



H3C SecPath 系列安全产品

操作手册

杭州华三通信技术有限公司

<http://www.h3c.com.cn>

资料版本：20090812-C-1.07

声明

Copyright ©2006-2009 杭州华三通信技术有限公司及其许可者 版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

H3C、**H3C**、Aolynk、、H³Care、、TOP G、、IRF、NetPilot、Neocean、NeoVTL、SecPro、SecPoint、SecEngine、SecPath、Comware、Secware、Storware、NQA、VVG、V²G、VⁿG、PSPT、XGbus、N-Bus、TiGem、InnoVision、HUASAN、华三均为杭州华三通信技术有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。H3C 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，H3C 尽全力在本手册中提供准确的信息，但是 H3C 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

技术支持

用户支持邮箱：customer_service@h3c.com

技术支持热线电话：800-810-0504（固话拨打）

400-810-0504（手机、固话均可拨打）

网址：<http://www.h3c.com.cn>

相关资料及其获取方式

相关资料

手册名称	用途
《H3C SecPath 系列安全产品命令手册》	该手册介绍了 H3C SecPath 系列安全网关/防火墙所涉及的配置和操作命令。包括命令名、完整命令行、参数、操作视图、使用指导和操作举例。
《H3C SecPath 系列安全产品 Web 配置手册》	指导用户通过 Web 方式对 H3C SecPath 系列安全网关/防火墙进行配置操作。
《H3C SecPath SSL VPN 管理员使用手册》	该手册介绍了 H3C SecPath SSL VPN 系统的管理员对系统的用户、资源以及各类策略的操作指导。
《H3C SecPath SSL VPN 用户使用手册》	该手册介绍了 H3C SecPath SSL VPN 系统的用户对各类资源的访问方式。

资料获取方式

您可以通过 H3C 网站（www.h3c.com.cn）获取最新的产品资料：

H3C 网站与产品资料相关的主要栏目介绍如下：

- [产品技术]：可以获取产品介绍和技术介绍的文档。
- [解决方案]：可以获取解决方案类资料。
- [服务支持/文档中心]：可以获取安装类、配置类或维护类产品资料。
- [服务支持/软件下载]：可以获取与软件版本配套的资料。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail: info@h3c.com

感谢您的反馈，让我们做得更好！

前 言

本书简介

本手册各章节内容如下：

- **第 1 部分 基础配置。**该部分首先简要介绍安全网关/防火墙的特点及功能特性。VPN 的基础配置包括用户配置的接口（命令行接口）、系统维护管理、自动侦测配置、HWPing 配置、SNMP 的配置、RMON 配置、BIMS 配置、终端服务、Modem 配置以及接口配置，在用户配置的接口中说明了配置网关所需要搭建的环境，命令行接口特点，以及最基本的配置。在系统维护管理中描述了日志与调试信息中心、文件系统与文件操作、用户界面、用户管理系统和 NTP 配置。SNMP 配置介绍了安全网关/防火墙作为网管 Agent 所需要的设置。终端服务中介绍安全网关/防火墙可以接入的配置终端的种类和方法。接口配置包括安全网关/防火墙的几种物理接口和逻辑接口的配置。
- **第 2 部分 用户接入。**该部分主要介绍安全网关/防火墙接入用户的几种方式。包括 PPP 配置、PPPoE 配置和 VLAN 配置。其中 PPPoE 方式的配置包括 PPPoE Server 配置和 PPPoE Client 配置。
- **第 3 部分 网络层协议。**该部分包括 IP 地址的介绍和配置、IP 应用、IP 性能、IP 单播策略路由的配置，还包括安全网关/防火墙作为 DHCP Server、DHCP Client 及 DHCP 中继的配置、BOOTP 配置、UDP HELPER 配置。
- **第 4 部分 路由协议。**该部分包括 IP 单播路由协议的介绍和配置。包括静态路由、RIP、OSPF、BGP 等协议的配置和路由策略的配置。
- **第 5 部分 MPLS。**该部分包括 MPLS 的基本原理和应用的介绍、MPLS 基本能力的配置。
- **第 6 部分 VPN。**该部分介绍了 VPN 的技术原理和应用分类，说明实现 VPN 的协议 L2TP 和 GRE 的配置，动态 VPN 的配置以及与 VPN 安全相关的 IPsec 和 IKE 配置。该部分还简要说明了 BGP/MPLS VPN 的配置。
- **第 7 部分 安全。**该部分包括命令行分级保护、基于 RADIUS/HWTACACS 的 AAA、包过滤防火墙、状态防火墙、网络地址转换、SSL 和 PKI、透明防火墙、混合模式、面向对象管理、Web 和邮件过滤、攻击防范与报文统计、IDS 联动、日志维护统计等。与此相关的配置还有访问控制列表。
- **第 8 部分 可靠性。**该部分介绍了 VRRP 和双机热备的技术原理和配置。

- **第 9 部分 QoS。**该部分 QoS 的介绍，流分类、流量监管和流量整形的配置、拥塞管理配置、拥塞避免配置和 MPLS QoS 的配置。其中拥塞管理包括 FIFO、PQ、CQ、WFQ、CBQ 和 RTPQ 几种队列机制。
- **第 10 部分 附录。**包括本手册常用的缩略语，及对应的英文全称和中文解释。

本书约定

1. 命令行格式约定

格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x y ... }	表示从两个或多个选项选取一个。
[x y ...]	表示从两个或多个选项选取一个或者不选。
{ x y ... } *	表示从两个或多个选项选取多个，最少选取一个，最多选取所有选项。
[x y ...] *	表示从两个或多个选项选取多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入 1~n 次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格 式	意 义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[]	带方括号“[]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 **小心、注意：**提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。

 **警告：**该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。

 **说明、提示、窍门、思考：**对操作内容的描述进行必要的补充和说明。

目 录

第 1 章 安全产品概述	1-1
1.1 安全网关简介	1-1
1.2 防火墙简介	1-1
1.3 主要特点	1-2
1.3.1 安全保障	1-2
1.3.2 支持丰富的VPN业务	1-3
1.4 H3C SecPath系列安全产品功能特性列表	1-9
第 2 章 用户配置接口	2-1
2.1 配置环境搭建	2-1
2.1.1 通过Console口搭建	2-1
2.1.2 通过Telnet搭建	2-3
2.1.3 通过AUX口拨号搭建	2-4
2.1.4 通过SSH方式搭建	2-6
2.2 命令行接口	2-6
2.2.1 命令行视图	2-7
2.2.2 命令行在线帮助	2-9
2.2.3 命令行错误信息	2-10
2.2.4 历史命令	2-11
2.2.5 编辑特性	2-11
2.2.6 显示特性	2-12
2.2.7 正则表达式的使用	2-13
2.3 快捷键	2-15
2.3.1 快捷键的分类	2-15
2.3.2 快捷键的使用	2-16
2.3.3 快捷键使用举例	2-17
2.3.4 配置命令行别名	2-17
第 3 章 Comware的基本配置	3-1
3.1 进入和退出系统视图	3-1
3.2 设置防火墙的名称	3-1
3.3 设置系统时钟	3-1
3.4 设置提示信息	3-2
3.5 切换用户级别	3-2
3.6 锁定用户界面	3-3
3.7 设置命令级别	3-3

3.8 显示系统状态信息	3-4
第 4 章 系统维护管理	4-1
4.1 系统维护与调试.....	4-1
4.1.1 网络连接的测试工具	4-1
4.1.2 系统调试功能	4-3
4.1.3 配置系统重启	4-4
4.1.4 升级BootROM	4-5
4.1.5 配置热插拔	4-5
4.2 信息中心功能	4-6
4.2.1 信息中心简介	4-6
4.2.2 信息中心配置	4-7
4.2.3 显示终端的设置	4-11
4.2.4 syslog功能简介	4-12
4.2.5 信息中心的显示	4-14
4.2.6 信息中心配置举例.....	4-14
4.3 配置HTTP服务器.....	4-16
4.3.1 使能HTTP服务器	4-16
4.3.2 配置HTTP服务器的访问限制.....	4-16
第 5 章 自动侦测配置	5-1
5.1 自动侦测简介	5-1
5.2 自动侦测基本配置	5-1
5.2.1 自动侦测基本配置任务	5-1
5.2.2 自动侦测基本配置举例	5-2
5.3 自动侦测在静态路由中的应用	5-3
5.3.1 静态路由中的应用配置任务	5-3
5.3.2 静态路由中的应用举例	5-4
5.4 自动侦测在VRRP中的应用	5-5
5.4.1 VRRP中的应用配置任务	5-5
5.4.2 VRRP中的应用举例.....	5-5
第 6 章 HWPing配置	6-1
6.1 HWPing简介.....	6-1
6.2 HWPing的配置	6-1
6.2.1 HWPing服务器的配置	6-1
6.2.2 HWPing客户端的配置	6-2
6.3 执行测试.....	6-13
6.4 HWPing的显示和调试	6-13
6.5 HWPing典型配置举例	6-14
6.5.1 ICMP测试	6-14
6.5.2 DHCP测试	6-15

6.5.3 FTP测试	6-15
6.5.4 HTTP测试.....	6-17
6.5.5 Jitter测试	6-17
6.5.6 SNMP测试.....	6-19
6.5.7 指定端口的TCP测试.....	6-20
6.5.8 指定端口的UDP测试	6-21
第 7 章 文件管理	7-1
7.1 文件系统.....	7-1
7.1.1 文件系统简介.....	7-1
7.1.2 目录操作	7-1
7.1.3 文件操作	7-1
7.1.4 解包Web文件.....	7-2
7.1.5 存储设备操作.....	7-2
7.1.6 文件系统提示方式.....	7-2
7.1.7 文件系统使用举例.....	7-3
7.2 FTP配置	7-4
7.2.1 FTP简介	7-4
7.2.2 启动FTP服务器.....	7-4
7.2.3 配置FTP服务器的验证和授权.....	7-4
7.2.4 配置FTP服务器的运行参数	7-5
7.2.5 FTP服务器的显示和调试	7-6
7.2.6 FTP客户端介绍.....	7-7
7.2.7 使用FTP升级Comware应用程序典型配置举例 1.....	7-8
7.2.8 使用FTP升级Comware应用程序典型配置举例 2.....	7-10
7.3 TFTP配置	7-11
7.3.1 TFTP简介	7-11
7.3.2 TFTP协议配置	7-11
7.3.3 TFTP客户端的显示.....	7-13
7.4 配置文件管理	7-13
7.4.1 简介	7-13
7.4.2 配置文件命名及启动时的选择顺序	7-15
7.4.3 备份配置文件.....	7-16
第 8 章 用户界面配置	8-1
8.1 用户界面简介	8-1
8.1.1 用户界面概述.....	8-1
8.1.2 用户界面的编号	8-1
8.2 用户界面配置步骤	8-2
8.2.1 进入用户界面视图.....	8-2
8.2.2 设置所在用户界面支持的协议	8-3
8.2.3 配置异步接口属性.....	8-3

8.2.4 配置终端属性.....	8-5
8.2.5 Modem属性配置.....	8-7
8.2.6 配置自动执行命令.....	8-8
8.2.7 配置VTY类型用户界面的呼入呼出限制.....	8-8
8.3 用户界面的显示和调试.....	8-9
8.3.1 显示用户界面的使用信息.....	8-9
8.3.2 显示用户界面的物理属性和一些配置.....	8-9
第9章 用户管理	9-1
9.1 用户管理概述	9-1
9.1.1 用户分类.....	9-1
9.1.2 用户的优先级.....	9-1
9.1.3 认证方案.....	9-2
9.1.4 规划防火墙的用户.....	9-2
9.2 配置用户.....	9-2
9.2.1 配置认证用户的方式.....	9-3
9.2.2 配置用户名及口令.....	9-3
9.2.3 设置用户的优先级.....	9-4
9.2.4 设置用户按命令行进行计费.....	9-5
9.3 显示用户信息	9-6
9.4 用户管理举例	9-6
9.4.1 使用password方式认证用户	9-6
9.4.2 使用本地用户数据库进行用户认证	9-6
第10章 NTP配置	10-1
10.1 NTP协议简介	10-1
10.2 NTP协议配置	10-3
10.2.1 配置NTP工作模式	10-3
10.2.2 配置NTP身份验证功能	10-6
10.2.3 设置本地发送NTP消息的接口	10-7
10.2.4 设置NTP主时钟	10-8
10.2.5 设置禁止/允许接口接收NTP消息.....	10-8
10.2.6 设置对本地防火墙NTP服务的访问控制权限.....	10-9
10.2.7 设置本地允许建立的sessions数目.....	10-9
10.3 NTP显示与调试.....	10-10
10.4 NTP典型配置举例	10-10
10.4.1 配置NTP服务器	10-10
10.4.2 配置NTP对等体举例.....	10-12
10.4.3 配置NTP广播模式	10-13
10.4.4 配置带认证的NTP广播模式.....	10-15
10.4.5 配置NTP组播模式	10-17
10.4.6 配置带身份验证的NTP服务器模式	10-18

第 11 章 SNMP配置	11-1
11.1 协议简介	11-1
11.1.1 SNMP协议介绍	11-1
11.1.2 SNMP版本及支持的MIB	11-1
11.2 SNMP配置	11-2
11.2.1 启动或关闭SNMP Agent服务	11-2
11.2.2 使能或禁止SNMP协议的相应版本	11-3
11.2.3 设置团体名	11-3
11.2.4 设置/删除SNMP组	11-4
11.2.5 添加/删除用户	11-4
11.2.6 设置管理员的联系方式	11-5
11.2.7 允许/禁止发送Trap报文	11-5
11.2.8 设置本地设备的引擎ID	11-5
11.2.9 设置Trap目标主机的地址	11-6
11.2.10 设置接口发送状态Trap报文	11-6
11.2.11 设置防火墙的位置信息	11-6
11.2.12 指定发送Trap的源地址	11-7
11.2.13 MIB视图信息设置	11-7
11.2.14 设置消息包的最大值	11-7
11.2.15 设置Trap报文的队列长度	11-8
11.2.16 设置Trap报文的保存时间	11-8
11.3 SNMP显示和调试	11-9
11.4 SNMP典型配置举例	11-9
第 12 章 BIMS配置	12-1
12.1 BIMS概述	12-1
12.2 BIMS配置	12-2
12.2.1 配置使能BIMS功能	12-2
12.2.2 配置设备唯一标识符	12-2
12.2.3 配置BIMS中心的IP地址和端口号	12-3
12.2.4 配置BIMS设备发送报文时携带的源IP地址	12-3
12.2.5 配置BIMS设备侧和中心侧的共享密钥	12-3
12.2.6 配置当设备上电时是否触发设备访问BIMS中心	12-4
12.2.7 配置触发访问BIMS中心的间隔时间	12-4
12.2.8 配置设备在某一特定的时间访问BIMS中心以及访问的周期	12-4
12.2.9 配置设备立即访问BIMS中心	12-5
12.3 BIMS配置调试	12-5
12.4 BIMS典型配置举例	12-5
12.4.1 配置设备上电后立即访问BIMS中心	12-5
12.4.2 配置设备在一定时间段内周期性访问BIMS中心	12-7
12.5 BIMS常见配置错误举例	12-8

12.5.1 无法成功访问BIMS服务器	12-8
12.5.2 无法下载新文件	12-8
12.5.3 无法通过DHCP获取BIMS配置	12-9
12.5.4 访问BIMS服务器导致设备上的bims interval命令配置发生变化	12-9
第 13 章 RMON配置	13-1
13.1 RMON简介	13-1
13.2 RMON的配置	13-2
13.2.1 添加/删除事件表的一个表项	13-2
13.2.2 添加/删除告警表的一个表项	13-2
13.2.3 添加/删除RMON告警扩展表的一个表项	13-3
13.2.4 添加/删除历史控制表的一个表项	13-4
13.2.5 添加/删除统计表的一个表项	13-4
13.2.6 RMON显示和调试	13-5
13.3 RMON典型配置举例	13-5
第 14 章 终端服务	14-1
14.1 终端服务简介	14-1
14.2 Console口终端服务	14-1
14.3 AUX口的远程终端服务	14-1
14.3.1 功能描述	14-1
14.3.2 AUX口的远程配置终端服务特性	14-2
14.4 Telnet终端服务	14-2
14.4.1 Telnet服务种类	14-2
14.4.2 建立Telnet连接	14-3
14.4.3 为Telnet Server指定源接口或IP地址	14-5
14.4.4 Telnet显示和调试	14-5
14.5 SSH终端服务	14-6
14.5.1 SSH简介	14-6
14.5.2 SSH Server配置	14-9
14.5.3 SSH Client配置	14-15
14.5.4 SSH显示和调试	14-17
14.5.5 SSH Server配置举例	14-18
14.5.6 SSH Client配置举例	14-20
14.6 SFTP服务	14-21
14.6.1 SFTP简介	14-21
14.6.2 SFTP Server配置	14-22
14.6.3 SFTP Client配置	14-23
14.6.4 SFTP配置举例	14-26
14.7 哑终端服务	14-28
14.7.1 哑终端的功能描述	14-28

14.7.2 哑终端服务特性	14-29
14.7.3 哑终端的典型应用	14-29
14.7.4 配置哑终端服务	14-29
14.7.5 哑终端连接的定时断开	14-31
第 15 章 Modem管理配置	15-1
15.1 Modem管理简介	15-1
15.1.1 Comware提供的Modem管理功能.....	15-1
15.1.2 Modem脚本	15-1
15.2 Modem管理的配置	15-3
15.2.1 配置Modem的呼入和呼出权限	15-3
15.2.2 配置Modem脚本	15-4
15.2.3 手工执行Modem脚本.....	15-4
15.2.4 配置Modem的应答方式	15-4
15.3 Modem显示和调试	15-5
15.4 Modem典型配置举例	15-5
15.4.1 使用Modem脚本管理Modem.....	15-5
15.4.2 使用脚本进行直接拨号	15-6
15.5 Modem管理常见故障的诊断与排除.....	15-6
第 16 章 接口配置	16-1
16.1 接口配置概述	16-1
16.1.1 接口介绍	16-1
16.1.2 接口的配置	16-1
16.1.3 接口的显示和调试	16-3
16.2 以太网接口	16-4
16.2.1 以太网接口介绍	16-4
16.2.2 以太网接口的配置	16-4
16.2.3 以太网接口的显示和调试.....	16-8
16.2.4 以太网接口典型配置举例.....	16-8
16.2.5 以太网接口常见故障的诊断与排除	16-9
16.3 AUX接口	16-10
16.3.1 AUX接口介绍.....	16-10
16.3.2 AUX接口配置.....	16-11
16.4 逻辑接口配置	16-12
16.4.1 Dialer接口	16-12
16.4.2 Loopback接口.....	16-14
16.4.3 Null接口	16-15
16.4.4 子接口.....	16-16
16.4.5 虚拟模板接口和虚拟接口.....	16-17

第1章 安全产品概述

 说明：

- SecPath 系列安全产品包括 SecPath 系列安全网关及 SecPath 系列防火墙设备。本手册以 SecPath 防火墙为例进行了配置操作描述，同样适用于安全网关设备。
- SecPath 系列中不同型号的产品之间所支持的功能或命令行会略有不同，请用户以实际产品的版本为准。

1.1 安全网关简介

H3C SecPath 安全网关设备（以下简称安全网关）是面向企业用户开发的新一代专业安全网关设备，可以作为企业的汇聚及接入网关设备。

安全网关支持包过滤防火墙、AAA、NAT、QoS 等技术，可以确保在开放的 Internet 上实现安全的、满足可靠质量要求的私有网络。

安全网关支持多种 VPN 业务，如 L2TP VPN、IPsec VPN、SSL VPN、GRE VPN、动态 VPN 等等，可以针对客户需求通过拨号、租用线路、VLAN 或隧道等方式接入远端用户，构建 Intranet、Extranet、Access 等多种形式的 VPN。

安全网关支持完备的加密解决方案，通过加密芯片，实现高速 IPsec/SSL 特性。

安全网关提供基本的路由能力，支持 RIP/OSPF/BGP/路由策略及策略路由。

支持丰富的 QoS 特性，提供流分类、流量监管、流量整形及多种队列调度策略。

1.2 防火墙简介

除支持上述安全网关的所有特性外，H3C SecPath 防火墙还提供了多种安全特性。

H3C SecPath 防火墙支持攻击防范特性。防火墙的攻击防范功能能够检测出多种类型的网络攻击，如 IP 地址欺骗、地址扫描与端口扫描、SYN Flood 攻击、Ping of Death 攻击等等，并能采取相应的措施保护内部网络免受恶意攻击，保证内部网络及系统的正常运行。

H3C SecPath 防火墙支持 Web 和邮件过滤，以阻止内部用户访问非法的网址或访问含有非法内容的网页，防止内网用户向外网非法邮件地址发送邮件或向外发送与工作无关的邮件。同时，邮件过滤也能防止外部向内部发送邮件。

H3C SecPath 防火墙支持黑名单功能，可以以高速实现报文的过滤，从而有效地将特定 IP 地址发送来的报文屏蔽。

H3C SecPath 防火墙支持 MAC 和 IP 地址绑定，是避免 IP 地址欺骗攻击的一种方式，从而形成有效的保护。

H3C SecPath 防火墙支持 IDS（Intrusion Detect System）联动，通过协作外部 IDS 设备的深度检测功能，防止黑客、网络病毒的入侵。



注意：

- SecPath 系列防火墙使用安全区域的概念来表示与其相连接的网络。若要实现防火墙和其它设备的互通，必须先将相应的接口添加到某一安全区域中。
- 缺省情况下，SecPath 系列防火墙使能防火墙的包过滤功能，且缺省的过滤行为为拒绝所有报文通过。若要实现防火墙和其它设备的互通，需先关闭防火墙的包过滤功能，或将缺省的过滤行为改为允许报文通过，或在接口应用访问控制列表 ACL 以允许相应的报文通过。

关于以上内容的具体描述请参见本手册的“安全”部分。

1.3 主要特点

1.3.1 安全保障

1. 防火墙过滤

支持包过滤技术。借助报文中优先级、TOS、UDP 或 TCP 端口等信息作为过滤参考，通过在接口输入或输出方向上使用基本或高级访问控制规则，可以实现对数据包的过滤。同时，还可以按照时间段进行过滤，不仅保护内部网络免遭外来攻击，还可以有效控制内部主机对外部资源的访问，形成内外网络之间的安全保护屏障，同时，规则自动排序还简化了配置复杂度。

支持应用层报文过滤 ASPF（Application Specific Packet Filter），也称为状态防火墙。这是一种高级通信过滤，它检查基于 TCP/UDP 协议的应用层协议信息（目前可以检测 FTP、HTTP、SMTP、RTSP、H.323 协议），并且监控基于连接的应用层协议状态，维护每一个连接的状态信息，并动态地决定数据包是否允许通过防火墙。

2. 安全认证

防火墙提供了如下几方面的安全认证功能：

- 实现了用户身份管理，不同身份的用户拥有不同的命令执行权限，可以防止低权限用户非法获取或修改配置信息等。防火墙设置了如下四种身份的用户：参观（Visit）级、监控（Monitor）级、配置（Config）级和管理（Manage）级用户。

- 视图分级保护。将用户分成 4 级，每级用户赋予不同的配置权限，级别低的用户不能进入更高级的视图。
- 在 PPP 线路上支持 CHAP 和 PAP 验证协议。
- 支持基于 RADIUS（Remote Authentication Dial-In User Service）和 HWTACACS（HUAWEI Terminal Access Controller Access Control System）的 AAA（Authentication, Authorization, Accounting）服务，可以与 RADIUS 和 TACACS 服务器配合实施对接入用户的验证、授权和计费的安全服务，防止非法访问。
- 路由协议 OSPF、RIPv2 都具有 MD5 认证功能，确保所交换路由信息的可靠性。

3. NAT 应用

地址转换 NAT（Network Address Translation）又称地址代理，将内部网络主机的 IP 地址和端口号替换为外部网络地址和端口号，有效控制内部网络和外部网络之间的访问，不仅节约了宝贵的 IP 地址资源，而且为内部主机提供了“隐私”保护。

目前，提供一对一、多对一、地址池、ACL 控制等地址转换方式，在一个接口上支持多种地址转换服务，通过内部服务器可以向外提供 FTP、Telnet 和 WWW 等服务，实现公网和私网混合地址解决方案。

1.3.2 支持丰富的 VPN 业务

1. 支持 L2TP VPN

L2TP 协议提供了对 PPP 链路层数据包的通道（Tunnel）传输支持。按照 L2TP 协议实现 PPP 提供的认证（PAP、CHAP）功能，支持 RADIUS 服务器验证和内部地址分配功能，支持在隧道两端由运营商及企业网进行灵活计费。另外，结合防火墙、IPsec 等技术可为信息提供安全保障。L2TP 协议适合流动性很强的用户通过隧道构建 Access VPN。

两种典型的 L2TP 隧道模式：

(1) 由远程拨号用户发起

远程系统可以通过 PSTN/ISDN/ADSL/等多种方式拨入 LAC，由 LAC 通过 Internet 向 LNS 发起建立通道连接请求。拨号用户地址由 LNS 分配；对远程拨号用户的验证与计费既可由 LAC 侧的代理完成，也可在 LNS 侧完成。

(2) 直接由 LAC 客户（指可在本地支持 L2TP 协议的用户）发起

LAC 客户拥有公网地址后，可直接向 LNS 发起通道连接请求，无需再经过一个单独的 LAC 设备。此时，LAC 客户的私网地址分配由 LNS 来完成。

2. 支持 GRE VPN

GRE 是第三层隧道协议，在协议层之间采用了一种被称之为 Tunnel（隧道）的技术，在一个 Tunnel 的两端分别对数据报进行封装及解封装。Tunnel 是一个虚拟的对点的连接，在实际中可以看成仅支持点对点连接的虚拟接口，这个接口提供了一条通路使封装的数据报能够在这个通路上传输。采用这种方式对网络层协议（如：IP，IPX，AppleTalk 等）的数据报进行封装后，这些被封装的数据报能够在另一个网络层协议中传输。由于实现机制简单，所以隧道两端设备的 CPU 负担小。由于 GRE 不提供数据加密功能、不对数据源进行验证、不保证数据传输到正确的目的地，故一般与 IPsec 相结合使用构建 Intranet/Extranet VPN。

3. 支持 IPsec VPN

IPsec（IP security）协议族是 IETF 制定的一系列协议，它为 IP 数据报提供了高质量的、可互操作的、基于密码学的安全性。特定的通信方之间在 IP 层通过加密与数据源验证等方式，来保证数据报在网络上传输时的私有性、完整性、真实性和防重放。IPsec 通过 AH（Authentication Header，认证头）和 ESP（Encapsulating Security Payload，封装安全载荷）这两个安全协议来实现上述目标。IPsec 可以通过手工方式建立安全联盟，也可以通过 IKE 方式（Internet Key Exchange，因特网密钥交换协议）自动为 IPsec 提供自动协商交换密钥、建立和维护安全联盟的服务。IPsec 协议为对信息安全要求较高的用户提供了一个安全的 VPN 解决方案。通常情况下，IPsec 与 L2TP 协议和 GRE 协议等相结合使用。

(1) IPsec 协议的操作模式

IPsec 协议有两种操作模式：传输模式和隧道模式。SA 中指定了协议的操作模式。在传输模式下，AH 或 ESP 被插入到 IP 头之后但在所有传输层协议之前。在隧道模式下，AH 或 ESP 插在原始 IP 头之前，另外生成一个新头放到 AH 或 ESP 之前。不同安全协议在传输模式和隧道模式下的数据封装形式（传输协议以 TCP 为例）如下图所示：

模式 协议	transport						tunnel					
AH	IP Header	AH	TCP Header	data			new IP Header	AH	raw IP Header	TCP Header	data	
ESP	IP Header	ESP	TCP Header	data	ESP Tail	ESP Auth data	new IP Header	ESP	raw IP Header	TCP Header	data	ESP Tail ESP Auth data
AH-ESP	IP Header	AH	ESP	TCP Header	data	ESP Tail ESP Auth data	new IP Header	AH	ESP	raw IP Header	TCP Header	data ESP Tail ESP Auth data

图1-1 安全协议数据封装格式

从安全性来讲，隧道模式优于传输模式。它可以完全地对原始 IP 数据报进行验证和加密；此外，可以使用 IPsec 对等体的 IP 地址来隐藏客户机的 IP 地址。从性能来

讲，隧道模式比传输模式占用更多带宽，因为它有一个额外的 IP 头。因此，到底使用哪种模式需要在安全性和性能间进行权衡。

(2) 验证算法

AH 和 ESP 都能够对 IP 报文的完整性进行验证，以判别报文在传输过程中是否被篡改。验证算法的实现主要是通过 Hash 函数，Hash 函数是一种能够接受任意长的消息输入，并产生固定长度输出的算法，该输出称为消息摘要。IPsec 对等体计算摘要，如果两个摘要是相同的，则表示报文是完整未经篡改的。一般来说 IPsec 使用两种验证算法：

- MD5: MD5 通过输入任意长度的消息，产生 128bit 的消息摘要。
- SHA-1: SHA-1 通过输入长度小于 2 的 64 次方比特的消息，产生 160bit 的消息摘要。

SHA-1 的摘要长于 MD5，因而是更安全的。

(3) 加密算法

ESP 能够对 IP 报文内容进行加密保护，防止报文内容在传输过程中被窥探。加密算法实现主要通过对称密钥系统，它使用相同的密钥对数据进行加密和解密。Comware 中的 IPsec 实现了三种加密算法：

- DES: 使用 56bit 的密钥对每个 64bit 的明文块进行加密。
- 3DES: 使用三个 56bit 的 DES 密钥（共 168bit 密钥）对明文进行加密。3DES 具有更高的安全性，但其加密数据的速度要比 DES 慢得多。
- AES（Advanced Encryption Standard）: Comware 实现了 128bit、192bit 和 256bit 密钥长度的 AES 算法。

(4) 协商方式

有两种协商方式建立安全联盟，一种是手工方式（**manual**），一种是 IKE 自动协商（**isakmp**）方式。前者配置比较复杂，创建安全联盟所需的全部信息都必须手工配置，而且 IPsec 的一些高级特性（例如定时更新密钥）不被支持，但优点是可以不依赖 IKE 而单独实现 IPsec 功能。而后者则相对比较简单，只需要配置好 IKE 协商安全策略的信息，由 IKE 自动协商来创建和维护安全联盟。

当与之进行通信的对等体设备数量较少时，或是在小型静态环境中，手工配置安全联盟是可行的。对于中、大型的动态网络环境中，推荐使用 IKE 协商建立安全联盟。

(5) IKE

在实施 IPsec 的过程中，可以使用因特网密钥交换 IKE（Internet Key Exchange）协议来建立安全联盟，该协议建立在由 Internet 安全联盟和密钥管理协议 ISAKMP（Internet Security Association and Key Management Protocol）定义的框架上。IKE 为 IPsec 提供了自动协商交换密钥、建立安全联盟的服务，可以在不安全的网络上

安全地分发密钥、验证身份、建立 IPsec 安全联盟，即简化了 IPsec 的使用和管理，又进一步保障数据安全。IKE 的安全机制包括：

- **DH（Diffie-Hellman）交换及密钥分发**

Diffie-Hellman 算法是以蒂夫-海曼的名字命名的一种公共密钥算法。通信双方在不传送密钥的情况下通过交换一些数据，计算出共享的密钥。加密的前提是交换加密数据的双方必须要有共享的密钥。IKE 的精髓在于它永远不在不安全的网络上直接传送密钥，而是通过一系列数据的交换，最终计算出双方共享的密钥。即使第三者（如黑客）截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥。

- **完善的前向安全性（Perfect Forward Secrecy, PFS）**

PFS 特性是一种安全特性，指一个密钥被破解，并不影响其他密钥的安全性，因为这些密钥间没有派生关系。对于 IPsec，是通过在 IKE 阶段 2 协商中增加一次密钥交换来实现的。

- **身份验证**

身份验证确认通信双方的身份。对于 pre-shared key 验证方法，验证字用来作为一个输入产生密钥，验证字不同是不可能在双方产生相同的密钥的。验证字是验证双方身份的关键。

- **身份保护**

身份数据在密钥产生之后加密传送，实现了对身份数据的保护。

- **IKE 阶段的协商模式**

另外，为了使 IKE 支持目前广泛应用的通过 ADSL 方式构建 VPN 的方案中的特殊情况——即局端设备的 IP 地址为固定分配的，用户端设备的 IP 地址为动态获取的情况，在 IKE 阶段的协商模式中增加了 IKE 野蛮模式，它可以选择根据协商发起端的 IP 地址或者 ID 来查找对应的身份验证字，并最终完成协商。IKE 野蛮模式相对于主模式来说更加灵活，能够支持协商发起端为动态 IP 地址的情况。

- **NAT 穿越功能**

在 IPsec/IKE 组建的 VPN 隧道中，若存在 NAT 网关设备，且 NAT 网关设备对 VPN 业务数据流进行了 NAT 转换的话，则必须配置 IPsec/IKE 的 NAT 穿越功能。该功能删去了 IKE 协商过程中对端 UDP 端口号的验证过程，同时实现了对 VPN 隧道中 NAT 网关设备的发现功能，即如果发现 NAT 网关设备，则将在之后的 IPsec 数据传输中使用 UDP 封装（即将 IPsec 报文封装到 IKE 协商所使用的 UDP 连接隧道里）的方法，避免了 NAT 网关对 IPsec 报文进行篡改（NAT 网关设备将只能够修改最外层的 IP 和 UDP 报文头，对 UDP 报文封装的 IPsec 报文将不作修改），从而保证了 IPsec 报文的完整性（IPsec 数据加密解密验证过程中要求报文原封不动地被传送到接收端）。

4. 支持 SSL VPN

SSL 协议是一种在两台设备之间提供安全通道的协议。它具有保护传输数据以及识别通信机器的功能。SSL 协议设计目标主要有两个：第一是为客户端与服务器之间的传输提供保密性；第二是身份认证（包括服务器认证和可选客户端认证）。

SSL 协议提供了全面的安全策略：协商加密套件后，使用套件中的非对称加密算法实现会话密钥的交换，利用证书的身份认证方式保证用户的合法性，在传输过程中用密钥对数据进行加密，保证应用数据传输时的安全性。如果发生数据的篡改、用户身份验证非法等错误时，自动断开连接，防止各种类型的恶意攻击。

SSL（Security Socket Layer，安全套接层）VPN 是一种新兴的 VPN 技术。在 SSL 的基础上，实现 HTTPS 服务器和 HTTPS 客户端，保证远端合法用户可以安全的登录到设备上，同时实现了对网络资源细粒度的访问控制。在 SecPath SSL VPN 系统中，用户有三种方式可以访问资源：**Web 接入方式**、**TCP 接入方式**和 **IP 接入方式**。采用基于角色的权限管理方法，根据用户登录的身份，限制用户可以访问的资源；同时，结合用户主机安全检查可以实现动态分配用户可访问权限。**SecPath** 系列防火墙/安全网关支持 **SSL VPN Web 管理平台**，管理员可以使用 **Web 浏览器**来配置和管理 **SSL VPN 系统**。

SSL VPN 与传统 VPN 系统相比，有更好的易用性，无需用户配置、免客户端安装、部署简单，安全性高且安全控制力度大，极大地方便了企业的移动办公用户和网络管理。

5. 支持动态 VPN

动态 VPN（DVPN）提出了 NBMA（NonBroadcast MultiAccess，非广播多路访问）类型的隧道机制，采用了 **Client** 和 **Server** 的方式，解决了传统 VPN 的诸多缺陷，适合于通过骨干网将多个私网连成一个 VPN。其主要特点如下：

(1) 支持 GRE 及 UDP 两种隧道

不仅支持 **GRE** 方式建立隧道，还支持 **UDP** 方式的隧道。故能够穿越 **NAPT** 网关，解决了私网 **IP** 地址通过 **NAPT** 网关和其他设备建立 **VPN** 网络的问题。

(2) 支持依赖动态 IP 地址构建 VPN

动态 VPN 在同一个 VPN 内部构建隧道时，只需要指定相应的 **Server** 的 **IP** 地址，并不关心自己当前使用的 **IP** 地址是多少，更加适应如 **xDSL** 拨号使用动态 **IP** 地址的组网应用。

(3) 支持自动建立隧道技术

动态 VPN 中的每一个节点维护着一个公网-私网地址映射表，两个节点之间的隧道完全是自动建立的。每台作为 **Client** 的防火墙只需配置自己的相关信息，比如本地的 **IP** 地址、**UDP** 方式下使用的端口号、所属的 **VPN** 和 **Server** 等，不需要知道其

他 Client 的任何信息就可以互相通讯。不仅减少了维护管理的工作量，同时也减少了发生错误的可能性。

(4) 认证加密技术

动态 VPN 使用了认证、加密等技术，最大程度地保证用户数据的安全及用户网络的安全。首先，动态 VPN 提供了注册认证机制，Client 设备必须经过 Server 的认证才能加入到某个特定的动态 VPN 域内，而且在 Client 之间建立隧道时也提供了相互的身份认证功能。

(5) 支持多个 VPN 域

动态 VPN 允许用户在一台防火墙上支持多个 VPN 域。即一台防火墙不仅可以属于 VPN A，也可以属于 VPN B；同一设备可以在 VPN A 中作为 Client 设备，同时还在 VPN B 中作为 Server 设备使用。大大提高了组网的灵活性，也可以更加充分的使用网络设备资源，减少了用户的投资。

1.4 H3C SecPath 系列安全产品功能特性列表

表1-1 H3C SecPath 系列安全产品功能特性列表

属性	说明	
网络安全性	验证、授权和计帐（AAA）服务	● RADIUS ● HWTACACS ● CHAP 验证 ● PAP 验证
	防火墙	● 包过滤 基于接口的访问控制列表 基于时间段的访问控制列表 ● 防火墙 包过滤防火墙 状态防火墙 透明防火墙（仅 SecPath F100-C 防火墙和 SecPath F100-S 防火墙支持透明防火墙） 混合模式（仅 SecPath F1000-A 防火墙、SecPath F1000-S 防火墙、SecPath F1000-C 防火墙、SecPath F100-A 防火墙、SecPath F100-A-SI 防火墙、SecPath F100-M 防火墙、SecPath F100-E 防火墙、SecPath F100-C-EI 防火墙、SecPath F100-C II 防火墙即新一代 F100-C 支持混合模式） 黑名单（仅 SecPath 系列防火墙设备支持） MAC 地址绑定（仅 SecPath 系列防火墙设备支持） Web 和邮件过滤（仅 SecPath 系列防火墙设备支持） 攻击防范（仅 SecPath 系列防火墙设备支持） IDS 联动（仅 SecPath 系列防火墙设备支持） 面向对象管理（仅 SecPath F1000-A 防火墙、SecPath F1000-S 防火墙、SecPath F1000-C 防火墙、SecPath F100-A 防火墙、SecPath F100-A-SI 防火墙、SecPath F100-M 防火墙、SecPath F100-E 防火墙和 SecPath V1000-A 安全网关、SecPath V100-E 安全网关支持） 防火墙流日志（仅 SecPath F1000-A 防火墙、SecPath F1000-S 防火墙、SecPath F1000-C 防火墙、SecPath F100-A 防火墙、SecPath F100-A-SI 防火墙、SecPath F100-M 防火墙和 SecPath F100-E 防火墙支持）
	数据安全	● 支持终端访问安全 ● IPsec ● IKE

属性	说明	
	NAT	- 支持局域网内用户使用地址池中的 IP 地址访问外部网络 - 支持将访问控制列表与地址池的关联 - 支持将访问控制列表与接口的关联 - 支持外部网络主机访问内部的服务器 - 可配置支持地址转换的有效时间 - 支持多种 ALG（Application Layer Gateway，应用层网关）
VPN	L2TP VPN	可以根据 VPN 用户完整用户名、用户域名向指定 LNS 发起连接 可以为 VPN 用户分配地址 可以进行 LCP 重协商和二次 CHAP 验证
	IPsec/IKE	支持 AH、ESP 协议 支持手工或通过 IKE 自动建立安全联盟 ESP 支持 DES、3DES、AES 三种加密算法 支持 MD5 及 SHA-1 验证算法 支持 IKE 主模式及野蛮模式 支持 NAT 穿越
	SSL VPN	采用 SSL 协议建立的加密连接 VPN 网络。其协议工作在传输层之上，保护应用程序之间的安全连接： 支持对网络资源细粒度的访问控制 支持三种方式访问资源：Web 接入方式、TCP 接入方式和 IP 接入方式 支持基于角色的权限管理方法，根据用户登录的身份，分配用户可访问资源权限 支持用户主机安全检查实现动态分配用户可访问资源权限 （仅 SecPath F1000-A 防火墙、SecPath F1000-S 防火墙、SecPath F1000-C 防火墙、SecPath F100-A 防火墙、SecPath F100-A-SI 防火墙、SecPath F100-M 防火墙、SecPath F100-E 防火墙和 SecPath V1000-A 安全网关、SecPath V100-E 安全网关通过 SSL VPN Web 管理平台支持）
	GRE VPN	采用了虚拟的点对点的 Tunnel（隧道）技术，在一个 Tunnel 的两端分别对数据报进行封装及解封装。
	DVPN	提供 GRE、UDP 两种隧道（SecPath 系列防火墙仅支持 UDP 方式建立隧道） 支持 client 端接入认证及节点间的加密认证 支持依赖动态 IP 地址构建 VPN 同一个节点可以属于不同的 VPN 域 支持多个 VPN 域 支持 NAT 穿越 DVPN 隧道可以承载 IPsec 加密 通过动态建立隧道节省 Server 带宽

属性	说明	
	MPLS L3 VPN	支持 MPLS L3 VPN（仅 SecPath V1000-A 安全网关支持 MPLS 和 VPN 实例）
网络互连	局域网协议	Ethernet_II Ethernet_SNAP VLAN
	链路层协议	PPP PPPoE
网络协议	IP 服务	ARP 静态域名解析 IP 地址借用 DHCP 中继 DHCP 服务器 DHCP 客户端
	IP 路由	- 静态路由管理 - 动态路由协议 RIP-1/RIP-2 OSPF BGP - 路由策略 - 策略路由
网络可靠性	VRRP	确保在通信线路或设备故障时提供备用方案，从而保障数据通信的畅通，有效增强了网络的强壮性和可靠性。
	双机热备	在两台防火墙之间进行状态的备份，提供业务的不间断运行，解决了传统组网方案（例如 VRRP 等）的缺陷。（仅 SecPath F1000-A 防火墙、SecPath F1000-S 防火墙、SecPath F1000-C 防火墙、SecPath F100-A 防火墙、SecPath F100-A-SI 防火墙、SecPath F100-M 防火墙和 SecPath F100-E 防火墙设备支持）
服务质量保证（QoS）	流量监管	Traffic Policing
	拥塞管理	FIFO、PQ、CQ、WFQ、CBQ/LLQ、RTPQ
	拥塞避免	RED 及 WRED
	流量整形	TS
	接口速率限制	LR
	深度应用识别	DAR（Deeper Application Recognition）（仅 SecPath F1000-A 防火墙、SecPath F1000-S 防火墙、SecPath F1000-C 防火墙、SecPath F100-A 防火墙、SecPath F100-A-SI 防火墙、SecPath F100-M 防火墙、SecPath F100-E 防火墙和 SecPath V1000-A 安全网关、SecPath V100-E 安全网关支持）

属性	说明	
配置管理	命令行接口	通过 Console 口进行本地配置 通过 AUX 口进行远程配置 通过 Telnet 或 SSH 进行本地或远程配置 配置命令分级保护，确保未授权用户无法配置设备 提供全中文的提示和帮助信息 详尽的调试信息，帮助诊断网络故障 提供网络测试工具，如 Tracert、Ping 命令等，迅速诊断网络是否正常 用 Telnet 命令直接登录并管理其它网络设备 FTP Server/Client，可以使用 FTP 下载、上载配置文件和应用程序 支持 TFTP 上传下载文件 支持日志功能 文件系统管理 User-interface 配置，提供对登录用户多种方式的认证和授权功能。
		支持标准网管 SNMPV3，并且兼容 SNMP V2C、SNMP V1 支持 BIMS 支持 VPN Manager 支持 NTP 时间同步

第2章 用户配置接口

2.1 配置环境搭建

系统支持用户进行本地与远程配置，搭建配置环境可通过以下几种方法实现：

2.1.1 通过 Console 口搭建

第一步：建立本地配置环境，只需将计算机（或终端）的串口通过标准RS-232 电缆与防火墙的Console口连接，如图 2-1所示。

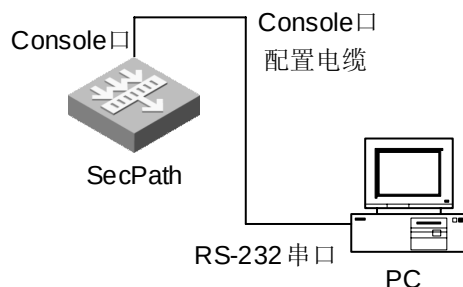


图2-1 通过 Console 口搭建本地配置环境

第二步：在计算机上运行终端仿真程序（如Windows 9X / Windows XP / Windows 2000 的超级终端等），设置终端通信参数为 9600bps、8 位数据位、1 位停止位、无奇偶校验和无流量控制，并选择终端类型为VT100，如图 2-2至 图 2-4所示。



图2-2 新建连接

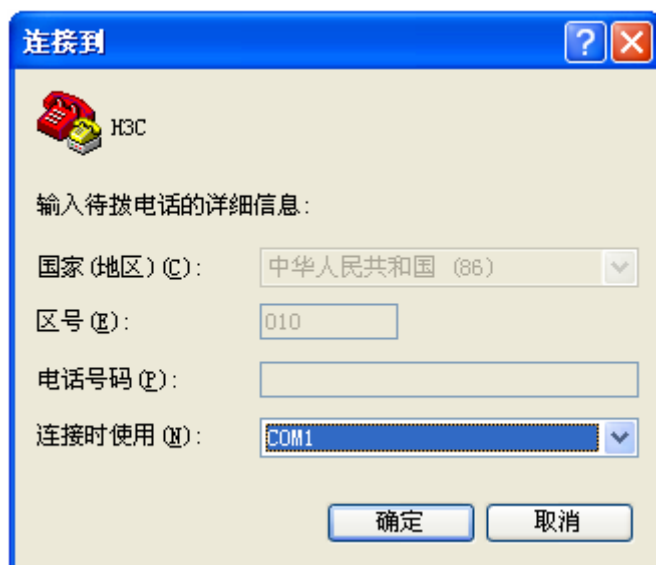


图2-3 连接端口设置

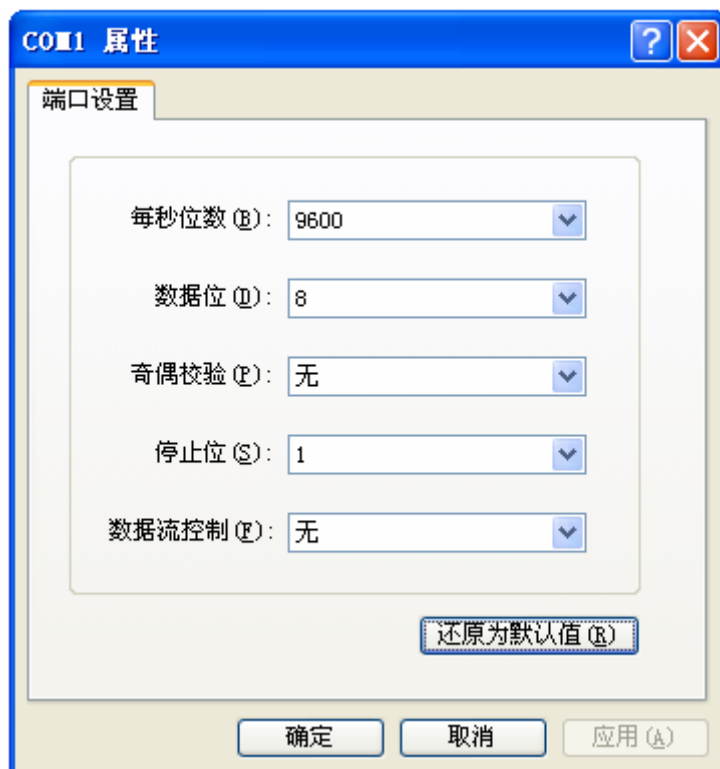


图2-4 端口通信参数设置

第三步：防火墙上电自检，系统自动进行配置，自检结束后提示用户键入回车，直到出现命令行提示符（如<SecPath>）。

第四步：键入命令，配置防火墙或查看防火墙运行状态，如需要帮助可以随时键入“？”，关于具体的命令请参考以后各章节。

2.1.2 通过 Telnet 搭建

如果不是防火墙第一次上电，而且用户已经正确配置了防火墙各接口的 IP 地址，并配置了正确的登录验证方式和访问控制规则，在配置终端与防火墙之间有可达路由前提下，可以用 Telnet 通过局域网或广域网登录到防火墙，然后对防火墙进行配置。

第一步：如图 2-5所示，建立本地配置环境，只需将计算机以太网口通过局域网与防火墙的以太网口连接；如果建立远程配置环境，如图 2-6所示，需要将计算机和防火墙通过广域网连接。

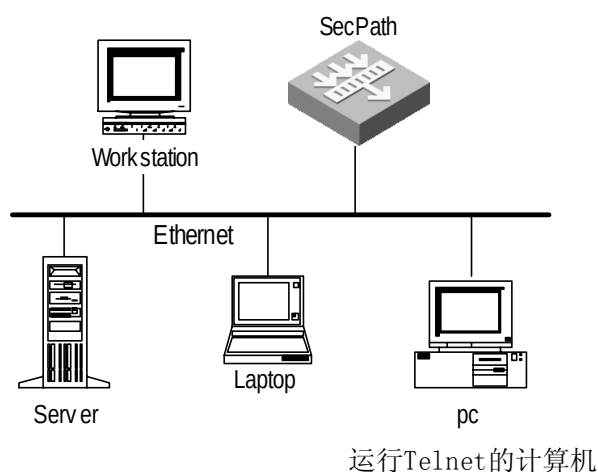


图2-5 通过局域网搭建本地配置环境

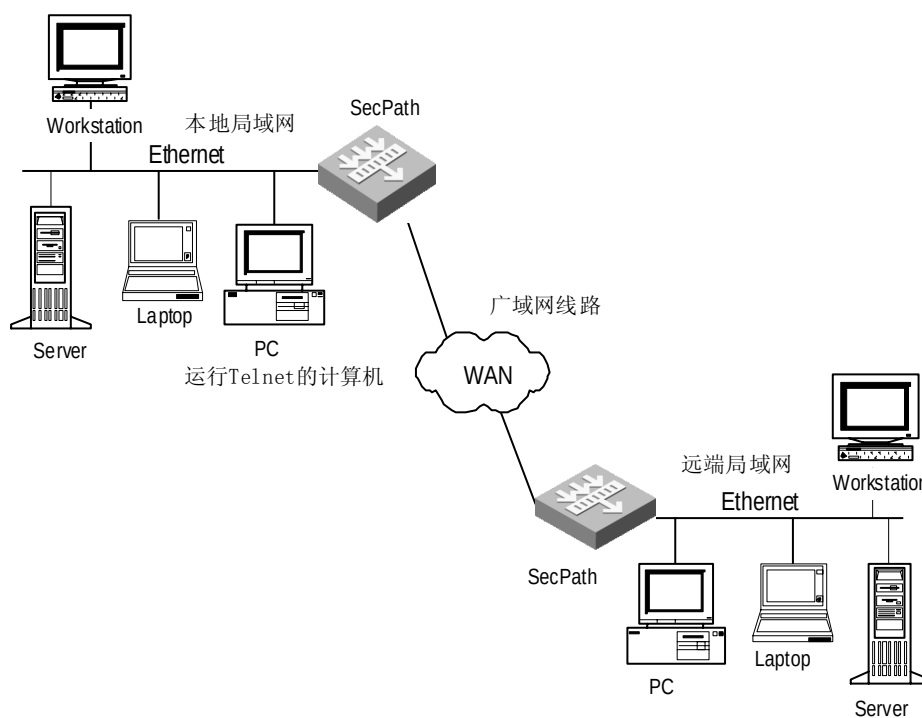


图2-6 通过广域网搭建远程配置环境

第二步：在计算机上运行Telnet程序，如 图 2-7所示。

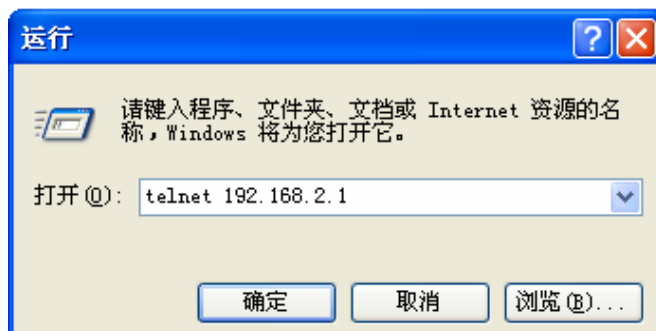


图2-7 运行 Telnet 程序并与防火墙建立 Telnet 连接

 说明：

不同操作系统的 Telnet 连接界面可能不同，上图仅作为参考示例。

第三步：与防火墙建立连接，认证通过后出现命令行提示符（如<SecPath>），如果出现 “All user interfaces are used, please try later!” 的提示，说明系统能够允许的 Telnet 用户已经达到上限，请待其他用户释放以后再连接。

第四步：键入命令，配置防火墙或查看防火墙运行状态，如需要帮助可以随时键入 “?”，关于具体的命令请参考以后各章节。

 说明：

通过 Telnet 配置防火墙时，请不要轻易改变防火墙的 IP 地址（由于修改可能会导致 Telnet 连接断开）。如有必要修改，须输入防火墙的新 IP 地址，重新建立连接。

2.1.3 通过 AUX 口拨号搭建

通过Modem拨号与防火墙的AUX口连接搭建配置环境，如 图 2-8所示，需要在计算机串口和防火墙的AUX口分别挂接Modem。

第一步：AUX 接口外接 Modem。

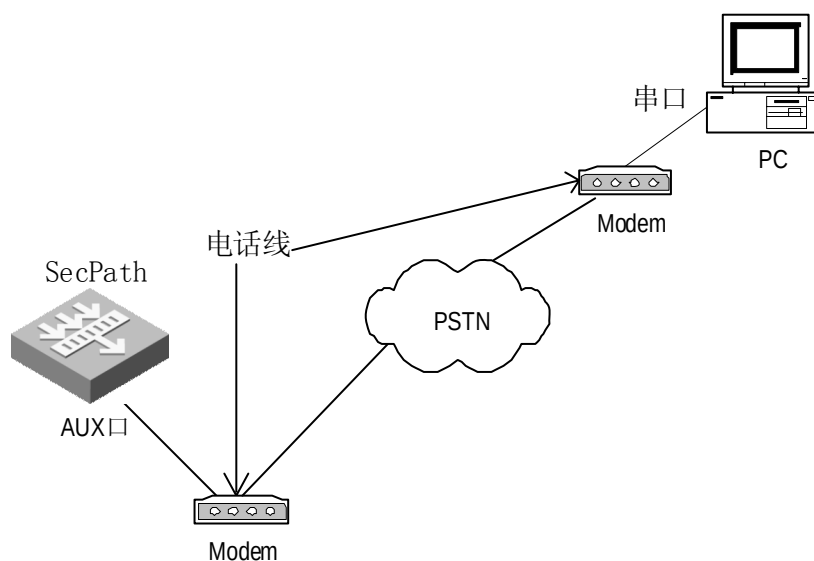


图2-8 搭建远程配置环境

第二步：在远端通过终端仿真程序（如Windows9X的Hyperterm（超级终端））向防火墙拨号，与防火墙建立连接。在终端仿真程序中选择实际连接时使用的PC的RS-232 串口，设置终端通信参数为 9600 波特率、8 位数据位、1 位停止位、无奇偶校验、无流量控制或硬件流量控制，并选择终端仿真类型为VT100——与通过Console口建立连接相同。如图 2-9、图 2-10所示。

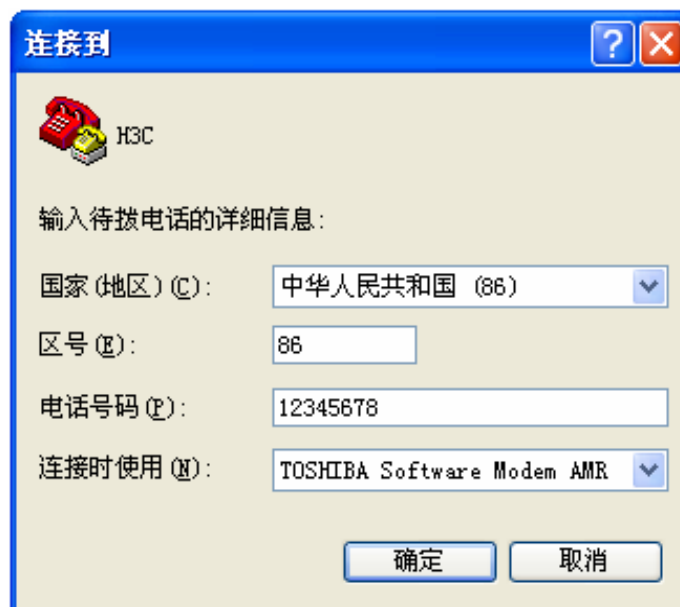


图2-9 拨号号码设置

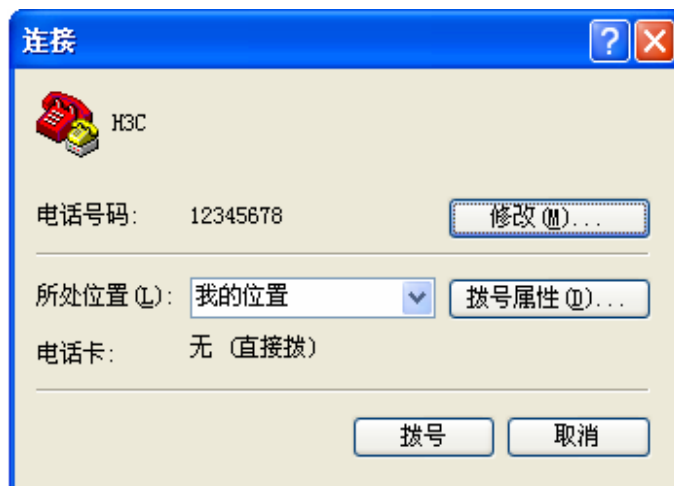


图2-10 在远地计算机上拨号

第三步：正确输入用户名和密码后，在远端的终端仿真程序上看到命令行提示符（如 <H3C>）后，即可对防火墙进行配置或管理。

2.1.4 通过 SSH 方式搭建

SSH 是 Secure Shell（安全外壳）的简称，用户通过一个不能保证安全的网络环境远程登录到防火墙时，SSH 特性可以提供安全的信息保障和强大的认证功能，以保护防火墙不受诸如 IP 地址欺诈、明文密码截取等攻击。防火墙可以同时接受多个 SSH 客户的连接。SSH 客户端允许用户与支持 SSH Server 的防火墙、UNIX 主机等建立 SSH 连接。搭建配置环境的方法和 Telnet 方式相似。

第一步：建立本地配置环境，只需将计算机以太网口通过局域网与防火墙的以太网口连接，也可以通过 HUB 或以太网交换机实现网络层互通；如果建立远程配置环境，需要将计算机和防火墙通过广域网连接。

第二步：在防火墙上配置SSH参数，具体请参见 第 14 章 终端服务。

第三步：在计算机上运行 SSH 客户端程序，并配置参数，包括远端防火墙 IP 地址、SSH 版本、RSA 私钥文件等，然后与防火墙建立连接后即可进行配置。

2.2 命令行接口

系统向用户提供一系列配置命令以及命令行接口，用户通过该接口可以配置和管理防火墙。命令行接口有如下特性：

- 通过 AUX 口进行本地或远程配置。
- 通过 Console 口进行本地配置。
- 通过 Telnet、SSH 进行本地或远程配置。
- 提供 User-interface 视图，管理各种终端用户的特定配置。

- 命令分级保护，不同级别的用户只能执行相应级别的命令。
- 通过本地、password、AAA 三种验证方式，确保未授权用户无法侵入防火墙，保证系统的安全。
- 用户可以随时键入“?”而获得在线帮助。
- 提供网络测试命令，如 **tracert**、**ping** 等，迅速诊断网络是否正常。
- 提供种类丰富、内容详尽的调试信息，帮助诊断网络故障。
- 用 **telnet** 命令直接登录并管理其它设备。
- 提供 FTP、TFTP 服务，方便用户上传、下载文件。
- 提供保存并执行历史命令的功能。
- 命令行解释器提供不完全匹配和上下文关联等多种智能命令解析方法，最大可能地方便用户的输入。

2.2.1 命令行视图

系统命令行采用分级保护方式，命令行划分为参观级、监控级、系统级、管理级 4 个级别，简介如下：

- 参观级：网络诊断工具命令（**ping**、**tracert**）、从本设备出发访问外部设备的命令（如 **Telnet** 客户端）等，该级别命令不允许进行配置文件保存的操作。
- 监控级：用于系统维护、业务故障诊断等，包括 **display**、**debugging** 命令，该级别命令不允许进行配置文件保存的操作。
- 系统级：业务配置命令，包括路由、各个网络层次的命令，这些用于向用户提供直接网络服务。
- 管理级：关系到系统基本运行，系统支撑模块的命令，这些命令对业务提供支撑作用，包括文件系统、FTP、TFTP、配置文件切换命令、电源控制命令、备板控制命令、用户管理命令、级别设置命令、系统内部参数设置命令（非协议规定、非 RFC 规定）等。

同时对登录用户划分等级，分为 4 级，分别与命令级别对应，即不同级别的用户登录后，只能使用等于或低于自己级别的命令。

为了防止未授权用户的非法侵入，在从低级别用户切换到高级别用户时，要进行用户身份验证，即需要输入高级别用户口令（如果用户设置了 **super password [level user-level] { simple | cipher } text**）。为了保密，用户键入的口令在屏幕上不作显示，如果三次以内输入正确的口令，则切换到高级别用户，否则保持原用户级别不变。

各命令视图是针对不同的配置要求实现的，它们之间有联系又有区别，比如，与防火墙建立连接即进入用户视图，它只完成查看运行状态和统计信息的简单功能，再

键入 **system-view** 进入系统视图，在系统视图下，键入不同的配置命令进入相应的协议、接口等视图。

命令行提供多种命令视图，以下只列出其中的部分视图：

- 用户视图
- 系统视图
- 路由协议视图，包括 OSPF 协议视图、RIP 协议视图、BGP 协议视图等。
- 接口视图，包括快速以太网接口视图、千兆以太网接口（GE）视图、以太网子接口视图、加密卡接口视图、虚拟模板接口视图、Dialer 接口视图、Loopback 接口视图、Null 接口视图、Tunnel 接口视图等。
- 用户界面视图
- L2TP 组视图
- 路由策略视图

各命令视图的功能特性、进入各视图的命令等的细则如表 2-1 所示：

表2-1 命令视图功能特性列表

命令视图	功能	提示符	进入命令	退出命令
用户视图	查看防火墙的简单运行状态和统计信息	<H3C>	与防火墙建立连接即进入	quit 断开与防火墙连接
系统视图	配置系统参数	[H3C]	在用户视图下键入 system-view	quit 返回用户视图
用户界面视图	管理防火墙的异步和逻辑接口	[H3C-ui0]	在系统视图下键入 user-interface 0	quit 返回系统视图
OSPF 协议视图	配置 OSPF 协议参数	[H3C-ospf]	在系统视图下键入 ospf	quit 返回系统视图
RIP 协议视图	配置 RIP 协议参数	[H3C-rip]	在系统视图下键入 rip	quit 返回系统视图
BGP 协议视图	配置 BGP 协议参数	[H3C-bgp]	在系统视图下键入 bgp 1	quit 返回系统视图
以太网口视图	配置以太网口参数	[H3C-Ethernet1/0/0]	在系统视图下键入 Interface ethernet 1/0/0	quit 返回系统视图
子接口视图	配置子接口参数	[H3C-Ethernet1/0/0.1]	在系统视图下键入 interface Ethernet 1/0/0.1	quit 返回系统视图
AUX 口视图	配置 AUX 口参数	[H3C-aux0]	在系统视图下键入 interface aux 0	quit 返回系统视图

命令视图	功能	提示符	进入命令	退出命令
虚拟模板接口视图	配置虚拟模板接口参数	[H3C-virtual-template0]	在系统视图下键入 interface virtual-template 0	quit 返回系统视图
Loopback 接口视图	配置 Loopback 接口参数	[H3C-Loopback 2]	在系统视图下键入 interface loopback 2	quit 返回系统视图
NULL 接口视图	配置 Null 接口参数	[H3C-NULL0]	在系统视图下键入 interface null 0	quit 返回系统视图
L2TP 组视图	配置 L2TP 组	[H3C-l2tp1]	在系统视图下键入了 l2tp-group 1	quit 返回系统视图
route-policy 视图	配置 BGP route-policy	[H3C-route-policy]	在系统视图下键入 route-policy test node permit node 10	quit 返回系统视图

说明：

命令行提示符以防火墙名称（缺省为 H3C）作前缀，视图名作后缀，括号中表明当前的视图，“<>”表示用户视图，“[]”表示系统视图和其它配置视图。

2.2.2 命令行在线帮助

命令行接口提供如下几种在线帮助：

- 完全帮助
- 部分帮助

通过上述各种在线帮助能够获取到帮助信息，分别描述如下：

(1) 在任一命令视图下，键入“?”获取该命令视图下所有的命令及其简单描述。

```
<H3C> ?
```

(2) 键入一命令，后接以空格分隔的“?”，如果该位置为关键字，则列出全部关键字及其简单描述。

```
<H3C> display ?
```

(3) 键入一命令，后接以空格分隔的“?”，如果该位置为参数，则列出有关的参数描述。

```
[H3C] interface ethernet ?
```

```
<3-3> Slot number
```

```
[H3C] interface ethernet 3?  
/  
[H3C] interface ethernet 3/?  
<0-0>  
[H3C] interface ethernet 3/0?  
/  
[H3C] interface ethernet 3/0/?  
<0-0>  
[H3C] interface ethernet 3/0/0 ?  
<cr>
```

其中<cr>表示该位置无参数，直接键入回车即可执行。

(4) 键入一字符串，其后紧接“？”，列出以该字符串开头的命令。

```
<H3C> d?  
debugging delete dir display
```

(5) 键入一命令，后接一字符串紧接“？”，列出命令以该字符串开头的关键字。

```
<H3C> display h?  
history-command hotkey
```

(6) 输入命令的某个关键字的前几个字母，按下<Tab>键，可以显示出完整的关键字。如果这几个字母不能唯一标示出该关键字，系统依次显示出以这几个字母所开头的命令。

(7) 所有命令的描述信息均可通过执行 **language-mode chinese** 命令切换为中文显示。

说明：

当在某视图下配置命令时，若在当前视图匹配不到相应的命令，则会到更高级别的视图下去匹配。如果匹配成功，则转到相应的视图下处理。例如，当在 OSPF 视图下执行 **interface** 命令时，由于在 OSPF 视图下匹配不到 **interface** 命令，则系统将在更高级别的视图（即系统视图）下处理，并进入相应的接口视图，如下所示。

```
[H3C] ospf  
[H3C-ospf-1] interface Ethernet 0/0/0  
[H3C-Ethernet0/0/0]
```

2.2.3 命令行错误信息

所有用户键入的命令，如果通过语法检查，则正确执行。否则，向用户报告错误信息，常见错误信息参见表 2-2。

表2-2 命令行常见错误信息表

英文错误信息	错误原因
Unrecognized command	没有查找到命令
	没有查找到关键字
	参数类型错
	参数值越界
Incomplete command	输入命令不完整
Too many parameters	输入参数太多
Ambiguous command	输入参数不明确

2.2.4 历史命令

命令行接口提供历史命令自动保存功能，用户可以随时调用命令行接口保存的历史命令，并重复执行。在缺省状态下，命令行接口为每个用户最多可以保存 10 条历史命令。操作如表 2-3所示。

表2-3 访问历史命令

操作	按键	结果
显示历史命令	display history-command	显示用户键入的历史命令
访问上一条历史命令	上光标键或者<Ctrl+P>	如果还有更早的历史命令，则取出上一条历史命令，否则响铃警告
访问下一条历史命令	下光标键或者<Ctrl+N>	如果还有更晚的历史命令，则取出下一条历史命令，否则清空命令，响铃警告

说明：

用光标键对历史命令进行访问，在 Windows 3.X 的 Terminal 和 Telnet 下都是有效的，但对于 Windows 9X 的超级终端，↑ 光标键会无效，这是由于 Windows 9x 的超级终端对这个键作了不同解释所致，这时可以用组合键<Ctrl+P>来代替↑ 光标键达到同样目的。

2.2.5 编辑特性

命令行接口提供了基本的命令编辑功能，支持多行编辑，每条命令的最大长度为 256 个字符，如表 2-4所示。

表2-4 编辑功能表

按键	功能
普通按键	若编辑缓冲区未满，则插入到当前光标位置，并向右移动光标，否则，响铃告警。
退格键 BackSpace	删除光标位置的前一个字符，光标前移，若已经到达命令首，则响铃告警。
左光标键←或<Ctrl+B>	光标向左移动一个字符位置，若已经到达命令首，则响铃告警。
右光标键→或<Ctrl+F>	光标向右移动一个字符位置，若已经到达命令尾，则响铃告警。
Tab 键	输入不完整的关键字后按下 Tab 键，系统自动执行部分帮助：如果与之匹配的关键字唯一，则系统用此完整的关键字替代原输入并换行显示；对于命令字的参数、不匹配或者匹配的关键字不唯一的情况，系统不作任何修改，重新换行显示原输入。

2.2.6 显示特性

命令行接口提供了如下的显示特性：

1. 切换语言模式

防火墙的帮助信息可以查看英文，也可以查看中文，可以在中英文之间切换。

请在用户视图使用下面的操作。

表2-5 切换语言模式

操作	命令
切换为英文模式	language-mode english
切换为中文模式	language-mode chinese

2. 暂停功能

在一次显示信息超过一屏时，提供了暂停功能，这时用户可以有三种选择，如 表 2-6 所示。

表2-6 显示功能表

按键或命令	功能
暂停显示时键入<Ctrl+C>	停止显示和命令执行
暂停显示时键入空格键	继续显示下一屏信息
暂停显示时键入回车键	继续显示下一行信息

3. 显示信息的输出

系统提供了大量的 **display** 命令，用于显示系统状态信息。在输出显示信息时，可以在命令中加入 “|” 对输出的信息进行筛选，有 3 个可选项，如下：

- **begin text**: 从匹配 **text** 的行开始显示。
- **exclude text**: 显示不包含 **text** 的行。
- **include text**: 显示包含 **text** 的行。

例如：输入命令 **display current-configuration | include ip**，将显示包含 **ip** 的行的配置信息。

2.2.7 正则表达式的使用

1. 正则表达式的介绍

正则表达式是一种可用于模式匹配和替换的工具，它的功能强大，使用也很灵活。在实际应用中，正则表达式已经超出了某种语言或某个系统的局限，成为人们广为接受的概念和功能。

在使用正则表达式时，用户需要根据一定的规则构建匹配模式，然后将匹配模式与目标对象进行匹配。最简单的正则表达式不包含任何元字符，例如，可以规定一个正则表达式 **hello**，它只匹配字符串 “**hello**”。

为帮助用户灵活地构建匹配模式，正则表达式提供了一些具有特殊含义的专用字符，也称为“元字符”（**metacharacter**），用来规定其它字符在目标对象中的出现模式。下表是对元字符的使用描述。

表2-7 元字符描述

元字符	含义
\	转义字符
.	匹配除 “\n” 之外任何单个字符，包括空格
*	之前的字符在目标对象中出现 0 次或连续多次
+	之前的字符在目标对象中出现 1 次或连续多次
	竖线左边和右边的字符为 “或” 的关系
^	之后的字符必须出现在目标对象的开始
\$	之前的字符必须出现在目标对象的结束
[xyz]	匹配方括号内列出的任意字符
[^xyz]	匹配除了方括号内列出的字符外的任意字符（^号在字符前）
[a-z]	匹配指定范围内的任意字符
[^a-z]	匹配不在指定范围内的任意字符
{n}	n 是一个非负整数，表示一次可以匹配连续出现 n 次的字符

元字符	含义
{n}	n 是一个非负整数，表示一次可以匹配连续出现的至少 n 次的字符
{n,m}	m 和 n 均为非负整数， $n \leq m$ 。匹配连续出现的次数为 n~m 次。使用时注意，逗号与 n 和 m 之间不能有空格

例如：

`^ip`：匹配以字符串“ip”开始的目标对象。

`ip$`：匹配以字符串“ip”结束的目标对象。

2. 正则表达式的使用

当有大量信息输出时，可以通过正则表达式来选择需要显示的内容，过滤掉不关心的内容。

(1) 在命令中指定过滤方式

进行过滤输出时，有三种类型的过滤可供选择，在支持正则表达式的命令中，这三种选择的表达方式分别为 `{ begin | exclude | include } regular-expression`：

- **begin**：输出以匹配指定正则表达式的行开始的所有行。
- **exclude**：输出不匹配指定正则表达式的所有行。
- **include**：只输出匹配指定正则表达式的所有行。

(2) 在分屏显示时指定过滤方式

当输出的内容非常多，并采用分屏显示时，可以在分屏提示符“---- More ----”中指定过滤类型：

- `/regular-expression`：输出以匹配指定正则表达式的行开始的所有行。
- `-regular-expression`：输出不匹配指定正则表达式的所有行。
- `+regular-expression`：只输出匹配指定正则表达式的所有行。

例如：查看当前配置信息

```
<H3C> display current-configuration
#
 sysname H3C
#
interface Ethernet0/2/0
 description Don't change the configuration please
 ip address 10.110.98.137 255.255.255.0
#
interface Ethernet1/0/0
#
interface Ethernet1/2/0
```

```
#
interface NULL0

当出现分屏提示符“---- More ----”时，用户可以手工输入正则表达式，对待显示的内容进行过滤，在本例中，指定只输出含有字符串“interface”的行：

---- More ----
+interface                                由用户手工输入

filtering
interface LoopBack0
user-interface con 0
user-interface vty 0 14
<H3C>
```

2.3 快捷键

2.3.1 快捷键的分类

系统中的快捷键可以分成两类。

一类是提供给用户的、可以自由定义的快捷键，共有 5 个。其中包括：CTRL_G、CTRL_L、CTRL_O、CTRL_T、CTRL_U。用户可以根据自己的需要将这 5 个快捷键与任意命令进行关联，当键入快捷键时，系统将自动执行它所对应的命令。

另一类我们称其为系统快捷键，是系统中固定的。这种快捷键不能由用户自由定义，他们代表固定的功能。系统主要包括的快捷键如下表。

表2-8 系统快捷键

按键或命令	功能
CTRL_A	将光标移动到当前行的开头
CTRL_B	将光标向左移动一个字符
CTRL_C	停止当前正在执行的功能
CTRL_D	删除当前光标所在位置的字符
CTRL_E	将光标移动到当前行的末尾
CTRL_F	将光标向右移动一个字符
CTRL_H	删除光标左侧的一个字符
CTRL_K	终止呼出的连接
CTRL_N	显示历史命令缓冲区中的后一条命令
CTRL_P	显示历史命令缓冲区中的前一条命令
CTRL_R	重新显示当前行信息

按键或命令	功能
CTRL_W	删除光标左侧的单词
CTRL_X	删除光标左侧所有的字符
CTRL_Y	删除光标右侧所有的字符
CTRL_Z	返回到用户视图
CTRL_]	终止呼入的连接或重定向连接
ESC_B	将光标向左移动一个单词
ESC_D	删除光标右侧的单词
ESC_F	将光标向右移动一个单词
ESC_<	将光标所在位置指定为剪贴板的开始位置
ESC_>	将光标所在位置指定为剪贴板的结束位置

2.3.2 快捷键的使用

- 在任何允许输入命令的地方都可以键入快捷键，系统执行时，会将该快捷键对应的命令显示在屏幕上，如同输入了完整的命令一样。
- 如果用户已经输入了命令的一部分，但是还没有键入回车以确认，此时键入快捷键将会把以前输入的字符全部清空，并将该快捷键对应的命令显示在屏幕上，效果与用户删除所有的输入，然后重新敲入完整的命令一样。
- 快捷键的执行与命令一样，也会将命令原形记录在命令缓冲区和日志中以备问题定位和查询。

 说明：

快捷键的功能可能受用户所用的终端影响，例如用户终端本身自定义的快捷键与防火墙系统中的快捷键功能发生冲突，此时如果用户键入快捷键将会被终端程序截获而不能执行它所对应的命令行。

请在系统视图下进行下列配置。

表2-9 定义快捷键

操作	命令
定义快捷键	<code>hotkey { CTRL_G CTRL_L CTRL_O CTRL_T CTRL_U } command_text</code>
恢复系统的默认值	<code>undo hotkey { CTRL_G CTRL_L CTRL_O CTRL_T CTRL_U }</code>

缺省情况下，系统给 CTRL_G、CTRL_L、CTRL_O 三个快捷键指定了默认值，其它快捷键默认值为空。分别为：

CTRL_G 对应命令 **display current-configuration**（显示当前配置）；

CTRL_L 对应命令 **display ip routing-table**（显示路由表信息）；

CTRL_O 对应命令 **undo debugging all**（停止所有调试信息的输出）。

请在所有视图下进行下列配置。

表2-10 显示快捷键的使用情况

操作	命令
显示快捷键的使用情况	display hotkey

2.3.3 快捷键使用举例

定义快捷键 CTRL_U，与命令 **display ip routing-table** 进行关联，并执行。

```
[SecPath] hotkey ctrl_u display ip routing-table
```

在提示符[H3C]下键入快捷键<Ctrl+U>即显示。

```
[H3C] display ip routing-table
```

```
Routing Table: public net
```

Destination/Mask	Proto	Pre	Cost	Nextthop	Interface
127.0.0.0/8	DIRECT	0	0	127.0.0.1	InLoopBack0
127.0.0.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0

2.3.4 配置命令行别名

通过配置命令行别名，可以满足用户将 **Comware** 的常用命令替换为自己惯用命令形式的要求。对命令行别名需求，在用户使用中有以下约定：

- (1) 当查看历史命令信息、当前配置信息以及保存配置信息时，用户输入的带别名的命令将以系统原始的命令形式被显示或存储，而不会以别名的形式。即用户的别名命令可以使用，但不会参与配置恢复。
- (2) 在用户启动别名功能的情况下，当用户输入不完整关键字，且该关键字与用户已匹配的别名以及现有某关键字同时部分匹配时，以别名替换优先。用户想输入现有关键字对应的命令需要完整输入该关键字。如果用户输入的字符串与多个所设置的别名部分匹配，则输出歧义匹配信息。
- (3) 当用户对别名关键字使用 **TAB** 键时，若该别名不存在歧义别名将联想出所对应的原始关键字。
- (4) 不支持对整个命令行的替换。只支持对第一关键字的别名设置，以及 **undo** 命令的第二关键字的别名替换。

1. 使能命令行别名功能

请在系统视图下配置下面命令。

表2-11 使能命令行别名功能

操作	命令
使能命令行别名功能	command-alias enable
关闭命令行别名功能	undo command-alias enable

缺省情况下，命令行别名功能是被关闭的。

2. 配置用户指定的命令行别名

请在系统视图下配置下面命令。

表2-12 使能命令行别名功能

操作	命令
配置用户指定的命令行别名	command-alias mapping <i>cmdkey alias</i>
取消用户设置的别名	undo command-alias mapping <i>alias</i>

缺省情况下，没有配置命令行别名。

3. 显示和调试

在任意视图下均可配置下面命令。

表2-13 显示和调试

操作	命令
显示当前用户设置别名的情况	display command-alias

第3章 Comware 的基本配置

3.1 进入和退出系统视图

在从 Console 口登录到防火墙后，即进入用户视图，此时屏幕显示的提示符是：<H3C>。进入和退出系统视图，可以使用如下的操作。

表3-1 进入和退出系统视图

操作	命令
从用户视图进入系统视图	system-view
从系统视图返回到用户视图	quit
从任意的非用户视图返回到用户视图	return

命令 **quit** 的功能是返回上一层视图，在用户视图下执行 **quit** 命令就会退出系统。**return** 命令的功能也可以用组合键<Ctrl+Z>完成。

3.2 设置防火墙的名称

防火墙的名称出现在命令提示符中，用户可以根据需要更改防火墙的名称。
请在系统视图下进行下面的操作。

表3-2 设置防火墙的名称

操作	命令
设置防火墙的名称	sysname sysname

3.3 设置系统时钟

为了保证与其他设备协调工作，需要准确设置系统的时间。
请在用户视图下进行下面的操作。

表3-3 设置系统时钟

操作	命令
设置标准时间	clock datetime time date
设置所在的时区	clock timezone time-zone-name { add minus } time

操作	命令
取消时区设置	undo clock timezone
设置采用夏时制	clock summer-time <i>summer-time-zone-name</i> { one-off repeating } <i>start-time start-date end-time end-date add-time</i>
取消夏时制	undo clock summer-time

3.4 设置提示信息

提示信息是用户在连接到防火墙、进行登录验证以及开始交互配置时系统显示的一段提示信息。

请在系统视图下进行下面的操作。

表3-4 设置提示信息

操作	命令
设置登录终端用户界面时的提示信息	header incoming <i>text</i>
设置登录验证时的提示信息	header login <i>text</i>
设置进入用户视图时的提示信息	header shell <i>text</i>
取消设置的提示信息	undo header { incoming login shell }

3.5 切换用户级别

1. 配置切换用户级别的口令

如果用户以较低级别的身份登录到防火墙后，需要切换到较高级别的用户身份上进行操作，需要输入用户级别的口令。该口令需要事先配置。

请在系统视图下进行如下操作。

表3-5 配置切换用户级别的口令

操作	命令
配置切换用户级别的口令	super password [level <i>user-level</i>] { simple cipher } <i>password</i>
取消配置的口令	undo super password [level <i>user-level</i>]

缺省情况下，若不指定级别，则设置的为切换到 3 级的密码。

2. 切换用户级别

要从较低级别用户切换到较高级别的用户，需要输入正确的口令。

请在用户视图下进行如下操作。

表3-6 切换用户级别

操作	命令
切换用户级别	super [<i>level</i>]

缺省情况下，若不指定级别，则切换到 3 级。

关于用户级别的配置请参见 第 9 章 用户管理

3.6 锁定用户界面

在用户需要暂时离开操作终端时，为防止未授权的用户操作该终端界面，可以锁定用户界面，锁定用户界面时，需要输入口令并确认口令。在解除锁定时，只有输入正确的口令才能操作用户界面。

请在用户视图下进行下列操作。

表3-7 锁定用户界面

操作	命令
锁定用户界面	lock

3.7 设置命令级别

所有命令分为参观（Visit）、监控（Monitor）、系统（System）、管理（Manage）4 个级别，级别标识为 0~3。系统管理员可以根据需要指定命令的级别及其所在视图。

请在系统视图下进行下列配置。

表3-8 命令优先级的设置

操作	命令
设置视图中命令的优先级	command-privilege level <i>level</i> view <i>view</i> <i>command-key</i>
恢复命令的缺省优先级	undo command-privilege view <i>view</i> <i>command-key</i>

表3-9 缺省的命令优先级

级别	名称	命令
0	参观	ping、tracert、telnet
1	监控	display、debugging
2	配置	所有配置命令（管理级的命令除外）
3	管理	文件系统命令、FTP 命令、TFTP 命令、SNMP 命令、XMODEM 命令等

 说明：

所有的命令都有默认的视图和优先级，一般不需要用户进行重新设置。

3.8 显示系统状态信息

利用 **display** 命令可以收集系统状态信息，根据功能可以划分为以下几类：

- 显示系统配置信息的命令
- 显示系统运行状态的命令
- 显示系统统计信息的命令

有关各协议和各种接口的 **display** 命令请参见相关章节。下面只介绍一些有关系统的 **display** 命令。

请在所有视图下进行下列操作。

表3-10 显示系统状态信息

操作	命令
显示系统版本信息	display version
显示详细的软件版本信息	vrbd
显示系统时钟	display clock
显示终端用户	display users [all]
显示起始配置信息	display saved-configuration
显示当前配置信息	display current-configuration
显示调试开关状态	display debugging [interface interface-type interface-number] [module-name]
显示当前视图的运行配置	display this
显示技术支持信息	display diagnostic-information
显示剪贴板的内容	display clipboard

操作	命令
显示当前系统内存使用情况	display memory [<i>limit</i>]
显示 CPU 占用率的统计信息	display cpu-usage [<i>configuration</i> <i>number</i> [<i>offset</i>] [<i>verbose</i>] [<i>from-device</i>]]
设置 CPU 占用率统计的周期	cpu-usage cycle { <i>5sec</i> <i>1min</i> <i>5min</i> <i>72min</i> }
以图形方式显示 CPU 占用率统计历史信息	display cpu-usage history [<i>task task-id</i>]

在系统出现故障或日常维护时，为了便于问题定位，需要收集很多的信息，但相应的 **display** 命令很多，很难一次把信息收集全，这时可以使用 **display diagnostic-information** 命令进行系统当前各个模块的运行信息收集。

display diagnostic-information 命令一次性收集了配置如下命令后终端显示的信息，包括：**display clock**、**display version**、**vrbd**、**display current-configuration**、**display saved-configuration**、**display interface**、**display ip interface**、**display ip statistics**、**display logbuffer** 等等。

第4章 系统维护管理

4.1 系统维护与调试

4.1.1 网络连接的测试工具

1. ping

ping 主要用于检查网络连接及主机是否可达。

请在任何视图下进行操作。

表4-1 ping 命令

操作	命令
支持 IP 协议 ping	ping [-a X.X.X.X] [-c count] [-d] [-f] [-h ttl_value] [-i interface-type interface-number] [ip] [-n] [-p pattern] [-q] [-r] [-s packetsize] [-t timeout] [-tos] [-v] [-vpn-instance vpn-instance-name] host

