交换机

S5120-LI 系列以太网交换机是二层线速智能型可网管的入门级千兆位以太网交换机产品，具有全千兆位接口、大缓存设计，具备高速率、低时延的转发性能，可以为用户提供高性能、低成本、可网管的千兆到桌面的解决方案。S5120-LI 系列交换机包括 S5120-28P-LI 和 S5120-52P-LI，如图 1-18 所示。

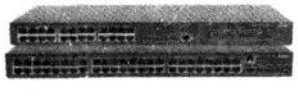


图 1-18 S5120-LI 系列交换机

7. 百兆位以太网交换机系列产品

(1) S3610 系列交换机

S3610 系列多协议交换机是支持 IPv4/IPv6 双栈的盒式路由交换机系列。系统支持 IPv4/IPv6 双栈及硬件转发、丰富的 IPv4/IPv6 路由协议和隧道技术，是大型园区网、网络实验室的汇聚、接入交换机以及中小企业、分支机构的核心交换机。H3C S3610 系列多协议交换机目前包含 S3610-28P、S3610-28TP、S3610-28F、S3610-52P 和 S3610-52M，如图 1-19 所示。

图 1-19 S3610 系列交换机

(2) S3600 系列交换机

S3600 系列交换机是智能弹性以太网交换机。系统采用 IRF 技术，在安全可靠、多业务融合、易管理和维护等方面为用户提供全新的技术特性和解决方案，是办公网、业务网和驻地网的汇聚、接入交换机以及中小企业、分支机构的核心交换机。S3600 系列智能弹性交换机目前包含 S3600-EI 和 S3600-SI 两个子系列。其中 S3600 EI 包含 S3600-28P-EI、S3600-52P-EI、S3600-28P-PWR-EI、S3600-52P-PWR-EI、S3600-28F-EI 等交换机；S3600-SI 包含 S3600-28P-SI、S3600-52P-SI、S3600-28TP-SI、S3600-28P-PWR-SI、S3600-52P-PWR-SI 等交换机，如图 1-20 所示。

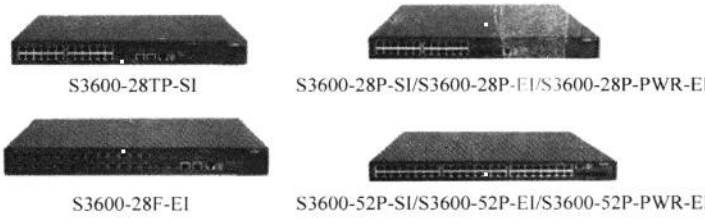


图 1-20 S3600 系列交换机

(3) S3100 系列交换机

S3100 系列交换机包含 S3100-EI 和 S3100-SI 两个子系列。

S3100-EI 系列交换机是 H3C 公司为构建高安全、高智能网络需求而设计的以太网交换机产品，在满足高性能接入的基础上，提供全面的安全接入策略和更强的网络管理维护易用性，是安全易用的接入层交换机。S3100-EI 系列交换机主要包含 S3100-8TP-EI、S3100-16TP-EI、S3100-26TP-EI、S3100-8TP-PWR-EI、S3100-16TP-PWR-EI、S3100-26TP-PWR-EI，如图 1-21 所示。

S3100-SI 系列交换机是二层线速智能型可网管以太网交换机产品，具有千兆位上行、可堆叠、无风扇静音设计、完备的安全和 QoS 控制策略等特点，满足企业用户多业务融合、高安全、可扩展、易管理的建网需求，适合行业、企业网、宽带小区的接入和中小企业、分支机构汇聚交换机。S3100-SI 系列交换机主要包含 S3100-8TP-SI、S3100-16TP-SI、S3100-

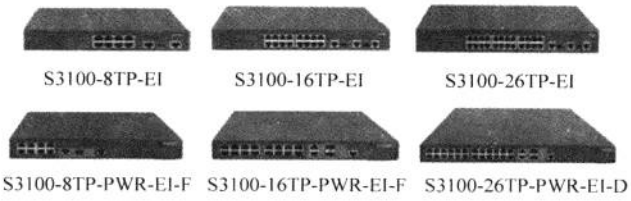


图 1-21 S3100-EI 系列交换机

26TP-SI 以及 S3100-52TP-SI，如图 1-22 所示。

图 1-22 S3100-SI 系列交换机

除了以上交换机外，H3C 还针对 SMB(Small and Midium-sized Business，中小企业商业)推出 S1000、S2000、S5000 系列网管型二层以太网交换机，针对教育行业构建高安全、高智能网络需求而推出 E 系列教育网以太网交换机。读者可以到 H3C 官方网站进行查看。

1.3 典型园区网交换机解决方案

科技以人为本，客户的需求就是产品开发导向。H3C 针对不同用户需求，开发出各类丰富、功能多样的网络设备产品，并对客户的不同业务需求而量身打造系列解决方案。

1. 中小园区网解决方案

(1) 网络需求

某企业需要构建高性能园区网络，目的是实现企业内资源共享、无纸化办公，提供管理应用系统，实现企业办公自动化，能够接入 Internet、收发 E-mail、共享 Internet 资源。

(2) 需求分析

企业当前有员工约 100 人，因此普通信息接入点在 100 个左右，在根据部门需要各部门会有一定数量的本地服务器、打印机等终端接入，最终信息接入点约 120 个，考虑到公司未来发展需要，规划网络最终规模可能达到 300 个信息接入点。为了能够确保无纸化办公真正得到实现，网络的可靠性要求较高，而且具备较强的网络管理能力，快速定位网络故障，恢复网络运行，且确保网络免受外网的攻击。鉴于此，本方案推荐采用 100Mbps 接入交换机，核心三层汇聚交换机完成所有信息点的互连互通。可在核心机房部署一套网络管理系统并在网络出口路由器与局域网之间部署硬件防火墙，隔离内部局域网和 Internet。

(3) H3C 推荐的解决方案(见图 1-23)

根据详细的需求分析和网络设备性能指标匹配，本方案推荐接入层交换机采用 S3100-EI 系列智能二层全线速交换机。S3100-EI 系列交换机可以灵活部署安全接入认证技术，实现局域网用户的安全接入，同时还支持其他丰富的安全特性，如端口安全、ARP Detection 等安全技术，打造安全局域网。核心层采用 S5500-SI 或者 S5500-EI 系列全线速千兆位三层交换机，作为各个业务部门的接入网关，实现各部门之间的内部高速互连。网络出口部署

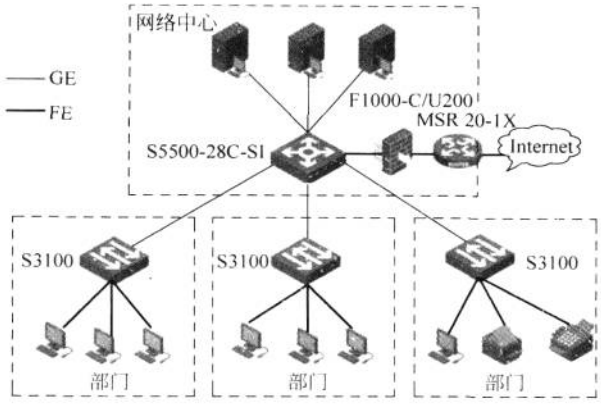


图 1-23 中、小园区网解决方案示意图

MSR 路由器，以满足内部用户访问 Internet 的需求。用户可在 MSR 路由器和核心交换机之间部署 F1000 或 U200 以实现网络安全隔离和移动 VPN 用户接入。

2. 大型园区网解决方案

（1）网络需求

某大学需要实现校园多校区互连，统一接入 CERNET、CERNET2 和 Internet，共享网络资源，建立学校的 IT 系统，实现教学信息化，同时提供一个对外宣传的信息平台，向外界宣传学校形象、各项学术活动及最新研究成果等。

（2）需求分析

校园分为多个校区，每个校区物理位置分布在同一城市的不同地方。因此需要在每个校区建立独立的局域网，通过核心设备将各校区互连后统一接入 CERNET 及 Internet。每个校区分为学生宿舍区、教师宿舍区以及教学办公区，同时在主校区建立学校的数据中心以及图书馆的局域网。

本方案在学生宿舍区采用接入认证技术实现用户身份认证和计费；在教学办公区采用接入认证技术实现终端身份认证但无计费需求；数据中心实现服务器的集中接入。CERNET2 为下一代教育网，专为 IPv6 终端和应用服务，因此网络设备需要支持 IPv4 和 IPv6 双栈转发。

（3）H3C 推荐的解决方案

本方案根据详细的需求分析和网络设备性能指标匹配，规划整个网络采用多台 S9500E 万兆位核心交换机组成校园核心网，实现了全网高性能、高带宽、高可靠的互连互通；核心层的 S9500E 交换机使用万兆位链路和分校区的 S9500E 交换机互连。

网络出口位置选用 H3C 企业级高可靠路由器 SR8800 系列路由器，全面支持 IPv4/IPv6 双栈协议。

楼宇汇聚选用 S7500E 和 S5500-EI 系列交换机，实现千兆位接入万兆位上行。

楼层接入选用 S5120-EI 或教育专用交换机 E126A 等实现接入终端的身份认证以及计费，确保接入用户的安全。

数据中心和图书馆局域网选用数据中心专用 S5800 系列交换机实现服务器的高速

访问。

整网从出口到接入全面支持 IPv4/IPv6 双栈协议，承载整个校园数万用户，多 GE 聚合接入 CERNET、Internet 以及 CERNET2，为学校的下一代网络的建设提供了有力保障。解决方案示意图如图 1-24 所示。

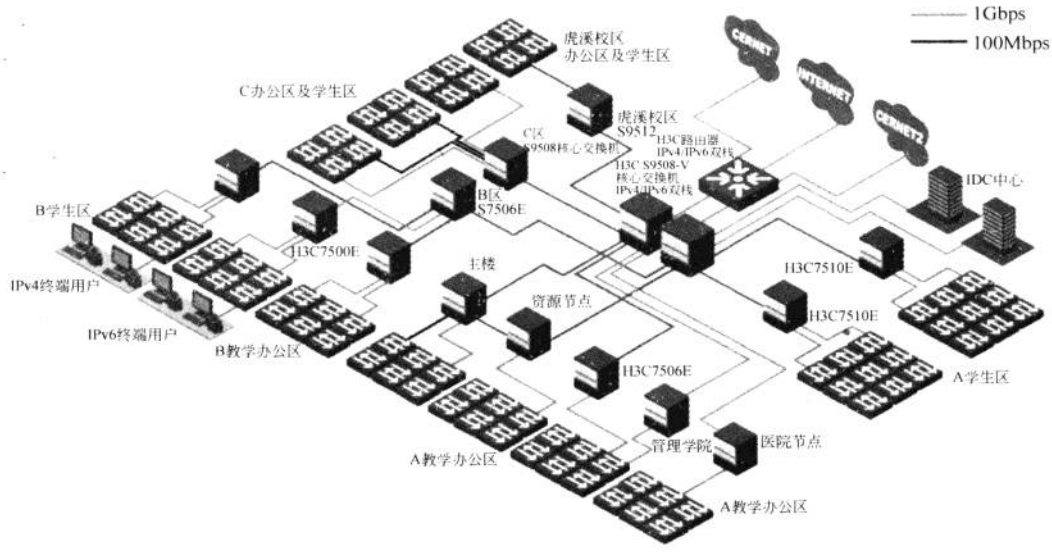


图 1-24 大型园区网解决方案示意图

有关更多的解决方案，读者可参见 H3C 网站。

第2章

基本配置指导

2.1 登录交换机典型配置指导

2.1.1 Console 口登录认证典型配置指导

1. 背景

M 公司的 IT 维护部门购买了一批 H3C 以太网交换机，由网络管理员负责对这些新设备进行相应的安装和配置。对于新的网络设备，通常会使用 PC 和配置电缆直接连接到设备的 Console 口进行初始配置。

默认情况下，交换机的 Console 口登录认证方式为 None，即不需要认证。为了设备安全起见，需要对其认证方式进行修改，并设定认证密码。

2. 组网图

图 2-1 所示为 Console 口登录认证典型配置组网图。

图 2-1 Console 口登录认证典型配置组网图

3. 配置需求

如图 2-1 所示，管理员对用户通过 Console 口登录到交换机的认证方式、参数进行相关配置，要求用户必须通过认证而登录到交换机，且用户级别是管理级(3 级)。

4. 配置过程和解释

Console 口登录有 3 种认证方式：None、Password 和 Scheme。下面分别描述这 3 种认证方式的配置。

(1) 设置登录用户的认证方式为 None。

```
[Sysname] user-interface aux 0
[Sysname-ui-aux0] authentication-mode none
```

(2) 设置登录用户的认证方式为 Password，并设置用户的认证口令为明文方式，口令为 123456。

```
[Sysname] user-interface aux 0
[Sysname-ui-aux0] authentication-mode password
[Sysname-ui-aux0] set authentication password simple 123456
```

(3) 设置登录用户的认证方式为 Scheme，采用本地认证的方式。

① 创建本地用户 guest，并进入本地用户视图。

```
[Sysname] local-user guest
```

② 设置本地用户的认证口令为明文方式，口令为 123456。

```
[Sysname-luser-guest] password simple 123456
```

③ 设置本地用户的服务类型为 Terminal 且用户级别为 2。

```
[Sysname-luser-guest] service-type terminal level 2
[Sysname-luser-guest] quit
```

④ 进入 AUX 用户界面视图。

```
[Sysname] user-interface aux 0
```

⑤ 设置通过 Console 口登录交换机的用户进行 Scheme 认证。

```
[Sysname-ui-aux0] authentication-mode scheme
```

⑥ 指定 system 域为默认域，并设置该域 Scheme 认证方式 local。

```
[Sysname] domain default enable system
[Sysname] domain system
[Sysname-isp-system] authentication default local
```

提示：本例中，管理员应该选择认证方式为 Password 或 Scheme。认证方式为 Scheme 有更高的安全性，因为用户需要同时知道用户名和密码才能够登录到设备。

2.1.2 Telnet 远程登录参数典型配置指导

1. 背景

管理员在完成新设备的上架安装和全部配置之后，M 公司的新网络设备已经可以正常运行了。在设备的运行维护过程中，管理员通常也需要时常登录设备查看一些信息或进行简单的调试。由于使用 Console 口登录设备需要本地直连，在这种情况下显得不那么方便。因此，需要在设备上进行 Telnet 远程登录的相关配置，以保证管理员可以通过网络远程登录设备进行操作。

2. 组网图

图 2-2 所示为 Telnet 远程登录参数典型配置组网图。

图 2-2 Telnet 远程登录参数典型配置组网图

3. 配置需求

如图 2-2 所示，管理员对用户通过 Telnet 登录到交换机的认证方式、参数进行相关配置。要求认证方式不限，但用户级别必须是管理级(3 级)。

4. 配置过程和解释

(1) 配置 Telnet 登录方式的公共属性。

① 进入系统视图，启动 Telnet 服务。

```
<Sysname> system-view
[Sysname] telnet server enable
```

② 配置从 VTY 用户界面登录后可以访问的命令级别为 3 级。

```
[Sysname] user-interface vty 0
[Sysname-ui-vty0] user privilege level 3
```

③ 设置 VTY 0 用户界面支持 Telnet 协议。

```
[Sysname-ui-vty0] protocol inbound telnet
```

④ 设置 VTY 0 用户的终端屏幕的一屏显示 30 行命令。

```
[Sysname-ui-vty0] screen-length 30
```

⑤ 设置 VTY 0 用户历史命令缓冲区可存放 20 条命令。

```
[Sysname-ui-vty0] history-command max-size 20
```

⑥ 设置 VTY 0 用户界面的超时时间为 6min。

```
[Sysname-ui-vty0] idle-timeout 6
```

提示：为了设备安全，默认情况下，系统设置成从 VTY 用户界面登录后可以访问的命令级别为 0 级，即最低权限级别。

(2) 配置通过 Telnet 登录用户的认证方式。Telnet 登录有 3 种认证方式：None、Password 和 Scheme。下面分别描述这几种认证方式的配置。

① 设置通过 VTY 0 用户界面登录交换机的 Telnet 用户不需要进行认证。

```
[Sysname] user-interface vty 0
[Sysname-ui-vty0] authentication-mode none
```

② 设置通过 VTY 0 口登录交换机的 Telnet 用户进行 Password 认证，并设置用户的认证口令为明文方式，口令为 123456。

```
[Sysname] user-interface vty 0
[Sysname-ui-vty0] authentication-mode password
[Sysname-ui-vty0] set authentication password simple 123456
```

③ 设置登录用户的认证方式为 Scheme，采用本地认证的方式。

a. 创建本地用户 guest，并进入本地用户视图。

```
[Sysname] local-user guest
```

b. 设置本地用户的认证口令为明文方式，口令为 123456。

```
[Sysname-luser-guest] password simple 123456
```

c. 设置 VTY 用户的服务类型为 Telnet 且用户级别为 3。

```
[Sysname-luser-guest] service-type telnet level 3
[Sysname-luser-guest] quit
```

d. 进入 VTY 用户界面视图。

```
[Sysname] user-interface vty 0
```

e. 设置通过 VTY 0 口登录交换机的 Telnet 用户进行 Scheme 认证。

```
[Sysname-ui-vty0] authentication-mode scheme
[Sysname-ui-vty0] quit
```

f. 指定 system 域为默认域，并设置该域 Scheme 认证方式 local。

```
[Sysname] domain default enable system
[Sysname] domain system
[Sysname-isp-system] authentication default local
```

提示：为了设备安全，不建议设置 Telnet 用户不需要进行认证。所以在本例中，应该选择认证方式为 Password 或 Scheme。

2.1.3 Web 网管远程登录交换机典型配置指导

1. 背景

无论是通过 Console 口登录或通过 Telnet 远程登录，都需要管理员与设备之间进行文本类指令交互，属于命令行接口(Command Line Interface，CLI)。虽然其有着输入简单、命令含义丰富的特点，但同时也有着界面不够友好、直观的缺点。

基于维护管理方便的考虑，M 公司的 IT 维护部门要求使用 Web 网管功能对交换机进行远程管理。这样对管理员来说，不需要记忆很多命令行，也一样能够进行一些例行化的配置和维护。

2. 组网图

图 2-3 所示为 Web 网管远程登录交换机典型配置组网图。

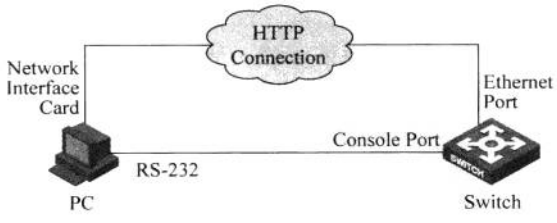


图 2-3 Web 网管远程登录交换机典型配置组网图

3. 配置需求

如图 2-3 所示，管理员通过配置交换机，从而实现网络中的 PC 通过 Web 网管登录交换机，实现对交换机的远程图形化管理。

4. 配置过程和解释

(1) 通过 Console 口正确配置以太网交换机 VLAN 1 接口的 IP 地址(VLAN 1 为交换机的默认 VLAN)为 10.153.17.82，子网掩码为 255.255.255.0。

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-VLAN-interface1] ip address 10.153.17.82 255.255.255.0
[Sysname-VLAN-interface1] quit
```

(2) 配置 Web 网管用户名为 admin，认证口令为 admin，用户级别为 3 级。

```
[Sysname] local-user admin
[Sysname-luser-admin] service-type telnet level 3
[Sysname-luser-admin] password simple admin
[Sysname-luser-admin] quit
```

(3) 开启交换机的 Web Server 功能。

```
[Sysname] ip http enable
```

(4) 通过浏览器登录交换机。在 Web 网管终端(PC)的浏览器地址栏内输入 http://10.153.17.82(Web 网管终端和以太网交换机之间要路由可达)，浏览器会显示 Web 网管的登录页面，如图 2-4 所示。

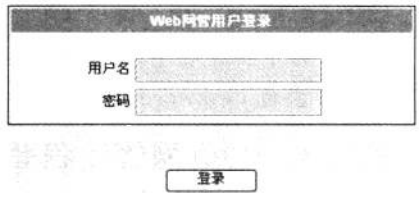


图 2-4 Web 网管用户登录页面

(5) 输入在交换机上添加的用户名和密码，单击“登录”按钮后即可登录，显示 Web 网管初始页面。

提示：如发生通过浏览器不能登录交换机的情况，可以先用 ping 命令来查看到交换机的网络连通性。HTTP 只有在 IP 层可达时才能正常工作。

2.1.4 对远程登录用户的控制典型配置指导

1. 背景

交换机作为重要的网络设备，其配置的安全性要得到保障。所以，M 公司的 IT 维护部门要求对登录用户进行控制，只允许相关的维护人员能够登录交换机。由于设备放置于 IT 维护部门的机房内，所以通过对进出机房人员进行控制，能够达到控制 Console 口本地登录的目的。但对于远程登录，则必须在交换机上配置 ACL 来进行访问控制。

通过对登录用户的控制，可以实现哪些用户(用 IP 地址来区分)能够访问网络设备，实现更高的安全性。

2. 组网图

图 2-5 所示为对远程登录用户的控制典型配置组网图。

3. 配置需求

如图 2-5 所示，为了安全起见，仅允许来自 10.110.100.52 和 10.110.100.46 的 Telnet/SNMP/Web 用户访问交换机。

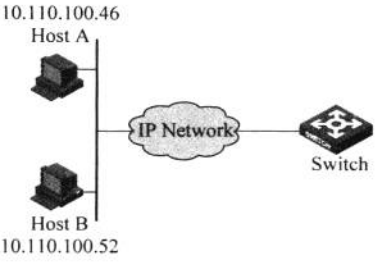


图 2-5 对远程登录用户的控制典型配置组网图

4. 配置过程和解释

(1) 创建并进入基本 ACL 视图 2000。

```
[Sysname] acl number 2000 match-order config
[Sysname-acl-basic-2000]
```

(2) 定义子规则，仅允许来自 10.110.100.52 和 10.110.100.46 的 Telnet/SNMP/Web 用户访问交换机。

```
[Sysname-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[Sysname-acl-basic-2000] rule 2 permit source 10.110.100.46 0
[Sysname-acl-basic-2000] rule 3 deny source any
[Sysname-acl-basic-2000] quit
```

(3) 引用访问控制列表 2000，通过源 IP 对 Telnet 用户进行控制。

```
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] acl 2000 inbound
```

(4) 引用访问控制列表 2000，通过源 IP 对网管用户进行控制。

```
[Sysname] snmp-agent community read aaa acl 2000
[Sysname] snmp-agent group v2c groupa acl 2000
[Sysname] snmp-agent usm-user v2c usera groupa acl 2000
```

(5) 引用访问控制列表 2000，通过源 IP 对 Web 用户进行控制。

```
[Sysname] ip http acl 2000
```

提示：默认情况下，中、低端交换机允许 5 个 Telnet/SNMP/Web 用户访问。所以，本例中需要用 ACL 对 5 个远程登录用户均定义访问规则。

2.2 在线远程升级交换机典型配置指导

2.2.1 交换机作为 FTP 客户端远程升级典型配置指导

1. 背景

C 公司使用了大量 H3C 交换机。因网络改造，需要将所有交换机升级成最新的系统文件，以适应新网络的需要。

管理员小 W 负责此次升级业务。他决定采取 FTP 方式，将系统文件从 FTP 服务器上下载到交换机上并完成升级，这是一个简单易用且快捷的方式。

2. 组网图

图 2-6 所示为交换机作为 FTP 客户端远程升级典型配置组网图。

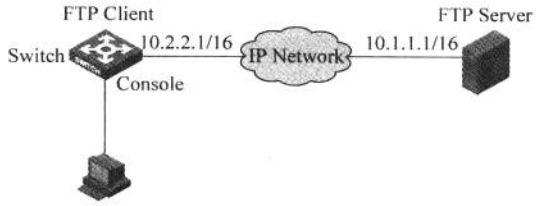


图 2-6 交换机作为 FTP 客户端远程升级典型配置组网图

3. 配置需求

如图 2-6 所示，服务器上已设置设备登录 FTP 服务器的用户名为 abc，密码为 pwd。设备以用户名 abc、密码 pwd 登录 FTP 服务器，下载系统启动文件并进行系统重启以升级设备。

4. 配置过程和解释

(1) 配置 FTP 服务器，包括启动 FTP 服务器并设置工作目录，具体配置步骤略。

(2) 配置交换机(FTP 客户端)。

① 删除设备中的多余文件，以保证剩余足够的空间，用于存储新的启动文件。

```
<Sysname> dir
Directory of flash:/

  0   drw-          -  Dec 07 2005 10:00:57   filename
  1   drw-          -  Jan 02 2006 14:27:51   logfile
  2   -rw-       1216  Jan 02 2006 14:28:59   config.cfg
  3   -rw-       1216  Jan 02 2006 16:27:26   backup.cfg

31496 KB total (12133 KB free)
<Sysname> delete /unreserved flash:/backup.cfg
```

② 以 FTP 方式登录服务器，获取系统启动文件。

```
<Sysname> ftp 10.1.1.1
Trying 10.1.1.1 ...
Press Ctrl+K to abort
Connected to 10.1.1.1.
220 FTP service ready.
User(10.1.1.1:(none)):abc
331 Password required for abc.
Password:
230 User logged in.
[ftp] binary
200 Type set to I.
[ftp] get aaa.bin bbb.bin

227 Entering Passive Mode (10.1.1.1,4,1).
125 BINARY mode data connection already open, transfer starting for aaa.bin.
...226 Transfer complete.
FTP: 5805100 byte(s) received in 19.898 second(s) 291.74 byte(s)/sec.
```

[ftp] bye

③ 用户可以通过 boot-loader 命令来指定获取的文件为下次启动时的主用启动文件，重启设备后，实现设备启动文件的升级。

<Sysname> boot-loader file bbb.bin main
<Sysname> reboot

提示：boot-loader 命令指定的下次启动时的启动文件必须存放在设备的根目录下。可使用文件的复制或移动操作来调整文件的路径为根目录。

对于框式交换机来说，指定主用启动文件时，boot-loader 命令中需要指定槽位编号，例如，boot-loader file bbb.app slot 1 main。

2.2.2 交换机作为 FTP 服务器远程升级典型配置指导

1. 背景

在升级过程中，小 W 发现将设备作为 FTP 客户端时，只能采取命令行方式，并没有他习惯使用的图形化交互界面。那能不能将设备作为 FTP 服务器，PC 作为 FTP 客户端呢？答案是肯定的。这样，小 W 就可以在 PC 上利用他经常使用的图形化 FTP 客户端软件而上传系统文件了。

2. 组网图

图 2-7 所示为交换机作为 FTP 服务器远程升级典型配置组网图。

图 2-7 交换机作为 FTP 服务器远程升级典型配置组网图

3. 配置需求

如图 2-7 所示，PC 作为 FTP 客户端，设备作为 FTP 服务器。PC 登录 FTP 服务器的用户名为 abc，密码为 pwd，登录后上传系统启动文件并进行系统重启以升级设备。

4. 配置过程和解释

(1) 配置 Device(FTP Server)。

① 在设备上添加一个本地用户 abc，并设置其认证密码为 pwd。

<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-abc] password simple pwd

② 指定 abc 可以使用的服务类型为 FTP，并设置其授权访问目录。

[Sysname-luser-abc] service-type ftp
[Sysname-luser-abc] work-directory flash:/

③ 配置 abc 的用户级别为 3 级，使其可以向访问目录中上传文件。

[Sysname-luser-abc] level 3

```
[Sysname-luser-abc] quit
```

④ 启动设备的 FTP 服务。

```
[Sysname] ftp server enable
[Sysname] quit
```

⑤ 删除设备中的多余文件，以保证剩余足够的空间，用于存储新的启动文件。

```
<Sysname> dir
Directory of flash:/
   0    drw-          -   Dec 07 2005 10:00:57    filename
   1    drw-          -   Jan 02 2006 14:27:51    logfile
   2    -rw-       1216   Jan 02 2006 14:28:59    config.cfg
   3    -rw-       1216   Jan 02 2006 16:27:26    back.cfg
   4    drw-          -   Jan 02 2006 15:20:21    ftp
31496 KB total (12133 KB free)
<Sysname> delete /unreserved flash:/back.cfg
```

(2) 配置 PC(FTP Client)。

① 以 FTP 方式登录 FTP 服务器，上传启动文件，并存放于 FTP 服务器的根目录下。

```
c:\> ftp 1.1.1.1
Connected to 1.1.1.1.
220 FTP service ready.
User(1.1.1.1:(none)):abc
331 Password required for abc.
Password:
230 User logged in.
ftp> put aaa.bin bbb.bin
200 Port command okay.
150 Opening BINARY mode data connection for bbb.bin.
226 Transfer complete.
ftp: 发送 2737556 字节，用时 7.02Seconds 390.24Kbytes/sec.
ftp>
```

② 用户可以通过 boot-loader 命令来指定上传的程序为下次启动时的主用启动文件(假设本例中的设备支持启动文件的主备用属性)，重启设备后，实现设备启动文件的升级。

```
<Sysname> boot-loader file bbb.bin
<Sysname> reboot
```

注意：设备作为 FTP 服务器时，对客户端的访问操作有级别限制。如果要对设备的文件系统执行写操作(如上传、删除、创建/删除文件夹)，则必须将 FTP 登录用户的级别设置为 3；如果执行其他操作(如普通的查看操作)，则 FTP 登录用户的级别不受限制，可以为 0～3 中的任意级别。

2.2.3 交换机作为 TFTP 客户端远程升级典型配置指导

1. 背景

小 W 升级了几台交换机后，还是觉得有些麻烦。因为每一次 FTP 登录交换机，都要输

入用户名和密码。这时，他想到 TFTP(Trivial File Transfer Protocol，简单文件传输协议)是个简单易用的文件传输协议，无须认证，也就不用输入用户名和密码。

2. 组网图

图 2-8 所示交换机作为 TFTP 客户端远程升级典型配置组网图。

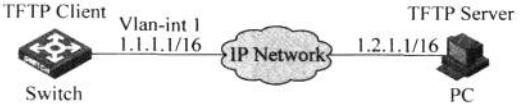


图 2-8 交换机作为 TFTP 客户端远程升级典型配置组网图

3. 配置需求

如图 2-8 所示，设备作为 TFTP 客户端，PC 作为 TFTP 服务器。设备通过 TFTP 从 TFTP 服务器上下载启动文件，同时将设备的配置文件 config. cfg 上传到 TFTP 服务器的工作目录实现配置文件的备份。

4. 配置过程和解释

(1) 配置 PC(TFTP 服务器)，包括启动 TFTP 服务器并设置工作目录，具体配置步骤略。

(2) 配置交换机(TFTP 客户端)。

① 将应用程序 aaa. bin 从 TFTP 服务器上下载到设备。

```
<Sysname> tftp 1.2.1.1 get aaa.bin bbb.bin
```

② 将设备的配置文件 config. cfg 上传到 TFTP 服务器。

```
<Sysname> tftp 1.2.1.1 put config.bin configback.bin
```

③ 用户可以通过 boot-loader 命令来指定下载的程序为下次启动时的主用启动文件(假设本例中的设备支持启动文件的主备用属性)，然后重启设备，实现设备启动文件的升级。

```
<Sysname> boot-loader file bbb.bin main
<Sysname> reboot
```

2.3 文件系统管理典型配置指导

2.3.1 文件系统管理典型配置指导

1. 背景

网络管理员在对设备完成配置后，通常要对设备运行过程中所需要的文件(主机软件、配置文件等)进行管理，主要包括目录的创建和删除、文件的复制和显示等。

2. 组网图

此处不涉及具体的组网需求。

3. 配置需求

此处不涉及配置需求。

4. 配置过程和解释

(1) 将现有配置文件备份到其他文件夹中。

① 查看当前目录下的文件及子目录。

```
<Sysname> dir
Directory of flash:/

  0   drw-          -   Feb 16 2006 11:45:36   logfile
  1   -rw-       1691   Feb 16 2006 11:46:19   config.cfg
  2   drw-          -   Feb 16 2006 15:20:27   test
  3   -rw-     184108   Feb 16 2006 15:30:20   aaa.bin

31496 KB total (10588 KB free)
```

② 创建名为 cfg_bak 的目录,用于备份配置文件。

```
<Sysname> mkdir cfg_bak
.
%Created dir flash:/cfg_bak.
```

③ 将 Flash 目录下的 config.cfg 文件复制到 cfg_bak 文件夹中。

```
<Sysname> copy contig.cfg flash:/cfg_bak
Copy flash:/config.cfg to flash:/cfg_bak/config.cfg?[Y/N]:y
..
%Copy file flash:/config.cfg to flash:/cfg_bak/config.cfg...Done.
<Sysname>
```

④ 进入 cfg_bak 目录,并查看当前工作目录。

```
<Sysname> cd cfg_bak
<Sysname> pwd
flash:/cfg_bak
```

⑤ 查看当前目录下的文件及子目录。

```
<Sysname> dir
Directory of flash:/cfg_bak/
  0     -rw-       1691   Apr 26 2007 18:32:23    config.cfg
31496 KB total (10588 KB free)
```

⑥ 将该文件重命名为 cfg_20080210.cfg,用于标识备份时间,并使用 dir 命令进行确认。

```
<Sysname> rename config.cfg cfg_20080210.cfg
Rename flash:/cfg_bak/config.cfg to flash:/cfg_bak/cfg_20080210.cfg?[Y/N]:y
.
%Renamed file flash:/cfg_bak/config.cfg to flash:/cfg_bak/cfg_20080210.cfg.
<Sysname> dir
Directory of flash:/cfg_bak/
  0     -rw-       1691   Apr 26 2000 18:52:03    cfg_20080210.cfg
31496 KB total (10588 KB free)
```

(2) 在配置出现错误时,将备份的配置文件进行恢复,以便迅速恢复网络畅通。

① 返回上一级目录。

```
<Sysname> cd ..
```

② 显示当前的工作路径。

```
<Sysname> pwd
flash:/
```

③ 将现有配置文件另存为 cfg_temp,保存到 cfg_bak 文件夹中。

```
<Sysname> copy config.cfg flash:/cfg_bak/cfg_temp.cfg
Copy flash:/config.cfg to flash:/cfg_bak/cfg_temp.cfg?[Y/N]:y
...
%Copy file flash:/config.cfg to flash:/cfg_bak/cfg_temp.cfg...Done.
```

④ 将 Flash 目录下的 config.cfg 文件彻底删除。

```
<Sysname> delete /unreserved config.cfg
The contents cannot be restored!!! Delete flash:/config.cfg?[Y/N]:y
Deleting a file permanently will take a long time. Please wait...
..
%Delete file flash:/config.cfg...Done.
```

⑤ 将 cfg_bak 目录中备份的 cfg_20080210.cfg 文件恢复到 Flash 根目录中,并重命名为 config.cfg。

```
<Sysname> copy flash:/cfg_bak/cfg_20080210.cfg flash:/config.cfg
Copy flash:/cfg_bak/cfg_20080210.cfg to flash:/config.cfg?[Y/N]:y
...
%Copy file flash:/cfg_bak/cfg_20080210.cfg to flash:/config.cfg...Done.
```

⑥ 使用 dir 命令确认配置文件已恢复成功。

```
<Sysname> dir
Directory of flash:/
  0   drw-        -   Feb 16 2006 11:45:36   logfile
  1   -rw-     1691   Feb 16 2006 12:15:19   config.cfg
  2   drw-        -   Feb 16 2006 15:20:27   test
  3   -rw-   184108   Feb 16 2006 15:30:20   aaa.bin
31496 KB total (10588 KB free)
```

说明:用户也可以在不删除错误的 config.cfg 文件的情况下,直接使用 copy 命令将备份的配置文件进行恢复,系统会在复制时提示用户是否进行覆盖,并选择覆盖。

2.3.2 配置文件管理典型配置指导

1. 背景

为了加强对配置文件的管理,管理员通常会对所有设备的配置文件进行集中式的管理。这样做的好处是降低管理成本,并在产生故障的时候能够快速恢复。

2. 组网图

此处不涉及组网图。

3. 配置需求

此处不涉及配置需求。

4. 配置过程和解释

(1) 将现有配置保存并进行远程备份。

① 将现有配置进行保存,使用默认文件名 config.cfg 并覆盖现有配置文件。

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/config.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/config.cfg exists, overwrite? [Y/N]:y

Validating file. Please wait...
Now saving current configuration to the device.
Saving configuration flash:/config.cfg. Please wait...
...
Configuration is saved to flash successfully.
```

② 将该配置文件备份到 TFTP 服务器(IP 地址为 192.168.0.4)上。

```
<Sysname> backup startup-configuration to 192.168.0.4
Backup next startup-configuration file to 192.168.0.4, please wait...
finished!
```

(2) 在设备上保存多个配置文件并指定下次启动时使用的配置文件。

① 在进行一系列配置后,将配置另存为 config_new.cfg 进行保存,并指定该配置文件的 backup 属性。

```
<Sysname> save backup
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/config.cfg]
(To leave the existing filename unchanged, press the enter key):config_new.cfg

Validating file. Please wait...
Now saving current configuration to the device.
Saving configuration flash:/config_new.cfg. Please wait...
...
Configuration is saved to flash successfully.
```

② 指定 config.cfg 作为下次启动时使用的配置文件。

```
<Sysname> startup saved-configuration config.cfg main
```

③ 如果当前启动的配置文件(config.cfg)出现问题,用户可以从 TFTP 服务器上将备份的配置文件进行恢复。

```
<Sysname> restore startup-configuration from 192.168.0.4 config.cfg
Configuration file config.cfg already exists. Overwrite? [Y/N]:y
Restore next startup-configuration file from 192.168.0.4. Please wait...
finished!
```

第3章

以太网接口配置指导

3.1 二层以太网接口典型配置指导

3.1.1 Combo 端口典型配置指导

Combo 端口是一个逻辑端口，一个 Combo 端口对应设备面板上的一个电口和一个光口。电口与其对应的光口均为设备上的以太网端口，是光电复用关系，两者不能同时工作（当激活其中的一个端口时，另一个端口就自动处于禁用状态），用户可根据组网需求选择使用电口或光口。

电口和光口有各自对应的端口视图。当用户需要激活电口或光口、配置电口或光口的属性（如速率、双工等）时，必须先进入对应的端口视图。

1. 背景

M 公司的 IT 维护部门购买了一批 H3C 以太网交换机，由网络管理员负责对这些新设备进行相应的安装和配置。对于这批新的网络设备，需要使用 Combo 端口中的光口进行设备互连。

2. 组网图

图 3-1 所示为 Combo 端口典型配置组网图。

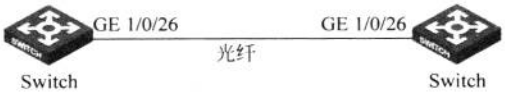


图 3-1 Combo 端口典型配置组网图

3. 配置需求

如图 3-1 所示，两台交换机之间通过 Combo 端口中的光口来实现设备之间的物理互连。

4. 配置过程和解释

配置准备过程如下：

(1) 通过 display port combo 命令了解设备上有哪些 Combo 端口，每个 Combo 端口是由哪两个物理端口组成的。

(2) 通过 display interface 命令了解组成 Combo 端口的两个物理端口中哪个是电口哪个是光口。如果显示信息中包含“Media type is twisted pair, Port hardware type is 1000_

BASE_T”，则表示该端口为电口；如果显示信息中包含“Media type is not sure，Port hardware type is No connector”，则表示该端口为光口。

完成配置准备工作，确认需要使用的物理端口为 GE 1/0/26 后，进行端口激活的配置。进入希望使用的以太网视图，激活 Combo 端口。

```
<Sysname> system-view
[Sysname] interface Gigabitethernet 1/0/26
[Sysname-GigabitEthernet1/0/26] undo shutdown
```

提示：默认情况下，Combo 端口之中编号较小的物理端口处于激活状态。

3.1.2 以太网接口双工与速率、MDI 典型配置指导

通常在网络设备互连过程中，设备的多样性会导致设备双工与速率、MDI 不匹配的情况出现，此时需要根据具体情况进行调整。

1. 背景

管理员在完成新设备的上架安装和全部配置之后，在连接服务器和 PC 的过程中发现由于设备型号较多，出现个别网络设备无法连通，或者物理连通后接口出现大量错包，ping 包丢包严重的情况。管理员需要对于接口工作的双工与速率、MDI 配置进行调整。

2. 组网图

图 3-2 所示为以太网接口双工与速率、MDI 典型配置组网图。

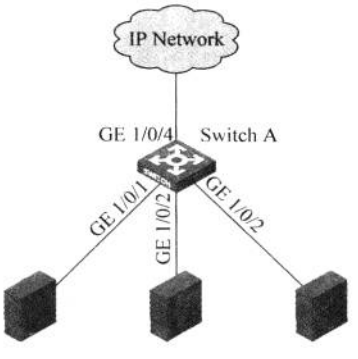


图 3-2 以太网接口双工与速率、MDI 典型配置组网图

3. 配置需求

如图 3-2 所示，管理员通过调整接口的双工与速率、MDI 配置来实现与不同网络设备间的匹配与互通。要求将 GE 1/0/1 接口的双工模式修改为全双工，GE 1/0/2 接口的自协商速率修改为 100Mbps，GE 1/0/3 接口的 MDI 修改为 across 模式以满足互通要求。

4. 配置过程和解释

(1) 进入 GE 1/0/1 端口，修改接口的双工模式为全双工。

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] duplex full
```

(2) 进入 GE 1/0/2 端口，修改接口的自协商速率为 100Mbps。

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] speed 100
```

(3) 进入 GE 1/0/3 端口，修改接口的 mdi 模式为 across。

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/3
[Sysname-GigabitEthernet1/0/3] mdi across
```

提示：默认情况下，以太网端口的双工模式为 auto(自协商)状态。光类型端口和配置了端口速率为 1000Mbps 的以太网电口不支持配置 half 参数。

默认情况下，以太网端口的速率为 auto(自协商)状态。千兆位光口不支持配置 10 和 10000 参数，万兆位光口不支持配置 10 和 100 参数。

默认情况下，以太网端口的 MDI 模式为 auto(自协商)状态。通常情况下，建议用户使用 auto 模式，只有当设备不能获取网线类型参数时，才需要将模式手动指定为 across 或 normal。

3.1.3 以太网接口环回测试典型配置指导

用户可以开启以太网接口环回测试功能，检验以太网接口能否正常工作。测试时接口将不能正常转发数据包。

以太网接口环回测试功能包括内部环回测试和外部环回测试。

(1) 内部环回测试：该测试在交换芯片内部建立自环，用于定位芯片内与该端口相关的功能是否出现故障，如图 3-3 所示。

(2) 外部环回测试：该测试需要在以太网接口上接一个自环头，从接口发出的报文通过自环头又环回到该接口，并被该接口接收，用于定位该端口的硬件功能是否出现故障，如图 3-4 所示。

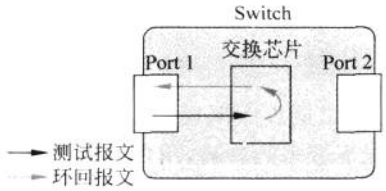


图 3-3 内部环回测试

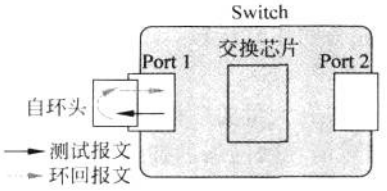


图 3-4 外部环回测试

一般按照先进行内部环回测试再进行外部环回测试的顺序来进行检验。

1. 背景

管理员通过修改接口的双工与速率、MDI 配置解决了大部分网络设备的互连互通问题，但是发现 GE 1/0/5 接口无论如何修改和调整这些参数还是无法实现互连，设备上的端口状态始终为 down 状态。这时候怀疑可能是端口的物理故障，需要做进一步的测试来验证端口功能是否正常。

2. 组网图

图 3-5 所示为以太网接口环回测试典型配置组网图。

图 3-5 以太网接口环回测试典型配置组网图

3. 配置需求

管理员通过配置接口的内部环回测试和外部环回测试来验证接口 GE 1/0/5 是否正常工作。

4. 配置过程和解释

进入需要测试的以太网接口视图，进行内部环回测试和外部环回测试。

```
[Sysname] interface GigabitEthernet1/0/5
[Sysname-GigabitEthernet1/0/5]loopback internal
Loop internal succeeded!
[Sysname-GigabitEthernet1/0/5]loopback external
Loop external succeeded!
```

提示：在进行某些特殊功能测试，如初步定位以太网故障时，需要开启以太网端口环回测试功能。

以太网端口开启环回测试功能时将工作在全双工状态；关闭环回测试功能后恢复原有配置。

环回测试配置是一次性操作，不会被记录在配置文件中。

3.1.4 风暴抑制比典型配置指导

在端口下进行配置，设置的是端口允许通过的最大广播/组播/未知单播报文流量。当端口上的广播/组播/未知单播流量超过用户设置的值后，系统将丢弃超出广播/组播/未知单播流量限制的报文，从而使端口广播/组播/未知单播流量所占的比例降低到限定的范围，保证网络业务的正常运行。

1. 背景

当网络中有大量的广播/组播/未知单播流量通过二层以太网端口时，会在端口上产生流量风暴，可能导致网络的拥塞。为了减少这种情况下带来的影响，用户可以通过在端口上配置风暴抑制比来限制二层以太网端口上允许通过的广播/组播/未知单播流量的大小。

2. 组网图

图 3-6 所示为风暴抑制比典型配置组网图。

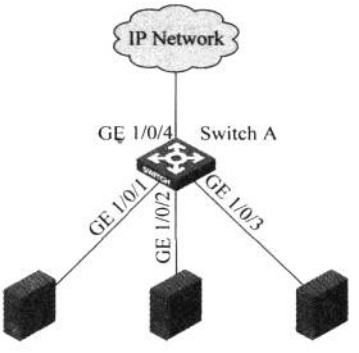


图 3-6 风暴抑制比典型配置组网图

3. 配置需求

设备上的 GE 1/0/1 到 GE 1/0/4 端口配置允许通过的最大广播流量为 1Mbps，最大组播流量为 512Kbps，最大未知单播流量为 512Kbps。为了简化配置，可以将GE 1/0/1 到 GE 1/0/4 放入端口组中，在端口组中进行配置。

4. 配置过程和解释

(1) 创建并进入端口组视图，添加对应的端口。

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group-manual-group1] group-member GigabitEthernet 1/0/1 to GigabitEthernet 1/0/4
```

(2) 在端口组中进行风暴抑制比的配置。

```
[Sysname-port-group-manual-group1] broadcast-suppression kbps 1024
[Sysname-port-group-manual-group1] multicast-suppression kbps 512
[Sysname-port-group-manual-group1] unicast-suppression kbps 512
```

提示：默认情况下，所有端口不对广播/组播/未知单播流量进行抑制。

在某些视频监控等需要使用广播、组播流量的应用下，需要取消或者将抑制比调整为合适的值，避免由于抑制功能影响业务。

3.1.5 接口统计典型配置指导

使用 flow-interval 配置命令可以设置统计以太网端口报文信息的时间间隔；使用 display interface 命令可以显示端口在该间隔时间内统计的报文信息；使用 reset counters interface 命令可以清除端口的统计信息。

1. 背景

以太网端口报文信息的时间间隔默认为 300s，网络管理员希望能够对设备的上行端口配置一个更小的时间间隔，以获取更为精确的接口统计信息。

2. 组网图

图 3-7 所示为接口统计典型配置组网图。

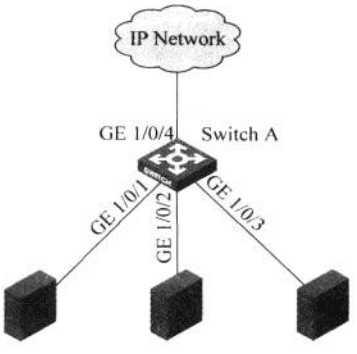


图 3-7 接口统计典型配置组网图

3. 配置需求

要求将上行端口 GE 1/0/4 默认的统计时间间隔修改为 120s，以获取更为精确的接口统计信息。

4. 配置过程和解释

进入 GE 1/0/4 端口，修改统计间隔为 120s。

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/4
[Sysname-GigabitEthernet1/0/4] flow-interval 120
```

3.2 三层以太网接口的 MTU 典型配置指导

MTU(Maximum Transmission Unit，最大传输单元)参数影响 IP 报文的分片与重组。

1. 背景

管理员发现在使用交换机三层以太网接口互连的时候，由于端口 MTU 值与实际链路允许值不相符，导致报文无法转发，需要对以太网接口上的 MTU 进行修改。

2. 组网图

图 3-8 所示为三层以太网接口的 MTU 典型配置组网图。

图 3-8 三层以太网接口的 MTU 典型配置组网图

3. 配置需求

要求将三层接口 GE 1/0/1 上的 MTU 修改为 1430B，以满足业务互通的要求。

4. 配置过程和解释

设置三层以太网接口 GE 1/0/1 的最大传输单元为 1430B。

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mtu 1430
```

提示：默认情况下，三层以太网接口的 MTU 值为 1500B。该命令只在三层以太网接口上生效。

第4章

以太网交换配置指导

4.1 MAC 地址表管理配置指导

默认情况下，MAC 地址表是交换机通过源 MAC 地址学习过程而自动建立的，而静态 MAC 地址表项需要用户手动配置。

1. 背景

为了提高端口安全性，M 公司的网络管理员手动在交换机的 MAC 地址表中加入特定 MAC 地址表项，将用户设备与端口绑定，从而防止假冒身份的非法用户骗取数据。

2. 组网图

图 4-1 所示为 MAC 地址表管理配置组网图。

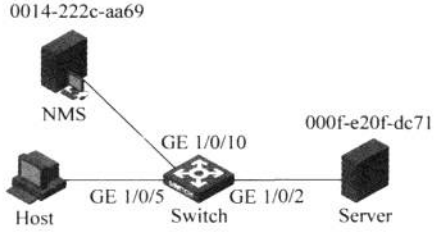


图 4-1 MAC 地址表管理配置组网图

3. 配置需求

服务器通过 GigabitEthernet 1/0/2 端口连接到交换机。为避免交换机在转发目的地址为服务器地址的报文时进行广播，要求在交换机上设置静态的服务器 MAC 地址表项，使交换机始终通过 GigabitEthernet 1/0/2 端口单播发送去往服务器的报文。端口 GigabitEthernet 1/0/10 连接 NMS(Network Management Server，网管服务器)，为增加网络管理的安全性，要求该端口仅允许这台 NMS 接入。

(1) 服务器的 MAC 地址为 000f-e20f-dc71。

(2) 图中所有端口均属于 VLAN 10。

(3) NMS 的 MAC 地址为 0014-222c-aa69。

(4) Switch 的 MAC 地址表项老化时间为 500s。

4. 配置过程和解释

(1) 创建 VLAN 10，并将 GigabitEthernet 1/0/2、GigabitEthernet 1/0/5、GigabitEthernet 1/0/10 端口加入 VLAN 10。

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] port GigabitEthernet 1/0/2 GigabitEthernet 1/0/5 GigabitEthernet 1/0/10
```

(2) 添加静态 MAC 地址。

```
[Sysname] mac-address static 000f-e20f-dc71 interface GigabitEthernet 1/0/2 vlan 10
```

(3) 设置交换机上动态 MAC 地址表项的老化时间为 500s。

```
[Sysname] mac-address timer aging 500
```

(4) 在系统视图下查看 MAC 地址配置。

```
[Sysname] display mac-address interface GigabitEthernet 1/0/2
MAC ADDR       VLAN ID  STATE          PORT INDEX              AGING TIME(s)
000f-e20f-dc71 1        Config static  GigabitEthernet 1/0/2   NOAGED
00e0-fc17-a7d6 1        Learned        GigabitEthernet 1/0/2   AGING
00e0-fc5e-b1fb 1        Learned        GigabitEthernet 1/0/2   AGING
00e0-fc55-f116 1        Learned        GigabitEthernet 1/0/2   AGING
---  4 mac address(es) found on port GigabitEthernet1/0/2 ---
```

(5) 通过配置最大 MAC 学习数为 0 与手动添加静态 MAC 表项功能的配合，实现 GigabitEthernet 1/0/10 端口只能转发源地址为 NMS 的报文，保证其他主机无法通过此端口通信。

```
[Sysname] interface GigabitEthernet 1/0/10
[Sysname-GigabitEthernet1/0/10] port access vlan 10
[Sysname-GigabitEthernet1/0/10] mac-address max-mac-count 0
[Sysname-GigabitEthernet1/0/10] mac-address static 0014-222c-aa69 vlan 10
```

(6) 配置当端口学习的 MAC 地址数达到设置的最大 MAC 地址数后，禁止转发收到的源 MAC 地址不在 MAC 地址表里的数据帧。

提示：MAC 地址的老化时间作用于全部端口上，地址老化只对动态的(设备学习到的或者用户配置的动态的)MAC 地址表项起作用，对用户配置的静态 MAC 地址表项不起作用。

4.2 链路聚合配置指导

链路聚合将多个物理以太网端口聚合在一起形成一个逻辑上的聚合组，使用链路聚合服务的上层实体将同一聚合组内的多条物理链路视为一条逻辑链路。

链路聚合可以实现出/入负荷在聚合组中各个成员端口之间分担，以增加带宽。同时，同一聚合组的各个成员端口之间彼此动态备份，提高了连接可靠性。

1. 背景

M 公司的两台交换机间原来使用单条链路连接，随着业务数据流量的增大，一条链路的带宽已经无法满足业务的需求，成为网络传输瓶颈。为了增加链路带宽，并且使链路具有更高的可靠性，网络管理员使用链路聚合进行扩容。

2. 组网图

图 4-2 所示为链路聚合配置组网图。

3. 配置需求

设备 Switch A 用 3 个端口聚合接入设备 Switch B，从而实现出/入负荷在各成员端口

中的分担。Switch A 的接入端口为 GigabitEthernet 1/0/1～GigabitEthernet 1/0/3。

4. 配置过程和解释

配置聚合组，实现端口的负载分担(下面两种方式任选其一)。

(1) 采用静态聚合模式(以下只列出 Switch A 的配置，Switch B 与 Switch A 相同)。

① 创建二层聚合端口 1。

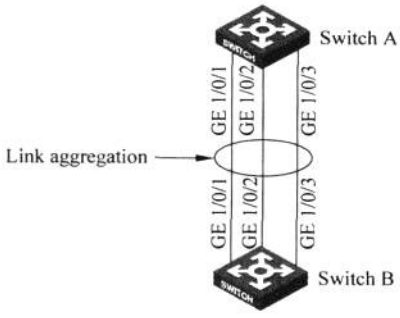


图 4-2 链路聚合配置组网图

```
<SwitchA> system-view
[SwitchA] interface bridge-aggregation 1
[SwitchA-Bridge-Aggregation1] quit
```

② 将以太网端口 GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 加入聚合组 1。

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/1] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/2] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-aggregation group 1
```

(2) 采用动态聚合模式(以下只列出 Switch A 的配置，Switch B 与 Switch A 相同)。

① 创建二层聚合端口 1，并配置成动态聚合模式。

```
<SwitchA> system-view
[SwitchA] interface bridge-aggregation 1
[SwitchA-Bridge-Aggregation1] link-aggregation mode dynamic
[SwitchA-Bridge-Aggregation1] quit
```

② 将以太网端口 GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 加入聚合组 1。

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/1] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/2] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-aggregation group 1
```

提示： 配置或使能了下列功能的端口将不能加入二层聚合组：RRPP、MAC 地址认证、端口安全模式、IP Source Guard 功能、802.1x 功能。

4.3 端口隔离配置指导

为了实现报文之间的隔离，可以将不同的端口加入不同的 VLAN，但会浪费有限的 VLAN 资源。采用端口隔离特性，可以实现同一 VLAN 内端口之间的隔离。用户只需要将端口加入隔离组中，就可以实现隔离组内端口之间数据的隔离。端口隔离功能为用户提供了更安全、更灵活的组网方案。

1. 背景

出于对安全和控制方面的需要，M 公司不希望某区域下的一台交换机所连接的主机之间互相访问，只允许这些主机访问上行端口外的数据。

2. 组网图

图 4-3 所示为端口隔离典型配置组网图。

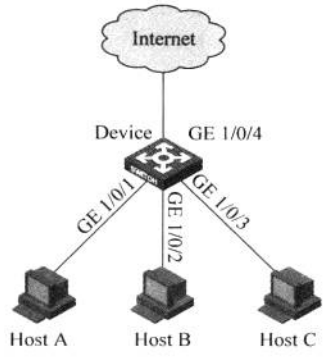


图 4-3 端口隔离典型配置组网图

3. 配置需求

(1) 用户 Host A、Host B、Host C 分别与 Device 的端口 GigabitEthernet 1/0/1、GigabitEthernet 1/0/2、GigabitEthernet 1/0/3 相连。

(2) 设备通过 GigabitEthernet 1/0/4 端口与外部网络相连。

(3) 端口 GigabitEthernet 1/0/1、GigabitEthernet 1/0/2、GigabitEthernet 1/0/3 和 GigabitEthernet 1/0/4 属于同一 VLAN，实现用户 Host A、Host B 和 Host C 彼此之间不能互通，但可以和外部网络通信。

4. 配置过程和解释

(1) 将端口 GigabitEthernet 1/0/1、GigabitEthernet 1/0/2、GigabitEthernet 1/0/3 加入隔离组。

```
<Device> system-view
[Device] interface GigabitEthernet 1/0/1
[Device-GigabitEthernet1/0/1] port-isolate enable
[Device-GigabitEthernet1/0/1] quit
[Device] interface GigabitEthernet 1/0/2
[Device-GigabitEthernet1/0/2] port-isolate enable
[Device-GigabitEthernet1/0/2] quit
[Device] interface GigabitEthernet 1/0/3
[Device-GigabitEthernet1/0/3] port-isolate enable
```

(2) 显示隔离组中的信息。

```
<Device> display port-isolate group
Port-isolate group information:
Uplink port support: NO
Group ID: 1
    GigabitEthernet 1/0/1      GigabitEthernet 1/0/2      GigabitEthernet 1/0/3
```

提示： 目前，设备只支持一个隔离组，即由系统自动创建的隔离组 1，用户不可删除该隔离组或创建其他的隔离组。

隔离组内可以加入的端口数量没有限制。

隔离组内的端口和隔离组外相同 VLAN 端口数据流量双向互通，隔离组内端口之间不可互通。

4.4 VLAN 典型配置指导

4.4.1 基于端口的 VLAN 典型配置指导

基于端口划分 VLAN 是 VLAN 最简单、最有效的划分方法。它按照设备端口来定义 VLAN 成员，将指定端口加入指定 VLAN 中之后，端口就可以转发指定 VLAN 的报文。

1. 背景

M 公司的 IT 维护部门要求使用 VLAN 技术对公司网络部署虚拟工作组，划分不同的部门到不同的工作组。这样，同一工作组的用户不必局限于某一固定的物理范围，限制了广播域，增强了局域网的安全性。

2. 组网图

图 4-4 所示为基于端口的 VLAN 典型配置组网图。

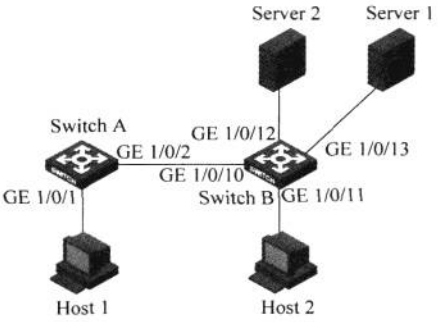


图 4-4 基于端口的 VLAN 典型配置组网图

3. 配置需求

(1) 如图 4-4 所示，Switch A 和 Switch B 分别连接了不同部门使用的 Host 1/Host 2 和 Server 1/Server 2。

(2) 为保证部门间数据的二层隔离，现要求将 Host 1 和 Server 1 划分到 VLAN 100 中，Host 2 和 Server 2 划分到 VLAN 200 中，并分别为两个 VLAN 设置描述字符为 Dept1 和 Dept2。

(3) 在 Switch A 上配置 VLAN 接口，对 Host 1 发往 Server 2 的数据进行三层转发。

4. 配置过程和解释

(1) 配置 Switch A。

① 创建 VLAN 100，并配置 VLAN 100 的描述字符串为 Dept1，将端口 GigabitEthernet 1/0/1 加入 VLAN 100。

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] description Dept1
[SwitchA-vlan100] port GigabitEthernet 1/0/1
[SwitchA-vlan100] quit
```

② 创建 VLAN 200，并配置 VLAN 200 的描述字符串为 Dept2。

```
[SwitchA] vlan 200
[SwitchA-vlan200] description Dept2
[SwitchA-vlan200] quit
```

③ 创建 VLAN 100 和 VLAN 200 的接口，IP 地址分别配置为 192.168.1.1 和 192.168.2.1，用来对 Host 1 发往 Server 2 的报文进行三层转发。

```
[SwitchA] interface Vlan-interface 100
```

```
[SwitchA-Vlan-interface100] ip address 192.168.1.1 24
[SwitchA-Vlan-interface100] quit
[SwitchA] interface Vlan-interface 200
[SwitchA-Vlan-interface200] ip address 192.168.2.1 24
```

(2) 配置 Switch B。

① 创建 VLAN 100，并配置 VLAN 100 的描述字符串为 Dept1，将端口 GigabitEthernet 1/0/13 加入 VLAN 100。

```
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-vlan100] description Dept1
[SwitchB-vlan100] port GigabitEthernet 1/0/13
[SwitchB-vlan100] quit
```

② 创建 VLAN 200，并配置 VLAN 200 的描述字符串为 Dept2，将端口 GigabitEthernet 1/0/11 和 GigabitEthernet 1/0/12 加入 VLAN 200。

```
[SwitchB] vlan 200
[SwitchB-vlan200] description Dept2
[SwotchB-vlan200] port GigabitEthernet 1/0/11 GigabitEthernet 1/0/12
[SwitchB-vlan200] quit
```

(3) 配置 Switch A 和 Switch B 之间的链路。由于 Switch A 和 Switch B 之间的链路需要同时传输 VLAN 100 和 VLAN 200 的数据，所以可以配置两端的端口为 Trunk 端口，且允许这两个 VLAN 的报文通过。

① 配置 Switch A 的 GigabitEthernet 1/0/2 端口。

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

② 配置 Switch B 的 GigabitEthernet 1/0/10 端口。

```
[SwitchB] interface GigabitEthernet 1/0/10
[SwitchB-GigabitEthernet1/0/10] port link-type trunk
[SwitchB-GigabitEthernet1/0/10] port trunk permit vlan 100 200
```

提示：VLAN 1 为系统默认 VLAN，用户不能手动创建和删除。

在创建 VLAN 接口之前，对应的 VLAN 必须已经存在；否则，将不能创建指定的 VLAN 接口。

4.4.2 基于 MAC 的 VLAN 典型配置指导

基于 MAC 划分 VLAN 是 VLAN 的另一种划分方法，它根据报文的源 MAC 地址来决定报文从哪个 VLAN 中转发。

1. 背景

M 公司 IT 维护部门在会议室区域部署 VLAN 时，使用了基于 MAC 划分的方式，以使笔记本电脑这种位置不固定的移动终端方便地接入所属部门的工作组中。

2. 组网图

图 4-5 所示为基于 MAC 的 VLAN 典型配置组网图。

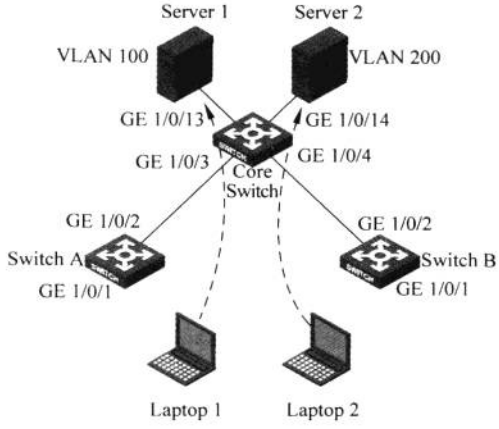


图 4-5 基于 MAC 的 VLAN 典型配置组网图

3. 配置需求

(1) 如图 4-5 所示，Switch A 和 Switch B 的 GigabitEthernet 1/0/1 端口分别连接到两个会议室，Laptop 1 和 Laptop 2 是会议用笔记本电脑，在两个会议室间移动使用。

(2) Laptop 1 和 Laptop 2 分别属于两个部门，两个部门间使用 VLAN 100 和 VLAN 200 进行隔离。现要求这两台笔记本电脑无论在哪个会议室使用，均只能访问自己部门的服务器，即 Server 1 和 Server 2。

(3) Laptop 1 和 Laptop 2 的 MAC 地址分别为 000d-88f8-4e71、0014-222c-aa69。

4. 配置过程和解释

(1) Switch A 的配置。

① 创建 VLAN 100 和 VLAN 200，并将 GigabitEthernet 1/0/2 配置为 Trunk 端口，允许 VLAN 100 和 VLAN 200 的报文通过。

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] quit
[SwitchA] vlan 200
[SwitchA-vlan200] quit
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[SwitchA-GigabitEthernet1/0/2] quit
```

② 将 GigabitEthernet 1/0/1 配置为 Hybrid 端口，并使其在发送 VLAN 100 和 VLAN 200 的报文时去掉 VLAN Tag。

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type hybrid
[SwitchA-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
[SwitchA-GigabitEthernet1/0/1] quit
```

③ 创建 Laptop 1 的 MAC 地址与 VLAN 100 的关联，创建 Laptop 2 的 MAC 地址与 VLAN 200 的关联，开启 GigabitEthernet 1/0/1 端口的 MAC-VLAN 功能。

```
[SwitchA] mac-vlan mac-address 000d-88f8-4e71 vlan 100
[SwitchA] mac-vlan mac-address 0014-222c-aa69 vlan 200
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] mac-vlan enable
```

(2) Switch B 的配置。

Switch B 的配置与 Switch A 完全一致，这里不再赘述。

(3) Core Switch 的配置。

① 创建 VLAN 100 和 VLAN 200，并将 GigabitEthernet 1/0/13 和 GigabitEthernet 1/0/14 端口分别加入这两个 VLAN。

```
<CoreSwitch> system-view
[CoreSwitch] vlan 100
[CoreSwitch-vlan100] port GigabitEthernet 1/0/13
[CoreSwitch-vlan100] quit
[CoreSwitch] vlan 200
[CoreSwitch-vlan200] port GigabitEthernet 1/0/14
[CoreSwitch-vlan200] quit
```

② 配置 GigabitEthernet 1/0/3 和 GigabitEthernet 1/0/4 端口为 Trunk 端口，均允许 VLAN 100 和 VLAN 200 的报文通过。

```
[CoreSwitch] interface GigabitEthernet 1/0/3
[CoreSwitch-GigabitEthernet1/0/3] port link-type trunk
[CoreSwitch-GigabitEthernet1/0/3] port trunk permit vlan 100 200
[CoreSwitch-GigabitEthernet1/0/3] quit
[CoreSwitch] interface GigabitEthernet 1/0/4
[CoreSwitch-GigabitEthernet1/0/4] port link-type trunk
[CoreSwitch-GigabitEthernet1/0/4] port trunk permit vlan 100 200
[CoreSwitch-GigabitEthernet1/0/4] quit
```

提示：基于 MAC 的 VLAN 只能在 Hybrid 端口上配置。

基于 MAC 的 VLAN 的配置主要用于在用户的接入设备的下行端口上进行配置，因此不能和聚合功能同时使用。

4.4.3 基于协议的 VLAN 典型配置指导

基于协议的 VLAN 是根据端口接收到的报文所属的协议(族)类型以及封装格式来给报文分配不同的 VLAN ID。

1. 背景

M 公司的实验室网络中大部分主机运行 IPv4 网络协议，另外为了测试需要还布置了 IPv6 实验室，因此有些主机运行了 IPv6 网络协议。为了避免互相干扰，IT 维护部门要求基于网络协议将 IPv4 流量和 IPv6 流量二层互相隔离。

2. 组网图

图 4-6 所示为基于协议的 VLAN 典型配置组网图。

3. 配置需求

如图 4-6 所示，通过配置交换机的协议 VLAN 功能，使办公区与实验室中基于 IPv4 网络和基于 IPv6 网络的主机能分别与处在不同 VLAN 内的对应服务器进行通信，且两种网络协议的报文能够通过 VLAN 进行隔离，其中 IPv4 网络使用 VLAN 100，IPv6 网络使用 VLAN 200。

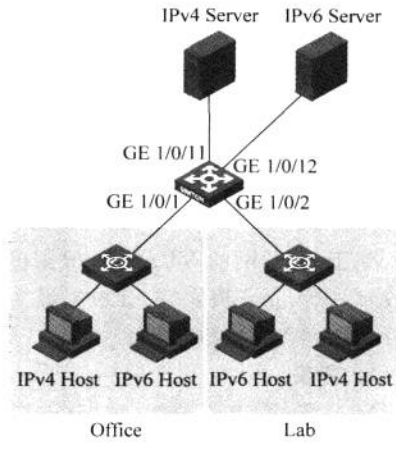


图 4-6 基于协议的 VLAN 典型配置组网图

4. 配置过程和解释

(1) 上行端口的配置。

① 创建 VLAN 100，将端口 GigabitEthernet 1/0/11 加入 VLAN 100。

```
<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100] port GigabitEthernet 1/0/11
```

② 创建 VLAN 200，将端口 GigabitEthernet 1/0/12 加入 VLAN 200。

```
[Sysname-vlan100] quit
[Sysname] vlan 200
[Sysname-vlan200] port GigabitEthernet 1/0/12
```

(2) 配置协议模板并与下行端口绑定。

① 创建 VLAN 200 和 VLAN 100 的协议模板，分别匹配 IPv4 和 IPv6 协议。

```
[Sysname-vlan200] protocol-vlan ipv6
[Sysname-vlan200] quit
[Sysname] vlan100
[Sysname-vlan100] protocol-vlan ipv4
[Sysname-vlan100] quit
```

② 配置端口 GigabitEthernet 1/0/1 为 Hybrid 端口，并在转发 VLAN 100 和 VLAN 200 的报文时去掉 VLAN Tag。

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

③ 配置端口 GigabitEthernet 1/0/1 分别与 VLAN 100 的协议模板 0、VLAN 200 的协议模板 0 进行绑定。

```
[Sysname-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 100 0
[Sysname-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 200 0
```

④ 同理配置端口 GigabitEthernet 1/0/2 为 Hybrid 端口，在转发 VLAN 100 和 VLAN 200的报文时去掉 VLAN Tag，并与 VLAN 100 和 VLAN 200 的协议模板 0 进行绑定。

```
[Sysname] interface GigabitEthernet 1/0/2
```

```
[Sysname-GigabitEthernet1/0/2] port link-type hybrid
[Sysname-GigabitEthernet1/0/2] port hybrid vlan 100 200 untagged
[Sysname-GigabitEthernet1/0/2] port hybrid protocol-vlan vlan 100 0
[Sysname-GigabitEthernet1/0/2] port hybrid protocol-vlan vlan 200 0
```

提示：基于协议的 VLAN 只对 Hybrid 端口配置才有效。

4.4.4 基于 IP 子网的 VLAN 典型配置指导

基于 IP 子网的 VLAN 是根据报文源 IP 地址及子网掩码来进行划分的。设备从端口接收到 untagged 报文后，会根据报文的源地址来确定报文所属的 VLAN，然后将报文自动划分到指定 VLAN 中传输。

1. 背景

M 公司的 IT 维护部门对分支机构交换机使用基于 IP 子网的 VLAN 划分方式，来实现不同网段的部门划分到不同的工作组 VLAN 中。

2. 组网图

图 4-7 所示为基于 IP 子网的 VLAN 典型配置组网图。

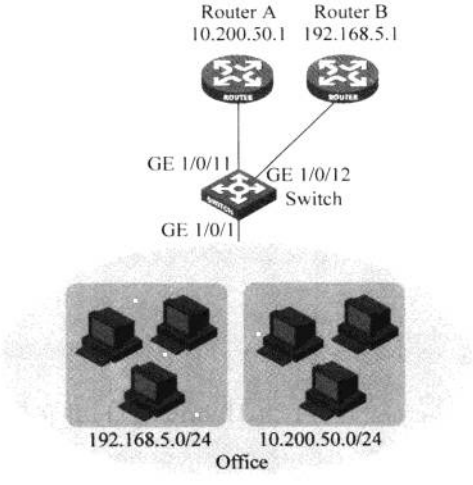


图 4-7 基于 IP 子网的 VLAN 典型配置组网图

3. 配置需求

如图 4-7 所示，办公区内的主机被配置到两个不同的网段(192.168.5.0/24 和 10.200.50.0/24)中，要求通过配置 IP 子网 VLAN 功能，使交换机能够将从 GigabitEthernet 1/0/1 端口收到的报文根据源主机所属网段的不同，分别在不同的 VLAN 内传输，并到达指定的网关(Router A 和 Router B)。其中 192.168.5.0/24 网段的报文分发到 VLAN 100 中传输，10.200.50.0/24 网段的报文分发到 VLAN 200 中传输。

4. 配置过程和解释

(1) 上行端口的配置。

① 创建 VLAN 100，将端口 GigabitEthernet 1/0/12 加入 VLAN 100。

```
[Sysname] vlan 100
[Sysname-vlan100] port GigabitEthernet 1/0/12
```

② 创建 VLAN 200，将端口 GigabitEthernet 1/0/11 加入 VLAN 200。

```
[Sysname-vlan100] quit
[Sysname] vlan 200
[Sysname-vlan200] port GigabitEthernet 1/0/11
```

(2) 配置 IP 子网 VLAN 并与下行端口绑定。

① 将 10.200.50.0/24 网段与 VLAN 200 进行关联，将 192.168.5.0/24 网段与 VLAN 100 进行关联。

```
[Sysname-vlan200] ip-subnet-vlan ip 10.200.50.0 255.255.255.0
[Sysname-vlan200] quit
[Sysname] vlan100
[Sysname-vlan100] ip-subnet-vlan ip 192.168.5.0 255.255.255.0
```

② 配置端口 GigabitEthernet 1/0/1 为 Hybrid 端口，并在转发 VLAN 100 和 VLAN 200 的报文时去掉 VLAN Tag。

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

③ 配置端口 GigabitEthernet 1/0/1 分别与 VLAN 100 和 VLAN 200 的子网进行关联。

```
[Sysname-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 100
[Sysname-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 200
```

提示：基于 IP 子网的 VLAN 只对 Hybrid 端口配置有效。

4.4.5 Isolate-user-VLAN 典型配置指导

Isolate-user-VLAN 采用二层 VLAN 结构，它在同一台设备上设置 Isolate-user-VLAN 和 Secondary VLAN 两类 VLAN。

(1) Isolate-user-VLAN 用于上行，不同的 Secondary VLAN 关联到同一个 Isolate-user-VLAN。上行连接的设备只知道 Isolate-user-VLAN，而不必关心 Secondary VLAN，简化了网络配置，节省了 VLAN 资源。

(2) Secondary VLAN 用于连接用户，Secondary VLAN 之间的二层报文互相隔离。

(3) 一个 Isolate-user-VLAN 可以和多个 Secondary VLAN 相关联。Isolate-user-VLAN 下面的 Secondary VLAN 对上行设备不可见。

(4) Secondary VLAN 内学习到的动态 MAC 地址自动同步到 Isolate-user-VLAN 内。

1. 背景

M 公司 IT 维护部门需要将新建区域网络和原有区域网络连接起来，由于两个区域存在重复的 VLAN 编号，为了避免它们直接互通而带来安全隐患，要求使用 Isolate-user-VLAN 技术解决。

2. 组网图

图 4-8 所示为 Isolate-user-VLAN 典型配置组网图。

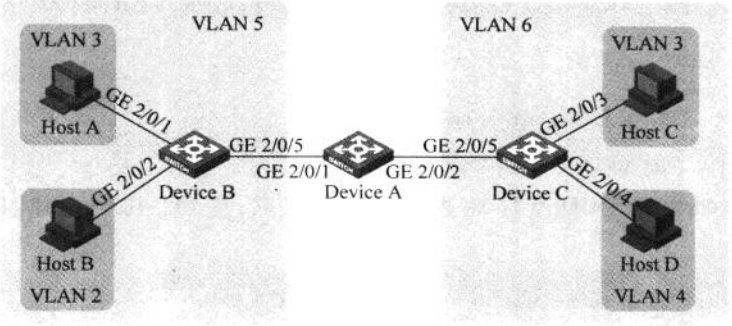


图 4-8 Isolate-user-VLAN 典型配置组网图

3. 配置需求

(1) Device B 和 Device C 在初始状态下分别位于两个独立的网络中，并根据自身情况创建了相应的 VLAN；由于网络规划的变更，现要求使用 Device A 将 Device B 和 Device C 连通。

(2) 出于安全性的考虑，要求 Device B 和 Device C 所连接的设备间不能直接通信，如图 4-8 所示。由于这两台设备本地创建的 VLAN 编号有重复，Host A 和 Host C 处在同一个 VLAN 中，存在一定安全隐患，因此需要使用 Isolate-user-VLAN 功能，使 Device B 和 Device C 上配置的 VLAN 2/VLAN 3 和 VLAN 3/VLAN 4 仅在本地有效。Device A 使用 VLAN 5 和 VLAN 6 对这两个网络进行划分，而无须考虑这两个网络内部 VLAN 的配置。

(3) Device A 使用 VLAN 接口对两个网络间的报文进行三层转发。

4. 配置过程和解释

(1) 配置 Device B。

① 配置 Isolate-user-VLAN。

```
<DeviceB> system-view
[DeviceB] vlan 5
[DeviceB-vlan5] isolate-user-vlan enable
[DeviceB-vlan5] port GigabitEthernet 2/0/5
[DeviceB-vlan5] quit
[DeviceB] interface GigabitEthernet 2/0/5
[DeviceB-GigabitEthernet2/0/5] port isolate-user-vlan promiscuous
[DeviceB-GigabitEthernet2/0/5] quit
```

② 配置 Secondary VLAN。

```
[DeviceB] vlan 3
[DeviceB-vlan3] port GigabitEthernet 2/0/1
[DeviceB-vlan3] quit
[DeviceB] interface GigabitEthernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] port isolate-user-vlan host
[DeviceB-GigabitEthernet2/0/1] quit
[DeviceB] vlan 2
```

```
[DeviceB-vlan2] port GigabitEthernet 2/0/2
[DeviceB-vlan2] quit
[DeviceB] interface GigabitEthernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] port isolate-user-vlan host
[DeviceB-GigabitEthernet2/0/2] quit
```

③ 配置 Isolate-user-VLAN 和 Secondary VLAN 之间的映射关系。

```
[DeviceB] isolate-user-vlan 5 secondary 2 to 3
```

(2) 配置 Device C。

① 配置 Isolate-user-VLAN。

```
<DeviceC> system-view
[DeviceC] vlan 6
[DeviceC-vlan6] isolate-user-vlan enable
[DeviceC-vlan6] port GigabitEthernet 2/0/5
[DeviceC-vlan6] quit
[DeviceC] interface GigabitEthernet 2/0/5
[DeviceC-GigabitEthernet2/0/5] port isolate-user-vlan promiscuous
[DeviceC-GigabitEthernet2/0/5] quit
```

② 配置 Secondary VLAN。

```
[DeviceC] vlan 3
[DeviceC-vlan3] port GigabitEthernet 2/0/3
[DeviceC-vlan3] quit
[DeviceC] interface GigabitEthernet 2/0/3
[DeviceC-GigabitEthernet2/0/3] port isolate-user-vlan host
[DeviceC-GigabitEthernet2/0/3] quit
[DeviceC] vlan 4
[DeviceC-vlan4] port GigabitEthernet 2/0/4
[DeviceC] interface GigabitEthernet 2/0/4
[DeviceC-GigabitEthernet2/0/4] port isolate-user-vlan host
[DeviceC-GigabitEthernet2/0/4] quit
```

③ 配置 Isolate-user-VLAN 和 Secondary VLAN 之间的映射关系。

```
[DeviceC-vlan4] quit
[DeviceC] isolate-user-vlan 6 secondary 3 to 4
```

(3) 配置 Device A。

① 创建 VLAN 5 和 VLAN 6，并将 GigabitEthernet 2/0/1 和 GigabitEthernet 2/0/2 端口分别加入 VLAN 5 和 VLAN 6，本例中以这两个端口为 Access 端口为例进行配置。

```
[DeviceA] vlan 5
[DeviceA-vlan5] port GigabitEthernet 2/0/1
[DeviceA-vlan5] quit
[DeviceA] vlan 6
[DeviceA-vlan6] port GigabitEthernet 2/0/2
[DeviceA-vlan6] quit
```

② 创建 VLAN 5 和 VLAN 6 的接口，使两个网络间的数据可以通过 Device A 进行三

层转发，IP 地址分别为 192.168.0.1 和 192.168.1.1。

```
[DeviceA] interface Vlan-interface 5
[DeviceA-Vlan-interface5] ip address 192.168.0.1 24
[DeviceA-Vlan-interface5] quit
[DeviceA] interface Vlan-interface 6
[DeviceA-Vlan-interface6] ip address 192.168.1.1 24
```

用户也可以将 GigabitEthernet 2/0/1 和 GigabitEthernet 2/0/2 端口配置为 Trunk 端口或 Hybrid 端口，只需要保证这两个端口分别在发送 VLAN 5 和 VLAN 6 的报文时去掉 VLAN Tag 即可。

提示：Isolate-user-VLAN 与 Secondary VLAN 建立映射后，系统将禁止进行以下配置。

① 禁止向 Isolate-user-VLAN 和 Secondary VLAN 中添加/删除 Access 类型的端口以及删除 VLAN 的操作。

② 禁止修改端口的 Isolate-user-VLAN 类型。

用户只有在解除 Isolate-user-VLAN 与 Secondary VLAN 的映射关系后才可以执行以上配置。

4.4.6 Super VLAN 典型配置指导

一个 Super VLAN 和多个 Sub VLAN 关联，Super VLAN 内不能加入物理端口，但可以创建对应的 VLAN 接口，VLAN 接口下可以配置 IP 地址；Sub VLAN 可以加入物理端口，但不能创建对应的 VLAN 接口，所有 Sub VLAN 内的端口共用 Super VLAN 的 VLAN 接口 IP 地址，不同 Sub VLAN 之间的二层相互隔离。当 Sub VLAN 内的用户需要进行三层通信时，将使用 Super VLAN 的 IP 地址作为网关地址，这样多个 Sub VLAN 共享一个网关地址，从而节省了 IP 地址资源。

1. 背景

M 公司某区域交换机下有多个部门，为了节约地址资源，IT 维护部门计划使用 Super VLAN 技术让不同 VLAN 的部门共享一个地址段和同一个网关。

2. 组网图

图 4-9 所示为 Super VLAN 典型配置组网图。

3. 配置需求

(1) Switch A 作为汇聚层交换机，下面通过接入层交换机连接了大量的客户端，这些客户端都使用了 10.0.0.0/24 网段的地址。现要求按图 4-9 所示，将主机划分到 3 个 VLAN 中进行管理，保证不同 VLAN 内的主机之间为二层隔离。

(2) 为节约 IP 地址，不对 3 个 VLAN 分别划分子网，要求使用 Switch A 的 Vlan-interface 10 接口作为所有主机的网关，转发主机对外网的访问需求，同时通过 ARP 代理实现 VLAN 间主机的三层互通。

(3) Switch A 通过 Vlan-interface 20 接口连接到外部网络。

4. 配置过程和解释

(1) 创建 VLAN 20，将 GigabitEthernet 2/0/20 加入 VLAN 20，并配置 Vlan-interface 20 接口的地址为 10.0.1.1/24。

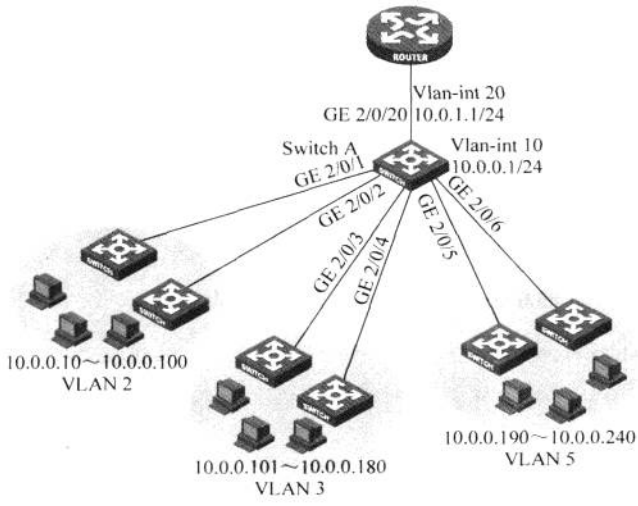


图 4-9 Super VLAN 典型配置组网图

```
<Sysname> system-view
[Sysname] vlan 20
[Sysname-vlan20] port GigabitEthernet 2/0/20
[Sysname-vlan20] quit
[Sysname] interface vlan-interface 20
[Sysname-Vlan-interface20] ip address 10.0.1.1 255.255.255.0
```

(2) 创建 VLAN 10,并配置 VLAN 10 接口的 IP 地址为 10.0.0.1/24。

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ip address 10.0.0.1 255.255.255.0
```

(3) 开启 VLAN 10 接口的本地 ARP 代理功能,使 VLAN 2、VLAN 3、VLAN 5 之间能够通过 VLAN 10 接口的处理完成 ARP 请求和答复过程。

```
[Sysname-Vlan-interface10] local-proxy-arp enable
[Sysname-Vlan-interface10] quit
```

(4) 创建 VLAN 2,并添加端口 GigabitEthernet 2/0/1 和端口 GigabitEthernet 2/0/2。

```
[Sysname] vlan 2
[Sysname-vlan2] port GigabitEthernet 2/0/1 GigabitEthernet 2/0/2
```

(5) 创建 VLAN 3,并添加端口 GigabitEthernet 2/0/3 和端口 GigabitEthernet 2/0/4。

```
[Sysname-vlan2] quit
[Sysname] vlan 3
[Sysname-vlan3] port GigabitEthernet 2/0/3 GigabitEthernet 2/0/4
```

(6) 创建 VLAN 5,并添加端口 GigabitEthernet 2/0/5 和端口 GigabitEthernet 2/0/6。

```
[Sysname-vlan3] quit
```

```
[Sysname] vlan 5
[Sysname-vlan5] port GigabitEthernet 2/0/5 GigabitEthernet 2/0/6
```

(7) 指定 VLAN 10 为 Super VLAN，VLAN 2、VLAN 3 和 VLAN 5 为 Sub VLAN。

```
[Sysname-vlan5] quit
[Sysname] vlan 10
[Sysname-vlan10] supervlan
[Sysname-vlan10] subvlan 2 3 5
```

(8) 查看 VLAN 10 的相关信息，验证以上配置是否生效。

```
<Sysname> display supervlan
SuperVLAN ID :  10
SubVLAN ID :  2-3 5

VLAN ID: 10
VLAN Type: static
It is a Super VLAN.
Route Interface: configured
IP Address: 10.0.0.1
Subnet Mask: 255.255.255.0
Description: VLAN 0010
Tagged   Ports: none
Untagged Ports: none

VLAN ID: 2
VLAN Type: static
It is a Sub VLAN.
Route Interface: configured
IP Address: 10.0.0.1
Subnet Mask: 255.255.255.0
Description: VLAN 0002
Tagged   Ports: none
Untagged Ports:
    GigabitEthernet 2/0/1       GigabitEthernet 2/0/2

VLAN ID: 3
VLAN Type: static
It is a Sub VLAN.
Route Interface: configured
IP Address: 10.0.0.1
Subnet Mask: 255.255.255.0
Description: VLAN 0003
Tagged   Ports: none
Untagged Ports:
    GigabitEthernet 2/0/3       GigabitEthernet 2/0/4

VLAN ID: 5
VLAN Type: static
It is a Sub VLAN.
Route Interface: configured
IP Address: 10.0.0.1
Subnet Mask: 255.255.255.0
```

Description: VLAN 0005
Tagged Ports: none
Untagged Ports:
GigabitEthernet 2/0/5 GigabitEthernet 2/0/6

提示：如果某个 VLAN 被指定为 Super VLAN，则该 VLAN 不能被指定为某个端口的 GuestVlan；同样，如果某个 VLAN 被指定为某个端口的 GuestVlan，则该 VLAN 不能被指定为 Super VLAN。

4.5 GVRP 配置指导

通过使用 GVRP，可以使同一局域网内的交换机接收来自其他交换机的 VLAN 注册信息，并动态更新本地的 VLAN 注册信息，包括当前的 VLAN 成员，这些 VLAN 成员可以通过哪个端口到达等，而且设备能够将本地的 VLAN 注册信息向其他设备传播。

1. 背景

M 公司的 IT 维护部门在其局域网中部署 GVRP，以使同一局域网内所有设备的 VLAN 信息达成一致，减少人工配置的工作量。

2. 组网图

图 4-10 所示为 GVRP 配置组网图。

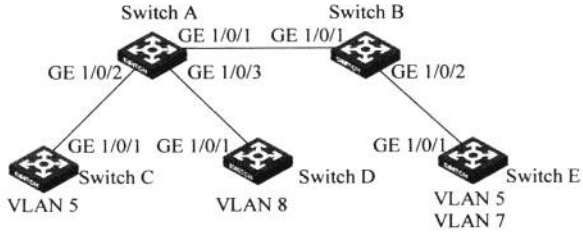


图 4-10 GVRP 配置组网图

3. 配置需求

组网情况如图 4-10 所示。

(1) 交换机上涉及的以太网端口均配置为 Trunk 端口，且允许所有 VLAN 通过。

(2) 所有交换机均开启全局 GVRP 和端口 GVRP 功能。

(3) Switch C 配置静态 VLAN 5，Switch D 配置静态 VLAN 8，Switch E 配置静态 VLAN 5 和 VLAN 7，Switch A 和 Switch B 未进行静态 VLAN 的配置。

(4) 配置 Switch E 的以太网端口 GigabitEthernet 1/0/1 的注册模式为 fixed，显示 Switch A、Switch B 和 Switch E 上动态注册的 VLAN 信息。

(5) 配置 Switch E 的以太网端口 GigabitEthernet 1/0/1 的注册模式为 forbidden，显示 Switch A、Switch B 和 Switch E 上动态注册的 VLAN 信息。

4. 配置过程和解释

(1) 配置 Switch A。

① 开启全局 GVRP。

```
<SwitchA> system-view
[SwitchA] gvrp
```

② 将以太网端口 GigabitEthernet 1/0/1 配置为 Trunk 端口，并允许所有 VLAN 通过。

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan all
```

③ 在以太网端口 GigabitEthernet 1/0/1 上开启 GVRP。

```
[SwitchA-GigabitEthernet1/0/1] gvrp
[SwitchA-GigabitEthernet1/0/1] quit
```

④ 将以太网端口 GigabitEthernet 1/0/2 配置为 Trunk 端口，并允许所有 VLAN 通过。

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan all
```

⑤ 在以太网端口 GigabitEthernet 1/0/2 上开启 GVRP。

```
[SwitchA-GigabitEthernet1/0/2] gvrp
[SwitchA-GigabitEthernet1/0/2] quit
```

⑥ 将以太网端口 GigabitEthernet 1/0/3 配置为 Trunk 端口，并允许所有 VLAN 通过。

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan all
```

⑦ 在以太网端口 GigabitEthernet 1/0/3 上开启 GVRP。

```
[SwitchA-GigabitEthernet1/0/3] gvrp
```

(2) 配置 Switch B。

配置 GigabitEthernet 1/0/1 和 GigabitEthernet 1/0/2 端口为 Trunk 端口，允许所有 VLAN 通过，并开启全局和以上两个端口的 GVRP 功能。配置过程可参见 Switch A 的配置。

(3) 配置 Switch C。

① 创建 VLAN 5。

```
<SwitchC> system-view
[SwitchC] vlan5
[SwitchC-vlan5]
```

② 配置 GigabitEthernet 1/0/1 端口为 Trunk 端口，允许所有 VLAN 通过，并开启全局和该端口的 GVRP 功能。配置过程可参见 SwitchA 的配置。

说明：为避免重复，以下设备的配置只描述配置要点，具体配置命令可参考上述设备的配置。

(4) 配置 Switch D。

① 配置 GigabitEthernet 1/0/1 端口为 Trunk 端口，允许所有 VLAN 通过，同时开启全

局和该端口的 GVRP 功能。

② 创建 VLAN 8。

(5) 配置 Switch E。

① 配置 GigabitEthernet 1/0/1 端口为 Trunk 端口，允许所有 VLAN 通过，同时开启全局和该端口的 GVRP 功能。

② 创建 VLAN 5 和 VLAN 7。

(6) 显示 Switch A、Switch B 和 Switch E 上动态注册的 VLAN 信息。

① 显示 Switch A 上的动态 VLAN 信息。

```
[SwitchA] display vlan dynamic
Total 3 dynamic VLAN exist(s).
The following dynamic VLANs exist:
  5, 7, 8,
```

② 显示 Switch B 上的动态 VLAN 信息。

```
[SwitchB] display vlan dynamic
Total 3 dynamic VLAN exist(s).
The following dynamic VLANs exist:
  5, 7, 8,
```

③ 显示 Switch E 上的动态 VLAN 信息。

```
[SwitchE] display vlan dynamic
Total 1 dynamic VLAN exist(s).
The following dynamic VLANs exist:
  8
```

(7) 配置 Switch E 的以太网端口 GigabitEthernet 1/0/1 的注册模式为 fixed，显示 Switch A、Switch B 和 Switch E 上动态注册的 VLAN 信息。

① 配置 Switch E 的以太网端口 GigabitEthernet 1/0/1 的注册模式为 fixed。

```
[SwitchE] interface GigabitEthernet 1/0/1
[SwitchE-GigabitEthernet1/0/1] gvrp registration fixed
```

② 显示 Switch A 上的动态 VLAN 信息。

```
[SwitchA] display vlan dynamic
Total 3 dynamic VLAN exist(s).
The following dynamic VLANs exist:
  5, 7, 8,
```

③ 显示 Switch B 上的动态 VLAN 信息。

```
[SwitchB] display vlan dynamic
Total 3 dynamic VLAN exist(s).
The following dynamic VLANs exist:
  5, 7, 8,
```

④ 显示 Switch E 上的动态 VLAN 信息。

```
[SwitchE-GigabitEthernet1/0/1] display vlan dynamic
```

```
No dynamic vlans exist!
```

(8) 配置 Switch E 的以太网端口 GigabitEthernet 1/0/1 的注册模式为 forbidden，显示 Switch A、Switch B 和 Switch E 上动态注册的 VLAN 信息。

① 配置 Switch E 的以太网端口 GigabitEthernet 1/0/1 的注册模式为 forbidden。

```
[SwitchE-GigabitEthernet1/0/1] gvrp registration forbidden
```

② 显示 Switch A 上的动态 VLAN 信息。

```
[SwitchA] display vlan dynamic
Total 2 dynamic VLAN exist(s).
The following dynamic VLANs exist:
  5, 8,
```

③ 显示 Switch B 上的动态 VLAN 信息。

```
[SwitchB] display vlan dynamic
Total 2 dynamic VLAN exist(s).
The following dynamic VLANs exist:
  5, 8,
```

④ 显示 Switch E 上的动态 VLAN 信息。

```
[SwitchE] display vlan dynamic
  No dynamic vlans exist!
```

提示：port trunk permit vlan all 命令只在 GVRP 功能配置过程中是必须执行的，在没有配置 GVRP 的情况下，建议用户不要使用该命令，以防止未授权 VLAN 的用户通过该端口访问受限资源。

开启端口 GVRP 功能前，必须先开启全局 GVRP 功能。

GVRP 功能只能运行在 MSTP 的 CIST 实例上，并且 CIST 实例上被 MSTP 阻塞的端口不能收发 GVRP 报文。

4.6 Voice VLAN 配置指导

在自动模式下，Voice VLAN 功能将自动侦测进入端口报文的源 MAC 地址，如果能够与系统可识别的 OUI 地址相匹配，则将该报文识别为语音报文，在 Voice VLAN 中传输。

如果一段时间后，该端口没有再次收到源 MAC 地址符合 OUI 地址的报文，将自动退出 Voice VLAN，这段时间也称为 Voice VLAN 的老化时间。

在手动模式下，需要管理员通过手动配置命令将端口加入 Voice VLAN 或从 Voice VLAN 中删除。

1. 背景

M 公司内部有大量的 IP 话机，网络中同时存在语音数据和业务数据两种流量，语音数据在传输时需要具有比业务数据更高的优先级，以减少传输过程中可能产生的时延和丢包现象。IT 维护部门通过划分 Voice VLAN 并将连接语音设备的端口加入 Voice VLAN，系统会自动为语音报文修改 QoS(Quality of Service，服务质量)参数，来提高语音数据报文优

先级，保证通话质量。

2. 组网图

图 4-11 所示为自动模式 Voice VLAN 配置组网图。

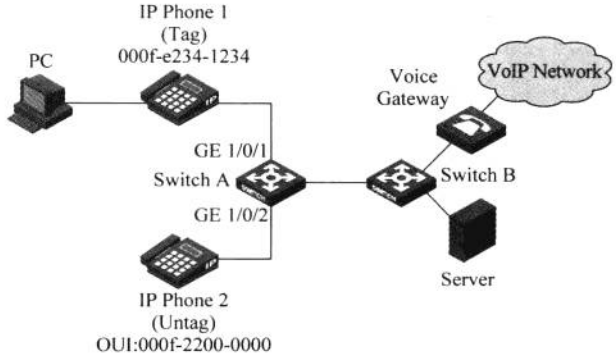


图 4-11 自动模式 Voice VLAN 配置组网图

3. 配置需求

如图 4-11 所示，PC 通过与 IP Phone 1 串联后接入 Switch A 的 GigabitEthernet 1/0/1 端口，IP Phone 2 单独接入 GigabitEthernet 1/0/2 端口。其中 IP Phone 1 发出的是 Tag 语音流(携带有 Voice VLAN 的 VLAN Tag)，IP Phone 2 发出的是 Untag 语音流(未携带任何 VLAN Tag)。现需要配置 Voice VLAN 功能，达到如下的要求。

(1) 配置 VLAN 2 为 Voice VLAN，用来传输语音数据，老化时间是 100min。传输用户业务数据的 VLAN 为 VLAN 6。

(2) 要求使 GigabitEthernet 1/0/1 和 GigabitEthernet 1/0/2 端口能够自动识别语音流，并将语音数据与 PC 的业务数据划分到不同 VLAN，通过 Switch B 分别发送至语音网关和服务器。

(3) IP Phone 1 和 IP Phone 2 的 OUI 地址不在交换机的默认 OUI 范围内，需要增加 OUI 地址 000f-e200-0000 和 000f-2200-0000，描述字符分别为 IP Phone 1 和 IP Phone 2。

4. 配置过程和解释

(1) 创建 VLAN 2、VLAN 6。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] quit
[SwitchA] vlan 6
[SwitchA-vlan6] quit
```

(2) 设置 Voice VLAN 的老化时间。

```
[SwitchA] voice vlan aging 100
```

(3) 设置 OUI 地址 000f-e200-0000，描述字符为 IP Phone 1。

```
[SwitchA] voice vlan mac-address 000f-e200-0000 mask ffff-ff00-0000 description IP Phone 1
```

(4) 设置 OUI 地址 000f-2200-0000，描述字符为 IP Phone 2。

```
[SwitchA] voice vlan mac-address 000f-2200-0000 mask ffff-ff00-0000 description IP Phone 2
```

(5) 全局开启 Voice VLAN 功能。

```
[SwitchA] voice vlan 2 enable
```

(6) 将端口 GigabitEthernet 1/0/1 上 Voice VLAN 的工作模式设置为自动模式(可选，默认情况下，端口的 Voice VLAN 工作在自动模式。)。

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] voice vlan mode auto
```

(7) 将端口 GigabitEthernet 1/0/1 设定为 Trunk 端口。

```
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
```

(8) 设置端口的默认 VLAN 为 VLAN 6，并允许 VLAN 6 的报文通过，以供 PC 的正常数据通信使用。

```
[SwitchA-GigabitEthernet1/0/1] port trunk pvid vlan 6
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan 6
```

(9) 开启端口 Voice VLAN 功能。

```
[SwitchA-GigabitEthernet1/0/1] voice vlan enable
```

提示：完成以上配置后，当 PC 报文通过时，数据自动在端口的默认 VLAN，也就是业务 VLAN 中传输；当 IP Phone 的报文通过时，端口自动将 Voice VLAN 加入到端口允许通过的 VLAN 列表中，而且在发送时以带有 Tag 的形式发送，使 IP Phone 可以正常接收报文。

端口 GigabitEthernet 1/0/1 也可以配置为 Hybrid 端口，配置过程与 Trunk 端口类似，只需要将业务 VLAN 配置为默认 VLAN 即可。当 IP Phone 发出的报文通过时，端口自动将 Voice VLAN 加入允许通过的 Tagged Port 列表中，保证 Voice VLAN 的报文带有 VLAN Tag 发送。

(10) 由于 IP Phone 2 只能发出 Untag 的语音流，因此 GigabitEthernet 1/0/2 端口只能配置为手动模式。

```
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] undo voice vlan mode auto
```

(11) 配置 GigabitEthernet 1/0/2 端口为 Access 端口，设置允许通过的 VLAN 为 Voice VLAN。

```
[SwitchA-GigabitEthernet1/0/2] port access vlan 2
```

(12) 开启端口 Voice VLAN 功能。

```
[SwitchA-GigabitEthernet1/0/2] voice vlan enable
```

提示：端口 GigabitEthernet 1/0/2 也可以配置为 Trunk 端口或 Hybrid 端口，同样需要将 Voice VLAN 配置为默认 VLAN，且必须配置在发送 Voice VLAN 的报文时去掉 VLAN Tag。

如果 IP Phone 2 发出的是 Tag 语音流，则 GigabitEthernet 1/0/2 端口只能配置为 Trunk 端口或 Hybrid 端口，并以保留 VLAN Tag 的方式发送 VLAN 2 的报文。

默认情况下，系统将以下地址预置为 Voice VLAN 的 OUI 地址，用户可以自行删除或修改这些预置地址，如表 4-1 所示。

表 4-1 设备预置的 OUI 地址

序号	OUI 地址	生产厂商
1	0001-e300-0000	Siemens phone
2	0003-6b00-0000	Cisco phone
3	0004-0d00-0000	Avaya phone
4	00d0-1e00-0000	Pingtel phone
5	0060-b900-0000	Philips/NEC phone
6	00e0-7500-0000	Polycom phone
7	00e0-bb00-0000	3com phone

4.7 QinQ 配置指导

4.7.1 QinQ 典型配置指导

基本 QinQ 功能添加的外层 VLAN Tag 是端口默认 VLAN 的 Tag，灵活的 QinQ 功能则可以为不同的内层 VLAN Tag 添加不同的外层 VLAN Tag。

1. 背景

运营商 N 公司为 M 公司提供广域网互连服务，N 公司使用 QinQ 技术在 M 公司总部和各个分支机构之间建立二层 VPN 隧道，M 公司可以规划自己的私网 VLAN ID，不会导致与运营商公网 VLAN ID 冲突的问题。

2. 组网图

图 4-12 所示为 QinQ 典型配置组网图。

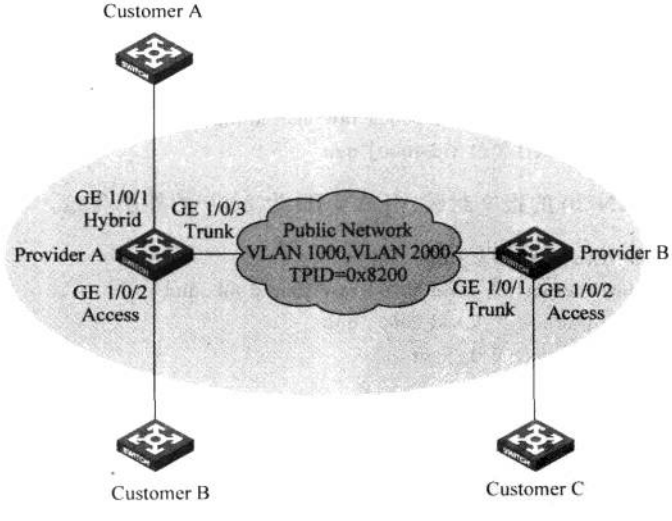


图 4-12 QinQ 典型配置组网图

3. 配置需求

Provider A、Provider B作为运营商网络边缘设备，Customer A、Customer B、Customer C为用户网络边缘设备。Provider A、Provider B之间通过Trunk端口连接，Provider A属于运营商网络的VLAN 1000，Provider B属于运营商网络的VLAN 2000。Provider A和Provider B之间，运营商采用其他厂商的设备，TPID值为0x8200。

配置完成后希望达到下列要求。

(1) Customer A的VLAN 10的报文可以和Customer B的VLAN 10的报文经过运营商网络的VLAN 1000转发后互通。

(2) Customer A的VLAN 20的报文可以和Customer C的VLAN 20的报文经过运营商网络的VLAN 2000转发后互通。

4. 配置过程和解释

(1) Provider A的配置。

创建VLAN 1000和VLAN 2000：

```
<ProviderA> system-view
[ProviderA] vlan 1000
[ProviderA-vlan1000] quit
[ProviderA] vlan 2000
[ProviderA-vlan2000] quit
```

① GigabitEthernet 1/0/1端口的配置。

a. 配置端口为Hybrid端口，允许VLAN 1000和VLAN 2000的报文通过，并且在发送时去掉外层Tag。

```
[ProviderA] interface GigabitEthernet 1/0/1
[ProviderA-GigabitEthernet1/0/1] port link-type hybrid
[ProviderA-GigabitEthernet1/0/1] port hybrid vlan 1000 2000 untagged
```

b. 将来自VLAN 10的报文封装VLAN ID为1000的外层Tag。

```
[ProviderA-GigabitEthernet1/0/1] qinq vid 1000
[ProviderA-GigabitEthernet1/0/1-vid-1000] raw-vlan-id inbound 10
[ProviderA-GigabitEthernet1/0/1-vid-1000] quit
```

c. 将来自VLAN 20的报文封装VLAN ID为2000的外层Tag。

```
[ProviderA-GigabitEthernet1/0/1] qinq vid 2000
[ProviderA-GigabitEthernet1/0/1-vid-2000] raw-vlan-id inbound 20
[ProviderA-GigabitEthernet1/0/1-vid-2000] quit
[ProviderA-GigabitEthernet1/0/1] quit
```

② GigabitEthernet 1/0/2端口的配置。

a. 配置端口为Access端口，允许VLAN 1000的报文通过。

```
[ProviderA] interface GigabitEthernet 1/0/2
[ProviderA-GigabitEthernet1/0/2] port access vlan 1000
```

b. 配置该端口的基本 QinQ 功能，将来自 VLAN 10 的报文封装 VLAN ID 为 1000 的外层 Tag。

```
[ProviderA-GigabitEthernet1/0/2] qinq enable
[ProviderA-GigabitEthernet1/0/2] quit
```

③ GigabitEthernet 1/0/3 端口的配置。

a. 配置端口为 Trunk 端口，且允许 VLAN 1000 和 VLAN 2000 的报文通过。

```
[ProviderA] interface GigabitEthernet 1/0/3
[ProviderA-GigabitEthernet1/0/3] port link-type trunk
[ProviderA-GigabitEthernet1/0/3] port trunk permit vlan 1000 2000
```

b. 为与公共网络中的设备进行互通，配置交换机发送报文时携带运营商 VLAN Tag 的 TPID 值为 0x8200。

```
[ProviderA-GigabitEthernet1/0/3] quit
[ProviderA] qinq ethernet-type service-tag 8200
```

(2) Provider B 的配置。

创建 VLAN 1000 和 VLAN 2000：

```
<ProviderB> system-view
[ProviderB] vlan 1000
[ProviderB-vlan1000] quit
[ProviderB] vlan 2000
[ProviderB-vlan2000] quit
```

① GigabitEthernet 1/0/1 端口的配置。

a. 配置端口为 Trunk 端口，且允许 VLAN 1000 和 VLAN 2000 的报文通过。

```
<ProviderB> system-view
[ProviderB] interface GigabitEthernet 1/0/1
[ProviderB-GigabitEthernet1/0/1] port link-type trunk
[ProviderB-GigabitEthernet1/0/1] port trunk permit vlan 1000 2000
```

b. 为与公共网络中的设备进行互通，配置交换机发送报文时携带运营商 VLAN Tag 的 TPID 值为 0x8200。

```
[ProviderB-GigabitEthernet1/0/1] quit
[ProviderB] qinq ethernet-type service-tag 8200
```

② GigabitEthernet 1/0/2 端口的配置。

a. 配置端口为 Access 端口，允许 VLAN 2000 的报文通过。

```
[ProviderB] interface GigabitEthernet 1/0/2
[ProviderB-GigabitEthernet1/0/2] port access vlan 2000
```

b. 配置该端口的基本 QinQ 功能，将来自 VLAN 20 的报文封装 VLAN ID 为 2000 的外层 Tag。

```
[ProviderB-GigabitEthernet1/0/2] qinq enable
```

(3) 公共网络设备的配置。由于 Provider A 和 Provider B 之间使用的公共网络设备可能来自其他厂商，这里只介绍基本原理。配置公共网络中与 Provider A 的 GigabitEthernet 1/0/3 端口和 Provider B 的 GigabitEthernet 1/0/1 端口连接的设备，使其相应的端口允许 VLAN 1000 和 VLAN 2000 的报文携带 VLAN Tag 进行发送即可。

提示： 默认情况下，H3C 系列交换机使用的 TPID 值为 0x8100。

一个内层 VLAN Tag 只能对应一个外层 VLAN Tag。如果用户想改变报文的外层 VLAN Tag，需要先删除旧的外层 VLAN Tag 配置，然后再配置新的外层 VLAN Tag。

4.7.2 基于流的灵活 QinQ 典型配置指导

灵活 QinQ 功能也可以通过 QoS 策略的方式实现，通过配置匹配报文原有 VLAN Tag 的流分类和封装外层 VLAN Tag 的流行为，并将其在 QoS 策略中进行关联，然后应用到连接用户的端口，即可以实现根据报文内层 VLAN 封装外层 VLAN Tag 的功能。

1. 背景

运营商 N 公司通过使用灵活 QinQ 技术，在能够隔离运营商网络和用户网络的同时，又能够提供丰富的业务特性和更加灵活的组网能力。

2. 组网图

图 4-13 所示为基于流的灵活 QinQ 典型配置组网图。

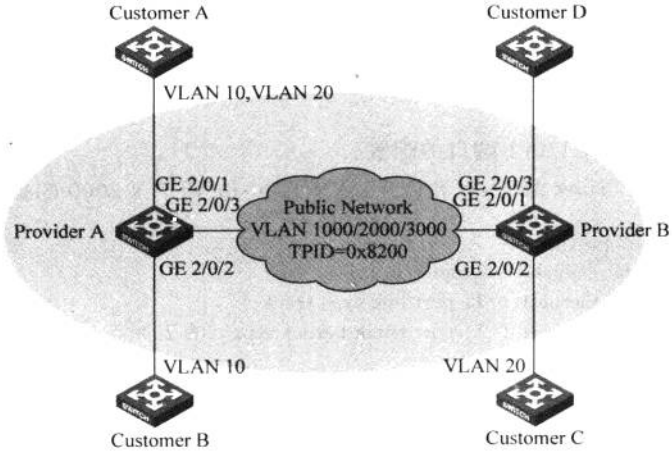


图 4-13 基于流的灵活 QinQ 典型配置组网图

3. 配置需求

Provider A、Provider B 为运营商网络边缘设备，Customer A、Customer B、Customer C、Customer D 为用户网络边缘设备。Provider A、Provider B 之间通过 Trunk 端口连接，允许运营商网络的 VLAN 1000、VLAN 2000 和 VLAN 3000 通过。Provider A 和Provider B 之间，运营商采用其他厂商的设备，TPID 值为 0x8200。

希望配置完成后达到下列要求。

(1) Customer A 的 VLAN 10 的报文可以和 Customer B 的 VLAN 10 的报文经过运营商网络的 VLAN 1000 转发后互通。

(2) Customer A 的 VLAN 20 的报文可以和 Customer C 的 VLAN 20 的报文经过运营商网络的 VLAN 2000 转发后互通。

(3) Customer A 的其余 VLAN 的报文可以通过运营商网络的 VLAN 3000 转发至 Customer D。

4. 配置过程和解释

(1) Provider A 的配置。

创建 VLAN 1000、VLAN 2000 和 VLAN 3000：

```
<ProviderA> system-view
[ProviderA] vlan 1000
[ProviderA-vlan1000] quit
[ProviderA] vlan 2000
[ProviderA-vlan2000] quit
[ProviderA] vlan 3000
[ProviderA-vlan3000] quit
```

① GigabitEthernet 2/0/1 端口的配置。

a. 配置端口为 Hybrid 端口，且允许 VLAN 1000、VLAN 2000 和 VLAN 3000 的报文通过，并且在发送时去掉外层 Tag。

```
[ProviderA] interface GigabitEthernet 2/0/1
[ProviderA-GigabitEthernet2/0/1] port link-type hybrid
[ProviderA-GigabitEthernet2/0/1] port hybrid vlan 1000 2000 3000 untagged
```

b. 将 VLAN 3000 配置为该端口的默认 VLAN，并配置基本 QinQ 功能，为接收的报文封装 VLAN 3000 的 Tag。

```
[ProviderA-GigabitEthernet2/0/1] port hybrid pvid vlan 3000
[ProviderA-GigabitEthernet2/0/1] qinq enable
[ProviderA-GigabitEthernet2/0/1] quit
```

c. 创建流分类规则，将 Customer A 的 VLAN 10 的报文定义为 A10 类。

```
[ProviderA] traffic classifier A10
[ProviderA-classifier-A10] if-match customer-vlan-id 10
[ProviderA-classifier-A10] quit
```

d. 定义流行为，为报文封装 VLAN 1000 的外层 VLAN Tag，流行为命名为 P1000。

```
[ProviderA] traffic behavior P1000
[ProviderA-behavior-P1000] nest top-most vlan-id 1000
[ProviderA-behavior-P1000] quit
```

e. 与以上配置类似，创建流分类 A20 匹配用户 VLAN ID 为 20 的报文，并创建流行为，为此类报文封装外层 VLAN 2000 的 Tag。

```
[ProviderA] traffic classifier A20
[ProviderA-classifier-A20] if-match customer-vlan-id 20
```

```
[ProviderA-classifier-A20] quit
[ProviderA] traffic behavior P2000
[ProviderA-behavior-P2000] nest top-most vlan-id 2000
[ProviderA-behavior-P2000] quit
```

f. 创建 QoS 策略，将流分类 A10 和流行为 P1000 进行关联，将流分类 A20 和流行为 P2000 关联，该策略命名为“qinq”。

```
[ProviderA] qos policy qinq
[ProviderA-qospolicy-qinq] classifier A10 behavior P1000
[ProviderA-qospolicy-qinq] classifier A20 behavior P2000
[ProviderA-qospolicy-qinq] quit
```

g. 在 GigabitEthernet 2/0/1 端口的接收方向应用 qinq 规则。

```
[ProviderA] interface GigabitEthernet 2/0/1
[ProviderA-GigabitEthernet2/0/1] qos apply policy qinq inbound
```

② GigabitEthernet 2/0/2 端口的配置。

a. 配置端口的默认 VLAN 为 VLAN 1000。

```
[ProviderA] interface GigabitEthernet 2/0/2
[ProviderA-GigabitEthernet2/0/2] port access vlan 1000
```

b. 配置端口的基本 QinQ 功能，将来自 VLAN 10 的报文封装 VLAN ID 为 1000 的外层 Tag。

```
[ProviderA-GigabitEthernet2/0/2] qinq enable
[ProviderA-GigabitEthernet2/0/2] quit
```

③ GigabitEthernet 2/0/3 端口的配置。

a. 配置端口为 Trunk 端口，且允许 VLAN 1000、VLAN 2000 和 VLAN 3000 的报文通过。

```
[ProviderA] interface GigabitEthernet 2/0/3
[ProviderA-GigabitEthernet2/0/3] port link-type trunk
[ProviderA-GigabitEthernet2/0/3] port trunk permit vlan 1000 2000 3000
```

b. 为与公共网络中的设备进行互通，配置运营商网络的 TPID 为 0x8200，即配置端口在添加外层 Tag 时使用的 TPID 值为 0x8200。

```
[ProviderA-GigabitEthernet2/0/3] qinq ethernet-type service-tag 8200
```

(2) Provider B 的配置。

创建 VLAN 1000、VLAN 2000 和 VLAN 3000：

```
<ProviderA> system-view
[ProviderA] vlan 1000
[ProviderA-vlan1000] quit
[ProviderA] vlan 2000
[ProviderA-vlan2000] quit
```

```
[ProviderA] vlan 3000
[ProviderA-vlan3000] quit
```

① GigabitEthernet 2/0/1 端口的配置。

a. 配置端口为 Trunk 端口，且允许 VLAN 1000、VLAN 2000 和 VLAN 3000 的报文通过。

```
<ProviderB> system-view
[ProviderB] interface GigabitEthernet 2/0/1
[ProviderB-GigabitEthernet2/0/1] port link-type trunk
[ProviderB-GigabitEthernet2/0/1] port trunk permit vlan 1000 2000 3000
```

b. 为与公共网络中的设备进行互通，配置运营商网络的 TPID 为 0x8200，即配置端口添加外层 Tag 时使用的 TPID 值为 0x8200。

```
[ProviderB-GigabitEthernet2/0/1] qinq ethernet-type service-tag 8200
[ProviderB-GigabitEthernet2/0/1] quit
```

② GigabitEthernet 2/0/2 端口的配置。

a. 配置端口的默认 VLAN 为 VLAN 2000。

```
[ProviderB] interface GigabitEthernet 2/0/2
[ProviderB-GigabitEthernet2/0/2] port access vlan 2000
```

b. 配置端口的基本 QinQ 功能，将来自 VLAN 20 的报文封装 VLAN ID 为 2000 的外层 Tag。

```
[ProviderB-GigabitEthernet2/0/2] qinq enable
[ProviderB-GigabitEthernet2/0/2] quit
```

③ GigabitEthernet 2/0/3 端口的配置。

a. 配置端口的默认 VLAN 为 VLAN 3000。

```
[ProviderB] interface GigabitEthernet 2/0/3
[ProviderB-GigabitEthernet2/0/3] port access vlan 3000
```

b. 配置端口的基本 QinQ 功能，为来自所有用户 VLAN 的报文封装 VLAN ID 为 3000 的外层 Tag。

```
[ProviderB-GigabitEthernet2/0/3] qinq enable
```

(3) 公共网络设备的配置。由于 Provider A 和 Provider B 之间使用的公共网络设备可能来自其他厂商，这里只介绍基本原理。配置公共网络中与 Provider A 的 GigabitEthernet 2/0/3 端口和 Provider B 的 GigabitEthernet 2/0/1 端口连接的设备，使其相应的端口允许 VLAN 1000、VLAN 2000 和 VLAN 3000 的报文携带 VLAN Tag 进行发送即可。

提示：开启灵活 QinQ 前必须先配置端口的基本 QinQ 功能，灵活 QinQ 的优先级高于基本 QinQ，即在端口接收的报文不能匹配流分类规则的情况下，才根据基本 QinQ 的功能封装外层 VLAN Tag。

4.8 BPDU Tunnel 配置指导

BPDU Tunnel 功能可使运行 STP 功能的用户私网和运营商网络拥有各自的生成树，互不干扰，它具有下列作用。

(1) 对 BPDU 报文进行透明传输。可以使同一个用户网络的 BPDU 报文在运营商网络内指定的 VLAN 中进行广播，使得在不同地域的同一个用户网络可以跨越运营商网络进行统一的生成树计算。

(2) 同时，由于不同用户网络的 BPDU 报文在运营商网络的不同 VLAN 中进行广播，所以不同用户网络的 BPDU 报文相互隔离，可以独立进行生成树计算。

1. 背景

M 公司为避免环路，需要在私网中启用 STP 功能，当一侧私网发生拓扑变化时，会发送 BPDU 报文给另一侧私网，否则将无法完成在整个用户私网内的生成树计算。但由于 BPDU 报文是二层组播报文，所有开启 STP 功能的设备都会接收并处理该报文，因此若用户私网和运营商网络的生成树一起计算将导致每个网络都无法生成正确的生成树。运营商 N 公司使用 BPDU Tunnel 技术解决了该问题。

2. 组网图

图 4-14 所示为 BPDU Tunnel 配置组网图。

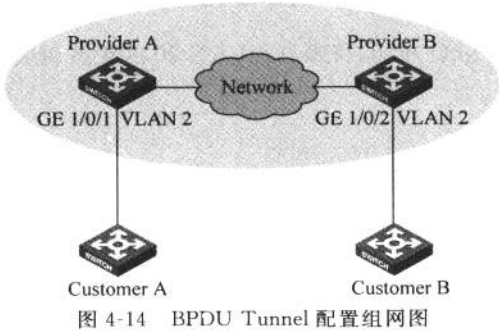


图 4-14 BPDU Tunnel 配置组网图

3. 配置需求

Customer A、Customer B 为用户网络接入设备，Provider A、Provider B 为运营商网络接入设备，运营商网络中的设备之间通过配置好的 Trunk 端口实现连接。

要求通过配置实现以下两点。

(1) 处于不同地域的用户 Customer A、Customer B 可以跨越运营商网络进行统一的生成树计算。

(2) BPDU Tunnel 报文采用的组播目的 MAC 地址为 0x0100-0ccd-cdd0。

4. 配置过程和解释

(1) Provider A 的配置。

① 配置 BPDU Tunnel 报文采用的组播目的 MAC 地址为 0x0100-0ccd-cdd0。

```
<ProviderA> system-view
[ProviderA] bpdu-tunnel tunnel-dmac 0100-0ccd-cdd0
```

② 配置 GigabitEthernet 1/0/1 端口使用 VLAN 2 对用户报文进行传输。

```
[ProviderA] interface GigabitEthernet 1/0/1
[ProviderA-GigabitEthernet1/0/1] port access vlan 2
```

③ 配置 GigabitEthernet 1/0/1 端口对 BPDU 报文进行透明传输。

```
[ProviderA-GigabitEthernet1/0/1] stp disable
[ProviderA-GigabitEthernet1/0/1] bpdu-tunnel dot1q stp
```

(2) Provider B 的配置。

① 配置 BPDU Tunnel 报文采用的组播目的 MAC 地址为 0x0100-0ccd-cdd0。

```
<ProviderB> system-view
[ProviderB] bpdu-tunnel tunnel-dmac 0100-0ccd-cdd0
```

② 配置 GigabitEthernet 1/0/2 端口使用 VLAN 2 对用户报文进行传输。

```
[ProviderB] interface GigabitEthernet1/0/2
[ProviderB-GigabitEthernet1/0/2] port access vlan 2
```

③ 配置 GigabitEthernet 1/0/2 端口对 BPDU 报文进行透明传输。

```
[ProviderB-GigabitEthernet1/0/2] stp disable
[ProviderB-GigabitEthernet1/0/2] bpdu-tunnel dot1q stp
```

提示：在端口上使能 DLDP、EOAM、GVRP、HGMP、LLDP 或 STP 协议的 BPDU Tunnel 功能之前，必须在该端口上关闭相应的协议。由于 PVST 协议是一种特殊的 STP 协议，因此在端口上使能 PVST 协议的 BPDU Tunnel 功能之前，也必须在该端口上关闭 STP 协议并使能 STP 协议的 BPDU Tunnel 功能。

在运营商网络两端的报文输入/输出设备上配置的 BPDU Tunnel 报文采用的组播目的 MAC 地址必须保持一致，否则系统无法对 BPDU Tunnel 报文进行正确的识别。

4.9 VLAN 映射配置指导

4.9.1 1∶1 VLAN 映射和 *N*∶1 VLAN 映射典型配置指导

1∶1 VLAN 映射是指将来自某一特定 VLAN 的报文所携带的 VLAN Tag 替换为新的 VLAN Tag。

N∶1 VLAN 映射是指将来自两个或多个 VLAN 的报文所携带的不同 VLAN Tag 替换为相同的 VLAN Tag。

1. 背景

在 M 公司职工住宅小区规划中，为了区分不同的用户，需要在楼道交换机处用不同的 VLAN 来承载不同用户的相同业务，即进行 1∶1 VLAN 映射，这就要用到大量的 VLAN。但汇聚层网络接入设备可提供的 VLAN 数量有限，因此需要在园区交换机上来进行 VLAN 的汇聚，用一个 VLAN 来承载原本由多个 VLAN 承载的不同用户的相同业务，即进行 *N*∶1 VLAN 映射，节省了 VLAN 资源。