各选项及参数意义详见命令手册 **ping** 命令章节。

命令执行结果输出包括：

- 对每个 **ping** 报文的响应情况，如果在超时时间到后仍没有收到响应报文，则输出“Request time out”，否则显示响应报文中数据字节数、报文序号、TTL 和响应时间等。
- 最后的统计信息，包括发送报文数、接收报文数、未响应报文百分比和响应时间的最小、平均和最大值。

```
<H3C> ping 202.38.160.244
PING 202.38.160.244 : 56 data bytes, press CTRL_C to break
Reply from 202.38.160.244 : bytes=56 Sequence=1 ttl=255 time = 1ms
Reply from 202.38.160.244 : bytes=56 Sequence=2 ttl=255 time = 2ms
Reply from 202.38.160.244 : bytes=56 Sequence=3 ttl=255 time = 1ms
Reply from 202.38.160.244 : bytes=56 Sequence=4 ttl=255 time = 3ms
Reply from 202.38.160.244 : bytes=56 Sequence=5 ttl=255 time = 2ms
--202.38.160.244 ping statistics--
5 packets transmitted
5 packets received
0.00% packet loss
round-trip min/avg/max = 1/2/3 ms
```

2. tracert

tracert 用于测试数据包从发送主机到目的地所经过的网关，它主要用于检查网络连接是否可达，以及分析网络什么地方发生了故障。

tracert 的执行过程是：首先发送一个 TTL 为 1 的数据包，因此第一跳发送回一个 ICMP 错误消息以指明此数据包不能被发送（因为 TTL 超时），之后此数据包被重新发送，TTL 为 2，同样第二跳返回 TTL 超时，这个过程不断进行，直到到达目的地。执行这些过程的目的是记录每一个 ICMP TTL 超时消息的源地址，以提供一个 IP 数据包到达目的地所经历的路径。

请在任何视图下进行下列操作。

表4-2 tracert 命令

操作	命令
测试数据包从发送主机到目的地所经过的网关	tracert [-a X.X.X.X] [-f <i>first_TTL</i>] [-m <i>max_TTL</i>] [-p <i>port</i>] [-q <i>nqueries</i>] [vpn-instance <i>vpn-instance-name</i>] [-w <i>timeout</i>] * <i>host</i>

该命令各选项及参数意义详见命令手册 **tracert** 命令章节。

下面是应用 **tracert** 分析网络情况的例子。

例 1:

```
<H3C> tracert 35.1.1.48
tracert to nis.nsf.net(35.1.1.48) 30 hops max,40 bytes packet
press CTRL_C to break
1  helios.ee.lbl.gov (128.3.112.1)  19 ms  19 ms  0 ms
2  lilac-dmc.Berkeley.EDU (128.32.216.1)  39 ms  39 ms  19 ms
3  ccngw-ner-cc.Berkeley.EDU (128.32.136.23)  39 ms  40 ms  39 ms
4  ccn-nerif22.Berkeley.EDU (128.32.168.22)  39 ms  39 ms  39 ms
5  128.32.197.4 (128.32.197.4)  40 ms  59 ms  59 ms
6  131.119.2.5 (131.119.2.5)  59 ms  59 ms  59 ms
7  129.140.70.13 (129.140.70.13)  99 ms  99 ms  80 ms
8  129.140.71.6 (129.140.71.6)  139 ms  239 ms  319 ms
9  129.140.81.7 (129.140.81.7)  220 ms  199 ms  199 ms
10 nic.merit.edu (35.1.1.48)  239 ms  239 ms  239 ms
```

从上面结果可以看出，从源主机到目的地都经过了哪些网关，这对于网络分析是非常有用的。

例 2:

```
<H3C> tracert 18.26.0.115
tracert to allspice.lcs.mit.edu(18.26.0.115) 30 hops max,40 bytes packet
press CTRL_C to break
1  helios.ee.lbl.gov (128.3.112.1)  0 ms  0 ms  0 ms
```

```
2 lilac-dmc.Berkeley.EDU (128.32.216.1) 19 ms 19 ms 19 ms
3 lilac-dmc.Berkeley.EDU (128.32.216.1) 39 ms 19 ms 19 ms
4 ccngw-ner-cc.Berkeley.EDU (128.32.136.23) 19 ms 39 ms 39 ms
5 ccn-nerif22.Berkeley.EDU (128.32.168.22) 20 ms 39 ms 39 ms
6 128.32.197.4 (128.32.197.4) 59 ms 119 ms 39 ms
7 131.119.2.5 (131.119.2.5) 59 ms 59 ms 39 ms
8 129.140.70.13 (129.140.70.13) 80 ms 79 ms 99 ms
9 129.140.71.6 (129.140.71.6) 139 ms 139 ms 159 ms
10 129.140.81.7 (129.140.81.7) 199 ms 180 ms 300 ms
11 129.140.72.17 (129.140.72.17) 300 ms 239 ms 239 ms
12 * * *
13 128.121.54.72 (128.121.54.72) 259 ms 499 ms 279 ms
14 * * *
15 * * *
16 * * *
17 * * *
18 ALLSPICE.LCS.MIT.EDU (18.26.0.115) 339 ms 279 ms 279 ms
```

从上述结果中可以看出，从源主机到目的主机经过了哪些网关，以及哪些网关出现了故障。

4.1.2 系统调试功能

系统的命令行接口提供了种类丰富的调试功能，对于防火墙所支持的各种协议和功能，基本上都提供了相应的调试功能，帮助用户对错误进行诊断和定位。

调试信息的输出可以由两个开关控制：

- 协议调试开关，控制是否输出某协议的调试信息。
- 屏幕输出开关，控制是否在某个用户屏幕上输出调试信息。

二者关系如下图所示。

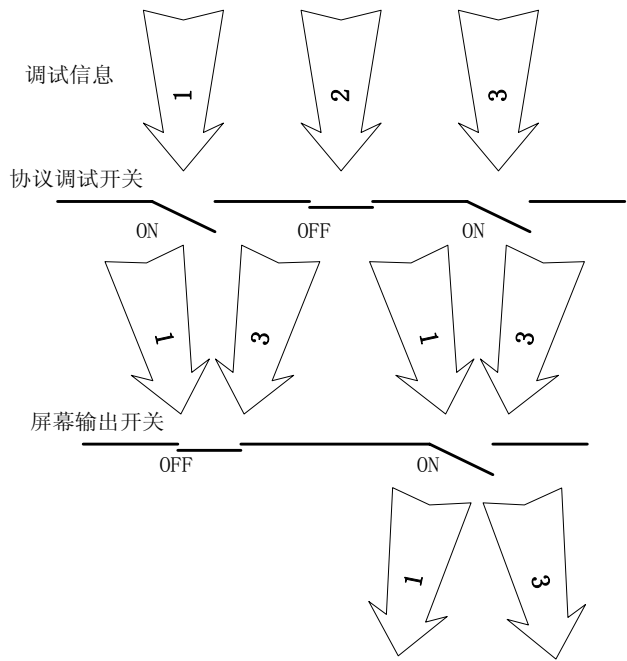


图4-1 调试信息输出示意图

协议调试开关由 **debugging** 控制，请在用户视图下进行下列配置。

表4-3 调试开关的打开、关闭和显示

操作	命令
打开协议调试开关	debugging { <i>all</i> <i>module-name</i> [<i>debug-option1</i>] [<i>debug-option2</i>] ... }
关闭协议调试开关	undo debugging { <i>all</i> <i>module-name</i> [<i>debug-option1</i>] [<i>debug-option2</i>] ... }
显示已经打开的调试开关	display debugging [<i>interface interface-type</i> <i>interface-number</i>] [<i>module-name</i>]

具体调试命令的使用和调试信息的格式介绍，参见相关章节。

屏幕输出开关由信息中心控制，详细说明参见下节。

4.1.3 配置系统重启

在防火墙运行过程中，由于系统文件升级等原因，需要重启防火墙。这时，您可以对防火墙下电再上电，也可以使用 **reboot** 命令。

请在用户视图下进行下列配置。

表4-4 配置系统重启

操作	命令
直接重新启动防火墙	reboot
使能定时重启功能，并设置具体的重启日期和时间	schedule reboot at time [date]
使能定时重启功能，并设定等待时延	schedule reboot delay { time minutes }
取消定时重启功能	undo schedule reboot
查看定时重启功能的配置信息	display schedule reboot

**注意：**

- 一般情况下，不要轻易重新启动系统，因为它将导致网络工作在短时间内瘫痪，另外在重启系统时，要确认是否需要保存系统当前的配置文件。
- 使用 **schedule reboot at** 命令设置系统的重启日期和时间后，若通过 **clock** 或 **NTP** 等方式修改了系统的时间，则 **schedule reboot at** 的设置将失效。
- 配置了 **schedule reboot at** 命令之后，将启动一个定时器，这个定时器是以分钟为单位的循环定时器。因此如果在 12: 05: 26 设置了 12: 06 重启，将在 12: 06: 26 秒重启，而不是 12: 06: 00 重启。

4.1.4 升级 BootROM

在系统运行过程中，可以使用 Flash Memory 中的 BootROM 程序升级防火墙上正在运行的 BootROM。可以在远端利用 FTP 或 TFTP 将 BootROM 上传到防火墙中，然后使用此命令升级 BootROM。

请在用户视图下进行下列配置：

表4-5 升级 BootROM

操作	命令
升级 BootROM	boot bootrom file-url

4.1.5 配置热插拔

在可靠性要求较高的应用环境中，热插拔特性可以在不影响业务的情况下，更换网络设备的插卡，确保业务可以不间断地运行。

在不支持热插拔的环境下，插卡必须随设备一起启动，且在设备运行过程中不能随意的插拔插槽中的插卡。这样，在插卡出现异常或者业务需求发生变化（例如需要更换插卡）的情况下，必须中断当前业务并重新启动系统，这对于需要长时间连续不间断运行的业务是不允许的。热插拔特性实现了在系统运行过程中可随意插拔插

卡的功能，并确保其他业务正常运行，同时对于同类型的板卡还具有业务恢复的功能。

请在用户视图下进行下列配置，可对设备中的插卡进行拔出预处理操作，之后就可以将插卡拔出并更换插卡。

表4-6 对插槽中的插卡进行拔出预处理

操作	命令
对插槽中的插卡进行拔出预处理	remove slot slot-id
取消拔出预处理操作	undo remove slot slot-id
显示设备和插卡的信息（任意视图）	display device [slot-id]

缺省情况下，未对插卡进行拔出预处理操作。



注意：

- 若在拔出插卡前，未使用 **remove slot** 命令对插卡进行拔出预处理操作，则设备可能会出现异常。
- 系统启动过程中，请勿进行插卡的插拔操作。
- 当前静态路由不支持插卡热插拔事件，即拔掉插卡后，相应的静态路由仍然存在，需要手工删除。
- 当前 **ftp source-interface** 命令、**ftp-server source-interface** 命令、**tftp source-interface** 命令、**telnet source-interface** 命令、**telnet-server source-interface** 命令、**ssh-server source-interface** 命令、**ssh2 source-interface** 命令、**sftp source-interface** 命令、Tunnel 接口下的 **source** 命令、HWPing 测试组视图下的 **source-interface** 命令、BGP 的 **peer connect-interface** 命令、路由策略视图下的 **if-match interface** 命令和 **apply output-interface** 命令不支持插卡热插拔事件，即拔掉插卡后，相应的配置仍然存在，需要手工删除。
- 目前，热插拔支持的插卡包括 1FE、2FE、4FE、1GBE、2GBE、1GEF、2GEF 插卡，不支持加密卡等其他类型的 PCI 插卡。

4.2 信息中心功能

4.2.1 信息中心简介

信息中心是防火墙主体软件中不可或缺的一部分，它作为防火墙的信息枢纽而存在。信息中心接管大多数的信息输出，并能进行细致的分类，从而能够有效地进行信息筛选。它通过与 Debug 程序的结合，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。

系统的信息中心具有以下一些特性：

- 信息中心共有三类信息：**log** 类（日志类信息）、**trap** 类（告警类信息）、**debug** 类（调试类信息）。
- 信息按重要性划分为八种等级，可按等级进行信息过滤。
- 系统支持十个通道，其中前六个通道（通道 0～通道 5）有缺省通道名，并且这六个通道缺省的与六个输出方向相关联，可以通过命令改变通道名，也可以改变通道与输出方向之间的关联。
- 支持控制台（**console**）、Telnet 终端和配置终端（**monitor**）、日志缓冲区（**logbuffer**）、日志主机（**loghost**）、告警缓冲区（**trapbuffer**）、SNMP 6 个方向的信息输出。
- 系统由众多的协议模块、单板驱动程序、配置模块构成，信息可按来源模块进行划分，可按模块进行信息过滤。
- 信息在输出时可以进行中英文选择。
- 每个信息的头部由固定的部分组成，包括时间戳、信息来源的模块、信息级别、信息来源的槽号、信息摘要等。

总之，信息中心的主要工作就是将各种模块的三种类型的信息，按照八种重要程度，根据用户的设置输出到十个信息通道中去，然后，将这十个信息通道再定位到六个输出方向上去。

4.2.2 信息中心配置

1. 开启/关闭信息中心的功能

请在系统视图下进行下列配置。

表4-7 开启/关闭信息中心功能

操作	命令
开启信息中心	info-center enable
关闭信息中心	undo info-center enable

说明：

信息中心缺省情况下处于开启状态。在信息中心开启时，特别是在处理信息较多时，由于信息分类、输出的原因，对系统性能有一定的影响。

2. 信息通道的命名

请在系统视图下进行下列配置。

表4-8 信息通道的命名

操作	命令
将编号为 <i>channel-number</i> 的信息通道命名为 <i>channel-name</i>	info-center channel <i>channel-number</i> name <i>channel-name</i>

channel-number 是通道号，取值为 0~9，即系统有 10 个通道。*channel-name* 是通道名，最长为 30 个字符，不支持“-”、“/”和“\”等字符。

通道 0~5 系统指定了缺省名，如下表：

表4-9 通道的缺省名

channel-number（通道号）	channel-name（通道名）
0	console
1	monitor
2	loghost
3	trapbuffer
4	logbuffer
5	snmpagent

3. 信息优先级（severity）

信息中心按信息的严重等级或紧急程度将其划分为八个等级；在按等级来进行信息过滤时，采用的规则是：禁止严重等级大于所设阈值的信息输出。越紧急的信息报文，其严重等级越小，**emergencies** 表示的等级为 0，**debugging** 为 7，因此，当设置严重等级阈值为 **debugging** 时，所有的信息都会输出。

表4-10 syslog 定义的优先级（severity）

严重等级	描述
emergencies	致命错误
alerts	需立即纠正的错误
critical	关键错误
errors	需关注但不关键的错误
warnings	警告，可能存在某种差错
notifications	需注意的信息
informational	一般提示信息
debugging	调试信息

设置将 SNMP 通道中的 IP 协议模块的日志类信息打开，且允许严重等级值小于等于 warning 级别的信息输出。

```
[H3C] info-center source IP channel snmpagent log level warnings
```

4. 定义信息通道的内容

请在系统视图下进行下列配置。

表4-11 定义信息通道的内容

操作	命令
向信息通道中添加记录	info-center source { <i>module-name</i> default } { channel { <i>channel-number</i> <i>channel-name</i> } } [log { state { on off } level severity }*] [trap { state { on off } level severity }*] [debug { state { on off } level severity }*]*
删除信息通道中的记录	undo info-center source { <i>module-name</i> default } { channel { <i>channel-number</i> <i>channel-name</i> } }

module-name 是模块名。**default** 代表信息通道中的缺省记录。**level** 设置信息级别，禁止信息级别大于所设置的 *severity* 的信息输出。*severity* 是信息级别。*channel-number* 是要设置的信息通道号。*channel-name* 是要设置的信息通道名。

对每个信息通道设有一条缺省记录，它的模块名为 **default**，但对于不同信息通道，此记录对日志、告警、调试类信息的缺省设置值可能不同。当某一个模块在此通道中没有明确的配置记录时，使用这条缺省的配置记录。

注意：

同时有多个 Telnet 用户时，各个用户之间共享一些配置参数，这些参数包括按模块过滤设置，中英文选择，严重等级阈值等，这些设置被某一个用户改变时，在别的用户端也有反映。

5. 信息的输出

目前，防火墙主体软件的信息中心可以在 6 个方向上输出各种信息：

- 通过 **Console** 口向本地控制台输出信息。
- 向远程 **Telnet** 终端输出信息。此功能有助于远程维护。
- 在防火墙内部分配适当大小的日志缓冲区，用于记录信息。
- 配置日志主机，信息中心直接将信息发往日志主机，并在其上以文件的形式保存起来，供随时查看。
- 在防火墙内部分配适当大小的告警缓冲区，用于记录信息。
- 向 **SNMP Agent** 输出信息。

每个输出方向通过配置命令指定所需要的通道，所有信息经过通道的过滤后，再发送到相应的输出方向；可根据需要，通过配置输出方向所使用的通道以及通道的过滤信息，来完成对各类信息的过滤以及重定向。

请在系统视图下进行下列配置。

表4-12 输出信息

操作	命令
向 Console 方向输出信息	info-center console channel { channel-number channel-name }
取消向 Console 方向输出信息	undo info-center console channel
向 Telnet 终端输出信息	info-center monitor channel { channel-number channel-name }
取消向 Telnet 终端输出信息	undo info-center monitor channel
向 SNMP 输出信息	info-center snmp channel { channel-number channel-name }
取消向 SNMP 输出信息	undo info-center snmp channel
设置向日志缓冲区输出信息的通道和日志缓冲区的大小	info-center logbuffer [channel { channel-number channel-name } size buffersize] *
关闭日志缓冲区或恢复默认值	undo info-center logbuffer [channel max-size]
设置向日志主机输出信息的信息通道以及其它参数	info-center loghost X.X.X.X [channel { channel-number channel-name } facility local-number language { chinese english }] *
取消向日志主机输出信息	undo info-center loghost X.X.X.X
设置发向日志主机的包的源地址	info-center loghost source interface-type interface-number
取消发向日志主机的包的源地址的配置	undo info-center loghost source
设置向告警缓冲区输出信息的通道和告警缓冲区的大小	info-center trapbuffer [channel { channel-number channel-name } max-size buffersize] *
关闭告警缓冲区或恢复默认值	undo info-center trapbuffer [channel size]

目前，系统缺省设置了 6 个信息通道，它们是：

输出方向 信息通道号 缺省的信息通道名

控制台	0	console
监视终端	1	monitor
日志主机	2	loghost
告警缓冲区	3	trapbuffer

日志缓冲区	4	logbuffer
snmp	5	snmpagent

 说明：

六个输出方向的设置相互独立，但首先需要开启信息中心，设置才会生效。

6. 设置发送日志信息的源地址

请在系统视图下进行下列配置。

表4-13 设置发送信息的源地址

操作	命令
设置发送信息的源地址	info-center loghost source <i>interface-type interface-number</i>
取消当前配置	undo info-center loghost source

7. 设置时间戳格式

请在系统视图下进行下列配置。

表4-14 设置时间戳格式

操作	命令
设置输出到终端和 buffer 的调试/告警/日志信息的时间戳格式	info-center timestamp { trap debugging log } { boot date none }
恢复输出到终端和 buffer 的调试/告警/日志信息的时间戳格式为缺省设置	undo info-center timestamp { trap debugging log }
设置输出到日志主机的日志信息的时间戳格式	info-center timestamp loghost { date no-year-date none }
恢复输出到日志主机的日志信息的时间戳格式为缺省设置	undo info-center timestamp loghost

缺省情况下，输出到终端和 buffer 的 debugging 信息使用 boot 时间戳，其他信息都使用 date 时间戳；输出到日志主机的日志信息的时间戳格式为 date。

4.2.3 显示终端的设置

显示终端的设置就是控制是否在用户屏幕上输出 debug/log/trap 信息，这些信息是从信息中心发送来的。

请在用户视图下进行下列配置。

表4-15 显示终端的设置

操作	命令
打开终端显示信息功能	terminal monitor
打开终端显示日志信息功能	terminal logging
打开终端显示告警信息功能	terminal trapping
打开终端显示调试信息功能	terminal debugging
关闭终端显示信息功能	undo terminal monitor
关闭终端显示日志信息功能	undo terminal logging
关闭终端显示告警信息功能	undo terminal trapping
关闭终端显示调试信息功能	undo terminal debugging

此命令只影响输入命令的当前终端的显示。

在 **undo terminal monitor**（显示终端关闭）的情况下，相当于执行 **undo terminal debugging, undo terminal logging, undo terminal trapping** 命令，所有的调试/日志/告警信息在本终端都不显示；在 **terminal monitor** 为打开的情况下，可以分别使用 **terminal debugging/undo terminal debugging, terminal logging/undo terminal logging, terminal trapping/undo terminal trapping** 打开或关闭调试/日志/告警信息。

缺省情况下，控制台用户（Console 用户）的终端显示功能为打开，所有提示信息都能够直接输出到配置终端；其它终端用户（AUX、VTY 用户）的终端显示功能缺省为关闭，因此配置 **terminal monitor** 命令后其提示信息才能输出到配置终端。

4.2.4 syslog 功能简介

syslog 功能是通过信息中心模块（**info-center**）实现的，它是信息中心模块所具有的一个子功能。本小节主要对输出到日志主机的系统信息格式（包括 **log**、**debug**、**trap** 三种信息）做简略的说明。输出到日志主机采用端口号 **514**。

本格式根据 RFC3164 (The BSD syslog Protocol) 制定，并对消息头部进行扩展。

系统信息格式如下:

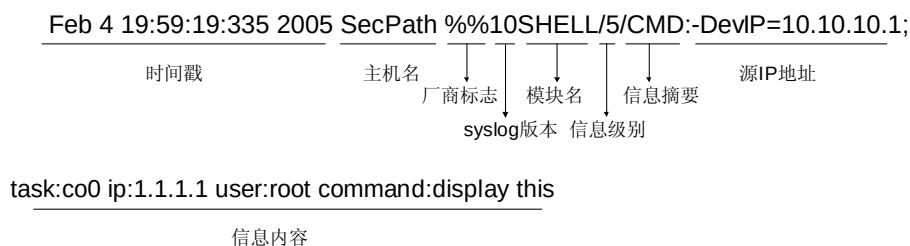


图4-2 系统信息格式示意图

以下对关键字段做详细说明。

1. 时间戳

info-center timestamp loghost 命令可以用来设置输出到日志主机的系统信息的时间戳格式，包括以下三种：

- **date:** 含年份的时间戳格式，此时系统信息中含年份信息。中文格式的时间戳为 YYYY/MM/DD hh:mm:ss，英文格式的时间戳为 MM DD hh:mm:ss YYYY。
- **no-year-date:** 不含年份时间戳格式，此时系统信息中不含年份信息。中文格式的时间戳为 MM/DD hh:mm:ss，英文格式的时间戳为 MM DD hh:mm:ss。
- **none:** 无时间戳，此时系统信息中不含时间信息。

“YYYY”为年份。

“MM”为月份。中文格式为 01~12 的数字，英语格式为月份的缩写，即为如下的值：Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec。

“DD”为日期，如果日期的值小于 10，则必须写为“空格+日期”，如“7”。

“hh:mm:ss”为本地时间，hh 采用 24 小时制，从 00 到 23；分钟和秒的值均从 00 到 59。

时间戳与主机名之间以一个空格隔开。

2. 主机名

主机名是本机的系统名，默认为“H3C”。

可用 **sysname** 命令修改主机名。

主机名与厂商标志之间以一个空格隔开。

3. 厂商标志

我们公司的标志为“%%”。

4. Syslog 版本

系统信息的 syslog 版本，本例中的 syslog 版本为 10。

5. 模块名

该字段表示日志是由哪个模块产生的，模块列表可以通过在系统视图下输入命令 **info-center source ?** 查看到。

模块名与级别之间以一个斜杠(/)隔开。

6. 信息级别

日志的级别共分为 8 级，从 0~7，它们的定义和说明见 表 4-10。

级别与信息摘要之间以一个斜杠(/)隔开。

7. 信息摘要

信息摘要是一个短语，代表了该信息的内容大意。

信息摘要与内容之间以一个冒号（:）隔开。

8. 源地址

当配置了 **info-center loghost source** 命令时会显示此项，表示发往日志主机的报文的源地址。

源地址与信息内容之间以分号（;）隔开。

9. 信息内容

信息具体内容，由各模块自己定义。

例如：“task:co0 ip:** user:root command:display this”的意思是 Console 口用户（用户名为 root），输入命令 display this。

4.2.5 信息中心的显示

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置信息中心后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **debugging** 命令可对信息中心进行调试。

表4-16 信息中心显示与调试

操作	命令
显示信息中心记录的信息	display info-center
显示日志缓冲区记录的信息	display logbuffer [size size-value summary] [level level-number] [{ begin include exclude } string]
显示信息通道的内容	display channel [channel-number channel-name]
显示告警缓冲区记录的信息	display trapbuffer [size size-value]

4.2.6 信息中心配置举例

1. 控制台信息输出配置举例

(1) 开启信息系统。

```
[H3C] info-center enable
```

(2) 配置控制台日志输出，允许 PPP 模块的日志输出，严重等级限制为 emergencies~debugging。

```
[H3C] info-center console channel console
```

```
[H3C] info-center source ppp channel console log level debugging
```

(3) 打开 PPP 模块的调试开关

```
<H3C> debugging ppp all
```

2. 向日志主机（UNIX 工作站）输出日志信息配置举例

第一步：防火墙侧配置如下

(1) 开启信息中心。

```
[H3C] info-center enable
```

(2) 将 IP 地址为 202.38.1.10 的 UNIX 工作站用作日志主机，设置严重等级阈值为 informational，输出语言为英文，允许输出信息的模块为 PPP 和 IP，使用 UNIX 设备 Local4。

```
[H3C] info-center loghost 202.38.1.10 language english
```

```
[H3C] info-center loghost 202.38.1.10 facility local4
```

```
[H3C] info-center source ppp channel loghost log level informational
```

```
[H3C] info-center source ip channel loghost log level informational
```

第二步：日志主机侧配置如下

UNIX 主机上也要进行相应设置以完成上述功能。下面以 SunOS 4.0 举例说明，其它厂商 UNIX 操作系统上的配置操作基本与之相同。

(3) 以超级用户（root）的身份执行以下命令

```
# mkdir /var/log/H3C
```

```
# touch /var/log/H3C/information
```

(4) 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）。

```
# H3C configuration messages
```

```
local4.info /var/log/H3C/information
```

说明：

在编辑/etc/syslog.conf 时应注意以下问题：

- 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受的日志信息级别与防火墙上配置的 **info-center loghost** 和 **info-center loghost a.b.c.d facility** 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。

当日志文件 config 建立且/etc/syslog.conf 文件被修改了之后，应执行以下命令，给系统守护进程 syslogd 发一个 HUP 信号，使 syslogd 重新读取它的配置文件 /etc/syslog.conf。

```
#ps -ae | grep syslogd
```

```
147
```

```
#kill -HUP 147
```

进行以上操作后，防火墙的相关信息就可以输出到相应的日志文件中了。

上面的配置只向日志主机输出严重程度为 **informational** 及以上的日志信息，即级别为 1~7 的日志信息。

日志信息的最低级别为 **debugging**，设置为 **debugging** 将导致所有的日志信息都发送到日志主机，对系统性能可能产生影响，因此，通常情况下，不建议用户将日志信息级别设置为 **debugging**。

 说明：

综合配置设备名称（**facility**），严重等级阈值（**severity**），模块名称（**filter**）以及 **syslog.conf** 文件，可以进行相当细致的分类，达到信息筛选的目的。

4.3 配置 HTTP 服务器

4.3.1 使能 HTTP 服务器

SecPath 系列安全产品支持以 HTTP 方式登录到系统中，并通过 Web 管理界面对系统进行配置和管理。在使用 Web 界面登录到系统前，必须先使能 HTTP 服务器功能。请在系统视图下进行下列配置。

表4-17 使能/关闭 HTTP 服务器

操作	命令
使能 HTTP 服务器	undo ip http shutdown
关闭 HTTP 服务器	ip http shutdown

缺省情况下，系统使能 HTTP 服务器。

仅当登录用户具有 Telnet 的服务类型时（**service-type telnet**），才允许登录 HTTP 服务器，且不同等级的用户在 Web 界面中的可配置项也会不同。

4.3.2 配置 HTTP 服务器的访问限制

可以配置 HTTP 服务器，使仅具有特定 IP 地址的用户才可以登录 HTTP 服务器，对设备进行配置和管理。

请在系统视图下进行下列配置。

表4-18 配置 HTTP 服务器的访问限制

操作	命令
配置 HTTP 服务器的访问限制	ip http acl <i>acl-number</i>
取消对 HTTP 服务器的访问限制	undo ip http acl

缺省情况下，未配置 HTTP 服务器的访问限制。

仅 ACL 中允许的 IP 地址才可以访问 HTTP 服务器。

第5章 自动侦测配置

5.1 自动侦测简介

自动侦测（Auto detect）是一种利用 ICMP 的 Request/Reply 报文，定期检测网络连通状况的功能。

自动侦测的对象是侦测组中目的 IP 地址的集合，侦测的结果反映出了当前网络的连通状态，即目的主机可达或不可达，从而保证设备能够及时发现网络中存在的问题，并产生相应的动作。

自动侦测的返回结果（可达或者不可达）可以被其他特性所引用，作为该特性配置是否生效的一个必要条件。自动侦测的应用包括：

(1) 静态路由

(2) VRRP（Virtual Router Redundancy Protocol）

某一个自动侦测组可以同时被多个应用实例所引用；同样，某一个应用实例也可以引用多个自动侦测组。

 说明：

- 对于静态路由的详细介绍，请参见本手册中有关“路由协议”的章节。
- 对于 VRRP 的详细介绍，请参见本手册中有关“可靠性”的章节。

5.2 自动侦测基本配置

5.2.1 自动侦测基本配置任务

表5-1 自动侦测配置任务

序号	配置项	命令	说明
1	进入系统视图	<H3C> system-view	-
2	创建并进入侦测组视图	[H3C] detect-group <i>group-number</i>	必选
3	配置侦测对象列表	[H3C-detect-group-X] detect-list <i>list-number</i> ip address <i>ip-address</i> [nexthop <i>ip-address</i>]	必选
4	配置各个侦测对象间关系	[H3C-detect-group-X] option { and or }	可选：缺省情况为 and

序号	配置项	命令	说明
5	配置侦测组的侦测周期	[H3C-detect-group-X] timer loop seconds	可选：缺省值为 15 秒
6	配置一次侦测中的最大重试次数	[H3C-detect-group-X] retry retry-times	可选：缺省值为 2 次
7	配置一次侦测的超时时间	[H3C-detect-group-X] timer wait seconds	可选：缺省值为 2 秒
8	显示指定侦测组或所有侦测组的配置信息	<H3C> display detect-group [group-number]	可选：该命令可在任意视图下执行

说明：

- 侦测组视图的提示符和用户的具体配置有关。
- 具体的参数介绍和取消相关配置的 **undo** 命令，请参见命令手册。

5.2.2 自动侦测基本配置举例

1. 组网需求

- 在 SecPathA 上创建侦测组 10，配置两个侦测对象，分别侦测目的地址 10.1.1.4 和 192.168.2.2；
- 设置两个侦测对象之间的关系为逻辑或；
- 设置侦测循环周期为 60 秒，一轮侦测中的重试次数为 3，一次侦测的超时时间为 3 秒；
- SecPathA、B、C 之间路由可达。

2. 组网图

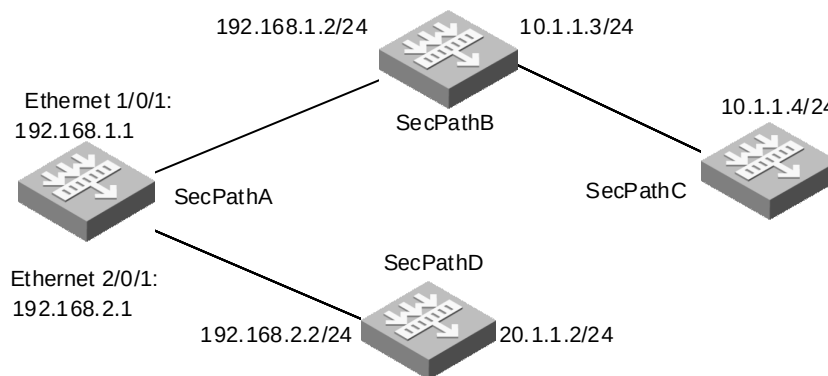


图5-1 自动侦测基本配置组网图

3. 配置步骤

(1) 配置 SecPath A

进入系统视图。

```
<H3C> system-view
```

创建一个自动侦测组 10。

```
[H3C] detect-group 10
```

从下一跳地址 192.168.1.2 开始，侦测目的地址 10.1.1.4，侦测序号为 1。

```
[H3C-detect-group-10] detect-list 1 ip address 10.1.1.4 nexthop 192.168.1.2
```

侦测目的地址 192.168.2.2，侦测序号为 2。

```
[H3C-detect-group-10] detect-list 2 ip address 192.168.2.2
```

设置侦测组 10 中的两个侦测对象之间的关系为逻辑或。

```
[H3C-detect-group-10] option or
```

设置侦测循环周期为 60 秒。

```
[H3C-detect-group-10] timer loop 60
```

设置一轮侦测中的重试次数为 3。

```
[H3C-detect-group-10] retry 3
```

设置一次侦测的超时时间为 3 秒。

```
[H3C-detect-group-10] timer wait 3
```

```
[H3C-detect-group-10] quit
```

显示侦测组 10 的配置信息。

```
[H3C] display detect-group 10
```

5.3 自动侦测在静态路由中的应用

用户可以将某条静态路由和某个侦测组进行绑定，利用自动侦测的返回结果来控制静态路由的有效性：

- 当侦测组可达时，静态路由生效
- 当侦测组不可达时，静态路由无效

5.3.1 静态路由中的应用配置任务

 说明：

在进行以下配置前，用户应先完成侦测组的定义。

表5-2 侦测组配置任务

序号	配置项	命令	说明
1	进入系统视图	<H3C> system-view	-
2	静态路由模块引用侦测组	[H3C] ip route-static <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } { <i>interface-type</i> <i>interface-number</i> <i>nexthop</i> } [preference <i>preference-value</i>] detect-group <i>group-number</i>	必选

具体的参数介绍请参见命令手册。

5.3.2 静态路由中的应用举例

1. 组网需求

- 在 SecPath A 上创建侦测组 8；
- 在 SecPath A 和 SecPath C 之间创建一条静态路由；
- 当侦测组 8 可达时使静态路由生效。

2. 组网图

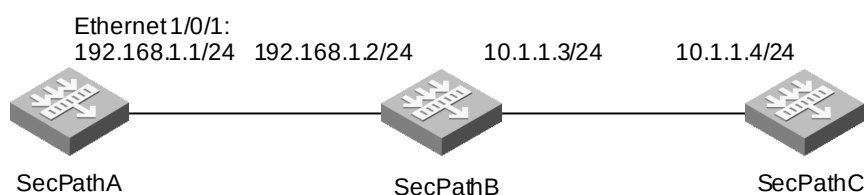


图5-2 静态路由的应用组网图

3. 配置步骤

配置 SecPath A:

进入系统视图。

```
<H3C> system-view
```

创建一个自动侦测组 8。

```
[H3C] detect-group 8
```

从下一跳地址 192.168.1.2 侦测 10.1.1.4，侦测序号为 1。

```
[H3C-detect-group-8] detect-list 1 ip address 10.1.1.4 nexthop 192.168.1.2
```

```
[H3C-detect-group-8] quit
```

侦测组可达时使静态路由生效，否则静态路由无效。

```
[H3C] ip route-static 10.1.1.0 24 192.168.1.2 detect-group 8
```

5.4 自动侦测在 VRRP 中的应用

用户可以利用自动侦测的返回结果来控制 VRRP 备份组中备份接口的优先级，实现主备路由器的自动切换：

- 当侦测组不可达时，降低备份组中备份接口的优先级
- 当侦测组可达时，恢复备份组中备份接口的优先级

5.4.1 VRRP 中的应用配置任务

 说明：

在进行以下配置前，用户应先完成侦测组的定义和 VRRP 的配置。

表5-3 侦测组配置任务

序号	配置项	命令	说明
1	进入系统视图	<H3C> system-view	-
2	进入接口视图	[H3C] interface <i>interface-type</i> <i>interface-number</i>	-
3	在 VRRP 中启动侦测功能	[H3C-InterfaceX] vrrp vrid <i>virtual-router-ID</i> track detect-group <i>group-number</i> [reduced <i>value-reduced</i>]	必选

 说明：

- 接口视图下显示的提示符和用户的设置有关。
- 具体的参数介绍和取消相关配置的 **undo** 命令，请参见命令手册。

5.4.2 VRRP 中的应用举例

1. 组网需求

- 保证 SecPathA、SecPathB、SecPathC 之间及 SecPathA、SecPathD、SecPathC 之间动态路由可达；
- SecPathB 和 SecPathD 组成一个 VRRP 备份组 1，虚拟 IP 地址为 192.168.1.100；
- 正常情况下，SecPathA 的数据通过 SecPathB 到达 SecPathC；

当 SecPathB 和 SecPathC 之间的链路失效后，SecPathD 自动成为备份组 1 中的 Master，SecPathA 的数据通过 SecPathD 到达 SecPathC。

2. 组网图

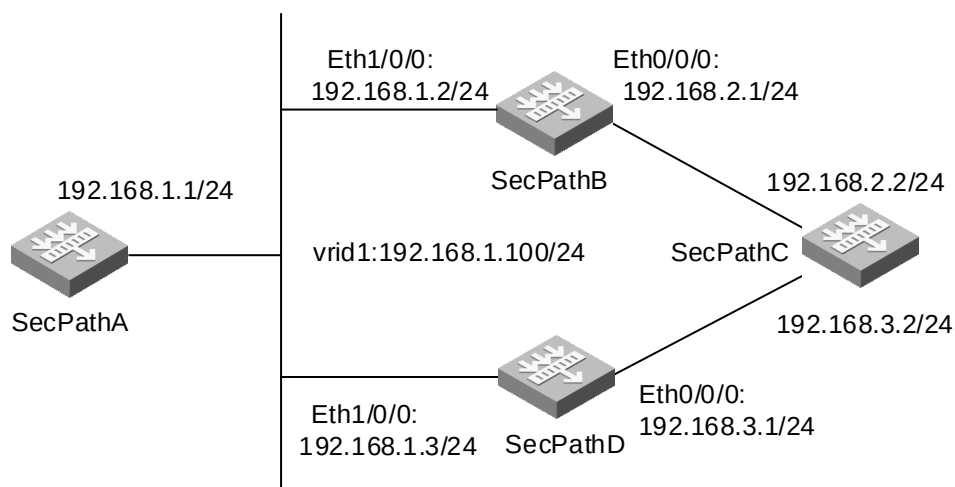


图5-3 VRRP 的应用组网图

3. 配置步骤

(1) 配置 SecPathB

进入系统视图。

```
<H3C> system-view
```

创建一个自动侦测组 9。

```
[H3C] detect-group 9
```

增加侦测对象 192.168.2.2，侦测序号为 1。

```
[H3C-detect-group-9] detect-list 1 ip address 192.168.2.2
```

```
[H3C-detect-group-9] quit
```

配置接口 Ethernet1/0/0 的 IP 地址。

```
[H3C] interface ethernet1/0/0
```

```
[H3C-Ethernet1/0/0] ip address 192.168.1.2 24
```

创建 VRRP 备份组，设置虚拟 IP 地址。

```
[H3C-Ethernet1/0/0] vrrp vrid 1 virtual-ip 192.168.1.100
```

设置 SecPathB 的备份组优先级为 110，当侦测组 9 不可达时将优先级降低 20。

```
[H3C-Ethernet1/0/0] vrrp vrid 1 priority 110
```

```
[H3C-Ethernet1/0/0] vrrp vrid 1 track detect-group 9 reduced 20
```

配置 Ethernet0/0/0 接口。

```
[H3C-Ethernet1/0/0] interface Ethernet0/0/0
```

```
[H3C-Ethernet0/0/0] ip address 192.168.2.1 24
```

配置动态路由（略）。

(2) 配置 SecPathD

在接口 Ethernet1/0/0 上启用 VRRP，设置 IP 地址及虚拟 IP 地址。

```
<H3C> system-view
```

```
[H3C] interface ethernet1/0/0
```

```
[H3C-Ethernet1/0/0] ip address 192.168.1.3 24
```

```
[H3C-Ethernet1/0/0] vrrp vrid 1 virtual-ip 192.168.1.100
```

设置 SecPathD 的备份组优先级为 100。

```
[H3C-Ethernet1/0/0] vrrp vrid 1 priority 100
```

配置动态路由（略）。

这里仅对 SecPathB 和 SecPathD 的自动侦测及 VRRP 配置做重点说明。

第6章 HWPing 配置

6.1 HWPing 简介

HWPing 是测量网络上运行的各种协议性能的一种工具，它是对 ping 功能的增强。可以通过网管来设置 HWPing 操作的各项参数，并启动 HWPing，最后查看操作的结果，也可以通过 **display hwping results** 命令来查看 HWPing 操作的统计结果。



图6-1 HWPing 客户端和服务端之间的关系图

6.2 HWPing 的配置

用户在使用 HWPing 功能之前首先必须分别配置好 HWPing 服务器和 HWPing 客户端。

6.2.1 HWPing 服务器的配置

HWPing 服务器的配置包括：

- 使能 HWPing 服务器
- 配置 HWPing 服务器监听的服务

1. 使能服务器

HWPing 功能中有些测试操作，如 jitter（对 UDP 报文传输的延时变化分析）、指定端口的 UDP 测试和指定端口的 TCP 测试等，需要服务器和客户端配合才能完成，HWPing 服务器负责处理 HWPing 客户端发来的测试包。只有在防火墙上使能了 HWPing 服务器功能，HWPing 服务器才能工作。

可以在同一台防火墙上同时使能 HWPing 客户端和 HWPing 服务器。也就是说，同一台防火墙既可以做 HWPing 服务器，又可以做 HWPing 客户端。

请在系统视图下进行下列配置。

表6-1 使能 HWPing 服务器

操作	命令
使能 HWPing 服务器功能	hwping-server enable
关闭 HWPing 服务器功能	undo hwping-server enable

缺省情况下，关闭服务器功能。

2. 配置监听服务

对于 TCP 和 UDP 的 HWPing 测试，HWPing 服务器通过监听功能响应客户端发起的测试。HWPing 服务器只对特定的客户端进行响应，即只有在 HWPing 服务器上配置了相应的目的地址和端口号的客户端才能得到服务器的响应。

可以在一个 HWPing 服务器上创建多个 TCP 和 UDP 监听服务，每个监听服务对应一个指定的目的地址和端口号。

请在系统视图下进行下列配置。

表6-2 配置监听端口

操作	命令
配置 UDP 监听服务	hwping-server udpecho <i>ip-address port-num</i>
取消 UDP 监听服务	undo hwping-server udpecho <i>ip-address port-num</i>
配置 TCP 监听服务	hwping-server tcpconnect <i>ip-address port-num</i>
取消 TCP 监听服务	undo hwping-server tcpconnect <i>ip-address port-num</i>

缺省情况下，未配置 UDP 和 TCP 监听服务。

说明：

配置 UDP 监听服务时，如果配置了系统已监听的端口号，当在进行 UDP 类型的测试时测试将不成功，但配置仍存在。

6.2.2 HWPing 客户端的配置

HWPing 客户端的配置包括：

- 使能 HWPing 客户端
- 建立测试组
- 配置同时能进行测试的最大数目
- 配置 trap 开关

1. 使能 HWPing 客户端

只有使能了 HWPing 客户端功能，才能进行各类测试的设置和测试。

请在系统视图下进行下列配置。

表6-3 使能 HWPing 客户端

操作	命令
打开 HWPing 客户端	hwping-agent enable
关闭 HWPing 客户端	undo hwping-agent enable

缺省情况下，关闭 HWPing 客户端。

2. 建立测试组

HWPing 测试组是一个 HWPing 测试项的集合。一个测试组中可以包含若干个测试项目。每个测试组都有一个管理员名称和一个测试标签。管理员名称和测试标签可以唯一确定一个测试组。

建立了测试组并配置好测试项参数之后就可以在测试组中通过测试命令进行 HWPing 测试。

在系统视图下进行下列配置。

表6-4 建立测试组

操作	命令
建立测试组	hwping administrator-name test-tag
删除测试组	undo hwping administrator-name test-tag

缺省情况下，没有配置测试组。

HWPing 测试组包含以下配置：

(1) 配置目的地址

目的地址指的是 HWPing 服务器的 IP 地址，相当于 ping 命令中的目的地址。该目的地址必须是 HWPing 服务器上配置了 TCP 或 UDP 监听服务的 IP 地址。

请在 HWPing 测试组视图下进行下列配置。

表6-5 配置目的地址

操作	命令
配置 HWPing 服务器目的地址	destination-ip ipaddress
删除 HWPing 服务器目的地址	undo destination-ip

缺省情况下，没有配置目的地址。

(2) 配置目的端口

在进行 TCP 或 UDP 测试时必须指定 HWPing 服务器的端口号。该端口号必须是 HWPing 服务器上配置了 TCP 或 UDP 监听服务的端口号。

请在 HWPing 测试组视图下进行下列配置。

表6-6 配置目的端口

操作	命令
配置 HWPing 服务器目的端口	destination-port <i>port-number</i>
删除 HWPing 服务器目的端口	undo destination-port

缺省情况下，没有配置目的端口。

(3) 配置源接口

在进行 DHCP 测试时，必须指定发送 DHCP 请求报文使用的源接口，系统将使用该源接口发送 DHCP 请求报文。另外，DHCP 请求报文中的源 IP 地址将使用该接口的 IP 地址。

在进行其它类型的测试时，可以指定发送报文使用的源接口。如果指定了源接口，系统将直接使用该源接口发送报文，而不是通过路由来确定发送报文的接口。

请在 HWPing 测试组视图下进行下列配置。

表6-7 绑定源接口

操作	命令
绑定源接口	source-interface <i>interface-type interface-number</i>
删除源接口	undo source-interface

缺省情况下，没有配置源接口。

(4) 配置源地址

在进行除 DHCP 以外的测试时，可以指定发送报文的源 IP 地址，这样服务器将使用此 IP 地址作为响应报文的目的地址。该参数相当于防火墙的 ping 命令中的“-a”参数。

请在 HWPing 测试组视图下进行下列配置。

表6-8 配置源地址

操作	命令
配置源地址	source-ip <i>ipaddress</i>
删除源地址	undo source-ip

缺省情况下，没有指定源 IP 地址。FTP 测试必须配置该命令。

(5) 配置源端口

在进行 HWPing 测试时，可以指定发送报文的源端口号，这样服务器将使用此端口号作为响应报文的目的端口号。

请在 HWPing 测试组视图下进行下列配置。

表6-9 配置源端口

操作	命令
配置源端口	source-port <i>port-number</i>
删除源端口	undo source-port

缺省情况下，没有指定源端口。

说明：

对于 TCP 类型的测试，当使用此命令指定源端口时，只有第一次测试能够成功（一次测试中进行探测的次数通过 **count** 命令进行配置），后续测试将会失败。若不指定源端口，系统会自动选择没有使用的端口发送报文，所有测试均可成功。

(6) 配置测试类型

HWPing 可以测试很多种类型的连接。但是每一次测试只能测试某一种类型，也就是说每一个测试组只能是某一类型的 HWPing 测试。

HWPing 的测试类型包括：**icmp**、**udppublic**、**udpprivate**、**tcppublic**、**tcpprivate**、**jitter**、**dhcp**、**snmpquery**、**ftp**、**http**。

请在 HWPing 测试组视图下进行下列配置。

表6-10 配置测试类型

操作	命令
配置测试类型	test-type <i>type</i>

缺省情况下，测试类型为 ICMP。

 说明：

udppublic 测试和 tcppublic 测试分别是对 7 号端口的 UDP 连接测试和 7 号端口的 TCP 连接测试。当进行这两种测试时，也必须在服务器端使用 **hwping-server udpecho ip-address 7** 命令和 **hwping-server tcpconnect ip-address 7** 命令配置监听服务端，否则测试将失败。

(7) 配置一次测试中进行探测的次数

如果配置一次测试中探测的次数大于 1，那么系统在进行第一次探测之后，如果收到响应报文就进行第二次探测。如果一直没有收到响应报文，则等到测试定时器超时后，再进行第二次探测。如此直到完成最后一次探测。该参数相当于防火墙的 ping 命令中的“-n”参数。

请在 HWPing 测试组视图下进行下列配置。

表6-11 配置一次测试中进行探测的次数

操作	命令
配置一次测试中进行探测的次数	count times
恢复一次测试中进行探测的次数到默认值	undo count times

缺省情况下，一次测试中进行探测的次数为 1。

(8) 配置数据段的长度

在进行 ICMP、UDP 和 jitter 测试时，可以对发送报文的数据段的长度进行配置。对于 ICMP 测试，ICMP 数据包的数据段长度是指进行 ICMP 测试时 ECHO-REQUEST 报文长度（不包括 IP 和 ICMP 报文头），该参数相当于防火墙的 ping 命令中的“-s”参数。

请在 HWPing 测试组视图下进行下列配置。

表6-12 配置数据段的长度

操作	命令
配置数据段的长度	datasize size
恢复为默认值	undo datasize

测试类型为 ICMP 时，数据段长度的缺省值为 56 个字节；测试类型为 UDP 时，数据段长度的缺省值为 100 个字节；测试类型为 jitter 时，数据段长度在 68~100 字节之间（此时取其它值无效）。

只有 ICMP、UDP 和 jitter 测试支持配置报文数据段的长度，此配置对于其它测试类型无效。

(9) 配置自动测试的时间间隔

配置自动测试时系统自动的每隔一段时间就进行一次测试。

请在 HWPing 测试组视图下进行下列配置。

表6-13 配置自动测试的时间间隔

操作	命令
配置自动测试的时间间隔	frequency interval
取消自动测试	undo frequency

缺省情况下，自动测试的时间间隔为 0，即只进行一次测试。

(10) 配置测试超时时间

测试超时时间是指发送完 ECHO-REQUEST 后，等待 ECHO-RESPONSE 的时间，如果超过此时间还没有收到 ECHO-RESPONSE，则认为该次测试不通。该参数相当于防火墙的 ping 命令中的“-t”参数，但是时间单位不一样。

请在 HWPing 测试组视图下进行下列配置。

表6-14 配置测试超时时间

操作	命令
配置测试超时时间	timeout time
恢复为默认值	undo timeout

缺省情况下，超时时间为 3 秒。

(11) 配置报文生存时间

报文生存时间是指测试报文的 TTL 值。该参数相当于防火墙的 ping 命令中的“-h”参数。

请在 HWPing 测试组视图下进行下列配置。

表6-15 配置报文生存时间

操作	命令
配置 ttl	ttl number
取消配置	undo ttl

缺省情况下，TTL 的值为 20。

 说明：

此命令适用于除 DHCP 类型外的其它测试类型。当配置了 **sendpacket passroute** 命令时，**tll** 命令不起作用。

(12) 配置服务类型

服务类型是指 IP 报文头中的 ToS 域值。该参数相当于防火墙的 ping 命令中的“-tos”参数

请在 HWPing 测试组视图下进行下列配置。

表6-16 配置服务类型

操作	命令
配置服务类型	tos value
恢复默认值	undo tos

缺省情况下，服务类型为 0。

(13) 报文填充字符

进行 ICMP、UDP 和 jitter 测试时，要对所发送的报文的数据段的内容进行填充。填充时，如果测试数据包大小比配置的填充数据小，那么只使用此字符串的前一部分；如果测试数据包大小比配置的填充数据大，那么将使用此字符串循环进行填充。例如，配置填充数据为“abcd”，当测试数据包大小为 3 时，则只使用“abc”作为填充数据；当测试数据包大小为 6 时，则只使用“abcdab”作为填充数据。

请在 HWPing 测试组视图下进行下列配置。

表6-17 配置报文填充字符

操作	命令
配置填充字符	datafill string
取消填充字符	undo datafill

缺省情况下，从 0 到 255 循环填充数据。

只有 ICMP、UDP 和 jitter 测试支持配置填充字符，此配置对于其它测试类型无效。

(14) 配置 HTTP 操作类型

HWPing 客户端可以配置和服务端进行 HTTP 交互的类型。

此配置必须在测试类型为 HTTP 时进行。

请在 HWPing 测试组视图下进行下列配置。

表6-18 配置 HTTP 操作类型

操作	命令
配置操作类型	http-operation { get post }

缺省情况下，使用 **get** 操作。

(15) 配置 FTP 操作类型

HWPing 客户端可以配置和服务端进行 FTP 交互的类型。

此配置必须在测试类型为 **FTP** 时进行。

请在 HWPing 测试组视图下进行下列配置。

表6-19 配置 FTP 操作类型

操作	命令
配置操作类型	ftp-operation { get put }

缺省情况下，FTP 操作类型为 **get** 操作。

(16) 配置 FTP 操作用户名和密码

进行 FTP 操作时需要使用用户名和密码。

此配置必须在测试类型为 **FTP** 时进行。

请在 HWPing 测试组视图下进行下列配置。

表6-20 配置 FTP 操作用户名和密码

操作	命令
配置用户名	username <i>name</i>
删除用户名	undo username
配置密码	password <i>password</i>
删除密码	undo password

缺省情况下，没有配置用户名和密码。

(17) 配置 FTP 操作文件名

配置 FTP 所要操作的服务器端的文件名。

此配置必须在测试类型为 **FTP** 时进行。

请在 HWPing 测试组视图下进行下列配置。

表6-21 配置 FTP 操作文件名

操作	命令
配置文件名	filename <i>file-name</i>
删除文件名	undo filename

缺省情况下，没有配置操作的文件名。

(18) 配置 Jitter 测试时发送的测试包个数

Jitter 测试是为了对 UDP 报文传输的延时变化进行统计分析。在测试时，源端会以一定的时间间隔（可配置）发送一系列的数据包，目的端收到数据包后，将数据包打上时间戳，然后再发回到源端。源端收到数据包后就可计算出抖动时间。因此每次探测必须发送多个测试包进行测试。每次探测发送的测试包个数越多，统计分析越准确，但完成测试所需的时间也越长。

此配置必须在测试类型为 Jitter 时进行。

请在 HWPing 测试组视图下进行下列配置。

表6-22 配置 Jitter 测试时发送的测试包个数

操作	命令
Jitter 测试时发送的测试包个数	jitter-packetnum <i>number</i>
恢复为默认值	undo jitter-packetnum

缺省情况下，Jitter 测试时发送的测试包为 10 个。

(19) 配置 Jitter 测试时发送测试包的时间间隔

Jitter 测试每次探测都要发送多个 UDP 测试包，可以配置发送测试包的时间间隔。发送测试包的时间间隔越小，完成测试就越快，但是发送测试包的时间间隔太小可能会对网络带来一定的冲击。

此配置必须在测试类型为 Jitter 时进行。

请在 HWPing 测试组视图下进行下列配置。

表6-23 配置 Jitter 测试时发送测试包的时间间隔

操作	命令
Jitter 测试时发送测试包的时间间隔	jitter-interval <i>interval</i>
恢复为默认值	undo jitter-interval

缺省情况下，Jitter 测试时发送测试包的时间间隔为 20 毫秒。

(20) 配置保存历史记录的最大数目

指定在一个测试组中能保存的历史记录数的最大数目，当超过这个数目时，它会丢弃最先测试的结果。

请在 HWPing 测试组视图下进行下列配置。

表6-24 配置保存历史记录的最大数目

操作	命令
配置保存历史记录的最大数目	history-records <i>number</i>
恢复为默认值	undo history-records

缺省情况下，最大历史记录数为 50 条。

(21) 配置路由表旁路

路由表旁路是指，远端主机将不进行通常的路由表查找，而直接发送 ICMP 报文到相连网络上的主机。如果主机所在网络不是直连的，就返回错误。例如，在接口上 ping 一个无路由的本地主机时可以使用本功能。

请在 HWPing 测试组视图下进行下列配置。

表6-25 配置路由表旁路

操作	命令
启动路由表旁路功能	sendpacket passroute
关闭路由表旁路功能	undo sendpacket passroute

缺省情况下，关闭路由表旁路功能。

(22) 配置 VPN instance 信息

请在 HWPing 测试组视图下进行下列配置。

表6-26 配置 VPN instance 信息

操作	命令
设置 ICMP 的 VPN instance 信息	vpninstance <i>name</i>
取消 ICMP 的 VPN instance 信息	undo vpninstance

缺省情况下，未设置 ICMP 的 VPN instance 信息。

(23) 配置测试组描述

用户可以对一个测试组进行简要的描述。通常用于描述一个测试组所做的测试项或测试的目的。

请在 HWPing 测试组视图下进行下列配置。

表6-27 配置测试描述

操作	命令
配置测试描述	description <i>string</i>
取消测试描述	undo description

缺省情况下，无任何描述信息。

(24) 配置 trap

HWPing 测试成功或者失败都会产生 trap 信息，可以通过设置 trap 开关控制是否向网管发送该 trap。

可以设置 HWPing 测试以及每一次测试内的探测连续失败若干次才发送 trap。缺省情况下，探测一次失败及测试一次失败就发送 trap。

请在 HWPing 测试组视图下进行下列配置。

表6-28 打开 trap 开关

操作	命令
打开 trap 开关	send-trap { all { probefailure testcomplete testfailure } * }
关闭 trap 开关	undo send-trap { all { probefailure testcomplete testfailure } * }
设置 HWPing 测试连续多少次测试失败之后发送 Trap	test-failtimes <i>times</i>
设置 HWPing 测试连续多少次探测失败之后发送 Trap	probe-failtimes <i>times</i>

缺省情况下，不发送 trap 到网管站。

3. 配置同时能进行测试的最大数目

可以设定一个防火墙（HWPing 客户端）最多能同时进行测试的数目。

请在系统视图下进行下列配置。

表6-29 配置同时进行测试的最大数目

操作	命令
设定最大数目	hwping-agent max-requests <i>number</i>
恢复最大数目的缺省值	undo hwping-agent max-requests

缺省情况下，最大数目为 5 条。

6.3 执行测试

建立了测试组并配置好测试项参数之后就可以在测试组中通过测试命令进行 HWPing 测试。

请在 HWPing 测试组视图下进行下列配置。

表6-30 测试

操作	命令
执行测试	test-enable
取消测试	undo test-enable

 说明：

HWPing 测试不会显示测试结果，要查看显示结果请使用显示测试信息命令。

6.4 HWPing 的显示和调试

在任意视图下执行 **display hwping** 命令可以分别用来查看测试的历史记录信息和最新测试结果信息。

通过历史记录可以查看测试中记录的每一次探测的结果。

通过最新测试结果可以查看最近一次测试的结果。

在用户视图下执行 **debugging hwping** 命令可以对 HWPing 进行调试。

表6-31 HWPing 的显示和调试

操作	命令
显示测试的结果信息	display hwping { history results jitter } [<i>administrator-name test-tag</i>]
打开 HWPing 的调试信息开关	debugging hwping { all error event }
关闭 HWPing 的调试信息开关	undo debugging hwping { all error event }

6.5 HWPing 典型配置举例

 说明：

在进行任何测试之前，都需先使能 HWPing 客户端。

6.5.1 ICMP 测试

1. 介绍

HWPing ICMP 测试和 ping 测试一样，是使用 ICMP 协议来测试数据包在本端和指定的目的端之间的往返时间。

2. ICMP 测试配置步骤

 说明：

要想成功创建并启动一个 ICMP echo 功能的测试操作。必须执行以下步骤 1, 2, 3, 6, 其它步骤为可选项。

使能 HWPing 客户端。

```
[H3C] hwping-agent enable
```

步骤 1：创建一个 HWPing 测试组。在本例中指定的管理员名字为 administrator，测试操作标签为 icmp。

```
[H3C] hwping administrator icmp
```

步骤 2：配置测试的类型为 ICMP。

```
[H3C-hwping-administrator-icmp] test-type icmp
```

步骤 3：配置目的 IP 地址为 169.254.10.2。

```
[H3C-hwping-administrator-icmp] destination-ip 169.254.10.2
```

步骤 4：配置一次测试中进行探测的次数。

```
[H3C-hwping-administrator-icmp] count 10
```

步骤 5：配置超时时间。

```
[H3C-hwping-administrator-icmp] timeout 3
```

步骤 6：启动测试操作。

```
[H3C-hwping-administrator-icmp] test-enable
```

步骤 7：查看测试结果。

```
[H3C-hwping-administrator-icmp] display hwping results administrator icmp
```

```
[H3C-hwping-administrator-icmp] display hwping history administrator icmp
```

6.5.2 DHCP 测试

1. 介绍

HWPing DHCP 测试用来测试从 DHCP 服务器分配到 IP 地址所需的时间。

2. DHCP 测试配置步骤

说明：

要想成功创建并启动一个 DHCP 类型的测试。必须执行以下步骤 1，2，3，6，其它步骤为可选项。

使能 HWPing 客户端。

```
[H3C] hwping-agent enable
```

步骤 1：创建一个 HWPing 测试组。在本例中指定的管理员名字为 administrator，测试操作标签为 dhcp。

```
[H3C] hwping administrator dhcp
```

步骤 2：配置测试的类型为 DHCP。

```
[H3C-hwping-administrator-dhcp] test-type dhcp
```

步骤 3：配置源接口，此接口必须为以太网口，DHCP 服务器位于和此接口相连的网络上。

```
[H3C-hwping-administrator-dhcp] source-interface ethernet1/0/0
```

步骤 4：配置一次测试中进行探测的次数。

```
[H3C-hwping-administrator-dhcp] count 10
```

步骤 5：配置超时时间。

```
[H3C-hwping-administrator-dhcp] timeout 3
```

步骤 6：启动测试操作。

```
[H3C-hwping-administrator-dhcp] test-enable
```

步骤 7：查看测试结果。

```
[H3C-hwping-administrator-dhcp] display hwping results administrator dhcp
```

```
[H3C-hwping-administrator-dhcp] display hwping history administrator dhcp
```

6.5.3 FTP 测试

1. 介绍

HWPing FTP 测试用来测试和指定的 FTP 服务器建立连接，及传送一个文件所用的时间。可以从 FTP 服务器得到一个文件，也可以向 FTP 服务器写一个文件。

2. FTP 测试配置步骤

说明:

要想成功创建并启动一个 FTP 类型的测试操作。必须执行以下步骤 1, 2, 3, 4, 5, 6, 9 其它步骤为可选项。

使能 HWPing 客户端。

```
[H3C] hwping-agent enable
```

步骤 1: 创建一个 HWPing 测试组。在本例中指定的管理员名字为 administrator, 测试操作标签为 ftp。

```
[H3C] hwping administrator ftp
```

步骤 2: 配置测试的类型为 FTP。

```
[H3C-hwping-administrator-ftp] test-type ftp
```

步骤 3: 配置 FTP 服务器的 IP 地址为 169.254.10.2。

```
[H3C-hwping-administrator-ftp] destination-ip 169.254.10.2
```

步骤 4: 配置用户名。

```
[H3C-hwping-administrator-ftp] username administrator
```

步骤 5: 配置口令

```
[H3C-hwping-administrator-ftp] password hwping
```

步骤 6: 配置要获取的文件名。

```
[H3C-hwping-administrator-ftp] filename config.txt
```

步骤 7: 配置一次测试中进行探测的次数。

```
[H3C-hwping-administrator-ftp] count 10
```

步骤 8: 配置超时时间。

```
[H3C-hwping-administrator-ftp] timeout 30
```

步骤 9: 配置源地址。

```
[H3C-hwping-administrator-ftp] source-ip 169.254.0.1
```

步骤 10: 启动测试操作。

```
[H3C-hwping-administrator-ftp] test-enable
```

步骤 11: 查看测试结果。

```
[H3C-hwping-administrator-ftp] display hwping results administrator ftp
```

```
[H3C-hwping-administrator-ftp] display hwping history administrator ftp
```

对端仅需要启动 FTP Server, 并配置相应的用户即可。

6.5.4 HTTP 测试

1. 介绍

HWPing HTTP 测试用来测试与指定的 HTTP 服务器之间建立连接并从 HTTP 服务器获取一个文件所用的时间。

2. HTTP 测试配置步骤

说明：

要想成功创建并启动一个 HTTP 类型的测试操作。必须执行以下步骤 1，2，3，其它步骤为可选项。

使能 HWPing 客户端。

```
[H3C] hwping-agent enable
```

步骤 1：创建一个 HWPing 测试组。在本例中指定的管理员名字为 administrator，测试操作标签为 http。

```
[H3C] hwping administrator http
```

步骤 2：配置测试的类型为 HTTP。

```
[H3C-hwping-administrator-http] test-type http
```

步骤 3：配置 HTTP 服务器的 IP 地址为 169.254.10.2。

```
[H3C-hwping-administrator-http] destination-ip 169.254.10.2
```

步骤 4：配置一次测试中进行探测的次数。

```
[H3C-hwping-administrator-http] count 10
```

步骤 5：配置超时时间。

```
[H3C-hwping-administrator-http] timeout 30
```

步骤 6：启动测试操作。

```
[H3C-hwping-administrator-http] test-enable
```

步骤 7：查看测试结果。

```
[H3C-hwping-administrator-http] display hwping results administrator http
```

```
[H3C-hwping-administrator-http] display hwping history administrator http
```

6.5.5 Jitter 测试

1. 介绍

HWPing Jitter 测试用来测试本端（HWPing 客户端）和指定的目的端（HWPing 服务器）之间传送 UDP 报文的抖动时间。

2. Jitter 测试配置步骤

说明:

要想成功创建并启动一个 Jitter 类型的测试操作。必须在 HWPing 客户端执行以下步骤 1, 2, 3, 4, 8 其它步骤为可选项。

使能 HWPing 客户端。

```
[H3C] hwping-agent enable
```

步骤 1: 创建一个 HWPing 测试组。在本例中指定的管理员名字为 administrator, 测试操作标签为 jitter。

```
[H3C] hwping administrator jitter
```

步骤 2: 配置测试的类型为 Jitter。

```
[H3C-hwping-administrator-jitter] test-type jitter
```

步骤 3: 配置 HWPing 服务器的 IP 地址为 169.254.10.2。

```
[H3C-hwping-administrator-jitter] destination-ip 169.254.10.2
```

步骤 4: 配置 HWPing 服务器的目的端口。

```
[H3C-hwping-administrator-jitter] destination-port 9000
```

步骤 5: 配置一次测试中进行探测的次数。

```
[H3C-hwping-administrator-jitter] count 10
```

步骤 6: 配置超时时间。

```
[H3C-hwping-administrator-jitter] timeout 30
```

步骤 7: 启动测试操作。

```
[H3C-hwping-administrator-jitter] test-enable
```

步骤 8: 查看测试结果。

```
[H3C-hwping-administrator-jitter] display hwping results administrator jitter
```

```
[H3C-hwping-administrator-jitter] display hwping history administrator jitter
```

```
[H3C-hwping-administrator-jitter] display hwping jitter administrator jitter
```

**注意：**

必须在目的端启动 HWPing 服务器，目的端的配置如下：

```
[SecPath] hwping-server enable
```

```
[SecPath] hwping-server udpecho 169.254.10.2 9000
```

在 HWPing 服务器上使用命令 `hwping-server udpecho` 创建响应 UDP 包的 HWPing 服务器时，指定的 IP 地址和端口号是服务器所要处理的包的目的地址和目的端口。它们必须和上面步骤 3，4 中配置的 IP 地址和端口号一样。

6.5.6 SNMP 测试

1. 介绍

HWPing SNMP 测试用来测试从发出一个 SNMP 协议查询包到接收到响应所用的时间。

2. SNMP 测试配置步骤

**说明：**

要想成功创建并启动一个 SNMP 类型的测试操作，必须在 HWPing 客户端执行以下步骤 1，2，3，6，其它步骤为可选项。

使能 SNMP 客户端。

```
[H3C] snmp-agent trap enable
```

使能 hwping 客户端。

```
[H3C] hwping-agent enable
```

步骤 1：创建一个 HWPing 测试组。在本例中指定的管理员名字为 `administrator`，测试操作标签为 `snmp`。

```
[H3C] hwping administrator snmp
```

步骤 2：配置测试的类型为 SNMP。

```
[H3C -hwping-administrator-snm] test-type snmpquery
```

步骤 3：配置目的 IP 地址为 169.254.10.2。

```
[H3C-hwping-administrator-snm] destination-ip 169.254.10.2
```

步骤 4：配置一次测试中进行探测的次数。

```
[H3C-hwping-administrator-snm] count 10
```

步骤 5：配置超时时间。

```
[H3C-hwping-administrator-snm] timeout 30
```

步骤 6：启动测试操作。

```
[H3C-hwping-administrator-snmp] test-enable
```

步骤 7：查看测试结果。

```
[H3C] display hwping results administrator snmp
```

```
[H3C] display hwping history administrator snmp
```



注意：

在上面步骤 3 中配置的目的 IP 地址所指定的机器上必须启动网管功能，否则将收不到回应包。在本公司设备上可使用 **snmp-agent** 命令启动网管功能，相关内容请参考第 11 章 SNMP 配置。

6.5.7 指定端口的 TCP 测试

1. 介绍

指定端口的 HWPing TCP 测试用来测试本端和指定的目的端之间建立 TCP 连接的时间。

2. 指定端口的 TCP 测试配置步骤



说明：

要想成功创建并启动一个 TCP 类型的测试操作。必须执行以下步骤 1, 2, 3, 4, 7, 其它步骤为可选项。

使能 HWPing 客户端。

```
[H3C] hwping-agent enable
```

步骤 1：创建一个 HWPing 测试组。在本例中指定的管理员名字为 administrator，测试操作标签为 tcpprivate。

```
[H3C] hwping administrator tcpprivate
```

步骤 2：配置测试的类型为 tcpprivate。

```
[H3C-hwping-administrator-tcpprivate] test-type tcpprivate
```

步骤 3：配置 HWPing 服务器的 IP 地址为 169.254.10.2。

```
[H3C-hwping-administrator-tcpprivate] destination-ip 169.254.10.2
```

步骤 4：配置 HWPing 服务器的目的端口。

```
[H3C-hwping-administrator-tcpprivate] destination-port 9000
```

步骤 5：配置一次测试中进行探测的次数。

```
[H3C-hwping-administrator-tcpprivate] count 10
```

步骤 6：配置超时时间。

```
[H3C-hwping-administrator-tcpprivate] timeout 3
```

步骤 7：启动测试操作。

```
[H3C-hwping-administrator-tcpprivate] test-enable
```

步骤 8：查看测试结果。

```
[H3C] display hwping results administrator tcpprivate
```

```
[H3C] display hwping history administrator tcpprivate
```



注意：

必须在目的端启动 HWPing 服务器并创建 HWPing TCP 监听服务，在目的端的配置如下：

```
[SecPath] hwping-server enable
```

```
[SecPath] hwping-server tcpconnect 169.254.10.2 9000
```

在 HWPing 服务器上使用命令 `hwping-server tcpconnect` 创建建立 TCP 监听服务时，指定的 IP 地址和端口号必须和上面步骤 3，4 中配置的 IP 地址和端口号一样。

6.5.8 指定端口的 UDP 测试

1. 介绍

指定端口的 HWPing UDP 测试用来测试本端和指定的目的端之间 UDP 协议包的往返时间。

2. 指定端口的 UDP 测试配置步骤

 说明：

要想成功创建并启动一个指定端口的 UDP 类型的测试操作。必须执行以下步骤 1，2，3，4，7，其它步骤为可选项。

使能 HWPing 客户端。

```
[H3C] hwping-agent enable
```

步骤 1：创建一个 HWPing 测试组。在本例中指定的管理员名字为 `administrator`，测试操作标签为 `udpprivate`。

```
[H3C] hwping administrator udpprivate
```

步骤 2：配置测试的类型为 `udpprivate`。

```
[H3C-hwping-administrator-udpprivate] test-type udpprivate
```

步骤 3：配置 HWPing 服务器的 IP 地址为 `169.254.10.2`。

```
[H3C-hwping-administrator-udpprivate] destination-ip 169.254.10.2
```

步骤 4：配置 HWPing 服务器的目的端口。

```
[H3C-hwping-administrator-udpprivate] destination-port 9000
```

步骤 5：配置一次测试中进行探测的次数。

```
[H3C-hwping-administrator-udpprivate] count 10
```

步骤 6：配置超时时间。

```
[H3C-hwping-administrator-udpprivate] timeout 3
```

步骤 7：启动测试操作。

```
[H3C-hwping-administrator-udpprivate] test-enable
```

步骤 8：查看测试结果。

```
[H3C] display hwping results administrator udpprivate
```

```
[H3C] display hwping history administrator udpprivate
```



注意：

要在目的端启动 HWPing 服务器，需进行如下配置：

```
[H3C] hwping-server enable
```

```
[H3C] hwping-server udpecho 169.254.10.2 9000
```

在 HWPing 服务器上使用命令 `hwping-server udpecho` 创建响应 UDP 包的 HWPing 服务时，指定的 IP 地址和端口号是服务器所要处理的包的目的地址和目的端口。它们必须和上面步骤 3、4 中配置的 IP 地址和端口号一样。

第7章 文件管理

7.1 文件系统

7.1.1 文件系统简介

文件系统的主要功能为管理存储设备，把文件保存在存储设备中。防火墙目前支持的存储设备是 **FLASH**。

文件系统是指对存储设备中的文件、目录的管理，包括创建文件系统，创建、删除、修改、更名文件和目录，以及显示文件的内容。

7.1.2 目录操作

文件系统可以创建并删除目录，以及显示当前的工作目录，显示指定目录下的文件或目录信息。

请在用户视图下进行下列操作。

表7-1 目录操作

操作	命令
创建目录	mkdir <i>directory</i>
删除目录	rmdir <i>directory</i>
显示当前的工作目录	pwd
显示目录或文件信息	dir [/all] [<i>file-url</i> flash:]
改变当前目录	cd <i>directory</i>

7.1.3 文件操作

文件系统可以删除文件、恢复删除的文件、彻底删除回收站中的文件、显示文件的内容、重新命名、拷贝文件、移动文件、执行批处理文件、显示指定文件的信息和私有文件信息，如下表所示。

请在用户视图下进行下列操作，其中 **execute** 命令在系统视图下执行。

表7-2 文件操作

操作	命令
删除文件	delete [/unreserved] { <i>file-url</i> flash: }
恢复删除文件	undelete { <i>file-url</i> flash: }

操作	命令
彻底删除回收站中的文件	reset recycle-bin [<i>filename</i> flash:] [/force]
显示文件的内容	more <i>file-url</i>
重新命名文件或目录	rename <i>source-name new-name</i>
拷贝文件	copy <i>fileurl_source fileurl_dest</i>
移动文件	move <i>fileurl_source fileurl_dest</i>
显示目录或文件信息	dir [/ all] [<i>file-url</i> flash:]
执行批处理文件	execute { <i>filename</i> flash: }

7.1.4 解包 Web 文件

当系统中有包含 Web 文件的文件时，可以将其解包分离出来。

请在用户视图下进行下列配置。

表7-3 解包捆绑 Web 文件的文件

操作	命令
解包捆绑 Web 文件的文件	detach web-bind-filename [<i>http-filename</i>]

如果要解包的文件没有捆绑 Web 文件，则提示文件中没有捆绑 Web 文件；如果没有指定解包出的 Web 文件名，则 Web 文件名缺省为 http.zip。

7.1.5 存储设备操作

文件系统可以格式化指定的存储设备。

请在用户视图下进行下列操作。

表7-4 存储设备操作

操作	命令
格式化存储设备	format <i>device-name</i>

7.1.6 文件系统提示方式

用户通过命令可以修改当前文件系统的提示方式。

请在系统视图下进行下列操作。

表7-5 设置文件系统提示方式

操作	命令
文件系统的提示方式	file prompt { alert quiet }

7.1.7 文件系统使用举例

查看根目录及 test 目录下当前的文件。

```
<H3C> dir
Directory of flash:/
  1  -rw-   2145123   Jul 12 2001 12:28:08   system
  2  -rw-     595    Jul 12 2001 10:47:50   config.cfg
  3  drw-      -    Jul 12 2001 19:41:20   test
6477 KB total (2144 KB free)
<H3C> dir flash:/test/
Directory of flash:/test/
  1  drw-      -    Jul 12 2001 20:23:37   subdir
  2  -rw-     595    Jul 12 2001 20:13:19   config.cfg
  3  -rw-     50    Jul 12 2001 20:08:32   sample.txt
6477 KB total (2144 KB free)
```

移动文件从 flash:/test/sample.txt 到 flash:/sample.txt。

```
<H3C> move flash:/test/sample.txt flash:/sample.txt
Move flash:/test/sample.txt to flash:/sample.txt ?[Y/N]:y
%Moved file flash:/test/sample.txt to flash:/sample.txt
```

查看移动后的显示结果。

```
<H3C> dir
Directory of flash:/
  1  -rw-   2145123   Jul 12 2001 12:28:08   ne80.bin
  2  -rw-     595    Jul 12 2001 10:47:50   config.cfg
  3  drw-      -    Jul 12 2001 19:41:20   test
  4  -rw-     50    Jul 12 2001 20:26:48   sample.txt
6477 KB total (2144 KB free)
<H3C> dir flash:/test/
Directory of flash:/test/
  1  drw-      -    Jul 12 2001 20:23:37   subdir
  2  -rw-     595    Jul 12 2001 20:13:19   config.cfg
6477 KB total (2144 KB free)
```

7.2 FTP 配置

7.2.1 FTP 简介

FTP 协议在 TCP/IP 协议族中属于应用层协议，主要向用户提供与远程主机之间的文件传输，FTP 协议基于相应的文件系统实现。

系统提供的 FTP 服务包括：

- FTP Server 服务，用户可以运行 FTP 客户端程序登录到防火墙上，访问防火墙上的文件。
- FTP Client 服务，用户通过终端仿真程序或 Telnet 程序建立与防火墙的连接后，可以通过输入 FTP 命令，建立防火墙与远程 FTP Server 的连接，并访问远程主机上的文件。

FTP 服务器配置包括：

- 启动 FTP 服务器
- 配置 FTP 服务器的验证和授权
- 配置 FTP 服务器的运行参数
- FTP 服务器的显示和调试

7.2.2 启动 FTP 服务器

只有启动 FTP 服务器功能，FTP 客户端才能登录到服务器上，访问服务器上的文件。

请在系统视图下进行下列配置。

表7-6 启动 FTP 服务器

操作	命令
启动 FTP 服务器	ftp server enable
关闭 FTP 服务器	undo ftp server

缺省情况下，未启动 FTP 服务器。

7.2.3 配置 FTP 服务器的验证和授权

FTP 服务器的授权配置信息包含提供给 FTP 用户的工作目录的路径的配置等。只有验证通过和授权成功的用户，才能享受 FTP 服务器的服务。在使用 FTP 服务时，必须事先在防火墙上配置好用户类型和 FTP 工作目录。

表7-7 配置 FTP 服务器的验证和授权

操作	命令
创建新的本地 FTP 用户, 并且进入本地用户视图（系统视图）	local-user <i>user-name</i>
删除指定的本地用户	undo local-user { <i>user-name</i> all }
配置 FTP 用户的密码（本地用户视图）	password { cipher simple } <i>password</i>
取消 FTP 用户的密码（本地用户视图）	undo password
配置 FTP 用户的授权信息（本地用户视图）	service-type ftp [ftp-directory <i>directory</i>]
恢复对 FTP 用户授权的缺省目录	undo service-type ftp [<i>ftp-directory</i>]

FTP 服务器的验证和授权配置举例：

例：配置 FTP 用户名为 **ftpuuser**，口令为 **pwd**（明文），授权工作目录为 **flash:/ftp/ftpuuser**（防火墙文件系统支持的路径名）

配置 FTP 用户的验证及相关信息。

```
[H3C] local-user ftpuuser
[H3C-luser-ftpuuser] password simple pwd
[H3C-luser-ftpuuser] service-type ftp ftp-directory flash:/ftp/ftpuuser
```

7.2.4 配置 FTP 服务器的运行参数

1. 设置 FTP 升级方式

用户从 PC 机登录到 FTP Server，使用 **put** 命令上载文件时，FTP Server 有两种升级方式，快速升级方式和普通升级方式。

- 快速升级方式，即 FTP Server 在全部接收完用户上传的文件后，再开始将该文件写入 Flash 中。采用这种方式，即使文件传送过程发生断电等异常情况，也不会损坏防火墙的现有文件。
- 普通升级方式，即 FTP Server 一边接收用户的文件，一边将其写入 Flash 中。采用这种方式，可能会因为断电等异常情况导致防火墙现有文件被损坏。与快速升级方式相比，普通升级方式只需要防火墙较少的空闲内存。

请在系统视图下进行下列配置。

表7-8 设置 FTP 升级方式

操作	命令
设置 FTP 升级方式	ftp update { fast normal }
恢复 FTP 缺省的升级方式	undo ftp update

缺省情况下，FTP 服务器采用快速升级方式。

说明：

当 FTP Server 将文件写入 Flash 中时，禁止用户使用 **reboot** 命令重启设备。

2. 设置 FTP 服务的连接时限

为了防止未授权用户的非法入侵，如果在一定时间内没有收到 FTP 用户的服务请求，则断开与该 FTP 客户端的连接。

请在系统视图下进行下列配置。

表7-9 配置 FTP 服务器的超时断连时间

操作	命令
配置 FTP 服务器的超时断开时间	ftp timeout minutes
恢复 FTP 服务器的超时断开时间的缺省值	undo ftp timeout

缺省情况下，连接空闲超时时间为 30 分钟。

3. 为 FTP Server 指定源接口或源 IP 地址

请在系统视图下进行下列配置。

表7-10 为 FTP Server 指定源接口或源 IP 地址

操作	命令
为 FTP Server 指定源接口	ftp-server source-interface interface-type interface-number
删除为 FTP Server 指定的源接口	undo ftp-server source-interface
为 FTP Server 指定发送报文中的源 IP 地址	ftp-server source-ip ip-address
删除为 FTP Server 指定的源 IP 地址	undo ftp-server source-ip

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

说明：

指定源 IP 地址和指定源接口命令是互斥的，后配置的命令将覆盖先前的配置。

7.2.5 FTP 服务器的显示和调试

在完成上述配置后，在任何视图下执行 **display** 命令可以显示配置后 FTP 的运行情况，通过查看显示信息验证配置的效果。

表7-11 FTP 服务器的显示和调试命令

操作	命令
查看 FTP 服务器	display ftp-server
显示当前为 FTP Server 设置的源 IP 地址	display ftp-server source-ip
查看登录的 FTP 用户	display ftp-user

display ftp-server 命令显示当前 FTP 服务器的配置情况，包括 FTP 服务器支持的最大用户数和超时断开时间。**display ftp-user** 显示登录的 FTP 用户的详细情况。

7.2.6 FTP 客户端介绍

防火墙可以作为 FTP 客户端与远程 FTP 服务器连接，并键入 FTP 客户端的命令来进行相应的操作。目前只支持一个 FTP 客户端。



注意：

- 当使用 Windows 操作系统的 Internet Explorer 作为 FTP 客户端时，建议使用指定用户名和密码的方式进行登录，即“ftp://username:password@ftp_server_ip”的形式。如果使用仅指定 FTP 服务器地址的方式登录，即“ftp://ftp_server_ip”的形式，则会提示登录不成功，这是因为 Comware 实现的 FTP 不支持匿名用户登录。这时可以单击鼠标右键，在菜单中选择“登录”后，输入正确的用户名和密码即可。
- 建议用户使用其它第三方 FTP 客户端软件进行 FTP 操作。

1. FTP 客户端操作命令

FTP 客户端可以执行的操作命令如：建立 FTP 连接，建立、删除目录等。具体命令应用详见“命令手册 FTP 客户端命令”一节。



说明：

当使用 FTP 客户端进行文件传输时，如果本地设备已存在同名文件，则用户需要手动删除该文件后再启动文件传输，以免造成 FTP 响应超时，导致连接中断。

2. 为 FTP Client 指定源接口或 IP 地址

请在系统视图下进行下列配置。

表7-12 为 FTP Client 指定源接口或 IP 地址

操作	命令
为 FTP Client 指定源接口	ftp source-interface <i>interface-type</i> <i>interface-number</i>
删除为 FTP Client 指定的源接口	undo ftp source-interface
为 FTP Client 指定发送报文中的源 IP 地址	ftp source-ip <i>ip-address</i>
删除为 FTP Client 指定的源 IP 地址	undo ftp source-ip

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

 说明：

指定源 IP 地址和指定源接口命令是互斥的，后配置的命令将覆盖先前的配置。

3. FTP 客户端的显示

在完成上述配置后，在任意视图下执行 **display** 命令。

表7-13 FTP 客户端的显示

操作	命令
显示当前为 FTP Client 设置的源 IP 地址	display tftp source-ip

7.2.7 使用 FTP 升级 Comware 应用程序典型配置举例 1

1. 组网需求

使用 FTP 升级 Comware 主体软件，防火墙作为 Client。FTP 服务器 IP 地址为 172.16.104.110。FTP 用户名为 ftpuser，密码为 pwd。

2. 组网图

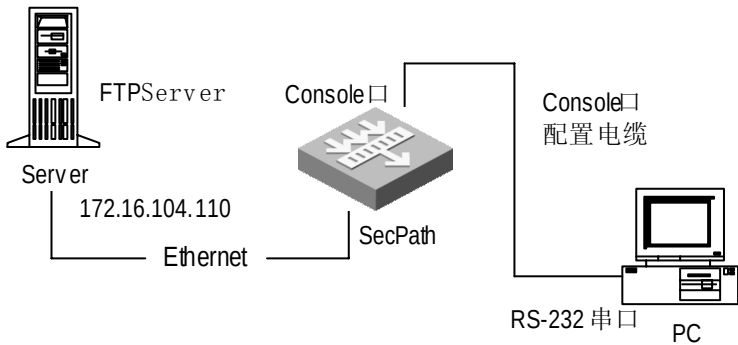


图7-1 利用 FTP Client 功能实现平滑升级

3. 配置步骤

请按如下方法进行操作：

（提示）删除防火墙存储设备中的多余文件，以保证剩余足够的空间，用于存储新的系统文件。

```
<H3C> dir
```

```
Directory of flash:/
```

```
  1  -rw-          939  Nov 29 2004 15:08:44  config.cfg
  2  -rw-    8985472  Dec 19 2004 14:52:08  main.bin
  3  -rw-          969  Oct 29 2004 16:10:20  sip.cfg
```

```
31877 KB total (17007 KB free)
```

```
<H3C> delete /unreserved sip.cfg
```

以 **FTP** 方式登录服务器，获取系统主体软件，并存放于防火墙存储设备的根目录下。

获取的系统文件必须存放在防火墙存储设备的根目录下（flash:），文件名为“system”。

```
<H3C> ftp 172.16.104.110
```

```
Trying 172.16.104.110 ...
```

```
Connected to 172.16.104.110.
```

```
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
```

```
User(172.16.104.110:(none)):ftppuser
```

```
331 Give me your password, please
```

```
Password:xxxxxxx
```

```
230 Logged in successfully
```

```
[ftp] binary
```

```
[ftp] get comware3.cc system
```

```
200 PORT command okay
```

```
150 "D:\ftppuser\system\comware3.cc" file ready to send (5805100 bytes) in
IMAGE / Binary mode
```

```
226 Transfer finished successfully.
```

```
FTP: 5805100 byte(s) received in 19.898 second(s) 291.74Kbyte(s)/sec.
```

```
[ftp] bye
```