2. 组网图

图 4-15 所示为 1：1 VLAN 映射和 *N*：1 VLAN 映射典型配置组网图。

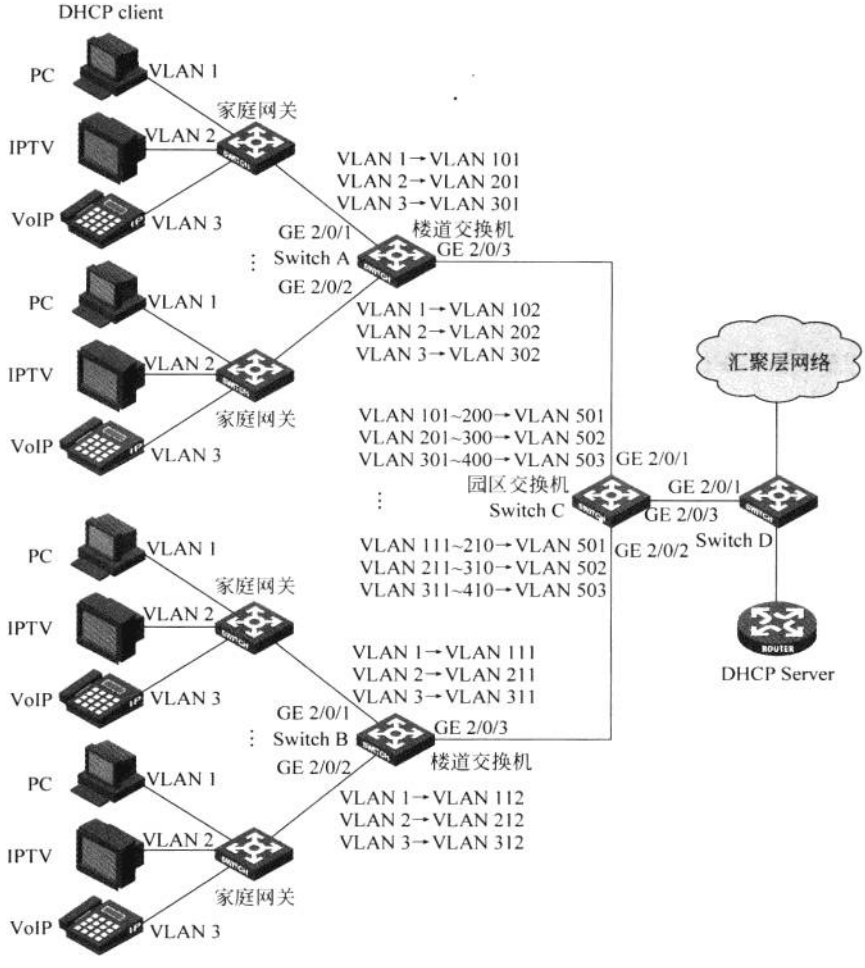


图 4-15　1：1 VLAN 映射和 *N*：1 VLAN 映射典型配置组网图

3. 配置需求

在多业务智能小区中，每户家庭都有 PC、IPTV 和 VoIP 这 3 种网络业务应用，各个业务终端均使用汇聚层的 DHCP 服务器自动分配 IP 地址。

家庭网关将这些业务分别使用 VLAN 1、VLAN 2 和 VLAN 3 发送至楼道交换机，再经由园区交换机发送至汇聚层网络。为实现对多个用户的多种业务进行精确划分，现要求使用 1：1 和 *N*：1 VLAN 映射功能完成以下使用需求。

(1) 在楼道交换机上使用 1：1 VLAN 映射功能，实现将不同家庭网关发出的相同 VLAN 的报文进行区分。

(2) 在园区交换机上使用 *N*：1 VLAN 映射功能，根据业务类型将所有用户的报文分为 3 类上传至汇聚层交换机。

4. 配置过程和解释

(1) 配置 Switch A。

① VLAN 和端口的配置。

a. 创建 CVLAN(Custom VLAN)和 SVLAN(Service VLAN)。

```
<SwitchA> system-view
[SwitchA] vlan 2 to 3
[SwitchA] vlan 101 to 102
[SwitchA] vlan 201 to 202
[SwitchA] vlan 301 to 302
```

b. 配置端口 GigabitEthernet 2/0/1 允许第一个家庭的 CVLAN 和对应 SVLAN 的报文通过。

```
[SwitchA] interface GigabitEthernet 2/0/1
[SwitchA-GigabitEthernet2/0/1] port link-type trunk
[SwitchA-GigabitEthernet2/0/1] port trunk permit vlan 1 2 3 101 201 301
```

c. 开启端口 GigabitEthernet 2/0/1 的基本 QinQ 功能。

```
[SwitchA-GigabitEthernet2/0/1] qinq enable
[SwitchA] quit
```

d. 配置端口 GigabitEthernet 2/0/2 允许第二个家庭的 CVLAN 和对应 SVLAN 的报文通过。

```
[SwitchA] interface GigabitEthernet 2/0/2
[SwitchA-GigabitEthernet2/0/2] port link-type trunk
[SwitchA-GigabitEthernet2/0/2] port trunk permit vlan 1 2 3 102 202 302
```

e. 开启端口 GigabitEthernet 2/0/2 的基本 QinQ 功能。

```
[SwitchA-GigabitEthernet2/0/2] qinq enable
[SwitchA] quit
```

② 配置上行报文映射策略。

a. 配置流分类 c1～c3,分别匹配家庭网关发出的 CVLAN。

```
[SwitchA] traffic classifier c1
[SwitchA-classifier-c1] if-match customer-vlan-id 1
[SwitchA-classifier-c1] traffic classifier c2
[SwitchA-classifier-c2] if-match customer-vlan-id 2
[SwitchA-classifier-c2] traffic classifier c3
[SwitchA-classifier-c3] if-match customer-vlan-id 3
[SwitchA-classifier-c3] quit
```

b. 配置流行为 b1～b6,分别定义替换不同的 SVLAN(101、201、301、102、202、302)的动作。

```
[SwitchA] traffic behavior b1
[SwitchA-behavior-b1] remark service-vlan-id 101
[SwitchA-behavior-b1] traffic behavior b2
```

```
[SwitchA-behavior-b2] remark service-vlan-id 201
[SwitchA-behavior-b2] traffic behavior b3
[SwitchA-behavior-b3] remark service-vlan-id 301
[SwitchA-behavior-b3] traffic behavior b4
[SwitchA-behavior-b4] remark service-vlan-id 102
[SwitchA-behavior-b4] traffic behavior b5
[SwitchA-behavior-b5] remark service-vlan-id 202
[SwitchA-behavior-b5] traffic behavior b6
[SwitchA-behavior-b6] remark service-vlan-id 302
[SwitchA-behavior-b6] quit
```

c. 配置 QoS 策略 p1 和 p2，根据网络规划将流分类和流行为进行绑定。

```
[SwitchA] qos policy p1
[SwitchA-policy-p1] classifier c1 behavior b1
[SwitchA-policy-p1] classifier c2 behavior b2
[SwitchA-policy-p1] classifier c3 behavior b3
[SwitchA-policy-p1] quit
[SwitchA] qos policy p2
[SwitchA-policy-p2] classifier c1 behavior b4
[SwitchA-policy-p2] classifier c2 behavior b5
[SwitchA-policy-p2] classifier c3 behavior b6
[SwitchA-policy-p2] quit
```

③ 配置下行报文映射策略。配置下行策略，将 SVLAN 映射回原来的 CVLAN，配置思路类似于配置上行策略，这里不再赘述。

```
[SwitchA] traffic classifier c11
[SwitchA-classifier-c11] if-match service-vlan-id 101
[SwitchA-classifier-c11] traffic classifier c22
[SwitchA-classifier-c22] if-match service-vlan-id 201
[SwitchA-classifier-c22] traffic classifier c33
[SwitchA-classifier-c33] if-match service-vlan-id 301
[SwitchA-classifier-c33] traffic classifier c44
[SwitchA-classifier-c44] if-match service-vlan-id 102
[SwitchA-classifier-c44] traffic classifier c55
[SwitchA-classifier-c55] if-match service-vlan-id 202
[SwitchA-classifier-c55] traffic classifier c66
[SwitchA-classifier-c66] if-match service-vlan-id 302
[SwitchA-classifier-c66] quit
[SwitchA] traffic behavior b11
[SwitchA-behavior-b11] remark customer-vlan-id 1
[SwitchA-behavior-b11] traffic behavior b22
[SwitchA-behavior-b22] remark customer-vlan-id 2
[SwitchA-behavior-b22] traffic behavior b33
[SwitchA-behavior-b33] remark customer-vlan-id 3
[SwitchA-behavior-b33] quit
[SwitchA] qos policy p11
[SwitchA-policy-p11] classifier c11 behavior b11
[SwitchA-policy-p11] classifier c22 behavior b22
[SwitchA-policy-p11] classifier c33 behavior b33
```

```
[SwitchA-policy-p11] quit
[SwitchA] qos policy p22
[SwitchA-policy-p22] classifier c44 behavior b11
[SwitchA-policy-p22] classifier c55 behavior b22
[SwitchA-policy-p22] classifier c66 behavior b33
[SwitchA-policy-p22] quit
```

④ 在端口上应用 QoS 策略。

a. 在端口 GigabitEthernet 2/0/1 的入方向应用上行策略 p1。

```
[SwitchA] interface GigabitEthernet 2/0/1
[SwitchA-GigabitEthernet2/0/1] qos apply policy p1 inbound
```

b. 在端口 GigabitEthernet 2/0/1 的出方向应用下行策略 p11。

```
[SwitchA-GigabitEthernet2/0/1] qos apply policy p11 outbound
[SwitchA-GigabitEthernet2/0/1] quit
```

c. 在端口 GigabitEthernet 2/0/2 的入方向应用上行策略 p2。

```
[SwitchA] interface GigabitEthernet 2/0/2
[SwitchA-GigabitEthernet2/0/2] qos apply policy p2 inbound
```

d. 在端口 GigabitEthernet 2/0/2 的出方向应用下行策略 p22。

```
[SwitchA-GigabitEthernet2/0/2] qos apply policy p22 outbound
[SwitchA-GigabitEthernet2/0/2] quit
```

⑤ 配置上行端口。配置端口 GigabitEthernet 2/0/3 允许 SVLAN 的报文通过。

```
[SwitchA] interface GigabitEthernet 2/0/3
[SwitchA-GigabitEthernet2/0/3] port link-type trunk
[SwitchA-GigabitEthernet2/0/3] port trunk permit vlan 101 201 301 102 202 302
```

(2) 配置 Switch B。

① VLAN 和端口的配置。

a. 创建 CVLAN 和 SVLAN。

```
<SwitchB> system-view
[SwitchB] vlan 2 to 3
[SwitchB] vlan 111 to 112
[SwitchB] vlan 211 to 212
[SwitchB] vlan 311 to 312
```

b. 配置端口 GigabitEthernet 2/0/1 允许 CVLAN 和 SVLAN 的报文通过。

```
[SwitchB] interface GigabitEthernet 2/0/1
[SwitchB-GigabitEthernet2/0/1] port link-type trunk
[SwitchB-GigabitEthernet2/0/1] port trunk permit vlan 1 2 3 111 211 311
```

c. 开启端口 GigabitEthernet 2/0/1 的基本 QinQ 功能。

```
[SwitchB-GigabitEthernet2/0/1] qinq enable
[SwitchB] quit
```

d. 配置端口 GigabitEthernet 2/0/2 允许 CVLAN 和 SVLAN 的报文通过。

```
[SwitchB] interface GigabitEthernet 2/0/2
[SwitchB-GigabitEthernet2/0/2] port link-type trunk
[SwitchB-GigabitEthernet2/0/2] port trunk permit vlan 1 2 3 112 212 312
```

e. 开启端口 GigabitEthernet 2/0/2 的基本 QinQ 功能。

```
[SwitchB-GigabitEthernet2/0/2] qinq enable
[SwitchB] quit
```

② 配置上行报文映射策略。配置上行策略，将不同用户的不同业务 CVLAN 映射到不同的 SVLAN。配置思路与 Switch A 上的配置类似，这里不再赘述。

```
[SwitchB] traffic classifier c1
[SwitchB-classifier-c1] if-match customer-vlan-id 1
[SwitchB-classifier-c1] traffic classifier c2
[SwitchB-classifier-c2] if-match customer-vlan-id 2
[SwitchB-classifier-c2] traffic classifier c3
[SwitchB-classifier-c3] if-match customer-vlan-id 3
[SwitchB-classifier-c3] quit
[SwitchB] traffic behavior b1
[SwitchB-behavior-b1] remark service-vlan-id 111
[SwitchB-behavior-b1] traffic behavior b2
[SwitchB-behavior-b2] remark service-vlan-id 211
[SwitchB-behavior-b2] traffic behavior b3
[SwitchB-behavior-b3] remark service-vlan-id 311
[SwitchB-behavior-b3] traffic behavior b4
[SwitchB-behavior-b4] remark service-vlan-id 112
[SwitchB-behavior-b4] traffic behavior b5
[SwitchB-behavior-b5] remark service-vlan-id 212
[SwitchB-behavior-b5] traffic behavior b6
[SwitchB-behavior-b6] remark service-vlan-id 312
[SwitchB-behavior-b6] quit
[SwitchB] qos policy p1
[SwitchB-policy-p1] classifier c1 behavior b1
[SwitchB-policy-p1] classifier c2 behavior b2
[SwitchB-policy-p1] classifier c3 behavior b3
[SwitchB-policy-p1] quit
[SwitchB] qos policy p2
[SwitchB-policy-p2] classifier c1 behavior b4
[SwitchB-policy-p2] classifier c2 behavior b5
[SwitchB-policy-p2] classifier c3 behavior b6
[SwitchB-policy-p2] quit
```

③ 配置下行报文映射策略。配置下行策略，将 SVLAN 映射回原来的 CVLAN。配置思路与 Switch A 上的配置类似，这里不再赘述。

```
[SwitchB] traffic classifier c11
[SwitchB-classifier-c11] if-match service-vlan-id 111
```

```
[SwitchB-classifier-c11] traffic classifier c22
[SwitchB-classifier-c22] if-match service-vlan-id 211
[SwitchB-classifier-c22] traffic classifier c33
[SwitchB-classifier-c33] if-match service-vlan-id 311
[SwitchB-classifier-c33] traffic classifier c44
[SwitchB-classifier-c44] if-match service-vlan-id 112
[SwitchB-classifier-c44] traffic classifier c55
[SwitchB-classifier-c55] if-match service-vlan-id 212
[SwitchB-classifier-c55] traffic classifier c66
[SwitchB-classifier-c66] if-match service-vlan-id 312
[SwitchB-classifier-c66] quit
[SwitchB] traffic behavior b11
[SwitchB-behavior-b11] remark customer-vlan-id 1
[SwitchB-behavior-b11] traffic behavior b22
[SwitchB-behavior-b22] remark customer-vlan-id 2
[SwitchB-behavior-b22] traffic behavior b33
[SwitchB-behavior-b33] remark customer-vlan-id 3
[SwitchB-behavior-b33] quit
[SwitchB] qos policy p11
[SwitchB-policy-p11] classifier c11 behavior b11
[SwitchB-policy-p11] classifier c22 behavior b22
[SwitchB-policy-p11] classifier c33 behavior b33
[SwitchB-policy-p11] quit
[SwitchB] qos policy p22
[SwitchB-policy-p22] classifier c44 behavior b11
[SwitchB-policy-p22] classifier c55 behavior b22
[SwitchB-policy-p22] classifier c66 behavior b33
[SwitchB-policy-p22] quit
```

④ 在端口上应用 QoS 策略。

a. 在端口 GigabitEthernet 2/0/1 的入方向应用上行策略 p1。

```
[SwitchB] interface GigabitEthernet 2/0/1
[SwitchB-GigabitEthernet2/0/1] qos apply policy p1 inbound
```

b. 在端口 GigabitEthernet 2/0/1 的出方向应用下行策略 p11。

```
[SwitchB-GigabitEthernet2/0/1] qos apply policy p11 outbound
[SwitchB-GigabitEthernet2/0/1] quit
```

c. 在端口 GigabitEthernet 2/0/2 的入方向应用上行策略 p2。

```
[SwitchB-GigabitEthernet2/0/2] qos apply policy p2 inbound
```

d. 在端口 GigabitEthernet 2/0/2 的出方向应用下行策略 p22。

```
[SwitchB-GigabitEthernet2/0/2] qos apply policy p22 outbound
[SwitchB-GigabitEthernet2/0/2] quit
```

⑤ 配置上行端口。配置端口 GigabitEthernet 2/0/3 允许 SVLAN 的报文通过。

```
[SwitchB] interface GigabitEthernet 2/0/3
[SwitchB-GigabitEthernet2/0/3] port link-type trunk
```

```
[SwitchB-GigabitEthernet2/0/3] port trunk permit vlan 111 211 311 112 212 312
```

(3) 配置 Switch C。

① VLAN 和端口的配置。

a. 根据楼道交换机发送的报文创建所有对应的 CVLAN，以及根据业务分类映射后的 SVLAN 501、SVLAN 502、SVLAN 503，配置过程这里省略。

b. 配置端口 GigabitEthernet 2/0/1 允许 CVLAN 和 SVLAN 的报文通过。

```
<SwitchC> system-view
[SwitchC] interface GigabitEthernet 2/0/1
[SwitchC-GigabitEthernet2/0/1] port link-type trunk
[SwitchC-GigabitEthernet2/0/1] port trunk permit vlan 101 201 301 102 202 302 501 502 503
```

c. 开启端口 GigabitEthernet 2/0/1 的用户侧 QinQ 功能。

```
[SwitchC-GigabitEthernet2/0/1] qinq enable downlink
[SwitchC-GigabitEthernet2/0/1] quit
```

d. 配置端口 GigabitEthernet 2/0/2 允许 CVLAN 和 SVLAN 的报文通过。

```
[SwitchC] interface GigabitEthernet 2/0/2
[SwitchC-GigabitEthernet2/0/2] port link-type trunk
[SwitchC-GigabitEthernet2/0/2] port trunk permit vlan 111 211 311 112 212 312 501 502 503
```

e. 开启端口 GigabitEthernet 2/0/2 的用户侧 QinQ 功能。

```
[SwitchC-GigabitEthernet2/0/2] qinq enable downlink
[SwitchC-GigabitEthernet2/0/2] quit
```

② DHCP Snooping 和 ARP Detection 的配置。

a. 开启 DHCP Snooping 功能。交换机在接收下行报文时，可以通过查找 SVLAN 对应的 DHCP Snooping 表项中的 DHCP 客户端 IP 地址、MAC 地址以及 CVLAN 的绑定表项，将报文的 SVLAN 修改为原来的 CVLAN。

```
[SwitchC] dhcp-snooping
```

b. 在每个进行映射的 VLAN 上都使能 ARP Detection 功能，以便对 ARP 报文进行 VLAN 映射处理。

```
[SwitchC] vlan 101
[SwitchC-vlan101] arp detection enable
[SwitchC-vlan101] vlan 201
[SwitchC-vlan201] arp detection enable
[SwitchC-vlan201] vlan 301
[SwitchC-vlan301] arp detection enable
[SwitchC-vlan301] vlan 102
[SwitchC-vlan102] arp detection enable
[SwitchC-vlan102] vlan 202
[SwitchC-vlan202] arp detection enable
[SwitchC-vlan202] vlan 302
[SwitchC-vlan302] arp detection enable
```

```
[SwitchC-vlan302] vlan 111
[SwitchC-vlan111] arp detection enable
[SwitchC-vlan111] vlan 211
[SwitchC-vlan211] arp detection enable
[SwitchC-vlan211] vlan 311
[SwitchC-vlan311] arp detection enable
[SwitchC-vlan311] vlan 112
[SwitchC-vlan112] arp detection enable
[SwitchC-vlan112] vlan 212
[SwitchC-vlan212] arp detection enable
[SwitchC-vlan212] vlan 312
[SwitchC-vlan312] arp detection enable
[SwitchC-vlan312] vlan 501
[SwitchC-vlan501] arp detection enable
[SwitchC-vlan501] vlan 502
[SwitchC-vlan502] arp detection enable
[SwitchC-vlan502] vlan 503
[SwitchC-vlan503] arp detection enable
[SwitchC-vlan503] quit
```

③ 配置上行报文映射策略。配置上行策略，将不同用户的相同业务 VLAN(CVLAN)映射到同一个 VLAN(SVLAN)。

```
[SwitchC] traffic classifier c1
[SwitchC-classifier-c1] if-match customer-vlan-id 101 to 200
[SwitchC-classifier-c1] traffic classifier c2
[SwitchC-classifier-c2] if-match customer-vlan-id 201 to 300
[SwitchC-classifier-c2] traffic classifier c3
[SwitchC-classifier-c3] if-match customer-vlan-id 301 to 400
[SwitchC-classifier-c3] traffic classifier c4
[SwitchC-classifier-c4] if-match customer-vlan-id 111 to 210
[SwitchC-classifier-c4] traffic classifier c5
[SwitchC-classifier-c5] if-match customer-vlan-id 211 to 310
[SwitchC-classifier-c5] traffic classifier c6
[SwitchC-classifier-c6] if-match customer-vlan-id 311 to 410
[SwitchC-classifier-c6] quit
[SwitchC] traffic behavior b1
[SwitchC-behavior-b1] remark service-vlan-id 501
[SwitchC-behavior-b1] traffic behavior b2
[SwitchC-behavior-b2] remark service-vlan-id 502
[SwitchC-behavior-b2] traffic behavior b3
[SwitchC-behavior-b3] remark service-vlan-id 503
[SwitchC-behavior-b3] quit
[SwitchC] qos policy p1
[SwitchC-policy-p1] classifier c1 behavior b1 mode dot1q-tag-manipulation
[SwitchC-policy-p1] classifier c2 behavior b2 mode dot1q-tag-manipulation
[SwitchC-policy-p1] classifier c3 behavior b3 mode dot1q-tag-manipulation
[SwitchC-policy-p1] quit
[SwitchC] qos policy p2
[SwitchC-policy-p2] classifier c4 behavior b1 mode dot1q-tag-manipulation
[SwitchC-policy-p2] classifier c5 behavior b2 mode dot1q-tag-manipulation
```

```
[SwitchC-policy-p2] classifier c6 behavior b3 mode dot1q-tag-manipulation
[SwitchC-policy-p2] quit
```

④ 在端口上应用 QoS 策略。

a. 在端口 GigabitEthernet 2/0/1 的入方向应用上行策略 p1。

```
[SwitchC] interface GigabitEthernet 2/0/1
[SwitchC-GigabitEthernet2/0/1] qos apply policy p1 inbound
[SwitchC-GigabitEthernet2/0/1] quit
```

b. 在端口 GigabitEthernet 2/0/2 的入方向应用上行策略 p2。

```
[SwitchC] interface GigabitEthernet 2/0/2
[SwitchC-GigabitEthernet2/0/2] qos apply policy p2 inbound
[SwitchC-GigabitEthernet2/0/2] quit
```

⑤ 配置上行端口。

a. 配置端口 GigabitEthernet 2/0/3 允许 SVLAN 的报文通过。

```
[SwitchC] interface GigabitEthernet 2/0/3
[SwitchC-GigabitEthernet2/0/3] port link-type trunk
[SwitchC-GigabitEthernet2/0/3] port trunk permit vlan 501 502 503
```

b. 配置端口 GigabitEthernet 2/0/3 为 DHCP Snooping 信任端口。

```
[SwitchC-GigabitEthernet2/0/3] dhcp-snooping trust
```

c. 配置端口 GigabitEthernet 2/0/3 为 ARP 信任端口。

```
[SwitchC-GigabitEthernet2/0/3] arp detection trust
```

d. 开启端口 GigabitEthernet 2/0/3 的网络侧 QinQ 功能。

```
[SwitchC-GigabitEthernet2/0/3] qinq enable uplink
```

(4) 配置 Switch D。

① 创建 SVLAN 501、SVLAN 502、SVLAN 503，配置过程这里不再赘述。

② 使能 DHCP Snooping 功能。

```
<SwitchD> system-view
[SwitchD] dhcp-snooping
```

③ 配置端口 GigabitEthernet 2/0/1 允许 SVLAN 的报文通过。

```
[SwitchD] interface GigabitEthernet 2/0/1
[SwitchD-GigabitEthernet2/0/1] port link-type trunk
[SwitchD-GigabitEthernet2/0/1] port trunk permit vlan 501 502 503
```

提示：在配置前，需要事先规划好 CVLAN 和 SVLAN 的映射关系。

在下行端口上应用策略前，需要先开启端口的用户侧 QinQ 功能；在下行端口上关闭用户侧 QinQ 功能之前，需要先解除 QoS 策略在该端口上的绑定。

在 N：1 VLAN 映射中，如果用户想改变 VLAN 映射关系，必须先用 reset dhcp-snooping 命令清除 DHCP Snooping 表项，或用 ip check source 命令取消下行端口与源 IP

和源 MAC 的动态绑定后再重新绑定，然后再修改 QoS 策略中的 VLAN 映射关系。

在配置 N：1 VLAN 映射时，不能在交换机上为 SVLAN 和 CVLAN 创建 VLAN 接口。

4.9.2 1：2 VLAN 映射和 2：2 VLAN 映射典型配置指导

2：2 VLAN 映射是指将携带有两层 VLAN Tag 的报文的内、外层 VLAN Tag 都替换为新的 VLAN Tag。

1. 背景

M 公司在两个地市的办公区域之间创建了 VPN 1 的连接，两地发送给运营商的报文分别使用 VLAN 10 和 VLAN 30 的标签。该 VPN 连接在公网中穿越两个 SP（Service Provider，网络服务提供商），需要实现互通。

2. 组网图

图 4-16 所示为 1：2 VLAN 映射和 2：2 VLAN 映射典型配置组网图。

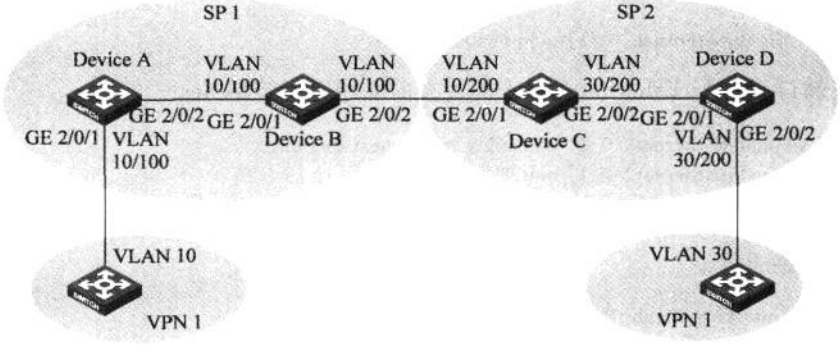


图 4-16 1：2 VLAN 映射和 2：2 VLAN 映射典型配置组网图

3. 配置需求

要求在 SP 网络的设备上使用 1：2 VLAN 映射和 2：2 VLAN 映射功能，完成以下的需求。

（1）两个 SP 网络均使用两层标签传输用户数据，SP 1 为用户分配的外层标签为 VLAN 100，SP 2 为用户分配的外层标签为 VLAN 200，且数据在穿越两个 SP 网络时标签可以自行修改以适应下一 SP 网络的规划。

（2）要求处于不同地域的 VPN 1 内的不同 VLAN 之间可以互通。

4. 配置过程和解释

（1）配置 Device A。

① 创建 VLAN 100。

```
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA-vlan100] quit
```

② 配置上行策略，为 VLAN 10 报文添加 VLAN ID 为 100 的外层 VLAN Tag。

```
[DeviceA] traffic classifier nest
```

```
[DeviceA-classifier-nest] if-match customer-vlan-id 10
[DeviceA-classifier-nest] quit
[DeviceA] traffic behavior nest
[DeviceA-behavior-nest] nest top-most vlan-id 100
[DeviceA-behavior-nest] quit
[DeviceA] qos policy nest
[DeviceA-qospolicy-nest] classifier nest behavior nest
[DeviceA-qospolicy-nest] quit
```

③ 配置端口 GigabitEthernet 2/0/1 为 Hybrid 端口，且在发送 VLAN 100 的报文时去掉 VLAN 标签。

```
[DeviceA] intface GigabitEthernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] port link-type hybrid
[DeviceA-GigabitEthernet2/0/1] port hybrid vlan 100 untagged
```

④ 开启端口 GigabitEthernet 2/0/1 的基本 QinQ 功能。

```
[DeviceA-GigabitEthernet2/0/1] qinq enable
```

⑤ 在端口 GigabitEthernet 2/0/1 的入方向应用上行策略 nest。

```
[DeviceA-GigabitEthernet2/0/1] qos apply policy nest inbound
[DeviceA-GigabitEthernet2/0/1] quit
```

⑥ 配置上行端口 GigabitEthernet 2/0/2 为 Trunk 端口，且允许 VLAN 100 的报文携带 VLAN 标签通过。

```
[DeviceA] interface GigabitEthernet 2/0/2
[DeviceA-GigabitEthernet2/0/2] port link-type trunk
[DeviceA-GigabitEthernet2/0/2] port trunk permit vlan 100
```

(2) 配置 Device B。

① 创建 VLAN 100。

```
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB-vlan100] quit
```

② 配置端口 GigabitEthernet 2/0/1 为 Trunk 端口，且允许 VLAN 100 的报文携带 VLAN 标签通过。

```
[DeviceB] interface GigabitEthernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] port link-type trunk
[DeviceB-GigabitEthernet2/0/1] port trunk permit vlan 100
[DeviceB-GigabitEthernet2/0/1] quit
```

③ 配置端口 GigabitEthernet 2/0/2 为 Trunk 端口，且允许 VLAN 100 的报文携带 VLAN 标签通过。

```
[DeviceB] interface GigabitEthernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] port link-type trunk
[DeviceB-GigabitEthernet2/0/2] port trunk permit vlan 100
```

(3) 配置 Device C。

① 创建 VLAN 200。

```
<DeviceC> system-view
[DeviceC] vlan 200
[DeviceC-vlan200] quit
```

② 配置端口 GigabitEthernet 2/0/1 入方向对报文的分类规则 downlink_in，匹配内层 VLAN 为 10、外层 VLAN 为 100 的报文。

```
[DeviceC] traffic classifier downlink_in
[DeviceC-classifier-downlink_in] if-match customer-vlan-id 10
[DeviceC-classifier-downlink_in] if-match service-vlan-id 100
[DeviceC-classifier-downlink_in] quit
```

③ 配置端口 GigabitEthernet 2/0/1 入方向对报文的流行为 downlink_in，将报文的外层 VLAN 替换为 200。

```
[DeviceC] traffic behavior downlink_in
[DeviceC-behavior-downlink_in] remark service-vlan-id 200
[DeviceC-behavior-downlink_in] quit
```

④ 配置端口 GigabitEthernet 2/0/1 入方向的策略 downlink_in，将入方向的流分类和流行为进行绑定。

```
[DeviceC] qos policy downlink_in
[DeviceC-qospolicy-downlink_in] classifier downlink_in behavior downlink_in
[DeviceC-qospolicy-downlink_in] quit
```

⑤ 配置端口 GigabitEthernet 2/0/1 出方向对报文的分类规则 downlink_out，匹配内层 VLAN 为 30、外层 VLAN 为 200 的报文。

```
[DeviceC] traffic classifier downlink_out
[DeviceC-classifier-downlink_out] if-match customer-vlan-id 30
[DeviceC-classifier-downlink_out] if-match service-vlan-id 200
[DeviceC-classifier-downlink_out] quit
```

⑥ 配置端口 GigabitEthernet 2/0/1 出方向对报文的流行为 downlink_out，将报文的内层 VLAN 替换为 10，外层 VLAN 替换为 100。

```
[DeviceC] traffic behavior downlink_out
[DeviceC-behavior-downlink_out] remark customer-vlan-id 10
[DeviceC-behavior-downlink_out] remark service-vlan-id 100
[DeviceC-behavior-downlink_out] quit
```

⑦ 配置端口 GigabitEthernet 2/0/1 出方向的策略 downlink_out，将出方向的流分类和流行为进行绑定。

```
[DeviceC] qos policy downlink_out
[DeviceC-qospolicy-downlink_out] classifier downlink_out behavior downlink_out
[DeviceC-qospolicy-downlink_out] quit
```

⑧ 配置端口 GigabitEthernet 2/0/2 出方向对报文的分类规则 uplink_out，匹配内层 VLAN 为 10、外层 VLAN 为 200 的报文。

```
[DeviceC] traffic classifier uplink_out
[DeviceC-classifier-uplink_out] if-match customer-vlan-id 10
[DeviceC-classifier-uplink_out] if-match service-vlan-id 200
[DeviceC-classifier-uplink_out] quit
```

⑨ 配置端口 GigabitEthernet 2/0/2 出方向对报文的流行为 uplink_out，将报文的内层 VLAN 替换为 30。

```
[DeviceC] traffic behavior uplink_out
[DeviceC-behavior-uplink_out] remark customer-vlan-id 30
[DeviceC-behavior-uplink_out] quit
```

⑩ 配置端口 GigabitEthernet 2/0/2 出方向的策略 uplink_out，将出方向的流分类和流行为进行绑定。

```
[DeviceC] qos policy uplink_out
[DeviceC-qospolicy-uplink_out] classifier uplink_out behavior uplink_out
[DeviceC-qospolicy-uplink_out] quit
```

⑪ 将策略应用到端口 GigabitEthernet 2/0/1 和 GigabitEthernet 2/0/2。

```
[DeviceC] interface GigabitEthernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] port link-type trunk
[DeviceB-GigabitEthernet2/0/1] port trunk permit vlan 200
[DeviceC-GigabitEthernet2/0/1] qos apply policy downlink_in inbound
[DeviceC-GigabitEthernet2/0/1] qos apply policy downlink_out outbound
[DeviceC-GigabitEthernet2/0/1] quit
[DeviceC] interface gigabitethernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] port link-type trunk
[DeviceB-GigabitEthernet2/0/2] port trunk permit vlan 200
[DeviceC-GigabitEthernet2/0/2] qos apply policy uplink_out outbound
[DeviceC-GigabitEthernet2/0/2] quit
```

(4) 配置 Device D。

① 创建 VLAN 200。

```
<DeviceD> system-view
[DeviceD] vlan 200
[DeviceD-vlan200] quit
```

② 配置上行策略，为 VLAN 30 的报文添加 VLAN ID 为 200 的外层 VLAN Tag。

```
[DeviceD] traffic classifier nest
[DeviceD-classifier-nest] if-match customer-vlan-id 30
[DeviceD-classifier-nest] quit
[DeviceD] traffic behavior nest
[DeviceD-behavior-nest] nest top-most vlan-id 200
[DeviceD-behavior-nest] quit
[DeviceD] qos policy nest
```

```
[DeviceD-qospolicy-nest] classifier nest behavior nest
[DeviceD-qospolicy-nest] quit
```

③ 配置端口 GigabitEthernet 2/0/1 为 Trunk 端口，且允许 VLAN 200 的报文携带 VLAN 标签通过。

```
[DeviceD] interface GigabitEthernet 2/0/1
[DeviceD-GigabitEthernet2/0/1] port link-type trunk
[DeviceD-GigabitEthernet2/0/1] port trunk permit vlan 200
```

④ 配置端口 GigabitEthernet 2/0/2 为 Hybrid 端口，且允许 VLAN 200 的报文不带 VLAN 标签通过。

```
[DeviceD] interface GigabitEthernet 2/0/2
[DeviceD-GigabitEthernet2/0/2] port link-type hybrid
[DeviceD-GigabitEthernet2/0/2] port hybrid vlan 200 untagged
```

⑤ 开启端口 GigabitEthernet 2/0/2 的基本 QinQ 功能。

```
[DeviceD-GigabitEthernet2/0/2] qinq enable
```

⑥ 在端口 GigabitEthernet 2/0/2 的入方向应用上行策略 nest。

```
[DeviceD-GigabitEthernet2/0/2] qos apply policy nest inbound
[DeviceD-GigabitEthernet2/0/2] quit
```

提示：通过配置下行端口的上行策略，来修改 SVLAN 的值。
通过配置下行端口的下行策略，来将 SVLAN 和 CVLAN 的值都修改为原来的值。
通过配置上行端口的上行策略，来修改 CVLAN 的值。

第5章

生成树协议配置指导

5.1 RSTP 典型配置指导

RSTP(Rapid Spanning Tree Protocol,快速生成树协议)是 STP 协议的优化版。其"快速"体现在,当一个端口被选为根端口和指定端口后,其进入转发状态的延时在某种条件下大大缩短,从而缩短了网络最终达到拓扑稳定所需要的时间。

1. 背景

基于可靠性的考虑,局域网中通常会存在冗余链路。为了避免形成广播风暴,消除路径环路,并且在主用链路中断时可以将冗余链路自动切换为转发状态,恢复网络的连通性,M 公司要求在整个局域网中部署生成树协议。

2. 组网图

图 5-1 所示为 RSTP 典型配置组网图。

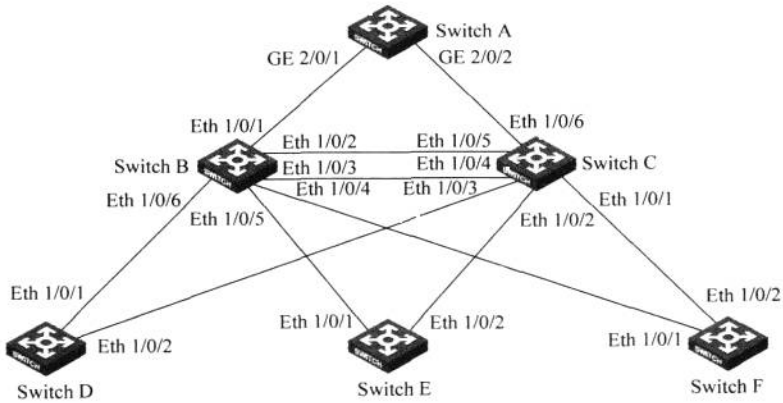


图 5-1 RSTP 典型配置组网图

3. 配置需求

(1) Switch A 为核心层交换机,作为树根。

(2) Switch B、Switch C 为汇聚层交换机。

① Switch C 为 Switch B 的备份交换机,当 Switch B 出现故障时,由 Switch C 转发数据。

② Switch C 和 Switch B 之间通过两条链路相连，保证在一条链路发生故障的时候，另一条可以正常工作。

(3) Switch D、Switch E、Switch F 为接入层交换机。

① Switch D、Switch E、Switch F 下面直接挂接用户的计算机。

② Switch D、Switch E、Switch F 分别通过一个端口与 Switch C、Switch B 相连。

后面的配置步骤中仅列出了 RSTP 相关的配置，由于 Switch D、Switch E 和 Switch F 的 RSTP 配置基本一致，本例只列出了 Switch D 上面的 RSTP 配置。

4. 配置过程和解释

(1) Switch A 的配置。

① 设备启动 RSTP。

```
<Sysname> system-view
[Sysname] stp enable
[Sysname] stp mode rstp
```

② 设备 RSTP 启动后，各个端口的 RSTP 默认为启动状态，在不参与 RSTP 计算的端口上关闭 RSTP，注意不要将参与 RSTP 计算的端口 RSTP 关闭（此处仅列举出 GigabitEthernet 2/0/4）。

```
[Sysname] interface GigabitEthernet 2/0/4
[Sysname-GigabitEthernet2/0/4] stp disable
```

③ 配置 Switch A 为树根，有两种方法。

a. 将 Switch A 的 Bridge 优先级配置为 0。

```
[Sysname] stp priority 0
```

b. 直接使用命令将 Switch A 指定为树根。

```
[Sysname] stp root primary
```

④ 在与 Swtich B、Swtich C 相连的指定端口上启动根保护功能。

```
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp root-protection
[Sysname-GigabitEthernet2/0/1] quit
[Sysname] interface GigabitEthernet 2/0/2
[Sysname-GigabitEthernet2/0/2] stp root-protection
[Sysname-GigabitEthernet2/0/2] quit
```

⑤ 启动 Switch A 的 TC 防攻击功能。

```
[Sysname] stp tc-protection enable
```

(2) Switch B 的配置。

① 设备启动 RSTP。

```
<Sysname> system-view
[Sysname] stp enable
[Sysname] stp mode rstp
```

② 设备 RSTP 启动后，各个端口的 RSTP 默认为启动状态，在不参与 RSTP 计算的端口上关闭 RSTP，注意不要将参与 RSTP 计算的端口 RSTP 关闭（此处仅列举出 Ethernet 1/0/8）。

```
[Sysname] interface Ethernet 1/0/8
[Sysname-Ethernet1/0/8] stp disable
[Sysname-Ethernet1/0/8] quit
```

③ 配置 Switch B 的 Bridge 优先级配置为 4096。

```
[Sysname] stp priority 4096
```

④ 在各个指定端口上启动根保护功能。

```
[Sysname] interface Ethernet 1/0/4
[Sysname-Ethernet1/0/4] stp root-protection
[Sysname-Ethernet1/0/4] quit
[Sysname] interface Ethernet 1/0/5
[Sysname-Ethernet1/0/5] stp root-protection
[Sysname-Ethernet1/0/5] quit
[Sysname] interface Ethernet 1/0/6
[Sysname-Ethernet1/0/6] stp root-protection
[Sysname-Ethernet1/0/6] quit
```

⑤ RSTP 的工作模式、时间参数、端口上的参数都采用默认值。

(3) Switch C 的配置。

① 设备启动 RSTP。

```
<Sysname> system-view
[Sysname] stp enable
[Sysname] stp mode rstp
```

② 设备 RSTP 启动后，各个端口的 RSTP 默认为启动状态，在不参与 RSTP 计算的端口上关闭 RSTP，注意不要将参与 RSTP 计算的端口 RSTP 关闭（此处仅列举出 Ethernet 1/0/8）。

```
[Sysname] interface Ethernet 1/0/8
[Sysname-Ethernet1/0/8] stp disable
[Sysname-Ethernet1/0/8] quit
```

③ 配置 Switch C 的 Bridge 优先级配置为 8192，充当 Switch B 的备份交换机。

```
[Sysname] stp priority 8192
```

④ 在各个指定端口上启动根保护功能。

```
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] stp root-protection
[Sysname-Ethernet1/0/1] quit
[Sysname] interface Ethernet 1/0/2
[Sysname-Ethernet1/0/2] stp root-protection
```

```
[Sysname-Ethernet1/0/2] quit
[Sysname] interface Ethernet 1/0/3
[Sysname-Ethernet1/0/3] stp root-protection
[Sysname-Ethernet1/0/3] quit
```

⑤ RSTP 的工作模式、时间参数、端口上的参数都采用默认值。

(4) Switch D 的配置。

① 设备启动 RSTP。

```
<Sysname> system-view
[Sysname] stp enable
[Sysname] stp mode rstp
```

② 设备 RSTP 启动后，各个端口的 RSTP 默认为启动状态，在不参与 RSTP 计算的端口上关闭 RSTP，注意不要将参与 RSTP 计算的端口 RSTP 关闭（此处仅列举出 Ethernet 1/0/3）。

```
[Sysname] interface Ethernet 1/0/3
[Sysname-Ethernet1/0/3] stp disable
```

③ 将直接与用户相连的端口配置为边缘端口，并使能 BPDU 保护功能（此处仅列举出 Ethernet 1/0/3）。

```
[Sysname-Ethernet1/0/3] stp edged-port enable
[Sysname-Ethernet1/0/3] quit
[Sysname] stp bpdu-protection
```

④ RSTP 的工作模式、时间参数、端口的其他参数都采用默认值。

⑤ Swicth E 和 Swicth F 的配置同 Swicth D。

提示：stp mode 命令用于设置交换机的 STP 工作模式：STP、RSTP 或 MSTP，默认工作于 MSTP 模式。

5.2 MSTP 典型配置指导

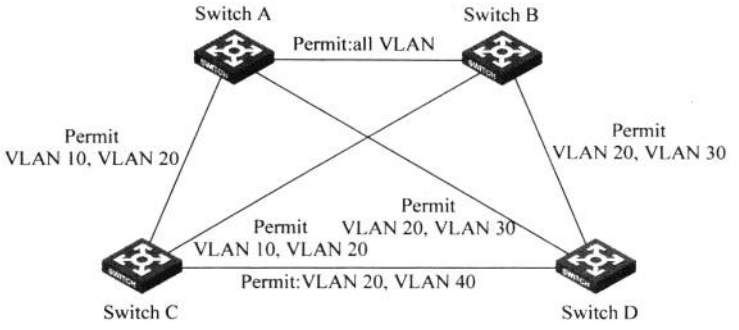
MSTP（Multiple Spanning Tree Protocol，多生成树协议）功能允许用户将一个或者多个 VLAN 映射到 MSTI（Multiple Spanning Tree Instance，多生成树实例）上，但每个 VLAN 只允许对应一个 MSTI，使指定 VLAN 的报文只在建立了映射关系的实例内发送，以节省通信开销和减少资源占用率。

1. 背景

RSTP 可以快速收敛，但是和 STP 一样存在以下缺陷：局域网内所有网桥共享一棵生成树，不能按 VLAN 阻塞冗余链路，所有 VLAN 的报文都沿着一棵生成树进行转发。MSTP 可以弥补 STP 和 RSTP 的缺陷，既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径转发，从而为冗余链路提供了更好的负载分担机制。M 公司 IT 维护部门要求在局域网中部署 MSTP 替代 RSTP。

2. 组网图

图 5-2 所示为 MSTP 典型配置组网图。



VLAN	所属实例
VLAN 10	MSTI 1
VLAN 20	MSTI 0
VLAN 30	MSTI 3
VLAN 40	MSTI 4

图 5-2 MSTP 典型配置组网图

3. 配置需求

配置 MSTP，使图 5-2 中不同 VLAN 的报文按照不同的生成树实例转发。具体配置如下：

(1) 网络中所有交换机属于同一个 MST 域。

(2) VLAN 10 的报文沿着实例 1 转发，VLAN 30 沿着实例 3 转发，VLAN 40 沿着实例 4 转发，VLAN 20 沿着实例 0 转发。

图 5-2 中 Switch A 和 Switch B 为汇聚层设备，Switch C 和 Switch D 为接入层设备。VLAN 10、VLAN 30 在汇聚层设备终结，VLAN 40 在接入层设备终结，因此可以配置实例 1 和实例 3 的树根分别为 Switch A 和 Switch B，实例 4 的树根为 Switch C。

4. 配置过程和解释

(1) 配置 Switch A。

① 进入 MST 域视图。

```
<Sysname> system-view
[Sysname] stp region-configuration
```

② 配置 MST 域的域名、VLAN 映射关系和修订级别。

```
[Sysname-mst-region] region-name example
[Sysname-mst-region] instance 1 vlan 10
[Sysname-mst-region] instance 3 vlan 30
[Sysname-mst-region] instance 4 vlan 40
[Sysname-mst-region] revision-level 0
```

③ 手动激活 MST 域的配置。

```
[Sysname-mst-region] active region-configuration
```

④ 定义 Switch A 为实例 1 的树根。

```
[Sysname] stp instance 1 root primary
```

(2) 配置 Switch B。

① 进入 MST 域视图。

```
<Sysname> system-view
[Sysname] stp region-configuration
```

② 配置 MST 域的域名、VLAN 映射关系和修订级别。

```
[Sysname-mst-region] region-name example
[Sysname-mst-region] instance 1 vlan 10
[Sysname-mst-region] instance 3 vlan 30
[Sysname-mst-region] instance 4 vlan 40
[Sysname-mst-region] revision-level 0
```

③ 手动激活 MST 域的配置。

```
[Sysname-mst-region] active region-configuration
```

④ 定义 Switch B 为实例 3 的树根。

```
[Sysname] stp instance 3 root primary
```

(3) 配置 Switch C。

① 进入 MST 域视图,并配置 MST 域名、VLAN 映射关系和修订级别。

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] region-name example
[Sysname-mst-region] instance 1 vlan 10
[Sysname-mst-region] instance 3 vlan 30
[Sysname-mst-region] instance 4 vlan 40
[Sysname-mst-region] revision-level 0
```

② 手动激活 MST 域的配置。

```
[Sysname-mst-region] active region-configuration
```

③ 定义 Switch C 为实例 4 的树根。

```
[Sysname] stp instance 4 root primary
```

(4) 配置 Switch D。

① 进入 MST 域视图。

```
<Sysname> system-view
[Sysname] stp region-configuration
```

② 配置 MST 域名、VLAN 映射关系和修订级别。

```
[Sysname-mst-region] region-name example
[Sysname-mst-region] instance 1 vlan 10
```

```
[Sysname-mst-region] instance 3 vlan 30
[Sysname-mst-region] instance 4 vlan 40
[Sysname-mst-region] revision-level 0
```

③ 手动激活 MST 域的配置。

```
[Sysname-mst-region] active region-configuration
```

提示：不能同时在端口上配置 MSTP 和以下功能：业务环回、RRPP、Smart Link 和 STP 协议的 BPDU Tunnel 功能。

在多台使能了 MSTP 协议的设备上，只有当选择因子(默认为 0，不可配)、域名、VLAN 映射表和 MSTP 修订级别的配置都相同，且这些设备之间有链路相通时，它们才能属于同一个 MST 域。

第6章

堆叠技术配置指导

6.1 集群技术典型配置指导

集群(Cluster)功能通过 HGMP V2(Huawei Group Management Protocol,华为组管理协议)实现。使用 HGMP V2 功能,网络管理员可以通过一个主交换机的公网 IP 地址,实现对多个交换机的管理。主交换机称为管理设备,其他被管理的交换机称为成员设备。成员设备一般不设置公网 IP 地址,通过管理设备重定向来实现对成员设备的管理和维护。管理设备和成员设备组成了一个“集群”。

1. 背景

W 运营商在小区宽带接入中使用了大量的 H3C 交换机。为了管理维护方便,W 运营商打算对这些交换机进行统一管理。但是,W 运营商面临着公网 IP 不足的问题。所以,经过综合考虑,W 运营商决定使用 HGMP V2 对交换机进行统一管理。

使用 HGMP 功能的另一个好处可以节省大量的重复配置时间,降低配置复杂程度。

2. 组网图

如图 6-1 所示为 HGMP 典型配置组网图。

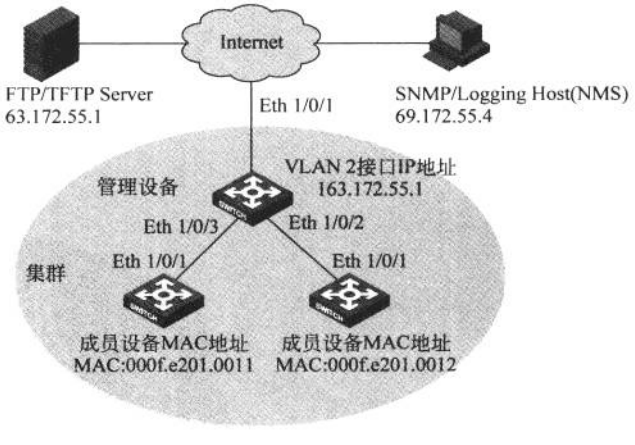


图 6-1 HGMP 典型配置组网图

3. 配置需求

(1) 如图 6-1 所示,3 台交换机构成一个集群,其中 1 台为管理设备,其他两台为成员设备。

(2) 管理设备通过端口 Ethernet 1/0/2 和端口 Ethernet 1/0/3 下挂两台成员设备,通过端口 Ethernet 1/0/1 接入到外部网络;Ethernet 1/0/1 属于 VLAN 2,VLAN 2 的接口 IP 地址为 163.172.55.1。

(3) 整个集群使用相同的 FTP Server、TFTP Server,IP 地址为 63.172.55.1。

(4) 网管工作站及日志主机的 IP 地址为 69.172.55.4。

4. 配置过程和解释

(1) 配置成员设备(以 1 台成员设备为例)。

① 启动设备上的 NDP 和端口 Ethernet 1/0/1 上的 NDP。

```
<Sysname> system-view
[Sysname] ndp enable
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] ndp enable
[Sysname-Ethernet1/0/1] quit
```

② 启动设备上的 NTDP 和端口 Ethernet 1/0/1 上的 NTDP。

```
[Sysname] ntdp enable
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] ntdp enable
[Sysname-Ethernet1/0/1] quit
```

③ 启动集群功能。

```
[Sysname] cluster enable
```

(2) 配置管理设备。

① 启动设备上的全局 NDP 和端口 Ethernet 1/0/2、Ethernet 1/0/3 上的 NDP。

```
<Sysname> system-view
[Sysname] ndp enable
[Sysname] interface Ethernet 1/0/2
[Sysname-Ethernet1/0/2] ndp enable
[Sysname-Ethernet1/0/2] quit
[Sysname] interface Ethernet 1/0/3
[Sysname-Ethernet1/0/3] ndp enable
[Sysname-Ethernet1/0/3] quit
```

② 配置 NDP 信息的有效保留时间为 200s。

```
[Sysname] ndp timer aging 200
```

③ 配置 NDP 报文发送的时间间隔为 70s。

```
[Sysname] ndp timer hello 70
```

④ 启动设备上的 NTDP 和端口 Ethernet 1/0/2、Ethernet 1/0/3 上的 NTDP。

```
[Sysname] ntdp enable
[Sysname] interface Ethernet 1/0/2
[Sysname-Ethernet1/0/2] ntdp enable
[Sysname-Ethernet1/0/2] quit
[Sysname] interface Ethernet 1/0/3
[Sysname-Ethernet1/0/3] ntdp enable
[Sysname-Ethernet1/0/3] quit
```

⑤ 配置拓扑收集范围为 2 跳。

```
[Sysname] ntdp hop 2
```

⑥ 配置被收集设备转发拓扑收集请求的延迟时间为 150ms。

```
[Sysname] ntdp timer hop-delay 150
```

⑦ 配置被收集设备的端口转发拓扑收集请求的延迟时间为 15ms。

```
[Sysname] ntdp timer port-delay 15
```

⑧ 配置定时拓扑收集的时间间隔为 3min。

```
[Sysname] ntdp timer 3
```

⑨ 启动集群功能。

```
[Sysname] cluster enable
```

⑩ 进入集群视图。

```
[Sysname] cluster
[Sysname-cluster]
```

⑪ 配置集群内部使用的 IP 地址池，起始地址为 172.16.0.1，有 8 个地址。

```
[Sysname-cluster] ip-pool 172.16.0.1 255.255.255.248
```

⑫ 配置集群名字，建立集群。

```
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster]
```

⑬ 将下挂的两台交换机加入集群中。

```
[aaa_0.Sysname-cluster] add-member 1 mac-address 000f-e201-0011
[aaa_0.Sysname-cluster] add-member 17 mac-address 000f-e201-0012
```

⑭ 配置成员设备信息的保留时间为 100s。

```
[aaa_0.Sysname-cluster] holdtime 100
```

⑮ 配置握手报文定时发送的时间间隔为 10s。

```
[aaa_0.Sysname-cluster] timer 10
```

⑯ 配置集群内部公用的 FTP Server、TFTP Server、Logging Host 及 SNMP Host。

```
[aaa_0.Sysname-cluster] ftp-server 63.172.55.1
[aaa_0.Sysname-cluster] tftp-server 63.172.55.1
[aaa_0.Sysname-cluster] logging-host 69.172.55.4
[aaa_0.Sysname-cluster] snmp-host 69.172.55.4
```

(3) 集群成员上的操作。管理设备将下挂的设备加入集群以后，在成员设备上做下列操作。

① 连接到集群公用的远程 FTP 服务器。

```
<aaa_1.Sysname> ftp cluster
```

② 成员设备从集群内部公用的 TFTP 服务器下载文件 aaa.txt 到本地。

```
<aaa_1.Sysname> tftp cluster get aaa.txt
```

③ 成员设备上载文件 bbb.txt 到集群内部公用的 TFTP 服务器。

```
<aaa_1.Sysname> tftp cluster put bbb.txt
```

6.2 IRF 技术典型配置指导

6.2.1 IRF 环形堆叠基本配置

IRF(Intelligent Resilient Framework，智能弹性架构)是 H3C 自主研发的软件虚拟化技术。它的核心思想是将多台设备通过 IRF 物理端口连接在一起，进行必要的配置后，虚拟化成一台“分布式设备”。使用这种虚拟化技术可以实现多台设备的协同工作、统一管理和不间断维护。

IRF 的优点如下：

(1) 简化管理。

(2) 高可靠性。

(3) 强大的网络扩展能力。

IRF 的连接拓扑有两种：链形连接和环形连接。其特点如下：

(1) 链形连接对成员设备的物理位置要求低，主要用于成员设备物理位置分散的组网。

(2) 环形连接比链形连接更可靠。因为当链形连接中出现链路故障时，会引起 IRF 分裂；而环形连接中某条链路故障时，会形成链形连接，IRF 的业务不会受到影响。

1. 背景

T 公司新建立了一个大型数据中心，使用了大量的 H3C 公司千兆位与万兆位交换机。因数据中心所承载的业务非常重要，所以对交换网络的可靠性和可管理性都提出了很高的要求。经过一段时间的前期调研与测试，T 公司决定使用 H3C 独有的 IRF 技术来增强交换网络的可靠性，并简化网络管理。

2. 组网图

如图 6-2 所示为 IRF 环形堆叠基本配置组网图。

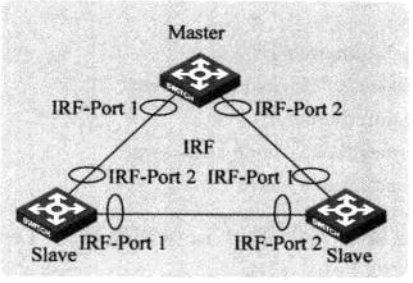


图 6-2 IRF 环形堆叠基本配置组网图

3. 配置需求

如图 6-2 所示,3 台交换机组成 IRF。其中 1 台作为 Master 设备,另外 2 台作为 Slave 设备。

4. 配置过程和解释

(1) 配置设备编号。

① Device A 保留默认编号为 1,不需要进行配置。

② 在 Device B 上将设备的成员编号修改为 2。

```
<DeviceB> system-view
[DeviceB] irf member 1 renumber 2
Warning: Renumbering the switch number may result in configuration change or loss. Continue? [Y/N]:y
[DeviceB]
```

③ 在 Device C 上将设备的成员编号修改为 3。

```
<DeviceC> system-view
[DeviceC] irf member 1 renumber 3
Warning: Renumbering the switch number may result in configuration change or loss. Continue? [Y/N]:y
[DeviceC]
```

将 3 台设备断电后,按图所示连接 IRF 链路,然后将 3 台设备通电。

(2) 配置 IRF 端口。

① 配置 Device A 的优先级为 10,以使 Device A 成为 Master。

```
<Sysname> system-view
[Sysname] irf member 1 priority 10
```

② 在 Device A 上创建设备的 IRF 端口 1,与物理端口 Ten-GigabitEthernet 1/0/25 绑定;IRF 端口 2,与物理端口 Ten-GigabitEthernet 1/0/26 绑定,并保存配置。

```
[Sysname] interface ten-gigabitethernet 1/0/25
[Sysname-Ten-GigabitEthernet1/0/25] shutdown
[Sysname] interface ten-gigabitethernet 1/0/26
[Sysname-Ten-GigabitEthernet1/0/26] shutdown
[Sysname] irf-port 1/1
```

```
[Sysname-irf-port 1/1] port group interface ten-gigabitethernet 1/0/25
[Sysname] irf-port 1/2
[Sysname-irf-port 1/2] port group interface ten-gigabitethernet 1/0/26
[Sysname-irf-port 1/2] quit
[Sysname] interface ten-gigabitethernet 1/0/25
[Sysname-Ten-GigabitEthernet1/0/25] undo shutdown
[Sysname] interface ten-gigabitethernet 1/0/26
[Sysname-Ten-GigabitEthernet1/0/26] undo shutdown
[Sysname-Ten-GigabitEthernet1/0/26] save
```

③ 在 Device B 上创建设备的 IRF 端口 1，与物理端口 Ten-GigabitEthernet 2/0/25 绑定；IRF 端口 2，与物理端口 Ten-GigabitEthernet 2/0/26 绑定，并保存配置。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 2/0/25
[Sysname-Ten-GigabitEthernet2/0/25] shutdown
[Sysname] interface ten-gigabitethernet 2/0/26
[Sysname-Ten-GigabitEthernet2/0/26] shutdown
[Sysname] irf-port 2/1
[Sysname-irf-port 2/1] port group interface ten-gigabitethernet 2/0/25
[Sysname] irf-port 2/2
[Sysname-irf-port 2/2] port group interface ten-gigabitethernet 2/0/26
[Sysname-irf-port 2/2] quit
[Sysname] interface ten-gigabitethernet 2/0/25
[Sysname-Ten-GigabitEthernet2/0/25] undo shutdown
[Sysname] interface ten-gigabitethernet 2/0/26
[Sysname-Ten-GigabitEthernet2/0/26] undo shutdown
[Sysname-Ten-GigabitEthernet2/0/26] save
```

④ 在 Device C 上创建设备的 IRF 端口 1，与物理端口 Ten-GigabitEthernet 3/0/25 绑定；IRF 端口 2，与物理端口 Ten-GigabitEthernet 3/0/26 绑定，并保存配置。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 3/0/25
[Sysname -Ten-GigabitEthernet3/0/25] shutdown
[Sysname] interface ten-gigabitethernet 3/0/26
[Sysname -Ten-GigabitEthernet3/0/26] shutdown
[Sysname] irf-port 3/1
[Sysname-irf-port 3/1] port group interface ten-gigabitethernet 3/0/25
[Sysname] irf-port 3/2
[Sysname-irf-port 3/2] port group interface ten-gigabitethernet 3/0/26
[Sysname-irf-port 3/2] quit
[Sysname] interface ten-gigabitethernet 3/0/25
[Sysname-Ten-GigabitEthernet3/0/25] undo shutdown
[Sysname] interface ten-gigabitethernet 3/0/26
[Sysname-Ten-GigabitEthernet3/0/26] undo shutdown
[Sysname-Ten-GigabitEthernet3/0/26] save
```

⑤ 激活 Device A 的 IRF 端口配置。

```
[Sysname] irf-port-configuration active
```

⑥ 激活 Device B 的 IRF 端口配置。

```
[Sysname] irf-port-configuration active
```

⑦ 激活 Device C 的 IRF 端口配置。

```
[Sysname] irf-port-configuration active
```

3 台设备间会进行 Master 竞选，竞选失败的设备将自动重启。重启完成后，IRF 形成。

⑧ 在 Device A 上查看设备的 IRF 信息。

```
[Sysname]display irf
Switch     Role     Priority     CPU-Mac
* +1       Master   10           3822-d669-1782
  2        Slave    1            3822-d669-42db
  3        Slave    1            3822-d669-12c3
--------------------------------------------------
* indicates the device is the master.
+ indicates the device through which the user logs in.
The Bridge MAC of the IRF is: 3822-d669-1781
Auto upgrade                  : yes
Mac persistent                : 6 min
Domain ID                     : 0
```

⑨ 在 Master 上重定向到编号为 2 的 Device B。

```
<Sysname> system-view
[Sysname] irf switch-to 2
```

注意：IRF 编号一旦曾经更改，则一直有效，擦除配置文件也不会丢失。

6.2.2 IRF 典型配置指导(LACP MAD 检测方式)

IRF 链路故障会导致一个 IRF 变成两个新的 IRF。这两个 IRF 拥有相同的 IP 地址等三层配置，会引起地址冲突，导致故障在网络中扩大。为了提高系统的可用性，当 IRF 分裂时就需要一种机制，能够检测出网络中同时存在多个 IRF，并进行相应的处理以尽量降低 IRF 分裂对业务的影响。MAD(Multi-Active Detection，多 Active 检测)就是这样一种检测和处理机制。

IRF 支持的常见 MAD 检测方式有 LACP MAD 检测和 BFD MAD 检测。LACP MAD 检测用于基于 LACP 的组网检测需求，需要支持 LACP 协议扩展功能的 H3C 设备作为中间设备。

1. 背景

T 公司部署了 IRF 后，发现在 IRF 链路故障情况下，网络中会产生大量的地址冲突报错信息，并且网络性能急剧下降。为解决以上问题，T 公司决定配置使用 IRF 的多 Active 检测。

2. 组网图

如图 6-3 所示为 IRF 典型配置(LACP MAD 检测方式)组网图。

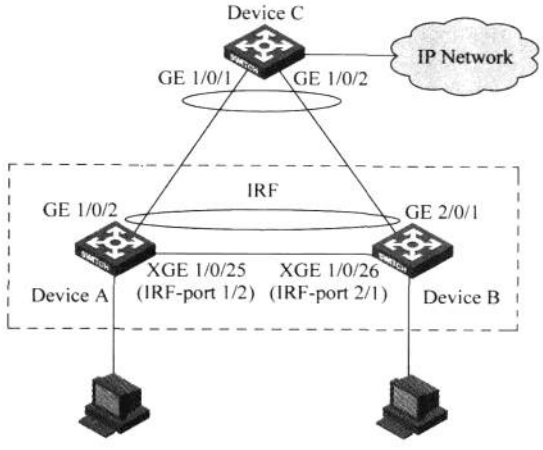


图 6-3 IRF 典型配置(LACP MAD 检测方式)组网图

3. 配置需求

(1) 如图 6-3 所示,Device A 和 Device B 上配置 IRF 功能,使之成为 IRF 堆叠。

(2) 为了防止万一 IRF 链路故障导致 IRF 分裂,网络中存在两个配置冲突的 IRF,需要启用 MAD 检测功能。因为接入层设备较多,故采用 LACP MAD 检测。

4. 配置过程和解释

(1) 配置设备编号。

① Device A 保留默认编号为 1,不需要进行配置。

② 在 Device B 上将设备的成员编号修改为 2。

```
<DeviceB> system-view
[DeviceB] irf member 1 renumber 2
Warning: Renumbering the switch number may result in configuration change or loss. Continue? [Y/N]:y
[DeviceB]
```

将两台设备断电后,按图 6-3 所示连接 IRF 链路,然后将两台设备通电。

(2) 配置 IRF 端口。

① 在 Device A 上创建设备的 IRF 端口 2,与物理端口 Ten-GigabitEthernet 1/0/25 绑定,并保存配置。

```
<DeviceA> system-view
[DeviceA] interface ten-gigabitethernet 1/0/25
[DeviceA-Ten-GigabitEthernet1/0/25] shutdown
[DeviceA] irf-port 1/2
[DeviceA-irf-port 1/2] port group interface ten-gigabitethernet 1/0/25
[DeviceA-irf-port 1/2] quit
[DeviceA] interface ten-gigabitethernet 1/0/25
[DeviceA-Ten-GigabitEthernet1/0/25] undo shutdown
[DeviceA-Ten-GigabitEthernet1/0/25] save
```

② 在 Device B 上创建设备的 IRF 端口 1，与物理端口 Ten-GigabitEthernet 2/0/26 绑定，并保存配置。

```
<DeviceB> system-view
[DeviceB] interface ten-gigabitethernet 2/0/26
[DeviceB-Ten-GigabitEthernet2/0/26] shutdown
[DeviceB] irf-port 2/1
[DeviceB-irf-port 2/1] port group interface ten-gigabitethernet 2/0/26
[DeviceB-irf-port 2/1] quit
[DeviceB] interface ten-gigabitethernet 2/0/26
[DeviceB-Ten-GigabitEthernet2/0/26] undo shutdown
[DeviceB-Ten-GigabitEthernet2/0/26] save
```

③ 激活 Device A 的 IRF 端口配置。

```
[DeviceA-Ten-GigabitEthernet1/0/25] quit
[DeviceA] irf-port-configuration active
```

④ 激活 Device B 的 IRF 端口配置。

```
[DeviceB-Ten-GigabitEthernet2/0/26] quit
[DeviceB] irf-port-configuration active
```

两台设备间会进行 Master 竞选，竞选失败的一方将自动重启。重启完成后，IRF 形成，系统名称统一为 Device A。

(3) 配置 LACP MAD 检测。

① 创建一个动态聚合端口，并使能 LACP MAD 检测功能。

```
<DeviceA> system-view
[DeviceA] interface bridge-aggregation 2
[DeviceA-Bridge-Aggregation2] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation2] mad enable
[DeviceA-Bridge-Aggregation2] quit
```

② 在聚合端口中添加成员端口 GigabitEthernet 1/0/1 和 GigabitEthernet 2/0/1，专用于两台 IRF 成员设备与中间设备进行 LACP MAD 检测。

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 2
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface GigabitEthernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] port link-aggregation group 2
```

(4) 中间设备 Device C 的配置。Device C 作为一台中间设备需要支持 LACP 功能，用来转发、处理 LACP 协议报文，协助 Device A 和 Device B 进行多 Active 检测。从节约成本的角度考虑，使用一台支持 LACP 功能的交换机即可。

① 创建一个动态聚合端口。

```
<DeviceC> system-view
[DeviceC] interface bridge-aggregation 2
[DeviceC-Bridge-Aggregation2] link-aggregation mode dynamic
```

```
[DeviceC-Bridge-Aggregation2] quit
```

② 在聚合端口中添加成员端口 GigabitEthernet 1/0/1 和 GigabitEthernet 1/0/2，用于进行 LACP MAD 检测。

```
[DeviceC] interface GigabitEthernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-aggregation group 2
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface GigabitEthernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port link-aggregation group 2
```

按组网图 6-3 所示连接 LACP MAD 链路。

6.2.3 IRF 典型配置指导(BFD MAD 检测方式)

BFD MAD 检测是通过 BFD 协议来实现，IRF 中的成员设备每两台之间都要建立 BFD MAD 检测链路，每台设备都需要为 BFD MAD 检测预留专门的检测 VLAN。

1. 背景

在接入层部署 LACP MAD 检测方式的 IRF 后，按照规划，T 公司也要在汇聚层的交换机上部署 IRF。因汇聚层设备可靠性要求较接入层要高，所以 T 公司决定采用 BFD MAD 检测方式来对 IRF 进行多 Active 检测。

2. 组网图

图 6-4 所示为 IRF 典型配置(BFD MAD 检测方式)组网图。

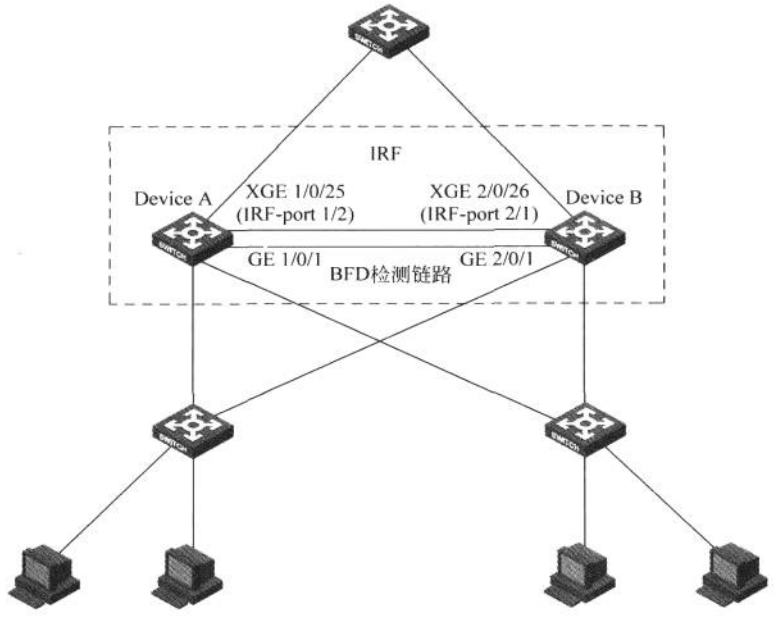


图 6-4 IRF 典型配置(BFD MAD 检测方式)组网图

3. 配置需求

(1) 如图 6-4 所示，Device A 和 Device B 处于局域网的汇聚层，需要组成 IRF。

(2) 为了防止IRF链路故障导致IRF分裂,网络中存在两个配置冲突的IRF,需要启用MAD检测功能。成员设备比较少,故采用BFD MAD检测方式来监测IRF的状态。

4. 配置过程和解释

(1) 配置设备编号。

① Device A保留默认编号为1,不需要进行配置。

② 在Device B上将设备的成员编号修改为2。

```
<DeviceB> system-view
[DeviceB] irf member 1 renumber 2
Warning: Renumbering the switch number may result in configuration change or loss. Continue? [Y/N]:y
[DeviceB]
```

将两台设备断电后,按图6-4所示连接IRF链路,然后将两台设备通电。

(2) 配置IRF端口。

① 在Device A上创建设备的IRF端口2,与物理端口Ten-GigabitEthernet 1/0/25绑定,并保存配置。

```
<DeviceA> system-view
[DeviceA] interface ten-gigabitethernet 1/0/25
[DeviceA-Ten-GigabitEthernet1/0/25] shutdown
[DeviceA] irf-port 1/2
[DeviceA-irf-port 1/2] port group interface ten-gigabitethernet 1/0/25
[DeviceA-irf-port 1/2] quit
[DeviceA] interface ten-gigabitethernet 1/0/25
[DeviceA-Ten-GigabitEthernet1/0/25] undo shutdown
[DeviceA-Ten-GigabitEthernet1/0/25] save
```

② 在Device B上创建设备的IRF端口1,与物理端口Ten-GigabitEthernet 2/0/26绑定,并保存配置。

```
<DeviceB> system-view
[DeviceB] interface ten-gigabitethernet 2/0/26
[DeviceB-Ten-GigabitEthernet2/0/26] shutdown
[DeviceB] irf-port 2/1
[DeviceB-irf-port 2/1] port group interface ten-gigabitethernet 2/0/26
[DeviceB-irf-port 2/1] quit
[DeviceB] interface ten-gigabitethernet 2/0/26
[DeviceB-Ten-GigabitEthernet2/0/26] undo shutdown
[DeviceB-Ten-GigabitEthernet2/0/26] save
```

③ 激活Device A的IRF端口配置。

```
[DeviceA-Ten-GigabitEthernet1/0/25] quit
[DeviceA] irf-port-configuration active
```

④ 激活Device B的IRF端口配置。

```
[DeviceB-Ten-GigabitEthernet2/0/26] quit
[DeviceB] irf-port-configuration active
```

两台设备间将会进行 Master 竞选，竞选失败的一方将自动重启。重启完成后，IRF 形成，系统名称统一为 Device A。

(3) 配置 BFD MAD 检测。

① 创建 VLAN 3，并将 Device A 上的端口 GigabitEthernet 1/0/1 和 Device B 上的端口 GigabitEthernet 2/0/1 加入 VLAN 中。

```
<DeviceA> system-view
[DeviceA] vlan 3
[DeviceA-vlan3] port GigabitEthernet 1/0/1 GigabitEthernet 2/0/1
[DeviceA-vlan3] quit
```

② 创建 VLAN 接口 3，并配置 MAD IP 地址。

```
[DeviceA] interface vlan-interface 3
[DeviceA-Vlan-interface3] mad bfd enable
[DeviceA-Vlan-interface3] mad ip address 192.168.2.1 24 member 1
[DeviceA-Vlan-interface3] mad ip address 192.168.2.2 24 member 2
[DeviceA-Vlan-interface3] quit
```

按组网图 6-4 所示连接 BFD MAD 链路。

③ 因为 BFD MAD 和生成树功能互斥，所以在 GigabitEthernet 1/0/1 和 GigabitEthernet 2/0/1 上关闭生成树协议。

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet-1/0/1] undo stp enable
[Sysname-GigabitEthernet-1/0/1] quit
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet-2/0/1] undo stp enable
```

第7章

三层技术——IP业务配置指导

7.1 IP地址与IP性能典型配置指导

7.1.1 IP地址典型配置指导

设备的每个接口可以配置多个IP地址，其中一个为主IP地址，其余为从IP地址。一般情况下，一个接口只需配置一个主IP地址，但在有些特殊情况下需要配置从IP地址。

1. 背景

M公司的网络进行了IP地址的划分，局域网中的主机分别属于多个子网，但交换机上没有划分VLAN，所有主机均属于同一VLAN，为了使交换机与局域网中的所有主机通信，网络管理员需要对网络设备进行IP地址配置，使所有主机均能正常通信，同时也能通过交换机与外部网络通信。

2. 组网图

图7-1所示为IP地址典型配置组网图。

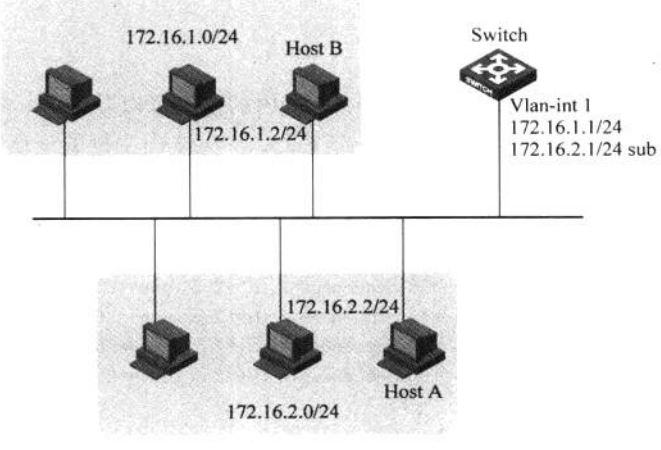


图7-1 IP地址典型配置组网图

3. 配置需求

如图7-1所示，局域网中的计算机分别属于2个子网：172.16.1.0/24和172.16.2.0/24。

要求这两个网段的主机都可以通过交换机与外部网络通信，且这两个网段中的主机能够互通信。

4. 配置过程和解释

针对上述需求，如果在 Switch 的 VLAN 接口 1 上只配置一个 IP 地址，则只有一部分主机能够通过 Switch 与外部网络通信。为了使局域网内的所有主机都能够通过 Switch 访问外部网络，需要配置 VLAN 接口 1 的从 IP 地址。为了使两个网段中的主机能够互通，两个网段中的主机都需要将 Switch 设置为网关。

(1) 配置 VLAN 接口 1 的主 IP 地址和从 IP 地址。

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 172.16.1.1 255.255.255.0
[Switch-Vlan-interface1] ip address 172.16.2.1 255.255.255.0 sub
[Switch-Vlan-interface1] return
```

172.16.1.0/24 网段中的主机上配置网关为 172.16.1.1；172.16.2.0/24 网段中的主机上配置网关为 172.16.2.1。

(2) 使用 ping 命令检测 Switch 与网络 172.16.1.0/24 内主机的连通性。

```
<Switch> ping 172.16.1.2
  PING 172.16.1.2: 56  data bytes, press Ctrl_C to break
    Reply from 172.16.1.2: bytes=56 Sequence=1 ttl=255 time=25 ms
    Reply from 172.16.1.2: bytes=56 Sequence=2 ttl=255 time=27 ms
    Reply from 172.16.1.2: bytes=56 Sequence=3 ttl=255 time=26 ms
    Reply from 172.16.1.2: bytes=56 Sequence=4 ttl=255 time=26 ms
    Reply from 172.16.1.2: bytes=56 Sequence=5 ttl=255 time=26 ms
  --- 172.16.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 25/26/27 ms
```

显示信息表示 Switch 与网络 172.16.1.0/24 内的主机可以互通。

(3) 使用 ping 命令检测 Switch 与网络 172.16.2.0/24 内主机的连通性。

```
<Switch> ping 172.16.2.2
  PING 172.16.2.2: 56  data bytes, press Ctrl_C to break
    Reply from 172.16.2.2: bytes=56 Sequence=1 ttl=255 time=25 ms
    Reply from 172.16.2.2: bytes=56 Sequence=2 ttl=255 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=3 ttl=255 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=4 ttl=255 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=5 ttl=255 time=26 ms
  --- 172.16.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 25/25/26 ms
```

显示信息表示 Switch 与网络 172.16.2.0/24 内的主机可以互通。

(4) 使用 ping 命令检测网络 172.16.1.0/24 和网络 172.16.2.0/24 内主机的连通性。在 Host A 上可以 ping 通 Host B。

提示：一个接口只能有一个主 IP 地址。新配置的主 IP 地址将覆盖原有主 IP 地址。

当接口被配置为通过 BOOTP、DHCP 方式获取 IP 地址后，则不能再给该接口配置从 IP 地址。

同一接口的主、从 IP 地址可以在同一网段，但不同接口之间的 IP 地址不可以在同一网段。

7.1.2 IP 性能典型配置指导

定向广播报文是指发送给特定网络的广播报文。该报文的目的 IP 地址中网络号码字段为特定网络的网络号，主机号码字段为 1。默认情况下，交换机丢弃定向广播报文，设备需要开启定向广播报文功能后才会转发定向广播报文。

WOL 功能除了交换机使能定向广播功能，PC、电源等硬件也需要支持 WOL 功能。

1. 背景

M 公司的网络已经连接上了 Internet，IT 维护部门提供了远程唤醒 Wake On LAN (WOL)功能。通过远程控制软件，公司员工可以方便地通过 Internet 控制自己的主机，网络管理员需要在网络设备上配置定向广播功能，允许交换机接收并转发定向广播报文。

2. 组网图

图 7-2 所示为配置收发定向广播报文组网图。

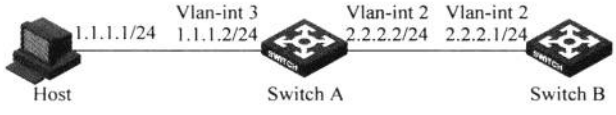


图 7-2 配置收发定向广播报文组网图

3. 配置需求

如图 7-2 所示，Host 的接口和 Switch A 的 VLAN 接口 3 处于同一个网段(1.1.1.0/24)，Switch A 的 VLAN 接口 2 和 Switch B 的 VLAN 接口 2 处于另外一个网段(2.2.2.0/24)。Host 上配置默认网关为 Switch A 的 VLAN 接口 3 的地址(1.1.1.2/24)，Switch B 上配置静态路由使得 Host 与 Switch B 之间路由可达。要求配置定向广播功能使 Host 发送的定向广播报文到达 Switch B 的 VLAN 接口 2。

4. 配置过程和解释

配置定向广播功能，如下所示。

(1) 配置 Switch A。

① 配置允许 Switch A 接收定向的广播报文。

```
<SwitchA> system-view
[SwitchA] ip forward-broadcast
```

② 创建 VLAN 2 和 VLAN 3。

```
[SwitchA] Vlan 2
[SwitchA-Vlan2] quit
```

```
[SwitchA] Vlan 3
[SwitchA-Vlan3] quit
```

③ 配置 VLAN 接口 3 和 VLAN 接口 2 的 IP 地址。

```
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ip address 1.1.1.2 24
[SwitchA-Vlan-interface3] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 2.2.2.2 24
```

④ 配置允许 VLAN 接口 2 转发定向广播报文。

```
[SwitchA-Vlan-interface2] ip forward-broadcast
```

(2) 配置 Switch B。

① 配置允许 Switch B 接收定向的广播报文。

```
<SwitchB> system-view
[SwitchB] ip forward-broadcast
```

② 创建 VLAN 2。

```
[SwitchB] Vlan 2
[SwitchB-Vlan2] quit
```

③ 配置 Switch B 到 Host 的静态路由。

```
[SwitchB] ip route-static 1.1.1.1 24 2.2.2.2
```

④ 配置 VLAN 接口 2 的 IP 地址。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 2.2.2.1 24
```

配置完成以后，在 Host 上 ping Switch A 的 VLAN 接口 2 所在子网网段的广播地址(2.2.2.255)时，Switch B 的 VLAN 接口 2 可以收到该报文。取消掉任何一个 ip forward-broadcast 的配置，Switch B 的 VLAN 接口 2 都不能收到该报文。

提示：允许接口转发定向的广播报文时，如果配置了 ACL 规则，则在转发广播报文的同时还需要对报文进行过滤，不符合 ACL 规则的报文将被丢弃，只转发符合 ACL 规则的报文。

如果在同一接口下重复执行 ip forward-broadcast acl 命令，则后面配置的 ACL 会覆盖以前配置的 ACL；如果后配置的命令不带 acl acl-number，则以前配置中的 ACL 规则将被取消。

7.2 ARP 典型配置指导

7.2.1 ARP 基本功能典型配置指导

默认情况下，设备上的 ARP 表老化时间是 20min。ARP 为动态学习，每个 VLAN 虚接口下的 ARP 数量也没有限制，可以通过在交换机上修改 ARP 的参数，达到优化网络设

备的目的。

1. 背景

M公司的交换机作为服务器的网关，设备上存在多条ARP表项。在设备运行维护过程中，管理员可以对设备上的ARP表进行参数调整，达到优化ARP表的目的。

2. 组网图

无。

3. 配置需求

设置交换机的动态ARP表项的老化时间为10min。

设置接口Vlan-interface 10上可以学习动态ARP表项的最大个数为1000。

增加一条长静态ARP表项，IP地址为192.168.1.1/24，对应的MAC地址为000f-e201-0000，表项对应的出端口为属于VLAN 10的端口GigabitEthernet 1/0/10。

增加一条短静态ARP表项，IP地址为192.168.1.2/24，对应的MAC地址为000f-e201-0001。

4. 配置过程和解释

(1) 设置交换机的动态ARP表项的老化时间为10min。

```
[Switch] arp timer aging 10
```

(2) 设置接口Vlan-interface 10上可以学习动态ARP表项的最大个数为1000。

```
[Switch] vlan 10
[Switch-vlan10] quit
[Switch-GigabitEthernet1/0/10] port access vlan 10
[Switch-GigabitEthernet1/0/10] quit
[Switch] interface vlan-interface 10
[Switch-vlan-interface10] arp max-learning-num 1000
[Switch-vlan-interface10] quit
```

(3) 增加一条长静态ARP表项。

```
[Switch] arp static 192.168.1.1 000f-e201-0000 10 GigabitEthernet 1/0/10
```

(4) 增加一条短静态ARP表项。

```
[Switch] arp static 192.168.1.2 000f-e201-0001
```

提示： 静态ARP表项在设备正常工作时间一直有效，当设备的ARP表项所对应的VLAN或VLAN接口被删除时，如果是长静态ARP表项则被删除，若是已经解析的短静态ARP表项则重新变为未解析状态。

7.2.2 代理ARP典型配置指导

对于没有配置默认网关的计算机要和其他网络中的计算机实现通信，网关收到源计算机的ARP请求会使用自己的MAC地址与目标计算机的IP地址对源计算机进行应答。如果ARP请求是从一个网络的主机发往同一网段却不在同一物理网络上的另一台主机，那么连接它们的具有代理ARP功能的设备就可以回答该请求，将一台主机作为对另一台主机ARP直接进行应答。

1. 背景

M公司的业务部门主机在同一个VLAN内，所有主机均没有配置默认网关，近期业务部门提出需要临时和财务部门(处于和业务部门同一网段但不同VLAN)用户进行通信，但主机比较多，业务部门不想通过逐一更改主机默认网关的方式来解决此问题。因此，网络管理员需要配置代理ARP来解决类似的要求。

2. 组网图

图7-3所示为代理ARP典型配置组网图。

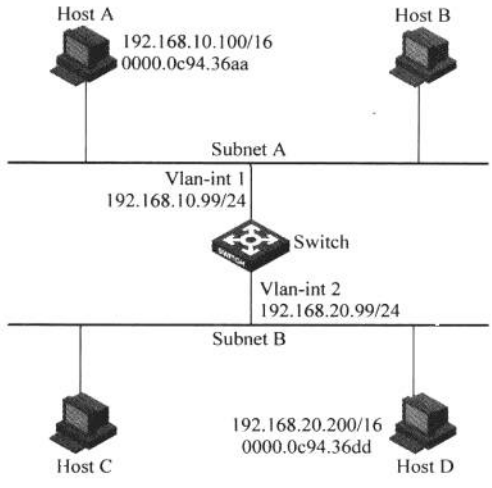


图7-3 代理ARP典型配置组网图

3. 配置需求

如图7-3所示，管理员通过配置代理ARP，使得原本同一网段不同VLAN的主机在不需要配置网关的情况下能够互相通信。

Host A和Host D配置为同一网段的主机(Host A的IP地址是192.168.10.100/16，Host D的IP地址是192.168.20.200/16)，但却被设备Switch分在两个不同的子网(Host A属于VLAN 1，Host D属于VLAN 2)。Host A和Host D没有配置默认网关，要求在设备Switch上启用代理ARP功能，使处在两个子网的Host A和Host D能互通。

4. 配置过程和解释

(1) 配置VLAN 1接口的IP地址，并开启代理ARP功能。

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.10.99 255.255.255.0
[Switch-Vlan-interface1] proxy-arp enable
[Switch-Vlan-interface1] quit
```

(2) 配置VLAN 2接口的IP地址，并开启代理ARP功能。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.20.99 255.255.255.0
[Switch-Vlan-interface2] proxy-arp enable
[Switch-Vlan-interface2] quit
```

7.2.3 端口隔离时的本地代理 ARP 典型配置指导

本地代理 ARP 可以在下列 3 种情况下实现主机之间的三层互通。

(1) 想要互通的主机分别连接到同一个 VLAN 中的不同二层隔离端口下。

(2) 使能 Super VLAN 功能后，想要互通的主机属于不同的 Sub VLAN。

(3) 使能 Isolate-user-VLAN 功能后，想要互通的主机属于不同的 Secondary VLAN。

1. 背景

M 公司财务部门分为财务信息部和会计部，两个部门的部分服务器处于同一台交换机的同一个 VLAN 内，但服务器之间配置了端口隔离，使得服务器之间不能通信。近期因为业务的需要，这些服务器需要进行业务交流，但交互流量不能在直连的交换机上直接转发，需要到上层网关设备上进行监控后再转发。网络管理员可以配置本地代理 ARP 来处理解决此类问题。

2. 组网图

图 7-4 所示为端口隔离时的本地代理 ARP 典型配置组网图。

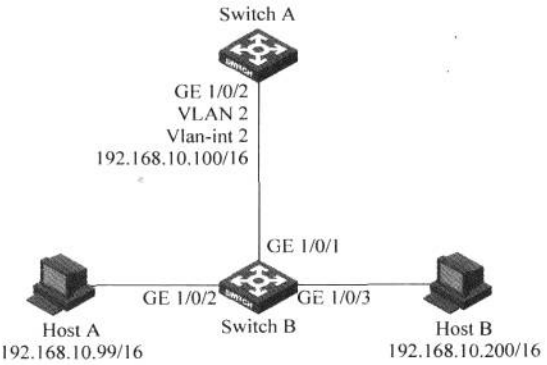


图 7-4 端口隔离时的本地代理 ARP 典型配置组网图

3. 配置需求

如图 7-4 所示，管理员通过配置本地代理 ARP，使得原本被端口隔离控制不能互通的两台主机能够三层互通。

Host A 和 Host B 属于同一个 VLAN，分别与设备 Switch B 的端口 GigabitEthernet 1/0/2 和 GigabitEthernet 1/0/3 相连。

设备 Switch B 通过端口 GigabitEthernet 1/0/1 端口与 Switch A 相连。

实现被二层隔离的端口 GigabitEthernet 1/0/2 和 GigabitEthernet 1/0/3 能够三层互通。

4. 配置过程和解释

(1) 配置 Switch B 的端口 GigabitEthernet 1/0/1、GigabitEthernet 1/0/2、GigabitEthernet 1/0/3 属于 VLAN 2。

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port GigabitEthernet 1/0/1
[SwitchB-vlan2] port GigabitEthernet 1/0/2
[SwitchB-vlan2] port GigabitEthernet 1/0/3
[SwitchB-vlan2] quit
```

(2) 配置 Switch B 的端口 GigabitEthernet 1/0/2 和 GigabitEthernet 1/0/3 隔离。

```
[SwitchB] interface GigabitEthernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port-isolate enable
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface GigabitEthernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port-isolate enable
[SwitchB-GigabitEthernet1/0/3] quit
```

(3) 配置 Switch A 的 VLAN 接口 2 的 IP 地址。

```
[SwitchA] vlan 2
[SwitchA-vlan2] port GigabitEthernet 1/0/2
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.10.100 255.255.0.0
```

(4) 配置本地代理 ARP,实现 Host A 和 Host B 之间的三层互通。

```
[SwitchA-Vlan-interface2] local-proxy-arp enable
[SwitchA-Vlan-interface2] quit
```

7.2.4 ARP Detection 典型配置指导

通过配置 ARP Detection 功能,只允许合法用户的 ARP 报文进行正常转发,丢弃非法 ARP 报文,从而防止仿冒用户、仿冒网关的攻击。

1. 背景

M 公司业务部门后期采用了 DHCP 的方式动态分配地址,网络使用正常。但最近 IT 维护部门发现业务部门网络中某些主机中了病毒,存在假冒网关的 ARP、短时间内发送大量 ARP 报文等异常现象,IT 维护部门通过调整交换机配置,增加 ARP Detection 特性,来避免网络中 ARP 攻击的泛滥。

2. 组网图

图 7-5 所示为 ARP Detection 典型配置组网图。

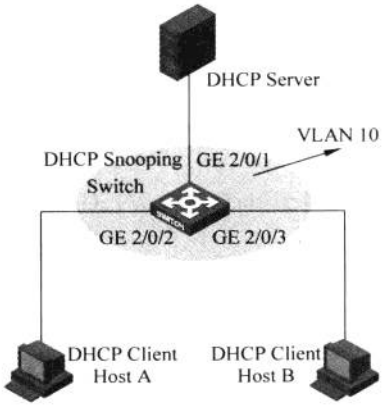


图 7-5 ARP Detection 典型配置组网图

3. 配置需求

(1) Switch 是 DHCP Snooping 设备，在 VLAN 10 内启用 ARP Detection 功能，对 DHCP 客户端进行保护，保证合法用户可以正常转发报文，否则丢弃。

(2) Host A 和 Host B 是 DHCP 客户端。

4. 配置过程和解释

(1) 配置 DHCP 服务器(略)。

(2) 配置 Host A 和 Host B 通过 DHCP 自动获取 IP 地址(略)。

(3) 配置 Switch 为 DHCP Snooping 设备。

① 配置 Switch 所有端口属于 VLAN 10(略)。

② 配置 DHCP Snooping 功能。

```
<Switch> system-view
[Switch] dhcp-snooping
[Switch] interface GigabitEthernet 2/0/1
[Switch-GigabitEthernet2/0/1] dhcp-snooping trust
[Switch-GigabitEthernet2/0/1] quit
```

③ 配置 ARP Detection 特性，端口状态默认为非信任状态，上行端口配置为信任状态，下行端口保持默认配置。

```
[Switch] vlan 10
[Switch-vlan10] arp detection enable
[Switch-vlan10] quit
[Switch] interface GigabitEthernet 2/0/1
[Switch-GigabitEthernet2/0/1] arp detection trust
[Switch-GigabitEthernet2/0/1] quit
```

④ 配置报文有效性检查。

```
[Switch] arp detection validate dst-mac ip src-mac
```

⑤ 配置 ARP 报文上送限速，速率为 150pps。

```
[Switch] interface GigabitEthernet 2/0/2
[Switch-GigabitEthernet2/0/2] arp rate-limit rate 150 drop
[Switch-GigabitEthernet2/0/2] quit
[Switch] interface gigabitethernet 2/0/3
[Switch-GigabitEthernet2/0/3] arp rate-limit rate 150 drop
[Switch-GigabitEthernet2/0/3] quit
```

提示：ARP Detection 包含 3 个功能：用户合法性检查、ARP 报文有效性检查、ARP 报文强制转。

如果既配置了报文有效性检查功能，又配置了用户合法性检查功能，那么先进行报文有效性检查，然后进行用户合法性检查。

7.3 DHCP 典型配置指导

7.3.1 DHCP 服务器静态绑定地址典型配置指导

某些客户端需要固定的 IP 地址，可以通过将客户端的 MAC 地址与 IP 地址绑定的方式实现。当具有此 MAC 地址的客户端申请 IP 地址时，DHCP 服务器将根据客户端的 MAC 地址查找到对应的 IP 地址，并分配给客户端。

1. 背景

M 公司采用 DHCP 动态分配地址，但公司公共资源如打印机、文件服务器采用动态地址分配，有可能会在打印机、服务器重启时分配地址发生变化，带来网络维护不变，因此可以采用静态绑定地址的方式，为公共资源分配不同的固定 IP 地址。网络管理员可以在 DHCP Server 端配置静态地址绑定，打印机、文件服务器采用统一分配的静态地址。

2. 组网图

图 7-6 所示为 DHCP 服务器静态绑定地址典型配置组网图。

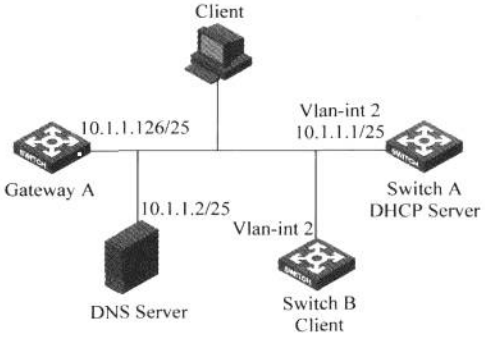


图 7-6 DHCP 服务器静态绑定地址典型配置组网图

3. 配置需求

如图 7-6 所示，Switch B 作为 DHCP 客户端，从 DHCP 服务器 Switch A 获取静态绑定的 IP 地址、域名服务器、网关地址等信息。

4. 配置过程和解释

(1) 配置接口的 IP 地址。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.1 25
[SwitchA-Vlan-interface2] quit
```

(2) 使能 DHCP 服务。

```
[SwitchA] dhcp enable
```

(3) 配置 DHCP 地址池 0，采用静态绑定方式分配 IP 地址。

```
[SwitchA] dhcp server ip-pool 0
```

```
[SwitchA-dhcp-pool-0] static-bind ip-address 10.1.1.5
[SwitchA-dhcp-pool-0] static-bind mac-address 000f-e200-0002
[SwitchA-dhcp-pool-0] dns-list 10.1.1.2
[SwitchA-dhcp-pool-0] gateway-list 10.1.1.126
[SwitchA-dhcp-pool-0] quit
```

提示：静态绑定的IP地址不能是DHCP服务器的接口IP地址，否则会导致IP地址冲突，被绑定的客户端将无法正常获取到IP地址。

目前一个DHCP地址池中只能配置一个静态绑定，可以是IP地址与MAC地址的绑定，也可以是IP地址与客户端ID(用于唯一标识一个客户端的，4～160个字符的字符串)的绑定。

静态绑定的客户端ID，要与在待绑定客户端通过display dhcp client verbose命令显示的客户端ID一致，否则，客户端无法成功获取IP地址。

7.3.2 DHCP服务器动态分配地址典型配置指导

通过配置DHCP动态分配地址，可以自动为主机分配地址。

1. 背景

M公司业务发展越来越广泛，原有的静态地址分配方式已经不能满足用户方便、易用的要求，网络管理员可以通过配置DHCP来动态分配地址，同时通过配置相关参数进行优化。

2. 组网图

图7-7所示为DHCP服务器动态分配地址典型配置组网图。

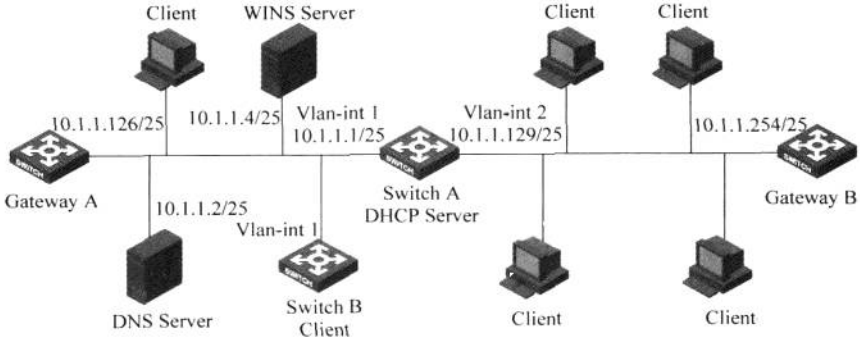


图7-7 DHCP服务器动态分配地址典型配置组网图

3. 配置需求

如图7-7所示，管理员配置DHCP动态分配地址，同时根据需求配置DHCP服务器相关参数，保证本网内DHCP使用最优。

4. 配置过程和解释

(1) 使能DHCP服务。

```
[SwitchA] dhcp enable
```

(2) 配置不参与自动分配的IP地址(DNS服务器、WINS服务器和网关地址)。

```
[SwitchA] dhcp server forbidden-ip 10.1.1.2
[SwitchA] dhcp server forbidden-ip 10.1.1.4
```

```
[SwitchA] dhcp server forbidden-ip 10.1.1.126
[SwitchA] dhcp server forbidden-ip 10.1.1.254
```

(3) 配置伪服务器检测功能。

```
[SwitchA] dhcp server detect
```

(4) 配置 DHCP 地址池 0 的共有属性(地址池范围、DNS 服务器地址)。

```
[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
[SwitchA-dhcp-pool-0] domain-name aabbcc.com
[SwitchA-dhcp-pool-0] dns-list 10.1.1.2
[SwitchA-dhcp-pool-0] quit
```

(5) 配置 DHCP 地址池 1 的属性(地址池范围、网关、WINS 服务器地址、地址租用期限)。

```
[SwitchA] dhcp server ip-pool 1
[SwitchA-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.128
[SwitchA-dhcp-pool-1] gateway-list 10.1.1.126
[SwitchA-dhcp-pool-1] expired day 10 hour 12
[SwitchA-dhcp-pool-1] nbns-list 10.1.1.4
[SwitchA-dhcp-pool-1] quit
```

(6) 配置 DHCP 地址池 2 的属性(地址池范围、地址租用期限、网关)。

```
[SwitchA] dhcp server ip-pool 2
[SwitchA-dhcp-pool-2] network 10.1.1.128 mask 255.255.255.128
[SwitchA-dhcp-pool-2] expired day 5
[SwitchA-dhcp-pool-2] gateway-list 10.1.1.254
[SwitchA-dhcp-pool-2] quit
```

开启伪服务器检测功能后,Switch A 记录所有 DHCP 服务器的信息,包括合法的 DHCP 服务器。管理员需要从系统日志中查找伪 DHCP 服务器。当 Switch A 发现网络中的其他 DHCP 服务器时,会记录如下所示的日志信息。

```
<SwitchA>
%Apr 30 08:07:51:896 2000 H3C DHCPS/4/DHCPS_Local_Server:
Local DHCP server information: Server IP (detected by DHCP server) =
  10.1.1.5, DHCP server interface = Vlan-interface1
Source client information: DHCP message type = DHCPREQUEST, DHCP
  client hardware address = 000f-e200-000b
```

提示:如果 DHCP 服务器的地址池中没有足够的可供分配的 IP 地址,则服务器无法为客户端分配地址,服务器不会将父地址池中的 IP 地址分配给客户端。故在本例中,建议从 VLAN 接口 1 申请 IP 地址的客户端数目不要超过 122 个;从 VLAN 接口 2 申请 IP 地址的客户端不要超过 124 个。

DHCP 服务器与客户端在同一网段的情况下,如果服务器的接口视图下配置了 dhcp select server global-pool subaddress 命令,则当 DHCP 服务器为客户端分配 IP 地址时,从与服务器接口(与客户端相连的接口)的从 IP 地址在同一网段的地址池中选择地址分配给

客户端。如果接口有多个从IP地址，则从第一个从IP地址开始依次匹配。否则，服务器从与接口主IP地址在同一网段的地址池中选择地址分配给客户端。

7.3.3 DHCP中继典型配置指导

由于在IP地址动态获取过程中采用广播方式发送报文，因此DHCP只适用于DHCP客户端与服务器处于同一个子网内的情况。为进行动态主机配置，需要在所有网段上都设置一台DHCP服务器，这显然是很不经济的。DHCP中继功能解决了这一问题。子网内的客户端可以通过DHCP中继与其他子网的DHCP服务器通信，最终获取到IP地址。这样，多个网络上的DHCP客户端可以使用同一台DHCP服务器，既节约了成本，又便于进行集中管理。

1. 背景

M公司的网络划分了多个VLAN，每个VLAN对应不同的部门，由于整个网络只有一台DHCP服务器，网络管理员需要配置DHCP中继来保证不同VLAN的客户端使用同一台服务器分配地址。

2. 组网图

图7-8所示为DHCP中继典型配置组网图。

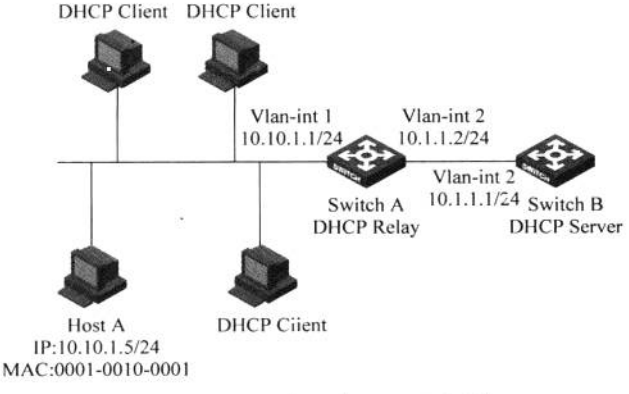


图7-8 DHCP中继典型配置组网图

3. 配置需求

如图7-8所示，管理员通过配置DHCP中继功能，报文客户端可以动态分配地址，同时配置主机A不参与动态地址分配，使用固定的静态地址，同时开启DHCP中继地址表项检查功能，使合法固定IP地址用户和通过DHCP服务器获取IP地址的用户访问网络，防止客户端私自修改IP地址访问网络。

4. 配置过程和解释

(1) 使能DHCP服务。

```
<SwitchA> system-view
[SwitchA] dhcp enable
```

(2) 配置VLAN接口1工作在DHCP中继模式。

```
[SwitchA] interface vlan-interface 1
```

```
[SwitchA-Vlan-interface1] ip address 10.10.1.1 24
[SwitchA-Vlan-interface1] dhcp select relay
[SwitchA-Vlan-interface1] quit
```

(3) 配置 DHCP 服务器的地址,并配置 VLAN 接口 1 对应 DHCP 服务器组 1。

```
[SwitchA] dhcp relay server-group 1 ip 10.1.1.1
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] dhcp relay server-select 1
[SwitchA-Vlan-interface1] quit
```

(4) 在 DHCP 中继上为 Host A 配置一条静态用户地址表项,IP 地址为 10.10.1.5/24,MAC 地址为 0001-0010-0001。

```
[SwitchA] dhcp relay security static 10.10.1.5 0001-0010-0001
```

(5) 开启 DHCP 中继地址匹配检查功能。

```
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] dhcp relay address-check enable
[SwitchA-Vlan-interface1] quit
```

提示:DHCP 中继与 DHCP 服务器之间必须有路由可达。

DHCP 中继的地址匹配检查功能与 DHCP 中继的其他配置无直接关系,即只要执行了 dhcp relay address-check enable 命令,地址匹配检查功能就可以生效,不需要配置 DHCP 中继的其他功能,如使能 DHCP、配置接口工作在 DHCP 中继模式等。

7.3.4 DHCP Snooping 典型配置指导

DHCP Snooping 通过两种方法来获得用户从 DHCP Server 获取的 IP 地址和用户 MAC 地址信息:监听 DHCP-ACK 报文和监听 DHCP-REQUEST 报文。

1. 背景

M 公司网络有时存在非法用户连接进网络中的情况。出于安全性的考虑,网络管理员需要记录用户上网时所用的 IP 地址等信息,确认用户从 DHCP Server 获取的 IP 地址和用户主机的 MAC 地址的对应关系,可以通过开启 DHCP Snooping 来实现。

2. 组网图

图 7-9 所示为 DHCP Snooping 典型配置组网图。

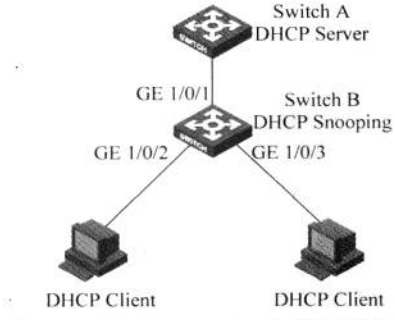


图 7-9 DHCP Snooping 典型配置组网图

3. 配置需求

如图 7-9 所示，管理员通过开启 DHCP Snooping 功能，既保证客户端从合法服务器获得地址，也记录 DHCP 客户端 IP 地址与 MAC 地址的对应关系。

4. 配置过程和解释

(1) 使能 DHCP Snooping 功能。

```
<SwitchB> system-view
[SwitchB] dhcp-snooping
```

(2) 配置 GigabitEthernet 1/0/1 端口为信任端口。

```
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] dhcp-snooping trust
[SwitchB-GigabitEthernet1/0/1] quit
```

(3) 在端口 GigabitEthernet 1/0/2 上配置 DHCP Snooping 支持 Option 82 功能。

```
[SwitchB] interface GigabitEthernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] dhcp-snooping information enable
```

(4) 在端口 GigabitEthernet 1/0/2 上配置 Option 82 以 verbose 格式进行填充。

```
[SwitchB-GigabitEthernet1/0/2] dhcp-snooping information format verbose node-identifier sysname
[SwitchB-GigabitEthernet1/0/2] quit
```

(5) 在端口 GigabitEthernet 1/0/3 上配置 DHCP Snooping 支持 Option 82 功能。

```
[SwitchB] interface GigabitEthernet1/0/3
[SwitchB-GigabitEthernet1/0/3] dhcp-snooping information enable
```

(6) 在端口 GigabitEthernet 1/0/3 上配置 Option 82 以 verbose 格式进行填充。

```
[SwitchB-GigabitEthernet1/0/3] dhcp-snooping information format verbose node-identifier sysname
```

提示：设备只有位于 DHCP 客户端与 DHCP 服务器或 DHCP 客户端与 DHCP 中继之间时，DHCP Snooping 功能配置后才能正常工作；设备位于 DHCP 服务器与 DHCP 中继之间时，DHCP Snooping 功能配置后不能正常工作。

使能 DHCP Snooping 功能的设备，不能作为 DHCP 服务器和 DHCP 中继。

为了使 DHCP 客户端能从合法的 DHCP 服务器获取 IP 地址，必须将与合法 DHCP 服务器相连的端口设置为信任端口，设置的信任端口和与 DHCP 客户端相连的端口必须在同一个 VLAN 内。

7.3.5 DHCP Snooping 支持 Option 82 典型配置指导

DHCP Snooping 设备通过在 DHCP 请求报文中添加 Option 82 选项，将 DHCP 客户端的位置信息告诉给 DHCP 服务器，从而使得 DHCP 服务器能够为主机分配合适的 IP 地址和其他配置信息，并实现对客户端的安全和计费等控制。

1. 背景

M公司业务部使用192.168.0.0/24的网段，共包含3个办公室。管理员可以通过配置Option 82为每个办公室分配不同范围的地址，同时在DHCP服务器上记录客户端的接入物理端口和接入设备标识等信息。

2. 组网图

图7-10所示为DHCP Snooping支持Option 82典型配置组网图。

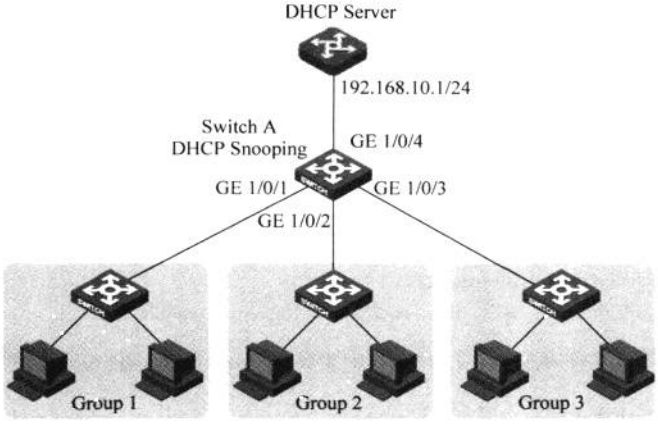


图7-10 DHCP Snooping支持Option 82典型配置组网图

3. 配置需求

如图7-10所示，管理员通过配置3个小组Group 1、Group 2和Group 3，为每个小组分配同一网段内不同地址范围地址，使Group 1、Group 2、Group 3分别分配地址段192.168.10.2～192.168.10.100、192.168.10.101～192.168.10.200、192.168.10.201～192.168.10.240。

为实现需求，需要在Switch A上配置DHCP Snooping支持Option 82。

4. 配置过程和解释

(1) 使能DHCP Snooping功能。

```
<SwitchA> system-view
[SwitchA] dhcp-snooping
```

(2) 配置GigabitEthernet 1/0/4端口为信任端口。

```
[SwitchA] interface GigabitEthernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] dhcp-snooping trust
[SwitchA-GigabitEthernet1/0/4] quit
```

(3) 在端口GigabitEthernet 1/0/1上配置DHCP Snooping支持Option 82功能，并配置Option 82的填充方式为Normal。

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] dhcp-snooping information enable
[SwitchA-GigabitEthernet1/0/1] dhcp-snooping information format normal
[SwitchA-GigabitEthernet1/0/1] quit
```

(4) 在端口GigabitEthernet 1/0/2上配置DHCP Snooping支持Option 82功能，并配

置 Option 82 的填充方式为 Normal。

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] dhcp-snooping information enable
[SwitchA-GigabitEthernet1/0/2] dhcp-snooping information format normal
[SwitchA-GigabitEthernet1/0/2] quit
```

(5) 在端口 GigabitEthernet 1/0/3 上配置 DHCP Snooping 支持 Option 82 功能，并配置 Option 82 的填充方式为 Normal。

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] dhcp-snooping information enable
[SwitchA-GigabitEthernet1/0/3] dhcp-snooping information format normal
[SwitchA-GigabitEthernet1/0/3] quit
```

提示：只有使能 DHCP Snooping 功能之后，DHCP Option 82 功能才能生效。

DHCP Snooping Option 82 功能建议在最靠近 DHCP Client 的 Snooping 设备上使用，以达到精确定位用户位置的目的。

DHCP Snooping Option 82 功能的使用需要 DHCP Server 做相应配置。

7.3.6 DHCP 客户端典型配置指导

默认情况下，网络设备没有配置任何地址，设备无法进行管理，通过为设备动态分配地址的方式，为网络设备配置管理地址。

1. 背景

M 公司的网络设备配置了管理地址用于远程管理网络设备，管理员可以通过将网络设备配置为 DHCP 客户端，动态地为网络设备分配管理地址。

2. 组网图

图 7-11 所示为 DHCP 客户端典型配置组网图。

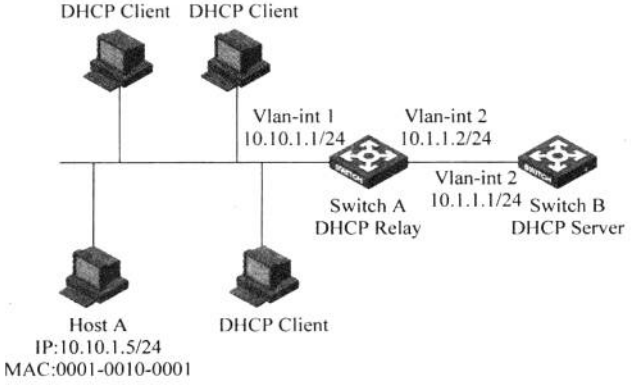


图 7-11 DHCP 客户端典型配置组网图

3. 配置需求

如图 7-11 所示，在交换机上配置 VLAN 接口 1 通过 DHCP 方式来获取 IP 地址。

4. 配置过程和解释

(1) 创建交换机 VLAN 1 接口并进入 Vlan-interface 1 接口视图。

```
[SwitchB] interface Vlan-interface 1
```

(2) 配置 Vlan-interface 1 通过 DHCP 方式来获取 IP 地址。

```
[SwitchB-Vlan-interface1] ip address dhcp-alloc
[SwitchB-Vlan-interface1] quit
```

提示：建议不要在同一台设备上同时配置 DHCP 客户端和 DHCP Snooping 功能，否则可能无法生成 DHCP Snooping 表项，DHCP 客户端也可能申请不到 IP 地址。

7.3.7 自动配置典型配置指导

自动配置功能是指在设备空配置启动时自动获取并执行配置文件的功能。自动配置功能简化了网络配置，便于实现对设备的集中管理。

自动配置的基本工作过程如下。

(1) 交换机在空配置启动时，系统会自动将处于 UP 状态的接口(如默认 VLAN 对应的接口)配置为通过 DHCP 方式获得 IP 地址及后续获取配置文件所需要的信息(例如，配置文件名、TFTP 服务器的域名、TFTP 服务器的 IP 地址、DNS 服务器 IP 地址等信息)。

(2) 如果交换机成功地从 DHCP 服务器获取到 IP 地址及配置文件名等相关信息，则发起 TFTP 请求，从指定的 TFTP 服务器获取配置文件。如果设备没有获取到相关信息，则在空配置文件的情况下正常启动。

1. 背景

M 公司新购买了一批交换机，交换机新上线时通常都需要网络管理员手动给交换机做相应配置。由于数量巨大，单独一台一台手动配置比较麻烦，网络管理员可以采用自动配置功能，在设备空配置启动时自动获取并执行配置文件，极大缩短了设备上线时间。

2. 组网图

图 7-12 所示为自动配置组网图。

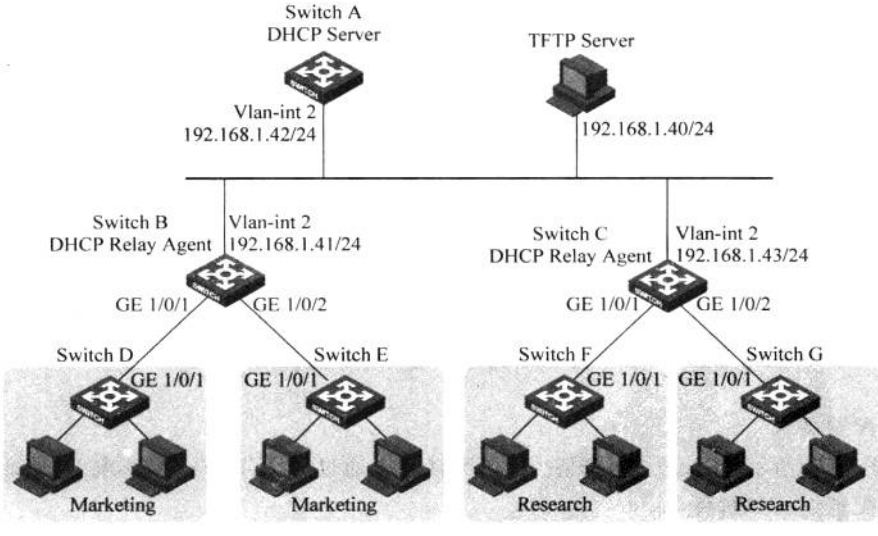


图 7-12 自动配置组网图

3. 配置需求

如图 7-12 所示，某公司下属两个部门：市场部门和研发部门，连接终端主机的交换机分别通过不同的网关设备(同时作为 DHCP 中继)连入网络。

Switch A 作为 DHCP Server，分别为市场部和研发部的主机分配 IP 地址和其他网络配置参数。

主机上运行 TFTPD32 软件，作为 TFTP Server。

(1) 市场部的网关设备为 Switch B，Switch B 同时作为 DHCP 中继，通过 VLAN 接口 2 与 DHCP Server、TFTP Server 相连，通过 VLAN 接口 3 与连接终端主机的 Switch D 和 Switch E 相连。VLAN 接口 3 的 IP 地址为 192.168.2.1/24。

(2) Switch D 和 Switch E 分别通过 VLAN 接口 3 与 DHCP 中继 Switch B 连接。

(3) 研发部的网关设备为 Switch C，Switch C 同时作为 DHCP 中继，通过 VLAN 接口 2 与 DHCP Server、TFTP Server 相连，通过 VLAN 接口 3 与连接终端主机的 Switch F 和 Switch G 相连。VLAN 接口 3 的 IP 地址为 192.168.3.1/24。

(4) Switch F 和 Switch G 分别通过 VLAN 接口 3 与 DHCP 中继 Switch C 连接。

为了简化对网络中设备的管理，使网络管理员能够通过 Telnet 方式登录、控制设备，并提供一定的安全保证，连接终端主机的交换机运行自动配置功能，使得交换机启动后自动获取配置文件。配置文件包括如下内容。

(1) 接口通过 DHCP 获取 IP 地址。

(2) 启动 Telnet 服务器功能。

(3) 创建本地用户。

(4) 配置通过 Telnet 方式登录设备时，需要进行认证。

4. 配置过程和解释

(1) DHCP Server 设备 Switch A 的配置。

① 配置 VLAN 接口 2 的 IP 地址。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port GigabitEthernet 1/0/1
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.1.42
[SwitchA-Vlan-interface2] quit
```

② 使能 DHCP 服务。

```
[SwitchA] dhcp enable
```

③ 配置 DHCP 地址池 market，为市场部动态分配 192.168.2.0/24 网段的地址，并指定 TFTP 服务器、网关地址和配置文件名。

```
[SwitchA] dhcp server ip-pool market
[SwitchA-dhcp-pool-market] network 192.168.2.0 24
[SwitchA-dhcp-pool-market] tftp ip-address 192.168.1.40
[SwitchA-dhcp-pool-market] gateway-list 192.168.2.1
```

```
[SwitchA-dhcp-pool-market] bootfile-name market.cfg
[SwitchA-dhcp-pool-market] quit
```

④ 配置 DHCP 地址池 research，为研发部动态分配 192.168.3.0/24 网段的地址，并指定 TFTP 服务器、网关地址和配置文件名。

```
[SwitchA] dhcp server ip-pool research
[SwitchA-dhcp-pool-research] network 192.168.3.0 24
[SwitchA-dhcp-pool-research] tftp ip-address 192.168.1.40
[SwitchA-dhcp-pool-research] gateway-list 192.168.3.1
[SwitchA-dhcp-pool-research] bootfile-name research.cfg
[SwitchA-dhcp-pool-research] quit
```

⑤ 配置到达 DHCP 中继的静态路由。

```
[SwitchA] ip route-static 192.168.2.0 24 192.168.1.41
[SwitchA] ip route-static 192.168.3.0 24 192.168.1.43
[SwitchA] quit
```

(2) DHCP 中继设备 Switch B 的配置。

① 配置 VLAN 接口 2 和 VLAN 接口 3 的 IP 地址。

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port GigabitEthernet 1/0/3
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.168.1.41
[SwitchB-Vlan-interface2] quit
[SwitchB] vlan 3
[SwitchB-vlan3] port GigabitEthernet 1/0/1
[SwitchB-vlan3] port GigabitEthernet 1/0/2
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ip address 192.168.2.1
[SwitchB-Vlan-interface3] quit
```

② 使能 DHCP 服务。

```
[SwitchB] dhcp enable
```

③ 配置 DHCP 服务器的地址。

```
[SwitchB] dhcp relay server-group 1 ip 192.168.1.42
```

④ 配置 VLAN 接口 3 工作在 DHCP 中继模式。

```
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] dhcp select relay
```

⑤ 配置 VLAN 接口 3 对应 DHCP 服务器组 1。

```
[SwitchB-Vlan-interface3] dhcp relay server-select 1
```

(3) DHCP 中继设备 Switch C 的配置。

① 配置接口的 IP 地址。

```
<SwitchC> system-view
[SwitchC] vlan 2
[SwitchC-vlan2] port GigabitEthernet 1/0/3
[SwitchC-vlan2] quit
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ip address 192.168.1.43
[SwitchC-Vlan-interface2] quit
[SwitchC] vlan 3
[SwitchC-vlan3] port GigabitEthernet 1/0/1
[SwitchC-vlan3] port GigabitEthernet 1/0/2
[SwitchC-vlan3] quit
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] ip address 192.168.3.1
[SwitchC-Vlan-interface3] quit
```

② 使能 DHCP 服务。

```
[SwitchC] dhcp enable
```

③ 配置 DHCP 服务器的地址。

```
[SwitchC] dhcp relay server-group 1 ip 192.168.1.42
```

④ 配置 VLAN 接口 3 工作在 DHCP 中继模式。

```
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] dhcp select relay
```

⑤ 配置 VLAN 接口 3 对应 DHCP 服务器组 1。

```
[SwitchC-Vlan-interface3] dhcp relay server-select 1
```

(4) 配置主机作为 TFTP Server。

① 在主机的“D:/TFTP Server”目录下创建配置文件 market.cfg,文件内容如下:

```
sysname Market
telnet server enable
vlan 3
local-user market
password simple market
service-type telnet
level 3
interface Vlan-interface3
ip address dhcp-alloc
interface GigabitEthernet 1/0/1
port access vlan 3
user-interface vty 0 4
authentication-mode scheme
user privilege level 3
return
```

② 在主机的“D:/TFTP Server”目录下创建配置文件 research.cfg，文件内容如下：

```
sysname Research
telnet server enable
vlan 3
local-user research
password simple research
service-type telnet
level 3
interface Vlan-interface3
ip address dhcp-alloc
interface GigabitEthernet 1/0/1
port access vlan 3
user-interface vty 0 4
authentication-mode scheme
user privilege level 3
return
```

③ 运行 TFTPD32 软件，单击 Settings 按钮，如图 7-13 所示。

④ 将配置文件保存的路径设置为 Base Directory，单击 OK 按钮，如图 7-14 所示。

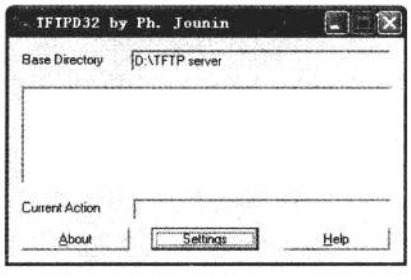


图 7-13 TFTP Server 配置界面

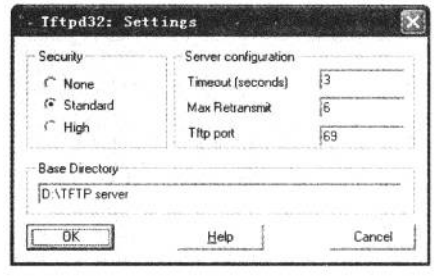


图 7-14 设置文件保存的路径

⑤ 配置主机到达 192.168.2.0/24 和 192.168.3.0/24 网段的路由，即在主机上执行如下命令。

```
route add 192.168.2.0 mask 255.255.255.0 192.168.1.41
route add 192.168.3.0 mask 255.255.255.0 192.168.1.43
```

7.4 域名解析典型配置指导

7.4.1 静态域名解析典型配置指导

静态域名解析就是手动建立域名和 IP 地址之间的对应关系。当用户使用域名进行某些应用(如 Telnet 应用)时，系统查找静态域名解析表，从中获取指定域名对应的 IP 地址。

1. 背景

M 公司 IT 维护部门对部分服务器开通了 Telnet 服务，可以通过 Telnet 方式连接服务

器后执行命令。为了便于记忆，统一在网络设备上对这些服务器手动配置了域名和 IP 地址间的对应关系，这样公司员工可以通过 Telnet 域名的方式访问服务器。

2. 组网图

图 7-15 所示为静态域名解析典型配置组网图。

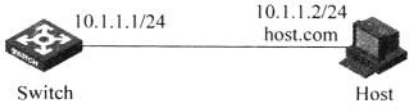


图 7-15 静态域名解析典型配置组网图

3. 配置需求

如图 7-15 所示，交换机利用静态域名解析功能，实现通过主机名 host.com 访问 IP 地址为 10.1.1.2 的主机 Host。

4. 配置过程和解释

(1) 配置主机名 host.com 对应的 IP 地址为 10.1.1.2。

```
<Sysname> system-view
[Sysname] ip host host.com 10.1.1.2
```

(2) 执行 ping host.com 命令，Switch 通过静态域名解析可以解析到 host.com 对应的 IP 地址为 10.1.1.2。

```
[Sysname] ping host.com
  PING host.com (10.1.1.2):
  56  data bytes, press Ctrl_C to break
    Reply from 10.1.1.2: bytes=56 Sequence=1 ttl=128 time=2 ms
    Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=128 time=2 ms
    Reply from 10.1.1.2: bytes=56 Sequence=3 ttl=128 time=2 ms
    Reply from 10.1.1.2: bytes=56 Sequence=4 ttl=128 time=2 ms
    Reply from 10.1.1.2: bytes=56 Sequence=5 ttl=128 time=2 ms
  --- host.com ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/2 ms
```

7.4.2 动态域名解析典型配置指导

域名系统(Domain Name System，DNS)是一种用于 TCP/IP 应用程序的分布式数据库，提供域名与 IP 地址之间的转换。通过域名系统，用户进行某些应用时，可以直接使用便于记忆的、有意义的域名，由网络中的域名解析服务器解析为正确的 IP 地址。

1. 背景

M 公司 IT 维护部门新设立了一个公司网页，公司员工可以通过 Web 页面来了解公司动态。网络管理员给 Web 服务器分配固定 IP 地址，并且为了便于员工使用，公司配置了统一的 DNS 服务器，这样员工可以通过 Web 方式访问公司网页。

2. 组网图

图 7-16 所示为动态域名解析典型配置组网图。

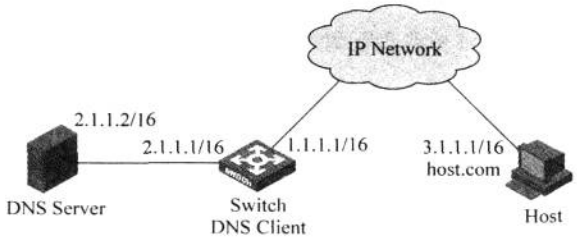


图 7-16 动态域名解析典型配置组网图

3. 配置需求

如图 7-16 所示，域名服务器的 IP 地址是 2.1.1.2/16，配置域名后缀为 com，交换机作为 DNS 客户端，使用动态域名解析和域名后缀列表功能，实现通过输入 host 来访问域名为 host.com、IP 地址为 3.1.1.1/16 的主机 Host。

4. 配置过程和解释

(1) 使能动态域名解析功能。

```
<Sysname> system-view
[Sysname] dns resolve
```

(2) 配置域名服务器的 IP 地址为 2.1.1.2。

```
[Sysname] dns server 2.1.1.2
```

(3) 配置域名后缀 com。

```
[Sysname] dns domain com
```

(4) 在设备上执行 ping host 的命令，可以 ping 通主机，且对应的目的地址为 3.1.1.1。

```
[Sysname] ping host
Trying DNS resolve, press Ctrl_C to break
Trying DNS server (2.1.1.2)
  PING host.com (3.1.1.1):
  56  data bytes, press Ctrl_C to break
    Reply from 3.1.1.1: bytes=56 Sequence=1 ttl=126 time=3 ms
    Reply from 3.1.1.1: bytes=56 Sequence=2 ttl=126 time=1 ms
    Reply from 3.1.1.1: bytes=56 Sequence=3 ttl=126 time=1 ms
    Reply from 3.1.1.1: bytes=56 Sequence=4 ttl=126 time=1 ms
    Reply from 3.1.1.1: bytes=56 Sequence=5 ttl=126 time=1 ms
  --- host.com ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/3 ms
```

提示：在开始上面的配置之前，确保设备与主机之间的路由可达，设备和主机都已经配置完毕。

DNS客户端需要和域名服务器配合使用，才能根据域名解析到正确的IP地址。

7.4.3 DNS Proxy典型配置举例指导

DNS代理(DNS Proxy)用来在DNS Client与DNS Server之间转发DNS请求和应答报文，代替DNS Client进行域名解析。局域网内的DNS Client将DNS Proxy当做DNS Server，将DNS请求报文发送给DNS Proxy。DNS Proxy将该请求报文转发到真正的DNS Server，并将DNS Server的应答报文返回给DNS Client，从而实现域名解析。

1. 背景

M公司IT维护部门最近在进行网络优化，DNS Server的IP地址可能会重新分配。当DNS Server的IP发生变化时，需要调整所有DNS Client上的DNS Server配置，配置工作量比较大。管理员想到，可以通过配置DNS代理功能，这样当DNS Server的地址发生变化时，只需改变DNS Proxy上的配置，无须改变局域网内每个DNS Client的配置，简化了网络管理。

2. 组网图

图7-17所示为DNS Proxy典型配置组网图。

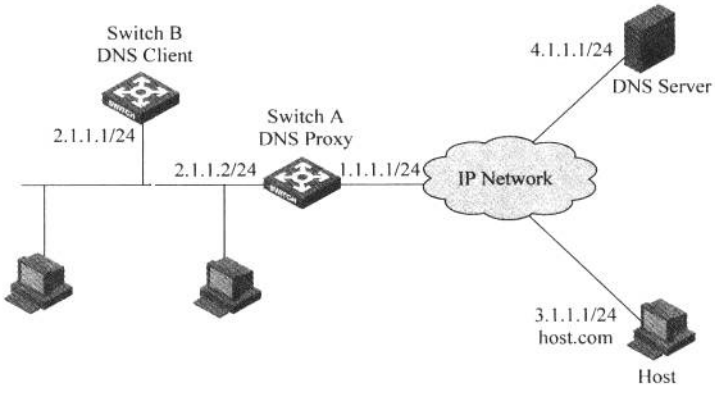


图7-17 DNS Proxy典型配置组网图

3. 配置需求

如图7-17所示，Switch B作为DNS客户端，指定域名服务器为Switch A，Switch A作为DNS代理。实际域名服务器的IP地址为4.1.1.1，Switch B通过DNS代理Switch A实现域名解析。

4. 配置过程和解释

(1) 配置DNS代理Switch A。

① 配置域名服务器的IP地址为4.1.1.1。

```
<SwitchA> system-view
[SwitchA] dns server 4.1.1.1
```

② 使能DNS Proxy功能。

```
[SwitchA] dns proxy enable
```

(2) 配置 DNS 客户端 Switch B。

① 使能动态域名解析功能。

```
<SwitchB> system-view
[SwitchB] dns resolve
```

② 配置域名服务器的 IP 地址为 2.1.1.2。

```
[SwitchB] dns server 2.1.1.2
```

(3) 验证配置结果。

在 Switch B 上执行 ping host.com 命令,可以 ping 通主机,且对应的目的地址为 3.1.1.1。

```
[SwitchB] ping host.com
Trying DNS resolve, press Ctrl_C to break
Trying DNS server (2.1.1.2)
  PING host.com (3.1.1.1):
  56  data bytes, press Ctrl_C to break
    Reply from 3.1.1.1: bytes=56 Sequence=1 ttl=126 time=3 ms
    Reply from 3.1.1.1: bytes=56 Sequence=2 ttl=126 time=1 ms
    Reply from 3.1.1.1: bytes=56 Sequence=3 ttl=126 time=1 ms
    Reply from 3.1.1.1: bytes=56 Sequence=4 ttl=126 time=1 ms
    Reply from 3.1.1.1: bytes=56 Sequence=5 ttl=126 time=1 ms
  --- host.com ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/3 ms
```

提示:在开始上面的配置之前,确保设备与主机之间的路由可达,设备和主机都已经配置完毕。

DNS 客户端需要和域名服务器配合使用,才能根据域名解析到正确的 IP 地址。

7.5 UDP Helper 典型配置指导

UDP Helper 功能可以实现对指定 UDP 端口的 IP 广播报文进行中继转发,即将指定 UDP 端口的广播报文转换为单播报文发送给指定的目的服务器,起到中继的作用。

使能 UDP Helper 功能后,如果设备接收到广播报文,将根据报文的 UDP 目的端口号来判断是否要对其中继转发,并进行相应的处理。如果报文的 UDP 目的端口号与配置的需要中继转发的 UDP 端口号相匹配,则修改 IP 报文头的目的 IP 地址,将报文发给指定的目的服务器;否则,直接将报文送给上层协议处理。

1. 背景

随着业务的拓展,M 公司开发了一套视频监控系统,3 个视频终端在一个网段内,视频采集源位于不同的网段,视频源持续不断地发送图像信息(UDP 广播报文)至视频终端。默认情况下,交换机不能转发 UDP 的广播报文,管理员可以在交换机上配置 UDP Helper 功能将视频源数据转发到指定服务器。

2. 组网图

图 7-18 所示为 UDP Helper 典型配置组网图。

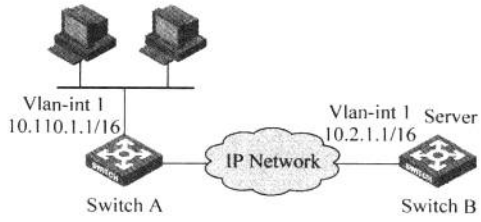


图 7-18 UDP Helper 典型配置组网图

3. 配置需求

如图 7-18 所示，Switch A 的 VLAN 接口 1 的 IP 地址为 10.110.1.1/16，连接到网段 10.110.0.0/16。配置将目的 UDP 端口号为 55、目的 IP 地址为 255.255.255.255 和此网段子网广播地址 10.110.255.255 的广播报文，中继转发到目的服务器 10.2.1.1/16。

4. 配置过程和解释

在开始下面的配置之前，需确保 Switch A 到 10.2.0.0 网段路由可达。

(1) 在 Switch A 上使能 UDP Helper 功能。

```
<SwitchA> system-view
[SwitchA] udp-helper enable
```

(2) 配置将目的 UDP 端口号为 55 的广播报文进行中继转发。

```
[SwitchA] udp-helper port 55
```

(3) 配置中继转发的目的服务器为 10.2.1.1。

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.110.1.1 16
[SwitchA-Vlan-interface1] udp-helper server 10.2.1.1
```

提示：UDP Helper 功能不能中继转发 DHCP 广播报文，即中继转发的 UDP 端口不能配置为 67 和 68。只有开启 UDP Helper 功能后，才能配置需要中继转发的 UDP 端口；否则，将会有错误提示信息。当关闭 UDP Helper 功能后，所有已配置的指定 UDP 端口都被取消。

第8章

三层技术——IP路由配置指导

8.1 静态路由典型配置指导

静态路由是一种特殊的路由，由管理员手动配置。在组网结构比较简单的网络中，只需配置静态路由就可以实现网络互通。恰当地设置和使用静态路由可以改善网络的性能，并可为重要的网络应用保证带宽。

静态路由的缺点在于，不能自动适应网络拓扑结构的变化，当网络发生故障或者拓扑发生变化后，可能会出现路由不可达，导致网络中断的现象，此时必须由 IT 维护人员手动修改静态路由的配置。

默认路由是在路由器没有找到匹配的路由表入口项时才使用的路由。

(1) 如果报文的目的地址不能与路由表的任何入口项相匹配，那么该报文将选取默认路由。

(2) 如果没有默认路由且报文的目的地不在路由表中，那么该报文将被丢弃，将向源端返回一个 ICMP 报文报告该目的地址或网络不可达。

默认路由可以通过静态路由配置，以到网络 0.0.0.0(掩码也为 0.0.0.0)的形式在路由表中出现，也可以由某些动态路由协议生成，如 OSPF、IS-IS 和 RIP。

1. 背景

M 公司的网络是在公司成立初(2001 年)建立起来的。最初，员工人数只有 100 多人，用了 10 台左右 H3C 以太网交换机，其中有 3 台是三层。网络分布跨越不同的楼层，楼层间以三层交换机作为网关设备，进行 IP 层通信。由于楼层较少，网络较为简单，网络维护员考虑通过部署静态路由即可使楼层间路由可达，配置简单、易于理解。

2. 组网图

图 8-1 所示为静态路由典型配置组网图。

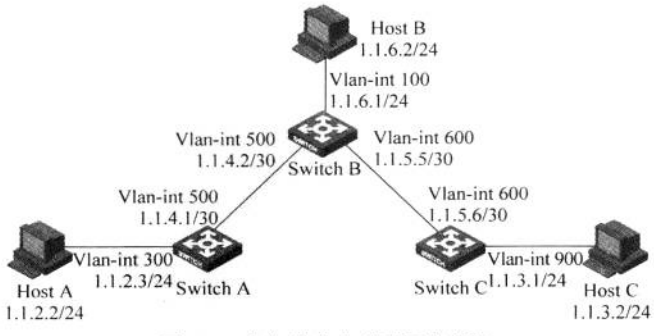


图 8-1 静态路由典型配置组网图

3. 配置需求

交换机各接口及主机的IP地址和掩码如图8-1所示，要求采用静态路由，使图中任意两个网段内的主机之间都能互相访问。

4. 配置过程和解释

(1) 配置各接口的IP地址(略)。

(2) 配置静态路由。

① 在Switch A上配置默认路由。

```
<SwitchA> system-view
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
```

② 在Switch B上配置两条静态路由。

```
<SwitchB> system-view
[SwitchB] ip route-static 1.1.2.0 255.255.255.0 1.1.4.1
[SwitchB] ip route-static 1.1.3.0 255.255.255.0 1.1.5.6
```

③ 在Switch C上配置默认路由。

```
<SwitchC> system-view
[SwitchC] ip route-static 0.0.0.0 0.0.0.0 1.1.5.5
```

(3) 配置主机。配置Host A的默认网关为1.1.2.3，Host B的默认网关为1.1.6.1，Host C的默认网关为1.1.3.1，具体配置过程略。

提示：经过不同下一跳到达相同目的地址的静态路由，可以通过配置优先级来使它们之间形成主备或者负载分担的关系。配置不同的优先级可以形成主备关系；配置相同的优先级可以形成负载分担关系。

8.2 RIP协议典型配置指导

8.2.1 RIP基本功能典型配置指导

RIP(Routing Information Protocol，路由信息协议)是一种较为简单的内部网关协议(Interior Gateway Protocol，IGP)，主要用于规模较小的网络中，如校园网以及结构较简单的地区性网络。对于更为复杂的环境和大型网络，一般不使用RIP。

由于RIP的实现较为简单，在配置和维护管理方面也远比OSPF和IS-IS容易，因此在实际组网中仍有广泛的应用。

1. 背景

随着公司日益发展，办公网络在不断扩大，M公司网络拓扑也越来越复杂。2003年时，公司网络已经使用了近10台三层交换机了。这时网络维护人员发现，虽然用静态路由可以达到网络互连，但是配置工作量变得越来越大而且不便于维护。因此，必须寻找一种可以自动学习路由，感知拓扑变化的路由方案。经过分析，维护人员最终决定使用RIP这种简单易用的动态路由协议来连通各个网段，使交换机之间可以自动发现邻居、路由学习，降低了维护难度。

2. 组网图

图 8-2 所示为 RIP 基本功能典型配置组网图。

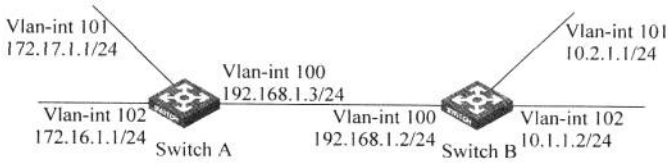


图 8-2 RIP 基本功能典型配置组网图

3. 配置需求

如图 8-2 所示，要求在 Switch A 和 Switch B 的所有接口上使能 RIP，使用 RIP-2 发布路由网段，最终达到使 Switch A、Switch B 都能够学习到对方接口下网段路由的目的。

4. 配置过程和解释

(1) 配置各接口的 IP 地址(略)。

(2) 配置 RIP 基本功能。

① 配置 Switch A。

```
<SwitchA> system-view
[SwitchA] rip
[SwitchA-rip-1] network 192.168.1.0
[SwitchA-rip-1] network 172.16.0.0
[SwitchA-rip-1] network 172.17.0.0
[SwitchA-rip-1] quit
```

② 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] rip
[SwitchB-rip-1] network 192.168.1.0
[SwitchB-rip-1] network 10.0.0.0
[SwitchB-rip-1] quit
```

③ 查看 Switch A 的 RIP 路由表。

```
[SwitchA] display rip 1 route
Route Flags: R - RIP, T - TRIP
             P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
----------------------------------------------------------------------------
Peer 192.168.1.2 on Vlan-interface100
     Destination/Mask    Nexthop         Cost   Tag    Flags    Sec
     10.0.0.0/8          192.168.1.2     1      0      RA       11
```

从路由表中可以看出，RIP-1 发布的路由信息使用的是自然掩码。

(3) 配置 RIP 的版本。

① 在 Switch A 上配置 RIP-2。

```
[SwitchA] rip
[SwitchA-rip-1] version 2
```

```
[SwitchA-rip-1] undo summary
```

② 在 Switch B 上配置 RIP-2。

```
[SwitchB] rip
[SwitchB-rip-1] version 2
[SwitchB-rip-1] undo summary
```

③ 查看 Switch A 的 RIP 路由表。

```
[SwitchA] display rip 1 route
Route Flags: R-RIP, T-TRIP
             P-Permanent, A-Aging, S-Suppressed, G-Garbage-collect
----------------------------------------------------------------------

 Peer 192.168.1.2 on Vlan-interface100
     Destination/Mask    Nexthop          Cost   Tag    Flags    Sec
     10.2.1.0/24         192.168.1.2      1      0      RA       16
     10.1.1.0/24         192.168.1.2      1      0      RA       16
```

从路由表中可以看出，RIP-2 发布的路由中带有更为精确的子网掩码信息。

提示：运行 RIP 协议的网络半径不宜过大，因为在比较大的网络中，RIP 路由的收敛速度会比较慢。RIP 动态路由协议的最大有效跳数为 15 跳，在更为大型的网络中一般使用 OSPF 路由协议进行部署。

8.2.2 RIP 引入外部路由典型配置指导

1. 背景

M 公司有若干办公区域，各办公区域规模都比较大，统一运行 RIP 协议会使网络收敛速度变得很慢，因此各区域内部各自运行 RIP 路由协议。由于各个区域业务互通的需要，一个区域的 RIP 路由必须发布给另一个区域，IT 维护人员通过将区域间 RIP 路由相互引入的方法实现这一需求。

2. 组网图

图 8-3 所示为 RIP 引入外部路由典型配置组网图。

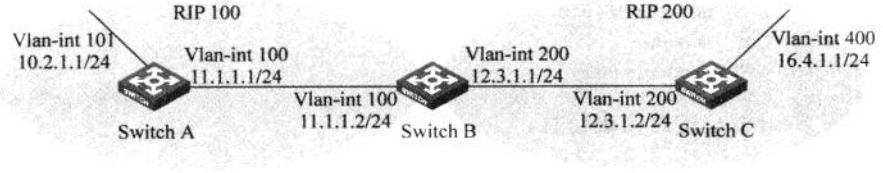


图 8-3 RIP 引入外部路由典型配置组网图

3. 配置需求

(1) Switch B 上运行两个 RIP 进程：RIP 100 和 RIP 200。Switch B 通过 RIP 100 和 Switch A 交换路由信息，通过 RIP 200 和 Switch C 交换路由信息。

(2) 在 Switch B 上配置 RIP 进程 200 引入外部路由，引入直连路由和 RIP 进程 100 的路由，使得 Switch C 能够学习到达 10.2.1.0/24 和 11.1.1.0/24 的路由，但 Switch A 不能学习到达 12.3.1.0/24 和 16.4.1.0/24 的路由。

(3) 在 Switch B 配置过滤策略，对引入的 RIP 100 的一条路由(10.2.1.1/24)进行过滤，使其不发布给 Switch C。

4. 配置过程和解释

(1) 配置各接口的 IP 地址(略)。

(2) 配置 RIP 基本功能。

① 在 Switch A 上启动 RIP 进程 100，并配置 RIP 版本号为 2。

```
<SwitchA> system-view
[SwitchA] rip 100
[SwitchA-rip-100] network 10.0.0.0
[SwitchA-rip-100] network 11.0.0.0
[SwitchA-rip-100] version 2
[SwitchA-rip-100] undo summary
[SwitchA-rip-100] quit
```

② 在 Switch B 上启动两个 RIP 进程，进程号分别为 100 和 200，并配置 RIP 版本号为 2。

```
<SwitchB> system-view
[SwitchB] rip 100
[SwitchB-rip-100] network 11.0.0.0
[SwitchB-rip-100] version 2
[SwitchB-rip-100] undo summary
[SwitchB-rip-100] quit
[SwitchB] rip 200
[SwitchB-rip-200] network 12.0.0.0
[SwitchB-rip-200] version 2
[SwitchB-rip-200] undo summary
[SwitchB-rip-200] quit
```

③ 在 Switch C 上启动 RIP 进程 200，并配置 RIP 版本号为 2。

```
<SwitchC> system-view
[SwitchC] rip 200
[SwitchC-rip-200] network 13.0.0.0
[SwitchC-rip-200] network 16.0.0.0
[SwitchC-rip-200] version 2
[SwitchC-rip-200] undo summary
```

④ 查看 Switch C 的路由表信息。

```
[SwitchC] display ip routing-table
Routing Tables: Public
         Destinations : 6        Routes : 6
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
12.3.1.0/24         Direct  0    0         12.3.1.2        Vlan200
12.3.1.2/32         Direct  0    0         127.0.0.1       InLoop0
16.4.1.0/24         Direct  0    0         16.4.1.1        Vlan400
16.4.1.1/32         Direct  0    0         127.0.0.1       InLoop0
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop0
```

(3) 配置 RIP 引入外部路由。

① 在 Switch B 配置 RIP 进程 200 引入外部路由，引入直连路由和 RIP 进程 100 的路由。

```
[SwitchB] rip 200
[SwitchB-rip-200] import-route rip 100
[SwitchB-rip-200] import-route direct
[SwitchB-rip-200] quit
```

② 查看路由引入后 Switch C 的路由表信息。

```
[SwitchC] display ip routing-table
Routing Tables: Public
         Destinations : 8        Routes : 8
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
10.2.1.0/24         RIP     100  1         12.3.1.1        Vlan200
11.1.1.0/24         RIP     100  1         12.3.1.1        Vlan200
12.3.1.0/24         Direct  0    0         12.3.1.2        Vlan200
12.3.1.2/32         Direct  0    0         127.0.0.1       InLoop0
16.4.1.0/24         Direct  0    0         16.4.1.1        Vlan400
16.4.1.1/32         Direct  0    0         127.0.0.1       InLoop0
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop0
```

(4) 配置 RIP 对引入的路由进行过滤。

① 在 Switch B 上配置 ACL，并对引入的 RIP 进程 100 的路由进行过滤，使其不发布给 Switch C。

```
[SwitchB] acl number 2000
[SwitchB-acl-basic-2000] rule deny source 10.2.1.1 0.0.0.255
[SwitchB-acl-basic-2000] rule permit
[SwitchB-acl-basic-2000] quit
[SwitchB] rip 200
[SwitchB-rip-100] filter-policy 2000 export rip 100
```

② 查看过滤后 Switch C 的路由表。

```
[SwitchC] display ip routing-table
Routing Tables: Public
         Destinations : 7        Routes : 7
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
11.1.1.0/24         RIP     100  1         12.3.1.1        Vlan200
12.3.1.0/24         Direct  0    0         12.3.1.2        Vlan200
12.3.1.2/32         Direct  0    0         127.0.0.1       InLoop0
16.4.1.0/24         Direct  0    0         16.4.1.1        Vlan400
16.4.1.1/32         Direct  0    0         127.0.0.1       InLoop0
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop0
```

提示：路由引入可以是双向的，上例中可以通过在 RIP 100 进程中引入 RIP 200 路由使 Switch A 上学习到 16.4.1.0/24 网段的路由。

8.2.3 RIP接口附加度量值典型配置指导

1. 背景

M公司主要是运行RIP协议搭建办公网络连通不同网段的办公区域，在网络部署过程中，IT维护人员发现由A区域到B区域有两条路径可达，其中一条路径较另一条更加稳定，因此维护人员通过更改接口附加度量值的方法使RIP路由优选稳定的路径进行数据转发。

2. 组网图

图8-4所示为RIP接口附加度量值典型配置组网图。

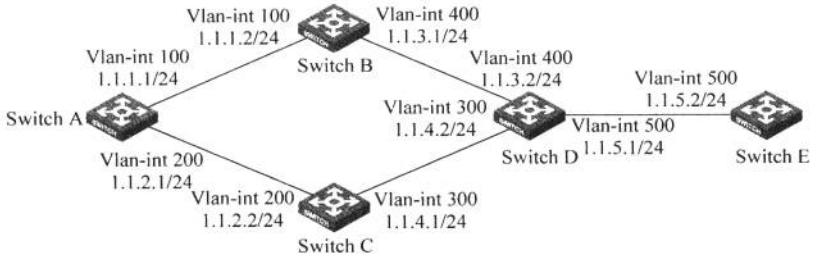


图8-4 RIP接口附加度量值典型配置组网图

3. 配置需求

(1) 在Switch A、Switch B、Switch C、Switch D和Switch E的所有接口上使能RIP，并使用RIP-2进行网络互连。

(2) Switch A有两条链路可以到达Switch D，其中，通过Switch B到达Switch D的链路比通过Switch C到达Switch D的链路更加稳定。通过在Switch A的Vlan-interface 200上配置接口接收RIP路由的附加度量值，使得Switch A优选从Switch B学到的1.1.5.0/24网段的路由。

4. 配置过程和解释

(1) 配置各接口的地址(略)。

(2) 配置RIP基本功能。

① 配置Switch A。

```
<SwitchA> system-view
[SwitchA] rip 1
[SwitchA-rip-1] network 1.0.0.0
[SwitchA-rip-1] version 2
[SwitchA-rip-1] undo summary
[SwitchA-rip-1] quit
```

② 配置Switch B。

```
<SwitchB> system-view
[SwitchB] rip 1
[SwitchB-rip-1] network 1.0.0.0
[SwitchB-rip-1] version 2
```

```
[SwitchB-rip-1] undo summary
```

③ 配置 Switch C。

```
<SwitchC> system-view
[SwitchB] rip 1
[SwitchC-rip-1] network 1.0.0.0
[SwitchC-rip-1] version 2
[SwitchC-rip-1] undo summary
```

④ 配置 Switch D。

```
<SwitchD> system-view
[SwitchD] rip 1
[SwitchD-rip-1] network 1.0.0.0
[SwitchD-rip-1] version 2
[SwitchD-rip-1] undo summary
```

⑤ 配置 Switch E。

```
<SwitchE> system-view
[SwitchE] rip 1
[SwitchE-rip-1] network 1.0.0.0
[SwitchE-rip-1] version 2
[SwitchE-rip-1] undo summary
```

⑥ 查看 Switch A 的 IP 路由表。

```
[SwitchA] display rip 1 database
  1.0.0.0/8, cost 0, ClassfulSumm
      1.1.1.0/24, cost 0, nexthop 1.1.1.1, Rip-interface
      1.1.2.0/24, cost 0, nexthop 1.1.2.1, Rip-interface
      1.1.3.0/24, cost 1, nexthop 1.1.1.2
      1.1.4.0/24, cost 1, nexthop 1.1.2.2
      1.1.5.0/24, cost 2, nexthop 1.1.1.2
      1.1.5.0/24, cost 2, nexthop 1.1.2.2
```

可以看到，到达网段 1.1.5.0/24 有两条 RIP 路由，下一跳分别是 Switch B(IP 地址为 1.1.1.2)和 Switch C(IP 地址为 1.1.2.2)，cost 值都是 2；到达网段 1.1.4.0/24 的下一跳是 Switch B，cost 为 1。

(3) 配置 RIP 接口附加度量值。在 Switch A 上配置接口 Vlan-interface 200 的接口附加度量值为 3。

```
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] rip metricin 3
[SwitchA-Vlan-interface200] display rip 1 database
  1.0.0.0/8, cost 0, ClassfulSumm
      1.1.1.0/24, cost 0, nexthop 1.1.1.1, Rip-interface
      1.1.2.0/24, cost 0, nexthop 1.1.2.1, Rip-interface
      1.1.3.0/24, cost 1, nexthop 1.1.1.2
      1.1.4.0/24, cost 2, nexthop 1.1.1.2
      1.1.5.0/24, cost 2, nexthop 1.1.1.2
```

可以看到，到达网段 1.1.5.0/24 的 RIP 路由仅有一条，下一跳是 Switch B(IP 地址为 1.1.1.2)，cost 值为 2。

提示：RIP 接口附加度量值分为接收附加度量值和发送附加度量值，其中接收附加度量值(默认值为 0)会影响本地路由器 RIP 路由的度量值，而发送附加度量值不影响本地 RIP 路由度量值，只是在发送给邻居的时候添加在原有的默认度量值上(默认发送度量值为 1)。

8.2.4 RIP 发布聚合路由典型配置指导

1. 背景

由于网络规模越来越大，M 公司办公网络中 RIP 路由的数目也迅速增加。IT 维护人员需要在满足网络连通的情况下尽量减少交换机上 RIP 路由的条目来确保路由条目不超过交换机的性能规格，使网络健康运行，因此维护人员选择在交换机上发布合理的 RIP 聚合路由来满足这一优化需求。

2. 组网图

图 8-5 所示为 RIP 发布聚合路由典型配置组网图。

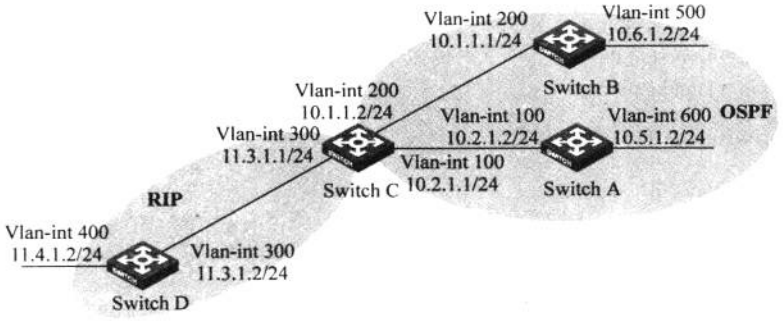


图 8-5 RIP 发布聚合路由典型配置组网图

3. 配置需求

(1) Switch A、Switch B 运行 OSPF，Switch D 运行 RIP，Switch C 同时运行 OSPF 和 RIP。

(2) 在 Switch C 上配置 RIP 进程引入 OSPF 路由，使 Switch D 有到达 10.1.1.0/24、10.2.1.0/24、10.5.1.0/24 和 10.6.1.0/24 网段的路由。

(3) 为了减小 Switch D 的路由表规模，在 Switch C 上配置路由聚合，只发布聚合后的路由 10.0.0.0/8。

4. 配置过程和解释

(1) 配置各接口的地址(略)。

(2) 配置 OSPF 基本功能。

① 配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ospf
```

```
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.5.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
```

② 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 10.6.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
```

③ 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
```

(3) 配置 RIP 基本功能。

① 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] rip 1
[SwitchC-rip-1] network 11.3.1.0
[SwitchC-rip-1] version 2
[SwitchC-rip-1] undo summary
```

② 配置 Switch D。

```
<SwitchD> system-view
[SwitchD] rip 1
[SwitchD-rip-1] network 11.0.0.0
[SwitchD-rip-1] version 2
[SwitchD-rip-1] undo summary
[SwitchD-rip-1] quit
```

③ 在 Switch C 上配置 RIP 引入外部路由，引入 OSPF 进程 1 的路由和直连路由。

```
[SwitchC-rip-1] import-route direct
[SwitchC-rip-1] import-route ospf 1
```

④ 查看 Switch D 的路由表信息。

```
[SwitchD] display ip routing-table
Routing Tables: Public
         Destinations : 10       Routes : 10
Destination/Mask    Proto   Pre  Cost        NextHop         Interface
```

10.1.1.0/24	RIP	100	1	11.3.1.1	Vlan300
10.2.1.0/24	RIP	100	1	11.3.1.1	Vlan300
10.5.1.0/24	RIP	100	1	11.3.1.1	Vlan300
10.6.1.0/24	RIP	100	1	11.3.1.1	Vlan300
11.3.1.0/24	Direct	0	0	11.3.1.2	Vlan300
11.3.1.2/32	Direct	0	0	127.0.0.1	InLoop0
11.4.1.0/24	Direct	0	0	11.4.1.2	Vlan400
11.4.1.2/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

(4) 在 Switch C 上配置路由聚合，只发布聚合路由 10.0.0.0/8。

```
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] rip summary-address 10.0.0.0 8
```

查看 Switch D 的路由表信息：

```
[SwitchD] display ip routing-table
Routing Tables: Public
         Destinations : 7        Routes : 7
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.0.0.0/8	RIP	100	1	11.3.1.1	Vlan300
11.3.1.0/24	Direct	0	0	11.3.1.2	Vlan300
11.3.1.2/32	Direct	0	0	127.0.0.1	InLoop0
11.4.1.0/24	Direct	0	0	11.4.1.2	Vlan400
11.4.1.2/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

提示：将多条 RIP 路由聚合成为一条聚合路由后，聚合路由的 metric 值将取所有普通路由中的最小值。

8.3 OSPF 协议典型配置指导

8.3.1 OSPF 基本功能典型配置指导

OSPF(Open Shortest Path First，开放最短路径优先)是 IETF 组织开发的一个基于链路状态的内部网关协议。目前针对 IPv4 协议使用的是 OSPF Version 2(RFC 2328)。

OSPF 具有适应范围广、快速收敛、无自环、区域划分、等价路由、路由分级、支持验证、组播发送等特点。

1. 背景

2006 年，M 公司经过多年快速发展，已经成长为几千人的大公司了。公司的部门分布在各个办公楼内，之间用三层交换机互连。由于网络规模较大，原有的 RIP 协议不再适用，主要体现为收敛时间有些长。为了能够适应网络规模大、网络快速收敛的需求，IT 维护人员最终决定采用 OSPF 协议部署办公楼间路由。

2. 组网图

图 8-6 所示为 OSPF 基本功能典型配置组网图。

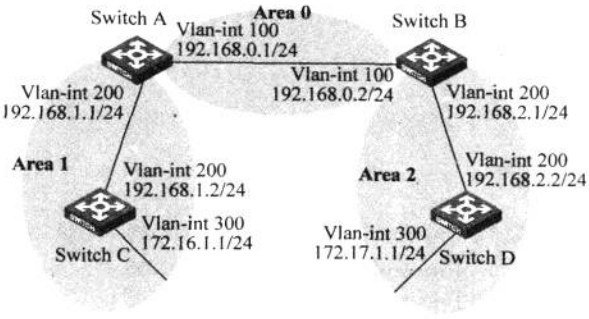


图 8-6 OSPF 基本功能典型配置组网图

3. 配置需求

(1) 所有的交换机都运行 OSPF,并将整个自治系统划分为 3 个区域。

(2) 其中 Switch A 和 Switch B 作为 ABR 来转发区域之间的路由。

(3) 配置完成后,每台交换机都应学到 AS 内的到所有网段的路由。

4. 配置过程和解释

(1) 配置各接口的 IP 地址(略)。

(2) 配置 OSPF 基本功能。

① 配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

② 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] area 2
[SwitchB-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.2] quit
[SwitchB-ospf-1] quit
```

③ 配置 Switch C。

```
<SwitchC> system-view
```

```
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] network 172.16.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

④ 配置 Switch D。

```
<SwitchD> system-view
[SwitchD] ospf
[SwitchD-ospf-1] area 2
[SwitchD-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] network 172.17.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] quit
[SwitchD-ospf-1] quit
```

(3) 检验配置结果。

① 查看 Switch A 的 OSPF 邻居。

```
[SwitchA] display ospf peer verbose
          OSPF Process 1 with Router ID 192.168.0.1
                    Neighbors
 Area 0.0.0.0 interface 192.168.0.1(Vlan-interface 100)'s neighbors
 Router ID: 192.168.0.2       Address: 192.168.0.2         GR State: Normal
   State: Full  Mode:Nbr is Master  Priority: 1
   DR: 192.168.0.2  BDR: 192.168.0.1  MTU: 0
   Dead timer due in 36 sec
   Neighbor is up for 00:15:04
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 3
                    Neighbors
Area 0.0.0.1 interface 192.168.1.1(Vlan-interface 200)'s neighbors
Router ID: 192.168.1.2       Address: 192.168.1.2         GR State: Normal
   State: Full  Mode:Nbr is Slave  Priority: 1
   DR: 192.168.1.2  BDR: 192.168.1.1  MTU: 0
   Dead timer due in 39 sec
   Neighbor is up for 00:07:32
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 2
```

② 显示 Switch A 的 OSPF 路由信息。

```
[SwitchA] display ospf routing
          OSPF Process 1 with Router ID 192.168.0.1
                    Routing Tables
 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 172.16.1.0/24      1563  Stub       192.168.1.2     172.16.1.1      0.0.0.1
 172.17.1.0/24      3125  Inter-area 192.168.0.2     192.168.2.1     0.0.0.0
 192.168.1.0/24     1562  Stub       192.168.1.1     192.168.0.1     0.0.0.1
 192.168.2.0/24     3124  Inter-area 192.168.0.2     192.168.2.1     0.0.0.0
```

```
192.168.0.0/24      1562   Stub          192.168.0.1      192.168.0.1      0.0.0.0
Total Nets: 5
Intra Area: 3  Inter Area: 2  ASE: 0  NSSA: 0
```

③ 显示 Switch A 的 LSDB。

```
[SwitchA] display ospf lsdb
          OSPF Process 1 with Router ID 192.168.0.1
                Link State Data Base
                      Area: 0.0.0.0
Type       LinkState ID     AdvRouter        Age  Len  Sequence    Metric
Router     192.168.2.1      192.168.2.1      874  48   80000006    1562
Router     192.168.0.1      192.168.0.1      976  48   80000005    1562
Sum-Net    192.168.1.0      192.168.0.1      630  28   80000001    1562
Sum-Net    172.17.1.0       192.168.2.1      411  28   80000001    1563
Sum-Net    192.168.2.0      192.168.2.1      429  28   80000001    1562
Sum-Net    172.16.1.0       192.168.0.1      565  28   80000001    1563
                      Area: 0.0.0.1
Type       LinkState ID     AdvRouter        Age  Len  Sequence    Metric
Router     192.168.1.2      192.168.1.2      964  48   80000003    1562
Router     192.168.0.1      192.168.0.1      590  48   80000002    1562
Router     172.16.1.1       172.16.1.1       526  60   80000005    1562
Sum-Net    172.17.1.0       192.168.0.1      410  28   80000001    3125
Sum-Net    192.168.2.0      192.168.0.1      428  28   80000001    3124
Sum-Net    192.168.0.0      192.168.0.1      630  28   80000001    1562
```

④ 查看 Switch D 的路由表。

```
[SwitchD] display ospf routing
          OSPF Process 1 with Router ID 192.168.2.2
                Routing Tables
Routing for Network
Destination        Cost   Type        NextHop          AdvRouter        Area
172.16.1.0/24      4687   Inter-area  192.168.2.1      192.168.2.1      0.0.0.2
172.17.1.0/24      1      Stub        172.17.1.1       192.168.2.2      0.0.0.2
192.168.1.0/24     4686   Inter-area  192.168.2.1      192.168.2.1      0.0.0.2
192.168.2.0/24     1562   Stub        192.168.2.2      192.168.2.2      0.0.0.2
192.168.0.0/24     3124   Inter-area  192.168.2.1      192.168.2.1      0.0.0.2
Total Nets: 5
Intra Area: 2  Inter Area: 3  ASE: 0  NSSA: 0
```

⑤ 使用 ping 测试连通性。

```
[SwitchD] ping 172.16.1.1
  PING 172.16.1.1: 56 data bytes, press Ctrl_C to break
    Reply from 172.16.1.1: bytes=56 Sequence=1 ttl=253 time=62 ms
    Reply from 172.16.1.1: bytes=56 Sequence=2 ttl=253 time=16 ms
    Reply from 172.16.1.1: bytes=56 Sequence=3 ttl=253 time=62 ms
    Reply from 172.16.1.1: bytes=56 Sequence=4 ttl=253 time=94 ms
    Reply from 172.16.1.1: bytes=56 Sequence=5 ttl=253 time=63 ms
  --- 172.16.1.1 ping statistics ---
```

```
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 16/59/94 ms
```

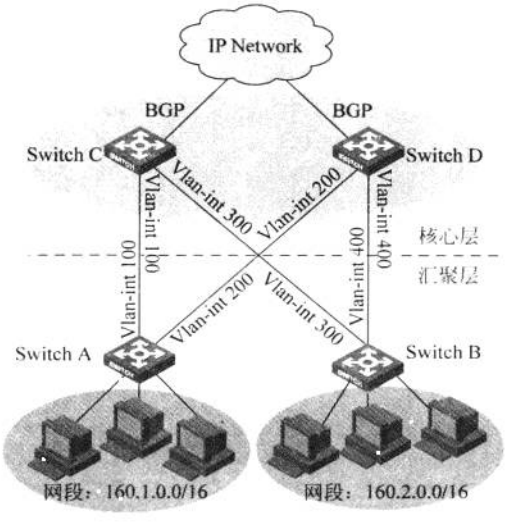
8.3.2 OSPF 应用典型配置指导

1. 背景

为了提高公司网络的可扩展性、可用性，M 公司决定对网络进行重新规划，将原来的扁平化网络改成核心—汇聚—接入架构的分层网络。各分支机构为接入层，通过总部网络访问外网。总部网络分为核心层与汇聚层，汇聚层设备通过部署 OSPF 动态路由协议连接核心层以及各个分支，通过 OSPF 将分支路由发布给核心层设备；核心层采用 BGP 协议获取外部网络路由。

2. 组网图

图 8-7 所示为 OSPF 应用典型配置组网图。



设　备	接　口	IP 地址	设　备	接　口	IP 地址
Switch A	Vlan-int 100	10.1.1.1/24	Switch C	Vlan-int 100	10.1.1.2/24
	Vlan-int 200	10.1.2.1/24		Vlan-int 300	10.1.3.2/24
Switch B	Vlan-int 300	10.1.3.1/24	Switch D	Vlan-int 200	10.1.2.2/24
	Vlan-int 400	10.1.4.1/24		Vlan-int 400	10.1.4.2/24

图 8-7　OSPF 应用典型配置组网图

3. 配置需求

各分支网络通过核心网与外部网络连接。该核心网由 4 台核心交换机组成，其中两台交换机作为汇聚层设备分别连接各分支网络。两台交换机均为双上行（提供冗余备份链路），上连两台核心交换机，负责连接外部网络。实现以下访问需求。

(1) 汇聚层和核心层交换机之间均采用三层互连,使用 OSPF 路由协议,且均属于区域 0。

(2) 在汇聚层设备上将去往分支网络的聚合路由(与 Switch A 上下连分支网络均属于 160.1.0.0/16 网段,与 Switch B 上下连分支网络均属于 160.2.0.0/16 网段)发布到 OSPF 网络,让两台核心层设备能够通过 OSPF 学习到去往分支网络的路由。

(3) 在核心层交换机上通过 BGP 学习路由,并将 BGP 学到的路由重新注入 OSPF 网络,最终达到在两台汇聚层交换机上去往外网的路由形成两条等价路由。

4. 配置过程和解释

本配置举例仅列出与 OSPF 相关内容,有关 BGP 路由学习和引入的内容请参见 BGP 部分。

(1) 配置接口的 IP 地址(略)。

(2) 配置 OSPF。

① 配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

② 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.4.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
```

③ 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

④ 配置 Switch D。

```
<SwitchD> system-view
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 10.1.4.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

⑤ 查看 Switch A 的路由表信息(假定 Switch A 下连 3 个分支网络)。

```
[SwitchA] display ip routing-table
Routing Tables: Public
         Destinations : 14        Routes : 14
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
10.1.1.0/24         Direct  0    0         10.1.1.1        Vlan100
10.1.1.1/32         Direct  0    0         127.0.0.1       InLoop0
10.1.2.0/24         Direct  0    0         10.1.2.1        Vlan200
10.1.2.1/32         Direct  0    0         127.0.0.1       InLoop0
10.1.3.0/24         OSPF    10   2         10.1.1.2        Vlan100
10.1.4.0/24         OSPF    10   2         10.1.2.2        Vlan200
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop0
160.1.1.0/24        Direct  0    0         160.1.1.1       Vlan1
160.1.1.1/32        Direct  0    0         127.0.0.1       InLoop0
160.1.2.0/24        Direct  0    0         160.1.2.1       Vlan2
160.1.2.1/32        Direct  0    0         127.0.0.1       InLoop0
160.1.3.0/24        Direct  0    0         160.1.3.1       Vlan3
160.1.3.1/32        Direct  0    0         127.0.0.1       InLoop0
```

(3) 配置路由引入。

① 在 Switch A 上配置 OSPF 引入直连路由(一部分分支网络与 Switch A 直连),只发布聚合路由 160.1.0.0/16。

```
[SwitchA] ospf
[SwitchA-ospf-1] import-route direct
[SwitchA-ospf-1] asbr-summary 160.1.0.0 16
```

② 在 Switch B 上配置 OSPF 引入直连路由(另一部分各分支网络与 Switch B 直连),只发布聚合路由 160.2.0.0/16。

```
[SwitchB] ospf
[SwitchB-ospf-1] import-route direct
[SwitchB-ospf-1] asbr-summary 160.2.0.0 16
```

③ 在 Switch C 上配置 OSPF 引入 BGP 路由。

```
[SwitchC] ospf
[SwitchC-ospf-1] import-route bgp
```

④ 在 Switch D 上配置 OSPF 引入 BGP 路由。

```
[SwitchD] ospf
[SwitchD-ospf-1] import-route bgp
```

8.3.3 OSPF 发布聚合路由典型配置指导

1. 背景

M 公司在北京和上海各建有一个测试中心,由于测试业务的特殊性,两个测试中心间

需要搭建独立于办公网络之外的网络。IT 维护部门使用 BGP 连接两地测试中心，测试中心内部网络全部使用 OSPF 进行部署。由于上海测试中心下网段较多，如果将 OSPF 路由全部发布给北京，北京测试中心的路由数量有可能超出规格，因此 IT 维护人员先将上海中心的 OSPF 路由进行聚合，然后将聚合路由发布给北京，达到精简北京测试中心总部交换机上路由条目的目的。

2. 组网图

图 8-8 所示为 OSPF 发布聚合路由典型配置组网图。

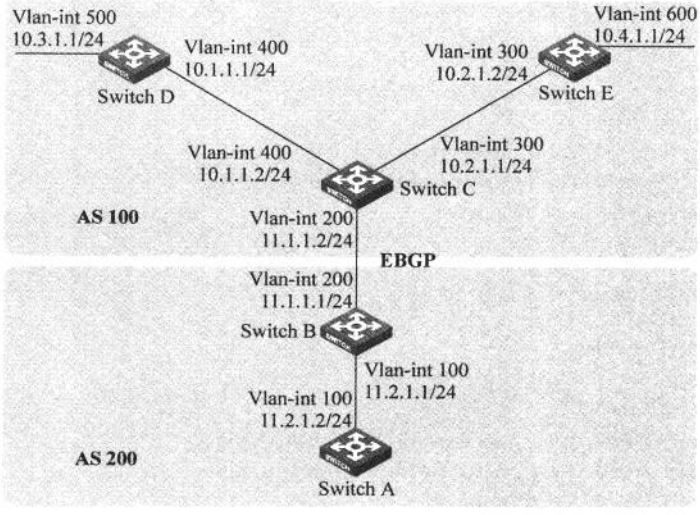


图 8-8 OSPF 发布聚合路由典型配置组网图

3. 配置需求

(1) Switch A 和 Switch B 位于 AS 200 内，AS 200 内使用 OSPF 作为 IGP 协议。

(2) Switch C、Switch D 和 Switch E 位于 AS 100 内，AS 100 内使用 OSPF 作为 IGP 协议。

(3) Switch B 和 Switch C 之间建立 EBGP 连接，在 Switch C 上配置 BGP 引入 OSPF 路由。

(4) 在 Switch B 上配置 OSPF 进程引入 BGP 路由，为了减小 Switch A 的路由表规模，在 Switch B 上配置路由聚合，只发布聚合后的路由 10.0.0.0/8。

4. 配置过程和解释

(1) 配置接口的 IP 地址(略)。

(2) 配置 OSPF。

① 配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 11.2.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
```

```
[SwitchA-ospf-1] quit
```

② 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 11.2.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
```

③ 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

④ 配置 Switch D。

```
<SwitchD> system-view
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
```

⑤ 配置 Switch E。

```
<SwitchE> system-view
[SwitchE] ospf
[SwitchE-ospf-1] area 0
[SwitchE-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[SwitchE-ospf-1-area-0.0.0.0] network 10.4.1.0 0.0.0.255
[SwitchE-ospf-1-area-0.0.0.0] quit
[SwitchE-ospf-1] quit
```

(3) 配置 BGP。

① 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] bgp 200
[SwitchB-bgp] peer 11.1.1.2 as-number 100
[SwitchB-bgp] quit
```

② 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] bgp 100
[SwitchC-bgp] peer 11.1.1.1 as-number 200
[SwitchC-bgp] import-route ospf
```

(4) 在 Switch B 上配置路由引入。

① 在 Switch B 上配置 OSPF 引入 BGP 路由。

```
[SwitchB] ospf
[SwitchB-ospf-1] import-route bgp
```

② 查看 Switch A 的路由表信息。

```
[SwitchA] display ip routing-table
Routing Tables: Public
         Destinations : 8        Routes : 8
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
10.1.1.0/24         O_ASE   150  1         11.2.1.1        Vlan100
10.2.1.0/24         O_ASE   150  1         11.2.1.1        Vlan100
10.3.1.0/24         O_ASE   150  1         11.2.1.1        Vlan100
10.4.1.0/24         O_ASE   150  1         11.2.1.1        Vlan100
11.2.1.0/24         Direct  0    0         11.2.1.2        Vlan100
11.2.1.2/32         Direct  0    0         127.0.0.1       InLoop0
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop0
```

(5) 在 Switch B 上配置路由聚合，只发布聚合路由 10.0.0.0/8。

```
[SwitchB-ospf-1] asbr-summary 10.0.0.0 8
```

查看 Switch A 的路由表信息：

```
[SwitchA] display ip routing-table
Routing Tables: Public
         Destinations : 5        Routes : 5
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
10.0.0.0/8          O_ASE   150  2         11.2.1.1        Vlan100
11.2.1.0/24         Direct  0    0         11.2.1.2        Vlan100
11.2.1.2/32         Direct  0    0         127.0.0.1       InLoop0
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop0
```

8.3.4 OSPF 的 Stub 区域典型配置指导

OSPF 划分区域后，可以减少网络中 LSA 的数量，OSPF 的扩展性也得以增强。对于位于 AS 边缘的一些非骨干区域，为了更多地缩减其路由表规模和降低 LSA 的数量，可以将它们配置为 Stub 区域。

1. 背景

M 公司北京测试中心内部网络采用 OSPF 路由部署，IT 维护部门在部署网络的过程中发现，测试中心下的大部分部门所处的 OSPF 区域中并没有 ASBR 的存在，即未在该部门所在区域中引入外部路由。类似这样的区域交换机上的路由条目可以做合理的精简。因此，IT 维护人员通过将该部门的 OSPF 区域配置成为 Stub 区域来精简该部门交换机上的路由数目。

2. 组网图

图 8-9 所示为 OSPF 的 Stub 区域典型配置组网图。

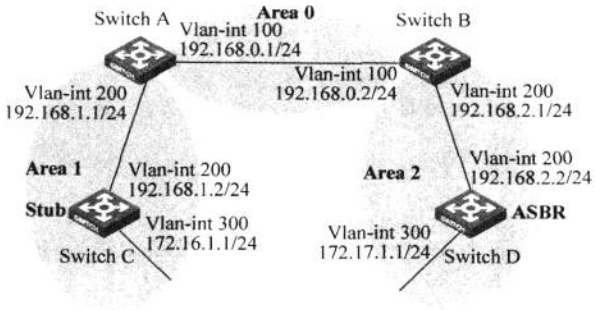


图 8-9 OSPF 的 Stub 区域典型配置组网图

3. 配置需求

(1) 所有的交换机都运行 OSPF，整个自治系统划分为 3 个区域。

(2) 其中 Switch A 和 Switch B 作为 ABR 来转发区域之间的路由，Switch D 作为 ASBR 引入了外部路由(静态路由)。

(3) 要求将 Area 1 配置为 Stub 区域，减少通告到此区域内的 LSA 数量，但不影响路由的可达性。

4. 配置过程和解释

(1) 配置接口的 IP 地址(略)。

(2) 配置 OSPF(同前例 8.3.3)。

(3) 配置 Switch D 引入静态路由。

```
[SwitchD] ip route-static 200.0.0.0 8 null 0
[SwitchD] ospf
[SwitchD-ospf-1] import-route static
[SwitchD-ospf-1] quit
```

① 查看 Switch C 的 ABR/ASBR 信息。

```
[SwitchC] display ospf abr-asbr
          OSPF Process 1 with Router ID 172.16.1.1
                    Routing Table to ABR and ASBR
 Type        Destination     Area        Cost   Nexthop         RtType
 Intra-area  192.168.0.1     0.0.0.1     1562   192.168.1.1     ABR
 Inter-area  172.17.1.1      0.0.0.1     4686   192.168.1.1     ASBR
```

② 查看 Switch C 的 OSPF 路由表。

```
[SwitchC] display ospf routing
          OSPF Process 1 with Router ID 172.16.1.1
                    Routing Tables
 Routing for Network
 Destination          Cost    Type        NextHop         AdvRouter       Area
```

172.16.1.0/24	1	Stub	172.16.1.1	172.16.1.1	0.0.0.1
172.17.1.0/24	4687	Inter-area	192.168.1.1	192.168.0.1	0.0.0.1
192.168.1.0/24	1562	Stub	192.168.1.2	172.16.1.1	0.0.0.1
192.168.2.0/24	4686	Inter-area	192.168.1.1	192.168.0.1	0.0.0.1
192.168.0.0/24	3124	Inter-area	192.168.1.1	192.168.0.1	0.0.0.1

Routing for ASEs

Destination	Cost	Type	Tag	NextHop	AdvRouter
200.0.0.0/8	10	Type2	1	192.168.1.1	172.17.1.1

Routing for NSSAs

Destination	Cost	Type	Tag	NextHop	AdvRouter

Total Nets: 6
Intra Area: 2 Inter Area: 3 ASE: 1 NSSA: 0

提示：当 Switch C 所在区域为普通区域时，可以看到路由表中存在 AS 外部路由。

(4) 配置 Area 1 为 Stub 区域。

① 配置 Switch A。

```
[SwitchA] ospf
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] stub
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

② 配置 Switch C。

```
[SwitchC] ospf
[SwitchC-ospf-1] stub-router
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] stub
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

③ 显示 Switch C 的 OSPF 路由表。

```
[SwitchC] display ospf routing
          OSPF Process 1 with Router ID 172.16.1.1
                Routing Tables
```

Routing for Network

Destination	Cost	Type	NextHop	AdvRouter	Area
0.0.0.0/0	65536	Inter-area	192.168.1.1	192.168.0.1	0.0.0.1
172.16.1.0/24	1	Stub	172.16.1.1	172.16.1.1	0.0.0.1
172.17.1.0/24	68660	Inter-area	192.168.1.1	192.168.0.1	0.0.0.1
192.168.1.0/24	1562	Stub	192.168.1.2	172.16.1.1	0.0.0.1
192.168.2.0/24	68659	Inter-area	192.168.1.1	192.168.0.1	0.0.0.1
192.168.0.0/24	67097	Inter-area	192.168.1.1	192.168.0.1	0.0.0.1

Total Nets: 6
Intra Area: 2 Inter Area: 4 ASE: 0 NSSA: 0

提示：Stub 区域不允许其他区域引入的 O_ASE LSA 进入，当将 Area 1 配置成为 Stub 区域后，Switch 上已经看不到 AS 外部路由，取而代之的是一条默认路由。

④ 配置禁止向 Stub 区域通告 Type 3 LSA。

```
[SwitchA] ospf
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] stub no-summary
[SwitchA-ospf-1-area-0.0.0.1] quit
```

⑤ 查看 Switch C 的 OSPF 路由表。

```
[SwitchC] display ospf routing
          OSPF Process 1 with Router ID 172.16.1.1
                    Routing Tables
 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 0.0.0.0/0          1563  Inter-area 192.168.1.1     192.168.0.1     0.0.0.1
 172.16.1.0/24      1     Stub       172.16.1.1      172.16.1.1      0.0.0.1
 192.168.1.0/24     1562  Stub       192.168.1.2     172.16.1.1      0.0.0.1
 Total Nets: 3
 Intra Area: 2  Inter Area: 1  ASE: 0  NSSA: 0
```

提示：所有连接到 Stub 区域的路由器必须使用 stub 命令将该区域配置成 Stub 属性。骨干区域不能配置成 Stub 区域。

Stub 区域内不能存在 ASBR，即自治系统外部的路由不能在本区域内传播。

虚连接不能穿过 Stub 区域。

stub no-summary 命令仅能用于 ABR 上，用于禁止 ABR 向 Stub 区域内发布 3 类 LSA。配置该命令后，Stub 区域成为 Totally Stub 区域，区域内的路由表项进一步减少，只留下默认路由和少量区域内路由。

8.3.5 OSPF 的 NSSA 区域典型配置指导

Stub 区域不能引入外部路由，为此又产生了 NSSA 区域的概念。NSSA 区域中允许 Type 7 LSA(NSSA External LSA)的传播。Type 7 LSA 由 NSSA 区域的 ASBR 产生，当它到达 NSSA 区域的 ABR 时，就会转换成 Type 5 LSA(AS External LSA)，并通告到其他区域。

1. 背景

M 公司北京测试中心内部网络采用 OSPF 动态路由协议进行部署，IT 维护部门在部署过程中发现部分下属部门所处区域可以通过配置成为 NSSA 区域，以达到既精简区域内路由表，又可以通过 NSSA 区域引入 7 类的外部路由的作用。

2. 组网图

图 8-10 所示为 OSPF 的 NSSA 区域典型配置组网图。

3. 配置需求

(1) 所有的交换机都运行 OSPF，整个自治系统划分为 3 个区域。

(2) 其中 Switch A 和 Switch B 作为 ABR 来转发区域之间的路由，Switch D 作为 ASBR 引入了外部路由(静态路由)。

(3) 要求将 Area 1 配置为 NSSA 区域，同时将 Switch C 配置为 ASBR 引入外部路由(静态路由)，且路由信息可正确地在 AS 内传播。

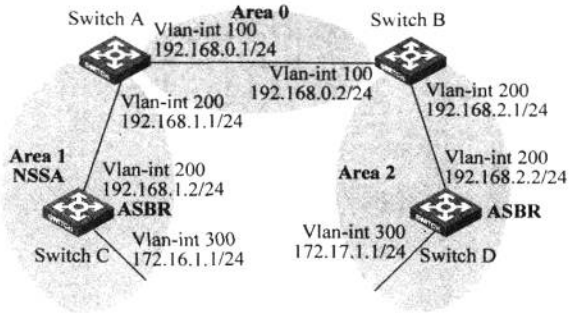


图 8-10 OSPF 的 NSSA 区域典型配置组网图

4. 配置过程和解释

(1) 配置各接口的 IP 地址(略)。

(2) 配置 OSPF(略)。

(3) 配置 Switch D 引入静态路由(略)。

(4) 配置 Area 1 区域为 NSSA 区域。

① 配置 Switch A。

```
[SwitchA] ospf
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] nssa default-route-advertise no-summary
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

② 配置 Switch C。

```
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] nssa
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

提示：nssa default-route-advertise 可以使用在 NSSA 区域的 ABR 或者 ASBR 上，在 ABR 上使用时不论 ABR 上是否存在默认路由，ABR 均会向 NSSA 区域内发布一条 Type 7-LSA 的默认路由；在 ASBR 上使用时，只有 ASBR 上存在默认路由 ASBR 才会向 NSSA 区域内发布一条 Type 7-LSA 默认路由。

nssa no-summary 命令只能使用在 NSSA ABR 路由器上，配置该命令后 NSSA 区域成为 Totally NSSA 区域，ABR 只向 NSSA 区域内部发布一条 Type 3-LSA 默认路由，不再发布其他任何 3 类 LSA。

③ 查看 Switch C 的 OSPF 路由表。

```
[SwitchC] display ospf routing
          OSPF Process 1 with Router ID 172.16.1.1
                    Routing Tables
 Routing for Network
```

```
Destination        Cost   Type        NextHop        AdvRouter      Area
0.0.0.0/0          1563   Inter-area  192.168.1.1    192.168.0.1    0.0.0.1
172.16.1.0/24      1      Stub        172.16.1.1     172.16.1.1     0.0.0.1
192.168.1.0/24     1562   Stub        192.168.1.2    172.16.1.1     0.0.0.1
Total Nets: 3
Intra Area: 2  Inter Area: 1  ASE: 0  NSSA: 0
```

(5) 配置 Switch C 引入静态路由。

```
[SwitchC] ip route-static 100.0.0.0 8 null 0
[SwitchC] ospf
[SwitchC-ospf-1] import-route static
[SwitchC-ospf-1] quit
```

查看 Switch D 的 OSPF 路由表：

```
[SwitchD-ospf-1] display ospf routing
          OSPF Process 1 with Router ID 172.17.1.1
                  Routing Tables
Routing for Network
Destination        Cost   Type        NextHop        AdvRouter      Area
172.16.1.0/24      4687   Inter-area  192.168.2.1    192.168.0.2    0.0.0.2
172.17.1.0/24      1      Stub        172.17.1.1     172.17.1.1     0.0.0.2
192.168.1.0/24     4686   Inter-area  192.168.2.1    192.168.0.2    0.0.0.2
192.168.2.0/24     1562   Stub        192.168.2.2    172.17.1.1     0.0.0.2
192.168.0.0/24     3124   Inter-area  192.168.2.1    192.168.0.2    0.0.0.2
Routing for ASEs
Destination        Cost     Type       Tag         NextHop        AdvRouter
100.0.0.0/8        10       Type2      1           192.168.2.1    192.168.0.1
Routing for NSSAs
Destination        Cost     Type       Tag         NextHop        AdvRouter
Total Nets: 6
Intra Area: 2  Inter Area: 3  ASE: 1  NSSA: 0
```

提示： 所有连接到 NSSA 区域的路由器必须使用 nssa 命令将该区域配置成 NSSA 属性。

8.3.6 OSPF 的 DR 选择典型配置指导

在广播网和 NBMA 网络中，任意两台路由器之间都要交换路由信息。如果网络中有 n 台路由器，则需要建立 $n(n-1)/2$ 个邻接关系。这使得任何一台路由器的路由变化都会导致多次传递，浪费了带宽资源。为解决这一问题，OSPF 协议定义了指定路由器 DR (Designated Router)，所有路由器都只将信息发送给 DR，由 DR 将网络链路状态发送出去。

如果 DR 由于某种故障而失效，则网络中的路由器必须重新选举 DR，再与新的 DR 同步。这需要较长的时间，在这段时间内，路由的计算是不正确的。为了能够缩短这个过程，OSPF 提出了 BDR(Backup Designated Router，备份指定路由器)的概念。

BDR 实际上是对 DR 的一个备份，在选举 DR 的同时也选举出 BDR，BDR 也和本网段内的所有路由器建立邻接关系并交换路由信息。当 DR 失效后，BDR 会立即成为 DR。由于不需要重新选举，并且邻接关系事先已建立，所以这个过程是非常短暂的。当然这时还需要再重新选举出一个新的 BDR，虽然一样需要较长的时间，但并不会影响路由的计算。

运行 OSPF 进程的网络中，既不是 DR 也不是 BDR 的路由器为 DR Other。DR Other 仅与 DR 和 BDR 之间建立邻接关系。DR Other 之间不交换任何路由信息，这样就减少了广播网和 NBMA 网络上各路由器之间邻接关系的数量，同时减少网络流量，节约了带宽资源。

1. 背景

M 公司的北京测试中心采用 H3C 以太网交换机部署 OSPF 路由协议的方式互连各个部门，网络中的 OSPF 交换机大多工作在广播网络环境中。随着部门的不断增多，OSPF 交换机数量也在不断地增多，此时 IT 维护人员发现，在广播网络环境下 OSPF 交换机在同一网段上会选择 DR 与 BDR 来达到节约网络资源的目的。但是由于选择没有人为因素干预，因此选择出的 DR 和 BDR 通常不是网段上性能最佳的交换机，这可能会对性能一般的交换机造成一定的影响。因此，IT 维护人员通过对于 DR、BDR 选举参数的配置，达到由管理员控制 DR、BDR 选择的目的，使网络资源分配更加合理。

2. 组网图

图 8-11 所示为 OSPF 的 DR 选择典型配置组网图。

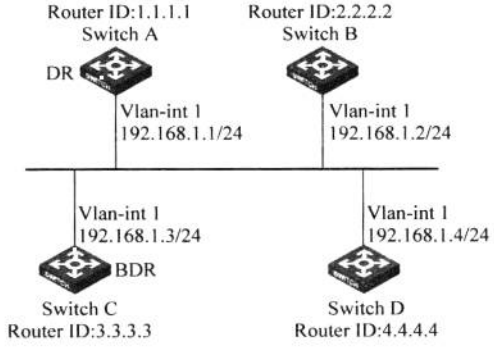


图 8-11 OSPF 的 DR 选择典型配置组网图

3. 配置需求

(1) Switch A、Switch B、Switch C、Switch D 在同一网段，运行 OSPF 协议。

(2) 配置 Switch A 为 DR，Switch C 为 BDR。

4. 配置过程和解释

(1) 配置各接口的 IP 地址(略)。

(2) 配置 OSPF 基本功能。

① 配置 Switch A，启动 OSPF，并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] router id 1.1.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

② 配置 Switch B，启动 OSPF，并设置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] router id 2.2.2.2
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

③ 配置 Switch C，启动 OSPF，并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
[SwitchC] router id 3.3.3.3
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

④ 配置 Switch D，启动 OSPF，并设置其 Router ID 为 4.4.4.4。

```
<SwitchD> system-view
[SwitchD] router id 4.4.4.4
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

⑤ 查看 Switch A 的邻居信息。

```
[SwitchA] display ospf peer verbose
          OSPF Process 1 with Router ID 1.1.1.1
                    Neighbors
 Area 0.0.0.0 interface 192.168.1.1(Vlan-interface1)'s neighbors
 Router ID: 2.2.2.2          Address: 192.168.1.2      GR State: Normal
   State: 2-Way  Mode: None  Priority: 1
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 38 sec
   Neighbor is up for 00:01:31
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 2

 Router ID: 3.3.3.3          Address: 192.168.1.3      GR State: Normal
   State: Full  Mode: Nbr is Master  Priority: 1
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 31 sec
   Neighbor is up for 00:01:28
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 2

 Router ID: 4.4.4.4          Address: 192.168.1.4      GR State: Normal
   State: Full  Mode: Nbr is Master  Priority: 1
```

```
  DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
  Dead timer due in 31 sec
  Neighbor is up for 00:01:28
  Authentication Sequence: [ 0 ]
  Neighbor state change count: 2
```

可以看到，Switch D 为 DR，Switch C 为 BDR。

(3) 配置接口上的路由器优先级。

① 配置 Switch A。

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ospf dr-priority 100
[SwitchA-Vlan-interface1] quit
```

② 配置 Switch B。

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ospf dr-priority 0
[SwitchB-Vlan-interface1] quit
```

③ 配置 Switch C。

```
[SwitchC] interface vlan-interface 1
[SwitchC-Vlan-interface1] ospf dr-priority 2
[SwitchC-Vlan-interface] quit
```

④ 查看 Switch D 的邻居信息。

```
[SwitchD] display ospf peer verbose
          OSPF Process 1 with Router ID 4.4.4.4
                    Neighbors
 Area 0.0.0.0 interface 192.168.1.4(Vlan-interface1)'s neighbors
 Router ID: 1.1.1.1          Address: 192.168.1.1        GR State: Normal
   State: Full  Mode:Nbr is Slave  Priority: 100
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 31 sec
   Neighbor is up for 00:11:17
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 3

 Router ID: 2.2.2.2          Address: 192.168.1.2        GR State: Normal
   State: Full  Mode:Nbr is Slave  Priority: 0
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 35 sec
   Neighbor is up for 00:11:19
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 3

 Router ID: 3.3.3.3          Address: 192.168.1.3        GR State: Normal
   State: Full  Mode:Nbr is Slave  Priority: 2
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 33 sec
```

```
  Neighbor is up for 00:11:15
  Authentication Sequence: [ 0 ]
  Neighbor state change count: 3
```

可以看到，网络中 DR/BDR 并没有改变。

提示：OSPF 为保证网络的稳定性，在网络中 DR/BDR 已经存在的情况下，接口上的路由器优先级的配置并不会立即生效，即不允许抢占。

(4) 重启 OSPF 进程(略)。

① 查看 Switch D 的邻居信息。

```
[SwitchD] display ospf peer verbose
            OSPF Process 1 with Router ID 4.4.4.4
                    Neighbors
 Area 0.0.0.0 interface 192.168.1.4(Vlan-interface1)'s neighbors
 Router ID: 1.1.1.1          Address: 192.168.1.1        GR State: Normal
   State: Full  Mode: Nbr is Slave  Priority: 100
   DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 39 sec
   Neighbor is up for 00:01:40
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 2

 Router ID: 2.2.2.2          Address: 192.168.1.2        GR State: Normal
   State: 2-Way  Mode: None  Priority: 0
   DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 35 sec
   Neighbor is up for 00:01:44
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 2

 Router ID: 3.3.3.3          Address: 192.168.1.3        GR State: Normal
   State: Full  Mode: Nbr is Slave  Priority: 2
   DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
   Dead timer due in 39 sec
   Neighbor is up for 00:01:41
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 2
```

可以看到，Switch A 成为 DR，Switch C 为 BDR。

提示：如果邻居的状态是 Full，这说明它和邻居之间形成了邻接关系；如果邻居的状态是 2-Way，则说明它们都不是 DR 或 BDR，两者之间不需要交换 LSA。

② 查看 OSPF 接口的状态。

```
[SwitchA] display ospf interface
            OSPF Process 1 with Router ID 1.1.1.1
                    Interfaces
 Area: 0.0.0.0
 IP Address      Type       State  Cost  Pri  DR            BDR
 192.168.1.1     Broadcast  DR     1     100  192.168.1.1   192.168.1.3
```

```
[SwitchB] display ospf interface
          OSPF Process 1 with Router ID 2.2.2.2
                    Interfaces
Area: 0.0.0.0
IP Address      Type       State    Cost  Pri  DR            BDR
192.168.1.2     Broadcast  DROther  1     0    192.168.1.1   192.168.1.3
```

提示：如果 OSPF 接口的状态是 DROther，则说明它既不是 DR，也不是 BDR。

8.3.7 OSPF 虚连接典型配置指导

OSPF 划分区域之后，并非所有的区域都是平等的关系。其中有一个区域是与众不同的，它的区域号(Area ID)是 0，通常被称为骨干区域。骨干区域负责区域之间的路由，非骨干区域之间的路由信息必须通过骨干区域来转发。对此，OSPF 有以下两个规定。

(1) 所有非骨干区域必须与骨干区域保持连通。

(2) 骨干区域自身也必须保持连通。

但在实际应用中，可能会因为各方面条件的限制，无法满足这个要求。这时可以通过配置 OSPF 虚连接(Virtual Link)予以解决。

虚连接是指在两台 ABR 之间通过一个非骨干区域而建立的一条逻辑上的连接通道。它的两端必须是 ABR，而且必须在两端同时配置方可生效。为虚连接两端提供一条非骨干区域内部路由的区域称为传输区(Transit Area)。

1. 背景

M 公司的 IT 维护人员小 L 采用 H3C 以太网交换机配置测试中心内部网络，在配置后发现有些区域的交换机上虽然使能了 OSPF，但是路由信息却一直无法学习到。经过仔细查看，原来是自己误将两个非骨干区域直接通过 ABR 连接起来，导致其中一个非骨干区域没有和 Area 0 相连，ABR 上的域间路由信息无法直接传递。由于网络拓扑已经规划完毕，不宜轻易改动，因此，小 L 通过配置虚连接的方式成功地解决了这一问题。

2. 组网图

图 8-12 所示为 OSPF 虚连接典型配置组网图。

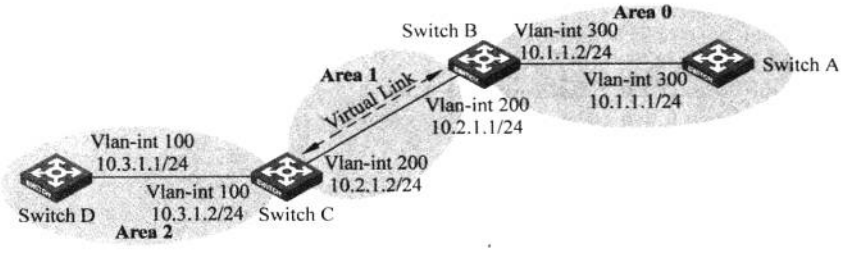


图 8-12 OSPF 虚连接典型配置组网图

3. 配置需求

(1) Area 2 与 Area 0 没有直接相连。Area 1 被用做传输区域(Transit Area)来连接 Area 2 和 Area 0。在 Switch B 和 Switch C 之间配置一条虚连接。

(2) 配置完成后，Switch B 能够学到 Area 2 中的路由。

4. 配置过程和解释

(1) 配置各接口的 IP 地址(略)。

(2) 配置 OSPF 基本功能。

① 配置 Switch A，启动 OSPF，并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] ospf 1 router-id 1.1.1.1
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
```

② 配置 Switch B，启动 OSPF，并设置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] ospf 1 router-id 2.2.2.2
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] area 1
[SwitchB-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.1] quit
```

③ 配置 Switch C，启动 OSPF，并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
[SwitchC] ospf 1 router-id 3.3.3.3
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] area 2
[SwitchC-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.2] quit
```

④ 配置 Switch D，启动 OSPF，并设置其 Router ID 为 4.4.4.4。

```
<SwitchD> system-view
[SwitchD] ospf 1 router-id 4.4.4.4
[SwitchD-ospf-1] area 2
[SwitchD-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] quit
```

⑤ 查看 Switch B 的 OSPF 路由表。

```
[SwitchB] display ospf routing
          OSPF Process 1 with Router ID 2.2.2.2
                  Routing Tables
 Routing for Network
 Destination        Cost   Type      NextHop         AdvRouter       Area
 10.2.1.0/24        2      Transit   10.2.1.1        3.3.3.3         0.0.0.1
 10.1.1.0/24        2      Transit   10.1.1.2        2.2.2.2         0.0.0.0
 Total Nets: 2
 Intra Area: 2  Inter Area: 0  ASE: 0  NSSA: 0
```

提示：由于 Area 0 没有与 Area 2 直接相连，所以 Switch B 的路由表中没有 Area 2 的路由。

(3) 配置虚连接。

① 配置 Switch B。

```
[SwitchB] ospf
[SwitchB-ospf-1] area 1
[SwitchB-ospf-1-area-0.0.0.1] vlink-peer 3.3.3.3
[SwitchB-ospf-1-area-0.0.0.1] quit
[SwitchB-ospf-1] quit
```

② 配置 Switch C。

```
[SwitchC] ospf 1
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] vlink-peer 2.2.2.2
[SwitchC-ospf-1-area-0.0.0.1] quit
```

③ 查看 Switch B 的 OSPF 路由表。

```
[SwitchB] display ospf routing
          OSPF Process 1 with Router ID 2.2.2.2
                    Routing Tables
 Routing for Network
 Destination        Cost   Type      NextHop         AdvRouter       Area
 10.2.1.0/24        2      Transit   10.2.1.1        3.3.3.3         0.0.0.1
 10.3.1.0/24        5      Inter     10.2.1.2        3.3.3.3         0.0.0.0
 10.1.1.0/24        2      Transit   10.1.1.2        2.2.2.2         0.0.0.0
 Total Nets: 3
 Intra Area: 2  Inter Area: 1  ASE: 0  NSSA: 0
```

可以看到，Switch B 已经学到了 Area 2 的路由 10.3.1.0/24。

提示：为使虚连接生效，在虚连接的两端都需配置 vlink-peer 命令，并且两端配置的 hello、dead 等参数必须一致。

虚连接不能穿过 Stub 区域，也不能穿过 NSSA 区域。

8.3.8 OSPF GR 典型配置指导

OSPF GR 的主要工作机制如下：

(1) 在 OSPF 协议重启前，GR Restarter 产生 Grace-LSA 协商 GR 能力。在重启过程中，GR Helper 继续宣告与 GR Restarter 的邻接状态不变。

(2) OSPF 协议重启完毕后，GR Restarter 会立即向其邻接的 GR Helper 发送一个 OSPF GR 信号。这样，OSPF 邻居就不会复位与其的邻居关系。在收到其 OSPF 邻居的响应后，GR Restarter 会重新恢复与其的邻居关系列表。

(3) 邻居关系重新建立后，GR Restarter 与其所有具备 GR 感知能力的 OSPF 邻居之间同步数据库，并交换路由信息。交换完成后，GR Restarter 根据新的路由转发信息更新路由表和转发表，删除失效的路由，完成 OSPF 协议收敛。

1. 背景

M公司IT维护人员小L在维护OSPF网络的时候发现，通过对交换机配置OSPF GR功能，能够在OSPF进程重启后加快路由重新学习的速度，缩减网络中断的时间。因此，小L正在尝试为部分OSPF交换机配置GR功能。

2. 组网图

图8-13所示为OSPF GR典型配置组网图。

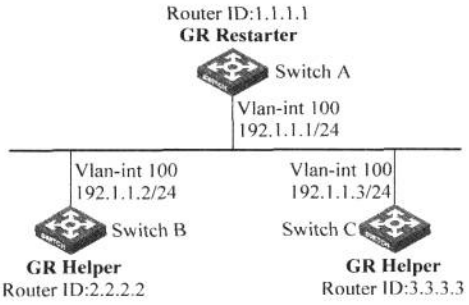


图8-13 OSPF GR典型配置组网图

3. 配置需求

(1) Switch A、Switch B和Switch C既属于同一自治系统，也属于同一OSPF域，通过OSPF协议实现网络互连，并提供GR机制。

(2) Switch A作为非IETF标准GR Restarter，Switch B和Switch C作为非IETF标准GR Helper，并且通过GR机制与Switch A保持带外同步。

4. 配置过程和解释

(1) 配置Switch A，启动OSPF，并设置其Router ID为1.1.1.1。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 192.1.1.1 255.255.255.0
[SwitchA-Vlan-interface100] quit
[SwitchA] router id 1.1.1.1
[SwitchA] ospf 100
[SwitchA-ospf-100] enable link-local-signaling
[SwitchA-ospf-100] enable out-of-band-resynchronization
[RouterA-ospf-100] graceful-restart
[SwitchA-ospf-100] area 0
[SwitchA-ospf-100-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[SwitchA-ospf-100-area-0.0.0.0] return
```

(2) 配置Switch B，启动OSPF，并设置其Router ID为2.2.2.2。

```
<SwitchB> system-view
[SwitchB] acl number 2000
[SwitchB-acl-basic-2000] rule 10 permit source 192.1.1.1 0.0.0.0
[SwitchB-acl-basic-2000] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 192.1.1.2 255.255.255.0
```

```
[SwitchB-Vlan-interface100] quit
[SwitchB] router id 2.2.2.2
[SwitchB] ospf 100
[SwitchB-ospf-100] enable link-local-signaling
[SwitchB-ospf-100] enable out-of-band-resynchronization
[SwitchB-ospf-100] graceful-restart help 2000
[SwitchB-ospf-100] area 0
[SwitchB-ospf-100-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[SwitchB-ospf-100-area-0.0.0.0] quit
```

(3) 配置 Switch C,启动 OSPF,并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] ip address 192.1.1.3 255.255.255.0
[SwitchC-Vlan-interface100] quit
[SwitchC] router id 3.3.3.3
[SwitchC] ospf 100
[SwitchC-ospf-100] enable link-local-signaling
[SwitchC-ospf-100] enable out-of-band-resynchronization
[SwitchC-ospf-100] area 0
[SwitchC-ospf-100-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[SwitchC-ospf-100-area-0.0.0.0] quit
```

(4) 检验配置效果。运行稳定后,在 Switch A 上重启 OSPF 协议的 GR 进程。

```
<SwitchA> reset ospf 100 process graceful-restart
```

8.3.9 OSPF 路由过滤典型配置指导

1. 背景

M 公司北京测试中心采用 H3C 交换机部署 OSPF 网络,网络部署完毕后基于某些特殊的 IT 管理要求,IT 部门需要对特定的路由发布进行限制,使某些用户间不能互相访问。IT 维护人员实施中发现对 OSPF 交换机配置路由过滤是一种简单实用的路由控制方式,可以很好地达到 IT 管理需求。

2. 组网图

图 8-14 所示为 OSPF 路由过滤典型配置组网图。

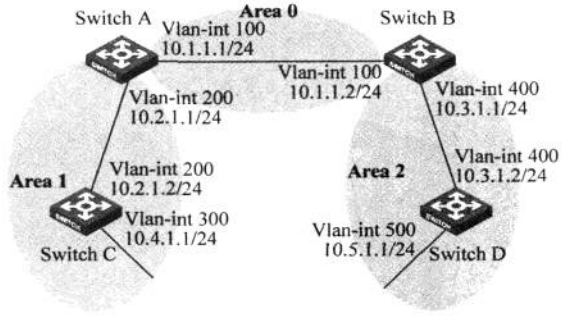


图 8-14 OSPF 路由过滤典型配置组网图

3. 配置需求

(1) 所有的交换机都运行 OSPF，整个自治系统划分为 3 个区域。

(2) 其中 Switch A 和 Switch B 作为 ABR 来转发区域之间的路由。

(3) 在 Switch C 上配置为 ASBR 引入外部路由(静态路由)，并在 Switch C 上配置过滤策略，对引入的一条路由(3.1.3.0/24)进行过滤。

(4) 在 Switch A 上配置路由策略，对路由(10.5.1.0/24)进行过滤。

4. 配置过程和解释

(1) 配置各接口的 IP 地址(略)。

(2) 配置 OSPF。

① 配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

② 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] area 2
[SwitchB-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.2] quit
[SwitchB-ospf-1] quit
```

③ 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] network 10.4.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

④ 配置 Switch D。

```
<SwitchD> system-view
[SwitchD] ospf
[SwitchD-ospf-1] area 2
[SwitchD-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
```

```
[SwitchD-ospf-1-area-0.0.0.2] network 10.5.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] quit
[SwitchD-ospf-1] quit
```

(3) 配置引入自治系统外部路由。

① 在 Switch C 上配置一条到目的网段 3.1.1.0/24 的静态路由。

```
[SwitchC] ip route-static 3.1.1.0 24 10.4.1.2
```

② 在 Switch C 上配置一条到目的网段 3.1.2.0/24 的静态路由。

```
[SwitchC] ip route-static 3.1.2.0 24 10.4.1.2
```

③ 在 Switch C 上配置一条到目的网段 3.1.3.0/24 的静态路由。

```
[SwitchC] ip route-static 3.1.3.0 24 10.4.1.2
```

④ 在 Switch C 上配置 OSPF 引入静态路由。

```
[SwitchC] ospf 1
[SwitchC-ospf-1] import-route static
[SwitchC-ospf-1] quit
```

⑤ 在 Switch A 上查看路由信息。

```
[SwitchA] display ip routing-table
Routing Tables: Public
         Destinations : 12        Routes : 12
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
3.1.1.0/24	O_ASE	150	1	10.2.1.2	Vlan200
3.1.2.0/24	O_ASE	150	1	10.2.1.2	Vlan200
3.1.3.0/24	O_ASE	150	1	10.2.1.2	Vlan200
10.1.1.0/24	Direct	0	0	10.1.1.1	Vlan200
10.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.2.1.0/24	Direct	0	0	10.2.1.1	Vlan200
10.2.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.3.1.0/24	OSPF	10	4	10.1.1.2	Vlan100
10.4.1.0/24	OSPF	10	13	10.2.1.2	Vlan200
10.5.1.0/24	OSPF	10	14	10.1.1.2	Vlan100
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

(4) 在 Switch C 上配置对路由 3.1.3.0/24 进行过滤。

① 配置 IPv4 地址前缀列表。

```
[SwitchC] ip ip-prefix prefix1 index 1 deny 3.1.3.0 24
[SwitchC] ip ip-prefix prefix1 index 2 permit 3.1.1.0 24
[SwitchC] ip ip-prefix prefix1 index 3 permit 3.1.2.0 24
```

② 配置对引入的静态路由信息进行过滤，过滤掉路由 3.1.3.0/24。

```
[SwitchC] ospf 1
[SwitchC-ospf-1] filter-policy ip-prefix prefix1 export static
```

③ 在 Switch A 上查看路由信息。

```
[SwitchA] display ip routing-table
Routing Tables: Public
         Destinations : 11        Routes : 11
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
3.1.1.0/24          O_ASE   150  1         10.2.1.2        Vlan200
3.1.2.0/24          O_ASE   150  1         10.2.1.2        Vlan200
10.1.1.0/24         Direct  0    0         10.1.1.1        Vlan100
10.1.1.1/32         Direct  0    0         127.0.0.1       InLoop0
10.2.1.0/24         Direct  0    0         10.2.1.1        Vlan200
10.2.1.1/32         Direct  0    0         127.0.0.1       InLoop0
10.3.1.0/24         OSPF    10   4         10.1.1.2        Vlan100
10.4.1.0/24         OSPF    10   13        10.2.1.2        Vlan200
10.5.1.0/24         OSPF    10   14        10.1.1.2        Vlan100
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop0
```

可以看到，到目的网段 3.1.3.0/24 的路由被过滤掉了。

(5) 在 Switch A 上配置对路由 10.5.1.1/24 进行过滤。

① 在 Switch A 上配置访问控制列表。

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule 0 deny source 10.5.1.0 0.0.0.255
[SwitchA-acl-basic-2000] rule 1 permit source any
[SwitchA-acl-basic-2000] quit
```

② 配置对通过 LSA 计算出来的路由信息 10.5.1.0/24 进行过滤。

```
[SwitchA] ospf 1
[SwitchA-ospf-1] filter-policy 2000 import
[SwitchA-ospf-1] quit
```

③ 在 Switch A 上查看路由信息。

```
[SwitchA] display ip routing-table
Routing Tables: Public
         Destinations : 10        Routes : 10
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
3.1.1.0/24          O_ASE   150  1         10.2.1.2        Vlan200
3.1.2.0/24          O_ASE   150  1         10.2.1.2        Vlan200
10.1.1.0/24         Direct  0    0         10.1.1.1        Vlan100
10.1.1.1/32         Direct  0    0         127.0.0.1       InLoop0
10.2.1.0/24         Direct  0    0         10.2.1.1        Vlan200
10.2.1.1/32         Direct  0    0         127.0.0.1       InLoop0
10.3.1.0/24         OSPF    10   4         10.1.1.2        Vlan100
10.4.1.0/24         OSPF    10   13        10.2.1.2        Vlan200
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop0
```

可以看到，到 10.5.1.1/24 的路由被过滤掉了。

8.4 IS-IS 协议典型配置指导

8.4.1 IS-IS 基本功能典型配置指导

IS-IS(Intermediate System-to-Intermediate System Intra-domain Routing Information Exchange Protocol,中间系统到中间系统的域内路由信息交换协议)最初是国际标准化组织(the International Organization for Standardization,ISO)为它的无连接网络协议(Connectionless Network Protocol,CLNP)设计的一种动态路由协议。

为了提供对 IP 的路由支持,IETF 在 RFC 1195 中对 IS-IS 进行了扩充和修改,使它能够同时应用在 TCP/IP 和 OSI 环境中,称为集成化 IS-IS(Integrated IS-IS 或 Dual IS-IS)。

IS-IS 属于内部网关协议(Interior Gateway Protocol,IGP),用于自治系统内部。IS-IS 是一种链路状态协议,使用最短路径优先(Shortest Path First,SPF)算法进行路由计算。

1. 背景

M 公司主用办公网络和测试中心网络均是由 OSPF 协议构建而成的,但研发中心由于保密性的要求,需要路由与其他网络隔离,因此在设计网络时 IT 维护部门使用另外一种 IGP 路由协议 IS-IS 对研发中心内部网络进行部署和构架,使研发中心网络相对独立。

2. 组网图

图 8-15 所示为 IS-IS 基本功能典型配置组网图。

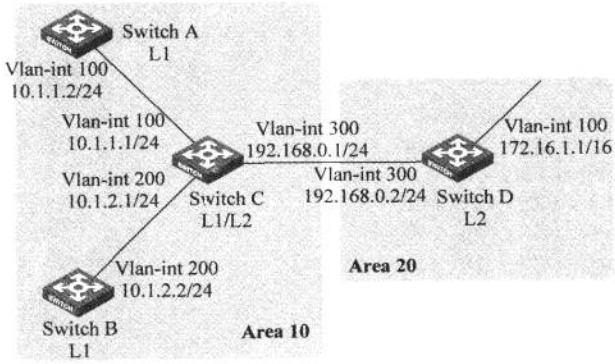


图 8-15 IS-IS 基本功能典型配置组网图

3. 配置需求

如图 8-15 所示,Switch A、Switch B、Switch C 和 Switch D 属于同一自治系统,要求它们之间通过 IS-IS 协议达到 IP 网络互连的目的。

其中,Switch A 和 Switch B 为 Level-1 交换机,Switch D 为 Level-2 交换机,Switch C 作为 Level-1-2 交换机将两个区域相连。Switch A、Switch B 和 Switch C 的区域号为 10,Switch D 的区域号为 20。

4. 配置过程和解释

(1) 配置各接口的 IPv4 地址(略)。

(2) 配置 IS-IS。

① 配置 Switch A。

```
<SwitchA> system-view
[SwitchA] isis 1
[SwitchA-isis-1] is-level level-1
[SwitchA-isis-1] network-entity 10.0000.0000.0001.00
[SwitchA-isis-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] isis enable 1
[SwitchA-Vlan-interface100] quit
```

② 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] isis 1
[SwitchB-isis-1] is-level level-1
[SwitchB-isis-1] network-entity 10.0000.0000.0002.00
[SwitchB-isis-1] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] isis enable 1
[SwitchB-Vlan-interface200] quit
```

③ 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] isis 1
[SwitchC-isis-1] network-entity 10.0000.0000.0003.00
[SwitchC-isis-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] isis enable 1
[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] isis enable 1
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] isis enable 1
[SwitchC-Vlan-interface300] quit
```

④ 配置 Switch D。

```
<SwitchD> system-view
[SwitchD] isis 1
[SwitchD-isis-1] is-level level-2
[SwitchD-isis-1] network-entity 20.0000.0000.0004.00
[SwitchD-isis-1] quit
[SwitchD] interface vlan-interface 100
[SwitchD-Vlan-interface100] isis enable 1
[SwitchD-Vlan-interface100] quit
[SwitchD] interface vlan-interface 300
[SwitchD-Vlan-interface300] isis enable 1
[SwitchD-Vlan-interface300] quit
```

(3) 验证配置结果。

① 显示各交换机的 IS-IS LSDB 信息，查看 LSP 是否完整。

```
[SwitchA] display isis lsdb
                    Database information for ISIS(1)
                    --------------------------------
                      Level-1 Link State Database
LSPID                 Seq Num     Checksum  Holdtime  Length  ATT/P/OL
--------------------------------------------------------------------------------
0000.0000.0001.00-00 *  0x00000004  0xdf5e    1096      68      0/0/0
0000.0000.0002.00-00    0x00000004  0xee4d    1102      68      0/0/0
0000.0000.0002.01-00    0x00000001  0xdaaf    1102      55      0/0/0
0000.0000.0003.00-00    0x00000009  0xcaa3    1161      111     1/0/0
0000.0000.0003.01-00    0x00000001  0xadda    1112      55      0/0/0
     * -Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload

[SwitchB] display isis lsdb
                    Database information for ISIS(1)
                    --------------------------------
                      Level-1 Link State Database
LSPID                 Seq Num     Checksum  Holdtime  Length  ATT/P/OL
--------------------------------------------------------------------------------
0000.0000.0001.00-00    0x00000006  0xdb60    988       68      0/0/0
0000.0000.0002.00-00 *  0x00000008  0xe651    1189      68      0/0/0
0000.0000.0002.01-00 *  0x00000005  0xd2b3    1188      55      0/0/0
0000.0000.0003.00-00    0x00000014  0x194a    1190      111     1/0/0
0000.0000.0003.01-00    0x00000002  0xabdb    995       55      0/0/0
     * -Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload

[SwitchC] display isis lsdb
                    Database information for ISIS(1)
                    --------------------------------
                      Level-1 Link State Database
LSPID                 Seq Num     Checksum  Holdtime  Length  ATT/P/OL
--------------------------------------------------------------------------------
0000.0000.0001.00-00    0x00000006  0xdb60    847       68      0/0/0
0000.0000.0002.00-00    0x00000008  0xe651    1053      68      0/0/0
0000.0000.0002.01-00    0x00000005  0xd2b3    1052      55      0/0/0
0000.0000.0003.00-00 *  0x00000014  0x194a    1051      111     1/0/0
0000.0000.0003.01-00 *  0x00000002  0xabdb    854       55      0/0/0
     * -Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload
                      Level-2 Link State Database
LSPID                 Seq Num     Checksum  Holdtime  Length  ATT/P/OL
--------------------------------------------------------------------------------
0000.0000.0003.00-00 *  0x00000012  0xc93c    842       100     0/0/0
0000.0000.0004.00-00    0x00000026  0x331     1173      84      0/0/0
0000.0000.0004.01-00    0x00000001  0xee95    668       55      0/0/0
     * -Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload

[SwitchD] display isis lsdb
```

```
                Database information for ISIS(1)
                --------------------------------

                    Level-2 Link State Database
LSPID                 Seq Num     Checksum  Holdtime  Length  ATT/P/OL
-------------------------------------------------------------------------------
0000.0000.0003.00-00  0x00000013  0xc73d    1003      100     0/0/0
0000.0000.0004.00-00* 0x0000003c  0xd647    1194      84      0/0/0
0000.0000.0004.01-00* 0x00000002  0xec96    1007      55      0/0/0
    * -Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload
```

② 显示各交换机的 IS-IS 路由信息。Level-1 交换机的路由表中应该有一条默认路由，且下一跳为 Level-1-2 交换机，Level-2 交换机的路由表中应该有所有 Level-1 和 Level-2 的路由。

```
[SwitchA] display isis route
                Route information for ISIS(1)
                -----------------------------

               ISIS(1) IPv4 Level-1 Forwarding Table
               -------------------------------------

IPV4 Destination    IntCost  ExtCost  ExitInterface  NextHop       Flags
-------------------------------------------------------------------------------
10.1.1.0/24         10       NULL     Vlan100        Direct        D/L/-
10.1.2.0/24         20       NULL     Vlan100        10.1.1.1      R/-/-
192.168.0.0/24      20       NULL     Vlan100        10.1.1.1      R/-/-
0.0.0.0/0           10       NULL     Vlan100        10.1.1.1      R/-/-
     Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

[SwitchC] display isis route
                Route information for ISIS(1)
                -----------------------------

               ISIS(1) IPv4 Level-1 Forwarding Table
               -------------------------------------

IPV4 Destination    IntCost  ExtCost  ExitInterface  NextHop       Flags
-------------------------------------------------------------------------------
192.168.0.0/24      10       NULL     Vlan300        Direct        D/L/-
10.1.1.0/24         10       NULL     Vlan100        Direct        D/L/-
10.1.2.0/24         10       NULL     Vlan200        Direct        D/L/-
     Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
               ISIS(1) IPv4 Level-2 Forwarding Table
               -------------------------------------

IPV4 Destination    IntCost  ExtCost  ExitInterface  NextHop       Flags
-------------------------------------------------------------------------------
192.168.0.0/24      10       NULL     Vlan300        Direct        D/L/-
10.1.1.0/24         10       NULL     Vlan100        Direct        D/L/-
10.1.2.0/24         10       NULL     Vlan200        Direct        D/L/-
172.16.0.0/16       20       NULL     Vlan300        192.168.0.2   R/-/-
     Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

[SwitchD] display isis route
                Route information for ISIS(1)
                -----------------------------

               ISIS(1) IPv4 Level-2 Forwarding Table
```

IPV4 Destination	IntCost	ExtCost	ExitInterface	NextHop	Flags
192.168.0.0/24	10	NULL	Vlan300	Direct	D/L/-
10.1.1.0/24	20	NULL	Vlan300	192.168.0.1	R/-/-
10.1.2.0/24	20	NULL	Vlan300	192.168.0.1	R/-/-
172.16.0.0/16	10	NULL	Vlan100	Direct	D/L/-

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

提示：属于不同区域的 Level-1 路由器不能形成邻居关系。Level-2 路由器是否形成邻居关系则与区域无关。

当路由器是 Level-1 或者 Level-2 类型时，接口的路由层次类型只能由路由器的类型决定，不能通过 isis circuit-level 命令改变；当路由器是 Level-1-2 类型时，接口的路由层次类型可以通过 isis circuit-level 命令改变，以建立不同层次的邻接关系。

8.4.2 IS-IS 的 DIS 选择典型配置指导

在广播网络中，IS-IS 需要在所有的路由器中选举一个路由器作为 DIS（Designated Intermediate System，指定中间系统）。

DIS 用来创建和更新伪节点（Pseudonodes），并负责生成伪节点的 LSP，用来描述这个网络上有哪些路由器。

伪节点是用来模拟广播网络的一个虚拟节点，并非真实的路由器。在 IS-IS 中，伪节点用 DIS 的 System ID 和 1 字节的 Circuit ID（非 0 值）标识。

使用伪节点可以简化网络拓扑，使产生的 LSP 数量较少，减少 SPF 的资源消耗。

1. 背景

M 公司研发中心网络通过 H3C 交换机采用 IS-IS 协议进行部署，且大部分交换机工作在广播网络中。IT 维护人员小 L 发现可以通过配置修改 DIS 参数人为控制 DIS 的选举，将性能较高的交换机选举为 DIS，达到合理分配网络资源的目的。

2. 组网图

图 8-16 所示为 IS-IS 的 DIS 选择典型配置组网图。

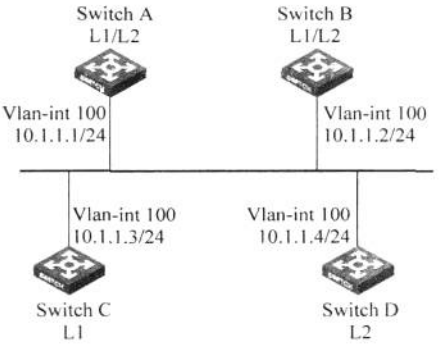


图 8-16 IS-IS 的 DIS 选择典型配置组网图

3. 配置需求

如图 8-16 所示，Switch A、Switch B、Switch C 和 Switch D 都运行 IS-IS 路由协议以实现互连，它们属于同一区域 10，网络类型为广播网（以太网）。其中，Switch A 和 Switch B 是 Level-1-2 交换机，Switch C 为 Level-1 交换机，Switch D 为 Level-2 交换机。

要求通过改变接口的 DIS 优先级，将 Switch A 配置为 Level-1-2 的 DIS。

4. 配置过程和解释

（1）配置各接口的 IPv4 地址（略）。

(2) 配置 IS-IS。

① 配置 Switch A。

```
<SwitchA> system-view
[SwitchA] isis 1
[SwitchA-isis-1] network-entity 10.0000.0000.0001.00
[SwitchA-isis-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] isis enable 1
[SwitchA-Vlan-interface100] quit
```

② 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] isis 1
[SwitchB-isis-1] network-entity 10.0000.0000.0002.00
[SwitchB-isis-1] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] isis enable 1
[SwitchB-Vlan-interface100] quit
```

③ 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] isis 1
[SwitchC-isis-1] network-entity 10.0000.0000.0003.00
[SwitchC-isis-1] is-level level-1
[SwitchC-isis-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] isis enable 1
[SwitchC-Vlan-interface100] quit
```

④ 配置 Switch D。

```
<SwitchD> system-view
[SwitchD] isis 1
[SwitchD-isis-1] network-entity 10.0000.0000.0004.00
[SwitchD-isis-1] is-level level-2
[SwitchD-isis-1] quit
[SwitchD] interface vlan-interface 100
[SwitchD-Vlan-interface100] isis enable 1
[SwitchD-Vlan-interface100] quit
```

⑤ 查看 Switch A 的 IS-IS 邻居信息。

```
[SwitchA] display isis peer
                        Peer information for ISIS(1)
                        ----------------------------

  System Id: 0000.0000.0002
  Interface: Vlan-interface100        Circuit Id: 0000.0000.0003.01
  State: Up     HoldTime: 21s         Type: L1(L1L2)     PRI: 64

  System Id: 0000.0000.0003
```

```
Interface: Vlan-interface100          Circuit Id: 0000.0000.0003.01
State: Up     HoldTime: 27s           Type: L1              PRI: 64

System Id: 0000.0000.0002
Interface: Vlan-interface100          Circuit Id: 0000.0000.0004.01
State: Up     HoldTime: 28s           Type: L2(L1L2)        PRI: 64

System Id: 0000.0000.0004
Interface: Vlan-interface100          Circuit Id: 0000.0000.0004.01
State: Up     HoldTime: 30s           Type: L2              PRI: 64
```

⑥ 显示 Switch A 的 IS-IS 接口信息。

```
[SwitchA] display isis interface
                    Interface information for ISIS(1)
                    ----------------------------

Interface: Vlan-interface100
Id     IPV4.State     IPV6.State     MTU     Type     DIS
001        Up             Down       1497    L1/L2    No/No
```

⑦ 显示 Switch C 的 IS-IS 接口信息。

```
[SwitchC] display isis interface
                    Interface information for ISIS(1)
                    ----------------------------

Interface: Vlan-interface100
Id     IPV4.State     IPV6.State     MTU     Type     DIS
001        Up             Down       1497    L1/L2    Yes/No
```

⑧ 显示 Switch D 的 IS-IS 接口信息。

```
[SwitchD] display isis interface
                    Interface information for ISIS(1)
                    ----------------------------

Interface: Vlan-interface100
Id     IPV4.State     IPV6.State     MTU     Type     DIS
001        Up             Down       1497    L1/L2    No/Yes
```

提示：从接口信息中可以看到，在使用默认 DIS 优先级的情况下，Switch C 为 Level-1 的 DIS，Switch D 为 Level-2 的 DIS。Level-1 和 Level-2 的伪节点分别是 0000.0000.0003.01 和 0000.0000.0004.01。

由此也可以说明 Level-1 的 DIS 和 Level-2 的 DIS 是分别进行选举的。

(3) 配置 Switch A 的 DIS 优先级。

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] isis dis-priority 100
[SwitchA-Vlan-interface100] quit
```

① 查看 Switch A 的 IS-IS 邻居信息。

```
[SwitchA] display isis peer
```

```
                Peer information for ISIS(1)
                ----------------------------

  System Id: 0000.0000.0002
  Interface: Vlan-interface100          Circuit Id: 0000.0000.0001.01
  State: Up     HoldTime: 21s           Type: L1(L1L2)     PRI: 64

  System Id: 0000.0000.0003
  Interface: Vlan-interface100          Circuit Id: 0000.0000.0001.01
  State: Up     HoldTime: 27s           Type: L1           PRI: 64


  System Id: 0000.0000.0002
  Interface: Vlan-interface100          Circuit Id: 0000.0000.0001.01
  State: Up     HoldTime: 28s           Type: L2(L1L2)     PRI: 64

  System Id: 0000.0000.0004
  Interface: Vlan-interface100          Circuit Id: 0000.0000.0001.01
  State: Up     HoldTime: 30s           Type: L2           PRI: 64
```

② 查看 Switch A 的 IS-IS 接口信息。

```
[SwitchA] display isis interface
                Interface information for ISIS(1)
                ---------------------------------

Interface: Vlan-interface100
Id     IPV4.State     IPV6.State     MTU     Type     DIS
001        Up             Down       1497    L1/L2    Yes/Yes
```

提示：从上述信息中可以看到，在改变 IS-IS 接口的 DIS 优先级后，Switch A 立即成为 Level-1-2 的 DR(DIS)，且伪节点是 0000.0000.0001.01。

由此也可以说明 DIS 与 OSPF 中的 DR 是不同的，DIS 的选举是允许抢占的。

③ 显示 Switch C 的 IS-IS 邻居和接口信息。

```
[SwitchC] display isis peer
                Peer information for ISIS(1)
                ----------------------------

  System Id: 0000.0000.0002
  Interface: Vlan-interface100          Circuit Id: 0000.0000.0001.01
  State: Up     HoldTime: 25s           Type: L1     PRI: 64

  System Id: 0000.0000.0001
  Interface: Vlan-interface100          Circuit Id: 0000.0000.0001.01
  State: Up     HoldTime: 7s            Type: L1     PRI: 100

[SwitchC] display isis interface
                Interface information for ISIS(1)
                ---------------------------------

Interface: Vlan-interface100
Id     IPV4.State     IPV6.State     MTU     Type     DIS
001        Up             Down       1497    L1/L2    No/No
```

④ 显示 Switch D 的 IS-IS 邻居和接口信息。

```
[SwitchD] display isis peer
                    Peer information for ISIS(1)
                    --------------------------

 System Id: 0000.0000.0001
 Interface: Vlan-interface100          Circuit Id: 0000.0000.0001.01
 State: Up     HoldTime: 9s            Type: L2     PRI: 100

 System Id: 0000.0000.0002
 Interface: Vlan-interface100          Circuit Id: 0000.0000.0001.01
 State: Up     HoldTime: 28s           Type: L2     PRI: 64

[SwitchD] display isis interface
                  Interface information for ISIS(1)
                  ---------------------------------

Interface: Vlan-interface100
Id      IPV4.State      IPV6.State      MTU     Type    DIS
001         Up              Down        1497    L1/L2   No/No
```

提示：对于 IS-IS，Level-1 和 Level-2 的 DIS 是分别选举的，可以为不同级别的 DIS 选举设置不同的优先级。优先级数值越高，被选中的可能性就越大。

当广播网络中优先级最高的路由器有多台时，则其中 MAC 地址最大的路由器会被选中。如果所有路由器的 DIS 优先级都是 0，仍然会选择其中 MAC 地址最大的路由器作为 DIS。

8.4.3 IS-IS 引入外部路由典型配置指导

1. 背景

为了信息保密，M 公司的研发中心网络没有直接连接至外部网络，但为了在特殊情况下访问外网，IT 维护部门需为研发中心开辟一条公网的路由。因连接外网的其他网络均部署 OSPF、RIP 等其他路由协议，因此研发中心网络需通过将其他路由协议路由引入到 IS-IS 中使外网路由可达。

2. 组网图

图 8-17 所示为 IS-IS 引入外部路由典型配置组网图。

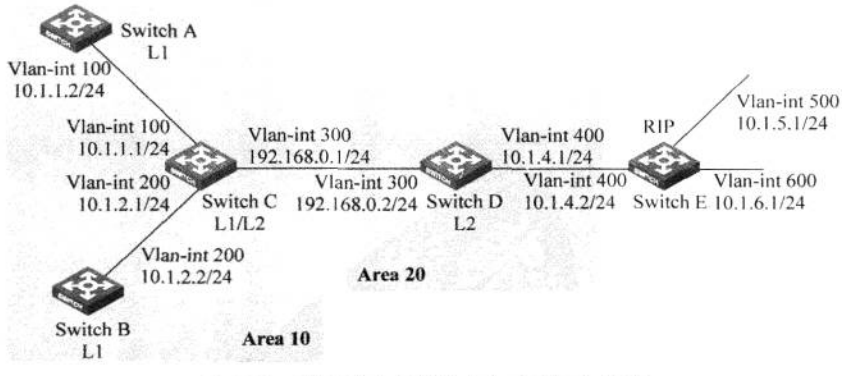


图 8-17 IS-IS 引入外部路由典型配置组网图

3. 配置需求

(1) Switch A、Switch B、Switch C 和 Switch D 属于同一自治系统，要求它们之间通过 IS-IS 协议达到 IP 网络互连的目的。

(2) Switch A 和 Switch B 为 Level-1 路由器，Switch D 为 Level-2 路由器，Switch C 作为 Level-1-2 路由器将两个区域相连。Switch A、Switch B 和 Switch C 的区域号为 10，Switch D 的区域号为 20。

(3) 在 Switch D 的 IS-IS 进程中引入 RIP 路由。

4. 配置过程和解释

(1) 配置各接口的 IP 地址(略)。

(2) 配置 IS-IS 基本功能。

① 配置 Switch A。

```
<SwitchA> system-view
[SwitchA] isis 1
[SwitchA-isis-1] is-level level-1
[SwitchA-isis-1] network-entity 10.0000.0000.0001.00
[SwitchA-isis-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] isis enable 1
[SwitchA-Vlan-interface100] quit
```

② 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] isis 1
[SwitchB-isis-1] is-level level-1
[SwitchB-isis-1] network-entity 10.0000.0000.0002.00
[SwitchB-isis-1] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] isis enable 1
[SwitchB-Vlan-interface200] quit
```

③ 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] isis 1
[SwitchC-isis-1] network-entity 10.0000.0000.0003.00
[SwitchC-isis-1] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] isis enable 1
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] isis enable 1
[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] isis enable 1
[SwitchC-Vlan-interface300] quit
```

④ 配置 Switch D。

```
<SwitchD> system-view
[SwitchD] isis 1
[SwitchD-isis-1] is-level level-2
[SwitchD-isis-1] network-entity 20.0000.0000.0004.00
[SwitchD-isis-1] quit
[SwitchD] interface interface vlan-interface 300
[SwitchD-Vlan-interface300] isis enable 1
[SwitchD-Vlan-interface300] quit
```

⑤ 显示各路由器的 IS-IS 路由信息。

```
[SwitchA] display isis route
                    Route information for ISIS(1)
                    --------------------------
                   ISIS(1) IPv4 Level-1 Forwarding Table
                   -------------------------------------
 IPV4 Destination    IntCost  ExtCost  ExitInterface  NextHop       Flags
--------------------------------------------------------------------------
 10.1.1.0/24         10       NULL     VLAN100        Direct        D/L/-
 10.1.2.0/24         20       NULL     VLAN100        10.1.1.1      R/-/-
 192.168.0.0/24      20       NULL     VLAN100        10.1.1.1      R/-/-
 0.0.0.0/0           10       NULL     VLAN100        10.1.1.1      R/-/-
      Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

[SwitchC] display isis route
                    Route information for ISIS(1)
                    --------------------------
                   ISIS(1) IPv4 Level-1 Forwarding Table
                   -------------------------------------
 IPV4 Destination    IntCost  ExtCost  ExitInterface  NextHop       Flags
--------------------------------------------------------------------------
 10.1.1.0/24         10       NULL     VLAN100        Direct        D/L/-
 10.1.2.0/24         10       NULL     VLAN200        Direct        D/L/-
 192.168.0.0/24      10       NULL     VLAN300        Direct        D/L/-
      Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
                   ISIS(1) IPv4 Level-2 Forwarding Table
                   -------------------------------------
 IPV4 Destination    IntCost  ExtCost  ExitInterface  NextHop       Flags
--------------------------------------------------------------------------
 10.1.1.0/24         10       NULL     VLAN100        Direct        D/L/-
 10.1.2.0/24         10       NULL     VLAN200        Direct        D/L/-
 192.168.0.0/24      10       NULL     VLAN300        Direct        D/L/-
      Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

[SwitchD] display isis route
                    Route information for ISIS(1)
                    --------------------------
                   ISIS(1) IPv4 Level-2 Forwarding Table
                   -------------------------------------
 IPV4 Destination    IntCost  ExtCost  ExitInterface  NextHop       Flags
```

```
192.168.0.0/24      10        NULL      VLAN300         Direct          D/L/-
10.1.1.0/24         20        NULL      VLAN300         192.168.0.1     R/-/-
10.1.2.0/24         20        NULL      VLAN300         192.168.0.1     R/-/-
     Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

(3) 在 Switch D 和 Switch E 之间运行 RIPv2，在 Switch D 上配置 IS-IS 进程引入 RIP 路由。

① 在 Switch D 上配置 RIPv2。

```
[SwitchD] rip 1
[SwitchD-rip-1] network 10.0.0.0
[SwitchD-rip-1] version 2
[SwitchD-rip-1] undo summary
```

② 在 Switch E 上配置 RIPv2。

```
[SwitchE] rip 1
[SwitchE-rip-1] network 10.0.0.0
[SwitchE-rip-1] version 2
[SwitchE-rip-1] undo summary
```

③ 在 Switch D 上配置 IS-IS 进程引入 RIP 进程的路由。

```
[Switch-rip-1] quit
[SwitchD] isis 1
[SwitchD-isis]import-route rip level-2
```

④ 显示 Switch C 的 IS-IS 路由信息。

```
[SwitchC] display isis route
                    Route information for ISIS(1)
                    ------------------------------
                ISIS(1) IPv4 Level-1 Forwarding Table
                -------------------------------------
IPV4 Destination    IntCost  ExtCost  ExitInterface  NextHop         Flags
-------------------------------------------------------------------------------
10.1.1.0/24         10       NULL     VLAN100        Direct          D/L/-
10.1.2.0/24         10       NULL     VLAN200        Direct          D/L/-
192.168.0.0/24      10       NULL     VLAN300        Direct          D/L/-
     Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
                ISIS(1) IPv4 Level-2 Forwarding Table
                -------------------------------------
IPV4 Destination    IntCost  ExtCost  ExitInterface  NextHop         Flags
-------------------------------------------------------------------------------
10.1.1.0/24         10       NULL     VLAN100        Direct          D/L/-
10.1.2.0/24         10       NULL     VLAN200        Direct          D/L/-
192.168.0.0/24      10       NULL     VLAN300        Direct          D/L/-
10.1.4.0/24         10       NULL     VLAN300        192.168.0.2     R/L/-
10.1.5.0/24         20       NULL     VLAN300        192.168.0.2     R/L/-
10.1.6.0/24         20       NULL     VLAN300        192.168.0.2     R/L/-
     Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

8.4.4 IS-IS GR 典型配置指导

IS-IS GR 的基本工作机制如下：

(1) IS-IS 协议重启完毕后，GR Restarter 会立即向邻接的 GR Helper 发送一个 IS-IS GR 信号。这样，IS-IS 邻居就不会复位与其的邻居关系。在收到其 IS-IS 邻居的响应后，GR Restarter 会重新恢复与其的邻居关系列表。

(2) 邻居关系重新建立后，GR Restarter 与其所有具备 GR 感知能力的 IS-IS 邻居之间同步数据库，并交换路由信息。交换完成后，GR Restarter 根据新的路由转发信息更新路由表和转发表，删除失效的路由，完成 IS-IS 协议收敛。

1. 背景

M 公司的研发中心网络通过 H3C 以太网交换机采用 IS-IS 协议进行部署，IT 维护人员小 L 在部署过程中按照先前测试中心网络中 OSPF GR 的配置思路，对研发中心网络也进行了 IS-IS GR 的部署，用于在 IS-IS 进程重启后达到加快网络收敛速度、缩短业务中断时间的目的。

2. 组网图

图 8-18 所示为 IS-IS GR 典型配置组网图。

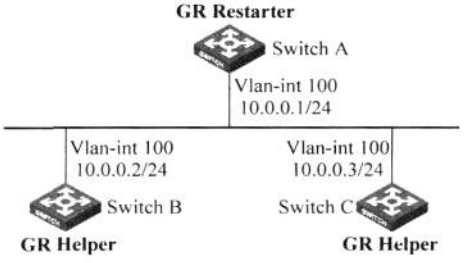


图 8-18 IS-IS GR 典型配置组网图

3. 配置需求

如图 8-18 所示，Switch A、Switch B 和 Switch C 属于同一域。这 3 台交换机都运行 IS-IS 协议以实现路由互连，并提供 GR 机制。

4. 配置过程和解释

(1) 配置各交换机接口的 IP 地址和 IS-IS 协议。

① 配置各接口的 IP 地址和子网掩码，具体配置过程略。

② 配置各交换机之间采用 IS-IS 协议进行互连，确保 Switch A、Switch B 和 Switch C 之间能够在网络层互通，并且各交换机之间能够借助 IS-IS 协议实现动态路由更新，具体配置过程略。

(2) 配置 IS-IS GR。使能 Switch A 的 IS-IS 协议的 GR 能力，并配置重启间隔时间。

```
<SwitchA> system-view
[SwitchA] isis 1
[SwitchA-isis-1] graceful-restart
[SwitchA-isis-1] graceful-restart interval 150
[SwitchA-isis-1] return
```

Switch B 和 Switch C 的配置与 Switch A 相似，配置过程略。

(3) 检验配置效果。Switch A 分别与 Switch B 和 Switch C 建立邻接关系后，3 台交换机开始交换路由信息。Switch A 的 IS-IS 协议重启，进入重启模式后，通过 GR 机制向邻居重新发送连接请求，同步数据库。使用 display isis graceful-restart status 命令，可查看 Switch A 上 IS-IS 协议的 GR 状态。

① 重启 Switch A。

```
<SwitchA> reset isis all 1
Warning : Reset ISIS process? [Y/N]:y
```

② 查看 Switch A 上 IS-IS 协议的 GR 状态。

```
<SwitchA> display isis graceful-restart status
                        Restart information for ISIS(1)
                        ------------------------------

IS-IS(1) Level-1 Restart Status
Restart Interval: 150
SA Bit Supported
  Total Number of Interfaces = 1
  Restart Status: RESTARTING
  T3 Timer Status:
    Remaining Time: 65535
  T2 Timer Status:
    Remaining Time: 59
  Interface Vlan1
    T1 Timer Status:
      Remaining Time: 1
    RA Not Received
    Complete CSNP Not Received
    Number of T1 Pre Expiry: 0

IS-IS(1) Level-2 Restart Status
Restart Interval: 150
SA Bit Supported
  Total Number of Interfaces = 1
  Restart Status: RESTARTING
  T3 Timer Status:
    Remaining Time: 65535
  T2 Timer Status:
    Remaining Time: 59
  Interface Vlan1
    T1 Timer Status:
      Remaining Time: 1
    RA Not Received
    Complete CSNP Not Received
    Number of T1 Pre Expiry: 0
```

8.4.5 IS-IS 验证典型配置指导

1. 背景

M 公司研发中心网络采用 H3C 以太网交换机通过 IS-IS 协议进行部署，由于研发网络安全性的需求，IT 维护部门需要在使能 IS-IS 的交换机上配置 IS-IS 验证，以确保设备间建立合法的邻居关系，并能学习到正确的路由信息。

2. 组网图

图 8-19 所示为 IS-IS 验证典型配置组网图。

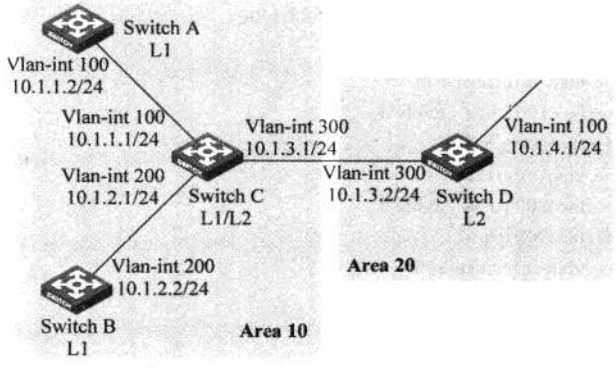


图 8-19 IS-IS 验证典型配置组网图

3. 配置需求

如图 8-19 所示，Switch A、Switch B、Switch C 和 Switch D 属于同一路由域，要求它们之间通过 IS-IS 协议达到 IP 网络互连的目的。其中，Switch A、Switch B 和 Switch C 属于同一个区域，区域号为 10；Switch D 属于另外一个区域，区域号为 20。

在区域 10 内配置区域验证，防止不可信任的路由信息加入到区域 10 的 LSDB 中；在 Switch C 和 Switch D 上配置路由域验证，防止将不可信的路由信息注入当前路由域；分别在 Switch A、Switch B、Switch C 和 Switch D 上配置邻居关系验证。

4. 配置过程和解释

(1) 配置各接口的 IP 地址(略)。

(2) 配置 IS-IS 基本功能。

① 配置 Switch A。

```
<SwitchA> system-view
[SwitchA] isis 1
[SwitchA-isis-1] network-entity 10.0000.0000.0001.00
[SwitchA-isis-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] isis enable 1
[SwitchA-Vlan-interface100] quit
```

② 配置 Switch B。

```
<SwitchB> system-view
```

```
[SwitchB] isis 1
[SwitchB-isis-1] network-entity 10.0000.0000.0002.00
[SwitchB-isis-1] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] isis enable 1
[RouterB-Vlan-interface200] quit
```

③ 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] isis 1
[SwitchC-isis-1] network-entity 10.0000.0000.0003.00
[SwitchC-isis-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] isis enable 1
[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] isis enable 1
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] isis enable 1
[SwitchC-Vlan-interface300] quit
```

④ 配置 Switch D。

```
<SwitchD> system-view
[SwitchD] isis 1
[SwitchD-isis-1] network-entity 20.0000.0000.0001.00
[SwitchD-isis-1] quit
[SwitchD] interface vlan-interface 300
[SwitchD-Vlan-interface300] isis enable 1
[SwitchD-Vlan-interface300] quit
```

(3) 在 Switch A、Switch B、Switch C 和 Switch D 之间建立邻居关系验证。

① 分别在 Switch A 的 Vlan-interface 100、Switch C 的 Vlan-interface 100 上配置邻居关系验证，验证方式为 MD5 密文，验证密码为“eRg”。

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] isis authentication-mode md5 eRg
[SwitchA-Vlan-interface100] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] isis authentication-mode md5 eRg
[SwitchC-Vlan-interface100] quit
```

② 分别在 Switch B 的 Vlan-interface 200、Switch C 的 Vlan-interface 200 上配置邻居关系验证，验证方式为 MD5 密文，验证密码为“t5Hr”。

```
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] isis authentication-mode md5 t5Hr
[SwitchB-Vlan-interface200] quit
[SwitchC] interface vlan-interface 200
```

```
[SwitchC-Vlan-interface200] isis authentication-mode md5 t5Hr
[SwitchC-Vlan-interface200] quit
```

③ 分别在 Switch C 的 Vlan-interface 300、Switch D 的 Vlan-interface 300 上配置邻居关系验证，验证方式为 MD5 密文，验证密码为“hSec”。

```
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] isis authentication-mode md5 hSec
[SwitchC-Vlan-interface300] quit
[SwitchD] interface vlan-interface 300
[SwitchD-Vlan-interface300] isis authentication-mode md5 hSec
[SwitchD-Vlan-interface300] quit
```

(4) 在 Switch A、Switch B 和 Switch C 上配置区域验证，验证方式为 MD5 密文验证，验证密码为“10Sec”。

```
[SwitchA] isis 1
[SwitchA-isis-1] area-authentication-mode md5 10Sec
[SwitchA-isis-1] quit
[SwitchB] isis 1
[SwitchB-isis-1] area-authentication-mode md5 10Sec
[SwitchB-isis-1] quit
[SwitchC] isis 1
[SwitchC-isis-1] area-authentication-mode md5 10Sec
[SwitchC-isis-1] quit
```

(5) 在 Switch C 和 Switch D 上配置路由域验证，验证方式为 MD5 密文验证，验证密码为“1020Sec”。

```
[SwitchC] isis 1
[SwitchC-isis-1] domain-authentication-mode md5 1020Sec
[SwitchC-isis-1] quit
[SwitchD] isis 1
[SwitchD-isis-1] domain-authentication-mode md5 1020Sec
```

8.5 BGP 协议典型配置指导

8.5.1 BGP 基本功能典型配置指导

(1) BGP 是一种外部网关协议(Exterior Gateway Protocol，EGP)，与 OSPF、RIP 等内部网关协议(Interior Gateway Protocol，IGP)不同，其着眼点不在于发现和计算路由，而在于控制路由的传播和选择最佳路由。

(2) BGP 使用 TCP 作为其传输层协议(端口号 179)，提高了协议的可靠性。

(3) BGP 支持 CIDR(Classless Inter-Domain Routing，无类别域间路由)。

(4) 路由更新时，BGP 只发送更新的路由，大大减少了 BGP 传播路由所占用的带宽，适用于在 Internet 上传播大量的路由信息。

(5) BGP 路由通过携带 AS 路径信息彻底解决路由环路问题。

(6) BGP 提供了丰富的路由策略,能够对路由实现灵活的过滤和选择。

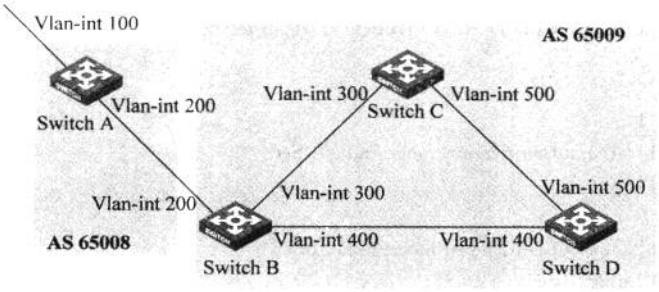
(7) BGP 易于扩展,能够适应网络新的发展。

1. 背景

M 公司不同省市之间研发中心、测试中心间均通过广域网线路互连,广域网线路的特点是带宽较低。BGP 路由作为外部网关协议,具有很好的路由控制能力,也比较节省带宽资源,因此 IT 维护部门采用 BGP 协议部署各地研发、测试中心。

2. 组网图

图 8-20 所示为 BGP 基本功能典型配置组网图。



设 备	接 口	IP 地址	设 备	接 口	IP 地址
Switch A	Vlan-int 100	8.1.1.1/8	Switch D	Vlan-int 400	9.1.1.2/24
	Vlan-int 200	200.1.1.2/24		Vlan-int 500	9.1.2.2/24
Switch B	Vlan-int 400	9.1.1.1/24	Switch C	Vlan-int 500	9.1.2.1/24
	Vlan-int 200	200.1.1.1/24		Vlan-int 300	9.1.3.2/24
	Vlan-int 300	9.1.3.1/24			

图 8-20 BGP 基本功能典型配置组网图

3. 配置需求

如图 8-20 所示,所有交换机均运行 BGP,Switch A 和 Switch B 之间建立 EBGP 连接,Switch B、Switch C 和 Switch D 之间建立 IBGP 全连接。在 Switch A 上通告路由 8.0.0.0/8,观察其他 BGP 交换机上的路由学习情况。

4. 配置过程和解释

(1) 配置各接口的 IP 地址(略)。

(2) 配置 IBGP 连接。

① 配置 Switch B,启动 BGP,并设置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] bgp 65009
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] peer 9.1.1.2 as-number 65009
[SwitchB-bgp] peer 9.1.3.2 as-number 65009
[SwitchB-bgp] quit
```