升级成功后重新启动防火墙，运行升级的版本。

说明：

当在升级过程中时，若 **FTP** 服务器因故障或其它原因导致与防火墙（**FTP Client**）的连接中断时，用户可以通过键入 **<Ctrl+k>** 快捷键强行退出。

7.2.8 使用 FTP 升级 Comware 应用程序典型配置举例 2

1. 组网需求

使用 FTP 升级 Comware 主体软件，防火墙作为 Server。防火墙以太网口的 IP 地址为 172.16.104.110。FTP 用户名为 ftpuser，密码为 pwd。

2. 组网图

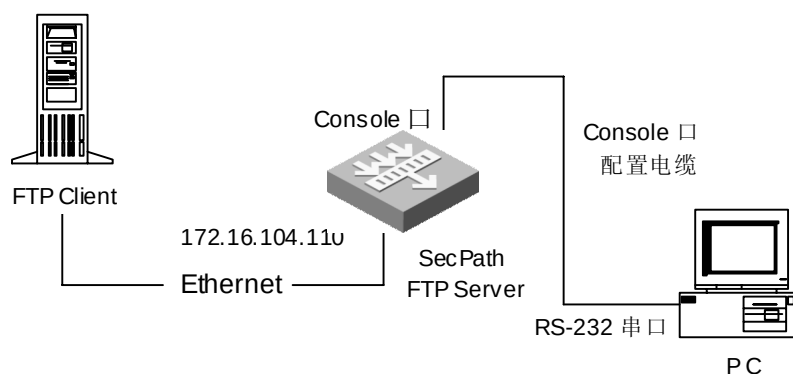


图7-2 利用 FTP Server 功能实现平滑升级

3. 配置步骤

(1) 配置防火墙

添加 FTP 授权用户名和密码。

```
[H3C] local-user ftpuser
[H3C-luser-ftpuser] password simple pwd
[H3C-luser-ftpuser] service-type ftp ftp-directory flash:/ftp/ftpuser
```

启动 FTP 服务。

```
[H3C] ftp server enable
```

（提示）删除防火墙存储设备中的多余文件，以保证剩余足够的空间，用于存储新的系统文件。

```
<H3C> dir
```

```
Directory of flash:/
```

	Permissions	Size	Date	Time	File Name
1	-rw-	939	Nov 29 2004	15:08:44	config.cfg
2	-rw-	8985472	Dec 19 2004	14:52:08	system
3	-rw-	969	Oct 29 2004	16:10:20	sip.cfg

```
31877 KB total (17007 KB free)
```

```
<H3C> delete /unreserved sip.cfg
```


(2) 配置 PC

以 FTP 方式登录防火墙，上传 Comware 软件，并存放于防火墙存储设备的根目录下。

```
ftp> put comware3.cc system
```

升级成功后重新启动防火墙，运行升级的版本。

说明：

利用 FTP 功能升级配置文件时，操作步骤与上述介绍完全一致，需要注意的是获取后的配置文件 config.cfg 同样要放在防火墙的根目录下（flash:）。

7.3 TFTP 配置

7.3.1 TFTP 简介

TFTP（Trivial File Transfer Protocol）是一种简单文件传输协议。相对于另一种文件传输协议 FTP，TFTP 不具有复杂的交互存取接口和认证控制，适用于客户机和服务器之间不需要复杂交互的环境。例如，在系统启动时，使用 TFTP 协议来获取系统的内存映像。TFTP 协议一般在 UDP 的基础上实现。

TFTP 传输是由客户端发起的。当需要下载文件时，先由客户端向 TFTP 服务器发送读请求包，然后从服务器接收数据包，并向服务器发送确认；当需要上传文件时，先由客户端向 TFTP 服务器发送写请求包，然后向服务器发送数据包，并接收服务器的确认。防火墙提供了 TFTP 客户端的功能。

7.3.2 TFTP 协议配置

1. 下载文件

请在用户视图下进行下列配置。

表7-14 用 TFTP 下载文件

操作	命令
用 TFTP 下载文件	tftp host [source-interface interface-type interface-number source-ip ip-address] { get sget } source-filename [destination-filename]

**注意：**

- 当采用安全方式下载时，要求当前系统有足够的内存空间和 Flash 空间以存放待下载文件。
- 不能使用安全方式下载系统应用程序。

2. 上传文件

请在用户视图下进行下列配置。

表7-15 用 TFTP 上传文件

操作	命令
用 TFTP 上传文件	tftp host [source-interface interface-type interface-number source-ip ip-address] put source-filename [destination-filename]

3. 设置相应的访问控制列表

该配置任务用来设置 TFTP 服务器访问控制列表，即与 **acl** 命令设置的访问控制列表相关联，实现对远端 TFTP 服务器地址的访问控制。

请在系统视图下进行下列配置。

表7-16 设置访问控制列表

操作	命令
指定可以访问 TFTP 服务器的访问控制列表	tftp-server acl acl-number
删除设置的访问控制列表	undo tftp-server acl

4. 为 TFTP Client 指定源接口或 IP 地址

请在系统视图下进行下列配置。

表7-17 为 TFTP Client 指定源接口或 IP 地址

操作	命令
为 TFTP Client 指定源接口	tftp source-interface interface-type interface-number
删除为 TFTP Client 指定的源接口	undo tftp source-interface
为 TFTP Client 指定发送报文中的源 IP 地址	tftp source-ip ip-address
删除为 TFTP Client 指定的源 IP 地址	undo tftp source-ip

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

 说明：

指定源 IP 地址和指定源接口命令是互斥的，后配置的命令将覆盖先前的配置。

7.3.3 TFTP 客户端的显示

在完成上述配置后，在任意视图下执行 **display** 命令。

表7-18 TFTP 客户端的显示

操作	命令
显示当前为 TFTP Client 设置的源 IP 地址	display tftp source-ip

7.4 配置文件管理

7.4.1 简介

1. 配置文件内容及格式

配置文件为一文本文件，其格式如下：

- 以命令格式保存。
- 为了节省空间，只保存非缺省的参数（各配置参数的缺省值详见以后各章节）。
- 命令的组织以命令视图为基本框架，同一命令视图的命令组织在一起，形成一节，节与节之间通常用空行或注释行隔开（以#开始的为注释行）。空行或注释行可以是一行或多行。
- 节的顺序安排通常为：全局配置、物理接口配置、逻辑接口配置、路由协议配置等。
- 以 **return** 为结束。

2. 查看防火墙配置

使用 **save** 命令保存的防火墙配置以文件形式存放在 **Flash** 之中。防火墙启动时，根据从 **Flash** 中读取的配置文件进行防火墙的初始化工作，因此，该配置文件中的配置称为起始配置。运行过程中，防火墙正在使用的配置称为当前配置，当前配置存放在防火墙的内存之中，在防火墙重启之后就会丢失。

请在任何视图下，进行下列操作。

表7-19 查看防火墙配置

操作	命令
显示下次启动时加载的配置文件	display saved-configuration [<i>by-linenum</i>]
显示系统本次启动及下次启动使用的配置文件	display startup
显示当前视图的配置	display this
显示防火墙的当前的运行配置	display current-configuration [<i>interface</i> <i>interface-type</i> [<i>interface-number</i>] configuration [<i>isp</i> <i>zone</i> <i>interzone</i> <i>radius-template</i> <i>system</i> <i>user-interface</i>]] [<i>by-linenum</i>] [{ <i>begin</i> <i>include</i> <i>exclude</i> } <i>string</i>]

 说明：

配置文件的显示格式与保存格式相同。

3. 保存当前配置

通过命令行接口，用户可以修改防火墙当前配置。为了使当前配置能够作为防火墙下次上电时的起始配置，需要用 **save** 命令保存当前配置到 Flash 中，形成配置文件。请在所有视图下进行下列操作。

表7-20 保存当前配置

操作	命令
保存当前配置	save [<i>file-name</i> safely]

当没有指定 *file-name* 时，配置文件缺省保存到下次启动加载的配置文件中。

不带 **safely** 参数表示快速保存配置文件，保存过程中不能对设备进行重启、断电等。否则，会丢失配置文件。带有 **safely** 参数，保存配置文件的速度会慢一点。但是，如果保存过程中出现设备重启、断电等问题，配置文件会在 Flash 中一直保存，不会丢失。

缺省方式下，采用快速保存模式。对于电源稳定程度较好的环境，推荐使用默认的快速模式。对于电源环境恶劣，或者远程维护等情况，推荐使用带有 **safely** 参数的保存配置命令。

 说明：

为了保证防火墙重启之后能够使用与当前相同的配置，在重启防火墙之前，建议用户使用 **save** 命令保存配置。

4. 擦除配置文件

用 **reset saved-configuration** 命令可以删除 Flash 中保存的下次启动时加载的配置文件。配置文件被删除后，防火墙下次上电时将采用缺省的或预先指定的配置文件进行初始化，以下几种情况时，需要删除存储设备中的配置文件：

- 在防火墙软件升级之后，可能会引起防火墙软件和配置文件不匹配。
- 发现配置文件遭到破坏，如加载了错误的配置文件。

删除配置文件后，可用 **save** 命令保存当前配置为新的配置文件。

请在用户视图下进行下列操作。

表7-21 擦除存储设备中的配置文件

操作	命令
删除 Flash 中保存的下次启动时加载的配置文件	reset saved-configuration

5. 设置系统下次启动时使用的配置文件

请在用户视图下进行下列操作。

表7-22 设置系统下次启动时使用的配置文件

操作	命令
设置系统下次启动时使用的配置文件	startup saved-configuration filename

7.4.2 配置文件命名及启动时的选择顺序

1. 配置文件的命名

config.cfg：是用户保存配置的缺省文件名，名字由厂商规定，内容可由用户修改。

2. 配置文件的选择顺序

系统启动时配置文件的选择顺序分为如下三种情况：

- (1) 如果用户没有设置跳过配置文件启动，就按下面（2）、（3）的顺序进行选择；
否则，以空配置启动：
- (2) 如果用户指定了启动的配置文件，则按下面的顺序进行选择：
 - 若配置文件存在，则以该文件为启动配置文件。
 - 若配置文件不存在，以空配置启动。
- (3) 如果用户不指定启动配置文件，则按下面的顺序进行选择。
 - 若 **config.cfg** 存在，则以 **config.cfg** 为启动文件；
 - 若 **config.cfg** 不存在，则以空配置启动。

7.4.3 备份配置文件

配置文件可以通过以下三种方法备份下来：

- 备份 **display current-configuration** 命令显示。
- 通过 FTP 备份。
- 通过 TFTP 备份

1. 备份 current-configuration 命令显示

使用 **display current-configuration** 命令可以显示防火墙的所有配置（缺省配置除外）。在超级终端中，拷贝其中所有的配置显示内容到一个文本文件中，就可以备份配置文件。

2. 通过 FTP 备份

通过 FTP 备份配置文件有两种方法：

一是防火墙作为 **FTP Server**，将防火墙上的配置文件下载到 PC（**FTP Client**）上。

防火墙启动后，进行如下配置：

```
[H3C] local-user ftpuser
[H3C-luser-ftpuser] password simple pwd
[H3C-luser-ftpuser] service-type ftp ftp-directory flash:/ftp/ftpuser
```

然后在已经与防火墙连通的 PC 上建立到防火墙的 FTP 连接，并备份配置文件：

```
C:\>ftp x.x.x.x
<ftp> get remotefile [localfile]
200 Port command okay.
150 Server okay , now transmit file .
226 file transmit success.
ftp: 735 bytes received in 0.06Seconds 12.25Kbytes/sec.
```

其中 *remotefile* 文件为防火墙上的配置文件。

二是防火墙作为 **FTP Client**，将防火墙中的配置文件上传到 PC（**FTP Server**）中。

在已经与防火墙连通的 PC 上启动 **FTP Server** 并配置授权信息，然后在防火墙上执行如下命令：

```
<H3C> ftp x.x.x.x
[ftp] put localfile [ remotefile ]
```

其中 *localfile* 文件应为防火墙上的配置文件。

3. 通过 TFTP 备份

防火墙作为 **TFTP Client**，将防火墙上的配置文件上传到 PC（**TFTP Server**）上。

在防火墙上执行如下命令：

```
<H3C> tftp x.x.x.x put localfile [ remotefile ]
```

其中 *localfile* 文件应为防火墙上的配置文件, *remotefile* 为上传到 TFTP Server 后保存的配置文件名。

第8章 用户界面配置

8.1 用户界面简介

8.1.1 用户界面概述

用户界面视图（User-interface view）是与接口视图类似的视图，是系统提供的一种新的视图，用来管理那些工作在流方式下的异步物理和逻辑接口。由于这类接口常用于对系统进行配置管理，因此，通过用户界面视图，可以达到统一管理各种用户配置的目的。

目前系统支持的配置方式有：

- Console 口本地配置。
- AUX 口本地或远程配置。
- Telnet 或 SSH 本地或远程登录配置。

与这些配置方式对应的是三种类型的用户界面：

- CON 口（Console）

“控制口”（Console port）是一种线设备端口，防火墙提供一个 Console 口，端口类型为 EIA/TIA-232 DCE，便于我们进行配置。

- AUX 口（AUX）

“辅助端口”（Auxiliary port）也是一种线设备端口，防火墙提供一个 AUX 口，端口类型为 EIA/TIA-232 DTE，通常用于通过 Modem 进行拨号访问。

- 虚拟线路（VTY）

“虚拟连接”（Virtual port）属于逻辑终端线，用于对防火墙进行 Telnet 访问，通常简称为 VTY。

8.1.2 用户界面的编号

用户界面的编号有两种方式：绝对编号方式和相对编号方式。

1. 绝对编号方式

系统的用户界面共分三类，并按照一定的先后顺序排列：

分别是控制台（CON）、辅助接口（AUX）、虚拟接口（VTY）三种类型。控制台和辅助接口分别只有一个；VTY 类型的用户界面可能有多个，而每种类型的多个用户界面内部又按照顺序排列。绝对编号的起始编号是 ui0（即 CON 口），其它接口

依次类推。CON、AUX 口各占一个编号；VTY 接口，不同产品可以支持的数量不同，请使用 **display user-interface** 查看即可得知。绝对编号可以唯一的指定一个用户界面或一组用户界面。

2. 相对编号方式

相对编号方式的形式是：“用户界面类型”+“编号”。此编号是每种类型的用户界面的内部编号。此种编号方式只能指定某种类型的用户界面中的一个或一组，而不能跨类型操作。相对编号方式遵守的规则如下：

- 控制台的编号：con 0；
- 辅助线的编号：aux 0；
- VTY 的编号：第一条为 VTY 0，第二条为 VTY 1，依此类推。

8.2 用户界面配置步骤

用户界面配置包括：

- 进入 User-interface 视图
- 配置用户界面支持的协议
- 配置异步接口属性
- 配置终端属性
- 用户管理
- Modem 属性设置
- 配置自动执行命令
- 配置 VTY 类型用户界面的呼入/呼出限制

8.2.1 进入用户界面视图

在系统视图下，键入相应的命令，即进入相应的用户界面视图。可以进入单一用户界面视图，对一个 User-interface 进行配置，也可以进入多条用户界面视图，同时配置多条 User-interface。

表8-1 进入用户界面视图

操作	命令
进入单一用户界面视图或多个用户界面视图	user-interface [<i>type-keyword</i>] <i>number</i> [<i>ending-number</i>]

进入 User-interface aux 口视图。

```
[H3C] user-interface aux 0
[H3C-ui-aux0]
```

在用户界面视图下，可以配置和管理接口的属性，包括：

- (1) 异步属性：速率（**speed**），流控方式（**flowcontrol**），校验（**parity**），停止位（**stopbits**），数据位（**databits**）。
- (2) 终端属性配置：使能终端服务功能（**shell**），终端用户超时断开设定（**idle-timeout**），设置终端屏幕的一屏长度（**screen-length**），验证配置，设置历史命令缓冲区大小。
- (3) 优先级设置：设置通过用户界面登录系统的用户的优先级。
- (4) Modem 属性配置：Modem 和脚本配置。

8.2.2 设置所在用户界面支持的协议

该配置任务用来指定所在的用户界面支持的协议，缺省为支持所有协议，包括 Telnet 和 SSH。

请在 VTY 类型的用户界面视图下进行下列配置。

表8-2 设置所在用户界面支持的协议

操作	命令
设置所在用户界面支持的协议	protocol inbound { all ssh telnet }

8.2.3 配置异步接口属性

在用户界面视图下，可以配置其异步属性。这些配置命令都只有工作在异步流方式下才有效。

请在用户界面视图下进行下列配置。

1. 配置传输速率

表8-3 配置传输速率

操作	命令
设置传输速率	speed speed-value
恢复传输速率的缺省值	undo speed

异步口支持的传输速率有：

- 1200bps
- 2400bps
- 4800bps
- 9600bps

- 19200bps
- 38400bps
- 57600bps
- 115200bps

缺省的异步口传输速率为 9600bps。

2. 配置流控方式

表8-4 配置流控方式

操作	命令
配置流控方式	flow-control { none software hardware }
恢复流控方式为缺省方式	undo flow-control

AUX 口缺省的流控方式为硬件流控。

参数说明如下：

none: 不进行流控。

software: 进行软件流控。

hardware: 进行硬件流控，只对 AUX 口有效。

3. 设置校验位

表8-5 设置校验位

操作	命令
设置校验位	parity { none even odd mark space }
设置校验位为缺省值	undo parity

参数说明如下：

none: 无校验。

even: 进行偶校验。

odd: 进行奇校验。

mark: 进行 mark 校验。

space: 进行 space 校验。

缺省为 **none**，不进行校验。

4. 设置停止位

表8-6 设置停止位

操作	命令
设置停止位	stopbits { 1.5 1 2 }
恢复停止位为缺省值	undo stopbits

停止位的缺省值是 1。

5. 设置数据位

表8-7 设置数据位

操作	命令
设置数据位	databits { 5 6 7 8 }
恢复数据位为缺省值	undo databits

异步口支持的数据位为：5，6，7，8。

缺省为 8 位数据位。

8.2.4 配置终端属性

1. 启动终端服务功能

请在用户界面视图下进行下列配置。

表8-8 启动终端服务功能

操作	命令
启动终端服务	shell
禁止终端服务	undo shell



注意：

缺省在所有的用户界面上启动终端服务。

例如：

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] undo shell
```

对于当前执行该命令的 Telnet 用户没有影响，其它的 Telnet 用户都将被迫下线，而新发起的 Telnet 连接也无法建立。例如，当前有两个 Telnet 用户，分别登录到 vty1 和 vty2，当 vty1 用户在 vty2 视图下执行 **undo shell** 命令时，vty2 用户将被迫下线。

2. 终端用户超时断开设定

请在用户界面视图下进行下列配置。

表8-9 设置终端用户超时断开功能

操作	命令
设置用户超时断连功能	idle-timeout <i>minutes</i> [<i>seconds</i>]
恢复用户超时断连缺省值	undo idle-timeout

缺省为启动终端用户定时断开功能，时间为 10 分钟。也就是说，如果 10 分钟没有操作，此终端线路自动断开。用户可以配置 **idle-timeout 0**，即关闭定时断开功能。

3. 配置锁住用户界面

请在用户视图下进行下列配置。

该配置用来锁住当前使用的终端线路，并提示您输入密码。防止当您离开时，其它人对该终端线路进行操作。

表8-10 锁住用户界面

操作	命令
配置锁住用户界面	lock

当前以 VTY 1 线路登录防火墙，有事要离开，需要锁住 user-interface vty 1:

```
<H3C> lock
Password:xxxx
Again:xxxx
```

4. 设置终端屏幕的一屏长度

请在用户界面视图下进行下列配置。

表8-11 设置终端屏幕的一屏长度

操作	命令
设置终端屏幕的一屏长度	screen-length <i>screen-length</i>
恢复终端屏幕一屏长度的缺省设置	undo screen-length

终端屏幕一屏长度的缺省为 24 行。

screen-length 0 表示关闭分屏功能。

undo screen-length 表示恢复缺省设置。

5. 设置历史命令缓冲区大小

请在用户界面视图下进行下列配置。

表8-12 设置历史命令缓冲区大小

操作	命令
设置历史命令缓冲区大小	history-command max-size <i>size-value</i>
恢复历史命令缓冲区大小为缺省值	undo history-command max-size

size-value 为历史缓冲区大小。缺省值为 10，意味着缺省可存放 10 条历史命令。

6. 配置用户界面之间传递消息

请在用户视图下进行下列配置。

表8-13 配置在用户界面之间传递消息

操作	命令
设置在用户界面间传递消息	send { all <i>number</i> <i>type-name number</i> }

8.2.5 Modem 属性配置

在异步口通过 **modem** 拨入，通过用户界面视图可管理和配置 **modem** 的有关参数，相关配置命令只对 AUX 口有效。

表8-14 modem 配置

操作	命令
设置系统收到了 RING 信号到等待 CD_UP 的时间间隔	modem timer answer <i>seconds</i>
恢复系统缺省的收到 RING 信号到等待 CD_UP 的时间间隔	undo modem timer answer
设置自动应答	modem auto-answer
设置手动应答	undo modem auto-answer
设置呼入呼出开关	modem [call-in call-out both]
设置禁止呼入呼出	undo modem [call-in call-out both]

在 **aux** 口设置 **modem** 自动应答。

```
[H3C-ui-aux0] modem auto-answer
```

8.2.6 配置自动执行命令

auto-execute command 命令使用时有如下的限制：

- Console 口不支持 **auto-execute command**。
- 如果防火墙上只有一个 AUX 口，没有 Console 口（Console 口和 AUX 口共用），则此 AUX 口也不支持 **auto-execute command**。
- 对其他类型的接口不做限制。

用户在登录时，自动执行某条在该终端上用 **auto-execute command** 配置好的命令，命令执行结束后，自动断开用户线。

通常的用法是，在终端用 **auto-execute command** 配置 Telnet 命令，使用户自动连接到指定的主机。



注意：

使用该命令后，将导致不能通过该终端线对本系统进行常规配置，需谨慎使用。

在配置 **auto-execute command** 命令并保存配置（执行 **save** 操作）之前，要确保可以通过其他方法登录系统，以去掉此配置。

请在用户界面视图下进行下列配置。

表8-15 设置自动执行命令

操作	命令
设置自动执行命令	auto-execute command <i>command</i>
取消自动执行命令	undo auto-execute command

配置自动执行命令后，在用户重新登录时，自动执行此命令。

用户登录后，实现自动执行 **telnet** 命令，登录到目的主机。

执行步骤为：

(1) 在用户界面视图下，执行 **auto-execute command** 命令。

```
[H3C-ui4] auto-execute command telnet 10.110.100.1
```

(2) 退出系统视图，重新登录，自动执行 **telnet 10.110.100.1** 命令。

8.2.7 配置 VTY 类型用户界面的呼入呼出限制

该配置通过引用 ACL 控制列表，对 VTY（Telnet）类型的用户界面的呼入/呼出权限进行限制。

请在用户界面视图下进行下列配置。

表8-16 配置 VTY 类型用户界面的呼入呼出限制

操作	命令
配置 VTY 类型用户界面的呼入/呼出限制	acl <i>acl-number</i> { inbound outbound }
取消 VTY 类型用户界面的呼入/呼出限制	undo acl { inbound outbound }

8.3 用户界面的显示和调试

8.3.1 显示用户界面的使用信息

请在任何视图下进行下列操作。

表8-17 显示每个用户界面的用户使用信息

操作	命令
显示用户界面的使用信息	display users [all]

8.3.2 显示用户界面的物理属性和一些配置

请在任何视图下进行下列操作。

表8-18 显示用户界面的物理属性和一些配置

操作	命令
显示用户界面的物理属性和一些配置	display user-interface [[<i>type-name</i>] <i>number</i>] [summary]

第9章 用户管理

9.1 用户管理概述

第一次启动防火墙时，防火墙没有设置用户名和口令。在不对登录用户进行验证的情况下，只要将计算机终端通过 **Console** 口与防火墙连接，任何用户可以对防火墙进行配置；如果为接口配置了 IP 地址，任何远端用户可能使用 **Telnet** 登录到防火墙；远端用户还可能与防火墙建立 **PPP** 连接从而访问网络。这显然对防火墙和网络是不安全的。为此需要为防火墙创建用户，并为用户设置口令，对用户进行管理。

 说明：

本章侧重于阐述 **Terminal** 用户及 **Telnet** 用户的认证管理，其他用户及 **AAA RADIUS/HWTACACS** 认证方面的内容请参见本手册的“安全”部分。

9.1.1 用户分类

从用户所获得的服务来划分，可以将防火墙的用户划分为：

- **Terminal** 用户，通过 **Console** 口或 **AUX** 口登录到防火墙；
- **Telnet** 用户，使用 **Telnet** 命令登录到防火墙；
- **FTP** 用户，与防火墙建立 **FTP** 连接进行文件传输；
- **PPP** 用户，与防火墙建立 **PPP** 连接（例如拨号、**PPPoE** 等），从而访问网络；
- **SSH** 用户，与防火墙建立 **SSH** 连接，登录到防火墙；

一个用户可能同时获得几种服务，这样只需一个用户便可以执行多种功能。

9.1.2 用户的优先级

系统可以对超级终端用户和 **Telnet** 用户进行分级管理。与命令的优先级一样，用户的优先级分为参观（**Visit**）、监控（**Monitor**）、系统（**System**）、管理（**Manage**）4 个级别，级别标识为 0~3。用户所能访问命令的级别，由用户的级别确定。如果不对用户进行认证或采用 **password** 认证的情况下，登录到防火墙的用户所能访问的命令级别由登录所使用的用户界面的级别确定。

用户所能访问的命令包括用户级别的命令以及低于用户级别的命令，例如用户的级别为 2，则用户可以访问级别为 0、1、2 的命令。级别为 3 的用户可以访问所有的命令。各级别用户所能访问的命令如表 9-1 所示。

表9-1 用户优先级

用户级别	名称	所能访问的命令
0	参观	ping、tracert、telnet、rsh、nslookup、super、language-mode、display、quit
1	监控	0 级命令、reboot、reset、send、terminal、undo、upgrade、debugging
2	系统	所有配置命令（管理级的命令除外）和 0、1 级命令
3	管理	所有命令

说明：

管理级的命令是指文件系统命令、设置用户界面的验证方式和用户访问级别、FTP 命令、TFTP 命令。

9.1.3 认证方案

用户登录防火墙时，系统会对用户的身份进行认证。对用户的认证有 4 种方案：不认证、password 认证、本地认证、AAA 服务器认证。不认证即不需用户名和口令，就可登录防火墙。为安全起见，不认证方案是不可取的。password 认证只需口令，不需用户名，可以获得一定的安全性。本地认证需要用户提供用户名和口令，该用户名和口令必须与防火墙上的配置保持一致；AAA 服务器认证也需要用户提供用户名和口令，该用户名和密码必须与 AAA 服务器上配置的一致，拨号用户常采用这种认证方案。

对 Telnet 用户和 Terminal 用户一般采用本地认证。

9.1.4 规划防火墙的用户

可以根据需要规划防火墙的用户。通常，防火墙至少需要创建一个超级终端用户——Console 用户。如果需从远端使用 Telnet 登录到防火墙，则需配置一个 Telnet 用户。为了让远端用户向防火墙加载或下载文件，可以配置 FTP 用户。为了让用户通过与防火墙建立的 PPP 连接访问网络，则需要配置 PPP 用户。

本章主要介绍如何配置 Telnet 用户和超级终端用户。FTP 用户的配置请参考本模块的《文件管理》中的 FTP 配置的内容。PPP 用户的配置请参考本手册的“用户接入”及“安全”部分的内容。

9.2 配置用户

配置用户的任务包括：

- 配置认证用户的方式
- 配置用户名及口令
- 设置用户优先级
- 设置用户按命令行进行计费

认证用户的作用是使合法用户能登录并使用防火墙，非法用户不能通过认证而不能使用防火墙。

9.2.1 配置认证用户的方式

配置认证用户的方式是用来设置指定用户登录防火墙时所需的认证方法。

请在用户界面视图下，执行如下的命令：

表9-2 配置认证用户的方式

操作	命令
设置进行用户认证	authentication-mode { password scheme [command-authorization] }
设置不进行用户认证	authentication-mode none

关键字 **none** 表示不认证用户身份。关键字 **password** 表示认证不需用户名，只需口令字。**scheme** 表示使用 AAA 配置的认证方案进行认证（包括本地认证方案和 RADIUS、HWTACACS 认证，具体认证方案由 **scheme** 命令来指定）。

VTY 类型（即 Telnet、SSH 用户）、AUX 的用户界面缺省为 **password** 方式认证，其它类型用户界面缺省不进行终端认证。

在配置 Telnet 用户和 Teminal 用户的认证方式时，通常设置为 **scheme** 方式中的本地认证方案。

scheme 认证方式请参考本手册的“安全”部分。

9.2.2 配置用户名及口令

1. 设置 password 方式认证的口令

如果在配置认证方式时选择 **password** 方式进行用户认证，则需设置 **password** 认证的口令。

请在用户界面视图下进行如下配置。

表9-3 设置 password 认证的口令

操作	命令
设置 password 认证的口令	set authentication password { cipher simple } password
取消 password 认证的口令	undo set authentication password

cipher 表示配置密文密码，**simple** 表示配置明文密码。

2. 设置进行本地认证的用户名和口令

如果选择本地认证，则需先设置用户名和口令。

表9-4 配置进行 AAA 本地认证的用户名及口令

操作	命令
配置用户（系统视图）	local-user user-name
取消用户（系统视图）	undo local-user { user-name all }
设置本地用户的密码（本地用户视图）	password { cipher simple } password
取消本地用户的密码（本地用户视图）	undo password

cipher 表示配置密文密码，**simple** 表示配置明文密码。

然后配置用户使用本地认证方案。

表9-5 配置域用户使用本地认证方案

操作	命令
创建一个 ISP 域，或者进入已创建 ISP 域的视图（系统视图）	domain { isp-name default { disable enable isp-name } }
删除指定的 ISP 域（系统视图）	undo domain isp-name
配置当前 ISP 域用户使用本地认证方案（ISP 域视图）	scheme local

9.2.3 设置用户的优先级

用户所能访问的系统命令可以从两方面进行限制，一个是用户界面的优先级，一个是用户的优先级。

1. 设置用户界面的优先级

本命令可以设置各用户界面的优先级。

请在用户界面视图下进行下列配置。

表9-6 设置用户界面的优先级

操作	命令
设置用户界面的优先级	user privilege level <i>level</i>
恢复用户界面缺省的优先级	undo user privilege level

Console 口对应的优先级缺省为 3，其它用户界面的优先级缺省为 0。

例如，设置 Console 口的优先级为 3，VTY 0 的优先级为 2。

[H3C-ui-console0] user privilege level 3

[H3C-ui-vty0] user privilege level 2

这样当同一个用户分别从 CON 口和 VTY 0 登录时，其所能访问的命令是不同的（假设从这 2 个用户界面登录时均不需要认证）。当他从 CON 口登录时，可以使用所有的命令；但当他从 VTY 0 登录时，只能访问 2 级以下的命令。

2. 设置用户的优先级

本命令可以根据用户名来配置指定用户的优先级。

请在本地用户视图下进行下列配置。

表9-7 设置用户优先级

操作	命令
设置用户优先级	level <i>level</i>
恢复用户优先级的默认值	undo level

level 代表用户的优先级，其范围是 0~3。0 级别最低，3 级别最高。在配置用户以后，用户默认的优先级为 0。

说明：

如果配置的认证方式为不认证或采用 password 认证，则用户登录到系统后所能访问的命令级别由用户界面的优先级确定。如果配置的认证方式需要用户名和口令，则用户登录系统后所能访问的命令级别由用户的优先级确定。

9.2.4 设置用户按命令行进行计费

请在用户界面视图下执行下面命令。

表9-8 设置用户按命令行进行计费

操作	命令
配置 Terminal 用户登录用户界面后以命令行方式进行计费	accounting commands scheme
取消 Terminal 用户的命令行计费	undo accounting commands scheme

缺省情况下，未设定命令行计费。

9.3 显示用户信息

在配置了用户账号后，可以使用下面的命令显示所配置的用户、本地用户以及在线用户信息。

请在所有视图下进行下列操作。

表9-9 显示用户信息

操作	命令
显示用户界面的使用信息	display users [all]
查看本地用户列表	display local-user

9.4 用户管理举例

9.4.1 使用 password 方式认证用户

要求对从 VTY 0 登录的用户进行 password 认证，用户登录时需要输入口令 **pwd** 才能登录成功，用户优先级为 3。操作命令如下：

```
<H3C> system-view
[H3C] user-interface vty 0
[H3C-ui-vty0] authentication-mode password
[H3C-ui-vty0] set authentication password simple pwd
[H3C-ui-vty0] user privilege level 3
```

9.4.2 使用本地用户数据库进行用户认证

要求用户从 VTY 0 登录时输入已配置的用户名 **myuser** 和对应的口令 **pwd**，用户名和口令正确才能登录成功。操作命令如下：

```
<H3C> system-view
[H3C] user-interface vty 0
[H3C-ui-vty0] authentication-mode scheme
```

```
[H3C-ui-vty0] quit
[H3C] local-user myuser
[H3C-luser-myuser] password simple pwd
[H3C-luser-myuser] service-type telnet
[H3C-luser-myuser] level 3
[H3C] domain system
[H3C-isp-system] scheme local
```

第10章 NTP 配置

10.1 NTP 协议简介

网络时间协议（Network Time Protocol，简称 NTP）是用来在整个网络内发布精确时间的 TCP/IP 协议，其本身的传输基于 UDP。其基本原理如下：

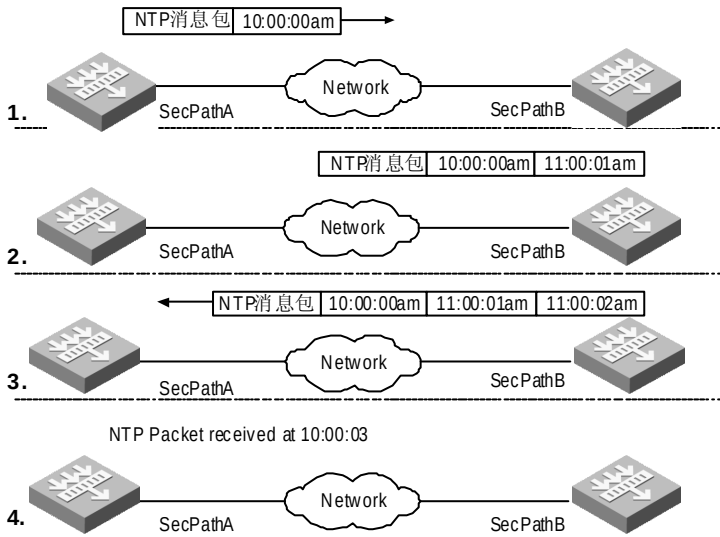


图10-1 NTP 基本原理图

上图所示的是 NTP 基本工作原理，防火墙 A 和防火墙 B 通过网络相连，它们都有自己独立的系统时钟，要实现各自系统时钟的自动同步，作如下假设：

- 在防火墙 A 和 B 的系统时钟同步之前，防火墙 A 的时钟设定为 10:00:00am，防火墙 B 的时钟设定为 11:00:00am。
- 以防火墙 B 为 NTP 时间服务器，即防火墙 A 将使自己的时钟与防火墙 B 的时钟同步。
- 数据包在防火墙 A 和 B 之间单向传输所需要的时间为 1 秒。

系统时钟同步的工作过程如下：

- 防火墙 A 发送一个 NTP 消息包给防火墙 B，该消息包带有它离开防火墙 A 时的时间戳，该时间戳为 10:00:00am（ T_1 ）。
- 当此 NTP 消息包到达防火墙 B 时，防火墙 B 加上自己的时间戳，该时间戳为 11:00:01am（ T_2 ）。

- 当此 NTP 消息包离开防火墙 B 时，防火墙 B 再加上自己的时间戳，该时间戳为 11:00:02am (T_3)。
- 当防火墙 A 接收到该响应消息包时，加上一个新的时间戳，该时间戳为 10:00:03am (T_4)。

至此，防火墙 A 已经拥有足够的信息，来计算两个重要的参数：

- NTP 消息来回一个周期的时延 $\text{Delay} = (T_4 - T_1) - (T_3 - T_2)$ 。
- 防火墙 A 相对防火墙 B 的时间差 $\text{offset} = ((T_2 - T_1) + (T_3 - T_4)) / 2$ 。

这样，防火墙 A 就能够根据这些信息，来设定自己的时钟，使之与防火墙 B 的时钟同步。

这只是 NTP 工作原理的一个粗略描述，在 RFC1305 规范中，NTP 使用复杂的算法，来确保时钟同步的精确性。

根据网络结构以及防火墙在网络中的位置，NTP 有六种工作模式，其中前两种模式也称单播模式。

- 设置远程服务器为本地时间服务器，此时本地防火墙工作在 **client** 模式。在这种工作模式下，只能是本地客户机同步到远程服务器，而远程服务器不会同步到本地客户机；
- 设置远程服务器作为本地防火墙的对等体，本地运行在 **symmetric active** 模式（即主动模式）在。这种配置下，本地服务器能同步到远程服务器（被动模式），远程服务器也能同步到本地服务器。如果双方都有参考时钟，以层数小的为准；
- 设置本地防火墙的一个接口发送 NTP 的广播消息包，此时，本地防火墙工作在广播服务器模式；
- 设置本地防火墙的一个接口接收 NTP 的广播信息包，此时，本地防火墙工作在广播客户模式；
- 设置本地防火墙的一个接口发送 NTP 组播消息包，本地防火墙运行在组播服务器模式；
- 设置本地防火墙的一个接口接收 NTP 组播消息包，本地防火墙运行在组播客户模式。

前两种模式，也即单播模式，支持 NTP 多实例，可以实现 MPLS VPN 网络的时间同步，即物理位置不同的网络设备（CE、PE），只要属于同一个 VPN，就可以通过 MPLS VPN 相连来获得时间同步。具体功能如下：

- CE 上的 NTP Client 可以同步到 PE 上 NTP Server；
 - PE 上的 NTP Client 可以通过指定的 VPN 实例同步到 CE 上的 NTP Server；
- PE 上的 NTP Server 可以支持同步多个不同 CE 上的 NTP Client。

10.2 NTP 协议配置

NTP 协议用于整个网络内的时间同步，NTP 配置包括：

- 配置 NTP 工作模式
- 设置 NTP 身份验证功能
- 设置本地发送 NTP 消息的接口
- 设置本地时钟作为 NTP 主时钟
- 允许/禁止接口接收 NTP 消息
- 设置对本地防火墙服务的访问控制权限
- 设置本地允许建立的 sessionss 的数目

10.2.1 配置 NTP 工作模式

根据网络结构以及防火墙在网络中的位置，可设置六种 NTP 工作模式。

- 配置 NTP 服务器模式
- 配置 NTP 对等体模式
- 配置 NTP 广播服务器模式
- 配置 NTP 广播客户模式
- 配置 NTP 组播服务器模式
- 配置 NTP 组播客户模式

1. 配置 NTP 服务器模式

设置以 *X.X.X.X* 或 *server-name* 所指定的远程服务器作为本地时间服务器。*X.X.X.X* 是一个主机地址，不能为广播、组播地址或参考时钟的 IP 地址。本地防火墙工作在 **client** 模式，在这种工作模式下，只能是本地客户机同步到远程服务器，而远程服务器不会同步到本地客户机。当在 PE 上指定了 *vpn-instance-name* 时，PE 上的 NTP 客户端通过指定的 VPN 实例可以同步 CE 上的 NTP 服务器，此时远程服务器不会同步到本地客户机。

请在系统视图下进行下列配置。

表10-1 配置 NTP 服务器模式

操作	命令
配置 NTP 服务器模式	ntp-service unicast-server [<i>vpn-instance vpn-instance-name</i>] { <i>X.X.X.X</i> <i>server-name</i> } [version <i>number</i> authentication-keyid <i>keyid</i> source-interface <i>interface-type</i> <i>interface-number</i> priority] *
取消 NTP 服务器模式	undo ntp-service unicast-server { <i>X.X.X.X</i> <i>server-name</i> }

NTP 版本号 *number* 范围是 1~3, 缺省值为 3; 身份验证密钥 ID 号 *keyid* 范围为 1~4294967295; *interface-type interface-number* 指定一个接口, 本地防火墙给时间服务器发送 NTP 消息时, 消息包中的源 IP 地址从该接口获取; **priority** 指定该时间服务器为优先选择的时间服务器。

2. 配置 NTP 对等体模式

设置以 *X.X.X.X* 或 *server-name* 所指定的远程服务器作为本地的对等体, 本地运行在 **symmetric active** 模式。*X.X.X.X* 是一个主机地址, 不能为广播、组播地址或参考时钟的 IP 地址。在这种配置下, 本地防火墙能同步到远程服务器, 远程服务器也能同步到本地服务器。当在 PE 上指定了 *vpn-instance-name* 时, PE 上的本地 NTP 服务器通过指定的 VPN 实例可以同步到 CE 上的 NTP 服务器, 同时 CE 的 NTP 服务器也能同步到 PE 的 NTP 服务器。

请在系统视图下进行下列配置。

表10-2 配置 NTP 对等体模式

操作	命令
配置 NTP 对等体模式	ntp-service unicast-peer [vpn-instance <i>vpn-instance-name</i>] { <i>X.X.X.X</i> <i>server-name</i> } [version <i>number</i> authentication-key <i>keyid</i> source-interface <i>interface-type interface-number</i> priority] *
取消 NTP 对等体模式	undo ntp-service unicast-peer { <i>X.X.X.X</i> <i>server-name</i> }

NTP 版本号 *number* 范围是 1~3, 缺省值为 3; 身份验证密钥 ID 号 *keyid* 范围为 1~4294967295; *interface-type interface-number* 指定本地防火墙给对等体发送 NTP 消息时, 消息包中的源 IP 地址从该接口获取; **priority** 指定该对等体为优先选择的时间服务器。

3. 配置 NTP 广播服务器模式

指定本地防火墙上一个接口来发送 NTP 广播消息包, 本地运行在广播服务器模式, 作为广播服务器周期性地发送广播消息到广播客户端。

请在接口视图下进行下列配置。

表10-3 配置 NTP 广播服务器模式

操作	命令
配置 NTP 广播服务器模式	ntp-service broadcast-server [authentication-keyid <i>keyid</i> version <i>number</i>] *
取消 NTP 广播服务器模式	undo ntp-service broadcast-server

NTP 版本号 *number* 范围是 1~3, 缺省值为 3; 身份验证密钥 ID 号 *keyid* 范围 1~4294967295; 此命令必须在欲发送 NTP 广播消息包的接口下配置。

4. 配置 NTP 广播客户模式

指定本地防火墙上的某接口来接收 NTP 广播消息包，并运行在广播客户模式。本地防火墙首先侦听来自服务器的广播消息包，当接收到第一个广播消息包时，本地防火墙为了估计网络延迟，先启用一个短暂的 **client/server** 模式与远程服务器交换消息。然后，本地防火墙就进入广播客户模式，继续侦听广播消息包的到来，根据到来的广播消息包，对本地时钟进行同步。

请在接口视图下进行下列配置。

表10-4 配置 NTP 广播客户模式

操作	命令
配置 NTP 广播客户模式	ntp-service broadcast-client
取消 NTP 广播客户模式	undo ntp-service broadcast-client

此命令必须在欲接收 NTP 广播消息包的接口下配置。

5. 配置 NTP 组播服务器模式

指定本地防火墙上的一个接口来发送 NTP 组播消息包，本地运行在组播服务器模式，作为组播服务器，周期性地发送组播消息到组播客户端。

请在接口视图下进行下列配置。

表10-5 配置 NTP 组播服务器模式

操作	命令
配置 NTP 组播服务器模式	ntp-service multicast-server [<i>X.X.X.X</i>] [authentication-keyid <i>keyid</i> ttl <i>ttn-number</i> version <i>number</i>] *
取消 NTP 组播服务器模式	undo ntp-service multicast-server

NTP 版本号 *number* 范围是 1~3，缺省值为 3；身份验证密钥 ID 号 *keyid* 范围 1~4294967295；组播包的生存期 *ttn-number* 范围为 1~255；组播 IP 地址缺省为 224.0.1.1；

此命令必须在欲发送 NTP 组播消息包的接口下配置。

6. 配置 NTP 组播客户模式

指定本地防火墙上的接口，来接收 NTP 组播消息包，本地防火墙运行在组播客户模式。本地防火墙首先侦听来自服务器的组播消息包，当接收到第一个组播消息包时，本地防火墙为了估计网络延迟，先启用一个短暂的 **client/server** 模式与远程服务器交换消息。然后，本地防火墙就进入组播客户模式，继续侦听组播消息包的到来，根据到来的组播消息包，对本地时钟进行同步。

请在接口视图下进行下列配置。

表10-6 配置 NTP 组播客户模式

操作	命令
配置 NTP 组播客户模式	ntp-service multicast-client [X.X.X.X]
取消配置 NTP 组播客户模式	undo ntp-service multicast-client [X.X.X.X]

组播 IP 地址 X.X.X.X 缺省为 224.0.1.1；此命令必须在欲接收 NTP 组播消息包的接口下配置。

10.2.2 配置 NTP 身份验证功能

NTP 身份验证功能需要在 Server 端和 Client 端同时配置，保证密钥一致，并为可信密钥，验证才能通过。

1. 启动 NTP 身份验证功能

请在系统视图下进行下列配置。

表10-7 配置 NTP 身份验证功能

操作	命令
启动 NTP 身份验证功能	ntp-service authentication enable
停止 NTP 身份验证功能	undo ntp-service authentication enable

2. 设置 NTP 验证密钥

该配置任务用来设置 NTP 验证密钥。

请在系统视图下进行下列配置。

表10-8 配置 NTP 验证密钥

操作	命令
设置 NTP 验证密钥	ntp-service authentication-keyid number authentication-mode md5 value
取消 NTP 验证密钥	undo ntp-service authentication-keyid number

密钥编号 *number* 范围为 1~4294967295；密钥值 *value* 为 1~32 个 ASCII 码字符。

3. 设置指定密钥是可信的

该配置用来指定密钥是可信的。

请在系统视图下进行下列配置。

表10-9 设置指定密钥是可信的

操作	命令
指定密钥是可信的	ntp-service reliable authentication-keyid <i>key-number</i>
取消指定可信密钥	undo ntp-service reliable authentication-keyid <i>key-number</i>

密钥编号 *key-number* 范围为 1~4294967295。

4. 将 NTP Server 与验证密钥关联

对于服务器模式和对等体模式，应在 Client 端将指定密钥与对应的 NTP Server 关联。这两种模式下，Client 端可能同时配置了多个 Server，所以需要利用认证密钥来决定同步哪一个 Server。

表10-10 将指定密钥与对应的 NTP Server 关联

操作	命令
服务器模式下，将指定密钥与对应的 NTP Server 关联	ntp-service unicast-server { <i>X.X.X.X</i> <i>server-name</i> } authentication-keyid <i>keyid</i>
对等体模式下，将指定密钥与对应的 NTP Server 关联	ntp-service unicast-peer { <i>X.X.X.X</i> <i>server-name</i> } authentication-key <i>keyid</i>

对于广播服务器模式和组播服务器模式，应在 Server 端将 Server 与对应的密钥关联。

表10-11 将指定密钥与对应的 NTP Server 关联

操作	命令
广播服务器模式下，将指定密钥与对应的 NTP Server 关联	ntp-service broadcast-server authentication-keyid <i>keyid</i>
组播服务器模式下，将指定密钥与对应的 NTP Server 关联	ntp-service multicast-server authentication-keyid <i>keyid</i>

10.2.3 设置本地发送 NTP 消息的接口

指定本地发送 NTP 消息时，消息包中的源 IP 地址都用一个特定 IP 地址，该 IP 地址就是从所指定的接口上获取的。

请在系统视图下进行下列配置。

表10-12 设置本地发送 NTP 消息的接口

操作	命令
设置本地发送 NTP 消息的接口	ntp-service source-interface <i>interface-type</i> <i>interface-number</i>
取消设置本地发送 NTP 消息的接口	undo ntp-service source-interface

接口由 *interface-type interface-number* 确定，消息包中的源 IP 地址从该接口获取接口的主 IP 地址，如果 **ntp-service unicast-server** 或 **ntp-service unicast-peer** 中也指定了发送接口，则以 **ntp-service unicast-server** 或 **ntp-service unicast-peer** 指定的为准。

10.2.4 设置 NTP 主时钟

该配置用来设置本地时钟作为 NTP 主时钟。

请在系统视图下进行下列配置。

表10-13 设置本地时钟作为 NTP 主时钟

操作	命令
设置本地时钟作为 NTP 主时钟	ntp-service refclock-master [<i>X.X.X.X</i>] [<i>layers-number</i>]
取消 NTP 主时钟设置	undo ntp-service refclock-master [<i>X.X.X.X</i>]

X.X.X.X 是参考时钟 IP 地址 127.127.1.u，其中 u 的取值范围为 0~3；*layers-number* 用来指定本地时钟所在的层数，范围为 1~15，缺省为 8。当不指定 IP 地址时，默认设置本地时钟为 NTP 主时钟；可以指定 NTP 主时钟所处的层次数。

10.2.5 设置禁止/允许接口接收 NTP 消息

该配置任务用来设置禁止或允许接口接收 NTP 消息。

请在接口视图下进行下列配置。

表10-14 设置禁止/允许接口接收 NTP 消息

操作	命令
设置禁止接口接收 NTP 消息	ntp-service in-interface disable
设置允许接口接收 NTP 消息	undo ntp-service in-interface disable

该配置任务必须在需要禁止/允许接收 NTP 消息的接口下配置。

10.2.6 设置对本地防火墙 NTP 服务的访问控制权限

设置对本地防火墙 NTP 服务的访问控制权限。这里提供了一种最小限度的安全措施，更安全的方法是进行身份验证。当有一个访问请求时，按照最小访问限制到最大访问限制依次匹配，以第一个匹配的为准，匹配顺序为 **peer**、**server**、**server only (synchronization)**、**query only**。

请在系统视图下进行下列命令的操作。

表10-15 设置对本地防火墙服务的访问控制权限

操作	命令
设置对本地防火墙服务的访问控制权限	ntp-service access { query synchronization server peer } <i>acl-number</i>
取消设置对本地防火墙服务的访问控制权限	undo ntp-service access { query synchronization server peer }

IP 地址访问列表标号 *acl-number* 范围为 2000～2999。其访问权限含义为：

query：只允许对本地 NTP 服务进行控制查询。

synchronization：只允许对本地 NTP 服务进行时间请求。

server：可以对本地 NTP 服务进行时间请求和控制查询，但本地时钟不会同步到远程服务器。

peer：既可以对本地 NTP 服务进行时间请求和控制查询，本地时钟又可以同步到远程服务器。

10.2.7 设置本地允许建立的 sessions 数目

该配置任务用来设置本地允许建立的 sessions 的数目。

请在系统视图下进行下列配置。

表10-16 设置本地允许建立的 sessions 数目

操作	命令
设置本地允许建立的 sessions 数目	ntp-service max-dynamic-sessions <i>number</i>
恢复本地允许建立的 sessions 数目为缺省值	undo ntp-service max-dynamic-sessions

本地允许建立 sessions 的数目 *number*，范围 0～100，缺省值为 100。

10.3 NTP 显示与调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 NTP 的运行情况，通过查看显示信息，验证配置的效果。

在用户视图下，执行 **debugging** 命令可对 NTP 进行调试。

表10-17 NTP 显示与调试

操作	命令
显示 NTP 服务的状态信息	display ntp-service status
显示 NTP 服务维护的 sessions 状态	display ntp-service sessions [verbose]
显示从本地设备回溯到参考时钟源的各个 NTP 时间服务器的简要信息。	display ntp-service trace
打开 NTP 的调试开关	debugging ntp-service { all adjustment authentication event filter packet parameter refclock selection synchronization validity }

10.4 NTP 典型配置举例

10.4.1 配置 NTP 服务器

1. 组网需求

SecPath1 设置本地时钟作为 NTP 主时钟，层数为 2，SecPath2 以 SecPath1 作为时间服务器，将其设为 **server** 模式，自己为 **client** 模式。

2. 组网图

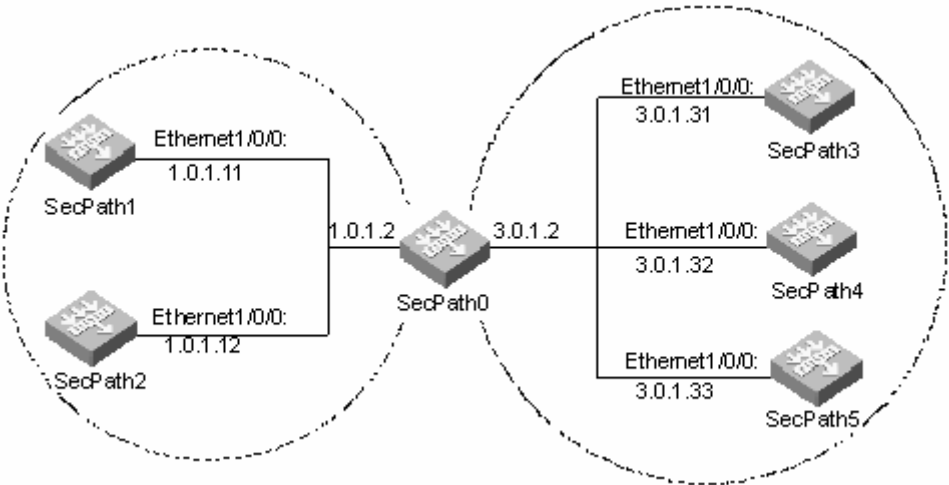


图10-2 NTP 典型配置的组网图

3. 配置步骤

(1) 配置 SecPath1

进入系统视图。

```
<H3C> system-view
```

设置本地时钟作为 NTP 主时钟，层数为 2。

```
[H3C] ntp-service refclock-master 2
```

(2) 配置 SecPath2

进入系统视图。

```
<H3C> system-view
```

设置 SecPath1 为时间服务器。

```
[H3C] ntp-service unicast-server 1.0.1.11
```

以上配置将 SecPath2 向 SecPath1 进行时间同步，同步前观察 SecPath2 的状态为：

```
[H3C] display ntp-service status
```

Clock status: unsynchronized

Clock stratum: 16

Reference clock ID: none

Nominal frequency: 99.8562 Hz

Actual frequency: 99.8562 Hz

Clock precision: 2⁷

Clock offset: 0.0000 ms

Root delay : 0.00 ms

Root dispersion: 0.00 ms

Peer dispersion: 0.00 ms

Reference time: 00:00:00.000 UTC Jan 1 1900 (00000000.00000000)

同步后观测 SecPath2 的状态为：

```
[H3C] display ntp-service status
```

Clock status: synchronized

Clock stratum: 3

Reference clock ID: 1.0.1.11

Nominal frequency: 250.0000 Hz

Actual frequency: 249.9992 Hz

Clock precision: 2¹⁹

Clock offset: 198.7425 ms

Root delay : 27.47 ms

Root dispersion: 208.39 ms

Peer dispersion: 9.63 ms

Reference time: 17:03:32.022 UTC Sep 6 2001 (BF422AE4.05AEA86C)

此时 SecPath2 已经与 SecPath1 同步，层数比 SecPath1 大 1，为 3。

观察 SecPath2 的 sessions 情况，SecPath2 与 SecPath1 建立了连接。

```
[H3C] display ntp-service sessions
      source      reference  stra  reach  poll now offset delay  disper
*****
[12345]1.0.1.11  LOCL(0)    2    377    64    1    199.53 26.1    9.7
Total associations : 1
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

10.4.2 配置 NTP 对等体举例

1. 组网需求

SecPath3 设置本地时钟作为 NTP 主时钟，层数为 2，SecPath4 以 SecPath3 作为时间服务器，将其设为 server 模式，自己为 client 模式。同时，SecPath5 将 SecPath4 设为对等体。

2. 组网图

如图 10-2 所示。

3. 配置步骤

(1) 配置 SecPath 3

进入系统视图。

```
<H3C> system-view
```

设置本地时钟作为 NTP 主时钟，层数为 2。

```
[H3C] ntp-service refclock-master 2
```

(2) 配置 SecPath 4

进入系统视图。

```
<H3C> system-view
```

设置 SecPath3 为时间服务器，同步后层数为 3。

```
[H3C] ntp-service unicast-server 3.0.1.31
```

(3) 配置 SecPath5（SecPath4 已经向 SecPath3 同步后）

进入系统视图。

```
<H3C> system-view
```

设置本地时钟作为 NTP 主时钟，层数为 1。

```
[H3C] ntp-service refclock-master 1
```

本地同步后，设置 SecPath4 为对等体。

```
[H3C] ntp-service unicast-peer 3.0.1.32
```

以上配置将 SecPath4 和 SecPath5 配置为对等体，SecPath5 处于主动对等体模式，SecPath4 处于被动对等体模式，由于 SecPath5 的层数为 1，而 SecPath4 的层数为 3，所以 SecPath4 向 SecPath5 同步。

同步后观测 SecPath4 的状态为：

```
[H3C] display ntp-service status
Clock status: synchronized
Clock stratum: 2
Reference clock ID: 3.0.1.33
Nominal frequency: 250.00000 Hz
Actual frequency: 249.9992 Hz
Clock precision: 2^19
Clock offset: 198.7425 ms
Root delay : 27.47 ms
Root dispersion: 208.39 ms
Peer dispersion: 9.63 ms
Reference time: 17:03:32.022 UTC Sep 6 2001 (BF422AE4.05AEA86C)
```

此时 SecPath 4 已经与 SecPath 5 同步，层数比 SecPath 5 大 1，为 2。

观察 SecPath 4 的 sessions 情况，SecPath 4 与 SecPath 5 建立了连接。

```
[H3C] display ntp-service sessions
          source          reference      stra reach poll now offset  delay disper
*****
[25]3.0.1.31      127.127.1.0      2    31   64   55 466670.4    1.0    0.9
[1234]3.0.1.33    127.127.1.0      1     7   64   59 -2771.6    -0.1    0.5
Total associations : 2
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

10.4.3 配置 NTP 广播模式

1. 组网需求

SecPath3 设置本地时钟作为 NTP 主时钟，层数为 2，并从接口 Ethernet 1/0/0 向外发送广播消息包，设置 SecPath4 和 SecPath1 分别从各自的接口 Ethernet 1/0/0 监听广播消息。

2. 组网图

如图 10-2 所示。

3. 配置步骤

(1) 配置 SecPath 3

进入系统视图。

```
<H3C> system-view
```

设置本地时钟作为 NTP 主时钟，层数为 2。

```
[H3C] ntp-service refclock-master 2
```

进入接口 Ethernet 1/0/0 视图。

```
[H3C] interface ethernet 1/0/0
```

设置为广播服务器。

```
[H3C-Ethernet1/0/0] ntp-service broadcast-server
```

(2) 配置 SecPath 4

进入系统视图。

```
<H3C> system-view
```

进入接口 Ethernet 1/0/0 视图。

```
[H3C] interface ethernet 1/0/0
```

```
[H3C-Ethernet1/0/0] ntp-service broadcast-client
```

(3) 配置 SecPath1

进入系统视图。

```
<H3C> system-view
```

进入接口 Ethernet 1/0/0 视图。

```
[H3C] interface ethernet 1/0/0
```

```
[H3C-Ethernet1/0/0] ntp-service broadcast-client
```

以上配置将 SecPath4 和 SecPath1 配置为从接口 Ethernet 1/0/0 监听广播消息，而 SecPath3 从接口 Ethernet 1/0/0 发送广播消息包，由于 SecPath1 与 SecPath3 不在同一的网段，所以接收不到 SecPath3 发出的广播包，而 SecPath4 接收到 SecPath 3 发出的广播包后与其同步。

同步后观测 SecPath4 的状态为：

```
[H3C] display ntp-service status
```

```
Clock status: synchronized
```

```
Clock stratum: 3
```

```
Reference clock ID: 3.0.1.3
```

```
Nominal frequency: 250.0000 Hz
```

```
Actual frequency: 249.9992 Hz
```

```
Clock precision: 2^19
```

```
Clock offset: 198.7425 ms
```

```
Root delay : 27.47 ms
```

```
Root dispersion: 208.39 ms
```

```
Peer dispersion: 9.63 ms
```

```
Reference time: 17:03:32.022 UTC Sep 6 2001 (BF422AE4.05AEA86C)
```

此时 SecPath 4 已经与 SecPath 3 同步，层数比 SecPath3 大 1，为 3。

观察 SecPath 4 的 sessions 情况，SecPath 4 与 SecPath 3 建立了连接。

```
[H3C] display ntp-service sessions
```

```

      source      reference  stra  reach  poll now offset delay  disper
*****

```

```
[1234]3.0.1.31  LOCL(0)    2    377    64    1    199.53 26.1    9.7
```

```
Total associations : 1
```

```
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

10.4.4 配置带认证的 NTP 广播模式

1. 组网需求

SecPath3 设置本地时钟作为 NTP 主时钟，层数为 3，并从接口 Ethernet 1/0/0 向外发送广播消息包，设置 SecPath 4 从接口 Ethernet 1/0/0 监听广播消息。

2. 组网图

如图 10-2 所示。

3. 配置步骤

(1) 配置 SecPath 3

进入系统视图。

```
<H3C> system-view
```

设置本地时钟作为 NTP 主时钟，层数为 3。

```
[H3C] ntp-service refclock-master 3
```

启动认证功能。

```
[H3C] ntp-service authentication enable
```

设置 NTP 验证密钥。

```
[H3C] ntp-service authentication-keyid 88 authentication-mode md5 123456
```

设置本验证密钥可信。

```
[H3C] ntp-service reliable authentication-keyid 88
```

进入接口 Ethernet 1/0/0 视图。

```
[H3C] interface ethernet 1/0/0
```

设置本为 NTP 广播服务器并指定验证 ID。

```
[H3C-Ethernet1/0/0] ntp-service broadcast-server authentication-id 88
```

(2) 配置 SecPath4

进入系统视图。

```
<H3C> system-view
```

启动认证功能。

```
[H3C] ntp-service authentication enable
```

设置 NTP 验证密钥。

```
[H3C] ntp-service authentication-keyid 88 authentication-mode md5 123456
```

设置本验证密钥可信。

```
[H3C] ntp-service reliable authentication-keyid 88
```

进入接口 Ethernet 1/0/0 视图。

```
[H3C] interface ethernet 1/0/0
```

设置防火墙为 NTP 广播客户端。

```
[H3C-Ethernet1/0/0] ntp-service broadcast-client
```

以上配置将 SecPath4 配置为从接口 Ethernet 1/0/0 监听广播消息，而 SecPath3 从接口 Ethernet 1/0/0 发送广播消息包，SecPath 4 接收到 SecPath3 发出的广播包后与其同步。

同步后观测 SecPath 4 的状态为：

```
<H3C> display ntp-service status
```

```
Clock status: synchronized
```

```
Clock stratum: 4
```

```
Reference clock ID: 3.0.1.31
```

```
Nominal frequency: 250.0000 Hz
```

```
Actual frequency: 249.9992 Hz
```

```
Clock precision: 2^19
```

```
Clock offset: 198.7425 ms
```

```
Root delay : 27.47 ms
```

```
Root dispersion: 208.39 ms
```

```
Peer dispersion: 9.63 ms
```

```
Reference time: 17:03:32.022 UTC Sep 6 2003(BF422AE4.05AEA86C)
```

此时 SecPath4 已经与 SecPath3 同步，层数比 SecPath3 大 1，为 4。

10.4.5 配置 NTP 组播模式

1. 组网需求

SecPath3 设置本地时钟作为 NTP 主时钟，层数为 2，并从接口 Ethernet 1/0/0 向外发送组播消息包；设置 SecPath4 和 SecPath1 分别从各自的接口 Ethernet 1/0/0 监听组播消息。

2. 组网图

如图 10-2 所示。

3. 配置步骤

(1) 配置 SecPath3

进入系统视图。

```
<H3C> system-view
```

设置本地时钟作为 NTP 主时钟，层数为 2。

```
[H3C] ntp-service refclock-master 2
```

进入接口 Ethernet 1/0/0 的视图。

```
[H3C] interface ethernet 1/0/0
```

设置为组播服务器。

```
[H3C-Ethernet1/0/0] ntp-service multicast-server
```

(2) 配置 SecPath4

进入系统视图。

```
<H3C> system-view
```

进入接口 Ethernet 1/0/0 的视图。

```
[H3C] interface Ethernet 1/0/0
```

设置为组播客户模式。

```
[H3C-Ethernet1/0/0] ntp-service multicast-client
```

(3) 配置 SecPath1

进入系统视图。

```
<H3C> system-view
```

进入接口 Ethernet 1/0/0 的视图。

```
[H3C] interface ethernet 1/0/0
```

设置为组播客户模式。

```
[H3C-Ethernet1/0/0] ntp-service multicast-client
```


以上配置将 SecPath4 和 SecPath1 配置为从接口 Ethernet 1/0/0 监听组播消息，而 SecPath3 从接口 Ethernet 1/0/0 发送组播消息包，由于 SecPath1 与 SecPath3 不在同一的网段，所以 SecPath1 收不到 SecPath3 发出的组播包，而 SecPath4 接收到 SecPath3 发出的组播包后与其同步。

同步后观测 SecPath 4 的状态为：

```
[H3C] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 3.0.1.31
Nominal frequency: 250.0000 Hz
Actual frequency: 249.9992 Hz
Clock precision: 2^19
Clock offset: 198.7425 ms
Root delay : 27.47 ms
Root dispersion: 208.39 ms
Peer dispersion: 9.63 ms
Reference time: 17:03:32.022 UTC Sep 6 2001 (BF422AE4.05AEA86C)
```

此时 SecPath4 已经与 SecPath3 同步，层数比 SecPath3 大 1，为 3。

观察 SecPath4 的 sessions 情况，SecPath4 与 SecPath3 建立了连接。

```
[H3C] display ntp-service sessions
      source          reference  stra  reach  poll now offset delay  disper
*****
[1234]3.0.1.31  LOCL(0)    2    377    64    1    199.53 26.1    9.7
Total associations : 1
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

10.4.6 配置带身份验证的 NTP 服务器模式

1. 组网需求

SecPath1 设置本地时钟作为 NTP 主时钟，层数为 2；SecPath 2 以 SecPath 1 作为时间服务器，将其设为 server 模式，自己为 client 模式，同时加入身份验证。

2. 组网图

如图 10-2 所示。

3. 配置步骤

(1) 配置 SecPath 1

进入系统视图。

```
<H3C> system-view
```

设置本地时钟作为 NTP 主时钟，层数为 2。

```
[H3C] ntp-service refclock-master 2
```

(2) 配置 SecPath2

进入系统视图。

```
<H3C> system-view
```

启动身份验证。

```
[H3C] ntp-service authentication enable
```

设置密钥。

```
[H3C] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

指定密钥为可信密钥。

```
[H3C] ntp-service reliable authentication-keyid 42
```

设置 SecPath1 为时间服务器，并设置向 SecPath1 同步时所使用的密钥。

```
[H3C] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

以上配置将 SecPath2 向 SecPath1 进行时间同步，由于 SecPath1 没有启动身份验证，所以，SecPath 2 还是无法向 SecPath1 同步。现在，向 SecPath1 增加以下配置：

启动身份验证。

```
[H3C] ntp-service authentication enable
```

设置密钥。

```
[H3C] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

指定密钥为可信密钥。

```
[H3C] ntp-service reliable authentication-keyid 42
```

此时，SecPath2 可以向 SecPath1 同步，同步后观测 SecPath2 的状态为：

```
[H3C] display ntp-service status
```

Clock status: synchronized

Clockstratum: 3

Reference clock ID: 1.0.1.11

Nominal frequency: 250.0000 Hz

Actual frequency: 249.9992 Hz

Clock precision: 2^19

Clock offset: 198.7425 ms

Root delay : 27.47 ms

Root dispersion: 208.39 ms

Peer dispersion: 9.63 ms

Reference time: 17:03:32.022 UTC Sep 6 2001 (BF422AE4.05AEA86C)

可以看出，SecPath2 已经与 SecPath1 同步，层数比 SecPath1 大 1，为 3。

第11章 SNMP 配置

11.1 协议简介

11.1.1 SNMP 协议介绍

简单网络管理协议（Simple Network Management Protocol，简称 SNMP）是被广泛接受并投入使用的一项工业标准，是目前使用得最广泛的计算机网络管理协议。它的目标是保证管理信息在任意两点间传送，便于网络管理员在网络上的任何节点检索信息，对信息进行修改，寻找故障，完成故障诊断、容量规划和报告的生成。它采用轮询机制，提供最基本的功能集，适合于小型、快速和低成本的环境使用。它只要求无连接的传输层协议 UDP，受到了广泛的支持。

SNMP 的结构分为 NMS（Network Management Station）和 Agent 两部分，NMS 是运行客户端程序的工作站，常用的网管平台有 Sun NetManager 和 IBM NetView；Agent 是运行在网络设备上的服务器端软件。NMS 和 Agent 之间通过如下方式进行消息交互。一方面，NMS 可以向 Agent 发出 GetRequest、GetNextRequest、GetBulkRequest 和 SetRequest 请求报文，Agent 接收到 NMS 的请求报文后，根据报文类型对管理变量进行 Read 或 Write 操作，并生成 Response 报文，返回给 NMS。另一方面，Agent 在设备发生冷/热启动等异常情况时，也会主动向 NMS 发送 Trap 报文，报告所发生的事件。

11.1.2 SNMP 版本及支持的 MIB

设备中的管理对象在 SNMP 报文中用管理变量来描述，为了唯一标识设备中的管理对象，SNMP 用层次结构命名方案来识别管理对象。整个层次结构就像一棵树，树的节点表示管理对象，如下图所示。每一个节点，都可以用从根开始的一条路径唯一地标识。

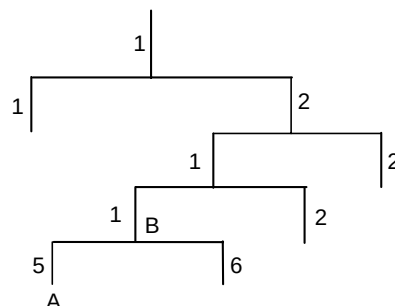


图11-1 MIB 树结构

在上图中，管理对象 B 可以用一串数字{1.2.1.1}唯一确定，这串数字是管理对象的 Object Identifier（客体标识符）。而 MIB（Management Information Base）的作用就是用来描述树的层次结构，它是所监控网络设备的标准变量定义的集合。

目前，防火墙中的 SNMP Agent 支持标准网管 SNMP v3，兼容 SNMP v1、SNMP v2c，相关 MIB 信息请参看 MIB companion 文档。

11.2 SNMP 配置

SNMP 的配置包括：

- 启动或关闭 SNMP Agent 服务
- 使能或禁止 SNMP 协议的相应版本
- 设置团体名
- 配置一个 SNMP 的组
- 为一个 SNMP 组添加或删除用户
- 设置管理员的联系方式
- 允许/禁止发送 Trap 报文
- 设置本地设备的引擎 ID
- 设置 Trap 目标主机的地址
- 设置防火墙的位置信息
- 指定发送 Trap 报文的源地址
- 创建或者更新 MIB 视图的信息
- 设置发往目的主机（host）的 Trap 报文的队列长度
- 设置 Trap 报文的保存时间
- 设置 Agent 能接收/发送的 SNMP 消息包的大小

11.2.1 启动或关闭 SNMP Agent 服务

该配置任务用来启动 SNMP Agent 服务，缺省情况为关闭 SNMP Agent 服务。
请在系统视图下进行下列配置。

表11-1 启动/关闭 SNMP Agent 服务

操作	命令
启动 SNMP Agent 服务	snmp-agent
关闭 SNMP Agent 服务	undo snmp-agent

11.2.2 使能或禁止 SNMP 协议的相应版本

该配置任务用来使能 SNMP 协议的相应版本，缺省情况为使能 SNMP v3 版本。如果要使能 SNMP v1 版本、SNMP v2c 版本，需要用该命令进行设置。

请在系统视图下进行下列配置。

表11-2 使能/禁止 SNMP 相应版本

操作	命令
使能 SNMP 协议的相应版本	snmp-agent sys-info version { { v1 v2c v3 } * all }
禁止 SNMP 协议的相应版本	undo snmp-agent sys-info version { { v1 v2c v3 } * all }

*: 表示从 **v1**、**v2c**、**v3** 这三个选项中选取多个，最少选取一个，最多选取所有三个选项。

使能 SNMP V2C、SNMP V3 版本。

```
[H3C] snmp-agent sys-info version v3 v2c
```

禁止 SNMP V2C、SNMP V1 版本。

```
[H3C] undo snmp-agent sys-info version v1 v2c
```

11.2.3 设置团体名

SNMPV1、SNMPV2C 采用团体名认证，与设备认可的团体名不符的 SNMP 报文将被丢弃。SNMP 团体（Community）由一字符串来命名，称为团体名（Community Name）。不同的团体可具有只读（read）或读写（write）访问模式。具有只读权限的团体只能对设备信息进行查询，而具有读写权限的团体还可以对设备进行配置。请在系统视图下进行下列配置。

表11-3 设置或删除团体名

操作	命令
设置团体名及访问权限	snmp-agent community { read write } community-name [mib-view view-name acl acl-number]*
取消先前设置的团体名	undo snmp-agent community community-name

对同一个团体名进行重复配置时，后配置的属性会覆盖先前配置的属性。

设置 **public** 团体具有只读权限。

```
[H3C] snmp-agent community read public
```

设置 **private** 团体具有读写权限。

```
[H3C] snmp-agent community write private
```

11.2.4 设置/删除 SNMP 组

该配置任务可以设置或删除 SNMP 的一个组。

请在系统视图下进行下列配置。

表11-4 设置或删除一个 SNMP 组

操作	命令
设置一个 SNMP 组	snmp-agent group { v1 v2c } group-name [read-view read-view] [write-view write-view] [notify-view notify-view] [acl acl-number] snmp-agent group v3 group-name [authentication privacy] [read-view read-view] [write-view write-view] [notify-view notify-view] [acl acl-number]
删除一个 SNMP 组	undo snmp-agent group { v1 v2c } group-name undo snmp-agent group v3 group-name [authentication privacy]

snmp-agent group v3 命令在不配置视图的情况下有默认的 ViewDefault 视图，该视图是只读视图，其他的视图需要配置。

snmp-agent group { v1 | v2c } 实际上是配置 SNMP 的团体属性。缺省情况下，与 **snmp-agent group v3** 相同。

11.2.5 添加/删除用户

该配置任务用来为一个 SNMP 的组添加或删除一个用户。

请在系统视图下进行下列配置。

表11-5 为 SNMP 组添加一个新用户或删除一个用户

操作	命令
为一个 SNMP 组添加一个新用户	snmp-agent usm-user { v1 v2c } user-name group-name [acl acl-number] snmp-agent usm-user v3 user-name group-name [authentication-mode { md5 sha } auth-password [privacy des56 priv-password]] [acl acl-number]
删除 SNMP 组的一个用户	undo snmp-agent usm-user { v1 v2c } user-name group-name undo snmp-agent usm-user v3 user-name group-name { engineid engine-id local }

为 SNMP 组 Johngroup 加入一个用户 John，安全级别为需要认证、指定认证协议为 HMAC-MD5-96、认证密码为 hello。

```
[H3C] snmp-agent usm-user v3 John Johngroup authentication-mode md5 hello
```

11.2.6 设置管理员的联系方式

设置管理员的联系方式（**system contact**）是 MIB II 中 **system** 组的一个管理变量，内容为被管理设备（防火墙）相关人员的标识及联系方式。您可以通过设置此参数，将重要信息存储在防火墙中，以便出现紧急问题时查询使用。

请在系统视图下进行下列配置。

表11-6 设置或删除管理员的联系方式

操作	命令
设置管理员的标识及联系方式	snmp-agent sys-info contact <i>sysContact</i>
恢复管理员的标识及联系方式为缺省值	undo snmp-agent sys-info contact

例：[H3C] snmp-agent sys-info contact Mr.zhang 13800138002

11.2.7 允许/禁止发送 Trap 报文

Trap 是被管理设备主动向 NMS 发送的、不经请求的信息，用于报告一些紧急的重要事件。

请在系统视图下进行下列配置。

表11-7 允许或禁止发送 Trap 报文

操作	命令
允许发送 Trap 报文	snmp-agent trap enable [<i>trap-type</i> [<i>trap-list</i>]]
禁止发送 Trap 报文	undo snmp-agent trap enable [<i>trap-type</i> [<i>trap-list</i>]]

缺省为允许发送 Trap 报文。

snmp-agent trap enable 命令不带参数时，表示允许发送所有模块的所有类型的 Trap 报文。

11.2.8 设置本地设备的引擎 ID

该配置任务可以设置本地设备的引擎 ID。引擎 ID 是十六进制数字串，并且长度为 10~64 个十六进制数，缺省为公司的企业号+设备信息。设备信息可以是 IP 地址、MAC 地址或自己定义的十六进制数字串。

请在系统视图下进行下列配置。

表11-8 设置本地设备的引擎 ID

操作	命令
设置设备的引擎 ID	snmp-agent local-engineid <i>engineid</i>
设置设备的引擎 ID 为缺省值	undo snmp-agent local-engineid

11.2.9 设置 Trap 目标主机的地址

请在系统视图下进行下列配置。

表11-9 设置或取消 Trap 目标主机的地址

操作	命令
设置 Trap 主机的地址	snmp-agent target-host trap address udp-domain <i>X.X.X.X</i> [udp-port <i>port-number</i>] params securityname <i>security-string</i> [v1 v2c v3 [authentication privacy]]
取消 Trap 主机的地址	undo snmp-agent target-host <i>X.X.X.X securityname</i> <i>security-string</i>

例：允许向地址 202.38.160.6 发送 Trap 报文，使用的团体名为 public。

```
[H3C] snmp-agent target-host trap address udp-domain 202.38.160.6 udp-port 5000 params securityname public
```

11.2.10 设置接口发送状态 Trap 报文

当接口的状态改变时（例如，由 up 变为 down），可以向 Trap 目标主机发送 Trap 报文。

请在接口视图下进行下列配置。

表11-10 设置接口发送状态 Trap 报文

操作	命令
设置接口发送状态 Trap 报文	enable snmp trap updown
禁止接口发送状态 Trap 报文	undo enable snmp trap updown

缺省情况下，接口发送状态 Trap 报文。

11.2.11 设置防火墙的位置信息

防火墙的位置信息是 MIB 中 system 组的一个管理变量，用于表示被管理设备的位置。

请在系统视图下进行下列配置。

表11-11 设置防火墙的位置信息

操作	命令
设置防火墙位置	snmp-agent sys-info location <i>sysLocation</i>
恢复防火墙位置为缺省值	undo snmp-agent sys-info location

例：将防火墙的位置信息设为 bj。

```
[H3C] snmp-agent sys-info location bj
```

11.2.12 指定发送 Trap 的源地址

该配置任务可以设定或删除发送 Trap 的源地址。

请在系统视图下进行下列配置。

表11-12 设定发送 Trap 的源地址

操作	命令
指定发送 Trap 的源地址	snmp-agent trap source <i>interface-type interface-number</i>
取消发送 Trap 的源地址	undo snmp-agent trap source

例：将以太网接口 1/0/0 的 IP 地址作为 Trap 报文的源地址。

```
[H3C] snmp-agent trap source ethernet 1/0/0
```

11.2.13 MIB 视图信息设置

该配置任务可以创建、更新或者删除视图的信息。

请在系统视图下进行下列配置。

表11-13 创建或更新视图的信息或删除视图

操作	命令
创建或更新视图的信息	snmp-agent mib-view { included excluded } <i>view-name oid-tree</i>
删除视图	undo snmp-agent mib-view <i>view-name</i>

例：创建一个视图包含 internet（1.3.6.1）的所有对象。

```
[H3C] snmp-agent mib-view included myview 1.3.6.1
```

11.2.14 设置消息包的最大值

该配置任务可以设置 Agent 能接收/发送的 SNMP 消息包的最大值。

请在系统视图下进行下列配置。

表11-14 设置 Agent 接收/发送的 SNMP 消息包的最大值

操作	命令
设置 Agent 接收/发送的 SNMP 消息包的最大值	snmp-agent packet max-size <i>byte-count</i>
恢复 SNMP 消息包的最大值的缺省值	undo snmp-agent packet max-size

Agent 能接收/发送的 SNMP 消息包的最大值的取值范围为<484~17940>，单位为字节，缺省值为 1500 字节。

设置 Agent 能接收/发送的 SNMP 消息包的最大值为 1042 字节。

```
[H3C] snmp-agent packet max-size 1042
```

11.2.15 设置 Trap 报文的消息队列的长度

该配置任务可以设置发往目的主机（host）的 Trap 报文的消息队列的长度。

请在系统视图下进行下列配置。

表11-15 设置 Trap 报文的消息队列的长度

操作	命令
设置发往目的主机（host）的 Trap 报文的消息队列的长度	snmp-agent trap queue-size <i>size</i>
恢复消息队列长度的缺省值	undo snmp-agent trap queue-size

消息队列长度的取值范围为<1~1000>，缺省值为 100。

设置发送 Trap 报文的主机的消息队列的长度为 200。

```
[H3C] snmp-agent trap queue-size 200
```

11.2.16 设置 Trap 报文的保存时间

该配置任务用来设置 Trap 报文的保存时间，超过该时间的 Trap 报文将被丢弃。

请在系统视图下进行下列配置。

表11-16 设置 Trap 报文的保存时间

操作	命令
设置 Trap 报文的保存时间	snmp-agent trap life <i>seconds</i>
恢复 Trap 报文保存时间的缺省值	undo snmp-agent trap life

seconds 取值范围为<1~2592000>，缺省值为 120 秒。

设置 Trap 报文的保存时间为 60 秒。

```
[H3C] snmp-agent trap life 60
```

11.3 SNMP 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令，均可以显示配置后 SNMP 的运行情况，通过查看显示信息，来验证配置的效果。

在用户视图下，执行 **debugging** 命令可对 SNMP 进行调试。

表11-17 SNMP 的显示与调试

操作	命令
显示 SNMP 使能的版本信息	display snmp-agent sys-info version
显示 SNMP 报文统计信息	display snmp-agent statistics
显示当前设备的引擎 ID	display snmp-agent { local-engineid remote-engineid }
显示防火墙上的组名、安全模式、各种视图的状态以及各组存储方式的信息	display snmp-agent group [group-name]
显示组用户名表中所有 SNMP 用户名称的信息	display snmp-agent usm-user [engineid engineid username user-name group group-name] *
显示当前配置的团体名	display snmp-agent community [read write]
显示当前配置的 MIB 视图	display snmp-agent mib-view [exclude include viewname view-name]
显示系统维护联络信息字符串	display snmp-agent sys-info contact
显示系统位置字符串	display snmp-agent sys-info location
打开 SNMP 调试开关	debugging snmp-agent { header packet trap process }

 说明：

使用 **display snmp-agent remote-engineid** 命令，目前软件版本尚无内容显示。

11.4 SNMP 典型配置举例

1. 组网需求

以下图为例，网管工作站（NMS）与防火墙通过以太网相连，网管工作站 IP 地址为 129.102.149.23，防火墙以太网口 IP 地址为 129.102.0.1。

2. 组网图

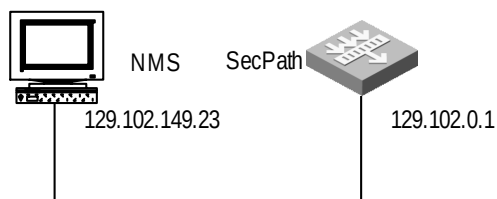


图11-2 SNMP 配置举例组网图

3. 配置步骤

第一步：使能 SNMP V1 版本

```
<H3C> system-view
[H3C] snmp-agent
[H3C] snmp-agent sys-info version v1
```

第二步：设置团体名和访问权限

```
[H3C] snmp-agent community read public
[H3C] snmp-agent community write private
```

第三步：设置管理员标识、联系方法以及防火墙物理位置

```
[H3C] snmp-agent sys-info contact Mr.Wang-Tel:3306
[H3C] snmp-agent sys-info location telephone-closet,3rd-floor
```

第四步：允许向网管工作站（NMS）129.102.149.23 发送 Trap 报文，使用的团体名为 public，NMS 接收 trap 的端口号为 5000，并使用 v1 格式 trap 发送。

```
[H3C] snmp-agent trap enable
[H3C] snmp-agent target-host trap address udp-domain 129.102.149.23 udp-port 5000 params securityname public
```

第12章 BIMS 配置

12.1 BIMS 概述

当通过 SNMP、Telnet 等方式管理网络设备时，一般需要知道设备 IP 地址等信息，这对于通过 DHCP 方式获得地址或 NAT 后面的设备，增加了主动管理的难度。BIMS（Branch Intelligent Management System）就是要解决上述问题，实现设备自动更新配置文件和应用程序功能。

BIMS 分 BIMS 中心侧和 BIMS 设备侧两个部分，其基本原理是：设备侧启动中或启动以后按照某种策略定期或间隔一定的时间向 BIMS 中心发出特定的信息请求，BIMS 中心侧根据管理员下达的策略指示不同设备进行信息交互。在中心侧和设备侧的信息交互过程中，管理员可以对设备进行管理，执行诸如升级软件版本、更改配置、查看配置信息和状态信息等任务，从而达到管理员对设备实施集中管理的功能。

BIMS 中心侧可以是运行于 PC 或服务器上的服务软件。BIMS 设备侧部分则集成在设备的软件系统中，实现 BIMS 功能的设备通过访问 BIMS 中心侧的服务器或 PC 来实现设备自动更新配置文件和应用程序。

BIMS 特性主要实现了以下功能：

- 支持通过执行命令立即访问 BIMS 中心获取新的配置文件或应用程序；
- 支持在设备启动时立即访问 BIMS 中心获取新的配置文件或应用程序；
- 支持设备每隔一定间隔时间访问 BIMS 中心获取新的配置文件或应用程序；
- 支持设备在某一特定时间点访问 BIMS 中心获取新的配置文件或应用程序。