② 配置 Switch C，启动 BGP，并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
[SwitchC] bgp 65009
[SwitchC-bgp] router-id 3.3.3.3
[SwitchC-bgp] peer 9.1.3.1 as-number 65009
[SwitchC-bgp] peer 9.1.2.2 as-number 65009
[SwitchC-bgp] quit
```

③ 配置 Switch D，启动 BGP，并设置其 Router ID 为 4.4.4.4。

```
<SwitchD> system-view
[SwitchD] bgp 65009
[SwitchD-bgp] router-id 4.4.4.4
[SwitchD-bgp] peer 9.1.1.1 as-number 65009
[SwitchD-bgp] peer 9.1.2.1 as-number 65009
[SwitchD-bgp] quit
```

(3) 配置 EBGP 连接。

① 配置 Switch A，启动 BGP，并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] bgp 65008
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] peer 200.1.1.1 as-number 65009
```

② 将 8.0.0.0/8 网段路由通告到 BGP 路由表中。

```
[SwitchA-bgp] network 8.0.0.0
[SwitchA-bgp] quit
```

③ 配置 Switch B。

```
[SwitchB] bgp 65009
[SwitchB-bgp] peer 200.1.1.2 as-number 65008
[SwitchB-bgp] quit
```

④ 查看 Switch B 的 BGP 对等体的连接状态。

```
[SwitchB] display bgp peer
 BGP local router ID : 2.2.2.2
 Local AS number : 65009
 Total number of peers : 3                 Peers in established state : 3
 Peer            V    AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
 9.1.1.2         4    65009  56       56       0     0        00:40:54 Established
 9.1.3.2         4    65009  49       62       0     0        00:44:58 Established
 200.1.1.2       4    65008  49       65       0     1        00:44:03 Established
```

可以看出，Switch B 到其他交换机的 BGP 连接均已建立。

⑤ 查看 Switch A 路由表信息。

```
[SwitchA] display bgp routing-table
 Total Number of Routes: 1
```

```
BGP Local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
   Network          NextHop        MED        LocPrf     PrefVal  Path/Ogn
*> 8.0.0.0          0.0.0.0        0                     0        i
```

⑥ 查看 Switch B 的路由表。

```
[SwitchB] display bgp routing-table
 Total Number of Routes: 1
 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history, i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
    Network          NextHop        MED        LocPrf     PrefVal  Path/Ogn
 *> 8.0.0.0          200.1.1.2      0                     0        65008i
```

⑦ 查看 Switch C 的路由表。

```
[SwitchC] display bgp routing-table
 Total Number of Routes: 1
 BGP Local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - damped,
               h - history, i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
    Network          NextHop        MED        LocPrf     PrefVal  Path/Ogn
 i 8.0.0.0          200.1.1.2      0          100        0        65008i
```

提示：从路由表可以看出，Switch A 没有学到 AS 65009 内部的任何路由；Switch C 虽然学到了 AS 65008 中的 8.0.0.0 的路由，但因为下一跳 200.1.1.2 不可达，所以也不是有效路由。这是由于 Switch B 上通过 EBGP 对等体学习到的路由，在向 IBGP 对等体 Switch C 发布的时候不改变下一跳。这一问题可以采用下面步骤(4)中的方法解决。

(4) 配置 BGP 引入直连路由。

① 配置 Switch B。

```
[SwitchB] bgp 65009
[SwitchB-bgp] import-route direct
```

② 显示 Switch A 的 BGP 路由表。

```
[SwitchA] display bgp routing-table
 Total Number of Routes: 4
 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history, i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
    Network          NextHop        MED        LocPrf     PrefVal  Path/Ogn
 *> 8.0.0.0          0.0.0.0        0                     0        i
 *> 9.1.1.0/24       200.1.1.1      0                     0        65009?
 *> 9.1.3.0/24       200.1.1.1      0                     0        65009?
 * 200.1.1.0         200.1.1.1      0                     0        65009?
```

③ 显示 Switch C 的路由表。

```
[SwitchC] display bgp routing-table
 Total Number of Routes: 4
 BGP Local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - damped,
               h - history, i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
    Network          NextHop         MED        LocPrf    PrefVal  Path/Ogn
 * >i 8.0.0.0        200.1.1.2       0          100       0        65008i
 * >i 9.1.1.0/24     9.1.3.1         0          100       0        ?
 *  i 9.1.3.0/24     9.1.3.1         0          100       0        ?
 * >i 200.1.1.0      9.1.3.1         0          100       0        ?
```

可以看出，到 8.0.0.0 的路由变为有效路由，下一跳为 Switch A 的地址。

④ 使用 ping 进行验证。

```
[SwitchC] ping 8.1.1.1
  PING 8.1.1.1: 56 data bytes, press Ctrl_C to break
    Reply from 8.1.1.1: bytes=56 Sequence=1 ttl=254 time=31 ms
    Reply from 8.1.1.1: bytes=56 Sequence=2 ttl=254 time=47 ms
    Reply from 8.1.1.1: bytes=56 Sequence=3 ttl=254 time=31 ms
    Reply from 8.1.1.1: bytes=56 Sequence=4 ttl=254 time=16 ms
    Reply from 8.1.1.1: bytes=56 Sequence=5 ttl=254 time=31 ms
  --- 8.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 16/31/47 ms
```

8.5.2 BGP 与 IGP 交互典型配置指导

BGP 可以向邻居 AS 发送本地 AS 内部网络的路由信息，但 BGP 不是自己去发现 AS 内部的路由信息，而是引入 IGP 的路由信息到 BGP 路由表中，并发布给对等体。在引入 IGP 路由时，还可以针对不同的路由协议来对路由信息进行过滤。

1. 背景

M 公司两地测试中心之间采用 BGP 路由协议部署，由于 BGP 不会主动发现路由，因此为了使本地测试中心下的 IGP 路由能够通过 BGP 发布给异地，BGP 中必须引入本地测试中心的 IGP 路由(OSPF 等)。

2. 组网图

图 8-21 所示为 BGP 与 IGP 交互典型配置组网图。

3. 配置需求

(1) 在 AS 65009 内使用 OSPF 作为 IGP 协议。

(2) Switch A 和 Switch B 建立 EBGP 连接，Switch C 为 AS 内部的一台非 BGP 交换机。

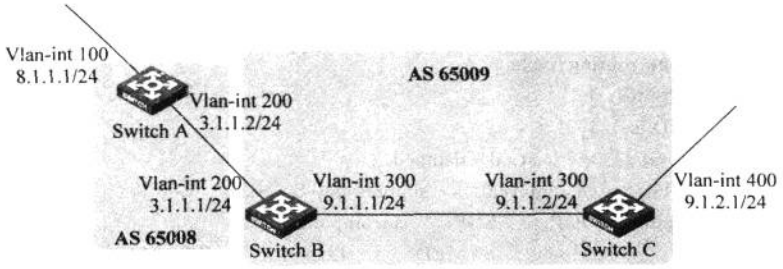


图 8-21 BGP 与 IGP 交互典型配置组网图

(3) 通过配置 BGP 与 IGP 的相互引入使 Switch A 和 Switch C 可以互相通信。

(4) 在 Switch B 上配置路由聚合向 Switch A 发布聚合网段路由。

4. 配置过程和解释

(1) 配置各接口的 IP 地址(略)。

(2) 配置 OSPF(略)。

(3) 配置 EBGP 连接。

① 配置 Switch A,启动 BGP,并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] bgp 65008
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] peer 3.1.1.1 as-number 65009
```

② 将 8.1.1.0/24 网段通告到 BGP 路由表中。

```
[SwitchA-bgp] network 8.1.1.0 24
[SwitchA-bgp] quit
```

③ 配置 Switch B,启动 BGP,并设置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] bgp 65009
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] peer 3.1.1.2 as-number 65008
[SwitchB-bgp] quit
```

(4) 配置 BGP 与 IGP 交互。

① 在 Switch B 上配置 BGP 引入 OSPF 路由。

```
[SwitchB] bgp 65009
[SwitchB-bgp] import-route ospf 1
[SwitchB-bgp] quit
```

② 查看 Switch A 的路由表。

```
[SwitchA] display bgp routing-table
 Total Number of Routes: 3
 BGP Local router ID is 1.1.1.1
```

```
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
   Network          NextHop        MED        LocPrf    PrefVal  Path/Ogn
*> 8.1.1.0/24       0.0.0.0        0                    0        i
*> 9.1.1.0/24       3.1.1.1        0                    0        65009?
*> 9.1.2.0/24       3.1.1.1        2                    0        65009?
```

③ 在 Switch B 上配置 OSPF 引入 BGP 路由。

```
[SwitchB] ospf
[SwitchB-ospf-1] import-route bgp
[SwitchB-ospf-1] quit
```

④ 显示 Switch C 的路由表。

```
<SwitchC> display ip routing-table
Routing Tables: Public
         Destinations : 7        Routes : 7
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
8.1.1.0/24          O_ASE   150  1         9.1.1.1         Vlan300
9.1.1.0/24          Direct  0    0         9.1.1.2         Vlan300
9.1.1.2/32          Direct  0    0         127.0.0.1       InLoop0
9.1.2.0/24          Direct  0    0         9.1.2.1         Vlan400
9.1.2.1/32          Direct  0    0         127.0.0.1       InLoop0
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop0
```

(5) 配置路由自动聚合。

① 配置 Switch B。

```
[SwitchB] bgp 65009
[SwitchB-bgp] summary automatic
```

② 显示 Switch A 的 BGP 路由表。

```
[SwitchA] display bgp routing-table
 Total Number of Routes: 2
 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history, i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
    Network          NextHop        MED        LocPrf    PrefVal  Path/Ogn
 *> 8.1.1.0/24       0.0.0.0        0                    0        i
 *> 9.0.0.0          3.1.1.1                             0        65009?
```

③ 使用 ping 进行验证。

```
[SwitchA] ping -a 8.1.1.1 9.1.2.1
  PING 9.1.2.1: 56 data bytes, press Ctrl_C to break
    Reply from 9.1.2.1: bytes=56 Sequence=1 ttl=254 time=15 ms
    Reply from 9.1.2.1: bytes=56 Sequence=2 ttl=254 time=31 ms
    Reply from 9.1.2.1: bytes=56 Sequence=3 ttl=254 time=47 ms
```

```
Reply from 9.1.2.1: bytes=56 Sequence=4 ttl=254 time=46 ms
Reply from 9.1.2.1: bytes=56 Sequence=5 ttl=254 time=47 ms
--- 9.1.2.1 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 15/37/47 ms
```

提示：通过 import-route 命令引入到 BGP 路由表中的路由的 ORIGIN 属性为 Incomplete。使用 network 命令发布到 BGP 路由表中的网段路由的 ORIGIN 属性为 IGP。

要发布的网段路由必须存在于本地的 IP 路由表中，使用路由策略可以更为灵活地控制所发布的路由。

8.5.3 BGP 负载分担典型配置指导

基于迭代的 BGP 负载分担，即如果依赖路由本身是负载分担的(假设有 3 个下一跳地址)，则 BGP 也会生成相同数量的下一跳地址来指导报文转发。需要说明的是，基于迭代的 BGP 负载分担并不需要命令配置，这一特性在交换机上始终启用。

在实现方法上，BGP 的负载分担与 IGP 的负载分担有所不同。

(1) IGP 是通过协议定义的路由算法，对到达同一目的地址的不同路由，根据计算结果，将度量值(Metric)相等的路由(如 RIP、OSPF)进行负载分担，选择的标准很明确(按 Metric)。

(2) BGP 本身并没有路由计算的算法，它只是一个选路的路由协议，因此，不能根据一个明确的度量值决定是否对路由进行负载分担。但 BGP 有丰富的选路规则，可以在对路由进行一定的选择后，有条件地进行负载分担，也就是将负载分担加入到 BGP 的选路规则中去。

MED 属性仅在相邻两个 AS 之间交换，收到此属性的 AS 一方不会再将其通告给任何其他第三方 AS。

MED 属性相当于 IGP 使用的度量值(Metric)，它用于判断流量进入 AS 时的最佳路由。当一个运行 BGP 的路由器通过不同的 EBGP 对等体得到目的地址相同但下一跳不同的多条路由时，在其他条件相同的情况下，将优先选择 MED 值较小者作为最佳路由。

1. 背景

M 公司两地测试中心之间通过 BGP 路由协议进行部署，北京测试中心有两台 BGP 出口交换机均连接到上海测试中心，正常情况下上海测试中心的 BGP 出口交换机只会选择其中一台作为最优下一跳，但这样会使的另外一条线路长期处于空闲状态。IT 维护部门通过对 BGP 配置负载分担，来使两条线路都能被合理地利用。

2. 组网图

图 8-22 所示为 BGP 负载分担典型配置组网图。

3. 配置需求

(1) 所有交换机都配置 BGP，Switch A 在 AS 65008 中，Switch B 和 Switch C 在 AS 65009 中。

(2) Switch A 与 Switch B、Switch C 之间运行 EBGP，Switch B 和 Switch C 之间运行

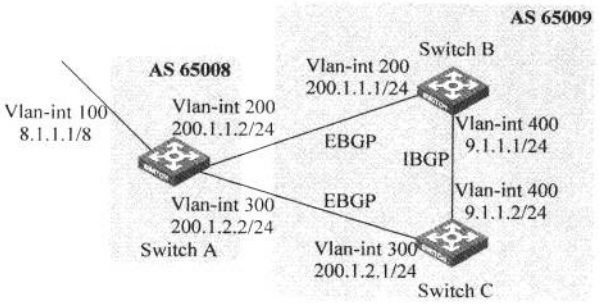


图 8-22 BGP 负载分担典型配置组网图

IBGP。

(3) 在 Switch A 上配置负载分担的路由条数为 2,以提高链路利用率。

4. 配置过程和解释

(1) 配置各接口的 IP 地址(略)。

(2) 配置 BGP 连接。

① 配置 Switch A,启动 BGP,并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] bgp 65008
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] peer 200.1.1.1 as-number 65009
[SwitchA-bgp] peer 200.1.2.1 as-number 65009
```

② 将 8.0.0.0/8 网段路由通告到 BGP 路由表中。

```
[SwitchA-bgp] network 8.0.0.0 255.0.0.0
[SwitchA-bgp] quit
```

③ 配置 Switch B,启动 BGP,并设置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] bgp 65009
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] peer 200.1.1.2 as-number 65008
[SwitchB-bgp] peer 9.1.1.2 as-number 65009
[SwitchB-bgp] network 9.1.1.0 255.255.255.0
[SwitchB-bgp] quit
```

④ 配置 Switch C,启动 BGP,并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
[SwitchC] bgp 65009
[SwitchC-bgp] router-id 3.3.3.3
[SwitchC-bgp] peer 200.1.2.2 as-number 65008
[SwitchC-bgp] peer 9.1.1.1 as-number 65009
[SwitchC-bgp] network 9.1.1.0 255.255.255.0
[SwitchC-bgp] quit
```

⑤ 查看 Switch A 的路由表。

```
[SwitchA] display bgp routing-table
 Total Number of Routes: 3
 BGP Local router ID is 1.1.1.1
 Status codes:  * - valid, > - best, d - damped,
                h - history, i - internal, s - suppressed, S - Stale
                Origin : i - IGP, e - EGP, ? - incomplete
    Network          NextHop        MED        LocPrf     PrefVal  Path/Ogn
 *> 8.0.0.0          0.0.0.0        0                     0        i
 *> 9.1.1.0/24       200.1.1.1      0                     0        65009i
 *                   200.1.2.1      0                     0        65009i
```

从路由表中可以看出，到目的地址 9.1.1.0/24 有两条有效路由，其中下一跳为 200.1.1.1 的路由是最优路由(因为 Switch B 的路由器 ID 要小一些)。

(3) 配置负载分担。

① 配置 Switch A。

```
[SwitchA] bgp 65008
[SwitchA-bgp] balance 2
[SwitchA-bgp] quit
```

② 查看 Switch A 的路由表。

```
[SwitchA] display bgp routing-table
 Total Number of Routes: 3
 BGP Local router ID is 1.1.1.1
 Status codes:  * - valid, > - best, d - damped,
                h - history, i - internal, s - suppressed, S - Stale
                Origin : i - IGP, e - EGP, ? - incomplete
    Network          NextHop        MED        LocPrf     PrefVal  Path/Ogn
 *> 8.0.0.0          0.0.0.0        0                     0        i
 *> 9.1.1.0/24       200.1.1.1      0                     0        65009i
 *>                  200.1.2.1      0                     0        65009i
```

从路由表中可以看到，BGP 路由 9.1.1.0/24 存在两个下一跳，分别是 200.1.1.1 和 200.1.2.1，且都是最优路由。

提示：BGP 只对 AS_PATH 属性、ORIGIN 属性、LOCAL_PREF 和 MED 值完全相同的路由进行负载分担。

BGP 负载分担特性适用于 EBGP、IBGP 以及联盟之间。

如果有多条到达同一目的地的路由，则根据配置的路由条数选择多条路由进行负载分担。

8.5.4 BGP 团体典型配置指导

对等体组可以使一组对等体共享相同的策略，而利用团体可以使多个 AS 中的一组 BGP 路由器共享相同的策略。团体是一个路由属性，在 BGP 对等体之间传播，它并不受到 AS 范围的限制。

BGP 路由器在将带有团体属性的路由发布给其他对等体之前，可以改变此路由原有的团体属性。

除了使用公认的团体属性外，用户还可以使用团体属性列表自定义扩展团体属性，以便更为灵活地控制路由策略。

1. 背景

M 公司两地研发中心、测试中心之间采用 BGP 进行部署，IT 维护人员小 L 在进行路由优化和维护时发现，有很多路由的目的地址是分散的，用目的地址的方式对路由进行划分和处理很不方便。因此小 L 开始利用 BGP 的团体属性对地址散列的一系列路由进行团体化，以便于后期对于 BGP 路由的优化。

2. 组网图

图 8-23 所示为 BGP 团体典型配置组网图。

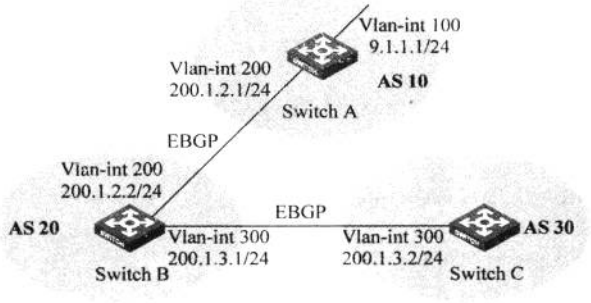


图 8-23 BGP 团体典型配置组网图

3. 配置需求

(1) Switch B 分别与 Switch A、Switch C 之间建立 EBGP 连接。

(2) 通过在 Switch A 上配置 NO_EXPORT 团体属性，使得 AS 10 发布到 AS 20 中的路由不再被 AS 20 向其他 AS 发布。

4. 配置过程和解释

(1) 配置各接口的 IP 地址(略)。

(2) 配置 EBGP。

① 配置 Switch A，启动 BGP，并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] bgp 10
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] peer 200.1.2.2 as-number 20
[SwitchA-bgp] network 9.1.1.0 255.255.255.0
[SwitchA-bgp] quit
```

② 配置 Switch B，启动 BGP，并设置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] bgp 20
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] peer 200.1.2.1 as-number 10
```

```
[SwitchB-bgp] peer 200.1.3.2 as-number 30
[SwitchB-bgp] quit
```

③ 配置 Switch C，启动 BGP，并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
[SwitchC] bgp 30
[SwitchC-bgp] router-id 3.3.3.3
[SwitchC-bgp] peer 200.1.3.1 as-number 20
[SwitchC-bgp] quit
```

④ 查看 Switch B 的路由表。

```
[SwitchB] display bgp routing-table 9.1.1.0
 BGP local router ID : 2.2.2.2
 Local AS number : 20
 Paths:1 available, 1 best
BGP routing table entry information of 9.1.1.0/24:
 From: 200.1.2.1 (1.1.1.1)
 Original nexthop: 200.1.2.1
 AS-path: 10
 Origin: igp
 Attribute value: MED 0, pref-val 0, pre 255
 State: valid, external, best,
 Advertised to such 1 peers: 200.1.3.2
```

可以看出，Switch B 将收到的路由发布给了位于 AS 30 内的 Switch C。

⑤ 查看 Switch C 的路由表。

```
[SwitchC] display bgp routing-table
 Total Number of Routes: 1
 BGP Local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - damped,
               h - history, i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
    Network          NextHop        MED        LocPrf    PrefVal   Path/Ogn
 *> 9.1.1.0/24       200.1.3.1                 0         20        10i
```

从路由表可以确认，Switch C 从 Switch B 那里学到了目的地址为 9.1.1.0/24 的路由。

(3) 配置 BGP 团体属性。

① 配置路由策略。

```
[SwitchA] route-policy comm_policy permit node 0
[SwitchA-route-policy] apply community no-export
[SwitchA-route-policy] quit
```

② 应用路由策略。

```
[SwitchA] bgp 10
[SwitchA-bgp] peer 200.1.2.2 route-policy comm_policy export
[SwitchA-bgp] peer 200.1.2.2 advertise-community
```

③ 查看 Switch B 的路由表。

```
[SwitchB] display bgp routing-table 9.1.1.0
 BGP local router ID : 2.2.2.2
 Local AS number : 20
 Paths: 1 available, 1 best
 BGP routing table entry information of 9.1.1.0/24:
 From: 200.1.2.1 (1.1.1.1)
 Original nexthop: 200.1.2.1
 Community: No-Export
 AS-path: 10
 Origin: igp
 Attribute value: MED 0, pref-val 0, pre 255
 State: valid, external, best,
 Not advertised to any peers yet
```

在 Switch B 的 BGP 路由表中可以看到配置的团体属性，此时在 Switch C 的 BGP 路由表中已经没有到目的地址 9.1.1.0/24 的路由了。

8.5.5 BGP 路由反射器典型配置指导

为保证 IBGP 对等体之间的连通性，需要在 IBGP 对等体之间建立全连接关系。假设在一个 AS 内部有 n 台路由器，那么应该建立的 IBGP 连接数就为 $n(n-1)/2$。当 IBGP 对等体数目很多时，对网络资源和 CPU 资源的消耗都很大。

利用路由反射可以解决这一问题。在一个 AS 内，其中一台路由器作为路由反射器 RR (Router Reflector)，其他路由器作为客户机(Client)与路由反射器之间建立 IBGP 连接。路由反射器在客户机之间传递(反射)路由信息，而客户机之间不需要建立 BGP 连接。

既不是反射器也不是客户机的 BGP 路由器称为非客户机(Non-Client)。非客户机与路由反射器之间，以及所有的非客户机之间仍然必须建立全连接关系。

1. 背景

M 公司 IT 管理人员小 L 在进行 BGP 路由部署时发现，为了避免 IBGP 对等体之间学习的路由不再互相转发现象的发生，必须在所有 IBGP 交换机之间建立全连接关系，随着 IBGP 交换机数量的上升，全连接关系也呈平方数增长的现象成为一个问题。经过研究，小 L 最终通过在 AS 内配置路由反射器成功地解决了这一难题。

2. 组网图

图 8-24 所示为 BGP 路由反射器典型配置组网图。

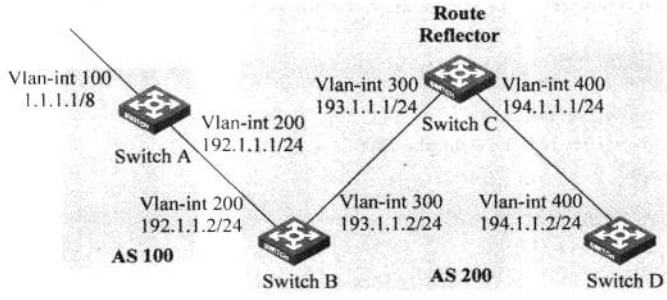


图 8-24 BGP 路由反射器典型配置组网图

3. 配置需求

(1) 所有交换机运行 BGP 协议，Switch A 与 Switch B 建立 EBGP 连接，Switch C 与 Switch B 和 Switch D 之间建立 IBGP 连接。

(2) Switch C 作为路由反射器，Switch B 和 Switch D 为 Switch C 的客户机。

(3) Switch D 能够通过 Switch C 学到路由 1.0.0.0/8。

4. 配置过程和解释

(1) 配置各接口的 IP 地址(略)。

(2) 配置 BGP 连接。

① 配置 Switch A，启动 BGP，并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] bgp 100
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] peer 192.1.1.2 as-number 200
```

② 通告 1.0.0.0/8 网段路由到 BGP 路由表中。

```
[SwitchA-bgp] network 1.0.0.0
[SwitchA-bgp] quit
```

③ 配置 Switch B，启动 BGP，并设置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] bgp 200
[SwitchB-bgp] router-id 2 2.2.2
[SwitchB-bgp] peer 192.1.1.1 as-number 100
[SwitchB-bgp] peer 193.1.1.1 as-number 200
[SwitchB-bgp] peer 193.1.1.1 next-hop-local
[SwitchB-bgp] quit
```

④ 配置 Switch C，启动 BGP，并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
[SwitchC] bgp 200
[SwitchC-bgp] router-id 3.3.3.3
[SwitchC-bgp] peer 193.1.1.2 as-number 200
[SwitchC-bgp] peer 194.1.1.2 as-number 200
[SwitchC-bgp] quit
```

⑤ 配置 Switch D，启动 BGP，并设置其 Router ID 为 4.4.4.4。

```
<SwitchD> system-view
[SwitchD] bgp 200
[SwitchD-bgp] router-id 4.4.4.4
[SwitchD-bgp] peer 194.1.1.1 as-number 200
[SwitchD-bgp] quit
```

(3) 配置路由反射器。

配置 Switch C：

```
[SwitchC] bgp 200
```

```
[SwitchC-bgp] peer 193.1.1.2 reflect-client
[SwitchC-bgp] peer 194.1.1.2 reflect-client
[SwitchC-bgp] quit
```

(4) 验证配置效果。

① 查看 Switch B 的 BGP 路由表。

```
[SwitchB] display bgp routing-table
 Total Number of Routes: 1
 BGP Local router ID is 2.2.2.2
 Status codes:  * - valid, > - best, d - damped,
                h - history, i - internal, s - suppressed, S - Stale
                Origin : i - IGP, e - EGP, ? - incomplete
    Network         NextHop         MED         LocPrf    PrefVal    Path/Ogn
 *> 1.0.0.0         192.1.1.1       0                     0          100i
```

② 查看 Switch D 的 BGP 路由表。

```
[SwitchD] display bgp routing-table
 Total Number of Routes: 1
 BGP Local router ID is 4.4.4.4
 Status codes:  * - valid, > - best, d - damped,
                h - history, i - internal, s - suppressed, S - Stale
                Origin : i - IGP, e - EGP, ? - incomplete
    Network         NextHop         MED         LocPrf    PrefVal    Path/Ogn
 i 1.0.0.0         193.1.1.2       0           100       0          100i
```

可以看出，Switch D 从 Switch C 已经学到了 1.0.0.0/8 路由。

提示：通常情况下，路由反射器的客户之间不要求是全连接的，路由默认通过反射器从一个客户反射到其他客户；如果客户之间是全连接的，可以禁止客户间的反射，以便减少开销。

禁止客户机之间的路由反射后，客户机到非客户机之间的路由仍然可以被反射。

通常，一个集群里只有一个路由反射器，此时是由反射器的路由器 ID 来识别该集群的。设置多个路由反射器可提高网络的稳定性。如果一个集群中配有多个路由反射器，可使用相关命令为所有的路由反射器配置同样的集群 ID，以避免路由环路。

8.5.6 BGP 联盟典型配置指导

联盟(Confederation)是处理 AS 内部的 IBGP 网络连接激增的另一种方法，它将一个自治系统划分为若干个子自治系统，每个子自治系统内部的 IBGP 对等体建立全连接关系，子自治系统之间建立 EBGP 连接关系。

在不属于联盟的 BGP 发言者看来，属于同一个联盟的多个子自治系统是一个整体，外界不需要了解内部的子自治系统情况，联盟 ID 就是标识联盟这一整体的自治系统号。

联盟的缺陷是，从非联盟方案向联盟方案转变时，要求路由器重新进行配置，逻辑拓扑也要改变。

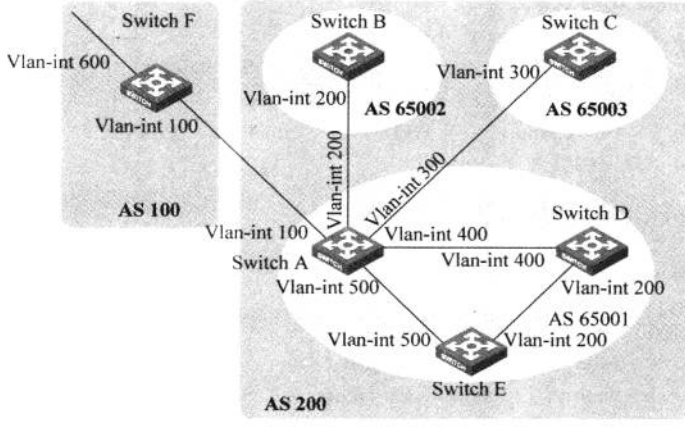
在大型 BGP 网络中，路由反射器和联盟可以被同时使用。

1. 背景

M公司在部署BGP网络时，随着BGP网络规模的扩大，为了避免IBGP全连接关系，一般采用AS内配置路由反射器的方式解决。IT维护人员小L在部署中发现联盟与子自治制系统方式也可以很好地解决IBGP全连接的问题，因而开始在部署中广泛地应用。

2. 组网图

图8-25所示为BGP联盟典型配置组网图。



设　备	接　口	IP地址	设　备	接　口	IP地址
Switch A	Vlan-int 100	200.1.1.1/24	Switch D	Vlan-int 200	10.1.5.1/24
	Vlan-int 200	10.1.1.1/24		Vlan-int 400	10.1.3.2/24
	Vlan-int 300	10.1.2.1/24	Switch E	Vlan-int 200	10.1.5.2/24
	Vlan-int 400	10.1.3.1/24		Vlan-int 500	10.1.4.2/24
	Vlan-int 500	10.1.4.1/24	Switch F	Vlan-int 100	200.1.1.2/24
Switch B	Vlan-int 200	10.1.1.2/24		Vlan-int 600	9.1.1.1/24
Switch C	Vlan-int 300	10.1.2.2/24			

图8-25　BGP联盟典型配置组网图

3. 配置需求

AS 200中有多台BGP交换机，为了减少IBGP的连接数，现将它们划分为3个子自治系统：AS 65001、AS 65002和AS 65003，其中AS 65001内的3台交换机建立IBGP全连接。

4. 配置过程和解释

(1) 配置各接口的IP地址(略)。

(2) 配置BGP联盟。

① 配置Switch A，启动BGP，并设置其Router ID为1.1.1.1。

```
<SwitchA> system-view
[SwitchA] bgp 65001
[SwitchA-bgp] router-id 1.1.1.1
```

```
[SwitchA-bgp] confederation id 200
[SwitchA-bgp] confederation peer-as 65002 65003
[SwitchA-bgp] peer 10.1.1.2 as-number 65002
[SwitchA-bgp] peer 10.1.1.2 next-hop-local
[SwitchA-bgp] peer 10.1.2.2 as-number 65003
[SwitchA-bgp] peer 10.1.2.2 next-hop-local
[SwitchA-bgp] quit
```

② 配置 Switch B,启动 BGP,并设置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] bgp 65002
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] confederation id 200
[SwitchB-bgp] confederation peer-as 65001 65003
[SwitchB-bgp] peer 10.1.1.1 as-number 65001
[SwitchB-bgp] quit
```

③ 配置 Switch C,启动 BGP,并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
[SwitchC] bgp 65003
[SwitchC-bgp] router-id 3.3.3.3
[SwitchC-bgp] confederation id 200
[SwitchC-bgp] confederation peer-as 65001 65002
[SwitchC-bgp] peer 10.1.2.1 as-number 65001
[SwitchC-bgp] quit
```

(3) 配置 AS 65001 内的 IBGP 连接。

① 配置 Switch A。

```
[SwitchA] bgp 65001
[SwitchA-bgp] peer 10.1.3.2 as-number 65001
[SwitchA-bgp] peer 10.1.3.2 next-hop-local
[SwitchA-bgp] peer 10.1.4.2 as-number 65001
[SwitchA-bgp] peer 10.1.4.2 next-hop-local
[SwitchA-bgp] quit
```

② 配置 Switch D,启动 BGP,并设置其 Router ID 为 4.4.4.4。

```
<SwitchD> system-view
[SwitchD] bgp 65001
[SwitchD-bgp] router-id 4.4.4.4
[SwitchD-bgp] confederation id 200
[SwitchD-bgp] peer 10.1.3.1 as-number 65001
[SwitchD-bgp] peer 10.1.5.2 as-number 65001
[SwitchD-bgp] quit
```

③ 配置 Switch E,启动 BGP,并设置其 Router ID 为 5.5.5.5。

```
<SwitchE> system-view
[SwitchE] bgp 65001
```

```
[SwitchE-bgp] router-id 5.5.5.5
[SwitchE-bgp] confederation id 200
[SwitchE-bgp] peer 10.1.4.1 as-number 65001
[SwitchE-bgp] peer 10.1.5.1 as-number 65001
[SwitchE-bgp] quit
```

(4) 配置 AS 100 和 AS 200 之间的 EBGP 连接。

① 配置 Switch A。

```
[SwitchA] bgp 65001
[SwitchA-bgp] peer 200.1.1.2 as-number 100
[SwitchA-bgp] quit
```

② 配置 Switch F。

```
<SwitchF> system-view
[SwitchF] bgp 100
[SwitchF-bgp] router-id 6.6.6.6
[SwitchF-bgp] peer 200.1.1.1 as-number 200
[SwitchF-bgp] network 9.1.1.0 255.255.255.0
[SwitchF-bgp] quit
```

(5) 验证配置结果。

① 查看 Switch B 的 BGP 路由表。

```
[SwitchB] display bgp routing-table
 Total Number of Routes: 1
 BGP Local router ID is 2.2.2.2
 Status codes:  * - valid, > - best, d - damped,
                h - history, i - internal, s - suppressed, S - Stale
                Origin : i - IGP, e - EGP, ? - incomplete
     Network          NextHop        MED        LocPrf    PrefVal   Path/Ogn
 *>i 9.1.1.0/24       10.1.1.1       0          100       0         (65001) 100i

[SwitchB] display bgp routing-table 9.1.1.0
 BGP local router ID : 2.2.2.2
 Local AS number : 65002
 Paths: 1 available, 1 best

 BGP routing table entry information of 9.1.1.0/24:
 From: 10.1.1.1 (1.1.1.1)
 Relay Nexthop: 0.0.0.0
 Original nexthop: 10.1.1.1
 AS-path: (65001) 100
 Origin: igp
 Attribute value: MED 0, localpref 100, pref-val 0, pre 255
 State: valid, external-confed, best,
 Not advertised to any peers yet
```

② 查看 Switch D 的 BGP 路由表。

```
[SwitchD] display bgp routing-table
 Total Number of Routes: 1
 BGP Local router ID is 4.4.4.4
 Status codes: * - valid, > - best, d - damped,
               h - history, i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
    Network          NextHop        MED        LocPrf    PrefVal  Path/Ogn
 *>i 9.1.1.0/24      10.1.3.1       0          100       0        100i

[SwitchD] display bgp routing-table 9.1.1.0
 BGP local router ID : 4.4.4.4
 Local AS number : 65001
 Paths: 1 available, 1 best

 BGP routing table entry information of 9.1.1.0/24:
 From: 10.1.3.1 (1.1.1.1)
 Relay Nexthop: 0.0.0.0
 Original nexthop: 10.1.3.1
 AS-path: 100
 Origin: igp
 Attribute value: MED 0, localpref 100, pref-val 0, pre 255
 State: valid, internal, best,
 Not advertised to any peers yet
```

8.5.7 BGP 路径选择典型配置指导

BGP 选择路由时采取如下策略。

(1) 首先丢弃下一跳(NEXT_HOP)不可达的路由。

(2) 优选 Preferred-value 值最大的路由。

(3) 优选本地优先级(LOCAL_PREF)最高的路由。

(4) 优选本路由器始发的路由。

(5) 优选 AS 路径(AS_PATH)最短的路由。

(6) 依次选择 ORIGIN 类型为 IGP、EGP、Incomplete 的路由。

(7) 优选 MED 值最低的路由。

(8) 依次选择从 EBGP、联盟、IBGP 学来的路由。

(9) 优选下一跳 Cost 值最低的路由。

(10) 优选 CLUSTER_LIST 长度最短的路由。

(11) 优选 ORIGINATOR_ID 最小的路由。

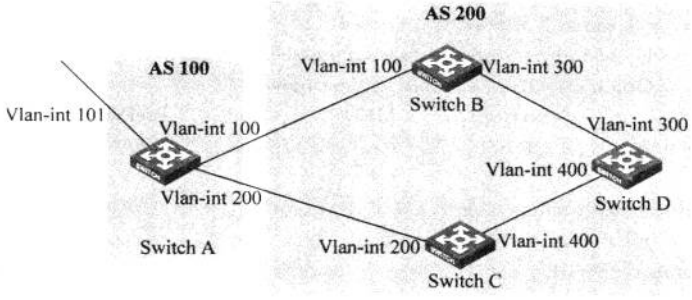
(12) 优选 Router ID 最小的路由器发布的路由。

1. 背景

M 公司广域网间全部使用 BGP 协议进行部署，由于公司规模扩大，BGP 网络也日渐复杂，网络中有时会出现次优路径以及负载不均的情况。IT 维护人员小 L 通过对多项 BGP 路由属性的综合控制，达到对 BGP 选路进行优化的目的，使公司业务的广域网路径简单而且易于维护。

2. 组网图

图 8-26 所示为 BGP 路径选择典型配置组网图。



设　备	接　口	IP 地址	设　备	接　口	IP 地址
Switch A	Vlan-int 101	1.0.0.1/8	Switch D	Vlan-int 400	195.1.1.1/24
	Vlan-int 100	192.1.1.1/24		Vlan-int 300	194.1.1.1/24
	Vlan-int 200	193.1.1.1/24	Switch C	Vlan-int 400	195.1.1.2/24
Switch B	Vlan-int 100	192.1.1.2/24		Vlan-int 200	193.1.1.2/24
	Vlan-int 300	194.1.1.2/24			

图 8-26　BGP 路径选择典型配置组网图

3. 配置需求

(1) 所有交换机都运行 BGP 协议。Switch A 与 Switch B 和 Switch C 之间运行 EBGP；Switch D 与 Switch B 和 Switch C 之间运行 IBGP。

(2) AS 200 中运行 OSPF 协议。

(3) 配置不同的路由策略，使得 Switch D 优选 Switch C 学到的 1.0.0.0/8 路由。

4. 配置过程和解释

(1) 配置各接口的 IP 地址(略)。

(2) 配置 Switch B、Switch C 和 Switch D 之间运行 OSPF 协议。

① 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

② 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 193.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

③ 配置 Switch D。

```
<SwitchD> system-view
[SwitchD] ospf
[SwitchD-ospf] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

(3) 配置 BGP 连接。

① 配置 Switch A。

```
<SwitchA> system-view
[SwitchA] bgp 100
[SwitchA-bgp] peer 192.1.1.2 as-number 200
[SwitchA-bgp] peer 193.1.1.2 as-number 200
```

② 将 1.0.0.0/8 网段通告到 Switch A 的 BGP 路由表中。

```
[SwitchA-bgp] network 1.0.0.0 8
[SwitchA-bgp] quit
```

③ 配置 Switch B。

```
[SwitchB] bgp 200
[SwitchB-bgp] peer 192.1.1.1 as-number 100
[SwitchB-bgp] peer 194.1.1.1 as-number 200
[SwitchB-bgp] quit
```

④ 配置 Switch C。

```
[SwitchC] bgp 200
[SwitchC-bgp] peer 193.1.1.1 as-number 100
[SwitchC-bgp] peer 195.1.1.1 as-number 200
[SwitchC-bgp] quit
```

⑤ 配置 Switch D。

```
[SwitchD] bgp 200
[SwitchD-bgp] peer 194.1.1.2 as-number 200
[SwitchD-bgp] peer 195.1.1.2 as-number 200
[SwitchD-bgp] quit
```

(4) 通过配置 1.0.0.0/8 路由的不同属性值，使得 Switch D 优选 Switch C 学到的路由。

① 在 Switch A 上对发布给对等体 192.1.1.2 的 1.0.0.0/8 路由配置较高的 MED 属性值，使得 Switch D 优选 Switch C 学到的路由。

a. 定义编号为 2000 的 ACL，允许路由 1.0.0.0/8 通过。

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 1.0.0.0 0.255.255.255
[SwitchA-acl-basic-2000] quit
```

b. 定义两个 Route-policy，一个名为 apply_med_50，为路由 1.0.0.0/8 设置 MED 属性值为 50；另一个名为 apply_med_100，为路由 1.0.0.0/8 设置 MED 属性值为 100。

```
[SwitchA] route-policy apply_med_50 permit node 10
[SwitchA-route-policy] if-match acl 2000
[SwitchA-route-policy] apply cost 50
[SwitchA-route-policy] quit
[SwitchA] route-policy apply_med_100 permit node 10
[SwitchA-route-policy] if-match acl 2000
[SwitchA-route-policy] apply cost 100
[SwitchA-route-policy] quit
```

c. 对发布给对等体 193.1.1.2(Switch C)的路由应用名为 apply_med_50 的 Route-policy，对发布给对等体 192.1.1.2(Switch B)的路由应用名为 apply_med_100 的 Route-policy。

```
[SwitchA] bgp 100
[SwitchA-bgp] peer 193.1.1.2 route-policy apply_med_50 export
[SwitchA-bgp] peer 192.1.1.2 route-policy apply_med_100 export
[SwitchA-bgp] quit
```

d. 查看 Switch D 的 BGP 路由表。

```
[SwitchD] display bgp routing-table
 Total Number of Routes: 2
 BGP Local router ID is 194.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history, i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
    Network         NextHop         MED         LocPrf    PrefVal   Path/Ogn
 *>i 1.0.0.0        193.1.1.1       50          100       0         100i
 * i                192.1.1.1       100         100       0         100i
```

可以看到，Switch D 从 Switch C 学到 1.0.0.0/8 的路由是最优的。

② 在 Switch B 和 Switch C 上分别对 1.0.0.0/8 路由配置不同的本地优先级，使得 Switch D 优选 Switch C 学到的路由。

a. 在 Switch C 上定义编号为 2000 的 ACL，允许 1.0.0.0/8 路由通过。

```
[SwitchC] acl number 2000
[SwitchC-acl-basic-2000] rule permit source 1.0.0.0 0.255.255.255
[SwitchC-acl-basic-2000] quit
```

b. 在 Switch C 上定义名为 localpref 的 Route-policy，设置路由 1.0.0.0/8 的本地优先级为 200(默认的本地优先级为 100)。

```
[SwitchC] route-policy localpref permit node 10
[SwitchC-route-policy] if-match acl 2000
[SwitchC-route-policy] apply local-preference 200
[SwitchC-route-policy] quit
```

c. 为从 BGP 对等体 193.1.1.1 的路由应用名为 localpref 的 Route-policy。

```
[SwitchC] bgp 200
[SwitchC-bgp] peer 193.1.1.1 route-policy localpref import
[SwitchC-bgp] quit
```

d. 查看 Switch D 的 BGP 路由表。

```
[SwitchD] display bgp routing-table
 Total Number of Routes: 2
 BGP Local router ID is 194.1.1.1
 Status codes:  * - valid, > - best, d - damped,
                h - history, i - internal, s - suppressed, S - Stale
                Origin : i - IGP, e - EGP, ? - incomplete
    Network         NextHop       MED        LocPrf     PrefVal    Path/Ogn
 * >i 1.0.0.0       193.1.1.1     0          200        0          100i
 * i                 192.1.1.1     0          100        0          100i
```

可以看到，Switch D 从 Switch C 学到 1.0.0.0/8 的路由是最优的。

8.6 路由策略典型配置指导

8.6.1 在 IPv4 路由引入中应用路由策略典型配置指导

路由策略(Routing Policy)是为了改变网络流量所经过的途径而修改路由信息的技术，主要通过改变路由属性(包括可达性)来实现。

路由器在发布与接收路由信息时，可能需要实施一些策略，以便对路由信息进行过滤，例如，只接收或发布满足一定条件的路由信息。一种路由协议可能需要引入其他的路由协议发现的路由信息，路由器在引入其他路由协议的路由信息时，可能只需要引入一部分满足条件的路由信息，并控制所引入的路由信息的某些属性，以使其满足本协议的要求。

为实现路由策略，首先要定义将要实施路由策略的路由信息的特征，即定义一组匹配规则。可以以路由信息中的不同属性作为匹配依据进行设置，如目的地址、发布路由信息的路由器地址等。匹配规则可以预先设置好，然后再将它们应用于路由的发布、接收和引入等过程的路由策略中。

1. 背景

M 公司 IT 维护人员小 L 负责公司整网维护工作，涉及局域网和广域网范畴，因此，维护的路由协议也涉及 OSPF、RIP、IS-IS 以及 BGP 等 IPv4 路由协议。由于不同协议间路由要互通就必须在协议间进行相互引入，但某些情况下又必须对引入路由的过程进行严格的控制，避免路由重复引入、路由环路等问题的发生。因此小 L 在路由引入的过程中充分、合理地运用路由策略对路由属性进行修改，避免了错误路由的产生，很好地完成维护工作。

2. 组网图

图 8-27 所示为在 IPv4 路由引入中应用路由策略典型组网图。

3. 配置需求

如图 8-27 所示，Switch B 与 Switch A 之间通过 OSPF 协议交换路由信息，与 Switch C

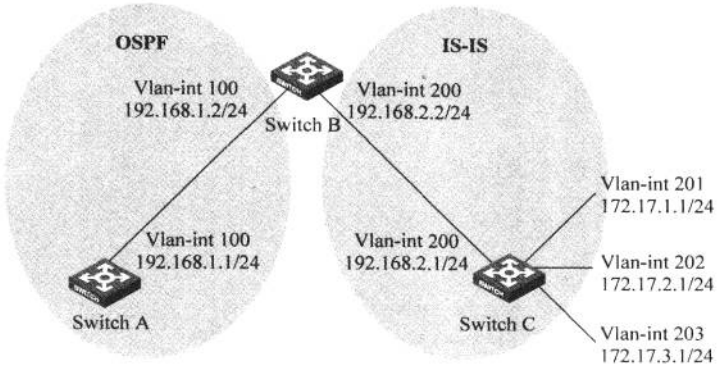


图 8-27 在 IPv4 路由引入中应用路由策略典型组网图

之间通过 IS-IS 协议交换路由信息。

要求在 Switch B 上配置路由引入，将 IS-IS 路由引入到 OSPF 中去，并同时使用路由策略设置路由的属性。其中，设置 172.17.1.0/24 的路由的开销为 100，设置 172.17.2.0/24 的路由的 Tag 属性为 20。

4. 配置过程和解释

(1) 配置各接口的 IP 地址(略)。

(2) 配置 IS-IS 路由协议。

① 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] isis
[SwitchC-isis-1] is-level level-2
[SwitchC-isis-1] network-entity 10.0000.0000.0001.00
[SwitchC-isis-1] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] isis enable
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 201
[SwitchC-Vlan-interface201] isis enable
[SwitchC-Vlan-interface201] quit
[SwitchC] interface vlan-interface 202
[SwitchC-Vlan-interface202] isis enable
[SwitchC-Vlan-interface202] quit
[SwitchC] interface vlan-interface 203
[SwitchC-Vlan-interface203] isis enable
[SwitchC-Vlan-interface203] quit
```

② 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] isis
[SwitchB-isis-1] is-level level-2
[SwitchB-isis-1] network-entity 10.0000.0000.0002.00
```

```
[SwitchB-isis-1] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] isis enable
[SwitchB-Vlan-interface200] quit
```

(3) 配置 OSPF 路由协议及路由引入。

① 配置 Switch A,启动 OSPF。

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

② 配置 Switch B,启动 OSPF,并引入 IS-IS 路由。

```
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] import-route isis 1
[SwitchB-ospf-1] quit
```

③ 查看 SwitchA 的 OSPF 路由表,可以看到引入的路由。

```
[SwitchA] display ospf routing
          OSPF Process 1 with Router ID 192.168.1.1
                Routing Tables
 Routing for Network
 Destination        Cost   Type       NextHop         AdvRouter       Area
 192.168.1.0/24     1562   Stub       192.168.1.1     192.168.1.1     0.0.0.0

 Routing for ASEs
 Destination        Cost   Type       Tag    NextHop         AdvRouter
 172.17.1.0/24      1      Type2      1      192.168.1.2     192.168.2.2
 172.17.2.0/24      1      Type2      1      192.168.1.2     192.168.2.2
 172.17.3.0/24      1      Type2      1      192.168.1.2     192.168.2.2
 Total Nets: 4
 Intra Area: 1  Inter Area: 0  ASE: 3  NSSA: 0
```

(4) 配置过滤列表。

① 配置编号为 2002 的 ACL,允许 172.17.2.0/24 的路由通过。

```
[SwitchB] acl number 2002
[SwitchB-acl-basic-2002] rule permit source 172.17.2.0 0.0.0.255
[SwitchB-acl-basic-2002] quit
```

② 配置名为 prefix-a 的地址前缀列表,允许 172.17.1.0/24 的路由通过。

```
[SwitchB] ip ip-prefix prefix-a index 10 permit 172.17.1.0 24
```

(5) 配置路由策略。

```
[SwitchB] route-policy isis2ospf permit node 10
[SwitchB-route-policy] if-match ip-prefix prefix-a
[SwitchB-route-policy] apply cost 100
[SwitchB-route-policy] quit
[SwitchB] route-policy isis2ospf permit node 20
[SwitchB-route-policy] if-match acl 2002
[SwitchB-route-policy] apply tag 20
[SwitchB-route-policy] quit
[SwitchB] route-policy isis2ospf permit node 30
[SwitchB-route-policy] quit
```

(6) 在路由引入时应用路由策略。

① 配置 Switch B,设置在路由引入时应用路由策略。

```
[SwitchB] ospf
[SwitchB-ospf-1] import-route isis 1 route-policy isis2ospf
[SwitchB-ospf-1] quit
```

② 查看 Switch A 的 OSPF 路由表,可以看到目的地址为 172.17.1.0/24 的路由的开销为 100,目的地址为 172.17.2.0/24 的路由的标记域(Tag)为 20,而其他外部路由没有变化。

```
[SwitchA] display ospf routing
          OSPF Process 1 with Router ID 192.168.1.1
                    Routing Tables
 Routing for Network
 Destination        Cost    Type       NextHop         AdvRouter       Area
 192.168.1.0/24     1       Transit    192.168.1.1     192.168.1.1     0.0.0.0
 Routing for ASEs
 Destination        Cost    Type       Tag             NextHop         AdvRouter
 172.17.1.0/24      100     Type2      1               192.168.1.2     192.168.2.2
 172.17.2.0/24      1       Type2      20              192.168.1.2     192.168.2.2
 172.17.3.0/24      1       Type2      1               192.168.1.2     192.168.2.2
 192.168.2.0/24     1       Type2      1               192.168.1.2     192.168.2.2
 Total Nets: 5
 Intra Area: 1  Inter Area: 0  ASE: 4  NSSA: 0
```

提示：permit 指定节点的匹配模式为允许模式。当路由信息通过该节点的过滤后,将执行该节点的 apply 子句,不进入下一个节点的测试;如果路由信息没有通过该节点过滤,将进入下一个节点继续测试。

deny 指定节点的匹配模式为拒绝模式(此模式下 apply 子句不会被执行)。当路由项满足该节点的所有 if-match 子句时,将不执行 apply 子句,不进入下一个节点的测试;如果路由项不满足该节点的 if-match 子句,将进入下一个节点继续测试。

如果路由策略中定义了一个以上的节点,则各节点中至少应该有一个节点的匹配模式是 permit。当路由策略用于路由信息过滤时,如果某路由信息没有通过任一节点,则认为该路由信息没有通过该路由策略。如果路由策略的所有节点都是 deny 模式,则没有路由信息能通过该路由策略。

对于同一个 Route-policy 节点，在匹配的过程中，各个 if-match 子句间是“与”的关系，即路由信息必须同时满足所有匹配条件，才可以执行 apply 子句的动作。

在一个节点中，可以没有 if-match 子句，也可以有多个 if-match 子句。当不指定 if-match 子句时，如果该节点的匹配模式为允许模式，则所有路由信息都会通过该节点的过滤；如果该节点的匹配模式为拒绝模式，则所有路由信息都会被拒绝。

8.6.2 应用路由策略过滤 BGP 路由典型配置指导

1. 背景

M 公司两地间采用 BGP 路由协议进行部署，在业务部署初期没有对 BGP 路由进行控制策略，但随着网络日渐成熟，业务模型也发生一些调整，原有的 BGP 路由需要进行更改，有些路由需要隔离。IT 维护人员小 L 通过使用路由策略对 BGP 对等体间接收路由进行过滤，对 AS 域间 BGP 路由进行了有效的控制。

2. 组网图

图 8-28 所示为应用路由策略过滤 BGP 路由典型组网图。

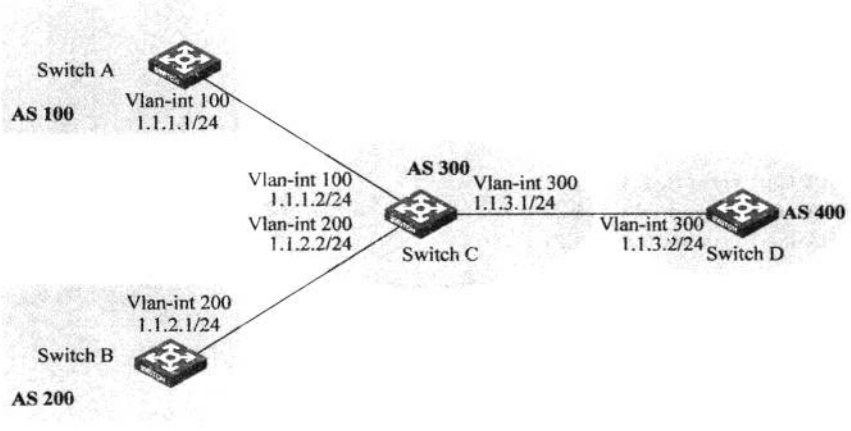


图 8-28 应用路由策略过滤 BGP 路由典型组网图

3. 配置需求

(1) 所有交换机均运行 BGP 协议，Switch A、Switch B 和 Switch C 之间建立 EBGP 连接，Switch C 和 Switch D 之间建立 EBGP 连接。

(2) 通过配置路由策略，使得 Switch D 拒绝接收来自 AS 200 的路由。

4. 配置过程和解释

(1) 配置接口 IP 地址(略)。

(2) 配置 BGP 基本功能。

① 配置 Switch A。

```
<SwitchA> system-view
[SwitchA] bgp 100
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] peer 1.1.1.2 as-number 300
```

② 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] bgp 200
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] peer 1.1.2.2 as-number 300
```

③ 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] bgp 300
[SwitchC-bgp] router-id 3.3.3.3
[SwitchC-bgp] peer 1.1.1.1 as-number 100
[SwitchC-bgp] peer 1.1.2.1 as-number 200
[SwitchC-bgp] peer 1.1.3.2 as-number 400
```

④ 配置 Switch D。

```
<SwitchD> system-view
[SwitchD] bgp 400
[SwitchD-bgp] router-id 4.4.4.4
[SwitchD-bgp] peer 1.1.3.1 as-number 300
[SwitchD-bgp] quit
```

⑤ 配置 Switch A,将网段路由 4.4.4.4/24、5.5.5.5/24、6.6.6.6/24 发布到 BGP 路由表中。

```
[SwitchA-bgp] network 4.4.4.4 24
[SwitchA-bgp] network 5.5.5.5 24
[SwitchA-bgp] network 6.6.6.6 24
```

⑥ 配置 Switch B,将网段路由 7.7.7.7/24、8.8.8.8/24、9.9.9.9/24 发布到 BGP 路由表中。

```
[SwitchB-bgp] network 7.7.7.7 24
[SwitchB-bgp] network 8.8.8.8 24
[SwitchB-bgp] network 9.9.9.9 24
```

⑦ 查看 Switch D 的 BGP 路由表。

```
[SwitchD-bgp] display bgp routing-table
 Total Number of Routes: 6
 BGP Local router ID is 4.4.4.4
 Status codes:  * - valid, > - best, d - damped,
                h - history, i - internal, s - suppressed, S - Stale
                Origin : i - IGP, e - EGP, ? - incomplete
    Network          NextHop         MED        LocPrf    PrefVal   Path/Ogn
 *> 4.4.4.0/24       1.1.3.1                               0         300 100i
 *> 5.5.5.0/24       1.1.3.1                               0         300 100i
 *> 6.6.6.0/24       1.1.3.1                               0         300 100i
 *> 7.7.7.0/24       1.1.3.1                               0         300 200i
 *> 8.8.8.0/24       1.1.3.1                               0         300 200i
 *> 9.9.9.0/24       1.1.3.1                               0         300 200i
```

从路由表可以看出,Switch D 同时学到了来自 AS 100 的路由 4.4.4.0/24、5.5.5.0/24、6.6.6.0/24 和来自 AS 200 的路由 7.7.7.0/24、8.8.8.0/24、9.9.9.0/24。

(3) 配置 Switch D 拒绝接收来自 AS 200 的路由。

① 在 Switch D 上配置编号为 1 的 AS 路径过滤列表。

```
[SwitchD] ip as-path 1 permit . * 200. *
```

② 在 Switch D 上配置名称为“rt1”的路由策略。

```
[SwitchD] route-policy rt1 deny node 1
[SwitchD] if-match as-path 1
[SwitchD] route-policy rt2 permit node 2
```

③ 在 Switch D 上,配置对从对等体 1.1.3.1 接收的路由指定名称为“rt1”的路由策略。

```
[SwitchD] bgp 400
[SwitchD] peer 1.1.3.1 route-policy rt1 import
```

④ 查看 Switch D 的 BGP 路由表。

```
[SwitchD] display bgp routing-table
 Total Number of Routes: 3
 BGP Local router ID is 4.4.4.4
 Status codes: * - valid, > - best, d - damped,
               h - history, i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
    Network          NextHop          MED        LocPrf     PrefVal  Path/Ogn
 * > 4.4.4.0/24      1.1.3.1                                 0        300 100i
 * > 5.5.5.0/24      1.1.3.1                                 0        300 100i
 * > 6.6.6.0/24      1.1.3.1                                 0        300 100i
```

从路由表可以看出,Switch D 只学到了来自 AS 100 的路由 4.4.4.0/24、5.5.5.0/24、6.6.6.0/24。

提示:正则表达式的含义和使用方法可参照 BGP 相关手册。

第9章

IPv6配置指导

9.1 IPv6 地址典型配置指导

当用户需要访问 IPv6 网络时，交换机上必须要配置 IPv6 地址，并确保用户和交换机之间网络层互通。全球单播地址、站点本地地址、链路本地地址三者必选其一。特别当用户需要访问使用 IPv6 的公网时，必须配置 IPv6 全球单播地址。

(1) IPv6 站点本地地址和全球单播地址可以通过下面方式配置。

① 采用 EUI-64 格式形成。当配置采用 EUI-64 格式形成 IPv6 地址时，接口的 IPv6 地址的前缀是所配置的前缀，而接口标识符则由接口的链路层地址转化而来。

② 手动配置。用户手动配置 IPv6 站点本地地址或全球单播地址。

(2) IPv6 的链路本地地址可以通过两种方式获得。

① 自动生成。设备根据链路本地地址前缀(FE80::/64)及接口的链路层地址，自动为接口生成链路本地地址。

② 手动指定。用户手动配置 IPv6 链路本地地址。

1. 背景

A 校区校园网络原先全部运行 IPv4，当 CERNET2(第二代中国教育和科研计算机网)运行后，学校计划接入 CERNET2，以给学生提供 IPv6 接入和应用服务。

拿到所分配的 IPv6 地址后，网管员小 L 准备对接入 CERNET2 的交换机进行 IPv6 地址配置。

2. 组网图

图 9-1 所示为 IPv6 地址典型配置组网图。

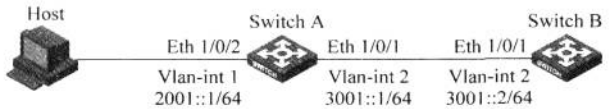


图 9-1 IPv6 地址典型配置组网图

3. 配置需求

(1) Host、Switch A 和 Switch B 通过以太网端口直接相连，将以太网端口分别加入相应的 VLAN 中，并在 VLAN 接口上配置 IPv6 地址，验证设备之间的互通性。

(2) Switch A 的 VLAN 接口 2 的全球单播地址为 3001::1/64，VLAN 接口 1 的全球单播地址为 2001::1/64。

(3) Switch B 的 VLAN 接口 2 的全球单播地址为 3001::2/64，有可以到 Host 的路由。

(4) Host 上安装了 IPv6，根据 IPv6 邻居发现协议自动配置 IPv6 地址。

4. 配置过程和解释

说明：对于 S3610/S5510 系列以太网交换机，在使能 IPv6 功能之前，必须先将设备运行模式切换到 IPv4/IPv6 双协议栈模式，即执行 switch-mode dual-ipv4-ipv6 命令；否则，即使使能 IPv6，设备也不支持 IPv6 报文的转发。另外需要注意的是，执行 switch-mode 命令切换的协议栈只有在重启设备后才能生效。

(1) 配置 Switch A。

① 使能交换机的 IPv6 转发功能。

```
<SwitchA> system-view
[SwitchA] ipv6
```

② 手动指定 VLAN 接口 2 的全球单播地址，同时会自动生成链路本地地址。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address 3001::1/64
[SwitchA-Vlan-interface2] quit
```

③ 手动指定 VLAN 接口 1 的全球单播地址，并允许其发布 RA 消息(默认情况下，所有的接口不会发布 RA 消息)。

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ipv6 address 2001::1/64
[SwitchA-Vlan-interface1] undo ipv6 nd ra halt
```

(2) 配置 Switch B。

① 使能交换机的 IPv6 转发功能。

```
<SwitchB> system-view
[SwitchB] ipv6
```

② 配置 VLAN 接口 2 的全球单播地址。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address 3001::2/64
[SwitchB-Vlan-interface2] quit
```

③ 配置 IPv6 静态路由，该路由的目的地址为 2001::/64，下一跳地址为 3001::1。

```
[SwitchB] ipv6 route-static 2001:: 64 3001::1
```

(3) 配置 Host。Host 上安装 IPv6，根据 IPv6 邻居发现协议自动配置 IPv6 地址。

```
[SwitchA] display ipv6 neighbors interface ethernet 1/0/2
                Type: S-Static    D-Dynamic
IPv6 Address                    Link-layer      VID  Interface     State T Age
FE80::215:E9FF:FEA6:7D14        0015-e9a6-7d14  1    Eth1/0/2      STALE D 1238
2001::15B:E0EA:3524:E791        0015-e9a6-7d14  1    Eth1/0/2      STALE D 1248
```

通过上面的信息可以知道 Host 上获得的 IPv6 全球单播地址为 2001::15B:E0EA:3524:E791。

(4) 验证配置结果。在 Host 上使用 ping 测试和 Switch A 及 Switch B 的互通性；在 Switch B 上使用 ping 测试和 Switch A 及 Host 的互通性。

```
[SwitchB] ping ipv6 -c 1 3001::1
  ping 3001::1 : 56 data bytes, press Ctrl_C to break
    Reply from 3001::1
    bytes=56 Sequence=1 hop limit=64 time = 2 ms
  --- 3001::1 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/2 ms
[SwitchB-Vlan-interface2] ping ipv6 -c 1 2001::15B:E0EA:3524:E791
  ping 2001::15B:E0EA:3524:E791 : 56 data bytes, press Ctrl_C to break
    Reply from 2001::15B:E0EA:3524:E791
    bytes=56 Sequence=1 hop limit=63 time = 3 ms
  --- 2001::15B:E0EA:3524:E791 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/3 ms
```

从 Host 上也可以 ping 通 Switch B 和 Switch A，证明它们是互通的。

提示： 当接口配置了 IPv6 站点本地地址或全球单播地址后，同时会自动生成链路本地地址。

如果同时手动指定和自动生成链路本地地址，手动指定方式的优先级高于自动生成方式。

9.2 IPv6 业务典型配置指导

9.2.1 IPv6 手动隧道典型配置指导

IPv6 over IPv4 隧道机制是将 IPv6 数据报文前封装上 IPv4 的报文头，通过隧道(Tunnel)使 IPv6 报文穿越 IPv4 网络，实现隔离的 IPv6 网络的互通。

根据隧道终点的 IPv4 地址的获取方式不同，隧道分为手动隧道及自动隧道。

(1) 如果 IPv6 over IPv4 隧道的终点地址不能从 IPv6 报文的目的地址中自动获取，需要进行手动配置，这样的隧道即为手动隧道。

(2) 如果 IPv6 over IPv4 隧道的接口地址采用内嵌 IPv4 地址的特殊 IPv6 地址形式，即可以从 IPv6 报文的目的地址中自动获取隧道终点的 IPv4 地址，这样的隧道即为自动隧道。

IPv6 手动隧道是点到点之间的链路，一条链路就是一个单独的隧道，主要用于边缘路由器—边缘路由器或主机—边缘路由器之间定期安全通信的稳定连接，可实现与远端 IPv6

网络的连接。

1. 背景

B校区校园网络也想接入到CERNET2。但是，B校区和A校区不同，它没有到CERNET2的直接连接。所以，网管员小L想利用IPv6 over IPv4隧道机制，穿越IPv4网络而与CERNET2的边缘接入路由器建立隧道连接。

因互连站点数量较少且地址固定，站点间要使用动态路由协议，所以经考虑，小L认为使用手动隧道方式比较合适。

2. 组网图

图9-2所示为IPv6手动隧道典型配置组网图。

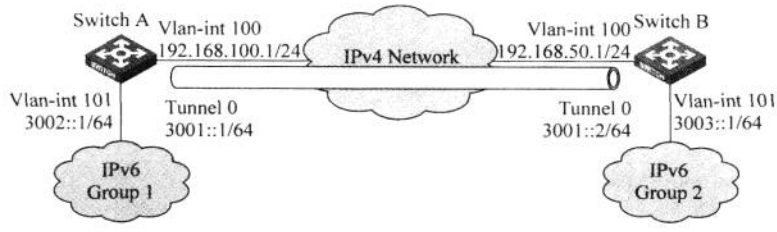


图9-2 IPv6手动隧道典型配置组网图

3. 配置需求

如图9-2所示，两个IPv6网络分别通过Switch A和Switch B与IPv4网络连接，要求在Switch A和Switch B之间建立IPv6手动隧道，使两个IPv6网络可以互通。

4. 配置过程和解释

(1) 配置Switch A。

① 使能交换机的IPv6转发功能。

```
<SwitchA> system-view
[SwitchA] ipv6
```

② 配置接口Vlan-interface 100的地址。

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 192.168.100.1 255.255.255.0
[SwitchA-Vlan-interface100] quit
```

③ 配置接口Vlan-interface 101的IPv6地址。

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] ipv6 address 3002::1 64
[SwitchA-Vlan-interface101] quit
```

④ 配置链路聚合组。需要注意的是，将端口加入到链路聚合组时，需要在端口上关闭STP功能。

```
[SwitchA] link-aggregation group 1 mode manual
[SwitchA] link-aggregation group 1 service-type tunnel
[SwitchA] interface GigabitEthernet 1/0/2
```

```
[SwitchA-GigabitEthernet1/0/2] stp disable
[SwitchA-GigabitEthernet1/0/2] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/2] quit
```

⑤ 配置手动隧道。

```
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] ipv6 address 3001::1/64
[SwitchA-Tunnel0] source vlan-interface 100
[SwitchA-Tunnel0] destination 192.168.50.1
[SwitchA-Tunnel0] tunnel-protocol ipv6-ipv4
```

⑥ 在 Tunnel 接口视图下配置隧道引用链路聚合组 1。

```
[SwitchA-Tunnel0] aggregation-group 1
[SwitchA-Tunnel0] quit
```

⑦ 配置从 Switch A 经过 Tunnel 0 接口到 Group 2 的静态路由。

```
[SwitchA] ipv6 route-static 3003:: 64 tunnel 0
```

(2) 配置 Switch B。

① 使能交换机的 IPv6 转发功能。

```
<SwitchB> system-view
[SwitchB] ipv6
```

② 配置接口 Vlan-interface 100 的地址。

```
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 192.168.50.1 255.255.255.0
[SwitchB-Vlan-interface100] quit
```

③ 配置接口 Vlan-interface 101 的 IPv6 地址。

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] ipv6 address 3003::1 64
[SwitchB-Vlan-interface101] quit
```

④ 配置链路聚合组。需要注意的是，将端口加入到链路聚合组时，需要在端口上关闭 STP 功能。

```
[SwitchB] link-aggregation group 1 mode manual
[SwitchB] link-aggregation group 1 service-type tunnel
[SwitchB] interface GigabitEthernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] stp disable
[SwitchB-GigabitEthernet1/0/2] port link-aggregation group 1
[SwitchB-GigabitEthernet1/0/2] quit
```

⑤ 配置手动隧道。

```
[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] ipv6 address 3001::2/64
[SwitchB-Tunnel0] source vlan-interface 100
```

```
[SwitchB-Tunnel0] destination 192.168.100.1
[SwitchB-Tunnel0] tunnel-protocol ipv6-ipv4
```

⑥ 在 Tunnel 接口视图下配置隧道引用链路聚合组 1。

```
[SwitchB-Tunnel0] aggregation-group 1
[SwitchB-Tunnel0] quit
```

⑦ 配置从 Switch B 经过 Tunnel 0 接口到 Group 1 的静态路由。

```
[SwitchB] ipv6 route-static 3002:: 64 tunnel 0
```

提示：隧道的两端应配置相同的隧道模式，否则可能造成报文传输失败。也可以在手动隧道上使用动态路由协议。

9.2.2 6to4 隧道典型配置指导

6to4 隧道是点到多点的自动隧道，主要用于将多个 IPv6 孤岛通过 IPv4 网络连接到 IPv6 网络。6to4 隧道通过 IPv6 报文的目的地址中嵌入的 IPv4 地址，可以自动获取隧道的终点。

6to4 隧道采用特殊的地址：6to4 地址，其格式为：2002:abcd:efgh:子网号::接口 ID/64。其中 2002 表示固定的 IPv6 地址前缀；abcd:efgh 表示该 6to4 隧道对应的 32 位 IPv4 源地址，用十六进制表示(如 1.1.1.1 可以表示为 0101:0101)。通过这个嵌入的 IPv4 地址可以自动确定隧道的终点，使隧道的建立非常方便。

由于 6to4 地址的 64 位地址前缀中的 16 位子网号可以由用户自定义，前缀中的前 48 位已由固定数值、隧道起点或终点设备的 IPv4 地址确定，使 IPv6 报文通过隧道进行转发成为可能。

1. 背景

C 校区校园网络未使用任何方式接入 CERNET2，所以无法使用因特网的 IPv6 资源。但为了满足学生接入 IPv6 因特网的需求，小 L 决定使用 6to4 隧道机制而直接接入到 IPv6 因特网。

2. 组网图

图 9-3 所示为 6to4 隧道典型配置组网图。

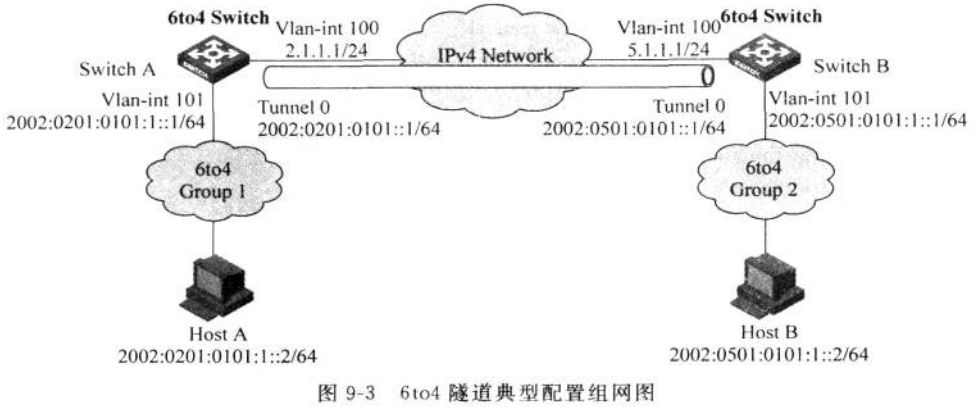


图 9-3 6to4 隧道典型配置组网图

3. 配置需求

如图 9-3 所示，两个 6to4 网络通过网络边缘 6to4 Switch(Switch A 和 Switch B)与 IPv4 网络相连，为了实现 6to4 网络中的主机 Host A 和 Host B 之间的互通，需要配置 6to4 隧道。

6to4 网络之间的互通需要为 6to4 网络内的主机及 6to4 Switch 配置 6to4 地址。

(1) Switch A 上接口 Vlan-int 100 的 IPv4 地址为 2.1.1.1/24，转换成 IPv6 地址后使用 6to4 前缀 2002:0201:0101::/48。对此前缀进行子网划分，Tunnel 0 使用 2002:0201:0101::/64 子网，Vlan-int 101 使用 2002:0201:0101:1::/64 子网。

(2) Switch B 上接口 Vlan-int 100 的 IPv4 地址为 5.1.1.1/24，转换成 IPv6 地址后使用 6to4 前缀 2002:0501:0101::/48。对此前缀进行子网划分，Tunnel 0 使用 2002:0501:0101::/64 子网，Vlan-int 101 使用 2002:0501:0101:1::/64 子网。

4. 配置过程和解释

(1) 配置 Switch A。

① 使能交换机的 IPv6 转发功能。

```
<SwitchA> system-view
[SwitchA] ipv6
```

② 配置接口 Vlan-interface 100 的地址。

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 2.1.1.1 24
[SwitchA-Vlan-interface100] quit
```

③ 配置接口 Vlan-interface 101 的地址。

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] ipv6 address 2002:0201:0101:1::1/64
[SwitchA-Vlan-interface101] quit
```

④ 配置链路聚合组。需要注意的是，将端口加入到链路聚合组时，需要在端口上关闭 STP 功能。

```
[SwitchA] link-aggregation group 1 mode manual
[SwitchA] link-aggregation group 1 service-type tunnel
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] stp disable
[SwitchA-GigabitEthernet1/0/3] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/3] quit
```

⑤ 配置 6to4 隧道。

```
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] ipv6 address 2002:201:101::1/64
[SwitchA-Tunnel0] source vlan-interface 100
[SwitchA-Tunnel0] tunnel-protocol ipv6-ipv4 6to4
```

⑥ 在 Tunnel 接口视图下配置隧道引用链路聚合组 1。

```
[SwitchA-Tunnel0] aggregation-group 1
[SwitchA-Tunnel0] quit
```

⑦ 配置到目的地址 2002::/16，下一跳为 Tunnel 接口的静态路由。

```
[SwitchA] ipv6 route-static 2002:: 16 tunnel 0
```

(2) 配置 Switch B。

① 使能交换机的 IPv6 转发功能。

```
<SwitchB> system-view
[SwitchB] ipv6
```

② 配置接口 Vlan-interface 100 的地址。

```
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 5.1.1.1 24
[SwitchB-Vlan-interface100] quit
```

③ 配置接口 Vlan-interface 101 的地址。

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] ipv6 address 2002:0501:0101:1::1/64
[SwitchB-Vlan-interface101] quit
```

④ 配置链路聚合组。需要注意的是，将端口加入到链路聚合组时，需要在端口上关闭 STP 功能。

```
[SwitchB] link-aggregation group 1 mode manual
[SwitchB] link-aggregation group 1 service-type tunnel
[SwitchB] interface GigabitEthernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] stp disable
[SwitchB-GigabitEthernet1/0/3] port link-aggregation group 1
[SwitchB-GigabitEthernet1/0/3] quit
```

⑤ 配置 6to4 隧道。

```
[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] ipv6 address 2002:0501:0101::1/64
[SwitchB-Tunnel0] source vlan-interface 100
[SwitchB-Tunnel0] tunnel-protocol ipv6-ipv4 6to4
```

⑥ 在 Tunnel 接口视图下配置隧道引用链路聚合组。

```
[SwitchB-Tunnel0] aggregation-group 1
[SwitchB-Tunnel0] quit
```

⑦ 配置到目的地址 2002::/16，下一跳为 Tunnel 接口的静态路由。

```
[SwitchB] ipv6 route-static 2002:: 16 tunnel 0
```

提示：自动隧道不支持动态路由协议。

9.2.3 ISATAP隧道典型配置指导

ISATAP隧道是点到点的自动隧道技术，通过在IPv6报文的目的地址中嵌入的IPv4地址，可以自动获取隧道的终点。

使用ISATAP隧道时，IPv6报文的目的地址和隧道接口的IPv6地址都要采用特殊的ISATAP地址。ISATAP地址格式为：Prefix(64bit):0:5EFE:ip-address。其中，64位的Prefix为任何合法的IPv6单播地址前缀；ip-address为32位IPv4源地址，形式为a.b.c.d或者abcd:efgh，且该IPv4地址不要求全球唯一。通过这个嵌入的IPv4地址就可以自动建立隧道，完成IPv6报文的传送。

ISATAP隧道主要用于在IPv4网络中IPv6主机—IPv6路由器的连接。其最大特点是能够在IPv4承载网上运行ND协议，从而使IPv6主机通过IPv4网络而自动获得IPv6前缀。

1. 背景

在A校区内进行IPv6改造时，小L发现有几个宿舍楼使用的三层交换机不支持IPv6协议。如果将这些交换机全部硬件升级，投入的成本比较大。有没有办法在使用原有交换机的基础上向学生提供IPv6接入服务呢？小L想到了另外一种适用于这种场景下的隧道技术——ISATAP隧道。

2. 组网图

图9-4所示为ISATAP隧道典型配置组网图。

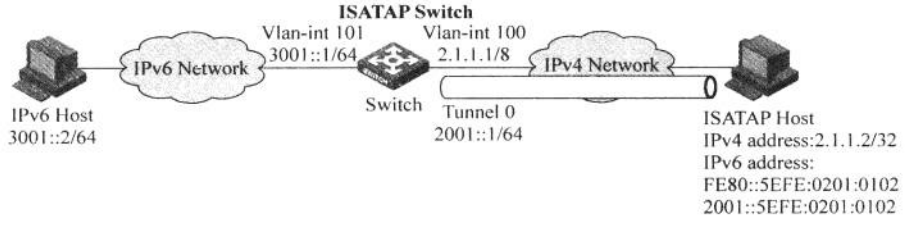


图9-4 ISATAP隧道典型配置组网图

3. 配置需求

如图9-4所示，IPv6网络和IPv4网络通过ISATAP交换机相连，要求将IPv4网络中的IPv6主机通过ISATAP隧道接入到IPv6网络。

4. 配置过程和解释

(1) 配置Switch。

① 使能IPv6转发功能。

```
<Switch> system-view
[Switch] ipv6
```

② 配置各接口地址。

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 address 3001::1/64
[Switch-Vlan-interface100] quit
```

```
[Switch] interface vlan-interface 101
[Switch-Vlan-interface101] ip address 2.1.1.1 255.0.0.0
[Switch-Vlan-interface101] quit
```

③ 配置链路聚合组。需要注意的是，将端口加入到链路聚合组时，需要在端口上关闭STP功能。

```
[Switch] link-aggregation group 1 mode manual
[Switch] link-aggregation group 1 service-type tunnel
[Switch] interface GigabitEthernet 1/0/3
[Switch-GigabitEthernet1/0/3] stp disable
[Switch-GigabitEthernet1/0/3] port link-aggregation group 1
[Switch-GigabitEthernet1/0/3] quit
```

④ 配置ISATAP隧道。

```
[Switch] interface tunnel 0
[Switch-Tunnel0] ipv6 address 2001::1/64 eui-64
[Switch-Tunnel0] source vlan-interface 101
[Switch-Tunnel0] tunnel-protocol ipv6-ipv4 isatap
```

⑤ 在Tunnel接口视图下配置隧道引用链路聚合组1。

```
[Switch-Tunnel0] aggregation-group 1
```

⑥ 取消对RA消息发布的抑制，使主机可以通过交换机发布的RA消息获取地址前缀等信息。

```
[Switch-Tunnel0] undo ipv6 nd ra halt
[Switch-Tunnel0] quit
```

⑦ 配置到ISATAP主机的静态路由。

```
[Switch] ipv6 route-static 2001:: 16 tunnel 0
```

(2) 配置主机。ISATAP主机上的具体配置与主机的操作系统有关，下面仅以Windows XP操作系统为例进行说明。

① 在Windows XP上，ISATAP接口通常为接口2，只要在该接口上配置ISATAP交换机的IPv4地址即可完成主机侧的配置。先看看这个ISATAP接口的信息，如下所示。

```
C:\>ipv6 if 2
Interface 2: Automatic Tunneling Pseudo-Interface
  Guid {48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
  does not use Neighbor Discovery
  does not use Router Discovery
  routing preference 1
  EUI-64 embedded IPv4 address: 0.0.0.0
  router link-layer address: 0.0.0.0
    preferred link-local fe80::5efe:2.1.1.2, life infinite
  link MTU 1280 (true link MTU 65515)
  current hop limit 128
```

```
  reachable time 42500ms (base 30000ms)
  retransmission interval 1000ms
  DAD transmits 0
  default site prefix length 48
```

② 它自动生成了一个 ISATAP 格式的 link-local 地址(fe80::5efe:2.1.1.2)。下面需要设置这个接口上的 ISATAP 交换机的 IPv4 地址。

```
C:\>ipv6 rlu 2 2.1.1.1
```

③ 只需要这么一个命令，就完成了主机的配置，下面再来看看这个 ISATAP 接口的信息。

```
C:\>ipv6 if 2
Interface 2: Automatic Tunneling Pseudo-Interface
  Guid {48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
  does not use Neighbor Discovery
  uses Router Discovery
  routing preference 1
  EUI-64 embedded IPv4 address: 2.1.1.2
  router link-layer address: 2.1.1.1
    preferred global 2001::5efe:2.1.1.2, life 29d23h59m46s/6d23h59m46s (public)
    preferred link-local fe80::5efe:2.1.1.2, life infinite
  link MTU 1500 (true link MTU 65515)
  current hop limit 255
  reachable time 42500ms (base 30000ms)
  retransmission interval 1000ms
  DAD transmits 0
  default site prefix length 48
```

④ 通过对比前后的区别可以看到，主机获取了 2001::/64 的前缀，自动生成地址 2001::5efe:2.1.1.2，同时还会发现这么一行“uses Router Discovery”，表明主机启用了路由器发现，这时 ping 一下交换机上隧道接口的 IPv6 地址，可以 ping 通，这时候表明 ISATAP 隧道已经成功建立。

提示：在 Windows XP 系统下，可以在命令行下用 C:\>ipv6 if 来查看所有接口的 IPv6 配置信息。其他操作系统(如 Windows 7、Vista 等)相关命令可能会有所不同，可查阅操作系统相关帮助。

9.3 IPv6 路由典型配置指导

9.3.1 IPv6 静态路由典型配置指导

静态路由由管理员手动配置。当网络结构比较简单时，只需配置静态路由就可以使网络正常工作。恰当地设置和使用静态路由可以改进网络的性能，并可为重要的应用保证带宽。

静态路由的缺点在于，当网络发生故障或者拓扑发生变化后，可能会出现路由不可达，

导致网络中断，此时必须由网络管理员手动修改静态路由的配置。

1. 背景

Y学校校园网络包含了1个总校区和2个分校区，规划在总校区和分校区间部署IPv6路由。考虑到总校区与分校区间是星形连接，没有链路冗余，所以管理员小W决定使用静态路由，以简化配置和降低协议流量。

2. 组网图

图9-5所示为IPv6静态路由典型配置组网图。

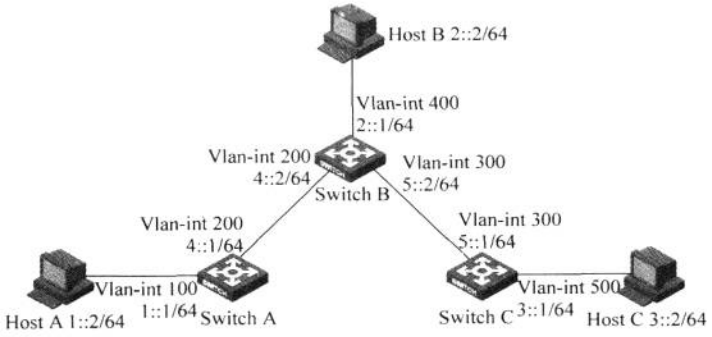


图9-5 IPv6静态路由典型配置组网图

3. 配置需求

各交换机之间配置IPv6静态路由后，使所有主机和交换机之间互通。

4. 配置过程和解释

(1) 配置各VLAN虚接口的IPv6地址(略)。

(2) 配置IPv6静态路由。

① 在Switch A上配置IPv6默认路由。

```
<SwitchA> system-view
[SwitchA] ipv6
[SwitchA] ipv6 route-static :: 0 4::2
```

② 在Switch B上配置两条IPv6静态路由。

```
<SwitchB> system-view
[SwitchB] ipv6
[SwitchB] ipv6 route-static 1:: 64 4::1
[SwitchB] ipv6 route-static 3:: 64 5::1
```

③ 在Switch C上配置IPv6默认路由。

```
<SwitchC> system-view
[SwitchC] ipv6
[SwitchC] ipv6 route-static :: 0 5::2
```

(3) 配置主机地址和网关。根据组网图配置好各主机的IPv6地址，并将Host A的默认网关配置为1::1，Host B的默认网关配置为2::1，Host C的默认网关配置为3::1。

提示：在本拓扑中，Switch A 和 Switch C 上也可以配置到对端具体网段的静态路由。注意，不要将两个站点间都配置默认路由互指对方，否则容易引起路由环路。

9.3.2 IPv6 RIPng 路由协议典型配置指导

RIPng 又称为下一代 RIP 协议(RIP Next Generation)，它是对原来的 IPv4 网络中 RIP-2 协议的扩展。大多数 RIP 的概念都可以用于 RIPng。

1. 背景

Y 学校校园网络使用静态路由后，运行稳定。几个月后，网管中心决定要对校园网络进行升级，各校区间增加冗余线路以提高可靠性。在此情况下，静态路由扩展性不强的问题就显现出来了。故此，网管中心决定重新部署动态路由协议来替代静态路由。

因 RIPng 配置简单，故先对 RIPng 进行部署测试。

2. 组网图

图 9-6 所示为 IPv6 RIPng 路由协议典型配置组网图。

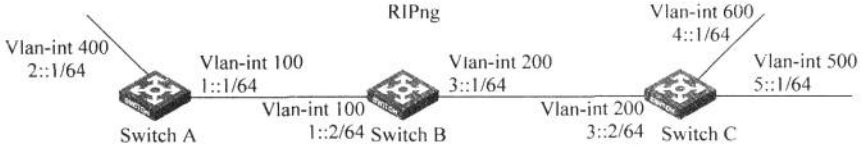


图 9-6 IPv6 RIPng 路由协议典型配置组网图

3. 配置需求

(1) Switch A、Switch B 和 Switch C 相连并通过 RIPng 来学习网络中的 IPv6 路由信息。

(2) 在 Switch B 上对接收的 Switch C 的路由(3::/64)进行过滤，使其不加入到 Switch B 的 RIPng 进程的路由表中，也不发布给 Switch A。

4. 配置过程和解释

(1) 配置各接口的 IPv6 地址(略)。

(2) 配置 RIPng 的基本功能。

① 配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ipv6
[SwitchA] ripng 1
[SwitchA-ripng-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ripng 1 enable
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 400
[SwitchA-Vlan-interface400] ripng 1 enable
[SwitchA-Vlan-interface400] quit
```

② 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ipv6
[SwitchB] ripng 1
[SwitchB-ripng-1] quit
```

```
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ripng 1 enable
[SwitchB-Vlan-interface200] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ripng 1 enable
[SwitchB-Vlan-interface100] quit
```

③ 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ipv6
[SwitchC] ripng 1
[SwitchC-ripng-1] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] ripng 1 enable
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 500
[SwitchC-Vlan-interface500] ripng 1 enable
[SwitchC-Vlan-interface500] quit
[SwitchC] interface vlan-interface 600
[SwitchC-Vlan-interface600] ripng 1 enable
[SwitchC-Vlan-interface600] quit
```

④ 查看 Switch B 的 RIPng 路由表。

```
[SwitchB] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
-----------------------------------------------------------------
Peer FE80::20F:E2FF:FE23:82F5 on Vlan-interface 100
Dest 1::/64,
     via FE80::20F:E2FF:FE23:82F5, cost 1, tag 0, A, 6 Sec
Dest 2::/64,
     via FE80::20F:E2FF:FE23:82F5, cost 1, tag 0, A, 6 Sec

Peer FE80::20F:E2FF:FE00:100 on Vlan-interface 200
Dest 3::/64,
     via FE80::20F:E2FF:FE00:100, cost 1, tag 0, A, 11 Sec
Dest 4::/64,
     via FE80::20F:E2FF:FE00:100, cost 1, tag 0, A, 11 Sec
Dest 5::/64,
     via FE80::20F:E2FF:FE00:100, cost 1, tag 0, A, 11 Sec
```

⑤ 查看 Switch A 的 RIPng 路由表。

```
[SwitchA] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
-----------------------------------------------------------------
Peer FE80::200:2FF:FE64:8904 on Vlan-interface 100
Dest 1::/64,
     via FE80::200:2FF:FE64:8904, cost 1, tag 0, A, 31 Sec
Dest 4::/64,
     via FE80::200:2FF:FE64:8904, cost 2, tag 0, A, 31 Sec
```

```
Dest 5::/64,
    via FE80::200:2FF:FE64:8904, cost 2, tag 0, A, 31 Sec
Dest 3::/64,
    via FE80::200:2FF:FE64:8904, cost 1, tag 0, A, 31 Sec
```

(3) 配置 Switch B 对接收和发布的路由进行过滤。

```
[SwitchB] acl ipv6 number 2000
[SwitchB-acl6-basic-2000] rule deny source 3::/64
[SwitchB-acl6-basic-2000] rule permit
[SwitchB-acl6-basic-2000] quit
[SwitchB] ripng 1
[SwitchB-ripng-1] filter-policy 2000 import
[SwitchB-ripng-1] filter-policy 2000 export
[SwitchB-ripng-1] quit
```

查看 Switch B 和 Switch A 的 RIPng 路由表：

```
[SwitchB] display ripng 1 route
  Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
----------------------------------------------------------------
Peer FE80::20F:E2FF:FE23:82F5 on Vlan-interface 100
Dest 1::/64,
    via FE80::20F:E2FF:FE23:82F5, cost 1, tag 0, A, 2 Sec
Dest 2::/64,
    via FE80::20F:E2FF:FE23:82F5, cost 1, tag 0, A, 2 Sec

Peer FE80::20F:E2FF:FE00:100 on Vlan-interface 200
Dest 4::/64,
    via FE80::20F:E2FF:FE00:100, cost 1, tag 0, A, 5 Sec
Dest 5::/64,
    via FE80::20F:E2FF:FE00:100, cost 1, tag 0, A, 5 Sec
[SwitchA] display ripng 1 route
  Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
----------------------------------------------------------------
Peer FE80::20F:E2FF:FE00:1235 on Vlan-interface 100
Dest 1::/64,
    via FE80::20F:E2FF:FE00:1235, cost 1, tag 0, A, 2 Sec
Dest 4::/64,
    via FE80::20F:E2FF:FE00:1235, cost 2, tag 0, A, 2 Sec
Dest 5::/64,
    via FE80::20F:E2FF:FE00:1235, cost 2, tag 0, A, 2 Sec
```

注意：如果接口没有使能 RIPng，那么 RIPng 进程在该接口上既不发送也不接收 RIPng 路由。所以，路由器连接到主机侧的接口上也要使能 RIPng。

9.3.3 IPv6 RIPng 跨越 IPv4 网络应用典型配置指导

1. 背景

Y 学校校园网络在使用 RIPng 进行部署测试中，发现到一个图书馆的线路仍是 IPv4。因经费问题，网管中心暂不想升级，而想采用 IPv6 over IPv4 隧道技术进行过渡。

2. 组网图

图 9-7 所示为 IPv6 RIPng 跨越 IPv4 网络应用典型配置组网图。

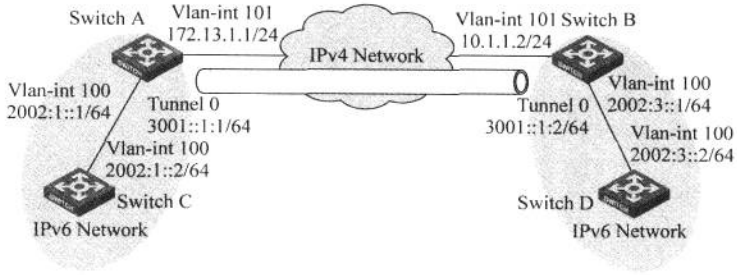


图 9-7 IPv6 RIPng 跨越 IPv4 网络应用典型配置组网图

3. 配置需求

如图 9-7 所示，两个 IPv6 网络分别通过 Switch A 和 Switch B 与 IPv4 网络连接，Switch A 与 Switch B 之间路由可达，要求在 Switch A 和 Switch B 之间建立 IPv6 手动隧道，使两个 IPv6 网络可以使用 RIPng 进行网络互连。

4. 配置过程和解释

(1) 配置各接口的 IPv6 地址和 IPv4 地址(略)。

(2) 配置 Switch A。

① 使能 IPv6 转发功能。

```
<SwitchA> system-view
[SwitchA] ipv6
```

② 配置手动隧道。

```
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] ipv6 address 3001::1:1 64
[SwitchA-Tunnel0] source vlan-interface 101
[SwitchA-Tunnel0] destination 10.1.1.2
[SwitchA-Tunnel0] tunnel-protocol ipv6-ipv4
[SwitchA-Tunnel0] quit
```

③ 配置 RIPng 的基本功能。

```
[SwitchA] ripng 1
[SwitchA-ripng-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ripng 1 enable
[SwitchA-Vlan-interface100] quit
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] ripng 1 enable
[SwitchA-Tunnel0] quit
```

(3) 配置 Switch B。

① 使能 IPv6 转发功能。

```
<SwitchB> system-view
```

```
[SwitchB] ipv6
```

② 配置手动隧道。

```
[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] ipv6 address 3001::1:2 64
[SwitchB-Tunnel0] source vlan-interface 101
[SwitchB-Tunnel0] destination 172.13.1.1
[SwitchB-Tunnel0] tunnel-protocol ipv6-ipv4
[SwitchB-Tunnel0] quit
```

③ 配置 RIPng 的基本功能。

```
[SwitchA] ripng 1
[SwitchA-ripng-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ripng 1 enable
[SwitchA-Vlan-interface100] quit
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] ripng 1 enable
[SwitchA-Tunnel0] quit
```

(4) 配置 Switch C。

① 使能 IPv6 转发功能。

```
<SwitchB> system-view
[SwitchB] ipv6
```

② 配置 RIPng 的基本功能

```
[SwitchA] ripng 1
[SwitchA-ripng-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ripng 1 enable
[SwitchA-Vlan-interface100] quit
```

(5) 配置 Switch D。

① 使能 IPv6 转发功能。

```
<SwitchB> system-view
[SwitchB] ipv6
```

② 配置 RIPng 的基本功能。

```
[SwitchA] ripng 1
[SwitchA-ripng-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ripng 1 enable
[SwitchA-Vlan-interface100] quit
```

在 Switch C 上用命令 display ipv6 routing-table，可以看到 Switch C 已知道网络 2002:3::/64 的存在。

在 Switch D 上用命令 display ipv6 routing-table，可以看到 Switch D 也知道网络 2002:1::/64 的存在。

9.3.4 OSPFv3 典型配置指导

OSPFv3 是 OSPF(Open Shortest Path First，开放式最短路径优先)版本 3 的简称，主要提供对 IPv6 的支持，遵循的标准为 RFC 2740(OSPF for IPv6)。

OSPFv3 和 OSPFv2 在很多方面是相同的。

(1) Router ID、Area ID 仍然是 32 位的。

(2) 相同类型的报文：Hello 报文、DD(Database Description，数据库描述)报文、LSR(Link State Request，链路状态请求)报文、LSU(Link State Update，链路状态更新)报文和 LSAck(Link State Acknowledgment，链路状态确认)报文。

(3) 相同的邻居发现机制和邻接形成机制。

(4) 相同的 LSA 扩散机制和老化机制。

1. 背景

Y 学校校园网络使用 RIPng 进行测试一段时间后，发现测试结果不太理想。主要原因是 RIPng 的收敛时间有些慢，网络故障恢复时间超出了业务所允许的范围；另外，校园网的三层网络设备日后还会大量增加，担心 RIPng 协议管理不好这么多网段。故此，网管中心决定使用另外一种可扩展性强的链路状态型路由协议——OSPFv3 来进行测试。

2. 组网图

图 9-8 所示为 OSPFv3 典型配置组网图。

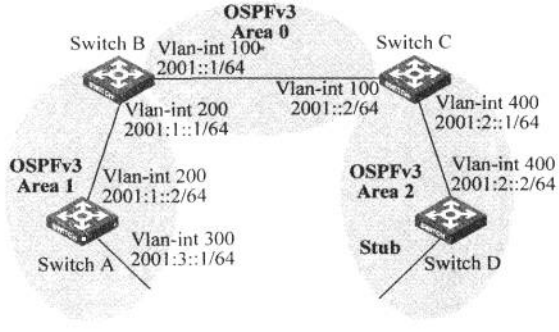


图 9-8 OSPFv3 典型配置组网图

3. 配置需求

(1) 所有的交换机都运行 OSPFv3，整个自治系统划分为 3 个区域。其中 Switch B 和 Switch C 作为 ABR 来转发区域之间的路由。

(2) 将 Area 2 配置为 Stub 区域，减少通告到此区域内的 LSA 数量，可进一步减少 Stub 区域路由表规模。将 Area 2 配置为 Totally Stub 区域，但不能影响路由的可达性。

4. 配置过程和解释

(1) 配置各接口的 IPv6 地址(略)。

(2) 配置 OSPFv3 基本功能。

① 配置 Switch A，启动 OSPFv3，并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] ipv6
[SwitchA] ospfv3
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 300
[SwitchA-Vlan-interface300] ospfv3 1 area 1
[SwitchA-Vlan-interface300] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ospfv3 1 area 1
[SwitchA-Vlan-interface200] quit
```

② 配置 Switch B，启动 OSPFv3，并设置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] ipv6
[SwitchB] ospfv3
[SwitchB-ospf-1] router-id 2.2.2.2
[SwitchB-ospf-1] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ospfv3 1 area 0
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ospfv3 1 area 1
[SwitchB-Vlan-interface200] quit
```

③ 配置 Switch C，启动 OSPFv3，并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
[SwitchC] ipv6
[SwitchC] ospfv3
[SwitchC-ospfv3-1] router-id 3.3.3.3
[SwitchC-ospfv3-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] ospfv3 1 area 0
[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 400
[SwitchC-Vlan-interface400] ospfv3 1 area 2
[SwitchC-Vlan-interface400] quit
```

④ 配置 Switch D，启动 OSPFv3，并设置其 Router ID 为 4.4.4.4。

```
<SwitchD> system-view
[SwitchD] ipv6
[SwitchD] ospfv3
[SwitchD-ospfv3-1] router-id 4.4.4.4
[SwitchD-ospfv3-1] quit
[SwitchD] interface vlan-interface 400
[SwitchD-Vlan-interface400] ospfv3 1 area 2
[SwitchD-Vlan-interface400] quit
```

⑤ 查看 Switch B 的 OSPFv3 邻居状态。

```
[SwitchB] display ospfv3 peer

            OSPFv3 Area ID 0.0.0.0 (Process 1)

Neighbor ID     Pri   State            Dead Time      Interface     Instance ID
3.3.3.3         1     Full/DR          00:00:39       Vlan100       0

            OSPFv3 Area ID 0.0.0.1 (Process 1)

Neighbor ID     Pri   State            Dead Time      Interface     Instance ID
1.1.1.1         1     Full/Backup      00:00:38       Vlan200       0
```

⑥ 查看 Switch C 的 OSPFv3 邻居状态。

```
[SwitchC] display ospfv3 peer
            OSPFv3 Area ID 0.0.0.0 (Process 1)

Neighbor ID     Pri   State            Dead Time      Interface     Instance ID
2.2.2.2         1     Full/Backup      00:00:39       Vlan100       0
            OSPFv3 Area ID 0.0.0.2 (Process 1)

Neighbor ID     Pri   State            Dead Time      Interface     Instance ID
4.4.4.4         1     Full/DR          00:00:38       Vlan400       0
```

⑦ 查看 Switch D 的 OSPFv3 路由表信息。

```
[SwitchD] display ospfv3 routing
E1 - Type 1 external route,    IA - Inter area route,      I - Intra area route
E2 - Type 2 external route,    * - Seleted route
             OSPFv3 Router with ID (4.4.4.4) (Process 1)

 * Destination: 2001::/64
 Type         : IA                                  Cost      : 2
 NextHop      : FE80::F40D:0:93D0:1                 Interface : Vlan400
 * Destination: 2001:1::/64
 Type         : IA                                  Cost      : 3
 NextHop      : FE80::F40D:0:93D0:1                 Interface : Vlan400
 * Destination: 2001:2::/64
 Type         : I                                   Cost      : 1
 NextHop      : directly-connected                  Interface : Vlan400
 * Destination: 2001:3::/64
 Type         : IA                                  Cost      : 4
 NextHop      : FE80::F40D:0:93D0:1                 Interface : Vlan400
```

(3) 配置 Stub 区域。

① 配置 Switch D 的 Stub 区域。

```
[SwitchD] ospfv3
[SwitchD-ospfv3-1] area 2
[SwitchD-ospfv3-1-area-0.0.0.2] stub
```

② 配置 Switch C 的 Stub 区域，设置发送到 Stub 区域的默认路由的开销为 10。

```
[SwitchC] ospfv3
[SwitchC-ospfv3-1] area 2
[SwitchC-ospfv3-1-area-0.0.0.2] stub
[SwitchC-ospfv3-1-area-0.0.0.2] default-cost 10
```

③ 查看 Switch D 的 OSPFv3 路由表信息，可以看到路由表中多了一条默认路由，它的开销值为直连路由的开销和所配置的开销值之和。

```
[SwitchD] display ospfv3 routing
E1 - Type 1 external route,    IA - Inter area route,      I - Intra area route
E2 - Type 2 external route,    * - Seleted route
            OSPFv3 Router with ID (4.4.4.4) (Process 1)
------------------------------------------------------------------------
 * Destination: ::/0
Type         : IA                                  Cost     : 11
NextHop      : FE80::F40D:0:93D0:1                 Interface: Vlan400
 * Destination: 2001::/64
Type         : IA                                  Cost     : 2
NextHop      : FE80::F40D:0:93D0:1                 Interface: Vlan400
 * Destination: 2001:1::/64
Type         : IA                                  Cost     : 3
NextHop      : FE80::F40D:0:93D0:1                 Interface: Vlan400
 * Destination: 2001:2::/64
Type         : I                                   Cost     : 1
NextHop      : directly-connected                  Interface: Vlan400
 * Destination: 2001:3::/64
Type         : IA                                  Cost     : 4
NextHop      : FE80::F40D:0:93D0:1                 Interface: Vlan400
```

(4) 进一步减少 Stub 区域路由表规模，将 Area 2 配置为 Totally Stub 区域。

① 配置 Switch C，设置 Area 2 为 Totally Stub 区域。

```
[SwitchC-ospfv3-1-area-0.0.0.2] stub no-summary
```

② 查看 Switch D 的 OSPFv3 路由表，可以发现路由表项数目减少了，其他非直连路由都被抑制，只有默认路由被保留。

```
[SwitchD] display ospfv3 routing
E1 - Type 1 external route,    IA - Inter area route,      I - Intra area route
E2 - Type 2 external route,    * - Seleted route
            OSPFv3 Router with ID (4.4.4.4) (Process 1)
------------------------------------------------------------------------
 * Destination: ::/0
Type         : IA                                  Cost     : 11
NextHop      : FE80::F40D:0:93D0:1                 Interface: Vlan400
 * Destination: 2001:2::/64
Type         : I                                   Cost     : 1
NextHop      : directly-connected                  Interface: Vlan400
```

注意： 要在路由器上使能 OSPFv3 功能，必须先创建 OSPFv3 进程、指定该进程的 Router ID

以及在接口上使能 OSPFv3 功能。

在 OSPFv3 中，用户必须手动配置一个 Router ID，而且必须保证自治系统中任意两台路由器的 Router ID 都不相同。

9.3.5 IPv6 IS-IS 路由协议典型配置指导

IS-IS(Intermediate System-to-Intermediate System Intra-domain Routing Information Exchange Protocol，IS-IS 路由协议)支持多种网络层协议，其中包括 IPv6 协议。支持 IPv6 协议的 IS-IS 路由协议又称为 IPv6 IS-IS 动态路由协议。

1. 背景

Y 学校校园网络进行测试后，发现 OSPFv3 协议确实很好用，其收敛时间短、协议开销小，且其“骨干区域—非骨干区域”的分层方式也正好符合校园网中的“主校区—分校区”的二层结构。

那另外一种链路状态型协议 IS-IS 是否也有这样的特性呢？网络中心计划对其进行测试，再根据测试结果来选择其中一种在校园网内最终部署。

2. 组网图

图 9-9 所示为 IPv6 IS-IS 路由协议典型配置组网图。

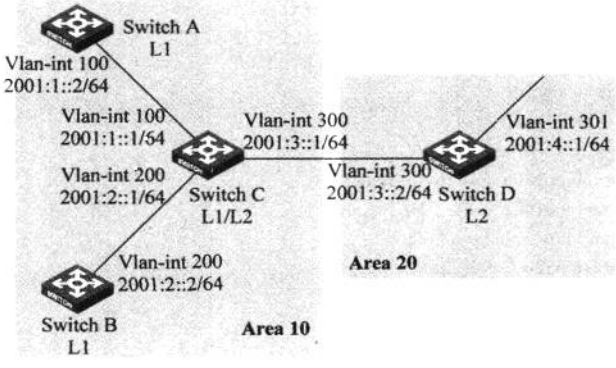


图 9-9 IPv6 IS-IS 路由协议典型配置组网图

3. 配置需求

如图 9-9 所示，Switch A、Switch B、Switch C 和 Switch D 属于同一自治系统，其中 Switch A 和 Switch B 是 Level-1 交换机，Switch D 是 Level-2 交换机，Switch C 是 Level-1-2 交换机。Switch A、Switch B 和 Switch C 属于区域 10，而 Switch D 属于区域 20。所有交换机已使能了 IPv6 能力，要求它们之间通过 IPv6 IS-IS 协议达到 IPv6 网络互连的目的。

4. 配置过程和解释

(1) 配置各接口的 IPv6 地址(略)。

(2) 配置 IPv6 IS-IS。

① 配置 Switch A。

```
<SwitchA> system-view
[SwitchA] isis 1
```

```
[SwitchA-isis-1] is-level level-1
[SwitchA-isis-1] network-entity 10.0000.0000.0001.00
[SwitchA-isis-1] ipv6 enable
[SwitchA-isis-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] isis ipv6 enable 1
[SwitchA-Vlan-interface100] quit
```

② 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] isis 1
[SwitchB-isis-1] is-level level-1
[SwitchB-isis-1] network-entity 10.0000.0000.0002.00
[SwitchB-isis-1] ipv6 enable
[SwitchB-isis-1] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] isis ipv6 enable 1
[SwitchB-Vlan-interface200] quit
```

③ 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] isis 1
[SwitchC-isis-1] network-entity 10.0000.0000.0003.00
[SwitchC-isis-1] ipv6 enable
[SwitchC-isis-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] isis ipv6 enable 1
[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] isis ipv6 enable 1
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] isis ipv6 enable 1
[SwitchC-Vlan-interface300] quit
```

④ 配置 Switch D。

```
<SwitchD> system-view
[SwitchD] isis 1
[SwitchD-isis-1] is-level level-2
[SwitchD-isis-1] network-entity 20.0000.0000.0004.00
[SwitchD-isis-1] ipv6 enable
[SwitchD-isis-1] quit
[SwitchD] interface vlan-interface 300
[SwitchD-Vlan-interface300] isis ipv6 enable 1
[SwitchD-Vlan-interface300] quit
[SwitchD] interface vlan-interface 301
[SwitchD-Vlan-interface301] isis ipv6 enable 1
[SwitchD-Vlan-interface301] quit
```

注意：不要忘记，配置任意的 IPv6 地址、ND 协议、路由协议前，都要在路由器上使能

IPv6 功能。其命令是在全局视图下用关键字 ipv6。

9.3.6 IPv6 BGP 路由协议基本配置指导

传统的 BGP-4 只能管理 IPv4 的路由信息，对于使用其他网络层协议（如 IPv6 等）的应用，在跨自治系统传播时就受到一定限制。

为了提供对多种网络层协议的支持，IETF 对 BGP-4 进行了扩展，形成 IPv6 BGP。目前的 IPv6 BGP 标准是 RFC 2858（Multi-protocol Extensions for BGP-4，BGP-4 多协议扩展）。

1. 背景

最终，Y 学校网管中心选择了 OSPFv3 协议作为校内网络的路由协议，主要原因是网管员对 OSPF 比较熟悉，使用起来得心应手。IPv6 IS-IS 尽管测试结果也很理想，但相对冷门一些，也就放弃了。

校园内路由协议部署完成后，还要考虑如何和教育网进行互连。因为教育网与校园网是不同 AS，所以只能用静态或 BGP；而考虑到 BGP 可以更好地使用策略来进行路由控制，所以最终网管中心选择了 BGP 作为与教育网互连的协议。

2. 组网图

图 9-10 所示为 IPv6 BGP 路由协议基本配置组网图。

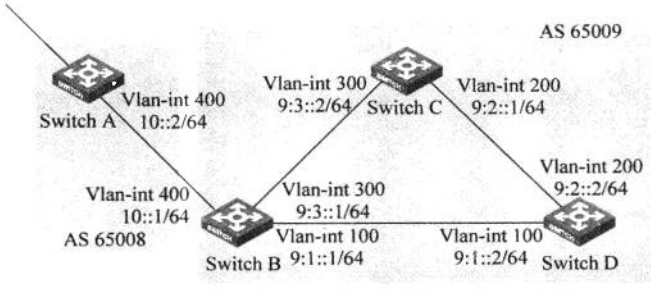


图 9-10 IPv6 BGP 路由协议基本配置组网图

3. 配置需求

如图 9-10 所示，所有交换机运行 IPv6 BGP 协议，Switch A 和 Switch B 之间建立了 EBGP 连接，Switch B、Switch C 和 Switch D 之间建立了 IBGP 全连接。

4. 配置过程和解释

（1）配置各 VLAN 接口的 IPv6 地址（略）。

（2）配置 IBGP 连接。

① 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ipv6
[SwitchB] bgp 65009
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] ipv6-family
[SwitchB-bgp-af-ipv6] peer 9:1::2 as-number 65009
[SwitchB-bgp-af-ipv6] peer 9:3::2 as-number 65009
[SwitchB-bgp-af-ipv6] quit
```

```
[SwitchB-bgp] quit
```

② 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ipv6
[SwitchC] bgp 65009
[SwitchC-bgp] router-id 3.3.3.3
[SwitchC-bgp] ipv6-family
[SwitchC-bgp-af-ipv6] peer 9:3::1 as-number 65009
[SwitchC-bgp-af-ipv6] peer 9:2::2 as-number 65009
[SwitchC-bgp-af-ipv6] quit
[SwitchC-bgp] quit
```

③ 配置 Switch D。

```
<SwitchD> system-view
[SwitchD] ipv6
[SwitchD] bgp 65009
[SwitchD-bgp] router-id 4.4.4.4
[SwitchD-bgp] ipv6-family
[SwitchD-bgp-af-ipv6] peer 9:1::1 as-number 65009
[SwitchD-bgp-af-ipv6] peer 9:2::1 as-number 65009
[SwitchD-bgp-af-ipv6] quit
[SwitchD-bgp] quit
```

(3) 配置 EBGP 连接。

① 配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ipv6
[SwitchA] bgp 65008
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] ipv6-family
[SwitchA-bgp-af-ipv6] peer 10::1 as-number 65009
[SwitchA-bgp-af-ipv6] quit
[SwitchA-bgp] quit
```

② 配置 Switch B。

```
[SwitchB] bgp 65009
[SwitchB-bgp] ipv6-family
[SwitchB-bgp-af-ipv6] peer 10::2 as-number 65008
```

③ 查看 Switch B 的对等体信息。

```
[SwitchB] display bgp ipv6 peer
 BGP local router ID : 2.2.2.2
 Local AS number : 65009
 Total number of peers : 3                 Peers in established state : 3
```

Peer	V	AS	MsgRcvd	MsgSent	OutQ	PrefRcv	Up/Down	State
10::2	4	65008	3	3	0	0	00:01:16	Established
9:3::2	4	65009	2	3	0	0	00:00:40	Established

9:1::2	4	65009	2	4	0	0	700:00:19	Established

④ 查看 Switch C 的对等体信息。

```
[SwitchC] display bgp ipv6 peer
 BGP local router ID : 3.3.3.3
 Local AS number : 65009
 Total number of peers : 2                    Peers in established state : 2
  Peer       V    AS      MsgRcvd   MsgSent   OutQ   PrefRcv   Up/Down      State

  9:3::1     4    65009   4         4         0      0         00:02:18     Established
  9:2::2     4    65009   4         5         0      0         00:01:52     Established
```

可以看出，Switch A 和 Switch B 之间建立了 EBGP 连接，Switch B、Switch C 和 Switch D 之间建立了 IBGP 连接。

注意：为了提高 BGP 连接的可靠性和稳定性，可将 BGP 连接所使用的本地接口配置成 Loopback 接口，这样当网络中存在冗余链路时，不会因为其中某个接口或链路的故障而使 BGP 连接中断。

通常情况下，EBGP 对等体之间必须具有直连的物理链路，如果不满足这一要求，则必须使用 peer ebgp-max-hop 命令允许它们之间经过多跳建立 TCP 连接。

第10章

IP组播配置指导

10.1 IGMP协议典型配置指导

10.1.1 IGMP典型配置指导

IGMP用来在组播接收主机和相邻的组播路由器(或三层交换机)之间建立、维护组播组成员关系。

IGMP先后推出3个协议版本。与IGMPv1相比,IGMPv2主要增加了查询器选举机制和离开组机制并能兼容IGMPv1;IGMPv3在兼容和继承IGMPv1和IGMPv2的基础上,进一步增强了接收主机的控制能力,即增加了针对组播源的过滤模式,使接收主机在加入某组播组G的同时,能够明确要求接收或拒绝来自某特定组播源S的组播信息。

IGMPv3通常配合PIM-SSM使用,技术实现复杂;目前支持IGMPv2的主机和网络设备占主流。H3C以太网交换机在使能IGMP后的默认版本为IGMPv2。

1. 背景

M公司为加强研发区域、库房等重点场所的安全防范,选择并购买了一套H3C iVS IP监控解决方案。该解决方案使用组播技术实现前端的编码器单点发送视频图像,后端的解码器和视频管理客户端多点接收,从而有效地减轻了编码器的负担,同时充分地节省了网络带宽。为此,需要在现有网络中H3C以太网交换机上配置相应的IGMP协议。

2. 组网图

图10-1所示为IGMP典型配置组网图。

3. 配置需求

(1) 接收者(Receiver)通过组播方式接收视频信息,不同部门的接收者组成末梢网络N1和N2,Host A与Host C分别为N1和N2中的组播信息接收者。

(2) PIM网络中的Switch A连接N1,Switch B与Switch C共同连接N2。

(3) Switch A通过Vlan-interface 100连接N1,通过Vlan-interface 101连接PIM网络中的其他设备。

(4) Switch B与Switch C分别通过各自的Vlan-interface 200连接N2,并分别通过Vlan-interface 201和Vlan-interface 202连接PIM网络中的其他设备。

(5) Switch A与N1之间运行IGMPv2;Switch B和Switch C与N2之间也分别运行IGMPv2。且由于Switch B的接口IP地址较小,因此在N2中通常由其来充当IGMP查询器。

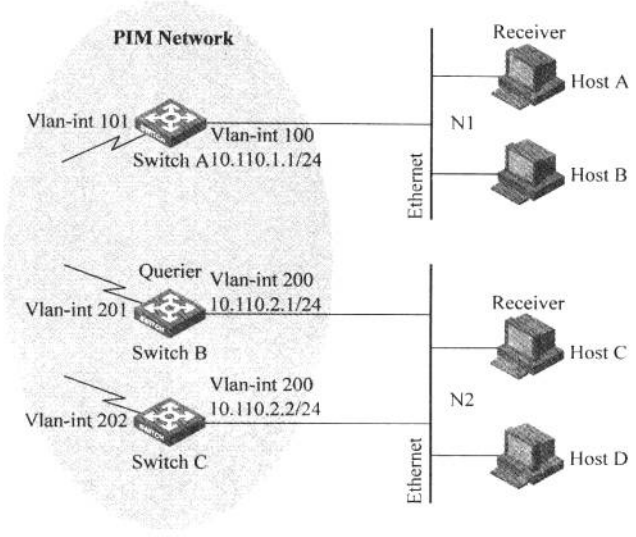


图 10-1 IGMP 典型配置组网图

(6) 配置 Switch A 发送 IGMP 普遍组查询报文的时间间隔为 30s，最大响应时间为 5s，发送 IGMP 特定组查询报文的时间间隔为 2s。

4. 配置过程和解释

(1) 配置 IP 地址和单播路由协议。按照图 10-1 配置各接口的 IP 地址和子网掩码，具体配置过程略。

配置 PIM 网络内各交换机之间采用 OSPF 协议进行互连，确保 PIM 网络内部在网络层互通，并且各交换机之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IP 组播路由，并使能 PIM-DM 和 IGMP。

① 在 Switch A 上使能 IP 组播路由，在各接口上使能 PIM-DM，并在主机侧接口 Vlan-interface 100 上使能 IGMP。

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] pim dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim dm
[SwitchA-Vlan-interface101] quit
```

② 在 Switch A 上配置发送 IGMP 通用组查询报文的时间间隔、最大响应时间以及发送特定组查询报文的时间间隔。

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp timer query 30
[SwitchA-Vlan-interface100] igmp max-response-time 5
```

```
[SwitchA-Vlan-interface100] igmp last-member-query-interval 2
```

③ 在 Switch B 上使能 IP 组播路由，在各接口上使能 PIM-DM，并在主机侧接口 Vlan-interface 200 上使能 IGMP。

```
<SwitchB> system-view
[SwitchB] multicast routing-enable
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] igmp enable
[SwitchB-Vlan-interface200] pim dm
[SwitchB-Vlan-interface200] quit
[SwitchB] interface vlan-interface 201
[SwitchB-Vlan-interface201] pim dm
[SwitchB-Vlan-interface201] quit
```

④ 在 Switch C 上使能 IP 组播路由，在各接口上使能 PIM-DM，并在主机侧接口 Vlan-interface 200 上使能 IGMP。

```
<SwitchC> system-view
[SwitchC] multicast routing-enable
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] igmp enable
[SwitchC-Vlan-interface200] pim dm
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 202
[SwitchC-Vlan-interface202] pim dm
[SwitchC-Vlan-interface202] quit
```

(3) 检验配置效果。通过使用 display igmp interface 命令可以查看各交换机接口上 IGMP 的配置和运行情况。例如，查看 Switch B 在 Vlan-interface 200 上的 IGMP 信息。

```
[SwitchB] display igmp interface vlan-interface 200
Vlan-interface 200(10.110.2.1):
  IGMP is enabled
  Current IGMP version is 2
  Value of query interval for IGMP(in seconds): 60
  Value of other querier present interval for IGMP(in seconds): 125
  Value of maximum query response time for IGMP(in seconds): 10
  Querier for IGMP: 10.110.2.1 (this router)
  Total 1 IGMP Group reported
```

提示：配置时应确保发送 IGMP 普遍组查询报文的时间间隔大于 IGMP 普遍组查询的最大响应时间，否则有可能造成对组播组成员的误删除；对 IGMP 普遍组查询的最大响应时间、发送 IGMP 特定组查询报文的时间间隔以及 IGMP 其他查询器的存在时间所做的配置，只有当设备运行在 IGMPv2 或 IGMPv3 时才有效。

10.1.2 IGMP Snooping 典型配置指导

IGMP Snooping 是运行在二层交换机上的组播约束机制，用于管理和控制组播组。

当二层交换机没有运行 IGMP Snooping 时，组播数据将在入端口所属的 VLAN 内被广播。而运行 IGMP Snooping 的二层交换机通过对收到的 IGMP 报文进行侦听并分析，为端口和 MAC 组播地址建立起映射关系，并根据这样的映射关系将组播数据转发至指定的接收者。

1. 背景

为降低网络成本，M 公司在接入层中部署了二层以太网交换机。在正常情况下，二层以太网交换机会在所有端口（收到组播报文的源端口除外）泛洪组播报文，造成带宽浪费及网络流量过大。为了解决以上问题，M 公司在二层以太网交换机上配置 IGMP Snooping。

2. 组网图

图 10-2 所示为 IGMP Snooping 典型配置组网图。

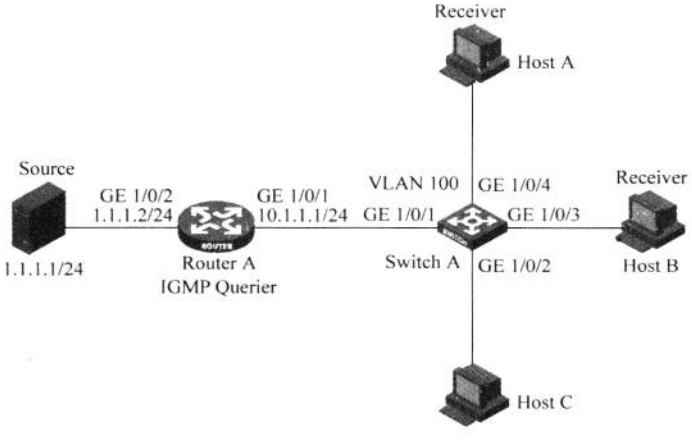


图 10-2 IGMP Snooping 典型配置组网图

3. 配置需求

（1）如图 10-2 所示，Router A 通过 GigabitEthernet 1/0/2 接口连接组播源（Source），通过 GigabitEthernet 1/0/1 接口连接 Switch A。

（2）Router A 与 Switch A 之间运行 IGMPv2，Switch A 上运行版本 2 的 IGMP Snooping，并由 Router A 充当 IGMP 查询器。

（3）通过配置，使连接在 Switch A 上的接收者（Receiver）Host A 和 Host B 只能接收发往组播组 224.1.1.1 的组播数据。

（4）要求通过配置，使连接在 Switch A 上的接收者（Receiver）Host A 和 Host B 即使由于突然出现了某种意外而临时中断接收组播数据，组播数据也能够不间断地通过 Switch A 的接口 GigabitEthernet 1/0/3 和 GigabitEthernet 1/0/4 转发出去。

4. 配置过程和解释

（1）配置各设备接口的 IP 地址。按照图 10-2 配置各接口的 IP 地址和子网掩码，具体配置过程略。

（2）配置 Router A。使能 IP 组播路由，在各接口上使能 PIM-DM，并在接口 GigabitEthernet 1/0/1 上使能 IGMPv2。

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface GigabitEthernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] pim dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface GigabitEthernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim dm
[RouterA-GigabitEthernet1/0/2] quit
```

(3) 配置 Switch A。

① 全局使能 IGMP Snooping。

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

② 创建 VLAN 100,将端口 GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 添加到该 VLAN 中,在该 VLAN 内使能 IGMP Snooping,并开启丢弃未知组播数据报文功能。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port GigabitEthernet 1/0/1 to GigabitEthernet 1/0/4
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] igmp-snooping drop-unknown
[SwitchA-vlan100] quit
```

③ 配置组播组过滤器,使 VLAN 100 内的主机只能加入组播组 224.1.1.1。

```
[SwitchA] acl number 2001
[SwitchA-acl-basic-2001] rule permit source 224.1.1.1 0
[SwitchA-acl-basic-2001] quit
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] group-policy 2001 vlan 100
[SwitchA-igmp-snooping] quit
```

④ 在 GigabitEthernet 1/0/3 和 GigabitEthernet 1/0/4 上分别使能模拟主机加入功能。

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] igmp-snooping host-join 224.1.1.1 vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
[SwitchA] interface GigabitEthernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] igmp-snooping host-join 224.1.1.1 vlan 100
[SwitchA-GigabitEthernet1/0/4] quit
```

(4) 检验配置效果。查看 Switch A 上 VLAN 100 内 IGMP Snooping 组播组的详细信息。

```
[SwitchA] display igmp-snooping group vlan 100 verbose
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
  Port flags: D-Dynamic port, S-Static port, A-Aggregation port, C-Copy port
```

```
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):100.
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Router port(s):total 1 port.
        GE1/0/1              (D) ( 00:01:30 )
  IP group(s):the following ip group(s) match to one mac group.
    IP group address:224.1.1.1
      (0.0.0.0, 224.1.1.1):
        Attribute: Host Port
        Host port(s):total 2 port.
          GE1/0/3            (D) ( 00:03:23 )
          GE1/0/4            (D) ( 00:03:23 )
  MAC group(s):
    MAC group address:0100-5e01-0101
        Host port(s):total 2 port.
          GE1/0/3
          GE1/0/4
```

由此可见，Switch A 上的端口 GigabitEthernet 1/0/3 和 GigabitEthernet 1/0/4 已经加入了组播组(0.0.0.0,224.1.1.1)。

提示：二、三层组播协议可以同时运行在交换机上，但是在同一个 VLAN 和该 VLAN 对应的虚接口上不能同时运行二层和三层组播协议。

在启动指定 VLAN 的 IGMP Snooping 前，应首先在系统视图下启动全局 IGMP Snooping 功能；否则，将无法配置成功。

与静态成员端口不同，配置了模拟主机加入的端口会作为动态成员端口而参与动态成员端口的老化过程。

10.1.3 组播 VLAN 典型配置指导

在传统的组播点播方式下，当属于不同 VLAN 的主机分别进行组播点播时，组播转发器需要将组播数据在每个 VLAN 内都复制一份。这样既造成了带宽的浪费，也给组播转发器增加了额外的负担。

可以使用组播 VLAN 功能解决这个问题。在设备上配置了组播 VLAN 后，组播转发器只需将组播数据在组播 VLAN 内复制一份发送给下游二层交换机，而不必在每个用户 VLAN 内都复制一份。

1. 背景

在 M 公司网络中，出于隔离不必要广播的目的，后端的解码器和视频管理客户端处于不同 VLAN 中。但这样就使得设备会复制多份组播到多个 VLAN，导致网络中组播流量的泛洪。基于上述原因，管理员决定使用组播 VLAN。

2. 组网图

图 10-3 所示为组播 VLAN 典型配置组网图。

3. 配置需求

(1) 如图 10-3 所示，Router A 通过 GigabitEthernet 1/0/2 接口连接组播源(Source)，通过 GigabitEthernet 1/0/1 接口连接 Switch A。

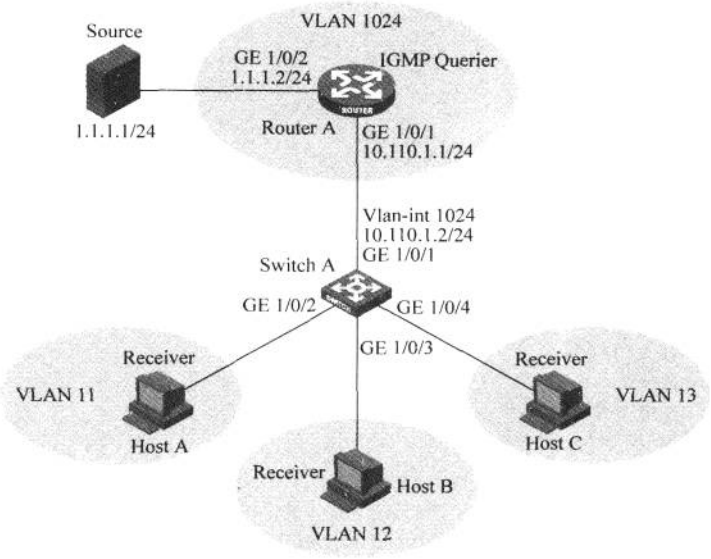


图 10-3 组播 VLAN 典型配置组网图

(2) Router A 与 Switch A 之间运行 IGMP，Switch A 上运行 IGMP Snooping，并由 Router A 充当 IGMP 查询器。

(3) Switch A 的端口 GigabitEthernet 1/01 属于 VLAN 1024，端口 GigabitEthernet 1/0/2～GigabitEthernet 1/0/4 分别属于 VLAN 11～VLAN 13，Host A～Host C 分别连接到 Switch A 的端口 GigabitEthernet 1/0/2～GigabitEthernet 1/0/4 上。

(4) 通过配置组播 VLAN，使 Router A 向 Switch A 下的这 3 台主机传送组播数据时，只需要向 VLAN 1024 发送一份即可，而不必向每个 VLAN 都发送。

4. 配置过程和解释

(1) 配置各设备接口的 IP 地址。按照图 10-3 配置各接口的 IP 地址和子网掩码，具体配置过程略。

(2) 配置 Router A。使能 IP 组播路由，在各接口上使能 PIM-DM，并在接口GigabitEthernet 1/0/1 上使能 IGMP。

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface GigabitEthernet 1/0/1
[RouterA-GigabitEthernet1/0/1] pim dm
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface GigabitEthernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim dm
[RouterA-GigabitEthernet1/0/2] quit
```

(3) 配置 Switch A。

① 全局使能 IGMP Snooping。

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

② 创建 VLAN 11，并将端口 GigabitEthernet 1/0/2 添加到该 VLAN 中。

```
[SwitchA] vlan 11
[SwitchA-vlan11] port GigabitEthernet 1/0/2
[SwitchA-vlan11] quit
```

VLAN 12 与 VLAN 13 的配置与 VLAN 11 相似，配置过程略。

③ 创建 VLAN 1024，将端口 GigabitEthernet 1/0/1 添加到该 VLAN 中，并在该 VLAN 内使能 IGMP Snooping。

```
[SwitchA] vlan 1024
[SwitchA-vlan1024] port GigabitEthernet 1/0/1
[SwitchA-vlan1024] igmp-snooping enable
[SwitchA-vlan1024] quit
```

④ 使能 VLAN 1024 为组播 VLAN，并将 VLAN 11～VLAN 13 都配置为该组播 VLAN 的子 VLAN。

```
[SwitchA] multicast-vlan 1024 enable
[SwitchA] multicast-vlan 1024 subvlan 11 to 13
```

(4) 检验配置效果。查看 Switch A 上所有组播 VLAN 及其子 VLAN 的信息。

```
[SwitchA] display multicast-vlan
multicast vlan 1024's subvlan list:
vlan 11-13
```

提示：如果设备上已使能了 IP 组播路由，则不允许在该设备上配置组播 VLAN。

在配置成为组播 VLAN 的 VLAN 内必须使能 IGMP Snooping，才能实现组播 VLAN 功能；而在组播 VLAN 的子 VLAN 内不必使能 IGMP Snooping。

10.2 PIM 协议配置指导

10.2.1 PIM-DM 典型配置指导

PIM-DM 属于密集模式的组播路由协议，使用“推(Push)模式”传送组播数据，通常适用于组播组成员相对比较密集的小型网络。

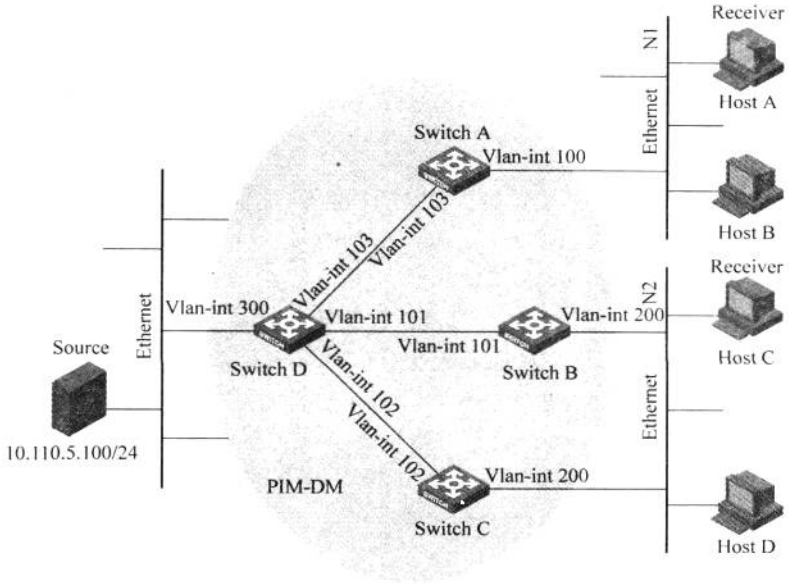
PIM-DM 通过“扩散-剪枝”方式而构建的转发路径是有源树(Source Tree，即以组播源为“根”、组播组成员为“枝叶”的一棵转发树)，而有源树使用的是从组播源到接收者的最短路径，因此也被称为最短路径树(Shortest Path Tree，SPT)。

1. 背景

M 公司部署使用组播路由协议。因 M 公司网络较小，只在一个楼宇范围内，出于配置简单的目的，先使用 PIM-DM 协议进行测试。

2. 组网图

图 10-4 所示为 PIM-DM 典型配置组网图。



设　备	接　口	IP 地址	设　备	接　口	IP 地址
Switch A	Vlan-int 100	10.110.1.1/24	Switch D	Vlan-int 300	10.110.5.1/24
	Vlan-int 103	192.168.1.1/24		Vlan-int 103	192.168.1.2/24
Switch B	Vlan-int 200	10.110.2.1/24		Vlan-int 101	192.168.2.2/24
	Vlan-int 101	192.168.2.1/24		Vlan-int 102	192.168.3.2/24
Switch C	Vlan-int 200	10.110.2.2/24			
	Vlan-int 102	192.168.3.1/24			

图 10-4　PIM-DM 典型配置组网图

3. 配置需求

(1) 接收者通过组播方式接收视频信息，不同部门的接收者组成末梢网络，每个末梢网络中都存在至少一个接收者，整个 PIM 域采用 DM 模式。

(2) Host A 和 Host C 为两个末梢网络中的组播信息接收者。

(3) Switch D 通过 Vlan-interface 300 接口与组播源(Source)所在的网络连接。

(4) Switch A 通过 Vlan-interface 100 接口连接末梢网络 N1，通过 Vlan-interface 103 接口连接 Switch D。

(5) Switch B 和 Switch C 通过各自的 Vlan-interface 200 接口连接末梢网络 N2，分别通过 Vlan-interface 101 和 Vlan-interface 102 接口连接 Switch D。

(6) Switch A 与末梢网络 N1 之间运行 IGMPv2；Switch B 和 Switch C 与末梢网络 N2 之间也运行 IGMPv2。

4. 配置过程和解释

(1) 配置 IP 地址和单播路由协议。按照图 10-4 配置各接口的 IP 地址和子网掩码，具

体配置过程略。

配置 PIM-DM 域内的各交换机之间采用 OSPF 协议进行互连，确保 PIM-DM 域内部在网络层互通，并且各交换机之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IP 组播路由，并在各接口上使能 PIM-DM 和 IGMP。

① 在 Switch A 上使能 IP 组播路由，在各接口上使能 PIM-DM，并在 Switch A 连接末梢网络的接口 Vlan-interface 100 上使能 IGMPv2。

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] pim dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 103
[SwitchA-Vlan-interface103] pim dm
[SwitchA-Vlan-interface103] quit
```

Switch B 和 Switch C 的配置与 Switch A 相似，配置过程略。

② 在 Switch D 上使能 IP 组播路由，并在其各接口上使能 PIM-DM。

```
<SwitchD> system-view
[SwitchD] multicast routing-enable
[SwitchD] interface vlan-interface 300
[SwitchD-Vlan-interface300] pim dm
[SwitchD-Vlan-interface300] quit
[SwitchD] interface vlan-interface 103
[SwitchD-Vlan-interface103] pim dm
[SwitchD-Vlan-interface103] quit
[SwitchD] interface vlan-interface 101
[SwitchD-Vlan-interface101] pim dm
[SwitchD-Vlan-interface101] quit
[SwitchD] interface vlan-interface 102
[SwitchD-Vlan-interface102] pim dm
[SwitchD-Vlan-interface102] quit
```

(3) 检验配置效果。

① 通过使用 display pim interface 命令可以查看交换机接口上 PIM 的配置和运行情况。例如，查看 Switch D 上 PIM 的配置信息。

```
[SwitchD] display pim interface
Interface          NbrCnt HelloInt   DR-Pri     DR-Address
Vlan300            0      30         1          10.110.5.1      (local)
Vlan103            1      30         1          192.168.1.2     (local)
Vlan101            1      30         1          192.168.2.2     (local)
Vlan102            1      30         1          192.168.3.2     (local)
```

② 通过使用 display pim neighbor 命令可以查看交换机之间的 PIM 邻居关系。例如，

查看 Switch D 上 PIM 的邻居关系信息。

```
[SwitchD] display pim neighbor
 Total Number of Neighbors = 3
Neighbor        Interface       Uptime      Expires     Dr-Priority
192.168.1.1     Vlan103         00:02:22    00:01:27    1
192.168.2.1     Vlan101         00:00:22    00:01:29    3
192.168.3.1     Vlan102         00:00:23    00:01:31    5
```

③ 假如 Host A 需要接收组播组 G(225.1.1.1)的信息，当组播源 S(10.110.5.100/24)向组播组 G 发送组播数据时，通过扩散生成 SPT，SPT 路径中各交换机(Switch A 和 Switch D)上都存在(S,G)表项，Host A 向 Switch A 注册，在 Switch A 上生成(*,G)表项。通过使用 display pim routing-table 命令可以查看交换机的 PIM 路由表信息。例如：

a. 查看 Switch A 上的 PIM 路由表信息。

```
[SwitchA] display pim routing-table
Total 1 (*, G) entry; 1 (S, G) entry
  (*, 225.1.1.1)
      Protocol: pim-dm, Flag: WC
      UpTime: 00:04:25
      Upstream interface: NULL
          Upstream neighbor: NULL
          RPF prime neighbor: NULL
      Downstream interface(s) information:
        Total number of downstreams: 1
            1: Vlan-interface100
                  Protocol: igmp, UpTime: 00:04:25, Expires: never
  (10.110.5.100, 225.1.1.1)
      Protocol: pim-dm, Flag: ACT
      UpTime: 00:06:14
      Upstream interface: Vlan-interface 103,
          Upstream neighbor: 192.168.1.2
          RPF prime neighbor: 192.168.1.2
      Downstream interface(s) information:
        Total number of downstreams: 1
            1: Vlan-interface 100
                  Protocol: pim-dm, UpTime: 00:04:25, Expires: never
```

Switch B 和 Switch C 上的显示信息与 Switch A 类似。

b. 查看 Switch D 上的 PIM 路由表信息。

```
[SwitchD] display pim routing-table
Total 0 (*, G) entry; 1 (S, G) entry
  (10.110.5.100, 225.1.1.1)
      Protocol: pim-dm, Flag: LOC ACT
      UpTime: 00:03:27
      Upstream interface: Vlan-interface 300
          Upstream neighbor: NULL
          RPF prime neighbor: NULL
```

```
Downstream interface(s) information:
  Total number of downstreams: 3
    1: Vlan-interface 103
          Protocol: pim-dm, UpTime: 00:03:27, Expires: never
    2: Vlan-interface 101
          Protocol: pim-dm, UpTime: 00:03:27, Expires: never
    3: Vlan-interface 102
          Protocol: pim-dm, UpTime: 00:03:27, Expires: never
```

提示：在部署 PIM-DM 域时，建议在非边界三层交换机的所有接口上启动 PIM-DM。在连接组播源的三层交换机接口上也必须启动 PIM-DM。

在连接组播接收者的三层交换机接口上可不用启动 PIM-DM。但如果存在多台三层交换机同时连接组播接收者，则建议都在该接口上启动 PIM-DM 用以选定唯一的组播转发器，当运行 IGMPv1 时 DR(Designated Router，指定路由器)还可以充当 IGMP 查询器。

10.2.2 PIM-SM 典型配置指导

PIM-DM 构建的 SPT 虽然转发路径最短，但是其建立的过程效率较低，并不适合大中型网络。而 PIM-SM 属于稀疏模式的组播路由协议，使用“拉(Pull)模式”传送组播数据，通常适用于组播组成员分布相对分散、范围较广的大中型网络。

PIM-SM 实现组播转发的核心任务就是构造并维护 RPT(Rendezvous Point Tree，共享树或汇集树)，RPT 选择 PIM 域中某台路由器作为公用的根节点 RP(Rendezvous Point，汇集点)，组播数据通过 RP 沿着 RPT 转发给接收者。

通过 PIM-SM“注册/加入”机制在组播源和 RP 之间建立 SPT，完整的组播转发路径由 SPT 和 RPT 组成，而组播数据到达接收者侧 DR(Designated Router，指定路由器)后，该 DR 可以发起 SPT 切换，从而在组播源和接收者之间建立 SPT。

RP 是 PIM-SM 域中的核心设备。在结构简单的小型网络中，组播信息量少，此时可以在 PIM-SM 域中的各路由器上静态指定 RP 的位置。但是在更多的情况下，PIM-SM 域的规模都很大，通过 RP 转发的组播信息量巨大。为了缓解 RP 的负担并优化 RPT 的拓扑结构，可以在 PIM-SM 域中配置多个 C-RP(Candidate-RP，候选 RP)，通过自举机制来动态选举 RP，使不同的 RP 服务于不同的组播组，此时需要配置 BSR(BootStrap Router，自举路由器)。

BSR 是 PIM-SM 域的管理核心，一个 PIM-SM 域内只能有一个 BSR，但可以配置多个 C-BSR(Candidate-BSR，候选 BSR)。这样，一旦 BSR 发生故障，其余 C-BSR 能够通过自动选举产生新的 BSR，从而确保业务免受中断。

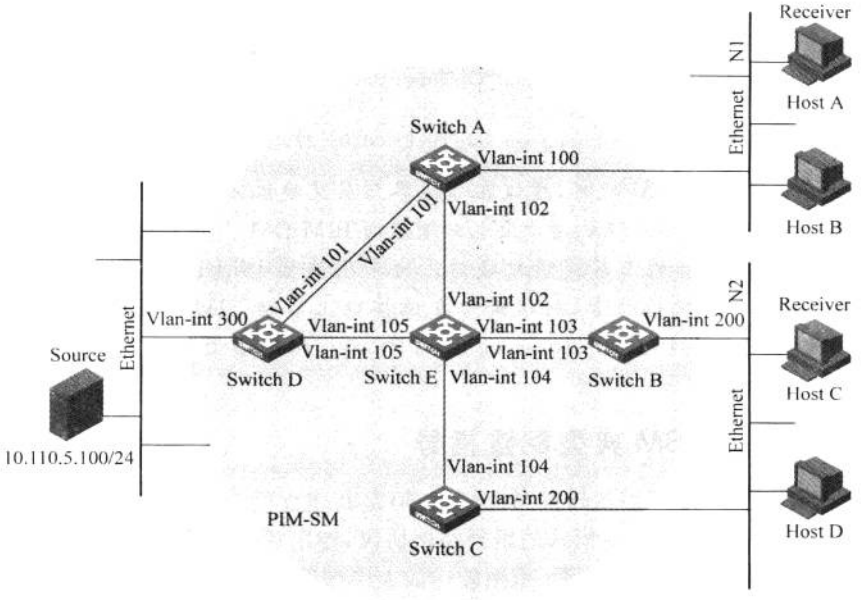
一个 RP 可以同时服务于多个组播组，但一个组播组只能唯一对应一个 RP。一台设备可以同时充当 C-RP 和 C-BSR。

1. 背景

PIM-DM 协议配置使用简单。然而，由于其天然的“推(Push)模式”特性，使得网络中时刻充满组播报文，随着组播源的数量增多，情况越来越严重。所以，M 公司使用 PIM-SM 协议进行测试。

2. 组网图

图 10-5 所示为 PIM-SM 典型配置组网图。



设　备	接　口	IP 地址	设　备	接　口	IP 地址
Switch A	Vlan-int 100	10.110.1.1/24	Switch D	Vlan-int 300	10.110.5.1/24
	Vlan-int 101	192.168.1.1/24		Vlan-int 101	192.168.1.2/24
	Vlan-int 102	192.168.9.1/24		Vlan-int 105	192.168.4.2/24
Switch B	Vlan-int 200	10.110.2.1/24	Switch E	Vlan-int 104	192.168.3.2/24
	Vlan-int 103	192.168.2.1/24		Vlan-int 103	192.168.2.2/24
Switch C	Vlan-int 200	10.110.2.2/24		Vlan-int 102	192.168.9.2/24
	Vlan-int 104	192.168.3.1/24		Vlan-int 105	192.168.4.1/24

图 10-5　PIM-SM 典型配置组网图

3. 配置需求

(1) 接收者通过组播方式接收视频信息，不同部门的接收者组成末梢网络，每个末梢网络中都存在至少一个接收者，整个 PIM 域采用 SM 非管理域模式。

(2) Host A 和 Host C 为两个末梢网络中的组播信息接收者。

(3) Switch D 通过 Vlan-interface 300 接口与组播源(Source)所在网络连接。

(4) Switch A 通过 Vlan-interface 100 接口连接末梢网络 N1，通过 Vlan-interface 101 接口和 Vlan-interface 102 接口分别连接 Switch D 和 Switch E。

(5) Switch B 和 Switch C 通过各自的 Vlan-interface 200 接口连接末梢网络 N2，分别通过 Vlan-interface 103 和 Vlan-interface 104 接口连接 Switch E。

(6) 将 Switch D 的 Vlan-interface 105 接口和 Switch E 的 Vlan-interface 102 接口都配置为 C-BSR 和 C-RP，其中 Switch E 上 C-BSR 的优先级较高。C-RP 所服务的组播组范

围为 225.1.1.0/24，通过改变哈希掩码长度使此范围内的组地址间隔映射到这两个 C-RP 上。

(7) Switch A 与末梢网络 N1 之间运行 IGMPv2；Switch B 和 Switch C 与末梢网络 N2 之间也运行 IGMPv2。

4. 配置过程和解释

(1) 配置 IP 地址和单播路由协议。按照图 10-5 配置各接口的 IP 地址和子网掩码，具体配置过程略。

配置 PIM-SM 域内的各交换机之间采用 OSPF 协议进行互连，确保 PIM-SM 域内部在网络层互通，并且各交换机之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IP 组播路由，并在各接口上使能 PIM-SM 和 IGMP。在 Switch A 上使能 IP 组播路由，在各接口上使能 PIM-SM，并在 Switch A 连接末梢网络的接口 Vlan-interface 100 上使能 IGMPv2。

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim sm
[SwitchA-Vlan-interface102] quit
```

Switch B 和 Switch C 的配置与 Switch A 相似，Switch D 和 Switch E 除了不需要在相应接口上使能 IGMP 外，其他的配置也与 Switch A 相似，配置过程略。

(3) 配置 C-BSR 和 C-RP。

① 在 Switch D 上配置 RP 通告的服务范围，以及 C-BSR 和 C-RP 的位置，并指定哈希掩码长度为 32，C-BSR 的优先级为 10。

```
<SwitchD> system-view
[SwitchD] acl number 2005
[SwitchD-acl-basic-2005] rule permit source 225.1.1.0 0.0.0.255
[SwitchD-acl-basic-2005] quit
[SwitchD] pim
[SwitchD-pim] c-bsr vlan-interface 105 32 10
[SwitchD-pim] c-rp vlan-interface 105 group-policy 2005
[SwitchD-pim] quit
```

② 在 Switch E 上配置 RP 通告的服务范围，以及 C-BSR 和 C-RP 的位置，并指定哈希掩码长度为 32，C-BSR 的优先级为 20。

```
<SwitchE> system-view
[SwitchE] acl number 2005
[SwitchE-acl-basic-2005] rule permit source 225.1.1.0 0.0.0.255
```

```
[SwitchE-acl-basic-2005] quit
[SwitchE] pim
[SwitchE-pim] c-bsr vlan-interface 102 32 20
[SwitchE-pim] c-rp vlan-interface 102 group-policy 2005
[SwitchE-pim] quit
```

(4) 检验配置效果。

① 通过使用 display pim interface 命令可以查看交换机接口上 PIM 的配置和运行情况。例如,查看 Switch A 上 PIM 的配置信息。

```
[SwitchA] display pim interface
 Interface          NbrCnt  HelloInt    DR-Pri     DR-Address
 Vlan100            0       30          1          10.110.1.1   (local)
 Vlan101            1       30          1          192.168.1.2
 Vlan102            1       30          1          192.168.9.2
```

② 通过使用 display pim bsr-info 命令可以查看交换机上 BSR 选举的信息,以及本地配置并生效的 C-RP 信息。例如:

a. 查看 Switch A 上的 BSR 信息,以及本地配置并生效的 C-RP 信息。

```
[SwitchA] display pim bsr-info
Elected BSR Address: 192.168.9.2
    Priority: 20
    Hash mask length: 32
    State: Accept Preferred
    Scope: Not scoped
    Uptime: 01:40:40
    Expires: 00:01:42
```

b. 查看 Switch D 上的 BSR 信息,以及本地配置并生效的 C-RP 信息。

```
[SwitchD] display pim bsr-info
Elected BSR Address: 192.168.9.2
    Priority: 20
    Hash mask length: 32
    State: Accept Preferred
    Scope: Not scoped
    Uptime: 00:05:26
    Expires: 00:01:45
 Candidate BSR Address: 192.168.4.2
    Priority: 10
    Hash mask length: 32
    State: Candidate
    Scope: Not scoped
 Candidate RP: 192.168.4.2(Vlan-interface105)
    Priority: 0
    HoldTime: 150
    Advertisement Interval: 60
    Next advertisement scheduled at: 00:00:34
```

c. 查看 Switch E 上的 BSR 信息,以及本地配置并生效的 C-RP 信息。

```
[SwitchE] display pim bsr-info
Elected BSR Address: 192.168.9.2
    Priority: 20
    Hash mask length: 32
    State: Elected
    Scope: Not scoped
    Uptime: 00:00:18
    Next BSR message scheduled at: 00:01:52
 Candidate BSR Address: 192.168.9.2
    Priority: 20
    Hash mask length: 32
    State: Elected
    Scope: Not scoped
Candidate RP: 192.168.9.2(Vlan-interface102)
    Priority: 0
    HoldTime: 150
    Advertisement Interval: 60
    Next advertisement scheduled at: 00:00:48
```

③ 通过使用 display pim rp-info 命令可以查看交换机上获取的 RP 信息。例如，查看 Switch A 上的 RP 信息。

```
[SwitchA] display pim rp-info
PIM-SM BSR RP information:
Group/MaskLen: 225.1.1.0/24
    RP: 192.168.4.2
    Priority: 0
    HoldTime: 150
    Uptime: 00:51:45
    Expires: 00:02:22

    RP: 192.168.9.2
    Priority: 0
    HoldTime: 150
    Uptime: 00:51:45
    Expires: 00:02:22
```

④ 假如 Host A 需要接收组播组 G(225.1.1.0)的信息，由于根据哈希算法得出 G 对应的 RP 为 Switch E，Switch A 和 Switch E 之间会生成 RPT。组播源 S(10.110.5.100/24)向 RP 发起注册后，Switch D 和 Switch E 之间会生成 SPT。当 Switch A 收到组播数据后立即执行从 RPT 到 SPT 的切换。RPT 路径中的交换机(Switch A 和 Switch E)上存在(*，G)表项，而 SPT 路径中的交换机(Switch A 和 Switch D)上存在(S，G)表项，通过使用 display pim routing-table 命令可以查看交换机的 PIM 路由表信息。例如：

a. 查看 Switch A 上的 PIM 路由表信息。

```
[SwitchA] display pim routing-table
Total 1 (*, G) entry; 1 (S, G) entry
 (*, 225.1.1.0)
     RP: 192.168.9.2
```

```
        Protocol: pim-sm, Flag: WC
        UpTime: 00:13:46
        Upstream interface: Vlan-interface 102,
            Upstream neighbor: 192.168.9.2
            RPF prime neighbor: 192.168.9.2
        Downstream interface(s) information:
          Total number of downstreams: 1
              1: : Vlan-interface 100
                    Protocol: igmp, UpTime: 00:13:46, Expires:00:03:06
  (10.110.5.100, 225.1.1.0)
        RP: 192.168.9.2
        Protocol: pim-sm, Flag: SPT ACT
        UpTime: 00:00:42
        Upstream interface: Vlan-interface 101,
            Upstream neighbor: 192.168.1.2
            RPF prime neighbor: 192.168.1.2
        Downstream interface(s) information:
          Total number of downstreams: 1
              1: : Vlan-interface 100
                    Protocol: pim-sm, UpTime: 00:00:42, Expires:00:03:06
```

Switch B 和 Switch C 上的显示信息与 Switch A 类似。

b. 查看 Switch D 上的 PIM 路由表信息。

```
[SwitchD] display pim routing-table
Total 0 ( * , G) entry; 1 (S, G) entry
  (10.110.5.100, 225.1.1.0)
        RP: 192.168.9.2
        Protocol: pim-sm, Flag: SPT ACT
        UpTime: 00:00:42
        Upstream interface: Vlan-interface 300
            Upstream neighbor: NULL
            RPF prime neighbor: NULL
        Downstream interface(s) information:
          Total number of downstreams: 1
              1: : Vlan-interface 105
                    Protocol: pim-sm, UpTime: 00:00:42, Expires:00:02:06
```

c. 查看 Switch E 上的 PIM 路由表信息。

```
[SwitchE] display pim routing-table
Total 1 ( * , G) entry; 0 (S, G) entry
  ( * , 225.1.1.0)
        RP: 192.168.9.2 (local)
        Protocol: pim-sm, Flag: WC
        UpTime: 00:13:16
        Upstream interface: Register
            Upstream neighbor: 192.168.4.2
            RPF prime neighbor: 192.168.4.2
```

```
Downstream interface(s) information:
  Total number of downstreams: 1
    1: : Vlan-interface102
          Protocol: pim-sm, UpTime: 00:13:16, Expires: 00:03:22
```

提示：在部署 PIM-SM 域时，建议在非边界三层交换机的所有接口上启动 PIM-SM。在连接组播源的三层交换机接口上也必须启动 PIM-SM。

在连接组播接收者的三层交换机接口上可不用启动 PIM-SM。但如果存在多台三层交换机同时连接组播接收者，则建议都在该接口上启动 PIM-SM 用以选定唯一的组播转发器，当运行 IGMPv1 时 DR(Designated Router，指定路由器)还可以充当 IGMP 查询器。

10.2.3 PIM-SSM 典型配置指导

不同于 ASM (Any-Source Multicast，任意信源组播)模型，SSM (Source-Specific Multicast，指定信源组播)模型为指定源组播提供了解决方案，通过 IGMPv3 来维护接收主机与路由器(或三层交换机)之间的关系。

在实际应用中，通常采用 PIM-SM 模式的一部分技术来实现 SSM 模型。由于接收者已经通过带外方式(如广告咨询等)知道了组播源的具体位置，因此在 SSM 模型中无须 RP，无须构建 RPT，也无须通过 MSDP(Multicast Source Discovery Protocol，组播源发现协议)来发现其他 PIM 域内的组播源。

1. 背景

M 公司网络中的 PIM-SM 协议运行很成功，网络中流量大大减少，且组播运行效果也不错。但随着网络规模扩大，组播域有可能会扩散到其他的运营商，PIM-SM 协议中的 RP 机制在跨越 AS 时工作并不是很好。基于上述考虑，M 公司未雨绸缪，测试部署 PIM-SSM。

2. 组网图

图 10-6 所示为 PIM-SSM 典型配置组网图。

3. 配置需求

(1) 接收者通过组播方式接收视频信息，不同部门的接收者群体组成末梢网络，每个末梢网络中都存在至少一个接收者，整个 PIM 域采用 SSM 模式。

(2) Host A 和 Host C 为两个末梢网络中的组播信息接收者。

(3) Switch D 通过 Vlan-interface 300 接口与组播源(Source)所在网络连接。

(4) Switch A 通过 Vlan-interface 100 接口连接末梢网络 N1，通过 Vlan-interface 101 接口和 Vlan-interface 102 接口分别连接 Switch D 和 Switch E。

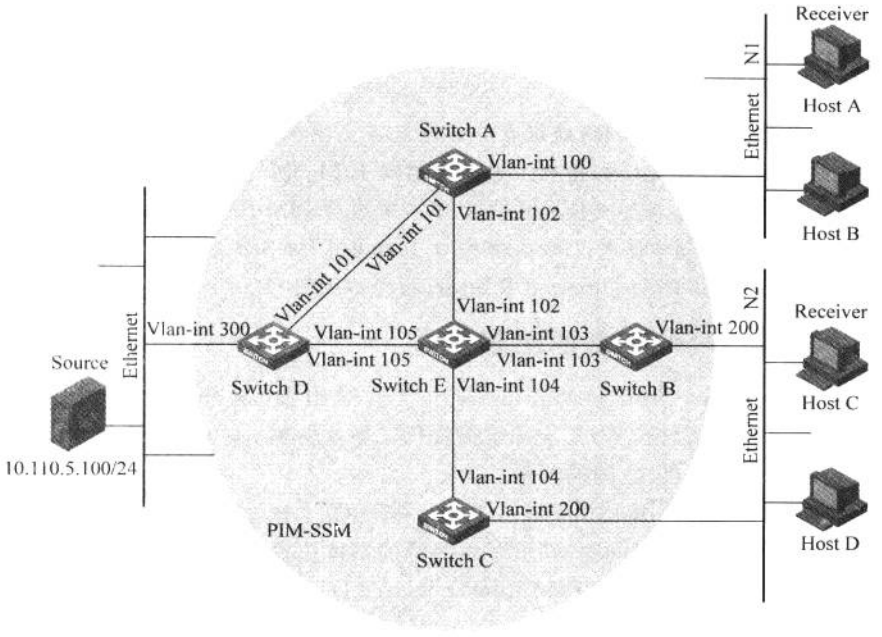
(5) Switch B 和 Switch C 通过各自的 Vlan-interface 200 接口连接末梢网络 N2，分别通过 Vlan-interface 103 和 Vlan-interface 104 接口连接 Switch E。

(6) SSM 组播组的范围是 232.1.1.0/24。

(7) Switch A 与末梢网络 N1 之间运行 IGMPv3；Switch B 和 Switch C 与末梢网络 N2 之间也运行 IGMPv3。

4. 配置过程和解释

(1) 配置 IP 地址和单播路由协议。按照图 10-6 配置各接口的 IP 地址和子网掩码，具体配置过程略。



设　备	接　口	IP 地址	设　备	接　口	IP 地址
Switch A	Vlan-int 100	10.110.1.1/24	Switch D	Vlan-int 300	10.110.5.1/24
	Vlan-int 101	192.168.1.1/24		Vlan-int 101	192.168.1.2/24
	Vlan-int 102	192.168.9.1/24		Vlan-int 105	192.168.4.2/24
Switch B	Vlan-int 200	10.110.2.1/24	Switch E	Vlan-int 104	192.168.3.2/24
	Vlan-int 103	192.168.2.1/24		Vlan-int 103	192.168.2.2/24
Switch C	Vlan-int 200	10.110.2.2/24		Vlan-int 102	192.168.9.2/24
	Vlan-int 104	192.168.3.1/24		Vlan-int 105	192.168.4.1/24

图 10-6　PIM-SSM 典型配置组网图

配置 PIM-SM 域内的各交换机之间采用 OSPF 协议进行互连，确保 PIM-SM 域内部网络层互通，并且各交换机之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IP 组播路由，并在各接口上使能 PIM-SM 和 IGMP。在 Switch A 上使能 IP 组播路由，在各接口上使能 PIM-SM，并在 Switch A 连接末梢网络的接口Vlan-interface 100上使能 IGMPv3。

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] igmp version 3
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
```

```
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim sm
[SwitchA-Vlan-interface102] quit
```

Switch B 和 Switch C 的配置与 Switch A 相似，Switch D 和 Switch E 除了不需要在相应接口上使能 IGMP 外，其他的配置也与 Switch A 相似，配置过程略。

(3) 配置 SSM 组播组的地址范围。在 Switch A 上配置 SSM 组播组地址范围为 232.1.1.0/24。

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 232.1.1.0 0.0.0.255
[SwitchA-acl-basic-2000] quit
[SwitchA] pim
[SwitchA-pim] ssm-policy 2000
[SwitchA-pim] quit
```

Switch B、Switch C、Switch D 和 Switch E 的配置与 Switch A 相似，配置过程略。

(4) 检验配置效果。

① 通过使用 display pim interface 命令可以查看交换机接口上 PIM 的配置和运行情况。例如，查看 Switch A 上 PIM 的配置信息。

```
[SwitchA] display pim interface
Interface          NbrCnt  HelloInt  DR-Pri  DR-Address
Vlan100            0       30        1       10.110.1.1   (local)
Vlan101            1       30        1       192.168.1.2
Vlan102            1       30        1       192.168.9.2
```

② 假如 Host A 需要接收指定组播源 S(10.110.5.100/24)发往组播组 G(232.1.1.1)的信息，Switch A 会向组播源方向构造 SPT，SPT 路径中的交换机(Switch A 和 Switch D)上生成(S,G)表项，而 SPT 路径之外的交换机(Switch E)上没有组播路由项，通过使用 display pim routing-table 命令可以查看交换机的 PIM 路由表信息。例如：

a. 查看 Switch A 上的 PIM 路由表信息。

```
[SwitchA] display pim routing-table
    Total 0 (*, G) entry; 1 (S, G) entry
 (10.110.5.100, 232.1.1.1)
      Protocol: pim-ssm, Flag:
      UpTime: 00:13:25
      Upstream interface: Vlan-interface 101
          Upstream neighbor: 192.168.1.2
          RPF prime neighbor: 192.168.1.2
      Downstream interface(s) information:
        Total number of downstreams: 1
            1: : Vlan-interface 100
                  Protocol: igmp, UpTime: 00:13:25, Expires: -
```

Switch B 和 Switch C 上的显示信息与 Switch A 类似。

b. 查看 Switch D 上的 PIM 路由表信息。

```
[SwitchD] display pim routing-table
Total 0 (*, G) entry; 1 (S, G) entry
  (10.110.5.100, 232.1.1.1)
      Protocol: pim-ssm, Flag:LOC
      UpTime: 00:12:05
      Upstream interface: Vlan-interface 300
          Upstream neighbor: NULL
          RPF prime neighbor: NULL
      Downstream interface(s) information:
        Total number of downstreams: 1
            1: : Vlan-interface 105
                  Protocol: pim-ssm, UpTime: 00:12:05, Expires: 00:03:25
```

提示：在部署 PIM-SM 域时，建议在非边界三层交换机的所有接口上启动 PIM-SM。在连接组播源的三层交换机接口上也必须启动 PIM-SM。

在连接组播接收者的三层交换机接口上可不用启动 PIM-SM。但如果存在多台三层交换机同时连接组播接收者，则建议都在该接口上启动 PIM-SM 用以选定唯一的组播转发器。

PIM-SSM 模型需要 IGMPv3 的支持，因此应确保连接有接收者的 PIM 路由器上使能了 IGMPv3。

如果某组播组属于 SSM 组播组范围，但该组成员使用 IGMPv1 或 IGMPv2 发送加入报文，则设备不会触发(*,G)加入报文。

应确保域内所有路由器上配置的 SSM 组播组地址范围都一致；否则，组播信息将无法通过 SSM 模型进行传输。

IANA(Internet Assigned Numbers Authority，互联网数字分配机构)分配的 SSM 组播组地址范围：IPv4 为 232/8；IPv6 为 FF3x::/96。

第11章

ACL与QoS配置指导

11.1 IPv4 ACL 典型配置指导

11.1.1 基本 IPv4 ACL 典型配置指导

基本 IPv4 ACL 只根据源 IP 地址信息制定匹配规则，对报文进行相应的分析处理，基本 IPv4 ACL 的序号取值范围为 2000～2999。

1. 背景

M 公司的部分工作人员上班时间利用公司网络访问外网，公司要求 IT 维护部门在网络设备上配置访问控制列表，实现上班时间只能访问公司内部网段，下班时间可以任意访问外部网络。

2. 组网图

图 11-1 所示为基本 IPv4 ACL 典型配置组网图。

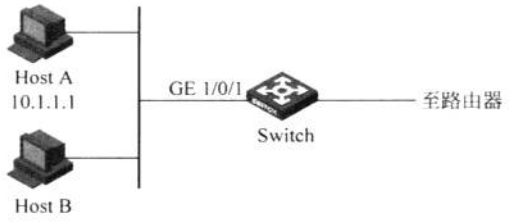


图 11-1 基本 IPv4 ACL 典型配置组网图

3. 配置需求

如图 11-1 所示，Host A 和 Host B 通过端口 GigabitEthernet 1/0/1 接入交换机，Host A 的 IP 地址为 10.1.1.1。要求配置基本 IPv4 ACL，实现在每天 8:00～18:00 的时间段内，只允许 Host A 发出的 IP 报文通过，拒绝其他的 IP 报文通过。

4. 配置过程和解释

(1) 定义周期时间段 trname，时间范围为每天的 8:00～18:00。

```
<Switch> system-view
[Switch] time-range trname 8:00 to 18:00 daily
```

(2) 定义基本 IPv4 ACL 2000，配置源 IP 地址为 10.1.1.1 的访问规则。

```
[Switch] acl number 2000
```

```
[Switch-acl-basic-2000] rule permit source 10.1.1.1 0 time-range trname
[Switch-acl-basic-2000] quit
```

(3) 定义基本 IPv4 ACL 2001,配置源 IP 地址为任意地址的访问规则。

```
[Switch] acl number 2001
[Switch-acl-basic-2001] rule deny time-range trname
[Switch-acl-basic-2001] quit
```

(4) 定义类 classifier_hostA,对匹配基本 IPv4 ACL 2000 的报文进行分类。

```
[Switch] traffic classifier classifier_hostA
[Switch-classifier-classifier_hostA] if-match acl 2000
[Switch-classifier-classifier_hostA] quit
```

(5) 定义流行为 behavior_hostA,动作为允许报文通过。

```
[Switch] traffic behavior behavior_hostA
[Switch-behavior-behavior_hostA] filter permit
[Switch-behavior-behavior_hostA] quit
```

(6) 定义类 classifier_hostB,对匹配基本 IPv4 ACL 2001 的报文进行分类。

```
[Switch] traffic classifier classifier_hostB
[Switch-classifier-classifier_hostB] if-match acl 2001
[Switch-classifier-classifier_hostB] quit
```

(7) 定义流行为 behavior_hostB,动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_hostB
[Switch-behavior-behavior_hostB] filter deny
[Switch-behavior-behavior_hostB] quit
```

(8) 定义策略 policy_host,为类 classifier_hostA 指定流行为 behavior_hostA,为类 classifier_hostB 指定流行为 behavior_hostB。其中 filter permit 和 filter deny 动作必须配置到不同的 classifier-behavior 中,并且在配置过程中需要注意两者的先后顺序,以保证应用策略后实际的运行结果与用户的配置意图一致。

```
[Switch] qos policy policy_host
[Switch-qospolicy-policy_host] classifier classifier_hostA behavior behavior_hostA
[Switch-qospolicy-policy_host] classifier classifier_hostB behavior behavior_hostB
[Switch-qospolicy-policy_host] quit
```

(9) 将策略 policy_host 应用到端口 GigabitEthernet 1/0/1。

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy_host inbound
```

提示:新创建或修改后的规则不能和已经存在的规则相同,否则会导致创建或修改不成功,系统会提示该规则已经存在。

当基本 IPv4 ACL 被 QoS 策略引用对报文进行流分类时,ACL 规则中定义的动作(deny 或 permit)不起作用,交换机对匹配此 ACL 的报文采取的动作由 QoS 策略中流行为

定义的动作决定。

交换机硬件转发数据流仅有“先下发先生效”一种匹配规则，软件处理报文有 Auto 和 Config 两种规则。交换机的 ACL 为硬件实现，支持的条目数和功能性与本交换机使用的硬件芯片有关，具体需要查看各产品典型配置手册。

11.1.2 高级 IPv4 ACL 典型配置指导

高级 IPv4 ACL 可以使用报文的源 IP 地址信息、目的 IP 地址信息、IP 承载的协议类型、协议的特性(例如，TCP 或 UDP 的源端口、目的端口，ICMP 协议的消息类型、消息码等)等信息来制定匹配规则。用户可以利用高级 IPv4 ACL 定义比基本 IPv4 ACL 更准确、更丰富、更灵活的匹配规则。

高级 IPv4 ACL 的序号取值范围为 3000～3999。

1. 背景

M 公司通过交换机实现各部门之间的互连。部分研发和市场部门员工在上班时间访问工资查询服务器，公司要求 IT 维护部门配置高级 IPv4 ACL，禁止研发部门和市场部门在上班时间(8:00～18:00)访问工资查询服务器，而总裁办公室不受限制，可以随时访问。

2. 组网图

图 11-2 所示为高级 IPv4 ACL 典型配置组网图。

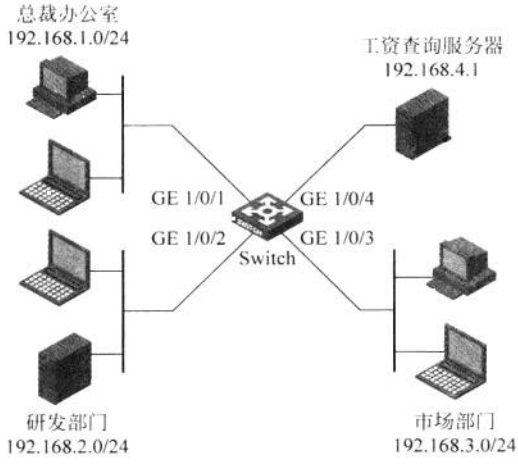


图 11-2 高级 IPv4 ACL 典型配置组网图

3. 配置需求

如图 11-2 所示，要求网络管理员配置高级 IPv4 ACL，禁止 192.168.2.0/24 和 192.168.3.0/24 在 8:00～18:00 访问 192.168.4.1，其他网段不受影响，可以随时访问。

4. 配置过程和解释

(1) 定义工作时间段。定义 8:00～18:00 的周期时间段。

```
<Switch> system-view
[Switch] time-range trname 8:00 to 18:00 working-day
```

(2) 定义到工资查询服务器的访问规则。

① 定义研发部门到工资查询服务器的访问规则。

```
[Switch] acl number 3000
[Switch-acl-adv-3000] rule deny ip source 192.168.2.0 0.0.0.255 destination 192.168.4.1 0 time-range trname
[Switch-acl-adv-3000] quit
```

② 定义市场部门到工资查询服务器的访问规则。

```
[Switch] acl number 3001
[Switch-acl-adv-3001] rule deny ip source 192.168.3.0 0.0.0.255 destination 192.168.4.1 0 time-range trname
[Switch-acl-adv-3001] quit
```

(3) 应用访问规则。

① 定义类 classifier_rd,对匹配高级 IPv4 ACL 3000 的报文进行分类。

```
[Switch] traffic classifier classifier_rd
[Switch-classifier-classifier_rd] if-match acl 3000
[Switch-classifier-classifier_rd] quit
```

② 定义流行为 behavior_rd,动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_rd
[Switch-behavior-behavior_rd] filter deny
[Switch-behavior-behavior_rd] quit
```

③ 定义类 classifier_market,对匹配高级 IPv4 ACL 3001 的报文进行分类。

```
[Switch] traffic classifier classifier_market
[Switch-classifier-classifier_market] if-match acl 3001
[Switch-classifier-classifier_market] quit
```

④ 定义流行为 behavior_market,动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_market
[Switch-behavior-behavior_market] filter deny
[Switch-behavior-behavior_market] quit
```

⑤ 定义策略 policy_rd,为类 classifier_rd 指定流行为 behavior_rd。

```
[Switch] qos policy policy_rd
[Switch-qospolicy-policy_rd] classifier classifier_rd behavior behavior_rd
[Switch-qospolicy-policy_rd] quit
```

⑥ 定义策略 policy_market,为类 classifier_market 指定流行为 behavior_market。

```
[Switch] qos policy policy_market
[Switch-qospolicy-policy_market] classifier classifier_market behavior behavior_market
[Switch-qospolicy-policy_market] quit
```

⑦ 将策略 policy_rd 应用到端口 GigabitEthernet 1/0/2。

```
[Switch] interface GigabitEthernet 1/0/2
```

```
[Switch-GigabitEthernet1/0/2] qos apply policy policy_rd inbound
[Switch-GigabitEthernet1/0/2] quit
```

⑧ 将策略 policy_market 应用到端口 GigabitEthernet 1/0/3。

```
[Switch] interface GigabitEthernet 1/0/3
[Switch-GigabitEthernet1/0/3] qos apply policy policy_market inbound
```

提示：新创建或修改后的规则不能和已经存在的规则相同，否则会导致创建或修改不成功，系统会提示该规则已经存在。

当高级 IPv4 ACL 被 QoS 策略引用对报文进行流分类时，ACL 规则中定义的动作(deny 或 permit)不起作用，交换机对匹配此 ACL 的报文采取的动作由 QoS 策略中流行为定义的动作决定。

交换机硬件转发数据流仅有"先下发先生效"一种匹配规则，软件处理报文有 Auto 和 Config 两种规则。交换机的 ACL 为硬件实现，支持的条目数和功能性与本交换机使用的硬件芯片有关，具体需要查看各产品典型配置手册。

11.1.3 二层 ACL 典型配置指导

二层 ACL 根据报文的源 MAC 地址、目的 MAC 地址、802.1p 优先级、二层协议类型等二层信息制定匹配规则，对报文进行相应的分析处理，二层 ACL 的序号取值范围为 4000～4999。

1. 背景

M 公司企业网通过交换机实现各部门之间的互连。IT 维护部门发现有部分公司员工在上班时间访问公司内部的生活论坛服务器，所以在交换机上配置高级 IPv4 ACL，禁止所有部门在上班时间(8:00～18:00)访问生活论坛服务器。

2. 组网图

图 11-3 所示为二层 ACL 典型配置组网图。

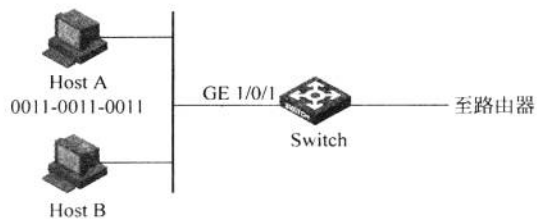


图 11-3 二层 ACL 典型配置组网图

3. 配置需求

如图 11-3 所示，Host A 和 Host B 通过端口 GigabitEthernet 1/0/1 接入交换机，Host A 的 MAC 地址为 0011-0011-0011。要求配置二层 ACL，实现在每天 8:00～18:00 的时间段内，对 Host A 发出的目的 MAC 为 0011-0011-0012 的报文进行过滤。

4. 配置过程和解释

(1) 定义周期时间段 trname，时间范围为每天的 8:00～18:00。

```
<Switch> system-view
```

```
[Switch] time-range trname 8:00 to 18:00 daily
```

(2) 定义二层 ACL 4000，配置源 MAC 地址为 0011-0011-0011、目的 MAC 地址为 0011-0011-0012 的报文的访问规则。

```
[Switch] acl number 4000
[Switch-acl-basic-4000] rule deny source-mac 0011-0011-0011 ffff-ffff-ffff dest-mac 0011-0011-0012
ffff-ffff-ffff time-range trname
[Switch-acl-basic-4000] quit
```

(3) 定义类 classifier_hostA，对匹配二层 ACL 4000 的报文进行分类。

```
[Switch] traffic classifier classifier_hostA
[Switch-classifier-classifier_hostA] if-match acl 4000
[Switch-classifier-classifier_hostA] quit
```

(4) 定义流行为 behavior_hostA，动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_hostA
[Switch-behavior-behavior_hostA] filter deny
[Switch-behavior-behavior_hostA] quit
```

(5) 定义策略 policy_hostA，为类 classifier_hostA 指定流行为 behavior_hostA。

```
[Switch] qos policy policy_hostA
[Switch-qospolicy-policy_hostA] classifier classifier_hostA behavior behavior_hostA
[Switch-qospolicy-policy_hostA] quit
```

(6) 将策略 policy_hostA 应用到端口 GigabitEthernet 1/0/1。

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy_hostA inbound
```

提示：新创建或修改后的规则不能和已经存在的规则相同，否则会导致创建或修改不成功，系统会提示该规则已经存在。

当高级 IPv4 ACL 被 QoS 策略引用对报文进行流分类时，ACL 规则中定义的动作(deny 或 permit)不起作用，交换机对匹配此 ACL 的报文采取的动作由 QoS 策略中流行为定义的动作决定。

交换机硬件转发数据流仅有“先下发先生效”一种匹配规则，软件处理报文有 Auto 和 Config 两种规则。交换机的 ACL 为硬件实现，支持的条目数和功能性与本交换机使用的硬件芯片有关，具体需要查看各产品配置手册。

11.1.4 用户自定义 ACL 和流模板典型配置指导

用户自定义 ACL 可以以报文的二层报文头、IP 报文头等为基准，指定从第几个字节开始与掩码进行“与”操作，将从报文提取出来的字符串和用户定义的字符串进行比较，找到匹配的报文，然后进行相应的处理。用户自定义 ACL 的序号取值范围为5000～5999。

流模板的主要功能是对硬件下发的 ACL 规则中所能包含的信息进行限制。在以太网端口下发的 ACL 规则中包含的信息必须是该端口下发流模板中定义信息的子集。例如，流模板定义了源 IP 地址、目的 IP 地址、源 TCP 端口、目的 TCP 端口等限制，只有在上述范

围内的 ACL 规则可以正确下发到硬件中，用于 QoS 等功能；否则 ACL 规则将不能下发到硬件中，导致 QoS 功能不能引用此 ACL 规则。

1. 背景

M 公司随着业务的发展，外来人员办公增多，公司内部网络有时会因为外来人员电脑存在 ARP 病毒，导致公司某部门网络被攻击而中断。为了避免这种情况，网络管理员在接入层交换机配置用户自定义 ACL，防止假冒网关的非法 ARP 报文通过。

2. 组网图

图 11-4 所示为用户自定义 ACL 和流模板典型配置组网图。

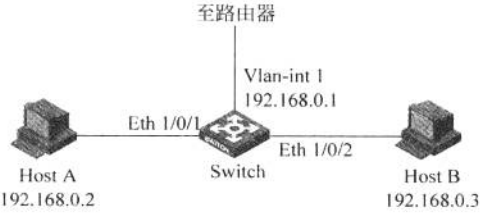


图 11-4 用户自定义 ACL 和流模板典型配置组网图

3. 配置需求

如图 11-4 所示，公司企业网通过交换机(以 S3610 为例)实现互连，网络环境描述如下：

(1) Host A 的 IP 地址为 192.168.0.2，通过端口 Ethernet 1/0/1 接入交换机；Host B 的 IP 地址为 192.168.0.3，通过端口 Ethernet 1/0/2 接入交换机。

(2) Host A 和 Host B 属于 VLAN 1，两者的网关都设置为 192.168.0.1(交换机 VLAN 1 接口的 IP 地址)，通过交换机访问 Internet。

配置用户自定义 ACL，对 Host A 发出的仿冒网关 IP 地址的 ARP 报文进行过滤。

4. 配置过程和解释

(1) 定义用户自定义 ACL 5000，配置源 IP 地址为 192.168.0.1 的 ARP 报文的访问规则。其中 L2 表示从报文的二层头开始计算，0806 为 ARP 协议号，ffff 为掩码，12 为以太网报文中协议类型字段的偏移量，start 表示从报文的报文头开始计算，c0a80001 为 192.168.0.1 的十六进制形式，28 为 ARP 报文中源 IP 地址字段的偏移量。

```
<Switch> system-view
[Switch] acl number 5000
[Switch-acl-user-5000] rule deny L2 0806 ffff 12 start c0a80001 ffffffff 28
```

(2) 定义扩展型流模板 ftemplate_hostA。

```
[Switch] flow-template ftemplate_hostA extend L2 12 2 start 28 4
```

(3) 在端口 Ethernet 1/0/1 上应用流模板 ftemplate_hostA。

```
[Switch] interface Ethernet 1/0/1
[Switch-Ethernet1/0/1] flow-template ftemplate_hostA
[Switch-Ethernet1/0/1] quit
```

(4) 定义类 classifier_hostA，对匹配用户自定义 ACL 5000 的报文进行分类。

```
[Switch] traffic classifier classifier_hostA
```

```
[Switch-classifier-classifier_hostA] if-match acl 5000
[Switch-classifier-classifier_hostA] quit
```

(5) 定义流行为 behavior_hostA，动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_hostA
[Switch-behavior-behavior_hostA] filter deny
[Switch-behavior-behavior_hostA] quit
```

(6) 定义策略 policy_hostA，为类 classifier_hostA 指定流行为 behavior_hostA。

```
[Switch] qos policy policy_hostA
[Switch-qospolicy-policy_hostA] classifier classifier_hostA behavior behavior_hostA
[Switch-qospolicy-policy_hostA] quit
```

(7) 将策略 policy_hostA 应用到端口 Ethernet 1/0/1。

```
[Switch] interface Ethernet 1/0/1
[Switch-Ethernet1/0/1] qos apply policy policy_hostA inbound
```

提示：和其他类型的 IPv4 ACL 不同，用户自定义 ACL 中包含的规则不支持修改，只能进行覆盖性配置。用户自定义 ACL 需要和扩展型用户自定义流模板配合使用，用户自定义 ACL 中设置的偏移范围必须包含在扩展型用户自定义流模板中设置的偏移范围之内，否则用户自定义 ACL 不能成功应用。

11.2 IPv6 ACL 典型配置指导

11.2.1 基本 IPv6 ACL 典型配置指导

基本 IPv6 ACL 只根据源 IPv6 地址信息制定匹配规则，对报文进行相应的分析处理。基本 IPv6 ACL 的序号取值范围为 2000～2999。

1. 背景

M 公司开通了 IPv6 业务，公司要求 IT 维护部门在网络设备上配置访问控制列表，实现上班时间只能访问公司内部 IPv6 网段，下班时间可以访问任意 IPv6 外部网络。

2. 组网图

图 11-5 所示为基本 IPv6 ACL 典型配置组网图。

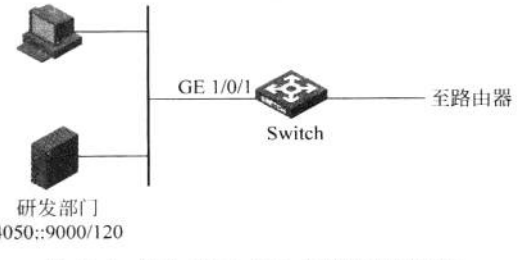


图 11-5 基本 IPv6 ACL 典型配置组网图

3. 配置需求

如图 11-5 所示，公司企业网通过交换机实现各部门之间的互连，要求配置基本 IPv6 ACL，禁止 4050::9000/120 访问网络。

4. 配置过程和解释

(1) 定义基本 IPv6 ACL 2000，配置访问规则。

```
<Switch> system-view
[Switch] acl ipv6 number 2000
[Switch-acl6-basic-2000] rule deny source 4050::9000/120
[Switch-acl6-basic-2000] quit
```

(2) 定义类 classifier_rd，对匹配 IPv6 ACL 2000 的报文进行分类。

```
[Switch] traffic classifier classifier_rd
[Switch-classifier-classifier_rd] if-match acl ipv6 2000
[Switch-classifier-classifier_rd] quit
```

(3) 定义流行为 behavior_rd，动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_rd
[Switch-behavior-behavior_rd] filter deny
[Switch-behavior-behavior_rd] quit
```

(4) 定义策略 policy_rd，为类 classifier_rd 指定流行为 behavior_rd。

```
[Switch] qos policy policy_rd
[Switch-qospolicy-policy_rd] classifier classifier_rd behavior behavior_rd
[Switch-qospolicy-policy_rd] quit
```

(5) 将策略 policy_rd 应用到端口 GigabitEthernet 1/0/1。

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy_rd inbound
```

提示：新创建或修改后的规则不能和已经存在的规则相同，否则会导致创建或修改不成功，系统会提示该规则已经存在。

当高级 IPv6 ACL 被 QoS 策略引用对报文进行流分类时，ACL 规则中定义的动作(deny 或 permit)不起作用，交换机对匹配此 ACL 的报文采取的动作由 QoS 策略中流行为定义的动作决定。

交换机硬件转发数据流仅有“先下发先生效”一种匹配规则，软件处理报文有 Auto 和 Config 两种规则。交换机的 ACL 为硬件实现，支持的条目数和功能性与本交换机使用的硬件芯片有关，具体需要查看各产品典型配置手册。

11.2.2 高级 IPv6 ACL 典型配置指导

高级 IPv6 ACL 可以使用报文的源 IPv6 地址信息、目的 IPv6 地址信息、IPv6 承载的协议类型、协议的特性(例如，TCP 或 UDP 的源端口、目的端口，ICMP 协议的消息类型、消息码等)等信息来制定匹配规则。用户可以利用高级 IPv6 ACL 定义比基本 IPv6 ACL 更准确、更丰富、更灵活的规则。高级 IPv6 ACL 的序号取值范围为 3000～3999。

1. 背景

M公司开通了通过IPv6查询工资服务器的业务，部分研发部门和市场部门员工上班时间访问IPv6工资服务器。公司要求网络管理员配置高级IPv6 ACL，禁止研发部门和市场部门在上班时间(8:00～18:00)访问IPv6工资查询服务器。

2. 组网图

图11-6所示为高级IPv6 ACL典型配置组网图。

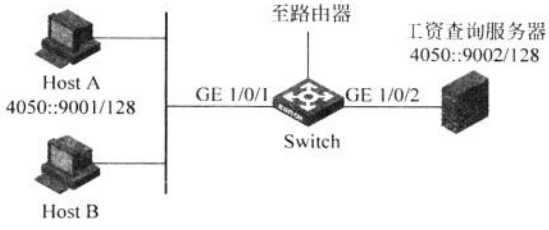


图11-6 高级IPv6 ACL典型配置组网图

3. 配置需求

如图11-6所示，公司企业网通过交换机实现各部门之间的互连。Host A和Host B通过端口GigabitEthernet 1/0/1接入交换机，Host A的IPv6地址为4050::9001，工资查询服务器的IPv6地址为4050::9002。要求配置高级IPv6 ACL，禁止Host A访问工资查询服务器。

4. 配置过程和解释

(1) 定义高级IPv6 ACL 3000，配置Host A的访问规则。

```
<Switch> system-view
[Switch] acl ipv6 number 3000
[Switch-acl6-adv-3000] rule deny ipv6 source 4050::9001 128 destination 4050::9002 128
[Switch-acl6-adv-3000] quit
```

(2) 定义类classifier_hostA，对匹配IPv6 ACL 3000的报文进行分类。

```
[Switch] traffic classifier classifier_hostA
[Switch-classifier-classifier_hostA] if-match acl ipv6 3000
[Switch-classifier-classifier_hostA] quit
```

(3) 定义流行为behavior_hostA，动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_hostA
[Switch-behavior-behavior_hostA] filter deny
[Switch-behavior-behavior_hostA] quit
```

(4) 定义策略policy_hostA，为类classifier_hostA指定流行为behavior_hostA。

```
[Switch] qos policy policy_hostA
[Switch-qospolicy-policy_hostA] classifier classifier_hostA behavior behavior_hostA
[Switch-qospolicy-policy_hostA] quit
```

(5) 将策略policy_hostA应用到端口GigabitEthernet 1/0/1。

```
[Switch] interface GigabitEthernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] qos apply policy policy_hostA inbound
```

提示：新创建或修改后的规则不能和已经存在的规则相同，否则会导致创建或修改不成功，系统会提示该规则已经存在。

当高级 IPv6 ACL 被 QoS 策略引用对报文进行流分类时，ACL 规则中定义的动作(deny 或 permit)不起作用，交换机对匹配此 ACL 的报文采取的动作由 QoS 策略中流行为定义的动作决定。

交换机硬件转发数据流仅有“先下发先生效”一种匹配规则，软件处理报文有 Auto 和 Config 两种规则。

11.3 报文过滤典型配置指导

通过将配置好的不同类型的 ACL 规则应用到指定端口/VLAN 接口的入或出方向上，可以对该端口/VLAN 接口收到或发出的相应类型报文(包括 IPv4 报文和 IPv6 报文)进行过滤。

1. 背景

M 公司的财务服务器为财务部门专用服务器，上班时间(8:00～18:00)只允许财务部门人员访问，禁止其他部门用户工作时间访问，非工作时间其他部门员工可以正常访问服务器。

2. 组网图

图 11-7 所示为应用 ACL 对报文过滤组网图。

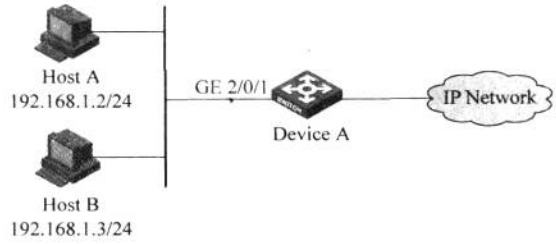


图 11-7 应用 ACL 对报文过滤组网图

3. 配置需求

如图 11-7 所示，要求通过在 Device A 的端口 GigabitEthernet 2/0/1 上配置 IPv4 报文过滤功能，实现在每天的 8:00～18:00 期间只允许来自 Host A 的报文通过。

4. 配置过程和解释

(1) 创建名为 study 的时间段，其时间范围为每天的 8:00～18:00。

```
<DeviceA> system-view
[DeviceA] time-range study 8:00 to 18:00 daily
```

(2) 创建 IPv4 基本 ACL 2009，并定义如下规则：在名为 study 的时间段内只允许来自 Host A(192.168.1.2)的报文通过，禁止来自其他 IP 地址的报文通过。

```
[DeviceA] acl number 2009
```

```
[DeviceA-acl-basic-2009] rule permit source 192.168.1.2 0 time-range study
[DeviceA-acl-basic-2009] rule deny source any time-range study
[DeviceA-acl-basic-2009] quit
```

(3) 应用 IPv4 基本 ACL 2009 对端口 GigabitEthernet 2/0/1 收到的 IPv4 报文进行过滤。

```
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] packet-filter 2009 inbound
```

11.4 QoS 典型配置指导

11.4.1 端口限速和流量监管典型配置指导

流量监管(Traffic Policing,TP)就是对流量进行控制,通过监督进入网络的流量速率,对超出部分的流量进行"惩罚",使进入的流量被限制在一个合理的范围之内,以保护网络资源和运营商的利益。

1. 背景

M 公司的 Internet 出口带宽为 2Mbps,近期接到员工反馈访问外网速度比较慢,IT 管理员检查后发现公司部分交换机连接的主机占用了大量的带宽,因此网络管理员需要配置端口限速来限制这些主机的访问速率,使网络访问 Internet 正常。

2. 组网图

图 11-8 所示为端口限速和流量监管典型配置组网图。

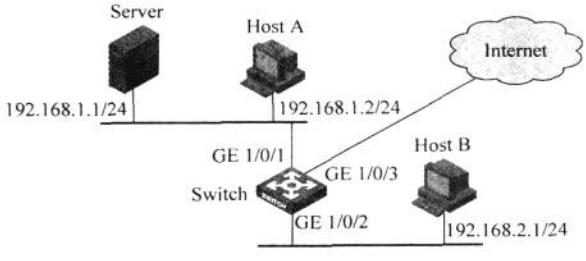


图 11-8 端口限速和流量监管典型配置组网图

3. 配置需求

如图 11-8 所示,公司企业网通过交换机实现互连。网络环境描述如下:

(1) Host A 的 IP 地址为 192.168.1.2,Server 的 IP 地址为 192.168.1.1,两者通过端口 GigabitEthernet 1/0/1 接入交换机。

(2) Host B 的 IP 地址为 192.168.2.1,通过端口 GigabitEthernet 1/0/2 接入交换机。

配置端口限速和流量监管,实现如下需求。

① 限制 Switch 向 Internet 发送的流量为 640Kbps,丢弃超出限制的报文。

② 限制 Host A 向外发出的流量为 320Kbps,丢弃超出限制的报文。

③ 限制 Host B 与 Server 之间的流量为 64Kbps,丢弃超出限制的报文。

4. 配置过程和解释

(1) 针对 Switch 配置端口限速。在端口 GigabitEthernet 1/0/3 上配置端口限速,限制端口发送报文的速率为 640Kbps。

```
<Switch> system-view
[Switch] interface GigabitEthernet 1/0/3
[Switch-GigabitEthernet1/0/3] qos lr outbound cir 640
[Switch-GigabitEthernet1/0/3] quit
```

(2) 针对 Host A 配置流量监管。

① 定义基本 ACL 2000,对源 IP 地址为 192.168.1.2 的报文进行分类。

```
[Switch] acl number 2000
[Switch-acl-basic-2000] rule permit source 192.168.1.2 0
[Switch-acl-basic-2000] quit
```

② 定义类 classifier_hostA,匹配基本 ACL 2000。

```
[Switch] traffic classifier classifier_hostA
[Switch-classifier-classifier_hostA] if-match acl 2000
[Switch-classifier-classifier_hostA] quit
```

③ 定义流行为 behavior_hostA,动作为限制报文的流量为 320Kbps。

```
[Switch] traffic behavior behavior_hostA
[Switch-behavior-behavior_hostA] car cir 320
[Switch-behavior-behavior_hostA] quit
```

④ 定义策略 policy_hostA,为类 classifier_hostA 指定流行为 behavior_hostA。

```
[Switch] qos policy policy_hostA
[Switch-qospolicy-policy_hostA] classifier classifier_hostA behavior behavior_hostA
[Switch-qospolicy-policy_hostA] quit
```

⑤ 将策略 policy_hostA 应用到端口 GigabitEthernet 1/0/1 上。

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy_hostA inbound
[Switch-GigabitEthernet1/0/1] quit
```

(3) 针对 Host B 和 Server 配置流量监管。

① 定义基本 ACL 3001,对源 IP 地址为 192.168.2.1、目的地址为 192.168.1.1 的报文进行分类。

```
[Switch] acl number 3001
[Switch-acl-adv-3001] rule permit ip source 192.168.2.1 0 destination 192.168.1.1 0
[Switch-acl-adv-3001] quit
```

② 定义基本 ACL 3002,对源 IP 地址为 192.168.1.1、目的地址为 192.168.2.1 的报文进行分类。

```
[Switch] acl number 3002
[Switch-acl-adv-3002] rule permit ip source 192.168.1.1 0 destination 192.168.2.1 0
```

```
[Switch-acl-adv-3002] quit
```

③ 定义类 classifier_hostB，匹配基本 ACL 3001。

```
[Switch] traffic classifier classifier_hostB
[Switch-classifier-classifier_hostB] if-match acl 3001
[Switch-classifier-classifier_hostB] quit
```

④ 定义类 classifier_Server，匹配基本 ACL 3002。

```
[Switch] traffic classifier classifier_Server
[Switch-classifier-classifier_Server] if-match acl 3002
[Switch-classifier-classifier_Server] quit
```

⑤ 定义流行为 behavior_hostB，动作为限制报文的流量为 64Kbps。

```
[Switch] traffic behavior behavior_hostB
[Switch-behavior-behavior_hostB] car cir 64
[Switch-behavior-behavior_hostB] quit
```

⑥ 定义流行为 behavior_Server，动作为限制报文的流量为 64Kbps。

```
[Switch] traffic behavior behavior_Server
[Switch-behavior-behavior_Server] car cir 64
[Switch-behavior-behavior_Server] quit
```

⑦ 定义策略 policy_hostB，为类 classifier_hostB 指定流行为 behavior_hostB。

```
[Switch] qos policy policy_hostB
[Switch-qospolicy-policy_hostB] classifier classifier_hostB behavior behavior_hostB
[Switch-qospolicy-policy_hostB] quit
```

⑧ 定义策略 policy_Server，为类 classifier_Server 指定流行为 behavior_Server。

```
[Switch] qos policy policy_Server
[Switch-qospolicy-policy_Server] classifier classifier_Server behavior behavior_Server
[Switch-qospolicy-policy_Server] quit
```

⑨ 将策略 policy_hostB 和 policy_Server 分别应用到端口 GigabitEthernet 1/0/2 的入方向和出方向上。

```
[Switch] interface GigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] qos apply policy policy_hostB inbound
[Switch-GigabitEthernet1/0/2] qos apply policy policy_Server outbound
```

提示：一个策略可以应用到多个端口上，支持在双向(inbound/outbound)下发策略。

一个策略可以物理端口、VLAN、全局下发。

配置端口限速时，要求 CBS 大小至少为 6.25×Cir，否则可能会造成限速不准确。

交换机产品 QoS 和具体产品有关，详细信息可查阅各个产品操作手册。

11.4.2 优先级重标记和队列调度典型配置指导

报文在进入设备以后，设备会根据自身情况和相应规则分配或修改报文的各种优先级

的值，为队列调度和拥塞控制服务。优先级重标记功能将报文的优先级或者标志位进行设置，通过手动重新定义流量优先级，可以全面、有效地控制报文的转发调度能力。

1. 背景

M公司有数据查询、邮件处理、文件传输3种业务。因公司业务的重要性不同，业务部门对IT维护部门提出需求，要求数据查询的业务优先处理，其次为邮件处理，最后是文件传输。因此，网络管理员需要在交换机上进行优先级标记和队列调度的配置，保证数据查询业务高优先级转发，其次是邮件处理业务，最后是文件传输业务。

2. 组网图

图11-9所示为优先级重标记和队列调度典型配置组网图。

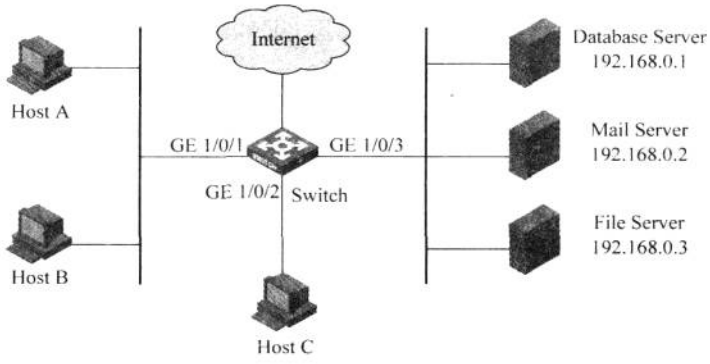


图11-9 优先级重标记和队列调度典型配置组网图

3. 配置需求

如图11-9所示，公司企业网通过交换机实现互连。网络环境描述如下：

(1) Host A和Host B通过端口GigabitEthernet 1/0/1接入交换机。

(2) Host C通过端口GigabitEthernet 1/0/2接入交换机。

(3) 数据库服务器、邮件服务器和文件服务器通过端口GigabitEthernet 1/0/3接入交换机。

配置优先级重标记和队列调度，实现如下需求。

(1) 当Host A和Host B访问服务器时，交换机优先处理Host A和Host B访问数据库服务器的报文，其次处理Host A和Host B访问邮件服务器的报文，最后处理Host A和Host B访问文件服务器的报文。

(2) 无论Host C访问Internet或访问服务器，交换机都优先处理Host C发出的报文。

4. 配置过程和解释

(1) 针对Host A和Host B的配置。

① 定义高级ACL 3000，对目的IP地址为192.168.0.1的报文进行分类。

```
<Switch> system-view
[Switch] acl number 3000
[Switch-acl-adv-3000] rule permit ip destination 192.168.0.1 0
[Switch-acl-adv-3000] quit
```

② 定义高级 ACL 3001，对目的 IP 地址为 192.168.0.2 的报文进行分类。

```
<Switch> system-view
[Switch] acl number 3001
[Switch-acl-adv-3001] rule permit ip destination 192.168.0.2 0
[Switch-acl-adv-3001] quit
```

③ 定义高级 ACL 3002，对目的 IP 地址为 192.168.0.3 的报文进行分类。

```
<Switch> system-view
[Switch] acl number 3002
[Switch-acl-adv-3002] rule permit ip destination 192.168.0.3 0
[Switch-acl-adv-3002] quit
```

④ 定义类 classifier_dbserver，匹配高级 ACL 3000。

```
[Switch] traffic classifier classifier_dbserver
[Switch-classifier-classifier_dbserver] if-match acl 3000
[Switch-classifier-classifier_dbserver] quit
```

⑤ 定义类 classifier_mserver，匹配高级 ACL 3001。

```
[Switch] traffic classifier classifier_mserver
[Switch-classifier-classifier_mserver] if-match acl 3001
[Switch-classifier-classifier_mserver] quit
```

⑥ 定义类 classifier_fserver，匹配高级 ACL 3002。

```
[Switch] traffic classifier classifier_fserver
[Switch-classifier-classifier_fserver] if-match acl 3002
[Switch-classifier-classifier_fserver] quit
```

⑦ 定义流行为 behavior_dbserver，动作为重标记报文的本地优先级为 4。

```
[Switch] traffic behavior behavior_dbserver
[Switch-behavior-behavior_dbserver] remark local-precedence 4
[Switch-behavior-behavior_dbserver] quit
```

⑧ 定义流行为 behavior_mserver，动作为重标记报文的本地优先级为 3。

```
[Switch] traffic behavior behavior_mserver
[Switch-behavior-behavior_mserver] remark local-precedence 3
[Switch-behavior-behavior_mserver] quit
```

⑨ 定义流行为 behavior_fserver，动作为重标记报文的本地优先级为 2。

```
[Switch] traffic behavior behavior_fserver
[Switch-behavior-behavior_fserver] remark local-precedence 2
[Switch-behavior-behavior_fserver] quit
```

⑩ 定义策略 policy_server，为类指定流行为。

```
[Switch] qos policy policy_server
[Switch-qospolicy-policy_server] classifier classifier_dbserver behavior behavior_dbserver
[Switch-qospolicy-policy_server] classifier classifier_mserver behavior behavior_mserver
[Switch-qospolicy-policy_server] classifier classifier_fserver behavior behavior_fserver
```

```
[Switch-qospolicy-policy_server] quit
```

⑪ 将策略 policy_server 应用到端口 GigabitEthernet 1/0/1 上。

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy_server inbound
[Switch-GigabitEthernet1/0/1] quit
```

⑫ 配置端口 GigabitEthernet 1/0/3 的队列调度方式为 SP(Strict-Priority,严格优先级)。

```
[Switch] interface GigabitEthernet 1/0/3
[Switch-GigabitEthernet1/0/3] qos sp
[Switch-GigabitEthernet1/0/3] quit
```

(2) 针对 Host C 的配置。配置端口 GigabitEthernet 1/0/2 的优先级信任模式为信任端口的优先级(默认情况下即为信任端口的优先级,用户无须配置),并且设置端口的优先级为 5。

```
[Switch] interface GigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] qos priority 5
```

11.4.3 优先级映射和队列调度典型配置指导

报文在进入设备以后,设备会根据自身情况和相应规则分配或修改报文的各种优先级的值,为队列调度和拥塞控制服务。优先级映射功能通过报文所携带的优先级字段来映射其他优先级字段值,就可以获得各种用以决定报文调度能力的优先级字段,从而可以全面、有效地控制报文的转发调度能力。

1. 背景

M 公司 IT 维护部门对数据查询、邮件处理、文件传输 3 种业务进行调整,网络管理员通过在交换机上进行优先级映射和队列调度的配置,使这 3 种不同的报文进入不同的优先级队列,将 3 种业务统一进行加权轮询调度。

2. 组网图

图 11-10 所示为优先级映射和队列调度典型配置组网图。

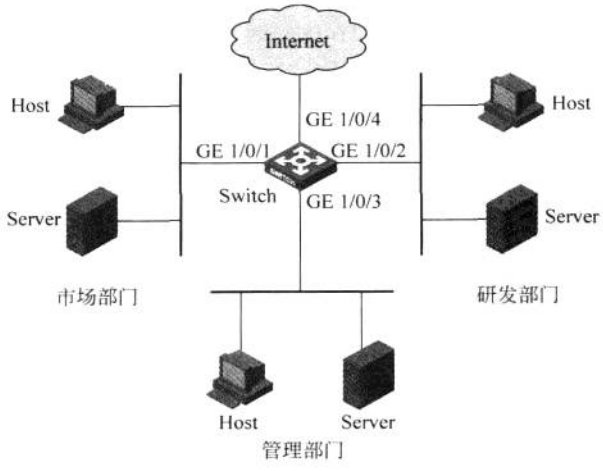


图 11-10 优先级映射和队列调度典型配置组网图

3. 配置需求

如图 11-10 所示，公司企业网通过交换机实现各部门之间的互连。网络环境描述为：市场部门、研发部门和管理部门内的设备发出的报文都不带有 802.1Q 标签头(VLAN Tag)。

要求配置优先级映射和队列调度，实现如下需求。

(1) 标记市场部门发出的报文的 802.1p 优先级为 3，通过优先级映射，将此类报文放入队列 4 中。

(2) 标记研发部门发出的报文的 802.1p 优先级为 4，通过优先级映射，将此类报文放入队列 3 中。

(3) 标记管理部门发出的报文的 802.1p 优先级为 5，通过优先级映射，将此类报文放入队列 6 中。

(4) 在端口 GigabitEthernet 1/0/4 上配置调度算法为 WRR，队列 3、队列 4 和队列 6 所占的权重分别为 5、10 和 15。

4. 配置过程和解释

(1) 配置端口的端口优先级。

① 配置端口 GigabitEthernet 1/0/1 的端口优先级为 3。

```
<Switch> system-view
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos priority 3
[Switch-GigabitEthernet1/0/1] quit
```

② 配置端口 GigabitEthernet 1/0/2 的端口优先级为 4。

```
[Switch] interface GigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] qos priority 4
[Switch-GigabitEthernet1/0/2] quit
```

③ 配置端口 GigabitEthernet 1/0/3 的端口优先级为 5。

```
[Switch] interface GigabitEthernet 1/0/3
[Switch-GigabitEthernet1/0/3] qos priority 5
[Switch-GigabitEthernet1/0/3] quit
```

(2) 配置优先级映射表。配置 802.1p 优先级到本地优先级映射表，将 802.1p 优先级 3、4、5 对应的本地优先级配置为 4、3、6。

```
[Switch] qos map-table dot1p-lp
[Switch-maptbl-dot1p-lp] import 3 export 4
[Switch-maptbl-dot1p-lp] import 4 export 3
[Switch-maptbl-dot1p-lp] import 5 export 6
[Switch-maptbl-dot1p-lp] quit
```

(3) 配置队列调度。配置端口 GigabitEthernet 1/0/4 的队列调度算法为 WRR，队列 3、队列 4 和队列 6 所占的权重分别为 5、10 和 15。

```
[Switch] interface GigabitEthernet 1/0/4
[Switch-GigabitEthernet1/0/4] qos wrr 3 group 1 weight 5
[Switch-GigabitEthernet1/0/4] qos wrr 4 group 1 weight 10
[Switch-GigabitEthernet1/0/4] qos wrr 6 group 1 weight 15
```

提示：对于不带有802.1Q标签头的报文，交换机将使用端口的优先级作为该端口接收的报文的本地优先级。

对于带有802.1Q标签头的报文，交换机提供两种优先级信任模式：信任报文的优先级（根据报文的802.1p优先级，查找802.1p优先级到本地优先级/丢弃优先级映射表，然后为报文标记本地优先级和丢弃优先级）和信任端口的优先级（使用接收端口的端口优先级作为本地优先级）。

802.1p优先级到本地优先级/丢弃优先级映射表和端口上的优先级信任模式相关联。配置了端口上的信任模式为信任报文的802.1p优先级后，这些映射表才能起作用。

DSCP优先级映射到本地优先级/丢弃优先级/802.1p优先级/DSCP优先级映射表和流行为中primap动作相关联。在流行为中配置了primap动作后，这些映射表才能起作用。

11.4.4 流镜像和重定向至端口典型配置指导

流镜像通过QoS策略实现，即使用流分类技术来定义需要被镜像的报文的匹配条件，再通过配置流行为将符合条件的报文镜像至指定的方向。

流镜像可以将数据镜像到以下两个方向。

（1）流镜像到端口，将符合要求的数据包复制一份，然后发送到目的端口。

（2）流镜像到CPU，是将符合要求的数据包复制一份，然后发送到CPU以供分析诊断，这里的CPU指的是配置了流镜像的端口所在单板上的CPU。

流量重定向到端口是指当收到需要由某个端口处理的报文时，可以通过此配置将报文重定向到此端口，只针对二层转发报文。

1. 背景

M公司近来访问数据库服务器的业务逐渐增多，IT管理部门研究后决定使用流量分析软件来分析访问数据库业务的流量分布情况，然后对非正常访问流量进行统一调度，网络管理员需要配置流镜像将数据库业务流镜像到流量分析软件进行分析。

另外，M公司配置了IPS（入侵防御）对数据服务器进行保护，网络管理员需要配置重定向将所有访问数据服务器的流量重定向至IPS，经IPS处理后再到达数据服务器。

2. 组网图

图11-11所示为流镜像和重定向至端口典型配置组网图。

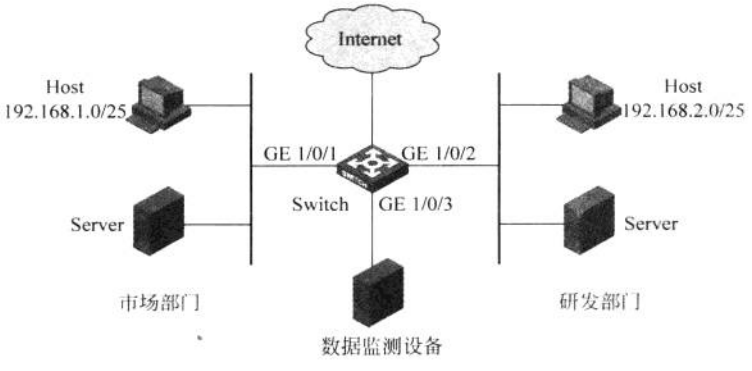


图11-11 流镜像和重定向至端口典型配置组网图

3. 配置需求

如图 11-11 所示，公司企业网通过交换机实现各部门之间的互连。网络环境描述如下：

(1) 市场部门通过端口 GigabitEthernet 1/0/1 接入交换机，其中 Host 的 IP 地址为 192.168.1.0/25，通过交换机访问 Internet。

(2) 研发部门通过端口 GigabitEthernet 1/0/2 接入交换机，其中 Host 的 IP 地址为 192.168.2.0/25，通过交换机访问 Internet。

(3) 数据监测设备通过端口 GigabitEthernet 1/0/3 接入交换机。

配置流镜像和重定向，实现如下需求。

(1) 在工作时间段(8:00～18:00)内，将市场部门内 Host 访问 Internet 的流量镜像到数据监测设备。

(2) 在工作时间段(8:00～18:00)内，将研发部门内 Host 访问 Internet 的流量重定向到数据监测设备。

网络管理员可以使用数据监测设备对各部门访问 Internet 的流量进行分析。

4. 配置过程和解释

(1) 定义工作时间段。定义 8:00～18:00 的周期时间段。

```
<Switch> system-view
[Switch] time-range trname 8:00 to 18:00 working-day
```

(2) 定义针对市场部门的策略。

① 定义基本 ACL 2000，对市场部门内的 Host 进行分类。

```
[Switch] acl number 2000
[Switch-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.127 time-range trname
[Switch-acl-basic-2000] quit
```

② 定义类 classifier_market，匹配基本 ACL 2000。

```
[Switch] traffic classifier classifier_market
[Switch-classifier-classifier_market] if-match acl 2000
[Switch-classifier-classifier_market] quit
```

③ 定义流行为 behavior_market，动作为流镜像至端口 GigabitEthernet 1/0/3。

```
[Switch] traffic behavior behavior_market
[Switch-behavior-behavior_market] mirror-to interface GigabitEthernet 1/0/3
[Switch-behavior-behavior_market] quit
```

④ 定义策略 policy_market，为类 classifier_market 指定流行为 behavior_market。

```
[Switch] qos policy policy_market
[Switch-qospolicy-policy_market] classifier classifier_market behavior behavior_market
[Switch-qospolicy-policy_market] quit
```

(3) 定义针对研发部门的策略。

① 定义基本 ACL 2001，对研发部门内的 Host 进行分类。

```
[Switch] acl number 2001
[Switch-acl-basic-2001] rule permit source 192.168.2.0 0.0.0.127 time-range trname
[Switch-acl-basic-2001] quit
```

② 定义类 classifier_rd，匹配基本 ACL 2001。

```
[Switch] traffic classifier classifier_rd
[Switch-classifier-classifier_rd] if-match acl 2001
[Switch-classifier-classifier_rd] quit
```

③ 定义流行为 behavior_rd，动作为重定向至端口 GigabitEthernet 1/0/3。

```
[Switch] traffic behavior behavior_rd
[Switch-behavior-behavior_rd] redirect interface GigabitEthernet 1/0/3
[Switch-behavior-behavior_rd] quit
```

④ 定义策略 policy_rd，为类 classifier_rd 指定流行为 behavior_rd。

```
[Switch] qos policy policy_rd
[Switch-qospolicy-policy_rd] classifier classifier_rd behavior behavior_rd
[Switch-qospolicy-policy_rd] quit
```

(4) 应用策略。

① 将策略 policy_market 应用到端口 GigabitEthernet 1/0/1 上。

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy_market inbound
[Switch-GigabitEthernet1/0/1] quit
```

② 将策略 policy_rd 应用到端口 GigabitEthernet 1/0/2 上。

```
[Switch] interface GigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] qos a policy policy_rd inbound
```

11.4.5 重定向至下一跳典型配置指导

流量重定向至下一跳就是将符合分类的流重定向到一个出接口。

1. 背景

M 公司访问 Internet 有两个出口线路，分别是电信和网通，公司内网数据库服务器也划分为电信和网通两个部分，分别给电信和网通来访问的用户提供数据查询服务。正常情况下，网通服务器给网通线路过来的查询信息提供数据访问服务，电信服务器给电信线路过来的查询信息提供数据访问服务。网络管理员需要在交换机上进行重定向至下一跳的配置，将网通服务器流量向网通出口转发，电信服务器流量向电信出口转发。

2. 组网图

图 11-12 所示为重定向至下一跳典型配置组网图。

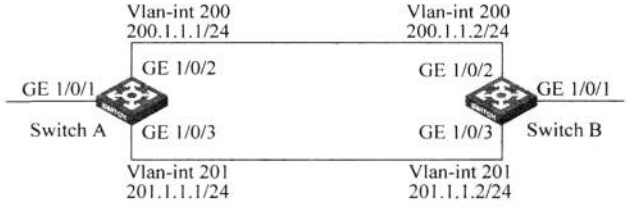


图 11-12 重定向至下一跳典型配置组网图

3. 配置需求

如图 11-12 所示，网络环境描述如下：

(1) 交换机 Switch A 通过两条链路与 Switch B 连接，同时 Switch A 和 Switch B 各自连接其他的设备。

(2) Switch A 上的端口 GigabitEthernet 1/0/2 和 Switch B 上的端口 GigabitEthernet 1/0/2 属于 VLAN 200。

(3) Switch A 上的端口 GigabitEthernet 1/0/3 和 Switch B 上的端口 GigabitEthernet 1/0/3 属于 VLAN 201。

(4) Switch A 上 VLAN 200 虚接口的 IP 地址为 200.1.1.1，VLAN 201 虚接口的 IP 地址为 201.1.1.1；Switch B 上 VLAN 200 虚接口的 IP 地址为 200.1.1.2，VLAN 201 虚接口的 IP 地址为 201.1.1.2。

配置重定向至下一跳，实现策略路由功能，满足如下需求。

(1) 将 Switch A 的端口 GigabitEthernet 1/0/1 接收到的源 IP 地址为 2.1.1.1 的报文转发至 200.1.1.2。

(2) 将 Switch A 的端口 GigabitEthernet 1/0/1 接收到的源 IP 地址为 2.1.1.2 的报文转发至 201.1.1.2。

(3) 对于 Switch A 的端口 GigabitEthernet 1/0/1 接收到的其他报文，按照查找路由表的方式进行转发。

4. 配置过程和解释

(1) 定义基本 ACL 2000，对源 IP 地址为 2.1.1.1 的报文进行分类。

```
<Switch> system-view
[Switch] acl number 2000
[Switch-acl-basic-2000] rule permit source 2.1.1.1 0
[Switch-acl-basic-2000] quit
```

(2) 定义基本 ACL 2001，对源 IP 地址为 2.1.1.2 的报文进行分类。

```
[Switch] acl number 2001
[Switch-acl-basic-2001] rule permit source 2.1.1.2 0
[Switch-acl-basic-2001] quit
```

(3) 定义类 classifier_1，匹配基本 ACL 2000。

```
[Switch] traffic classifier classifier_1
[Switch-classifier-classifier_1] if-match acl 2000
[Switch-classifier-classifier_1] quit
```

(4) 定义流行为 behavior_1，动作为重定向至 200.1.1.2。

```
[Switch] traffic behavior behavior_1
[Switch-behavior-behavior_1] redirect next-hop 200.1.1.2
[Switch-behavior-behavior_1] quit
```

(5) 定义类 classifier_2，匹配基本 ACL 2001。

```
[Switch] traffic classifier classifier_2
```

```
[Switch-classifier-classifier_2] if-match acl 2001
[Switch-classifier-classifier_2] quit
```

(6) 定义流行为 behavior_2,动作为重定向至 201.1.1.2。

```
[Switch] traffic behavior behavior_2
[Switch-behavior-behavior_2] redirect next-hop 201.1.1.2
[Switch-behavior-behavior_2] quit
```

(7) 定义策略 policy,为类 classifier_1 指定流行为 behavior_1,为类 classifier_2 指定流行为 behavior_2。

```
[Switch] qos policy policy
[Switch-qospolicy-policy] classifier classifier_1 behavior behavior_1
[Switch-qospolicy-policy] classifier classifier_2 behavior behavior_2
[Switch-qospolicy-policy] quit
```

(8) 将策略 policy 应用到端口 GigabitEthernet 1/0/1 的入方向上。

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy inbound
```

提示:用户可以根据实际情况需要配置策略路由。与单纯依照 IP 报文的目的地址查找路由表进行转发不同,策略路由基于到达报文的源地址等信息可以灵活地进行路由选择。

策略路由的优先级要高于普通路由,即报文首先按照策略路由进行转发。如果无法匹配所有的策略路由条件,则再按照普通路由进行转发。

第12章

安全特性配置指导

12.1 AAA 典型配置指导

AAA(Authentication,Authorization,Accounting,认证、授权、计费)是网络安全的一种管理机制,提供了认证、授权、计费 3 种安全功能。

AAA 是运行于 NAS(Network Access Server,网络接入服务器)上的客户端程序,它提供了一个对认证、授权和计费这 3 种安全功能进行统一配置的框架。

AAA 一般采用客户机/服务器结构,客户端运行于 NAS 上,服务器上则集中管理用户信息。NAS 对于用户来讲是服务器,对于服务器来说是客户端。AAA 的基本组网结构示意图如图 12-1 所示。

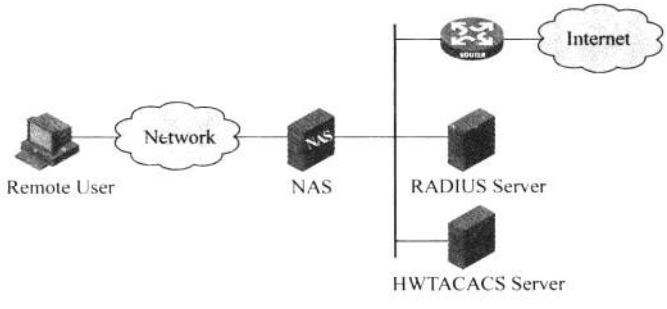


图 12-1 AAA 基本组网结构示意图

当用户想要通过某网络与 NAS 建立连接,从而获得访问其他网络的权利或取得某些网络资源的权利时,NAS 起到了验证用户或对应连接的作用。NAS 负责将用户的认证、授权、计费信息透传给服务器(RADIUS 服务器或 HWTACACS 服务器),RADIUS 协议或 HWTACACS 协议规定了 NAS 与服务器之间如何传递用户信息。

HWTACACS(HW Terminal Access Controller Access Control System,HW 终端访问控制器控制系统协议)是在 TACACS(RFC 1492)基础上进行了功能增强的安全协议。该协议与 RADIUS 协议类似,采用客户端/服务器模式实现 NAS 与 HWTACACS 服务器之间的通信。

HWTACACS 协议主要用于 PPP(Point-to-Point Protocol,点对点协议)和 VPDN(Virtual Private Dial-up Network,虚拟私有拨号网络)接入用户及终端用户的认证、授权和

计费。其典型应用是对需要登录到设备上进行操作的终端用户进行认证、授权、计费。设备作为 HWTACACS 的客户端，将用户名和密码发给 HWTACACS 服务器进行验证。用户验证通过并得到授权之后可以登录到设备上进行操作。

12.1.1 Telnet 用户通过 HWTACACS 服务器认证、授权、计费典型配置指导

1. 背景

M 公司的 IT 维护部门新安装了 HWTACACS 服务器，拟对 Telnet 登录设备的管理用户进行 HWTACACS 认证，并为不同级别的管理用户做不同的授权以实现分级管理增强设备的安全性。

2. 组网图

图 12-2 所示为 Telnet 用户的远端 HWTACACS 认证、授权和记费典型配置组网图。

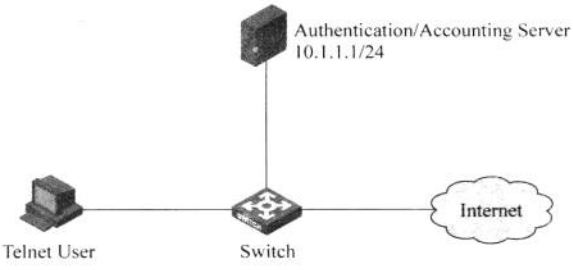


图 12-2 Telnet 用户的远端 HWTACACS 认证、授权和计费典型配置组网图

3. 配置需求

通过配置 Switch 实现 HWTACACS 服务器对登录 Switch 的用户进行认证、授权、计费，如果 HWTACACS 服务器无响应，则切换为备选 Local 认证。

(1) 一台 HWTACACS 服务器(担当认证、授权、计费的职责)与 Switch 相连，服务器 IP 地址为 10.1.1.1。

(2) Switch 与认证、授权、计费 HWTACACS 服务器交互报文时的共享密钥均为 expert，发送给 HWTACACS 服务器的用户名中不带域名。

(3) 在 HWTACACS 服务器上设置与 Switch 交互报文时的共享密钥为 expert。

4. 配置过程和解释

(1) 开启 Switch 的 Telnet 服务器功能。

```
<Switch> system-view
[Switch] telnet server enable
```

(2) 配置 Telnet 用户登录采用 AAA 认证方式。

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
[Switch-ui-vty0-4] quit
```

(3) 配置 HWTACACS 方案。

```
[Switch] hwtacacs scheme hwtac
```

```
[Switch-hwtacacs-hwtac] primary authentication 10.1.1.1 49
[Switch-hwtacacs-hwtac] primary authorization 10.1.1.1 49
[Switch-hwtacacs-hwtac] primary accounting 10.1.1.1 49
[Switch-hwtacacs-hwtac] key authentication expert
[Switch-hwtacacs-hwtac] key authorization expert
[Switch-hwtacacs-hwtac] key accounting expert
[Switch-hwtacacs-hwtac] user-name-format without-domain
[Switch-hwtacacs-hwtac] quit
```

(4) 配置 ISP 域的 AAA 方案。

```
[Switch] domain 1
[Switch-isp-1] authentication login hwtacacs-scheme hwtac local
[Switch-isp-1] authorization login hwtacacs-scheme hwtac local
[Switch-isp-1] accounting login hwtacacs-scheme hwtac local
[Switch-isp-1] quit
```

(5) 创建本地用户 Telnet。

```
[Switch] local-user telnet
[Switch-luser-telnet] service-type telnet
[Switch-luser-telnet] password simple telnet
```

提示：本例只介绍了设备的配置，实际操作中也要对 HWTACACS 服务器进行配置，且为了实现远端 HWTACACS 服务器无响应时自动转本地，HWTACACS 服务器和本地用户应使用同样的用户名和密码。

因为设备默认认证域是 system，在 Telnet 设备登录时，需要输入用户名为 userid@1，以使用域 1 进行认证。

12.1.2 Telnet 用户通过 Local 认证、HWTACACS 授权、RADIUS 计费的应用典型配置指导

1. 背景

尽管认证、授权、计费都可以在一台 HWTACACS 服务器上完成配置，但为了增强服务器的健壮性，可以将认证、授权、计费设计成由不同服务器完成。M 公司的网络就规划成由设备 Local 方式认证，HWTACACS 进行授权，RADIUS 服务器进行计费。

2. 组网图

图 12-3 所示为 Telnet 用户通过 Local 认证、HWTACACS 授权和 RADIUS 计费的应用典型配置组网图。

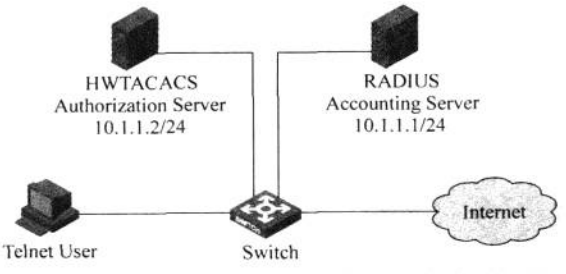


图 12-3 Telnet 用户通过 Local 认证、HWTACACS 授权和 RADIUS 计费的应用典型配置组网图

3. 配置需求

通过配置 Switch 实现 Local 认证、HWTACACS 授权和 RADIUS 计费。Telnet 用户的用户名和密码为 telnet。

(1) 一台 HWTACACS 服务器(担当授权服务器的职责)与 Switch 相连,服务器 IP 地址为 10.1.1.2。Switch 与授权 HWTACACS 服务器交互报文时的共享密钥均为 expert,发送给 HWTACACS 服务器的用户名中不带域名。

(2) 一台 RADIUS 服务器(担当计费服务器的职责)与 Switch 相连,服务器 IP 地址为 10.1.1.1。Switch 与计费 RADIUS 服务器交互报文时的共享密钥为 expert。

4. 配置过程和解释

(1) 配置各接口的 IP 地址(略)。

(2) 开启 Switch 的 Telnet 服务器功能。

```
<Switch> system-view
[Switch] telnet server enable
```

(3) 配置 Telnet 用户登录采用 AAA 认证方式。

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
[Switch-ui-vty0-4] quit
```

(4) 配置 HWTACACS 方案。

```
[Switch] hwtacacs scheme hwtac
[Switch-hwtacacs-hwtac] primary authorization 10.1.1.2 49
[Switch-hwtacacs-hwtac] key authorization expert
[Switch-hwtacacs-hwtac] user-name-format without-domain
[Switch-hwtacacs-hwtac] quit
```

(5) 配置 RADIUS 方案。

```
[Switch] radius scheme rd
[Switch-radius-rd] primary accounting 10.1.1.1 1813
[Switch-radius-rd] key accounting expert
[Switch-radius-rd] server-type extended
[Switch-radius-rd] user-name-format without-domain
[Switch-radius-rd] quit
```

(6) 创建本地用户 telnet。

```
[Switch] local-user telnet
[Switch-luser-telnet] service-type telnet
[Switch-luser-telnet] password simple telnet
```

(7) 配置 ISP 域的 AAA 方案。

```
[Switch] domain 1
[Switch-isp-1] authentication login local
[Switch-isp-1] authorization login hwtacacs-scheme hwtac
[Switch-isp-1] accounting login radius-scheme rd
```

[Switch-isp-1] quit

12.1.3 SSH 用户通过 RADIUS 服务器认证、授权、计费的应用典型配置指导

1. 背景

Telnet 协议采用明文方式来传输密码，其安全性不高。为了进一步加强登录设备的安全性，IT 维护部门决定采用 SSH 来替代 Telnet，同样对 SSH 用户通过 RADIUS 服务器进行认证、授权和计费。

2. 组网图

图 12-4 所示为 SSH 用户通过 RADIUS 服务器认证、授权和计费的应用典型配置组网图。

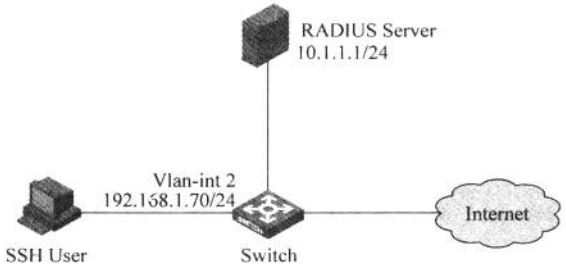


图 12-4 SSH 用户通过 RADIUS 服务器认证、授权和计费的应用典型配置组网图

3. 配置需求

如图 12-4 所示，配置 Switch 实现 RADIUS 服务器对登录 Switch 的 SSH 用户进行认证、授权和计费。

(1) 一台 RADIUS 服务器(其担当认证 RADIUS 服务器和计费 RADIUS 服务器的职责)与 Switch 相连，服务器 IP 地址为 10.1.1.1。

(2) Switch 与认证、计费 RADIUS 服务器交互报文时的共享密钥均为 expert，发送给 RADIUS 服务器的用户名带域名。

(3) RADIUS 服务器使用 CAMS 服务器。

4. 配置过程和解释

(1) 配置 RADIUS Server。

说明：本书以 CAMS 服务器 V2.10 为例，说明该例中 RADIUS Server 的基本配置。

① 增加接入设备。登录进入 CAMS 管理平台，选择左侧菜单树中“系统管理”→“系统配置”→“接入设备配置”→“修改”→“增加”命令后，进入“接入设备配置”页面。

a. 添加 Switch 的 IP 地址“192.168.1.70”。

b. 设置与 Switch 交互报文时的认证、计费共享密钥为“expert”。

c. 选择协议类型为“LAN 接入业务”。

d. 设置认证及计费的端口号分别为“1812”和“1813”。

e. 选择 RADIUS 协议类型为“扩展协议”。

f. 选择 RADIUS 报文类型为“标准报文”。

② 增加设备管理用户。选择左侧菜单树中“用户管理”→“设备管理用户”→“增加”命令后，进入“设备管理用户配置”页面。

a. 添加用户名“hello@bbb”和密码。

b. 选择服务类型为 SSH。

c. 设置 EXEC 权限级别为“3”。

d. 添加所管理主机 IP 地址范围。

(2) 配置 Switch。

① 配置 VLAN 接口 2 的 IP 地址，SSH 客户端将通过该地址连接 SSH 服务器。

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
```

② 生成 RSA 及 DSA 密钥对，并启动 SSH 服务器。

```
[Switch] public-key local create rsa
[Switch] public-key local create dsa
[Switch] ssh server enable
```

③ 配置 SSH 用户登录采用 AAA 认证方式。

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
```

④ 配置用户远程登录 Switch 的协议为 SSH。

```
[Switch-ui-vty0-4] protocol inbound ssh
[Switch-ui-vty0-4] quit
```

⑤ 配置 RADIUS 方案。

```
[Switch] radius scheme rad
[Switch-radius-rad] primary authentication 10.1.1.1 1812
[Switch-radius-rad] primary accounting 10.1.1.1 1813
[Switch-radius-rad] key authentication expert
[Switch-radius-rad] key accounting expert
[Switch-radius-rad] user-name-format with-domain
[Switch-radius-rad] quit
```

⑥ 配置 ISP 域的 AAA 方案。

```
[Switch] domain bbb
[Switch-isp-bbb] authentication login radius-scheme rad
[Switch-isp-bbb] authorization login radius-scheme rad
[Switch-isp-bbb] accounting login radius-scheme rad
[Switch-isp-bbb] quit
```

使用 SSH 登录时输入用户名为 userid@bbb，以使用域 bbb 进行认证。

(3) SSH 用户建立与 Switch 的连接。在 SSH 客户端按照提示输入用户名 hello@bbb 及密码，即可进入 Switch 的用户界面。用户登录系统后所能访问的命令级别由 CAMS 服

务器授权，可通过设备管理用户界面的 EXEC 权限级别来设置。

12.2 802.1x 与 EAD 典型配置指导

IEEE 802 LAN/WAN 委员会为解决无线局域网网络安全问题，提出了 802.1x 协议。后来，802.1x 协议作为局域网端口的一个普通接入控制机制在以太网中被广泛应用，主要解决以太网内认证和安全方面的问题。

802.1x 协议是一种基于端口的网络接入控制协议（Port Based Network Access Control）。基于端口的网络接入控制是指在局域网接入设备的端口这一级对所接入的用户设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

EAD（Endpoint Admission Defense，端点准入防御）是一个网络端点接入控制方案，它通过安全客户端、安全策略服务器、接入设备以及第三方服务器的连动，加强了对用户的集中管理，提升了网络的整体防御能力。

12.2.1 802.1x 典型配置指导

1. 背景

H 公司网络建好后，需要考虑如何限制外部用户非法访问。最初，网管员采取物理分离的方案，即单独安排一间办公室给外部用户上网。实际使用中，发现因为各种原因，外部用户仍然可能会到内部员工区域上网，且无法对其进行监察。

经过技术分析后，网管员认为在交换机上采用 802.1x 认证，配合 RADIUS 认证服务器，可达到限制用户接入的目的。

2. 组网图

图 12-5 所示为 802.1x 典型配置组网图。

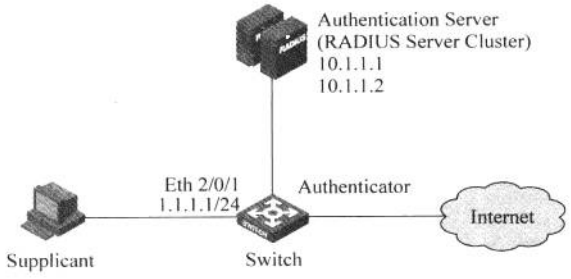


图 12-5 802.1x 典型配置组网图

3. 配置需求

（1）要求在各端口上对接入用户进行认证，以控制其访问 Internet；接入控制方式要求是基于 MAC 地址的接入控制。

（2）所有接入用户都属于一个默认的域：aabbcc.net，该域最多可容纳 30 个用户；认证时，先进行 RADIUS 认证，如果 RADIUS 服务器没有响应再转而进行本地认证；计费时，如

果 RADIUS 计费失败，则切断用户连接使其下线。

(3) 由两台 RADIUS 服务器组成的服务器组与交换机相连，其 IP 地址分别为 10.1.1.1和 10.1.1.2，要求使用前者作为主认证/备份计费服务器，使用后者作为备份认证/主计费服务器。

(4) 设置系统与认证 RADIUS 服务器交互报文时的共享密钥为 name，与计费 RADIUS 服务器交互报文时的共享密钥为 money。

(5) 设置系统在向 RADIUS 服务器发送报文后 5s 内如果没有得到响应就向其重新发送报文，发送报文的次数总共为 5 次，设置系统每 15min 就向 RADIUS 服务器发送一次实时计费报文。

(6) 设置系统从用户名中去除用户域名后再将之传给 RADIUS 服务器。

(7) 本地 802.1x 接入用户的用户名为 localuser，密码为 localpass，使用明文输入；闲置切断功能处于打开状态，正常连接时用户空闲时间超过 20min，则切断其连接。

4. 配置过程和解释

(1) 配置各接口的 IP 地址(略)。

(2) 添加本地接入用户，启动闲置切断功能并设置相关参数。

```
<Sysname> system-view
[Sysname] local-user localuser
[Sysname-luser-localuser] service-type lan-access
[Sysname-luser-localuser] password simple localpass
[Sysname-luser-localuser] attribute idle-cut 20
[Sysname-luser-localuser] quit
```

(3) 创建 RADIUS 方案 radius1 并进入其视图。

```
[Sysname] radius scheme radius1
```

(4) 设置主认证/计费 RADIUS 服务器的 IP 地址。

```
[Sysname-radius-radius1] primary authentication 10.1.1.1
[Sysname-radius-radius1] primary accounting 10.1.1.2
```

(5) 设置备份认证/计费 RADIUS 服务器的 IP 地址。

```
[Sysname-radius-radius1] secondary authentication 10.1.1.2
[Sysname-radius-radius1] secondary accounting 10.1.1.1
```

(6) 设置系统与认证 RADIUS 服务器交互报文时的共享密钥。

```
[Sysname-radius-radius1] key authentication name
```

(7) 设置系统与计费 RADIUS 服务器交互报文时的共享密钥。

```
[Sysname-radius-radius1] key accounting money
```

(8) 设置系统向 RADIUS 服务器重发报文的时间间隔与次数。

```
[Sysname-radius-radius1] timer response-timeout 5
[Sysname-radius-radius1] retry 5
```

(9) 设置系统向 RADIUS 服务器发送实时计费报文的时间间隔。

```
[Sysname-radius-radius1] timer realtime-accounting 15
```

(10) 指示系统从用户名中去除用户域名后再将之传给 RADIUS 服务器。

```
[Sysname-radius-radius1] user-name-format without-domain
[Sysname-radius-radius1] quit
```

(11) 创建域 aabbcc.net 并进入其视图。

```
[Sysname] domain aabbcc.net
```

(12) 指定 radius1 为该域用户的 RADIUS 方案,并采用 local 作为备选方案。

```
[Sysname-isp-aabbcc.net] authentication default radius-scheme radius1 local
[Sysname-isp-aabbcc.net] authorization default radius-scheme radius1 local
[Sysname-isp-aabbcc.net] accounting default radius-scheme radius1 local
```

(13) 设置该域最多可容纳 30 个用户。

```
[Sysname-isp-aabbcc.net] access-limit enable 30
```

(14) 启动闲置切断功能并设置相关参数。

```
[Sysname-isp-aabbcc.net] idle-cut enable 20
[Sysname-isp-aabbcc.net] quit
```

(15) 配置域 aabbcc.net 为默认用户域。

```
[Sysname] domain default enable aabbcc.net
```

(16) 开启全局 802.1x 特性。

```
[Sysname] dot1x
```

(17) 开启指定端口 Ethernet 2/0/1 的 802.1x 特性。

```
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet2/0/1] dot1x
[Sysname-Ethernet2/0/1] quit
```

(18) 设置接入控制方式(该命令可以不配置,因为端口的接入控制在默认情况下就是基于 MAC 地址的)。

```
[Sysname] dot1x port-method macbased interface Ethernet 2/0/1
```

提示:只有同时开启全局和端口的 802.1x 特性后,802..1x 的配置才能在端口上生效。

接入控制方式分两种:portbased 和 macbased。在 portbased 方式下,一个用户认证通过,整个端口的受限状态就打开,其他用户无须认证也能访问网络;在 macbased 方式下,每个用户必须都通过认证。

12.2.2 Guest VLAN、动态下发 VLAN 典型配置指导

1. 背景

在接入交换机配置了 802.1x 之后,外部用户在内部网络就无法接入网络,无法访问任

何资源。但在实际使用中，相当一部分外部用户表示只能到特定的办公室才能上网不够方便，希望能够随时接入网络从而访问 Internet；同时，公司内员工也表示部分公用资源没有必要限制，希望不经过认证也能访问。另外，由于公司内各种不同部门职责不同，也需要有不同的访问权限。综合考虑上述需求后，网管员觉得可以采用在交换机上配置 Guest VLAN 和动态下发 VLAN。

配置 Guest VLAN 后，未认证用户仅能够访问某个特定 VLAN(Guest VLAN)。而动态下发 VLAN 则使认证后用户能够划分到预先设置好的 VLAN 内。

2. 组网图

图 12-6 所示为 Guest VLAN、动态下发 VLAN 典型配置组网图。

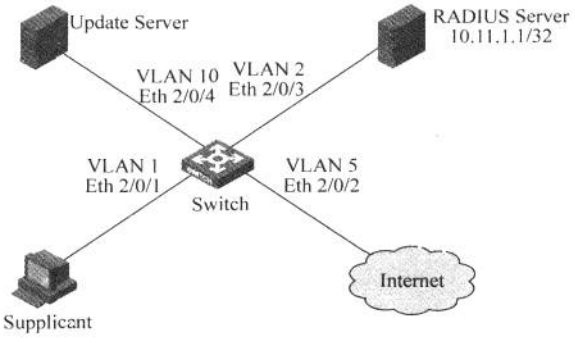


图 12-6 Guest VLAN、动态下发 VLAN 典型配置组网图

3. 配置需求

(1) 主机通过 802.1x 认证接入网络，认证服务器为 RADIUS 服务器，RADIUS 服务器支持动态 VLAN 下发功能。

(2) 设置系统与 RADIUS 服务器交互报文时的共享密钥为 abc。

(3) Update Server 是用于客户端软件下载和升级的服务器，在 VLAN 10 内。

(4) 交换机连接 Internet 的端口 Ethernet 2/0/2 在 VLAN 5 内。

(5) 当交换机从端口发送触发认证报文(EAP-Request/Identity)超过设定的最大次数而没有收到任何回应报文后，Ethernet 2/0/1 被加入 Guest VLAN 中，此时 Supplicant 和 Update Server 都在 VLAN 10 内，Supplicant 可以访问 Update Server 并下载 802.1x 客户端。

(6) 当用户认证成功上线，认证服务器下发 VLAN 5。此时 Supplicant 和Ethernet 2/0/2 都在 VLAN 5 内，Supplicant 可以访问 Internet。

4. 配置过程和解释

(1) 配置 RADIUS 方案 2000。

```
<Sysname> system-view
[Sysname] radius scheme 2000
[Sysname-radius-2000] primary authentication 10.11.1.1 1812
[Sysname-radius-2000] primary accounting 10.11.1.1 1813
```

```
[Sysname-radius-2000] key authentication abc
[Sysname-radius-2000] key accounting abc
[Sysname-radius-2000] user-name-format without-domain
[Sysname-radius-2000] quit
```

(2) 配置 domain，该 domain 使用刚才配置好的 RADIUS 方案 2000。

```
[Sysname] domain system
[Sysname-isp-system] authentication default radius-scheme 2000
[Sysname-isp-system] authorization default radius-scheme 2000
[Sysname-isp-system] accounting default radius-scheme 2000
[Sysname-isp-system] quit
```

(3) 开启全局 802.1x 特性。

```
[Sysname] dot1x
```

(4) 开启指定端口的 802.1x 特性。

```
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet2/0/1] dot1x
```

(5) 配置端口上进行接入控制的方式为 portbased。

```
[Sysname-Ethernet2/0/1] dot1x port-method portbased
```

(6) 配置端口上进行接入控制的模式为 auto。

```
[Sysname-Ethernet2/0/1] dot1x port-control auto
[Sysname-Ethernet2/0/1] quit
```

(7) 创建 VLAN 10。

```
[Sysname] vlan 10
[Sysname-vlan10] quit
```

(8) 配置指定端口的 Guest VLAN。

```
[Sysname] dot1x guest-vlan 10 interface Ethernet 2/0/1
```

通过命令 display current-configuration 或者 display interface Ethernet 2/0/1 可以查看 Guest VLAN 配置情况。

在没有用户上线、用户认证失败或用户成功下线等情况下发送触发认证报文(EAP-Request/Identity)超过设定的最大次数时，通过命令 display vlan 10 可以查看端口配置的 Guest VLAN 是否生效。

在用户成功上线后，通过命令 display vlan 5 可以查看服务器下发的动态 VLAN 是否生效。

提示： 在组播触发功能开启的情况下，Guest VLAN 才能生效。

不同的端口可以配置不同的 Guest VLAN，但一个端口只能配置一个 Guest VLAN。

动态下发的 VLAN 需要在 Radius Server 上进行相关配置。

12.2.3 下发 ACL 应用典型配置指导

1. 背景

配置了 Guest VLAN 和动态下发 VLAN，实际上是增加了网络中 VLAN 配置的灵活性，从 VLAN 接入上对用户进行了限制。

但为了进一步加强网络的安全，IT 维护部门希望能够对不同类别的用户下发不同的 ACL，从而使不同用户有不同的网络访问权限。针对此需求，可以使用 RADIUS 属性来下发 ACL。

2. 组网图

图 12-7 所示为下发 ACL 典型配置组网图。

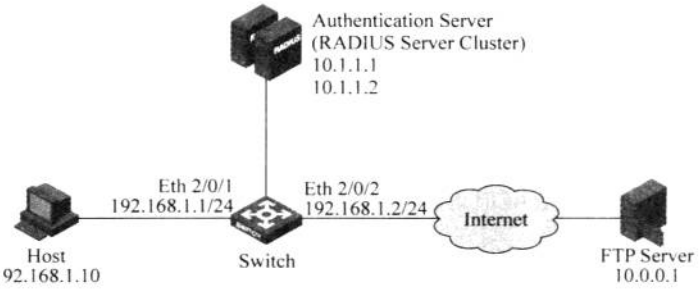


图 12-7 下发 ACL 典型配置组网图

3. 配置需求

如图 12-7 所示，主机 Host 通过 802.1x 认证接入网络，认证服务器为 RADIUS 服务器。Internet 中有一台 FTP 服务器，IP 地址为 10.0.0.1。

(1) 在认证服务器上配置授权下发 ACL 3000。

(2) 在 Switch 的 Ethernet 2/0/1 上开启 802.1x 认证，并配置 ACL 3000。

当用户认证成功上线后，认证服务器下发 ACL 3000。此时 ACL 3000 在Ethernet 2/0/1 上生效，Host 可以访问 Internet，但不能访问 FTP 服务器。

4. 配置过程和解释

(1) 配置各接口的 IP 地址(略)。

(2) 配置 RADIUS 方案。

```
<Sysname> system-view
[Sysname] radius scheme 2000
[Sysname-radius-2000] primary authentication 10.1.1.1 1812
[Sysname-radius-2000] primary accounting 10.1.1.2 1813
[Sysname-radius-2000] key authentication abc
[Sysname-radius-2000] key accounting abc
[Sysname-radius-2000] user-name-format without-domain
[Sysname-radius-2000] quit
```

(3) 配置 ISP 域的 AAA 方案。

```
[Sysname] domain 2000
```

```
[Sysname-isp-2000] authentication default radius-scheme 2000
[Sysname-isp-2000] authorization default radius-scheme 2000
[Sysname-isp-2000] accounting default radius-scheme 2000
[Sysname-isp-2000] quit
```

(4) 配置 ACL 3000,拒绝目的 IP 地址为 10.0.0.1 的报文通过。

```
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 0 deny ip destination 10.0.0.1 0
```

(5) 开启全局 802.1x 特性。

```
[Sysname] dot1x
```

(6) 开启指定端口的 802.1x 特性。

```
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet2/0/1] dot1x
```

提示:本例中,还需要在认证服务器上配置下发 ACL 3000,读者可自行参考服务器相关配置手册。

动态 ACL 下发是通过 RADIUS 标准属性下发的,主流的 RADIUS Server 都支持。

12.2.4 EAD 快速部署典型配置指导

1. 背景

公司网络中部署了 EAD 解决方案。但是 EAD 客户端的部署工作量很大,例如,需要网络管理员手动为每一个 EAD 客户端下载、升级客户端软件,这在 EAD 客户端数目较多的情况下会给管理员带来了操作上的不便。

802.1x 认证支持的 EAD 快速部署可以解决以上问题,可为所有接入网络的终端用户提供自动下载并安装 EAD 客户端的方便途径。

2. 组网图

图 12-8 所示为 EAD 快速部署典型配置组网图。

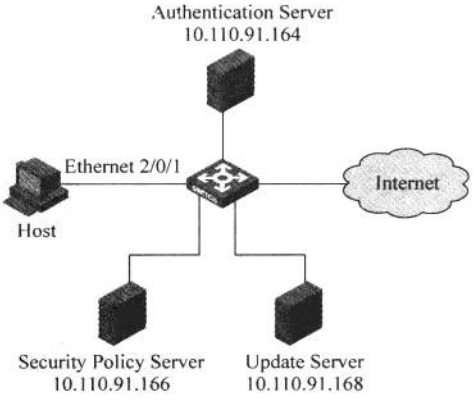


图 12-8 EAD 快速部署典型配置组网图

3. 配置需求

(1) Host 与以太网交换机的端口 Ethernet 2/0/1 相连接。

(2) 通过对交换机的配置,认证成功之前,Host 通过浏览器访问外部网络会被重定向至 Update 服务器,进行 802.1x 客户端的下载及安装。

(3) 通过对交换机、RADIUS 服务器、安全策略服务器的配置,实现 RADIUS 服务器对接入用户的远端认证和安全策略服务器对用户的 EAD 操作控制。

4. 配置过程和解释

(1) 配置 Web 服务器。用户在使用 EAD 快速部署功能之前首先必须配置好 Update 服务器作为 Web 服务器,即用于下载 802.1x 客户端的重定向服务器。

(2) 配置 EAD 快速部署。

① 配置 Free IP。

```
<Switch> system-view
[Switch] dot1x free-ip 10.110.91.0 24
```

② 配置 IE 访问的重定向 URL。

```
[Switch] dot1x url http:// 10.110.91.168
```

③ 开启全局 802.1x 特性。

```
[Switch] dot1x
```

④ 开启指定端口的 802.1x 特性。

```
[Switch] interface ethernet 2/0/1
[Switch-Ethernet2/0/1] dot1x
```

(3) 配置 EAD 功能。

① 配置 RADIUS 方案。

```
[Switch] radius scheme cams
[Switch-radius-cams] primary authentication 10.110.91.164 1812
[Switch-radius-cams] primary accounting 10.110.91.164 1813
[Switch-radius-cams] key authentication expert
[Switch-radius-cams] key accounting expert
[Switch-radius-cams] user-name-format with-domain
[Switch-radius-cams] server-type extended
```

② 配置安全策略服务器地址。

```
[Switch-radius-cams] security-policy-server 10.110.91.166
```

③ 配置默认的 AAA 方案。

```
[Switch] domain aaa
[Switch-isp-aaa] authentication default radius-scheme cams
[Switch-isp-aaa] authorization default radius-scheme cams
[Switch-isp-aaa] accounting default radius-scheme cams
```

使用 Telnet 登录时输入用户名为 userid@aaa,以使用域 aaa 进行认证。

(4) 用户连接。用户在802.1x认证成功之前，通过浏览器访问任何外部网站都会被重定向到Update Server页面，此页面提供客户端的下载服务。

下载客户端，并输入正确的用户名、密码，客户端通过认证服务器的身份验证以后，安全客户端对Host的安全状况进行检测，并与安全策略服务器交互，如果不符合安全认证的标准，安全策略服务器下发ACL控制报文到交换机，交换机只允许客户端访问Update服务器。

只有当客户端安装了补丁，并且客户端的安全标准满足了安全认证的标准以后，安全客户端才将客户端的安全状态传递到安全策略服务器，安全策略服务器将再次下发ACL，使交换机打开客户端的访问权限，使之能够访问更多的网络资源。

提示：EAD需要在对应的安全策略服务器上设置一系列的安全策略，此处没有列出，具体设置可以参考所使用的服务器文档。

采用重定向到Web页面方式需要先设置Web Server来提供客户端下载页面，当然也可以通过其他方式，如FTP等，但要确保Server地址在Free-IP范围内。

输入域名来重定向到Web Server页面时，要确保DNS网段也配置在Free-IP内，使得域名能够被解析，否则无法重定向到Web Server页面。

12.3 MAC地址认证典型配置指导

MAC地址认证是一种基于端口和MAC地址对用户的网络访问权限进行控制的认证方法，不需要用户安装任何客户端软件。设备在首次检测到用户的MAC地址以后，即启动对该用户的认证操作。认证过程中，也不需要用户手动输入用户名或者密码。

目前设备支持两种方式的MAC地址认证。

(1) 通过RADIUS(Remote Authentication Dial-In User Service，远程认证拨号用户服务)服务器认证。

(2) 本地认证。

认证方式确定后，可根据需求选择MAC认证用户名的类型，包括以下两种方式。

(1) MAC地址用户名：使用用户的MAC地址作为认证时的用户名和密码。

(2) 固定用户名：不论用户的MAC地址为何值，所有用户均使用在设备上预先配置的本地用户名和密码进行认证。

12.3.1 MAC地址本地认证典型配置指导

1. 背景

M公司的IT维护部门对终端接入用户进行802.1x认证，并安装iNode客户端实施EAD解决方案。但部署时发现网络内有些终端无法安装客户端，如网络里的打印机，根本就没有提供输入用户名、密码的界面。对于这种情况，可以采用MAC地址认证。

2. 组网图

图12-9所示为启动MAC地址认证对接入用户进行本地认证。

3. 配置需求

如图12-9所示，某用户的工作站与以太网设备的端口GigabitEthernet 2/0/1相连接。

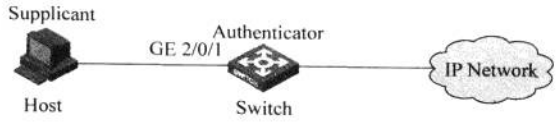


图 12-9 启动 MAC 地址认证对接入用户进行本地认证

(1) 设备的管理者希望在各端口上对用户接入进行 MAC 地址认证，以控制其对 Internet 的访问。

(2) 要求设备每隔 180s 就对用户是否下线进行检测；并且当用户认证失败时，需等待 3min 后才能对用户再次发起认证。

(3) 所有用户都属于域 aabbcc. net，认证时使用本地认证的方式。用户名为 aaa，密码为 123456。

4. 配置过程和解释

(1) 添加本地接入用户。

```
<Switch> system-view
[Switch] local-user aaa
[Switch-luser-aaa] password simple 123456
[Switch-luser-aaa] service-type lan-access
[Switch-luser-aaa] quit
```

(2) 配置 ISP 域，使用本地认证方式。

```
[Switch] domain aabbcc.net
[Switch-isp-aabbcc.net] authentication lan-access local
[Switch-isp-aabbcc.net] quit
```

(3) 开启全局 MAC 地址认证特性。

```
[Switch] mac-authentication
```

(4) 开启端口 GigabitEthernet 2/0/1 的 MAC 地址认证特性。

```
[Switch] mac-authentication interface GigabitEthernet 2/0/1
```

(5) 配置 MAC 地址认证用户所使用的 ISP 域。

```
[Switch] mac-authentication domain aabbcc.net
```

(6) 配置 MAC 地址认证的定时器。

```
[Switch] mac-authentication timer offline-detect 180
[Switch] mac-authentication timer quiet 180
```

(7) 配置 MAC 地址认证使用固定用户名、密码格式。

```
[Switch] mac-authentication user-name-format fixed account aaa password simple 123456
```

提示：本地用户的服务类型应设置为 lan-access。

12.3.2 MAC地址RADIUS认证典型配置指导

1. 背景

采用MAC地址的本地认证时，需要在交换机本地数据库中添加打印机的MAC地址作为用户名和密码。但这种本地认证方式不利于用户的集中管理，比较好的方式是在RADIUS服务器上添加打印机的MAC地址作为认证的用户名和密码。这种集中认证带来的另外一个好处是不用担心交换机数据库没有足够的容量来容纳数量众多的用户。

2. 组网图

图12-10所示为启动MAC地址认证对接入用户进行RADIUS认证。

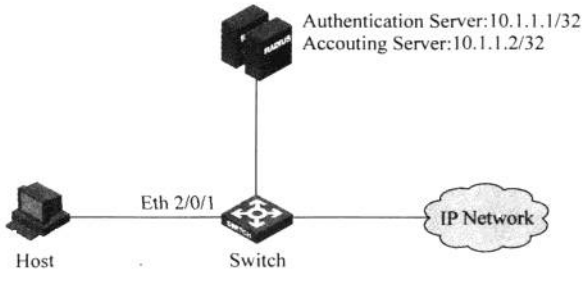


图12-10 启动MAC地址认证对接入用户进行RADIUS认证

3. 配置需求

如图12-10所示，用户主机Host通过端口Ethernet 2/0/1连接到设备上，设备通过RADIUS服务器对用户进行身份认证。

(1) 设备的管理者希望在各端口上对用户接入进行MAC地址认证，以控制其对Internet的访问。

(2) 要求设备每隔180s就对用户是否下线进行检测；并且当用户认证失败时，需等待3min后才能对用户再次发起认证。

4. 配置过程和解释

(1) 配置各接口的IP地址(略)。

(2) 配置RADIUS方案。

```
<Switch> system-view
[Switch] radius scheme 2000
[Switch-radius-2000] primary authentication 10.1.1.1 1812
[Switch-radius-2000] primary accounting 10.1.1.2 1813
[Switch-radius-2000] key authentication abc
[Switch-radius-2000] key accounting abc
[Switch-radius-2000] user-name-format without-domain
[Switch-radius-2000] quit
```

(3) 配置ISP域的AAA方案。

```
[Switch] domain 2000
[Switch-isp-2000] authentication default radius-scheme 2000
[Switch-isp-2000] authorization default radius-scheme 2000
```

```
[Switch-isp-2000] accounting default radius-scheme 2000
[Switch-isp-2000] quit
```

(4) 开启全局 MAC 地址认证特性。

```
[Switch] mac-authentication
```

(5) 开启端口 Ethernet 2/0/1 的 MAC 地址认证特性。

```
[Switch] mac-authentication interface Ethernet 2/0/1
```

(6) 配置 MAC 地址认证用户所使用的 ISP 域。

```
[Switch] mac-authentication domain 2000
```

(7) 配置 MAC 地址认证的定时器。

```
[Switch] mac-authentication timer offline-detect 180
[Switch] mac-authentication timer quiet 180
```

(8) 配置 MAC 地址认证使用用户的源 MAC 地址作为用户名与密码。MAC 地址带连字符"-"。

```
[Switch] mac-authentication user-name-format mac-address with-hyphen
```

提示：RADIUS 服务器上配置的用户名和密码必须与用户的 MAC 地址保持一致。RADIUS 服务器上配置的认证、计费 Key 需要和交换机上配置保持一致，才能认证成功。

12.3.3 下发 ACL 典型配置指导

1. 背景

为了更精细地控制访问权限，IT 维护部门拟对 MAC 地址认证的用户也同 802.1x 一样，定义动态下发 ACL。

2. 组网图

图 12-11 所示为下发 ACL 典型配置组网图。

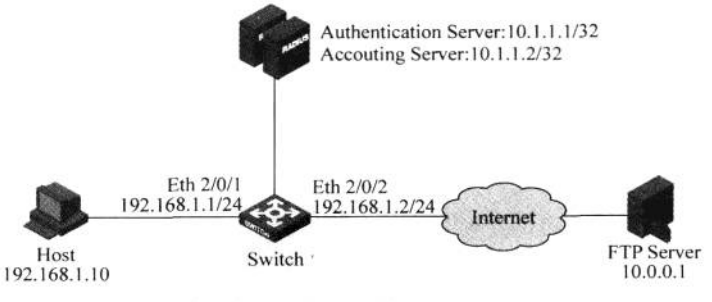


图 12-11 下发 ACL 典型配置组网图

3. 配置需求

如图 12-11 所示，主机 Host 通过 MAC 认证接入网络，认证服务器为 RADIUS 服务器。Internet 中有一台 FTP 服务器，IP 地址为 10.0.0.1。

(1) 在认证服务器上配置授权下发 ACL 3000。

(2) 在 Switch 的 Ethernet 2/0/1 上开启 MAC 认证，并配置 ACL 3000。

(3) 当用户认证成功上线后，认证服务器下发 ACL 3000。此时 ACL 3000 在 Ethernet 2/0/1 上生效，Host 可以访问 Internet，但不能访问 FTP 服务器。

4. 配置过程和解释

(1) 配置各接口的 IP 地址(略)。

(2) 配置 RADIUS 方案。

```
<Switch> system-view
[Switch] radius scheme 2000
[Switch-radius-2000] primary authentication 10.1.1.1 1812
[Switch-radius-2000] primary accounting 10.1.1.2 1813
[Switch-radius-2000] key authentication abc
[Switch-radius-2000] key accounting abc
[Switch-radius-2000] user-name-format without-domain
[Switch-radius-2000] quit
```

(3) 配置 ISP 域的 AAA 方案。

```
[Switch] domain 2000
[Switch-isp-2000] authentication default radius-scheme 2000
[Switch-isp-2000] authorization default radius-scheme 2000
[Switch-isp-2000] accounting default radius-scheme 2000
[Switch-isp-2000] quit
```

(4) 配置 ACL 3000，拒绝目的 IP 地址为 10.0.0.1 的报文通过。

```
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 0 deny ip destination 10.0.0.1 0
[Sysname-acl-adv-3000] quit
```

(5) 开启全局 MAC 地址认证特性。

```
[Switch] mac-authentication
```

(6) 开启端口 Ethernet 2/0/1 的 MAC 地址认证特性。

```
[Switch] mac-authentication interface Ethernet 2/0/1
```

(7) 配置 MAC 地址认证用户所使用的 ISP 域。

```
[Switch] mac-authentication domain 2000
```

(8) 配置 MAC 地址认证的定时器。

```
[Switch] mac-authentication timer offline-detect 180
[Switch] mac-authentication timer quiet 180
```

(9) 配置 MAC 地址认证用户名格式。使用带连字符的 MAC 地址作为用户名与密码。

```
[Switch] mac-authentication user-name-format mac-address with-hyphen
```

注意：作为用户名和密码的 MAC 地址中的字母必须为小写字母。

12.4 Portal 典型配置指导

Portal 在英语中是入口的意思。Portal 认证通常也称为 Web 认证，一般将 Portal 认证网站称为门户网站。

未认证用户上网时，设备强制用户登录到特定站点，用户可以免费访问其中的服务。当用户需要使用互联网中的其他信息时，必须在门户网站进行认证，只有认证通过后才可以使用互联网资源。

用户可以主动访问已知的 Portal 认证网站，输入用户名和密码进行认证，这种开始 Portal 认证的方式称为主动认证。反之，如果用户试图通过 HTTP 访问其他外网，将被强制访问 Portal 认证网站，从而开始 Portal 认证过程，这种方式称为强制认证。

Portal 业务可以为运营商提供方便的管理功能，门户网站可以开展广告、社区服务、个性化的业务等，使宽带运营商、设备提供商和内容服务提供商形成一个产业生态系统。此种认证方式常常被一些高校和酒店应用。

12.4.1 Portal 直接认证方式典型配置指导

1. 背景

M 公司在全网使用了 802.1x 认证之后很快就发现一个很棘手的问题，当很多合作伙伴来 M 公司参加会议时，需要接入 M 公司的网络收发邮件，但因为 802.1x 认证要安装客户端，操作不是很方便。有没有一种不需要安装客户端就能够认证的方式呢？经过调查，发现 Portal 认证比较适合这种情况使用。Portal 认证方式较为灵活，不需要安装客户端软件，直接使用 IE 浏览器就能认证。M 公司 IT 维护人员决定对外来人员访问区，如会议室等场所的网络采用 Portal 的认证方式。

2. 组网图

图 12-12 所示为 Portal 直接认证方式典型配置组网图。

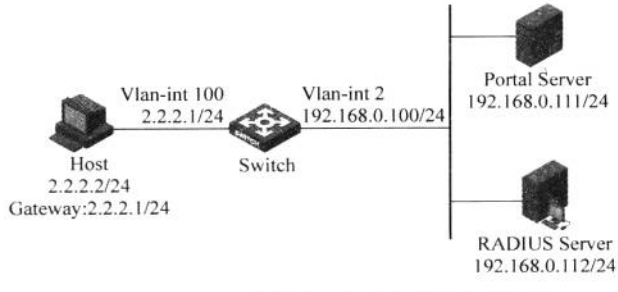


图 12-12 Portal 直接认证方式典型配置组网图

3. 配置需求

(1) 配置交换机采用直接方式的 Portal 认证。用户在未通过 Portal 认证前，只能访问 Portal 服务器；用户通过 Portal 认证后，可以访问外部网络。

(2) 采用 RADIUS 服务器作为认证/计费服务器。

4. 配置过程和解释

在接入设备上进行以下配置。

(1) 配置 RADIUS 方案。

① 创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<Switch> system-view
[Switch] radius scheme rs1
```

② 配置 RADIUS 方案的服务器类型为 extended。

```
[Switch-radius-rs1] server-type extended
```

③ 配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Switch-radius-rs1] primary authentication 192.168.0.112
[Switch-radius-rs1] primary accounting 192.168.0.112
[Switch-radius-rs1] key authentication radius
[Switch-radius-rs1] key accounting radius
```

④ 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[Switch-radius-rs1] user-name-format without-domain
[Switch-radius-rs1] quit
```

(2) 配置认证域。

① 创建并进入名字为 dm1 的 ISP 域。

```
[Switch] domain dm1
```

② 配置 ISP 域的 RADIUS 方案 rs1。

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
[Switch-isp-dm1] authorization portal radius-scheme rs1
[Switch-isp-dm1] accounting portal radius-scheme rs1
[Switch-isp-dm1] quit
```

③ 配置系统默认的 ISP 域 dm1，所有接入用户共用此默认域的认证和计费方式。

```
[Switch] domain default enable dm1
```

(3) 配置 Portal 认证。

① 配置 Portal 服务器。名称为 newpt，IP 地址为 192.168.0.111，密钥为 portal，端口为 50100，URL 为 http://192.168.0.111/portal。

```
[Switch] portal server newpt ip 192.168.0.111 key portal port 50100 url http://192.168.0.111/portal
```

② 在与用户 Host 相连的接口上使能 Portal 认证。

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 2.2.2.1 255.255.255.0
[Switch-Vlan-interface100] portal server newpt method direct
[Switch] quit
```

③ 配置与服务器通信的接口 IP 地址。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch-Vlan-interface2] quit
```

提示：Portal 没有形成统一的标准，各个厂商都有类似的功能，但具体协议实现可能不同，因此需要专门的 Portal 服务器与设备配合，需要配置对应的 Portal 服务器。H3C 的 Portal 服务器有 CAMS 和 iMC。

设备向 Portal 服务器主动发送报文时使用的目的端口号必须与远程 Portal 服务器实际使用的端口号保持一致。

12.4.2 Portal 二次地址分配认证方式典型配置指导

1. 背景

IT 维护信息部门的主管又提出了一个新的要求：为尽可能保护公司的信息安全，希望能够通过认证的方式对研发部门的网络访问实施内外网的隔离，只有有外网访问权限的研发人员才能访问外网。经过分析，了解到 Portal 认证有一种二次地址分配的方式可以满足这个需求。具体实现原理为：将研发人员的网络 IP 网段划分为私网 IP 和公网 IP 两部分，正常情况下只能获取私网地址，无法访问公网；需要进行公网访问的人员需申请公网账号，对公网账号的用户采用 Portal 二次地址分配的方式。

2. 组网图

图 12-13 所示为 Portal 二次地址分配认证方式典型配置组网图。

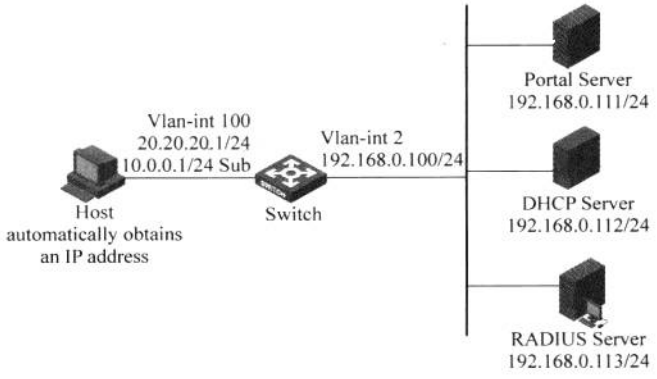


图 12-13 Portal 二次地址分配认证方式典型配置组网图

3. 配置需求

(1) 配置交换机采用二次地址分配方式的 Portal 认证。用户通过 DHCP 服务器获取 IP 地址，Portal 认证前分配一个私网地址；通过 Portal 认证后，用户申请到一个公网地址，才可以访问外部网络。

(2) 采用 RADIUS 服务器作为认证/计费服务器。

4. 配置过程和解释

说明：

(1) Portal 二次地址分配认证方式应用中，DHCP 服务器上需创建公网地址池(20.20.