设备使用 BIMS 功能进行配置文件或应用程序更新的过程如下：

- 在访问 BIMS 中心侧之前，设备必须开启 BIMS 功能，预先配置好设备的唯一标识符，BIMS 中心的 IP 地址，设备和 BIMS 中心双方的共享密钥。
- 设备因为某种原因被触发后，发送请求消息给 BIMS 中心，请求 BIMS 中心检查设备上的文件是否需要更新。
- BIMS 中心根据请求消息中上传的设备文件信息，判断各文件是否需要更新，需要更新则在回应消息中携带配置更新文件或需要更新的设备软件的 URL 路径信息和特征信息，或者是在回应消息中携带需要设备执行的命令内容及参数。
- 设备解析 BIMS 的回应消息，得到要更新的设备软件的 URL 或设备的加密后的配置文件或是需要执行的命令及参数。
- 设备得到配置文件后，执行配置文件命令并保存。

- 设备通过得到的 URL 向 BIMS 中心请求下载设备文件。
- 设备对从中心侧得到的设备软件校验后更新，之后给 BIMS 中心发确认消息。
- BIMS 中心侧根据设备发送的确认消息内容记录日志，并对设备发送的确认消息进行回应。

12.2 BIMS 配置

BIMS 为用户提供了一个很方便的管理方式，对设备提供了一个智能性的配置文件和应用程序的更新功能。对于设备侧来说主要包括以下几个方面的配置，其中启动 BIMS 功能、设备的唯一标识符、BIMS 中心的 IP 地址和端口以及 BIMS 双方的共享密钥是必须配置的，而设备访问 BIMS 中心的方式则可以选择配置，既可以是上电时自动访问后按照一定间隔时间进行访问，也可以是在指定的时间段内按照一定的时间间隔访问，或者是执行命令使设备立即访问 BIMS 中心。BIMS 的配置如下：

- 配置是否启动 BIMS 功能
- 配置设备的唯一标识符
- 配置 BIMS 中心的 IP 地址和端口号
- 配置 BIMS 设备发送报文时携带的源 IP 地址
- 设置 BIMS 设备侧和 BIMS 中心侧的共享密钥
- 配置当设备上电时是否触发设备访问 BIMS 中心
- 配置触发访问 BIMS 中心的间隔时间
- 配置设备在某一特定的时间访问 BIMS 中心以及访问的周期
- 配置设备立即访问 BIMS 中心。

12.2.1 配置使能 BIMS 功能

请在系统视图下进行下列配置。

表12-1 配置使能 BIMS 功能

操作	命令
配置在设备上使能 BIMS 功能	bims enable
取消在设备上使能 BIMS 功能	undo bims enable

缺省情况下，未使能 BIMS 功能。

12.2.2 配置设备唯一标识符

配置设备的唯一标识符，BIMS 中心根据设备的唯一标识符区分不同的设备。

请在系统视图下进行下列配置。

表12-2 配置设备的唯一标识符

操作	命令
配置设备的唯一标识符	bims device-id <i>string</i>
删除设备的唯一标识符	undo bims device-id

标识符最大长度 30 个字符。缺省情况下，没有配置设备的唯一标识符。

12.2.3 配置 BIMS 中心的 IP 地址和端口号

配置 BIMS 中心的 IP 地址和使用的端口号。

请在系统视图下进行下列配置。

表12-3 配置 BIMS 中心的 IP 地址和使用的端口号

操作	命令
配置 BIMS 中心的 IP 地址和使用的端口号	bims ip address <i>ip-address</i> [port <i>portnumber</i>]
删除配置的 BIMS 中心的 IP 地址	undo bims ip address

在配置 BIMS 中心的 IP 地址时，不输入端口号则默认为 BIMS 中心使用的端口号 80。

缺省情况下，没有配置 BIMS 中心的 IP 地址。

12.2.4 配置 BIMS 设备发送报文时携带的源 IP 地址

可以使用某个接口的 IP 地址作为 BIMS 设备发送报文时携带的源 IP 地址。

请在系统视图下进行下列配置。

表12-4 配置 BIMS 设备发送报文时携带的源 IP 地址

操作	命令
配置 BIMS 设备发送报文时携带的源 IP 地址	bims source ip-address <i>ip-address</i>
删除配置的源 IP 地址	undo bims source ip-address

缺省情况下，BIMS 设备未配置源 IP 地址。

12.2.5 配置 BIMS 设备侧和中心侧的共享密钥

设置 BIMS 设备侧和 BIMS 中心侧的共享密钥。

请在系统视图下进行下列配置。

表12-5 配置 BIMS 设备侧和 BIMS 中心侧的共享密钥

操作	命令
设置 BIMS 设备侧和 BIMS 中心侧的共享密钥	bims sharekey { simple cipher } sharekey
删除 BIMS 设备侧和 BIMS 中心侧之间的共享密钥	undo bims sharekey

缺省情况下，没有共享密钥。

12.2.6 配置当设备上电时是否触发设备访问 BIMS 中心

当配置了在设备上电时触发访问 BIMS 中心，则在设备上电启动完成后，立即访问 BIMS 中心。

请在系统视图下进行下列配置。

表12-6 配置当设备上电时是否触发设备访问 BIMS 中心

操作	命令
配置设备上电时访问 BIMS 中心	bims boot request
配置设备上电时不需要立即访问 BIMS 中心	undo bims boot request

缺省情况下，设备上电时立即访问 BIMS 中心。

12.2.7 配置触发访问 BIMS 中心的间隔时间

配置了触发访问 BIMS 中心的间隔时间后，设备按照该时间间隔周期性地访问 BIMS 中心。

请在系统视图下进行下列配置。

表12-7 配置触发访问 BIMS 中心的间隔时间

操作	命令
配置触发访问 BIMS 中心的间隔时间	bims interval number
取消配置的访问 BIMS 中心的间隔时间	undo bims interval

number 取值范围为 10~10080，单位为分钟。缺省情况下，没有配置该时间间隔。

12.2.8 配置设备在某一特定的时间访问 BIMS 中心以及访问的周期

配置设备在某一特定的时间访问 BIMS 中心，并在此基础上设定特定的访问周期以及访问的截止时间。

请在系统视图下进行下列配置。

表12-8 配置设备在某一特定的时间访问 BIMS 中心以及访问的周期

操作	命令
配置设备在特定的时间点访问 BIMS 中心，以及访问的周期和截至时间	bims specify-time <i>hh:mm yyyy/mm/dd</i> [[<i>hh:mm yyyy/mm/dd</i>] period-days <i>numberdays</i>]
取消该配置	undo bims specify-time

12.2.9 配置设备立即访问 BIMS 中心

执行该命令则设备立即访问一次 BIMS 中心。

请在系统视图下进行下列配置。

表12-9 配置设备立即访问一次 BIMS 中心

操作	命令
配置设备立即访问一次 BIMS 中心	bims request

12.3 BIMS 配置调试

在完成上述配置后，在所有视图下执行 **display current-configuration** 命令可以显示 BIMS 配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **debugging** 命令可以打开调试开关或者显示其各项状态参数，从而可以监控和维护 BIMS 配置。

表12-10 BIMS 配置的调试

操作	命令
打开 BIMS 调试信息开关	debugging bims all
关闭 BIMS 调试信息开关	undo debugging bims

12.4 BIMS 典型配置举例

12.4.1 配置设备上电后立即访问 BIMS 中心

1. 组网需求

设备上电后立即访问 BIMS 中心（IP 地址为 10.153.21.97，使用的端口号为 80），并且以后每隔 48 个小时访问一次 BIMS 中心。

2. 配置步骤

• BIMS 中心的配置

BIMS 中心一般采用 Quidview 网管系统的 BIMS 组件，在该组件中，需要作如下设置：

- (1) 在“参数设置”界面中设置 BIMS 中心侧和设备侧的共享密钥，该共享密钥必须与设备侧设置的一致。
- (2) 将设备添加到网管系统中进行管理：设备可以通过两种方式增加到网管系统中：

手工增加：用户输入设备的名称，在系统中添加该设备。

当设备访问 BIMS 中心时自动增加：采用自动增加方式时需要预先打开“自动添加上报设备”的开关，同时设置好 BIMS 中心侧与设备侧公用的密钥，这样当设备访问 BIMS 中心时，如果该设备还没有添加到 BIMS 中心，系统会自动添加该设备。

- (3) 为设备指定待升级的文件：包括配置文件以及应用软件，当设备访问 BIMS 中心时，系统会进行判断，确定是否要用待升级的文件升级设备上的文件。如果需要更新，则 BIMS 中心会将待升级文件下发到设备上，升级设备上相应的文件。

说明：

关于 Quidview 网管系统 BIMS 组件的详细使用说明，请参见 Quidview 网管系统 BIMS 组件的用户手册。

• 设备侧的配置

进入系统视图。

```
<H3C> system-view
```

在设备上配置启动 BIMS 功能

```
[H3C] bims enable
```

```
bims is enable
```

配置设备的唯一标识符为 secpaht-20-907。

```
[H3C] bims device-id secpaht-20-907
```

配置 BIMS 设备侧和中心侧的共享密钥。

```
[H3C] bims sharekey simple 1122334455667788
```

配置 BIMS 中心的 IP 地址，使用缺省的端口号 80。

```
[H3C] bims ip address 10.153.21.97
```

配置设备上电后立即访问 BIMS 中心。

```
[H3C] bims boot request
```

配置触发访问 BIMS 中心侧的间隔时间。

```
[H3C] bims interval 2880
```

进行上述配置后，设备在上电后立即访问 BIMS 中心，并且以后每隔 48 个小时访问一次 BIMS 中心。在设备每次访问 BIMS 中心时，BIMS 中心都会根据该设备的待升级文件列表来判断是否需要用待升级文件更新设备的相应文件。如果需要，则执行下发文件操作，更新设备侧的相应文件。

12.4.2 配置设备在一定时间段内周期性访问 BIMS 中心

1. 组网需求

设备从 2005 年 5 月 1 日 12 点 10 分开始访问 BIMS 中心（IP 地址为 10.153.21.97，使用的端口号为 80），每隔 2 天访问一次，直到 2005 年 10 月 1 日 23 点 50 分截至。

2. 配置步骤

BIMS 中心的配置请参见上面的例子。下面只描述设备侧的相关配置步骤。

进入系统视图。

```
<H3C> system-view
```

在设备上配置启动 BIMS 功能

```
[H3C] bims enable
```

```
bims is enable
```

配置设备的唯一标识符为 secpath-20-907。

```
[H3C] bims device-id secpath-20-907
```

配置 BIMS 设备侧和中心侧的共享密钥。

```
[H3C] bims sharekey simple 1122334455667788
```

配置 BIMS 中心的 IP 地址，使用缺省的端口号 80。

```
[H3C] bims ip address 10.153.21.97
```

配置设备从 2005 年 5 月 1 日 12 点 10 分开始访问 BIMS 中心，每隔 2 天访问一次，直到 2005 年 10 月 1 日 23 点 50 分截至。

```
[H3C] bims specify-time 12:10 2005/05/01 23:50 2005/10/01 period 2
```

进行上述配置后，设备在指定的时间段内按照指定的访问时间间隔对 BIMS 中心进行访问。在设备每次访问 BIMS 中心时，BIMS 中心都会根据该设备的待升级文件列表来判断是否需要用待升级文件更新设备的相应文件。如果需要，则执行下发文件操作，更新设备侧的相应文件。

12.5 BIMS 常见配置错误举例

12.5.1 无法成功访问 BIMS 服务器

1. 设备的 BIMS 基本配置没有配置完全或者正确

如果设备上的 BIMS 配置信息不完整或存在错误的话，都会造成无法访问 BIMS 服务器。所以在执行访问 BIMS 服务器之前，应该先检查 `bims device-id`；`bims ip address`；`bims sharekey` 这几条配置是否正确，并且保证 BIMS 功能已经被使能。

(1) 没有配置正确的服务器 IP 地址或者端口

这种情况下会导致连接 BIMS 服务器失败。由于设备上配置了错误的 BIMS 服务器的 IP 地址或端口号，导致它们之间建立连接超时，所以设备无法访问 BIMS 服务器。

(2) 设备上配置的 `bims sharekey` 与 BIMS 服务器的不一致

这种情况下会导致 BIMS 服务器无法解析消息而通信失败。这种情况下，设备可以接收到对端发送的报文，但是由于两端的共享密钥不一致，而导致无法解析报文。

2. 设备无启动软件导致访问 BIMS 服务器失败

设备每次访问 BIMS 服务器的时候都会对设备的启动软件映像文件进行查看，如果设备的启动软件映像文件不存在，会影响 BIMS 的业务。可以通过升级设备上的 BIMS 版本来解决该问题。

3. 设备空配置启动导致访问 BIMS 服务器失败

设备每次访问 BIMS 服务器的时候都会对设备的启动配置文件进行查看，如果设备的启动配置文件不存在，会影响 BIMS 的业务。可以通过升级设备上的 BIMS 版本来解决该问题。

12.5.2 无法下载新文件

1. 设备的存储部件的容量不足导致下载失败

在设备通过 BIMS 服务器下载新的文件时，如果设备的存储部件的容量不足，系统将自动中止下载更新，此时，可以删除存储部件中的一些不用的文件来释放资源，当剩余空间足够大时，重新访问 BIMS 服务器即可。

2. 设备内存不足导致下载失败

设备更新文件的时候需要占用较多的内存，尤其是 BIMS 实现更新设备的软件映像文件的过程中。所以当设备正在处理较多的业务的时候，同时通过 BIMS 更新文件，有可能出现内存不足导致下载失败的状况。如果出现该状况，会有内存耗尽的信息输出。

此时，可以等待其他业务处理完毕后，可用内存较大时再进行更新操作，或者扩充设备的内存。

12.5.3 无法通过 DHCP 获取 BIMS 配置

BIMS 支持设备通过 DHCP 方式获取 BIMS 相关配置。其目的是为了解决大量设备在空 BIMS 配置的状况下实现无人管理。

由于 DHCP 获取 IP 有租约时间的限制，所以在租约到期后，DHCP 服务器会重新下发 IP，同时也会重新下发 BIMS 相关配置。

- 如果设备上没有使能 BIMS，设备将接受 DHCP 服务器下发的 BIMS 配置；
- 如果设备上已经使能 BIMS，那么设备将丢弃 DHCP 服务器下发的 BIMS 配置。

如果需要设备通过 DHCP 获取 BIMS 配置，那么必须保证设备上的 BIMS 功能为关闭状态。

12.5.4 访问 BIMS 服务器导致设备上的 bims interval 命令配置发生变化

为了达到设备的无人管理的情况下，BIMS 服务器可能根据其业务量调整设备访问 BIMS 服务器的间隔周期，以减轻 BIMS 服务器业务负荷。

每次设备访问 BIMS 服务器的时候，都会从 BIMS 服务器获取新的轮询间隔时间，如果和设备上当前的 bims interval 配置不同的话会更新该配置。这是 BIMS 对于实现设备的无人化管理的一种灵活控制机制。

第13章 RMON 配置

13.1 RMON 简介

RMON（Remote Monitoring）是 IETF（Internet Engineering Task Force）定义的一种 MIB，是对 MIB II 标准最重要的增强。RMON MIB 由一组统计数据、分析数据和诊断数据组成。不像标准 MIB 仅提供被管理对象大量的关于端口的原始数据，它提供的是一个网段的统计数据和计算结果。RMON 主要用于对一个网段乃至整个网络中数据流量的监视，是目前应用相当广泛的网络管理标准之一。

RMON 的实现完全基于 SNMP 体系结构（这是它的一个突出优点），它与现存的 SNMP 框架相兼容，不需对该协议进行任何修改。RMON 包括 NMS 和运行在各网络设备上的 Agent 两部分。RMON Agent 在网络监视器或网络探测器上，跟踪统计其接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的报文总数，或发往某台主机的正确报文总数等）。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讯流量，从而可以简便而有力地管理大型互连网络。

RMON 允许有多个监控者，它可用两种方法收集数据：

- 一种方法利用专用的 RMON probe（探测器）收集数据，NMS 直接从 RMON probe 获取管理信息并控制网络资源。这种方式可以获取 RMON MIB 的全部信息；
- 第二种方法是将 RMON Agent 直接植入网络设备（防火墙、路由器、交换机、HUB 等）使它们成为带 RMON probe 功能的网络设施。RMON NMS 使用 SNMP 的基本命令与 SNMP Agent 交换数据信息，收集网络管理信息，但这种方式受设备资源限制，一般不能获取 RMON MIB 的所有数据，大多数只收集四个组的信息。这四个组是：报警信息、事件信息、历史信息和统计信息。

目前 Comware 以第二种方法实现 RMON。通过运行在网络监视器上的支持 RMON 的 SNMP Agent，NMS 可以获得与被管理网络设备接口相连的网段上的整体流量、错误统计和性能统计等信息，从而实现对网络的管理。

13.2 RMON 的配置

 说明：

在配置 RMON 功能之前，应先配置 SNMP Agent，保证 NMS 可以管理防火墙，这样用户才能通过 NMS 查询告警、日志等信息。

RMON 配置包括：

- 添加/删除事件表的一个表项
- 添加/删除告警表的一个表项
- 添加/删除历史控制表的一个表项
- 添加/删除 RMON 告警扩展表的一个表项
- 添加/删除统计表的一个表项

13.2.1 添加/删除事件表的一个表项

本配置用来定义事件号及事件的处理方式。事件有如下几种处理方式：

- 将事件记录在日志表中
- 向网管站发 Trap 消息
- 将事件记录在日志表中并向网管站发 Trap 消息

请在系统视图下进行下列配置。

表13-1 在事件表中添加/删除一个表项

操作	命令
在事件表中添加一个表项	rmon event event-entry [description string] { log trap trap-community log-trap log-trapcommunity none } [owner text]
在事件表中删除一个表项	undo rmon event event-entry

13.2.2 添加/删除告警表的一个表项

RMON 告警管理可对指定的告警变量（如接口的统计数据）进行监视，当被监视数据的值超过定义的阈值时会产生告警事件，然后按照事件的定义进行相应的处理。事件的定义在事件管理中实现。

 说明：

在添加告警表项之前，需要通过 **rmon event** 命令定义好告警表项中引用的事件。

请在系统视图下进行下列配置。

表13-2 在告警表中添加/删除一个表项

操作	命令
在告警表中添加一个表项	rmon alarm <i>entry-number alarm-variable sampling-time { delta absolute } rising_threshold threshold-value1 event-entry1 falling_threshold threshold-value2 event-entry2 [owner text]</i>
在告警表中删除一个表项	undo rmon alarm <i>entry-number</i>

用户定义了告警表项后，系统对告警表项的处理如下：

- 对所定义的告警变量按照定义的时间间隔进行采样
- 将采样值和设定的阈值进行比较，按照下表执行相应的处理过程

表13-3 告警表项的处理过程

实际情况	处理过程
采样值大于等于设定的上限	触发所定义的事件
采样值小于等于设定的下限	触发所定义的事件

13.2.3 添加/删除 RMON 告警扩展表的一个表项

该命令用来在 RMON 告警扩展表中添加/删除一个表项。告警扩展表项可以对告警变量的采样值进行运算，然后将运算结果和设置的阈值比较，实现更为丰富的告警功能。

说明：

在添加告警扩展表项之前，需要通过 **rmon event** 命令定义好告警表项中引用的事件。

请在系统视图下进行下列配置。

表13-4 在 RMON 告警扩展表中添加/删除一个表项

操作	命令
在 RMON 告警扩展表中添加一个表项	rmon prialarm <i>entry-number prialarm-formula prialarm-des sampling-timer { delta absolute changeratio } rising_threshold threshold-value1 event-entry1 falling_threshold threshold-value2 event-entry2 entrytype { forever cycle cycle-period } [owner text]</i>
在 RMON 告警扩展表中删除一个表项	undo rmon prialarm <i>entry-number</i>

用户定义了告警扩展表项后，系统对告警表项的处理如下：

- 对所定义的告警变量按照定义的时间间隔进行采样
- 将采样值按照定义的运算公式进行计算
- 将计算结果和设定的阈值进行比较，按照下表执行相应的处理过程

表13-5 告警扩展表项的处理过程

实际情况	处理过程
计算值大于等于设定的上限	触发所定义的事件
计算值小于等于设定的下限	触发所定义的事件

13.2.4 添加/删除历史控制表的一个表项

利用历史数据管理功能，可以对设备进行设置，设置的任务包括：采集历史数据、定期采集并保存指定接口的数据。抽样信息包括利用率、错误数和总包数等。

可以使用下面的命令在历史控制表中添加/删除一个表项。

请在以太网接口视图进行下列配置。

表13-6 在历史控制表中添加/删除一个表项

操作	命令
在历史控制表中添加一个表项	rmon history entry-number buckets number interval sampling-interval [owner text-string]
在历史控制表中删除一个表项	undo rmon history entry-number

历史控制表项统计的是采样时间间隔内的各种数据的统计值。用户可以通过 **display rmon history** 命令来显示历史控制表项的信息。

13.2.5 添加/删除统计表的一个表项

利用 RMON 统计管理功能，可以监视接口的使用情况、统计接口使用中发生的错误。统计信息包括冲突、循环冗余校验和队列、过小（或超大）的数据包、超时传送、碎片、广播、多播、单播消息以及带宽使用效率等。

可以使用下面的命令在统计表中添加/删除一个表项。

请在以太网接口视图下进行下列配置。

表13-7 在统计表中添加/删除一个表项

操作	命令
在统计表中添加一个表项	rmon statistics <i>entry-number</i> [owner <i>text-string</i>]
在统计表中删除一个表项	undo rmon statistics <i>entry-number</i>

统计表项统计的是从该事件定义的时间开始的一个累计的信息。用户可以通过 **display rmon statistics** 命令来显示统计表项的信息。

13.2.6 RMON 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示 RMON 的统计表、历史控制表、告警表、告警扩展表、事件表、事件日志中的信息。

表13-8 RMON 显示和调试

操作	命令
显示 RMON 统计表	display rmon statistics [<i>interface-type interface-number</i>]
显示 RMON 历史控制表	display rmon history [<i>interface-type interface-number</i>]
显示 RMON 告警表	display rmon alarm [<i>alarm-entry</i>]
显示 RMON 告警扩展表	display rmon prialarm [<i>prialarm-entry</i>]
显示 RMON 事件表	display rmon event [<i>event-entry</i>]
显示 RMON 事件日志	display rmon eventlog [<i>event-entry</i>]

13.3 RMON 典型配置举例

1. 组网需求

被检测防火墙通过 console 口连接配置终端，通过以太网连接 NMS。NMS 使用 Quidview 网管系统，可以通过网管查询防火墙的运行状况。

配置需求：

- 在 RMON 告警表中设定一个表项，1.3.6.1.2.1.16.1.1.1.4.1 节点的相对采样值超过上下限阈值分别可以触发两个 trap 事件；
- 进行以太网接口性能统计；
- 在防火墙上通过 **display rmon statistics** 命令查看显示结果，同时在网管上查看统计结果。

2. 组网图

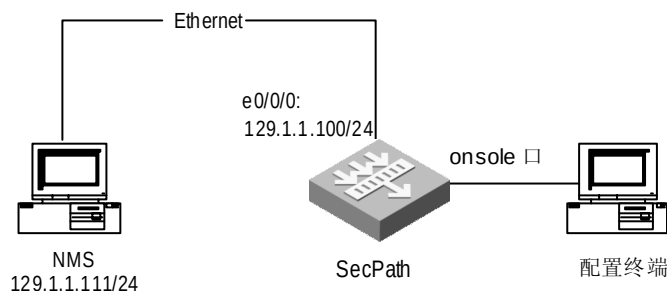


图13-1 RMON 典型应用举例

3. 配置步骤

配置 SNMP（注意：SNMP 的读、写团体及版本应与 Quidview 侧的配置一致）。

```
[H3C] snmp-agent
[H3C] snmp-agent community read public
[H3C] snmp-agent community write private
[H3C] snmp-agent sys-info version v1
[H3C] snmp-agent trap enable
[H3C] snmp-agent target-host trap address udp-domain 129.1.1.111 params
securityname secpath
```

配置 RMON 告警表项。

```
[H3C] rmon event 1 description rising trap gateway owner secpath-rmon
[H3C] rmon event 2 description falling trap gateway owner secpath-rmon
[H3C] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 5 delta rising_threshold 100 1
falling_threshold 50 2
```

配置以太网口 IP 地址。

```
[H3C] interface ethernet 0/0/0
[H3C-Ethernet0/0/0] ip address 129.1.1.100 255.255.255.0
```

配置 RMON 对以太网口进行统计。

```
[H3C-Ethernet0/0/0] rmon statistics 1 owner secpath-rmon
[H3C-Ethernet0/0/0] quit
```

查看 RMON 告警表信息及以太网口的统计信息。

```
<H3C> display rmon alarm 1
<H3C> display rmon statistics ethernet 0/0/0
```

当告警事件被触发时在 Quidview 的告警管理部分可以查看相应的记录。

第14章 终端服务

14.1 终端服务简介

系统提供多种终端服务，使用户可以进入命令行接口：

- 通过 Console 口进行本地配置
- 通过 AUX 口进行远程或本地配置
- 通过 Telnet 或者 SSH 进行本地或远程配置

14.2 Console 口终端服务

通过Console口即控制台，可以建立本地配置环境。配置环境的搭建参见 2.1.1 通过Console口搭建。

Console 口终端服务特性参见下表。

表14-1 Console 口终端服务特性

服务	特性
回显方式	本地不回显
终端类型	VT100
波特率	9600
数据位	8
奇偶校验	无
停止位	1 位
流控	无
二进制传输协议	XModem

14.3 AUX 口的远程终端服务

14.3.1 功能描述

AUX 口除了可以如 Console 口一样进行本地配置外，还可以进行远程配置，本地配置的方法请参见上一节，本节主要讲述远程终端服务。

系统支持通过 AUX 口对防火墙进行远程配置，在计算机串口和防火墙 AUX 口上挂接 Modem，通过 PSTN 相连，在计算机上通过拨号建立与远端防火墙的连接。拨号成功后，用户可以从终端敲入配置命令，设置远端防火墙工作参数。

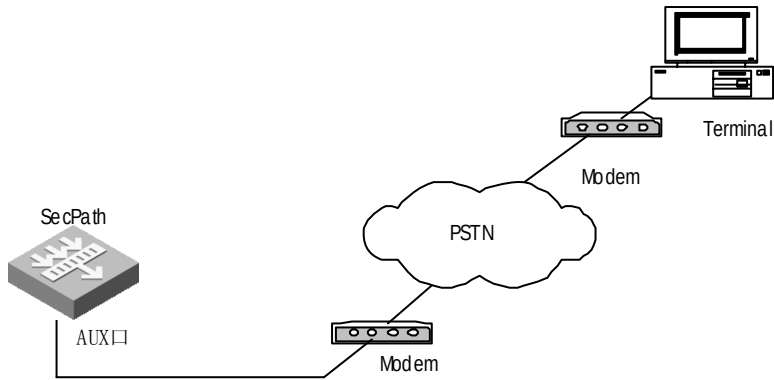


图14-1 通过 AUX 口搭建远程配置环境

14.3.2 AUX 口的远程配置终端服务特性

系统的远程配置终端服务特性参见下表。

表14-2 远程终端服务特性

服务	特性
回显方式	本地不回显
终端类型	VT100
波特率	与接口配置一致，缺省为 9600bps
数据位	与接口配置一致，缺省为 8 位
奇偶校验	与接口配置一致，缺省无
停止位	与接口配置一致，缺省为 1 位
流控	与接口配置一致，缺省为硬件流控

在计算机上运行的终端程序需按上表设置参数，其中波特率、数据位、奇偶校验及流控等参数要与相应的防火墙 AUX 口的配置一致。

14.4 Telnet 终端服务

14.4.1 Telnet 服务种类

Telnet 协议在 TCP/IP 协议族中属于应用层协议，通过网络提供远程登录和虚拟终端功能。防火墙系统提供的 Telnet 服务包括：

1. Telnet Server 服务

如下图所示，用户在计算机上可以运行 Telnet 客户端程序登录到防火墙上，对防火墙进行配置管理。

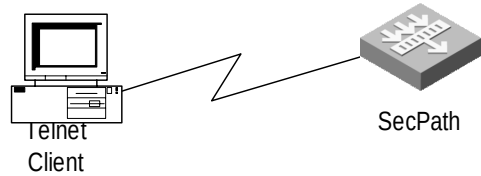


图14-2 提供 Telnet Server 服务

说明：

当使用 Linux 操作系统 Telnet 到防火墙时，Backspace 键的功能为删除光标后的一个字符，可以使用 CTRL+H 键删除光标前的一个字符。

2. Telnet Client 服务

如下图所示，用户在计算机上通过终端仿真程序或 Telnet 程序建立与防火墙的连接后，可以输入 Telnet 命令再登录其它防火墙，对其进行配置管理。

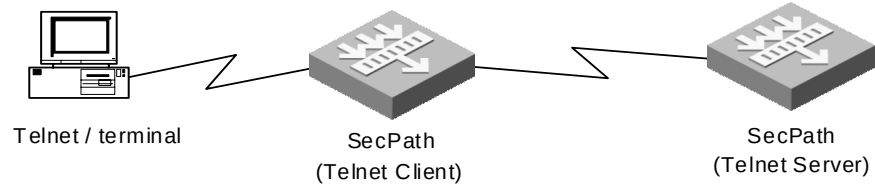


图14-3 提供 Telnet Client 服务

防火墙的 Telnet 服务特性参见下表。

表14-3 Telnet 服务特性

服务	特性
输入模式	字符模式
回显方式	本地不回显
终端类型	VT100

14.4.2 建立 Telnet 连接

1. 建立 Telnet 连接

请在用户视图下进行下面配置。

表14-4 建立 Telnet 连接

操作	命令
执行 Telnet 命令登录并管理其它设备	telnet <i>host-ip-address</i> [<i>service-port</i>] [source-interface <i>interface-type</i> <i>interface-number</i> source-ip <i>ip-address</i>]

例：PC 通过 Console 口与防火墙 SecPath1 建立连接，再执行 Telnet 命令登录防火墙 SecPath2，其 IP 地址为 129.102.0.1。

```
<SecPath1> telnet 129.102.0.1
Trying 129.102.0.1 ...
Connected to 129.102.0.1 ...
<SecPath2>
```

2. 配置 Telnet 超时时间

请在用户界面视图下进行下面配置。

表14-5 配置 Telnet 超时时间

操作	命令
允许定时断开 Telnet 连接	idle-timeout <i>minutes</i> [<i>seconds</i>]
恢复定时断开连接的缺省设置	undo idle-timeout

缺省情况下，超时时间为 10 分钟。

3. 配置 Telnet 源接口/源地址

请在系统视图下进行下面配置。

表14-6 配置 Telnet 源接口/源地址

操作	命令
指定 Telnet 客户端建立连接时使用的源接口	telnet source-interface <i>interface-type</i> <i>interface-number</i>
删除为 Telnet 客户端指定的源接口	undo telnet source-interface
指定 Telnet 客户端建立连接时使用的源 IP 地址	telnet source-ip <i>source-address</i>
删除为 Telnet 客户端指定的源 IP 地址	undo telnet source-ip

当同时配置了源接口和源 IP 地址时，后配置的有效。

该命令一般配合 ACL 使用。例如，当在 Telnet Client 端指定一个 loopback 接口为源接口时，其 Telnet 连接的源 IP 就是该接口的主 IP 地址，这样在 Telnet Server 端配置 ACL 时只需针对一个 IP 地址配置访问控制策略即可。

说明：

指定源 IP 地址和指定源接口的命令是互斥的，后配置的命令将覆盖先前的配置。

14.4.3 为 Telnet Server 指定源接口或 IP 地址

请在系统视图下进行下面配置。

表14-7 为 Telnet Server 指定源接口或 IP 地址

操作	命令
为 Telnet Server 指定源接口	telnet-server source-interface <i>interface-type interface-number</i>
删除为 Telnet Server 指定的源接口	undo telnet-server source-interface
为 Telnet Server 指定发送报文中的源 IP 地址	telnet-server source-ip <i>source-address</i>
删除为 Telnet Server 指定的源 IP 地址	undo telnet-server source-ip

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

说明：

指定源 IP 地址和指定源接口的命令是互斥的，后配置的命令将覆盖先前的配置。

14.4.4 Telnet 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令，可以显示配置后 Telnet 的运行情况，通过查看显示信息，验证配置的效果。

在用户视图下，执行 **debugging** 命令，可对 Telnet 进行调试。

表14-8 Telnet 连接的显示和调试

操作	命令
显示当前用户界面连接情况	display users
显示每个用户界面连接情况	display users all
显示当前建立的所有 TCP 连接情况	display tcp status
显示当前为 Telnet Server 设置的源 IP 地址	display telnet-server source-ip
显示当前为 Telnet Client 设置的源 IP 地址	display telnet source-ip
打开 Telnet 连接的调试开关	debugging telnet
关闭 Telnet 连接的调试开关	undo debugging telnet

display users 命令只能显示与防火墙连接的 Telnet 客户使用的接口。如果要查看与防火墙建立连接的 Telnet 服务器 IP 地址，则需要执行 **display tcp status** 命令，其中端口号为 23 的 TCP 连接均为 Telnet 连接，包括 Telnet 客户和 Telnet 服务器连接。

在 Telnet 连接过程中，可以使用快捷键来中断连接。如下图所示，SecPathA Telnet 连接到 SecPathB，再 Telnet 连接到 SecPathC，成为级连结构，此时，SecPathA 是 SecPathB 的 client，SecPathB 是 SecPathC 的 client，下面，以此结构简单地说明快捷键的用法：

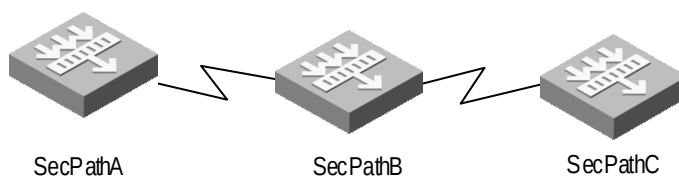


图14-4 Telnet 快捷键使用示意图

- <Ctrl+]>快捷键

在网络畅通的情况下，键入<Ctrl+]>，将通知 Telnet 服务器端要中断本次 Telnet 登录，作用与 **quit** 命令一样，即服务器端主动断开连接；如果由于某些原因网络断了，则快捷键的指令不能传送到服务器端，输入无效。

<SecPathC> （此时键入<Ctrl+]>，将退回到 SecPathB 的提示符。）

<SecPathB> （此时键入<Ctrl+]>，将退回到 SecPathA 的提示符。）

<SecPathA>

- <Ctrl+k>快捷键

在服务器端故障且客户端无法感知的情况下，此时，客户端输入任何指令服务器均无响应，这种情况下，键入<Ctrl+k>快捷键，客户端主动中断本次连接，并直接退出 Telnet 连接。

<SecPathC> （此时键入<Ctrl+k>，将直接中断，并退出到最初发起 Telnet 的设备 SecPathA。）

<SecPathA>

14.5 SSH 终端服务

14.5.1 SSH 简介

SSH 是 Secure Shell（安全外壳）的简称，用户通过一个不能保证安全的网络环境远程登录到防火墙时，SSH 特性可以提供安全保障和强大的认证功能，以保护防火墙不受诸如 IP 地址欺诈、明文密码截取等攻击。作为 SSH 服务器端，防火墙可以

接受多个 SSH 客户的连接。作为 SSH 客户端，防火墙可以与支持 SSH Server 的防火墙、路由器、UNIX 主机等建立 SSH 连接。目前防火墙支持的 SSH 服务器版本是 SSH 1.5 和 SSH 2.0，SSH 客户端版本是 SSH 2.0。如下图所示，可以通过本地连接或广域网连接建立 SSH 通道。

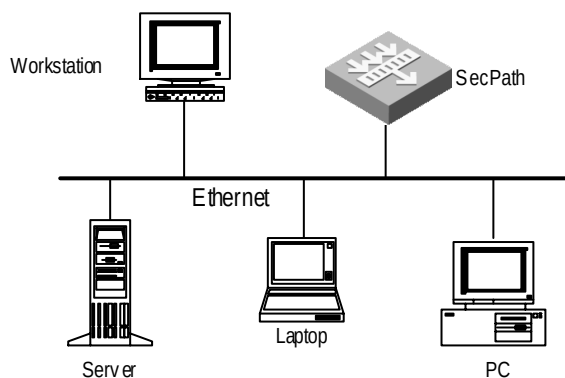


图14-5 在局域网内建立 SSH 通道

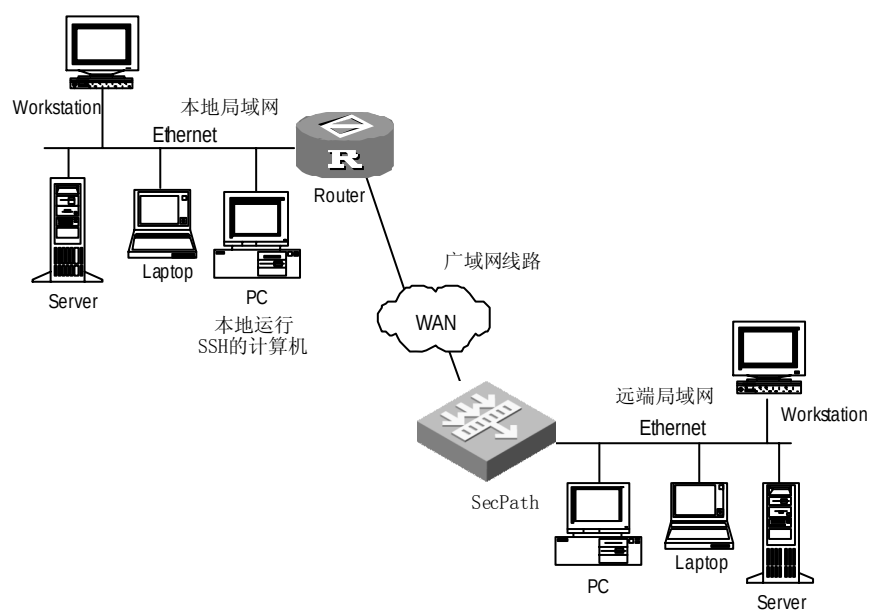


图14-6 通过广域网建立 SSH 通道

整个通讯过程中，为实现 SSH 认证的安全连接，服务器端与客户端经历如下五个阶段：

(1) 版本号协商阶段

- 客户端向服务器端发送 TCP 连接请求。
- TCP 连接建立后，服务器端和客户端进行版本号协商。
- 如果协商成功，则进入密钥算法协商阶段，否则服务器端断开 TCP 连接。

(2) 密钥算法协商阶段

- 服务器端生成 RSA 密钥对和一个 8 字节的随机数，并将密钥对的公钥部分和此随机数发送给客户端；
- 服务器端和客户端均以服务器端的公钥和此随机数为参数，使用相同的算法计算出一个 16 字节的会话 ID；
- 客户端以服务器端的公钥和本地产生的一个随机数为参数，计算出会话密钥；
- 客户端使用服务器端的公钥，对本地产生的这个用于计算会话密钥的随机数进行加密，回送给服务器端；
- 服务器端使用本地私钥对客户端回送回来的数据进行解密，得到客户端产生的随机数；
- 服务器端以本地公钥和客户端产生的随机数为参数，使用和客户端相同的算法计算出会话密钥。

通过以上步骤，服务器端和客户端就取得了相同的会话密钥。会话时，两端都使用会话密钥进行加密和解密，保证了数据传送的安全。

(3) 认证方法协商阶段

- 客户端向服务器端发送自己的用户名信息。
- 服务器端启动对该用户进行认证的程序。如果服务器端配置了该用户不需要认证，则直接进入会话请求阶段。
- 客户端采用某种认证方法对服务器端进行认证，直到认证通过或服务器由于超时而断开连接。

说明：

SSH 提供两种认证方法：口令认证和 RSA 认证。

(1) 口令认证过程如下：

- 客户端将认证用户名和口令发送给服务器端；
- 服务器端对客户端发送过来的用户名及口令与本地配置信息进行比较，如果两者完全匹配，则通过认证。

(2) RSA 认证过程如下：

- 服务器端进行客户端的 RSA 公钥配置；
 - 客户端向服务器端发送自己 RSA 公钥的成员模数；
 - 服务器端对此成员模数进行有效性认证，认证通过后产生一个随机数，使用客户端的 RSA 公钥加密后回送给客户端；
 - 服务器端和客户端均以此随机数和会话号作为参数计算出用于认证的数据；
 - 客户端将自己计算出来的认证数据发送给服务器端；
 - 服务器端将客户端发送过来的认证数据与本地计算出的认证数据进行比较，如果两者相同，则认证通过。
-

(4) 会话请求阶段

认证通过后，客户端将向服务器端发送会话请求；服务器端成功处理请求后，SSH 进入交互会话阶段。

(5) 交互会话阶段

客户端和服务端进行数据交互，直到会话结束。



注意：

当防火墙作为 SSH 服务器，且用户使用 SecureCRT 作为客户端软件时，如果客户端配置了“Enable OpenSSH agent forwarding”选项，将无法正常登录 SSH Server。

14.5.2 SSH Server 配置

SSH Server 配置包括：

- 设置所在用户界面支持的协议
- 配置和销毁本地 RSA 密钥对
- 为 SSH 用户配置验证方式
- 设置服务器密钥的更新时间
- 设置 SSH 认证超时时间
- 设置 SSH 验证重试次数
- 进入公共密钥视图
- 进入公共密钥编辑视图，编辑密钥
- 退出公共密钥编辑视图，返回系统视图
- 为 SSH 用户分配公共密钥
- 为 SSH 用户配置服务类型
- 设置 SSH 兼容方式（可选）
- 为 SSH Server 指定源接口或 IP 地址（可选）

1. 设置所在用户界面支持的协议

该配置任务用来指定所在的用户界面支持的协议，缺省为支持 Telnet 和 SSH。如果使能 SSH 的情况下，本机 RSA 密钥没有配置，则仍然不能通过 SSH 登录。配置结果在下次登录请求时生效。

请在 VTY 类型的用户界面视图下进行下列配置。

表14-9 设置所在用户界面支持的协议

操作	命令
设置所在用户界面支持的协议	protocol inbound { all ssh telnet }

**注意：**

如果在该用户界面上配置支持的协议是 SSH，为确保登录成功，请您务必配置相应的验证方式为 **authentication-mode scheme**；若配置其他验证方式为 **authentication-mode password** 和 **authentication-mode none**，则 **protocol inbound ssh** 配置结果将失败。反之亦然，如果某用户界面已经配置成支持 SSH 协议，则在此用户界面上 **authentication-mode password** 和 **authentication-mode none** 的配置将失败。

2. 配置和销毁本地 RSA 密钥对

该配置任务用来产生本地服务器密钥对和主机密钥对，如果此时已经有了 RSA 密钥，系统提示是否替换原有密钥。产生的密钥对的命名方式分别为：防火墙名称+server 和防火墙名称+host。服务器密钥和主机密钥的位数相差至少 128 位，服务器密钥和主机密钥的最小长度为 512 位，最大长度为 2048 位。

请在系统视图下进行下列配置。

表14-10 配置和销毁本地 RSA 密钥对

操作	命令
产生本地 RSA 密钥对	rsa local-key-pair create
销毁本地 RSA 密钥对	rsa local-key-pair destroy

**注意：**

- 成功完成 SSH 登录的首要操作是：配置并产生本地 RSA 密钥对。请您在进行其它 SSH 配置之前，一定记得完成 **rsa local-key-pair create** 配置，生成本地密钥对。此命令只需执行一遍，防火墙重启后不必再次执行。
- 如果服务器端和客户端都为 SecPath 防火墙时，则要求服务器端使用此命令生成的密钥对至少要为 768 位。当防火墙作为 SSH2.0 服务器端，且需要对客户端进行 RSA 认证，那么要求客户端生成的密钥对至少为 768 位。

3. 为 SSH 用户配置验证方式

该配置任务用来为 SSH 用户指定验证方式。新配置的验证方式在下次登录时生效。

请在系统视图下进行下列配置。

表14-11 为 SSH 用户配置验证方式

操作	命令
为 SSH 用户配置验证方式	ssh user <i>username</i> authentication-type { password rsa password-publickey all }
恢复系统默认无法登录方式	undo ssh user <i>username</i> authentication-type
为 SSH 用户指定一种缺省的认证方式	ssh authentication-type default { password rsa all password-publickey }
清除所指定的缺省认证方式	undo ssh authentication-type default

上面两个命令的区别是：

ssh user *username* authentication-type 命令用于为某一用户配置认证方式，**ssh authentication-type default** 命令为所有用户配置缺省的认证方式。

当两条命令同时配置，且认证方式不同时，用户 *username* 的认证方式以 **ssh user *username* authentication-type** 命令配置为准。

 说明：

配置 password 认证时，*username* 应与 AAA 中定义的有效用户名一致；配置 RSA 认证时，*username* 就是 SSH 用户名，不需要在 AAA 中配置本地用户。

4. 增加 SSH 用户

当用 **ssh authentication-type default** 命令指定了缺省认证类型时，可以用命令 **ssh user** 来增加用户，该用户的认证方式为缺省的认证方式。

请在系统视图下进行下列配置。

表14-12 增加 SSH 用户

操作	命令
增加 SSH 用户	ssh user <i>username</i>
删除 SSH 用户	undo ssh user <i>username</i>

 说明：

配置 password 认证时，*username* 应为 AAA 中定义的有效 SSH 用户名；配置 RSA 认证时，*username* 就是 SSH 本地用户名，与 AAA 中定义的用户无关。

如果用户配置的缺省验证方式是 password，并且采用 AAA 本地认证，则还需要用 **local-user** 命令在本地数据库中添加用户名和密码。在这种情况下，可以直接使用 **local-user** 命令配置用户名和密码（配置 service-type 为 ssh）登录 SSH 服务器，省略掉 **ssh user** 命令的配置。

5. 设置服务器密钥的更新时间

该配置任务用来设置服务器密钥的定时更新时间，更大限度的保证您的 SSH 连接的安全性。

请在系统视图下进行下列配置。

表14-13 设置服务器密钥的更新时间

操作	命令
设置服务器密钥的更新时间	ssh server rekey-interval hours
恢复缺省的更新时间	undo ssh server rekey-interval

系统缺省不对密钥进行更新。

6. 设置 SSH 认证超时时间

该配置任务用来设置 SSH 的认证超时时间。

请在系统视图下进行下列配置。

表14-14 设置 SSH 认证超时时间

操作	命令
设置 SSH 认证超时时间	ssh server timeout seconds
恢复 SSH 默认的认证超时时间	undo ssh server timeout

系统默认的认证超时时间为 60 秒。

7. 设置 SSH 验证重试次数

该配置任务用来设置 SSH 用户请求连接的验证重试次数，防止恶意猜测等非法行为。

请在系统视图下进行下列配置。

表14-15 设置 SSH 验证重试次数

操作	命令
设置 SSH 验证重试次数	ssh server authentication-retries times
恢复 SSH 默认的验证重试次数	undo ssh server authentication-retries

系统默认的验证重试次数为 3。

8. 进入公共密钥视图

该配置任务用来进入公共密钥视图，对客户端的公钥进行配置。此时的客户端密钥，是由支持 **SSH1.5** 的客户端软件随机生成的。

请在系统视图下进行下列第一项配置。

表14-16 公共密钥配置

操作	命令
进入公共密钥视图	rsa peer-public-key key-name
从公共密钥视图退回到系统视图	peer-public-key end

9. 进入公共密钥编辑视图，编辑密钥

该配置任务用来进入公共密钥编辑视图，输入由客户端软件生成的公共密钥数据。在对公钥进行编辑前，一定要在系统视图下，使用 **rsa peer-public-key key-name** 命令指定一个密钥名称。

在输入密钥数据时，字符之间可以有空格，也可以按回车键继续输入数据，所配置的公钥必须是按公钥格式编码的十六进制字符串。

请在公共密钥视图下进行下列配置。

表14-17 编辑公共密钥

操作	命令
进入公共密钥编辑视图	public-key-code begin

10. 退出公共密钥编辑视图

该配置任务用来从公共密钥编辑视图退回到公共密钥视图，并保存输入的公钥数据，也用来从公共密钥视图退回到系统视图。

请在公共密钥编辑视图下进行下列配置。

表14-18 退出公钥编辑视图

操作	命令
退出公钥编辑视图	public-key-code end

11. 为 SSH 用户分配公共密钥

该配置任务用来为 SSH 用户分配一个已经存在的公钥。

请在系统视图下进行下列配置。

表14-19 为 SSH 用户分配公钥

操作	命令
为 SSH 用户分配公钥	ssh user <i>username</i> assign rsa-key <i>keyname</i>
删除用户与公钥之间的对应关系	undo ssh user <i>username</i> assign rsa-key

12. 配置用户使用的服务类型

该配置任务用于设定 SSH 用户可以使用服务类型。

请在系统视图下进行下列配置。

表14-20 配置用户使用的服务类型

操作	命令
配置用户使用的服务类型	ssh user <i>username</i> service-type { stelnet sftp all }
恢复系统缺省的服务类型	undo ssh user <i>username</i> service-type { stelnet sftp all }

缺省情况下，系统默认的服务类型为 **stelnet**。

13. 配置服务器端兼容方式

该配置任务用来设置服务器端是否兼容 SSH1.x 版本的客户端。

请在系统视图下进行下列配置。

表14-21 配置兼容方式

操作	命令
设置服务器端兼容 SSH1.x 版本的客户端	ssh server compatible-ssh1x enable
设置服务器端不兼容 SSH1.x 版本的客户端	undo ssh server compatible-ssh1x

缺省情况下，服务器端兼容 SSH1.x 版本的客户端。

14. 为 SSH Server 指定源接口或 IP 地址

请在系统视图下进行下面配置。

表14-22 为 SSH Server 指定源接口或 IP 地址

操作	命令
为 SSH Server 指定源接口	ssh-server source-interface <i>interface-type</i> <i>interface-number</i>
删除为 SSH Server 指定的源接口	undo ssh-server source-interface
为 SSH Server 指定发送报文中的源 IP 地址	ssh-server source-ip <i>ip-address</i>
删除为 SSH Server 指定的源 IP 地址	undo ssh-server source-ip

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

说明：

指定源 IP 地址和指定源接口命令是互斥的，后配置的命令将覆盖先前的配置。

14.5.3 SSH Client 配置

SSH Client 配置包括：

- 设置对访问的 SSH 服务器进行首次认证
- 指定服务器公钥
- 启动 SSH 客户端

1. 启动 SSH 客户端

该配置任务用来启动 SSH 客户端与服务器建立连接，指定客户端和服务器的首选密钥交换算法、首选加密算法和首选 HMAC 算法。

请在系统视图下进行下列配置。

表14-23 启动 SSH 客户端

操作	命令
启动 SSH 客户端	ssh2 { <i>host-ip</i> <i>host-name</i> } [<i>port-num</i>] [prefer_kex { <i>dh_group1</i> <i>dh_exchange_group</i> }] [prefer_ctos_cipher { <i>des</i> <i>3des</i> <i>aes128</i> }] [prefer_stoc_cipher { <i>des</i> <i>3des</i> <i>aes128</i> }] [prefer_ctos_hmac { <i>sha1</i> <i>sha1_96</i> <i>md5</i> <i>md5_96</i> }] [prefer_stoc_hmac { <i>sha1</i> <i>sha1_96</i> <i>md5</i> <i>md5_96</i> }]

2. 指定服务器公钥

该配置任务用来在客户端上指定要连接的服务器的公钥，以便客户端认证连接的服务器是否为可信赖的服务器。

请在系统视图下进行下列配置。

表14-24 指定服务器公钥

操作	命令
指定服务器公钥	ssh client server assign rsa-key keyname
取消服务器与公钥间的对应关系	undo ssh client server assign rsa-key

3. 配置对服务器的首次认证

该配置任务用来配置或取消 SSH 客户端对服务器的首次认证。

所谓首次认证，是指如果当 SSH 客户端首次访问的服务器公钥在本地不存在时，用户可以选择继续访问该服务器，并在本地保存该服务器的公钥；当用户下次访问该服务器时，就以保存的公钥来认证该服务器。

如果不支持首次认证，那么当连接的服务器的公钥在本地不存在时，客户端将拒绝访问该服务器。

请在系统视图下进行下列配置。

表14-25 配置对服务器的首次认证

操作	命令
配置对服务器的首次认证	ssh client first-time enable
取消对服务器的首次认证	undo ssh client first-time

缺省情况下，客户端对服务器进行首次认证。

4. 为 SSH Client 指定源接口或 IP 地址

请在系统视图下进行下列配置。

表14-26 为 SSH Client 指定源接口或 IP 地址

操作	命令
为 SSH Client 指定源接口	ssh2 source-interface interface-type interface-number
删除为 SSH Client 指定的源接口	undo ssh2 source-interface
为 SSH Client 指定发送报文中的源 IP 地址	ssh2 source-ip ip-address
删除为 SSH Client 指定的源 IP 地址	undo ssh2 source-ip

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

说明：

指定源 IP 地址和指定源接口命令是互斥的，后配置的命令将覆盖先前的配置。

14.5.4 SSH 显示和调试

在完成上述配置后，在任何视图下执行 **display** 命令，可以显示配置后 SSH 的运行情况，通过查看显示信息，验证配置的效果。

在用户视图下执行 **debugging** 命令，可对 SSH 进行调试。

SSH 的显示和调试，就是查看各个 SSH 用户的配置情况，更好的利用系统资源，实现安全的信息连接。

请在任何视图下进行下列 **display** 操作，在用户视图下执行下列 **debugging** 操作。

表14-27 查看 SSH 相关信息

操作	命令
查看主机和服务器密钥对的公钥部分	display rsa local-key-pair public
显示客户端的 RSA 公共密钥	display rsa peer-public-key [brief name keyname]
显示 SSH 状态信息和会话信息	display ssh server { status session }
显示 SSH 用户信息	display ssh user-information [username]
显示 SSH 服务器信息	display ssh server-info
显示当前为 SSH Server 设置的源 IP 地址	display ssh-server source-ip
显示当前为 SSH Client 设置的源 IP 地址	display ssh2 source-ip

表14-28 调试 SSH 相关信息

操作	命令
打开 SSH 服务器调试开关	debugging ssh server { vty index all }
关闭 SSH 服务器调试开关	undo debugging ssh server { vty index all }
打开 SSH 客户端调试开关	debugging ssh client
关闭 SSH 客户端调试开关	undo debugging ssh client

14.5.5 SSH Server 配置举例

1. 组网需求

配置终端（SSH Client）与防火墙通过以太网口直接相连，在终端上运行 SSH1.5 的客户端软件可以安全地登录防火墙进行配置管理。SSH Client 用户名为 client001，口令为 pwd。

2. 组网图

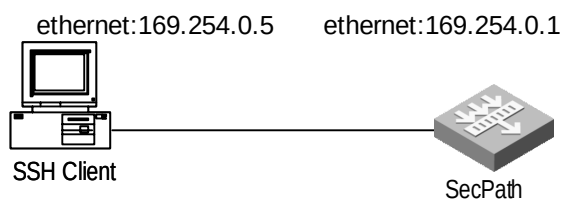


图14-7 SSH 本地配置组网图

3. 配置步骤

(1) 配置防火墙

根据登录验证方式不同分别介绍配置步骤，但开始任何一种配置之前，首要执行如下操作：

```
[H3C] rsa local-key-pair create
```

说明：

如果此前已完成生成本地密钥对的配置，可以略过此项操作。

- 配置 SSH 用户验证方式为 password。

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] authentication-mode scheme
[H3C-ui-vty0-4] protocol inbound ssh
[H3C-ui-vty0-4] quit
[H3C] local-user client001
[H3C-luser-client001] password simple pwd
[H3C-luser-client001] service-type ssh
[H3C-luser-client001] quit
[H3C] ssh user client001 authentication-type password
```

SSH 的验证超时时间、重试次数以及服务器密钥更新时间可以采用系统默认值，这些配置完成以后，您就可以在与防火墙连接的其它终端上，运行支持 SSH1.5 的客户端软件，以用户名 client001，密码 pwd，访问防火墙了。

- 配置 SSH 用户验证方式为 RSA。

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] authentication-mode scheme
[H3C-ui-vty0-4] protocol inbound ssh
[H3C-ui-vty0-4] quit
[H3C] ssh user client002 authentication-type RSA
```

这时您需要在支持 **SSH1.5** 的客户端软件上,随机产生 **RSA** 密钥对(含公钥及私钥),并按如下方式将 **RSA** 公钥(此处的 **RSA** 公钥是指用我司提供的 **SSHKEY.EXE** 软件进行 **PKCS** 标准编码后的 16 进制字符串)配置到 **SSH Server** 上指定的 **rsa peer-public-key** 中。

```
[H3C] rsa peer-public-key secpath002
[H3C-rsa-public-key] public-key-code begin
[H3C-rsa-key-code] 308186028180739A291ABDA704F5D93DC8FDF84C427463
[H3C-rsa-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[H3C-rsa-key-code] D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
[H3C-rsa-key-code] 0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
[H3C-rsa-key-code] C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
[H3C-rsa-key-code] BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[H3C-rsa-key-code] public-key-code end
[H3C-rsa-public-key] peer-public-key end
[H3C] ssh user client002 assign rsa-key secpath002
```

(2) 配置 SSH 客户端

- 对于 **password** 验证,需要在客户端上指定 **SSH Server** (防火墙)可达接口的 IP 地址 **169.254.0.1**,协议类型为 **SSH**,版本为 **1**。打开 **SSH** 连接后按提示输入用户名及口令,即可进入防火墙配置界面。

```
login as: client001
Sent username "client001"
client001@169.254.0.1's password:
*****
* Copyright(c) 2004-2007 Hangzhou H3C Technologies Co., Ltd. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
*****
<H3C>
```

- 对于 **RSA** 验证,不仅需要在客户端上指定 **SSH Server** 的 IP 地址、协议类型、版本,还需要指定 **RSA** 私钥文件(由客户端软件随机产生的)。打开 **SSH** 连接后按提示输入用户名即可进入防火墙配置界面。

```
login as: client002
Sent username "client002"
Trying public key authenticantion.
```

No passphrase required.

```
*****
* Copyright(c) 2004-2007 Hangzhou H3C Technologies Co., Ltd.      *
* Without the owner's prior written consent,                      *
* no decompiling or reverse-engineering shall be allowed.        *
*****
```

<H3C>

14.5.6 SSH Client 配置举例

1. 组网需求

SecPathB 作为 SSH 客户端，用户名 client003。SecPathA 作为 SSH 服务器，IP 地址为 10.165.87.136。

2. 组网图

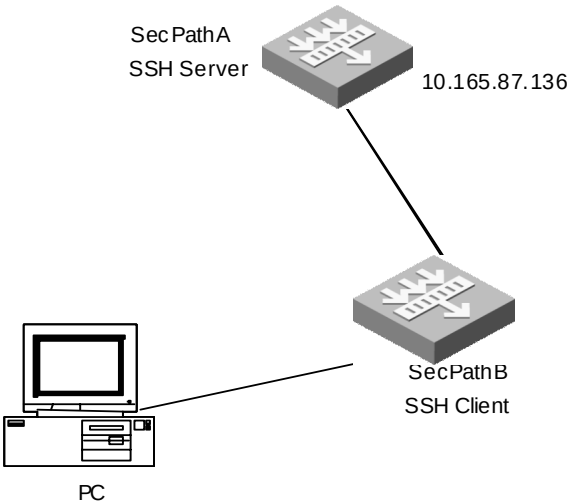


图14-8 SSH Client 配置组网图

3. 配置步骤

(1) 配置 SSH 服务器（SecPathA）

请参考 14.5.5 3. 配置步骤。

(2) 配置 SSH 客户端（SecPathB）

配置客户端对服务器进行首次认证。

```
[SecPath] ssh client first-time enable
```

启动 SSH 客户端。

下面分别按照服务器的两种认证方式进行配置。

- 采用 password 认证，按照缺省的加密算法启动。

```
[H3C] ssh2 10.165.87.136
Username: client003
Trying 10.165.87.136
Press CTRL+K to abort
Connected to 10.165.87.136...
The Server is not authencated.Do you continue access it?(Y/N):y
Do you want to save the server's public key?(Y/N):y
Enter password:
*****
* Copyright(c) 2004-2007 Hangzhou H3C Technologies Co., Ltd.          *
* Without the owner's prior written consent,                        *
* no decompiling or reverse-engineering shall be allowed.          *
*****
<H3C>
```

- 采用 RSA 公钥认证，按照所设置的相应加密算法启动。

```
[H3C] ssh2 10.165.87.136 22 perfer_kex dh_group1 perfer_ctos_cipher des
perfer_stoc_cipher 3des perfer_ctos_hmac md5 perfer_stoc_hmac md5
Username: client003
Trying 10.165.87.136...
Press CTRL+K to abort
Connected to 10.165.87.136...
The Server is not authencated.Do you continue access it?(Y/N):y
Do you want to save the server's public key?(Y/N):y
*****
* Copyright(c) 2004-2007 Hangzhou H3C Technologies Co., Ltd.          *
* Without the owner's prior written consent,                        *
* no decompiling or reverse-engineering shall be allowed.          *
*****
<H3C>
```

14.6 SFTP 服务

14.6.1 SFTP 简介

SFTP 是 Secure FTP 的简称，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到防火墙，进行文件管理和文件传送等操作（如进行系统升级），为数据传输提供了更高的安全

保障。同时，由于提供了客户端功能，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。

14.6.2 SFTP Server 配置

SFTP 服务器端配置包括：

表14-29 SFTP Server 配置

序号	配置项	命令	视图	说明
1	配置 SSH 用户使用的服务类型	ssh user username service-type { stelnet sftp all }	系统视图	可选
2	启动 SFTP 服务器	sftp server enable	系统视图	必选

1. 配置用户使用的服务类型

该配置任务用于设定 SSH 用户可以使用服务类型为 **sftp**。

请在系统视图下进行下列配置。

表14-30 配置 SSH 用户使用的服务类型

操作	命令
配置 SSH 用户使用的服务类型	ssh user username service-type sftp
恢复系统缺省的服务类型	undo ssh user username service-type

缺省情况下，系统默认的服务类型为 **Stelnet**。

2. 启动 SFTP 服务器

请在系统视图下进行下列配置。

表14-31 启动 SFTP 服务器

操作	命令
启动 SFTP 服务器	sftp server enable
关闭 SFTP 服务器	undo sftp server

缺省情况下，SFTP 服务器处于关闭状态。

说明：

防火墙的 SFTP 服务器支持的第三方软件为 PuTTY 的 PSFTP 客户端。

14.6.3 SFTP Client 配置

SFTP 客户端的配置包括：

表14-32 SFTP 客户端配置

序号	配置项		命令	视图	说明
1	启动 SFTP 客户端		sftp	系统视图	必选
2	关闭 SFTP 客户端		bye	SFTP 客户端视图	可选
			exit		
			quit		
3	SFTP 目录操作	改变用户的当前工作目录	cd	SFTP 客户端视图	可选
		返回上一级目录	cdup		
		显示当前工作目录	pwd		
		显示指定目录下的文件列表	dir		
			ls		
		创建新目录	mkdir		
		删除目录	rmdir		
4	SFTP 文件操作	改变服务器上指定的文件的 名字	rename	SFTP 客户端视图	可选
		下载远程服务器上的文件	get		
		上传本地文件到远程服务器	put		
		显示指定目录下的文件列表	dir		
			ls		
		删除服务器上文件	delete		
			remove		
5	客户端命令帮助		help	SFTP 客户端视图	可选

1. 启动 SFTP 客户端

该配置任务用来启动 SFTP 客户端程序，与远程 SFTP 服务器建立连接，并进入到 SFTP client 视图。

请在系统视图下进行下列配置。

表14-33 启动 SFTP 客户端

操作	命令
启动 SFTP 客户端	<code>sftp { host-ip host-name } [port-num] [prefer_kex { dh_group1 dh_exchange_group }] [prefer_ctos_cipher { des 3des aes128 }] [prefer_stoc_cipher { des 3des aes128 }] [prefer_ctos_hmac { sha1 sha1_96 md5 md5_96 }] [prefer_stoc_hmac { sha1 sha1_96 md5 md5_96 }]</code>

2. 关闭 SFTP 客户端

该配置任务用来关闭 SFTP 客户端程序。

请在 SFTP 客户端视图下进行下列配置。

表14-34 关闭 SFTP 客户端

操作	命令
关闭 SFTP 客户端	<code>bye</code>
	<code>exit</code>
	<code>quit</code>

 说明：

bye、**exit** 和 **quit** 三条命令的功能相同。

3. SFTP 目录操作

如表 14-35所示，可以进行的SFTP目录操作包括：改变或显示当前的工作目录，创建或删除目录，显示指定目录下的文件或目录信息。

请在 SFTP 客户端视图下进行下列操作。

表14-35 SFTP 目录操作

操作	命令
改变用户的当前工作目录	<code>cd remote-path</code>
返回上一级目录	<code>cdup</code>
显示用户的当前工作目录	<code>pwd</code>
显示指定目录下的文件列表	<code>dir [remote-path]</code>
	<code>ls [remote-path]</code>
在服务器上创建新的目录	<code>mkdir remote-path</code>
删除服务器上的目录	<code>rmdir remote-path</code>

 说明：

dir 和 **ls** 两条命令的功能相同。

4. SFTP 文件操作

如表 14-36所示，可以进行的SFTP文件操作包括：改变文件名、下载文件、上传文件、显示文件列表、删除文件。

请在 SFTP 用户视图下进行下列操作。

表14-36 SFTP 文件操作

操作	命令
改变服务器上指定的文件的名字	rename <i>old-name new-name</i>
下载远程服务器上的文件	get <i>remote-file [local-file]</i>
上传本地文件到远程服务器	put <i>local-file [remote-file]</i>
显示指定目录下的文件列表	dir <i>[remote-path]</i>
	ls <i>[remote-path]</i>
删除服务器上文件	delete <i>remote-file</i>
	remove <i>remote-file</i>

 说明：

- **dir** 和 **ls** 两条命令的功能相同。
- **delete** 和 **remove** 两条命令的功能相同。

5. SFTP Client 指定源接口或 IP 地址

请在系统视图下进行下列配置。

表14-37 SFTP Client 指定源接口或 IP 地址

操作	命令
SFTP Client 指定源接口	sftp source-interface <i>interface-type interface-number</i>
删除为 SFTP Client 指定的源接口	undo sftp source-interface
为 SFTP Client 指定发送报文中的源 IP 地址	sftp source-ip <i>ip-address</i>
删除为 SFTP Client 指定的源 IP 地址	undo sftp source-ip

缺省情况下，发送报文中的源 IP 地址为出接口的 IP 地址。

 **说明：**
指定源 IP 地址和指定源接口命令是互斥的，后配置的命令将覆盖先前的配置。

6. 显示帮助信息

该命令用于显示相关命令的帮助信息，如命令格式，参数配置等。
请在 SFTP 客户端视图下进行下列配置。

表14-38 显示客户端命令的帮助信息

操作	命令
显示客户端命令的帮助信息	help [<i>command-name</i>]

14.6.4 SFTP 配置举例

1. 组网需求

如图 14-9所示：

- SecPathA 和 SecPathB 已经建立起安全的 SSH 连接；
- SecPathA 作为 SFTP 服务器，IP 地址为 10.111.27.91；
- SecPathB 作为 SFTP 客户端；
- SFTP 的用户名为 ftpuser，密码为 pwd。

2. 组网图

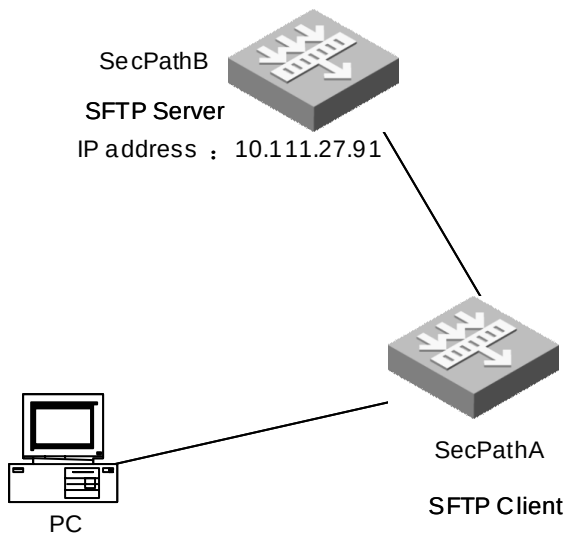


图14-9 SFTP 配置组网图

3. 配置步骤

(1) 配置服务器端 SecPathB。

启动 SFTP 服务器。

```
[H3C] sftp server enable
```

指定用户的服务类型为 SFTP。

```
[H3C] ssh user ftpuser service-type sftp
```

(2) 配置客户端 SecPathA。

与远程 SFTP 服务器建立连接，进入 SFTP client 视图。

```
[H3C] sftp 10.111.27.91
```

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
```

Remove this File?(Y/N)

flash:/zy

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
```

新增目录 new1，并检查是否新目录是否创建成功。

```
sftp-client> mkdir new1
```

New path 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
```

将目录名 new1 更名为 new2，并查看是否更名成功。

```
sftp-client> rename new1 new2
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

# 从服务器上下载文件 pubkey2 到本地，并更名为 pu。

sftp-client> get pubkey2 pu
Downloading file successfully ended

# 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
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 pu
-rwxrwxrwx  1 noone  nogroup   283 Sep 02 06:36 puk
sftp-client>

# 退出 SFTP。

sftp-client> quit
Bye
<H3C>
```

14.7 哑终端服务

14.7.1 哑终端的功能描述

当防火墙的异步口（如 AUX 口）工作在流方式时，将计算机（或终端）的串口与防火墙的异步口直连，可以进入防火墙的命令行接口，对防火墙进行配置，这称作哑终端工作方式。在哑终端基础上，可以建立其它应用，如执行 Telnet 命令登录其它设备。

用户在 PC 上运行超级终端可以与防火墙的异步口相连登录到防火墙，对防火墙进行配置管理。如下图所示。

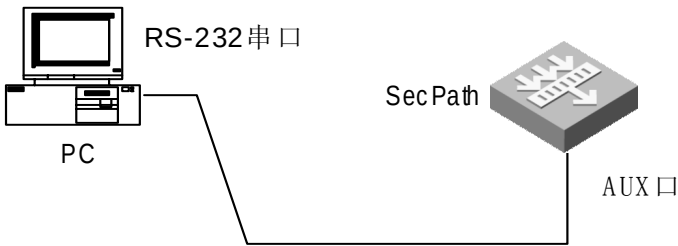


图14-10 哑终端连接方式

14.7.2 哑终端服务特性

参见 表 14-2，与远程服务终端方式一致。

14.7.3 哑终端的典型应用

哑终端的典型应用方式：

- 异步口工作在流方式下，通过专线连接直接进入防火墙的命令行接口，提供除 Console 口、Telnet 之外的另一种终端服务。
- 异步口工作在流方式下，通过异步专线直接登录到防火墙的命令行接口，再启动 Telnet Client 客户端程序登录到其它远程系统上工作。

14.7.4 配置哑终端服务

与哑终端相关的配置命令如下表所示。请在接口视图下进行 **async mode** 命令的配置。请在用户界面视图下进行 **auto-execute command** 命令的配置。

表14-39 建立哑终端连接相关命令

操作	命令
设置异步接口的流方式	async mode flow
禁止异步接口的流方式	async mode protocol
在异步口上自动执行配置命令	auto-execute command <i>command</i>
在异步口上禁止自动执行配置命令	undo auto-execute command

1. 哑终端方式配置

配置与终端连接的异步口。

对 AUX 口配置如下：

```
[H3C-ui-aux0] undo modem
[H3C-Aux0] async mode flow
```


在执行上述操作后，在该异步口的外接终端上键入回车，进入防火墙的配置界面；在配置过程中，如果执行 **quit** 退出命令行界面，必须重新键入回车。

 说明：

其中异步口设置为禁止 Modem 拨入，是在相应的用户界面视图下完成的。具体内容详见用户界面配置章节。

2. auto-execute command 配置

如果在防火墙的异步口配置了 **auto-execute command** 命令，那么，当用户在该异步口的外接终端上敲入两个回车后，防火墙将自动执行某些命令，直接进入工作状态。

auto-execute command 命令使用时有如下的限制：

- 如果防火墙上只有一个 Console 口或只有一个 AUX 口（Console 口和 AUX 口共一个口），那么这个口将不支持 **auto-execute command**。
- 如果防火墙上有一个 Console 口和一个 AUX 口（共两个口）则 Console 口不支持 **auto-execute command**，AUX 口支持 **auto-execute command**。
- 对其它类型接口不作限制。

用户在登录时，自动执行某条在该终端上用 **auto-execute command** 配置好的命令，命令执行结束后，自动断开用户线。通常的用法，是在终端用 **auto-execute command** 配置 Telnet 命令，使用户自动连接到指定的主机。使用该命令，将导致不能用该终端线对本系统进行常规的配置，需谨慎使用。



注意：

在配置 **auto-execute command** 命令并保存配置（执行 **save** 操作）之前，要确保可以通过其他方法登录系统，以去掉此配置。

auto-execute command 命令最典型的应用是用户以哑终端方式与防火墙建立连接后，可以通过 **auto-execute command** 指定的 Telnet 命令再远程登录到其它防火墙、路由器、主机或工作站上进行工作，这时，防火墙对终端用户来说是透明的。如下图所示：

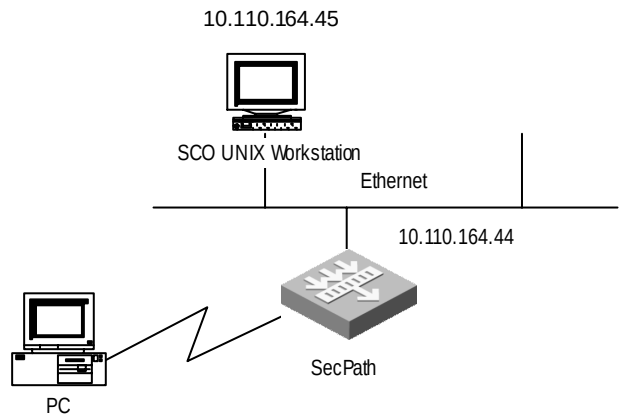


图14-11 auto-execute command 配置示意图

配置步骤：

- # 将 AUC 口配置成哑终端方式，参见上一小节配置。
- # 配置 **auto-execute command** 命令。在用户界面视图下键入：

```
[H3C-ui-aux0] auto-execute command telnet 10.110.164.45
```

配置完成后，在与防火墙的 AUC 口相连的终端上键入回车，直接登录到目的主机上。若退出目的主机，重新键入回车，可再次登录到目的主机上。

说明：

取消 **auto-execute command** 功能，在相应的用户界面视图下执行命令：**undo auto-execute command**。

14.7.5 哑终端连接的定时断开

请在用户界面视图下进行下列配置。

表14-40 哑终端连接的定时断开

操作	命令
允许定时断开哑终端连接	idle-timeout <i>minutes</i> [<i>seconds</i>]
恢复定时断开哑终端连接的默认值	undo idle-timeout

本功能是为了防止未授权用户的非法侵入。如果用户设置了 **idle-timeout**，在此时间内没有接收到哑终端用户的输入时，则断开与用户的连接。哑终端用户的定时断开时间为 10 分钟。用户可以在相应的用户界面视图下执行 **idle-timeout 0** 命令，关闭该功能。关闭该功能后，哑终端用户将永远不被断开。

禁止定时断开哑终端用户连接。

```
[H3C-ui-aux0] idle-timeout 0
```

第15章 Modem 管理配置

15.1 Modem 管理简介

15.1.1 Comware 提供的 Modem 管理功能

Modem 是目前使用广泛的一种网络设备，实现对 Modem 的良好管理和控制是防火墙的一个重要功能，但是由于 Modem 的厂家众多而且类型各异，虽然都支持业界标准的 AT 命令集，但在具体的实现和命令的细节上存在着或多或少的差别。

为了使防火墙可以提供尽可能好的灵活性，防火墙提供如下的 Modem 管理功能：

- (1) 提供用于 Modem 管理的脚本语言（以下称为 Modem 脚本），用来良好地控制与防火墙连接的 Modem 设备。Modem 脚本可以通过以下两种方式来执行：
 - 直接通过 **start-script** 命令执行 Modem 脚本，对 Modem 进行初始化或其它配置。
 - 通过特定事件（如防火墙启动、Modem 呼通等）触发 Modem 脚本的执行。
- (2) 脚本和其相关的命令相配合使用可以增强防火墙的远程配置功能，当异步口工作在 Flow 方式下，用户可通过哑终端方式或从远端通过 Modem 拨号方式建立与该异步口的连接，并配置管理防火墙。
- (3) 与其他设备提供商的设备进行互通，即双方的异步口都工作在 Flow 方式下并通过 Modem 进行互连。
- (4) 提供了丰富的调试信息，便于 Modem 的监控和维护。

15.1.2 Modem 脚本

1. Modem 脚本的用途

防火墙提供了 Modem 脚本，其主要用途有：

- 使用 Modem 脚本可以灵活地控制不同型号的 Modem 设备，通过执行不同的初始化 AT 指令串，使不同厂家和型号的 Modem 可以和防火墙更好地协调工作。
- 使用 Modem 脚本交互式地登录远端系统，通过脚本的交互协商转入不同的连接状态。当双方设备的异步口通过 Modem 建立连接之后，通过交互协商确定该物理链路上封装何种协议及采用哪些工作参数。

2. Modem 脚本的语法

Modem 脚本常见格式如下：

receive-string1 send-string1 receive-string2 send-string2.....

其中：

- *receive-string* 表示接收字符串，*send-string* 表示发送字符串。
- *receive-string* 和 *send-string* 一般成对出现，而且脚本必须以接收字符串为开始。如 *receive-string1 send-string1* 表示的执行流程为：希望从 Modem 接收到字符串 *receive-string1*，如果在超时之前接收到字符串与 *receive-string1* 匹配成功则继续执行以下脚本，向 Modem 发送字符串 *send-string1*，否则终止脚本的执行。
- 如果最后一个字符串为发送字符串，则表明发送该字符串后，即可结束脚本的执行，不需再等待接收字符串。
- 如果脚本的开始不需接收字符串，而直接等待发送字符串，这时可以将第一个发送字符串置为""，关于双引号的意义后面有详细介绍。
- 对于接收字符串，除以“\c”结束之外，发送时均会在字符串结尾自动附加一个回车符。
- 对于接收字符串的匹配，采用与位置无关的匹配方法，即只要接收的内容中含有希望接收的串，就认为匹配成功。
- 接收字符串的匹配，希望接收的字符串可以有多个，它们之间用“-”连接，只要与其中之一匹配，即认为匹配成功。
- 等待接收字符串的超时时间缺省为 5 秒，在脚本中可随时插入 **TIMEOUT seconds** 来调整等待接收字符串的超时时间，并在同一个脚本的下一次 **TIMEOUT** 设置前一直有效。
- 脚本中所有字符串和关键字都是大小写敏感的。
- 各字符串或关键字之间用空格进行分割，如果一个字符串内部包含空格，则需要用双引号（" "）括起来，如果双引号内没有任何内容（即为""），则该字符串可能有两重意义，如果""位于脚本的开始，表示不需要从 Modem 接收任何字符串，而直接向 Modem 发送字符串；如果""位于脚本其它位置，则表示一个内容为""的字符串。
- 在脚本中可随时插入 **ABORT receive-string** 来改变脚本的执行流程，表示如果接收字符串与 *receive-string* 完全匹配，则终止脚本的执行。在脚本中 **ABORT receive-string** 可以出现多次，它们将会共同起作用，只要与其中之一匹配，即终止脚本的执行，而且无论 **ABORT receive-string** 在何处出现，但它在整个脚本执行过程中均起作用。

- 在脚本中可以插入转义字符，用于更好地对脚本进行控制并增加脚本的灵活性，另外所有的转义字符同时也是字符串的分隔符。

表15-1 脚本关键字列表

关键字	说明
ABORT <i>receive-string</i>	ABORT 后跟一个字符串，用于和 Modem 或对端的 DTE 设备传来的字符串进行匹配，匹配的方式是完全匹配，一个脚本中可以有多条 ABORT 指定，每一个都在脚本的整个执行期有效。
TIMEOUT <i>seconds</i>	TIMEOUT 后跟一数字，用于设置接收字符串的等待超时时间，在等待的时间内如果没有收到希望的字符串，则脚本执行失败。此设置在设置以后有效，一直作用到下一次进行 TIMEOUT 设置。

其中，*seconds* 单位为秒，缺省值为 180，取值范围为 0~180。

表15-2 脚本转义字符列表

转义字符	说明
\c	表示只发送所指定的字符串，不自动附加回车符。 \c 位置只能在发送字符串的末尾，其他的位置无效。
\d	表示暂停 2 秒
\n	表示换行字符
\r	表示回车字符
\s	表示空格字符
\t	表示制表字符
\l	表示反斜杠字符
\T	表示电话号码

15.2 Modem 管理的配置

Modem 管理配置包括：

- 配置 Modem 的呼入和呼出权限
- 配置 Modem 脚本
- 手工执行 Modem 脚本
- 配置 Modem 的应答方式

15.2.1 配置 Modem 的呼入和呼出权限

请在用户界面视图下进行下列配置。

表15-3 配置 Modem 的呼入和呼出权限

操作	命令
只允许 Modem 呼入/呼出	modem [call-in call-out]
允许 Modem 呼入和呼出	modem both
禁止 Modem 呼入和呼出	undo modem both
禁止 Modem 呼入/呼出	undo modem [call-in call-out]

缺省情况下，禁止 Modem 呼入和呼出。

说明：

使能 modem 的时候系统自动禁止 undo detect dsr-dtr 命令，在 undo detect dsr-dtr 的时候系统禁止自动 modem 命令。

15.2.2 配置 Modem 脚本

请在系统视图下进行下列配置。

表15-4 配置 Modem 脚本

操作	命令
定义 Modem 脚本	script-string <i>script-name script-content</i>
删除 Modem 脚本	undo script-string <i>script-name</i>

关于 *script* 的具体格式请参考 Modem 脚本语法。

15.2.3 手工执行 Modem 脚本

可以在需要的时候用 **start-script** 命令执行指定的 Modem 脚本来管理该接口外接的 Modem。

请在用户视图下进行下列配置。

表15-5 手工执行 Modem 脚本

操作	命令
手工执行 Modem 脚本	start-script <i>script-name number</i>

15.2.4 配置 Modem 的应答方式

建议根据防火墙外接 Modem 的当前应答状态配置该命令，当 Modem 状态为自动应答（Modem 的 AA 灯亮）时，配置 **modem auto-answer**（以避免 Modem 自动应

答后，防火墙又发出应答指令）；如果外接 Modem 为非自动应答方式，则可配置 **undo modem auto-answer**。

 说明：

当该命令的配置与 Modem 当前的应答状态不一致时，对于某些 Modem 可能会造成应答不正常。

请在用户界面视图下进行下列配置。

表15-6 配置 Modem 的应答方式

操作	命令
Modem 为自动应答方式	modem auto-answer
Modem 为非自动应答方式	undo modem auto-answer

缺省情况下，Modem 为非自动应答方式。

15.3 Modem 显示和调试

在用户视图下，执行 **debugging** 命令可以打开调试开关或者显示其各项状态参数，从而可以监控和维护 Modem。

表15-7 Modem 显示和调试

操作	命令
打开 Modem 调试开关	debugging modem

15.4 Modem 典型配置举例

15.4.1 使用 Modem 脚本管理 Modem

1. 配置 Modem 适配波特率

(1) 组网需求

对于和 Modem 相连的异步口，使用标准的 AT 命令进行 Modem 的波特率的配置。在 AT 命令集中，向 Modem 发送“AT”，收到“OK”，则 Modem 可以自动地匹配相应的波特率，然后将配置写入 Modem 中进行保存，相应的 AT 命令是“AT&W”。

(2) 组网图

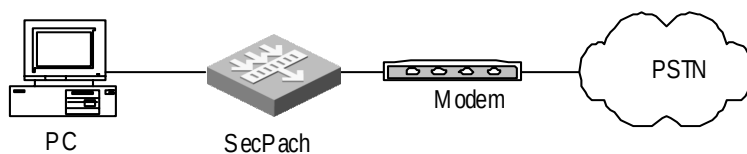


图15-1 防火墙对 Modem 管理配置组网图

(3) 配置步骤

配置 Modem 脚本。

```
[H3C] script-string baud "" AT OK AT&W OK
```

在用户视图下执行相应的脚本，假设 Modem 连接在接口 aux0 上。查看显示信息得到接口 aux0 对应的编号。

```
<H3C> start-script baud 1
```

2. 恢复 Modem 出厂设置

(1) 配置需求

恢复出厂配置的 Modem 命令是“AT&F”。

(2) 配置步骤

```
[H3C] script-string factory "" AT OK AT&F OK
```

在用户视图下执行相应的脚本，假设 Modem 连接在接口 aux0 上。查看显示信息得到接口 aux0 对应的编号。

```
<H3C> start-script factory 1
```

15.4.2 使用脚本进行直接拨号

1. 配置需求

配置 Modem 脚本，直接进行拨号。

2. 配置步骤

```
[H3C] script-string dial "" AT OK ATDT8810058 CONNECT
```

在用户视图下执行相应的脚本，假设 Modem 连接在接口 aux0 上。查看显示信息可得到接口 aux0 对应的编号。