20.0/24)及私网地址池(10.0.0.0/24),具体配置略。

(2) Portal 二次地址分配认证方式应用中,接入设备必须配置为 DHCP 中继(不能配置为 Server),且启动 Portal 的接口需要配置主 IP 地址(公网 IP)及从 IP 地址(私网 IP)。

在接入设备上进行以下配置。

(1) 配置 Portal 服务器。名称为 newpt,IP 地址为 192.168.0.111,密钥为 portal,端口为 50100,URL 为 http://192.168.0.111/portal。

```
<Switch> system-view
[Switch] portal server newpt ip 192.168.0.111 key portal port 50100 url http://192.168.0.
111/portal
```

(2) 配置 DHCP 中继,并启动 DHCP 中继的安全地址匹配检查功能。

```
[Switch] dhcp enable
[Switch] dhcp relay server-group 0 ip 192.168.0.112
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 20.20.20.1 255.255.255.0
[Switch-Vlan-interface100] ip address 10.0.0.1 255.255.255.0 sub
[Switch-Vlan-interface100] dhcp select relay
[Switch-Vlan-interface100] dhcp relay server-select 0
[Switch-Vlan-interface100] dhcp relay address-check enable
```

(3) 在与用户 Host 相连的接口上使能 Portal 认证。

```
[Switch-Vlan-interface100] portal server newpt method redhcp
[Switch-Vlan-interface100] quit
```

(4) 配置与服务器通信的接口 IP 地址。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch-Vlan-interface2] quit
```

12.4.3 三层 Portal 认证方式典型配置指导

三层认证方式和非三层认证方式的不同有以下两点。

(1) 组网方式不同。三层认证方式的认证客户端和接入设备之间可以跨接三层转发设备;非三层认证方式则要求认证客户端和接入设备之间没有三层转发。

(2) 用户标识不同。由于三层认证可以跨接三层设备,而接入设备不会学习认证客户端的 MAC 地址信息,所以其是以 IP 地址唯一标识用户的;而非三层认证方式中的接入设备则可以学习到认证客户端的 MAC 地址,所以其是以 IP 和 MAC 地址的组合来唯一标识用户的。

以上不同的组网方式和用户标识有以下两种特点。

(1) 认证客户端的 MAC 地址不变、IP 地址改变时,在三层认证方式下会激发新的 Portal 认证。

(2) 而在非三层认证方式下不会激发新的 Portal 认证。只有认证客户端的 MAC 地址和 IP 地址同时改变时,非三层认证方式下才会激发新的 Portal 认证。

1. 背景

M公司网络建成较久，有不少二层交换机不能支持Portal功能。如果将这些交换机都直接淘汰，预算又不足，也没有必要。经过研究，M公司找出了解决方案。

Portal认证方式可以分为二层Portal认证和三层Portal认证。如果Portal用户和Portal设备之间是二层网络，可以采用二层Portal认证；当Portal用户和Portal设备间是三层网络时，可以采用三层Portal的认证方式。

2. 组网图

图12-14所示为三层Portal认证方式典型配置组网图。

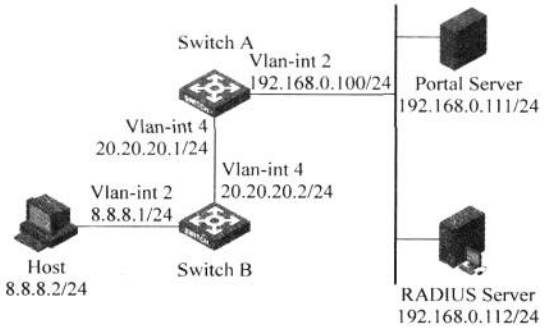


图12-14 三层Portal认证方式典型配置组网图

3. 配置需求

Switch A支持Portal认证功能。用户Host通过Switch B接入到Switch A。

(1) 配置Switch A采用三层Portal认证。用户在未通过Portal认证前，只能访问Portal服务器；通过Portal认证后，可以访问外部网络。

(2) 采用RADIUS服务器作为认证/计费服务器。

4. 配置过程和解释

在Switch A上进行以下配置。

(1) 配置Portal服务器。名称为newpt，IP地址为192.168.0.111，密钥为portal，端口为50100，URL为http://192.168.0.111/portal。

```
<SwitchA> system-view
[SwitchA] portal server newpt ip 192.168.0.111 key portal port 50100 url http://192.168.0.
111/portal
```

(2) 在与Switch B相连的接口上使能Portal认证。

```
[SwitchA] interface vlan-interface 4
[SwitchA-Vlan-interface4] ip address 20.20.20.1 255.255.255.0
[SwitchA-Vlan-interface4] portal server newpt method layer3
[SwitchA-Vlan-interface4] quit
```

(3) 配置与服务器通信的接口IP地址。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
```

[Switch-Vlan-interface2] quit

Switch B 上需要配置到 192.168.0.0/24 网段的默认路由，下一跳为 20.20.20.1，具体配置略。

12.4.4 Portal 直接认证方式(支持 EAD)典型配置指导

1. 背景

M 公司网络添加了 Portal 认证之后，又开始实施对 Portal 认证的用户部署 EAD 解决方案。这样做的好处是能够大大提升 Portal 终端接入的安全，且能通过 ACL 的下发做到灵活控制用户对网络资源的访问。

部署 Portal EAD 需要在终端安装 iNode 客户端和 H3C iMC 服务器配合。

2. 组网图

图 12-15 所示为 Portal 直接认证方式(支持 EAD)典型配置组网图。

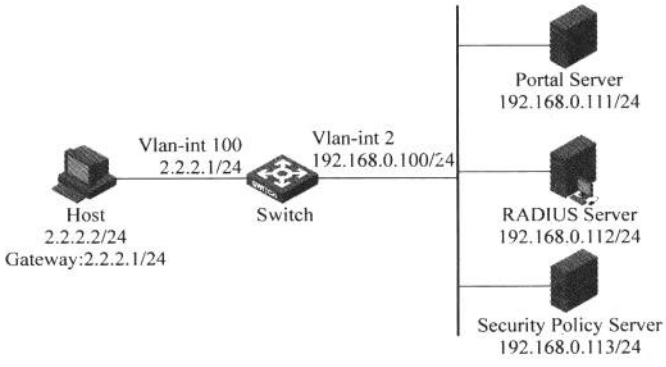


图 12-15 Portal 直接认证方式(支持 EAD)典型配置组网图

3. 配置需求

(1) 配置交换机采用直接方式的 Portal 认证，开启 EAD 认证。用户在通过身份认证而没有通过安全认证时可以访问 192.168.0.0/24 网段；用户通过安全认证后，可以随意访问外部网络。

(2) 采用 RADIUS 服务器作为认证/计费服务器。

(3) 需要配置安全策略服务器。

4. 配置过程和解释

在接入设备上进行以下配置。

(1) 配置 RADIUS 方案。

① 创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<Switch> system-view
[Switch] radius scheme rs1
```

② 配置 RADIUS 方案的服务器类型为 extended。

```
[Switch-radius-rs1] server-type extended
```

③ 配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Switch-radius-rs1] primary authentication 192.168.0.112
[Switch-radius-rs1] primary accounting 192.168.0.112
[Switch-radius-rs1] key accounting radius
[Switch-radius-rs1] key authentication radius
[Switch-radius-rs1] user-name-format without-domain
```

④ 配置 RADIUS 方案的安全策略服务器。

```
[Switch-radius-rs1] security-policy-server 192.168.0.113
[Switch-radius-rs1] quit
```

(2) 配置认证域。

① 创建并进入名字为 dm1 的 ISP 域。

```
[Switch] domain dm1
```

② 配置 ISP 域的 RADIUS 方案 rs1。

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
[Switch-isp-dm1] authorization portal radius-scheme rs1
[Switch-isp-dm1] accounting portal radius-scheme rs1
[Switch-isp-dm1] quit
```

③ 配置系统默认的 ISP 域 dm1,所有接入用户共用此默认域的认证和计费方式。

```
[Switch] domain default enable dm1
```

(3) 配置受限资源对应的 ACL 为 3000,非受限资源对应的 ACL 为 3001。

```
[Switch] acl number 3000
[Switch-acl-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
[Switch-acl-adv-3000] quit
[Switch] acl number 3001
[Switch-acl-adv-3001] rule permit ip
[Switch-acl-adv-3001] quit
```

(4) 配置 Portal 认证。

① 配置 Portal 服务器。名称为 newpt,IP 地址为 192.168.0.111,密钥为 portal,端口为 50100,URL 为 http://192.168.0.111/portal。

```
[Switch] portal server newpt ip 192.168.0.111 key portal port 50100 url http://192.168.0.111/portal
```

② 在与用户 Host 相连的接口上使能 Portal 认证。

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 2.2.2.1 255.255.255.0
[Switch-Vlan-interface100] portal server newpt method direct
[Switch] quit
```

③ 配置与服务器通信的接口 IP 地址。

```
[Switch] interface vlan-interface 2
```

[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0

提示：安全策略服务器上需要将 ACL 3000 和 ACL 3001 分别指定为隔离 ACL 和安全 ACL。

安全策略服务器的相关配置可参考 H3C 网站上相关文档。

12.5 端口安全典型配置指导

端口安全是一种基于 MAC 地址对网络接入进行控制的安全机制，是对已有的 802.1x 认证和 MAC 地址认证的扩充。这种机制通过检测端口收到的数据帧中的源 MAC 地址来控制非授权设备对网络的访问，通过检测从端口发出的数据帧中的目的 MAC 地址来控制对非授权设备的访问。

端口安全的主要功能是通过定义各种端口安全模式，让设备学习到合法的源 MAC 地址，以达到相应的网络管理效果。启动了端口安全功能之后，当发现非法报文时，系统将触发相应特性，并按照预先指定的方式进行处理，既方便用户的管理，又提高了系统的安全性。

12.5.1 端口安全 autolearn 模式典型配置指导

在端口安全 autolearn 模式下，端口学习到的 MAC 地址被保存在安全 MAC 地址表项中。当端口下的安全 MAC 地址数超过端口允许学习的最大安全 MAC 地址数后，端口模式会自动转变为 secure 模式。之后，该端口不会再添加新的安全 MAC，只有源 MAC 地址为安全 MAC 地址、已配置的静态 MAC 地址的报文，才能通过该端口。

1. 背景

M 公司的 A 办事处向总部的 IT 维护人员提出了一个新的需求，办事处为了加强网络的安全性，拟限制设备端口接入用户的数量，并且希望将用户的 MAC 地址静态绑定为安全 MAC，并当达到最大接入数量时，不再允许新的 PC 接入到此端口。

IT 维护人员决定采用 H3C 设备支持的端口安全 autolearn 模式来实现此需求。

2. 组网图

图 12-16 所示为端口安全 autolearn 模式典型配置组网图。

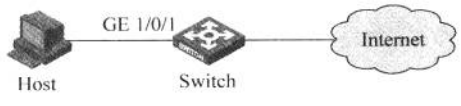


图 12-16 端口安全 autolearn 模式典型配置组网图

3. 配置需求

在交换机的端口 GigabitEthernet 1/0/1 上对接入用户做如下的限制。

(1) 允许 64 个用户自由接入，不进行认证，将学习到的用户 MAC 地址添加为安全 MAC 地址。

(2) 当安全 MAC 地址数量达到 64 后，停止学习；当再有新的 MAC 地址接入时，触发入侵检测，并将此端口关闭 30s。

4. 配置过程和解释

(1) 使能端口安全功能。

```
<Switch> system-view
[Switch] port-security enable
```

(2) 打开入侵检测 Trap 开关。

```
[Switch] port-security trap intrusion
```

(3) 设置端口允许的最大安全 MAC 地址数为 64。

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-security max-mac-count 64
```

(4) 设置端口安全模式为 autolearn。

```
[Switch-GigabitEthernet1/0/1] port-security port-mode autolearn
```

(5) 设置触发入侵检测特性后的保护动作为暂时关闭端口,关闭时间为 30s。

```
[Switch-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
[Switch-GigabitEthernet1/0/1] quit
[Switch] port-security timer disableport 30
```

上述配置完成后,可以用 display 命令显示端口安全配置情况。

```
<Switch> display port-security interface GigabitEthernet 1/0/1
  Equipment port-security is enabled
  Intrusion trap is enabled
  Disableport Timeout: 30s
  OUI value:
GigabitEthernet 1/0/1 is link-up
    Port mode is autolearn
    NeedToKnow mode is disabled
    Intrusion Protection mode is DisablePortTemporarily
    Max MAC address number is 64
    Stored MAC address number is 0
    Authorization is permitted
```

可以看到端口的最大安全 MAC 数为 64,端口模式为 autolearn,入侵检测 Trap 开关打开,入侵保护动作为 DisablePortTemporarily,入侵发生后端口禁用时间为 30s。

配置完成后,允许地址学习,学习到的 MAC 地址数可以用上述命令显示,如学习到 5 个,那么存储的安全 MAC 地址数就为 5。可以在端口视图下用 display this 命令查看学习到的 MAC 地址,例如:

```
<Switch> system-view
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet 1/0/1
 port-security max-mac-count 64
```

```
port-security port-mode autolearn
port-security mac-address security 0002-0000-0015 vlan 1
port-security mac-address security 0002-0000-0014 vlan 1
port-security mac-address security 0002-0000-0013 vlan 1
port-security mac-address security 0002-0000-0012 vlan 1
port-security mac-address security 0002-0000-0011 vlan 1
#
```

当学习到的 MAC 地址数达到 64 后，用命令 display port-security interface 可以看到端口模式变为 secure，再有新的 MAC 地址到达将触发入侵保护，Trap 信息如下：

```
#May 2 03:15:55:871 2000 Switch PORTSEC/1/VIOLATION:Traph3cSecureViolation
A intrusion occurs!
IfIndex: 9437207
Port: 9437207
MAC Addr: 0.2.0.0.0.21
VLAN ID: 1
IfAdminStatus: 1
```

并且可以通过下述命令看到端口安全将此端口关闭。

```
<Switch-GigabitEthernet1/0/1> display interface GigabitEthernet 1/0/1
GigabitEthernet 1/0/1 current state: Port Security Disabled
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-cb00-5558
Description: GigabitEthernet 1/0/1 Interface
...
```

30s 后，端口状态恢复。

```
[Switch-GigabitEthernet1/0/1] display interface GigabitEthernet 1/0/1
GigabitEthernet 1/0/1 current state: UP
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-cb00-5558
Description: GigabitEthernet 1/0/1 Interface
...
```

此时，如手动删除几条安全 MAC 地址后，端口安全的状态重新恢复为 autolearn，可以继续学习 MAC 地址。

注意：在使能端口安全功能之前，需要关闭全局的 802.1x 和 MAC 地址认证功能。

当多个用户通过认证时，端口下所允许的最大用户数根据不同的端口安全模式，取最大安全 MAC 地址数与相应模式下允许认证用户数的最小值。

12.5.2 端口安全 userLoginWithOUI 模式典型配置指导

端口安全除了提供 autolearn 方式之外，还提供了多种安全模式，在功能上可以涵盖 802.1x 和 MAC 地址认证，并且可以选择 802.1x 和 MAC 地址认证的不同组合来加强网络的安全性。

在 userLoginWithOUI 模式下，端口上除了允许 802.1x 认证用户接入之外，还额外允许特殊用户接入，该用户报文的源 MAC 的 OUI 需要与设备上配置的 OUI 值相符。

1. 背景

M 公司随着业务的扩展，新建了 800 热线服务部门，部门内的 PC 和 IP Phone 都连接

到接入交换机的同一个端口，在端口开启对 802.1x 认证后，发现 IP Phone 发出的报文无法通过。针对这种场景，IT 维护部门决定采用端口安全的 userLoginWithOUI。在此模式下，将 IP Phone 的 OUI 添加到设备上后，端口可以允许指定 OUI 的源 MAC 地址的报文通过。

2. 组网图

图 12-17 所示为端口安全 userLoginWithOUI 模式典型配置组网图。

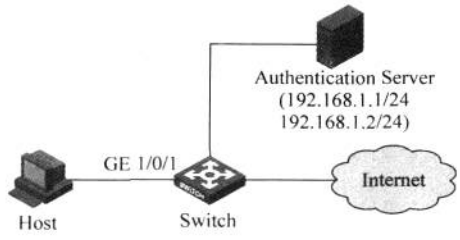


图 12-17 端口安全 userLoginWithOUI 模式典型配置组网图

3. 配置需求

客户端通过端口 GigabitEthernet 1/0/1 连接到交换机上，交换机通过 RADIUS 服务器对客户端进行身份认证，如果认证成功，客户端被授权允许访问 Internet 资源。

交换机的管理者希望对接入用户的端口 GigabitEthernet 1/0/1 做如下限制。

(1) 允许一个 802.1x 用户上线。

(2) 最多可以配置 16 个 OUI 值，还允许端口上有一个与 OUI 值匹配的 MAC 地址用户通过。

4. 配置过程和解释

(1) 配置 RADIUS 协议。

① 创建名为 radsun 的 RADIUS 方案。

```
<Switch> system-view
[Switch] radius scheme radsun
```

② 设置主认证 RADIUS 服务器的 IP 地址为 192.168.1.1，主计费 RADIUS 服务器的 IP 地址为 192.168.1.2。

```
[Switch-radius-radsun] primary authentication 192.168.1.1
[Switch-radius-radsun] primary accounting 192.168.1.2
```

③ 设置从认证 RADIUS 服务器的 IP 地址为 192.168.1.2，从计费 RADIUS 服务器的 IP 地址为 192.168.1.1。

```
[Switch-radius-radsun] secondary authentication 192.168.1.2
[Switch-radius-radsun] secondary accounting 192.168.1.1
```

④ 设置与认证 RADIUS 服务器交互报文时的加密密码为 name。

```
[Switch-radius-radsun] key authentication name
```

⑤ 设置与计费 RADIUS 服务器交互报文时的加密密码为 money。

```
[Switch-radius-radsun] key accounting money
```

⑥ 设置 RADIUS 服务器应答超时时间为 5s，RADIUS 报文的超时重传次数的最大值为 5。

```
[Switch-radius-radsun] timer response-timeout 5
[Switch-radius-radsun] retry 5
```

⑦ 设置向 RADIUS 服务器发送实时计费报文的时间间隔为 15min。

```
[Switch-radius-radsun] timer realtime-accounting 15
```

⑧ 设置将去除域名的用户名发送给 RADIUS 服务器。

```
[Switch-radius-radsun] user-name-format without-domain
[Switch-radius-radsun] quit
```

⑨ 创建名为 sun 的 ISP 域，并进入其视图。

```
[Switch] domain sun
```

⑩ 指定名为 radsun 的 RADIUS 方案为该域用户的默认 RADIUS 方案。

```
[Switch-isp-sun] authentication default radius-scheme radsun
```

⑪ 设置该 ISP 域最多可容纳 30 个用户。

```
[Switch-isp-sun] access-limit enable 30
[Switch-isp-sun] quit
```

(2) 配置端口安全特性。

① 使能端口安全功能。

```
[Switch] port-security enable
```

② 添加 5 个 OUI 值。

```
[Switch] port-security oui 1234-0100-1111 index 1
[Switch] port-security oui 1234-0200-1111 index 2
[Switch] port-security oui 1234-0300-1111 index 3
[Switch] port-security oui 1234-0400-1111 index 4
[Switch] port-security oui 1234-0500-1111 index 5
[Switch] interface GigabitEthernet 1/0/1
```

③ 设置端口安全模式为 userLoginWithOUI。

```
[Switch-GigabitEthernet1/0/1] port-security port-mode userlogin-withoui
```

(3) 验证配置结果。

① 查看名为 radsun 的 RADIUS 方案的配置信息。

```
<Switch> display radius scheme radsun
SchemeName = radsun
```

```
Index = 0                              Type = standard
Primary Auth IP   = 192.168.1.1        Port = 1812   State = active
Primary Acct IP   = 192.168.1.2        Port = 1813   State = active
Second  Auth IP   = 192.168.1.2        Port = 1812   State = active
Second  Acct IP   = 192.168.1.1        Port = 1813   State = active
Auth Server Encryption Key = name
Acct Server Encryption Key = money
Accounting-On packet disable, send times = 5 , interval = 3s
Interval for timeout(second)                          = 5
Retransmission times for timeout                      = 5
Interval for realtime accounting(minute)              = 15
Retransmission times of realtime-accounting packet    = 5
Retransmission times of stop-accounting packet        = 500
Quiet-interval(min)                                   = 5
Username format                                       = without-domain
Data flow unit                                        = Byte
Packet unit                                           = one
```

② 查看名为 sun 的 ISP 域的配置信息。

```
<Switch> display domain sun
  Domain = sun
  State = Active
  Access-limit = 30
  Accounting method = Required
  Default authentication scheme      : radius=radsun
  Default authorization scheme       : local
  Default accounting scheme          : local
  Domain User Template:
  Idle-cut = Disable
  Self-service = Disable
```

③ 查看端口安全的配置信息。

```
<Switch> display port-security interface GigabitEthernet 1/0/1
  Equipment port-security is enabled
  Trap is disabled
  Disableport Timeout: 20s
  OUI value:
    Index is 1,   OUI value is 123401
    Index is 2,   OUI value is 123402
    Index is 3,   OUI value is 123403
    Index is 4,   OUI value is 123404
    Index is 5,   OUI value is 123405
  GigabitEthernet 1/0/1 is link-up
    Port mode is userLoginWithOUI
    NeedToKnow mode is disabled
    Intrusion Protection mode is NoAction
    Max MAC address number is not configured
    Stored MAC address number is 0
    Authorization is permitted
```

④ 配置完成后，如果有 802.1x 用户上线，则可以看到存储的安全 MAC 地址数为 1。还可以通过下述命令查看 802.1x 用户的情况。

```
<Switch> display dot1x interface GigabitEthernet 1/0/1
  Equipment 802.1x protocol is enabled
  CHAP authentication is enabled
Configuration: Transmit Period    30 s,   Handshake Period          15 s
               Quiet Period       60 s,   Quiet Period Timer is disabled
               Supp Timeout       30 s,   Server Timeout            100 s
               The maximal retransmitting times      2
Total maximum 802.1x user resource number is 1024 per slot
 Total current used 802.1x resource number is 1

GigabitEthernet 1/0/1   is link-up
   802.1x protocol is enabled
   Handshake is enabled
   The port is an authenticator
   Authentication Mode is Auto
   Port Control Type is Mac-based
   Guest VLAN: 0
   Max number of on-line users is 256

   EAPOL Packet: Tx 16331, Rx 102
   Sent EAP Request/Identity Packets : 16316
       EAP Request/Challenge Packets: 6
       EAP Success Packets: 4, Fail Packets: 5
   Received EAPOL Start Packets : 6
            EAPOL LogOff Packets: 2
            EAP Response/Identity Packets : 80
            EAP Response/Challenge Packets: 6
            Error Packets: 0
 1. Authenticated user : MAC address: 0002-0000-0011
   Controlled User(s) amount to 1
```

⑤ 此外，端口还允许一个与 OUI 值匹配的 MAC 地址的用户通过，可以通过下述命令查看。

```
<Switch> display mac-address interface GigabitEthernet 1/0/1
MAC ADDR      VLAN ID   STATE          PORT INDEX              AGING TIME(s)
1234-0300-0011  1       Learned        GigabitEthernet 1/0/1   AGING
  ---  1 mac address(es) found  ---
```

12.5.3 端口安全 macAddressWithRadius 模式典型配置指导

1. 背景

在端口安全的 macAddressWithRadius 模式下，交换机将在启动端口安全的端口上对接入用户采用 MAC 地址认证。接入用户只有通过 MAC 地址认证之后才能访问网络。

2. 组网图

图 12-18 所示为端口安全 macAddressWithRadius 模式典型配置组网图。

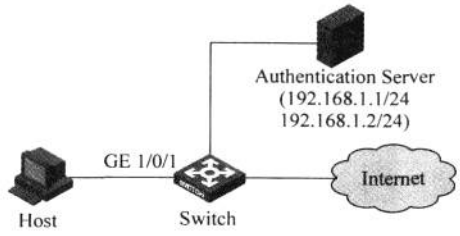


图 12-18 端口安全 macAddressWithRadius 模式典型配置组网图

3. 配置需求

客户端通过端口 GigabitEthernet 1/0/1 连接到交换机上，交换机通过 RADIUS 服务器对客户端进行身份认证。如果认证成功，客户端被授权允许访问 Internet 资源。

交换机的管理者希望对接入用户的端口 GigabitEthernet 1/0/1 做如下限制。

(1) 对接入用户进行 MAC 地址认证。

(2) 所有接入用户都属于一个默认的域 sun，MAC 地址认证时使用用户 Host 的 MAC 地址作为用户名和密码。

(3) 对未通过 MAC 认证的报文，触发入侵检测特性，丢弃源地址是此 MAC 地址的报文，保证该端口的安全性。

4. 配置过程和解释

(1) 配置 RADIUS 协议。

① 创建名为 radsun 的 RADIUS 方案。

```
<Switch> system-view
[Switch] radius scheme radsun
```

② 设置主认证 RADIUS 服务器的 IP 地址为 192.168.1.1，主计费 RADIUS 服务器的 IP 地址为 192.168.1.2。

```
[Switch-radius-radsun] primary authentication 192.168.1.1
[Switch-radius-radsun] primary accounting 192.168.1.2
```

③ 设置从认证 RADIUS 服务器的 IP 地址为 192.168.1.2，从计费 RADIUS 服务器的 IP 地址为 192.168.1.1。

```
[Switch-radius-radsun] secondary authentication 192.168.1.2
[Switch-radius-radsun] secondary accounting 192.168.1.1
```

④ 设置与认证 RADIUS 服务器交互报文时的加密密码为 name。

```
[Switch-radius-radsun] key authentication name
```

⑤ 设置与计费 RADIUS 服务器交互报文时的加密密码为 money。

```
[Switch-radius-radsun] key accounting money
```

⑥ 设置 RADIUS 服务器应答超时时间为 5s，RADIUS 报文的超时重传次数的最大值为 5。

```
[Switch-radius-radsun] timer response-timeout 5
[Switch-radius-radsun] retry 5
```

⑦ 设置向 RADIUS 服务器发送实时计费报文的时间间隔为 15min。

```
[Switch-radius-radsun] timer realtime-accounting 15
```

⑧ 设置将去除域名的用户名发送给 RADIUS 服务器。

```
[Switch-radius-radsun] user-name-format without-domain
[Switch-radius-radsun] quit
```

⑨ 创建名为 sun 的 ISP 域，并进入其视图。

```
[Switch] domain sun
```

⑩ 指定名为 radsun 的 RADIUS 方案为该域用户的默认 RADIUS 方案。

```
[Switch-isp-sun] authentication default radius-scheme radsun
[Switch-isp-sun] quit
```

(2) 配置端口安全特性。

① 使能端口安全功能。

```
[Switch] port-security enable
```

② 配置 MAC 地址认证用户所使用的 ISP 域。

```
[Switch] mac-authentication domain sun
```

③ 设置端口允许的最大安全 MAC 地址数为 64。

```
[Switch-GigabitEthernet1/0/1] port-security max-mac-count 64
```

④ 设置端口安全模式为 macAddressWithRadius。

```
[Switch-GigabitEthernet1/0/1] port-security port-mode mac-authentication
```

⑤ 配置入侵检测特性为 blockmac。

```
[Switch-GigabitEthernet1/0/1] port-security intrusion-mode blockmac
```

(3) 验证配置结果。

① 查看端口安全的配置信息。

```
<Switch> display port-security interface GigabitEthernet 1/0/1
  Equipment port-security is enabled
  Trap is disabled
  Disableport Timeout: 20s
  OUI value:
  GigabitEthernet 1/0/1 is link-up
    Port mode is macAddressWithRadius
    NeedToKnow mode is disabled
    Intrusion Protection mode is BlockMacAddress
    Max MAC address number is 64
```

```
    Stored MAC address number is 1
    Authorization is permitted
```

② 查看 MAC 地址认证情况。

```
<Switch> display mac-authentication interface GigabitEthernet 1/0/1
MAC address authentication is enabled.
 User name format is MAC address, like xxxxxxxxxxxx
 Fixed username:mac
 Fixed password:not configured
        Offline detect period is 300s
        Quiet period is 60s
        Server response timeout value is 100s
        The max allowed user number is 1024 per slot
        Current user number amounts to 1
        Current domain is sun
Silent MAC User info:
        MAC Addr          From Port                Port Index

GigabitEthernet 1/0/1 is link-up
  MAC address authentication is enabled
  Authenticate success: 1, failed: 0
  Current online user number is 1
        MAC Addr          Authenticate State                  Auth Index
        000f-3d80-2b38    MAC_AUTHENTICATOR_SUCCESS           11
```

此外，因为配置了入侵检测特性为 blockmac，对未通过 MAC 认证的报文，触发入侵检测特性，丢弃源地址是此 MAC 地址的报文，保证该端口的安全性。

12.5.4 端口安全 macAddressElseUserLoginSecure 模式典型配置指导

在端口安全 macAddressElseUserLoginSecure 模式下，端口同时处于 macAddressWithRadius 模式和 userLoginSecure 模式，用户需要通过 MAC 认证或 802.1x 认证两者中的一种之后才能正常访问网络，但 MAC 地址认证优先级大于 802.1x 认证。对于非 802.1x 报文直接进行 MAC 地址认证，对于 802.1x 报文先进行 MAC 地址认证，如果 MAC 地址认证失败再进行 802.1x 认证。

1. 背景

M 公司的 IT 维护人员进一步考虑既然能够通过端口安全实现 MAC 地址认证，能否在端口下既做 MAC 地址认证又做 dot1x 认证呢？这样在配置的时候，就不用去考虑端口下连接的终端具体是做何种认证了，减少了维护人员的工作量。他们查阅了 H3C 交换机操作手册之后，发现端口安全 macAddressElseUserLoginSecure 模式满足需求。

2. 组网图

图 12-19 所示为端口安全 macAddressElseUserLoginSecure 模式典型配置组网图。

3. 配置需求

客户端通过端口 GigabitEthernet 1/0/1 连接到交换机上，交换机通过 RADIUS 服务器对客户端进行身份认证。如果认证成功，客户端被授权允许访问 Internet 资源。

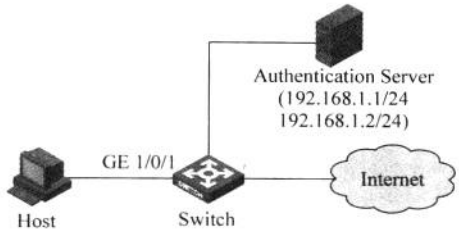


图 12-19 端口安全 macAddressElseUserLoginSecure 模式典型配置组网图

交换机的管理者希望对接入用户的端口 GigabitEthernet 1/0/1 做如下的限制。

(1) 可以有多个 MAC 认证用户上线。

(2) 如果是 802.1x 用户请求认证，先进行 MAC 地址认证，MAC 地址认证失败，再进行 802.1x 认证。802.1x 用户限制为 1 个。

(3) MAC 地址认证设置用户名格式为自定义用户名和密码的形式，上线的 MAC 地址认证用户和 802.1x 认证用户总和不能超过 64 个。

(4) 为防止报文发往未知目的 MAC 地址，启动 NeedToKnow 特性。

4. 配置过程和解释

(1) 配置 RADIUS 协议。

① 创建名为 radsun 的 RADIUS 方案。

```
<Switch> system-view
[Switch] radius scheme radsun
```

② 设置主认证 RADIUS 服务器的 IP 地址为 192.168.1.1，主计费 RADIUS 服务器的 IP 地址为 192.168.1.2。

```
[Switch-radius-radsun] primary authentication 192.168.1.1
[Switch-radius-radsun] primary accounting 192.168.1.2
```

③ 设置从认证 RADIUS 服务器的 IP 地址为 192.168.1.2，从计费 RADIUS 服务器的 IP 地址为 192.168.1.1。

```
[Switch-radius-radsun] secondary authentication 192.168.1.2
[Switch-radius-radsun] secondary accounting 192.168.1.1
```

④ 设置与认证 RADIUS 服务器交互报文时的加密密码为 name。

```
[Switch-radius-radsun] key authentication name
```

⑤ 设置与计费 RADIUS 服务器交互报文时的加密密码为 money。

```
[Switch-radius-radsun] key accounting money
```

⑥ 设置 RADIUS 服务器应答超时时间为 5s，RADIUS 报文的超时重传次数的最大值为 5。

```
[Switch-radius-radsun] timer response-timeout 5
[Switch-radius-radsun] retry 5
```

⑦ 设置向 RADIUS 服务器发送实时计费报文的时间间隔为 15min。

```
[Switch-radius-radsun] timer realtime-accounting 15
```

⑧ 设置将去除域名的用户名发送给 RADIUS 服务器。

```
[Switch-radius-radsun] user-name-format without-domain
[Switch-radius-radsun] quit
```

⑨ 创建名为 sun 的 ISP 域，并进入其视图。

```
[Switch] domain sun
```

⑩ 指定名为 radsun 的 RADIUS 方案为该域用户的默认 RADIUS 方案。

```
[Switch-isp-sun] authentication default radius-scheme radsun
[Switch-isp-sun] quit
```

(2) 配置端口安全特性。

① 使能端口安全功能。

```
[Switch] port-security enable
```

② 配置 MAC 地址认证用户所使用的 ISP 域。

```
[Switch] mac-authentication domain sun
```

③ 配置 MAC 认证的用户名为 aaa，密码为 123456。

```
[Switch] mac-authentication user-name-format fixed account aaa password simple 123456
[Switch] interface GigabitEthernet 1/0/1
```

④ 设置端口允许的最大安全 MAC 地址数为 64。

```
[Switch-GigabitEthernet1/0/1] port-security max-mac-count 64
```

⑤ 设置端口安全模式为 macAddressElseUserLoginSecure。

```
[Switch-GigabitEthernet1/0/1] port-security port-mode mac-else-userlogin-secure
```

⑥ 设置端口 NeedToKnow 模式为 ntkonly。

```
[Switch-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
```

(3) 验证配置结果。

① 查看端口安全的配置信息。

```
<Switch> display port-security interface GigabitEthernet 1/0/1
  Equipment port-security is enabled
  Trap is disabled
  Disableport Timeout: 20s
  OUI value:
  GigabitEthernet 1/0/1 is link-up
    Port mode is macAddressElseUserLoginSecure
    NeedToKnow mode is NeedToKnowOnly
```

```
    Intrusion Protection mode is NoAction
    Max MAC address number is 64
    Stored MAC address number is 0
    Authorization is permitted
```

② 查看 MAC 地址认证情况。

```
<Switch> display mac-authentication interface GigabitEthernet 1/0/1
MAC address authentication is enabled.
 User name format is fixed account
 Fixed username:aaa
 Fixed password:123456
        Offline detect period is 300s
        Quiet period is 60s
        Server response timeout value is 100s
        The max allowed user number is 1024 per slot
        Current user number amounts to 3
        Current domain is sun
Silent MAC User info:
        MAC Addr           From Port                    Port Index

GigabitEthernet 1/0/1 is link-up
  MAC address authentication is enabled
  Authenticate success: 3, failed: 1
  Current online user number is 3
    MAC Addr          Authenticate State                  Auth Index
    1234-0300-0011    MAC_AUTHENTICATOR_SUCCESS           13
    1234-0300-0012    MAC_AUTHENTICATOR_SUCCESS           14
    1234-0300-0013    MAC_AUTHENTICATOR_SUCCESS           15
```

③ 查看 802.1x 认证情况。

```
<Switch> display dot1x interface GigabitEthernet 1/0/1
  Equipment 802.1x protocol is enabled
  CHAP authentication is enabled
  Configuration: Transmit Period    30 s,  Handshake Period       15 s
                 Quiet Period       60 s,  Quiet Period Timer is disabled
                 Supp Timeout       30 s,  Server Timeout         100 s
                 The maximal retransmitting times     2
  EAD quick deploy configuration:
                  EAD timeout:    30 m
  The maximum 802.1x user resource number is 1024 per slot
  Total current used 802.1x resource number is 1
  GigabitEthernet 1/0/1   is link-up
    802.1x protocol is enabled
    Handshake is enabled
    The port is an authenticator
    Authentication Mode is Auto
    Port Control Type is Mac-based
    802.1x Multicast-trigger is enabled
    Guest VLAN: 0
    Max number of on-line users is 256
```

```
    EAPOL Packet: Tx 16331, Rx 102
    Sent EAP Request/Identity Packets : 16316
        EAP Request/Challenge Packets: 6
        EAP Success Packets: 4, Fail Packets: 5
    Received EAPOL Start Packets : 6
            EAPOL LogOff Packets: 2
            EAP Response/Identity Packets : 80
            EAP Response/Challenge Packets: 6
            Error Packets: 0
  1. Authenticated user : MAC address: 0002-0000-0011
    Controlled User(s) amount to 1
```

此外，因为设置了 NeedToKnow 特性，目的 MAC 地址未知、广播和多播报文都被丢弃。

12.6 SSH 典型配置指导

用户通过一个不能保证安全的网络环境远程登录到设备时，SSH(Secure Shell，安全外壳)可以利用加密和强大的认证功能提供安全保障，保护设备不受诸如 IP 地址欺诈、明文密码截取等攻击。

SSH 提供两种认证方法。

(1) password 认证：利用 AAA(Authentication，Authorization，Accounting，认证、授权、计费)对客户端身份进行认证。客户端向服务器发出 password 认证请求，将用户名和密码加密后发送给服务器；服务器将该信息解密后得到用户名和密码的明文，通过本地认证或远程认证验证用户名和密码的合法性，并返回认证成功或失败的消息。如果远程认证服务器要求用户进行二次密码认证，则会在发送给服务器的认证回应消息中携带一个提示信息，该提示信息被服务器透传给客户端，由客户端输出并要求用户再次输入一个指定类型的密码，当用户提交正确的密码并成功通过认证服务器的验证后，服务器才会返回认证成功的消息。

(2) publickey 认证：采用数字签名的方法来认证客户端。目前，设备上可以利用 DSA 和 RSA 两种公钥算法实现数字签名。客户端发送包含用户名、公钥和公钥算法的 publickey 认证请求给服务器。服务器对公钥进行合法性检查，如果不合法，则直接发送失败消息；否则，服务器利用数字签名对客户端进行认证，并返回认证成功或失败的消息。

H3C 设备既可以作为 SSH 的客户端，也可以作为 SSH 服务器。

SFTP(Secure FTP)是 SSH 2.0 中新增的功能。

SFTP 建立在 SSH 连接的基础之上，它使得远程用户可以安全地登录设备，进行文件管理和文件传送等操作，为数据传输提供了更高的安全保障。同时，由于设备支持作为客户端的功能，用户可以从本地设备安全登录到远程设备上，进行文件的安全传输。

12.6.1 设备作为 SSH 服务器并采用 password 认证时的典型配置指导

1. 背景

M 公司在整网部署了 EAD 解决方案之后，请 H3C 网络安全专家对全网的安全性能进

行了评估。H3C 安全专家发现 M 公司对设备远程管理时采用的都是 Telnet 的登录验证方式，这种方式下用户名和密码都是明文传输，存在用户名、密码泄露的危险。H3C 安全专家建议远程管理设备采用 SSH 的方式。

2. 组网图

图 12-20 所示为设备作为 SSH 服务器并采用 password 认证时的典型配置组网图。

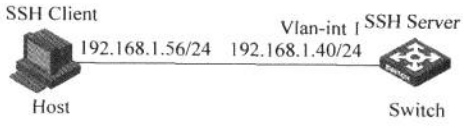


图 12-20 设备作为 SSH 服务器并采用 password 认证时的典型配置组网图

3. 配置需求

如图 12-20 所示，配置 Host(SSH 客户端)与 Switch 建立本地连接。Host 采用 SSH 协议登录到 Switch 上，以保证数据信息交换的安全。SSH 用户采用的认证方式为 password 认证。

4. 配置过程和解释

(1) 配置 SSH 服务器 Switch。生成 RSA 及 DSA 密钥对，并启动 SSH 服务器。

```
<Switch> system-view
[Switch] public-key local create rsa
[Switch] public-key local create dsa
[Switch] ssh server enable
```

注意： *生成服务器的 RSA 和 DSA 密钥对是完成 SSH 登录的必要操作。*

① 配置 VLAN 接口 1 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface1] quit
```

② 设置 SSH 客户端登录用户界面的认证方式为 AAA 认证。

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
```

③ 设置 Switch 上远程用户登录协议为 SSH。

```
[Switch-ui-vty0-4] protocol inbound ssh
[Switch-ui-vty0-4] quit
```

④ 创建本地用户 client001，并设置用户访问的命令级别为 3。

```
[Switch] local-user client001
[Switch-luser-client001] password simple aabbcc
[Switch-luser-client001] service-type ssh level 3
[Switch-luser-client001] quit
```

⑤ 配置 SSH 用户 client001 的服务类型为 Stelnet，认证方式为 password 认证。

[Switch] ssh user client001 service-type stelnet authentication-type password

(2) 配置 SSH 客户端 Host。

说明：SSH 客户端软件有很多，如 PuTTY、OpenSSH 等。本文中仅以客户端软件 PuTTY0.58 为例，说明 SSH 客户端的配置方法。

建立与 SSH 服务器的连接。打开 PuTTY.exe 程序，出现如图 12-21 所示的“SSH 客户端配置”界面。在 Host Name(or IP address)文本框中输入 SSH 服务器的 IP 地址为 192.168.1.40。

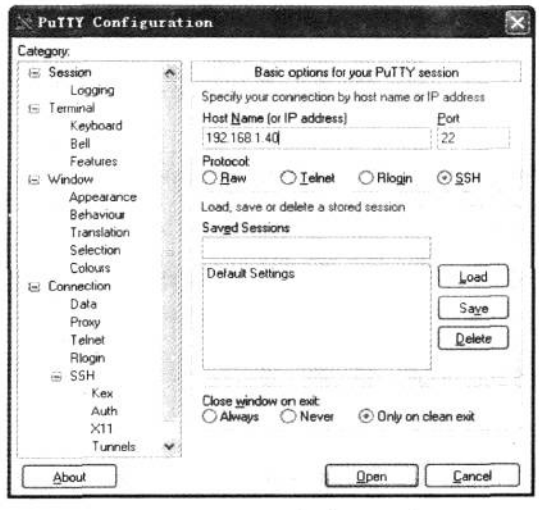


图 12-21 “SSH 客户端配置”界面

在图 12-21 中，单击 Open 按钮，按提示输入用户名 client001 及密码 aabbcc，即可进入 Switch 的配置界面。

提示：对于只支持 RSA 密钥的设备，作为服务器时只用生成 RSA 密钥对。

SSH 客户端通过 publickey 和 password 两种方式进行认证尝试的次数总和，不能超过 ssh server authentication-retries 命令配置的 SSH 连接认证尝试次数，否则客户端认证失败，无法登录 SSH 服务器。

12.6.2 设备作为 SSH 服务器并采用 publickey 认证(认证密钥算法为 RSA)时的典型配置指导

1. 背景

另外，SSH 还可以采用 publickey 认证，即采用数字签名的方法来认证客户端，具有更高的安全性。M 公司后来采用了 publickey 认证。

2. 组网图

图 12-22 所示为设备作为 SSH 服务器并采用 publickey 认证(认证密钥算法为 RSA)时的典型配置组网图。

3. 配置需求

如图 12-22 所示，配置 Host(SSH 客户端)与 Switch 建立本地连接。Host 采用 SSH

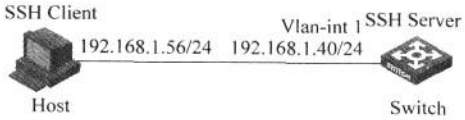


图 12-22 设备作为 SSH 服务器并采用 publickey 认证(认证密钥算法为 RSA)时的典型配置组网图

协议登录到 Switch 上,以保证数据信息交换的安全。SSH 用户采用的认证方式为 publickey 认证,认证时采用的公共密钥算法为 RSA。

4. 配置过程和解释

(1) 配置 SSH 服务器 Switch。

① 生成 RSA 及 DSA 密钥对,并启动 SSH 服务器。

```
<Switch> system-view
[Switch] public-key local create rsa
[Switch] public-key local create dsa
[Switch] ssh server enable
```

注意:生成服务器的 RSA 和 DSA 密钥对是完成 SSH 登录的必要操作。

② 配置 VLAN 接口 1 的 IP 地址,客户端将通过该地址连接 SSH 服务器。

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface1] quit
```

③ 设置用户接口上认证模式为 AAA 认证。

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
```

④ 设置 Switch 上远程用户登录协议为 SSH。

```
[Switch-ui-vty0-4] protocol inbound ssh
```

⑤ 设置用户能访问的命令级别为 3。

```
[Switch-ui-vty0-4] user privilege level 3
[Switch-ui-vty0-4] quit
```

提示:这里需要先在 SSH 客户端使用 SSH 客户端软件生成 RSA 密钥对,将生成的 RSA 公钥保存到指定文件中,并将此公钥文件通过 FTP/TFTP 方式上传到服务器,文件名为"key.pub"。相关配置可参见客户端的配置。

⑥ 从文件 key.pub 中导入远端的公钥。

```
[Switch] public-key peer Switch001 import sshkey key.pub
```

⑦ 设置 SSH 用户 client002 的认证方式为 publickey,并指定公钥为 Switch001。

```
[Switch] ssh user client002 service-type stelnet authentication-type publickey assign publickey
Switch001
```

(2) 配置 SSH 客户端 Host。

① 生成 RSA 密钥对。

a. 在客户端运行 PuTTYGen. exe，在参数栏中选择 SSH-2 RSA 单选按钮，如图 12-23 所示，单击 Generate 按钮，产生客户端密钥对。

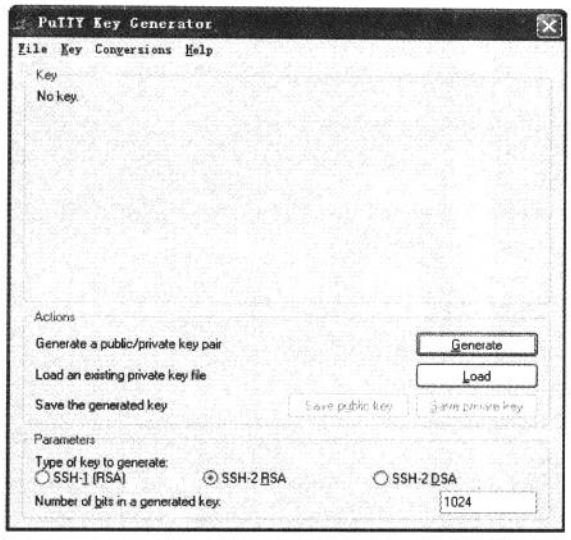


图 12-23 生成客户端密钥(1)

b. 在产生密钥对的过程中需不停地移动鼠标，鼠标移动仅限于图 12-24 蓝色框中除绿色标记进程条外的地方，否则进程条的显示会不动，密钥对将停止产生，如图 12-24 所示。

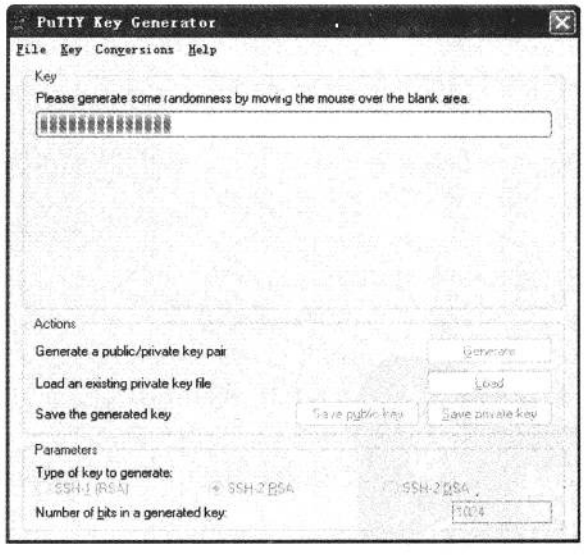


图 12-24 生成客户端密钥(2)

c. 密钥对产生后，如图 12-25 所示，单击 Save public key 按钮，输入存储公钥的文件名 key.pub，单击“保存”按钮。

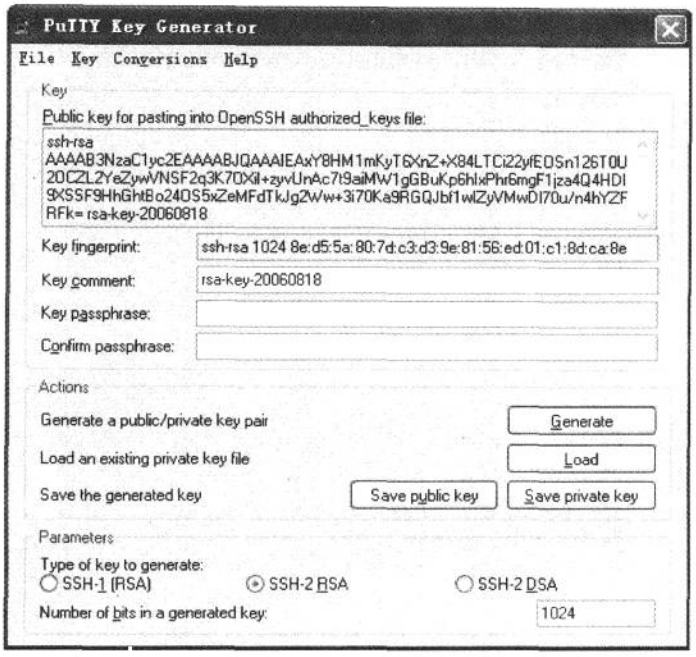


图 12-25 生成客户端密钥(3)

d. 单击 Save private key 按钮存储私钥，弹出警告框，提醒“是否保存没做任何保护措施的私钥”，如图 12-26 所示，单击 Yes 按钮，输入私钥文件名为 private，单击“保存”按钮。

说明：客户端生成密钥对后，需要将保存的公钥文件通过 FTP/TFTP 方式上传到服务器，并完成服务器的配置后，才可继续客户端的配置。

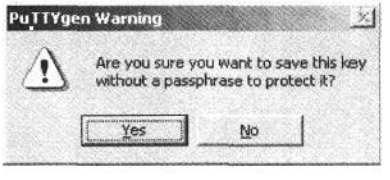


图 12-26 生成客户端密钥(4)

② 指定私钥文件，并建立与 SSH 服务器的连接。

a. 打开 PuTTY.exe 程序，出现如图 12-27 所示的“SSH 客户端配置”界面。在 Host Name(or IP address)文本框中输入 SSH 服务器的 IP 地址为 192.168.1.40。

b. 单击 SSH 下面的 Auth(认证)，出现如图 12-28 所示的界面。单击 Browse 按钮，弹出“文件选择”窗口，选择与配置到服务器的公钥对应的私钥文件 private。

c. 如图 12-28 所示，单击 Open 按钮，按提示输入用户名 client002，即可进入 Switch 的配置界面。

提示：SSH 客户端通过 publickey 和 password 两种方式进行认证尝试的次数总和，不能超过 ssh server authentication-retries 命令配置的 SSH 连接认证尝试次数，否则客户端认证失败，无法登录 SSH 服务器。

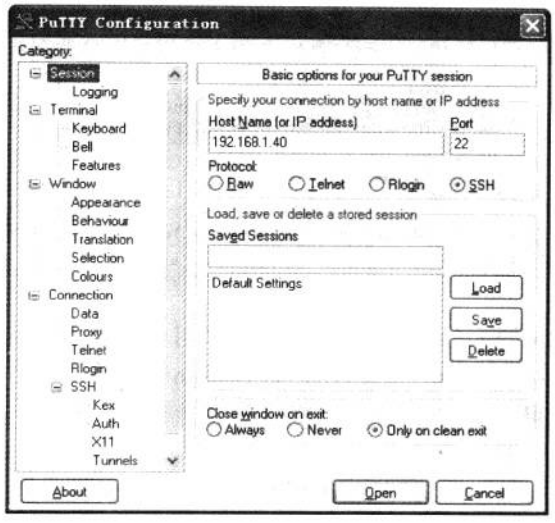


图 12-27 “SSH 客户端配置”界面(1)

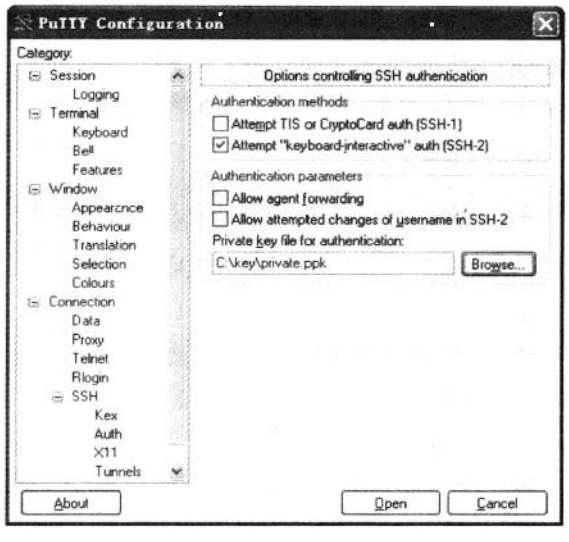


图 12-28 “SSH 客户端配置”界面(2)

12.6.3 设备作为 SSH 客户端并采用 password 认证时的典型配置指导

1. 背景

IT 维护人员配置了设备的 SSH 服务器功能之后，可以很安全地从 PuTTY、SecureCRT 等客户端登录管理设备了。但有时候为了管理方便，需要从设备 A 直接 SSH 登录到设备 B，这样设备 A 就需要作为 SSH 客户端，因此需要在设备 A 上添加 SSH 客户端的配置。

2. 组网图

图 12-29 所示为设备作为 SSH 客户端并采用 password 认证时的典型配置组网图。

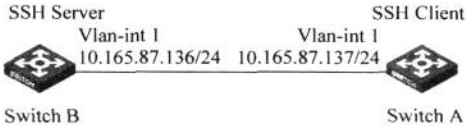


图 12-29 设备作为 SSH 客户端并采用 password 认证时的典型配置组网图

3. 配置需求

如图 12-29 所示，配置 Switch A 作为客户端，采用 SSH 协议登录到 Switch B 上。SSH 用户采用的认证方式为 password 认证，用户名为 client001，密码为 aabbcc。

4. 配置过程和解释

(1) 配置 SSH 服务器 Switch B。

① 生成 RSA 及 DSA 密钥对，并启动 SSH 服务器。

```
<SwitchB> system-view
[SwitchB] public-key local create rsa
[SwitchB] public-key local create dsa
[SwitchB] ssh server enable
```

注意：生成服务器的 RSA 和 DSA 密钥对是完成 SSH 登录的必要操作。

② 配置 VLAN 接口 1 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

③ 设置 SSH 客户端登录用户界面的认证方式为 AAA 认证。

```
[SwitchB] user-interface vty 0 4
[SwitchB-ui-vty0-4] authentication-mode scheme
```

④ 设置 Switch B 上远程用户登录协议为 SSH。

```
[SwitchB-ui-vty0-4] protocol inbound ssh
[SwitchB-ui-vty0-4] quit
```

⑤ 创建本地用户 client001。

```
[SwitchB] local-user client001
[SwitchB-luser-client001] password simple aabbcc
[SwitchB-luser-client001] service-type ssh level 3
[SwitchB-luser-client001] quit
```

⑥ 配置 SSH 用户 client001 的服务类型为 Stelnet，认证方式为 password 认证。

```
[SwitchB] ssh user client001 service-type stelnet authentication-type password
```

(2) 配置 SSH 客户端 Switch A。

① 配置 VLAN 接口 1 的 IP 地址。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

② 配置客户端对服务器不进行首次认证。

```
[SwitchA] undo ssh client first-time
```

③ 在客户端配置 SSH 服务器的 DSA 主机公钥。在“公共密钥编辑”视图输入服务器的主机公钥。

提示：因为部分以太网交换机只支持 RSA 密钥对，所以当它们作为服务器时配置到客户端的主机公钥只能为 RSA 密钥对。

```
[SwitchA] public-key peer key1
[SwitchA-pkey-public-key] public-key-code begin
[SwitchA-pkey-key-code]308201B73082012C06072A8648CE3804013082011F02818100
D757262C4584C44C211F18BD96E5F0
[SwitchA-pkey-key-code]61C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE6
5BE6C265854889DC1EDBD13EC8B274
[SwitchA-pkey-key-code]DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06
FD60FE01941DDD77FE6B12893DA76E
[SwitchA-pkey-key-code]EBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36
8950387811C7DA33021500C773218C
[SwitchA-pkey-key-code]737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
4EC474BAF2932E69D3B1F18517AD95
[SwitchA-pkey-key-code]94184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD35D024
92B3959EC6499625BC4FA5082E22C5
[SwitchA-pkey-key-code]B374E16DD00132CE71B020217091AC717B612391C76C1FB2E8
8317C1BD8171D41ECB83E210C03CC9
[SwitchA-pkey-key-code]B32E810561C21621C73D6DAAC028F4B1585DA7F42519718CC9
B09EEF0381840002818000AF995917
[SwitchA-pkey-key-code]E1E570A3F6B1C2411948B3B4FFA256699B3BF871221CC9C5DF
257523777D033BEE77FC378145F2AD
[SwitchA-pkey-key-code]D716D7DB9FCABB4ADBF6FB4FDB0CA25C761B308EF53009F710
1F7C62621216D5A572C379A32AC290
[SwitchA-pkey-key-code]E55B394A217DA38B65B77F0185C8DB8095522D1EF044B465E8
716261214A5A3B493E866991113B2D
[SwitchA-pkey-key-code]485348
[SwitchA-pkey-key-code] public-key-code end
[SwitchA-pkey-public-key] peer-public-key end
```

④ 指定服务器 10.165.87.136 对应的主机公钥名称为 key1。

```
[SwitchA] ssh client authentication server 10.165.87.136 assign publickey key1
[SwitchA] quit
```

⑤ 建立到服务器 10.165.87.136 的 SSH 连接。

```
<SwitchA> ssh2 10.165.87.136
```

```
Username: client001
Trying 10.165.87.136
Press Ctrl+K to abort
Connected to 10.165.87.136...
Enter password:
**********************************************************
* Copyright (c) 2004-2007 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.
**********************************************************
<SwitchB>
```

12.6.4 设备作为 SSH 客户端并采用 publickey 认证(认证密钥算法为 DSA)时的典型配置指导

1. 背景

IT 维护部门在配置设备 SSH 客户端时,为了加强安全,进一步采用了 publickey 的认证方式,在这种方式下可以选择 RSA 或者 DSA 算法。

2. 组网图

图 12-30 所示为设备作为 SSH 客户端并采用 publickey 认证(认证密钥算法为 DSA)时的典型配置组网图。

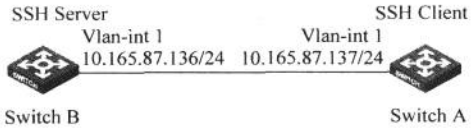


图 12-30 设备作为 SSH 客户端并采用 publickey 认证(认证密钥算法为 DSA)时的典型配置组网图

3. 配置需求

如图 12-30 所示,配置 Switch A 作为客户端,采用 SSH 协议登录到 Switch B 上。SSH 用户采用的认证方式为 publickey 认证,认证时采用的公共密钥算法为 DSA。

4. 配置过程和解释

(1) 配置 SSH 服务器 Switch B。

① 生成 RSA 及 DSA 密钥对,并启动 SSH 服务器。

```
<SwitchB> system-view
[SwitchB] public-key local create rsa
[SwitchB] public-key local create dsa
[SwitchB] ssh server enable
```

注意: 生成服务器的 RSA 和 DSA 密钥对是完成 SSH 登录的必要操作。

② 配置 VLAN 接口 1 的 IP 地址,客户端将通过该地址连接 SSH 服务器。

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

③ 设置 SSH 客户端登录用户界面的认证方式为 AAA 认证。

```
[SwitchB] user-interface vty 0 4
[SwitchB-ui-vty0-4] authentication-mode scheme
```

④ 设置 Switch B 上远程用户登录协议为 SSH。

```
[SwitchB-ui-vty0-4] protocol inbound ssh
```

⑤ 设置用户能访问的命令级别为 3。

```
[SwitchB-ui-vty0-4] user privilege level 3
[SwitchB-ui-vty0-4] quit
```

提示：这时需要先在 SSH 客户端生成 DSA 密钥对，将生成的 DSA 公钥保存到指定文件中，并将此公钥文件通过 FTP/TFTP 方式上传到服务器，文件名为 key.pub。有关配置可参见客户端的配置。

⑥ 从文件 key.pub 中导入远端的公钥。

```
[SwitchB] public-key peer Switch001 import sshkey key.pub
```

⑦ 设置 SSH 用户 client002 的认证方式为 publickey，并指定公钥为 Switch001。

```
[SwitchB] ssh user client002 service-type stelnet authentication-type publickey assign publickey
Switch001
```

(2) 配置 SSH 客户端 Switch A。

① 配置 VLAN 接口 1 的 IP 地址。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

② 生成 DSA 密钥对。

```
[SwitchA] public-key local create dsa
```

③ 将生成的 DSA 主机公钥导出到指定文件 key.pub 中。

```
[SwitchA] public-key local export dsa ssh2 key.pub
[SwitchA] quit
```

提示：客户端生成密钥对后，需要将保存的公钥文件通过 FTP/TFTP 方式上传到服务器，并完成服务器的配置后，才可继续客户端的配置。

④ 建立到服务器 10.165.87.136 的 SSH 连接。

```
<SwitchA> ssh2 10.165.87.136
Username: client002
Trying 10.165.87.136 ...
Press Ctrl+K to abort
Connected to 10.165.87.136 ...

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
```

```
**********************************************************
* Copyright (c) 2004-2007 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent,                                *
* no decompiling or reverse-engineering shall be allowed.
**********************************************************
<SwitchB>
```

12.6.5 设备作为 SFTP 客户端典型配置指导

1. 背景

H3C 安全专家发现 M 公司从文件服务器下载一些很重要的文件以及从设备上备份设备配置时，采用的是 FTP 的传输方式。因 FTP 也是采用明文传输用户名和密码，所以其是一个潜在的安全漏洞。

为了加强文件传输的安全性，防止备份设备的配置被别有用心的人员获取，H3C 安全专家推荐采用 SFTP 的方式来传输设备配置备份文件。

2. 组网图

图 12-31 所示为设备作为 SFTP 客户端典型配置组网图。

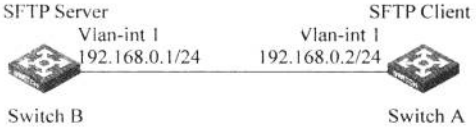


图 12-31 设备作为 SFTP 客户端典型配置组网图

3. 配置需求

如图 12-31 所示，Switch A 和 Switch B 之间建立 SSH 连接，Switch A 作为 SFTP 客户端登录到 Switch B，进行文件管理和文件传送等操作。SSH 用户采用的认证方式为 publickey 认证，认证时采用的公共密钥算法为 RSA。

4. 配置过程和解释

(1) 配置服务器 Switch B。

① 生成 RSA 及 DSA 密钥对，并启动 SSH 服务器。

```
<SwitchB> system-view
[SwitchB] public-key local create rsa
[SwitchB] public-key local create dsa
[SwitchB] ssh server enable
```

注意：生成服务器的 RSA 和 DSA 密钥对是完成 SFTP 登录的必要操作。

② 启动 SFTP 服务器。

```
[SwitchB] sftp server enable
```

③ 配置 VLAN 接口 1 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
```

```
[SwitchB-Vlan-interface1] quit
```

④ 设置 SSH 客户端登录用户界面的认证方式为 AAA 认证。

```
[SwitchB] user-interface vty 0 4
[SwitchB-ui-vty0-4] authentication-mode scheme
```

⑤ 设置 Switch B 上远程用户登录协议为 SSH。

```
[SwitchB-ui-vty0-4] protocol inbound ssh
[SwitchB-ui-vty0-4] quit
```

说明：这时需要先在 SFTP 客户端生成 RSA 密钥对，将生成的 RSA 公钥保存到指定文件中，并将此公钥文件通过 FTP/TFTP 方式上传到服务器，文件名为 pubkey。有关配置可参见客户端的配置。

⑥ 从文件 pubkey 中导入远端的公钥。

```
[SwitchB] public-key peer Switch001 import sshkey pubkey
```

⑦ 设置 SSH 用户 client001 的服务类型为 SFTP，认证方式为 publickey，并指定公钥为 Switch001，工作目录为 cf:/。

```
[SwitchB] ssh user client001 service-type sftp authentication-type publickey assign publickey
Switch001 work-directory cf:/
```

(2) 配置客户端 Switch A。

① 配置 VLAN 接口 1 的 IP 地址。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 192.168.0.2 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

② 生成 RSA 密钥对。

```
[SwitchA] public-key local create rsa
```

③ 将生成的 RSA 主机公钥导出到指定文件 pubkey 中。

```
[SwitchA] public-key local export rsa ssh2 pubkey
[SwitchA] quit
```

说明：客户端生成密钥对后，需要将保存的公钥文件通过 FTP/TFTP 方式上传到服务器，并完成服务器的配置后，才可继续客户端的配置。

④ 与远程 SFTP 服务器建立连接，进入 SFTP Client 视图。

```
<SwitchA> sftp 192.168.0.1
Input Username: client001
Trying 192.168.0.1 ...
Press Ctrl+K to abort
Connected to 192.168.0.1 ...
The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
```

```
sftp-client>
```

⑤ 显示服务器的当前目录，删除文件 z，并检查此目录是否删除成功。

```
sftp-client> dir
-rwxrwxrwx    1 noone     nogroup       1759 Aug 23 06:52 config.cfg
-rwxrwxrwx    1 noone     nogroup        225 Aug 24 08:01 pubkey2
-rwxrwxrwx    1 noone     nogroup        283 Aug 24 07:39 pubkey1
drwxrwxrwx    1 noone     nogroup          0 Sep 01 06:22 new
-rwxrwxrwx    1 noone     nogroup        225 Sep 01 06:55 pub
-rwxrwxrwx    1 noone     nogroup          0 Sep 01 08:00 z
sftp-client> delete z
The following files will be deleted:
/z
Are you sure to delete it? [Y/N]:y
This operation may take a long time. Please wait...
File successfully Removed
sftp-client> dir
-rwxrwxrwx    1 noone     nogroup       1759 Aug 23 06:52 config.cfg
-rwxrwxrwx    1 noone     nogroup        225 Aug 24 08:01 pubkey2
-rwxrwxrwx    1 noone     nogroup        283 Aug 24 07:39 pubkey1
drwxrwxrwx    1 noone     nogroup          0 Sep 01 06:22 new
-rwxrwxrwx    1 noone     nogroup        225 Sep 01 06:55 pub
```

⑥ 新增目录 new1，并检查新目录是否创建成功。

```
sftp-client> mkdir new1
Success
New directory created
sftp-client> dir
-rwxrwxrwx    1 noone     nogroup       1759 Aug 23 06:52 config.cfg
-rwxrwxrwx    1 noone     nogroup        225 Aug 24 08:01 pubkey2
-rwxrwxrwx    1 noone     nogroup        283 Aug 24 07:39 pubkey1
drwxrwxrwx    1 noone     nogroup          0 Sep 01 06:22 new
-rwxrwxrwx    1 noone     nogroup        225 Sep 01 06:55 pub
drwxrwxrwx    1 noone     nogroup          0 Sep 02 06:30 new1
```

⑦ 将目录名 new1 更名为 new2，并查看是否更名成功。

```
sftp-client> rename new1 new2
Success
File successfully renamed
sftp-client> dir
-rwxrwxrwx    1 noone     nogroup       1759 Aug 23 06:52 config.cfg
-rwxrwxrwx    1 noone     nogroup        225 Aug 24 08:01 pubkey2
-rwxrwxrwx    1 noone     nogroup        283 Aug 24 07:39 pubkey1
drwxrwxrwx    1 noone     nogroup          0 Sep 01 06:22 new
-rwxrwxrwx    1 noone     nogroup        225 Sep 01 06:55 pub
drwxrwxrwx    1 noone     nogroup          0 Sep 02 06:33 new2
```

⑧ 从服务器上下载文件 pubkey2 到本地，并更名为 public。

```
sftp-client> get pubkey2 public
Remote  file:/pubkey2 --->  Local file: public
Downloading file successfully ended
```

⑨ 将本地文件 pu 上传到服务器上，更名为 puk，并查看上传是否成功。

```
sftp-client> put pu puk
Local file:pu --->  Remote file: /puk
Uploading file successfully ended
sftp-client> dir
-rwxrwxrwx   1 noone     nogroup       1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone     nogroup        225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone     nogroup        283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone     nogroup          0 Sep 01 06:22 new
drwxrwxrwx   1 noone     nogroup          0 Sep 02 06:33 new2
-rwxrwxrwx   1 noone     nogroup        283 Sep 02 06:35 pub
-rwxrwxrwx   1 noone     nogroup        283 Sep 02 06:36 puk
sftp-client>
```

⑩ 退出 SFTP。

```
sftp-client> quit
Bye
Connection closed.
<SwitchA>
```

12.6.6 设备作为 SFTP 服务器典型配置指导

1. 背景

H3C 设备不仅可以作为 SFTP 客户端，也可以作为 SFTP 服务器。因此也可以让设备作为 SFTP 服务器，PC 主机作为 SFTP 客户端直接从设备获取文件或给设备上传文件。

2. 组网图

图 12-32 所示为设备作为 SFTP 服务器典型配置组网图。

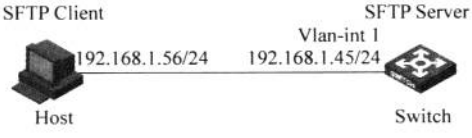


图 12-32 设备作为 SFTP 服务器典型配置组网图

3. 配置需求

如图 12-32 所示，Host 和 Switch 之间建立 SSH 连接，Host 作为 SFTP 客户端登录到 Switch，进行文件管理和文件传送等操作，用户名为 client002，密码为 aabbcc。

4. 配置过程和解释

(1) 配置 SFTP 服务器 Switch。

① 生成 RSA 及 DSA 密钥对，并启动 SSH 服务器。

```
<Switch> system-view
[Switch] public-key local create rsa
[Switch] public-key local create dsa
[Switch] ssh server enable
```

注意：生成服务器的 RSA 和 DSA 密钥对是完成 SFTP 登录的必要操作。

② 启动 SFTP 服务器。

```
[Switch] sftp server enable
```

③ 配置 VLAN 接口 1 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.45 255.255.255.0
[Switch-Vlan-interface1] quit
```

④ 设置 SSH 客户端登录用户界面的认证方式为 AAA 认证。

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
```

⑤ 设置 Switch 上远程用户登录协议为 SSH。

```
[Switch-ui-vty0-4] protocol inbound ssh
[Switch-ui-vty0-4] quit
```

⑥ 创建本地用户 client002。

```
[Switch] local-user client002
[Switch-luser-client002] password simple aabbcc
[Switch-luser-client002] service-type ssh
[Switch-luser-client002] quit
```

⑦ 配置 SSH 用户认证方式为 password，服务类型为 SFTP。

```
[Switch] ssh user client002 service-type sftp authentication-type password
```

(2) 配置 SFTP 客户端 Host。

说明：

① SFTP 客户端软件有很多，本书中仅以客户端软件 PuTTY0.58 中的 PSFTP 为例，说明 SFTP 客户端的配置方法。

② PSFTP 只支持 password 认证，不支持 publickey 认证。

建立与 SFTP 服务器的连接。打开 psftp.exe 程序，出现如图 12-33 所示的 SFTP 客户端登录界面。输入如下命令：

```
open 192.168.1.45
```

根据提示输入用户名 client002，密码 aabbcc，即可登录 SFTP 服务器。

提示：

① 设备作为 SFTP 服务器时，同时只能有一个用户访问 SFTP 服务器。如果以 WinSCP 作为 SFTP 客户端，则无法直接编辑服务器上的文件，需要采用将服务器上的文件

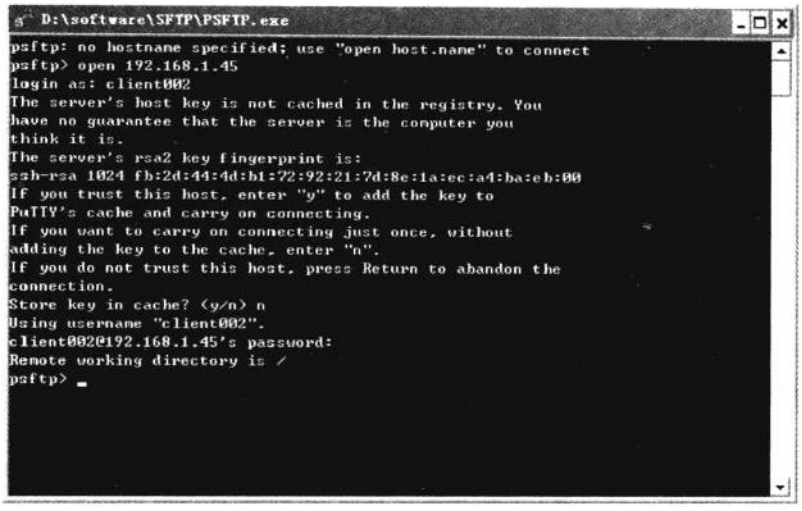


图 12-33 SFTP 客户端登录界面

下载到本地，在本地修改后上传到服务器的方式实现对文件的编辑。

② SSH 用户的服务类型设置为 sftp 或者 all。

第13章

可靠性配置指导

13.1 DLDP 典型配置指导

在实际组网中，有时会出现一种特殊的现象——单向链路(即单通)。所谓单向链路，是指本端设备可以通过链路层收到对端设备发送的报文，但对端设备不能收到本端设备的报文。单向链路会引起一系列问题，如生成树拓扑中存在环路等。

以光纤为例，单向链路分为两种类型：一种是光纤交叉相连；另一种是一条光纤未连接或一条光纤断路。图 13-1 中交叉的光纤表示光纤接反的情况，图 13-2 中空心线表示一条光纤未连接或一条光纤断路的情况。

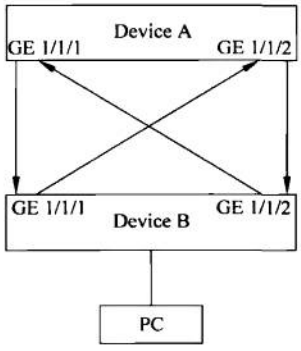


图 13-1 光纤交叉连接

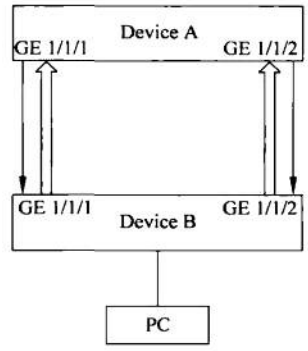


图 13-2 一条光纤未连接或一条光纤断路

DLDP(Device Link Detection Protocol，设备链路检测协议)可以监控光纤或铜质双绞线的链路状态。如果发现单向链路存在，DLDP 会根据用户配置，自动关闭或通知用户手动关闭相关端口，以防止网络问题的发生。

DLDP 是链路层协议，它与物理层协议协同工作来监控设备的链路状态。物理层的自动协商机制进行物理信号和故障的检测；DLDP 进行对端设备的识别、单向链路的识别和关闭不可达端口等工作。两者协同工作，可以检测和关闭物理和逻辑的单向连接。如果链路两端在物理层都能独立正常工作，DLDP 会在链路层检测这些链路是否正确连接、两端是否可以正确地交互报文。这种检测不能通过自动协商机制实现。

1. 背景

M 公司的 IT 维护部门购买了一批 H3C 以太网交换机，由网络管理员负责对这些新设

备进行相应的安装和配置。

因公司交换机间都使用光纤互连，为防止产生单通现象，要求在所有交换机上都配置DLDP。

2. 组网图

图 13-3 所示为 DLDP 典型配置示意图。

图 13-3 DLDP 典型配置示意图

3. 配置需求

如图 13-3 所示，管理员对光纤连接的交换机 SWA 和 SWB 配置 DLDP。管理员要求通过配置达到下列要求：当 DLDP 检测出单向链路后，自动断开单向链路；当网管人员正确连接光纤后，恢复被 DLDP Down 的端口。

4. 配置过程和解释

(1) 在交换机 SWA 上配置 DLDP。

① 在端口 GigabitEthernet 1/0/50 及 GigabitEthernet 1/0/51 使能 DLDP 功能。

```
<SWA>system-view
[SWA]interface gigabitethernet 1/0/50
[SWA-GigabitEthernet1/0/50] dldp enable
[SWA-GigabitEthernet1/0/50] quit
[SWA]interface gigabitethernet 1/0/51
[SWA-GigabitEthernet1/0/51] dldp enable
[SWA-GigabitEthernet1/0/51] quit
```

② 配置发送 Advertisement 报文的时间间隔为 6s。

```
[SWA]dldp interval 6
```

③ 配置 DelayDown 定时器的超时时间为 2s。

```
[SWA]dldp delaydown-timer 2
```

④ 配置 DLDP 的工作模式为加强模式。

```
[SWA]dldp work-mode enhance
```

⑤ 配置发现单向链路后端口的关闭模式为自动模式。

```
[SWA]dldp unidirectional-shutdown auto
```

⑥ 全局使能 DLDP 功能。

```
[SWA]dldp enable
```

(2) 在交换机 SWB 上配置 DLDP。SWB 上的配置与 SWA 上的配置完全一致，此处不再赘述。

(3) 当 DLDP 检测出单向链路后，在交换机上查看 DLDP 状态。

在 SWA 上显示 DLDP 状态信息：

```
[SWA] display dldp
DLDP global status : enable
```

```
DLDP interval : 6s
DLDP work-mode : enhance
DLDP authentication-mode  : none
DLDP unidirectional-shutdown : auto
DLDP delaydown-timer : 2s
The number of enabled ports is 2.

Interface GigabitEthernet 1/0/50
DLDP port state : disable
DLDP link state : down
The neighbor number of the port is 0.

Interface GigabitEthernet 1/0/51
DLDP port state : disable
DLDP link state : down
The neighbor number of the port is 0.
```

从上述显示信息可以看出，端口 GigabitEthernet 1/0/50 和 GigabitEthernet 1/0/51 均进入 Disable 状态且链路状态也均是 Down，表明 DLDP 在这两个端口探测到了单向链路，并且已经将这两个端口关闭。

(4) 当网管人员正确连接光纤后，在交换机 SWA、SWB 上恢复被 DLDP Down 的端口。

```
[SWA]dldp reset
[SWB]dldp reset
```

提示：在链路未连通的情况下，DLDP 不起作用，只有当链路连通后，DLDP 才能检测出单向链路，因此在使能 DLDP 之前，先连接好光纤或铜质双绞线。

只有在全局和端口均使能 DLDP 的情况下，才能启动 DLDP 功能，正常地收发 DLDP 报文。

dldp interval 命令配置的时间间隔应该小于 STP 收敛时间的 1/3。如果设定的时间太长，DLDP 在没有关闭单向链路的情况下已出现 STP 环路，并且设备需要经过较长时间才能发现单向链路，可能造成较多的错误流量转发；如果设定的时间太短，会增加网络的流量。因此，此时间间隔建议采用默认值。

13.2 VRRP 典型配置指导

如图 13-4 所示，通常，同一网段内的所有主机都设置一条相同的以网关为下一跳的默认路由。主机发往其他网段的报文将通过默认路由发往网关，再由网关进行转发，从而实现主机与外部网络的通信。当网关发生故障时，本网段内所有以网关为默认路由的主机将无法与外部网络通信。

默认路由为用户的配置操作提供了方便，但是对默认网关设备提出了很高的稳定性要求。增加出口网关是提高系统可靠性的常见方法，此时如何在多个出口之间进行选路就成为需要解决的问题。

VRRP(Virtual Router Redundancy Protocol，虚拟路由器冗余协议)将可以承担网关功能的路由器加入到备份组中，形成一台虚拟路由器，由 VRRP 的选举机制决定哪台路由器

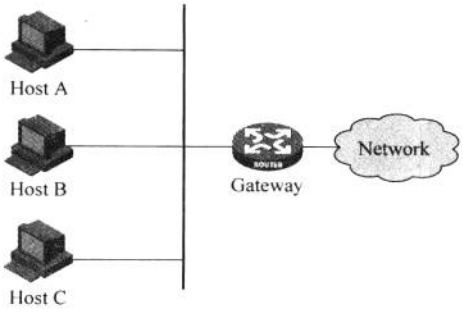


图 13-4 局域网组网方案

承担转发任务，局域网内的主机只需将虚拟路由器配置为默认网关。

VRRP 是一种容错协议，在提高可靠性的同时，简化了主机的配置。在具有多播或广播能力的局域网（如以太网）中，借助 VRRP 能在某台设备出现故障时仍然提供高可靠的默认链路，有效避免单一链路发生故障后网络中断的问题，而无须修改动态路由协议、路由发现协议等配置信息。

VRRP 的实现有 VRRPv2 和 VRRPv3 两个版本。其中，VRRPv2 基于 IPv4，VRRPv3 基于 IPv6。两个版本的 VRRP 在功能实现上并没有区别，只是在 IPv4 设备上和 IPv6 设备上使用的命令不同。

13.2.1 基于 IPv4 的 VRRP 单备份组典型配置指导

1. 背景

M 公司内有些服务器提供比较重要的业务，要求在网络故障时，服务器停止响应时间不能大于 10s。基于以上需求，IT 维护部门认为有必要在交换机上配置 VRRP，以确保服务器网关的高可靠性。

2. 组网图

图 13-5 所示为基于 IPv4 的 VRRP 单备份组配置示意图。

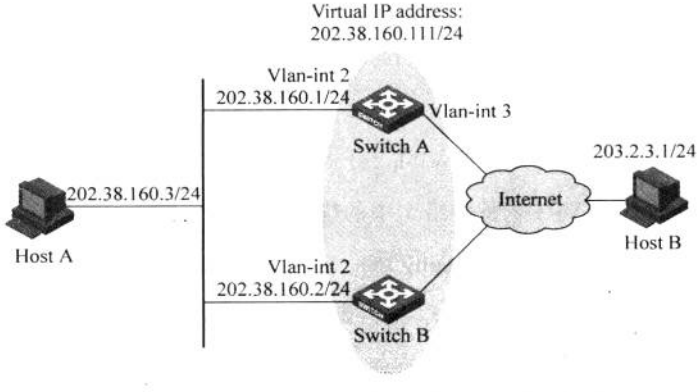


图 13-5 基于 IPv4 的 VRRP 单备份组配置示意图

3. 配置需求

如图 13-4 所示，网络管理员对光纤连接的交换机 SWA 和 SWB 配置 VRRP。网络管理员要求通过配置达到的要求有：Host A 需要访问 Internet 上的 Host B，Host A 的默认网关为 202.38.160.111/24；当 Switch A 正常工作时，Host A 发送给 Host B 的报文通过 Switch A 转发；当 Switch A 出现故障时，Host A 发送给 Host B 的报文通过 Switch B 转发。

4. 配置过程和解释

(1) 在交换机 SWA 上配置 VRRP。

① 配置 VLAN 2。

```
<SWA>system-view
[SWA]vlan 2
[SWA-vlan2]port Ethernet 1/0/6
[SWA-vlan2]quit
[SWA]interface Vlan-interface 2
[SWA-Vlan-interface2]ip address 202.38.160.1 255.255.255.0
```

② 创建一个 VRRP 备份组 1。

```
[SWA-Vlan-interface2]vrrp vrid 1 virtual-ip 202.38.160.111
```

③ 设置交换机 A 在 VRRP 备份组 1 中的优先级。

```
[SWA-Vlan-interface2]vrrp vrid 1 priority 110
```

④ 设置 Switch A 工作在抢占方式，抢占延迟时间为 5s。

```
[SWA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

(2) 在交换机 SWB 上配置 VRRP。

① 配置 VLAN 2。

```
[SWB]vlan 2
[SWB-Vlan2]port Ethernet 1/0/6
[SWB-Vlan2]quit
[SWB]interface Vlan-interface 2
[SWB-Vlan-interface2]ip address 202.38.160.2 255.255.255.0
```

② 创建一个 VRRP 备份组 1。

```
[SWB-Vlan-interface2]vrrp vrid 1 virtual-ip 202.38.160.111
```

③ 设置交换机 B 在 VRRP 备份组 1 中的优先级。

```
[SWB-Vlan-interface2]vrrp vrid 1 priority 100
```

④ 设置 Switch B 工作在抢占方式，抢占延迟时间为 5s。

```
[SWB-Vlan-interface2]vrrp vrid 1 preempt-mode timer delay 5
```

(3) 配置完成后，可以在交换机 SWA、SWB 上，通过 display vrrp 命令查看配置后的结果。

```
[SWA]display vrrp verbose
 IPv4 Standby Information:
     Run Mode          : Standard
     Run Method        : Virtual MAC
  Total number of virtual routers : 1
    Interface Vlan-interface 2
     VRID              : 1                 Adver Timer   : 1
     Admin Status      : Up                State         : Master
     Config Pri        : 110               Running Pri   : 110
     Preempt Mode      : Yes               Delay Time    : 5
     Auth Type         : None
     Virtual IP        : 202.38.160.111
     Virtual MAC       : 0000-5e00-0101
     Master IP         : 202.38.160.1

[SWB] display vrrp verbose
IPv4 Standby Information:
     Run Mode          : Standard
     Run Method        : Virtual MAC
  Total number of virtual routers : 1
    Interface Vlan-interface 2
     VRID              : 1                 Adver Timer   : 1
     Admin Status      : Up                State         : Backup
     Config Pri        : 100               Running Pri   : 100
     Preempt Mode      : Yes               Delay Time    : 5
     Auth Type         : None
     Virtual IP        : 202.38.160.111
     Master IP         : 202.38.160.1
```

从上述显示信息可以看出，正常情况下，Switch A 行使网关的职能，当 Switch A 关机或出现故障时，Switch B 将接替行使网关的职能。设置抢占方式的目的是 Switch A 恢复工作后，能够继续成为 Master 行使网关的职能。

提示：默认情况下，备份组工作在抢占方式，抢占延迟时间为 0s。

对于同一个 VRRP 备份组的配置，必须保证备份组虚拟路由器的 IP 地址个数、每个备份组虚拟路由器的 IP 地址、定时器间隔时间和认证方式完全一样。

13.2.2 基于 IPv4 的 VRRP 监视接口典型配置指导

1. 背景

在设备的运行维护过程中，网络管理员发现当交换机连接上行链路的接口出现故障时，VRRP 备份组无法感知上行链路接口的故障。如果该交换机此时处于 Master 状态，将会导致局域网内的主机无法访问外部网络。

网络管理员在所有的交换机上启用 VRRP 的监视接口功能。VRRP 的监视接口功能更好地扩充了 Backup 交换机的备份功能，即不仅能在备份组所在的接口出现故障时提供备份功能，还能在交换机的其他接口（如连接上行链路的接口）不可用时提供备份功能。当被监视的接口 Down 时，拥有这个接口的交换机的优先级会自动降低一个数值（Value-

reduced)，使得备份组内其他交换机的优先级高于这个交换机的优先级，以便其他优先级高的交换机转变为 Master，承担转发任务。

2. 组网图

图 13-6 所示为基于 IPv4 的 VRRP 监视接口典型配置示意图。

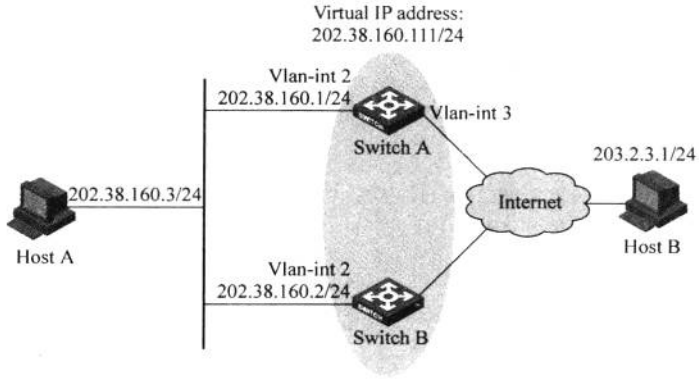


图 13-6 基于 IPv4 的 VRRP 监视接口典型配置示意图

3. 配置需求

如图 13-6 所示，网络管理员对光纤连接的交换机 SWA 和 SWB 配置 VRRP。网络管理员要求通过配置达到下列要求：Host A 需要访问 Internet 上的 Host B，Host A 的默认网关为 202.38.160.111/24；Switch A 和 Switch B 属于虚拟 IP 地址为 202.38.160.111 的备份组 1；当 Switch A 正常工作时，Host A 发送给 Host B 的报文通过 Switch A 转发；当 Switch A 连接 Internet 的 VLAN 接口 3 不可用时，Host A 发送给 Host B 的报文通过 Switch B 转发。

4. 配置过程和解释

(1) 在交换机 SWA 上配置 VRRP 及开启 VRRP 监视接口功能。

① 配置 VLAN 2。

```
<SWA>system-view
[SWA]vlan 2
[SWA-vlan2]port Ethernet 1/0/6
[SWA-vlan2]quit
[SWA]interface Vlan-interface 2
[SWA-Vlan-interface2]ip address 202.38.160.1 255.255.255.0
```

② 创建一个 VRRP 备份组 1。

```
[SWA-Vlan-interface2]vrrp vrid 1 virtual-ip 202.38.160.111
```

③ 设置交换机 A 在 VRRP 备份组 1 中的优先级。

```
[SWA-Vlan-interface2]vrrp vrid 1 priority 110
```

④ 设置 Switch A 工作在抢占方式，抢占延迟时间为 5s。

```
[SWA-Vlan-interface2]vrrp vrid 1 preempt-mode timer delay 5
```

⑤ 设置 Switch A 监视指定接口。

```
[SWA-Vlan-interface2]vrrp vrid 1 track interface Vlan-interface 3 reduced 30
```

(2) 在交换机 SWB 上配置 VRRP。

① 配置 VLAN 2。

```
[SWB]vlan 2
[SWB-Vlan2]port Ethernet 1/0/6
[SWB-Vlan2]quit
[SWB]interface Vlan-interface 2
[SWB-Vlan-interface2]ip address 202.38.160.2 255.255.255.0
```

② 创建一个 VRRP 备份组 1。

```
[SWB-Vlan-interface2]vrrp vrid 1 virtual-ip 202.38.160.111
```

③ 设置交换机 B 在 VRRP 备份组 1 中的优先级。

```
[SWB-Vlan-interface2]vrrp vrid 1 priority 100
```

④ 设置 Switch B 工作在抢占方式，抢占延迟时间为 5s。

```
[SWB-Vlan-interface2]vrrp vrid 1 preempt-mode timer delay 5
```

(3) 配置完成后，可以在交换机 SWA、SWB 上通过 display vrrp 命令查看配置后的结果。

```
[SWA] display vrrp verbose
 IPv4 Standby Information:
     Run Mode          : Standard
     Run Method        : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface 2
     VRID              : 1                 Adver Timer   : 5
     Admin Status      : Up                State         : Master
     Config Pri        : 110               Running Pri   : 110
     Preempt Mode      : Yes               Delay Time    : 0
     Auth Type         : Simple            Key           : hello
     Virtual IP        : 202.38.160.111
     Virtual MAC       : 0000-5e00-0101
     Master IP         : 202.38.160.1
   VRRP Track Information:
     Track Interface   : Vlan 3            State : Up          Pri Reduced : 30

[SWB] display vrrp verbose
 IPv4 Standby Information:
     Run Mode          : Standard
     Run Method        : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface 2
     VRID              : 1                 Adver Timer   : 5
     Admin Status      : Up                State         : Backup
     Config Pri        : 100               Running Pri   : 100
```

Preempt Mode	: Yes	Delay Time	: 0
Auth Type	: Simple	Key	: hello
Virtual IP	: 202.38.160.111		
Master IP	: 202.38.160.1		

从上述显示信息可以看出，正常情况下，Switch A 行使网关的职能。当 Switch A 的接口 Vlan-interface 3 不可用时，Switch A 的优先级降低 30，低于 Switch B 优先级，Switch B 将抢占成为 Master 行使网关的职能；当 Switch A 的接口 Vlan-interface 3 恢复工作后，Switch A 能够继续成为 Master 行使网关的职能。

提示：不允许对 IP 地址拥有者进行监视指定接口的配置。

建议用户在配置监视接口功能时，在上行 Trunk 端口禁止 VRRP 备份组监视接口所对应的 VLAN 通过。

被监视接口的状态由 Down 变为 Up 后，对应设备的优先级数会自动恢复。

用户在配置降低优先级幅度时，需要确保降低后的优先级比备份组内其他交换机的优先级要低，确保备份组内有其他交换机被选为 Master 交换机。

13.2.3 基于 IPv4 的 VRRP 多备份组典型配置指导

1. 背景

VRRP 单备份组中的缺点在于，正常情况下 Backup 交换机不转发数据流，没有充分利用交换机的能力。为了避免 Backup 交换机闲置，网络管理员决定使用 VRRP 多备份组功能。通过 VRRP 多备份组的组网，能够实现 VRRP 网络中的负载分担功能。

2. 组网图

图 13-7 所示为基于 IPv4 的 VRRP 多备份组典型配置示意图。

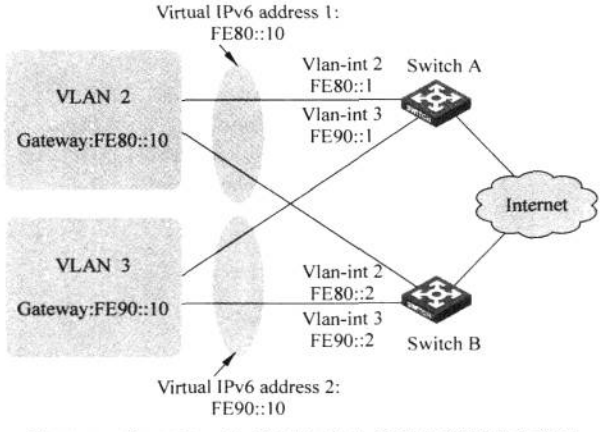


图 13-7 基于 IPv4 的 VRRP 多备份组典型配置示意图

3. 配置需求

如图 13-7 所示，网络管理员对光纤连接的交换机 SWA 和 SWB 配置 IPv6 VRRP。网络管理员要求通过配置达到的要求有：VLAN 2 内主机的默认网关为 1::10/64；VLAN 3 内主机的默认网关为 2::10/64；Switch A 和 Switch B 同时属于虚拟 IPv6 地址为 1::10/64、FE80::10 的备份组 1 和虚拟 IPv6 地址为 2::10/64、FE90::10 的备份组 2；在备份组 1 中

Switch A 的优先级高于 Switch B，在备份组 2 中 Switch B 的优先级高于 Switch A，从而保证 VLAN 2 和 VLAN 3 内的主机分别通过 Switch A 和 Switch B 通信，当 Switch A 或 Switch B 出现故障时，主机可以通过另一台设备继续通信，避免通信中断。

4. 配置过程和解释

(1) 在交换机 SWA 上配置 IPv6 VRRP。

① 配置 VLAN 2。

```
<SWA>system-view
[SWA]ipv6
[SWA]vlan 2
[SWA-vlan2]port Ethernet 1/0/5
[SWA-vlan2]quit
[SWA]interface Vlan-interface 2
[SWA-Vlan-interface2]ipv6 address fe80::1 link-local
[SWA-Vlan-interface2]ipv6 address 1::1 64
```

② 创建一个 VRRP 备份组 1。

```
[SWA-Vlan-interface2]vrrp vrid 1 virtual-ip 202.38.160.100
```

③ 设置交换机 A 在 VRRP 备份组 1 中的优先级。

```
[SWA-Vlan-interface2]vrrp vrid 1 priority 110
```

④ 配置 VLAN 3。

```
[SWA]vlan 3
[SWA-vlan3]port Ethernet 1/0/6
[SWA-vlan3]quit
[SWA]interface vlan-interface 3
[SWA-Vlan-interface3]ip address 202.38.160.130 255.255.255.128
```

⑤ 创建一个 VRRP 备份组 2。

```
[SWA-Vlan-interface3]vrrp vrid 2 virtual-ip 202.38.160.200
```

⑥ 设置交换机 A 在 VRRP 备份组 2 中的优先级。

```
[SWA-Vlan-interface3]vrrp vrid 1 priority 100
```

(2) 在交换机 SWB 上配置 VRRP。

① 配置 VLAN 2。

```
<SWB>system-view
[SWB]vlan 2
[SWB-vlan2]port Ethernet 1/0/5
[SWB-vlan2]quit
[SWB]interface Vlan-interface 2
[SWB-Vlan-interface2]ip address 202.38.160.2 255.255.255.128
```

② 创建一个 VRRP 备份组 1。

```
[SWB-Vlan-interface2]vrrp vrid 1 virtual-ip 202.38.160.100
```

③ 设置交换机 B 在 VRRP 备份组 1 中的优先级。

```
[SWB-Vlan-interface2]vrrp vrid 1 priority 100
```

④ 配置 VLAN 3。

```
[SWB]vlan 3
[SWB-vlan3]port Ethernet 1/0/6
[SWB-vlan3]quit
[SWB]interface vlan-interface 3
[SWB-Vlan-interface3]ip address 202.38.160.131 255.255.255.128
```

⑤ 创建一个 VRRP 备份组 2。

```
[SWB-Vlan-interface3]vrrp vrid 2 virtual-ip 202.38.160.200
```

⑥ 设置交换机 A 在 VRRP 备份组 2 中的优先级。

```
[SWB-Vlan-interface3]vrrp vrid 2 priority 110
```

(3) 配置完成后，可以在交换机 SWA、SWB 上通过 display vrrp 命令查看配置后的结果。

```
[SWA] display vrrp verbose
 IPv4 Standby Information:
     Run Mode          : Standard
     Run Method        : Virtual MAC
 Total number of virtual routers : 2
   Interface Vlan-interface 2
     VRID              : 1                 Adver Timer   : 1
     Admin Status      : Up                State         : Master
     Config Pri        : 110               Running Pri   : 110
     Preempt Mode      : Yes               Delay Time    : 0
     Auth Type         : None
     Virtual IP        : 202.38.160.100
     Virtual MAC       : 0000-5e00-0101
     Master IP         : 202.38.160.1
   Interface Vlan-interface 3
     VRID              : 2                 Adver Timer   : 1
     Admin Status      : Up                State         : Backup
     Config Pri        : 100               Running Pri   : 100
     Preempt Mode      : Yes               Delay Time    : 0
     Auth Type         : None
     Virtual IP        : 202.38.160.200
     Master IP         : 202.38.160.131

 [SWB] display vrrp verbose
 IPv4 Standby Information:
     Run Mode          : Standard
     Run Method        : Virtual MAC
 Total number of virtual routers : 2
   Interface Vlan-interface 2
     VRID              : 1                 Adver Timer   : 1
     Admin Status      : Up                State         : Backup
```

```
  Config Pri          : 100                  Running Pri    : 100
  Preempt Mode        : Yes                  Delay Time     : 0
  Auth Type           : None
  Virtual IP          : 202.38.160.100
  Master IP           : 202.38.160.1
Interface Vlan-interface 3
  VRID                : 2                    Adver Timer    : 1
  Admin Status        : Up                   State          : Master
  Config Pri          : 110                  Running Pri    : 110
  Preempt Mode        : Yes                  Delay Time     : 0
  Auth Type           : None
  Virtual IP          : 202.38.160.200
  Virtual MAC         : 0000-5e00-0102
  Master IP           : 202.38.160.131
```

从上述显示信息可以看出，正常情况下，在备份组 1 中 Switch A 为 Master 交换机，Switch B 为 Backup 交换机，默认网关为 202.38.160.100/25 的主机通过 Switch A 访问 Internet；备份组 2 中 Switch A 为 Backup 交换机，Switch B 为 Master 交换机，默认网关为 202.38.160.200/25 的主机通过 Switch B 访问 Internet。

提示：网络流量过大或者不同的交换机上的定时器差异等因素，会导致 Backup 路由器的定时器异常超时而发生状态转换。对于这种情况，可以通过将 VRRP 通告报文的发送时间间隔延长和设置抢占延迟时间的办法来解决。

13.2.4 基于 IPv6 的 VRRP 单备份组典型配置指导

1. 背景

M 公司准备在网络中运行 IPv6 协议，故需要在所有的交换机上启用基于 IPv6 的 VRRP。

2. 组网图

图 13-8 所示为基于 IPv6 的 VRRP 单备份组典型配置示意图。

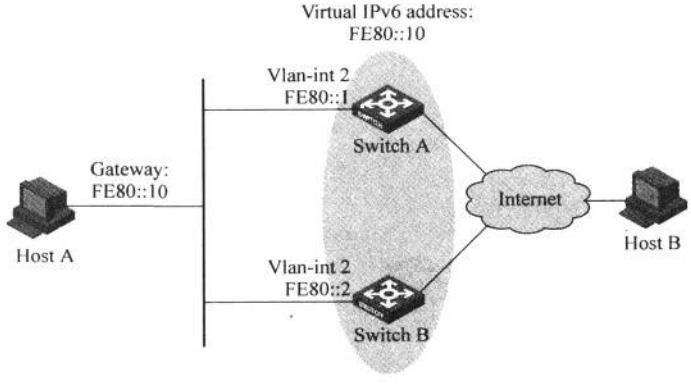


图 13-8 基于 IPv6 的 VRRP 单备份组典型配置示意图

3. 配置需求

如图 13-8 所示，网络管理员对光纤连接的交换机 SWA 和 SWB 配置基于 IPv6 的 VRRP。网络管理员要求通过配置达到的要求有：Host A 需要访问 Internet 上的 Host B，Host A 的默认网关为 FE80::10。Switch A 和 Switch B 属于虚拟 IPv6 地址为 FE80::10

的备份组 1。当 Switch A 正常工作时，Host A 发送给 Host B 的报文通过 Switch A 转发；当 Switch A 出现故障时，Host A 发送给 Host B 的报文通过 Switch B 转发。

4. 配置过程和解释

(1) 在交换机 SWA 上配置基于 IPv6 的 VRRP。

① 配置 VLAN 2。

```
<SWA>system-view
[SWA]ipv6
[SWA]vlan 2
[SWA-vlan2]port Ethernet 1/0/6
[SWA-vlan2]quit
[SWA]interface Vlan-interface 2
[SWA-Vlan-interface2]ipv6 address fe80::1 link-local
[SWA-Vlan-interface2]ipv6 address 1::1 64
```

② 创建一个 VRRP 备份组 1。

```
[SWA-Vlan-interface2]vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
```

③ 设置交换机 A 在 VRRP 备份组 1 中的优先级。

```
[SWA-Vlan-interface2]vrrp ipv6 vrid 1 priority 110
```

④ 设置 Switch A 工作在抢占方式，抢占延迟时间为默认值 0s。

```
[SWA-Vlan-interface2]vrrp ipv6 vrid 1 preempt-mode
```

⑤ 设置 Switch A 配置允许发布 RA 消息。

```
[SWA-Vlan-interface2]undo ipv6 nd ra halt
```

(2) 在交换机 SWB 上配置基于 IPv6 的 VRRP。

① 配置 VLAN 2。

```
<SWB>system-view
[SWB]ipv6
[SWB]vlan 2
[SWB-Vlan2]port Ethernet 1/0/6
[SWB-Vlan2]quit
[SWB]interface Vlan-interface 2
[SWB-Vlan-interface2]ipv6 address fe80::2 link-local
[SWB-Vlan-interface2]ipv6 address 1::2 64
```

② 创建一个 VRRP 备份组 1。

```
[SWB-Vlan-interface2]vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
```

③ 设置交换机 B 在 VRRP 备份组 1 中的优先级。

```
[SWB-Vlan-interface2]vrrp ipv6 vrid 1 priority 100
```

④ 设置 Switch B 工作在抢占方式，抢占延迟时间为默认值 0s。

```
[SWB-Vlan-interface2]vrrp ipv6 vrid 1 preempt-mode
```

⑤ 设置 Switch B 配置允许发布 RA 消息。

```
[SWB-Vlan-interface2]undo ipv6 nd ra halt
```

(3) 配置完成后，可以在交换机 SWA、SWB 上通过 display vrrp 命令查看配置后的结果。

```
[SWA] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode          : Standard
     Run Method        : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface 2
     VRID              :1                  Adver Timer   : 100
     Admin Status      :Up                  State        : Master
     Config Pri        :110                Running Pri   : 110
     Preempt Mode      :Yes                Delay Time    : 5
     Auth Type         None
     Virtual IP        FE80::10
                        1::10
     Virtual MAC       : 0000-5e00-0201
     Master IP         : FE80::1

[SWB] display vrrp ipv6 verbose
IPv6 Standby Information:
     Run Mode          : Standard
     Run Method        : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface 2
     VRID              : 1                 Adver Timer   : 100
     Admin Status      : Up                State         : Backup
     Config Pri        : 100               Running Pri   : 100
     Preempt Mode      : Yes               Delay Time    : 5
     Auth Type         : None
     Virtual IP        : FE80::10
                         1::10
     Master IP         : FE80::1
```

从上述显示信息可以看出，在备份组 1 中 Switch A 为 Master 路由器，Switch B 为 Backup 路由器，Host A 发送给 Host B 的报文通过 Switch A 转发。正常情况下，Switch A 行使网关的职能；当 Switch A 关机或出现故障时，Switch B 将接替行使网关的职能。

13.2.5 基于 IPv6 的 VRRP 监视接口典型配置指导

1. 背景

在设备的运行维护过程中，网络管理员发现当交换机连接上行链路的接口出现故障时，VRRP 备份组无法感知上行链路接口的故障。如果该交换机此时处于 Master 状态，将会导致局域网内的主机无法访问外部网络。

网络管理员在所有的交换机上启用 IPv6 VRRP 的监视接口功能。

2. 组网图

图 13-9 所示为基于 IPv6 的 VRRP 监视接口典型配置示意图。

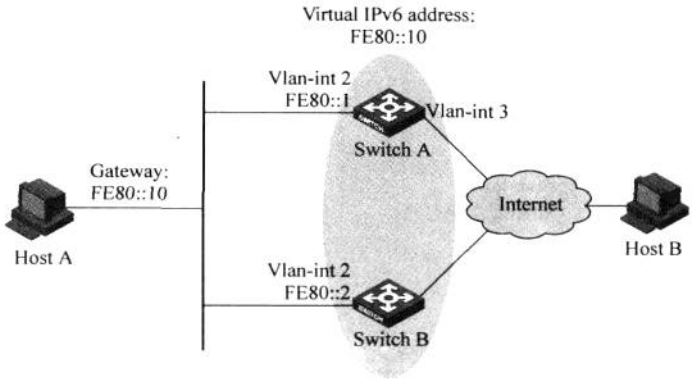


图 13-9 基于 IPv6 的 VRRP 监视接口典型配置示意图

3. 配置需求

如图 13-9 所示，网络管理员对光纤连接的交换机 SWA 和 SWB 配置 VRRP。网络管理员要求通过配置达到下列要求：Host A 需要访问 Internet 上的 Host B，Host A 的默认网关为 FE80::10；Switch A 和 Switch B 属于虚拟 IPv6 地址为 FE80::10 的备份组 1；当 Switch A 正常工作时，Host A 发送给 Host B 的报文通过 Switch A 转发；当 Switch A 连接 Internet 的 VLAN 接口 3 不可用时，Host A 发送给 Host B 的报文通过 Switch B 转发。

4. 配置过程和解释

(1) 在交换机 SWA 上配置基于 IPv6 的 VRRP。

① 配置 VLAN 2。

```
<SWA>system-view
[SWA]ipv6
[SWA]vlan 2
[SWA-vlan2]port Ethernet 1/0/6
[SWA-vlan2]quit
[SWA]interface Vlan-interface 2
[SWA-Vlan-interface2]ipv6 address fe80::1 link-local
[SWA-Vlan-interface2]ipv6 address 1::1 64
```

② 创建一个 VRRP 备份组 1。

```
[SWA-Vlan-interface2]vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
```

③ 设置交换机 A 在 VRRP 备份组 1 中的优先级。

```
[SWA-Vlan-interface2]vrrp ipv6 vrid 1 priority 110
```

④ 设置 Switch A 工作在抢占方式，抢占延迟时间为默认值 0s。

```
[SWA-Vlan-interface2]vrrp ipv6 vrid 1 preempt-mode
```

⑤ 设置 Switch A 配置监视接口。