```
<H3C> start-script dial 1
```

15.5 Modem 管理常见故障的诊断与排除

故障之一：Modem 状态不正常（如啸叫声长时间不停止或持续忙音）。

故障排除：可以按照如下步骤进行。

- 在与 Modem 连接的防火墙物理接口上执行 **shutdown** 和 **undo shutdown** 命令，检查 Modem 状态是否恢复正常；
- 若 Modem 状态仍不正常，则可将 Modem 重新上电。

第16章 接口配置

16.1 接口配置概述

16.1.1 接口介绍

防火墙的接口即指防火墙与网络中的其它设备交换数据并相互作用的部分，其功能就是完成防火墙与其它网络设备的数据交换。

Comware 支持防火墙上的物理接口和逻辑接口这两类接口。

物理接口就是真实存在、有对应器件支持的接口，如以太网接口。

逻辑接口是指能够实现数据交换功能但物理上不存在、需要通过配置建立的接口，包括 Dialer（拨号）接口、子接口以及虚拟模板接口等。

SecPath 系列安全产品上的物理接口目前只提供以太网接口和 AUX 接口。

16.1.2 接口的配置

1. 接口的视图

为了便于对接口进行配置和维护，在 Comware 软件中设置了接口视图。与接口有关的各种命令都必须在相应的接口视图下使用。

(1) 进入接口视图的方法

请在系统视图下进行下列操作，进入指定接口的视图。

表16-1 进入指定接口的视图

操作	命令
进入指定接口的视图	interface <i>type number</i>

(2) 退出接口视图的方法

在接口视图下，键入 **quit** 命令，就可以退回到系统视图。

2. 设置接口描述信息

防火墙的物理接口都有一个接口描述信息配置项，接口描述信息主要用来帮助识别接口的用途。请在接口视图下进行下列配置。

表16-2 设置接口描述信息

操作	命令
设置接口描述信息	description <i>interface-description</i>
恢复接口的缺省描述信息	undo description

可以使用 **display interface** 命令查看接口缺省的描述信息。

3. 配置接口平均速率统计周期

在系统视图下配置时，配置所有接口的统计周期。

表16-3 配置接口平均速率统计周期

操作	命令
配置接口平均速率的统计周期	flow-interval <i>seconds</i>
恢复接口平均速率的统计周期的缺省值	undo flow-interval <i>seconds</i>

缺省情况下，统计周期为 300 秒钟。

4. 设置 MTU

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

请在接口视图下进行下列配置。

表16-4 设置 MTU

操作	命令
设置 MTU	mtu <i>size</i>
恢复 MTU 的缺省值	undo mtu

以太网接口的 MTU 取值范围为 46~1500 字节；Dialer 接口的 MTU 取值范围为 128~1500 字节；Virtual-Template 的 MTU 取值范围为 128~1500 字节；Tunnel 接口的 MTU 取值范围为 100~64000 字节。

由于 QoS 队列长度有限，如果 MTU 太小而报文尺寸较大，可能会造成分片过多，报文被 QoS 队列丢弃。为避免这种情况，可适当增大 QoS 队列的长度。SecPath 防火墙的接口缺省使用的队列调度机制是 FIFO，可以在接口视图下使用命令 **qos fifo queue-length** 改变该队列长度。QoS 队列的具体配置可参考本手册的 QoS 配置部分。

5. 进一步配置接口的方法

在进一步配置一个接口前，需要对组网需求和组网图有一个完整、详细的了解。具体地配置一个接口至少需要完成以下工作：

- 如果该接口是物理接口，需要明确其连接情况、接口工作方式及相关工作参数。
- 配置该接口的网络协议（如 IP 协议）地址。
- 配置通过该接口能达到的目的网络的静态路由，或者配置动态路由协议在该接口上的工作参数。
- 如果需要在该接口上建立防火墙，则需要进行相关的报文过滤或地址转换等参数配置。

在接口视图下，需要配置的参数较多，本部分主要介绍物理接口所特有的一些参数的配置，同时，对逻辑接口的定义做简单介绍。有关链路层、网络层协议和参数的配置以及一些特殊功能的配置（如路由、防火墙等），在本手册的其它部分有专题介绍，本部分将不再赘述。

16.1.3 接口的显示和调试

表16-5 接口的显示和调试

操作	命令
显示接口当前运行状态和统计信息（所有视图下）	display interface [type [number]]
显示接口概要信息（所有视图下）	display brief interface [type [number]] [{ begin include exclude } text]
显示接口的 IP 信息（所有视图下）	display ip interface [type number]
清除接口统计信息（用户视图下）	reset counters interface [type [number]]
关闭接口（接口视图下）	shutdown
重启接口（接口视图下）	undo shutdown
打开指定接口的 debug 信息调试开关	debugging physical { all error event packet { all input output } } [interface interface-type interface-number]
关闭指定接口的 debug 信息调试开关	undo debugging physical { all error event packet { all input output } } [interface interface-type interface-number]

说明：

当防火墙的某物理接口闲置，没有连接电缆时，请使用 **shutdown** 命令关闭该接口，以防止由于干扰导致接口异常。

16.2 以太网接口

16.2.1 以太网接口介绍

1. 以太网接口类型

SecPath 防火墙支持的快速以太网接口 FE 分为电接口和光接口两种，分别符合 100Base-TX 和 100Base-FX 物理层规范；支持的千兆以太网接口 GE 也分为电接口和光接口两种，GE 电接口符合 1000Base-T 规范，GE 光接口符合 1000Base-LX 和 1000Base-SX 规范。

2. 工作速率及双工模式

在工作速率上，FE 电接口可以选择 10Mbit/s、100Mbit/s 两种速率；GE 电接口可以选择 10Mbit/s、100Mbit/s、1000Mbit/s 三种速率。

在工作方式上，FE 电接口和 GE 电接口都支持半双工和全双工两种方式。

为简化系统的配置和管理，FE 电接口和 GE 电接口都具有自动协商模式，可以与其他网络设备协商确定最合适的工作方式和速率。

光接口只能工作在全双工模式，并且速率也不能通过配置改变，FE 光接口只能以 100Mbit/s 的速率工作；GE 光接口只能以 1000Mbit/s 的速率工作。

3. 支持的帧格式

FE 和 GE 接口都能够接收帧格式为 Ethernet_II 或 Ethernet_SNAP 的以太网帧，并能自动辨认其格式，对于发送的帧则采用 Ethernet_II 格式。

16.2.2 以太网接口的配置

以太网接口配置包括：

- 进入指定以太网接口的视图
- 设置网络协议地址
- 选择以太网接口的工作速率
- 选择以太网接口的工作方式
- 允许或禁止对内自环
- 设置以太网接口的流控方式
- 配置以太网接口工作模式
- 配置以太网接口隔离

必须进入指定以太网接口的视图，才能对其进行配置。配置时，一般只要配置好 IP 地址就可以了。建议不要启用以太网接口的其它配置任务，因为其各项参数都有缺省值，可以保证系统在大多数情况下能够正常工作。

1. 进入指定以太网接口的视图

请在系统视图下进行下列配置。

表16-6 进入指定以太网接口的视图

操作	命令
进入指定以太网接口的视图	interface ethernet <i>number</i>
进入千兆以太网接口的视图	interface gigabitethernet <i>interface-number</i>

2. 设置网络协议地址

请在以太网接口视图下进行下列配置。

表16-7 设置接口的 IP 地址

操作	命令
设置接口的 IP 地址	ip address <i>ip-address mask</i> [sub]
取消接口的 IP 地址	undo ip address [<i>ip-address mask</i>] [sub]

当为一个以太网接口配置两个乃至两个以上的 IP 地址时，对第二个及以后的 IP 地址（即辅助的 IP 地址）可以用 **sub** 关键字加以指示。

3. 选择以太网接口的工作速率

以太网接口可以支持多种速率。FE 电接口支持 10Mbit/s、100Mbit/s 两种速率，FE 光接口只支持 100Mbit/s；GE 电接口支持 10Mbit/s、100Mbit/s、1000Mbit/s 三种速率，而 GE 光接口只能选用 1000Mbit/s 速率。因此，只需对以太网电接口进行配置，而光接口不需要配置。

请在以太网接口视图下进行下列配置。

表16-8 选择以太网接口的工作速率

操作	命令
选择快速以太网接口的工作速率	speed { 10 100 negotiation }
设置 GE 电接口的工作速率	speed { 10 100 1000 negotiation }
恢复缺省的工作速率	undo speed

缺省速率选择 **negotiation**，即系统自动协商最佳的工作速率。

 说明：

- FE 电接口和 GE 电接口的缺省速率及双工模式均为自动协商模式，用户也可强制更改速率及双工模式，但应确保速率及双工模式与连接对端相同。
- 如果在强制模式下执行自动协商命令（**duplex negotiation** 或 **speed negotiation**），则以太网电口转入自动协商模式，同时协商速率及双工模式。
- 对于 GE 电接口，工作速率 1000Mbit/s 与半双工模式是互斥的，不能同时配置。

4. 选择以太网接口的工作方式

如前所述，以太网接口可以工作在全双工和半双工两种工作方式下。与 Hub 相连时，防火墙以太网接口应选择工作在半双工方式下；与交换式 LAN Switch 相连时，防火墙以太网接口应选择工作在全双工方式下。FE 电接口和 GE 电接口对这两种模式都支持，而 FE 光接口和 GE 光接口只能工作在全双工模式。

可以在以太网接口视图下进行下列配置来选择工作方式。

表16-9 选择以太网接口的工作方式

操作	命令
选择以太网接口的工作方式	duplex { negotiation full half }
恢复以太网接口的缺省工作模式	undo duplex

缺省情况下，FE 电接口和 GE 电接口为 **negotiation** 方式，即系统自动协商最佳的双工模式。

 说明：

- 对于 GE 电接口，工作速率 1000Mbit/s 与半双工模式是互斥的，不能同时配置。
- SecPath F100-C 防火墙的 WAN 接口不支持自动协商。

5. 允许或禁止对内自环

在对以太网接口作特殊功能测试时，有时需要将其设为对内自环。可以在以太网接口视图下进行下列配置，允许其对内自环。

表16-10 允许或禁止对内自环

操作	命令
允许对内自环	loopback
禁止对内自环	undo loopback

缺省为禁止对内自环。

6. 设置以太网接口的流控方式

请在以太网接口视图下进行下列配置。

表16-11 设置以太网接口启用流控

操作	命令
设置以太网接口启用流控	flow-control
恢复缺省设置	undo flow-control

缺省情况下，不启用流控。如本端启用流控，那么只有在对端也支持流控时才有效。当启用流控时，如果协商失败，不能正常进入 UP 状态。并且，如果本端为流控方式，当对端的配置发生变化时，建议对本端先执行 **shutdown** 命令，再执行 **undo shutdown** 命令重启，以保证双方的流控方式仍保持一致。

7. 配置以太网接口工作模式

请在以太网接口视图下进行下列配置。

表16-12 配置以太网接口工作模式

操作	命令
将以太网接口设为混杂模式	promiscuous
取消以太网接口混杂模式	undo promiscuous

缺省情况下，以太网接口为非混杂模式。

当以太网接口被配置为混杂模式后将不再进行 MAC 地址过滤，接收所有正确的以太网报文。该模式主要用于网络监听功能。

当启动桥功能并将以太网接口加入 **bridge-set** 后，该以太网接口将自动进入混杂模式；当将以太网接口退出 **bridge-set** 后，该以太网接口将自动进入非混杂模式。

8. 配置以太网接口隔离

LAN 以太网接口可以工作在隔离模式下，也可以工作在非隔离模式下。所谓隔离模式，就是各个 LAN 以太网接口工作在第三层，作为可路由接口使用，即可以为其配置各种第三层属性，如 IP 地址等。所谓非隔离模式，就是各个 LAN 以太网接口工作在 Hub 方式，即工作在物理层，不能为其配置如 IP 地址等第三层属性。当 LAN 以太网接口工作在非隔离模式下时，可以通过配置一个管理 IP 地址以对其进行管理或使其提供网络服务（例如 Telnet、SNMP、NAT 等）。

请在系统视图下进行下列配置。

表16-13 配置以太网接口隔离

操作	命令
配置以太网接口隔离	insulate
取消以太网接口隔离	undo insulate

缺省情况下，LAN 以太网接口工作在隔离模式下。

仅 SecPath F100-A 防火墙、SecPath V100-S 安全网关支持此功能。

 说明：

- 当各个 LAN 以太网接口互相隔离时，所有 LAN 以太网接口都对用户可见，并可以对其进行单独配置如 IP 地址等第三层属性。
- 当各个 LAN 以太网接口未被隔离时，对用户可见的只有一个管理接口，其它所有的 LAN 以太网接口都不可见。可以在管理接口上配置 IP 地址作为管理 IP 地址。
- 由于接口性质的因素，只能在第一个 LAN 口（即编号最小的）上配置子接口。在隔离模式下扩展出来的另外三个 LAN 口都不能配置子接口，且第一个 LAN 口上配置的子接口只能在非隔离模式下工作。

16.2.3 以太网接口的显示和调试

请在所有视图下进行下列配置。

表16-14 显示指定以太网接口的状态

操作	命令
显示指定以太网接口的状态	display interface ethernet <i>number</i> display interface gigabitethernet <i>number</i>

16.2.4 以太网接口典型配置举例

1. 组网需求

如下图所示，防火墙的以太网接口连接到 IP 网络 192.168.0.0。局域网内的计算机通过防火墙连接到 Internet。将防火墙以太网接口的 MTU 设置为 1492 字节。

2. 组网图

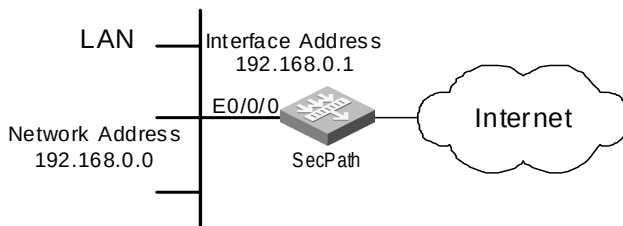


图16-1 以太网配置举例组网图

3. 配置步骤

指定以太网接口 Ethernet 0/0/0 的 IP 地址为 192.168.0.1，掩码为 255.255.0.0。

```
[H3C] interface ethernet 0/0/0
```

```
[H3C-Ethernet0/0/0] ip address 192.168.0.1 255.255.0.0
```

设置该接口的 MTU 为 1492 字节。

```
[H3C-Ethernet0/0/0] mtu 1492
```

16.2.5 以太网接口常见故障的诊断与排除

采用如下测试方法，可以判别以太网接口是否有故障：

- 从与防火墙位于同一局域网内的主机 ping 防火墙的以太网接口，观察是否能够正确返回全部报文。
- 查看连接双方（如防火墙和交换机）的统计信息，观察接收到的错误帧的统计数字是否快速增加。

只要这两项测试中有一项不能通过，就可以确定防火墙的以太网接口或其连接的以太网工作不正常。

在确认存在故障之后，可以按照如下步骤进行排查：

第一步：查看主机和防火墙的局域网连接是否正确。

若使用 Hub 或 LAN Switch 连接以太网，请确认 Hub 或 LAN Switch 上的相应连接（link）指示灯的亮/灭状态。如果均为亮，则表明主机与防火墙的以太网接口以及网线物理上是正常的；否则，请更换网卡、网线、防火墙或其相应接口模块等物理设备。

在使用非屏蔽双绞线连接以太网，且连接双方中至少有一方支持 100Base-TX 的情况下，还需考虑速率匹配问题。如果双方的工作速率设置不匹配，即一方工作于 100Mbps 模式，而另一方工作于 10Mbps 模式，则故障表现为：配置为 100Mbps 的一方显示没有连接；配置为 10Mbps 的一方显示连接建立，但物理层活动（ACTIVE）指示灯持续快速闪烁，并且不能正常收发。

在检查防火墙的快速以太网接口连接问题时，以下两条提示信息很有帮助。这两条信息都是在用户执行速率选择命令或连接网线时输出在控制台上的：

```
Ethernet 0/0/0: Warning--the link partner do not support 100M mode  
Ethernet 0/0/0: Warning--the link partner may not support 10M mode
```

其中第一条提示信息表明，防火墙以太网接口检测到所连接的对端不支持 100Mbps 工作速率，而本端的配置为强制工作在 100Mbps 速率下。此时，用户应确认对端也进行了相应配置，使之能够工作于 100Mbps 速率下。第二条提示信息表明，防火墙以太网接口检测到所连接的对端有可能不支持 10Mbps 工作速率，而本端的配置为强制工作在 10Mbps 速率下。此时，用户应确认对端能够工作于 10Mbps 速率下。不过，当防火墙快速以太网接口连接 Hub 的 10/100Mbps 自适应端口时，此条信息并不意味着设置错误。

第二步：查看主机和防火墙的以太网接口的 IP 地址是否位于同一子网内，即二者的网络地址必须是相同的，仅仅是主机地址不相同。如果不在同一子网内，请重新设置 IP 地址。

第三步：查看以太网接口的工作方式是否正确。使用非屏蔽双绞线或光纤连接以太网时，10Base-T/100Base-TX/100Base-FX 标准规定有全双工和半双工两种工作方式。在使用 Hub 时，应该以半双工方式工作。在使用交换式 LAN Switch 时，如果 LAN Switch 工作在半双工方式，则防火墙的以太网接口也工作在半双工方式；如果 LAN Switch 工作在全双工方式，则防火墙的以太网接口也工作在全双工方式。当工作方式不正确，即连接的一方工作于全双工方式而另一方工作于半双工方式时，故障现象为：网络流量增大时，配置为半双工工作方式的一侧显示网络冲突频繁（如连接 Hub 则整个网段上所有其它机器都显示网络冲突严重），配置为全双工工作方式的一侧则显示接收了大量的错误报文，同时伴有双方报文丢弃严重的现象。可用 **display interface** 命令查看以太网接口收发报文的错误率。冲突现象一般可以通过以太网接口状态指示灯观察到。

第四步：查看以太网接口的流控模式是否正确。

对于以太网接口，缺省不采用流控，如果对端为强制流控模式，则可能导致无法 UP。这种情况下，请配置两端的流控设置一致，并对接口执行 **shutdown**、**undo shutdown** 命令重启。

如果上述方法仍无法帮您排错，请与技术支持人员联系。

16.3 AUX 接口

16.3.1 AUX 接口介绍

AUX 接口是防火墙提供的一个固定端口，它可以作为普通的异步串口使用，最高速率为 115200bps。利用 AUX 接口，可以实现对防火墙的远程配置、线路备份等功能。

16.3.2 AUX 接口配置

AUX 接口的配置包括：

- 设置链路建立方式
- 设置电平检测功能
- 设置对内自环
- 设置链路层协议类型

1. 设置链路建立方式

AUX 接口有两种链路建立方式：

- **protocol**：协议方式，即物理连接建立之后，直接采用已有的链路层协议配置参数建立链路。
- **flow**：流方式，又称交互方式。指拨号成功之后，链路的两端进行交互，主叫端向接收端发送配置命令（与用户从远端手工键入配置命令效果相同），设置接收端的链路层协议工作参数，然后建立链路。一般用于拨号等人机交互的情况下。交互方式下的用户又称为 EXEC 用户。

请在 AUX 接口视图下进行下列配置。

表16-15 设置 AUX 接口建立链路方式

操作	命令
设置 AUX 接口采用协议方式建立链路	async mode protocol
设置 AUX 接口采用流方式建立链路	async mode flow

缺省情况下，采用流方式（flow）。

2. 设置电平检测功能

如果设置禁止 AUX 接口的电平检测功能，系统将不检测 AUX 接口是否外接电缆，自动向用户报告 AUX 口的状态为 UP，且 DTR=UP、DSR=UP；如果设置允许 AUX 接口的电平检测功能，则系统不仅检测 AUX 接口是否外接电缆，同时要检测 DSR（Data Set Ready）信号，只有当该信号有效时，系统才认为 AUX 接口处于 Up 状态，否则为 Down 状态。

请在 AUX 接口视图下进行下列配置。

表16-16 设置 AUX 接口的电平检测功能

操作	命令
允许 AUX 接口的电平检测功能	detect dsr-dtr
禁止 AUX 接口的电平检测功能	undo detect dsr-dtr

缺省情况下，允许电平检测。

3. 设置对内自环

在对 AUX 接口作特殊功能测试时，有时需要将其设为对内自环。

请在 AUX 接口视图下进行下列配置。

表16-17 允许或禁止 AUX 接口的对内自环

操作	命令
允许 AUX 接口对内自环	loopback
禁止 AUX 接口对内自环	undo loopback

缺省情况下，禁止对内自环。

4. 设置链路层协议类型

请在 AUX 接口视图下进行下列配置。

表16-18 设置 AUX 接口的链路层协议类型

操作	命令
设置链路层协议类型为 PPP	link-protocol ppp

AUX 接口的其他配置，如速率、停止位、校验方式、流控方式等，均在用户界面视图下配置，详细描述请参考本手册中“系统管理”部分的“用户界面配置”。

16.4 逻辑接口配置

逻辑接口指能够实现数据交换功能但物理上不存在，需要通过配置建立的接口，包括 Dialer（拨号）接口、子接口、LoopBack 接口、NULL 接口以及虚拟模板接口等等。

16.4.1 Dialer 接口

1. Dialer 接口介绍

Dialer 接口即拨号接口，在配置 PPPoE Client 时使用。

2. Dialer 接口配置

(1) 配置拨号控制列表

请在系统视图下进行下列配置。

表16-19 配置拨号控制列表

操作	命令
配置拨号控制列表	dialer-rule <i>dialer-number</i> { <i>protocol-name</i> { permit deny } acl <i>acl-number</i> }
删除拨号控制列表	undo dialer-rule <i>dialer-number</i>

(2) 创建 Dialer 接口

请在系统视图下进行下列配置。

表16-20 创建 Dialer 接口

操作	命令
创建 Dialer 接口，并进入 Dialer 接口视图	interface dialer <i>number</i>
删除 Dialer 接口的已有配置	undo interface dialer <i>number</i>

(3) 指定一个 Dialer 用户

请在拨号接口视图下进行下列配置。

表16-21 指定一个 Dialer 用户

操作	命令
指定一个 Dialer 用户	dialer user <i>username</i>

(4) 配置 Dialer 接口使用的 Dialer bundle

请在拨号接口视图下进行下列配置。

表16-22 配置 Dialer 接口使用的 Dialer bundle

操作	命令
配置 Dialer 接口使用的 Dialer bundle	dialer bundle <i>number</i>
删除 Dialer 接口使用的 Dialer bundle	undo dialer bundle

(5) 配置拨号接口的拨号访问组

请在拨号接口视图下进行下列配置。

表16-23 配置拨号接口的拨号访问组

操作	命令
配置拨号接口的拨号访问组	dialer-group <i>group-number</i>
将拨号接口从指定拨号访问组中删除	undo dialer-group

(6) 配置拨号接口的虚拟波特率

接口的虚拟波特率可以向上层协议（如 OSPF 路由协议）准确的告知接口的波特率，并使上层协议准确地运行。

请在拨号接口视图下进行下列配置。

表16-24 配置拨号接口的拨号访问组

操作	命令
配置拨号接口的拨号访问组	dialer-group <i>group-number</i>
将拨号接口从指定拨号访问组中删除	undo dialer-group

缺省情况下，未配置接口的虚拟波特率。

配置了 **virtualbaudrate** 命令后，需要使用命令 **shutdown** 关闭接口，然后再使用 **undo shutdown** 命令启用接口，这样该配置对于上层协议才能生效。

16.4.2 Loopback 接口

1. Loopback 接口介绍

TCP/IP 协议规定，127.0.0.0 网段的地址属于环回地址。包含这类地址的接口属于环回接口。在防火墙上，定义了接口 **Loopback0** 为环回接口，环回接口可以用来接收所有发送给本机的数据包。

有些应用（比如配置 SNA 的 **localpeer**）需要在不影响物理接口配置的情况下，配置一个带有指定 IP 地址的本地接口，并且出于节约 IP 地址的需要，需要配置 32 位掩码的 IP 地址，并且需要将这个接口上的地址通过路由协议发布出去。新增加的 Loopback 接口就是为了满足这种需要而设计的。

2. Loopback 接口的配置

Loopback 接口的配置包括：

- 创建 Loopback 接口
- 配置接口工作参数

(1) 创建 Loopback 接口

表16-25 创建/删除 Loopback 接口

操作	命令
创建 Loopback 接口并进入 Loopback 接口视图	interface loopback number
删除指定的 Loopback 接口	undo interface loopback number

(2) 配置接口工作参数

在 Loopback 接口上可以配置 IP 地址、IP 路由等参数，具体配置请参考本手册的其它部分。



注意：

在 Loopback 接口上可以配置 32 位的子网掩码，即子网掩码可以为 255.255.255.255。而且这个带有 32 位子网掩码的 IP 地址可以通过路由协议向外发布。

在配置 Loopback 接口的 IP 地址时，最好配置 32 位掩码的主机地址，这样既可以节约地址，也可以满足其它接口借用地址的需求。

Loopback 接口也可以被 **shutdown** 命令关闭。

16.4.3 Null 接口

1. Null 接口介绍

防火墙支持 Null 接口，它永远处于 Up 状态，但不能转发数据包，也不能配置 IP 地址或配置其它链路层协议。

Null 接口是一种纯软件性质的逻辑接口。任何送到该接口的网络数据报文都会被丢弃。

2. Null 接口的配置

配置 Null 接口就是创建 Null 接口。

在防火墙上可以创建一个 Null 0 接口，请在系统视图下进行下列配置。

表16-26 创建/删除 Null 接口

操作	命令
创建 Null 接口并进入 Null 接口视图	interface null 0
删除 Null 接口	undo interface null 0

由于任何到达 Null 接口的报文都会被丢弃，这就提供了另一种实现报文过滤的方法：可以简单地将不需要的网络流量发送到 Null0 接口，从而免去配置访问控制列表 ACL 的复杂工作。

例如：使用静态路由配置命令 **ip route-static 92.101.0.0 255.255.0.0 null 0** 将丢弃所有去往网段 92.101.0.0 的报文。

16.4.4 子接口

1. 子接口介绍

Comware 中支持子接口，允许用户在防火墙的单个物理接口上配置多个子接口，为用户提供提供了很高的灵活性。

所谓子接口，就是在一个物理接口上配置出来的多个逻辑上的虚接口。这些虚接口共用物理接口的物理层参数，又可以分别配置各自的链路层和网络层参数。因这样的多个虚接口可以对应一个物理接口，故常被称为“子接口”。

在 SecPath 系列防火墙中，支持以太网子接口。

2. 以太网子接口的配置

以太网子接口的配置包括：

- 配置以太网接口的子接口
- 配置以太网接口的子接口的封装类型及 VLAN ID
- 设置某个 VLAN 的每秒的最大处理报文数目（可选）

(1) 创建和删除以太网子接口

请在系统视图下进行下列配置。

表16-27 创建和删除以太网子接口

操作	命令
创建以太网子接口并进入以太网子接口视图	interface ethernet <i>number.sub-number</i> interface gigabitethernet <i>number.sub-number</i>
删除指定的以太网子接口	undo interface ethernet <i>number.sub-number</i> undo interface gigabitethernet <i>number.sub-number</i>

在进行上面的配置时，如果相应（与 *sub-number* 相同）的以太网子接口已经创建，则将直接进入该子接口视图；否则，将先创建以太网子接口，子接口号为指定的 *sub-number*，然后，再进入该子接口的视图。

系统最多支持创建 1024 个以太网子接口。

(2) 配置 VLAN 相关参数

请在系统视图或者以太网子接口视图下进行下列配置。

表16-28 配置 VLAN 相关参数

操作	命令
设置以太网子接口或千兆以太网子接口的封装类型以及相关联的 VLAN ID（接口视图下）	vlan-type dot1q vid vid
取消以太网子接口或千兆以太网子接口的封装类型以及相关联的 VLAN ID（接口视图下）	undo vlan-type dot1q vid
设置某个 VLAN 的每秒的最大处理报文数目（系统视图下）	max-packet-process count vid
将某个 VLAN 的每秒的最大处理报文数目恢复为缺省配置（系统视图下）	undo max-packet-process vid

缺省情况下，系统子接口上无封装，也没有与子接口关联的 VLAN ID，没有最大处理报文数目的限制。

当配置了以太网子接口的封装类型后，子接口就被设置为允许 VLAN 中继。

(3) 配置相关的其它工作参数

当以太网子接口没有配置 VLAN id 时，它只能支持 IPX 网络协议，因此，在以太网接口的子接口上，只能配置 IPX 网络地址以及其它的 IPX 工作参数等，具体的配置步骤和方法与配置以太网接口类同。在以太网子接口配置了 VLAN id 之后，它可以支持 IP 及 IPX 协议。相关配置请参考本手册的“网络层协议”部分。

(4) 以太网子接口的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示以太网子接口配置 VLAN ID 后的运行情况，通过查看显示信息验证配置的效果。

执行 **reset** 命令可以清除该运行情况的统计信息。

表16-29 以太网子接口的显示和调试

操作	命令
显示指定 VLAN 配置的最大处理报文数目	display vlan max-packet-process vid
显示指定 VLAN 的报文统计信息，包括接收和发送的报文数目	display vlan statistics vid vid
显示某个接口的 VLAN 配置信息	display vlan interface interface-type interface-num
清除指定 VLAN 的报文统计信息	reset vlan statistics vid vid

16.4.5 虚拟模板接口和虚拟接口

1. 虚拟模板接口和虚拟接口介绍

虚拟模板接口（Virtual-Template），主要应用于 VPN 及 MP 等应用环境。

在 VPN 会话连接建立之后，需要创建一个虚拟接口用于和对端交换数据。此时，系统将按照用户的配置，选择一个虚拟模板接口，根据该模板的配置参数，动态地创建一个虚拟接口。有关 VPN 的相应配置，可以参看本手册中的“VPN 配置”部分章节。

同样，将多个 PPP 链路捆绑成 MP 之后，也需要创建一个虚拟接口与对端交换数据。此时，也可选择一个接口模板，以便动态地创建一个虚拟接口。

2. 虚拟模板接口的配置

在 VPN 及 MP 等应用环境中，虚拟接口的创建和删除由系统自动完成，对于用户是完全透明的。用户只需要在相应的物理接口上配置 VPN 或 MP，然后创建并配置虚拟模板接口，再将虚拟模板接口与相应的物理接口建立联系即可。

虚拟模板接口的配置包括：

- 创建和删除虚拟模板接口
- 设置虚拟模板接口的工作参数
- 建立虚拟模板接口与相关物理接口的对应关系

(1) 创建和删除虚拟模板接口

请在系统视图下进行下列配置。

表16-30 创建和删除虚拟模板接口

操作	命令
创建虚拟模板接口并进入虚拟模板接口视图	interface virtual-template <i>number</i>
删除虚拟模板接口	undo interface virtual-template <i>number</i>

在执行 **interface virtual-template** 命令时，如果相应的虚拟模板接口已经创建，将直接进入该虚拟模板接口的视图；否则，将先创建虚拟模板接口，模板号为指定的 *number*，然后，再进入该虚拟模板接口的视图。

在删除虚拟模板接口时，要确保由其派生的虚拟接口都已经被删除，而且该虚拟模板接口已不再被使用。

(2) 设置虚拟模板接口的工作参数

虚拟模板接口与一般的物理接口相比，链路层协议只支持 PPP，网络协议支持 IP，因此，可以设置如下工作参数：

- 设置 PPP 的工作参数
- 设置虚拟接口的 IP 地址
- 设置为 PPP 对端分配的 IP 地址（或 IP 地址池）

这些参数在虚拟模板接口上的设置与在普通接口上没有任何区别。

(3) 建立虚拟模板接口与相关物理接口的对应关系

在 VPN 应用环境中，需要建立 L2TP 组与虚拟模板接口的对应关系；在 MP 应用环境中，需要建立 MP 用户与虚拟模板接口的对应关系。

详细说明请参考本手册的“VPN”部分。

3. 虚拟模板接口和虚拟接口的显示和调试

虚拟接口将在需要的时候由系统自动创建，并使用相应虚拟模板接口的参数进行工作，不需要用户手工创建和配置。虚拟接口会由于底层链路断开或用户干预而被删除。

请在所有视图下使用 **display** 命令来显示指定虚拟模板接口的状态。

表16-31 显示指定虚拟模板接口和虚拟接口的状态

操作	命令
显示指定虚拟模板的状态	display interface virtual-template <i>number</i>
显示虚拟访问接口的状态	display virtual-access { <i>dialer number</i> vt <i>vt-number</i> user <i>user-name</i> peer <i>peer-address</i> va-number }*

对于由 PPPoE Client 的 Dialer 接口所生成的虚拟访问接口，不能通过此命令来查看。

4. 虚拟模板接口常见故障的诊断与排除

在进行虚拟模板接口故障的排查之前，应先确定虚拟模板接口是用于 VPN 虚拟访问接口的创建还是用于 MP 虚拟接口的创建；然后，再根据应用环境，对虚拟模板接口的故障进行定位。

故障之一：不能创建虚拟接口。

故障排除：原因可能有以下几种：

- 虚拟模板接口没有配置 IP 地址，因此导致 PPP 协商不通过，虚拟接口不能变为 Up 状态。
- 虚拟模板接口没有配置为对端分配的 IP 地址（或 IP 地址池），在实际应用中，需要给对方分配地址的情况下，虚拟接口无法满足要求，也不会变为 Up 状态。
- PPP 验证参数设置不正确，如对方不是本地防火墙已经定义的用户，则 PPP 协商也不能通过。

目 录

第 1 章 PPP配置	1-1
1.1 PPP协议简介	1-1
1.1.1 PPP简介	1-1
1.2 PPP配置.....	1-2
1.2.1 配置接口封装的链路层协议为PPP	1-3
1.2.2 配置轮询时间间隔.....	1-3
1.2.3 配置PPP验证方式及用户名、用户口令	1-3
1.2.4 配置PPP协商参数	1-6
1.2.5 配置PPP链路质量监测	1-10
1.2.6 PPP的显示和调试.....	1-10
1.3 配置PPP链路效率机制.....	1-11
1.3.1 配置IP报文头压缩.....	1-12
1.3.2 配置PPP报文STAC-LZS压缩	1-13
1.3.3 配置PPP报文VJ TCP头压缩	1-14
1.3.4 PPP链路效率机制的显示与调试.....	1-14
1.4 PPP典型配置举例	1-15
1.4.1 PAP验证举例.....	1-15
1.4.2 CHAP验证举例.....	1-16
1.5 PPP故障诊断与排错	1-17
第 2 章 PPPoE Server配置.....	2-1
2.1 PPPoE简介	2-1
2.2 PPPoE Server配置	2-1
2.2.1 创建虚拟模板接口.....	2-1
2.2.2 启用/禁止PPPoE Server.....	2-2
2.2.3 配置PPPoE Server相关参数	2-2
2.2.4 关闭/打开PPPoE Server的PPP日志信息的显示	2-3
2.3 PPPoE Server的显示和调试	2-3
2.4 PPPoE Server配置举例	2-4
第 3 章 PPPoE Client配置	3-1
3.1 PPPoE Client简介	3-1
3.2 PPPoE Client配置	3-2
3.2.1 配置拨号接口	3-2
3.2.2 配置PPPoE会话	3-3
3.2.3 复位或删除PPPoE会话	3-4
3.3 PPPoE Client的显示和调试	3-4

3.4 PPPoE Client配置举例.....	3-5
3.4.1 PPPoE Client典型配置举例.....	3-5
3.4.2 利用ADSL Modem将局域网接入Internet.....	3-7
第 4 章 VLAN配置	4-1
4.1 VLAN简介	4-1
4.2 VLAN基本配置	4-3
4.3 VLAN显示和调试.....	4-3
4.4 VLAN典型配置举例	4-4

第1章 PPP 配置

1.1 PPP 协议简介

1.1.1 PPP 简介

PPP（Point to Point Protocol）协议是在点到点链路上承载网络层数据包的一种链路层协议，由于它能够为用户提供用户验证、易于扩充，并且支持同步通信，因而获得广泛应用。

PPP 定义了一整套的协议，包括链路控制协议（LCP）、网络层控制协议（NCP）和验证协议（PAP 和 CHAP）等。其中：

- 链路控制协议，Link Control Protocol，简称 LCP。主要用来建立、拆除和监控数据链路。
- 网络控制协议，Network Control Protocol，简称 NCP。主要用来协商在该数据链路上所传输的数据包的格式与类型。
- 用于网络安全方面的验证协议族。

(1) PAP 验证

PAP 验证为两次握手验证，口令为明文，PAP 验证的过程如下：

- 被验证方发送用户名和口令到验证方；
- 验证方根据本端用户表查看是否有此用户以及口令是否正确，然后返回不同的响应（Acknowledge or Not Acknowledge）。

(2) CHAP 验证

CHAP 验证为三次握手验证，口令为密文（密钥），CHAP 验证过程如下：

- 验证方主动发起验证请求，验证方向被验证方发送一些随机产生的报文（Challenge），并同时为本端的用户名附带上一起发送给被验证方；
- 被验证方接到验证方的验证请求后，被验证方根据此报文中验证方的用户名和本端的用户表查找用户口令字，如找到用户表中与验证方用户名相同的用户，便利用报文 ID、此用户的密钥（口令字）和 MD5 算法对该随机报文进行加密，将生成的密文和自己的用户名发回验证方（Response）；如果被验证方没有在本端用户表中找到匹配的用户名，则检查本端接口上是否配置了 **ppp chap password** 命令。如果配置了该命令，则被验证方利用报文 ID、此用户的密钥（口令字）和 MD5 算法对该随机报文进行加密，将生成的密文和自己的用户名发回验证方（Response）。

- 验证方用自己保存的被验证方口令字和 MD5 算法对原随机报文加密，比较二者的密文，根据比较结果返回不同的响应（Acknowledge or Not Acknowledge）。

PPP运行过程（参见图 1-1）如下：

- (1) 在开始建立 PPP 链路时，先进入到 Establish 阶段。

在 Establish 阶段 PPP 链路进行 LCP 协商，协商内容包括工作方式（是 SP 还是 MP）、验证方式和最大接收单元（MRU，Maximum-Receive-Unit）等。LCP 在协商成功后进入 Opened 状态，表示底层链路已经建立。

- (2) 如果配置了验证（远端验证本地或者本地验证远端）则进入 Authenticate 阶段，开始 CHAP 或 PAP 验证。
- (3) 如果验证失败进入 Terminate 阶段，拆除链路，LCP 状态转为 Down；如果验证成功就进入 Network 协商阶段（NCP），此时 LCP 状态仍为 Opened，而 IPCP 状态从 Initial 转到 Request。
- (4) NCP 协商支持 IPCP 协商，IPCP 协商主要包括双方的 IP 地址。通过 NCP 协商来选择和配置一个网络层协议。只有相应的网络层协议协商成功后，该网络层协议才可以通过这条 PPP 链路发送报文。
- (5) PPP 链路将一直保持通信，直至有明确的 LCP 或 NCP 帧关闭这条链路，或发生了某些外部事件（例如，用户的干预）。

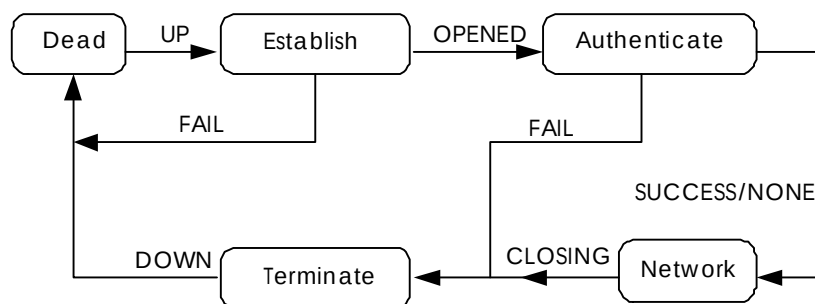


图1-1 PPP 运行流程图

有关 PPP 的详细说明，请参考 RFC1661。

1.2 PPP 配置

PPP 的基本配置包括：

- 配置接口封装的链路层协议为 PPP
- 配置轮询时间间隔
- 配置 PPP 验证方式及用户名、用户口令

PPP 的高级配置包括：

- 配置 PPP 协商参数
- 配置 PPP 链路质量监测

说明：PPP 基本配置任务，是在防火墙上运行 PPP 必须完成的配置，而高级配置任务是用户根据自己的需要进行的可选配置。

1.2.1 配置接口封装的链路层协议为 PPP

请在接口视图下进行下列配置。

命令 **link-protocol ppp** 可配置接口封装的链路层协议为 PPP。

表1-1 配置接口封装的链路层协议为 PPP

操作	命令
配置接口封装的链路层协议为 PPP	link-protocol ppp

Dialer 接口、虚拟模板接口缺省封装的链路层协议即为 PPP。

1.2.2 配置轮询时间间隔

PPP、FR、HDLC 等链路层协议都使用轮询定时器来确认链路状态是否正常。在配置轮询时间间隔时，应保证两端的设置相同。

请在接口视图下进行下列配置。

表1-2 设置轮询时间间隔

操作	命令
设置轮询时间间隔	timer hold seconds
禁止链路检测功能	undo timer hold

缺省情况下，轮询间隔为 10 秒。如果将轮询间隔设置为 0，则不进行链路有效性检测。

如果网络的延迟比较大，或拥塞程度较高，可以适当加大轮询时间间隔，以减少网络震荡的发生。

1.2.3 配置 PPP 验证方式及用户名、用户口令

本地和对端之间支持 CHAP 和 PAP 两种验证方式，以下将根据不同的验证方式分别介绍需要的配置步骤。

需要说明的是：下面的 PPP 验证命令都是在接口视图下进行的，**local-user** 命令是在系统视图下进行。本章只介绍本地认证方案，远端 AAA 认证方案请参见本手册的“安全”部分。

1. 配置本地以 PAP 方式验证对端

表1-3 配置本地以 PAP 方式验证对端

操作	命令
配置本地验证对端（方式为 PAP）（接口视图）	ppp authentication-mode pap [[call-in] domain <i>isp-name</i>]
取消配置的 PPP 验证方法，即不进行 PPP 验证（接口视图）	undo ppp authentication-mode
创建本地用户，并进入本地用户视图（系统视图）	local-user <i>username</i>
设置本地用户的密码（本地用户视图）	password { simple cipher } <i>password</i>
取消本地用户的密码（本地用户视图）	undo password
设置 PPP 用户的回呼及主叫号码属性（本地用户视图）	service-type ppp [callback-nocheck callback-number <i>callback-number</i> call-number <i>call-number</i> [:subcall-number]]
恢复 PPP 用户回呼及主叫号码属性的缺省设置（本地用户视图）	undo service-type ppp [callback-nocheck callback-number call-number]
创建一个 ISP 域，或者进入已创建 ISP 域的视图（系统视图）	domain { <i>isp-name</i> default { disable enable <i>isp-name</i> } }
配置域用户使用本地认证方案（域视图）	scheme local

PPP 缺省为不验证。

当配置 **ppp authentication-mode** { **pap** | **chap** } 后不加 **domain** 时，默认使用的 **domain** 是系统缺省的域 **system**，认证方式是本地验证，必须使用在该域中配置的地址池。如果在该命令加了 **domain**，则必须在对应的 **domain** 中配置地址池。

如果用户名中带有 **domain**，则以用户名中的 **domain** 为准（若该 **domain** 名不存在，则认证被拒绝），否则应使用为 PPP 认证配置的 **domain** 名。

2. 配置本地以 CHAP 方式验证对端

表1-4 配置本地以 CHAP 方式验证对端

操作	命令
配置本地验证对端（方式为 CHAP）（接口视图）	ppp authentication-mode chap [[call-in] domain <i>isp-name</i>]
取消配置的 PPP 验证方法，即不进行 PPP 验证（接口视图）	undo ppp authentication-mode

操作	命令
配置本地用户名称（接口视图）	ppp chap user username
删除配置的本地用户名称（接口视图）	undo ppp chap user
创建本地用户，并进入本地用户视图(系统视图)	local-user username
设置本地用户的密码（本地用户视图）	password { simple cipher } password
取消本地用户的密码（本地用户视图）	undo password
设置 PPP 用户的回呼及主叫号码属性（本地用户视图）	service-type ppp [callback-nocheck callback-number callback-number call-number call-number [:subcall-number]]
恢复 PPP 用户回呼及主叫号码属性的缺省设置（本地用户视图）	undo service-type ppp [callback-nocheck callback-number call-number]
创建一个 ISP 域，或者进入已创建 ISP 域的视图（系统视图）	domain { isp-name default { disable enable isp-name } }
配置域用户使用本地认证方案（域视图）	scheme local

PPP 缺省为不验证。对于拨号接口的验证，建议在物理接口和 Dialer 接口上都配置。因为当物理接口接收到 DCC 呼叫请求时，首先进行 PPP 协商并认证拨入用户的合法性，然后再将呼叫转交给上层协议进行处理。

3. 配置本地被对端以 PAP 方式验证

表1-5 配置本地被对端以 PAP 方式验证

操作	命令
配置本地被对端以 PAP 方式验证时本地发送的 PAP 用户名和口令（接口视图）	ppp pap local-user username password { simple cipher } password
删除以上配置的以 PAP 方式验证时发送的用户名和口令（接口视图）	undo ppp pap local-user

缺省情况下，被对端以 PAP 方式验证时，本地防火墙发送的用户名和口令均为空。

4. 配置本地被对端以 CHAP 方式验证

表1-6 配置本地被对端以 CHAP 方式验证

操作	命令
创建本地用户，并进入本地用户视图（系统视图）	local-user username
设置本地用户的密码（本地用户视图）	password { simple cipher } password
取消本地用户的密码（本地用户视图）	undo password
配置本地名称（接口视图）	ppp chap user username

操作	命令
删除配置的本地名称（接口视图）	undo ppp chap user
设置缺省的 CHAP 验证密码（当不配置本地用户和密码的时候使用该缺省密码）（接口视图）	ppp chap password { simple cipher } password
删除缺省的 CHAP 验证密码（接口视图）	undo ppp chap password

其中 **simple** 表示对 *password* 进行明文显示，**cipher** 表示对 *password* 进行加密显示。

说明：

在配置 CHAP 验证时，双方 **local-user** 命令中的 *username* 应该与对方 **ppp chap user** 的 *username* 一致，双方配置的 *password* 也应该一致。当被验证方没有通过 **local-user** 命令配置本地用户时，将对收到的所有的 PPP 用户的验证请求使用缺省的密钥（由 **ppp chap password** 命令配置）进行加密并响应。

1.2.4 配置 PPP 协商参数

可以配置的 PPP 协商参数包括：

协商超时时间间隔，在 PPP 协商过程中，如果在这个时间间隔内没有收到对端的应答报文，则 PPP 将会重发前一次发送的报文。超时时间间隔可选范围为 1 秒到 10 秒。

另外一些 NCP 的协商参数，如本地 IP 地址、分配给对方的 IP 地址等的配置请参见网络协议配置部分。例如 **ip address ppp-negotiate** 命令要求对端为本地分配 IP 地址，而 **remote address** 命令可以指定本地为对端分配 IP 地址。

1. 配置 PPP 协商超时时间间隔

请在接口视图下进行下列配置。

表1-7 配置 PPP 协商超时时间间隔

操作	命令
配置协商超时时间间隔	ppp timer negotiate seconds
恢复 PPP 协商超时时间的缺省值	undo ppp timer negotiate

缺省情况下，超时时间间隔为 3 秒。

2. 配置 PPP 协商 IP 地址

(a) 配置 Client 端

若接口封装了 PPP，本端接口还未配置 IP 地址而对端已有 IP 地址时，可为本端接口配置 IP 地址可协商属性。使本端接口接受 PPP 协商产生的由对端分配的 IP 地址。该配置主要用于在通过 ISP 访问 Internet 时，得到由 ISP 分配的 IP 地址。

请在接口视图下进行下列配置。

表1-8 设置接口 IP 地址可协商属性

操作	命令
设置接口 IP 地址可协商属性	ip address ppp-negotiate
取消接口 IP 地址可协商属性	undo ip address ppp-negotiate

缺省情况下，系统不允许接口协商 IP 地址。



注意：

- 因 PPP 支持 IP 地址的协商，所以只有当接口封装了 PPP 时，才能设置接口 IP 地址的协商，当 PPP 协议 down 时，协商产生的 IP 地址将被删除。
- 若接口原来配有地址，在配置接口 IP 地址协商后，原 IP 地址将被删除。
- 配置接口 IP 地址协商后，不需再给该接口配置 IP 地址，IP 地址由协商获得。
- 配置接口 IP 地址协商后，再次配置该接口协商，原协商产生的 IP 地址将被删除，接口再次协商获得 IP 地址。
- 在协商地址被删除后，接口将处于无地址状态。

(b) 配置 Server 端

若是防火墙作为 Server 为对端设备分配 IP 地址，有三种方法可以为 PPP 用户分配 IP 地址：

方法一：不配置地址池，在接口上直接给对方分配指定的 IP 地址。

表1-9 在接口上直接给对方分配 IP 地址

操作	命令
为 PPP 用户分配 IP 地址	remote address ip-address
取消为 PPP 用户分配 IP 地址	undo remote address

缺省情况下，若未配置 **remote address pool** 命令和域地址池，则接口不给对端分配 IP 地址。

方法二：通过使用全局地址池给对方分配地址。

首先在系统视图下定义全局地址池，然后在接口下通过 **remote address pool** 命令指定全局地址池号即可（仅能指定一个）。

表1-10 在接口上使用全局地址池给对方分配 IP 地址

操作	命令
定义全局 IP 地址池	ip pool <i>pool-number</i> <i>low-ip-address</i> [<i>high-ip-address</i>]
取消全局 IP 地址池	undo ip pool <i>pool-number</i>
使用全局地址池给 PPP 用户分配 IP 地址	remote address pool [<i>pool-number</i>]
取消为 PPP 用户分配 IP 地址	undo remote address

缺省情况下，若未配置 **remote address pool** 命令和域地址池，则接口不分配地址给对端。当配置了 **remote address pool** 命令，但没有指定 *pool-number* 时，缺省使用 0 号全局地址池。

前两种地址分配方法适用于不对 PPP 用户进行认证的情况，下面介绍的第三种分配方法适用于对 PPP 用户进行认证的情况。

方法三：通过使用域地址池给对方分配地址。

首先在域视图下定义域地址池，然后在接口下通过 **remote address pool** 命令指定域地址池号即可（仅能指定一个）；若不配置 **remote address pool** 命令，则在认证协商时依次使用相应域下的地址池给用户分配 IP 地址。

表1-11 定义 PPP 域用户的 IP 地址池

操作	命令
定义域 IP 地址池	ip pool <i>pool-number</i> <i>low-ip-address</i> [<i>high-ip-address</i>]
取消域 IP 地址池	undo ip pool <i>pool-number</i>
使用域地址池给 PPP 用户分配 IP 地址	remote address pool [<i>pool-number</i>]
取消为 PPP 用户分配 IP 地址	undo remote address

缺省情况下，若未配置 **remote address pool** 命令和域地址池，则接口不分配地址给对端。

下面总结一下 PPP 用户的 IP 地址分配原则：

- (1) 对于域的用户（包括 **userid** 和 **userid@isp-name** 两种用户）分配地址的优先级如下：
 - 如果采用 **RADIUS** 或 **TACACS** 认证和授权，并且服务器给用户下发了地址，则采用服务器下发的地址。
 - 如果服务器没有下发地址，而是下发地址池，则在域视图下相应的地址池中查找地址给用户。

- 如果上述两种方式没有分配到地址或是采用本地认证，则依次查找域视图下的地址池，并分配给用户。
- (2) 对于不认证用户，采用接口下指定的全局地址池（即在系统视图下定义的地址池）给用户分配地址。

当采用在接口下直接指定对端 IP 地址或使用地址池分配 IP 地址时，**remote address** 命令不具有地址分配的强制性，即在配置该命令后，也允许对端自行配置 IP 地址；如果不希望（或不允许）对端自行配置 IP 地址，必须接受本端分配的地址时，对端必须配置为协商 IP 地址，同时必须在 Server 端的接口视图下配置下面命令。

表1-12 配置/取消 PPP IPCP 地址分配的强制性

操作	命令
配置 PPP IPCP 不允许对端使用自行配置的固定 IP 地址	ppp ipcp remote-address forced
取消 PPP IPCP 地址分配的强制性	undo ppp ipcp remote-address forced

缺省情况下，PPP IPCP 的 IP 地址协商情况为本端不具有地址分配的强制，即防火墙本端允许对端自行配置地址。当对端明确请求本端分配地址时，本端给对端分配地址；若对端已自行配置 IP 地址时，本端不再强行给对端分配地址。

3. 配置 DNS 服务器地址协商

防火墙在进行 PPP 地址协商的过程中可以进行 DNS 地址协商，此时防火墙既可以配置为接收对端分配的 DNS 地址，也可以配置为向对方提供 DNS 地址。一般情况下，当 PC 与防火墙通过 PPP 协议相连时，防火墙应为对端设备分配 DNS 地址，这样 PC 就可以通过域名直接访问 Internet；当防火墙通过 PPP 协议连接运营商的接入服务器时，防火墙应配置为被动接收或主动请求对端分配 DNS 地址，这样防火墙就可以使用接入服务器分配的 DNS 服务器来解析域名。

请在接口视图下进行下面的配置。

表1-13 配置 DNS 服务器地址协商

操作	命令
配置防火墙可以被动地接收对端分配的 DNS 地址	ppp ipcp dns admit-any
禁止防火墙被动地接收对端分配的 DNS 地址	undo ppp ipcp dns admit-any
使能防火墙为对端分配 DNS 服务器地址	ppp ipcp dns primary-dns-address [secondary-dns-address]
禁止防火墙为对端分配 DNS 服务器地址	undo ppp ipcp dns primary-dns-address [secondary-dns-address]
配置 PPP IPCP 主动请求对端的 DNS 地址	ppp ipcp dns request

操作	命令
禁止 IPCP 请求对端的 DNS 地址	undo ppp ipcp dns request

缺省情况下，禁止 DNS 地址协商。

1.2.5 配置 PPP 链路质量监测

PPP 链路质量监测可以实时对 PPP 链路的质量进行监测。当链路的质量低于禁用链路质量百分比时，链路会被禁用；当链路质量恢复到恢复链路质量百分比时，链路会被自动重新启用。为了保证链路不会在禁用和恢复之间反复振荡，PPP 链路质量监测在重新启用链路时会有一定的时间延迟。

请在接口视图下进行下列配置。

表1-14 配置 PPP 链路质量监测

操作	命令
使能 PPP 链路质量检测功能	ppp lqc forbidden-percentage [resumptive-percentage]
禁用 PPP 链路质量检测功能	undo ppp lqc

缺省情况下，参数 *resumptive-percentage* 等于 *forbidden-percentage*。

说明：

在没有使能 PPP 链路质量检测功能之前，PPP 接口会每隔一段时间向对端发送 keepalive 报文；在使能此功能之后，PPP 接口会用 LQR 报文替换 keepalive 报文，即每隔一段时间向对端发送 LQR 报文，用以对链路情况进行监测。

当链路质量正常时，系统对每个 LQR 报文进行链路质量计算，如果连续两次链路质量计算不合格，链路会被禁用。当链路被禁用后，系统每隔十个 LQR 报文进行一次链路质量计算，只有连续三次链路质量计算均合格，链路才会被恢复。因此，当链路被禁用后，至少要在 30 个 keepalive 周期后才能恢复。如果 keepalive 周期设置过大，可能会导致链路长时间无法恢复。

1.2.6 PPP 的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示 PPP 配置后的运行情况，通过查看显示信息验证配置的效果。在用户视图下执行 **debugging** 命令可以对 PPP 进行调试。

表1-15 PPP 的显示和调试

操作	命令
显示接口的 PPP 配置和运行状态	display interface <i>interface-name</i>
打开 PPP 的部分调试开关	debugging ppp { chap { all event error packet state } pap { all event error packet state } vjcomp packet } [interface <i>interface-type</i> <i>interface-number</i>]
打开 PPP 的部分调试开关	debugging ppp compression iphc { rtp tcp } { all context_state error full_header general_info }
打开 PPP 的部分调试开关	debugging ppp { core event ip packet ipcp { all event error packet state } lcp { all event error packet state } lqc packet mp { all event error packet } } [interface <i>interface-type</i> <i>interface-number</i>]
打开 PPP 的部分调试开关	debugging ppp { all cbcp packet ccp { all event error packet state } scp packet } [interface <i>interface-type</i> <i>interface-number</i>]

1.3 配置 PPP 链路效率机制

PPP 链路上提供了四种提高传输效率的机制：IP 报文头压缩协议（IP Header Compression, IPHC），PPP 报文的 STAC-LZS 压缩、VJ TCP 头压缩和链路分片与交叉（Link Fragmentation and Interleaving, LFI），详细介绍如下。

1. IP 报文头压缩

IP 报文头压缩协议（IP Header Compression, IPHC）是一个主机-主机协议，用于在 IP 网络上承载语音、视频等实时多媒体业务。为了减少有效带宽的消耗，可以在 PPP 链路上使用 IP 报文头压缩功能，对 RTP 头（含 IP、UDP、RTP 头）或 TCP 头进行压缩。下面以 RTP 头压缩为例对压缩原理进行说明。

RTP 实际上是一种限定端口号与固定格式的 UDP 协议，包括数据部分和头部分，RTP 的数据部分相对小，而 RTP 的头部分较大。12 字节的 RTP 头，加上 20 字节的 IP 头和 8 字节的 UDP 头，就是 40 字节的 IP/UDP/RTP 头。而 RTP 典型的负载是 20 字节到 160 字节。为了避免不必要的带宽消耗，可以使用 IPHC 特性对报文头进行压缩。IPHC 将 IP/UDP/RTP 头从 40 字节压缩到 2~5 字节，对于 40 字节的负载，头压缩到 5 字节，压缩比为 $(40+40) / (40+5)$ ，约为 1.78，可见效果是相当可观的。IP 头压缩的处理过程如图所示。

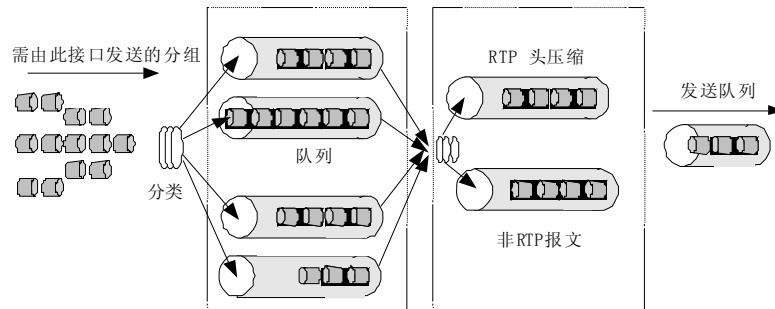


图1-2 IP 头压缩

2. STAC-LZS 压缩

STAC-LZS (STAC Lempel-Ziv standard) 压缩是一种链路层上的数据压缩标准，它由 STAC 有限公司开发并推广，仅对报文的净负荷进行压缩。STAC-LZS 压缩基于 Lempel-Ziv 算法，是用二进制编码替代一个连续的数据流，编码能够随数据的变化而变化，更加灵活，但也更加占用 CPU 资源。

3. VJ TCP 头压缩

VJ TCP 头压缩 (V. Jacobson Compressing TCP/IP Headers) 是一种应用在低速链路路上的 TCP/IP 头压缩算法，符合 RFC1144。

一个典型的 TCP/IP 报文头的长度是 40 字节，其中 IP 头 20 字节，TCP 头 20 字节，在 TCP 建立连接后，在每个连接上传输的大量的 TCP/IP 报文都会包含这些信息。通过分析发现这些报文头中有些字段的信息是固定不变的，只发送一次即可；有些字段虽然有变化，但变化的规律和范围很明确，故字段的长度可以压缩。通过 VJ TCP/IP 头压缩后，TCP/IP 头长度可以从 40 字节降至 3~5 字节，应用在 PPP 等低速串行链路上可以明显提高如 FTP 等应用的报文传输速度。

1.3.1 配置 IP 报文头压缩

配置 IP 报文头压缩包括下面步骤：

- 启动和关闭 IP 头压缩
- 配置 TCP 头压缩的最大连接数（可选）
- 配置 RTP 头压缩的最大连接数（可选）

1. 启动和关闭 IP 头压缩

使用该命令可以启动某接口上的 IP 头压缩功能。当启动 IP 头压缩时，建立 RTP 会话的 TCP 报文的头压缩也将被启动；当禁止 IP 头压缩时，建立 RTP 会话的 TCP 报文的头压缩也将被禁止。

用户必须在链路的两端同时配置 IP 头压缩命令。

请在接口视图下进行如下配置。

表1-16 启动和关闭 IP 头压缩

操作	命令
启动 IP 头压缩	ppp compression iphc [nonstandard]
关闭 IP 头压缩	undo ppp compression iphc

2. 配置 TCP 头压缩的最大连接数

使用该命令配置 TCP 头压缩的最大连接数。

请在接口视图下进行下列配置。

表1-17 配置 TCP 头压缩的最大连接数

操作	命令
配置 TCP 头压缩的最大连接数	ppp compression iphc tcp-connections <i>number</i>
恢复 TCP 头压缩的最大连接数的缺省值	undo ppp compression iphc tcp-connections

参数 *number* 指该接口上 TCP 头压缩的最大连接数。缺省方式下 *number* 值为 16。

3. 配置 RTP 头压缩的最大连接数

使用该命令配置 RTP 头压缩的最大连接数。

请在接口视图下进行下列配置。

表1-18 配置 RTP 头压缩的最大连接数

操作	命令
配置 RTP 头压缩的最大连接数	ppp compression iphc rtp-connections <i>number</i>
恢复 RTP 头压缩的最大连接数的缺省值	undo ppp compression iphc rtp-connections

参数 *number* 指该接口上 IPHC 功能的 RTP 头压缩的最大连接数，取值范围为 3～1000，缺省方式下 *number* 值为 16。

1.3.2 配置 PPP 报文 STAC-LZS 压缩

请在接口视图下进行下列配置。

目前的系统版本支持 Stac 压缩方法（RFC1974）。

表1-19 配置 PPP 的 STAC-LZS 压缩

操作	命令
配置接口允许 Stac 压缩	ppp compression stac-lzs
取消接口使用 Stac 压缩	undo ppp compression stac-lzs

缺省情况下，禁止使用压缩。

1.3.3 配置 PPP 报文 VJ TCP 头压缩

请在接口配置模式下进行下列配置。

表1-20 配置 VJ TCP 头压缩

操作	命令
在 PPP 接口上允许进行 VJ TCP 头压缩	ip tcp vjcompress
在 PPP 接口上禁止进行 VJ TCP 头压缩	undo ip tcp vjcompress

缺省情况下，PPP 接口上禁止进行 VJ TCP 头压缩。

1.3.4 PPP 链路效率机制的显示与调试

表1-21 PPP 链路效率机制的显示与调试

操作	命令
显示 TCP 头压缩的统计信息	display ppp compression iphc tcp [<i>interface-type</i> <i>interface-number</i>]
显示 RTP 头压缩的统计信息	display ppp compression iphc rtp [<i>interface-type</i> <i>interface-number</i>]
显示 stac-lzs 压缩统计信息	display ppp compression stac-lzs [<i>interface-type</i> <i>interface-number</i>]
打开 RTP 头压缩的调试开关	debugging ppp compression iphc rtp { all context_state error full_header general_info }
打开 TCP 头压缩的调试开关	debugging ppp compression iphc tcp { all context_state error full_header general_info }
清空 IP 头压缩的统计信息	reset ppp compression iphc [<i>interface-type</i> <i>interface-number</i>]
清除 Stac-lzs 压缩的统计信息	reset ppp compression stac-lzs [<i>interface-type</i> <i>interface-number</i>]

1.4 PPP 典型配置举例

1.4.1 PAP 验证举例

1. 配置需求

如图 1-3 所示, SecPath1 和 SecPath2 之间用接口 Ethernet1/0/0 互连, 要求 SecPath1 用 PAP 方式验证 SecPath2。

2. 组网图

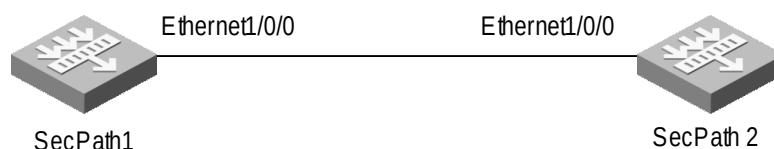


图1-3 PAP、CHAP 验证示例组网图

3. 配置步骤

(1) 配置 SecPath1

增加一个 PPPoE 用户。

```
[H3C] local-user SecPath2
[H3C-luser-SecPath2] password simple pwd
[H3C-luser-SecPath2] service-type ppp

# 配置虚拟模板参数。

[H3C] interface virtual-template 1
[H3C-Virtual-Template1] ppp authentication-mode pap
[H3C-Virtual-Template1] ip address 1.1.1.1 255.0.0.0
[H3C-Virtual-Template1] remote address 1.1.1.2
```

配置 PPPoE 参数。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] pppoe-server bind virtual-template 1
```

(2) 配置 SecPath2

```
[H3C] dialer-rule 1 ip permit
[H3C] interface dialer 1
[H3C-Dialer1] dialer user secpath1
[H3C-Dialer1] dialer-group 1
[H3C-Dialer1] dialer bundle 1
[H3C-Dialer1] ip address ppp-negotiate
[H3C-Dialer1] ppp pap local-user SecPath2 password simple pwd
```

配置 PPPoE 会话。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] pppoe-client dial-bundle-number 1
```

1.4.2 CHAP 验证举例

1. 配置需求

在图 1-2 中，要求 SecPath1 用 CHAP 方式验证 SecPath2。

2. 组网图

见图 1-3

3. 配置步骤

(1) 配置 SecPath1

增加一个 PPPoE 用户。

```
[H3C] local-user SecPath2
[H3C-luser-SecPath2] password simple pwd
[H3C-luser-SecPath2] service-type ppp
```

在 SecPath1 上配置虚拟模板参数。

```
[H3C] interface virtual-template 1
[H3C-Virtual-Template1] ppp authentication-mode chap
[H3C-Virtual-Template1] ppp chap user secpath1
[H3C-Virtual-Template1] ip address 1.1.1.1 255.0.0.0
[H3C-Virtual-Template1] remote address 1.1.1.2
```

在 SecPath1 上配置 PPPoE 参数。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] pppoe-server bind virtual-template 1
```

(2) 配置 SecPath2

```
[H3C] dialer-rule 1 ip permit
[H3C] interface dialer 1
[H3C-Dialer1] dialer user secpath1
[H3C-Dialer1] dialer-group 1
[H3C-Dialer1] dialer bundle 1
[H3C-Dialer1] ip address ppp-negotiate
[H3C-Dialer1] ppp chap user SecPath2
[H3C] local-user SecPath1
[H3C-luser-SecPath1] password simple pwd
```

配置 PPPoE 会话

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] pppoe-client dial-bundle-number 1
```

1.5 PPP 故障诊断与排错

故障之一：链路始终不能转为 Up 状态。

故障排除：可能是由于 PPP 验证参数配置不正确，导致 PPP 验证失败。

打开 PPP 的调试开关，会看到 LCP 协商成功并转为 Up 状态后进行 PAP 或 CHAP 协商，然后 LCP 转为 Down 状态。

故障之二：物理链路不能转为 Up 状态。

故障排除：可以执行 **display interface type number** 命令来查看接口当前状态。

第2章 PPPoE Server 配置

2.1 PPPoE 简介

PPPoE 是 Point-to-Point Protocol over Ethernet 的简称，它利用以太网将大量主机组成网络，通过一个远端接入设备连入因特网，并对接入的每个主机实现控制、计费功能，极高的性能价格比使 PPPoE 在包括小区组网建设等一系列应用中被广泛采用。

PPPoE 有两个明显的阶段：Discovery 阶段和 PPP Session 阶段，具体如下：

当一个主机想开始 PPPoE 进程的时候，它必须先识别接入端的以太网 MAC 地址，建立 PPPoE 的 SESSION ID。这就是 Discovery 阶段的目的。

当 PPPoE 进入 Session 阶段后，PPP 报文就可以作为 PPPoE 帧的净荷封装在以太网帧发到对端，SESSION ID 必须是 Discovery 阶段确定的 ID，MAC 地址必须是对端的 MAC 地址，PPP 报文从 Protocol ID 开始。在 Session 阶段，主机或服务器任何一方都可发 PADT 报文通知对方结束本 Session。

关于 PPPoE 的详细介绍，可以参考 RFC2516。

2.2 PPPoE Server 配置

PPPoE Server 配置包括：

PPPoE Server 的基本配置：

- 创建虚拟模板接口并配置相关参数
- 启用/禁止 PPPoE Server

PPPoE Server 的高级配置：

- 配置 PPPoE Server 相关参数

2.2.1 创建虚拟模板接口

1. 创建虚拟模板接口

请在系统视图下进行下列配置。

表2-1 创建和删除虚拟模板接口

操作	命令
创建虚拟模板接口并进入虚拟接口模板视图	interface virtual-template <i>number</i>
删除虚拟模板接口	undo interface virtual-template <i>number</i>

2. 设置虚拟模板接口的工作参数

虚拟模板接口与一般的物理接口相比，链路层协议只支持 PPP，网络协议支持 IP 和 IPX，因此，可以设置如下工作参数：

- 设置 PPP 的工作参数
- 设置虚拟模板接口的 IP 地址
- 设置为 PPP 对端分配的 IP 地址（或 IP 地址池）

2.2.2 启用/禁止 PPPoE Server

请在接口视图下进行下列配置。

下表命令是针对以太网接口的，并且只对相应的以太网接口有效。即：在一个以太网接口上启用 PPPoE 协议，其它的以太网接口并不随之启用 PPPoE 协议；而在一个以太网接口上禁止 PPPoE 协议，并不表示其它的以太网接口也随之禁止 PPPoE 协议。

表2-2 启用/禁止 PPPoE 协议

操作	命令
在以太网接口上启用 PPPoE 协议	pppoe-server bind virtual-template <i>number</i>
在以太网接口上禁止 PPPoE 协议	undo pppoe-server bind

其中，*number* 为虚拟模板接口（virtual-template）的编号。

缺省情况下，禁止 PPPoE 协议。

2.2.3 配置 PPPoE Server 相关参数

PPPoE Server 系列参数可以根据需要进行配置，一般情况下使用缺省值即可。

请在系统视图下进行下列配置。

表2-3 配置 PPPoE Server 相关参数

操作	命令
配置一个对端 MAC 地址上能创建的最大 PPPoE session 数目	pppoe-server max-sessions remote-mac number
恢复一个对端 MAC 地址上能创建的最大 PPPoE session 数目为缺省值	undo pppoe-server max-sessions remote-mac
配置一个本端 MAC 地址上能创建的最大 PPPoE session 数目	pppoe-server max-sessions local-mac number
恢复一个本端 MAC 地址上能创建的最大 PPPoE session 数目为缺省值	undo pppoe-server max-sessions local-mac
配置本系统能创建的最大 PPPoE session 数目	pppoe-server max-sessions total number
将系统能创建的最大 PPPoE session 数目恢复为缺省值	undo pppoe-server max-sessions total

2.2.4 关闭/打开 PPPoE Server 的 PPP 日志信息的显示

当终端显示的日志信息太多时，一方面会影响设备的性能，另一方面也会给用户进行配置带来不便。因此，可以在 PPPoE Server 端关闭日志信息的显示开关。

请在系统视图下进行下列配置。

表2-4 关闭/打开 PPPoE Server 的 PPP 日志信息的显示

操作	命令
关闭 PPPoE Server 的 PPP 日志信息的显示	pppoe-server log-information off
打开 PPPoE Server 的 PPP 日志信息的显示	undo pppoe-server log-information off

缺省情况下，终端显示 PPPoE Server 的 PPP 日志信息。

2.3 PPPoE Server 的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示 PPPoE 配置后的运行情况，通过查看显示信息验证配置的效果。

表2-5 PPPoE 显示和调试

操作	命令
监控 PPPoE session 的状态和统计数据	display pppoe-server session { all packet }

其中，**all** 参数表示显示各 **session** 的所有信息，**packet** 参数表示显示各 **session** 的报文统计信息。

2.4 PPPoE Server 配置举例

1. 配置需求

如图 2-1所示的主机Host使用PPPoE协议，通过防火墙接入到Internet。

2. 组网图

防火墙通过 Ethernet 1/0/0 接口连接以太网，Ethernet 3/0/0 接口连接 Internet。

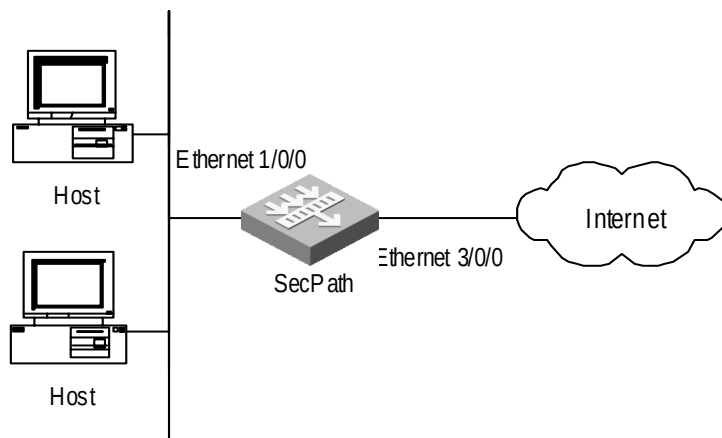


图2-1 PPPoE 示例组网图

3. 配置步骤

增加一个 PPPoE 用户。

```
[H3C] local-user NE
[H3C-luser-NE] password simple pwd
[H3C-luser-NE] service-type ppp
```

在防火墙上配置 PPPoE 参数。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] pppoe-server bind virtual-template 1
```

在防火墙上配置虚拟模板参数。

```
[H3C] interface virtual-template 1
[H3C-Virtual-Template1] ppp authentication-mode chap domain system
[H3C-Virtual-Template1] ppp chap user NE
[H3C-Virtual-Template1] remote address pool 1
[H3C-Virtual-Template1] ip address 1.1.1.1 255.0.0.0
```

配置域用户使用本地认证方案。

```
[H3C] domain system
[H3C-isp-system] scheme local
```

增加一个本地 IP 地址池（9 个 IP 地址）

```
[H3C-isp-system] ip pool 1 1.1.1.2 1.1.1.10
```

这样，以太网上各主机安装 PPPoE 客户端软件后，配置好用户名和密码就能使用 PPPoE 协议，通过防火墙接入到 Internet。

若认证方案配置为 **radius-scheme** 或 **hwtacacs-scheme**，那么还可以配置 RADIUS/HWTACAS 参数，使系统可以进行计费，具体配置步骤请参见本手册的“安全”部分。

第3章 PPPoE Client 配置

3.1 PPPoE Client 简介

1. PPPoE 介绍

PPPoE 是 Point-to-Point Protocol over Ethernet 的简称，可以使以太网的主机通过一个简单的桥接设备连到一个远端的接入集中器上。通过 PPPoE 协议，远端接入设备能够实现对每个接入用户的控制和计费。与传统的接入方式相比，PPPoE 具有较高的性能价格比，它在包括小区组网建设等一系列应用中被广泛采用，目前流行的宽带接入方式 ADSL 就使用了 PPPoE 协议。

PPPoE 协议采用 Client / Server 方式，它将 PPP 报文封装在以太网帧之内，在以太网上提供点对点的连接。

PPPoE 有两个不同的阶段：Discovery 阶段和 PPP Session 阶段。

- Discovery 阶段

当一个主机发起一个 PPP 会话的时候，它必须首先通过 Discovery 阶段去确认对端的以太网 MAC 地址并建立一个 PPPoE 的会话标识(Session ID)。与 PPP 协议不同的是，PPPoE 的 Discovery 阶段建立的是一种 Client/Server 关系，而 PPP 建立的是一种对等关系。通过 Discovery 阶段，一个主机（Client）可以发现一个接入集中器（Server），在 Discovery 阶段正常结束后，主机和接入集中器就可以通过 MAC 地址和会话标识来建立 PPPoE 会话。

- PPP Session 阶段

在 PPP Session 阶段开始后，主机和接入集中器之间就依据 PPP 协议传送 PPP 数据，进行 PPP 的各项协商和数据传输。PPP 报文作为 PPPoE 帧的净荷被封装在以太网帧内，发送到 PPPoE 链路的对端，此时所有的以太网帧都是单播的。

关于 PPPoE 协议的详细介绍，可以参考 RFC2516。

2. PPPoE Client 介绍

PPPoE 在 ADSL 宽带接入中被广泛使用。通常情况下，一台主机如果要通过 ADSL 接入 Internet，必须在主机上安装 PPPoE 客户端拨号软件。SecPath 系列防火墙实现了 PPPoE Client 功能（即 PPPoE 的客户端拨号功能），用户可以不用在 PC 上安装 PPPoE 客户端软件即可接入 Internet，而且同一个局域网中的所有 PC 可以共享一个 ADSL 帐号。

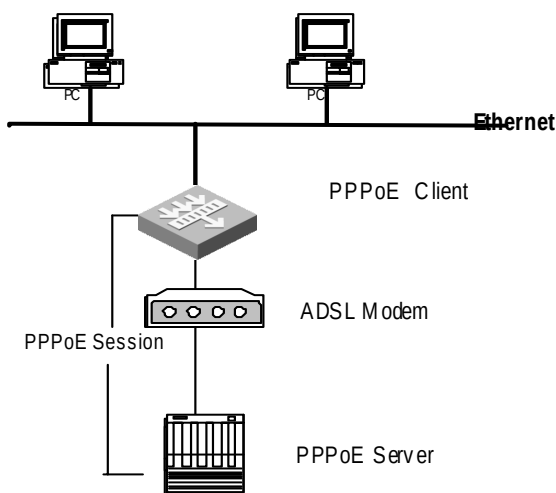


图3-1 PPPoE 典型组网图

从上图可以看到：以太网内的计算机连接到防火墙上，在防火墙上运行 **PPPoE Client**。上网的数据首先到达防火墙，再通过 **PPPoE** 协议对数据进行封装，经由防火墙挂接的 **ADSL Modem** 到达 **ADSL** 接入服务器，最终进入 **Internet**。整个上网过程，不需要用户另外在计算机上安装 **PPPoE** 客户端拨号软件就可以实现。

3.2 PPPoE Client 配置

PPPoE Client 的基本配置包括：

- 配置拨号接口
- 配置 PPPoE 会话

PPPoE Client 的高级配置包括：

- 中止 PPPoE 会话

3.2.1 配置拨号接口

在配置 **PPPoE** 会话之前，需要先配置一个 **Dialer** 接口，并在接口上配置 **dialer bundle**。每个 **PPPoE** 会话唯一对应一个 **dialer bundle**，而每个 **dialer bundle** 又唯一对应一个 **Dialer** 接口。这样就相当于通过一个 **Dialer** 接口可以创建一个 **PPPoE** 会话。

请在系统视图下使用 **dialer-rule** 和 **interface dialer** 命令，在 **Dialer** 接口视图下使用其他命令。

表3-1 配置拨号接口

操作	命令
配置 Dialer Rule	dialer-rule <i>dialer-group</i> { <i>protocol-name</i> { permit deny } acl <i>acl-number</i> }
创建一个 Dialer 接口	interface dialer <i>number</i>
使能共享 DCC，设定远程用户名	dialer user <i>username</i>
配置接口 IP 地址	ip address { <i>address mask</i> ppp-negotiate }
配置接口的 Dialer Bundle	dialer bundle <i>bundle-number</i>
配置接口的 Dialer Group	dialer-group <i>group-number</i>

PPPoE 只支持共享 DCC。根据需要，可能还要在 Dialer 接口上配置 PPP 验证等相关参数，关于拨号接口配置的详细介绍，可以参考《Comware V3 操作手册 拨号》中 DCC 配置部分的相关内容，此处不再赘述。

3.2.2 配置 PPPoE 会话

PPPoE 会话可以配置在物理以太网接口上，也可以配置在虚拟以太网接口上。当防火墙通过以太网接口连接 ADSL Modem 再连入 Internet 的时候，需要在以太网接口配置 PPPoE 会话。

请在系统视图下配置虚拟以太网接口，在 PVC 视图下配置 PPPoEoA 映射。

表3-2 配置虚拟以太网接口

操作	命令
创建虚拟以太网接口	interface virtual-ethernet <i>number</i>
删除虚拟以太网接口	undo interface virtual-ethernet <i>number</i>

请在以太网接口视图或虚拟以太网视图下进行下列配置，将 Dialer 口绑定到以太网口或虚拟以太网口。

表3-3 配置 PPPoE 会话

操作	命令
配置 PPPoE 会话（永久在线方式）	pppoe-client dial-bundle-number <i>number</i> [no-hostuniq]
配置 PPPoE 会话（报文触发方式）	pppoe-client dial-bundle-number <i>number</i> [no-hostuniq] idle-timeout <i>seconds</i> [queue-length <i>packets</i>]
删除 PPPoE 会话	undo pppoe-client dial-bundle-number <i>number</i>

防火墙支持两种 PPPoE 连接方式：永久在线方式和报文触发方式。

- 永久在线方式是指：当物理线路 UP 后，防火墙会立即发起 PPPoE 呼叫，建立 PPPoE 会话。除非用户使用命令 **undo pppoe-client** 命令删除 PPPoE 会话，否则此 PPPoE 会话将一直存在。
- 报文触发方式是指：当物理线路 UP 后，防火墙不会立即发起 PPPoE 呼叫，只有当有数据需要传送时，防火墙才会发起 PPPoE 呼叫，建立 PPPoE 会话。如果 PPPoE 链路的空闲时间超过用户的配置，防火墙会自动中止 PPPoE 会话。

3.2.3 复位或删除 PPPoE 会话

请在用户视图下使用 **reset pppoe-client** 和 **reset pppoe-server** 命令，请在以太网接口视图或者虚拟以太网接口视图下使用 **undo pppoe-client** 命令。

表3-4 复位或删除 PPPoE 会话

操作	命令
中止 PPPoE Client 端的会话，稍后再重新建立此会话	reset pppoe-client { all dial-bundle-number number }
中止 PPPoE Server 端的会话	reset pppoe-server { all virtual-template number interface interface-type interface-num }
中止 PPPoE Client 端的会话，此会话不会再被重新建立	undo pppoe-client dial-bundle-number number

reset pppoe-client 命令与 **undo pppoe-client** 命令的不同点在于：**reset pppoe-client** 命令仅仅是临时中止 PPPoE 会话，而 **undo pppoe-client** 命令则是永久删除 PPPoE 会话。

当 PPPoE 会话工作在永久在线方式时，如果使用 **reset pppoe-client** 命令中止 PPPoE 会话，防火墙会在 16 秒后自动重新建立 PPPoE 会话。当 PPPoE 会话工作在报文触发方式时，如果使用 **reset pppoe-client** 命令中止 PPPoE 会话，防火墙会在有数据需要传送时，才重新建立 PPPoE 会话。

无论 PPPoE 会话工作在永久在线方式或报文触发方式，使用 **undo pppoe-client** 命令都会永久删除 PPPoE 会话。如果需要重新建立 PPPoE 会话，用户需要重新配置。

3.3 PPPoE Client 的显示和调试

请在所有视图下使用 **display** 命令，在用户视图下使用 **debugging** 命令。

表3-5 PPPoE Client 的显示和调试

操作	命令
显示 PPPoE 会话的状态和统计信息	display pppoe-client session { summary packet } [dial-bundle-number number]
打开 PPPoE Client 的调试开关	debugging pppoe-client { all data error event packet verbose } [interface type number]

3.4 PPPoE Client 配置举例

3.4.1 PPPoE Client 典型配置举例

1. 组网需求

SecPath1 和 SecPath2 之间用接口 Ethernet1/0/0 互连，要求 SecPath1 用 PAP/CHAP 方式验证 SecPath2。

2. 组网图

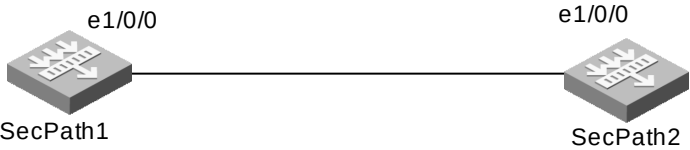


图3-2 PPPoE Client 典型配置举例

3. 配置步骤

方案一：PAP 认证

(1) 配置 SecPath1

增加一个 PPPoE 用户。

```
[H3C] local-user SecPath2
[H3C-luser-SecPath2] password simple pwd
[H3C-luser-SecPath2] service-type ppp
```

配置虚拟模板参数。

```
[H3C] interface virtual-template 1
[H3C-Virtual-Template1] ppp authentication-mode pap
[H3C-Virtual-Template1] ip address 1.1.1.1 255.0.0.0
[H3C-Virtual-Template1] remote address 1.1.1.2
```

配置 PPPoE Server。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] pppoe-server bind virtual-template 1
```

(2) 配置 SecPath2

```
[H3C] dialer-rule 1 ip permit
[H3C] interface dialer 1
[H3C-Dialer1] dialer user secpath1
[H3C-Dialer1] dialer-group 1
[H3C-Dialer1] dialer bundle 1
[H3C-Dialer1] ip address ppp-negotiate
[H3C-Dialer1] ppp pap local-user SecPath2 password simple pwd
# 配置 PPPoE 会话。
```

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] pppoe-client dial-bundle-number 1
```

方案二：CHAP 认证

(1) 配置 SecPath1

增加一个 PPPoE 用户。

```
[H3C] local-user SecPath2
[H3C-luser-SecPath2] password simple pwd
[H3C-luser-SecPath2] service-type ppp
```

配置虚拟模板参数。

```
[H3C] interface virtual-template 1
[H3C-Virtual-Template1] ppp authentication-mode chap
[H3C-Virtual-Template1] ppp chap user secpath1
[H3C-Virtual-Template1] ip address 1.1.1.1 255.0.0.0
[H3C-Virtual-Template1] remote address 1.1.1.2
```

配置 PPPoE Server。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] pppoe-server bind virtual-template 1
```

(2) 配置 SecPath2

```
[H3C] dialer-rule 1 ip permit
[H3C] interface dialer 1
[H3C-Dialer1] dialer user secpath1
[H3C-Dialer1] dialer-group 1
[H3C-Dialer1] dialer bundle 1
[H3C-Dialer1] ip address ppp-negotiate
[H3C-Dialer1] ppp chap user SecPath2
[H3C-Dialer1] ppp chap password simple pwd
[H3C-Dialer1] quit
[H3C] local-user SecPath1
[H3C-luser-SecPath1] password simple pwd
# 配置 PPPoE 会话。
```

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] pppoe-client dial-bundle-number 1
```

3.4.2 利用 ADSL Modem 将局域网接入 Internet

1. 组网需求

局域网内的计算机通过 SecPathA 访问 Internet，SecPathA 通过 ADSL Modem 采用永久在线的方式接入 DSLAM。ADSL 帐户的用户名为 adsluser，密码为 123456。SecPathB 作为 PPPoE Server 通过 Eth2/0/0 接口连接至 DSLAM，提供 RADIUS 认证、计费功能。在 SecPathA 上使能 PPPoE Client 功能，局域网内的主机不用安装 PPPoE 客户端软件即可访问 Internet。

2. 组网图

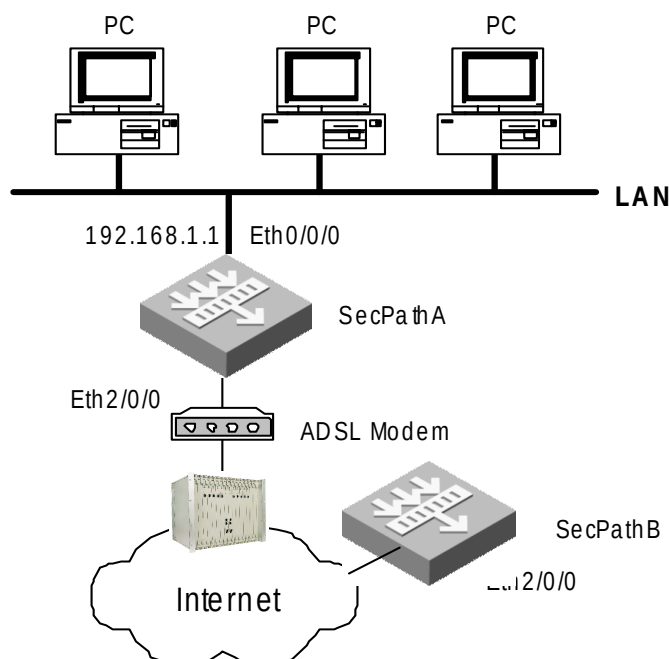


图3-3 利用 ADSL 将局域网接入 Internet

3. 配置步骤

(1) 配置 SecPathA

配置 Dialer 接口。

```
[H3C] dialer-rule 1 ip permit
[H3C] interface dialer 1
[H3C-Dialer1] dialer user secpathb
[H3C-Dialer1] dialer-group 1
[H3C-Dialer1] dialer bundle 1
[H3C-Dialer1] ip address ppp-negotiate
```

```
[H3C-Dialer1] ppp pap local-user adsluser password cipher 123456
```

配置 PPPoE 会话。

```
[H3C] interface ethernet 2/0/0
```

```
[H3C-Ethernet2/0/0] pppoe-client dial-bundle-number 1
```

配置局域网接口及缺省路由。

```
[H3C] interface ethernet 0/0/0
```

```
[H3C-Ethernet0/0/0] ip address 192.168.1.1 255.255.255.0
```

```
[H3C-Ethernet0/0/0] quit
```

```
[H3C] ip route-static 0.0.0.0 0 dialer 1
```

如果局域网内计算机使用的 IP 地址为私有地址，就还需要在防火墙上配置 NAT（Network Address Translation，网络地址转换）。关于 NAT 的配置在这里不再列出，请参阅本手册的“安全”部分中的 NAT 配置部分。

(2) 配置 SecPathB

增加一个 PPPoE 用户。

```
[H3C] local-user adsluser
```

```
[H3C-luser-adsluser] password simple 123456
```

```
[H3C-luser-adsluser] service-type ppp
```

在 SecPathB 上配置虚拟模板参数：

```
[H3C] interface virtual-template 1
```

```
[H3C-Virtual-Template1] ppp authentication-mode pap
```

```
[H3C-Virtual-Template1] ip address 1.1.1.1 255.0.0.0
```

```
[H3C-Virtual-Template1] remote address pool 1
```

在 SecPathB 上配置 PPPoE 参数：

```
[H3C] interface ethernet 2/0/0
```

```
[H3C-Ethernet2/0/0] pppoe-server bind virtual-template 1
```

配置域用户使用本地认证方案。

```
[H3C] domain system
```

```
[H3C-isp-domain] scheme radius-scheme cams
```

增加一个本地 IP 地址池（9 个 IP 地址）。

```
[H3C] ip pool 1 1.1.1.2 1.1.1.10
```

配置 RADIUS 方案。

```
[H3C] radius scheme cams
```

```
[H3C-radius-cams] primary authentication 10.110.91.146 1812
```

```
[H3C-radius-cams] primary accounting 10.110.91.146 1813
```

```
[H3C-radius-cams] key authentication expert
```

```
[H3C-radius-cams] key accounting expert
```

```
[H3C-radius-cams] server-type extended
```

```
[H3C-radius-cams] user-name-format with-domain
```

```
[H3C-radius-cams] quit
```

RADIUS Server 的具体配置，请参见 RADIUS Server 软件的相关资料。

第4章 VLAN 配置

4.1 VLAN 简介

以太网是一种基于 CSMA/CD（Carrier Sense Multiple Access/Collision Detect：载波侦听多路访问/冲突检测）的共享通讯介质的数据网络通讯技术，共享介质上的各节点轮流使用介质传送帧，同一时刻只能有一个主机发，其他主机只能收。

当多个主机通过双绞线连接到集线器（HUB，星型结构），或者通过同轴电缆串连（总线型结构）时，所有互联在共享物理介质上的主机形成一个物理上的冲突域（Collision Domain），一般看作一个局域网的网段（LAN segmentation）。根据上面说明的以太网的基本原理，可以看出用 HUB 作 LAN 互联的问题是：当主机数目较多时将导致冲突严重、广播泛滥、性能显著下降甚至使网络不可用。

解决上述问题的办法是使用透明网桥（Transparent Bridge）或者交换机（LAN Switch）作 LAN 互联。交换机通过接收到的数据帧的源 MAC 地址建立起 MAC-PORT 映射表，对于收到的数据帧，如果能够在表中查到目的 MAC 地址，则把帧只向对应的端口发送；如果找不到，就向除接收端口外的所有端口转发。这样，冲突域被交换机隔离在各自的端口，而不会扩展到其他端口。交换机并不改变以太帧的源地址和目的地址，而只是转发到适当的网段（LAN segmentation），是一种透明设备。交换机一般使用专用的 ASIC 芯片来实现桥接交换。交换机虽然解决了使用 HUB 带来冲突（Collision）严重的问题，但仍然不能隔离广播，实际上，所有用交换机互联起来的主机（可能包括多个交换机）是在一个广播域（Broadcast Domain），对于目的 MAC 地址为全 F（0xffffffff）的广播报文，比如 ARP 请求报文，交换机会向所有的端口转发，在主机较多的情况下，会造成广播风暴，导致整个网络的性能下降。

为了解决用交换机做 LAN 互联无法限制广播的问题，出现了 VLAN（Virtual Local Area Network）技术。把一个 LAN 划分成多个逻辑的“LAN”—VLAN，每个 VLAN 是一个广播域，VLAN 内的主机间通信就和在一个 LAN 内一样，而 VLAN 间则不能直接互通，这样，广播报文被限制在一个 VLAN 内，如图所示：

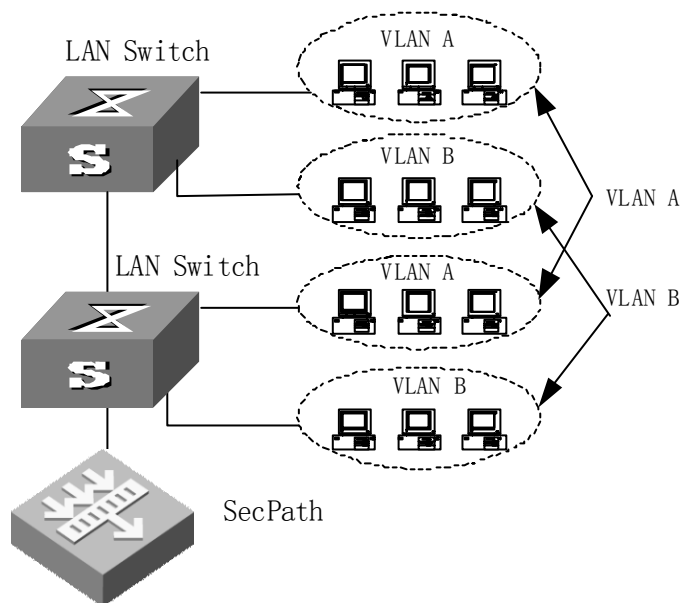


图4-1 一个 VLAN 的例子

VLAN 的组成不受物理位置的限制，一个 VLAN 可以在一个交换机内，也可以跨越交换机，甚至可以跨越路由器。

VLAN 的划分方法有很多，可以基于端口、基于 MAC 地址、基于协议类型、基于 IP 地址映射、基于组播、基于策略等，目前通用的划分方法是基于端口的 VLAN，本手册中的 VLAN，如果没有特别说明，都是指基于端口的 VLAN。

使用 VLAN 具有如下好处：

- 限制广播报文(广播风暴),节省带宽,提高了网络处理能力。**Broadcast Domain** 限制在一个 VLAN 内,交换机不会从一个 VLAN 向另外一个 VLAN 直接发送帧,除非它是一个三层交换机。
- 增强 LAN 的安全性。VLAN 间不能直接通信,即一个 VLAN 内的用户和其它 VLAN 内的用户不能直接互访,如果要访问需要通过路由器或三层交换机等三层设备。
- 虚拟工作组。用 VLAN 可以划分不同的用户到不同的工作组,当用户工作组改变时,不需要改变物理位置。在实际使用中,一般都是同一工作组的用户在一起协作,异地的情况比较少。

在交换机上,一般的端口只能属于一个 VLAN,只能识别和发送本 VLAN 的报文,但当 VLAN 跨越交换机时,就需要交换机间的端口(链路)能够同时识别和发送多个 VLAN 的报文,同样的问题也存在于支持 VLAN 的交换机和路由器之间,这样的链路称为 **Trunk**,其意义有二:一是“中继”,把 VLAN 报文透明传输到互联的交换机或路由器,使 VLAN 得到扩展;二是“干线”,一条链路上可以传输多个 VLAN 的数据。

实现 Trunk 的协议常见的有 IEEE802.1Q（简称 dot1q），是 IEEE 的标准协议，它在原以太报文的源地址字段后增加一个 4 字节的 VLAN TAG，达到识别 VLAN 的目的。

VLAN 之间是不能直接互通的，为了实现 VLAN 之间的互通，必须使用路由器连接各个 VLAN，连接的路由器必须支持 VLAN。一般这种互通是三层（IP 层）的互通。

SecPath 系列防火墙支持 VLAN。

4.2 VLAN 基本配置

请在系统视图或者以太网子接口视图下进行下列配置。

表4-1 VLAN 基本配置

操作	命令
创建并进入以太网子接口（系统视图下）	interface <i>subinterface-type interface-number</i>
设置以太网子接口的 IP 地址（接口视图下）	ip address <i>ip-address ip-mask</i>
设置以太网子接口或千兆以太网子接口的封装类型以及相关联的 VLAN ID（接口视图下）	vlan-type dot1q vid <i>vid</i>
设置某个 VLAN 的每秒的最大处理报文数目（系统视图下）	max-packet-process count <i>vid</i>
将某个 VLAN 的每秒的最大处理报文数目恢复为缺省配置（系统视图下）	undo max-packet-process <i>vid</i>

缺省情况下，系统子接口上无封装，也没有与子接口关联的 VLAN ID，没有最大处理报文数目的限制。

4.3 VLAN 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示 VLAN 配置后的运行情况，通过查看显示信息验证配置的效果。

执行 **reset** 命令可以清除该运行情况的统计信息。

表4-2 VLAN 显示和调试

操作	命令
显示指定 VLAN 配置的最大处理报文数目	display vlan max-packet-process <i>vid</i>
显示指定 VLAN 的报文统计信息，包括接收和发送的报文数目	display vlan statistics <i>vid vid</i>

操作	命令
显示某个接口的 VLAN 配置信息	display vlan interface <i>interface-type</i> <i>interface-num</i>
清除指定 VLAN 的报文统计信息	reset vlan statistics vid <i>vid</i>

4.4 VLAN 典型配置举例

1. 组网需求

这是一个三层转发（子接口）模式配置举例。如下图所示，交换机 1 和交换机 2 上指定了端口的 VLAN 属性，则与交换机相连的工作站 A、B、C、D 也就分别属于 VLAN10 或 VLAN20，要求：

- 防火墙子接口 Ethernet3/0/0.1、Ethernet3/0/0.2 和 Ethernet4/0/0.1、Ethernet4/0/0.2 的地址分别为 1.0.0.1、2.0.0.1、3.0.0.1 和 4.0.0.1；
- 工作站 A 和 B 之间、C 和 D 之间能够互相通信，即同一交换机、不同 VLAN 之间能够互相通信；
- 工作站 A 和 C 之间、B 和 D 之间能够互相通信，即不同交换机、同一 VLAN 之间能够互相通信；
- 工作站 A 和 D 之间、B 和 C 之间能够互相通信，即不同交换机、不同 VLAN 之间能够互相通信。

2. 组网图

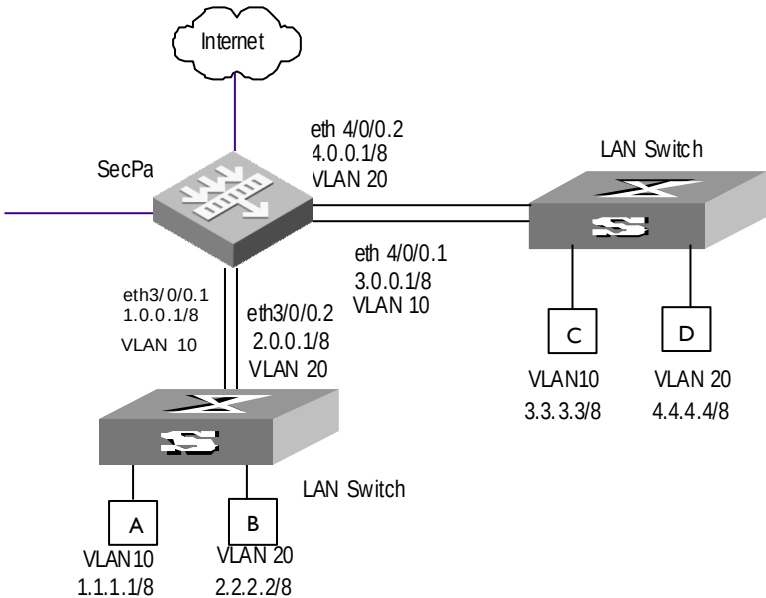


图4-2 三层交换模式 VLAN 组网图

3. 配置步骤

创建并进入以太网子接口（如图所示为 Ethernet3/0/0.1、Ethernet3/0/0.2、Ethernet4/0/0.1 和 Ethernet4/0/0.2），为其配置 IP 地址，设置每个子接口上的封装类型（以太网子接口的封装类型必须和交换机端口配置的封装类型保持一致）以及相关联的 VLAN ID。

注意：配置了以太网子接口的封装类型后，子接口就被设置为允许中继。

```
<H3C> system-view
[H3C] interface ethernet 3/0/0.1
[H3C-Ethernet3/0/0.1] ip address 1.0.0.1 255.0.0.0
[H3C-Ethernet3/0/0.1] vlan-type dot1q vid 10
[H3C] interface ethernet 3/0/0.2
[H3C-Ethernet3/0/0.2] ip address 2.0.0.1 255.0.0.0
[H3C-Ethernet3/0/0.2] vlan-type dot1q vid 20
[H3C] interface ethernet 4/0/0.1
[H3C-Ethernet4/0/0.1] ip address 3.0.0.1 255.0.0.0
[H3C-Ethernet4/0/0.1] vlan-type dot1q vid 10
[H3C] interface ethernet 4/0/0.2
[H3C-Ethernet4/0/0.2] ip address 4.0.0.1 255.0.0.0
[H3C-Ethernet4/0/0.2] vlan-type dot1q vid 20
```

设置 VLAN10 每秒处理报文的最大数目为 100000，VLAN20 每秒处理报文的最大数目为 200000。

```
[H3C] max-packet-process 100000 10
[H3C] max-packet-process 200000 20
```

目 录

第 1 章 IP地址配置	1-1
1.1 IP地址介绍	1-1
1.2 IP地址的配置.....	1-4
1.2.1 配置接口IP地址	1-4
1.2.2 配置接口借用IP地址（IP Address Unnumbered）	1-6
1.2.3 IP地址显示和调试.....	1-7
1.2.4 IP Address Unnumbered显示和调试.....	1-7
1.2.5 IP地址配置举例	1-8
第 2 章 IP应用配置	2-1
2.1 地址解析协议（ARP）的配置.....	2-1
2.1.1 动态ARP简介.....	2-1
2.1.2 静态ARP简介.....	2-1
2.1.3 静态ARP的配置	2-1
2.1.4 使能/关闭ARP表项的检查功能	2-2
2.1.5 使能/关闭支持自然网段的ARP请求.....	2-2
2.1.6 代理ARP的配置	2-2
2.1.7 免费ARP的配置	2-4
2.1.8 ARP显示和调试.....	2-5
2.2 域名解析（DNS）的配置.....	2-6
2.2.1 域名解析简介.....	2-6
2.2.2 静态域名解析的配置	2-6
2.2.3 域名解析表显示和调试	2-7
2.3 DNS Client配置	2-7
2.3.1 DNS Client的配置.....	2-8
2.3.2 DNS Client的显示和调试.....	2-9
2.3.3 使用DNS进行域名解析典型配置举例	2-10
2.3.4 故障诊断与排除	2-11
2.4 DNS Proxy配置	2-11
2.4.1 DNS Proxy简介	2-11
2.4.2 DNS Proxy的配置.....	2-12
2.4.3 DNS Proxy典型配置举例	2-12
2.5 URPF配置	2-14
2.5.1 URPF简介	2-14
2.5.2 URPF配置	2-15
2.5.3 URPF的显示与调试.....	2-15

第 3 章 UDP HELPER配置.....	3-1
3.1 UDP HELPER简介.....	3-1
3.2 UDP HELPER配置.....	3-1
3.2.1 启动/关闭UDP中继转发功能.....	3-1
3.2.2 配置需要中继转发的UDP端口	3-2
3.2.3 配置广播报文中继转发的目的服务器.....	3-2
3.3 UDP HELPER的显示和调试	3-3
第 4 章 BOOTP客户端配置	4-1
4.1 BOOTP客户端简介	4-1
4.2 BOOTP客户端配置	4-1
4.2.1 配置以太网接口通过BOOTP协议获取IP地址	4-1
4.3 BOOTP客户端的显示及调试.....	4-2
第 5 章 DHCP配置	5-1
5.1 DHCP简介.....	5-1
5.1.1 DHCP	5-1
5.1.2 DHCP服务器	5-2
5.1.3 DHCP Accounting简介	5-4
5.1.4 DHCP服务器支持BIMS option	5-6
5.1.5 DHCP服务器支持option 184	5-7
5.1.6 DHCP中继	5-9
5.2 DHCP公共配置	5-10
5.2.1 使能/禁止DHCP服务	5-10
5.2.2 配置伪DHCP服务器检测功能	5-10
5.3 DHCP服务器配置.....	5-11
5.3.1 配置接口工作在DHCP服务器模式.....	5-12
5.3.2 创建DHCP全局地址池.....	5-13
5.3.3 配置DHCP地址池的地址分配	5-13
5.3.4 配置DHCP地址池中不参与自动分配的IP地址.....	5-15
5.3.5 配置DHCP地址池的IP地址租用有效期限	5-15
5.3.6 配置DHCP客户端的域名	5-16
5.3.7 配置DHCP客户端的DNS服务器的IP地址.....	5-17
5.3.8 配置DHCP客户端的NetBIOS服务器的IP地址	5-18
5.3.9 配置DHCP客户端的NetBIOS节点类型.....	5-19
5.3.10 配置DHCP自定义选项.....	5-20
5.3.11 配置DHCP客户端的出口网关	5-21
5.3.12 配置DHCP服务器的ping包发送.....	5-21
5.3.13 配置DHCP服务器计费	5-22
5.3.14 DHCP服务器支持BIMS option配置	5-23
5.3.15 配置DHCP服务器支持option184.....	5-23
5.3.16 清除DHCP相关信息	5-26

5.4 DHCP客户端配置	5-27
5.5 DHCP中继配置	5-27
5.5.1 配置接口工作在DHCP中继模式	5-28
5.5.2 配置DHCP中继指定的外部服务器地址	5-28
5.5.3 通过DHCP中继配置DHCP服务器负载分担	5-29
5.5.4 通过DHCP中继释放客户端的IP地址	5-30
5.5.5 清除DHCP中继的统计信息	5-30
5.6 DHCP显示和调试	5-30
5.7 DHCP典型配置举例	5-32
5.7.1 DHCP服务器典型配置举例	5-32
5.7.2 DHCP中继典型配置举例	5-34
5.7.3 DHCP客户端典型配置举例	5-35
5.7.4 DHCP Accounting配置举例	5-37
5.7.5 IP电话请求option 184 组网案例	5-38
第 6 章 IP性能配置	6-1
6.1 配置接口最大传输单元（MTU）	6-1
6.2 配置TCP报文分片	6-1
6.3 配置TCP属性	6-1
6.4 配置ICMP发送重定向报文	6-2
6.5 IP性能显示和调试	6-3
6.6 快速转发配置	6-4
6.6.1 快速转发简介	6-4
6.6.2 快速转发配置	6-5
6.6.3 快速转发的显示和调试	6-6
6.7 IP性能配置排错	6-6
第 7 章 IP单播策略路由配置	7-1
7.1 IP单播策略路由简介	7-1
7.2 IP单播策略路由的配置	7-2
7.2.1 创建策略	7-2
7.2.2 设置Route-policy的if-match子句	7-3
7.2.3 设置Route-policy的apply子句	7-3
7.2.4 使能/禁止本地策略路由	7-4
7.2.5 使能/禁止接口策略路由	7-4
7.3 IP单播策略路由显示和调试	7-4
7.4 IP单播策略路由典型配置举例	7-5
7.4.1 配置基于源地址的策略路由	7-5
7.4.2 配置基于报文大小的策略路由	7-7

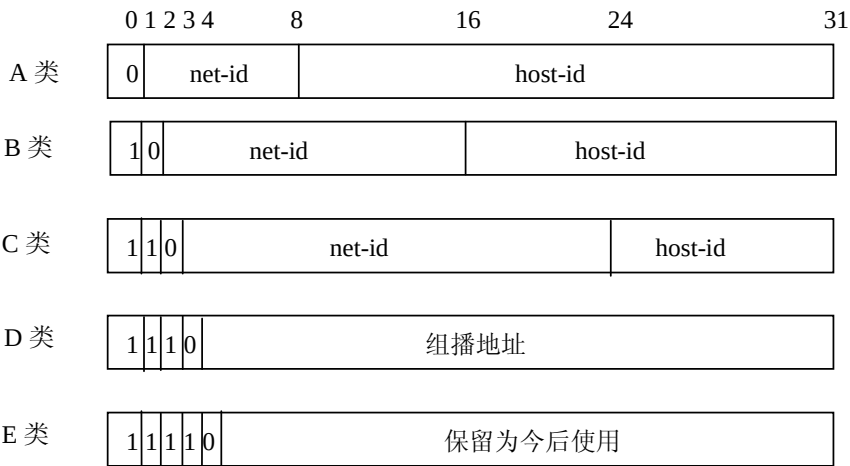
第1章 IP 地址配置

1.1 IP 地址介绍

所谓 IP 地址，是指分配给连接在 Internet 上的主机的一个唯一的 32 比特标识符。IP 地址一般由两部分组成：第一部分为网络号码，第二部分为主机号码。IP 地址的结构使我们可以在 Internet 上方便地进行寻址。IP 地址由美国国防数据网的网络信息中心（NIC）进行分配。

为了方便IP地址的管理以及组网，Internet的IP地址分成五类。如图 1-1所示，IP地址由下列两个字段组成：

- 网络号码字段（net-id）；网络号码字段的前几位称为类别字段（又称为类别比特），用来区分 IP 地址的类型。
- 主机号码字段（host-id）。



net-id—网络号码，host-id—主机号码

图1-1 五类 IP 地址

D 类地址是一种组播地址，主要是留给 Internet 体系结构委员会 IAB（Internet Architecture Board）使用。E 类地址保留在今后使用。目前大量使用中的 IP 地址属于 A、B、C 三类中的一种。

在使用 IP 地址时要知道一些 IP 地址是保留作为特殊用途的，一般不使用。下表列出用户可配置的 IP 地址范围。

表1-1 IP 地址分类及范围

网络类型	地址范围	用户可用的 IP 网络范围	说明
A	0.0.0.0~ 127.255.255.255	1.0.0.0~126.0.0.0	所有形如 127.X.Y.Z 的地址都保留作回路测试，发送到这个地址的分组不会输出到线路上，它们被内部处理并当作输入分组。
B	128.0.0.0~ 191.255.255.255	128.0.0.0~191.254.0.0	-
C	192.0.0.0~ 223.255.255.255	192.0.0.0~223.255.254.0	-
D	224.0.0.0~ 239.255.255.255	无	D 类地址是一种组播地址。
E	240.0.0.0~ 255.255.255.255	无	255.255.255.255 用于广播地址，其它地址保留今后使用。

IP 地址有一些重要的特点：

- (1) IP 地址是一种非等级的地址结构，和电话号码的结构不一样，也就是说，IP 地址不能反映任何有关主机位置的地理信息。
- (2) 当一个主机同时连接到两个网络上时，该主机就必须同时具有两个相应的 IP 地址，其网络号码 **net-id** 是不同的，这种主机成为多地址主机（**multihomed host**）。
- (3) 按照 **Internet** 的观点，用转发器或网桥连接起来的若干个局域网仍为一个网络，因此这些局域网都具有同样的网络号码 **net-id**。
- (4) 在 IP 地址中，所有分配到网络号码（**net-id**）的网络，不管是小的局域网还是很大的广域网，都是平等的。

从 1985 年起，为了使 IP 地址的使用更加灵活，只分配 IP 地址的网络号码 **net-id**，而后面的主机号码 **host-id** 则是受本单位控制。即某个单位申请到 IP 地址时，实际上只是拿到了一个网络号码 **net-id**，具体的各个主机号码 **host-id** 则由该单位自行分配，只要做到在该单位管辖的范围内无重复的主机号码即可。当一个单位的主机很多而且分布在很大的地理范围时，为了便于管理，可将单位内部的主机号码再进一步划分为多个子网。需要注意的是，子网的划分由本单位内部决定，在本单位以外是看不见划分的操作的。从外部看，这个单位只有一个网络号码。只有当外面的报文进入到本单位范围后，本单位的网络设备才根据子网号码再进行选路，找到目的主机。

如图 1-2 所示，为一个 B 类 IP 地址划分子网情况，其中子网掩码由一串连续的“1”和一串连续的“0”组成。“1”对应于网络号码和子网号码字段，而“0”对应于主机号码字段。

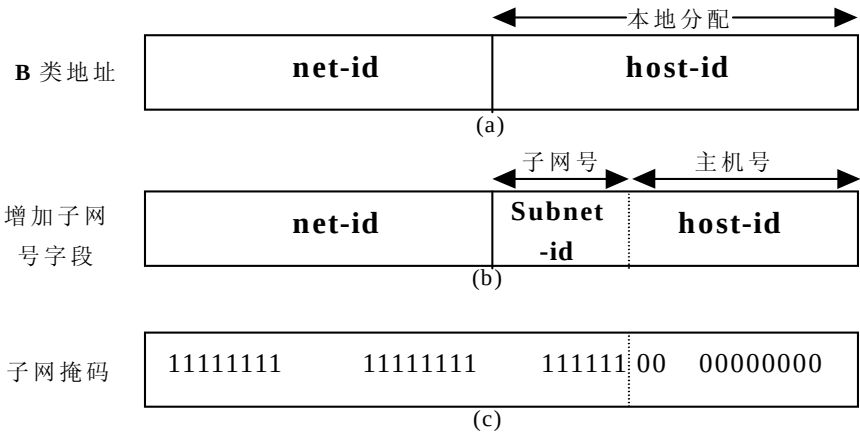


图1-2 IP 地址子网划分

多划分出一个子网号码字段是要付出代价的。举例来说，本来一个 B 类 IP 地址可以容纳 65534 个主机号码。但划分出 6bit 长的子网字段后，最多可有 64 个子网，每个子网有 10bit 的主机号码，即每个子网最多可有 1022 ($2^{10}-2$ ，去掉全 1 和全 0 的主机号码) 个主机号码。因此主机号码的总数是 $64 \times 1022 = 65408$ 个，比不划分子网时要少 126 个。

若一个单位不进行子网的划分，则其子网掩码即为默认值，此时子网掩码中“1”的长度就是网络号码的长度。因此，对于 A、B 和 C 类的 IP 地址，其对应子网掩码的默认值分别为 255.0.0.0；255.255.0.0 和 255.255.255.0。

一台防火墙可以用来连接多个网络，具有多个网络的 IP 地址。上面讲的 IP 地址还不能直接用来进行通信。这是因为：

- IP 地址只是主机在网络层中的地址，若要将网络层中传送的数据报交给目的主机，必须知道该主机的物理地址。因此必须将 IP 地址解析为物理地址。
- 用户平时不愿意使用难于记忆的 IP 地址，而是愿意使用易于记忆的主机名，因此也需要将主机名解析为 IP 地址。

下图表示了主机名、IP 地址和物理地址之间的关系。

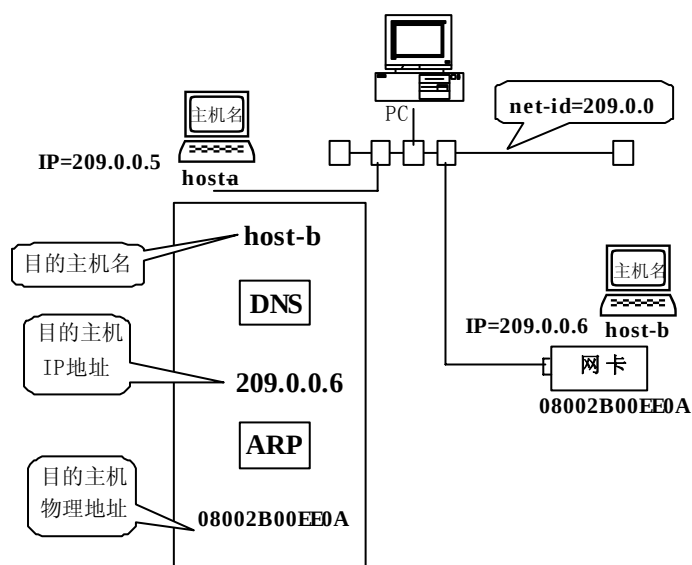


图1-3 主机名、IP 地址和物理地址之间的关系

1.2 IP 地址的配置

IP 地址配置包括：

- 配置接口 IP 地址
- 配置接口借用 IP 地址
- IP 地址的监控与维护

1.2.1 配置接口 IP 地址

防火墙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。

IP 地址的配置支持如下情况：

- 父接口和子接口之间不可以是同一网段。
- 兄弟接口之间不可以是同一网段。
- 主从地址可以是同一网段。

1. 配置接口主 IP 地址

一个接口只能有一个主 IP 地址，用下面的命令可修改接口的主 IP 地址和网络的掩码。

请在接口视图下进行下列配置。

表1-2 配置接口主 IP 地址

操作	命令
配置接口主 IP 地址	ip address <i>ip-address net-mask</i>

通过掩码来标识 IP 地址包含的网号，例如：防火墙以太网口的 IP 地址是 129.9.30.42，掩码是 255.255.0.0，将 IP 地址与掩码相“与”后，可知防火墙以太网接口所在网段的地址为 129.9.0.0。

当配置主 IP 地址时，如果接口上已经有主 IP 地址，则原主 IP 地址被删除，新配置的地址成为主 IP 地址。

缺省情况下，无主 IP 地址。

2. 配置接口从 IP 地址

除了主 IP 地址外，一个接口上还可配置多个从 IP 地址。配置从 IP 地址的主要目的在于使同一接口能位于不同的子网上，从而产生以同一接口为输出端口的网络路由，这样通过同一接口实现与多个子网相连。

请在接口视图下进行下列配置。

表1-3 配置接口从 IP 地址

操作	命令
配置接口从 IP 地址	ip address <i>ip-address net-mask sub</i>

缺省情况下，无从 IP 地址。

一个接口所能配置的 IP 地址总数最多为 32 个，包括主 IP 地址和从 IP 地址。

3. 删除接口 IP 地址

请在接口视图下进行下列配置。

表1-4 删除接口 IP 地址

操作	命令
删除 IP 地址	undo ip address [<i>ip-address net-mask</i> [sub]]

使用该命令时若不带任何参数，将删除该接口的所有 IP 地址。

undo ip address 命令不带任何参数表示删除该接口的所有 IP 地址。**undo ip address** *ip-address net-mask* 表示删除主 IP 地址，**undo ip address** *ip-address net-mask sub* 表示删除从 IP 地址。在删除主 IP 地址前必须先删除完所有的从 IP 地址。

4. 设置接口 IP 地址可协商属性

若接口封装了 PPP，本端接口还未配置 IP 地址而对端已有 IP 地址时，可为本端接口配置 IP 地址可协商属性（在本端防火墙上配置 **ip address ppp-negotiate** 命令，在对端防火墙上配置 **remote address** 命令），使本端接口接受 PPP 协商产生的由对端分配的 IP 地址。该配置主要用于在通过 ISP 访问 Internet 时，得到由 ISP 分配的 IP 地址。

请在接口视图下进行下列配置。

表1-5 设置接口 IP 地址可协商属性

操作	命令
设置接口 IP 地址可协商属性	ip address ppp-negotiate
取消接口 IP 地址可协商属性	undo ip address ppp-negotiate
配置为对端接口分配 IP 地址	remote address { ip-address pool [pool-number] }
取消为对端接口分配 IP 地址	undo remote address

系统缺省为不允许接口 IP 地址的协商。



注意：

- 因 PPP 支持 IP 地址的协商，所以只有当接口封装了 PPP 时，才能设置接口 IP 地址的协商，当 PPP 协议 down 时，协商产生的 IP 地址将被删除。
- 若接口原来配有地址，在配置接口 IP 地址协商后，原 IP 地址将被删除。
- 配置接口 IP 地址协商后，不需再给该接口配置 IP 地址，IP 地址由协商获得。
- 配置接口 IP 地址协商后，再次配置该接口协商，原协商产生的 IP 地址将被删除，接口再次协商获得 IP 地址。
- 在协商地址被删除后，接口将处于无地址状态。

1.2.2 配置接口借用 IP 地址（IP Address Unnumbered）

1. IP Address Unnumbered 简介

借用 IP 地址这种功能，其最主要的目的就是节省宝贵的 IP 地址资源。一个接口如果没有 IP 地址就无法生成路由，也就无法转发报文。所谓“借用 IP 地址”，其实质就是：一个接口上没有配置 IP 地址，但是还想使用该接口。就向其它有 IP 地址的接口借一个 IP 地址过来，以使该接口能够正常使用。如果被借用接口有多个 IP 地址，则只能借用主 IP 地址。如果被借用接口没有 IP 地址，则借用接口的 IP 地址为 0.0.0.0。该功能通过 **ip address unnumbered** 命令来实现。

需要注意的是：

- 借用方不能为以太网接口。
- 被借用方接口的地址本身不能为借用地址。
- 被借用方的地址可以借给多个接口。
- Loopback 的地址可被其它接口借用，但本身不能借用其它接口的地址。

2. 激活和关闭 IP Address Unnumbered

IP Address Unnumbered 属性在接口视图下进行，封装了 PPP 的 Dialer 接口、虚模板接口和 Tunnel 接口可借用以太网口或其它接口的 IP 地址。

请在接口视图下进行下列配置。

表1-6 接口借用 IP 地址的配置

操作	命令
激活 IP Address Unnumbered	ip address unnumbered interface <i>interface-type interface-number</i>
关闭 IP Address Unnumbered	undo ip address unnumbered

缺省情况下，不借用其它接口的 IP 地址。



注意：

在 Tunnel 接口配置地址借用后，必须手工配置到 Tunnel 对端接口的静态路由，且建议掩码为 32 位，以免与其它路由冲突，导致报文被错误路由。

1.2.3 IP 地址显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示 IP 地址配置后的运行情况，通过查看显示信息验证配置的效果。

表1-7 IP 地址显示和调试

操作	命令
显示接口 IP 信息	display ip interface [<i>interface-type interface-number</i>]
显示接口 IP 摘要信息	display ip interface brief [<i>interface-type interface-number</i>]

1.2.4 IP Address Unnumbered 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示 IP Address unnumbered 配置后的运行情况，通过查看显示信息验证配置的效果。

表1-8 IP Address Unnumbered 显示和调试

操作	命令
显示接口信息，其中包括 IP Address Unnumbered 信息	display interface [<i>interface-type</i> [<i>interface-number</i>]]

1.2.5 IP 地址配置举例

1. 组网需求

为防火墙 Ethernet1/0/1 接口配置 IP 地址，要求主 IP 地址为 129.2.2.1，从地址为 129.1.3.1。

2. 组网图

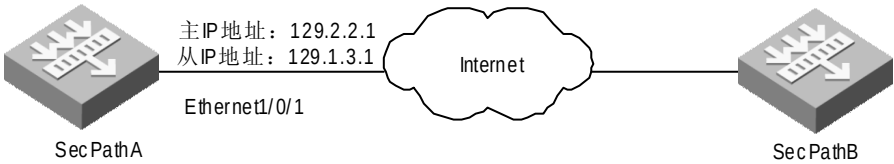


图1-4 为防火墙接口配置主从 IP 地址

3. 配置步骤

配置防火墙 Ethernet1/0/1 的主从 IP 地址。

```
[H3C] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] ip address 129.2.2.1 255.255.255.0
[H3C-Ethernet1/0/1] ip address 129.1.3.1 255.255.255.0 sub
```

第2章 IP 应用配置

2.1 地址解析协议（ARP）的配置

2.1.1 动态 ARP 简介

ARP 即地址解析协议，主要用于从 IP 地址到以太网 MAC 地址的解析。一般情况下，ARP 动态执行并自动寻求 IP 地址到以太网 MAC 地址的解析，无需管理员的介入。在 Comware 的实现中，如果收到的 ARP 报文满足以下任何一条条件，系统将创建或更新 ARP 表项：

- ARP 报文的源 IP 地址与入接口 IP 地址在同一网段，不是广播地址，目的 IP 地址是本接口 IP 地址。
- ARP 报文的源 IP 地址与入接口 IP 地址在同一网段，不是广播地址，目的 IP 地址是本接口的 VRRP 虚拟 IP 地址。
- ARP 报文的目的 IP 地址属于入接口上的配置的 NAT 地址池。

如果收到的 ARP 报文的源 IP 地址在入接口的 ARP 表中已经存在对应表项，也将对 ARP 表项进行更新。

2.1.2 静态 ARP 简介

在某些情况下，如将目的地址不在本网段的报文，绑定到某个特定网卡，使得到该 IP 地址的报文能通过该网关进行转发；或是当用户需要过滤掉一些非法 IP 地址（如将这些非法地址绑定到某个不存在的 MAC 地址），就需要用户手工配置静态 ARP 表中的映射项。

2.1.3 静态 ARP 的配置

静态 ARP 配置包括：

- 手工添加/删除静态 ARP 映射项

请在系统视图下进行下列配置。

表2-1 手工添加/删除静态 ARP 映射项

操作	命令
手工添加静态 ARP 映射项	arp static <i>ip-address ethernet-address</i> [<i>vpn-instance-name</i>]
手工删除静态 ARP 映射项	undo arp <i>ip-address</i> [<i>vpn-instance-name</i>]

静态 ARP 映射项在防火墙正常工作时间一直有效，而动态 ARP 映射项的有效时间为 20 分钟。

缺省情况下，由动态 ARP 协议获取地址映射。

2.1.4 使能/关闭 ARP 表项的检查功能

可以使用下面的命令控制设备是否学习 MAC 地址为组播 MAC 的 ARP 表项。

请在系统视图下进行下列配置。

表2-2 使能/关闭 ARP 表项的检查功能

操作	命令
使能 ARP 表项的检查功能，即不学习 MAC 地址为组播 MAC 的 ARP 表项	arp check enable
关闭 ARP 表项的检查功能，即学习 MAC 地址为组播 MAC 的 ARP 表项	undo arp check enable

缺省情况下，使能 ARP 表项的检查功能，即不学习 MAC 地址为组播 MAC 的 ARP 表项。

2.1.5 使能/关闭支持自然网段的 ARP 请求

可以使用下面的命令控制设备是否支持自然网段的 ARP 请求。

请在系统视图下进行下列配置。

表2-3 使能/关闭支持自然网段的 ARP 请求

操作	命令
使能支持自然网段的 ARP 请求	naturemask-arp enable
不支持自然网段的 ARP 请求	undo naturemask-arp enable

缺省情况下，不支持自然网段的 ARP 请求。

2.1.6 代理 ARP 的配置

1. 代理 ARP 简介

代理 ARP 的主要功能就是将处在同一网段（IP 地址在同一网段），却在不同的物理网络上的计算机或路由器连接起来，使它们互相通信，就好像在同一个物理网络上。

在 80 年代中后期，随着网络应用的发展，局域网的规模越来越大。一所大学的以太网中主机数目可以达到上百台，在这种情况下以太网中的碰撞和冲突的次数已经相当多了。此时新的应用需要继续扩大局域网的规模，若采用中继器的方式将新增的

计算机连入局域网，将会使局域网过载，产生的碰撞和冲突将严重降低以太网的性能。为解决这一问题，提出了代理 ARP 解决方案。

2. 代理 ARP 的应用环境

代理 ARP 主要是为连接两个在同一 IP 网段但位于不同物理位置上的网络。

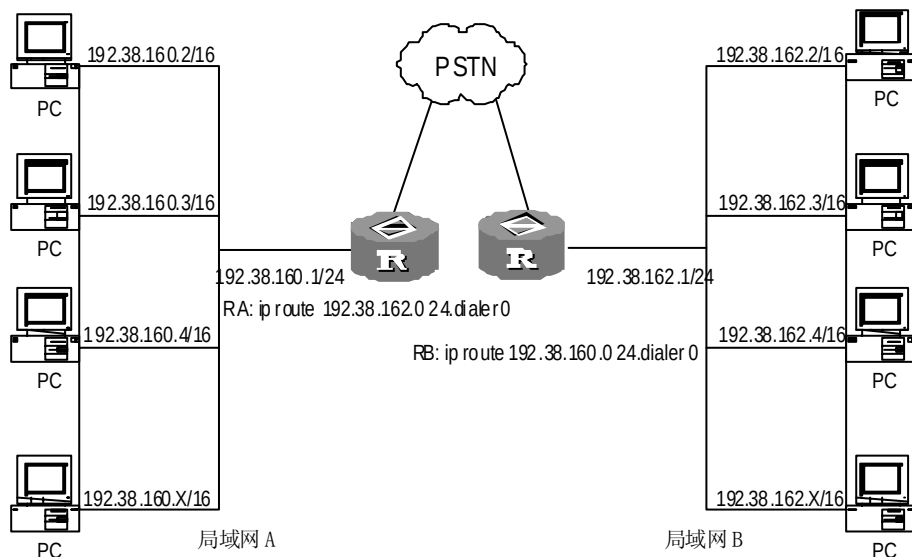


图2-1 代理 ARP 的应用环境

两个局域网分别与两台路由器的以太网口相连。两个局域网中的主机都在 192.38.0.0 网段上。实际上，局域网 A 占用了 192.38.160.0 这一子网段。局域网 B 占用了 192.38.162.0 这一子网段。但是两个局域网中主机的掩码一定是 16 位，即：只包括网络号（192.38.0.0），而不包括子网号（192.38.160.0 或 192.38.162.0）。两台路由器的以太网口都配置成 192.38.0.0 网段，并使能代理 ARP。两台路由器通过 PSTN 相连。在两台路由器上分别配置一条到对端局域网网段的静态路由。

当局域网 A 中的主机想访问局域网 B 中的主机，例如：IP 地址为 192.38.160.2 的主机（以下简称主机 A）想访问 192.38.162.2 的主机（以下简称主机 B）。其访问过程如下：

- 主机 A 发出对主机 B 的 ARP 请求报文。
- 路由器 A 收到该请求报文，查找路由表。若发现一条到主机 B 的路由项 (192.38.162.0)，就将自己的 MAC 地址添入 ARP 应答报文中，发送给主机 A。
- 主机 A 收到 ARP 应答报文后，就将 IP 报文发送给路由器 A。
- 路由器 A 接收到 IP 报文后，再查找路由表，将报文转发给路由器 B。
- 路由器 B 将接收到的 IP 报文转发给主机 B。
- 当主机 B 向主机 A 发送应答报文时，也将经过相同的过程。这样，两台处于不同物理网络上的主机相互访问，就好象处于同一物理网络上。

3. 配置代理 ARP

请在以太网接口视图下进行下面配置。

表2-4 配置代理 ARP

操作	命令
配置代理 ARP	arp-proxy enable
禁用代理 ARP 功能	undo arp-proxy enable

缺省情况下，禁用代理 ARP 功能。

2.1.7 免费 ARP 的配置

1. 免费 ARP 简介

免费 ARP 是指设备通过对外发送免费 ARP 报文，来实现以下功能：

网络中的设备可以通过发送免费 ARP 报文来确定其它设备的 IP 地址是否与自己冲突。

如果发送免费 ARP 报文的设备正好改变了硬件地址（很可能是设备关机了，并换了一块接口卡，然后重新启动），那么这个报文就可以使其它设备高速缓存中旧的硬件地址进行相应的更新。例如：设备收到某个 IP 地址的免费 ARP 请求，但在此设备的高速缓存中已经存在这个 IP 地址的 ARP 表项，那么就要用免费 ARP 请求中的发送端硬件地址（如以太网地址）对高速缓存中相应的内容进行更新。设备接收到任何 ARP 请求都要完成这个操作（ARP 请求是在网上广播的，因此每次发送 ARP 请求时网络上的所有主机都要这样做）。

免费 ARP 报文的特点：

报文的源和目的 IP 地址都是本机地址，报文源 MAC 地址是本机 MAC 地址。

当其它设备收到免费 ARP 报文后，如果发现免费 ARP 报文中的 IP 地址和自己的 IP 地址冲突，则给发送免费 ARP 报文的设备返回一个 ARP 应答。

2. 使能免费 ARP 报文学习功能

请在系统视图下进行下列配置。

表2-5 使能免费 ARP 学习功能

操作	命令
使能免费 ARP 学习功能	gratuitous-arp-learning enable
关闭免费 ARP 学习功能	undo gratuitous-arp-learning enable

缺省情况下，关闭免费 ARP 报文学习功能。

3. 使能应答不同网段的 ARP 请求报文的功能

请在系统视图下进行下列配置。

表2-6 使能应答不同网段的 ARP 请求报文的功能

操作	命令
使能应答不同网段的 ARP 请求报文的功能	gratuitous-arp-sending enable
关闭应答不同网段的 ARP 请求报文的功能	undo gratuitous-arp-sending enable

缺省情况下，关闭应答不同网段的 ARP 请求报文的功能。

4. 使能周期性发送免费 ARP 报文功能并设置发送周期

请在接口视图下进行下列配置。

表2-7 使能周期性发送免费 ARP 报文的功能并设置发送周期

操作	命令
使能周期性发送免费 ARP 报文功能并设置发送周期	arp send-gratuitous-arp seconds
关闭周期性发送免费 ARP 报文的功能	undo arp send-gratuitous-arp

缺省情况下，接口不会周期性发送免费 ARP 报文。

2.1.8 ARP 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示 ARP 配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可以清除该运行情况，执行 **debugging** 命令可以对 ARP 进行调试。

表2-8 ARP 显示和调试

操作	命令
显示 ARP 映射表	display arp [static dynamic all]
清除 ARP 映射表中的 ARP 项	reset arp [all dynamic static interface interface-type interface-number]
打开 ARP 调试信息开关	debugging arp packet
关闭 ARP 调试信息开关	undo debugging arp packet

2.2 域名解析（DNS）的配置

2.2.1 域名解析简介

TCP/IP 不仅提供了 IP 地址来确定设备，而且还专门设计了一种字符串形式的主机命名机制，这就是所谓的域名系统。此系统使用一种有层次的命名方式，为网间网上的设备指定一个有意义的名字，并且在网络上设有域名解析服务器，完成域名与 IP 地址的对应关系。这样一来用户就可以使用便于记忆的、有意义的域名，而不必去记忆晦涩难懂的 IP 地址。

域名解析分为动态解析和静态解析，二者可以相辅相成。在解析域名时，可以首先采用静态解析的方法，如果静态解析不成功，再采用动态解析的方法。可以将一些常用的域名放入静态域名解析表中，这样可以大大提高域名解析效率。

- 动态解析有专用的域名解析服务器，负责接受客户提出的域名解析请求。服务器首先在本机数据库内部解析，如果判断不属于本域范围之内，就将请求交给上一级的域名解析服务器，直到完成解析，解析的结果或者为 IP 地址，或者域名不存在，并将解析的结果反馈给客户机。
- 静态解析即手动建立域名和 IP 地址之间的对应关系。当客户机需要域名所对应的 IP 地址，即到静态域名解析表中去查找指定的域名，然后获得所对应的 IP 地址。

2.2.2 静态域名解析的配置

静态域名解析是通过静态域名解析表进行的，静态域名解析表类似于 Windows 操作系统之下的 hosts 文件，防火墙可以通过查询此表而获取常见域名的 IP 地址，同时用户可以使用便于记忆的主机名而不是抽象的 IP 地址来访问相应的设备。

请在系统视图下进行下列操作。

表2-9 配置主机名和对应 IP 地址

操作	命令
配置主机名和对应 IP 地址	ip host <i>hostname ip-address</i>
取消主机名和对应的 IP 地址	undo ip host <i>hostname [ip-address]</i>

每个主机名只能对应一个 IP 地址，当对同一主机名进行多次配置时，后配置的 IP 地址生效。

2.2.3 域名解析表显示和调试

表2-10 域名解析表显示和调试

操作	命令
显示静态域名解析表	display ip host

2.3 DNS Client 配置

由于 Internet 协议（IP）地址结构（由 32 位组成）不便于记忆（比如点分式表示的 202.112.131.109），所以大多数组织采用缩写词或有意义的名字（称为域名，如 www.sina.com.cn）来表示地址，而不是使用 IP 地址。但是，如何让非 IP 标识的域名映射为 IP 地址呢？IP 地址与其域名之间的映射是依靠解析器及域名服务器来完成的。

域名系统（DNS）是一种用于 TCP/IP 应用程序的分布式数据库，它提供主机名称和 IP 地址之间的转换及电子邮件的选路信息。从应用上来讲，对 DNS Server 的访问是通过一个地址解析器（Resolver）来完成的。DNS Client 主要完成 Resolver 的功能，它的主要功能是完成 IP 地址和主机的域名之间的转换。

一般一个 DNS 系统的工作过程为应用程序首先向 DNS Client 发出请求，DNS Client 收到请求后，首先查询本地数据库，如果发现没有，就向名称服务器发送查询报文，收到响应后再解析名称服务器发回来的响应报文，并根据响应报文的内容决定下一步的操作。

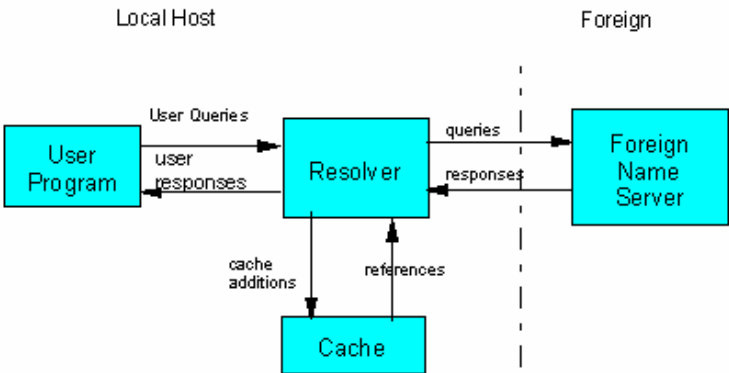


图2-2 DNS 系统组成框图

用户程序（User Program）依照自己的需要（需要域名或 IP 地址）向解析器（Resolver）发出询问，解析器首先查询本地缓冲区（Cache），如果在缓冲区中查到该映射项，则直接回复用户的请求。如果缓冲区中没有，它将根据查询的类型（需要 IP 地址还是需要域名）组织查询报文，该报文可以采用 TCP 或 UDP 格式（本程序中采用 UDP），然后根据本机上的 DNS 配置向缺省的域名服务器发出 UDP（或

TCP) 查询报文（域名服务器的端口号为 53），获得服务器的响应后，解析该响应报文并回答用户的请求。

应用程序、解析器和域名服务器以及解析器上的缓冲区关系如上图所示，其中，解析器和缓冲区集成在一起构成 DNS Client，它的作用是接受应用程序的 DNS 咨询，并对其作出应答。一般来说，“应用程序”和“域名解析器”是在同一台主机上，“域名服务器”可以和它们在同一台主机上，也可以在不同的主机上（一般情况下是在不同的主机上）。

2.3.1 DNS Client 的配置

DNS Client 的配置包括下面几个配置：

- 启动 DNS 解析
- 配置 DNS 服务器的 IP 地址
- 配置域名后缀搜索列表

其中必须的配置是启动 DNS 解析与配置 DNS 服务器的 IP 地址，如果设备上的接口使用 DHCP 客户端来分配 IP 地址，且 DHCP 服务器下发的给设备的信息中包括了 DNS 服务器的地址和域后缀搜索列表，那么只需要启动域名解析即可。

1. 启动 DNS 解析

要使用 DNS Client 功能，需要在设备上打开 DNS 解析的开关，使用下面的命令可以启动/关闭 DNS 解析。

请在系统视图下进行下面配置。

表2-11 启动/关闭 DNS 域名解析功能

操作	命令
启动 DNS 域名解析功能	dns resolve
关闭 DNS 域名解析功能	undo dns resolve

缺省情况下，关闭 DNS 域名解析功能。

2. 配置 DNS 服务器的 IP 地址

要进行 DNS 域名解析，需要知道域名服务器的地址，这样才能把查询请求报文发送到正确的服务器进行解析，使用下面的命令可以配置/删除 DNS 服务器的 IP 地址。

请在系统视图下进行下面配置。

表2-12 配置 DNS 服务器的 IP 地址

操作	命令
配置 DNS 服务器的 IP 地址	dns server <i>ip-address</i>
删除 DNS 服务器的 IP 地址	undo dns server [<i>ip-address</i>]

缺省情况下，未配置 DNS 服务器的 IP 地址。

3. 配置 DNS 域后缀搜索列表

用户在访问一些网站的时候，后缀往往都是相同的。如 sina.com.cn，h3c.com.cn，sohu.com.cn 等。

为了方便用户使用，可以设定一个 **domain** 为 com.cn，这样在用户敲入命令 **ping sina** 的时候，DNS 解析时会先查找字符串“sina.com.cn”对应的 IP 地址，如果没有得到回应，就发送 sina 的进行解析查找“sina”对应的 IP 地址。重复使用下面的命令可以配置域后缀搜索列表。

请在系统视图下进行下面配置。

表2-13 配置 DNS 域搜索后缀

操作	命令
配置 DNS 域搜索后缀	dns domain <i>domain-name</i>
删除 DNS 域搜索后缀	undo dns domain [<i>domain-name</i>]

说明：

根据 RFC1034 的规定如果用户输入“ping sina.”，那么将会先查找“sina”对应的 IP 地址，如果没有回应，则会发送“sina.com.cn”对应的 IP 地址解析请求报文。

2.3.2 DNS Client 的显示和调试

1. DNS Client 的显示

请在任意视图下进行下列操作。

表2-14 DNS Client 的显示

操作	命令
查看 DNS 解析功能是否启动	display current-configuration
显示 DNS 服务器的配置	display dns server [<i>dynamic</i>]
显示 DNS 域后缀搜索列表的配置	display dns domain [<i>dynamic</i>]

操作	命令
显示动态的域名缓存的内容	display dns dynamic-host
显示 DNS 解析结果	nslookup type { ptr ip-address a domain-name }

 说明：

如果使用 **dynamic** 参数，则显示的域名服务器是通过 DHCP 或者其它方式动态获取到的域名服务器的地址。

2. 清空动态的域名缓存的内容

在一次成功的域名解析之后，DNS Client 会把解析的结果放到缓存中。如果再有相同的域名解析请求，那么 DNS Client 会首先在缓存中查找，如果没有，再向 DNS 服务器发送域名解析请求，使用下面的命令可以清空当前缓存中的内容。

请在用户视图下进行下列操作。

表2-15 清空动态域名缓存的内容

操作	命令
清空动态的域名缓存的内容	reset dns dynamic-host

3. DNS Client 的调试

请在用户视图下进行下列操作。

表2-16 DNS Client 的调试

操作	命令
打开 DNS Client 调试开关	debugging dns
关闭 DNS Client 调试开关	undo debugging dns

缺省情况下，DNS Client 调试开关关闭。

2.3.3 使用 DNS 进行域名解析典型配置举例

1. 组网需求

在防火墙上使用域名解析功能。防火墙的 IP 地址是 10.110.10.1，DNS 服务器的 IP 地址是 10.110.10.66。

2. 组网图



图2-3 使用 DNS Client 典型组网

3. 配置步骤

防火墙配置

启动 DNS 域名解析功能。

```
[H3C] dns resolve
```

配置 DNS 服务器 IP 地址。

```
[H3C] dns server 10.110.10.66
```

配置 Ethernet 0/0/0 的 IP 地址。

```
[H3C] interface Ethernet 0/0/0
```

```
[H3C-Ethernet0/0/0] ip address 10.110.10.1 255.255.255.0
```

2.3.4 故障诊断与排除

1. 故障之一：域名解析失败

一般情况下域名解析失败的原因有如下几个：

(1) 软件原因

- 域名服务器的 IP 地址配置错误。
- 设备到域名服务器没有正确的路由
- 没有打开域名解析的开关

(2) 硬件原因

- 网络连接是否有故障，如网线折断，接口松动。

2.4 DNS Proxy 配置

2.4.1 DNS Proxy 简介

1. 概述

DNS Proxy 是指在防火墙上启动 DNS 代理功能，这样在局域网内部没有 DNS 服务器时，局域网内部客户端可以通过防火墙连接到外部 DNS 服务器，进行正确的 DNS 解析后，可以访问 Internet。

2. DNS Proxy 的工作机制

- (1) DNS 客户端将 DNS 请求报文发送给 DNS Proxy，此时请求报文的地址为 DNS Proxy 的 IP 地址；
- (2) DNS Proxy 收到请求报文后，将报文中的目的地址替换为 DNS 服务器的 IP 地址，然后根据已配置的 DNS 服务器的地址将报文转发给 DNS 服务器。若在 DNS Proxy 上配置了多个 DNS 服务器的地址，则 DNS Proxy 先向第一个 DNS 服务器上发送请求，若第一个 DNS 服务器没有响应，则 DNS 客户端等待超时会重新发送 DNS 请求报文，DNS Proxy 收到请求报文后向第二个 DNS 服务器转发，以此类推，直到 DNS 服务器发送响应报文为止。
- (3) DNS 服务器的响应报文返回给 DNS Proxy 后，DNS Proxy 将报文中的源 IP 地址替换为 DNS Proxy 的 IP 地址后转发给 DNS 客户端。这时，DNS 客户端就可以使用 DNS 解析到的 IP 地址访问 Internet。

2.4.2 DNS Proxy 的配置

1. 配置准备

在配置 DNS Proxy 功能前需要先进行如下配置：

- 在 DNS Proxy 上配置真实的 DNS 服务器的地址
- 在 PC 上指定 DNS Server 为启用了 DNS Proxy 的防火墙的 IP 地址
- 保证 DNS Proxy 与 DNS Client 及 DNS 服务器网络可达

2. 配置 DNS Proxy

DNS Proxy 功能是在防火墙上配置的。

表2-17 配置 DNS Proxy

操作	命令	说明
进入系统视图	system-view	-
启动 DNS 代理功能	dns-proxy enable	必选

2.4.3 DNS Proxy 典型配置举例

1. 组网需求

局域网内没有 DNS 服务器，要求内部 10.1.1.0/24 网段的 PC 可以通过外网的 DNS 服务器来解析域名。要求：

- 防火墙支持 DNS Proxy；
- 外网 DNS 服务器 IP 地址为 10.72.66.36/24。

2. 组网图

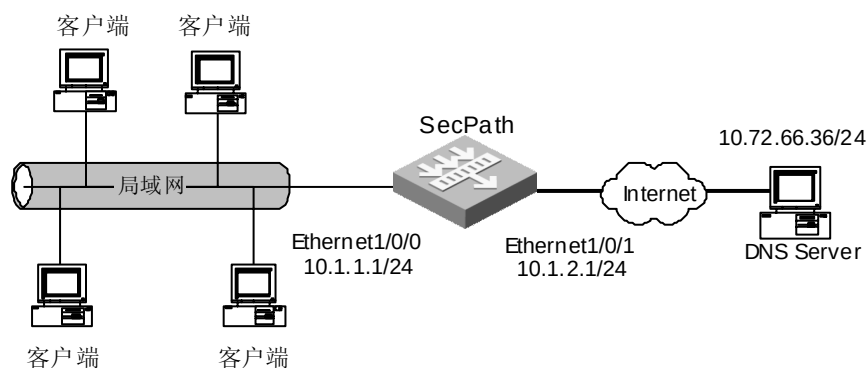


图2-4 DNS Proxy 典型配置举例

3. 配置步骤

(1) 配置防火墙

配置 Ethernet 1/0/0 的 IP 地址。

```
[H3C] interface Ethernet 1/0/0
```

```
[H3C-Ethernet1/0/0] ip address 10.1.1.1 255.255.255.0
```

配置 NAT 服务，使客户端可以通过 DNS Proxy 访问 Internet。

```
[H3C] acl number 2000
```

```
[H3C-acl-basic-2000] rule 0 permit source 10.1.1.0 0.0.0.255
```

```
[H3C-acl-basic-2000] quit
```

```
[H3C] interface Ethernet 1/0/1
```

```
[H3C-Ethernet1/0/1] ip address 10.1.2.1 255.255.255.0
```

```
[H3C-Ethernet1/0/1] nat outbound 2000
```

```
[H3C-Ethernet1/0/1] quit
```

启动 DNS Proxy 功能。

```
[H3C] dns-proxy enable
```

配置 DNS 服务器地址。

```
[H3C] dns server 10.72.66.36
```

配置路由（略）。

要确保防火墙与客户端和 DNS 服务器的路由可达。

(2) 配置 PC

将网关及 DNS 服务器指定为 10.1.1.1。

2.5 URPF 配置

2.5.1 URPF 简介

URPF（Unicast Reverse Path Forwarding，单播反向路径查找），主要功能是用于防止基于源地址欺骗的网络攻击行为。

源地址欺骗攻击为入侵者构造出一系列带有伪造源地址的报文，对于使用基于 IP 地址验证的应用来说，此攻击方法可以导致未被授权用户以他人身份获得访问系统的目的。即使响应报文不能达到攻击者，同样也会造成对被攻击对象的破坏。

一般的 URPF 检查有严格（Strict）型和松散（Loose）型两种，此外，还可以支持 ACL 与缺省路由的检查。

URPF 的处理流程如下：

- (1) 首先进行源地址合法性检查，如果报文的源地址不是合法的主机地址，直接将其丢弃。
- (2) 如果报文的源地址在防火墙的 FIB 表中存在，且找到的转发表项中的出接口与该报文的入接口相同：
 - 如果找到的转发表项是缺省路由，若配置了 **allow-default-route** 参数，则允许报文通过，若未配置 **allow-default-route** 参数，则进入 ACL 的检查流程。
 - 如果找到的转发表项不是缺省路由，则通过 URPF 检查，允许报文通过。
- (3) 如果报文的源地址在防火墙的 FIB 表中存在，但找到的转发表项中的出接口与该报文的入接口不同：
 - 对于 **strict** 型检查，直接进入 ACL 的检查流程。
 - 对于 **loose** 型检查，处理过程与第（2）步相同。
- (4) 如果报文的源地址在防火墙的 FIB 表中不存在，或者找到的转发表项为 Blackhole 或者 Reject，则进入 ACL 检查流程。
- (5) ACL 检查流程
 - 如果配置了 ACL，且 ACL 操作为允许，则允许报文通过，若操作为拒绝，则丢弃报文。
 - 如果未配置 ACL，则直接丢弃报文。

 说明：

URPF 不支持快速转发，即在已经建立快速转发表的情况下，URPF 检查失败的报文仍然能够被转发。

2.5.2 URPF 配置

请在接口视图下进行下列配置。

表2-18 使能或关闭 URPF 检查

操作	命令
使能 URPF 检查	ip urpf { strict loose } [allow-default-route] [acl acl-number]
关闭 URPF 检查	undo ip urpf

缺省为关闭 URPF 检查。

2.5.3 URPF 的显示与调试

请在用户视图下进行下列配置。

表2-19 显示 URPF 的丢包情况

操作	命令
打开 URPF 的丢包调试开关	debugging ip urpf discards [interface interface-type interface-num]
关闭 URPF 的丢包调试开关	undo debugging ip urpf discards [interface interface-type interface-num]

第3章 UDP HELPER 配置

3.1 UDP HELPER 简介

UDP HELPER 的主要功能是实现对指定 UDP 广播报文的中继转发，即它能将 UDP 广播报文转成单播报文发送给指定的服务器，起到一个中继的作用。

在启动 UDP HELPER 后，如果端口接收到 UDP 广播报文，则根据报文的 UDP 端口号来判断是否要对该报文进行中继转发，如果需要转发，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，将报文送给上层模块处理。对于 BOOTP/DHCP 广播报文的中继，如果客户端在请求报文中指明需要以广播报文的形式接收响应报文，则系统将以广播的方式向客户端发送响应报文；否则将以单播的方式向客户端发送响应报文。

3.2 UDP HELPER 配置

UDP HELPER 配置包括：

- 启动/关闭 UDP 中继转发功能
- 配置需要中继转发的 UDP 端口
- 配置广播报文中继转发的目的服务器

3.2.1 启动/关闭 UDP 中继转发功能

可以使用下面的命令启动/关闭 UDP 中继转发功能。当启动该功能后，用户就可以配置需要中继转发的 UDP 端口。在启动的同时，69、53、37、137、138、49 这六个默认的 UDP 端口的广播报文转发功能会被启动。当关闭该功能后，所有已配置的 UDP 端口都被取消，包括默认端口。

请在系统视图下进行下列配置。

表3-1 启动/关闭 UDP 中继转发功能

操作	命令
启动 UDP 中继转发功能	udp-helper enable
关闭 UDP 中继转发功能	undo udp-helper enable

缺省情况下，UDP 中继转发处于关闭状态。

3.2.2 配置需要中继转发的 UDP 端口

可以使用下面的命令配置需要中继转发的 UDP 端口。当启动 UDP 中继转发功能后，系统默认支持中继转发下面协议端口的广播报文，即这些默认 UDP 端口的广播报文会被单播转发到相应的目的服务器。系统最多支持配置 256 个需要中继转发的 UDP 端口。

表3-2 默认 UDP 端口列表

协议	UDP 端口号
TFTP (Trivial File Transfer Protocol)	69
DNS (Domain Name System)	53
Time service	37
NetBIOS-NS (NetBIOS Name Server)	137
NetBIOS-DS (NetBIOS Datagram Server)	138
TACACS (Terminal Access Controller Access Control System)	49

请在系统视图下进行下列配置。

表3-3 配置/删除需要中继转发的 UDP 端口

操作	命令
配置需要中继转发的 UDP 端口	udp-helper port { port dns netbios-ds netbios-ns tacacs tftp time }
删除需要中继转发的 UDP 端口	undo udp-helper port { port dns netbios-ds netbios-ns tacacs tftp time }

需要注意的是：

- 只有先启动 UDP 中继转发功能后，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。
- 参数 **dns|netbios-ds|netbios-ns|tacacs|tftp|time** 指 6 个默认端口。对默认端口可以有两种配置方法：(1) 指定端口号配置；(2) 指定参数配置。例如：**udp-helper port 53** 和 **udp-helper port dns** 的效果是一样的。
- 在用 **display current-configuration** 命令显示配置信息时，默认端口号是不显示的，只有当取消了一个默认端口的中继转发功能，该端口号才显示出来。

3.2.3 配置广播报文中继转发的目的服务器

可以使用下面的命令在以太网接口上配置广播报文被中继转发到的目的服务器。一个以太网接口最多对应 20 个目的服务器。在启动 UDP 中继转发功能，且在某个以

以太网接口上配置了目的服务器后，则从该以太网接口接收的指定 UDP 端口的广播报文都被单播发送到以太网接口对应的目的服务器。

请在以太网接口视图下进行下列配置。

表3-4 配置/删除广播报文中继转发的目的服务器

操作	命令
配置广播报文中继转发的目的服务器	udp-helper server <i>ip-address</i>
删除广播报文中继转发的目的服务器	undo udp-helper server [<i>ip-address</i>]

缺省情况下，没有配置目的服务器。

3.3 UDP HELPER 的显示和调试

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 UDP HELPER 的目的服务器，通过查看显示信息验证配置的效果。

在用户视图下，用户可以执行 **debugging** 命令对 UDP HELPER 进行调试。

表3-5 UDP HELPER 的显示和调试

操作	命令
显示以太网接口对应的目的服务器信息	display udp-helper server [interface <i>number</i>]
打开 UDP HELPER 的调试开关	debugging udp-helper { event packet [receive send] }
关闭 UDP HELPER 的调试开关	undo debugging udp-helper { event packet [receive send] }

第4章 BOOTP 客户端配置

4.1 BOOTP 客户端简介

BOOTP 客户端可以使用 BOOTP 协议向服务器请求分配一个 IP 地址。BOOTP 客户端主要包含两个过程：

- 向服务器发送 BOOTP 请求报文
- 处理服务器返回的 BOOTP 响应报文

BOOTP 客户端在使用 BOOTP 协议获取 IP 地址时，先向服务器发送 BOOTP 请求报文，服务器接收到请求报文后，将返回 BOOTP 响应报文。BOOTP 客户端从接收到响应报文中即可获取所分配到的 IP 地址。

BOOTP 协议报文是基于 UDP 的，为了保证报文的可靠传输，采取超时重传机制。BOOTP 客户端在向服务器发送请求报文时，同时启动一个重发定时器。若该定时器超时仍未收到服务器返回的响应报文，则要重传请求报文。重传报文每隔五秒重传一次，报文最多能传送三次，传送三次之后还不成功就不再重传报文。

4.2 BOOTP 客户端配置

BOOTP 客户端配置包括：

- 配置以太网接口通过 BOOTP 协议获取 IP 地址

4.2.1 配置以太网接口通过 BOOTP 协议获取 IP 地址

可以使用下面的命令配置以太网接口的 IP 地址通过 BOOTP 协议获取。

请在以太网接口视图下进行下列配置。

表4-1 配置以太网接口通过 BOOTP 协议获取 IP 地址

操作	命令
配置以太网接口通过 BOOTP 协议获取 IP 地址	ip address bootp-alloc
取消以太网接口通过 BOOTP 协议获取 IP 地址	undo ip address bootp-alloc

缺省情况下，以太网接口不通过 BOOTP 协议获取 IP 地址。

4.3 BOOTP 客户端的显示及调试

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后的 BOOTP 客户端，通过查看显示信息验证配置的效果。

表4-2 BOOTP 客户端的显示及调试

操作	命令
显示 BOOTP 客户端的相关信息	display bootp client [interface <i>interface-type interface-number</i>]

第5章 DHCP 配置

5.1 DHCP 简介

5.1.1 DHCP

1. DHCP 介绍

随着网络规模的扩大和网络复杂度的提高，网络配置越来越复杂，经常出现计算机位置变化（如便携机或无线网络）和计算机数量超过可分配的 IP 地址的情况。动态主机配置协议 DHCP（Dynamic Host Configuration Protocol）就是为满足这些需求而发展起来的。

与 BOOTP 相比，DHCP 也采用客户/服务器通信模式，由客户端向服务器提出配置申请（包括分配的 IP 地址、子网掩码、缺省网关等参数），服务器根据策略返回相应配置信息，两种协议的报文都采用 UDP 进行封装，并使用基本相同的报文结构。

BOOTP 运行在相对静态（每台主机都有固定的网络连接）的环境中，管理员为每台主机配置专门的 BOOTP 参数文件，该文件会在相当长的时间内保持不变。

DHCP 从两方面对 BOOTP 进行了扩展：DHCP 可使计算机仅用一个消息就获取它所需要的所有配置信息；DHCP 允许计算机快速、动态地获取 IP 地址，而不是静态为每台主机指定地址。

2. DHCP 的 IP 地址分配

(1) IP 地址分配策略

对于 IP 地址的占用时间，不同主机有不同的需求：对于服务器，可能需要长期使用固定的 IP 地址；对于某些主机，可能需要长期使用某个动态分配的 IP 地址；而某些个人则可能只在需要时分配一个临时的 IP 地址就可以了。

针对这些不同的需求，DHCP 服务器提供三种 IP 地址分配策略：

- 手工分配地址：由管理员为少数特定主机（如 WWW 服务器等）配置固定的 IP 地址。
- 自动分配地址：为首次连接到网络的某些主机分配固定 IP 地址，该地址将长期由该主机使用。
- 动态分配地址：以“租借”的方式将某个地址分配给客户端主机，使用期限到期后，客户端需要重新申请地址。大多数客户端主机得到的是这种动态分配的地址。

(2) IP 地址分配的优先次序

DHCP 服务器按照如下次序为客户端选择 IP 地址：

- DHCP 服务器的数据库中与客户端 MAC 地址静态绑定的 IP 地址；
- 客户端以前曾经使用过的 IP 地址，即客户端发送的 DHCP-REQUEST 报文中请求 IP 地址选项（Requested IP Addr Option）的地址；
- 在 DHCP 地址池中，顺序查找可供分配的 IP 地址，最先找到的 IP 地址；
- 如果未找到可用的 IP 地址，则依次查询超过租期、发生冲突的 IP 地址，如果找到则进行分配，否则报告错误。

5.1.2 DHCP 服务器

1. DHCP 服务器的应用环境

在以下场合通常利用 DHCP 服务器来完成 IP 地址分配：

- 网络规模较大，手工配置需要很大的工作量，并难以对整个网络进行集中管理。
- 网络中主机数目大于该网络支持的 IP 地址数量，无法给每个主机分配一个固定的 IP 地址。大量用户必须通过 DHCP 服务动态获得自己的 IP 地址，而且，对并发用户的数目也有限制。
- 网络中具有固定 IP 地址的主机比较少，大部分主机可以不使用固定的 IP 地址。

2. DHCP 服务器的基本原理

在 DHCP 的典型应用中，一般包含一台 DHCP 服务器和多台客户端（如 PC 和便携机），如下图所示：

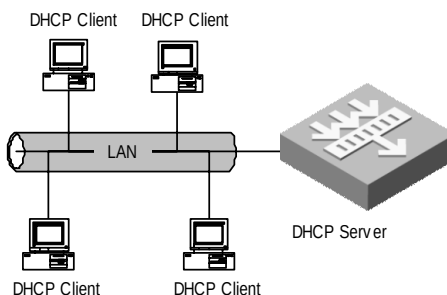


图5-1 DHCP 服务器典型组网应用

DHCP 客户端为了获取合法的动态 IP 地址，在不同阶段与服务器之间交互不同的信息，通常存在以下三种模式：

(1) DHCP 客户端首次登录网络

DHCP 客户端首次登录网络时，主要通过四个阶段与 DHCP 服务器建立联系。

- 发现阶段，即 DHCP 客户端寻找 DHCP 服务器的阶段。客户端以广播方式发送 DHCP_Discover 报文，只有 DHCP 服务器才会进行响应。
- 提供阶段，即 DHCP 服务器提供 IP 地址的阶段。DHCP 服务器接收到客户端的 DHCP_Discover 报文后，从 IP 地址池中挑选一个尚未分配的 IP 地址分配给客户端，向该客户端发送包含出租 IP 地址和其它设置的 DHCP_Offer 报文。服务器在发送 DHCP_Offer 报文之前，会以广播的方式发送 ARP 报文进行地址探测，以保证发送给客户端的 IP 地址的唯一性。
- 选择阶段，即 DHCP 客户端选择 IP 地址的阶段。如果有多台 DHCP 服务器向该客户端发来 DHCP_Offer 报文，客户端只接受第一个收到的 DHCP_Offer 报文，然后以广播方式向各 DHCP 服务器回应 DHCP_Request 报文，该信息中包含 DHCP 服务器在 DHCP_Offer 报文中分配的 IP 地址。
- 确认阶段，即 DHCP 客户端确认所提供 IP 地址的阶段。客户端收到 DHCP_ACK 确认报文后，广播 ARP 报文，目的地址是被分配的 IP 地址。如果在规定的时间内没有收到回应，客户端才使用此地址。
- 除 DHCP 客户端选中的服务器外，其它 DHCP 服务器本次未分配出的 IP 地址仍可用于其它客户端的 IP 地址申请。

(2) DHCP 客户端再次登录网络

当 DHCP 客户端再次登录网络时，主要通过以下几个步骤与 DHCP 服务器建立联系。

- DHCP 客户端首次正确登录网络后，以后再登录网络时，只需要广播包含上次分配 IP 地址的 DHCP_Request 报文即可，不需要再次发送 DHCP_Discover 报文。
- DHCP 服务器收到 DHCP_Request 报文后，如果客户端申请的地址没有被分配，则返回 DHCP_ACK 确认报文，通知该 DHCP 客户端继续使用原来的 IP 地址。
- 如果此 IP 地址无法再分配给该 DHCP 客户端使用（例如已分配给其它客户端），DHCP 服务器将返回 DHCP_NAK 报文。客户端收到后，重新发送 DHCP_Discover 报文请求新的 IP 地址。

(3) DHCP 客户端延长 IP 地址的租用有效期

DHCP 服务器分配给客户端的动态 IP 地址通常有一定的租借期限，期满后服务器会收回该 IP 地址。如果 DHCP 客户端希望继续使用该地址，需要更新 IP 租约（如延长 IP 地址租约）。

实际使用中，在 DHCP 客户端启动或 IP 地址租约期限达到一半时，DHCP 客户端会自动向 DHCP 服务器发送 DHCP_Request 报文，以完成 IP 租约的更新。如果此

IP 地址有效，则 DHCP 服务器回应 DHCP_ACK 报文，通知 DHCP 客户端已经获得新 IP 租约。

(4) 在 PC 机上的配置（以 Window XP 操作系统为例）

在用户 PC 机（即 DHCP 客户端）的 DOS 环境下使用 **ipconfig /release** 命令主动释放 IP 地址，此时，用户 PC 机向 DHCP 服务器发送 DHCP_Release 报文。然后，在用户 PC 机的 DOS 环境下使用 **ipconfig /renew** 命令申请新的 IP 地址，此时，用户 PC 机向 DHCP 服务器发送 DHCP_Discover 报文。

在用户 PC 机（DHCP 客户端）上也可以使用 **ipconfig /renew** 命令来更新其 IP 地址租约。

上述几个过程在下面的 DHCP 客户端状态迁移图中有完整体现：

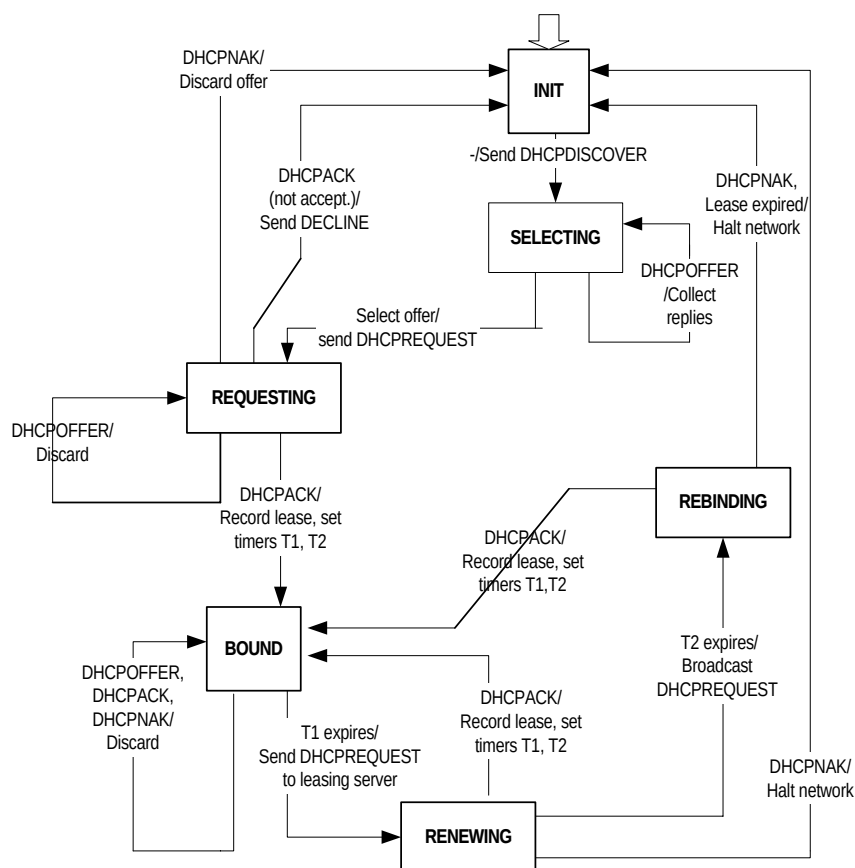


图5-2 DHCP 客户端状态迁移图

5.1.3 DHCP Accounting 简介

DHCP Accounting 又称为 DHCP 计费，是指 DHCP 服务器在分配和释放租约时，通知 RADIUS 服务器开始计费或停止计费。DHCP 服务器与 RADIUS 服务器配合使用，实现了网络计费功能，同时也在一定程度上保障了网络的安全性。

1. DHCP Accounting 报文结构

在 DHCP 服务器与 RADIUS 服务器进行交互主要是通过发送 Accounting start 和 Accounting stop 请求报文来进行的，这两种报文结构的结构大致相同，只是在 Attribute 字段稍有差别，报文结构如下：

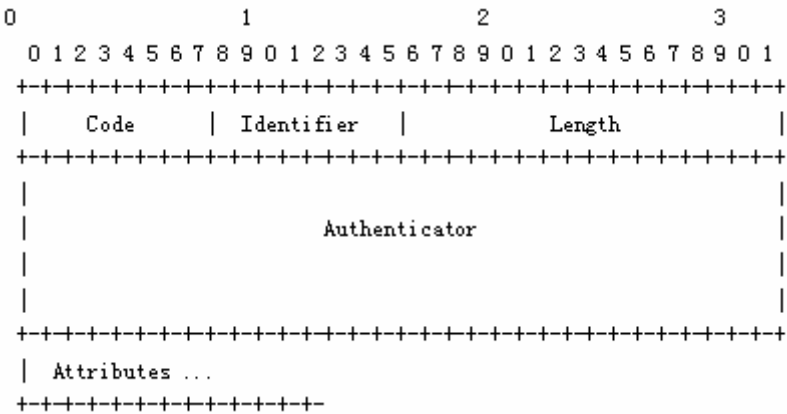


图5-3 Accounting 报文结构

- **Code:** Code 字段在报文中占用一个字节，用来表示 RADIUS 报文的类型。当收到的报文的 Code 字段非法时，该报文将会被丢弃。Code 值为 4 时表示是 Accounting start 报文，为 5 时表示是 Accounting stop 报文。
- **Identifier:** Identifier 字段在报文中占用一个字节，用来匹配请求和回应报文，RADIUS 服务器可以通过这个字段来检测从同一个客户端的相同 IP 地址和 UDP 端口发来的重复请求。
- **Length:** Length 字段在报文中占用两个字节，标识了整个 Accounting 报文的长度。
- **Authenticator:** Authenticator 字段在报文中占用 16 个字节。用来识别客户端和 RADIUS 计费服务器之间的信息。

2. DHCP Accounting 的工作机制

在运行 DHCP Server 功能的防火墙上配置好 AAA 认证和 RADIUS，则 DHCP Server 作为 RADIUS 的客户端。对于 DHCP Server 作为 RADIUS 客户端的认证过程，请参考本手册的“安全”部分，这里将介绍 DHCP Server 与 RADIUS Server 的计费交互过程。

- DHCP 服务器通过 DHCP ACK 报文将 IP 配置信息发送给 DHCP 客户端后，会发送 Accounting start 请求报文给指定的 RADIUS 服务器，RADIUS 服务器将对 Accounting start 请求进行相应的处理，并进行记录。同时 RADIUS 服务器给 DHCP 服务器发送回应报文。

- 当由于某种原因，DHCP 服务器的租约被释放后，DHCP 服务器将立刻发送 Accounting stop 请求报文通知 RADIUS 服务器停止记录，然后 RADIUS 服务器对 Accounting stop 报文进行相应的处理并停止记录。同时 RADIUS 服务器给 DHCP 服务器发送回应报文。释放租约的原因有：租约过期、收到用户的 release 请求、手工删除租约、手工删除地址池等。

若由于种种原因，指定域的 RADIUS 服务器不可达，则 Accounting start 报文将在一定的时间间隔发送三次，若三次后仍没有收到正确的相应报文，则不再发送 Accounting start 报文。

5.1.4 DHCP 服务器支持 BIMS option

1. DHCP 服务器支持 BIMS option 概述

DHCP 服务器支持 BIMS option 是指 DHCP 服务器在给 DHCP 客户端分配 IP 地址的同时将 BIMS（Branch Intelligent Management System）服务器的信息也同时告知 DHCP 客户端，使 DHCP 客户端在得到 IP 地址后能够通过 BIMS 服务器进行软件备份和升级。BIMS option 的 option 号为 217。

2. BIMS option 的报文结构

BIMS option 是在 DHCP 服务器给 DHCP 客户端的回应报文的 options 字段中添加的。由于不同厂商的 DHCP 客户端对 DHCP 回应报文的处理机制不同，因此 DHCP 服务器在 DHCP_OFFER 和 DHCP_ACK 报文中都将携带 BIMS option 选项。BIMS option 报文结构如下：

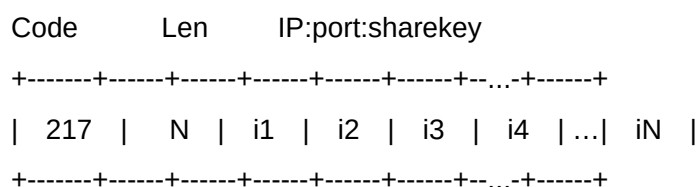


图5-4 BIMS option（option 217）报文结构

BIMS option 报文的结构与其它 option 报文的结构基本相同，也包含了 Code 和 Len 字段用来标识 option 的序号和 option 报文的长度。

i1~iN 字段主要用来携带 BIMS 服务器的 IP 地址、协议端口号以及 BIMS Server 的共享密钥。在该字段由字符串组成，例如 BIMS 服务器的 IP 地址为 192.168.1.1，端口号为 80，共享密钥为 abcdefg，则在 i 字段中表示为 192.168.1.1.80.abcdefg。

3. DHCP 服务器支持 BIMS option 工作机制

- (1) DHCP 客户端向 DHCP 服务器发送请求报文申请 IP 地址以及配置参数。

- (2) DHCP 服务器端收到请求报文后，查看本地配置的地址池，DHCP 服务器可以在全局地址池及接口地址池启动 BIMS option。若将要分配地址的地址池启动了 BIMS option，则 DHCP 服务器将在回应报文中除携带分配给客户端的 IP 配置信息外，还将携带 BIMS 服务器的 IP 地址、协议端口号以及共享密钥。

DHCP 客户端收到服务器带有 BIMS option 的回应报文后解析出 option 中的 BIMS 服务器 IP 地址、协议端口号以及共享密钥。客户端获得 BIMS 服务器的信息后就向 BIMS 服务器定期发送连接请求，以便通过 BIMS 服务器进行软件的备份和升级。