```
[SWA-Vlan-interface2] vrrp ipv6 vrid 1 track interface Vlan-interface 3 reduced 30
```

⑥ 设置 Switch A 配置允许发布 RA 消息。

```
[SWA-Vlan-interface2]undo ipv6 nd ra halt
```

(2) 在交换机 SWB 上配置基于 IPv6 的 VRRP。

① 配置 VLAN 2。

```
<SWB>system-view
[SWB]ipv6
[SWB]vlan 2
[SWB-Vlan2]port Ethernet 1/0/6
[SWB-Vlan2]quit
[SWB]interface Vlan-interface 2
[SWB-Vlan-interface2]ipv6 address fe80::2 link-local
[SWB-Vlan-interface2]ipv6 address 1::2 64
```

② 创建一个 VRRP 备份组 1。

```
[SWB-Vlan-interface2]vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
```

③ 设置交换机 B 在 VRRP 备份组 1 中的优先级。

```
[SWB-Vlan-interface2]vrrp ipv6 vrid 1 priority 100
```

④ 设置 Switch B 工作在抢占方式，抢占延迟时间为默认值 0s。

```
[SWB-Vlan-interface2]vrrp ipv6 vrid 1 preempt-mode
```

⑤ 设置 Switch B 配置允许发布 RA 消息。

```
[SWB-Vlan-interface2]undo ipv6 nd ra halt
```

(3) 配置完成后，可以在交换机 SWA、SWB 上通过 display vrrp 命令查看配置后的结果。

```
[SWA] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode          : Standard
     Run Method        : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface 2
     VRID              : 1                 Adver Timer   : 500
     Admin Status      : Up                State         : Master
     Config Pri        : 110               Running Pri   : 110
     Preempt Mode      : Yes               Delay Time    : 5
     Auth Type         : Simple            Key           : hello
     Virtual IP        : FE80::10
                         1::10
     Virtual MAC       : 0000-5e00-0201
```

```
    Master IP          : FE80::1
  VRRP Track Information:
    Track Interface    : Vlan 3                State : Up        Pri Reduced : 30display vrrp

[SWB] display vrrp ipv6 verbose
IPv6 Standby Information:
    Run Mode           : Standard
    Run Method         : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface 2
    VRID               : 1                     Adver Timer   : 100
    Admin Status       : Up                    State         : Backup
    Config Pri         : 100                   Running Pri   : 100
    Preempt Mode       : Yes                   Delay Time    : 5
    Auth Type          : None
    Virtual IP         : FE80::10
                         1::10
    Master IP          : FE80::1
```

从上述显示信息可以看出，正常情况下，Switch A 行使网关的职能。当 Switch A 的接口 Vlan-interface 3 不可用时，Switch A 的优先级降低 30，低于 Switch B 优先级，Switch B 将抢占成为 Master 行使网关的职能；当 Switch A 的接口 Vlan-interface 3 恢复工作后，Switch A 能够继续成为 Master 行使网关的职能。

13.2.6 基于 IPv6 的 VRRP 多备份组典型配置指导

1. 背景

为了避免 Backup 交换机闲置，网络管理员决定配置使用 IPv6 VRRP 多备份组功能。通过 VRRP 多备份组的组网，实现 VRRP 的负载分担功能。

2. 组网图

图 13-10 所示为基于 IPv6 的 VRRP 多备份组典型配置示意图。

3. 配置需求

如图 13-10 所示，网络管理员对光纤连接的交换机 SWA 和 SWB 配置 VRRP。网络管理员要求通过配置达到的要求有：VLAN 2 内主机的默认网关为 FE80::10；VLAN 3 内主机的默认网关为 FE90::10；Switch A 和 Switch B 同时属于虚拟 IPv6 地址为 FE80::10 的备份组 1 和虚拟 IPv6 地址为 FE90::10 的备份组 2；在备份组 1 中 Switch A 的优先级高于 Switch B，在备份组 2 中 Switch B 的优先级高于 Switch A，从而保证 VLAN 2 和 VLAN 3 内的主机分别通过 Switch A 和 Switch B 通信；当 Switch A 或 Switch B 出现故障时，主机可以通过另一台设备继续通信，避免通信中断。

4. 配置过程和解释

(1) 在交换机 SWA 上配置基于 IPv6 的 VRRP。

① 配置 VLAN 2。

```
<SWA>system-view
[SWA]ipv6
```

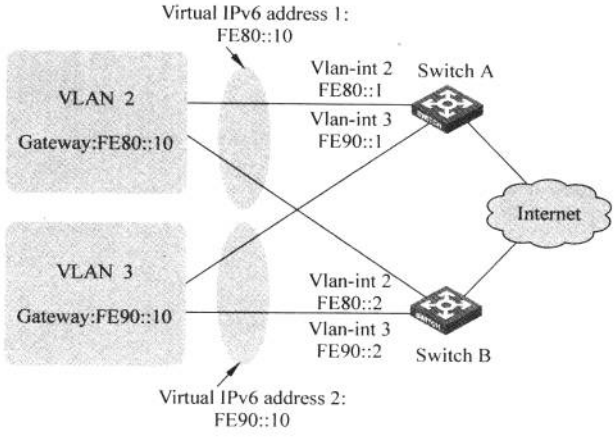


图 13-10 基于 IPv6 的 VRRP 多备份组典型配置示意图

```
[SWA]vlan 2
[SWA-vlan2]port Ethernet 1/0/6
[SWA-vlan2]quit
[SWA]interface Vlan-interface 2
[SWA-Vlan-interface2]ipv6 address fe80::1 link-local
[SWA-Vlan-interface2]ipv6 address 1::1 64
```

② 创建一个 VRRP 备份组 1。

```
[SWA-Vlan-interface2]vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
```

③ 设置交换机 A 在 VRRP 备份组 1 中的优先级。

```
[SWA-Vlan-interface2]vrrp ipv6 vrid 1 priority 110
```

④ 设置 Switch A 工作在抢占方式，抢占延迟时间为默认值 0s。

```
[SWA-Vlan-interface2]vrrp ipv6 vrid 1 preempt-mode
```

⑤ 设置 Switch A 配置允许发布 RA 消息。

```
[SWA-Vlan-interface2]undo ipv6 nd ra halt
```

⑥ 配置 VLAN 3。

```
[SWA] vlan 3
[SWA-vlan3] port Ethernet 1/0/7
[SWA-vlan3] quit
[SWA] interface vlan-interface 3
[SWA-Vlan-interface3] ipv6 address fe90::1 link-local
[SWA-Vlan-interface3] ipv6 address 2::1 64
```

⑦ 创建一个备份组 2，并配置备份组 2 的虚拟 IPv6 地址为 FE90::10。

```
[SWA-Vlan-interface2]vrrp ipv6 vrid 2 virtual-ip fe90::10 link-local
```

(2) 在交换机 SWB 上配置基于 IPv6 的 VRRP。

① 配置 VLAN 2。

```
<SWB>system-view
[SWB]ipv6
[SWB]vlan 2
[SWB-vlan2]port Ethernet 1/0/6
[SWB-vlan2]quit
[SWB]interface Vlan-interface 2
[SWB-Vlan-interface2]ipv6 address fe80::2 link-local
[SWB-Vlan-interface2]ipv6 address 1::2 64
```

② 创建一个 VRRP 备份组 1。

```
[SWB-Vlan-interface2]vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
```

③ 设置交换机 B 在 VRRP 备份组 1 中的优先级。

```
[SWB-Vlan-interface2]vrrp ipv6 vrid 1 priority 100
```

④ 设置 Switch B 工作在抢占方式，抢占延迟时间为默认值 0s。

```
[SWB-Vlan-interface2]vrrp ipv6 vrid 1 preempt-mode
```

⑤ 设置 Switch B 配置允许发布 RA 消息。

```
[SWB-Vlan-interface2]undo ipv6 nd ra halt
```

⑥ 配置 VLAN 3。

```
[SWB] vlan 3
[SWB-vlan3] port Ethernet 1/0/7
[SWB-vlan3] quit
[SWB] interface vlan-interface 3[SWB-Vlan-interface3] ipv6 address fe90::2 link-local
[SWB-Vlan-interface3] ipv6 address 2::2 64
```

⑦ 创建一个备份组 2，并配置备份组 2 的虚拟 IPv6 地址为 FE90::10。

```
[SWB-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip fe90::10 link-local
```

⑧ 设置交换机 B 在 VRRP 备份组 2 中的优先级。

```
[SWB-Vlan-interface2]vrrp ipv6 vrid 2 riority 110
```

(3) 配置完成后，可以在交换机 SWA、SWB 上通过 display vrrp 命令查看配置后的结果。

```
[SWA] display vrrp ipv6 verbose
 IPv6 Standby Information:
     Run Mode          : Standard
     Run Method        : Virtual MAC
 Total number of virtual routers : 2
   Interface Vlan-interface 2
     VRID              : 1                 Adver Timer   : 100
     Admin Status      : Up                State         : Master
```

```
    Config Pri          : 110                Running Pri    : 110
    Preempt Mode        : Yes                Delay Time     : 0
    Auth Type           : None
    Virtual IP          : FE80::10
                          1::10
    Virtual MAC         : 0000-5e00-0201
    Master IP           : FE80::1

  Interface Vlan-interface 3
    VRID                : 2                  Adver Timer    : 100
    Admin Status        : Up                 State          : Backup
    Config Pri          : 100                Running Pri    : 100
    Preempt Mode        : Yes                Delay Time     : 0
    Auth Type           : None
    Virtual IP          : FE90::10
                          2::10
    Master IP           : FE90::2

[SWB] display vrrp ipv6 verbose
 IPv6 Standby Information:
    Run Mode            : Standard
    Run Method          : Virtual MAC
 Total number of virtual routers : 2
   Interface Vlan-interface 2
    VRID                : 1                  Adver Timer    : 100
    Admin Status        : Up                 State          : Backup
    Config Pri          : 100                Running Pri    : 100
    Preempt Mode        : Yes                Delay Time     : 0
    Auth Type           : None
    Virtual IP          : FE80::10
                          1::10
    Master IP           : FE80::1

   Interface Vlan-interface 3
    VRID                : 2                  Adver Timer    : 100
    Admin Status        : Up                 State          : Master
    Config Pri          : 110                Running Pri    : 110
    Preempt Mode        : Yes                Delay Time     : 0
    Auth Type           : None
    Virtual IP          : FE90::10
                          2::10
    Virtual MAC         : 0000-5e00-0202
    Master IP           : FE90::2
```

从上述显示信息可以看出，正常情况下，在备份组 1 中 Switch A 为 Master 路由器，Switch B 为 Backup 路由器，默认网关为 1::10/64 的主机通过 Switch A 访问 Internet；备份组 2 中 Switch A 为 Backup 路由器，Switch B 为 Master 路由器，默认网关为 2::10/64 的主机通过 Switch B 访问 Internet。

13.3 RRPP典型配置指导

RRPP(Rapid Ring Protection Protocol,快速环网保护协议)是一个专门应用于以太网环的链路层协议。它在以太网环完整时能够防止数据环路引起的广播风暴,而当以太网环上一条链路断开时能迅速恢复环网上各个节点之间的通信通路。

和STP协议相比,RRPP协议的特点为:拓扑收敛速度快和拓扑收敛时间与环网上的节点数无关。

13.3.1 RRPP单环拓扑典型配置指导

1. 背景

T运营商组建了一个以太城域网,计划给用户提供高品质的网络服务。负责网络建设的集成商经过前期准备调研,认为RRPP协议能够满足用户网络高可靠性的要求,故准备在网络中部署RRPP。

2. 组网图

图13-11所示为RRPP单环拓扑典型配置示意图。

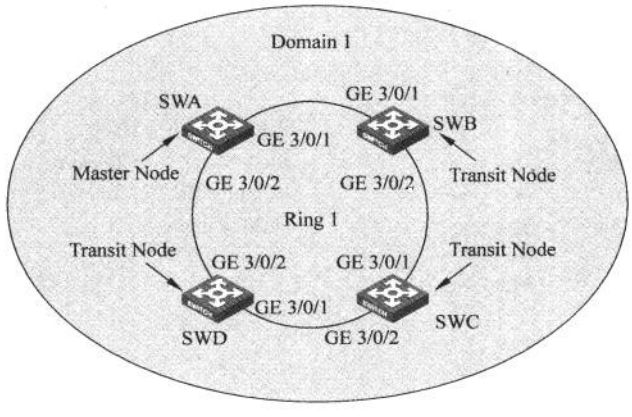


图13-11 RRPP单环拓扑典型配置示意图

3. 配置需求

如图13-11所示,网络管理员对光纤连接的交换机SWA、SWB、SWC、SWD配置RRPP。网络管理员要求通过配置达到下列要求。

(1) SWA、SWB、SWC和SWD构成RRPP域1,该域的控制VLAN为VLAN 4092,保护VLAN为VLAN 1～VLAN 30。

(2) SWA、SWB、SWC和SWD构成主环1。

(3) SWA为主环的主节点,GigabitEthernet 3/0/1为主端口,GigabitEthernet 3/0/2为副端口。

(4) SWB、SWC和SWD为主环的传输节点,各自的GigabitEthernet 3/0/1为主端口,GigabitEthernet 3/0/2为副端口。

4. 配置过程和解释

(1) 在交换机 SWA 上配置 RRPP。

① 创建 VLAN 1～VLAN 30,将这些 VLAN 都映射到 MSTP 实例 1 上,并激活 MST 域的配置。

```
<SWA> system-view
[SWA] vlan 1 to 30
[SWA] stp region-configuration
[SWA-mst-region] instance 1 vlan 1 to 30
[SWA-mst-region] active region-configuration
```

② 分别在端口 GigabitEthernet 3/0/1 和 GigabitEthernet 3/0/2 上配置物理连接状态 Up/Down 抑制时间为 0s,关闭 STP 功能,并将端口配置为 Trunk 端口且允许 VLAN 1～VLAN 30 通过。

```
[SWA] interface GigabitEthernet 3/0/1
[SWA-GigabitEthernet3/0/1] link-delay 0
[SWA-GigabitEthernet3/0/1] undo stp enable
[SWA-GigabitEthernet3/0/1] port link-type trunk
[SWA-GigabitEthernet3/0/1] port trunk permit vlan 1 to 30
[SWA] interface GigabitEthernet 3/0/2
[SWA-GigabitEthernet3/0/2] link-delay 0
[SWA-GigabitEthernet3/0/2] undo stp enable
[SWA-GigabitEthernet3/0/2] port link-type trunk
[SWA-GigabitEthernet3/0/2] port trunk permit vlan 1 to 30
```

③ 创建 RRPP 域 1,将 VLAN 4092 配置为该域的控制 VLAN,并将 MSTP 实例 1 所映射的 VLAN 配置为该域的保护 VLAN。

```
[SWA] rrpp domain 1
[SWA-rrpp-domain1] control-vlan 4092
[SWA-rrpp-domain1] protected-vlan reference-instance 1
```

④ 配置本设备为主环 1 的主节点,主端口为 GigabitEthernet 3/0/1,副端口为 GigabitEthernet 3/0/2,并使能该环。

```
[SWA-rrpp-domain1] ring 1 node-mode master primary-port GigabitEthernet 3/0/1 secondary-port
GigabitEthernet 3/0/2 level 0
[SWA-rrpp-domain1] ring 1 enable
```

⑤ 使能 RRPP 协议。

```
[SWA] rrpp enable
```

(2) 在交换机 SWB 上配置 RRPP。

① 创建 VLAN 1～VLAN 30,将这些 VLAN 都映射到 MSTP 实例 1 上,并激活 MST 域的配置。

```
<SWB> system-view
[SWB] vlan 1 to 30
[SWB] stp region-configuration
```

```
[SWB-mst-region] instance 1 vlan 1 to 30
[SWB-mst-region] active region-configuration
[SWB-mst-region] quit
```

② 分别在端口 GigabitEthernet 3/0/1 和 GigabitEthernet 3/0/2 上配置物理连接状态 Up/Down 抑制时间为 0s，关闭 STP 功能，并将端口配置为 Trunk 端口且允许 VLAN 1～VLAN 30 通过。

```
[SWB] interface GigabitEthernet 3/0/1
[SWB-GigabitEthernet3/0/1] link-delay 0
[SWB-GigabitEthernet3/0/1] undo stp enable
[SWB-GigabitEthernet3/0/1] port link-type trunk
[SWB-GigabitEthernet3/0/1] port trunk permit vlan 1 to 30
[SWB] interface GigabitEthernet 3/0/2
[SWB-GigabitEthernet3/0/2] link-delay 0
[SWB-GigabitEthernet3/0/2] undo stp enable
[SWB-GigabitEthernet3/0/2] port link-type trunk
[SWB-GigabitEthernet3/0/2] port trunk permit vlan 1 to 30
```

③ 创建 RRPP 域 1，将 VLAN 4092 配置为该域的控制 VLAN，并将 MSTP 实例 1 所映射的 VLAN 配置为该域的保护 VLAN。

```
[SWB] rrpp domain 1
[SWB-rrpp-domain1] control-vlan 4092
[SWB-rrpp-domain1] protected-vlan reference-instance 1
```

④ 配置本设备为主环 1 的传输节点，主端口为 GigabitEthernet 3/0/1，副端口为 GigabitEthernet 3/0/2，并使能该环。

```
[SWB-rrpp-domain1] ring 1 node-mode transit primary-port GigabitEthernet 3/0/1 secondary-port
GigabitEthernet 3/0/2 level 0
[SWB-rrpp-domain1] ring 1 enable
```

⑤ 使能 RRPP 协议。

```
[SWB] rrpp enable
```

(3) SWC、SWD 的配置与 SWB 相似，配置过程略。

配置完成后，用户可以使用 dis rrpp verbose 命令查看各设备上 RRPP 的配置和运行情况。

提示： 在配置 RRPP 环之前必须先配置控制 VLAN。

为 RRPP 域配置的控制 VLAN 必须是设备上没有创建过的 VLAN。

13.3.2 RRPP 相交环拓扑典型配置指导

1. 背景

T 运营商在规划以太城域网时，规划成二级结构，即骨干网是环网，每个接入设备双上行接入到骨干网上。基于这种结构，T 运营商在骨干网上配置了 RRPP 主环，同时还需要在接入设备与骨干网设备间配置 RRPP 子环。

2. 组网图

图 13-12 所示为 RRPP 相交环拓扑典型配置示意图。

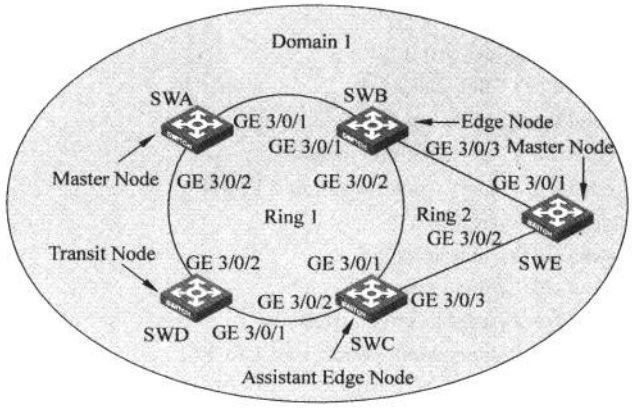


图 13-12 RRPP 相交环拓扑典型配置示意图

3. 配置需求

如图 13-12 所示，网络管理员对光纤连接的交换机 SWA、SWB、SWC、SWD、SWE 配置 RRPP。网络管理员要求通过配置达到下列要求。

(1) SWA、SWB、SWC、SWD 和 SWE 构成 RRPP 域 1，该域的控制 VLAN 为 VLAN 4092，保护 VLAN 为 VLAN 1～VLAN 30。

(2) SWA、SWB、SWC 和 SWD 构成主环 1，SWB、SWC 和 SWE 构成子环 2。

(3) SWA 为主环的主节点，GigabitEthernet 3/0/1 为主端口，GigabitEthernet 3/0/2 为副端口。

(4) SWE 为子环的主节点，GigabitEthernet 3/0/1 为主端口，GigabitEthernet 3/0/2 为副端口。

(5) SWB 为主环的传输节点和子环的边缘节点，GigabitEthernet 3/0/3 为边缘端口。

(6) SWC 为主环的传输节点和子环的辅助边缘节点，GigabitEthernet 3/0/3 为边缘端口。

(7) SWD 为主环的传输节点，GigabitEthernet 3/0/1 为主端口，GigabitEthernet 3/0/2 为副端口。

4. 配置过程和解释

(1) 在交换机 SWA 上配置 RRPP。

① 创建 VLAN 1～VLAN 30，将这些 VLAN 都映射到 MSTP 实例 1 上，并激活 MST 域的配置。

```
<SWA> system-view
[SWA] vlan 1 to 30
[SWA] stp region-configuration
[SWA-mst-region] instance 1 vlan 1 to 30
[SWA-mst-region] active region-configuration
[SWA-mst-region] quit
```

② 分别在端口 GigabitEthernet 3/0/1 和 GigabitEthernet 3/0/2 上配置物理连接状态 Up/Down 抑制时间为 0s，关闭 STP 功能，并将端口配置为 Trunk 端口且允许 VLAN 1～VLAN 30 通过。

```
[SWA] interface GigabitEthernet 3/0/1
[SWA-GigabitEthernet3/0/1] link-delay 0
[SWA-GigabitEthernet3/0/1] undo stp enable
[SWA-GigabitEthernet3/0/1] port link-type trunk
[SWA-GigabitEthernet3/0/1] port trunk permit vlan 1 to 30
[SWA] interface gigabitethernet 3/0/2
[SWA-GigabitEthernet3/0/2] link-delay 0
[SWA-GigabitEthernet3/0/2] undo stp enable
[SWA-GigabitEthernet3/0/2] port link-type trunk
[SWA-GigabitEthernet3/0/2] port trunk permit vlan 1 to 30
```

③ 创建 RRPP 域 1，将 VLAN 4092 配置为该域的控制 VLAN，并将 MSTP 实例 1 所映射的 VLAN 配置为该域的保护 VLAN。

```
[SWA] rrpp domain 1
[SWA-rrpp-domain1] control-vlan 4092
[SWA-rrpp-domain1] protected-vlan reference-instance 1
```

④ 设置 Switch A 为主环 1 的主节点，主端口为 GigabitEthernet 3/0/1，副端口为 GigabitEthernet 3/0/2，并使能该环。

```
[SWA-rrpp-domain1] ring 1 node-mode master primary-port GigabitEthernet 3/0/1 secondary-port
GigabitEthernet 3/0/2 level 0
[SWA-rrpp-domain1] ring 1 enable
[SWA-rrpp-domain1] quit
```

⑤ 使能 RRPP 协议。

```
[SWA] rrpp enable
```

(2) 在交换机 SWB 上配置 RRPP。

① 创建 VLAN 1～VLAN 30，将这些 VLAN 都映射到 MSTP 实例 1 上，并激活 MST 域的配置。

```
<SWB> system-view
[SWB] vlan 1 to 30
[SWB] stp region-configuration
[SWB-mst-region] instance 1 vlan 1 to 30
[SWB-mst-region] active region-configuration
[SWB-mst-region] quit
```

② 分别在端口 GigabitEthernet 3/0/1、GigabitEthernet 3/0/2 和 GigabitEthernet 3/0/3 上配置物理连接状态Up/Down 抑制时间为 0s，关闭 STP 功能，并将端口配置为 Trunk 端口且允许 VLAN 1～VLAN 30 通过。

```
[SWB] interface GigabitEthernet 3/0/1
[SWB-GigabitEthernet3/0/1] link-delay 0
[SWB-GigabitEthernet3/0/1] undo stp enable
[SWB-GigabitEthernet3/0/1] port link-type trunk
[SWB-GigabitEthernet3/0/1] port trunk permit vlan 1 to 30
[SWB] interface GigabitEthernet 3/0/2
[SWB-GigabitEthernet3/0/2] link-delay 0
[SWB-GigabitEthernet3/0/2] undo stp enable
[SWB-GigabitEthernet3/0/2] port link-type trunk
[SWB-GigabitEthernet3/0/2] port trunk permit vlan 1 to 30
[SWB] interface GigabitEthernet 3/0/3
[SWB-GigabitEthernet3/0/3] link-delay 0
[SWB-GigabitEthernet3/0/3] undo stp enable
[SWB-GigabitEthernet3/0/3] port link-type trunk
[SWB-GigabitEthernet3/0/3] port trunk permit vlan 1 to 30
```

③ 创建 RRPP 域 1，将 VLAN 4092 配置为该域的控制 VLAN，并将 MSTP 实例 1 所映射的 VLAN 配置为该域的保护 VLAN。

```
[SWB] rrpp domain 1
[SWB-rrpp-domain1] control-vlan 4092
[SWB-rrpp-domain1] protected-vlan reference-instance 1
```

④ 配置本设备为主环 1 的传输节点，主端口为 GigabitEthernet 3/0/1，副端口为 GigabitEthernet 3/0/2，并使能该环。

```
[SWB-rrpp-domain1] ring 1 node-mode transit primary-port GigabitEthernet 3/0/1 secondary-port
GigabitEthernet 3/0/2 level 0
[SWB-rrpp-domain1] ring 1 enable
```

⑤ 配置本设备为子环 2 的边缘节点，边缘端口为 GigabitEthernet 3/0/3，并使能该环。

```
[SWB-rrpp-domain1] ring 2 node-mode edge edge-port GigabitEthernet 3/0/3
[SWB-rrpp-domain1] ring 2 enable
[SWB-rrpp-domain1] quit
```

⑥ 使能 RRPP 协议。

```
[SWB] rrpp enable
```

(3) 在交换机 SWC 上配置 RRPP。

① 创建 VLAN 1～VLAN 30，将这些 VLAN 都映射到 MSTP 实例 1 上，并激活 MST 域的配置。

```
<SWC> system-view
[SWC] vlan 1 to 30
[SWC] stp region-configuration
[SWC-mst-region] instance 1 vlan 1 to 30
[SWC-mst-region] active region-configuration
[SWC-mst-region] quit
```

② 分别在端口 GigabitEthernet 3/0/1、GigabitEthernet 3/0/2 和GigabitEthernet 3/0/3上配置物理连接状态Up/Down 抑制时间为 0s，关闭 STP 功能，并将端口配置为 Trunk 端口且允许 VLAN 1～VLAN 30 通过。

```
[SWC] interface GigabitEthernet 3/0/1
[SWC-GigabitEthernet3/0/1] link-delay 0
[SWC-GigabitEthernet3/0/1] undo stp enable
[SWC-GigabitEthernet3/0/1] port link-type trunk
[SWC-GigabitEthernet3/0/1] port trunk permit vlan 1 to 30
[SWC] interface GigabitEthernet 3/0/2
[SWC-GigabitEthernet3/0/2] link-delay 0
[SWC-GigabitEthernet3/0/2] undo stp enable
[SWC-GigabitEthernet3/0/2] port link-type trunk
[SWC-GigabitEthernet3/0/2] port trunk permit vlan 1 to 30
[SWC] interface GigabitEthernet 3/0/3
[SWC-GigabitEthernet3/0/3] link-delay 0
[SWC-GigabitEthernet3/0/3] undo stp enable
[SWC-GigabitEthernet3/0/3] port link-type trunk
[SWC-GigabitEthernet3/0/3] port trunk permit vlan 1 to 30
```

③ 创建 RRPP 域 1，将 VLAN 4092 配置为该域的控制 VLAN，并将 MSTP 实例 1 所映射的 VLAN 配置为该域的保护 VLAN。

```
[SWC] rrpp domain 1
[SWC-rrpp-domain1] control-vlan 4092
[SWC-rrpp-domain1] protected-vlan reference-instance 1
```

④ 配置本设备为主环 1 的传输节点，主端口为 GigabitEthernet 3/0/1，副端口为 GigabitEthernet 3/0/2，并使能该环。

```
[SWC-rrpp-domain1] ring 1 node-mode transit primary-port GigabitEthernet 3/0/1 secondary-port
GigabitEthernet 3/0/2 level 0
[SWC-rrpp-domain1] ring 1 enable
```

⑤ 配置本设备为子环 2 的辅助边缘节点，边缘端口为 GigabitEthernet 3/0/3，并使能该环。

```
[SWC-rrpp-domain1] ring 2 node-mode assistant-edge edge-port GigabitEthernet 3/0/3
[SWC-rrpp-domain1] ring 2 enable
[SWC-rrpp-domain1] quit
```

⑥ 使能 RRPP 协议。

```
[SWC] rrpp enable
```

(4) 在交换机 SWD 上配置 RRPP。

① 创建 VLAN 1～VLAN 30，将这些 VLAN 都映射到 MSTP 实例 1 上，并激活 MST 域的配置。

```
<SWD> system-view
```

```
[SWD] vlan 1 to 30
[SWD] stp region-configuration
[SWD-mst-region] instance 1 vlan 1 to 30
[SWD-mst-region] active region-configuration
[SWD-mst-region] quit
```

② 分别在端口 GigabitEthernet 3/0/1 和 GigabitEthernet 3/0/2 上配置物理连接状态 Up/Down 抑制时间为 0s，关闭 STP 功能，并将端口配置为 Trunk 端口且允许 VLAN 1～VLAN 30 通过。

```
[SWD] interface GigabitEthernet 3/0/1
[SWD-GigabitEthernet3/0/1] link-delay 0
[SWD-GigabitEthernet3/0/1] undo stp enable
[SWD-GigabitEthernet3/0/1] port link-type trunk
[SWD-GigabitEthernet3/0/1] port trunk permit vlan 1 to 30
[SWD-GigabitEthernet3/0/1] quit
[SWD] interface GigabitEthernet 3/0/2
[SWD-GigabitEthernet3/0/2] link-delay 0
[SWD-GigabitEthernet3/0/2] undo stp enable
[SWD-GigabitEthernet3/0/2] port link-type trunk
[SWD-GigabitEthernet3/0/2] port trunk permit vlan 1 to 30
[SWD-GigabitEthernet3/0/2] quit
```

③ 创建 RRPP 域 1，将 VLAN 4092 配置为该域的控制 VLAN，并将 MSTP 实例 1 所映射的 VLAN 配置为该域的保护 VLAN。

```
[SWD] rrpp domain 1
[SWD-rrpp-domain1] control-vlan 4092
[SWD-rrpp-domain1] protected-vlan reference-instance 1
```

④ 配置本设备为主环 1 的传输节点，主端口为 GigabitEthernet 3/0/1，副端口为 GigabitEthernet 3/0/2，并使能该环。

```
[SWD-rrpp-domain1] ring 1 node-mode transit primary-port GigabitEthernet 3/0/1 secondary-port
GigabitEthernet 3/0/2 level 0
[SWD-rrpp-domain1] ring 1 enable
[SWD-rrpp-domain1] quit
```

⑤ 使能 RRPP 协议。

```
[SWD] rrpp enable
```

(5) 在交换机 SWE 上配置 RRPP。

① 创建 VLAN 1～VLAN 30，将这些 VLAN 都映射到 MSTP 实例 1 上，并激活 MST 域的配置。

```
<SWE> system-view
[SWE] vlan 1 to 30
[SWE] stp region-configuration
[SWE-mst-region] instance 1 vlan 1 to 30
```

```
[SWE-mst-region] active region-configuration
[SWE-mst-region] quit
```

② 分别在端口 GigabitEthernet 3/0/1 和 GigabitEthernet 3/0/2 上配置物理连接状态 Up/Down 抑制时间为 0s，关闭 STP 功能，并将端口配置为 Trunk 端口且允许 VLAN 1～VLAN 30 通过。

```
[SWE] interface GigabitEthernet 3/0/1
[SWE-GigabitEthernet3/0/1] link-delay 0
[SWE-GigabitEthernet3/0/1] undo stp enable
[SWE-GigabitEthernet3/0/1] port link-type trunk
[SWE-GigabitEthernet3/0/1] port trunk permit vlan 1 to 30
[SWE-GigabitEthernet3/0/1] quit
[SWE] interface GigabitEthernet 3/0/2
[SWE-GigabitEthernet3/0/2] link-delay 0
[SWE-GigabitEthernet3/0/2] undo stp enable
[SWE-GigabitEthernet3/0/2] port link-type trunk
[SWE-GigabitEthernet3/0/2] port trunk permit vlan 1 to 30
[SWE-GigabitEthernet3/0/2] quit
```

③ 创建 RRPP 域 1，将 VLAN 4092 配置为该域的控制 VLAN，并将 MSTP 实例 1 所映射的 VLAN 配置为该域的保护 VLAN。

```
[SWE] rrpp domain 1
[SWE-rrpp-domain1] control-vlan 4092
[SWE-rrpp-domain1] protected-vlan reference-instance 1
```

④ 配置本设备为子环 2 的主节点，主端口为 GigabitEthernet 3/0/1，副端口为 GigabitEthernet 3/0/2，并使能该环。

```
[SWE-rrpp-domain1] ring 2 node-mode master primary-port GigabitEthernet 3/0/1 secondary-port
GigabitEthernet 3/0/2 level 1
[SWE-rrpp-domain1] ring 2 enable
```

⑤ 使能 RRPP 协议。

```
[SWE] rrpp enable
```

配置完成后，用户可以使用 display rrpp verbose 命令查看各设备上 RRPP 的配置和运行情况。

提示：配置 RRPP 环之前，必须配置保护 VLAN。

13.3.3 RRPP 相交环负载分担典型配置指导

1. 背景

T 运营商的业务越来越多，环网中的数据流量也越来越多。为了合理利用链路的带宽，运维部门规划部署 RRPP 的负载分担，将各 VLAN 的数据流量分布到不同的链路上。

2. 组网图

图 13-13 所示为 RRPP 相交环负载分担典型配置示意图。

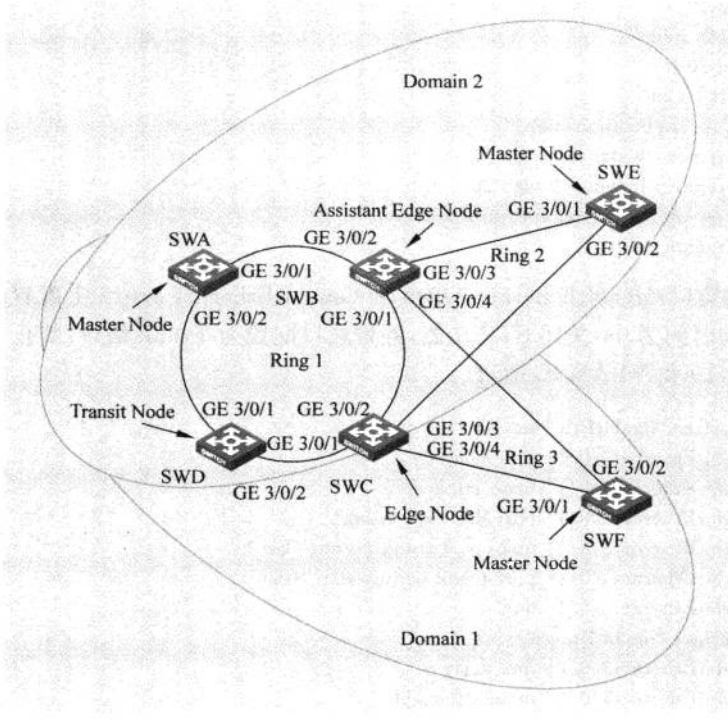


图 13-13 RRPP 相交环负载分担典型配置示意图

3. 配置需求

如图 13-13 所示，网络管理员对光纤连接的交换机配置 RRPP。网络管理员要求通过配置达到下列要求。

(1) SWA、SWB、SWC、SWD 和 SWF 构成 RRPP 域 1，该域的控制 VLAN 为 VLAN 100。在该域中，SWA 为主环 1 的主节点，SWD 为主环 1 的传输节点，SWF 为子环 3 的主节点，SWC 为子环 3 的边缘节点，SWB 为子环 3 的辅助边缘节点。

(2) SWA、SWB、SWC、SWD 和 SWE 构成 RRPP 域 2，该域的控制 VLAN 为 VLAN 105。在该域中，SWA 为主环 1 的主节点，SWD 为主环 1 的传输节点，SWE 为子环 2 的主节点，SWC 为子环 2 的边缘节点，SWB 为子环 2 的辅助边缘节点。

(3) RRPP 域 1 的保护 VLAN 为 VLAN 10，RRPP 域 2 的保护 VLAN 为 VLAN 20。由此可以按照 VLAN 在主环上实现负载分担。

(4) 由于子环 2 和子环 3 的边缘节点和辅助边缘节点的配置一样，并且对应的主环链路也相同，因此可以将子环 2 和子环 3 加入环组，从而减少 Edge-Hello 报文的收发数量。

4. 配置过程和解释

(1) 在交换机 SWA 上配置 RRPP。

① 创建 VLAN 10 和 VLAN 20，分别将 VLAN 10 映射到 MSTP 实例 1 上，VLAN 20

映射到 MSTP 实例 2 上，并激活 MST 域的配置。

```
<SWA> system-view
[SWA] vlan 10
[SWA-vlan10] quit
[SWA] vlan 20
[SWA-vlan20] quit
[SWA] stp region-configuration
[SWA-mst-region] instance 1 vlan 10
[SWA-mst-region] instance 2 vlan 20
[SWA-mst-region] active region-configuration
[SWA-mst-region] quit
```

② 分别在端口 GigabitEthernet 3/0/1 和 GigabitEthernet 3/0/2 上配置物理连接状态 Up/Down 抑制时间为 0s，关闭 STP 功能，并将端口配置为 Trunk 端口，禁止 VLAN 1 通过且允许 VLAN 10 和 VLAN 20 通过。

```
[SWA] interface GigabitEthernet 3/0/1
[SWA-GigabitEthernet3/0/1] link-delay 0
[SWA-GigabitEthernet3/0/1] undo stp enable
[SWA-GigabitEthernet3/0/1] port link-type trunk
[SWA-GigabitEthernet3/0/1] undo port trunk permit vlan 1
[SWA-GigabitEthernet3/0/1] port trunk permit vlan 10 20
[SWA-GigabitEthernet3/0/1] quit
[SWA] interface GigabitEthernet 3/0/2
[SWA-GigabitEthernet3/0/2] link-delay 0
[SWA-GigabitEthernet3/0/2] undo stp enable
[SWA-GigabitEthernet3/0/2] port link-type trunk
[SWA-GigabitEthernet3/0/2] undo port trunk permit vlan 1
[SWA-GigabitEthernet3/0/2] port trunk permit vlan 10 20
[SWA-GigabitEthernet3/0/2] quit
```

③ 创建 RRPP 域 1，将 VLAN 100 配置为该域的控制 VLAN，并将 MSTP 实例 1 所映射的 VLAN 配置为该域的保护 VLAN。

```
[SWA] rrpp domain 1
[SWA-rrpp-domain1] control-vlan 100
[SWA-rrpp-domain1] protected-vlan reference-instance 1
```

④ 在 RRPP 域 1 内配置本设备为主环 1 的主节点，主端口为 GigabitEthernet 3/0/1，副端口为 GigabitEthernet 3/0/2，并使能该环。

```
[SWA-rrpp-domain1] ring 1 node-mode master primary-port GigabitEthernet 3/0/1 secondary-port
GigabitEthernet 3/0/2 level 0
[SWA-rrpp-domain1] ring 1 enable
[SWA-rrpp-domain1] quit
```

⑤ 在 RRPP 域 2 内配置本设备为主环 1 的主节点，主端口为 GigabitEthernet 3/0/2，副端口为 GigabitEthernet 3/0/1，并使能该环。

```
[SWA-rrpp-domain2] ring 1 node-mode master primary-port GigabitEthernet 3/0/2 secondary-port
```

```
GigabitEthernet 3/0/1 level 0
[SWA-rrpp-domain2] ring 1 enable
[SWA-rrpp-domain2] quit
```

⑥ 使能 RRPP 协议。

```
[SWA] rrpp enable
```

(2) 在交换机 SWB 上配置 RRPP。

① 创建 VLAN 10 和 VLAN 20,分别将 VLAN 10 映射到 MSTP 实例 1 上,VLAN 20 映射到 MSTP 实例 2 上,并激活 MST 域的配置。

```
<SWB> system-view
[SWB] vlan 10
[SWB-vlan10] quit
[SWB] vlan 20
[SWB-vlan20] quit
[SWB] stp region-configuration
[SWB-mst-region] instance 1 vlan 10
[SWB-mst-region] instance 2 vlan 20
[SWB-mst-region] active region-configuration
[SWB-mst-region] quit
```

② 分别在端口 GigabitEthernet 3/0/1、GigabitEthernet 3/0/2 上配置物理连接状态 Up/Down 抑制时间为 0s,关闭 STP 功能,并将端口配置为 Trunk 端口,禁止 VLAN 1 通过且允许 VLAN 10 和 VLAN 20 通过。

```
[SWB] interface GigabitEthernet 3/0/1
[SWB-GigabitEthernet3/0/1] link-delay 0
[SWB-GigabitEthernet3/0/1] undo stp enable
[SWB-GigabitEthernet3/0/1] port link-type trunk
[SWB-GigabitEthernet3/0/1] undo port trunk permit vlan 1
[SWB-GigabitEthernet3/0/1] port trunk permit vlan 10 20
[SWB-GigabitEthernet3/0/1] quit
[SWB] interface GigabitEthernet 3/0/2
[SWB-GigabitEthernet3/0/2] link-delay 0
[SWB-GigabitEthernet3/0/2] undo stp enable
[SWB-GigabitEthernet3/0/2] port link-type trunk
[SWB-GigabitEthernet3/0/2] undo port trunk permit vlan 1
[SWB-GigabitEthernet3/0/2] port trunk permit vlan 10 20
[SWB-GigabitEthernet3/0/2] quit
```

③ 在端口 GigabitEthernet 3/0/3 上配置物理连接状态 Up/Down 抑制时间为 0s,关闭 STP 功能,并将端口配置为 Trunk 端口,禁止 VLAN 1 通过且允许 VLAN 20 通过。

```
[SWB] interface GigabitEthernet 3/0/3
[SWB-GigabitEthernet3/0/3] link-delay 0
[SWB-GigabitEthernet3/0/3] undo stp enable
[SWB-GigabitEthernet3/0/3] port link-type trunk
[SWB-GigabitEthernet3/0/3] undo port trunk permit vlan 1
[SWB-GigabitEthernet3/0/3] port trunk permit vlan 20
```

```
[SWB-GigabitEthernet3/0/3] quit
```

④ 在端口 GigabitEthernet 3/0/4 上配置物理连接状态 Up/Down 抑制时间为 0s，关闭 STP 功能，并将端口配置为 Trunk 端口，禁止 VLAN 1 通过且允许 VLAN 10 通过。

```
[SWB] interface GigabitEthernet 3/0/4
[SWB-GigabitEthernet3/0/4] link-delay 0
[SWB-GigabitEthernet3/0/4] undo stp enable
[SWB-GigabitEthernet3/0/4] port link-type trunk
[SWB-GigabitEthernet3/0/4] undo port trunk permit vlan 1
[SWB-GigabitEthernet3/0/4] port trunk permit vlan 10
[SWB-GigabitEthernet3/0/4] quit
```

⑤ 创建 RRPP 域 1，将 VLAN 100 配置为该域的控制 VLAN，并将 MSTP 实例 1 所映射的 VLAN 配置为该域的保护 VLAN。

```
[SWB] rrpp domain 1
[SWB-rrpp-domain1] control-vlan 100
[SWB-rrpp-domain1] protected-vlan reference-instance 1
```

⑥ 在 RRPP 域 1 内配置本设备为主环 1 的传输节点，主端口为 GigabitEthernet 3/0/1，副端口为 GigabitEthernet 3/0/2，并使能该环。

```
[SWB-rrpp-domain1] ring 1 node-mode transit primary-port GigabitEthernet 3/0/1 secondary-port
GigabitEthernet 3/0/2 level 0
[SWB-rrpp-domain1] ring 1 enable
```

⑦ 在 RRPP 域 1 内配置本设备为子环 3 的辅助边缘节点，边缘端口为GigabitEthernet 3/0/4，并使能该环。

```
[SWB-rrpp-domain1] ring 3 node-mode assistant-edge edge-port GigabitEthernet 3/0/4
[SWB-rrpp-domain1] ring 3 enable
[SWB-rrpp-domain1] quit
```

⑧ 创建 RRPP 域 2，将 VLAN 105 配置为该域的控制 VLAN，并将 MSTP 实例 2 所映射的 VLAN 配置为该域的保护 VLAN。

```
[SWB] rrpp domain 2
[SWB-rrpp-domain2] control-vlan 105
[SWB-rrpp-domain2] protected-vlan reference-instance 2
```

⑨ 在 RRPP 域 2 内配置本设备为主环 1 的传输节点，主端口为 GigabitEthernet 3/0/1，副端口为 GigabitEthernet 3/0/2，并使能该环。

```
[SWB-rrpp-domain2] ring 1 node-mode transit primary-port GigabitEthernet 3/0/1 secondary-port
GigabitEthernet 3/0/2 level 0
[SWB-rrpp-domain2] ring 1 enable
```

⑩ 在 RRPP 域 2 内配置本设备为子环 2 的辅助边缘节点，边缘端口为 GigabitEthernet 3/0/3，并使能该环。

```
[SWB-rrpp-domain2] ring 2 node-mode assistant-edge edge-port GigabitEthernet 3/0/3
```

```
[SWB-rrpp-domain2] ring 2 enable
[SWB-rrpp-domain2] quit
```

⑪ 使能 RRPP 协议。

```
[SWB] rrpp enable
```

(3) 在交换机 SWC 上配置 RRPP。

① 创建 VLAN 10 和 VLAN 20,分别将 VLAN 10 映射到 MSTP 实例 1 上,VLAN 20 映射到 MSTP 实例 2 上,并激活 MST 域的配置。

```
<SWC> system-view
[SWC] vlan 10
[SWC-vlan10] quit
[SWC] vlan 20
[SWC-vlan20] quit
[SWC] stp region-configuration
[SWC-mst-region] instance 1 vlan 10
[SWC-mst-region] instance 2 vlan 20
[SWC-mst-region] active region-configuration
[SWC-mst-region] quit
```

② 分别在端口 GigabitEthernet 3/0/1、GigabitEthernet 3/0/2 上配置物理连接状态 Up/Down 抑制时间为 0s,关闭 STP 功能,并将端口配置为 Trunk 端口,禁止 VLAN 1 通过且允许 VLAN 10 和 VLAN 20 通过。

```
[SWC] interface GigabitEthernet 3/0/1
[SWC-GigabitEthernet3/0/1] link-delay 0
[SWC-GigabitEthernet3/0/1] undo stp enable
[SWC-GigabitEthernet3/0/1] port link-type trunk
[SWC-GigabitEthernet3/0/1] undo port trunk permit vlan 1
[SWC-GigabitEthernet3/0/1] port trunk permit vlan 10 20
[SWC-GigabitEthernet3/0/1] quit
[SWC] interface GigabitEthernet 3/0/2
[SWC-GigabitEthernet3/0/2] link-delay 0
[SWC-GigabitEthernet3/0/2] undo stp enable
[SWC-GigabitEthernet3/0/2] port link-type trunk
[SWC-GigabitEthernet3/0/2] undo port trunk permit vlan 1
[SWC-GigabitEthernet3/0/2] port trunk permit vlan 10 20
[SWC-GigabitEthernet3/0/2] quit
```

③ 在端口 GigabitEthernet 3/0/3 上配置物理连接状态 Up/Down 抑制时间为 0s,关闭 STP 功能,并将端口配置为 Trunk 端口,禁止 VLAN 1 通过且允许 VLAN 20 通过。

```
[SWC] interface GigabitEthernet 3/0/3
[SWC-GigabitEthernet3/0/3] link-delay 0
[SWC-GigabitEthernet3/0/3] undo stp enable
[SWC-GigabitEthernet3/0/3] port link-type trunk
[SWC-GigabitEthernet3/0/3] undo port trunk permit vlan 1
[SWC-GigabitEthernet3/0/3] port trunk permit vlan 20
[SWC-GigabitEthernet3/0/3] quit
```

④ 在端口 GigabitEthernet 3/0/4 上配置物理连接状态 Up/Down 抑制时间为 0s，关闭 STP 功能，并将端口配置为 Trunk 端口，禁止 VLAN 1 通过且允许 VLAN 10 通过。

```
[SWC] interface GigabitEthernet 3/0/4
[SWC-GigabitEthernet3/0/4] link-delay 0
[SWC-GigabitEthernet3/0/4] undo stp enable
[SWC-GigabitEthernet3/0/4] port link-type trunk
[SWC-GigabitEthernet3/0/4] undo port trunk permit vlan 1
[SWC-GigabitEthernet3/0/4] port trunk permit vlan 10
[SWC-GigabitEthernet3/0/4] quit
```

⑤ 创建 RRPP 域 1，将 VLAN 100 配置为该域的控制 VLAN，并将 MSTP 实例 1 所映射的 VLAN 配置为该域的保护 VLAN。

```
[SWC] rrpp domain 1
[SWC-rrpp-domain1] control-vlan 100
[SWC-rrpp-domain1] protected-vlan reference-instance 1
```

⑥ 在 RRPP 域 1 内配置本设备为主环 1 的传输节点，主端口为 GigabitEthernet 3/0/1，副端口为 GigabitEthernet 3/0/2，并使能该环。

```
[SWC-rrpp-domain1] ring 1 node-mode transit primary-port GigabitEthernet 3/0/1 secondary-port
GigabitEthernet 3/0/2 level 0
[SWC-rrpp-domain1] ring 1 enable
```

⑦ 在 RRPP 域 1 内配置本设备为子环 3 的边缘节点，边缘端口为 GigabitEthernet 3/0/4，并使能该环。

```
[SWC-rrpp-domain1] ring 3 node-mode edge edge-port GigabitEthernet 3/0/4
[SWC-rrpp-domain1] ring 3 enable
[SWC-rrpp-domain1] quit
```

⑧ 创建 RRPP 域 2，将 VLAN 105 配置为该域的控制 VLAN，并将 MSTP 实例 2 所映射的 VLAN 配置为该域的保护 VLAN。

```
[SWC] rrpp domain 2
[SWC-rrpp-domain2] control-vlan 105
[SWC-rrpp-domain2] protected-vlan reference-instance 2
```

⑨ 在 RRPP 域 2 内配置本设备为主环 1 的传输节点，主端口为GigabitEthernet 3/0/1，副端口为 GigabitEthernet 3/0/2，并使能该环。

```
[SWC-rrpp-domain2] ring 1 node-mode transit primary-port GigabitEthernet 3/0/1 secondary-port
GigabitEthernet 3/0/2 level 0
[SWC-rrpp-domain2] ring 1 enable
```

⑩ 在 RRPP 域 2 内配置本设备为子环 2 的边缘节点，边缘端口为 GigabitEthernet 3/0/3，并使能该环。

```
[SWC-rrpp-domain2] ring 2 node-mode edge edge-port GigabitEthernet 3/0/3
[SWC-rrpp-domain2] ring 2 enable
[SWC-rrpp-domain2] quit
```

⑪ 使能 RRPP 协议。

```
[SWC] rrpp enable
```

(4) 在交换机 SWD 上配置 RRPP。

① 创建 VLAN 10 和 VLAN 20,分别将 VLAN 10 映射到 MSTP 实例 1 上,VLAN 20 映射到 MSTP 实例 2 上,并激活 MST 域的配置。

```
<SWD> system-view
[SWD] vlan 10
[SWD-vlan10] quit
[SWD] vlan 20
[SWD-vlan20] quit
[SWD] stp region-configuration
[SWD-mst-region] instance 1 vlan 10
[SWD-mst-region] instance 2 vlan 20
[SWD-mst-region] active region-configuration
[SWD-mst-region] quit
```

② 分别在端口 GigabitEthernet 3/0/1 和 GigabitEthernet 3/0/2 上配置物理连接状态 Up/Down 抑制时间为 0s,关闭 STP 功能,并将端口配置为 Trunk 端口,禁止 VLAN 1 通过且允许 VLAN 10 和 VLAN 20 通过。

```
[SWD] interface Gigabit Ethernet 3/0/1
[SWD-GigabitEthernet3/0/1] link-delay 0
[SWD-GigabitEthernet3/0/1] undo stp enable
[SWD-GigabitEthernet3/0/1] port link-type trunk
[SWD-GigabitEthernet3/0/1] undo port trunk permit vlan 1
[SWD-GigabitEthernet3/0/1] port trunk permit vlan 10 20
[SWD-GigabitEthernet3/0/1] quit
[SWD] interface GigabitEthernet 3/0/2
[SWD-GigabitEthernet3/0/2] link-delay 0
[SWD-GigabitEthernet3/0/2] undo stp enable
[SWD-GigabitEthernet3/0/2] port link-type trunk
[SWD-GigabitEthernet3/0/2] undo port trunk permit vlan 1
[SWD-GigabitEthernet3/0/2] port trunk permit vlan 10 20
[SWD-GigabitEthernet3/0/2] quit
```

③ 创建 RRPP 域 1,将 VLAN 100 配置为该域的控制 VLAN,并将 MSTP 实例 1 所映射的 VLAN 配置为该域的保护 VLAN。

```
[SWD] rrpp domain 1
[SWD-rrpp-domain1] control-vlan 100
[SWD-rrpp-domain1] protected-vlan reference-instance 1
```

④ 在 RRPP 域 1 内配置本设备为主环 1 的传输节点,主端口为 GigabitEthernet 3/0/1,副端口为 GigabitEthernet 3/0/2,并使能该环。

```
[SWD-rrpp-domain1] ring 1 node-mode transit primary-port GigabitEthernet 3/0/1 secondary-port
GigabitEthernet 3/0/2 level 0
[SWD-rrpp-domain1] ring 1 enable
```

```
[SWD-rrpp-domain1] quit
```

⑤ 创建 RRPP 域 2，将 VLAN 105 配置为该域的控制 VLAN，并将 MSTP 实例 2 所映射的 VLAN 配置为该域的保护 VLAN。

```
[SWD] rrpp domain 2
[SWD-rrpp-domain2] control-vlan 105
[SWD-rrpp-domain2] protected-vlan reference-instance 2
```

⑥ 在 RRPP 域 2 内配置本设备为主环 1 的传输节点，主端口为 GigabitEthernet 3/0/1，副端口为 GigabitEthernet 3/0/2，并使能该环。

```
[SWD-rrpp-domain2] ring 1 node-mode transit primary-port GigabitEthernet 3/0/1 secondary-port
GigabitEthernet 3/0/2 level 0
[SWD-rrpp-domain2] ring 1 enable
[SWD-rrpp-domain2] quit
```

⑦ 使能 RRPP 协议。

```
[SWD] rrpp enable
```

(5) 在交换机 SWE 上配置 RRPP。

① 创建 VLAN 20，将 VLAN 20 映射到 MSTP 实例 2 上，并激活 MST 域的配置。

```
<SWE> system-view
[SWE] vlan 20
[SWE-vlan20] quit
[SWE] stp region-configuration
[SWE-mst-region] instance 2 vlan 20
[SWE-mst-region] active region-configuration
[SWE-mst-region] quit
```

② 分别在端口 GigabitEthernet 3/0/1 和 GigabitEthernet 3/0/2 上配置物理连接状态 Up/Down 抑制时间为 0s，关闭 STP 功能，并将端口配置为 Trunk 端口，禁止 VLAN 1 通过且允许 VLAN 20 通过。

```
[SWE] interface GigabitEthernet 3/0/1
[SWE-GigabitEthernet3/0/1] link-delay 0
[SWE-GigabitEthernet3/0/1] undo stp enable
[SWE-GigabitEthernet3/0/1] port link-type trunk
[SWE-GigabitEthernet3/0/1] undo port trunk permit vlan 1
[SWE-GigabitEthernet3/0/1] port trunk permit vlan 20
[SWE-GigabitEthernet3/0/1] quit
[SWE] interface GigabitEthernet 3/0/2
[SWE-GigabitEthernet3/0/2] link-delay 0
[SWE-GigabitEthernet3/0/2] undo stp enable
[SWE-GigabitEthernet3/0/2] port link-type trunk
[SWE-GigabitEthernet3/0/2] undo port trunk permit vlan 1
[SWE-GigabitEthernet3/0/2] port trunk permit vlan 20
[SWE-GigabitEthernet3/0/2] quit
```

③ 创建 RRPP 域 2，将 VLAN 105 配置为该域的控制 VLAN，并将 MSTP 实例 2 所映射的 VLAN 配置为该域的保护 VLAN。

```
[SWE] rrpp domain 2
[SWE-rrpp-domain2] control-vlan 105
[SWE-rrpp-domain2] protected-vlan reference-instance 2
```

④ 在 RRPP 域 2 内配置本设备为子环 2 的主节点，主端口为 GigabitEthernet 3/0/2，副端口为 GigabitEthernet 3/0/1，并使能该环。

```
[SWE-rrpp-domain2] ring 2 node-mode master primary-port GigabitEthernet 3/0/2 secondary-port
GigabitEthernet 3/0/1 level 1
[SWE-rrpp-domain2] ring 2 enable
[SWE-rrpp-domain2] quit
```

⑤ 使能 RRPP 协议。

```
[SWE] rrpp enable
```

(6) 在交换机 SWF 上配置 RRPP。

① 创建 VLAN 10，将 VLAN 10 映射到 MSTP 实例 1 上，并激活 MST 域的配置。

```
<SWF> system-view
[SWF] vlan 10
[SWF-vlan10] quit
[SWF] stp region-configuration
[SWF-mst-region] instance 1 vlan 10
[SWF-mst-region] active region-configuration
[SWF-mst-region] quit
```

② 分别在端口 GigabitEthernet 3/0/1 和 GigabitEthernet 3/0/2 上配置物理连接状态 Up/Down 抑制时间为 0s，关闭 STP 功能，并将端口配置为 Trunk 端口，禁止 VLAN 1 通过且允许 VLAN 10 通过。

```
[SWF] interface GigabitEthernet 3/0/1
[SWF-GigabitEthernet3/0/1] link-delay 0
[SWF-GigabitEthernet3/0/1] undo stp enable
[SWF-GigabitEthernet3/0/1] port link-type trunk
[SWF-GigabitEthernet3/0/1] undo port trunk permit vlan 1
[SWF-GigabitEthernet3/0/1] port trunk permit vlan 10
[SWF-GigabitEthernet3/0/1] quit
[SWF] interface GigabitEthernet 3/0/2
[SWF-GigabitEthernet3/0/2] link-delay 0
[SWF-GigabitEthernet3/0/2] undo stp enable
[SWF-GigabitEthernet3/0/2] port link-type trunk
[SWF-GigabitEthernet3/0/2] undo port trunk permit vlan 1
[SWF-GigabitEthernet3/0/2] port trunk permit vlan 10
[SWF-GigabitEthernet3/0/2] quit
```

③ 创建 RRPP 域 1，将 VLAN 100 配置为该域的控制 VLAN，并将 MSTP 实例 1 所映

射的 VLAN 配置为该域的保护 VLAN。

```
[SWF] rrpp domain 1
[SWF-rrpp-domain1] control-vlan 100
[SWF-rrpp-domain1] protected-vlan reference-instance 1
```

④ 在 RRPP 域 2 内配置本设备为子环 3 的主节点，主端口为 GigabitEthernet 3/0/1，副端口为 GigabitEthernet 3/0/2，并使能该环。

```
[SWF-rrpp-domain1] ring 3 node-mode master primary-port GigabitEthernet 3/0/1 secondary-port
GigabitEthernet 3/0/2 level 1
[SWF-rrpp-domain1] ring 3 enable
[SWF-rrpp-domain1] quit
```

⑤ 使能 RRPP 协议。

```
[SWF] rrpp enable
```

(7) 完成以上配置后，在 SWB 和 SWC 上分别配置 RRPP 环组。

```
[SWB] rrpp ring-group 1
[SWB-rrpp-ring-group1] domain 2 ring 2
[SWB-rrpp-ring-group1] domain 1 ring 3
[SWC] rrpp ring-group 1
[SWC-rrpp-ring-group1] domain 2 ring 2
[SWC-rrpp-ring-group1] domain 1 ring 3
```

配置完成后，用户可以使用 display rrpp verbose 命令查看各设备上 RRPP 的配置和运行情况。

13.4 Smart Link 典型配置指导

如图 13-14 所示，双上行组网是目前常用组网之一。一般情况下，通过开启 STP (Spanning Tree Protocol，生成树协议)来实现网络中的链路冗余备份，但 STP 不适用于对收敛时间有很高要求的用户。

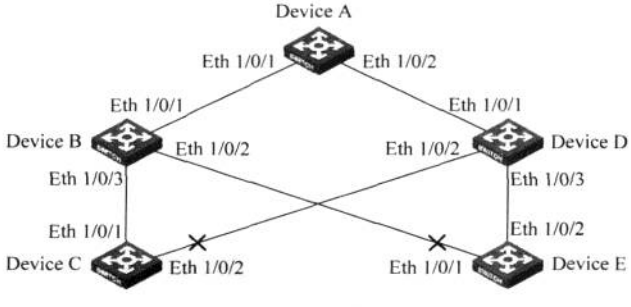


图 13-14 Smart Link 应用场景示意图

Smart Link 功能可以满足用户对链路快速收敛的需求，可以实现主备链路的冗余备份及其快速迁移。在双上行组网环境下，当主用链路出现故障时，设备自动将流量切换到备用

链路，这样就起到了冗余阻塞和链路备份的作用。

Smart Link 的主要特点是：专用于双上行组网；收敛速度快(达到亚秒级)；配置简单，便于用户操作。

13.4.1 单 Smart Link 组典型配置指导

1. 背景

M 公司网络架构是双上行组网，且对可靠性要求较高，所以网络管理员准备通过配置 Smart Link 来实现网络中的链路冗余备份。

2. 组网图

图 13-15 所示为单 Smart Link 组典型配置示意图。

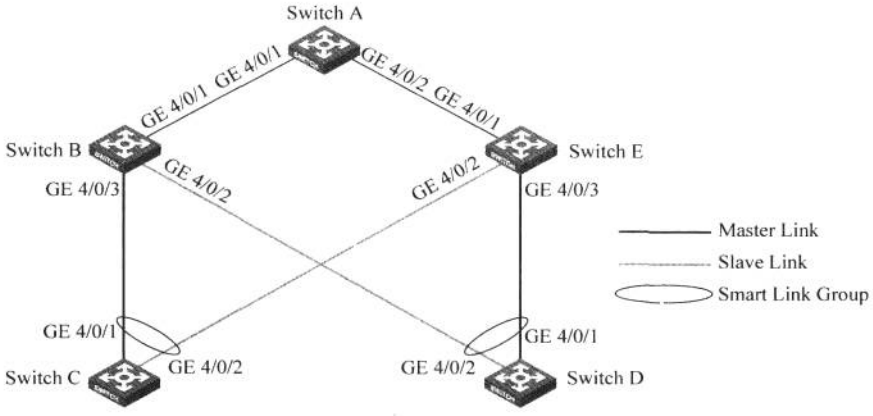


图 13-15 单 Smart Link 组典型配置示意图

3. 配置需求

如图 13-15 所示，网络管理员对光纤连接的交换机 SWA、SWB、SWC、SWD、SWE 配置 Smart Link。网络管理员要求通过配置达到下列要求。

(1) SWC、SWD 双上行到 Switch A。

(2) 双上行链路进行灵活备份。

(3) 在 VLAN 1 内发送和接收 Flush 报文。

4. 配置过程和解释

(1) 在交换机 SWC 上配置 Smart Link。

① 在相关端口上关闭 STP 功能。

```
<SWC> system-view
[SWC] interface GigabitEthernet 4/0/1
[SWC-GigabitEthernet4/0/1] stp disable
[SWC-GigabitEthernet4/0/1] interface GigabitEthernet 4/0/2
[SWC-GigabitEthernet4/0/2] stp disable
[SWC-GigabitEthernet4/0/2] quit
```

② 创建 Smart Link 组 1，并配置其保护 VLAN 为 MSTP 实例 0～15 所映射的 VLAN。

```
[SWC] smart-link group 1
```

```
[SWC-smlk-group1] protected-vlan reference-instance 0 to 15
```

③ 配置 Smart Link 组 1 的主端口为 GigabitEthernet 4/0/1，副端口为GigabitEthernet 4/0/2。

```
[SWC-smlk-group1] port GigabitEthernet 4/0/1 master
[SWC-smlk-group1] port GigabitEthernet 4/0/2 slave
```

④ 在 Smart Link 组 1 中使能发送 Flush 报文的功能。

```
[SWC-smlk-group1] flush enable
```

(2) 在交换机 SWD 上配置 Smart Link。

① 在相关端口上关闭 STP 功能。

```
<SWD> system-view
[SWD] interface GigabitEthernet 4/0/1
[SWD-GigabitEthernet4/0/1] stp disable
[SWD-GigabitEthernet4/0/1] interface GigabitEthernet 4/0/2
[SWD-GigabitEthernet4/0/2] stp disable
[SWD-GigabitEthernet4/0/2] quit
```

② 创建 Smart Link 组 1，并配置其保护 VLAN 为 MSTP 实例 0～15 所映射的 VLAN。

```
[SWD] smart-link group 1
[SWD-smlk-group1] protected-vlan reference-instance 0 to 15
```

③ 配置 Smart Link 组 1 的主端口为 GigabitEthernet 4/0/1，副端口为GigabitEthernet 4/0/2。

```
[SWD-smlk-group1] port GigabitEthernet 4/0/1 master
[SWD-smlk-group1] port GigabitEthernet 4/0/2 slave
```

④ 在 Smart Link 组 1 中使能发送 Flush 报文的功能。

```
[SWD-smlk-group1] flush enable
```

(3) 在交换机 SWB 上配置 Smart Link。在相关端口上使能接收 Flush 报文的功能。

```
<SWB> system-view
[SWB] interface GigabitEthernet 4/0/1
[SWB-GigabitEthernet4/0/1] smart-link flush enable
[SWB-GigabitEthernet4/0/1] interface GigabitEthernet 4/0/2
[SWB-GigabitEthernet4/0/2] smart-link flush enable
[SWB-GigabitEthernet4/0/2] interface GigabitEthernet 4/0/3
[SWB-GigabitEthernet4/0/3] smart-link flush enable
[SWB-GigabitEthernet4/0/3] quit
```

(4) 在交换机 SWE 上配置 Smart Link。在相关端口上使能接收 Flush 报文的功能。

```
<SWE> system-view
[SWE] interface GigabitEthernet 4/0/1
[SWE-GigabitEthernet4/0/1] smart-link flush enable
[SWE-GigabitEthernet4/0/1] interface GigabitEthernet 4/0/2
[SWE-GigabitEthernet4/0/2] smart-link flush enable
[SWE-GigabitEthernet4/0/2] interface GigabitEthernet 4/0/3
```

```
[SWE-GigabitEthernet4/0/3] smart-link flush enable
[SWE-GigabitEthernet4/0/3] quit
```

(5) 在交换机 SWA 上配置 Smart Link。在相关端口上关闭 STP 功能。

```
<SWA> system-view
[SWA] interface GigabitEthernet 4/0/1
[SWA-GigabitEthernet4/0/1] smart-link flush enable
[SWA-GigabitEthernet4/0/1] interface GigabitEthernet 4/0/2
[SWA-GigabitEthernet4/0/2] smart-link flush enable
[SWA-GigabitEthernet4/0/2] quit
```

(6) 配置完成后,用户可以通过使用 display smart-link group 命令可以查看各设备上 Smart Link 组的信息。

```
[SWC] display smart-link group 1
 Smart link group 1 information:
 Device ID: 000f-e23d-5af0
 Preemption mode: NONE
 Control VLAN: 1
 Protected VLAN: Reference Instance 0 to 15
 Member                    Role     State     Flush-count  Last-flush-time
 ------------------------------------------------------------------------------
 GigabitEthernet 4/0/1     MASTER   ACTVIE    5            16:37:20 2009/02/21
 GigabitEthernet 4/0/2     SLAVE    STANDBY   1            17:45:20 2009/02/21
```

提示：配置某端口为 Smart Link 组成员端口(即主端口和副端口)前,建议先手动关闭该端口,待 Smart Link 组配置完成后,再开启该端口,以避免形成环路,导致广播风暴。

13.4.2 多 Smart Link 组负载分担典型配置指导

1. 背景

网络管理员为了增强设备的利用率,准备配置多 Smart Link 组实现负载分担。

2. 组网图

图 13-16 所示为多 Smart Link 组负载分担典型配置示意图。

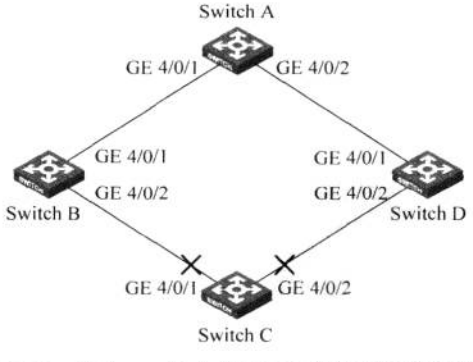


图 13-16 多 Smart Link 组负载分担典型配置示意图

3. 配置需求

如图 13-16 所示，网络管理员对光纤连接的交换机 SWA、SWB、SWC、SWD 配置 Smart Link。网络管理员要求通过配置达到下列要求。

(1) SWC 上 VLAN 1～VLAN 200 的流量通过 SWB、SWD 双上行到 SWA。要求进行负载分担，VLAN 1～VLAN 100 和 VLAN 101～VLAN 200 的两组流量分别通过不同的链路上行到 SWA。

(2) SWC 上进行双上行链路灵活备份，Smart Link 组 1 的引用实例 0(绑定 VLAN 1～VLAN 100)的流量从经过 SWB 所在的链路通向 SWA；而 Smart Link 组 2 的引用实例 2(绑定 VLAN 101～VLAN 200)的流量从经过 SWD 所在的链路通向 SWA。

(3) Smart Link 组 1 和组 2 分别在 VLAN 10 和 VLAN 101 内发送和接收 Flush 报文。

4. 配置过程和解释

(1) 在交换机 SWC 上配置 Smart Link。

① 创建 VLAN 1～VLAN 200，分别将 VLAN 1～VLAN 100 映射到 MSTP 实例 0 上，VLAN 101～VLAN 200 映射到 MSTP 实例 2 上，并激活 MST 域的配置。

```
<SWC> system-view
[SWC] vlan 1 to 200
[SWC] stp region-configuration
[SWC-mst-region] instance 0 vlan 1 to 100
[SWC-mst-region] instance 2 vlan 101 to 200
[SWC-mst-region] active region-configuration
```

② 关闭相关端口上的 STP 功能，并将端口配置为 Trunk 端口且允许 VLAN 1～VLAN 200 通过。

```
[SWC] interface GigabitEthernet 4/0/1
[SWC-GigabitEthernet4/0/1] stp disable
[SWC-GigabitEthernet4/0/1] port link-type trunk
[SWC-GigabitEthernet4/0/1] port trunk permit vlan 1 to 200
[SWC-GigabitEthernet4/0/1] interface GigabitEthernet 4/0/2
[SWC-GigabitEthernet4/0/2] stp disable
[SWC-GigabitEthernet4/0/2] port link-type trunk
[SWC-GigabitEthernet4/0/2] port trunk permit vlan 1 to 200
[SWC-GigabitEthernet4/0/2] quit
```

③ 创建 Smart Link 组 1，并配置其保护 VLAN 为 MSTP 实例 0 所映射的 VLAN。

```
[SWC] smart-link group 1
[SWC-smlk-group1] protected-vlan reference-instance 0
```

④ 配置 Smart Link 组 1 的主端口为 GigabitEthernet 4/0/1，副端口为GigabitEthernet 4/0/2。

```
[SWC-smlk-group1] port GigabitEthernet 4/0/1 master
[SWC-smlk-group1] port GigabitEthernet 4/0/2 slave
```

⑤ 在 Smart Link 组 1 中配置抢占模式为角色抢占模式；使能发送 Flush 报文的功能，并指定发送 Flush 报文的控制 VLAN 为 VLAN 10。

```
[SWC-smlk-group1] preemption mode role
[SWC-smlk-group1] flush enable control-vlan 10
[SWC-smlk-group1] quit
```

⑥ 创建 Smart Link 组 2，并配置其保护 VLAN 为 MSTP 实例 2 所映射的 VLAN。

```
[SWC] smart-link group 2
[SWC-smlk-group2] protected-vlan reference-instance 2
```

⑦ 配置 Smart Link 组 2 的副端口为 GigabitEthernet 4/0/1，主端口为GigabitEthernet 4/0/2。

```
[SWC-smlk-group2] port GigabitEthernet 4/0/1 slave
[SWC-smlk-group2] port GigabitEthernet 4/0/2 master
```

⑧ 在 Smart Link 组 2 中配置抢占模式为角色抢占模式；使能发送 Flush 报文的功能，并指定发送 Flush 报文的控制 VLAN 为 VLAN 101。

```
[SWC-smlk-group2] preemption mode role
[SWC-smlk-group2] flush enable control-vlan 101
[SWC-smlk-group2] quit
```

(2) 在交换机 SWB 上配置 Smart Link。

① 创建 VLAN 1～VLAN 200。

```
<SWB> system-view
[SWB] vlan 1 to 200
```

② 在相关端口上分别关闭 STP 功能，将端口配置为 Trunk 端口且允许 VLAN 1～VLAN 200 通过；使能接收 Flush 报文的功能，并指定接收 Flush 报文的控制 VLAN 为 VLAN 10 和 VLAN 101。

```
[SWB] interface GigabitEthernet 4/0/1
[SWB-GigabitEthernet4/0/1] port link-type trunk
[SWB-GigabitEthernet4/0/1] port trunk permit vlan 1 to 200
[SWB-GigabitEthernet4/0/1] smart-link flush enable control-vlan 10 101
[SWB-GigabitEthernet4/0/1] interface GigabitEthernet 4/0/2
[SWB-GigabitEthernet4/0/2] port link-type trunk
[SWB-GigabitEthernet4/0/2] port trunk permit vlan 1 to 200
[SWB-GigabitEthernet4/0/2] smart-link flush enable control-vlan 10 101
[SWB-GigabitEthernet4/0/2] quit
```

(3) 在交换机 SWD 上配置 Smart Link。

① 创建 VLAN 1～VLAN 200。

```
<SWD> system-view
[SWD] vlan 1 to 200
```

② 在相关端口上分别关闭 STP 功能，将端口配置为 Trunk 端口且允许 VLAN 1～VLAN 200 通过；使能接收 Flush 报文的功能，并指定接收 Flush 报文的控制 VLAN 为 VLAN 10 和 VLAN 101。

```
[SWD] interface GigabitEthernet 4/0/1
[SWD-GigabitEthernet4/0/1] port link-type trunk
[SWD-GigabitEthernet4/0/1] port trunk permit vlan 1 to 200
[SWD-GigabitEthernet4/0/1] smart-link flush enable control-vlan 10 101
[SWD-GigabitEthernet4/0/1] interface GigabitEthernet 4/0/2
[SWD-GigabitEthernet4/0/2] port link-type trunk
[SWD-GigabitEthernet4/0/2] port trunk permit vlan 1 to 200
[SWD-GigabitEthernet4/0/2] smart-link flush enable control-vlan 10 101
[SWD-GigabitEthernet4/0/2] quit
```

(4) 在交换机 SWA 上配置 Smart Link。

① 创建 VLAN 1～VLAN 200。

```
<SWA> system-view
[SWA] vlan 1 to 200
```

② 在相关端口上分别关闭 STP 功能，将端口配置为 Trunk 端口且允许 VLAN 1～VLAN 200 通过；使能接收 Flush 报文的功能，并指定接收 Flush 报文的控制 VLAN 为 VLAN 10 和 VLAN 101。

```
[SWA] interface GigabitEthernet 4/0/1
[SWA-GigabitEthernet4/0/1] port link-type trunk
[SWA-GigabitEthernet4/0/1] port trunk permit vlan 1 to 200
[SWA-GigabitEthernet4/0/1] smart-link flush enable control-vlan 10 101
[SWA-GigabitEthernet4/0/1] interface GigabitEthernet 4/0/2
[SWA-GigabitEthernet4/0/2] port link-type trunk
[SWA-GigabitEthernet4/0/2] port trunk permit vlan 1 to 200
[SWA-GigabitEthernet4/0/2] smart-link flush enable control-vlan 10 101
[SWA-GigabitEthernet4/0/2] quit
```

(5) 配置完成后，用户使用 display smart-link group 命令可以查看各设备上 Smart Link 组的信息。

① 查看 Switch C 上 Smart Link 组的信息。

```
[SWC] display smart-link group all
 Smart link group 1 information:
 Device ID: 000f-e23d-5af0
 Preemption mode: ROLE
 Control VLAN: 10
 Protected VLAN: Reference Instance 0
 Member                  Role     State      Flush-count   Last-flush-time
 ------------------------------------------------------------------------------
 GigabitEthernet 4/0/1   MASTER   ACTVIE     5             16:37:20 2009/02/21
 GigabitEthernet 4/0/2   SLAVE    STANDBY    1             17:45:20 2009/02/21
 Smart link group 2 information:
 Device ID: 000f-e23d-5af0
 Preemption mode: ROLE
 Control VLAN: 101
 Protected VLAN: Reference Instance 2
```

Member	Role	State	Flush-count	Last-flush-time
GigabitEthernet 4/0/2	MASTER	ACTVIE	5	16:37:20 2009/02/21
GigabitEthernet 4/0/1	SLAVE	STANDBY	1	17:45:20 2009/02/21

② 通过使用 display smart-link flush 命令可以查看各设备上收到的 Flush 报文信息。

```
[SWB] display smart-link flush
Received flush packets                          : 5
Receiving interface of the last flush packet    : GigabitEthernet 4/0/2
Receiving time of the last flush packet         : 16:25:21 2009/02/21
Device ID of the last flush packet              : 000f-e23d-5af0
Control VLAN of the last flush packet           : 10
```

13.5 Track 典型配置指导

Track 的用途是实现联动功能，如图 13-17 所示。

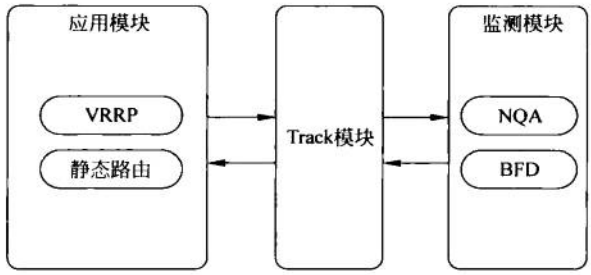


图 13-17 联动功能实现示意图

联动功能由应用模块、Track 模块和监测模块 3 部分组成。联动功能是指通过建立联动项，实现不同模块之间的联动，即由监测模块通过 Track 模块触发应用模块执行某种操作。监测模块负责对链路状态、网络性能等进行探测，并通过 Track 模块将探测结果通知给应用模块。应用模块感知到网络状态的变化后，及时进行相应的处理，从而避免通信的中断或服务质量的降低。

Track 模块位于应用模块和监测模块之间，主要功能是屏蔽不同监测模块的差异，为应用模块提供统一的接口。

13.5.1 VRRP、Track 与 NQA 联动典型配置指导

1. 背景

M 公司网络是双出口网络，在网络中部署了 VRRP 以增强网络的可靠性。但在实际使用中发现，VRRP 仅能感知到直连链路故障问题，而不能感知远端网络故障。故当双出口中的一个出口发生故障时，VRRP 并没有切换，导致业务发生中断。

根据以上业务特点与网络实际情况，网络管理员准备通过配置 Track 功能来实现网络中的 VRRP 与 NQA 联动。

2. 组网图

图 13-18 所示为 VRRP、Track 与 NQA 联动典型配置示意图。

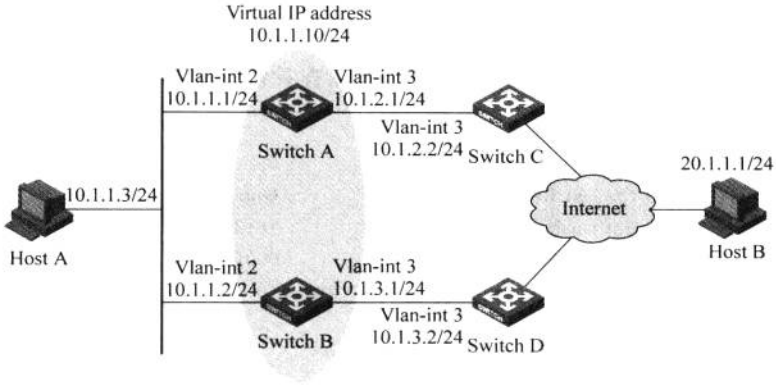


图 13-18 VRRP、Track 与 NQA 联动典型配置示意图

3. 配置需求

如图 13-18 所示，网络管理员对光纤连接的交换机 SWA、SWB、SWC、SWD 配置交换机的 VRRP、Track 与 NQA 联动功能。网络管理员要求通过配置达到下列要求。

(1) Host A 需要访问 Internet 上的 Host B，Host A 的默认网关为 10.1.1.10/24。

(2) SWA 和 SWB 属于虚拟 IP 地址为 10.1.1.10 的备份组 1。

(3) 当 SWA 正常工作时，Host A 发送给 Host B 的报文通过 SWA 转发；当通过 NQA 监测到 SWA 上行链路不通时，Host A 发送给 Host B 的报文通过 SWB 转发。

4. 配置过程和解释

(1) 在交换机 SWA、SWB、SWC、SWD 上按照图 13-18 创建 VLAN 并配置各 VLAN 接口的 IP 地址，将端口加入对应的 VLAN 中，具体配置过程略。

(2) 在交换机 SWA 上配置 VRRP、Track 与 NQA 联动功能。

① 创建管理员名为 admin、操作标签为 test 的 NQA 测试组。

```
[SWA] nqa entry admin test
```

② 配置测试类型为 ICMP-echo。

```
[SWA-nqa-admin-test] type icmp-echo
```

③ 配置目的地址为 10.1.2.2。

```
[SWA-nqa-admin-test-icmp-echo] destination ip 10.1.2.2
```

④ 测试频率为 100ms。

```
[SWA-nqa-admin-test-icmp-echo] frequency 100
```

⑤ 配置联动项 1(连续失败 5 次触发联动)。

```
[SWA-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type consecutive 5
action-type trigger-only
```

⑥ 启动探测。

```
[SWA] nqa schedule admin test start-time now lifetime forever
```

⑦ 配置 Track 项 1，关联 NQA 测试组(管理员为 admin，操作标签为 test)的联动项 1。

```
[SWA] track 1 nqa entry admin test reaction 1
```

⑧ 创建 VRRP 备份组 1，并配置备份组 1 的虚拟 IP 地址为 10.1.1.10。

```
[SWA] interface vlan-interface 2
[SWA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
```

⑨ 设置 SWA 在备份组 1 中的优先级为 110。

```
[SWA-Vlan-interface2] vrrp vrid 1 priority 110
```

⑩ 设置备份组的认证方式为 SIMPLE，认证字为 hello。

```
[SWA-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```

⑪ 设置 Master 发送 VRRP 报文的间隔时间为 5s。

```
[SWA-Vlan-interface2] vrrp vrid 1 timer advertise 5
```

⑫ 设置 SWA 工作在抢占方式，抢占延迟时间为 5s。

```
[SWA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

⑬ 设置监视 Track 项。

```
[SWA-Vlan-interface2] vrrp vrid 1 track 1 reduced 30
```

(3) 在交换机 SWB 上配置 VRRP。

① 创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 10.1.1.10。

```
<SWB> system-view
[SWB] interface vlan-interface 2
[SWB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
```

② 设置 SWB 在备份组 1 中的优先级为 100。

```
[SWB-Vlan-interface2] vrrp vrid 1 priority 100
```

③ 设置备份组的认证方式为 SIMPLE，认证字为 hello。

```
[SWB-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```

④ 设置 Master 发送 VRRP 报文的间隔时间为 5s。

```
[SWB-Vlan-interface2] vrrp vrid 1 timer advertise 5
```

⑤ 设置 SWB 工作在抢占方式，抢占延迟时间为 5s。

```
[SWB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

(4) 配置完成后，用户可以通过使用 display vrrp 命令查看配置后的结果。

① 显示 SWA 上备份组 1 的详细信息。

```
[SWA-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
    Run Mode          : Standard
    Run Method        : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface 2
     VRID             : 1                 Adver Timer   : 5
     Admin Status     : Up                State         : Master
     Config Pri       : 110               Running Pri   : 110
     Preempt Mode     : Yes               Delay Time    : 5
     Auth Type        : Simple            Key           : hello
     Virtual IP       : 10.1.1.10
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 10.1.1.1
   VRRP Track Information:
     Track Object     : 1                 State : Positive   Pri Reduced : 30
```

② 显示 SWB 上备份组 1 的详细信息。

```
[SWB-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
    Run Mode          : Standard
    Run Method        : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface 2
     VRID             : 1                 Adver Timer   : 5
     Admin Status     : Up                State         : Backup
     Config Pri       : 100               Running Pri   : 100
     Preempt Mode     : Yes               Delay Time    : 5
     Auth Type        : Simple            Key           : hello
     Virtual IP       : 10.1.1.10
     Master IP        : 10.1.1.1
```

SWA 与 SWC 不通时，在 Host A 上仍然可以 ping 通 Host B。通过 display vrrp 命令查看备份组的信息。

```
[SWA-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
    Run Mode          : Standard
    Run Method        : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface 2
     VRID             : 1                 Adver Timer   : 5
     Admin Status     : Up                State         : Backup
     Config Pri       : 110               Running Pri   : 80
     Preempt Mode     : Yes               Delay Time    : 5
     Auth Type        : Simple            Key           : hello
     Virtual IP       : 10.1.1.10
     Master IP        : 10.1.1.2
   VRRP Track Information:
     Track Object     : 1                 State : Negative   Pri Reduced : 30
```

```
[SWB-Vlan-interface2] display vrrp verbose
 IPv4 Standby Information:
     Run Mode          : Standard
     Run Method        : Virtual MAC
 Total number of virtual routers : 1
   Interface Vlan-interface 2
     VRID              : 1                 Adver Timer   : 5
     Admin Status      : Up                State         : Master
     Config Pri        : 100               Running Pri   : 100
     Preempt Mode      : Yes               Delay Time    : 5
     Auth Type         : Simple            Key           : hello
     Virtual IP        : 10.1.1.10
     Virtual MAC       : 0000-5e00-0101
     Master IP         : 10.1.1.2
```

从上述显示信息可以看出，SWA 与 SWC 不通时，SWA 的优先级降低为 80，成为 Backup，SWB 成为 Master，Host A 发送给 Host B 的报文通过 SWB 转发。

提示： 不允许对 IP 地址拥有者进行监视指定 Track 项的配置。

被监视 Track 项的状态由 Negative 变为 Positive 后，对应的交换机优先级会自动恢复。

被监视的 Track 项可以是未创建的 Track 项。可以通过 vrrp vrid track 命令指定监视的 Track 项后，再通过 track 命令创建该 Track 项。

13.5.2 静态路由、Track 与 NQA 联动典型配置指导

1. 背景

H 公司网络是双出口网络，同时在网络中部署了浮动静态路由以增强网络的可靠性。但是，当直连链路中断时，浮动静态路由能够切换成功；而当转发路径上的非直连链路故障时，静态路由无法切换。

为了解决上述问题，网络管理员准备通过配置 Track 功能来实现网络中的静态路由与 NQA 联动。

2. 组网图

图 13-19 所示为静态路由、Track 与 NQA 联动典型配置示意图。

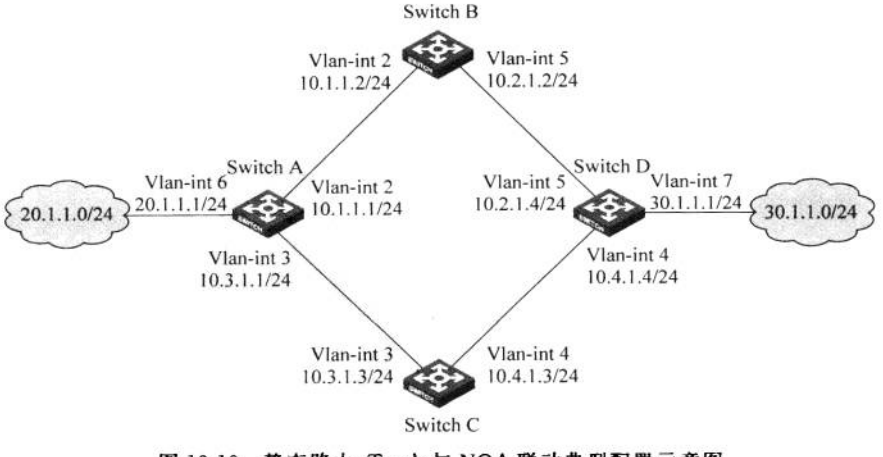


图 13-19 静态路由、Track 与 NQA 联动典型配置示意图

3. 配置需求

如图 13-19 所示，网络管理员对光纤连接的交换机 SWA、SWB、SWC、SWD 配置静态路由、Track 与 NQA 联动。SWA、SWB、SWC 和 SWD 连接了 20.1.1.0/24 和30.1.1.0/24 两个网段，在交换机上配置静态路由以实现两个网段的互通，并配置路由备份以提高网络的可靠性。

SWA 作为 20.1.1.0/24 网段内主机的默认网关，存在两条到达 30.1.1.0/24 网段的静态路由，下一跳分别为 SWB 和 SWC。这两条静态路由形成备份。

(1) 下一跳为 SWB 的静态路由优先级高，作为主路由。该路由可达时，SWA 通过 SWB 将报文转发到 30.1.1.0/24 网段。

(2) 下一跳为 SWC 的静态路由作为备份路由。

在 SWA 上通过静态路由、Track 与 NQA 联动，实时判断主路由是否可达。当主路由不可达时，备份路由生效，SWA 通过 SWC 将报文转发到 30.1.1.0/24 网段。

同样地，SWD 作为 30.1.1.0/24 网段内主机的默认网关，在 SWD 上存在两条到达 20.1.1.0/24 网段的静态路由，下一跳分别为 SWB 和 SWC。这两条静态路由形成备份。

(1) 下一跳为 SWB 的静态路由优先级高，作为主路由。该路由可达时，SWD 通过 SWB 将报文转发到 20.1.1.0/24 网段。

(2) 下一跳为 SWC 的静态路由作为备份路由。

在 SWD 上通过静态路由、Track 与 NQA 联动，实时判断主路由是否可达。当主路由不可达时，备份路由生效，SWD 通过 SWC 将报文转发到 20.1.1.0/24 网段。

4. 配置过程和解释

(1) 按照图 13-19 创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址，具体配置过程略。

(2) 在交换机 SWA 上配置静态路由、Track 与 NQA 联动。

① 配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.1.1.2，优先级为默认值 60，该路由与 Track 项 1 关联。

```
[SWA] ip route-static 30.1.1.0 24 10.1.1.2 track 1
```

② 配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.3.1.3，优先级为 80。

```
[SWA] ip route-static 30.1.1.0 24 10.3.1.3 preference 80
```

③ 配置到达 10.2.1.4 的静态路由：下一跳地址为 10.1.1.2。

```
[SWA] ip route-static 10.2.1.4 24 10.1.1.2
```

④ 创建管理员名为 admin、操作标签为 test 的 NQA 测试组。

```
[SWA] nqa entry admin test
```

⑤ 配置测试类型为 ICMP-echo。

```
[SWA-nqa-admin-test] type icmp-echo
```

⑥ 配置测试的目的地址为 10.2.1.4，下一跳地址为 10.1.1.2，以便通过 NQA 检测 SWA—SWB—SWD 这条路径的连通性。

```
[SWA-nqa-admin-test-icmp-echo] destination ip 10.2.1.4
[SWA-nqa-admin-test-icmp-echo] next-hop 10.1.1.2
```

⑦ 配置测试频率为 100ms。

```
[SWA-nqa-admin-test-icmp-echo] frequency 100
```

⑧ 配置联动项 1(连续失败 5 次触发联动)。

```
[SWA-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type consecutive 5
action-type trigger-only
```

⑨ 启动探测。

```
[SWA] nqa schedule admin test start-time now lifetime forever
```

⑩ 配置 Track 项 1,关联 NQA 测试组(管理员为 admin,操作标签为 test)的联动项 1。

```
[SWA] track 1 nqa entry admin test reaction 1
```

(3) 在交换机 SWB 上配置静态路由。

① 配置到达 30.1.1.0/24 网段的静态路由:下一跳地址为 10.2.1.4。

```
[SWB] ip route-static 30.1.1.0 24 10.2.1.4
```

② 配置到达 20.1.1.0/24 网段的静态路由:下一跳地址为 10.1.1.1。

```
[SWB] ip route-static 20.1.1.0 24 10.1.1.1
```

(4) 在交换机 SWC 上配置静态路由。

① 配置到达 30.1.1.0/24 网段的静态路由:下一跳地址为 10.4.1.4。

```
[SWC] ip route-static 30.1.1.0 24 10.4.1.4
```

② 配置到达 20.1.1.0/24 网段的静态路由:下一跳地址为 10.3.1.1。

```
[SWC] ip route-static 20.1.1.0 24 10.3.1.1
```

(5) 在交换机 SWD 上配置静态路由、Track 与 NQA 联动。

① 配置到达 20.1.1.0/24 网段的静态路由:下一跳地址为 10.2.1.2,优先级为默认值 60,该路由与 Track 项 1 关联。

```
[SWD] ip route-static 20.1.1.0 24 10.2.1.2 track 1
```

② 配置到达 20.1.1.0/24 网段的静态路由:下一跳地址为 10.4.1.3,优先级为 80。

```
[SWD] ip route-static 20.1.1.0 24 10.4.1.3 preference 80
```

③ 配置到达 10.1.1.1 的静态路由:下一跳地址为 10.2.1.2。

```
[SWD] ip route-static 10.1.1.1 24 10.2.1.2
```

④ 创建管理员名为 admin、操作标签为 test 的 NQA 测试组。

```
[SWD] nqa entry admin test
```

⑤ 配置测试类型为 ICMP-echo。

```
[SWD-nqa-admin-test] type icmp-echo
```

⑥ 配置测试的目的地址为 10.1.1.1，下一跳地址为 10.2.1.2，以便通过 NQA 检测 SWD—SWB—SWA 这条路径的连通性。

```
[SWD-nqa-admin-test-icmp-echo] destination ip 10.1.1.1
[SWD-nqa-admin-test-icmp-echo] next-hop 10.2.1.2
```

⑦ 配置测试频率为 100ms。

```
[SWD-nqa-admin-test-icmp-echo] frequency 100
```

⑧ 配置联动项 1(连续失败 5 次触发联动)。

```
[SWD-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type consecutive 5
action-type trigger-only
```

⑨ 启动探测。

```
[SWD] nqa schedule admin test start-time now lifetime forever
```

⑩ 配置 Track 项 1，关联 NQA 测试组(管理员为 admin，操作标签为 test)的联动项 1。

```
[SWD] track 1 nqa entry admin test reaction 1
```

(6) 配置完成后，用户使用 display 命令可以查看各设备上信息。

① 显示 SWA 上 Track 项的信息。

```
[SWA] display track all
Track ID: 1
  Status: Positive
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    NQA entry: admin test
    Reaction: 1
```

② 显示 SWA 的路由表。通过路由表可以看出，SWA NQA 测试的结果为主路由可达(Track 项状态为 Positive)，SWA 通过 SWB 将报文转发到 30.1.1.0/24 网段。

```
[SWA] display ip routing-table
Routing Tables: Public
         Destinations : 10        Routes : 10
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
10.1.1.0/24         Direct  0    0         10.1.1.1        Vlan 2
10.1.1.1/32         Direct  0    0         127.0.0.1       InLoop 0
10.2.1.0/24         Static  60   0         10.1.1.2        Vlan 2
10.3.1.0/24         Direct  0    0         10.3.1.1        Vlan 3
10.3.1.1/32         Direct  0    0         127.0.0.1       InLoop 0
20.1.1.0/24         Direct  0    0         20.1.1.1        Vlan 6
20.1.1.1/32         Direct  0    0         127.0.0.1       InLoop 0
30.1.1.0/24         Static  60   0         10.1.1.2        Vlan 2
```

127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop 0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop 0

③ 在 SWB 上删除 VLAN 接口 2 的 IP 地址，并显示 SWA 上 Track 项的信息。

```
<SWB> system-view
[SWB] interface vlan-interface 2
[SWB-Vlan-interface2] undo ip address
[SWA] display track all
Track ID: 1
  Status: Negative
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    NQA entry: admin test
    Reaction: 1
```

④ 显示 SWA 的路由表。通过路由表可以看出，SWA NQA 测试的结果为主路由不可达(Track 项状态为 Negative)，则备份路由生效，SWA 通过 SWC 将报文转发到 30.1.1.0/24 网段。

```
[SWA] display ip routing-table
Routing Tables: Public
         Destinations : 10        Routes : 10
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.1.1.0/24	Direct	0	0	10.1.1.1	Vlan 2
10.1.1.1/32	Direct	0	0	127.0.0.1	InLoop 0
10.2.1.0/24	Static	60	0	10.1.1.2	Vlan 2
10.3.1.0/24	Direct	0	0	10.3.1.1	Vlan 3
10.3.1.1/32	Direct	0	0	127.0.0.1	InLoop 0
20.1.1.0/24	Direct	0	0	20.1.1.1	Vlan 6
20.1.1.1/32	Direct	0	0	127.0.0.1	InLoop 0
30.1.1.0/24	Static	80	0	10.3.1.3	Vlan 3
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop 0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop 0

第14章

网络管理与监控配置指导

14.1 信息中心典型配置指导

信息中心是系统的信息枢纽，它能够对所有的系统信息进行分类、管理。通过与debugging程序的结合，信息中心为网络管理员和开发人员监控网络运行情况和诊断网络故障提供了强有力的支持。

14.1.1 日志发送到UNIX日志主机典型配置指导

1. 背景

网络管理员小周在处理问题的时候发现设备的日志信息已经被覆盖而无法准确定位。H3C工程师小张得知此事后，根据自己的专业知识而帮助小周进行相关的配置，能够将所有设备的日志信息都发送到指定服务器存储起来。

2. 组网图

图14-1所示为日志发送到UNIX日志主机典型配置组网图。

图14-1 日志发送到UNIX日志主机典型配置组网图

3. 配置需求

交换机的日志信息发送到UNIX日志主机上，日志主机的IP地址为202.38.1.10，只允许严重性高于informational的日志信息发送到日志主机上，允许输出信息的模块为ARP和IP。

4. 配置过程和解释

(1) 交换机上的配置。

① 开启信息中心。

```
<Sysname> system-view
[Sysname] info-center enable
```

② 默认情况下，系统向loghost通道输出所有模块的系统信息。为了得到ARP和IP模块的系统信息，需首先关闭所有模块向日志主机通道输出信息的功能。

```
[Sysname] undo info-center source default channel loghost
```

③ 将 IP 地址为 202.38.1.10 的主机用作日志主机，只允许严重等级高于或等于 informational 的日志信息输出至日志主机，允许输出信息的模块为 ARP 和 IP。

```
[Sysname] info-center loghost 202.38.1.10 facility local4
[Sysname] info-center source arp channel loghost log level informational debug state off trap state off
[Sysname] info-center source ip channel loghost log level informational debug state off trap state off
```

(2) 日志主机上的配置。下面的配置示例是在 SunOS 4.0 上完成的，在其他厂商的 UNIX 操作系统上的配置操作基本与之相似。

① 以超级用户(root)的身份执行以下命令。

```
# mkdir /var/log/Sysname
# touch /var/log/Sysname/information
```

② 以超级用户(root)的身份编辑文件/etc/syslog.conf，加入以下选择/动作组合(selector/action pairs)。

```
# Sysname configuration messages
local4.info     /var/log/Sysname/information
```

③ 当日志文件 information 建立且/etc/syslog.conf 文件被修改了之后，应通过执行以下命令给系统守护进程 syslogd 一个 HUP 信号来使 syslogd 重新读取它的配置文件/etc/syslog.conf。

```
# ps -ae | grep syslogd
147
# kill -HUP 147
```

注意：在编辑/etc/syslog.conf 时，要注意注释只允许独立成行，并以字符"#"开头；选择/动作组合之间必须以一个制表符分隔，而不能输入空格；在文件名之后不得有多余的空格。

/etc/syslog.conf 中指定的设备名及接收的日志信息级别与交换机上配置的 info-center loghost 和 info-center source 命令中的相应参数应保持一致，否则日志信息可能无法正确输出到日志主机上。

14.1.2 日志发送到 Linux 日志主机典型配置指导

1. 背景

另一个客户小李也需要将设备的日志信息保存到服务器上。但是小李现在使用 Linux 服务器，并没有像小周一样使用 UNIX 服务器。小张通过查询确认 Linux 日志主机通过简单配置也可以接收设备发送的日志信息。

2. 组网图

图 14-2 所示为日志发送到 Linux 日志主机典型配置组网图。

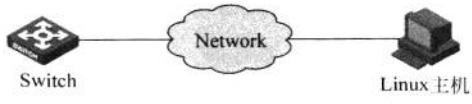


图 14-2 日志发送到 Linux 日志主机典型配置组网图

3. 配置需求

交换机的日志信息发送到Linux日志主机上，日志主机的IP地址为202.38.1.10，只允许严重性高于errors的日志信息发送到日志主机上，允许输出信息的模块为所有模块。

4. 配置过程和解释

(1) 交换机上的配置。

① 开启信息中心。

```
<Sysname> system-view
[Sysname] info-center enable
```

② 将IP地址为202.38.1.10的主机用作日志主机，只允许严重等级高于或等于errors的日志信息输出至日志主机，允许输出信息的模块为所有模块。

```
[Sysname] info-center loghost 202.38.1.10 facility local7
[Sysname] info-center source default channel loghost log level errors debug state off trap state off
```

(2) 日志主机上的配置。

① 以超级用户(root)的身份执行以下命令。

```
# mkdir /var/log/Sysname
# touch /var/log/Sysname/information
```

② 以超级用户(root)的身份编辑文件/etc/syslog.conf，加入以下选择/动作组合(selector/action pairs)。

```
# Sysname configuration messages
local7.info      /var/log/Sysname/information
```

③ 当日志文件information建立且/etc/syslog.conf文件被修改了之后，应通过执行以下命令查看系统守护进程syslogd的进程号，杀死syslogd进程，并重新用-r选项在后台启动syslogd。

```
# ps -ae | grep syslogd
147
# kill -9 147
# syslogd -r &
```

注意：对Linux日志主机，必须保证syslogd进程是以-r选项启动的。

14.1.3 日志发送到控制台典型配置指导

1. 背景

小张回想起自己定位问题时控制台输出的信息太多，以至于很难找到自己希望看到的那些信息。经过实践，小张发现原来控制台的信息输出是可以分模块按不同方向输出的。

2. 组网图

图14-3所示为日志发送到控制台典型配置组网示意图。

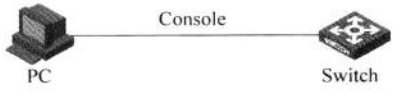


图14-3 日志发送到控制台典型配置组网示意图

3. 配置需求

交换机的严重性高于 informational 的日志信息将会发送到控制台上，允许输出信息的模块为 ARP 和 IP。

4. 配置过程和解释

(1) 开启信息中心。

```
<Sysname> system-view
[Sysname] info-center enable
```

(2) 系统默认向 console 通道输出所有模块的系统信息，为了得到 ARP 和 IP 模块的系统信息，需首先关闭所有模块向 console 通道输出信息的功能。

```
[Sysname] undo info-center source default channel console
```

(3) 配置控制台日志输出，只允许严重等级高于或等于 informational 的日志信息输出至控制台，允许输出信息的模块为 ARP 和 IP。

```
[Sysname] info-center console channel console
[Sysname] info-center source arp channel console log level informational debug state off trap state off
[Sysname] info-center source ip channel console log level informational debug state off trap state off
```

(4) 打开终端显示功能。

```
<Sysname> terminal monitor
<Sysname> terminal logging
```

14.2 SNMP 和 RMON 典型配置指导

SNMP(Simple Network Management Protocol，简单网络管理协议)是使用 TCP/IP 协议族对互联网上的设备进行管理的一个框架，它提供一组基本的操作来监视和维护互联网。SNMP 具有以下优势。

(1) 自动化网络管理。网络管理员可以利用 SNMP 平台在网络上的节点检索信息、修改信息、发现故障、完成故障诊断、进行容量规划和生成报告。

(2) 屏蔽不同设备的物理差异，实现对不同厂商产品的自动化管理。SNMP 只提供最基本的功能集，使得管理任务分别与被管设备的物理特性和下层的联网技术相对独立，从而实现对不同厂商设备的管理，特别适合在小型、快速和低成本的环境中使用。

RMON(Remote Network Monitoring，远程网络监视)主要实现了统计和告警功能，用于网络中管理设备对被管理设备的远程监控和管理。统计功能指的是被管理设备可以按周期或者持续跟踪统计其端口所连接的网段上的各种流量信息，如某段时间内某网段上收到的报文总数，或收到的超长报文的总数等。告警功能指的是被管理设备能监控指定 MIB 变量的值，当该值达到告警阈值时(如端口速率达到指定值，或者广播报文的比例达到指定值)，能自动记录日志，向管理设备发送 Trap 消息。

RMON 和 SNMP 都用于远程网络管理，其区别在于以下两点。

(1) SNMP 是 RMON 实现的基础，RMON 是 SNMP 功能的增强。RMON 使用 SNMP Trap 报文发送机制向管理设备发送 Trap 消息告知告警变量的异常。虽然 SNMP

也定义了 Trap 功能，但通常用于告知被管理设备上某功能是否运行正常、端口物理状态的变化等，两者监控的对象、触发条件以及报告的内容均不同。

(2) RMON 使 SNMP 能更有效、更积极主动地监测远程网络设备，为监控子网的运行提供了一种高效的手段。RMON 协议规定达到告警阈值时被管理设备能自动发送 Trap 信息，所以管理设备不需要多次去获取 MIB 变量的值，进行比较，从而能够减少管理设备同被管理设备的通信流量，达到简便而有力地管理大型互连网络的目的。

14.2.1 SNMPv2c 监控管理交换机典型配置指导

1. 背景

H 公司网络要求使用公有的网络管理协议，故打算在网络中部署 SNMP。因 SNMPv2c 有比 SNMPv1 更多的功能和更丰富的信息，所以先对 SNMPv2c 进行测试。另外，为了使设备能够迅速向网管服务器报告紧急重要事件(如被管理设备重新启动等)，H 公司决定开启 Trap 功能。

2. 组网图

图 14-4 所示为 SNMPv2c 监控管理交换机典型配置组网图。

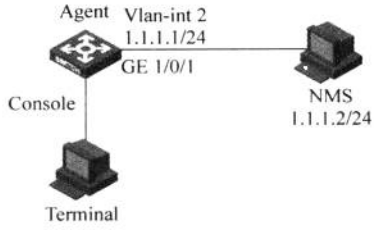


图 14-4 SNMPv2c 监控管理交换机典型配置组网图

3. 配置需求

(1) 网管工作站(NMS)与以太网交换机(Agent)通过以太网相连。

(2) 网管工作站 IP 地址为 1.1.1.2/24。

(3) 以太网交换机的 VLAN 接口 IP 地址为 1.1.1.1/24。

(4) NMS 通过 SNMPv2c 对 Agent 进行监控管理，Agent 在故障或者出错的时候能够主动向 NMS 报告情况。

4. 配置过程和解释

(1) 配置 Agent。

① 设置 SNMP 基本信息，包括版本、团体名。

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent community read public
[Sysname] snmp-agent community write private
```

② 设置网管使用的 Vlan-interface 2(IP 地址为 1.1.1.1/24)，将用于网管的端口 GigabitEthernet 1/0/1 加入到 VLAN 2 中。

```
[Sysname] vlan 2
[Sysname-vlan2] port GigabitEthernet 1/0/1
```

```
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip address 1.1.1.1 255.255.255.0
[Sysname-Vlan-interface2] quit
```

③ 设置交换机的联系人和位置信息，以方便维护。

```
[Sysname] snmp-agent sys-info version all
[Sysname] snmp-agent sys-info contact Mr.Chen-Tel:5651
[Sysname] snmp-agent sys-info location telephone-closet,3rd-floor
```

④ 允许向网管工作站(NMS)1.1.1.2/24 发送 Trap 报文，使用的团体名为 public。

```
[Sysname] snmp-agent trap enable
[Sysname] snmp-agent target-host trap address udp-domain 1.1.1.2 udp-port 5000 params securityname public
```

(2) 配置 NMS(具体设置请参考 NMS 配套手册)。

① 选择 SNMP 版本号为 SNMPv2c，设置只读团体名为 public，读/写团体名为 private，SNMP 端口号选择 161。

② 为了能够接收 Agent 发来的 Trap 报文，需在 NMS 端设置监听 Trap 报文的 UDP 端口号为 5000(和 Agent 端命令行配置端口一致)。

③ 配置完成后，即可实现 NMS 对交换机的远程监控和管理，交换机有告警事件发生时会主动向 NMS 发送 trap 报文。

注意：网管侧的配置必须和交换机侧保持一致；否则无法进行相应操作。

14.2.2 SNMPv3 监控管理交换机典型配置指导

1. 背景

SNMPv1 和 SNMPv2c 版本是基于团体属性的访问控制，在安全性方面存在一定的安全隐患，因此 H 公司最后决定采用更高安全性的 SNMPv3 来实现 SNMP 管理。

2. 组网图

图 14-5 所示为 SNMPv3 监控管理交换机典型配置组网图。

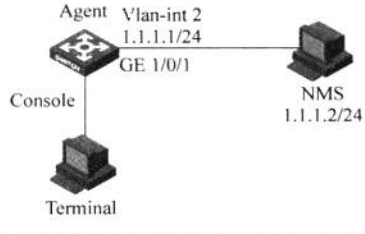


图 14-5 SNMPv3 监控管理交换机典型配置组网图

3. 配置需求

(1) 网管工作站(NMS)与以太网交换机(Agent)通过以太网相连。

(2) 网管工作站 IP 地址为 1.1.1.2/24。

(3) 以太网交换机的 VLAN 接口 IP 地址为 1.1.1.1/24。

(4) NMS 通过 SNMPv3 对 Agent 的接口状态进行监控管理，Agent 在故障或者出错的时候能够主动向 NMS 报告情况，NMS 接收 Trap 的端口号为 5000。

4. 配置过程和解释

(1) 配置 Agent。

① 设置访问权限。

```
<Sysname> system-view
[Sysname] undo snmp-agent mib-view ViewDefault
[Sysname] snmp-agent mib-view included test interfaces
[Sysname] snmp-agent group v3 managev3group read-view test write-view test
[Sysname] snmp-agent usm-user v3 managev3user managev3group
```

② 设置交换机的联系人和位置信息,以方便维护。

```
[Sysname] snmp-agent sys-info contact Mr.Chen-Tel:5651
[Sysname] snmp-agent sys-info location telephone-closet,2rd-floor
```

③ 设置网管使用的 Vlan-interface 2(IP 地址为 1.1.1.1/24),将用于网管的端口 GigabitEthernet 1/0/1 加入到 VLAN 2 中。

```
[Sysname] vlan 2
[Sysname-vlan2] port GigabitEthernet 1/0/1
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip address 1.1.1.1 255.255.255.0
[Sysname-Vlan-interface2] quit
```

④ 将 Vlan-interface 2 的 IP 地址作为 Trap 报文的源地址。

```
[Sysname] snmp-agent trap source Vlan-interface 2
```

⑤ 允许向网管工作站(NMS)1.1.1.2/24 发送 Trap 报文,使用的团体名为 public。

```
[Sysname] snmp-agent trap enable
[Sysname] snmp-agent target-host trap address udp-domain 1.1.1.2 udp-port 5000 params securityname public
```

(2) 配置 NMS。SNMPv3 采用认证和加密的安全机制,在 NMS 上需要设置用户名,选择安全级别。根据不同的安全级别,需要分别设置认证方式、认证密码、加密方式、加密密码等。另外,还要设置超时时间和重试次数。用户可利用网管系统完成对设备的查询和配置操作,具体情况可参考 NMS 的配套手册。

注意:网管侧的配置必须和交换机侧保持一致,否则无法进行相应操作。

14.2.3 SNMP 操作日志输出典型配置指导

1. 背景

SNMP 日志功能将记录 NMS 对 SNMP Agent 的 GET 和 SET 操作。这些日志将被发送到设备的信息中心,级别为 informational,即作为设备的一般提示信息。通过设置信息中心的参数,最终决定 SNMP 日志的输出规则(即是否允许输出以及输出方向)。

H 公司管理员希望能够明确看到设备接收到了哪些管理操作并做出了相应的动作,所以需要设备能够正常输出 SNMP 操作日志到控制终端。基于以上需求,网络管理员调整信息中心的控制终端日志信息级别。

2. 组网图

图 14-6 所示为 SNMP 操作日志输出典型配置组网图。

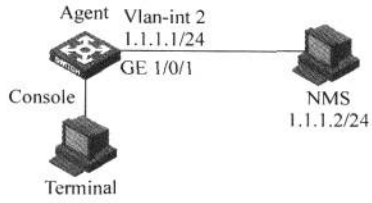


图 14-6 SNMP 操作日志输出典型配置组网图

3. 配置需求

(1) 网管工作站(NMS)与以太网交换机(Agent)通过以太网相连。

(2) 网管工作站 IP 地址为 1.1.1.2/24。

(3) 以太网交换机的 VLAN 接口 IP 地址为 1.1.1.1/24。

(4) NMS 对 Agent 执行的 GET/SET 操作日志通过 Console 通道输出到控制台。

4. 配置过程和解释

(1) 配置 Agent。

① 设置 SNMP 基本信息,包括版本、团体名。

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version all
[Sysname] snmp-agent community read public
[Sysname] snmp-agent community write private
```

② 设置网管使用的 Vlan-interface 2(IP 地址为 1.1.1.1/24),将用于网管的端口 GigabitEthernet 1/0/1 加入 VLAN 2 中。

```
[Sysname] vlan 2
[Sysname-vlan2] port GigabitEthernet 1/0/1
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip address 1.1.1.1 255.255.255.0
[Sysname-Vlan-interface2] quit
```

③ 打开控制台对日志信息的显示功能(可选,默认情况下,该功能是打开的)。

```
<Sysname> terminal monitor
<Sysname> terminal logging
```

④ 配置信息中心允许输出级别为 informational 及 informational 之上级别的 SNMP 系统信息到 Console 口。

```
<Sysname> system-view
[Sysname] info-center source snmp channel console log level informational
```

⑤ 打开 Agent 的 SNMP 日志开关,对 NMS 的 GET 和 SET 操作进行记录。

```
[Sysname] snmp-agent log get-operation
[Sysname] snmp-agent log set-operation
```

(2) NMS对Agent进行GET操作时,可以在控制台上看到如下日志信息。

```
%Sep  9 02:49:40:566 2007 Sysname SNMP/6/GET:
seqNO = <10> srcIP = <1.1.1.2> op = <get> node = <sysName(1.3.6.1.2.1.1.5.0)>
value=<>
```

(3) NMS对Agent进行SET操作时,可以在控制台上看到如下日志信息。

```
%Sep  9 02:59:42:576 2007 Sysname SNMP/6/SET:
seqNO = <11> srcIP = <1.1.1.2> op = <set> errorIndex = <0> errorStatus =<noError>
node = <sysName(1.3.6.1.2.1.1.5.0)> value = <Sysname>
```

注意:本例配置的前提是NMS已经能够对Agent进行GET/SET操作。

大量的日志记录会占用设备的存储空间,影响设备的性能。正常情况下,建议关闭SNMP日志功能。

14.2.4 RMON典型配置指导

RMON(Remote Monitoring,远程网络监视)的实现完全基于SNMP体系结构,它与现存的SNMP框架相兼容,不需对该协议进行任何修改。RMON使SNMP更有效、更积极主动地监测远程网络设备,为监控子网的运行提供了一种高效的手段。RMON能够减少网管站同代理间的通信流量,达到简便而有力地管理大型互连网络的目的。

1. 背景

H公司网络在运行过程中,发现某条出口链路经常会达到90%的利用率。为了对这条链路进行更好的监控,管理员决定在相关设备上配置RMON。

RMON协议的优点是网络设备自动在本地采集流量信息并将流量状态反馈给NMS,简化NMS的任务,降低了NMS和SNMP Agent间的流量。

2. 组网图

图14-7所示为RMON典型配置组网图。

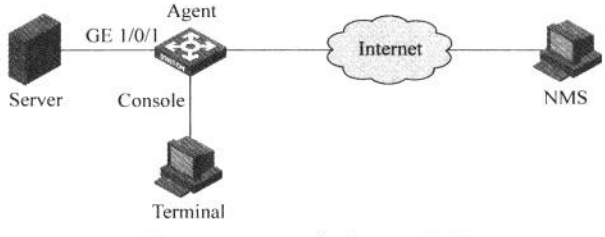


图14-7 RMON典型配置组网图

3. 配置需求

Agent通过Console口连接配置终端,通过Internet连接远端NMS。在RMON以太网统计表中设定一个表项,对以太网端口GigabitEthernet 1/0/1进行性能统计,当端口在一段时间内收到的字节数超过设置的门限后,记录日志。

4. 配置过程和解释

(1) 配置RMON对接口GigabitEthernet 1/0/1进行流量统计。

```
<Sysname> system-view
```

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1 owner user1-rmon
[Sysname-GigabitEthernet1/0/1] return
```

(2) 配置一个事件，在该事件被触发的时候，会记录日志。

```
<Sysname> system-view
[Sysname] rmon event 1 log owner 1-rmon
```

(3) 配置一个告警组，对接口 GigabitEthernet 1/0/1 收到的字节数进行抽样，当超过上下限值的时候，都会记录日志。

```
[Sysname] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 10 delta rising-threshold 1000 1 falling-threshold 100 1 owner 1-rmon
```

说明：节点 1.3.6.1.2.1.16.1.1.1.4.1 表示 RMON 统计组 1 接收到的字节数，即 GigabitEthernet 1/0/1 接收到的字节数。

14.3 端口镜像典型配置指导

端口镜像是指将设备的一个或多个端口(源端口)的报文复制到设备的一个监视端口(目的端口)，用于报文的监视和分析。其中，源端口和目的端口在同一台设备上的为本地镜像，在不同设备上的是远程镜像。

14.3.1 本地端口镜像典型配置指导

1. 背景

因信息安全需要，H 公司要求市场部门和研发部门的信息流量必须进行数据检测，以确保发生安全事故后进行事后审核。因网络已建好并正在运行，故要求网络管理员不得中断业务正常运转而实现流量监管。通常情况下，在网络设备中间串入透明监控设备可能会影响网络性能，并且在部署时需要中断业务。经过测试，H 公司确认采用设备镜像功能可以不中断当前业务而达到目的。

2. 组网图

图 14-8 所示为本地端口镜像典型配置组网图。

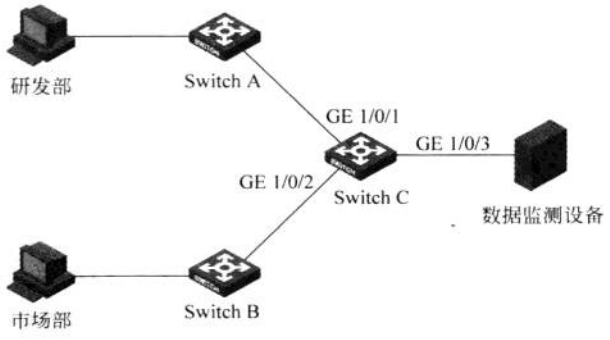


图 14-8 本地端口镜像典型配置组网图

3. 配置需求

某公司内部通过交换机(以 S5500-EI 系列以太网交换机为例,如图 14-8 中的 Switch C)实现各部门之间的互连,网络环境描述如下:

(1) 研发部通过端口 GigabitEthernet 1/0/1 接入 Switch C。

(2) 市场部通过端口 GigabitEthernet 1/0/2 接入 Switch C。

(3) 数据监测设备连接在 Switch C 的 GigabitEthernet 1/0/3 端口上。

网络管理员希望通过数据监测设备对研发部和市场部收发的报文进行监控。使用本地端口镜像功能实现该需求,在 Switch C 上进行如下配置。

(1) 端口 GigabitEthernet 1/0/1 和 GigabitEthernet 1/0/2 为镜像源端口。

(2) 连接数据监测设备的端口 GigabitEthernet 1/0/3 为镜像目的端口。

4. 配置过程和解释

(1) 创建本地镜像组。

```
<SwitchC> system-view
[SwitchC] mirroring-group 1 local
```

(2) 为本地镜像组配置源端口和目的端口。

```
[SwitchC] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 GigabitEthernet 1/0/2 both
[SwitchC] mirroring-group 1 monitor-port GigabitEthernet 1/0/3
```

(3) 显示所有镜像组的配置信息。

```
[SwitchC] display mirroring-group all
mirroring-group 1:
    type: local
    status: active
    mirroring port:
        GigabitEthernet 1/0/1   both
        GigabitEthernet 1/0/2   both
    monitor port: GigabitEthernet 1/0/3
```

注意:镜像后的报文是否带有 VLAN Tag,不同的产品有所不同,以各产品的实际情况为准。

一个镜像组只能配置一个目的端口,且目的端口上不要开启 STP、RSTP 或 MSTP,否则可能会影响镜像功能的正常使用。

目的端口不用做其他用途,仅用于端口镜像。

14.3.2 远程端口镜像典型配置指导

在远程镜像中,在本地设备上将流量镜像到镜像 VLAN,通过镜像 VLAN 将流量转发到目的设备上,从而转发到监控设备上,如图 14-9 所示。

图中各设备的作用如下:

(1) 源设备:源端口所在的设备,用户需要在源设备上创建远程源镜像组。本设备负责将源端口的报文复制一份,然后通过出端口将报文在远程镜像 VLAN 中进行广播,传输给中间设备或目的设备。

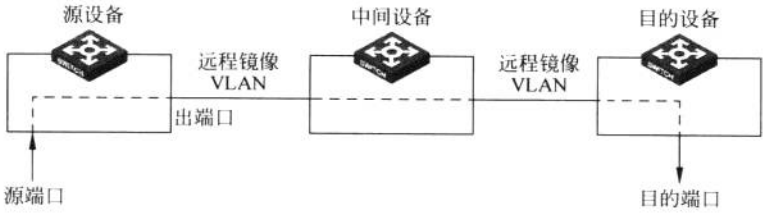


图 14-9 远程端口镜像应用示意图

(2) 中间设备：网络中处于源设备和目的设备之间的设备。本设备负责将镜像报文传输给下一个中间设备或目的设备。如果源设备与目的设备直接相连，则不存在中间设备。用户需要确保远程镜像 VLAN 内源设备到目的设备的二层互通性。

(3) 目的设备：远程镜像目的端口所在的设备，用户需要在目的设备上创建远程目的镜像组。目的设备收到报文后，比较报文的 VLAN ID 和远程目的镜像组的远程镜像 VLAN 是否相同，如果相同，则将该报文通过镜像目的端口转发给监控设备。

1. 背景

H 公司网络规模大，物理位置分散，且流量控制不集中。采用本地端口镜像功能需要消耗大量的业务端口用于连接监控设备且成本高昂，也不利于集中监控管理。如果能够将本地流量镜像后自动发送到远端监控设备，则能解决上述问题。基于上述原因，公司网络中使用远程镜像功能。

2. 组网图

图 14-10 所示为远程端口镜像典型配置组网图。

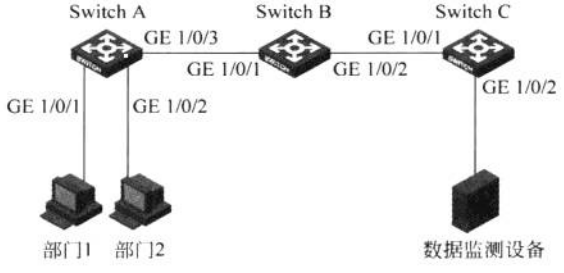


图 14-10 远程端口镜像典型配置组网图

3. 配置需求

某公司内部通过交换机实现各部门之间的互连，网络环境描述如下：

(1) 部门 1 通过端口 GigabitEthernet 1/0/1 接入 Switch A。

(2) 部门 2 通过端口 GigabitEthernet 1/0/2 接入 Switch A。

(3) Switch A 的端口 GigabitEthernet 1/0/3 和 Switch B 的端口 GigabitEthernet 1/0/1 相连。

(4) Switch B 的端口 GigabitEthernet 1/0/2 和 Switch C 的端口 GigabitEthernet 1/0/1 相连。

(5) 数据监测设备连接在 Switch C 的端口 GigabitEthernet 1/0/2 上。

网络管理员希望通过数据监测设备对部门 1 和部门 2 发送的报文进行监控。使用远程

端口镜像功能实现该需求，进行如下配置。

(1) Switch A 充当源设备，Switch B 充当中间设备，Switch C 充当目的设备。

(2) 在 Switch A 上配置远程源镜像组，定义 VLAN 2 为远程镜像 VLAN，端口 GigabitEthernet 1/0/1 和 GigabitEthernet 1/0/2 为镜像源端口，端口 GigabitEthernet 1/0/3 为出端口。

(3) 配置 Switch A 的端口 GigabitEthernet 1/0/3、Switch B 的端口 GigabitEthernet 1/0/1 和 GigabitEthernet 1/0/2、Switch C 的端口 GigabitEthernet 1/0/1 的端口类型为 Trunk 端口，并且都允许 VLAN 2 的报文通过。

(4) 在 Switch C 上配置远程目的镜像组，定义 VLAN 2 为远程镜像 VLAN，连接数据监测设备的端口 GigabitEthernet 1/0/2 为镜像目的端口。

4. 配置过程和解释

(1) 配置 Switch A(源设备)。

① 创建远程源镜像组。

```
<SwitchA> system-view
[SwitchA] mirroring-group 1 remote-source
```

② 创建 VLAN 2。