5.1.5 DHCP 服务器支持 option 184

1. DHCP 服务器支持 option184 简介

option 184 是 RFC 中规定的保留选项，用户可以自定义该选项中携带的信息。因此 3Com 使用该选项定义了四个私有的子选项，从而使 DHCP 服务器可以在回应 DHCP 客户端的请求时携带 DHCP 客户端需要的信息。option 184 中包含的子选项主要是携带了语音方面的信息，其子选项号和携带的信息具体如下：

- sub-option 1: NCP-IP (Network Call Processor IP Address)，网络呼叫处理器 IP 地址。
- sub-option 2: AS-IP (Alternate Server IP Address)，备选 NCP 服务器的 IP 地址。
- sub-option 3: Voice VLAN Configuration，语音 VLAN 配置。
- sub-option 4: Fail-Over Call Routing，Failover 呼叫路由。

(1) option 184 中各子选项的含义

- NCP-IP

NCP-IP 子选项携带了 NCP (Network Call Processor，网络呼叫处理器) 的 IP 地址。在 option 184 中若使用该子选项，必须将其作为第一个子选项 (sub-option 1)。option 184 的 sub-option 1 子选项携带的 NCP-IP 地址可以标识作为网络呼叫控制源的服务器及应用程序下载服务器。

- AS-IP

AS-IP 子选项携带了 AS (Alternate Server，备选服务器) 的 IP 地址，该子选项为 option 184 的第二个子选项 (sub-option 2)。只有定义了 sub-option 1，即只有定义了 NCP-IP 子选项，AS-IP 子选项才能生效。

option 184 中的 sub-option 2 子选项携带了备选 NCP 服务器的 IP 地址，用来作为 NCP-IP 的备份。当 NCP-IP 中携带的地址不可达或不合法时，才使用该选项指定的 NCP 服务器。

- Voice VLAN Configuration

Voice VLAN Configuration 子选项携带了语音 VLAN 是否使能的标记以及 VLAN ID，该子选项为 option 184 的第三个子选项（sub-option 3）。

option 184 的 sub-option 3 子选项共由两部分组成：一部分携带了语音 VLAN 识别是否使能的标记，另一部分携带了语音 VLAN 的 ID 信息。当语音 VLAN 使能域标记为 0 时，则表示没有使能语音 VLAN 识别功能，即使 VLAN ID 域中指定了语音 VLAN ID，也将忽略该 VLAN ID 信息；当语音 VLAN 使能域标记为 1 时，表示使能语音 VLAN 识别功能。

(2) Fail-Over Call Routing

Fail-Over Call Routing 子选项携带了 Failover 呼叫路由的 IP 地址及其关联的拨号串，该子选项为 option 184 的第四个子选项（sub-option 4）。

option 184 的 sub-option 4 子选项中的 Fail-Over 呼叫路由的 IP 地址和拨号串就是 SIP（Session Initiation Protocol，会话初始化协议）用户之间互相通信时对端的 IP 地址和呼叫号码。当 NCP 服务器不可达时，SIP 用户可以使用已配置的对端 IP 地址及呼叫号码直接与对端 SIP 用户建立连接并通信。

说明：

DHCP 服务器添加 option 184 的 sub-option 时，添加 sub-option 2、sub-option 3 或 sub-option 4 前必须先添加 sub-option 1 子选项，否则后面的子选项将无效。

(3) DHCP 服务器支持 option 184 的工作机制

DHCP 服务器携带的 option 184 信息是添加在服务器给 DHCP 客户端的回应报文中。下面假设 DHCP 客户端与 DHCP 服务器在同一网段，DHCP 服务器支持 option 184 的工作机制如下：

- DHCP 客户端向 DHCP 服务器发送请求报文，请求报文中携带 option 184 选项，该选项中指明了请求 option 184 的配置参数。
- DHCP 服务器查看请求报文中的请求列表，然后在回应报文的 options 字段中添加 option 184 及相应的 sub-option 后返回给 DHCP 客户端。

说明：

只有 DHCP 客户端在请求报文的 option 55 选项中指明要求回应 option 184 选项，DHCP 服务器才会回应 option 184。

5.1.6 DHCP 中继

1. DHCP 中继的应用环境

早期的 DHCP 协议只适用于 DHCP 客户端和服务端处于同一个子网内的情况，不能跨网段。因此，为进行动态主机配置，需要在所有网段上都设置一个 DHCP 服务器，这显然是很不经济的。

DHCP 中继功能（DHCP Relay）的引入解决了这一难题：局域网内的客户端可以通过 DHCP 中继与其它子网的 DHCP 服务器通信，最终取得合法的 IP 地址。这样，多个网络上的 DHCP 客户端可以使用同一个 DHCP 服务器，既节省了成本，又便于进行集中管理。

一般来说，DHCP 中继可以是主机，也可以是防火墙或路由器，只要对它启动 DHCP 中继代理的服务程序即可。

2. DHCP 中继的基本原理

下图是 DHCP 中继的典型应用示意图。

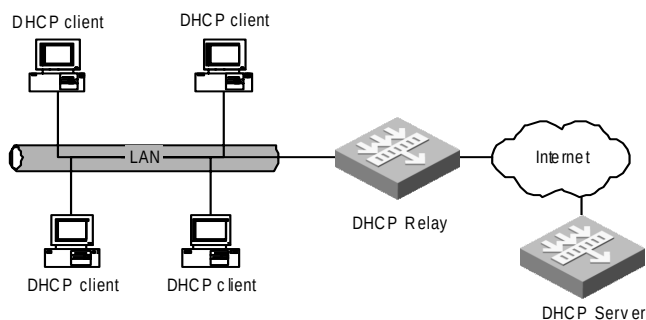


图5-5 DHCP 中继的典型组网应用

工作原理如下：

- 当 DHCP 客户端启动并进行 DHCP 初始化时，它在本地网络广播配置请求报文。
- 如果本地网络存在 DHCP 服务器，则可以直接进行 DHCP 配置，不需要 DHCP 中继；
- 如果本地网络没有 DHCP 服务器，则与本网络相连的、带 DHCP 中继功能的网络设备收到该广播报文后，进行适当处理并转发给指定的、其它网络上的 DHCP 服务器。
- DHCP 服务器根据客户端提供的信息进行相应的配置，并通过 DHCP 中继将配置信息发送给客户端，完成对客户端的动态配置。事实上，从开始配置到最终完成配置，可能存在多次这样的交互过程。

DHCP 中继提供了对 DHCP 广播报文的透明传输功能，能够把 DHCP 客户端（或服务）的广播报文透明地传送到其它网段的 DHCP 服务器（或客户端）上。

在实际网络环境中，DHCP 中继功能一般是在防火墙某个具体的接口上实现的。这时需要为该接口配置 IP 中继地址，用来指定 DHCP 服务器。

5.2 DHCP 公共配置

DHCP 的公共配置是指对于 DHCP 服务器和 DHCP 中继功能都适用的配置，包括：

- 使能/禁止 DHCP 服务
- 配置伪 DHCP 服务器检测功能

5.2.1 使能/禁止 DHCP 服务

对于 DHCP 服务器和 DHCP 中继，在进行 DHCP 配置之前，都需要先使能 DHCP 服务。只有启动该服务后，其它相关的 DHCP 配置才能生效。

请在系统视图下进行下列配置。

表5-1 使能/禁止 DHCP 服务

操作	命令
使能 DHCP 服务	dhcp enable
禁止 DHCP 服务	undo dhcp enable

缺省情况下，使能 DHCP 服务。

 说明：

在正确配置系统时钟后，DHCP 才会正常运行。

5.2.2 配置伪 DHCP 服务器检测功能

在网络中，如果有私自架设的 DHCP 服务器，当其它用户申请 IP 地址时，这台 DHCP 服务器就会与 DHCP 客户端进行交互，导致用户获得错误的 IP 地址，无法正常上网，这种私设的 DHCP 服务器称为伪 DHCP 服务器。

可以配置伪 DHCP 服务器检测功能，记录 DHCP 服务器的 IP 地址和接口等信息，以便管理员及时发现并处理伪 DHCP 服务器。

请在系统视图下进行下列配置。

表5-2 配置伪 DHCP 服务器检测功能

操作	命令
使能伪 DHCP 服务器检测功能	dhcp server detect
禁止伪 DHCP 服务器检测功能	undo dhcp server detect

缺省情况下，禁止伪 DHCP 服务器检测功能。

5.3 DHCP 服务器配置

DHCP 服务器配置包括：

- 配置接口工作在 DHCP 服务器模式
- 创建 DHCP 地址池
- 配置 DHCP 地址池的地址分配
- 配置 DHCP 地址池中不参与自动分配的 IP 地址
- 配置 DHCP 地址池的 IP 地址租用有效期限
- 配置 DHCP 客户端的域名
- 配置 DHCP 客户端的 DNS 服务器的 IP 地址
- 配置 DHCP 客户端的 NetBIOS 服务器的 IP 地址
- 配置 DHCP 客户端的 NetBIOS 节点类型
- 配置 DHCP 自定义选项
- 配置 DHCP 客户端的出口网关
- 配置 DHCP 服务器的 ping 包发送
- 配置 DHCP 服务器计费
- DHCP 服务器支持 BIMS option 配置
- 配置 DHCP 服务器支持 option184
- 清除 DHCP 相关信息

说明：

全局地址池与接口地址池：

- 全局地址池是通过系统视图下的 **dhcp server ip-pool** 命令创建的，在本地防火墙范围内有效。
 - 接口地址池是在为以太网接口配置了合法的单播 IP 地址后自动创建的，它的地址段范围就是此以太网接口所在的网段，并且只在此接口下有效。
-

5.3.1 配置接口工作在 DHCP 服务器模式

当收到 DHCP 客户端发出的、目的地址是本机的 DHCP 报文时，可以通过配置决定如何处理这些报文。如果配置为服务器模式，则将报文转给本地 DHCP 服务器；如果配置为中继模式，则将报文转给指定的外部 DHCP 服务器。

如果配置当前接口工作在服务器模式，请在接口视图下进行下列配置。

表5-3 配置当前接口工作在 DHCP 服务器模式

操作	命令
将 DHCP 报文发送到本地 DHCP 服务器，从全局地址池分配地址	dhcp select global [subaddress]
将 DHCP 报文发送到本地 DHCP 服务器，从接口地址池分配地址	dhcp select interface
恢复缺省设置	undo dhcp select

如果同时配置多个接口工作在服务器模式，请在系统视图下进行下列配置。

表5-4 配置指定范围的接口工作在 DHCP 服务器模式

操作	命令
将 DHCP 报文发送到本地 DHCP 服务器，从全局地址池分配地址	dhcp select global [subaddress] { interface ethernet-subinterface-range all }
将 DHCP 报文发送到本地 DHCP 服务器，从接口地址池分配地址	dhcp select interface { interface ethernet-subinterface-range all }
恢复缺省设置	undo dhcp select { interface ethernet-subinterface-range all }

缺省情况下，对 DHCP 报文的处理模式为服务器模式（**global**）。

说明：

- 如果需要使用接口地址池，必须将对 DHCP 报文的处理模式设置为 **interface**。
- **subaddress** 表示使能 DHCP Server 从地址分配功能，即服务器分配给客户端的 IP 地址为服务器上以太网口从地址网段的 IP 地址，该地址从全局地址池中分配。此时服务器端以太网接口下也要配置从 IP 地址，且要求全局地址池的网段与接口下从 IP 地址在同一网段。
- 当配置了 **subaddress** 从地址分配功能后，只有在接口的主 IP 地址对应的地址池中无可分配的地址后，才会使用从地址对应的地址池分配地址。当接口下配置了多个从地址时，系统将会按照从地址的配置顺序查找地址池并分配地址。即当第一个从地址对应的地址池中无可分配的地址时，才会使用第二个从地址对应的地址池进行分配。

5.3.2 创建 DHCP 全局地址池

DHCP 服务器通过地址池给用户分配 IP 地址。当客户端向服务器发出 DHCP 请求时，DHCP 服务器选择合适的地址池，并从中挑选一个空闲的 IP 地址与其它相关参数（如 DNS 服务器地址、地址租用期限等）一起传送给客户端。每个 DHCP 服务器可以配置多个地址池，Comware 目前支持 128 个全局地址池。

DHCP 服务器中的地址池采用树状结构：树根是自然网段地址，分支是该网段的子网地址，叶节点是手工绑定的客户端地址。这种树状结构实现了配置的继承性，即子网（子节点）配置继承自然网段（父节点）的配置，客户端（孙子节点）的配置继承子网（子节点）的配置。这样，对于一些通用参数（如域名），只需要在自然网段或者子网上配置即可。地址池的树状结构可以通过命令 **display dhcp server tree** 查看，同一级别地址池的顺序由配置的先后决定。

请在系统视图下进行下列配置。

表5-5 创建 DHCP 全局地址池

操作	命令
创建 DHCP 地址池或进入 DHCP 地址池视图	dhcp server ip-pool pool-name
删除 DHCP 地址池	undo dhcp server ip-pool pool-name

缺省情况下，没有创建任何 DHCP 全局地址池。

5.3.3 配置 DHCP 地址池的地址分配

根据客户端的实际需要，可以选择采用静态地址绑定方式或动态地址分配方式，但不能对同一个 DHCP 地址池同时配置这两种方式。

动态地址分配需要指定用于分配的地址范围，而静态地址绑定则可以看做是只包含一个地址的特殊的 DHCP 地址池。

1. 配置静态地址绑定

某些客户端可能需要固定的 IP 地址，即将客户端的 MAC 地址或 identifier 与某个 IP 地址绑定。当此 MAC 地址或 identifier 的客户端申请 DHCP 地址时，服务器根据客户端 MAC 地址或 identifier 寻找到对应的固定 IP 地址分配给客户端。

请在 DHCP 地址池视图下进行下列配置。

表5-6 配置静态地址绑定

操作	命令
配置静态绑定的 IP 地址	static-bind ip-address ip-address [mask netmask]
删除静态绑定的 IP 地址	undo static-bind ip-address

操作	命令
配置静态绑定的客户端 MAC 地址	static-bind { mac-address <i>mac-address</i> client-identifier <i>client-identifier</i> }
删除静态绑定的客户端 MAC 地址	undo static-bind { mac-address client-identifier }

缺省情况下，未配置 DHCP 客户端 IP 地址与 MAC 地址或 identifier 绑定。客户端的 MAC 地址或 identifier 类型缺省为以太。

说明：

- 命令 **static-bind ip-address** 和 **static-bind { mac-address *mac-address* | client-identifier *client-identifier* }** 必须配合使用，并且，如果多次执行，新的配置会覆盖已有配置。
- 当防火墙作为 DHCP 客户端动态获取 IP 地址时，由于防火墙发送的 DHCP Client 报文中带有 identifier 字段，所以在 DHCP 服务器端设置静态绑定时应该使用 identifier 与 IP 地址绑定，并非使用接口的 MAC 地址与 IP 地址绑定。
- 每个 MAC 地址或 identifier 只能与一个 IP 地址进行绑定。

2. 配置接口地址池的静态地址绑定

请在接口视图下进行下列配置。

表5-7 配置接口地址池的静态地址绑定

操作	命令
配置当前接口的接口地址池中的静态地址绑定	dhcp server static-bind ip-address <i>ip-address</i> { mac-address <i>mac-address</i> client-identifier <i>client-identifier</i> }
删除配置的静态地址绑定	undo dhcp server static-bind { ip-address <i>ip-address</i> mac-address <i>mac-address</i> client-identifier <i>client-identifier</i> }

3. 配置动态地址分配

对于动态分配给客户端的地址（包括永久的和租用期有限的动态地址），都需要配置地址池范围。目前，同一地址池中只能配置一个地址段，通过掩码设定地址范围的大小。

请在 DHCP 地址池视图下进行下列配置。

表5-8 配置动态分配的 IP 地址范围

操作	命令
配置动态分配的 IP 地址范围	network <i>ip-address</i> [mask <i>netmask</i>]
删除动态分配的 IP 地址范围	undo network

缺省情况下，未配置 DHCP 地址池，即没有可供分配的地址。

多次执行 **network** 命令，新的配置会覆盖已有配置。

5.3.4 配置 DHCP 地址池中不参与自动分配的 IP 地址

DHCP 服务器在分配地址时，需要排除已经被占用的某些 IP 地址（如网关、FTP 服务器等），否则，同一地址分配给两台主机会造成 IP 地址冲突。

请在系统视图下进行下列配置。

表5-9 配置 DHCP 地址池中不参与自动分配的 IP 地址

操作	命令
配置 DHCP 地址池中不参与自动分配的 IP 地址	dhcp server forbidden-ip <i>low-ip-address</i> [<i>high-ip-address</i>]
删除 DHCP 地址池中不参与自动分配的 IP 地址	undo dhcp server forbidden-ip <i>low-ip-address</i> [<i>high-ip-address</i>]

缺省情况下，DHCP 地址池中的所有 IP 地址都参与自动分配。

多次执行本命令，可以配置多个不参与自动分配的 IP 地址段。

5.3.5 配置 DHCP 地址池的 IP 地址租用有效期限

对于不同的地址池，DHCP 服务器可以指定不同的地址租用期限，但同一 DHCP 地址池中的地址都具有相同的期限。

地址租用有效期限不具有继承关系。

为方便用户，系统提供不同范围的地址租用有效期限配置方式。

1. 全局 DHCP 地址池

请在 DHCP 地址池视图下进行下列配置。

表5-10 配置全局 DHCP 地址池的 IP 地址租用有效期限

操作	命令
配置动态分配的 IP 地址租用有效期限	expired { <i>day day</i> [<i>hour hour</i> [<i>minute minute</i>]] unlimited }
恢复缺省的 IP 地址租用有效期限	undo expired

2. 接口 DHCP 地址池

请在接口视图下进行下列配置。

表5-11 配置接口 DHCP 地址池的 IP 地址租用有效期限

操作	命令
配置动态分配的 IP 地址租用有效期限	dhcp server expired { day day [hour hour [minute minute]] unlimited }
恢复缺省的 IP 地址租用有效期限	undo dhcp server expired

3. 多个接口的 DHCP 地址池

系统提供对指定范围的多个以太网子接口的 DHCP 地址池同时进行配置的功能，以减少某些应用中的重复配置工作。

请在系统视图下进行下列配置。

表5-12 配置多个接口的 DHCP 地址池 IP 地址租用有效期限

操作	命令
配置动态分配的 IP 地址租用有效期限	dhcp server expired { day day [hour hour [minute minute]] unlimited } { interface ethernet-subinterface-range all }
恢复缺省的 IP 地址租用有效期限	undo dhcp server expired { interface ethernet-subinterface-range all }

缺省情况下，IP 地址租用有效期限为 1 天。

说明：

为方便用户，对某些 DHCP 配置选项，系统提供不同范围的 DHCP 地址池的配置方式。用户可以分别对全局 DHCP 地址池、接口 DHCP 地址池或指定接口范围的多个以太网子接口的接口 DHCP 地址池进行配置，最后一种配置方式对于减少某些应用中的重复配置尤其有用。

这类配置任务包括：配置 DHCP 客户端的域名、DHCP 客户端的 DNS 服务器的 IP 地址、DHCP 客户端的 NetBIOS 服务器的 IP 地址、DHCP 客户端的 NetBIOS 节点类型以及 DHCP 自定义选项。

5.3.6 配置 DHCP 客户端的域名

在 DHCP 服务器上，可以为每个地址池分别指定客户端使用的域名。

如果配置全局 DHCP 地址池，请在 DHCP 地址池视图下进行下列配置。

表5-13 配置全局 DHCP 地址池的 DHCP 客户端域名

操作	命令
配置分配给 DHCP 客户端的域名	domain-name <i>domain-name</i>
删除分配给 DHCP 客户端的域名	undo domain-name

如果配置接口 DHCP 地址池，请在接口视图下进行下列配置。

表5-14 配置接口 DHCP 地址池的 DHCP 客户端域名

操作	命令
配置分配给 DHCP 客户端的域名	dhcp server domain-name <i>domain-name</i>
删除分配给 DHCP 客户端的域名	undo dhcp server domain-name

如果配置多个接口的 DHCP 地址池，请在系统视图下进行下列配置。

表5-15 配置多个接口的 DHCP 地址池的 DHCP 客户端域名

操作	命令
配置分配给 DHCP 客户端的域名	dhcp server domain-name <i>domain-name</i> { interface <i>ethernet-subinterface-range</i> all }
删除分配给 DHCP 客户端的域名	undo dhcp server domain-name { interface <i>ethernet-subinterface-range</i> all }

缺省情况下，未配置分给 DHCP 客户端的域名。

5.3.7 配置 DHCP 客户端的 DNS 服务器的 IP 地址

主机通过域名访问 Internet 时，需要将域名解析为 IP 地址，这是通过域名系统 DNS（Domain Name System）实现的。因此，为了使 DHCP 客户端成功接入 Internet，DHCP 服务器应在为客户端分配 IP 地址的同时指定 DNS 服务器地址。

在目前的实现中，每个 DHCP 地址池最多可以配置 8 个 DNS 服务器地址。

如果配置全局 DHCP 地址池，请在 DHCP 地址池视图下进行下列配置。

表5-16 配置全局 DHCP 地址池的 DNS 服务器地址

操作	命令
配置 DHCP 客户端的 DNS 服务器的 IP 地址	dns-list <i>ip-address</i> [<i>ip-address</i>]
删除 DHCP 客户端的 DNS 服务器的 IP 地址	undo dns-list { <i>ip-address</i> all }

如果配置接口 DHCP 地址池，请在接口视图下进行下列配置。

表5-17 配置接口 DHCP 地址池的 DNS 服务器地址

操作	命令
配置 DHCP 客户端的 DNS 服务器的 IP 地址	dhcp server dns-list <i>ip-address</i> [<i>ip-address</i>]
删除 DHCP 客户端的 DNS 服务器的 IP 地址	undo dhcp server dns-list { <i>ip-address</i> all }

如果配置多个接口的 DHCP 地址池，请在系统视图下进行下列配置。

表5-18 配置多个接口的 DHCP 地址池的 DNS 服务器地址

操作	命令
配置 DHCP 客户端的 DNS 服务器的 IP 地址	dhcp server dns-list <i>ip-address</i> [<i>ip-address</i>] { interface <i>ethernet-subinterface-range</i> all }
删除 DHCP 客户端的 DNS 服务器的 IP 地址	undo dhcp server dns-list { <i>ip-address</i> all } { interface <i>ethernet-subinterface-range</i> all }

缺省情况下，未配置 DNS 服务器的 IP 地址。

5.3.8 配置 DHCP 客户端的 NetBIOS 服务器的 IP 地址

对于使用 Microsoft 操作系统的客户端，由 WINS（Windows Internet Naming Service）服务器为通过 NetBIOS 协议通信的主机提供主机名到 IP 地址的解析。所以，大部分 Windows 网络客户端需要进行 WINS 的设置。

在目前的实现中，每个 DHCP 地址池最多可以配置 8 个 NetBIOS 地址。

如果配置全局 DHCP 地址池，请在 DHCP 地址池视图下进行下列配置。

表5-19 配置全局 DHCP 地址池客户端的 NetBIOS 服务器地址

操作	命令
配置 DHCP 客户端的 NetBIOS 服务器地址	nbns-list <i>ip-address</i> [<i>ip-address</i>]
删除 DHCP 客户端的 NetBIOS 服务器地址	undo nbns-list { <i>ip-address</i> all }

如果配置接口 DHCP 地址池，请在接口视图下进行下列配置。

表5-20 配置接口 DHCP 地址池客户端的 NetBIOS 服务器地址

操作	命令
配置 DHCP 客户端的 NetBIOS 服务器地址	dhcp server nbns-list <i>ip-address</i> [<i>ip-address</i>]
删除 DHCP 客户端的 NetBIOS 服务器地址	undo dhcp server nbns-list { <i>ip-address</i> all }

如果配置多个接口的 DHCP 地址池，请在系统视图下进行下列配置。

表5-21 配置多个接口的 DHCP 地址池客户端的 NetBIOS 服务器地址

操作	命令
配置 DHCP 客户端的 NetBIOS 服务器地址	dhcp server nbns-list <i>ip-address</i> [<i>ip-address</i>] { interface <i>ethernet-subinterface-range</i> all }
删除 DHCP 客户端的 NetBIOS 服务器地址	undo dhcp server nbns-list { <i>ip-address</i> all } { interface <i>ethernet-subinterface-range</i> all }

缺省情况下，未配置 NetBIOS 服务器的 IP 地址。

5.3.9 配置 DHCP 客户端的 NetBIOS 节点类型

DHCP 客户端在广域网上使用 NetBIOS 协议通信时，需要在主机名和 IP 地址之间建立映射关系。根据获取映射关系的方式不同，NetBIOS 节点分为四种：

- **b 类节点（b-node）**：“b”代表广播（broadcast），即，此类节点采用广播的方式获取映射关系。
- **p 类节点（p-node）**：“p”代表端到端（peer-to-peer），即，此类节点采用与 NetBIOS 服务器通信的方式获取映射关系。
- **m 类节点（m-node）**：“m”代表混合（mixed），是具有部分广播特性的 p 类节点。
- **h 类节点（h-node）**：“h”代表混合（hybrid），是具备“端对端”通信机制的 b 类节点。

如果配置全局 DHCP 地址池，请在 DHCP 地址池视图下进行下列配置。

表5-22 配置全局 DHCP 地址池的客户端 NetBIOS 节点类型

操作	命令
配置 DHCP 客户端的 NetBIOS 节点类型	netbios-type { b-node h-node m-node p-node }
恢复 DHCP 客户端的缺省 NetBIOS 节点类型	undo netbios-type

如果配置接口 DHCP 地址池，请在接口视图下进行下列配置。

表5-23 配置接口 DHCP 服务器的客户端的 NetBIOS 节点类型

操作	命令
配置 DHCP 客户端的 NetBIOS 节点类型	dhcp server netbios-type { b-node h-node m-node p-node }
恢复 DHCP 客户端的缺省 NetBIOS 节点类型	undo dhcp server netbios-type

如果配置多个接口的 DHCP 地址池，请在系统视图下进行下列配置。

表5-24 配置多个接口的 DHCP 地址池客户端的 NetBIOS 节点类型

操作	命令
配置 DHCP 客户端的 NetBIOS 节点类型	dhcp server netbios-type { b-node h-node m-node p-node } { interface ethernet-subinterface-range all }
恢复 DHCP 客户端的缺省 NetBIOS 节点类型	undo dhcp server netbios-type { interface ethernet-subinterface-range all }

缺省情况下，客户端采用 h 类节点（**h-node**）。

5.3.10 配置 DHCP 自定义选项

随着 DHCP 的不断发展，新的可选配置项会陆续出现，为了支持这些新的选项，可以通过手工定义的方式将新选项添加到 DHCP 服务器的属性列表中。

如果配置全局 DHCP 地址池，请在 DHCP 地址池视图下进行下列配置。

表5-25 配置全局 DHCP 地址池的自定义选项

操作	命令
配置 DHCP 自定义选项	option code { ascii ascii-string hex hex-string ip-address ip-address }
删除 DHCP 自定义选项	undo option code

如果配置接口 DHCP 地址池，请在接口视图下进行下列配置。

表5-26 配置接口 DHCP 服务器的自定义选项

操作	命令
配置 DHCP 自定义选项	dhcp server option code { ascii ascii-string hex hex-string ip-address ip-address }
删除 DHCP 自定义选项	undo dhcp server option code

如果配置多个接口的 DHCP 地址池，请在系统视图下进行下列配置。

表5-27 配置多个接口的 DHCP 自定义选项

操作	命令
配置 DHCP 自定义选项	dhcp server option code { ascii ascii-string hex hex-string ip-address ip-address } { interface ethernet-subinterface-range all }
删除 DHCP 自定义选项	undo dhcp server option code { interface ethernet-subinterface-range all }

code 为合法的 *option* 号，范围为 2~254 之间，其中 3、6、15、44、46、50~55、57~61、184 和 217 被系统保留使用。

5.3.11 配置 DHCP 客户端的出口网关

DHCP 客户端访问本网段以外的服务器或主机时，数据必须通过出口网关进行收发。请在 DHCP 地址池视图下进行下列配置。

表5-28 配置 DHCP 客户端的出口网关

操作	命令
配置 DHCP 客户端的出口网关	gateway-list <i>ip-address</i> [<i>ip-address</i>]
删除 DHCP 客户端的出口网关	undo gateway-list { <i>ip-address</i> all }

缺省情况下，未配置 DHCP 客户端的出口网关地址。

在目前的实现中，每个 DHCP 地址池最多可以配置 8 个出口网关地址。

说明：

当指定多个出口网关地址时，需要多个 *ip-address* 参数。

5.3.12 配置 DHCP 服务器的 ping 包发送

为防止 IP 地址重复分配导致地址冲突，DHCP 服务器为客户端分配地址前，需要先对该地址进行探测。

地址探测是通过 ping 命令实现的，检测是否能在指定时间内得到 ping 应答。如果没有得到应答，则继续发送 ping 报文，直到发送 ping 包数量达到最大值；如果仍然超时，则可以认为本网段内没有设备使用该 IP 地址，从而确保客户端被分得的 IP 地址唯一。

请在系统视图下进行下列配置。

表5-29 配置 DHCP 服务器的 ping 包发送

操作	命令
配置 DHCP 服务器发送 ping 包的最大数量	dhcp server ping packets <i>number</i>
恢复 DHCP 服务器发送 ping 包的缺省最大数量	undo dhcp server ping packets
配置 DHCP 服务器发送 ping 包的最长等待响应时间	dhcp server ping timeout <i>milliseconds</i>
恢复 DHCP 服务器发送 ping 包的缺省最长等待响应时间	undo dhcp server ping timeout

缺省情况下，发送 ping 包的最大数量为 2，等待 ping 响应的最长时间为 500 毫秒。

DHCP 服务器通过 ping 包的发送检测是否发生地址冲突，而 DHCP 客户端则通过 ARP 报文检测是否发生地址冲突。

5.3.13 配置 DHCP 服务器计费

DHCP 服务器计费功能用于 DHCP 服务器在分配和释放租约时，向指定域的 RADIUS 模式的计费服务器发送计费报文。

配置了 DHCP 服务器计费功能后，当用户申请 IP 地址时，DHCP 服务器会给用户分配带有 IP 地址、租约期限和其它配置信息的租约，成功分配租约后，会立刻通知指定域的 RADIUS 计费服务器，发送一个 RADIUS START 计费请求报文；当由于某种原因，DHCP Server 的租约被释放（释放租约的原因可能有租约过期，收到用户的 release 请求，手工删除租约，手工删除地址池等），那么 DHCP 服务器会立刻通知指定域的 RADIUS 计费服务器，发送一个 RADIUS STOP 计费结束报文。

此时 RADIUS 服务器只是记录了用户使用 IP 地址的情况，并不真正进行计费。

在 DHCP 服务器上，可以为每个地址池指定计费所使用的域。

如果配置全局 DHCP 地址池，请在 DHCP 地址池视图下进行下列配置。

表5-30 配置全局 DHCP 地址池中计费所使用的域

操作	命令
配置 DHCP 服务器计费所使用的域	accounting domain <i>domain-name</i>
删除 DHCP 服务器计费功能	undo accounting domain

如果配置接口 DHCP 地址池，请在接口视图下进行下列配置。

表5-31 配置接口 DHCP 地址池中计费所使用的域

操作	命令
配置 DHCP 服务器计费所使用的域	dhcp server accounting domain <i>domain-name</i>
删除 DHCP 服务器计费功能	undo dhcp server accounting domain

如果配置多个接口的 DHCP 地址池，请在系统视图下进行下列配置。

表5-32 配置多个接口的 DHCP 地址池中计费所使用的域

操作	命令
配置 DHCP 服务器计费所使用的域	dhcp server accounting domain <i>domain-name</i> { interface <i>ethernet-subinterface-range</i> all }
删除 DHCP 服务器计费功能	undo dhcp server accounting domain { interface <i>ethernet-subinterface-range</i> all }

缺省情况下，未启动 DHCP 服务器计费功能。

有关于 RADIUS 服务器及 domain 的配置，请参见本手册的“安全”部分。

5.3.14 DHCP 服务器支持 BIMS option 配置

1. 配置准备

在配置 DHCP 服务器支持 BIMS option 前应先进行如下配置：

- 在防火墙上启动 DHCP Server 服务器并配置地址池
- 配置 DHCP 客户端
- 保证 DHCP 客户端、DHCP 服务器以及 BIMS 服务器之间网络可达

2. 配置 BIMS option

表5-33 配置 BIMS option

操作	命令	说明
进入系统视图	system-view	-
启动并配置 BIMS option	dhcp server bims-server ip ip-address port port-number sharekey key { interface interface-type interface-number to interface-type interface-number all }	必选 该配置与下面的在 DHCP 全局地址池视图下配置 BIMS option 在实际应用中二者选其一
进入 DHCP 全局地址池并启动并配置 BIMS option	dhcp server ip-pool pool-name	-
	bims-server ip ip-address port port-number sharekey key	必选 该配置与上面的在系统视图下配置 BIMS option 在实际应用中二者选其一

说明：

若在全局地址池中配置了 BIMS option，则 DHCP 服务器从全局地址池分配 IP 地址给客户端时将携带 BIMS option。若在指定接口上配置了 BIMS option，则 DHCP 服务器从接口地址池中分配 IP 地址时携带 BIMS option。若在 **dhcp server bims-server ip** 命令中使用 **all** 关键字，则 DHCP 服务器从所有接口地址池中分配 IP 地址时都将携带 BIMS option。

5.3.15 配置 DHCP 服务器支持 option184

DHCP 服务器支持在系统视图、接口视图或在 DHCP 地址池视图下分别配置 option 184 的各 sub-option。无论是在系统视图下还是在接口视图下配置 option 184，都要在相应的接口上配置接口地址池。

1. 配置准备

在配置 DHCP 服务器支持 option184 特性前需要先进行下列配置：

- 配置 DHCP 服务器的网络参数、地址池及地址分配租期等分配策略
- 配置 DHCP 服务器与 DHCP 客户端网络可达

上述详细配置请参考本手册“网络层协议”的 DHCP 部分。

2. 在系统视图下配置 DHCP 服务器支持 option 184

表5-34 系统视图下配置 DHCP 服务器支持 option 184

操作	命令	说明
进入系统视图	system-view	-
配置接口工作在 DHCP 服务器模式，并从指定接口地址池中分配地址	dhcp select interface { all interface interface-type interface-number [to interface-type interface-number] }	必选
配置 option 184 的子选项 NCP-IP	dhcp server voice-config ncp-ip ip-address { all interface interface-type interface-number [to interface-type interface-number] }	必选
配置 option 184 的子选项 AS-IP	dhcp server voice-config as-ip ip-address { all interface interface-type interface-number [to interface-type interface-number] }	可选 只有配置了 NCP-IP 子选项才能配置该子选项
配置 option 184 的子选项 Voice VLAN Configuration	dhcp server voice-config voice-vlan vlan-id { enable disable } { all interface interface-type interface-number [to interface-type interface-number] }	可选 只有配置了 NCP-IP 子选项才能配置该子选项
配置 option 184 的子选项 Fail-Over Routing	dhcp server voice-config fail-over ip-address dialer-string { all interface interface-type interface-number [to interface-type interface-number] }	可选 只有配置了 NCP-IP 子选项才能配置该子选项
进入相应接口视图	interface interface-type interface-number	应对上面命令涉及的接口配置 IP 地址，才能创建接口地址池
配置接口 IP 地址	ip address ip-address net-mask	

说明：

该方式适用于从接口地址池中给客户端分配 IP 地址的情况。

这种配置方式可以配置接口范围，所以可以同时多个接口上配置 DHCP 支持 option 184 功能。

3. 在接口视图下配置 DHCP 服务器支持 option 184

表5-35 接口视图下配置 DHCP 服务器支持 option 184

操作	命令	说明
进入系统视图	system-view	-
进入接口视图	interface <i>interface-type</i> <i>interface-number</i>	-
配置接口 IP 地址	ip address <i>ip-address net-mask</i>	-
配置接口工作在 DHCP 服务器模式，并从接口地址池中分配地址	dhcp select interface	必选
配置 option 184 的子选项 NCP-IP	dhcp server voice-config ncp-ip <i>ip-address</i>	必选
配置 option 184 的子选项 AS-IP	dhcp server voice-config as-ip <i>ip-address</i>	可选 只有配置了 NCP-IP 子选项才能配置该子选项
配置 option 184 的子选项 Voice VLAN Configuration	dhcp server voice-config voice-vlan <i>vlan-id</i> { enable disable }	可选 只有配置了 NCP-IP 子选项才能配置该子选项
配置 option 184 的子选项 Fail-Over Routing	dhcp server voice-config fail-over <i>ip-address dialer-string</i>	可选 只有配置了 NCP-IP 子选项才能配置该子选项

 说明：

该方式适用于从接口地址池中给客户端分配 IP 地址的情况。

这种配置方式是在接口视图下配置 DHCP 支持 option 184 功能的，适用于配置单个接口支持 option 184 功能。

4. 在 DHCP 全局地址池视图下配置 DHCP 服务器支持 option 184

表5-36 DHCP 全局地址池视图下配置 DHCP 服务器支持 option 184

操作	命令	说明
进入系统视图	system-view	-
配置指定接口工作在 DHCP 服务器模式，并从 DHCP 全局地址池中分配地址	dhcp select global [subaddress] { all interface <i>interface-type</i> <i>interface-number</i> [to <i>interface-type</i> <i>interface-number</i>] }	必选
进入 DHCP 地址池视图	dhcp server ip pool <i>pool-name</i>	-

操作	命令	说明
配置动态分配的 IP 地址范围	network <i>ip-address</i> [<i>mask netmask</i>]	必选
配置 option 184 的子选项 NCP-IP	voice-config ncp-ip <i>ip-address</i>	必选
配置 option 184 的子选项 AS-IP	voice-config as-ip <i>ip-address</i>	可选 只有配置了 NCP-IP 子选项才能配置该子选项
配置 option 184 的子选项 Voice VLAN Configuration	voice-config voice-vlan <i>vlan-id</i> { <i>enable</i> <i>disable</i> }	可选 只有配置了 NCP-IP 子选项才能配置该子选项
配置 option 184 的子选项 Fail-Over Routing	voice-config fail-over <i>ip-address dialer-string</i>	可选 只有配置了 NCP-IP 子选项才能配置该子选项

 说明：

该方式适用于从 DHCP 全局地址池中给客户端分配 IP 地址的情况。

5.3.16 清除 DHCP 相关信息

在所有视图下执行 **display dhcp server ip-in-use** 命令可以查看到地址池的动态地址绑定信息，这些信息也可以通过命令清除。

在所有视图下执行 **display dhcp server conflict** 命令可以查看到 DHCP 地址冲突的统计信息，这些信息也可以通过命令清除。

在所有视图下执行 **display dhcp server statistics** 命令可以查看到 DHCP 服务器的统计信息，这些信息也可以通过命令清除。

请在用户视图下进行下列配置。

表5-37 清除 DHCP 相关信息

操作	命令
清除指定 IP 地址的绑定信息	reset dhcp server ip-in-use ip <i>ip-address</i>
清除全局地址池的动态地址绑定信息	reset dhcp server ip-in-use pool [<i>pool-name</i>]
清除接口地址池的动态地址绑定信息	reset dhcp server ip-in-use interface [<i>interface-type interface-number</i>]
清除所有地址池的地址绑定信息	reset dhcp server ip-in-use all
清除指定 IP 地址的冲突统计信息	reset dhcp server conflict ip <i>ip-address</i>
清除所有地址池的地址冲突统计信息	reset dhcp server conflict all

操作	命令
清除 DHCP 服务器的统计信息	reset dhcp server statistics

5.4 DHCP 客户端配置

DHCP 客户端的配置很简单，只需配置以太网接口通过 DHCP 方式获取地址。

请在以太网接口（包括子接口）视图下进行下列配置。

表5-38 配置 DHCP 客户端

操作	命令
配置接口通过 DHCP 方式获取 IP 地址	ip address dhcp-alloc
取消接口通过 DHCP 方式获取 IP 地址	undo ip address dhcp-alloc

缺省情况下，以太网接口未配置通过 DHCP 方式获取 IP 地址。

说明：

- 接口在配置 DHCP 动态获取 IP 地址后不再允许配置从 IP 地址，即命令 **ip address dhcp-alloc** 与命令 **ip address ip-address mask sub** 不能同时配置在一个以太网接口下，两者只能取其一。
- 若在 DHCP Server 上配置了 **gateway-list** 命令，那么防火墙在获得接口 IP 地址且接口 UP 后其路由表中会出现一条下一跳为指定网关的缺省路由。若防火墙通过 DHCP Server 获得了多个网关地址，那么防火墙在获得接口 IP 地址且接口 UP 后，将会使用第一个网关地址创建一条缺省路由，如下：

[Quidway] display ip routing-table

Routing Table: public net

Destination/Mask	Protocol	Pre	Cost	Nexthop	Interface
0.0.0.0/0	DHCPDEF	255	0	23.23.0.2	Ethernet1/0/0

该缺省路由的优先级为 255、花费为 0。

5.5 DHCP 中继配置

DHCP 中继配置包括：

- 配置接口工作在 DHCP 中继模式
- 配置 DHCP 中继指定的外部服务器地址
- 通过 DHCP 中继配置 DHCP 服务器负载分担
- 通过 DHCP 中继释放客户端的 IP 地址

- 清除 DHCP 中继的统计信息

5.5.1 配置接口工作在 DHCP 中继模式

当收到 DHCP 客户端发出的、目的地址是本机的 DHCP 报文时，可以通过配置决定如何处理这些报文。如果配置为服务器模式，则将报文转给本地 DHCP 服务器；如果配置为中继模式，则将报文转给指定的外部 DHCP 服务器。

如果配置当前接口工作在中介模式，请在接口视图下进行下列配置。

表5-39 配置当前接口工作在 DHCP 中介模式

操作	命令
将 DHCP 报文通过中介发送给外部 DHCP 服务器，由外部 DHCP 服务器分配地址	dhcp select relay
恢复缺省设置	undo dhcp select

如果同时配置多个接口工作在中介模式，请在系统视图下进行下列配置。

表5-40 配置指定范围的接口工作在 DHCP 中介模式

操作	命令
将 DHCP 报文通过中介发送给外部 DHCP 服务器，由外部 DHCP 服务器分配地址	dhcp select relay { interface ethernet-subinterface-range all }
恢复缺省设置	undo dhcp select { interface ethernet-subinterface-range all }

缺省情况下，对 DHCP 报文的处理模式为服务器模式（**global**）。

 说明：

以太网子接口支持 DHCP Relay 时，只能是子接口对子接口，也就是说客户端也必须使用子接口（此时如果是 PC 作为客户端则无法得到 IP 地址）。

5.5.2 配置 DHCP 中介指定的外部服务器地址

当配置 DHCP 中介功能时，从接口上收到的 DHCP 广播报文将被送到指定的外部 DHCP 服务器。

如果只需要在当前接口上指定外部 DHCP 服务器地址，请在接口视图下进行下列配置。

表5-41 配置当前接口的外部 DHCP 服务器地址

操作	命令
配置当前接口的外部 DHCP 服务器地址	ip relay-address <i>ip-address</i>
删除当前接口的外部 DHCP 服务器地址	undo ip relay address { <i>ip-address</i> all }

如果在指定范围的多个接口上指定外部 DHCP 服务器地址，请在系统视图下进行下列配置。

表5-42 配置指定范围的多个接口上的外部 DHCP 服务器地址

操作	命令
配置指定范围的多个接口上的外部 DHCP 服务器地址	ip relay address <i>ip-address</i> { interface <i>ethernet-subinterface-range</i> all }
删除指定范围的多个接口上的外部 DHCP 服务器地址	undo ip relay address { <i>ip-address</i> all } { interface <i>ethernet-subinterface-range</i> all }

说明：

由于 DHCP 客户端在 DHCP 的某些阶段发送的报文为广播报文，因此相应接口应当支持广播方式。

每个接口最多可以支持 20 个外部 DHCP 服务器地址。

5.5.3 通过 DHCP 中继配置 DHCP 服务器负载分担

使用 DHCP 中继功能可以配置多个 DHCP 服务器，并可以配置它们之间进行负载分担。

如果配置了多个 DHCP 服务器，DHCP 中继可以通过负载分担的方式将 DHCP 客户端的请求按 HASH 算法分给不同的 DHCP 服务器进行处理，实现多个 DHCP 服务器的负载分担。

请在系统视图下进行下列配置。

表5-43 配置 DHCP 服务器的负载分担

操作	命令
配置 DHCP 服务器的负载分担	ip relay address cycle
取消 DHCP 服务器的负载分担	undo ip relay address cycle

缺省情况下，DHCP 服务器之间不进行负载分担。

5.5.4 通过 DHCP 中继释放客户端的 IP 地址

在某些情况下，可能需要通过 DHCP 中继手工释放客户端申请到的 IP 地址。
请在接口视图或系统视图下进行下列配置。

表5-44 通过 DHCP 中继释放客户端的 IP 地址

操作	命令
向 DHCP 服务器请求释放客户端申请到的 IP 地址	dhcp relay release <i>client-ip mac-address</i>
向指定的 DHCP 服务器请求释放客户端申请到的 IP 地址	dhcp relay release <i>client-ip mac-address server-ip</i>

当不指定 DHCP 服务器时，如果在系统视图下，则向所有 DHCP 服务器发送释放申请，如果在接口视图下，向该接口下的所有中继地址发送释放申请。

 说明：

在 DHCP Relay 中配置手工释放 IP 地址后，会通知 DHCP Server 释放 DHCP ip-in-use 地址池中的地址，该 IP 地址在释放后会放入过期队列，一般情况下不会马上被分配出去；此时仅仅释放的是 DHCP ip-in-use 地址池中的地址，Client 端主机是无法真正释放该地址的，所以 Client 端主机会使用该地址直到租约超时。

5.5.5 清除 DHCP 中继的统计信息

在所有视图下执行 **display dhcp relay statistics** 命令可以查看到 DHCP 中继的统计信息，这些信息也可以通过命令清除。
请在用户视图下进行下列配置。

表5-45 清除 DHCP 中继的统计信息

操作	命令
清除 DHCP 中继的统计信息	reset dhcp relay statistics

5.6 DHCP 显示和调试

在完成上述配置后，可在所有视图下执行 **display** 命令显示配置后 DHCP 的运行情况，通过查看显示信息验证配置的效果。
在用户视图下，执行 **debugging** 命令可对 DHCP 进行调试。

1. DHCP 服务器的显示和调试

表5-46 DHCP 服务器的显示和调试

操作	命令
查看 DHCP 地址池的空闲地址信息	display dhcp server free-ip
查看 DHCP 的地址冲突统计信息	display dhcp server conflict { ip ip-address all }
查看 DHCP 地址池中超期的租约	display dhcp server expired { ip ip-address pool [pool-name] interface [interface-type interface-number] all }
查看 DHCP 的地址绑定信息	display dhcp server ip-in-use { all ip ip-address pool [pool-name] interface [interface-type interface-number] }
查看 DHCP 服务器的统计信息	display dhcp server statistics
查看 DHCP 地址池的树状结构信息	display dhcp server tree { pool [pool-name] interface [interface-type interface-number] all }
打开 DHCP 服务器的调试开关	debugging dhcp server { error event packet all }
关闭 DHCP 服务器的调试开关	undo debugging dhcp server { event packet error all }
清除 DHCP 动态地址绑定信息。	reset dhcp server ip-in-use { ip ip-address pool [pool-name] interface [interface-type interface-num] all }
清除 DHCP 地址冲突的统计信息	reset dhcp server conflict { ip ip-address all }
清除 DHCP 服务器的统计信息	reset dhcp server statistics

 说明：

DHCP 服务器的租约信息不会在执行 **save** 命令时保存到 flash 中，故系统重启或用 **reset dhcp server ip-in-use** 命令清除租约后配置文件中没有任何租约的信息，此时客户端如果发出续约请求将会被拒绝，系统会让客户端重新申请 IP 地址。

2. DHCP 中继的显示和调试

表5-47 DHCP 中继的显示和调试

操作	命令
查看 DHCP 中继的 IP 信息	display ip interface [interface-type interface-number]
查看 DHCP 中继的相关统计信息	display dhcp relay statistics
查看接口的 DHCP 中继地址配置	display dhcp relay address { interface interface-name all }
打开 DHCP 中继调试开关	debugging dhcp relay { all error event packet [client mac mac-address] }

操作	命令
关闭 DHCP 中继调试开关	undo debugging dhcp relay { all error event packet [client mac mac-address] }

3. DHCP 客户端的显示和调试

表5-48 DHCP 客户端的显示和调试

操作	命令
显示 DHCP 客户端统计信息	display dhcp client [verbose]
打开 DHCP 客户端的调试开关	debugging dhcp client { error event packet all }
关闭 DHCP 客户端的调试开关	undo debugging dhcp client { error event packet all }

5.7 DHCP 典型配置举例

5.7.1 DHCP 服务器典型配置举例

常见的 DHCP 组网方式可分为两类：一种是 DHCP 服务器和客户端都在一个子网内，直接进行 DHCP 协议的交互；第二种是 DHCP 服务器和客户端分别处于不同的子网中，则必须通过 DHCP 中继代理实现 IP 地址的分配。无论那种情况下，DHCP 的配置都是相同的。

1. 组网需求

DHCP 服务器为同一网段中的客户端动态分配 IP 地址，地址池网段 10.1.1.0/24 分为两个网段：10.1.1.0/25 和 10.1.1.128/25。DHCP 服务器两个 Ethernet 接口地址分别为 10.1.1.1/25 和 10.1.1.129/25。

网段 10.1.1.0/25 内的地址租用期限为 10 天 12 小时，域名为 h3c.com，DNS 地址为 10.1.1.2，无 NetBIOS 地址，出口防火墙地址为 10.1.1.126；网段 10.1.1.128/25 网段内的地址租用期限为 5 天，DNS 地址为 10.1.1.2，NetBIOS 地址为 10.1.1.4，出口防火墙的地址为 10.1.1.254。

2. 组网图

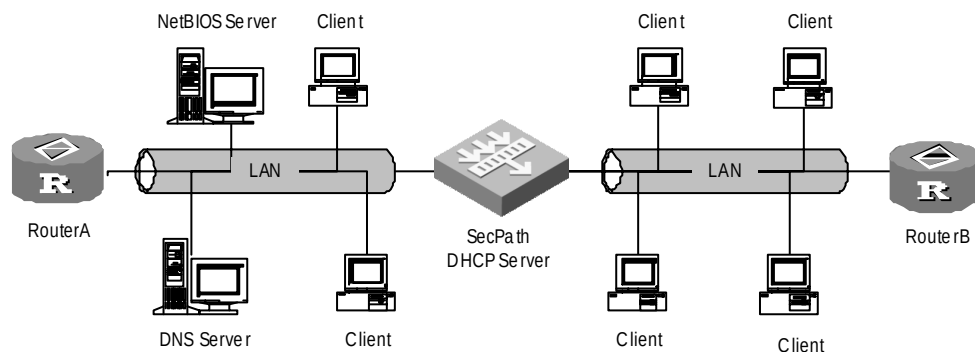


图5-6 DHCP 服务器与客户端在同一网络中

3. 配置步骤

启动 DHCP 服务。

```
[H3C] dhcp enable
```

配置不参与自动分配的 IP 地址（DNS、NetBIOS 和出口网关地址）。

```
[H3C] dhcp server forbidden-ip 10.1.1.2
```

```
[H3C] dhcp server forbidden-ip 10.1.1.4
```

```
[H3C] dhcp server forbidden-ip 10.1.1.126
```

```
[H3C] dhcp server forbidden-ip 10.1.1.254
```

配置 DHCP 地址池 0 的共有属性（地址池范围、DNS 地址）。

```
[H3C] dhcp server ip-pool 0
```

```
[H3C-dhcp-0] network 10.1.1.0 mask 255.255.255.0
```

```
[H3C-dhcp-0] dns-list 10.1.1.2
```

配置 DHCP 地址池 1 的属性（地址池范围、域名、出口网关、地址租用期限）。

```
[H3C] dhcp server ip-pool 1
```

```
[H3C-dhcp-1] network 10.1.1.0 mask 255.255.255.128
```

```
[H3C-dhcp-1] domain-name h3c.com
```

```
[H3C-dhcp-1] gateway-list 10.1.1.126
```

```
[H3C-dhcp-1] expired day 10 hour 12
```

配置 DHCP 地址池 2 的属性（地址池范围、出口网关、NetBIOS 地址、地址租用期限）。

```
[H3C] dhcp server ip-pool 2
```

```
[H3C-dhcp-2] network 10.1.1.128 mask 255.255.255.128
```

```
[H3C-dhcp-2] gateway-list 10.1.1.254
```

```
[H3C-dhcp-2] nbns-list 10.1.1.4
```

```
[H3C-dhcp-2] expired day 5
```

5.7.2 DHCP 中继典型配置举例

1. 组网需求

DHCP 客户端所在的网段为 10.110.0.0，而 DHCP 服务器所在的网段为 202.38.0.0。需要通过带 DHCP 中继功能的防火墙中继 DHCP 报文，使得 DHCP 客户端可以从 DHCP 服务器上申请到 IP 地址等相关配置信息。

DHCP 服务器应当分配一个 10.110.0.0 网段的 IP 地址池，以便将适当的 IP 地址分配给该网段上的 DHCP 客户端，并且 DHCP 服务器上应当配置有到 10.110.0.0 网段的路由。

2. 组网图

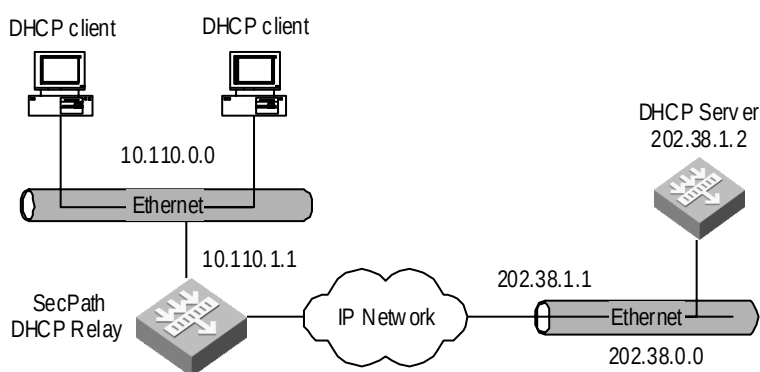


图5-7 DHCP 中继配置

3. 配置步骤

配置防火墙：

使能 DHCP 服务

```
[H3C] dhcp enable
```

进入要实现 DHCP 中继功能的接口，为其配置 IP 地址和地址掩码以使其和 DHCP 客户端属于同一个网段

```
[H3C] interface ethernet 0/0/0
```

```
[H3C-Ethernet0/0/0] ip address 10.110.1.1 255.255.0.0
```

为该接口配置 IP 中继地址以指明 DHCP 服务器的位置

```
[H3C-Ethernet0/0/0] dhcp select relay
```

```
[H3C-Ethernet0/0/0] ip relay address 202.38.1.2
```

DHCP 服务器的配置略。

5.7.3 DHCP 客户端典型配置举例

介绍两种 DHCP 客户端典型配置：一种是以以太网主接口动态获取 IP 地址；第二种是以以太网子接口动态获取 IP 地址(支持 VLAN)。

1. 以太网主接口作 DHCP 客户端

(1) 组网需求

防火墙 SecPathA 的以太网口 Ethernet1/0/0、Ethernet2/0/0 分别接入 LAN1、LAN2 中，在两个 LAN 中分别有 DHCP 服务器 server1、server2（都是防火墙）。LAN1 所在网段为 200.254.0.0/16，LAN2 所在网段为 172.10.0.0/16，要求配置防火墙 SecPathA 的上述两个以太网口通过 DHCP 的方式获取地址。

(2) 组网图

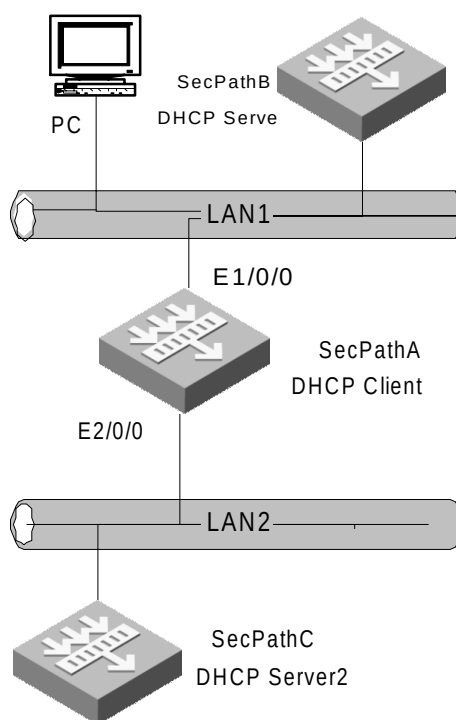


图5-8 主接口作 DHCP 客户端

(3) 配置步骤

以下同时列出 DHCP 服务器和客户端的配置过程。

配置 server1。

```
[H3C] dhcp enable
[H3C] interface ethernet0/0/0
[H3C -Ethernet0/0/0] ip address 200.254.0.1 16
[H3C] dhcp server ip-pool 1
[H3C -dhcp1] network 200.254.0.0 mask 255.255.0.0
```

配置 server2。

```
[H3C] dhcp enable
[H3C] interface ethernet0/0/0
[H3C-Ethernet0/0/0] ip address 172.10.0.1 16
[H3C] dhcp server ip-pool 2
[H3C-dhcp2] network 172.10.0.0 mask 255.255.0.0
```

配置 SecPathA 的 Ethernet1/0/0 通过 DHCP 动态获取地址。

```
[H3C] interface ethernet1/0/0
[H3C-Ethernet1/0/0] ip address dhcp-alloc
```

配置 SecPathA 的 Ethernet2/0/0 通过 DHCP 动态获取地址。

```
[H3C] interface ethernet2/0/0
[H3C-Ethernet2/0/0] ip address dhcp-alloc
```

2. 以太网子接口动态获取 IP 地址

(1) 组网需求

DHCP 服务器 1 和 2 分别接在不同的 VLAN 中，server1 在 VLAN10，server2 在 VLAN20，要求在 SecPath（DHCP client）的以太网 Ethernet0/0/0 上创建子接口，并分别从上述两个 DHCP 服务器中动态获取 IP 地址。

(2) 组网图

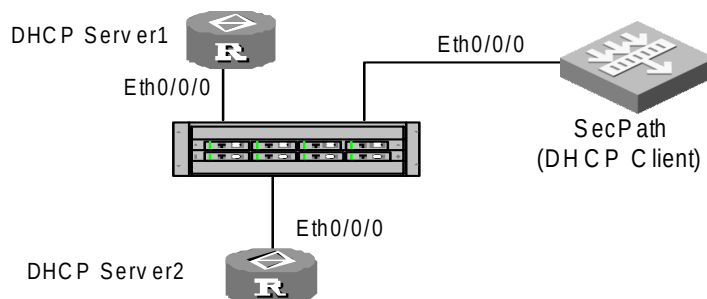


图5-9 子接口作 DHCP 客户端

(3) 配置步骤

LANSWITCH 的配置不在此列出，但要保证 sever1 接入到 VLAN10 中，server2 接入到 VLAN20 中，在防火墙上的作为 DHCP client 的端口配置为 TRUNK 端口，并能透传 vlan id 为 10 和 20 的报文。

DHCP 服务器 server1、server2 的配置过程同上例，以下仅列出 DHCP 客户端的配置过程。

配置从 server1 获取地址的子接口

```
[H3C] interface ethernet0/0/0.1
[H3C-Ethernet0/0/0.1] vlan-type dot1q vid 10
```

```
[H3C-Ethernet0/0/0.1] ip addr dhcp-alloc
# 配置从 server2 获取地址的子接口
[H3C] interface ethernet0/0/0.2
[H3C-Ethernet0/0/0.2] vlan-type dot1q vid 20
[H3C-Ethernet0/0/0.2] ip addr dhcp-alloc
```

5.7.4 DHCP Accounting 配置举例

1. 组网需求

- DHCP Server 通过 Ethernet1/0/0 和 Ethernet1/0/1 分别连接 DHCP Client 及 RADIUS Server。
- RADIUS Server 的 IP 地址为 10.1.2.2/24。
- DHCP Server 启动了 DHCP Accounting 功能。DHCP 全局地址池为 10.1.1.0，DHCP Server 作为 RADIUS Client 采用 AAA 方式进行认证

2. 组网图

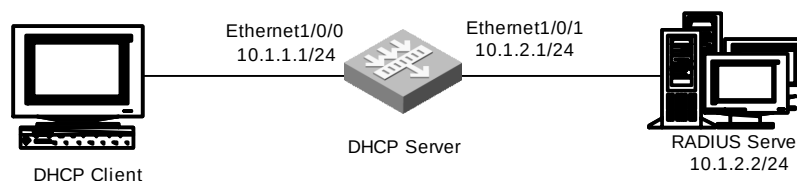


图5-10 DHCP Accounting 配置举例组网图

3. 配置步骤

配置 DHCP Server 的网络参数

```
<H3C> system-view
[H3C] interface Ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 10.1.1.1 255.255.255.0
[H3C-Ethernet1/0/0] quit
[H3C] interface Ethernet 1/0/1
[H3C-Ethernet1/0/1] ip address 10.1.2.1 255.255.255.0
[H3C-Ethernet1/0/1] quit
```

配置 Domain、创建 RADIUS 方案并配置 Domain 和 RADIUS 关联

```
[H3C] radius scheme 123
[H3C-radius-123] primary authentication 10.1.2.2
[H3C-radius-123] primary accounting 10.1.2.2
[H3C] domain 123
[H3C-isp-123] scheme radius-scheme 123
[H3C-isp-123] quit
```

配置 DHCP server 的地址池

```
[H3C] dhcp server ip-pool test
```

```
[H3C-dhcp-pool-test] network 10.1.1.0 mask 255.255.255.0
```

配置 DHCP Accounting

```
[H3C-dhcp-pool-test] accounting domain 123
```

5.7.5 IP 电话请求 option 184 组网案例

1. 组网需求

IP 电话作为 DHCP 客户端从 DHCP 服务器请求 option 184 的所有子选项配置，防火墙作为 DHCP 服务器，并在全局地址池下配置支持 option 184 功能。其中 NCP-IP 地址为 3.3.3.3; Alternate Server IP 地址为 2.2.2.2; 使能语音 VLAN，且语音 VLAN ID 为 1。Fail-Over IP 地址为 1.1.1.1，呼叫号码为 99*。

2. 组网图

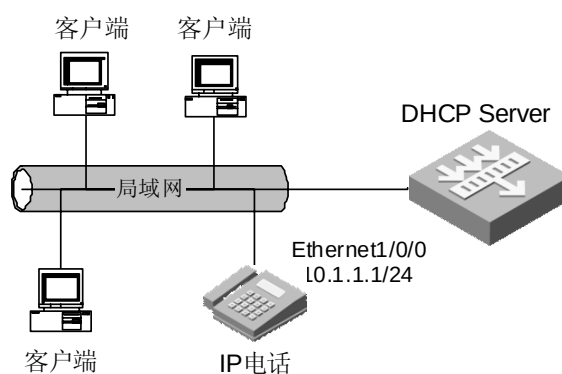


图5-11 option184 组网图

3. 配置步骤

(1) DHCP 客户端配置

作为 DHCP 客户端的 IP 电话使能 DHCP Client 功能，并配置请求 option 184 的所有子选项，配置过程略。

(2) DHCP 服务器配置

```
<H3C>
```

```
<H3C> system-view
```

```
[H3C] dhcp select global interface ethernet 1/0/0
```

```
[H3C] dhcp server ip-pool 123
```

```
[H3C-dhcp-pool-123] network 10.1.1.1 mask 255.255.255.0
```

```
[H3C-dhcp-pool-123] voice-config as-ip 2.2.2.2
```

```
[H3C-dhcp-pool-123] voice-config ncp-ip 3.3.3.3
```

```
[H3C-dhcp-pool-123] voice-config voice-vlan 1 enable
```



```
[H3C-dhcp-pool-123] voice-config fail-over 1.1.1.1 99*  
[H3C-dhcp-pool-123] quit
```

第6章 IP 性能配置

6.1 配置接口最大传输单元（MTU）

接口最大传输单元决定了在该接口上的报文是否需要分片。

请在接口视图下进行下列操作。

表6-1 配置接口最大传输单元

操作	命令
配置接口最大传输单元	mtu mtu-size
恢复接口最大传输单元的缺省值	undo mtu

接口最大传输单元的缺省值为 1500 字节。

6.2 配置 TCP 报文分片

该命令用来配置 TCP 最大报文分片的长度，这个长度决定了该接口上的 TCP 报文是否需要分片。

请在接口视图下进行下列操作。

表6-2 配置 TCP 报文分片

操作	命令
配置 TCP 报文分片	tcp mss value
取消 TCP 报文分片	undo tcp mss

缺省情况下，TCP 报文不分片。

6.3 配置 TCP 属性

可以配置的 TCP 属性包括：

- **synwait 定时器**：当发送 syn 报文时，TCP 启动 synwait 定时器，若 synwait 超时前未收到回应报文，则 TCP 连接将被终止。synwait 定时器的超时时间取值范围为 2～600 秒，缺省值为 75 秒。

- **finwait 定时器：**当 TCP 的连接状态由 FIN_WAIT_1 变为 FIN_WAIT_2 时启动 finwait 定时器，若 finwait 定时器超时前仍未收到 FIN 报文，则 TCP 连接被终止。finwait 的取值范围为 76~3600 秒，finwait 的缺省值为 675 秒。
- **面向连接 Socket 的接收和发送缓冲区的大小：**范围为 1~32K 字节，缺省值为 8K 字节。

请在系统视图下进行下列配置。

表6-3 配置 TCP 属性

操作	命令
配置 TCP 连接建立 synwait 定时器时间	tcp timer syn-timeout <i>time-value</i>
恢复 TCP 连接建立 synwait 定时器时间为缺省值	undo tcp timer syn-timeout
配置 TCP 的 FIN_WAIT_2 定时器时间	tcp timer fin-timeout <i>time-value</i>
恢复 TCP 的 FIN_WAIT_2 定时器时间为缺省值	undo tcp timer fin-timeout
配置 TCP 的 Socket 接收和发送缓冲区的大小	tcp window <i>window-size</i>
恢复 TCP 的 Socket 接收和发送缓冲区的大小为缺省值	undo tcp window

缺省情况下，TCP finwait 定时器缺省为 675 秒，TCP synwait 定时器缺省值为 75 秒，面向连接 Socket 的收发缓冲区大小缺省为 8K 字节。

6.4 配置 ICMP 发送重定向报文

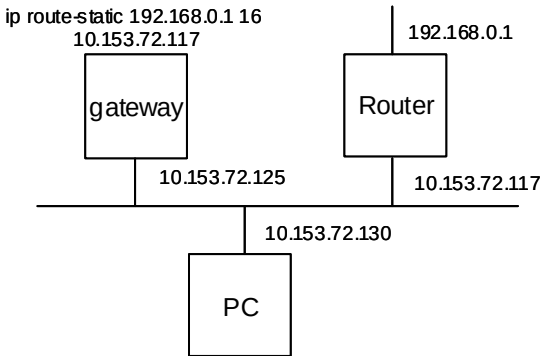


图6-1 配置 ICMP 发送重定向报文示意图

如上图示连接情况，PC 要发送报文到 Router，会先将报文发送到网关，再由网关转发给 Router。这种情况下可以在网关上使能 ICMP 发送重定向报文功能，这样网关会发送重定向报文给 PC，使 PC 直接将报文发送给 Router。

请在系统视图下进行下列配置。

表6-4 配置 ICMP 发送重定向报文

操作	命令
打开 ICMP 发送重定向报文功能	icmp redirect send
关闭 ICMP 发送重定向报文功能	undo icmp redirect send

缺省情况下，打开 ICMP 发送重定向报文功能。

6.5 IP 性能显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示 IP 性能配置后的运行情况，通过查看显示信息验证配置的效果。

执行 **reset** 命令可以清除该运行情况的统计信息。

在用户视图下，执行 **debugging** 命令可以对 IP 性能进行调试。

表6-5 IP 性能显示和调试

操作	命令
显示 TCP 连接状态	display tcp status
显示 TCP 流量统计信息	display tcp statistics
显示 UDP 流量统计信息	display udp statistics
显示系统当前所有的套接口信息	display ip socket [socktype sock_type] [task_id socket_id]
显示 IP 层接口表信息	display ip interface [interface-type interface-number]
显示接口板的 FIB 表	display fib
据正则表达式输出缓冲区中与包含字符串 <i>text</i> 相关的行	display fib { begin include exclude } <i>text</i>
过滤显示 FIB 信息	display fib acl <i>acl-number</i>
按照目的地址进行匹配显示 FIB 表项	display fib <i>dest-addr1</i> [<i>dest-mask1</i>] [longer]
显示目的地址在输入的 <i>dest-addr1</i> <i>dest-mask1</i> 到 <i>dest-addr2</i> <i>dest-mask2</i> 范围内的 FIB 表项	display fib <i>dest-addr1</i> <i>dest-mask1</i> <i>dest-addr2</i> <i>dest-mask2</i>
根据所输入的 <i>ip-prefix</i> 名字，把通过了该过滤规则的 FIB 表项按照一定格式显示出来	display fib ip-prefix <i>listname</i>
显示 FIB 表项的总数目	display fib statistics
打开 IP 报文调试信息开关	debugging ip packet [<i>acl</i> <i>acl-number</i>]
关闭 IP 报文调试信息开关	undo debugging ip packet
打开 ICMP 调试信息开关	debugging ip icmp

操作	命令
关闭 ICMP 调试信息开关	undo debugging ip icmp
打开 TCP 报文调试信息开关	debugging tcp packet [task_id socket_id]
关闭 TCP 报文调试信息开关	undo debugging tcp packet [task_id socket_id]
打开 UDP 报文的调试信息开关	debugging udp packet [task_id socket_id]
关闭 UDP 报文的调试信息开关	undo debugging udp packet [task_id socket_id]
打开 TCP 事件的调试开关	debugging tcp event [task_id socket_id]
关闭 TCP 事件的调试开关	undo debugging tcp event [task_id socket_id]
打开 TCP 连接的 MD5 认证调试开关	debugging tcp md5
关闭 TCP 连接的 MD5 认证调试开关	undo debugging tcp md5
清除 IP 统计信息	reset ip statistics
清除 TCP 流量统计信息	reset tcp statistics
清除 UDP 流量统计信息	reset udp statistics

说明：

当前版本尚不支持共同使用多种过滤方式查看 FIB 的信息。

6.6 快速转发配置

6.6.1 快速转发简介

报文转发效率是衡量防火墙性能的一项关键指标。按照常规流程，防火墙在一个报文到达后，将它从接口存储器拷贝至主 CPU 中，CPU 从 IP 地址中确定网络号，查找路由表以确定一条最佳的路径将报文转发出去，同时还为报文建立合适输出的 MAC 帧。建好后的 MAC 帧通过 DMA（直接内存访问）拷贝到输出队列中，这个过程两次经过主系统总线。每一个报文的转发都要重复这个过程。

快速转发是采用高速缓存来处理报文，采用了基于数据流的技术。我们知道在 Internet 网上的数据基本上都是基于数据流的。一个数据流就是指在网上两个特定主机之间的一次特定的应用，比如一次 FTP 操作传输一个文件。我们一般用一个 5 元组描述一个数据流：源 IP 地址、源端口号、目的 IP 地址、目的端口号、协议号。当一个数据流的第一个报文通过查找路由表转发后，在高速缓存中生成相应的交换信息，后续相同的报文的转发，就可以通过直接查找高速缓存来实现转发。这样便

大大缩减了 IP 报文的排队流程，减少路由查找时间，提高 IP 报文的转发吞吐量。由于高速缓存中的转发表已经做过优化，因此查找速度将大大提高。

Comware 实现的快速转发，具有下列特性：

- 支持在各类高速链路接口上（包括子接口）提供快速转发，包括以太网、同步 PPP、帧中继、HDLC 等。
- 支持在配置了普通防火墙的情况下，提供快速转发的功能。
- 支持在配置了 ASPF 防火墙的情况下，提供快速转发的功能。
- 支持在配置了地址转换的情况下，提供快速转发的功能。
- 支持在配置了 GRE 的情况下，提供快速转发的功能
- 能大幅度提高报文的转发效率。

快速转发的性能有时会受到某些特性的影响，比如报文的队列管理，报文头压缩等。另外，快速转发能处理已经分片的 IP 报文，但不支持对 IP 报文的再分片。

6.6.2 快速转发配置

用户可根据需要禁止快速转发，如对报文转发要求使用负载分担时，要在相应方向上禁止接口进行快速转发。

请在接口视图下进行下列配置。

表6-6 允许/禁止接口进行快速转发

操作	命令
允许接口双向进行快速转发	ip fast-forwarding
允许在入接口方向上进行快速转发	ip fast-forwarding inbound
允许在出接口方向上进行快速转发	ip fast-forwarding outbound
禁止接口进行快速转发	undo ip fast-forwarding [inbound outbound]

缺省情况下，接口在入/出的双向上都使能快速转发。

**注意：**

- 如果要求对报文转发使用负载分担，必须在相应方向上禁止接口进行快速转发。
- 在接口上配置了快速转发后，该接口将不再发送 ICMP 重定向报文。
- 在接口上配置了快速转发后，该接口上的 IP 报文的调试信息将不再输出，即命令 **debugging ip packet** 不起作用。
- 当在接口上配置了快速转发且应用了包过滤防火墙后，ACL 只对数据流（即相同五元组的报文）的首包进行检查。若允许报文通过则建立快速转发表项，之后匹配此快转表项的报文将不再经过 ACL 的检查，只对 ACL 的计数器进行添加。当同一数据流（即相同五元组的报文）中的报文拥有不同的五元组以外的字段值时（例如 ToS、DSCP 等），这些报文也将被视为同一数据流，并根据快转表项进行转发。故当在 ACL 规则中配置了对同一条数据流的不同五元组以外字段值的不同操作时，需要关闭快速转发功能。

6.6.3 快速转发的显示和调试

表6-7 快速转发的显示和调试

操作	命令
显示快速转发表信息	display ip fast-forwarding cache [ip-address]
清除快速转发缓冲区中的内容	reset ip fast-forwarding cache

6.7 IP 性能配置排错

故障之一：TCP 和 UDP 协议不能正常工作。

故障排除：可以打开相应的调试开关，查看调试信息。

- 用 **debugging udp packet** 命令打开 UDP 调试开关，跟踪 UDP 的数据包。
当防火墙发送或接收到 UDP 数据包，就可以实时显示出数据报的内容格式。
根据数据报的内容，来发现问题之所在。

以下为 UDP 数据报的格式：

*0.377770-SOCKET-8-UDP:

```
1043494431: Output: task = ROUT(6), socketid = 3,  
src = 1.1.1.1:520, dst = 255.255.255.255:520, datalen = 24
```

- 用 **debugging tcp packet** 命令打开 TCP 调试开关，跟踪 TCP 的数据包。TCP 可以有两种数据报的格式供选择。一种是调试跟踪所有以本设备为一端的 TCP 连接的 TCP 报文收发。操作如下：

```
[H3C] info-center enable
```

```
[H3C] quit
<H3C> debugging tcp packet
```

即可实时查看接收或发送的 TCP 报文，其具体报文格式如下：

```
*0.100070-SOCKET-8-TCP PACKET:
1043204051:  Input: Co0(5) socketId = 2, state = SYN_SENT,
src = 127.0.0.1:1025, dst = 2.2.2.2:23,
seq = 11084380, ack = 0, optlen = 4, flag = SYN ,
window = 8192
```

另外一种调试跟踪其中 SYN、FIN 或 RST 置位的报文。

操作如下：

```
[H3C] info-center enable
[H3C] quit
<H3C> debugging tcp event
```

这样即可实时查看接收或发送的 TCP 报文，其具体报文格式同上。

第7章 IP 单播策略路由配置

7.1 IP 单播策略路由简介

与单纯依照 IP 报文的目的地址查找路由表进行转发不同，策略路由是一种依据用户制定的策略进行路由选择的机制。本系统的策略路由支持基于到达报文的源地址、地址长度等信息，灵活地指定路由。

本系统的策略路由配置需要做两方面的工作，一是定义那些需要使用策略路由的报文，二是为这些报文指定路由，这可以通过对一个 **route-policy** 的定义来实现。**route-policy** 的配置在用作策略路由的定义时，**if-match** 子句定义了那些需要使用策略路由的报文，当报文满足 **route-policy** 中的 **if-match** 子句时，则执行策略中的 **apply** 子句，以完成报文的转发。

一个 **route-policy** 由若干节点组成，每一节点由一些 **if-match** 子句和 **apply** 子句组成。**if-match** 子句定义该节点的匹配规则，**apply** 子句定义通过该节点过滤后进行的动作。

节点的 **if-match** 子句之间的过滤关系是“与”的关系，即报文必须满足该节点的所有 **if-match** 子句，才会执行 **apply** 子句。目前 **route-policy** 提供了两种 **if-match** 子句，分别为 **if-match packet-length** 和 **if-match acl**；提供了 5 种 **route-policy** 的 **apply** 子句：**apply ip-precedence**，**apply output-interface**，**apply ip-address next-hop**，**apply default output-interface**，**apply ip-address default next-hop**。在满足所有 **if-match** 子句的情况下，**apply** 子句执行情况如下：

- 配置优先级：**apply ip-precedence**，只要配置了该子句，该子句就一定会执行；
- 配置出接口和下一跳：**apply output-interface** 和 **apply ip-address next-hop**，其中 **apply output-interface** 命令的优先级高于 **apply ip-address next-hop**。当两条命令同时配置并且都有效时，系统只会执行 **apply output-interface** 命令；
- 配置缺省出接口和下一跳：**apply default output-interface** 和 **apply ip-address default next-hop**，同样，**apply default output-interface** 命令的优先级高于 **apply ip-address default next-hop**。当两条命令同时配置并且都有效时，系统只会执行 **apply default output-interface** 命令。执行缺省出接口和下一跳命令的前提是，在策略路由中报文没有配置出接口或者下一

跳，或者配置的出接口和下一跳无效，并且报文在路由表中没有查找到相应的路由，这时才会使用策略路由配置的缺省下一跳或者出接口。

本系统提供的策略路由可以分为接口策略路由和本地策略路由。前者在接口视图下配置（应用于报文到达的接口上），作用于到达该接口的报文；后者在系统视图下配置，对本机产生的报文进行策略路由。对于一般转发和安全等方面的使用需求，大多数情况下使用的是接口策略路由。

策略路由可应用于安全、负载分担等目的。

7.2 IP 单播策略路由的配置

IP 单播策略路由配置包括：

- 创建策略
- 定义 Route-policy 的 **if-match** 子句
- 定义 Route-policy 的 **apply** 子句
- 使能/禁止本地策略路由
- 使能/禁止接口策略路由

7.2.1 创建策略

由策略名称指定的策略可以包含若干策略点，每个策略点由 *sequence-num* 来指定，*sequence-num* 的值越小优先级越高，其定义的策略会被先执行。该策略可以用来引入路由以及对 IP 报文转发进行策略路由。该策略的具体内容由 **if-match** 和 **apply** 子句来指定。

请在系统视图下进行下列配置。

表7-1 创建策略

操作	命令
创建策略或一个策略节点	route-policy <i>policy-name</i> { permit deny } node <i>sequence-number</i>
删除策略或一个策略节点	undo route-policy <i>policy-name</i> [permit deny node <i>sequence-number</i>]

permit 表示满足匹配条件的报文进行策略路由；**deny** 表示满足匹配条件的报文不进行策略路由。

缺省情况下，没有 **route-policy** 和相关的节点设置被定义。

7.2.2 设置 Route-policy 的 if-match 子句

if-match 子句用来匹配需要使用策略路由的报文。IP 单播策略路由提供两种 **if-match** 子句，**if-match packet-length** 子句和 **if-match acl** 子句。一条策略节点中可以包含多条 **if-match** 子句，子句之间是“与”的关系。

请在 **route-policy** 视图下进行下列配置。

表7-2 设置 Route-policy 的 if-match 子句

操作	命令
设置 IP 报文长度匹配条件	if-match packet-length <i>min-len max-len</i>
设置 IP 地址匹配条件	if-match acl <i>acl-number</i>

缺省情况下，没有 **if-match** 子句被定义。

7.2.3 设置 Route-policy 的 apply 子句

请在 **route-policy** 视图下进行下列配置。

IP 策略路由提供五种 **apply** 子句：**apply ip-precedence**，**apply output-interface**，**apply ip-address next-hop**，**apply default output-interface**，**apply ip-address default next-hop**。一条策略节点中可以包含多条 **apply** 子句，系统按配置顺序执行 **apply** 子句（无效的子句会跳过，继续去执行下一个子句）；当执行了一条有效的子句后，该策略即实施完毕。

表7-3 设置 Route-policy 的 apply 子句

操作	命令
设置报文的优先级	apply ip-precedence <i>precedence</i>
设置报文的发送接口	apply output-interface <i>interface-type interface-number</i> [<i>interface-type interface-number</i>]
设置报文的下一跳	apply ip-address next-hop <i>ip-address</i> [<i>ip address</i>]
设置报文缺省发送接口	apply default output-interface <i>interface-type interface-number</i> [<i>interface-type interface-number</i>]
设置报文缺省下一跳	apply ip-address default next-hop <i>ip-address</i> [<i>ip address</i>]

用户可指定多个下一跳或者设置多个出接口，此时，报文的转发将在多个合法参数中负载分担，即轮流在每一个下一跳或者出接口上发送一个报文。以上叙述只对于同种配置的多个参数有效，如果同时配置了出接口和下一跳，仅在出接口的设置中进行负载分担。

缺省情况下，没有 **apply** 子句被定义。

 说明：

配置策略路由的 **apply** 子句时，对于点到点接口（如虚拟点对点 Tunnel 接口和封装了 PPP 协议的 Dialer 接口），既可以设置报文的发送接口也可以设置下一跳；对于广播类型或 NBMA 类型的接口（如 Ethernet 接口），支持点到多点，则必须设置报文的下一跳地址。

7.2.4 使能/禁止本地策略路由

在系统视图下使能/禁止本地策略路由。最多只能配置一条本地策略。

表7-4 使能/禁止本地策略路由

操作	命令
使能本地策略路由	ip local policy route-policy <i>policy-name</i>
禁止本地策略路由	undo ip local policy route-policy <i>policy-name</i>

缺省情况下，禁止本地策略路由。

7.2.5 使能/禁止接口策略路由

在指定接口上使能/禁止策略路由。每个接口最多配置一个策略。

请在接口视图下进行下列配置。

表7-5 使能/禁止接口策略路由

操作	命令
使能接口策略路由	ip policy route-policy <i>policy-name</i>
禁止接口策略路由	undo ip policy route-policy <i>policy-name</i>

缺省情况下，禁止接口策略路由。

7.3 IP 单播策略路由显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示 IP 单播策略路由配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **debugging** 命令可以对 IP 单播策略路由进行调试。

表7-6 表 IP 单播策略路由显示和调试

操作	命令
显示本地和接口设置的策略路由的策略	display ip policy
显示本地策略路由的设置情况	display ip policy setup local
显示接口策略路由的设置情况	display ip policy setup interface <i>interface-type interface-number</i>
显示本地策略路由报文的统计信息	display ip policy statistic local
显示接口策略路由报文的统计信息	display ip policy statistic interface <i>interface-type interface-number</i>
打开策略路由的调试开关	debugging ip policy

7.4 IP 单播策略路由典型配置举例

7.4.1 配置基于源地址的策略路由

1. 配置需求

定义名为 **aaa** 的策略，控制所有从以太网口 **E2/0/0** 接收的 **TCP** 报文，使用接口 **Ethernet1/0/0** 发送，对其它报文，仍然按照查找路由表的方式进行转发。

- 5 号节点，表示匹配 **ACL 3101** 的以太网报文将被发往下一跳地址 **1.1.1.2**；
- 10 号节点，表示匹配 **ACL 3102** 的任何报文不做策略路由处理；

来自 **Ethernet2/0/0** 的报文将依次试图匹配 5、10 号节点的 **if-match** 子句。如果匹配了 **permit** 语句的节点，执行相应的 **apply** 子句；如果匹配了 **deny** 语句的节点，退出策略路由处理。

2. 组网图

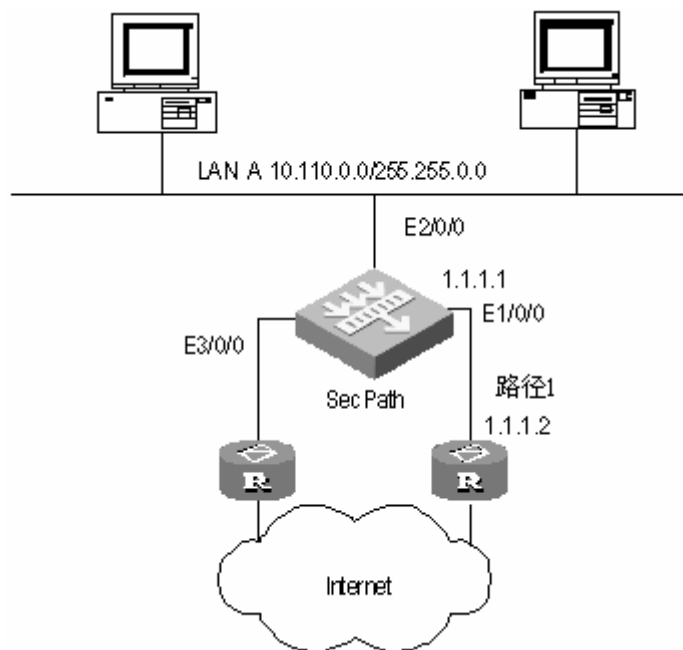


图7-1 配置基于源地址的策略路由组网图

3. 配置步骤

定义访问控制列表。

```
[H3C] acl number 3101
[H3C-acl-adv-3101] rule permit tcp
[H3C-acl-adv-3101] quit
[H3C] acl number 3102
[H3C-acl-adv-3102] rule permit ip
[H3C-acl-adv-3102] quit
```

定义 5 号节点，使匹配 ACL 3101 的任何 TCP 报文被发往下一跳地址 1.1.1.2。

```
[H3C] route-policy aaa permit node 5
[H3C-route-policy] if-match acl 3101
[H3C-route-policy] apply ip-address next-hop 1.1.1.2
[H3C-route-policy] quit
```