```
[SwitchA] vlan 2
[SwitchA-vlan2] quit
```

③ 为远程源镜像组配置远程镜像 VLAN、源端口和出端口。

```
[SwitchA] mirroring-group 1 remote-probe vlan 2
[SwitchA] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 GigabitEthernet 1/0/2 inbound
[SwitchA] mirroring-group 1 monitor-egress GigabitEthernet 1/0/3
```

④ 配置端口 GigabitEthernet 1/0/3 的端口类型为 Trunk 端口，允许 VLAN 2 的报文通过。

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 2
```

(2) 配置 Switch B(中间设备)。

① 配置端口 GigabitEthernet 1/0/1 的端口类型为 Trunk 端口，允许 VLAN 2 的报文通过。

```
<SwitchB> system-view
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchB-GigabitEthernet1/0/1] quit
```

② 配置端口 GigabitEthernet 1/0/2 的端口类型为 Trunk 端口，允许 VLAN 2 的报文通过。

```
[SwitchB] interface GigabitEthernet 1/0/2
```

```
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-GigabitEthernet1/0/2] port trunk permit vlan 2
```

(3) 配置 Switch C(目的设备)。

① 配置端口 GigabitEthernet 1/0/1 的端口类型为 Trunk 端口,允许 VLAN 2 的报文通过。

```
<SwitchC> system-view
[SwitchC] interface GigabitEthernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchC-GigabitEthernet1/0/1] quit
```

② 创建远程目的镜像组。

```
[SwitchC] mirroring-group 1 remote-destination
```

③ 创建 VLAN 2。

```
[SwitchC] vlan 2
[SwitchC-vlan2] quit
```

④ 为远程目的镜像组配置远程镜像 VLAN 和目的端口。

```
[SwitchC] mirroring-group 1 remote-probe vlan 2
[SwitchC] mirroring-group 1 monitor-port GigabitEthernet 1/0/2
[SwitchC] interface GigabitEthernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port access vlan 2
```

提示:远程镜像 VLAN 不应该用作其他用途,仅用于远程镜像功能。

14.4 NTP 典型配置指导

NTP(Network Time Protocol,网络时间协议)是由 RFC 1305 定义的时间同步协议,用来在分布式时间服务器和客户端之间进行时间同步。NTP 基于 UDP 报文进行传输,使用的 UDP 端口号为 123。

使用 NTP 的目的是对网络内所有具有时钟的设备进行时钟同步,使网络内所有设备的时钟保持一致,从而使设备能够提供基于统一时间的多种应用。

对于运行 NTP 的本地系统,既可以接受来自其他时钟源的同步,又可以作为时钟源同步其他的时钟,并且可以和其他设备互相同步。

14.4.1 NTP 服务器/客户端模式典型配置指导

1. 背景

H 公司组建网络,要求网络的可维护性、可管理性要高。在网络的故障诊断中,确保网络设备日志信息、Trap 信息的时间戳真实可靠是必要条件。如何能保证所有设备都有一致的时间呢?采用当前通用的 NTP 协议自动同步时钟能够达到目的。

针对不同应用情况,可以选择不同的工作模式。大多数情况下,可以采用 NTP 服务

器/客户端模式。

2. 组网图

图 14-11 所示为 NTP 服务器/客户端模式典型配置组网图。

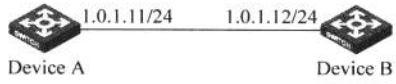


图 14-11 NTP 服务器/客户端模式典型配置组网图

3. 配置需求

(1) Device A 设置本地时钟作为参考时钟,层数为 2。

(2) Device B 工作在客户端模式,指定 Device A 为 NTP 服务器。

4. 配置过程和解释

(1) 配置 Device A。设置本地时钟作为参考时钟,层数为 2。

```
<DeviceA> system-view
[DeviceA] ntp-service refclock-master 2
```

(2) 配置 Device B。设置 Device A 为 Device B 的 NTP 服务器。

```
<DeviceB> system-view
[DeviceB] ntp-service unicast-server 1.0.1.11
```

提示:仅部分交换机支持设置本身时钟作为参考时钟。

对于不支持设置本身时钟为参考时钟的交换机来说,只有当其时钟被同步后,才能作为时钟源去同步其他设备。

14.4.2 NTP 对等体模式典型配置指导

1. 背景

在 NTP 的服务器/客户端运行模式下,客户端只能被同步,而服务器只能同步客户端。

在 NTP 对等体模式下,多个设备间可进行 NTP 相互同步。在网络中网络设备数量较少,而且处于同等时间同步地位的情况下建议配置对等体模式。

2. 组网图

图 14-12 所示为 NTP 对等体模式典型配置组网图。

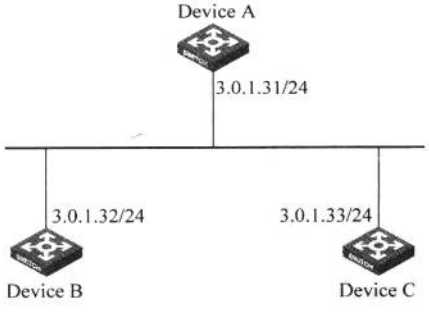


图 14-12 NTP 对等体模式典型配置组网图

3. 配置需求

(1) Device A 设置本地时钟作为参考时钟，层数为 2。

(2) Device B 工作在客户端模式，指定 Device A 为 NTP 服务器。

(3) Device C 工作在对等体模式，将 Device B 设为对等体。Device C 为主动对等体，Device B 为被动对等体。

4. 配置过程和解释

(1) 配置 Device A。设置本地时钟作为参考时钟，层数为 2。

```
<DeviceA> system-view
[DeviceA] ntp-service refclock-master 2
```

(2) 配置 Device B。设置 Device A 为 Device B 的 NTP 服务器。

```
<DeviceB> system-view
[DeviceB] ntp-service unicast-server 3.0.1.31
```

(3) 配置 Device C(Device B 向 Device A 同步后)。设置 Device B 为对等体。

```
<DeviceC> system-view
[DeviceC] ntp-service unicast-peer 3.0.1.32
```

14.4.3 NTP 广播模式典型配置指导

1. 背景

在常规服务器/客户端模式和对等体模式下，网络设备间需要进行 NTP 协议的交互。如果子网上的网络设备数量较多，则会产生大量的 NTP 协议交互报文。

采用 NTP 广播模式，可以减少子网中的 NTP 协议报文，减轻设备的负担。

2. 组网图

图 14-13 所示为 NTP 广播模式典型配置组网图。

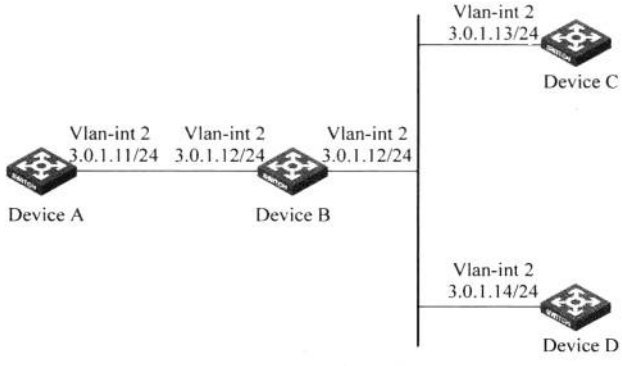


图 14-13 NTP 广播模式典型配置组网图

3. 配置需求

(1) Device C 是支持本地时钟作为主时钟的交换机，并设置本地时钟作为 NTP 主时钟，层数为 2。

(2) Device A 和 Device D 工作于广播客户端模式，分别从各自的 Vlan-interface 2 监听

广播消息。

4. 配置过程和解释

(1) 配置 Device C。设置为广播服务器,从 Vlan-interface 2 发送广播消息包。

```
<DeviceC> system-view
[DeviceC] interface Vlan-interface 2
[DeviceC-Vlan-interface2] ntp-service broadcast-server
```

(2) 配置 Device A。设置 Device A 为广播客户端,从 Vlan-interface 2 监听广播消息。

```
<DeviceA> system-view
[DeviceA] interface Vlan-interface 2
[DeviceA-Vlan-interface2] ntp-service broadcast-client
```

(3) 配置 Device D。设置 Device D 为广播客户端,从 Vlan-interface 2 监听广播消息。

```
<DeviceD> system-view
[DeviceD] interface Vlan-interface 2
[DeviceD-Vlan-interface2] ntp-service broadcast-client
```

14.4.4 NTP 组播模式典型配置指导

1. 背景

广播模式下,NTP 协议报文不能跨越子网,因此必须在每个子网中都选择 NTP 时间服务器。如果采用组播模式,则可以只配置一个时间服务器,通过三层组播转发路径将 NTP 组播报文在全网中转发。

2. 组网图

图 14-14 所示为 NTP 组播模式典型配置组网图。

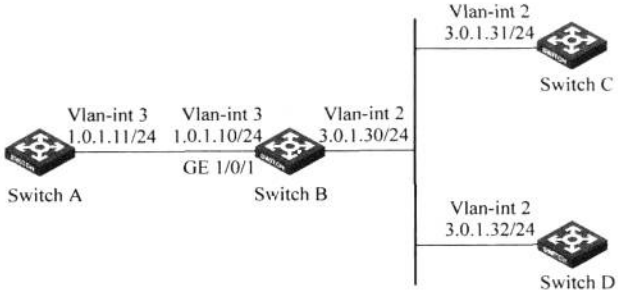


图 14-14 NTP 组播模式典型配置组网图

3. 配置需求

(1) Switch C 设置本地时钟作为参考时钟,层数为 2。

(2) Switch C 工作在组播服务器模式,从 VLAN 接口 2 向外发送组播报文。

(3) Switch A 和 Switch D 工作在组播客户端模式,Switch A 从 VLAN 接口 3 监听组播报文,Switch D 从 VLAN 接口 2 监听组播报文。

4. 配置过程和解释

(1) 配置 Switch C。

① 设置本地时钟作为参考时钟,层数为 2。

```
<SwitchC> system-view
[SwitchC] ntp-service refclock-master 2
```

② 设置 Switch C 为组播服务器，从 VLAN 接口 2 发送组播报文。

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ntp-service multicast-server
```

(2) 配置 Switch D。设置 Switch D 为组播客户端，从 VLAN 接口 2 监听组播报文。

```
<SwitchD> system-view
[SwitchD] interface vlan-interface 2
[SwitchD-Vlan-interface2] ntp-service multicast-client
```

(3) 配置 Switch B。由于 Switch A 与 Switch C 不在同一网段，所以 Switch B 上需要配置组播功能，否则 Switch A 收不到 Switch C 发出的组播报文。配置组播功能如下：

```
<SwitchB> system-view
[SwitchB] multicast routing-enable
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] pim dm
[SwitchB-Vlan-interface2] quit
[SwitchB] vlan 3
[SwitchB-vlan3] port GigabitEthernet 1/0/1
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] igmp enable
[SwitchB-Vlan-interface3] quit
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] igmp-snooping static-group 224.0.1.1 vlan 3
```

(4) 配置 Switch A。设置 Switch A 为组播客户端，从 VLAN 接口 3 监听组播报文。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ntp-service multicast-client
```

14.4.5 带身份验证的 NTP 广播模式典型配置指导

1. 背景

为了防止时间服务器的欺骗和仿冒，需要在 NTP 同步之前对 NTP 协议报文进行验证，以确保设备向正确的时间服务器同步时间。

2. 组网图

图 14-15 所示为带身份验证的 NTP 广播模式典型配置组网图。

3. 配置需求

(1) Switch C 设置本地时钟作为参考时钟，层数为 3。

(2) Switch C 工作在广播服务器模式，从 VLAN 接口 2 向外发送广播报文。

(3) Switch D 工作在广播客户端模式，从 VLAN 接口 2 监听广播报文。

(4) 同时在 Switch C 和 Switch D 上配置 NTP 验证。

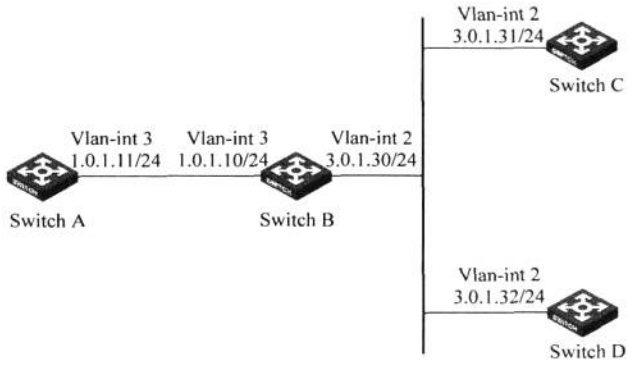


图 14-15 带身份验证的 NTP 广播模式典型配置组网图

4. 配置过程和解释

(1) 配置 Switch C。

① 设置本地时钟作为参考时钟,层数为 3。

```
<SwitchC> system-view
[SwitchC] ntp-service refclock-master 3
```

② 配置 NTP 验证。

```
[SwitchC] ntp-service authentication enable
[SwitchC] ntp-service authentication-keyid 88 authentication-mode md5 123456
[SwitchC] ntp-service reliable authentication-keyid 88
```

③ 设置 Switch C 为 NTP 广播服务器并指定密钥编号。

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ntp-service broadcast-server authentication-keyid 88
```

(2) 配置 Switch D。

① 配置 NTP 验证。

```
<SwitchD> system-view
[SwitchD] ntp-service authentication enable
[SwitchD] ntp-service authentication-keyid 88 authentication-mode md5 123456
[SwitchD] ntp-service reliable authentication-keyid 88
```

② 设置 Switch D 为 NTP 广播客户端。

```
[SwitchD] interface vlan-interface 2
[SwitchD-Vlan-interface2] ntp-service broadcast-client
```

14.5 LLDP 典型配置指导

网络设备的种类日益繁多且各自的配置错综复杂,为了使不同厂商的设备能够在网络中相互发现并交互各自的系统及配置信息,需要有一个标准的信息交流平台。

LLDP(Link Layer Discovery Protocol,链路层发现协议)就是在这样的背景下产生的,它提供了一种标准的链路层发现方式,可以将本端设备的主要能力、管理地址、设备标识、接口标识等信息组织成不同的 TLV(Type/Length/Value,类型/长度/值),并封装在 LLDPDU(Link Layer Discovery Protocol Data Unit,链路层发现协议数据单元)中发布给与自己直连的邻居,邻居收到这些信息后将其以标准 MIB(Management Information Base,管理信息库)的形式保存起来,以供网络管理系统查询及判断链路的通信状况。

1. 背景

H 公司的网络中有多家厂商的设备。为了能够对不同厂商设备间的二层链路进行状态监控,网络管理员决定配置 LLDP 协议。

2. 组网图

图 14-16 所示为 LLDP 典型配置组网图。

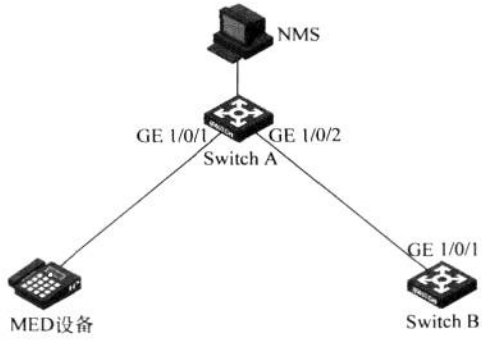


图 14-16 LLDP 典型配置组网图

3. 配置需求

(1) NMS 通过以太网与 Switch A 相连,Switch A 分别通过 GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 与 MED 设备、Switch B 相连。

(2) 在 Switch A 和 Switch B 的相应接口配置 LLDP 功能,使得 NMS 可以对 Switch A 链路的通信情况进行判断。

4. 配置过程和解释

(1) 配置 Switch A。

① 进入系统视图。

```
<SwitchA> system-view
```

② 全局使能 LLDP 功能。

```
[SwitchA] lldp enable
```

③ 分别在 GigabitEthernet 1/0/1 和 GigabitEthernet 1/0/2 接口使能 LLDP 功能并配置其工作模式为 rx。

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] lldp enable
[SwitchA-GigabitEthernet1/0/1] lldp admin-status rx
[SwitchA-GigabitEthernet1/0/1] quit
```

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] lldp enable
[SwitchA-GigabitEthernet1/0/2] lldp admin-status rx
[SwitchA-GigabitEthernet1/0/2] quit
```

(2) 配置 Switch B。

① 进入系统视图。

```
<SwitchB> system-view
```

② 全局使能 LLDP 功能。

```
[SwitchB] lldp enable
```

③ 在 GigabitEthernet 1/0/1 使能 LLDP 功能并配置其工作模式为 tx。

```
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] lldp enable
[SwitchB-GigabitEthernet1/0/1] lldp admin-status tx
```

(3) 验证配置结果。

① 在 Switch A 上显示全局和接口的状态信息。

```
<SwitchA> display lldp status
Global status of LLDP : Enable
The current number of neighbors    : 2
Neighbor information last changed time : 0 days, 0 hours, 4 minutes, 40 seconds
Transmit interval                  : 30s
Hold multiplier                    : 4
Reinit delay                       : 2s
Transmit delay                     : 2s
Trap interval                      : 5s
Fast start times                   : 3

Port 0 [GigabitEthernet1/0/1]      :
Port status of LLDP                : Enable
Admin status                       : Rx_Only
Trap flag                          : No
Roll time                          : 0s

Number of neighbors                : 1
Number of MED neighbors            : 1
Number of sent optional TLV        : 0
Number of received unknown TLV     : 0

Port 1 [GigabitEthernet1/0/2]      :
Port status of LLDP                : Enable
Admin status                       : Rx_Only
Trap flag                          : No
Roll time                          : 0s
```

```
Number of neighbors              : 1
Number of MED neighbors          : 0
Number of sent optional TLV      : 0
Number of received unknown TLV   : 3
...(其他端口的显示信息略)
```

② 默认情况下，Telnet 终端信息中心屏幕开关处于关闭状态。欲在 NMS 端看到 LLDP 状态变化产生的日志信息，需打开屏幕开关。

```
<SwitchA> terminal monitor
```

③ 将 Switch A 和 Switch B 上的链路断掉，Switch A 上会相继输出如下日志信息，Switch B 与此类似(此信息只有在终端屏幕开关打开的情况下才能看到)。

```
%Nov 21 11:38:42:86 2007 H3C IFNET/4/LINK UPDOWN: GigabitEthernet 1/0/2: link status is
DOWN
%Nov 21 11:40:26:846 2007 H3C LLDP/2/AGEOUTREM: Port GigabitEthernet 1/0/2 (IfIndex
9437201): Neighbor aged out, chassis ID: 000f-e272-8351, port ID: GigabitEthernet 1/0/1.
```

④ 在 Switch A 上显示全局和接口的状态信息。

```
<SwitchA> display lldp status
Global status of LLDP : Enable
The current number of neighbors    : 1
Neighbor information last changed time : 0 days, 0 hours, 5 minutes, 20 seconds
Transmit interval                  : 30s
Hold multiplier                    : 4
Reinit delay                       : 2s
Transmit delay                     : 2s
Trap interval                      : 5s
Fast start times                   : 3

Port 0 [GigabitEthernet1/0/1]      :
Port status of LLDP                : Enable
Admin status                       : Rx_Only
Trap flag                          : No
Roll time                          : 0s

Number of neighbors                : 1
Number of MED neighbors            : 1
Number of sent optional TLV        : 0
Number of received unknown TLV     : 5

Port 1 [GigabitEthernet1/0/2]      :
Port status of LLDP                : Enable
Admin status                       : Rx_Only
Trap flag                          : No
Roll time                          : 0s

Number of neighbors                : 0
```

```
Number of MED neighbors          : 0
Number of sent optional TLV      : 0
Number of received unknown TLV   : 0
...(其他端口的显示信息略)
```

注意：欲在终端屏幕上查看邻居变化产生的日志信息，需保证终端屏幕开关(通过命令 terminal monitor 打开)、日志信息开关(通过命令 terminal logging 打开)以及信息中心(通过命令 info-center enable 打开)处于打开状态。

第15章

MPLS与MCE配置指导

15.1 MPLS典型配置指导

MPLS(Multiprotocol Label Switching,多协议标签交换)是一种新兴的IP骨干网技术。MPLS在无连接的IP网络上引入面向连接的标签交换概念,将第三层路由技术和第二层交换技术相结合,充分发挥了IP路由的灵活性和二层交换的简捷性。

MPLS广泛应用于大规模网络中,具有以下优点。

(1) 在MPLS网络中,设备根据短而定长的标签转发报文,省去了通过软件查找IP路由的烦琐过程,为数据在骨干网络中的传输提供了一种高速、高效的方式。

(2) MPLS位于链路层和网络层之间,可以建立在各种链路层协议(如PPP、ATM、帧中继、以太网等)之上,为各种网络层(IPv4、IPv6、IPX等)提供面向连接的服务,兼容现有各种主流网络技术。

(3) 支持多层标签和面向连接的特点,使得MPLS在VPN、流量工程、QoS等方面得到广泛应用。

(4) 具有良好的扩展性,在MPLS网络基础上可以为客户提供各种服务。

VPLS(Virtual Private Lan Service,虚拟专用局域网业务)是一种MPLS二层VPN技术。在VPLS中,用户是由多点网络连接起来的,不同于传统VPN提供的P2P(Point to Point,点到点)的连接服务。VPLS实际上就是在PE上创建一系列的虚拟交换机租借给用户,虚拟交换机的组网和传统交换机完全相同,这样,用户就可以通过MAN(Metropolitan Area Network,城域网)或WAN(Wide Area Network,广域网)来实现自己的LAN(Local Area Network,局域网)。

BGP/MPLS VPN是服务提供商VPN解决方案中的一种基于PE的L3VPN技术,它使用BGP在服务提供商骨干网上发布VPN路由,使用MPLS在服务提供商骨干网上转发VPN报文。

BGP/MPLS VPN是一种基于MPLS的L3VPN,它组网方式灵活、可扩展性好,可以支持大规模的部署,实现不同VPN之间的路由隔离、地址空间隔离和访问隔离,支持大量VPN站点之间复杂的路由控制,并能够方便地支持MPLS QoS和MPLS TE,因此得到越来越多的应用。

15.1.1 MPLS基本配置指导

1. 背景

T电信公司购买了一批H3C三层以太网交换机，准备用这批设备构建基于MPLS的骨干运营网络，以便为客户提供VPN服务。要实现这一目标，T电信公司首先需要用H3C交换机部署骨干网，并在骨干网上完成基本的MPLS配置。

2. 组网图

图15-1所示为MPLS基本配置组网图。

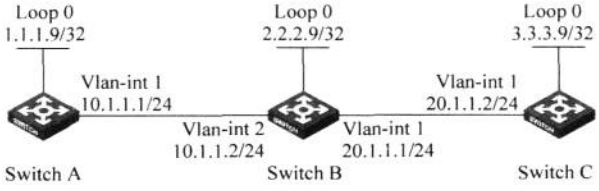


图15-1 MPLS基本配置组网图

3. 配置需求

如图15-1所示，配置需求如下：

(1) Switch A、Switch B和Switch C均运行OSPF作为MPLS骨干网上的IGP。

(2) Switch A、Switch B和Switch C均启动MPLS。

(3) 在Switch A和Switch B、Switch B和Switch C之间建立本地LDP会话。

(4) 在Switch A、Switch B和Switch C之间使用本地LDP会话建立一条LSP通道。

(5) 在Switch A和Switch C之间建立远端LDP会话。

4. 配置过程和解释

(1) 配置各接口的IP地址。按照图15-1配置各接口IP地址和掩码，包括VLAN接口和Loopback接口，配置方法可参见相关配置指导。

(2) 配置OSPF协议发布的路由信息。

① 配置Switch A。

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

② 配置Switch B。

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
```

```
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

③ 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[SwitchC-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

配置完成后，在各设备上执行 display ip routing-table 命令，可以看到其相互之间都学到了到对方的主机路由。下面以 Switch A 为例。

```
[SwitchA] display ip routing-table
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      NextHop         Interface

        1.1.1.9/32  Direct  0    0         127.0.0.1       InLoop 0
        2.2.2.9/32  OSPF    10   1563      10.1.1.2        Vlan 1
        3.3.3.9/32  OSPF    10   3125      10.1.1.2        Vlan 1
       10.1.1.0/24  Direct  0    0         10.1.1.1        Vlan 1
       10.1.1.1/32  Direct  0    0         127.0.0.1       InLoop 0
       10.1.1.2/32  Direct  0    0         10.1.1.2        Vlan 1
       20.1.1.0/24  OSPF    10   3124      10.1.1.2        Vlan 1
      127.0.0.0/8   Direct  0    0         127.0.0.1       InLoop 0
      127.0.0.1/32  Direct  0    0         127.0.0.1       InLoop 0
```

Switch A 和 Switch B、Switch B 和 Switch C 之间应建立起 OSPF 邻居关系，执行 display ospf peer verbose 命令可以看到邻居达到 FULL 状态。下面以 Switch A 为例。

```
[SwitchA] display ospf peer verbose
            OSPF Process 1 with Switch ID 1.1.1.9
                    Neighbors
 Area 0.0.0.0 interface 10.1.1.1(Vlan-interface1)'s neighbors
 Router ID: 2.2.2.9          Address: 10.1.1.2          GR State: Normal
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: None   BDR: None   MTU: 1500
   Dead timer due in 39  sec
   Neighbor is up for 00:02:13
   Authentication Sequence: [ 0 ]
```

(3) 配置 MPLS 基本能力，并使能 LDP。

① 配置 Switch A。

```
[SwitchA] mpls lsr-id 1.1.1.9
[SwitchA] mpls
[SwitchA-mpls] quit
[SwitchA] mpls ldp
[SwitchA-mpls-ldp] quit
```

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] mpls
[SwitchA-Vlan-interface1] mpls ldp
[SwitchA-Vlan-interface1] quit
```

② 配置 Switch B。

```
[SwitchB] mpls lsr-id 2.2.2.9
[SwitchB] mpls
[SwitchB-mpls] quit
[SwitchB] mpls ldp
[SwitchB-mpls-ldp] quit
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] mpls
[SwitchB-Vlan-interface1] mpls ldp
[SwitchB-Vlan-interface1] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] mpls
[SwitchB-Vlan-interface2] mpls ldp
[SwitchB-Vlan-interface2] quit
```

③ 配置 Switch C。

```
[SwitchC] mpls lsr-id 1.1.1.9
[SwitchC] mpls
[SwitchC-mpls] quit
[SwitchC] mpls ldp
[SwitchC-mpls-ldp] quit
[SwitchC] interface vlan-interface 1
[SwitchC-Vlan-interface1] mpls
[SwitchC-Vlan-interface1] mpls ldp
[SwitchC-Vlan-interface1] quit
```

完成上述配置后，Switch A 和 Switch B、Switch B 和 Switch C 之间的本地 LDP 会话建立成功。在各设备上执行 display mpls ldp session 命令，可以看到 LDP 会话的建立情况；执行 display mpls ldp peer 命令，可以看到 LDP 的对等体情况。下面以 Switch A 为例。

```
[SwitchA] display mpls ldp session
                LDP Session(s) in Public Network
 Total number of sessions: 1
 ------------------------------------------------------------------------
 Peer-ID       Status        LAM  SsnRole  FT   MD5  KA-Sent/Rcv
 ------------------------------------------------------------------------
 2.2.2.9:0     Operational   DU   Passive  Off  Off  5/5
 ------------------------------------------------------------------------
 LAM : Label Advertisement Mode          FT  : Fault Tolerance
[SwitchA] display mpls ldp peer
          LDP Peer Information in Public network
 Total number of peers: 1
 ------------------------------------------------------------------------
 Peer-ID                 Transport-Address   Discovery-Source
 ------------------------------------------------------------------------
```

```
2.2.2.9:0              2.2.2.9              Vlan-interface 1
------------------------------------------------------------------------------
```

(4) 配置远端 LDP 会话。

① 配置 Switch A。

```
[SwitchA] mpls ldp remote-peer peerc
[SwitchA-mpls-ldp-remote-peerc] remote-ip 3.3.3.9
[SwitchA-mpls-ldp-remote-peerc] quit
```

② 配置 Switch C。

```
[SwitchC] mpls ldp remote-peer peera
[SwitchC-mpls-ldp-remote-peera] remote-ip 1.1.1.9
[SwitchC-mpls-ldp-remote-peera] quit
```

完成上述配置后，在 Switch A 上查看 LDP 会话的建立情况和 LDP 的对等体情况，可以看到增加了与 Switch C 的远端 LDP 会话。

```
[SwitchA] display mpls ldp session
                LDP Session(s) in Public Network
 Total number of sessions: 2
 ------------------------------------------------------------------
 Peer-ID         Status       LAM  SsnRole  FT   MD5  KA-Sent/Rcv
 ------------------------------------------------------------------
 2.2.2.9:0       Operational  DU   Passive  Off  Off  35/35
 3.3.3.9:0       Operational  DU   Passive  Off  Off  8/8
 ------------------------------------------------------------------
 LAM : Label Advertisement Mode          FT  : Fault Tolerance
[SwitchA] display mpls ldp peer
          LDP Peer Information in Public network
 Total number of peers: 2
 ------------------------------------------------------------------
 Peer-ID                Transport-Address   Discovery-Source
 ------------------------------------------------------------------
 2.2.2.9:0              2.2.2.9             Vlan-interface 1
 3.3.3.9:0              3.3.3.9             Remote Peer : peerc
 ------------------------------------------------------------------
```

③ 配置 LSP 的触发策略为 all，即所有静态路由和 IGP 路由项都会触发 LDP 建立 LSP。

a. 配置 Switch A。

```
[SwitchA] mpls
[SwitchA-mpls] lsp-trigger all
[SwitchA-mpls] return
```

b. 配置 Switch B。

```
[SwitchB] mpls
[SwitchB-mpls] lsp-trigger all
```

```
[SwitchB-mpls] quit
```

c. 配置 Switch C。

```
[SwitchC] mpls
[SwitchC-mpls] lsp-trigger all
[SwitchC-mpls] quit
```

提示：由于 MPLS 功能会在原有报文上封装一层或多层标签，因此建议用户在使能某 VLAN 接口的 MPLS 功能后，将该 VLAN 内端口的 jumboframe 功能开启，并根据实际应用和标签嵌套层数配置相应的帧长，避免某些报文因超长而被丢弃。例如，如果需要对 FTP 报文封装两层 MPLS 标签，可配置端口的 jumboframe 帧长为 1544B(FTP 报文 1518B+MPLS 标签 4B×2+VLAN 标签 4B+以太网帧头长度 14B)。

15.1.2 VPLS 基本配置指导

1. 背景

M 公司准备依托 T 电信公司 MPLS 骨干网及其提供的 VPN 服务，构建公司内部网络，将其两个分支站点网络连接起来。由于 M 公司希望各站点以 LAN 方式连接在一起而隐藏其内部三层网络信息，所以要求部署基于 MPLS 的 VPLS 服务。

2. 组网图

图 15-2 所示为 VPLS 基本配置组网图。

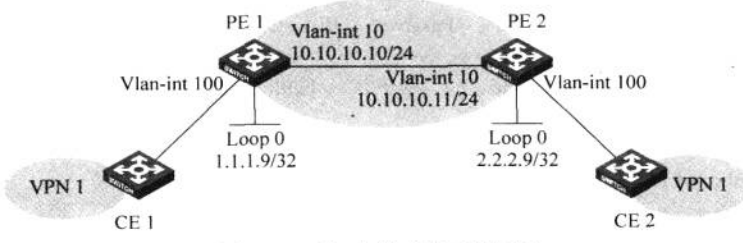


图 15-2 VPLS 基本配置组网图

3. 配置需求

如图 15-2 所示，两个站点通过 MPLS 骨干网连接在一起，CE 1 和 CE 2 分属于两个站点，同属于 VPN 1，要求如下：

(1) CE 1 和 CE 2 分别以接口 Vlan-interface 100 接入 PE 设备。

(2) PE 设备间以接口 Vlan-interface 10 连接。

(3) 配置 VPLS 实例 aaa 为 LDP 方式(Martini 方式)，bbb 为 BGP 方式(Kompella 方式)，AS 号为 100。

提示：本例采用两个实例的目的在于告诉读者应如何配置 Martini 和 Kompella 两种方式，实际使用时此处仅需配置一个实例即可。

4. 配置过程和解释

(1) PE 1 的配置。

① 配置 IGP 协议，此例选择 OSPF，具体配置略。

② 配置 MPLS 基本能力。

```
<Sysname> system-view
[Sysname] sysname PE1
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.9 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
```

③ 配置接口 Vlan-interface 10。

```
[PE1] interface vlan-interface 10
[PE1-Vlan-interface10] ip address 10.10.10.10 24
```

④ 配置接口 MPLS 基本能力。

```
[PE1-Vlan-interface10] mpls
[PE1-Vlan-interface10] mpls ldp
[PE1-Vlan-interface10] quit
```

⑤ 配置远端 LDP 会话。

```
[PE1] mpls ldp remote-peer 1
[PE1-mpls-remote-1] remote-ip 2.2.2.9
[PE1-mpls-remote-1] quit
```

⑥ 配置 BGP 扩展。

```
[PE1] bgp 100
[PE1-bgp] peer 2.2.2.9 as-number 100
[PE1-bgp] peer 2.2.2.9 connection-interface loopback 0
[PE1-bgp] vpls-family
[PE1-bgp-af-vpls] peer 2.2.2.9 enable
[PE1-bgp-af-vpls] quit
[PE1-bgp] quit
```

⑦ 使能 L2VPN 和 MPLS L2VPN。

```
[PE1] l2vpn
[PE1-l2vpn] mpls l2vpn
[PE1-l2vpn] quit
```

⑧ 配置 LDP 方式下的 VPLS 实例 aaa 基本属性。

```
[PE1] vsi aaa static
[PE1-vsi-aaa] pwsignal ldp
[PE1-vsi-aaa-ldp] vsi-id 500
[PE1-vsi-aaa-ldp] peer 2.2.2.9
[PE1-vsi-aaa-ldp] quit
[PE1-vsi-aaa] quit
```

⑨ 配置 BGP 方式下的 VPLS 实例 bbb 基本属性。

```
[PE1] vsi bbb auto
[PE1-vsi-bbb] pwsignal bgp
[PE1-vsi-bbb-bgp] route-distinguisher 100:1
[PE1-vsi-bbb-bgp] vpn-target 111:1
[PE1-vsi-bbb-bgp] site 1 range 10
[PE1-vsi-bbb-bgp] quit
[PE1-vsi-bbb] quit
```

⑩ 配置接口 Vlan-interface 100，并绑定 VPLS 实例 aaa 或 bbb。

```
[PE1] interface vlan-interface 100
// 如果 Vlan-interface 100 下绑定 VPLS 实例 aaa
[PE1-Vlan-interface100] l2 binding vsi aaa
// 如果 Vlan-interface 100 下绑定 VPLS 实例 bbb
[PE1-Vlan-interface100] l2 binding vsi bbb
[PE1-Vlan-interface100] quit
```

(2) PE 2 的配置。

① 配置 IGP 协议，此例选择 OSPF，具体配置略。

② 配置 MPLS 基本能力。

```
<Sysname> system-view
[Sysname] sysname PE2
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 2.2.2.9 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 2.2.2.9
[PE2] mpls
[PE1-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
```

③ 配置 VLAN 10，创建接口 Vlan-interface 10。

```
[PE2] interface vlan-interface 10
[PE2-Vlan-interface10] ip address 10.10.10.11 24
```

④ 配置 VLAN 接口 MPLS 基本能力。

```
[PE2-Vlan-interface10] mpls
[PE2-Vlan-interface10] mpls ldp
[PE2-Vlan-interface10] quit
```

⑤ 配置远端 LDP 会话。

```
[PE2] mpls ldp remote-peer 2
[PE2-mpls-remote-2] remote-ip 1.1.1.9
[PE2-mpls-remote-2] quit
```

⑥ 配置 BGP 扩展。

```
[PE2] bgp 100
```

```
[PE2-bgp] peer 1.1.1.9 as-number 100
[PE2-bgp] peer 1.1.1.9 connection-interface loopback 0
[PE2-bgp] vpls-family
[PE2-bgp-af-vpls] peer 1.1.1.9 enable
[PE2-bgp-af-vpls] quit
[PE2-bgp] quit
```

⑦ 使能 L2VPN 和 MPLS L2VPN。

```
[PE2] l2vpn
[PE2-l2vpn] mpls l2vpn
[PE2-l2vpn] quit
```

⑧ 配置 LDP 方式下的 VPLS 实例 aaa 基本属性。

```
[PE2] vsi aaa static
[PE2-vsi-aaa] pwsignal ldp
[PE2-vsi-aaa-ldp] vsi-id 500
[PE2-vsi-aaa-ldp] peer 1.1.1.9
[PE2-vsi-aaa-ldp] quit
[PE2-vsi-aaa] quit
```

⑨ 配置 BGP 方式下的 VPLS 实例 bbb 基本属性。

```
[PE2] vsi bbb auto
[PE2-vsi-bbb] pwsignal bgp
[PE2-vsi-bbb-bgp] route-distinguisher 100:1
[PE2-vsi-bbb-bgp] vpn-target 111:1
[PE2-vsi-bbb-bgp] site 2 range 10
[PE2-vsi-bbb-bgp] quit
[PE2-vsi-bbb] quit
```

⑩ 配置接口 Vlan-interface 100，并绑定 VPLS 实例 aaa 或 bbb。

```
[PE2] interface Vlan-interface 100
// 如果 Vlan-interface 100 下绑定 VPLS 实例 aaa
[PE2-Vlan-interface100] l2 binding vsi aaa
// 如果 Vlan-interface 100 下绑定 VPLS 实例 bbb
[PE2-Vlan-interface100] l2 binding vsi bbb
[PE2-Vlan-interface100] quit
```

(3) 配置完成后的检验。完成上述配置后，在 PE 上执行 display vpls connection 命令，可以看到建立了一条 PW 连接，状态为 Up。

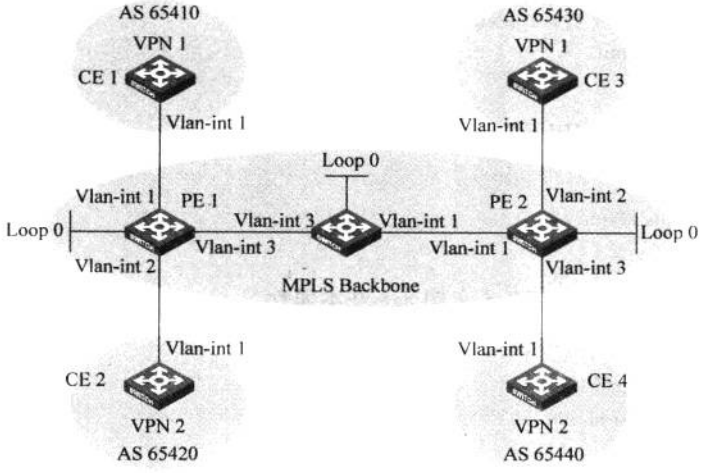
15.1.3 MPLS L3VPN 典型配置指导

1. 背景

T 电信公司建设 MPLS 骨干网，为企业提供 VPN 运营服务。A 公司和 B 公司同时提出申请，要求 T 公司能基于 BGP/MPLS VPN 为其提供第三层的连通服务，在确保本公司两站点连通的同时，禁止其他公司与本公司互通。

2. 组网图

图 15-3 所示为 MPLS L3VPN 典型配置组网图。



设　备	接　口	IP 地址	设　备	接　口	IP 地址
CE 1	Vlan-int 1	10.1.1.1/24	P	Loop 0	2.2.2.9/32
PE 1	Loop 0	1.1.1.9/32		Vlan-int 1	172.2.1.1/24
	Vlan-int 1	10.1.1.2/24		Vlan-int 3	172.1.1.2/24
	Vlan-int 3	172.1.1.1/24	PE 2	Loop 0	3.3.3.9/32
	Vlan-int 2	10.2.1.2/24		Vlan-int 1	172.2.1.2/24
CE 2	Vlan-int 1	10.2.1.1/24		Vlan-int 2	10.3.1.2/24
CE 3	Vlan-int 1	10.3.1.1/24		Vlan-int 3	10.4.1.2/24
CE 4	Vlan-int 1	10.4.1.1/24			

图 15-3　MPLS L3VPN 典型配置组网图

3. 配置需求

如图 15-3 所示，A 公司使用的 VPN 为 VPN 1，CE 1 和 CE 3 为 A 公司连接到运营商的 CE 设备；B 公司使用的 VPN 为 VPN 2，CE 2 和 CE 4 为 B 公司连接到运营商的 CE 设备。要求如下：

(1) CE 1、CE 3 属于 VPN 1，CE 2、CE 4 属于 VPN 2。

(2) VPN 1 使用的 VPN Target 属性为 111:1，VPN 2 使用的 VPN Target 属性为 222:2。不同 VPN 用户之间不能互相访问。

(3) PE、P 为支持 MPLS 的设备，在 PE 1 和 PE 2 之间建立 MPLS L3VPN，使 VPN 1 的站点之间可以互通，VPN 2 的站点之间可以互通，但 VPN 1 与 VPN 2 之间互相隔离。

4. 配置过程和解释

(1) 在 MPLS 骨干网上配置 IGP 协议，实现骨干网 PE 和 P 的互通。

① 配置 PE 1。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.9 32
```

```
[PE1-LoopBack0] quit
[PE1] interface vlan-interface 3
[PE1-Vlan-interface3] ip address 172.1.1.1 24
[PE1-Vlan-interface3] quit
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 172.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

② 配置 P。

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 2.2.2.9 32
[P-LoopBack0] quit
[P] interface vlan-interface 3
[P-Vlan-interface3] ip address 172.1.1.2 24
[P-Vlan-interface3] quit
[P] interface vlan-interface 1
[P-Vlan-interface1] ip address 172.2.1.1 24
[P-Vlan-interface1] quit
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 172.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 172.2.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

③ 配置 PE 2。

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 3.3.3.9 32
[PE2-LoopBack0] quit
[PE2] interface vlan-interface 1
[PE2-Vlan-interface1] ip address 172.2.1.2 24
[PE2-Vlan-interface1] quit
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 172.2.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

配置完成后，PE 1、P、PE 2 之间应能建立 OSPF 邻居，执行 display ospf peer 命令可以看到邻居达到 FULL 状态。执行 display ip routing-table 命令可以看到 PE 之间学习到对方的 Loopback 路由。以 PE 1 为例，有如下程序。

```
[PE1] display ip routing-table
```

```
Routing Tables: Public
         Destinations : 9        Routes : 9
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
1.1.1.9/32          Direct  0    0         127.0.0.1       InLoop 0
2.2.2.9/32          OSPF    10   1         172.1.1.2       Vlan 3
3.3.3.9/32          OSPF    10   2         172.1.1.2       Vlan 3
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop 0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop 0
172.1.1.0/24        Direct  0    0         172.1.1.1       Vlan 3
172.1.1.1/32        Direct  0    0         127.0.0.1       InLoop 0
172.1.1.2/32        Direct  0    0         172.1.1.2       Vlan 3
172.2.1.0/24        OSPF    10   1         172.1.1.2       Vlan 3
[PE1] display ospf peer verbose
            OSPF Process 1 with Router ID 1.1.1.9
                    Neighbors
 Area 0.0.0.0 interface 172.1.1.1(Vlan-interface3)'s neighbors
 Router ID: 172.1.1.2          Address: 172.1.1.2          GR State: Normal
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: None    BDR: None    MTU: 1500
   Dead timer due in 38  sec
   Neighbor is up for 00:02:44
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 5
```

(2) 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP。

① 配置 PE 1。

```
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
[PE1-mpls] lsp-trigger all
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface vlan-interface 3
[PE1-Vlan-interface3] mpls
[PE1-Vlan-interface3] mpls ldp
[PE1-Vlan-interface3] quit
```

② 配置 P。

```
[P] mpls lsr-id 2.2.2.9
[P] mpls
[P-mpls] lsp-trigger all
[P-mpls] quit
[P] mpls ldp
[P-mpls-ldp] quit
[P] interface vlan-interface 3
[P-Vlan-interface3] mpls
[P-Vlan-interface3] mpls ldp
[P-Vlan-interface3] quit
[P] interface vlan-interface 1
```

```
[P-Vlan-interface1] mpls
[P-Vlan0interface1] mpls ldp
[P-Vlan-interface1] quit
```

③ 配置 PE 2。

```
[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls
[PE2-mpls] lsp-trigger all
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface vlan-interface 1
[PE2-Vlan-interface1] mpls
[PE2-Vlan-interface1] mpls ldp
[PE2-Vlan-interface1] quit
```

上述配置完成后，PE 1、P、PE 2 之间应能建立 LDP 会话，执行 display mpls ldp session 命令可以看到显示结果中 Session State 项为 Operational。执行 display mpls ldp lsp 命令，可以看到 LDP LSP 的建立情况。以 PE 1 为例，有如下程序。

```
[PE1] display mpls ldp session
                LDP Session(s) in Public Network
------------------------------------------------------------------------------
Peer-ID          Status       LAM  SsnRole  FT   MD5  KA-Sent/Rcv
------------------------------------------------------------------------------
2.2.2.9:0        Operational  DU   Passive  Off  Off  5/5
------------------------------------------------------------------------------
LAM : Label Advertisement Mode          FT  : Fault Tolerance
[PE1] display mpls ldp lsp
                        LDP LSP Information
------------------------------------------------------------------------------
SN  DestAddress/Mask   In/OutLabel   Next-Hop      In/Out-Interface
------------------------------------------------------------------------------
1   1.1.1.9/32         3/NULL        127.0.0.1     Vlan-interface 3/InLoop0
2   2.2.2.9/32         NULL/3        172.1.1.2     -------/Vlan-interface 3
3   3.3.3.9/32         NULL/1024     172.1.1.2     -------/Vlan-interface 3
------------------------------------------------------------------------------
A '*' before an LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
```

(3) 在 PE 设备上配置 VPN 实例，将 CE 接入 PE。

① 配置 PE 1。

```
[PE1] ip vpn-instance vpn 1
[PE1-vpn-instance-vpn1] route-distinguisher 100:1
[PE1-vpn-instance-vpn1] vpn-target 111:1
[PE1-vpn-instance-vpn1] quit
[PE1] ip vpn-instance vpn 2
[PE1-vpn-instance-vpn2] route-distinguisher 100:2
[PE1-vpn-instance-vpn2] vpn-target 222:2
```

```
[PE1-vpn-instance-vpn2] quit
[PE1] interface vlan-interface 1
[PE1-Vlan-interface1] ip binding vpn-instance vpn 1
[PE1-Vlan-interface1] ip address 10.1.1.2 24
[PE1-Vlan-interface1] quit
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] ip binding vpn-instance vpn 2
[PE1-Vlan-interface2] ip address 10.2.1.2 24
[PE1-Vlan-interface2] quit
```

② 配置 PE 2。

```
[PE2] ip vpn-instance vpn 1
[PE2-vpn-instance-vpn1] route-distinguisher 200:1
[PE2-vpn-instance-vpn1] vpn-target 111:1
[PE2-vpn-instance-vpn1] quit
[PE2] ip vpn-instance vpn 2
[PE2-vpn-instance-vpn2] route-distinguisher 200:2
[PE2-vpn-instance-vpn2] vpn-target 222:2
[PE2-vpn-instance-vpn2] quit
[PE2] interface vlan-interface 2
[PE2-Vlan-interface2] ip binding vpn-instance vpn 1
[PE2-Vlan-interface2] ip address 10.3.1.2 24
[PE2-Vlan-interface2] quit
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] ip binding vpn-instance vpn 2
[PE2-Vlan-interface3] ip address 10.4.1.2 24
[PE2-Vlan-interface3] quit
```

③ 按图 15-3 配置各 CE 的接口 IP 地址，配置过程略。

配置完成后，在 PE 设备上执行 display ip vpn-instance 命令可以看到 VPN 实例的配置情况。各 PE 能 ping 通自己接入的 CE。以 PE 1 和 CE 1 为例，有如下程序。

```
[PE1] display ip vpn-instance
  Total VPN-Instances configured : 2
  VPN-Instance Name        RD            Create Time
  vpn1                     100:1         2006/08/13 09:32:45
  vpn2                     100:2         2006/08/13 09:42:59
[PE1] ping -vpn-instance vpn 1 10.1.1.1
  PING 10.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.1: bytes=56 Sequence=1 ttl=255 time=56 ms
    Reply from 10.1.1.1: bytes=56 Sequence=2 ttl=255 time=4 ms
    Reply from 10.1.1.1: bytes=56 Sequence=3 ttl=255 time=4 ms
    Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=255 time=52 ms
    Reply from 10.1.1.1: bytes=56 Sequence=5 ttl=255 time=3 ms
  --- 10.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/23/56 ms
```

(4) 在 PE 与 CE 之间建立 EBGP 对等体,引入 VPN 路由。

① 配置 CE 1。

```
<CE1> system-view
[CE1] bgp 65410
[CE1-bgp] peer 10.1.1.2 as-number 100
[CE1-bgp] import-route direct
[CE1-bgp] quit
```

说明:另外 3 个 CE 设备(CE 2~CE 4)配置与 CE 1 设备配置类似,配置过程省略。

② 配置 PE 1。

```
[PE1] bgp 100
[PE1-bgp] ipv 4-family vpn-instance vpn 1
[PE1-bgp-vpn1] peer 10.1.1.1 as-number 65410
[PE1-bgp-vpn1] import-route direct
[PE1-bgp-vpn1] quit
[PE1-bgp] ipv4-family vpn-instance vpn 2
[PE1-bgp-vpn2] peer 10.2.1.1 as-number 65420
[PE1-bgp-vpn2] import-route direct
[PE1-bgp-vpn2] quit
[PE1-bgp] quit
```

说明:PE 2 的配置与 PE 1 类似,配置过程省略。

配置完成后,在 PE 设备上执行 display bgp vpnv4 vpn-instance peer 命令,可以看到 PE 与 CE 之间的 BGP 对等体关系已建立,并达到 Established 状态。以 PE 1 与 CE 1 的对等体关系为例,有以下程序。

```
[PE1] display bgp vpnv4 vpn-instance vpn1 peer
 BGP local router ID : 1.1.1.9
 Local AS number : 100
 Total number of peers : 1                Peers in established state : 1

  Peer        V  AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down     State
  10.1.1.1    4  65410  11       9        0     1        00:06:37    Established
```

(5) 在 PE 之间建立 MP-IBGP 对等体。

① 配置 PE 1。

```
[PE1] bgp 100
[PE1-bgp] peer 3.3.3.9 as-number 100
[PE1-bgp] peer 3.3.3.9 connect-interface loopback 0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] peer 3.3.3.9 enable
[PE1-bgp-af-vpnv4] quit
[PE1-bgp] quit
```

② 配置 PE 2。

```
[PE2] bgp 100
[PE2-bgp] peer 1.1.1.9 as-number 100
```

```
[PE2-bgp] peer 1.1.1.9 connect-interface loopback 0
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpnv4] peer 1.1.1.9 enable
[PE2-bgp-af-vpnv4] quit
[PE2-bgp] quit
```

配置完成后，在 PE 设备上执行 display bgp peer 或 display bgp vpnv4 all peer 命令，可以看到 PE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

```
[PE1] display bgp peer
 BGP local router ID : 1.1.1.9
 Local AS number : 100
 Total number of peers : 1              Peers in established state : 1
  Peer       V    AS  MsgRcvd   MsgSent  OutQ     PrefRcv  Up/Down   State
  3.3.3.9    4    100     2         6       0          0    00:00:12  Established
```

(6) 配置完成后的检验。在 PE 设备上执行 display ip routing-table vpn-instance 命令，可以看到去往对端 CE 的路由。以 PE 1 为例，有如下程序。

```
[PE1] display ip routing-table vpn-instance vpn1
Routing Tables: vpn1
         Destinations : 3        Routes : 3
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
10.1.1.0/24         Direct  0    0         10.1.1.2        Vlan 1
10.1.1.2/32         Direct  0    0         127.0.0.1       InLoop 0
10.3.1.0/24         BGP     255  0         3.3.3.9         NULL 0
[PE1] display ip routing-table vpn-instance vpn2
Routing Tables: vpn2
         Destinations : 3        Routes : 3
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
10.2.1.0/24         Direct  0    0         10.2.1.2        Vlan 2
10.2.1.2/32         Direct  0    0         127.0.0.1       InLoop 0
10.4.1.0/24         BGP     255  0         3.3.3.9         NULL 0
```

同一 VPN 的 CE 能够相互 Ping 通，不同 VPN 的 CE 不能相互 ping 通。例如，CE 1 能够 ping 通 CE 3(10.3.1.1)，但不能 ping 通 CE 4(10.4.1.1)。

```
[CE1] ping 10.3.1.1
  PING 10.3.1.1: 56  data bytes, press Ctrl_C to break
    Reply from 10.3.1.1: bytes=56 Sequence=1 ttl=253 time=72 ms
    Reply from 10.3.1.1: bytes=56 Sequence=2 ttl=253 time=34 ms
    Reply from 10.3.1.1: bytes=56 Sequence=3 ttl=253 time=50 ms
    Reply from 10.3.1.1: bytes=56 Sequence=4 ttl=253 time=50 ms
    Reply from 10.3.1.1: bytes=56 Sequence=5 ttl=253 time=34 ms
  --- 10.3.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 34/48/72 ms
[CE1] ping 10.4.1.1
```

```
PING 10.4.1.1: 56  data bytes, press Ctrl_C to break
  Request time out
  Request time out
  Request time out
  Request time out
  Request time out
--- 10.4.1.1 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
  100.00% packet loss
```

提示：BGP/MPLS VPN 引入了 RD，即使两个 VPN 使用的地址空间完全相同，也完全可以正常工作，而不会发生地址冲突。例如，即使 CE 2 也使用地址 10.1.1.1/24，且 CE 4 也使用地址 10.3.1.1/24，VPN 1 与 VPN 2 仍然可以正常工作，而不会发生混淆或互通的情况。

执行 ip binding vpn-instance 命令将删除接口上已经配置的 IP 地址，因此需要重新配置接口的 IP 地址。

15.2 MCE 典型配置指导

BGP/MPLS VPN 以隧道的方式解决了在公网中传送私网数据的问题，但传统的 BGP/MPLS VPN 架构要求每个 VPN 实例单独使用一个 CE 与 PE 相连。

随着用户业务的不断细化和安全需求的提高，很多情况下一个私有网络内的用户需要划分成多个 VPN，不同 VPN 用户间的业务需要完全隔离。此时，为每个 VPN 单独配置一台 CE 将加大用户的设备开支和维护成本；而多个 VPN 共用一台 CE，使用同一个路由表项，又无法保证数据的安全性。

MCE 就是为解决这一问题应运而生的。

MCE 可以有效解决多 VPN 网络带来的用户数据安全与网络成本之间的矛盾，它使用 CE 设备本身的 VLAN 接口编号与网络内的 VPN 进行绑定，并为每个 VPN 创建和维护独立的路由转发表(Multi-VRF)。这样不但能够隔离私网内不同 VPN 的报文转发路径，而且通过与 PE 间的配合，也能够将每个 VPN 的路由正确发布至对端 PE，保证 VPN 报文在公网内的传输。

15.2.1 使用 OSPF/RIP/IS-IS 引入 VPN 路由的 MCE 典型配置指导

1. 背景

M 集团采购了一批网络设备，准备依托 T 电信公司 MPLS 骨干网及其提供的 BGP/MPLS VPN 服务，构建公司内部网络。M 集团将其内部网络根据业务部门划分为 3 个 VPN，某些分公司必须同时支持这 3 类业务，即必须同时属于这 3 个 VPN。为了减少网络设备的投入，M 公司在一些分公司采用具有 MCE 功能的交换机，在 BGP/MPLS VPN 组网应用中承担多个 VPN 实例的 CE 功能。

因私网规模较小，M 公司私网路由器全部配置 OSPF/RIP/IS-IS 等 IGP，因而需使用 IGP 引入 VPN 路由。

2. 组网图

图 15-4 所示为使用 OSPF/RIP/IS-IS 引入 VPN 路由的 MCE 典型配置组网图。

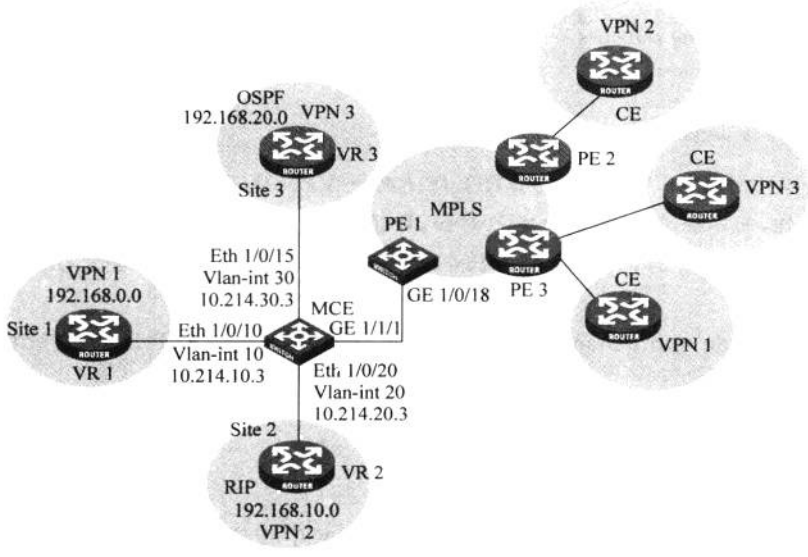


图 15-4 使用 OSPF/RIP/IS-IS 引入 VPN 路由的 MCE 典型配置组网图

3. 配置需求

如图 15-4 所示，设备 VR 1、VR 2、VR 3 和 MCE 均位于同一分公司内，该分公司因业务部署需要配置 3 个 VPN，但由于投资限制，只能配置一台交换机作为 CE，所以此交换机必须配置 MCE。

(1) MCE 设备通过 Vlan-interface 10 接口(IP 地址 10.214.10.3)连接到 VPN 1，地址范围为 192.168.0.0/16，通过 Vlan-interface 20(IP 地址 10.214.20.3)接口连接到 VPN 2，通过 Vlan-interface 30(IP 地址 10.214.30.3)接口连接到 VPN 3。

(2) 其中 Site 1 内未使用路由协议；Site 2 内运行 RIP 路由协议，地址范围为 192.168.10.0/24；Site 3 内运行 OSPF 路由协议，地址范围为 192.168.20.0/24。

(3) 要求 MCE 设备能够将 VPN 之间的路由隔离，并通过 OSPF 将各 VPN 的路由发布到 PE 设备。

(4) 对于使用 RIP、IS-IS 协议将 VPN 的路由发布到 PE 设备，其具体配置只在“5) MCE 与 PE 1 间的路由配置”处与使用 OSPF 作为 MCE 到 PE 间路由协议时有所不同，所以只在“5) MCE 与 PE 1 间的路由配置”中添加了相应 RIP 和 IS-IS 配置过程。

4. 配置过程和解释

1) 配置 MCE 上的 VPN 实例并与接口进行绑定

(1) 切换 MCE 设备的工作模式为 MCE 模式，并重新启动设备。

```
<MCE> system-view
[MCE] switch-mode mce
```

```
[MCE] quit
<MCE> reboot
```

说明：在配置 S7500E 系列交换机的 MCE 功能时，不需要配置 switch-mode mce 命令和重启设备。

(2) 在 MCE 设备上配置 VPN 实例，名称分别为 VPN 1、VPN 2 和 VPN 3，RD 分别取值为 10：1、20：1 和 30：1。

```
<MCE> system-view
[MCE] ip vpn-instance vpn 1
[MCE-vpn-instance-vpn1] route-distinguisher 10:1
[MCE-vpn-instance-vpn1] quit
[MCE] ip vpn-instance vpn 2
[MCE-vpn-instance-vpn2] route-distinguisher 20:1
[MCE-vpn-instance-vpn2] quit
[MCE] ip vpn-instance vpn 3
[MCE-vpn-instance-vpn3] route-distinguisher 30:1
```

(3) 创建 VLAN 10，将端口 Eth 1/0/10 加入 VLAN 10，并创建 Vlan-interface 10 接口。

```
[MCE-vpn-instance-vpn3] quit
[MCE] vlan 10
[MCE-vlan10] port Ethernet 1/0/10
[MCE-vlan10] quit
[MCE] interface Vlan-interface 10
```

(4) 配置 Vlan-interface 10 接口与 VPN 1 实例进行绑定，并配置 IP 地址为 10.214.10.3，掩码为 24 位。

```
[MCE-Vlan-interface10] ip binding vpn-instance vpn 1
[MCE-Vlan-interface10] ip address 10.214.10.3 24
[MCE-Vlan-interface10] quit
```

(5) 使用类似步骤配置 VLAN 20，将端口 Eth 1/0/20 加入 VLAN 20，配置接口与 VPN 2 实例绑定并配置 IP 地址。

```
[MCE] vlan 20
[MCE-vlan20] port Ethernet 1/0/20
[MCE-vlan20] quit
[MCE] interface Vlan-interface 20
[MCE-Vlan-interface20] ip binding vpn-instance vpn 2
[MCE-Vlan-interface20] ip address 10.214.20.3 24
[MCE-Vlan-interface20] quit
```

(6) 使用类似步骤配置 VLAN 30，将端口 Eth 1/0/15 加入 VLAN 30，配置接口与 VPN 3 实例绑定并配置 IP 地址。

```
[MCE] vlan 30
[MCE-vlan30] port Ethernet 1/0/15
[MCE-vlan30] quit
```

```
[MCE] interface Vlan-interface 30
[MCE-Vlan-interface30] ip binding vpn-instance vpn 3
[MCE-Vlan-interface30] ip address 10.214.30.3 24
[MCE-Vlan-interface30] quit
```

2) MCE 与 Site 1 之间的路由配置

说明：MCE 与 Site 1 直接相连，且 Site 1 内未使用路由协议，因此可以使用静态路由进行配置。

(1) 在 VR 1 上的配置。

① 配置与 MCE 连接的接口地址为 10.214.10.2/24，连接 Site 1 接口的地址为 192.168.0.1/24。向 VLAN 中增加端口和配置接口 IP 地址的配置这里省略。

② 在 VR 1 上配置默认路由，指定出方向报文的下一跳地址为 10.214.10.3。

```
<VR1> system-view
[VR1] ip route-static 0.0.0.0 0.0.0.0 10.214.10.3
```

(2) 在 MCE 上的配置。

① 在 MCE 上指定静态路由，去往 192.168.0.0 网段的报文，下一跳地址为 10.214.10.2，并将此路由与 VPN 1 实例绑定。

```
[MCE-Vlan-interface20] quit
[MCE] ip route-static vpn-instance vpn 1 192.168.0.0 16 10.214.10.2
```

② 显示 MCE 上为 VPN 1 实例维护的路由信息。

```
[MCE] display ip routing-table vpn-instance vpn 1
Routing Tables: vpn 1
         Destinations : 5        Routes : 5
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
127.0.0.0/8         Direct  0    0           127.0.0.1       InLoop 0
127.0.0.1/32        Direct  0    0           127.0.0.1       InLoop 0
10.214.10.0/24      Direct  0    0           10.214.10.3     Vlan 10
10.214.10.3/32      Direct  0    0           127.0.0.1       InLoop 0
192.168.0.0/16      Static  60   0           10.214.10.2     Vlan 10
```

可以看到，MCE 上已经为 Site 1 指定了静态路由。

3) MCE 与 Site 2 之间的路由配置

(1) 在 VR 2 上的配置。在 VR 2 上，配置与 MCE 连接的接口地址为 10.214.20.2/24（配置过程略），配置 RIP，将网段 192.168.10.0 和 10.214.20.0 发布。

```
<VR2> system-view
[VR2] rip 20
[VR2-rip-20] network 192.168.10.0
[VR2-rip-20] network 10.0.0.0
```

(2) 在 MCE 上的配置。

说明：Site 2 内已经运行了 RIP，因此可以在 MCE 上配置 RIP 路由协议，加入 Site 2 的路由运算中，自动更新路由信息。

① 配置 RIP 协议，进程为 20，并与 VPN 2 实例进行绑定。

```
[MCE] rip 20 vpn-instance vpn 2
```

② 将网段 10.214.10.0 发布，关闭路由自动聚合功能，引入 OSPF(进程号 20)的路由信息。

③ 需要注意的是，当 MCE 与 PE 间路由为 RIP 或 IS-IS 时，import-route 命令中参数 ospf 也对应改为 rip 或 isis。

```
[MCE-rip-20] network 10.0.0.0
[MCE-rip-20] undo summary
[MCE-rip-20] import-route ospf
```

④ 在 MCE 上查看 VPN 2 实例的路由信息。

```
[MCE-rip-20] display ip routing-table vpn-instance vpn 2
Routing Tables: vpn 2
         Destinations : 5        Routes : 5
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop 0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop 0
10.214.20.0/24      Direct  0    0         10.214.20.3     Vlan 20
10.214.20.3/32      Direct  0    0         127.0.0.1       InLoop 0
192.168.10.0/24     RIP     100  1         10.214.20.2     Vlan 20
```

可以看到，MCE 已经通过 RIP 学习到了 Site 2 内的私网路由，并与 Site 1 内的192.168.0.0 路由信息分别维护在两个路由表内，有效进行了隔离。

4) MCE 与 Site 3 之间的路由配置

(1) 在 VR 3 上的配置。将 VR 3 与 MCE 设备连接的接口 IP 地址设置为10.214.30.2/24，配置过程省略。在 VR 3 上配置 OSPF 协议，进程为 30，将 192.168.20.0 和 10.214.30.0 网段发布。

```
<VR3> system-view
[VR3] ospf 30
[VR3-ospf-30] area 0
[VR3-ospf-30-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[VR3-ospf-30-area-0.0.0.0] network 10.214.30.0 0.0.0.255
```

(2) 在 MCE 上的配置。

说明：Site 3 内已经运行了 OSPF，因此可以在 MCE 上配置 OSPF 路由协议，加入Site 3 的路由运算中，自动更新路由信息。

① 配置 MCE 的 Loopback 0 接口，用于指定 MCE 的 Router ID，地址为101.101.10.1。配置步骤这里省略。

② 在 MCE 设备上配置 OSPF 30 进程，与 VPN 3 实例绑定，开启 OSPF 多实例功能(当 MCE 上只有一个 OSPF 进程时不需要配制此功能)，发布 10.214.30.0 网段。

③ 需要注意的是，当 MCE 与 PE 间路由为 RIP 或 IS-IS 时，此处 OSPF 配置中不需要开启 OSPF 多实例功能。

```
<MCE> system-view
```

```
[MCE] ospf 30 router id 101.101.10.1 vpn-instance vpn 3
[MCE-ospf-30] vpn-instance-capability simple
[MCE-ospf-30] area 0
[MCE-ospf-30-area-0.0.0.0] network 10.214.30.0 0.0.0.255
```

④ 在 MCE 设备上查看 VPN 3 实例中的路由信息。

```
[MCE-ospf-30-area-0.0.0.0] display ip routing-table vpn-instance vpn 3
Routing Tables: vpn 3
         Destinations : 5        Routes : 5
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
10.214.30.0/24      Direct  0    0         10.214.30.3     Vlan 30
10.214.30.3/32      Direct  0    0         127.0.0.1       InLoop 0
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop 0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop 0
192.168.20.0/24     OSPF    10   2         10.214.30.2     Vlan 30
```

可以看到，MCE 已经通过 OSPF 学习到了 Site 3 内的私网路由。

5）MCE 与 PE 1 间的路由配置

（1）在 MCE 上的配置。

① MCE 使用 GigabitEthernet 1/1/1 端口连接到 PE1 的 GigabitEthernet 1/0/18 端口，需要配置这个端口为 Trunk 端口，并允许 VLAN 10、VLAN 20 和 VLAN 30 的报文携带 Tag 通过。

```
[MCE] interface GigabitEhternet 1/1/1
[MCE-GigabitEhternet1/1/1] port link-type trunk
[MCE-GigabitEhternet1/1/1] port trunk permit vlan 10 20 30
```

② 配置 MCE 启动 OSPF 进程 10，绑定到 VPN 1 实例，域 ID 设置为 10，在 Area 0 区域发布 10.214.10.0 网段，并引入 VPN 1 的静态路由。

```
[MCE-GigabitEhternet1/1/1] quit
[MCE] ospf 10 router-id 101.101.10.1 vpn-instance vpn 1
[MCE-ospf-10] domain-id 10
[MCE-ospf-10] area 0
[MCE-ospf-10-area-0.0.0.0] network 10.214.10.0 0.0.0.255
[MCE-ospf-10-area-0.0.0.0] quit
[MCE-ospf-10] import-route static
[MCE-ospf-10] quit
```

③ 配置 MCE 启动 OSPF 进程 20，绑定到 VPN 2 实例，域 ID 设置为 20，在 Area 0 区域发布 10.214.20.0 网段，并引入 VPN 2 的 RIP 路由。

```
[MCE] ospf 20 router-id 101.101.10.1 vpn-instance vpn 2
[MCE-ospf-20] domain-id 20
[MCE-ospf-20] area 0
[MCE-ospf-20-area-0.0.0.0] network 10.214.20.0 0.0.0.255
[MCE-ospf-20-area-0.0.0.0] quit
[MCE-ospf-20] import-route rip
```

④ 配置 MCE 的 OSPF 进程 30，域 ID 设置为 30，在 Area 0 区域发布 10.214.30.0 网段。

```
[MCE] ospf 30 router-id 101.101.10.1 vpn-instance vpn 3
```

```
[MCE-ospf-30] domain-id 30
[MCE-ospf-30] area 0
[MCE-ospf-30-area-0.0.0.0] network 10.214.30.0 0.0.0.255
[MCE-ospf-30-area-0.0.0.0] quit
```

(2) 在 PE 1 上的配置。

① 配置 PE 1 的 GigabitEthernet 1/0/18 端口允许 VLAN 10、VLAN 20 和 VLAN 30 的报文通过。

```
<PE1> system-view
[PE1] interface GigabitEthernet 1/0/18
[PE1-GigabitEthernet1/0/18] port link-type trunk
[PE1-GigabitEthernet1/0/18] port trunk permit vlan 10 20 30
```

② 配置 PE1 的 Vlan-interface 10、Vlan-interface 20 和 Vlan-interface 30 的接口分别为 10.214.10.4、10.214.20.4 和 10.214.30.4，并分别与 VPN 1、VPN 2 和 VPN 3 实例进行绑定。配置步骤这里省略。

③ 配置 PE 1 的 Loopback 0 接口，用于指定 PE 1 的 Router ID，地址为 100.100.10.1。配置过程这里省略。

④ 配置 PE 1 启动 OSPF 进程 10，绑定到 VPN 1 实例，域 ID 为 10，在 Area 0 区域发布 10.214.10.0 网段。

```
[PE1-GigabitEthernet1/0/18] quit
[PE1] ospf 10 router-id 100.100.10.1 vpn-instance vpn 1
[PE1-ospf-10] domain-id 10
[PE1-ospf-10] area 0
[PE1-ospf-10-area-0.0.0.0] network 10.214.10.0 0.0.0.255
```

⑤ 配置 PE 1 启动 OSPF 进程 20 和进程 30，绑定到 VPN 2 和 VPN 3 实例，域 ID 分别为 20 和 30，并分别在 Area 0 区域发布 10.214.20.0 和 10.214.30.0 网段。配置过程与上文类似，这里不再赘述。

⑥ 显示 PE 上的 VPN 1 路由信息。

```
[PE-ospf-10-area-0.0.0.0] display ip routing-table vpn-instance vpn 1
Routing Tables: vpn 1
         Destinations : 6        Routes : 6
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop 0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop 0
10.214.10.0/24      Direct  0    0         10.214.10.4     Vlan 10
10.214.10.4/32      Direct  0    0         127.0.0.1       InLoop 0
100.100.10.1/32     Direct  0    0         127.0.0.1       InLoop 0
192.168.0.0/16      O_ASE   150  1         10.214.10.2     Vlan 10
```

可以看到，Site 1 内的静态路由已经引入 MCE 与 PE 间的 OSPF 路由表中。

⑦ 显示 PE 上的 VPN 2 路由信息。

```
<PE> display ip routing-table vpn-instance vpn 2
Routing Tables: vpn 2
```

```
        Destinations : 6        Routes : 6
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop 0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop 0
10.214.20.0/24      Direct  0    0         10.214.20.4     Vlan 20
10.214.20.4/32      Direct  0    0         127.0.0.1       InLoop 0
200.200.20.1/32     Direct  0    0         127.0.0.1       InLoop 0
192.168.10.0/24     O_ASE   150  1         10.214.20.2     Vlan 20
```

⑧ 显示 PE 上的 VPN 3 路由信息。

```
<PE> display ip routing-table vpn-instance vpn 3
Routing Tables: vpn 3
        Destinations : 6        Routes : 6
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop 0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop 0
10.214.30.0/24      Direct  0    0         10.214.30.4     Vlan 30
10.214.30.4/32      Direct  0    0         127.0.0.1       InLoop 0
200.200.30.3/32     Direct  0    0         127.0.0.1       InLoop 0
192.168.20.0/24     OSPF    10   1         10.214.30.2     Vlan 30
```

至此，通过配置，已经将 3 个 VPN 站点内的路由信息完整地传播到 PE 中，配置完成。

(3) 当使用 RIP 作为 MCE 到 PE 间路由协议时，配置如下：

① 在 MCE 上的配置。

a. MCE 使用 GigabitEthernet 1/1/1 端口连接到 PE 1 的 GigabitEthernet 1/0/18 端口，需要配置这个端口为 Trunk 端口，并允许 VLAN 10、VLAN 20 和 VLAN 30 的报文携带 Tag 通过。

```
[MCE] interface GigabitEhternet 1/1/1
[MCE-GigabitEhternet1/1/1] port link-type trunk
[MCE-GigabitEhternet1/1/1] port trunk permit vlan 10 20 30
```

b. 配置 MCE 启动 RIP 进程 10，绑定到 VPN 1 实例，发布 10.214.10.0 网段，并引入 VPN 1 的静态路由。

```
[MCE-GigabitEhternet1/1/1] quit
[MCE] rip 10 vpn-instance vpn 1
[MCE-rip-10] network 10.0.0.0
[MCE-rip-10] import-route static
[MCE-rip-10] quit
```

c. 配置 MCE 启动 RIP 进程 20，发布 10.214.20.0 网段。

```
[MCE] rip 20 vpn-instance vpn 2
[MCE-rip-20] network 10.0.0.0
[MCE-rip-20] quit
```

d. 配置 MCE 启动 RIP 进程 30，绑定到 VPN 3 实例，发布 10.214.30.0 网段，并引入 VPN 2 的 OSPF 路由。

```
[MCE] rip 30 vpn-instance vpn 3
[MCE-rip-30] network 10.0.0.0
[MCE-rip-30] import-route ospf
[MCE-rip-30] quit
```

② 在 PE 1 上的配置。

a. 配置 PE 1 的 GigabitEthernet 1/0/18 端口允许 VLAN 10、VLAN 20 和 VLAN 30 的报文通过。

```
<PE1> system-view
[PE1] interface GigabitEthernet 1/0/18
[PE1-GigabitEthernet1/0/18] port link-type trunk
[PE1-GigabitEthernet1/0/18] port trunk permit vlan 10 20 30
[PE1-GigabitEthernet1/0/18] quit
```

b. 配置 PE 1 的 Vlan-interface 10、Vlan-interface 20 和 Vlan-interface 30 的接口分别为 10.214.10.4、10.214.20.4 和 10.214.30.4，并分别与 VPN 1、VPN 2 和 VPN 3 实例进行绑定。配置步骤这里省略。

c. 配置 PE 1 启动 RIP 进程 10，绑定到 VPN 1 实例，域 ID 为 10，发布 10.214.10.0 网段。

```
[PE1] rip 10 vpn-instance vpn 1
[PE1-rip-10] network 10.0.0.0
```

d. 配置 PE 1 启动 RIP 进程 20 和进程 30，绑定到 VPN 2 和 VPN 3 实例，并分别发布 10.214.20.0 和 10.214.30.0 网段。配置过程与上文类似，这里不再赘述。

(4) 当使用 IS-IS 作为 MCE 到 PE 间路由协议时，配置如下：

① 在 MCE 上的配置。

a. MCE 使用 GigabitEthernet 1/1/1 端口连接到 PE 1 的 GigabitEthernet 1/0/18 端口，需要配置这个端口为 Trunk 端口，并允许 VLAN 10、VLAN 20 和 VLAN 30 的报文携带 Tag 通过。

```
[MCE] interface GigabitEhternet 1/1/1
[MCE-GigabitEhternet1/1/1] port link-type trunk
[MCE-GigabitEhternet1/1/1] port trunk permit vlan 10 20 30
[MCE-GigabitEhternet1/1/1] quit
```

b. 配置 MCE 启动 IS-IS 进程 10，绑定到 VPN 1 实例；网络实体名称为 10.0000.0000.0001.00；路由类型为 level-1-2。同时在 Vlan-interface 10 接口上使能 IS-IS 进程 10，并引入 VPN 1 的静态路由。

```
[MCE] isis 10 vpn-instance vpn 1
[MCE-isis-10] network-entity 10.0000.0000.0001.00
[MCE-isis-10] is-level level-1-2
[MCE-isis-10] import-route static level-1-2
[MCE-isis-10] quit
[MCE] interface Vlan-interface 10
[MCE-vpn-instance-vpn10] isis enable 10
[MCE-vpn-instance-vpn10] quit
```

c. 配置 MCE 启动 IS-IS 进程 20，绑定到 VPN 2 实例；网络实体名称为 10.0000.0000.0002.00；路由类型为 level-1-2。同时在 Vlan-interface 20 接口上使能 IS-IS 进程 20，并引入 VPN 2 的 RIP 路由。

```
[MCE] isis 20 vpn-instance vpn 2
[MCE-isis-20] network-entity 10.0000.0000.0002.00
[MCE-isis-20] is-level level-1-2
[MCE-isis-20] import-route rip level-1-2
[MCE-isis-20] quit
[MCE] interface Vlan-interface 20
[MCE-vpn-instance-vpn20] isis enable 20
[MCE-vpn-instance-vpn20] quit
```

d. 配置 MCE 启动 IS-IS 进程 30，绑定到 VPN 3 实例；网络实体名称为 10.0000.0000.0003.00；路由类型为 level-1-2。同时在 Vlan-interface 30 接口上使能 IS-IS 进程 30，并引入 VPN 3 的 OSPF 路由。

```
[MCE] isis 30 vpn-instance vpn 3
[MCE-isis-30] network-entity 10.0000.0000.0003.00
[MCE-isis-30] is-level level-1-2
[MCE-isis-30] import-route ospf level-1-2
[MCE-isis-30] quit
[MCE] interface Vlan-interface 30
[MCE-vpn-instance-vpn30] isis enable 30
[MCE-vpn-instance-vpn30] quit
```

② 在 PE 1 上的配置。

a. 配置 PE 1 的 GigabitEthernet 1/0/18 端口允许 VLAN 10、VLAN 20 和 VLAN 30 的报文通过。

```
<PE1> system-view
[PE1] interface GigabitEthernet 1/0/18
[PE1-GigabitEthernet1/0/18] port link-type trunk
[PE1-GigabitEthernet1/0/18] port trunk permit vlan 10 20 30
[PE1-GigabitEthernet1/0/18] quit
```

b. 配置 PE 1 的 Vlan-interface 10、Vlan-interface 20 和 Vlan-interface 30 的接口分别为 10.214.10.4、10.214.20.4 和 10.214.30.4，并分别与 VPN 1、VPN 2 和 VPN 3 实例进行绑定。配置步骤这里省略。

c. 配置 PE 1 启动 IS-IS 进程 10，绑定到 VPN 1 实例；网络实体名称为 10.0000.0000.0004.00；路由类型为 level-1-2。同时在 Vlan-interface 10 接口上使能 IS-IS 进程 10。

```
[PE1] isis 10 vpn-instance vpn 1
[PE1-isis-30] network-entity 10.0000.0000.0004.00
[PE1-isis-30] is-level level-1-2
[PE1-isis-30] quit
[PE1] interface Vlan-interface 10
[PE1-Vlan-interface10] isis enable 10
[PE1-Vlan-interface10] quit
```

d. 配置 PE 1 启动 IS-IS 进程 20 和进程 30，绑定到 VPN 2 和 VPN 3 实例，网络实体名称分别为 10.0000.0000.0005.00 和 10.0000.0000.0006.00，并分别在 Vlan-interface 20 和 Vlan-interface 30 使能 IS-IS 进程 20 和 IS-IS 进程 30。配置过程与上文类似，这里不再赘述。

提示：此处仅列出 MCE 设备上的完整配置，组网中其他设备的配置可参见该产品的用户手册。

15.2.2 使用 BGP 引入 VPN 路由的 MCE 典型配置指导

1. 背景

M 集团采购了一批网络设备，准备依托 T 电信公司 MPLS 骨干网及其提供的 BGP/MPLS VPN 服务，构建公司内部网络。M 集团将其内部网络根据业务部门划分为两个 VPN，某些分公司必须同时支持这两类业务，即必须同时属于这两个 VPN。为了减少网络设备的投入，M 公司在一些分公司采用具有 MCE 功能的交换机，在 BGP/MPLS VPN 组网应用中承担多个 VPN 实例的 CE 功能。

因私网规模较大，M 公司的私网路由器配置了 BGP，因而需使用 BGP 引入 VPN 路由。

2. 组网图

图 15-5 所示为使用 BGP 引入 VPN 路由的 MCE 典型配置组网图。

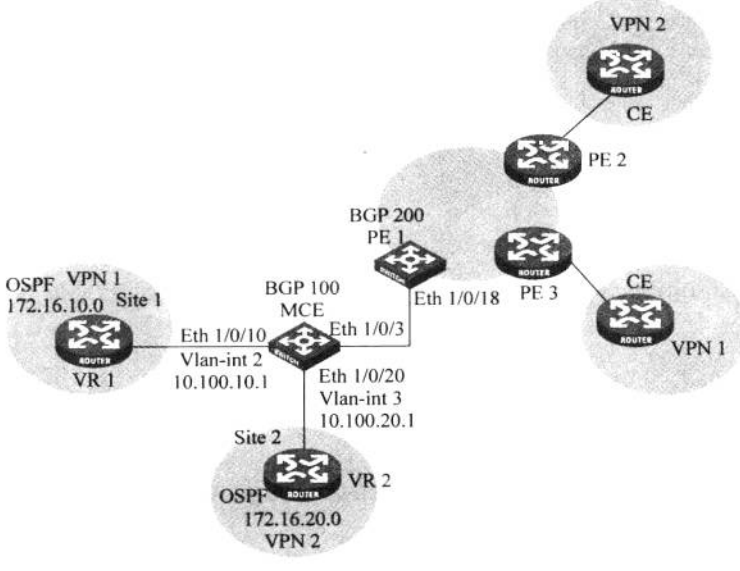


图 15-5 使用 BGP 引入 VPN 路由的 MCE 典型配置组网图

3. 配置需求

如图 15-5 所示，设备 VR 1、VR 2 和 MCE 均位于同一分公司内，该分公司因业务部署需要配置 2 个 VPN，但由于投资限制，只能配置一台交换机作为 CE，所以此交换机必须配置 MCE。

(1) 使用 H3C 设备作为 MCE 设备，将 Site 1 和 Site 2 内的 VPN 路由发布到 PE 设备，使穿过 MPLS 骨干网络的同一 VPN 内的设备间能够正常通信。

(2) Site 1 和 Site 2 内部均使用 OSPF 协议，MCE 与 PE 间使用 EBGP 协议。

4. 配置过程和解释

(1) 配置 MCE 上的 VPN 实例并与接口进行绑定。

① 切换 MCE 设备的工作模式为 MCE 模式，并重新启动设备。

```
<MCE> system-view
[MCE] switch-mode mce
[MCE] quit
<MCE> reboot
```

说明：在配置 S7500E 系列交换机的 MCE 功能时，不需要配置 switch-mode mce 命令和重启设备。

② 在 MCE 设备上配置 VPN 实例，名称分别为 VPN 1 和 VPN 2，RD 分别取值为10：1、20：1，VPN Target 取值与 RD 取值相同，Export 和 Import 均取此值。

```
<MCE> system-view
[MCE] ip vpn-instance vpn 1
[MCE-vpn-instance-vpn1] route-distinguisher 10:1
[MCE-vpn-instance-vpn1] vpn-target 10:1 both
[MCE-vpn-instance-vpn1] quit
[MCE] ip vpn-instance vpn 2
[MCE-vpn-instance-vpn2] route-distinguisher 20:1
[MCE-vpn-instance-vpn2] vpn-target 20:1 both
[MCE-vpn-instance-vpn2] quit
```

③ 创建 VLAN 2，将端口 Eth 1/0/10 加入 VLAN 2，并创建 Vlan-interface 2 接口。

```
[MCE] vlan 2
[MCE-vlan2] port Ethernet 1/0/10
[MCE-vlan2] quit
[MCE] interface Vlan-interface 2
```

④ 配置 Vlan-interface 2 接口与 VPN 1 实例进行绑定，并配置 IP 地址为10.100.10.1，掩码为 24 位。

```
[MCE-Vlan-interface2] ip binding vpn-instance vpn 1
[MCE-Vlan-interface2] ip address 10.100.10.1 24
[MCE-Vlan-interface2] quit
```

⑤ 使用类似步骤配置 VLAN 3，将端口 Eth 1/0/20 加入 VLAN 3，配置接口与 VPN 2 实例绑定并配置 IP 地址。

```
[MCE] vlan 3
[MCE-vlan3] port Ethernet 1/0/20
[MCE-vlan3] quit
[MCE] interface Vlan-interface 3
[MCE-Vlan-interface3] ip binding vpn-instance vpn 2
[MCE-Vlan-interface3] ip address 10.100.20.1 24
[MCE-Vlan-interface3] quit
```

(2) MCE 与 Site 1 之间的路由配置。

① 在 VR 1 上的配置。启动 OSPF 进程 10，将网段 172.16.10.0 和 10.100.10.0

发布。

```
<VR1> system-view
[VR1] ospf 10
[VR1-ospf-10] area 0
[VR1-ospf-10-area-0.0.0.0] network 10.100.10.0 0.0.0.255
[VR1-ospf-10-area-0.0.0.0] network 172.16.10.0 0.0.0.255
```

② 在 MCE 上的配置。

a. 配置 MCE 的 OSPF 协议，进程 10 与 VPN 1 实例绑定，Router ID 为 10.10.10.1，引入 VPN 1 中的 BGP 路由信息，开启 OSPF 多实例功能，并将网段 10.100.10.0 发布。

```
<MCE> system-view
[MCE] ospf 10 router-id 10.10.10.1 vpn-instance vpn 1
[MCE-ospf-10] vpn-instance capability simple
[MCE-ospf-10] import-route bgp
[MCE-ospf-10] area 0
[MCE-ospf-10-area-0.0.0.0] network 10.100.10.0 0.0.0.255
```

b. 显示 VPN 1 实例的路由信息。

```
[MCE-ospf-10-area-0.0.0.0] display ip routing-table vpn-instance vpn 1
Routing Tables: vpn 1
         Destinations : 5        Routes : 5
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop 0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop 0
10.100.10.0/24      Direct  0    0         10.100.10.1     Vlan 2
10.100.10.1/32      Direct  0    0         127.0.0.1       InLoop 0
172.16.10.0/24      OSPF    10   1         10.100.10.2     Vlan 2
```

可以看到，MCE 已经通过 OSPF 进程 10 学习到了 Site 1 内的路由。

(3) MCE 与 Site 2 之间的路由配置。

① 在 VR 2 上的配置。启动 OSPF 进程 20，将网段 172.16.20.0 和 10.100.20.0 发布。

```
<VR2> system-view
[VR2] ospf 20
[VR2-ospf-20] area 0
[VR2-ospf-20-area-0.0.0.0] network 10.100.20.0 0.0.0.255
[VR2-ospf-20-area-0.0.0.0] network 172.16.20.0 0.0.0.255
```

② 在 MCE 上的配置。

a. 配置 MCE 的 OSPF 协议，进程 20 与 VPN 2 实例绑定，Router ID 为 10.10.10.1，引入 VPN 2 中的 BGP 路由信息，开启 OSPF 多实例功能，并将网段 10.100.20.0 发布。

```
<MCE> system-view
[MCE] ospf 20 router-id 10.10.10.1  vpn-instance vpn 2
[MCE-ospf-20] vpn-instance capability simple
[MCE-ospf-20] import-route bgp
[MCE-ospf-20] area 0
```

```
[MCE-ospf-20-area-0.0.0.0] network 10.100.20.0 0.0.0.255
```

b. 显示 VPN 2 实例的路由信息。

```
[MCE] display ip routing-table vpn-instance vpn 2
Routing Tables: vpn 2
         Destinations : 5        Routes : 5
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop 0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop 0
10.100.20.0/24      Direct  0    0         10.100.20.1     Vlan 3
10.100.20.1/32      Direct  0    0         127.0.0.1       InLoop 0
172.16.20.0/24      OSPF    10   1         10.100.20.2     Vlan 3
```

(4) MCE 与 PE 1 之间的路由配置。

① 在 MCE 上的配置。

a. MCE 使用 Ethernet 1/0/3 端口连接到 PE 1 的 Ethernet 1/0/18 端口，需要配置这个端口为 Trunk 端口，并允许 VLAN 2 和 VLAN 3 的报文携带 Tag 通过。

```
[MCE] interface Ehternet 1/0/3
[MCE-Ethernet1/0/3] port link-type trunk
[MCE-Ethernet1/0/3] port trunk permit vlan 2 3
```

b. 配置 MCE 启动 BGP 进程 100。

```
[MCE] bgp 100
[MCE-bgp]
```

c. 进入 VPN 1 实例的 IPv4 地址族视图。

```
[MCE-bgp] ipv4-family vpn-instance vpn 1
[MCE-bgp-vpn1]
```

d. 指定 PE 1(假设与 VPN 1 绑定的接口地址为 10.100.10.3，BGP 进程为 200)为 EBGP 对等体，并引入 OSPF 进程 10 的路由信息。

```
[MCE-bgp-vpn1] peer 10.100.10.3 as-number 200
[MCE-bgp-vpn1] import-route ospf 10
[MCE-bgp-vpn1] quit
```

e. 进入 VPN 2 实例的 IPv4 地址族视图，指定 PE 1(假设与 VPN 2 绑定的接口地址为 10.100.20.3，BGP 进程为 200)为 EBGP 对等体，并引入 OSPF 进程 20 的路由信息。

```
[MCE-bgp] ipv4-family vpn-instance vpn 2
[MCE-bgp-vpn2] peer 10.100.20.3 as-number 200
[MCE-bgp-vpn2] import-route ospf 20
```

② 在 PE 1 上的配置。

a. 配置 PE 1 的 Ethernet 1/0/18 端口允许 VLAN 2 和 VLAN 3 的报文通过。

```
<PE1> system-view
[PE1] interface Ethernet 1/0/18
```

```
[PE1-Ethernet1/0/18] port link-type trunk
[PE1-Ethernet1/0/18] port trunk permit vlan 2 3
```

b. 配置 PE 1 的 Vlan-interface 2 和 Vlan-interface 3 接口的 IP 地址分别为10.100.10.3 和 10.100.20.3，并分别与 VPN 1 和 VPN 2 实例进行绑定。配置步骤这里省略。

c. 在 PE 1 上配置 BGP 200，并在两个 VPN 实例的 IPv4 地址族视图中分别指定 MCE 为 EBGP 对等体。

```
[PE1] bgp 200
[PE1-bgp] ipv4-family vpn-instance vpn 1
[PE1-bgp-vpn1] peer 10.100.10.1 as-number 100
[PE1-bgp-vpn1] quit
[PE1-bgp] ipv4-family vpn-instance vpn 2
[PE1-bgp-vpn2] peer 10.100.20.1 as-number 100
[PE1-bgp-vpn2] return
```

d. 显示 PE 1 上 VPN 1 实例的路由信息。

```
<PE1> display ip routing-table vpn-instance vpn 1
Routing Tables: vpn 1
         Destinations : 5        Routes : 5
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop 0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop 0
10.100.10.0/24      Direct  0    0         10.100.10.3     Vlan 2
10.100.10.3/32      Direct  0    0         127.0.0.1       InLoop 0
172.16.10.0/24      BGP     255  2         10.100.10.2     Vlan 2
```

e. 显示 PE 1 上 VPN 2 实例的路由信息。

```
<PE1> display ip routing-table vpn-instance vpn 2
Routing Tables: vpn 2
         Destinations : 5        Routes : 5
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop 0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop 0
10.100.20.0/24      Direct  0    0         10.100.20.3     Vlan 3
10.100.20.3/32      Direct  0    0         127.0.0.1       InLoop 0
172.16.20.0/24      BGP     255  2         10.100.20.2     Vlan 3
```

至此，MCE 设备已经将两个 VPN 实例内的 OSPF 路由全部引入 PE 的 EBGP 路由表中，配置完成。

提示：在 MCE 上为指定 VPN 实例配置的 VPN Target 必须与 PE 上为该 VPN 实例配置的 VPN Target 值一致。

第16章

EPON-OLT配置指导

EPON(Ethernet Passive Optical Network,以太网无源光网络)用于承载封装成802.3标准的以太网帧的PON(Passive Optical Network,无源光网络)。一个典型的EPON系统主要由OLT(Optical Line Terminal,光线路终端)、ONU(Optical Network Unit,光网络单元)和ODN(Optical Distribution Network,光分配网络)3部分组成。

以太网交换机充当EPON系统的OLT设备时,EPON系统有3种端口类型:OLT端口、ONU端口和UNI端口。

交换机的EPON业务板上的每个PON端口即是一台独立的OLT设备。OLT端口编号采用业务板槽位编号/子板槽位编号/OLT端口编号。

16.1 OLT端口隔离典型配置指导

1. 背景

某新建小区需要布设一个接入网,为小区用户提供宽带服务。某运营商在综合考虑了用户带宽需求、网络性能和可靠性、环保节能等因素之后,决定在这个小区中部署EPON网络。

为了小区接入用户的安全,要求各接入用户彼此之间不能通过二层进行访问。

2. 组网图

图16-1所示为OLT端口隔离典型配置组网图。

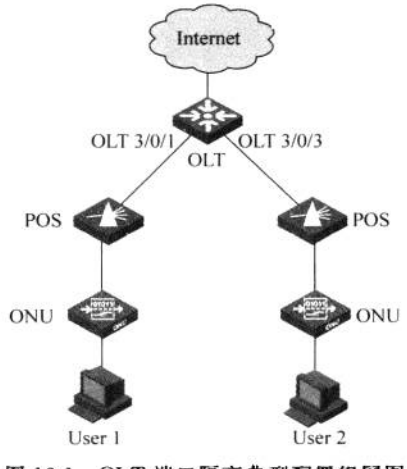


图16-1 OLT端口隔离典型配置组网图

3. 配置需求

(1) OLT 设备通过上行口与外部网络相连。

(2) 将端口 OLT 3/0/1 和 OLT 3/0/2 进行端口隔离，使其中两个 OLT 端口下的用户彼此之间二层报文不能互通，但可以和外部网络通信。

4. 配置过程和解释

(1) 将端口 OLT 3/0/1 和 OLT 3/0/2 加入隔离组。

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] port-isolate enable
[Sysname-Olt3/0/1] quit
[Sysname] interface olt 3/0/2
[Sysname-Olt3/0/2] port-isolate enable
[Sysname-Olt3/0/2] quit
```

(2) 显示隔离组中的信息。

```
<Sysname> display port-isolate group
  Port-isolate group information:
  Uplink port support: NO
  Group ID: 1
    olt 3/0/1       olt 3/0/2
```

16.2 光纤备份典型配置指导

1. 背景

小区中有一部分高端用户，为了保证这部分用户网络的稳定性，需要对光纤链路进行备份。

2. 组网图

图 16-2 所示为光纤备份典型配置组网图。

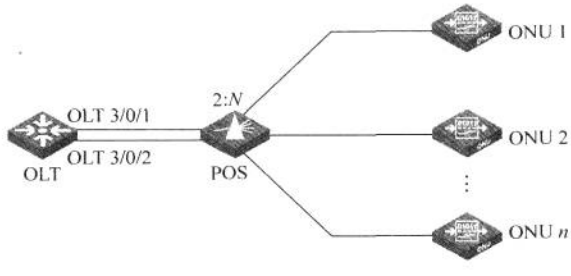


图 16-2 光纤备份典型配置组网图

3. 配置需求

(1) 交换机作为 OLT 设备，通过两条光纤连接到一个 POS(Passive Optical Splitter，无源光纤分支器)设备，POS 连接下面多个 ONU 设备。

(2) 为提高服务可靠性，需要在交换机上配置光纤备份功能，将两个接有光纤的 OLT

端口配置为一个光纤备份组，在某一条光纤出现故障时，交换机可以自动将业务切换至备份光纤上。在日常维护中，用户可以将业务手动切换到备份光纤，以便进行主用光纤的维护和检修。

4. 配置过程和解释

(1) 光纤备份组的配置。

① 在进行光纤备份配置前，首先完成 EPON OLT 和 ONU 连接的基本配置，保证 ONU 设备的正常注册和所有光纤的正常工作，具体配置可参见交换机的操作手册。

② 创建光纤备份组 1。

```
<Sysname> system-view
[Sysname] ftth
[Sysname-ftth] fiber-backup group 1
 Create group 1 successfully.
```

③ 将 OLT 3/0/1 端口和 OLT 3/0/2 端口加入该光纤备份组，使 OLT 3/0/1 端口为主用端口，OLT 3/0/2 端口为备用端口。

```
[Sysname-fiber-group1] group member olt 3/0/1
[Sysname-fiber-group1] group member olt 3/0/2
[Sysname-fiber-group1]
%Nov 23 12:53:02:491 2007 H3C IFNET/4/LINK UPDOWN:
  Olt3/0/2: link status is DOWN
%Nov 23 12:53:02:882 2007 H3C IFNET/4/LINK UPDOWN:
  Olt3/0/1: link status is UP
```

④ 查看光纤备份组端口状态。

```
[Sysname-fiber-group1] display fiber-backup group 1
 fiber backup group 1 information:
 Member          Role          State
 ----------------------------------------
 Olt 3/0/1       MASTER        ACTIVE
 Olt 3/0/2       SLAVE         READY
```

(2) 光纤备份组自动切换。

① 当 OLT 3/0/1 端口出现故障或其所连接的光纤无法正常通信时，设备可以自动将 OLT 3/0/2 端口切换为主用端口，同时将流量切换到该端口进行传输。

```
[Sysname-fiber-group1]
#Nov 23 12:57:23:907 2007 H3C EPON/1/TRAP_EPON_OLTSWITCH:
  Trap 1.3.6.1.4.1.25506.2.42.1.8.0.28<hh3cEponOltSwitchoverTrap>: An OLT switchover
trap has been detected,
  Master interface index is 29556737,
  Master interface description is Olt 3/0/2 Interface
  Slave interface index is 29556738,
  Slave interface description is Olt 3/0/1 Interface
  Reason is "olt shutdown"
%Nov 23 12:57:24:61 2007 H3C IFNET/4/LINK UPDOWN:
  Olt 3/0/1: link status is DOWN
```

```
%Nov 23 12:57:24:452 2007 H3C IFNET/4/LINK UPDOWN:
  Olt 3/0/2: link status is UP
```

② 显示切换后的主备端口状态。

```
[Sysname-fiber-group1] display fiber-backup group 1
 fiber backup group 1 information:
 Member          Role          State
 ----------------------------------------
 Olt 3/0/2       MASTER        ACTIVE
 Olt 3/0/1       SLAVE         DOWN
```

可以看到，OLT 3/0/2 端口已经成为主用端口，并处于 ACTIVE 状态；OLT 3/0/1 端口成为备用端口，处于 DOWN 状态。

(3) 光纤备份组手动切换。

① 在两条光纤均正常工作的情况下(即 OLT 3/0/1 端口为主用端口，处于 ACTIVE 状态；OLT 3/0/2 为备用端口，处于 READY 状态)，用户如果需要对 OLT 3/0/1 端口所连接的光纤进行维护和检修，可以手动将 OLT 3/0/1 端口和 OLT 3/0/2 端口进行主备切换，使业务流量通过 OLT 3/0/2 端口进行传输。

```
[Sysname-fiber-group1] port switch-over
[Sysname-fiber-group1]
#Nov 23 12:54:53:307 2007 H3C EPON/1/TRAP_EPON_OLTSWITCH:
  Trap 1.3.6.1.4.1.25506.2.42.1.8.0.28<hh3cEponOltSwitchoverTrap>: An OLT switchover
trap has been detected,
   Master interface index is 29556738,
   Master interface description is Olt 3/0/2 Interface
   Slave interface index is 29556737,
   Slave interface description is Olt 3/0/1 Interface
   Reason is "manual switch"
%Nov 23 12:54:53:537 2007 H3C IFNET/4/LINK UPDOWN:
  Olt 3/0/1: link status is DOWN
%Nov 23 12:54:53:927 2007 H3C IFNET/4/LINK UPDOWN:
  Olt 3/0/2: link status is UP
```

② 切换完成后，查看备份组的端口状态。

```
[Sysname-fiber-group1] display fiber-backup group 1
 fiber backup group 1 information:
 Member          Role          State
 ----------------------------------------
 Olt 3/0/2       MASTER        ACTIVE
 Olt 3/0/1       SLAVE         READY
```

可以看到，OLT 3/0/2 端口已经成为主用端口，并处于 ACTIVE 状态；OLT 3/0/1 端口成为备用端口，处于 READY 状态。

③ 如果关闭 OLT 3/0/2 端口，则 OLT 3/0/1 端口将再次成为主用端口。

```
[Sysname-fiber-group1] quit
[Sysname] interface olt 3/0/2
```

```
[Sysname-Olt3/0/2] shutdown
[Sysname-Olt3/0/2]
#Nov 23 12:57:23:907 2007 H3C EPON/1/TRAP_EPON_OLTSWITCH:
 Trap 1.3.6.1.4.1.25506.2.42.1.8.0.28<hh3cEponOltSwitchoverTrap>: An OLT switcho
ver trap has been detected,
  Master interface index is 29556737,
  Master interface description is Olt3/0/1 Interface
  Slave interface index is 29556738,
  Slave interface description is Olt3/0/2 Interface
  Reason is "olt shutdown"
%Nov 23 12:57:24:61 2007 H3C IFNET/4/LINK UPDOWN:
 Olt 3/0/2: link status is DOWN
%Nov 23 12:57:24:452 2007 H3C IFNET/4/LINK UPDOWN:
 Olt 3/0/1: link status is UP
[Sysname-Olt3/0/2] display fiber-backup group 1
 fiber backup group 1 information:
 Member          Role            State
 ----------------------------------------
 Olt 3/0/1       MASTER          ACTIVE
 Olt 3/0/2       SLAVE           DOWN
```

提示：先加入的端口为主用端口，后加入的端口为备用端口。

16.3 IP Source Guard 绑定配置指导

1. 背景

为了防止非法主机仿冒合法用户 IP 接入网络，提高网络的安全性，需要在交换机上启用 IP Source Guard 的功能。

2. 组网图

图 16-3 所示为 IP Source Guard 绑定配置组网图。

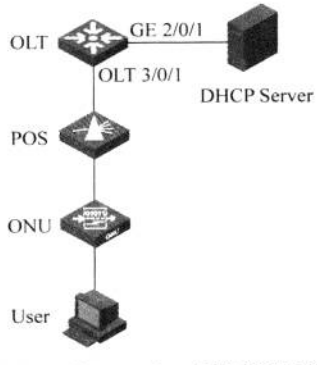


图 16-3 IP Source Guard 绑定配置组网图

3. 配置需求

(1) OLT 通过端口 GigabitEthernet 2/0/1 与 DHCP Server 相连，通过端口 OLT 3/0/1 和分光器下接一个 ONU，最后，ONU 的 UNI 1 下接一台用户。

(2) 在 OLT 上开启 DHCP Snooping 功能。

(3) 将 ONU(MAC 地址为 000f-e200-0001)与 ONU 端口 ONU 3/0/1:1 进行绑定。

(4) 用户(MAC 地址为 00-01-02-03-04-06)通过 DHCP Server 获取 IP 地址,则在 OLT 上生成 User 的 DHCP Snooping 表项。

(5) 在端口 OLT 3/0/1 上启用 IP 过滤功能,防止客户端使用伪造的不同源 IP 地址对服务器进行攻击。

4. 配置过程和解释

(1) 配置 OLT。

① 开启 DHCP Snooping 功能。

```
<Sysname> system-view
[Sysname] dhcp-snooping
```

② 配置与 DHCP 服务器相连的端口 GigabitEthernet 2/0/1 为信任端口。

```
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] dhcp-snooping trust
[Sysname-GigabitEthernet2/0/1] quit
```

③ 配置端口 OLT 3/0/1 的端口过滤功能。

```
[Sysname] interface Olt 3/0/1
[Sysname-Olt3/0/1] ip check source ip-address mac-address
```

④ 创建 ONU 端口 ONU 3/0/1:1,并将 ONU 与端口 ONU 3/0/1:1 进行绑定。

```
[Sysname-Olt3/0/1] using onu 1
[Sysname-Olt3/0/1] quit
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] bind onuid 000f-e200-0001
```

(2) 验证结果。

① 当用户从 DHCP 服务器成功获取 IP 地址后,可以在 OLT 设备上显示端口 OLT 3/0/1从 DHCP Snooping 获取的动态表项。

```
<Sysname> display ip check source interface olt 3/0/1
The Following User address bind have been configured:
 Mac                IP            Vlan    Port          Status
0001-0203-0406      192.168.0.1   1       Olt 3/0/1     DHCP-SNP
```

② 显示 DHCP Snooping 已有的动态表项,查看其是否和端口 OLT 3/0/1 获取的动态表项一致。

```
<Sysname> display dhcp-snooping
DHCP Snooping is enabled.
The client binding table for all untrusted ports.
Type : D--Dynamic , S--Static
Type    IP Address     MAC Address      Lease      VLAN  Interface
====    ========== ============== ========== ====  ========
D       192.168.0.1    0001-0203-0406   86335      1     Onu 3/0/1:1
```

从以上显示信息可以看出，端口 OLT 3/0/1 在配置 IP Source Guard 功能之后获取了 DHCP Snooping 产生的动态表项。

16.4 ONU 端口绑定典型配置指导

1. 背景

小区采用的是光纤到户的方案，即每家用户配置一个 ONU 设备。

交换机的每个 OLT 端口下都对应有 64 个逻辑的 ONU 端口。ONU 端口并非实际存在的物理端口，仅当将 ONU 设备绑定到指定 ONU 端口后，该 ONU 端口才具有实际意义，进入 ONU 端口视图下所进行的配置都是针对对应 ONU 设备的配置。ONU 端口编号采用业务板槽位编号/子板槽位编号/OLT 端口编号:ONU 端口编号。

2. 组网图

图 16-4 所示为 ONU 端口绑定典型配置组网图。

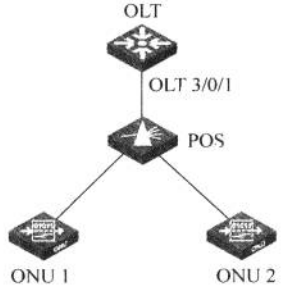


图 16-4 ONU 端口绑定典型配置组网图

3. 配置需求

将 ONU 1(MAC 地址为 000f-e200-0031)和 ONU 2(MAC 地址为 000f-e200-3749)分别与 ONU 3/0/1:1 端口和 ONU 3/0/1:2 端口进行绑定。

4. 配置过程和解释

(1) 创建 ONU 端口 ONU 3/0/1:1 和 ONU 3/0/1:2，并将 ONU 1 与端口 ONU 3/0/1:1进行绑定，ONU 2 与端口 ONU 3/0/1:2 进行绑定。

```
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] using onu 1 to 2
[Sysname-Olt3/0/1] quit
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] bind onuid 000f-e200-0031
[Sysname-Onu3/0/1:1] quit
[Sysname] interface onu 3/0/1:2
[Sysname-Onu3/0/1:2] bind onuid 000f-e200-3749
```

(2) 当该两 ONU 上电后，显示其绑定结果及状态信息。

```
<Sysname> display onuinfo interface Olt 3/0/1
  ONU Mac Address  LLID Dist(M)   Port         Board/Ver     Sft/Epm   State  Aging
  000f-e200-0031   1    <50       Onu3/0/1:1   ET704-A-L/B   110/100   Up     N/A
```

```
000f-e200-3749      2       <50       Onu 3/0/1:2  ET704-A-L/B  110/100    Up     N/A
---  2 entries found  ---
```

注意：一个 ONU 端口上只能绑定一台 ONU，且一台 ONU 也只能绑定到一个 OLT 下的一个 ONU 端口，即在一个 OLT 端口下，ONU 端口和 ONU 设备是一一对应的关系。

在光纤备份情况下，一台 ONU 可以绑定到互为备份的两个 OLT 端口下的两个 ONU 端口。

16.5 ONU 的 RSTP 典型配置指导

1. 背景

小区的用户可能会在家中使用多台电脑，或者接入 SOHO 交换机。这样，就有可能误将两个 UNI 端口连在一起，形成环路。为了防止环路，需要在 ONU 上配置 RSTP。

2. 组网图

图 16-5 所示为 ONU 的 RSTP 典型配置组网示意图。

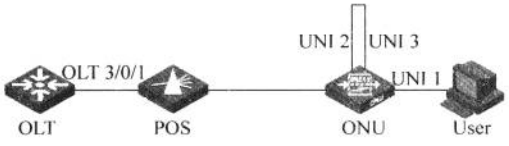


图 16-5 ONU 的 RSTP 典型配置组网示意图

3. 配置需求

(1) UNI 端口 1 连接一个用户，如果误将 UNI 端口 2 和 UNI 端口 3 互连，且 ONU 的 RSTP 功能处于关闭状态，那么当用户访问一个自己 PC 的 ARP 表项中不存在的 IP 地址时，UNI 端口 2 和 UNI 端口 3 之间会产生广播风暴。

(2) 开启 ONU 的 RSTP 功能后，则可以抑制该现象的产生。

4. 配置过程和解释

开启 ONU 的 RSTP 功能后，可抑制 UNI 端口 2 和 UNI 端口 3 之间广播风暴的产生。

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] onu-protocol stp enable
```

注意：在交换机全局开启 STP 功能的情况下，所有 ONU 都必须开启 STP 功能，且 ONU 不能作为 STP 根桥，以免网络出现异常。

16.6 IGMP Snooping 模式下的组播典型配置指导

1. 背景

运营商除了给用户提供网络服务之外，还提供一些视频点播服务，需要在网络中启用组播 VLAN 来支持这些业务。

2. 组网图

图 16-6 所示为 IGMP Snooping 模式下的组播典型配置组网图。

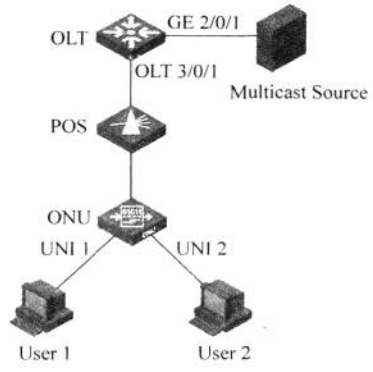


图 16-6 IGMP Snooping 模式下的组播典型配置组网图

3. 配置需求

(1) 交换机的 GigabitEthernet 2/0/1 与组播源相连，通过端口 OLT 3/0/1 和分光器下接一台 ONU(该 ONU 已与 ONU 3/0/1：1 端口绑定)，UNI 端口 1 和 UNI 端口 2 下分别接有 User 1 和 User 2。

(2) 现要求 User 1 可点播 225.1.2.1～225.1.2.255 之间的频道，User 2 可点播 225.1.3.1～225.1.3.255 之间的频道。

4. 配置过程和解释

(1) 配置组播 IP 地址与组播 VLAN 的对应关系。

```
<Sysname> system-view
[Sysname] ftth
[Sysname-ftth] multicast vlan-id 1002 dest-ip 225.1.2.1 to 225.1.2.255
[Sysname-ftth] multicast vlan-id 1003 dest-ip 225.1.3.1 to 225.1.3.255
[Sysname-ftth] quit
```

(2) 全局开启 IGMP Snooping 功能。

```
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
```

(3) 在 VLAN 1002 和 VLAN 1003 内启动 IGMP Snooping 功能。

```
[Sysname] vlan 1002
[Sysname-vlan1002] igmp-snooping enable
[Sysname-vlan1002] quit
[Sysname] vlan 1003
[Sysname-vlan1003] igmp-snooping enable
[Sysname-vlan1003] quit
```

(4) 配置 ONU 的组播模式为 IGMP Snooping 模式。

```
[Sysname] interface Onu 3/0/1:1
```

```
[Sysname-Onu3/0/1:1] multicast-mode igmp-snooping
```

(5) 将 ONU 的 UNI 1 端口和 UNI 2 端口各加入组播 VLAN 1002 和 VLAN 1003，并配置 ONU 为 Trunk 类型(配置成 Trunk 类型后将允许所有 VLAN 的报文通过)。

```
[Sysname-Onu3/0/1:1] uni 1 multicast vlan 1002
[Sysname-Onu3/0/1:1] uni 2 multicast vlan 1003
[Sysname-Onu3/0/1:1] port link-type trunk
```

(6) 开启 UNI 1 和 UNI 2 端口删除下行组播流 VLAN Tag 功能。

```
[Sysname-Onu3/0/1:1] uni 1 multicast-strip-tag enable
[Sysname-Onu3/0/1:1] uni 2 multicast-strip-tag enable
[Sysname-Onu3/0/1:1] quit
```

(7) 配置端口 OLT 3/0/1 为 Hybrid 类型，允许 VLAN 1002 和 VLAN 1003 的报文通过，且发送 VLAN 1002 和 VLAN 1003 的报文时携带 Tag。

```
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] port link-type hybrid
[Sysname-Olt3/0/1] port hybrid vlan 1002 1003 tagged
```

(8) 配置端口 GigabitEthernet 2/0/1 为 Trunk 类型，并允许 VLAN 1002 和 VLAN 1003 的报文通过。

```
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] port link-type trunk
[Sysname-GigabitEthernet2/0/1] port trunk permit vlan 1002 1003
```

注意：一个组播 IP 地址只能属于一个组播 VLAN。

16.7 可控组播配置指导

1. 背景

运营商给小区的用户提供了多种视频节目套餐，订阅不同套餐的用户享受的访问权限是不一样的，因此，需要在设备上进行相关配置。

2. 组网图

图 16-7 所示为可控组播配置组网图。

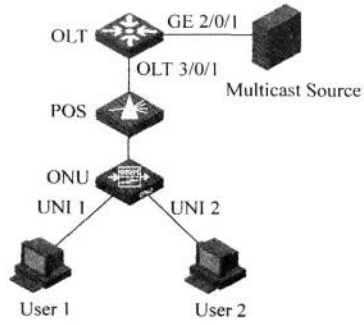


图 16-7 可控组播配置组网图

3. 配置需求

交换机的 GigabitEthernet 2/0/1 与组播源相连，并通过端口 OLT 3/0/1 和分光器下接一台 ONU(该 ONU 已与 ONU 3/0/1：1 端口绑定)；最后，UNI 端口 1 和 UNI 端口 2 下分别接有 User 1 和 User 2。

通过配置组播控制，使得 User 1 和 User 2 对频道 1(225.1.1.1)和频道 2(225.1.2.1)拥有不同的访问权限。

(1) User 1：允许观看频道 1，且仅对频道 2 拥有 60s 的预览。

(2) User 2：不允许观看频道 1，但可以观看频道 2。

4. 配置过程和解释

(1) 配置组播 IP 与组播 VLAN 的对应关系。

```
<Sysname> system-view
[Sysname] ftth
[Sysname-ftth] multicast vlan-id 1002 dest-ip 225.1.1.1
[Sysname-ftth] multicast vlan-id 1003 dest-ip 225.1.2.1
[Sysname-ftth] quit
```

(2) 全局开启 IGMP Snooping 功能。

```
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
```

(3) 在 VLAN 1002 和 VLAN 1003 内启动 IGMP Snooping 功能。

```
[Sysname] vlan 1002
[Sysname-vlan1002] igmp-snooping enable
[Sysname-vlan1002] vlan 1003
[Sysname-vlan1003] igmp-snooping enable
[Sysname-vlan1003] quit
```

(4) 配置 ONU 的组播模式为可控组播模式。

```
[Sysname-Onu3/0/1:1] multicast-mode multicast-control
```

(5) 配置 ONU UNI 端口 1 下的用户可观看频道 1，且仅对频道 2 拥有 60s 的预览，并开启该端口删除下行组播流 VLAN Tag 功能。

```
[Sysname-Onu3/0/1:1] uni 1 multicast-control multicast-address 225.1.1.1 rule permit
[Sysname-Onu3/0/1:1] uni 1 multicast-control multicast-address 225.1.2.1 rule preview time-slice 1
[Sysname-Onu3/0/1:1] uni 1 multicast-strip-tag enable
```

(6) 配置 ONU UNI 端口 2 下的用户不允许观看频道 1，但可观看频道 2，并开启该端口删除下行组播流 VLAN Tag 功能。

```
[Sysname-Onu3/0/1:1] uni 2 multicast-control multicast-address 225.1.1.1 rule deny
[Sysname-Onu3/0/1:1] uni 2 multicast-control multicast-address 225.1.2.1 rule permit
[Sysname-Onu3/0/1:1] uni 2 multicast-strip-tag enable
```

(7) 配置 ONU 为 Trunk 类型(配置成 Trunk 类型后将允许所有 VLAN 的报文通过)。

```
[Sysname-Onu3/0/1:1] port link-type trunk
```

(8) 配置端口 OLT 3/0/1 为 Hybrid 类型，允许 VLAN 1002 和 VLAN 1003 的报文通过，且发送 VLAN 1002 和 VLAN 1003 的报文时携带 Tag。

```
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] port link-type hybrid
[Sysname-Olt3/0/1] port hybrid vlan 1002 1003 tagged
```

(9) 配置端口 GigabitEthernet 2/0/1 为 Trunk 类型，并允许 VLAN 1002 和 VLAN 1003 的报文通过。

```
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] port link-type trunk
[Sysname-GigabitEthernet2/0/1] port trunk permit vlan 1002 1003
```

16.8 ONU 升级配置指导

1. 背景

运营商通过 EPON 厂商得知，ONU 设备新发布了两个版本，其中 109 版本解决了当前版本的几个软件问题，可以让 ONU 更加稳定地运行；而 110 版本在 109 版本的基础上还实现了某个新的业务特性，可以满足运营商开展某项新的应用业务的需求。于是，该运营商的主管工程师决定对当前的 ONU 版本进行升级。

2. 组网图

图 16-8 所示为 ONU 升级配置组网图。

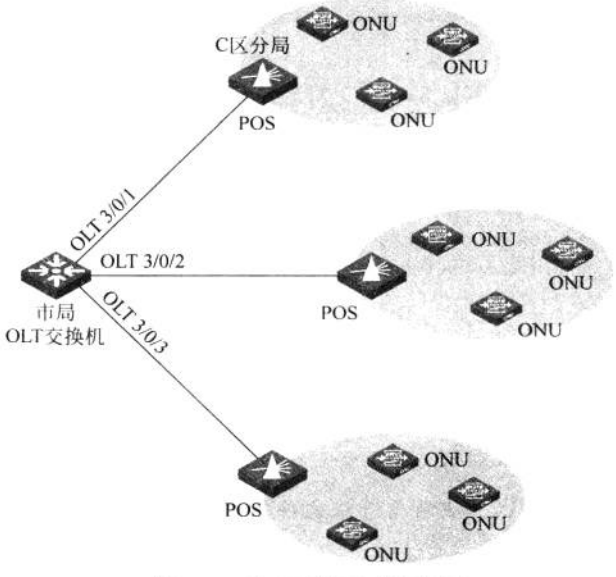


图 16-8 ONU 升级配置组网图

3. 配置需求

(1) 市局交换机有 12 个 OLT 端口下挂了 150 台 A 类型的 ONU。

(2) 其中 OLT 3/0/1 连接的是 C 区分局大楼。为了保证 C 区分局网络运行的稳定性，主管工程师计划对其中大部分 ONU 只升级至 109 版本，而对其中 ONU 3/0/1:1 连接的 ONU 升级至 110 版本，用于新业务测试。

(3) 对于接入到各个小区的 ONU，都需要进行升级至 110 版本。

4. 配置过程和解释

(1) 上传升级文件 a110.app 和 a109.app 到交换机主用主控板和备用主控板，详细过程可参见交换机的软件维护部分。

(2) 用户可以在端口视图(包括 OLT 端口视图、ONU 端口视图)和 FTTH 视图下配置升级 ONU 设备的软件版本。其中，在两种端口视图下的配置优先级高于 FTTH 视图下的配置，而两种端口视图下的配置优先级相等，即后进行的配置会覆盖前面的配置。因此，根据组网需求，升级 ONU 软件版本的配置过程如下：

① 在 OLT 3/0/1 端口视图下配置，将其下挂的 A 类型 ONU 全部升级到 109 版本。

② 在 ONU 3/0/1:1 端口视图下配置，使该端口下挂的 A 类型 ONU 升级到 110 版本。

③ 在 FTTH 视图下配置，将交换机的 12 个 OLT 下挂的 ONU 全部升级到 110 版本。由于 OLT 端口视图下的升级配置优先级高于 FTTH 视图，故此操作不会影响到 OLT 3/0/1 端口下挂的 ONU 设备。

(3) 在 OLT 3/0/1 端口视图下配置升级所有下挂 A 类型的 ONU 到 109 版本。

```
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] update onu filename a109.app
Update flash:/ a109.app?[Y/N]:y
 Info: Download file to onu may take a long time, please wait...
 Please wait while the firmware is being burnt, and check the software version after re-registration!
[Sysname-Olt3/0/1] quit
```

(4) 升级 C 区分局大楼 ONU 3/0/1:1 对应的 A 型 ONU 到 110 版本。

```
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] update onu filename a110.app
Update flash:/ a110.app?[Y/N]:y
 Info: Download file to onu may take a long time, please wait...
 Please wait while the firmware is being burnt, and check the software version after re-registration!
[Sysname-Onu3/0/1:1] quit
```

(5) 配置交换机对所有下挂 A 类型的 ONU 升级到 110 版本。

```
<Sysname> system-view
[Sysname] ftth
[Sysname-ftth] update onu onu-type a filename a110.app
```

注意：不同类型的 ONU 升级所需升级文件不同，如果 ONU 和升级文件不匹配，升级将不会成功。

为了实现批量升级，节省系统资源，升级命令配置后，OLT 会延迟 15～20s 后再执行升级命令。在 ONU 软件更新过程中，建议用户不要对 ONU 断电，以免更新失败。

16.9 UNI端口优先级重标记配置指导

1. 背景

每个用户家里存在多种业务，而这些业务流量的优先级是不一样的。例如，对于视频流，需要提供高优先级；对于普通PC产生的流量，可以设成低优先级。

UNI(User Network Interface，用户网络接口)端口是ONU设备的连接用户的端口。

2. 组网图

图16-9所示为UNI端口优先级重标记配置组网图。

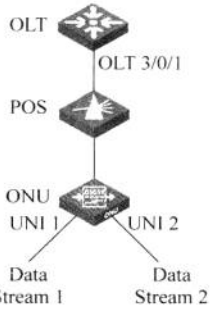


图16-9 UNI端口优先级重标记配置组网图

3. 配置需求

(1) 配置ONU上行带宽为50Mbps。

(2) 配置UNI端口1和UNI端口2的VLAN操作模式均为透传模式。

(3) 配置UNI端口1优先级重标记：对源MAC地址为000A-EB7F-AAAB的带Tag报文重新打上CoS 3的优先级。

(4) 配置UNI端口2优先级重标记：对源MAC为001B-EB7F-21AC的带Tag报文重新打上CoS 1的优先级。

4. 配置过程和解释

(1) 创建ONU端口ONU 3/0/1:1，并将ONU绑定到此ONU端口。

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] using onu 1
[Sysname-Olt3/0/1] quit
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] bind onuid 000f-e200-0104
```

(2) 配置ONU上行带宽为50Mbps(64Kbps×800)。

```
[Sysname-Onu3/0/1:1] upstream-sla minimum-bandwidth 800 maximum-bandwidth 800
```

(3) 配置UNI端口1和UNI端口2的VLAN操作模式为透传模式。

```
[Sysname-Onu3/0/1:1] uni 1 vlan-mode transparent
[Sysname-Onu3/0/1:1] uni 2 vlan-mode transparent
```

(4) 配置 UNI 端口 1 和 UNI 端口 2 优先级重标记。

```
[Sysname-Onu3/0/1:1] uni 1 classification-marking index 1 queue 3 priority 3 src-mac equal 000A-EB7F-AAAB
[Sysname-Onu3/0/1:1] uni 2 classification-marking index 1 queue 1 priority 1 src-mac equal 001B-EB7F-21AC
```

配置完成后，当从 ONU 的两个 UNI 端口进来的两条数据流(流量各为 50Mbps)往 OLT 侧转发时，由于 ONU 端口产生拥塞，则丢弃了源 MAC 地址为 001B-EB7F-21AC 的报文，因为该报文的队列优先级比源 MAC 地址为 000A-EB7F-AAAB 的报文低。

注意：ONU 的每个 UNI 端口所支持的匹配规则数量有限，可根据交换机参数规划。

H3C以太网交换机典型配置指导

本书是H3C网络学院参考书系列之一，是一本易懂、详细、全面的H3C以太网交换机典型配置手册。

本书从简到难，通过贴近实际应用的场景，给出大量的交换机配置实例。本书的最大特点是将配置实例与实际应用场景紧密结合，通过给定场景与相应的配置实例，能够使读者更快、更直观地掌握交换机特性的应用和配置，增强读者的动手技能。

本书是为希望快速、简易配置H3C交换机特性的人员编写的。

清华大学出版社数字出版网站
WQBook 书文局泉
www.wqbook.com

ISBN 978-7-302-28415-4
9 787302 284154 >
定价：60.00元