定义 10 号节点，表示匹配 ACL 3102 的报文不做策略路由处理。

```
[H3C] route-policy aaa deny node 10
[H3C-route-policy] if-match acl 3102
[H3C-route-policy] quit
```

在以太网口上应用策略 aaa。

```
[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip policy route-policy aaa
```

7.4.2 配置基于报文大小的策略路由

1. 配置需求

SecPathA 将大小为 64~100 字节的报文从 ethernet 2/0/0 发送；而将大小为 101~1000 字节的报文从 ethernet 2/0/1 发送；所有其它长度的报文均按正常方式路由。

在 SecPathA 的 E1/0/0 接口上应用 IP 策略路由 lab1。这个策略将大小为 64~100 字节的报文设置 150.1.1.2 作为下一转发 IP 地址；而将大小为 101~1000 字节的报文设置 151.1.1.2 作为下一转发 IP 地址。所有其它长度的报文都按基于目的地址的路由方法路由。

2. 组网图

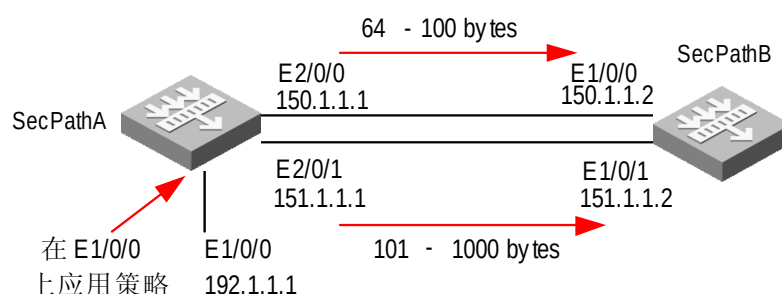


图7-2 配置基于报文大小的策略路由组网图

3. 配置步骤

配置 SecPath A

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 192.1.1.1 255.255.255.0
[H3C-Ethernet1/0/0] ip policy route-policy lab1
[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 150.1.1.1 255.255.255.0
[H3C] interface ethernet 2/0/1
[H3C-Ethernet2/0/1] ip address 151.1.1.1 255.255.255.0
[H3C] rip
[H3C-rip] network 192.1.1.0
[H3C-rip] network 150.1.0.0
[H3C-rip] network 151.1.0.0
[H3C] route-policy lab1 permit node 10
[H3C-route-policy] if-match packet-length 64 100
[H3C-route-policy] apply ip-address next-hop 150.1.1.2
[H3C] route-policy lab1 permit node 20
[H3C-route-policy] if-match packet-length 101 1000
[H3C-route-policy] apply ip-address next-hop 151.1.1.2
```

配置 SecPath B

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 150.1.1.2 255.255.255.0
[H3C] interface ethernet 1/0/1
[H3C-Ethernet1/0/1] ip address 151.1.1.2 255.255.255.0
[H3C] rip
[H3C-rip] network 150.1.0.0
[H3C-rip] network 151.1.0.0
```

在 SecPathA 用 **debugging ip policy** 命令监视策略路由。注意 64 字节的报文与路由策略 lab1 的序号为 10 的入口项匹配，因此向 150.1.1.2 转发。

```
<H3C> debugging ip policy
*0.483448-POLICY-8-POLICY-ROUTING:IP Policy routing success : next-hop :
150.1.1.2
```

在 SecPathA，改变报文长为 101 字节，再用 **debugging ip policy** 命令监视策略路由。注意 101 字节的报文与路由策略 lab1 的序号为 20 的入口项匹配，从而向 151.1.1.2 转发。

```
<H3C> debugging ip policy
*0.483448-POLICY-8-POLICY-ROUTING:IP Policy routing success : next-hop :
151.1.1.2
```

在 SecPathA，改变报文长为 1001 字节，再用 **debugging ip policy** 命令监视策略路由。注意这个报文不匹配 lab1 中的任何入口项，所以按正常方式转发，策略路由没有输出转发报文的调试信息。

目 录

第 1 章 IP路由协议概述	1-1
1.1 IP路由和路由表介绍	1-1
1.1.1 路由和路由段	1-1
1.1.2 通过路由表进行选路	1-1
1.2 路由管理策略	1-3
1.2.1 路由协议及其发现路由的优先级	1-3
1.2.2 对负载分担与路由备份的支持	1-4
1.2.3 路由协议之间的共享	1-4
第 2 章 静态路由配置	2-1
2.1 静态路由简介	2-1
2.1.1 静态路由	2-1
2.1.2 缺省路由	2-1
2.2 静态路由配置	2-2
2.2.1 配置静态路由	2-2
2.2.2 配置缺省路由	2-3
2.2.3 删除全部静态路由	2-4
2.3 路由表的显示和调试	2-4
2.4 静态路由典型配置举例	2-5
2.5 静态路由配置的故障诊断与排除	2-6
第 3 章 RIP配置	3-1
3.1 RIP简介	3-1
3.1.1 RIP的工作机制	3-1
3.1.2 RIP的启动和运行过程	3-2
3.1.3 Comware支持的RIP特性	3-2
3.2 RIP配置	3-3
3.2.1 启动RIP	3-4
3.2.2 在指定网段使能RIP	3-4
3.2.3 配置RIP报文定点传送	3-5
3.2.4 配置水平分割	3-5
3.2.5 配置附加路由权	3-6
3.2.6 配置RIP的路由引入	3-6
3.2.7 配置RIP的路由过滤	3-7
3.2.8 禁止RIP接收主机路由	3-8
3.2.9 配置RIP的路由聚合	3-8
3.2.10 配置RIP非直连邻居的路由交互	3-8

3.2.11 配置RIP在接口间实现负载分担功能.....	3-10
3.2.12 配置RIP优先级	3-10
3.2.13 配置RIP定时器	3-10
3.2.14 配置RIP的零域检查	3-11
3.2.15 配置接口的RIP版本	3-11
3.2.16 配置RIP报文认证.....	3-12
3.2.17 配置接口的工作状态.....	3-13
3.2.18 复位RIP协议的系统配置参数.....	3-13
3.2.19 配置RIP多实例	3-13
3.3 RIP显示和调试.....	3-14
3.4 RIP典型配置举例	3-14
3.4.1 配置指定接口的工作状态.....	3-14
3.4.2 调整RIP网络的收敛时间.....	3-16
3.4.3 RIP非直连邻居的路由交互配置举例.....	3-17
3.5 RIP故障诊断与排除.....	3-20
第4章 OSPF配置.....	4-1
4.1 OSPF简介	4-1
4.1.1 OSPF概述	4-1
4.1.2 OSPF的路由计算过程	4-1
4.1.3 OSPF相关的基本概念	4-2
4.1.4 OSPF的协议报文.....	4-4
4.1.5 OSPF的LSA类型	4-5
4.1.6 Comware支持的OSPF特性	4-6
4.2 OSPF的配置	4-7
4.2.1 配置Router ID	4-8
4.2.2 启动OSPF	4-9
4.2.3 进入OSPF区域视图	4-9
4.2.4 在指定网段使能OSPF	4-10
4.2.5 配置OSPF虚连接.....	4-10
4.2.6 配置OSPF网络类型	4-11
4.2.7 配置邻接点	4-12
4.2.8 配置OSPF的路由引入	4-12
4.2.9 在OSPF中生成缺省路由.....	4-14
4.2.10 配置OSPF的路由过滤	4-15
4.2.11 配置OSPF的路由聚合	4-16
4.2.12 配置OSPF优先级	4-17
4.2.13 配置OSPF定时器	4-18
4.2.14 配置选举DR时的优先级.....	4-19
4.2.15 配置接口发送报文的开销.....	4-20
4.2.16 配置OSPF的SPF计算间隔	4-21
4.2.17 配置发送链路状态更新报文所需时间	4-21

4.2.18 配置接口发送DD报文时是否填充MTU值.....	4-22
4.2.19 配置OSPF等价路由的最大个数.....	4-22
4.2.20 配置OSPF认证	4-22
4.2.21 配置接口的工作状态.....	4-23
4.2.22 配置OSPF的STUB区域.....	4-24
4.2.23 配置OSPF的NSSA区域.....	4-25
4.2.24 配置OSPF与网管系统的配合	4-27
4.2.25 重启OSPF	4-27
4.3 OSPF显示和调试	4-28
4.4 OSPF典型配置举例.....	4-29
4.4.1 OSPF典型配置举例	4-29
4.4.2 配置OSPF多进程.....	4-31
4.4.3 配置OSPF优先级的“DR”选择	4-32
4.4.4 配置OSPF虚链路.....	4-34
4.4.5 配置OSPF邻居认证	4-36
4.4.6 配置OSPF的STUB区	4-38
4.5 OSPF故障诊断与排除	4-39
第 5 章 BGP配置	5-1
5.1 BGP简介	5-1
5.2 BGP的配置.....	5-2
5.2.1 启动BGP.....	5-3
5.2.2 指定BGP要通告的网络路由.....	5-3
5.2.3 配置BGP对等体组	5-4
5.2.4 配置BGP对等体/对等体组的路由过滤	5-9
5.2.5 取消IGP和IBGP路由同步	5-11
5.2.6 配置BGP定时器.....	5-11
5.2.7 配置本地优先级	5-11
5.2.8 配置自治系统的MED值	5-12
5.2.9 比较来自不同AS邻居路径的MED值	5-13
5.2.10 配置BGP团体属性	5-13
5.2.11 配置BGP路由聚合	5-14
5.2.12 配置BGP协议的优先级.....	5-14
5.2.13 配置BGP路由反射器	5-15
5.2.14 配置BGP自治系统联盟属性.....	5-17
5.2.15 配置BGP路由衰减.....	5-18
5.2.16 配置BGP与IGP的交互.....	5-19
5.2.17 配置本地AS号的重复次数	5-19
5.2.18 定义访问控制列表、AS路径列表和Route-policy.....	5-19
5.2.19 配置BGP路由过滤	5-20
5.2.20 复位BGP连接	5-21
5.2.21 配置BGP路由刷新	5-21

5.3 BGP显示和调试	5-22
5.4 BGP典型配置举例	5-24
5.4.1 配置自治系统联盟属性	5-24
5.4.2 配置BGP路由反射器	5-26
5.4.3 配置BGP路径选择	5-28
5.5 BGP故障诊断与排除	5-31
5.6 MBGP简介	5-31
5.6.1 MBGP概述	5-31
5.6.2 MBGP的扩展属性	5-32
5.6.3 安全网关的MBGP应用	5-32
5.7 MBGP配置	5-32
5.7.1 配置地址族	5-33
5.7.2 激活对等体/对等体组	5-33
5.8 MBGP典型配置举例	5-34
5.8.1 配置MBGP路由反射器	5-34
第 6 章 IP路由策略配置	6-1
6.1 IP路由策略简介	6-1
6.2 IP路由策略配置	6-2
6.2.1 配置路由过滤	6-3
6.2.2 通过Route-policy实现路由策略	6-6
6.3 IP路由策略显示和调试	6-9
6.4 路由策略典型配置举例	6-9
6.4.1 配置引入其它协议的路由信息	6-9
6.4.2 配置过滤发布的路由信息	6-10
6.4.3 配置过滤接收的路由信息	6-11
6.4.4 通过配置BGP的cost属性来选择路径	6-13
6.4.5 基于BGP next-hop/as-path/origin/local-preference属性的路由策略配置举例	6-16
6.5 路由策略故障诊断与排错	6-20
第 7 章 路由容量配置	7-1
7.1 路由容量配置简介	7-1
7.1.1 概述	7-1
7.1.2 防火墙实现的路由容量限制	7-1
7.2 路由容量配置	7-1
7.2.1 配置防火墙内存的下限与安全值	7-2
7.2.2 禁止防火墙的自动恢复连接功能	7-2
7.2.3 使能防火墙的自动恢复连接功能	7-2
7.3 路由容量显示和调试	7-3

第1章 IP 路由协议概述

1.1 IP 路由和路由表介绍

1.1.1 路由和路由段

在因特网中进行路由选择要使用路由器，路由器根据所收到的报文的目的地址选择一条合适的路由（通过某一网络），将报文传送到下一个路由器，路由中最后的路由器负责将报文送交目的主机。

例如，在图 1-1 中，主机 A 到主机 C 共经过了 3 个网络和 2 个路由器，跳数为 2。由此可见，若一节点通过一个网络与另一节点相连接，则此二节点相隔一个路由段，因而在因特网中是相邻的。同理，相邻的路由器是指这两个路由器都连接在同一个网络上。一个路由器到本网络中的某个主机的路由段数算作零。在图中用粗的箭头表示这些路由段。至于每一个路由段又由哪几条物理链路构成，路由器并不关心。

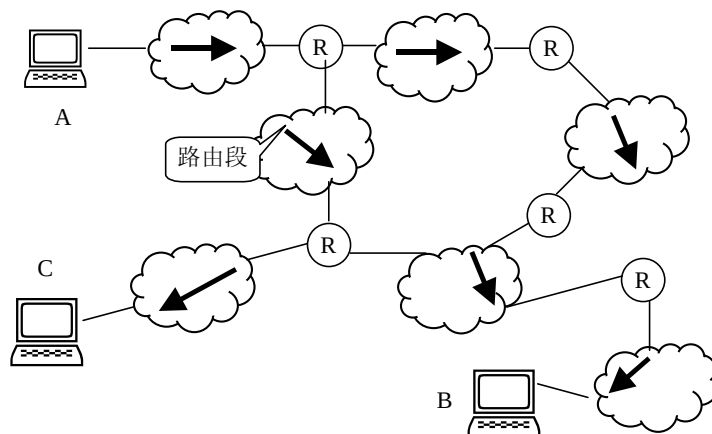


图1-1 路由段的概念

由于网络大小可能相差很大, 而每个路由段的实际长度并不相同, 因此对不同的网络, 可以将其路由段乘以一个加权系数, 用加权后的路由段数来衡量通路的长短。

如果把网络中的路由器看成是网络中的节点，把因特网中的一个路由段看成是网络中的一条链路，那么因特网中的路由选择就与简单网络中的路由选择相似了。采用路由段数最小的路由有时也并不一定是最理想的。例如，经过三个高速局域网段的路由可能比经过两个低速广域网段的路由快得多。

1.1.2 通过路由表进行选路

路由器转发分组的关键是路由表。每个路由器中都保存着一张路由表，表中每条路由项都指明分组到某子网或某主机应通过路由器的哪个物理端口发送，然后就可到

达该路径的下一个路由器，或者不再经过别的路由器而传送到直接相连的网络中的目的主机。

路由表中包含了下列关键项：

- 目的地址：用来标识 IP 包的目的地或目的网络。
- 网络掩码：与目的地址一起来标识目的主机或路由器所在的网段的地址。将目的地址和网络掩码“逻辑与”后可得到目的主机或路由器所在网段的地址。例如：目的地址为 129.102.8.10，掩码为 255.255.0.0 的主机或路由器所在网段的地址为 129.102.0.0。掩码由若干个连续“1”构成，既可以以点分十进制表示，也可以用掩码中连续“1”的个数来表示。
- 输出接口：说明 IP 包将从该路由器哪个接口转发。
- 下一跳 IP 地址：说明 IP 包所经由的下一个路由器。
- 本条路由加入 IP 路由表的优先级：针对同一目的地，可能存在不同下一跳的若干条路由，这些不同的路由可能是由不同的路由协议发现的，也可以是手工配置的静态路由。优先级高（数值小）的将成为当前的最优路由。

根据路由的目的地不同，可以划分为：

- 子网路由：目的地为子网
- 主机路由：目的地为主机

另外，根据目的地与该路由器是否直接相连，又可分为：

- 直接路由：目的地所在网络与路由器直接相连
- 间接路由：目的地所在网络与路由器不是直接相连

为了不使路由表过于庞大，可以设置一条缺省路由。凡遇到查找路由表失败后的数据包，就选择缺省路由转发。

在图 1-2 比较复杂的因特网中，各网络中的数字是该网络的网络地址。路由器 8 与三个网络相连，因此有三个 IP 地址和三个物理端口，其路由表如图所示。

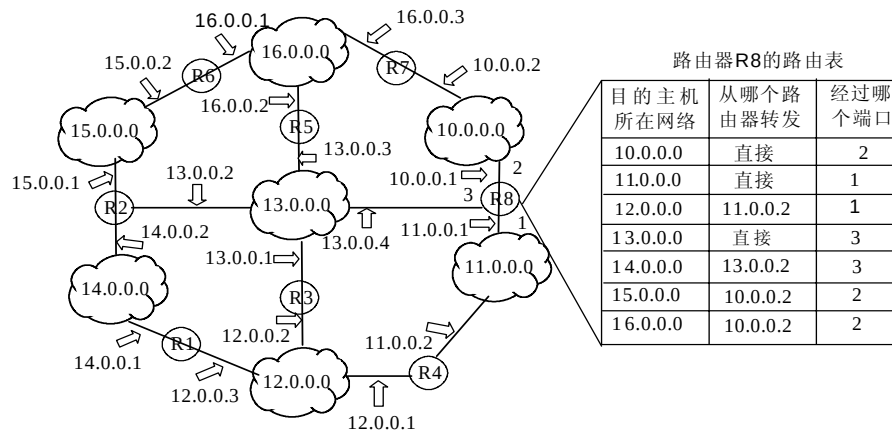


图1-2 路由表示意图

防火墙支持对静态路由的配置，同时支持 RIP、OSPF 和 BGP 等一系列动态路由协议，另外防火墙在运行过程中根据接口状态和用户配置，会自动获得一些直接路由。

1.2 路由管理策略

可以使用手工配置到某一特定目的地的静态路由，也可以配置动态路由协议与网络中其它路由器交互，并通过路由算法来发现路由。用户配置的静态路由和由路由协议发现的动态路由在路由器中是统一管理的。

1.2.1 路由协议及其发现路由的优先级

到相同的目的地，不同的路由协议（包括静态路由）可能会发现不同的路由，但并非这些路由都是最优的。事实上，在某一时刻，到某一目的地的当前路由仅能由唯一的路由协议来决定。这样，各路由协议（包括静态路由）都被赋予了一个优先级，这样当存在多个路由信息源时，具有较高优先级的路由协议发现的路由将成为当前的最优路由。各种路由协议及其发现路由的缺省优先级（数值越小表明优先级越高）如表 1-1 所示。

其中：0 表示直接连接的路由，255 表示任何来自不可信源端的路由。

表1-1 路由协议及其发现路由的优先级

路由协议或路由种类	相应路由的优先级
DIRECT	0
OSPF	10
IS-IS	15
STATIC	60
RIP	100
OSPF ASE	150
OSPF NSSA	150
IBGP	256
EBGP	256
UNKNOWN	255

除了直连路由（DIRECT）外，各动态路由协议的优先级都可根据用户需求，手工进行配置。另外，每条静态路由的优先级都可以不相同。

1.2.2 对负载分担与路由备份的支持

1. 负载分担

支持多路由模式，即允许配置多条到同一目的地而且优先级相同的路由。到同一目的地而且优先级相同的路由指的是目的网络和掩码相同，优先级相同，但下一跳地址或者出接口不相同。当没有比到此目的地优先级更高的路由时，这几条路由都被系统采纳，在转发报文时，依次通过各条路径发送，从而实现网络的负载分担。路由负载分担只能在同一个路由协议的等价路由（即路由的 **cost** 代价相等）之间进行，例如不能在所配置的静态路由和 **OSPF** 路由之间进行。

目前，支持负载分担的路由协议有：静态路由、**RIP**、**OSPF**、**BGP** 和 **IS-IS**。

负载分担的实现方式有两种：

- 基于流的负载分担。例如，当前路由器上存在两条等价路由，如果此时只有一个数据流，那么将从一条路由上转发；如果有两个数据流，那么两条路由各转发一个。子接口也支持快转，实现基于流的负载分担。
- 基于报文的负载分担。当关闭了快转功能时，并且路由器拥有到同一目的地的多条等价路由时，路由器将基于报文进行负载分担，即将待发送报文均匀分配到两条路由上。

2. 路由备份

当主路由发生故障时，自动切换到备份路由，提高用户网络的可靠性。为了实现路由的备份，用户可根据实际情况，配置到同一目的地的多条路由，其中一条路由的优先级最高，称为主路由，其余的路由优先级依次递减，称为备份路由。这样，正常情况下，路由器采用主路由发送数据。当线路发生故障时，路由器会选择余下的优先级最高的备份路由作为数据发送的途径。这样，也就实现了主路由到备份路由的切换。当主路由恢复正常时，路由器恢复相应的路由，并重新选择路由。由于该路由的优先级最高，路由器选择主路由来发送数据。上述过程是备份路由到主路由的自动切换。

1.2.3 路由协议之间的共享

由于各路由协议的算法不同，不同的协议可能会发现不同的路由，因此各路由协议之间存在如何共享各自发现结果的问题。路由器支持将一种路由协议发现的路由引入（**import-route**）到另一种路由协议中，每种协议都有相应的路由引入机制，具体内容请参见各路由协议的配置指导中引入外部路由部分的描述。

第2章 静态路由配置

说明：

本章中有关 VPN 实例的具体参数解释，请参见本手册的“VPN”部分。

2.1 静态路由简介

2.1.1 静态路由

静态路由是一种特殊的路由，它由管理员手工配置而成。通过静态路由的配置可建立一个互通的网络，但这种配置缺点在于：当一个网络故障发生后，静态路由不会自动发生改变，必须有管理员的介入。

在组网结构比较简单的网络中，只需配置静态路由就可以使路由器正常工作，仔细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。

静态路由还有如下的属性：

- 可达路由，正常的路由都属于这种情况，即 IP 报文按照目的地标示的路由被送往下一跳，这是静态路由的一般用法。
- 目的地不可达的路由，当到某一目的地的静态路由具有“**reject**”属性时，任何去往该目的地的 IP 报文都将被丢弃，并且通知源主机目的地不可达。
- 目的地为黑洞的路由，当到某一目的地的静态路由具有“**blackhole**”属性时，任何去往该目的地的 IP 报文都将被丢弃，并且不通知源主机。

其中“**reject**”和“**blackhole**”属性一般用来控制本路由器可达目的地的范围，辅助网络故障的诊断。

2.1.2 缺省路由

缺省路由是一种特殊的路由，可以通过静态路由配置，某些动态路由协议也可以生成缺省路由，如 OSPF 等。

简单地说，缺省路由就是在没有找到匹配的路由时才使用的路由。即只有当没有合适的路由时，缺省路由才被使用。在路由表中，缺省路由以到网络 0.0.0.0（掩码为 0.0.0.0）的路由形式出现。可通过命令 **display ip routing-table** 的输出看它是否被设置。如果报文的目的地不能与任何路由相匹配，那么系统将使用缺省路由转发该报文。如果没有缺省路由且报文的目的地不在路由表中，那么该报文被丢弃，同时，向源端返回一个 ICMP 报文，报告该目的地或网络不可达。

2.2 静态路由配置

静态路由的配置包括：

- 配置静态路由
- 配置缺省路由
- 配置静态路由优先级
- 删除静态路由

2.2.1 配置静态路由

请在系统视图下进行下列配置。

表2-1 配置静态路由

操作	命令
增加一条静态路由	<pre> ip route-static ip-address { mask mask-length } { interface-type interface-number nexthop-address } [preference value] [reject blackhole] [detect-group group-number] [description text] ip route-static vpn-instance { vpn-instance-name1 vpn-instance-name2 ... ip-address } { mask mask-length } [interface-type interface-number [nexthop-address] vpn-instance vpn-nexthop-name nexthop-address nexthop-address [public]] [preference preference-value] [reject blackhole] [detect-group group-number] [description text] </pre>
删除一条静态路由	<pre> undo ip route-static ip-address { mask mask-length } [interface-name nexthop-address] [preference value] undo ip route-static vpn-instance { vpn-instance-name1 vpn-instance-name2 ... ip-address } { mask mask-length } [interface-type interface-number vpn-instance vpn-nexthop-name nexthop-address nexthop-address [public]] [preference preference-value] </pre>

其中各参数的解释如下：

(1) VPN 实例的名字

(2) IP 地址和掩码

IP 地址为点分十进制格式，由于要求掩码 32 位中 ‘1’ 必须是连续的，因此掩码可以用点分十进制表示，也可用掩码长度（即掩码中 ‘1’ 的位数）表示。

(3) 发送接口或下一跳地址

在配置静态路由时，可指定发送接口 *interface-type interface-number*，也可指定下一跳地址 *nexthop-address*，是指定发送接口还是指定下一跳地址要视具体情况而定。

实际上，所有的路由项都必须明确下一跳地址。在发送报文时，首先根据报文的目的地地址寻找路由表中与之匹配的路由。只有路由指定了下一跳地址，链路层才能通过下一跳 IP 地址找到对应的链路层地址，然后按照该地址将报文转发。

在以下几种情况下可以指定发送接口：

- 对于点到点接口，指定发送接口即隐含指定了下一跳地址，这时认为与该接口相连的对端接口地址就是路由的下一跳地址。如 Serial 封装 PPP 协议，通过 PPP 协商获取对端的 IP 地址，这时可以不用指定下一跳地址，只需指定发送接口即可。
- 对于 NBMA 接口（如 ATM 接口），支持点到多点，这时除了配置 IP 路由外，还需在链路层建立二次路由，即 IP 地址到链路层地址的映射。这种情况下应配置下一跳 IP 地址。
- 在配置静态路由时，建议不要指定为以太网接口或 Virtual-template 接口作发送接口。因为以太网接口是广播类型的接口，而 Virtual-template 接口下可以关联多个虚拟访问接口（Virtual Access Interface），这都会导致出现多个下一跳，无法唯一确定下一跳。在某些特殊应用中，如果必须指定广播接口（如以太网接口）或 NBMA 接口做为发送接口，应同时指定通过该接口发送时对应的下一跳地址。

(4) 优先级

对优先级 **preference** 的不同配置，可以灵活应用路由管理策略。

(5) 其它参数

属性 **reject** 和 **blackhole** 分别指明不可达路由和黑洞路由。属性 **detect-group** 将侦测组返回的结果（可达或不可达）作为静态路由是否生效的一个必要条件。属性 **description** 用来为静态路由添加描述信息。

2.2.2 配置缺省路由

请在系统视图下进行下列配置。

表2-2 配置缺省路由

操作	命令
配置缺省路由	<pre> ip route-static 0.0.0.0 { 0.0.0.0 0 } {<i>interface-type interface-number</i> <i>nexthop-address</i> } [preference value] ip route-static vpn-instance <i>vpn-instance-name</i> 0.0.0.0 { 0.0.0.0 0 } {<i>interface-type interface-number</i> <i>nexthop-address</i> } [preference value] </pre>

操作	命令
删除缺省路由	undo ip route-static 0.0.0.0 { 0.0.0.0 0 } { <i>interface-type</i> <i>interface-number</i> <i>nexthop-address</i> } [preference value] undo ip route-static vpn-instance <i>vpn-instance-name</i> 0.0.0.0 { 0.0.0.0 0 } { <i>interface-type</i> <i>interface-number</i> <i>nexthop-address</i> } [preference value]

命令中各参数意义与静态路由相同。

2.2.3 删除全部静态路由

请在系统视图下进行下列配置。

表2-3 删除全部静态路由

操作	命令
删除全部静态路由	delete static-routes all

使用此命令可以删除配置的全部静态路由，包括缺省路由。

2.3 路由表的显示和调试

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后静态路由信息，用户可以通过查看显示信息验证配置的效果。

表2-4 路由表的显示和调试

操作	命令
查看路由表摘要信息	display ip routing-table
查看路由表详细信息	display ip routing-table verbose
查看指定目的地址的路由	display ip routing-table <i>ip-address</i> [<i>mask</i>] [<i>longer-match</i>] [<i>verbose</i>]
查看指定目的地址范围内的路由	display ip routing-table <i>ip-address1 mask1 ip-address2 mask2</i> [<i>verbose</i>]
查看通过指定基本访问控制列表过滤的路由	display ip routing-table acl <i>acl-number</i> [<i>verbose</i>]
查看通过指定前缀列表过滤的路由	display ip routing-table ip-prefix <i>ip-prefix-number</i> [<i>verbose</i>]
查看指定协议发现的路由	display ip routing-table protocol <i>protocol</i> [<i>inactive</i> <i>verbose</i>] [<i>vpn-instance vpn-instance-name</i>]
查看树形式路由表	display ip routing-table radix
查看路由表的统计信息	display ip routing-table [<i>vpn-instance vpn-instance-name</i>] statistics

操作	命令
查看私网路由表摘要信息	display ip routing-table vpn-instance <i>vpn-instance-name</i> [<i>ip-address</i>]
查看私网路由表详细信息	display ip routing-table vpn-instance <i>vpn-instance-name</i> [<i>ip-address</i>] verbose
清除路由表信息	reset ip routing-table [<i>vpn-instance</i> <i>vpn-instance-name</i>] statistics protocol <i>protocol-type</i>

2.4 静态路由典型配置举例

1. 组网需求

如下图所示，要求配置静态路由，使任意两台主机或防火墙之间都能互通。

2. 组网图

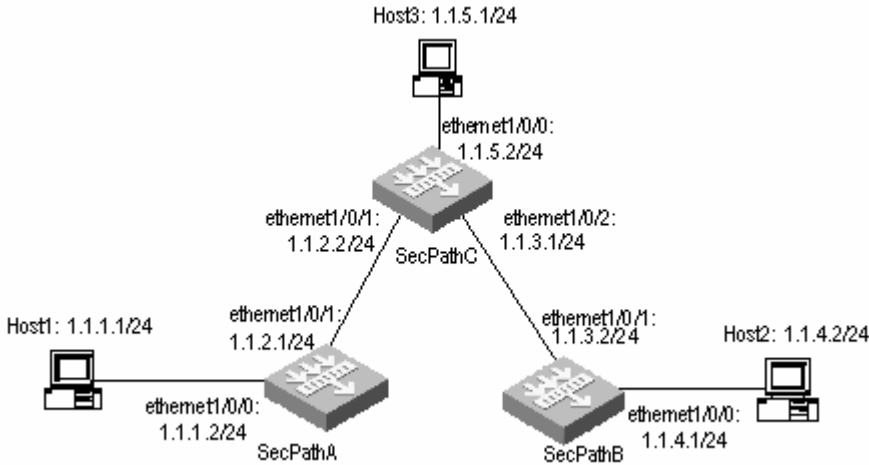


图2-1 静态路由配置举例组网图

3. 配置步骤

配置 SecPathA 静态路由：

```
[H3C] ip route-static 1.1.3.0 255.255.255.0 1.1.2.2
[H3C] ip route-static 1.1.4.0 255.255.255.0 1.1.2.2
[H3C] ip route-static 1.1.5.0 255.255.255.0 1.1.2.2
```

或只配缺省路由：

```
[H3C] ip route-static 0.0.0.0 0.0.0.0 1.1.2.2
```

配置 SecPathB 静态路由：

```
[H3C] ip route-static 1.1.2.0 255.255.255.0 1.1.3.1
[H3C] ip route-static 1.1.5.0 255.255.255.0 1.1.3.1
```

```
[H3C] ip route-static 1.1.1.0 255.255.255.0 1.1.3.1
```

或只配缺省路由：

```
[H3C] ip route-static 0.0.0.0 0.0.0.0 1.1.3.1
```

配置 SecPathC 静态路由：

```
[H3C] ip route-static 1.1.1.0 255.255.255.0 1.1.2.1
```

```
[H3C] ip route-static 1.1.4.0 255.255.255.0 1.1.3.2
```

主机 Host1 上配缺省网关为 1.1.1.2

主机 Host 2 上配缺省网关为 1.1.4.1

主机 Host 3 上配缺省网关为 1.1.5.2

至此 图 2-1中所有主机或防火墙之间能两两互通。

2.5 静态路由配置的故障诊断与排除

故障之一：防火墙没有配置动态路由协议，接口的物理状态和链路层协议状态均已处于 UP，但 IP 报文不能正常转发。

故障排除：

- 用 **display ip routing-table protocol static** 命令查看是否正确配置相应静态路由。
- 用 **display ip routing-table** 命令查看该静态路由是否已经生效。

第3章 RIP 配置

说明：

本章中有关 VPN 实例的具体参数解释，请参见本手册的“VPN”部分。

3.1 RIP 简介

RIP 是 Routing Information Protocol（路由信息协议）的简称。它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。

由于 RIP 的实现较为简单，协议本身的开销对网络的性能影响比较小，并且在配置和维护管理方面也比 OSPF 或 IS-IS 容易，因此在实际组网中仍有广泛的应用。

3.1.1 RIP 的工作机制

1. RIP 的基本概念

RIP 是一种基于距离矢量（Distance-Vector）算法的协议，它通过 UDP 报文进行路由信息的交换。

RIP 使用跳数（Hop Count）来衡量到达目的网络的距离，称为路由权（Routing Cost）。在 RIP 中，路由器到与它直接相连网络的跳数为 0，通过一个路由器可达的网络的跳数为 1，其余依此类推。为限制收敛时间，RIP 规定 cost 取值 0~15 之间的整数，大于或等于 16 的跳数被定义为无穷大，即目的网络或主机不可达。

为提高性能，防止产生路由环，RIP 支持水平分割（Split Horizon），即不从某接口发送从该接口学到的路由。RIP 还可引入其它路由协议所得到的路由。

2. RIP 的路由数据库

每个运行 RIP 的路由器管理一个路由数据库，该路由数据库包含了到所有可达目的网络的路由项，这些路由项包含下列信息：

- 目的地址：指主机或网络的地址。
- 下一跳地址：指为到达目的地，本路由器要经过的下一个路由器地址。
- 接口：指转发报文的接口。
- 路由权值：指本路由器到达目的地的跳数，是一个 0~15 之间的整数。
- 路由时间：从路由项最后一次被修改到现在所经过的时间，路由项每次被修改时，路由时间重置为 0。

- 路由标记：区分路由为内部路由协议的路由还是引入外部路由协议的路由的标记。

3. RIP 使用的定时器

在 RFC1058 中规定，RIP 受三个定时器的控制，分别是 Period update、Timeout 和 Garbage-Collection：

- Period update 定时触发，向所有邻居发送全部 RIP 路由；
- RIP 路由如果在 Timeout 时间内没有被更新（收到邻居发来的路由刷新报文），则认为该路由不可达；
- 如果在 Garbage-Collection 时间内，不可达路由没有收到来自同一邻居的更新，则该路由被从路由表中删除。

3.1.2 RIP 的启动和运行过程

RIPv1 启动和运行的整个过程可描述如下：

- 某路由器刚启动 RIP 时，以广播的形式向相邻路由器发送请求报文，运行 RIP 协议的相邻路由器的 RIP 收到请求报文后，响应该请求，回送包含本地路由表信息的响应报文。
- 路由器收到响应报文后，更新本地路由表，同时向相邻路由器发送更新报文，广播路由更新信息。运行 RIP 协议的相邻路由器收到更新报文后，又向其各自的相邻路由器发送更新报文。在一连串的更新广播后，各路由器都能得到并保持最新的路由信息。
- 同时，RIP 每隔 Period update 的时间向相邻路由器广播本地路由表，运行 RIP 协议的相邻路由器在收到报文后，对本地路由进行维护，选择一条最佳路由，再向其各自相邻网络广播更新信息，使更新的路由最终能达到全部网络。同时，RIP 采用超时机制对过时的路由进行超时处理，以保证路由的实时性和有效性。

RIPv2 的启动和运行过程与 RIPv1 基本相同，但缺省情况下其更新报文是发送到组播地址 224.0.0.9。根据不同需求，也可以配置 RIPv2 发送广播更新报文以对 RIPv1 进行向后兼容。

RIP 正被大多数 IP 路由器厂商广泛使用。它可用于大多数校园网及结构较简单的连续性强的地区性网络。对于更复杂环境及大型网络，一般不使用 RIP。

3.1.3 Comware 支持的 RIP 特性

SecPath 系列防火墙可以支持 RIP-1 和 RIP-2 协议。

3.2 RIP 配置

配置 RIP 时，必须先启动 RIP，才能配置其它特性。而配置与接口相关的特性不受 RIP 是否使能的限制。需要注意的是，在关闭 RIP 后，与 RIP 相关的接口参数也同时失效。

(1) 基本的 RIP 配置

对于基本的 RIP 配置，需要进行的操作包括：

- 启动 RIP
- 在指定网段使能 RIP

如果在不支持广播或组播报文的链路上运行 RIP，需要配置 RIP 报文定点传送，以正确建立 RIP 邻居。

对于采用 Frame Relay 子接口等 NBMA 链路组网的情况，为保证路由信息的正确传播，可能还需要禁止水平分割特性。

(2) RIP 路由管理

在对路由信息的发布和接收上，可以对 RIP 进行以下配置：

- 配置附加路由权
- 配置 RIP 的路由引入
- 配置 RIP 的路由过滤
- 禁止 RIP 接收主机路由
- 配置 RIP 的路由聚合
- 配置 RIP 非直连邻居的路由交互
- 配置 RIP 在接口间实现负载分担功能

(3) RIP 协议本身的参数配置

- 配置 RIP 优先级
- 配置 RIP 定时器
- 配置 RIP 的零域检查
- 配置接口的 RIP 版本

(4) 安全性考虑

为提高 RIP 在交换路由信息时的安全性，或控制 RIP 报文的扩散范围，可以选择以下配置：

- 配置 RIP 报文认证
- 配置接口的工作状态

(5) RIP 对 MPLS VPN 的支持

- 配置 RIP 多实例

3.2.1 启动 RIP

启动 RIP 后，将进入 RIP 视图。

请在系统视图下进行下列配置。

表3-1 启动 RIP

操作	命令
启动 RIP，进入 RIP 视图	rip
停止 RIP 协议的运行	undo rip

缺省情况下，不运行 RIP。

RIP 的大部分特性都需要在 RIP 视图下配置，接口视图下也有部分 RIP 相关属性的配置。如果启动 RIP 前先在接口视图下进行了 RIP 相关的配置，这些配置只有在 RIP 启动后才会生效。需要注意的是，在执行 **undo rip** 命令关闭 RIP 后，接口上与 RIP 相关的配置也将被删除。

3.2.2 在指定网段使能 RIP

为了灵活地控制 RIP 工作，可以指定某些接口，将其所在的相应网段配置成 RIP 网络，使这些接口可收发 RIP 报文。

请在 RIP 视图下进行下列配置。

表3-2 在指定网段使能 RIP

操作	命令
在指定的网络接口上应用 RIP	network network-address
在指定的网络接口上取消应用 RIP	undo network network-address

RIP 只在指定网段上的接口运行；对于不在指定网段上的接口，RIP 不在此接口上面接收和发送路由，也不将它的接口路由转发出去。因此，RIP 启动后必须指定其工作网段。**network-address** 为使能或不使能的网络的地址，也可配置为各个接口 IP 网络的地址。

当对某一地址使用命令 **network** 时，效果是使能该地址的网段的接口。例如：**network 129.102.1.1**，用 **display current-configuration** 和 **display rip** 命令看到的均是 **network 129.102.0.0**。

对于 RIP v1，路由协议在发布路由信息时有如下情况需要注意：

- 如果当前路由的目的地址和发送接口的地址不在同一主网（指自然网段），那么对于超网路由则不发送给邻居；对于子网路由则按自然网段聚合后发送给邻居。
- 如果当前的路由的目的地址和发送接口地址在同一主网，那么如果路由的目的地址的掩码和接口掩码不相等，就不发送给邻居；否则直接发送给邻居。

缺省情况下，任何网段都未使能 RIP。

3.2.3 配置 RIP 报文定点传送

通常情况下，RIP 使用广播地址发送报文，如果需要在不支持广播报文的链路上运行 RIP，就必须采用定点传送的方式，否则将不能正常地建立 RIP 邻居关系。

请在 RIP 视图下进行下列配置。

表3-3 配置 RIP 报文定点传送

操作	命令
配置 RIP 报文的定点传送	peer ip-address
取消 RIP 报文的定点传送	undo peer ip-address

缺省情况下，RIP 不向任何定点地址发送报文。

需要注意的是：**peer** 在发送报文时受接口工作状态的限制，接口的工作状态由 **rip work**、**rip output**、**rip input** 和 **network** 等命令进行配置。

3.2.4 配置水平分割

水平分割是指不从本接口发送从该接口学到的路由。它可以在一定程度上避免产生路由环。但在某些特殊情况下，却需要禁止水平分割，以保证路由的正确传播。禁止水平分割对点到点链路不起作用，但对以太网来说是可行的。

请在接口视图下进行下列配置。

表3-4 配置水平分割

操作	命令
启动水平分割	rip split-horizon
禁止水平分割	undo rip split-horizon

缺省情况下，接口允许水平分割。

3.2.5 配置附加路由权

附加路由权是对 RIP 路由添加的输入或输出路由权值，附加路由权并不直接改变路由表中的路由权值，而是在接收或发送路由时增加一个指定的权值。

请在接口视图下进行下列配置。

表3-5 设置附加路由权

操作	命令
设置接口在接收 RIP 报文时给路由附加路由权值	rip metricin value
禁止接口在接收 RIP 报文时给路由附加路由权值	undo rip metricin
设置接口在发送 RIP 报文时给路由附加路由权值	rip metricout value
禁止接口在发送 RIP 报文时给路由附加路由权值	undo rip metricout

缺省情况下，RIP 在发送报文时给路由增加的附加路由权值为 1；在接收报文时给路由增加的附加路由权值为 0。

3.2.6 配置 RIP 的路由引入

RIP 允许用户将其它路由协议的路由信息引入到 RIP 中，并可以设置引入时使用的缺省路由权。

可引入到 RIP 中的路由类型包括：Direct、Static、OSPF 和 BGP。

请在 RIP 视图下进行下列配置。

表3-6 配置 RIP 的路由引入

操作	命令
引入其它协议的路由	import-route protocol [allow-ibgp] [cost value] [route-policy route-policy-name]
取消对其它协议路由的引入	undo import-route protocol
设定缺省路由权值	default cost value
恢复缺省路由权值	undo default cost

缺省情况下，RIP 不引入其它协议的路由。

当 *protocol* 为 BGP 时，**allow-ibgp** 为可选关键字。**import-route bgp** 表示只引入 EBGp 路由，**import-route bgp allow-ibgp** 表示将 IBGP 路由也引入，该配置危险，请慎用！

如果在引入路由时没有指定路由权，则使用缺省路由权，其缺省值为 1。

3.2.7 配置 RIP 的路由过滤

RIP 提供路由过滤功能，通过指定访问控制列表和地址前缀列表，可以配置策略规则，对路由的接收和发布进行过滤。

在接收路由时，还可以指定只接收来自某个邻居的路由。

请在 RIP 视图下进行下列配置。

1. 配置 RIP 对接收的路由进行过滤

表3-7 配置 RIP 对接收路由的过滤

操作	命令
对接收的由指定地址发布的路由信息进行过滤	filter-policy gateway <i>ip-prefix-name</i> import
取消对接收的由指定地址发布的路由信息的过滤	undo filter-policy gateway <i>ip-prefix-name</i> import
对接收的全局路由信息进行过滤	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> [gateway <i>ip-prefix-name</i>] } import
取消对接收的全局路由信息过滤	undo filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> [gateway <i>ip-prefix-name</i>] } import
对接收的全局路由信息按路由策略进行过滤	filter-policy route-policy <i>route-policy-name</i> import
取消对接收的全局路由信息按路由策略进行过滤	undo filter-policy route-policy <i>route-policy-name</i> import

2. 配置 RIP 对发布的路由进行过滤

表3-8 配置 RIP 对发布路由的过滤

操作	命令
对发布的路由进行过滤	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> route-policy <i>route-policy-name</i> } export [<i>routing-protocol</i>]
对发布的路由信息取消过滤	undo filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> route-policy <i>route-policy-name</i> } export [<i>routing-protocol</i>]

缺省情况下，RIP 不对接收与发布的任何路由信息进行过滤。

当在此命令中指定 *routing-protocol* 时，可用于过滤从指定路由协议引入的路由。

更详细的描述请参见 6.2.1 配置路由过滤。

3.2.8 禁止 RIP 接收主机路由

在某些特殊情况下，防火墙会收到大量来自同一网段的主机路由，这些路由对于路由寻址没有多少作用，却占用了大量网络资源。配置了禁止主机路由功能后，防火墙能够拒绝它所收到的主机路由。

请在 RIP 视图下进行下列配置。

表3-9 禁止 RIP 接收主机路由

操作	命令
允许接收主机路由	host-route
禁止接收主机路由	undo host-route

缺省情况下，防火墙接收主机路由。

3.2.9 配置 RIP 的路由聚合

路由聚合是指：同一自然网段内的不同子网的路由在向外（其它网段）发送时聚合成一条自然掩码的路由发送。这一功能主要用于减小路由表的尺寸，进而减少网络上的流量。

路由聚合对 RIP-1 不起作用。RIP-2 支持无类地址域间路由。当需要将所有子网路由广播出去时，可关闭 RIP-2 的路由聚合功能。

请在 RIP 视图下进行下列配置。

表3-10 配置 RIP 路由聚合

操作	命令
启动 RIP-2 的路由聚合功能	summary
关闭 RIP-2 的路由聚合功能	undo summary

缺省情况下，RIP-2 启用路由聚合功能。

3.2.10 配置 RIP 非直连邻居的路由交互

缺省情况下，RIP 只往直连的网段发送 RIP 报文，在发送单播报文时，会检查目的地址是否是直连地址；在收到 RIP 报文时，会检查报文的源地址，通过报文的源地址来找到入接口。基于这种原理，当两个设备为 RIP 非直连邻居时，无法实现 RIP 路由信息的交互。

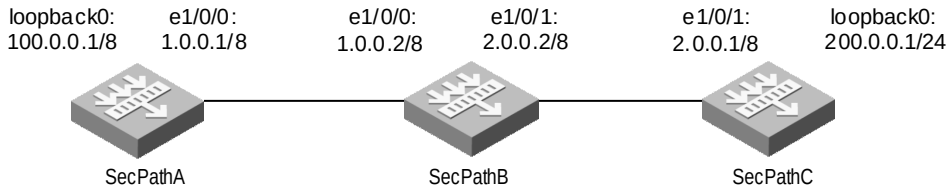


图3-1 RIP 非直连邻居的路由交互应用示意图

如上图所示,当在 SecPathA 和 SecPathC 为非直连邻居(仅 SecPathA 的 1.0.0.0/8, SecPathC 的 2.0.0.0/8 网段使能 RIP, SecPathB 没有使能 RIP), 此时如要实现 SecPathA 和 SecPathC 上的 RIP 路由交互, 需要进行如下配置:

- 配置 SecPathA 和 SecPathC 互为 RIP peer
- 取消检查收到的 RIP 报文的源地址
- 配置静态路由, 使 RIP 非直连邻居间的路由可达, 以保证报文被正确发送到非直连邻居。

此时, 防火墙在发送单播报文时, 就不会检查目的地址是否是直连地址, 并会去掉导致 SecPathB 不转发报文的标志信息; 在收到 RIP 报文时, 也不会检查报文的源地址, 并能通过报文的源地址和目的地址找到入接口。

1. 配置 RIP 报文定点传送

通常情况下, RIP 使用广播或组播地址发送报文, 如果需要在不支持广播报文的链路上运行 RIP, 就必须采用定点传送的方式, 否则将不能正常地建立 RIP 邻居关系; 在运行 RIP 协议的防火墙为非直连邻居时, 也必须配置 RIP 报文定点传送。

请在 RIP 视图下进行下列配置。

表3-11 配置 RIP 报文定点传送

操作	命令
配置 RIP 报文的定点传送	peer ip-address
取消 RIP 报文的定点传送	undo peer ip-address

缺省情况下, RIP 不向任何定点地址发送报文。

需要注意的是: peer 在发送报文时受接口工作状态的限制, 接口的工作状态由 **rip work**、**rip output**、**rip input** 和 **network** 等命令进行配置。

2. 配置检查/不检查收到的 RIP 报文的源地址

请在 RIP 视图下进行下列配置。

表3-12 配置检查/不检查收到的 RIP 报文的源地址

操作	命令
配置检查 RIP 报文的源地址	validate-source-address
取消检查 RIP 报文的源地址	undo validate-source-address

缺省情况下，检查 RIP 报文的源地址。

3.2.11 配置 RIP 在接口间实现负载分担功能

当启动了 RIP 接口间的负载分担功能时，可以使流量通过等价路由均衡地在各个接口之间分配。

请在 RIP 视图下进行下列配置。

表3-13 配置 RIP 在接口间实现负载分担功能

操作	命令
配置 RIP 在接口间实现负载分担功能	traffic-share-across-interface
关闭 RIP 在接口间的负载分担功能	undo traffic-share-across-interface

缺省情况下，关闭 RIP 接口间流量负载分担功能。

3.2.12 配置 RIP 优先级

每一种路由协议都有自己的优先级，协议的优先级将影响路由策略采用哪种路由协议获取的路由作为最优路由。优先级的数值越大，其实际的优先级越低。可以手工设定 RIP 的优先级。

请在 RIP 视图下进行下列配置。

表3-14 设置 RIP 的优先级

操作	命令
设置 RIP 协议的优先级	preference value
将 RIP 协议的优先级恢复为缺省值	undo preference

缺省情况下，RIP 的优先级为 100。

3.2.13 配置 RIP 定时器

在本章开始已经介绍过，RIP 有三个定时器：Period update、Timeout 和 Garbage-collection。改变这几个定时器的值，可以影响 RIP 的收敛速度。

请在 RIP 视图下进行下列配置。

表3-15 配置 RIP 定时器

操作	命令
配置 RIP 定时器的值	timers { update <i>update-timer-length</i> timeout <i>timeout-timer-length</i> } *
恢复 RIP 定时器的缺省值	undo timers { update timeout } *

RIP 定时器的值在更改后立即生效。

缺省情况下，Period update 定时器是 30 秒，Timeout 定时器是 180 秒，Garbage-collection 定时器则是 Period update 定时器的 4 倍，即 120 秒。

在实际应用中，用户可能会发现 Garbage-collection 定时器的超时时间并不固定，当 Period update 定时器设为 30 秒时，Garbage-collection 定时器可能在 90 到 120 秒之间。这是因为：不可达路由在被从路由表中彻底删除前，需要等待 4 个来自同一邻居的更新报文，但路由变为不可达状态并不总是恰好在一个更新周期的开始，因此，Garbage-collection 定时器的实际时长是 Period update 定时器的 3~4 倍。

说明：

在配置 RIP 定时器时需要注意，定时器值的调整应考虑网络的性能，并在所有运行 RIP 的防火墙、路由器上进行统一配置，以免增加不必要的网络流量或引起网络路由震荡。

3.2.14 配置 RIP 的零域检查

RFC1058 规定，RIP-1 报文中的有些区域必须为零，称之为零域（zero field）。RIP-1 在接收报文时将对零域进行检查，值不为零的 RIP-1 报文将不被处理。由于 RIP-2 的报文没有零域，此项配置对 RIP-2 无效。

请在 RIP 视图下进行下列配置。

表3-16 配置报文的零域检查

操作	命令
设置对 RIP-1 报文进行零域检查	checkzero
禁止对 RIP-1 报文进行零域检查	undo checkzero

缺省情况下，RIP-1 对报文进行零域检查。

3.2.15 配置接口的 RIP 版本

RIP 有 RIP-1 和 RIP-2 两个版本，可以指定接口所处理的 RIP 报文版本。

RIP-1 的报文传送方式为广播方式。RIP-2 有两种报文传送方式：广播方式和组播方式，缺省将采用组播方式发送报文。RIP-2 中组播地址为 224.0.0.9。组播发送报文的好处是在同一网络中那些没有运行 RIP 的主机可以避免处理 RIP 的广播报文；另外，以组播方式发送报文还可以使运行 RIP-1 的主机避免错误地接收和处理 RIP-2 中带有子网掩码的路由。当接口运行 RIP-2 时，也可接收 RIP-1 的报文。

请在接口视图下进行下列配置。

表3-17 配置接口的 RIP 版本

操作	命令
指定接口的 RIP 版本为 RIP-1	rip version 1
指定接口的 RIP 版本为 RIP-2	rip version 2 [broadcast multicast]
将接口运行的 RIP 版本恢复为缺省值	undo rip version

缺省情况下，接口接收和发送 RIP-1 报文；指定接口 RIP 版本为 RIP-2 时，缺省使用组播形式传送报文。

3.2.16 配置 RIP 报文认证

RIP-1 不支持报文认证。但当接口运行 RIP-2 时，可以配置报文的认证方式。

RIP-2 支持两种认证方式：明文认证和 MD5 密文认证。MD5 密文认证的报文格式有两种：一种遵循 RFC2453，另一种遵循 RFC2082。

明文认证不能提供安全保障。未加密的认证字随报文一同传送，所以明文认证不能用于安全性要求较高的情况。

请在接口视图下进行下列配置。

表3-18 设置对 RIP 报文认证

操作	命令
对 RIP-2 进行明文认证	rip authentication-mode simple <i>password</i>
对 RIP-2 进行通用的 MD5 认证	rip authentication-mode md5 rfc2453 <i>key-string</i>
对 RIP-2 进行非标准兼容的 MD5 认证	rip authentication-mode md5 rfc2082 <i>key-string key-id</i>
取消对 RIP-2 的认证	undo rip authentication-mode

如果配置 MD5 认证，则必须配置 MD5 的类型，其中 **rfc2453** 类型支持 RFC2453 规定的报文格式，**rfc2082** 类型支持 RFC2082 规定的报文格式。

3.2.17 配置接口的工作状态

在接口视图中可指定 RIP 在接口上的工作状态，如接口上是否运行 RIP，即是否在接口发送和接收 RIP 更新报文；还可单独指定发送（或接收）RIP 更新报文。

请在接口视图下进行下列配置。

表3-19 配置接口的工作状态

操作	命令
指示接口运行 RIP	rip work
禁止接口运行 RIP	undo rip work
允许接口接收 RIP 更新报文	rip input
禁止接口接收 RIP 更新报文	undo rip input
允许接口发送 RIP 更新报文	rip output
禁止接口发送 RIP 更新报文	undo rip output

undo rip work 命令的功能与 **undo network** 命令功能相近，但它们并不完全相同。相同点在于，两命令都可使相应接口不再收发 RIP 路由。区别在于：执行了 **undo rip work** 命令的情况下，其它接口对使用该命令的接口的路由仍然转发；而执行 **undo network** 命令，则相应的接口路由不能被 RIP 传播出去，导致到该接口的报文不能被转发。

rip work 从功能上等价于 **rip input** 与 **rip output** 两个命令。

缺省情况下，一个接口既接收 RIP 更新报文，也发送 RIP 更新报文。

3.2.18 复位 RIP 协议的系统配置参数

当需要重新配置 RIP 协议参数时，可以使用该命令恢复 RIP 协议的缺省配置。

请在 RIP 视图下进行下列配置。

表3-20 复位 RIP 协议的系统配置参数。

操作	命令
复位 RIP 协议的系统配置参数	reset

3.2.19 配置 RIP 多实例

支持 RIP 多实例功能，能够提供对 MPLS VPN 的支持。

请在 RIP 视图下进行下列配置。

表3-21 配置 RIP 多实例

操作	命令
进入 RIP 的地址族视图	ipv4-family [unicast] vpn-instance <i>vpn-instance-name</i>
删除 RIP 的地址族配置	undo ipv4-family [unicast] vpn-instance <i>vpn-instance-name</i>

执行 **undo ipv4-family** 命令后，将删除所有在地址族视图下进行的配置。

地址族视图用于 BGP/MPLS VPN，相关内容请参见本手册的“VPN”部分。

3.3 RIP 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 RIP 的运行情况，用户可以通过查看显示信息验证配置的效果。在用户视图下执行 **debugging** 命令可对 RIP 进行调试。

表3-22 RIP 显示和调试

操作	命令
显示 RIP 的当前运行状态及配置信息	display rip
显示 RIP 的接口信息	display rip interface [vpn-instance <i>vpn-instance-name</i>]
显示 RIP 的地址族相关配置	display rip vpn-instance <i>vpn-instance-name</i>
显示 RIP 路由表	display rip routing [vpn-instance <i>vpn-instance-name</i>]
打开 RIP 的报文调试信息开关	debugging rip packet [interface type number]
关闭 RIP 的报文调试信息开关	undo debugging rip packet
打开 RIP 的接收报文情况调试开关	debugging rip receive [interface type number]
关闭 RIP 的接收报文情况调试开关	undo debugging rip receive
打开 RIP 的发送报文情况调试开关	debugging rip send [interface type number]
关闭 RIP 的发送报文情况调试开关	undo debugging rip send

3.4 RIP 典型配置举例

3.4.1 配置指定接口的工作状态

1. 组网需求

一个企业的内部网络通过 SecPathA 连到 Internet，内部网络的主机直接连接到 SecPathB 或 SecPathC 上。

要求三个网关上均运行 RIP。SecPathA 只接收从外部网络发来的路由信息，但不对外发布内部网络的路由信息。SecPathA、B、C 之间能够交互 RIP 信息，以便于内部主机能够访问 Internet。

2. 组网图

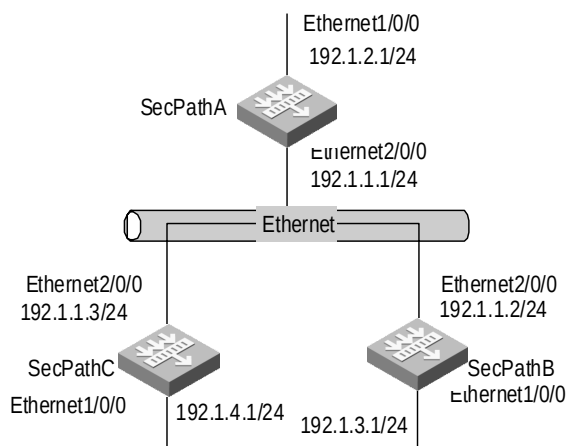


图3-2 配置接口的工作状态

3. 配置步骤

(1) 配置 SecPathA:

配置接口 Ethernet2/0/0 和 Ethernet1/0/0。

```
[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 192.1.1.1 255.255.255.0
[H3C-Ethernet2/0/0] quit
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 192.1.2.1 255.255.255.0
```

启动 RIP，并配置在接口 Ethernet2/0/0 和 Ethernet1/0/0 上运行 RIP。

```
[H3C] rip
[H3C-rip] network 192.1.1.0
[H3C-rip] network 192.1.2.0
```

配置接口 Ethernet 1/0/0 只接收 RIP 报文。

```
[H3C-Ethernet1/0/0] undo rip output
[H3C-Ethernet1/0/0] rip input
```

(2) 配置 SecPathB:

配置接口 Ethernet1/0/0 和 Ethernet2/0/0

```
[H3C] interface Ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 192.1.1.2 255.255.255.0
[H3C] interface Ethernet 1/0/0
```

```
[H3C-Ethernet1/0/0] ip address 192.1.3.1 255.255.255.0
```

启动 RIP，并配置在接口 Ethernet1/0/0 和 Ethernet2/0/0 上运行 RIP。

```
[H3C] rip
```

```
[H3C-rip] network 192.1.1.0
```

```
[H3C-rip] network 192.1.3.0
```

(3) 配置 SecPathC:

配置接口 Ethernet1/0/0 和 Ethernet2/0/0

```
[H3C] interface Ethernet 2/0/0
```

```
[H3C-Ethernet2/0/0] ip address 192.1.1.3 255.255.255.0
```

```
[H3C] interface Ethernet 1/0/0
```

```
[H3C-Ethernet1/0/0] ip address 192.1.4.1 255.255.255.0
```

启动 RIP，并配置在接口 Ethernet1/0/0 和 Ethernet2/0/0 运行 RIP。

```
[H3C] rip
```

```
[H3C-rip] network 192.1.1.0
```

```
[H3C-rip] network 192.1.4.0
```

3.4.2 调整 RIP 网络的收敛时间

1. 组网需求

SecPathA、SecPathB 和 SecPath C 上运行 RIP，要求网络的收敛时间在 30 秒以内。

2. 组网图

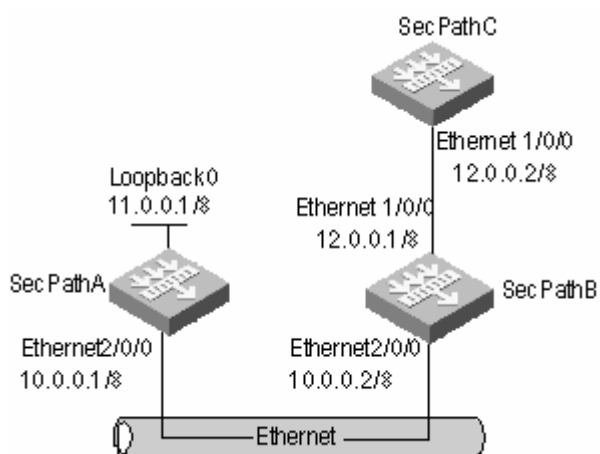


图3-3 RIP 定时器配置组网图

3. 配置步骤

说明:

接口的IP地址配置如图 3-3所示，配置步骤中不再赘述。

(1) 配置 SecPathA:

启动 RIP，并使能 SecPathA 的接口 Ethernet2/0/0 和 LoopBack0 运行 RIP。

```
[H3C] rip
[H3C-rip] network 10.0.0.0
[H3C-rip] network 11.0.0.0
[H3C-rip] timers update 10 timeout 30
```

(2) 配置 SecPathB:

启动 RIP，并使能 SecPathB 的接口 Ethernet2/0/0 和 Ethernet1/0/0 运行 RIP。

```
[H3C] rip
[H3C-rip] network 10.0.0.0
[H3C-rip] network 12.0.0.0
[H3C-rip] timers update 10 timeout 30
```

(3) 配置 SecPathC:

启动 RIP，并使能 SecPathC 的接口 Ethernet1/0/0 运行 RIP。

```
[H3C] rip
[H3C-rip] network 12.0.0.0
[H3C-rip] timers update 10 timeout 30
```

配置结束后，在 SecPathB 和 SecPathC 执行 **display ip routing-table** 命令能看到 11.0.0.0/8 的路由。将 SecPathA 的 Ethernet2/0/0 接口 shutdown，30 秒内，可以观察到 SecPathB 和 SecPathC 上的路由 11.0.0.0/8 变成不可达。

在调整定时器之前，SecPathA 的 Ethernet2/0/0 接口 shutdown 后，SecPathB 和 SecPathC 需要 180 秒的时间才能感知到路由不可达，可见，调整定时器后，RIP 网络的收敛时间缩短了。

3.4.3 RIP 非直连邻居的路由交互配置举例

1. 组网需求

如下图所示，SecPathB 不支持 RIP 协议。SecPathA 在 e1/0/0 口使能 RIP，引入直连路由，并配置指向 2.0.0.0/8 的静态路由；SecPath C 上在 e1/0/0 口使能 RIP，引入直连路由，并配置指向 1.0.0.0/8 的静态路由。SecPath A 和 SecPath C 上配置互为 RIP peer，取消检查收到的 RIP 报文的源地址。最终实现在 SecPath A 上获得到 SecPath C 的 200.0.0.1/24 RIP 路由，SecPathC 上也能获得到 SecPathA 的 100.0.0.1/8 RIP 路由。

2. 组网图

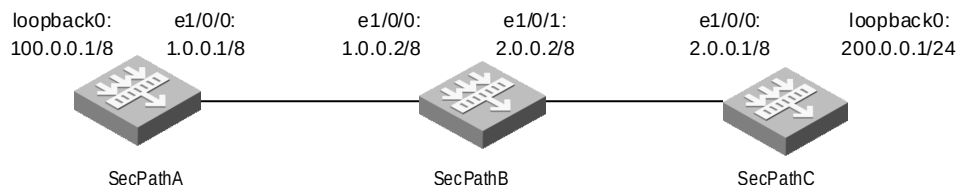


图3-4 RIP 非直连邻居的路由交互配置举例

3. 配置步骤

(1) 配置 SecPathA

配置接口 IP 地址。

```
[H3C] interface Ethernet1/0/0
[H3C-Ethernet1/0/0] ip address 1.0.0.1 255.0.0.0
[H3C-Ethernet1/0/0] rip version 2
[H3C-Ethernet1/0/0] interface LoopBack0
[H3C-LoopBack0] ip address 100.0.0.1 255.0.0.0
```

配置启动 RIP 协议。

```
[H3C] rip
[H3C-rip] undo summary
[H3C-rip] network 1.0.0.0
```

配置启动 RIP peer，并配置不检查 RIP 报文源地址。

```
[H3C-rip] peer 2.0.0.1
[H3C-rip] undo validate-source-address
```

配置 RIP 协议引入直连路由。

```
[H3C-rip] import-route direct
```

配置到 2.0.0.0 网段的静态路由。

```
[H3C] ip route-static 2.0.0.0 255.0.0.0 1.0.0.2 preference 60
```

(2) 配置 SecPathB

配置接口 IP 地址。

```
[H3C] interface Ethernet1/0/0
[H3C-Ethernet1/0/0] ip address 1.0.0.2 255.0.0.0
[H3C-Ethernet1/0/0] interface Ethernet1/0/1
[H3C-Ethernet1/0/1] ip address 2.0.0.2 255.0.0.0
[H3C-Ethernet1/0/1] quit
```

配置到 200.0.0.0/24 网段的静态路由。

```
[H3C] ip route-static 200.0.0.0 255.255.255.0 2.0.0.1
```


配置到 100.0.0.0/8 网段的静态路由。

```
[H3C] ip route-static 100.0.0.0 255.0.0.0 1.0.0.1
```

(3) 配置 SecPathC

配置接口 IP 地址。

```
[H3C] interface Ethernet1/0/0
```

```
[H3C-Ethernet1/0/0] ip address 2.0.0.1 255.0.0.0
```

```
[H3C-Ethernet1/0/0] rip version 2
```

```
[H3C-Ethernet1/0/0] interface LoopBack0
```

```
[H3C-LoopBack0] ip address 200.0.0.1 255.255.255.0
```

启动 RIP 协议。

```
[H3C] rip
```

```
[H3C-rip] undo summary
```

```
[H3C-rip] network 2.0.0.0
```

配置 RIP peer，并配置不检查收到的 RIP 报文。

```
[H3C-rip] peer 1.0.0.1
```

```
[H3C-rip] undo validate-source-address
```

配置进入直连路由。

```
[H3C-rip] import-route direct
```

配置到 1.0.0.0 网段的静态路由。

```
[H3C] ip route-static 1.0.0.0 255.0.0.0 2.0.0.2 preference 60
```

在 SecPathA，SecPathC 上必须配置到达对端的静态路由，保证路由可达，否则 RIP 报文无法发送给 peer。

另外，若 SecPathC 为 PE，则需要配置 RIP 多实例，并在 RIP 的地址族视图下配置取消检查 RIP 接收报文：

配置 vpn-instance。

```
[H3C] ip vpn-instance in
```

```
[H3C-vpn-in] route-distinguisher 100:1
```

```
[H3C-vpn-in] vpn-target 100:1 export-extcommunity
```

```
[H3C-vpn-in] vpn-target 100:1 import-extcommunity
```

配置 RIP 多实例。

```
[H3C] rip
```

```
[H3C-rip] ipv4-family vpn-instance in
```

```
[H3C-rip-af-vpn-instance] undo validate-source-address
```

3.5 RIP 故障诊断与排除

故障之一：在物理连接正常的情况下收不到更新报文。

故障排除，可能是下列原因：

相应的接口上 RIP 没有运行（如执行了 **undo rip work** 命令）或该接口未通过 **network** 命令使能。对端防火墙、路由器上配置的是组播方式（如执行了 **rip version 2 multicast** 命令），但在本地防火墙上没有配置组播方式。

故障之二：运行 RIP 的网络发生路由震荡。

故障排除：在各运行 RIP 的防火墙、路由器上使用 **display rip** 命令查看 RIP 定时器的配置，如果不同设备的 **Period Update** 定时器和 **Timeout** 定时器值不同，重新将全网的定时器配置一致，并确保 **Timeout** 定时器时间长度大于 **Period Update** 定时器的时间长度。

第4章 OSPF 配置

4.1 OSPF 简介

4.1.1 OSPF 概述

OSPF 是 Open Shortest Path First（开放最短路由优先协议）的缩写。它是 IETF 组织开发的一个基于链路状态的内部网关协议。目前使用的是版本 2（RFC2328），其特性如下：

- 适应范围——支持各种规模的网络，最多可支持几百台路由器。
- 快速收敛——在网络的拓扑结构发生变化后立即发送更新报文，使这一变化在自治系统中同步。
- 无自环——由于 OSPF 根据收集到的链路状态用最短路径树算法计算路由，从算法本身保证了不会生成自环路由。
- 区域划分——允许自治系统的网络被划分成区域来管理，从而减少了占用的网络带宽。
- 等价路由——支持到同一目的地址的多条等价路由。
- 路由分级——使用 4 类不同的路由，按优先顺序来说分别是：区域内路由、区域间路由、第一类外部路由、第二类外部路由。
- 支持验证——支持基于接口的报文验证以保证路由计算的安全性。
- 组播发送——支持组播地址。

4.1.2 OSPF 的路由计算过程

OSPF 协议的路由计算过程可简单描述如下：

- 每个支持 OSPF 协议的路由器都维护着一份描述整个自治系统拓扑结构的链路状态数据库（Link State Database，简称为 LSDB）。每台路由器根据自己周围的网络拓扑结构生成链路状态广播（Link State Advertisement，简称为 LSA），通过相互之间发送协议报文将 LSA 发送给网络中其它路由器。这样每台路由器都收到了其它路由器的 LSA，所有的 LSA 一起组成链路状态数据库。

- 由于 LSA 是对路由器周围网络拓扑结构的描述，那么 LSDB 则是对整个网络的拓扑结构的描述。路由器很容易将 LSDB 转换成一张带权的有向图，这张图便是对整个网络拓扑结构的真实反映。显然，各个路由器得到的是一张完全相同的图。
- 每台路由器都使用 SPF 算法计算出一棵以自己为根的最短路径树，这棵树给出了到自治系统中各节点的路由，外部路由信息为叶子节点，外部路由可由广播它的路由器进行标记以记录关于自治系统的额外信息。显然，各个路由器各自得到的路由表是不同的。

此外，为使每台路由器能将本地状态信息（如可用接口信息、可达邻居信息等）广播到整个自治系统中，在路由器之间要建立多个邻接关系，这使得任何一台路由器的路由变化都会导致多次传递，既没有必要，也浪费了宝贵的带宽资源。为解决这一问题，OSPF 协议定义了“指定路由器”（DR），所有路由器都只将信息发送给 DR，由 DR 将网络链路状态广播出去。这样就减少了多址访问网络上各路由器之间邻接关系的数量。

OSPF 协议支持基于接口的报文验证以保证路由计算的安全性；并使用 IP 多播方式发送和接收报文。

4.1.3 OSPF 相关的基本概念

1. Router ID

一台路由器如果要运行 OSPF 协议，必须存在 Router ID。如果没有配置 Router ID，系统会选择所有 loopback 接口中最大的 IP 地址作为路由器的 Router ID。如果没有 loopback 接口，系统会选择所有物理接口的最大 IP 地址作为路由器的 Router ID。一般建议选择 loopback 接口的 IP 地址作为本机 ID 号，因为该接口永远处于 UP 状态（除非手工 shutdown）。

2. DR 和 BDR

- DR（Designated Router，指定路由器）

在广播网络或者多点访问网络中，为使每台路由器能将本地状态信息广播到整个自治系统中，在路由器之间要建立多个邻居关系，但这使得任何一台路由器的路由变化都会导致多次传递，浪费了宝贵的带宽资源。为解决这一问题，OSPF 协议定义了 DR，所有路由器都只将信息发送给 DR，由 DR 将网络链路状态广播出去，除 DR/BDR 外的路由器（称为 DR Other）之间将不再建立邻居关系，也不再交换任何路由信息。

哪一台路由器会成为本网段内的 DR 并不是人为指定的，而是由本网段中所有的路由器共同选举出来的。

- BDR（Backup Designated Router，备份指定路由器）

如果 DR 由于某种故障而失效，这时必须重新选举 DR，并与之同步。这需要较长的时间，在这段时间内，路由计算是不正确的。为了能够缩短这个过程，OSPF 提出了 BDR 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，并重新选举 BDR。

3. 区域（Area）

随着网络规模日益扩大，当一个网络中的 OSPF 路由器数量非常多时，会导致 LSDB 变得很庞大，占用大量存储空间，并消耗很多 CPU 资源来进行 SPF 计算。并且，网络规模增大后，拓扑结构发生变化的概率也会增大，导致大量的 OSPF 协议报文在网络中传递，降低网络的带宽利用率。

OSPF 协议将自治系统划分成多个区域（Area）来解决上述问题。区域在逻辑上将路由器划分为不同的组。不同的区域以区域号（Area ID）标识，其中一个最重要的区域是区域 0，也称为骨干区域（backbone area）。

骨干区域完成非骨干区域之间的路由信息交换，它必须是连续的，对于物理上不连续的区域，需要配置虚连接（virtual links）来保持骨干区域在逻辑上的连续性。

连接骨干区域和非骨干区域的路由器称作区域边界路由器（Area Border Router，简称为 ABR）。

OSPF 中还有一类自治系统边界路由器（Autonomous System Boundary Router，简称为 ASBR），实际上，这里的 AS 并不是严格意义的自治系统，连接 OSPF 路由域（routing domain）和其它路由协议域的路由器都是 ASBR，可以认为 ASBR 是引入 OSPF 外部路由信息的路由器。

4. 路由聚合

AS 被划分成不同的区域，每一个区域通过 OSPF 边界路由器（ABR）相连，区域间可以通过路由汇聚来减少路由信息，减小路由表的规模，提高路由器的运算速度。

ABR 在计算出一个区域的区域内路由之后，查询路由表，将其中每一条 OSPF 路由封装成一条 LSA 发送到区域之外。

例如，图 4-1 中，Area 19 内有三条区域内路由 19.1.1.0/24，19.1.2.0/24，19.1.3.0/24，如果此时配置了路由聚合，将三条路由聚合成一条 19.1.0.0/16，在 RTA 上就只生成一条描述聚合后路由的 LSA。

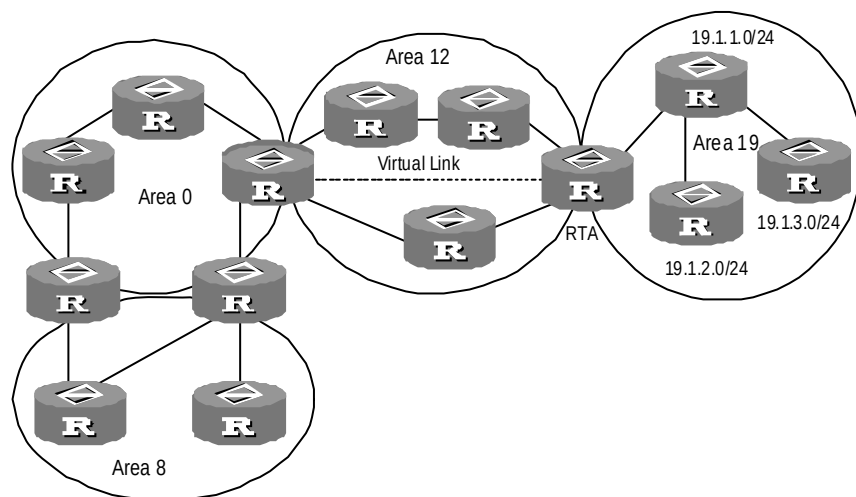


图4-1 区域及路由聚合示意图

4.1.4 OSPF 的协议报文

OSPF 有五种报文类型：

- HELLO 报文（Hello Packet）：

最常用的一种报文，周期性的发送给本路由器的邻居。HELLO 报文的内容包括一些定时器的数值、DR、BDR 以及自己已知的邻居。

- DD 报文（Database Description Packet）：

两台路由器进行数据库同步时，用 DD 报文来描述自己的 LSDB，内容包括 LSDB 中每一条 LSA 的摘要（摘要是指 LSA 的 HEAD，通过该 HEAD 可以唯一标识一条 LSA）。这样做是为了减少路由器之间传递信息的量，因为 LSA 的 HEAD 只占一条 LSA 的整个数据量的一小部分，根据 HEAD，对端路由器就可以判断出是否已有这条 LSA。

- LSR 报文（Link State Request Packet）：

两台路由器互相交换 DD 报文之后，知道对端的路由器有哪些 LSA 是本地的 LSDB 所缺少的，这时需要发送 LSR 报文向对方请求所需的 LSA。内容包括所需要的 LSA 的摘要。

- LSU 报文（Link State Update Packet）：

用来向对端路由器发送所需要的 LSA，内容是多条 LSA（全部内容）的集合。

- LSAck 报文（Link State Acknowledgment Packet）

用来对接收到的 LSU 报文进行确认。内容是需要确认的 LSA 的 HEAD（一个报文可对多个 LSA 进行确认）。

4.1.5 OSPF 的 LSA 类型

1. 五类基本的 LSA

根据前面几节的介绍可以了解到，链路状态广播报文 LSA 是 OSPF 协议计算和维护路由信息的主要来源。在 RFC2328 中定义了五类 LSA，描述如下：

- **Router-LSAs:** 第一类 LSA (Type-1)，由每个路由器生成，描述本路由器的链路状态和花费，只在路由器所处区域内传播。
- **Network-LSAs:** 第二类 LSA (Type-2)，由广播网络和 NBMA 网络的 DR 生成，描述本网段的链路状态，只在 DR 所处区域内传播。
- **Summary-LSAs:** 包含第三类 LSA 和第四类 LSA (Type-3, Type-4)，由区域边界路由器 ABR 生成，在与该 LSA 相关的区域内传播。每一条 Summary-LSA 描述一条到达本自治系统的、其它区域的某一目的地的路由（即区域间路由：inter-area route）。Type-3 Summary-LSAs 描述去往网络的路由（目的地为网段），Type-4 Summary-LSAs 描述去往自治系统边界路由器 ASBR 的路由。
- **AS-external-LSAs:** 第五类 LSA (Type-5)，由自治系统边界路由器 ASBR 生成，描述到达其它 AS 的路由，传播到整个 AS（Stub 区域除外）。AS 的缺省路由也可以用 AS-external-LSAs 来描述。

2. 第七类 LSA

在 RFC1587 (OSPF NSSA Option) 中增加了一类新的 LSA：NSSA LSAs，也称为 Type-7 LSAs。

根据 RFC1587 的描述，Type-7 LSAs 与 Type-5 LSAs 主要有以下两点区别：

- Type-7 LSAs 在 NSSA 区域 (Not-So-Stubby Area) 内产生和发布；但 NSSA 区域内不会产生或发布 Type-5 LSAs。
- Type-7 LSAs 只能在一个 NSSA 内发布，当到达区域边界路由器 ABR 时，由 ABR 将 Type-7 LSAs 转换成 Type-5 LSAs 再发布，不直接发布到其它区域或骨干区域。

3. Opaque LSAs

为了使 OSPF 能够支持更多新的业务应用，在 RFC2370 (The OSPF Opaque LSA) 中定义了用于对 OSPF 进行扩展的 Opaque LSAs。

Opaque LSAs 包含三种类型的 LSA，不同类型的 LSA 扩散范围不同：

- **Type-9:** 扩散范围为 link-local，可以认为只在某一个接口所在的网段扩散，不会发布到本地网段或本地子网以外。

- **Type-10:** 扩散范围为 area-local，即，只在本区域以内扩散。
- **Type-11:** 与 Type-5 LSAs 具有相同的扩散范围，可以在除 STUB 区域和 NSSA 区域之外的整个自治系统内部扩散。

Opaque LSAs 包括一个标准的 20 字节 LSA 头和一个应用信息相关的域，其报文结构如下图所示：

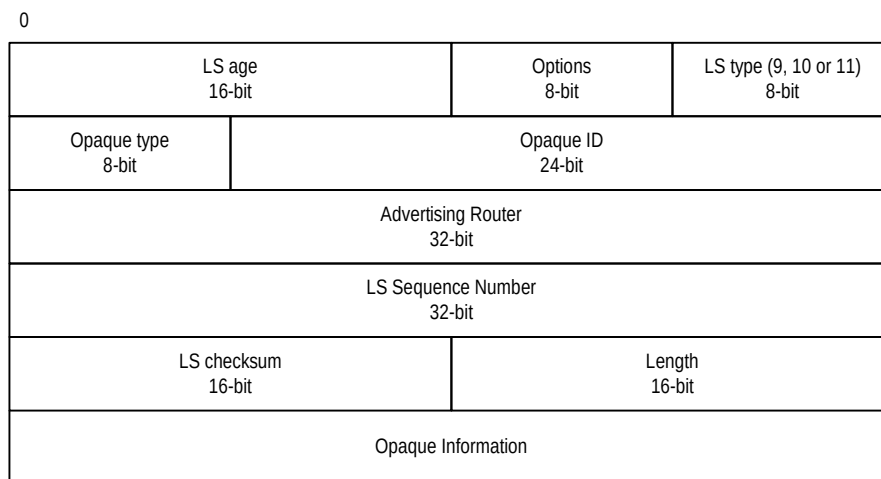


图4-2 Opaque LSAs 结构示意图

其中，Opaque Type 字节用来标识此 LSA 的应用类型，Opaque ID 则对同一应用类型的 LSA 做进一步的区分。

Opaque Information 字段中是 LSA 携带的信息，具体的信息格式可由不同的应用根据自己的需求来定义。

4.1.6 Comware 支持的 OSPF 特性

在 Comware 目前的实现中，支持以下 OSPF 特性：

- 支持 OSPF STUB 区域；
- 支持 OSPF NSSA 区域；
- 支持 OSPF 多进程（Multi-Process），可以在一台路由器上运行多个 OSPF 进程；
- 支持 OSPF 多实例（Multi-VPN-Instance），可以作为 VPN 内部路由协议，在 MPLS VPN 解决方案的 CE-PE 之间运行；

OSPF 在 MPLS VPN 中的应用请参考本手册“VPN”部分。

4.2 OSPF 的配置

在各项配置中，必须先启动 OSPF、指定接口与区域号后，才能配置其它的功能特性。

而配置与接口相关的功能特性不受 OSPF 是否使能的限制。需要注意的是，在关闭 OSPF 后，原来与 OSPF 相关的接口参数也同时失效。

(1) 基本的 OSPF 配置

对于基本的 OSPF 配置，需要进行的操作包括：

- 配置 Router ID
- 启动 OSPF
- 进入 OSPF 区域视图
- 在指定网段使能 OSPF

如果 OSPF 的骨干区域不连续，则需要：

- 配置 OSPF 虚连接

根据 OSPF 的网络类型不同，可能还需要进行以下配置：

- 配置 OSPF 网络类型
- 配置邻接点

(2) OSPF 路由的管理

- 配置 OSPF 的路由引入
- 配置 OSPF 的路由过滤
- 配置 OSPF 的路由聚合

(3) OSPF 协议本身的参数配置

- 配置 OSPF 优先级
- 配置 OSPF 定时器
- 配置选举 DR 时的优先级
- 配置接口发送报文的开销
- 配置 OSPF 的 SPF 计算间隔
- 配置发送链路状态更新报文所需时间
- 配置接口发送 DD 报文时是否填充 MTU 值
- 配置 OSPF 等价路由的最大个数

(4) 安全性考虑

为提高 OSPF 在交换路由信息时的安全性，或控制 OSPF 报文的扩散范围，可以选择以下配置：

- 配置 OSPF 认证
 - 配置接口的工作状态
- (5) OSPF 高级特性的配置
- 配置 OSPF 的 STUB 区域
 - 配置 OSPF 的 NSSA 区域
 - 使能 OSPF 的 Opaque 能力
 - 配置 OSPF 与网管系统的配合
 - 重启 OSPF

 说明：

OSPF 多实例的具体应用和在 MPLS VPN 中的配置，请参考本手册的“VPN”部分。

4.2.1 配置 Router ID

路由器的 ID 是一个 32 比特无符号整数，采用 IP 地址形式，是一台路由器在自治系统中的唯一标识。路由器的 ID 可以手工配置，如果没有配置 ID 号，系统会选择所有 loopback 接口中最大的 IP 地址作为路由器的 Router ID。如果没有 loopback 接口，系统会选择所有物理接口的最大 IP 地址作为路由器的 Router ID。手工配置路由器的 ID 时，必须保证自治系统中任意两台路由器的 ID 都不相同。通常的做法是将路由器的 ID 配置为与该路由器某个接口的 IP 地址一致。

请在系统视图下进行下列配置。

表4-1 配置路由器 ID 号

操作	命令
配置防火墙的 Router ID 号	router id router-id
取消防火墙的 Router ID 号	undo router id

为保证 OSPF 运行的稳定性，在进行网络规划时，应确定防火墙的 Router ID 的划分并手工配置。

 说明：

OSPF 启动后修改的 Router ID，需要重新启动 OSPF 进程之后，Router ID 才能在 OSPF 中生效。

4.2.2 启动 OSPF

防火墙支持 OSPF 多进程，一台防火墙上启动的多个 OSPF 进程之间由不同的进程号区分。OSPF 进程号在启动 OSPF 时进行设置，它只在本地有效，不影响与其它路由器之间的报文交换。

请在系统视图下进行下列配置。

表4-2 启动/关闭 OSPF

操作	命令
启动 OSPF，进入 OSPF 视图	ospf [<i>process-id</i> [[router-id <i>router-id</i>] vpn-instance <i>vpn-instance-name</i>]]
关闭 OSPF 路由协议进程	undo ospf [<i>process-id</i>]

缺省情况下，不运行 OSPF。

启用 OSPF 时，需要注意：

- 如果在启动 OSPF 时不指定进程号，将使用缺省的进程号 1；关闭 OSPF 时不指定进程号，缺省关闭进程 1。
- 在同一个区域中的进程号必须一致，否则会造成进程之间的隔离。
- 当在一台防火墙上运行多个 OSPF 进程时，建议用户使用以上命令中的 **router-id** 为不同进程指定不同的 Router ID。
- 以上命令中的 **vpn-instance** 用于将 OSPF 进程与 VPN 实例进行绑定，用于 MPLS VPN 解决方案，详细介绍请参考本手册的“VPN”部分。

4.2.3 进入 OSPF 区域视图

OSPF 协议将自治系统划分成不同的区域（Area），在逻辑上将路由器分为不同的组。在区域视图下可以进行区域相关配置。

请在 OSPF 视图下进行下列配置。

表4-3 进入 OSPF 区域视图

操作	命令
进入 OSPF 区域视图	area <i>area-id</i>
删除指定的 OSPF 区域	undo area <i>area-id</i>

区域 ID 可以采用十进制整数或 IP 地址形式输入，但显示时使用 IP 地址形式。

在配置同一区域内的 OSPF 路由器时，应注意：大多数配置数据都应该对区域统一考虑，否则可能会导致相邻路由器之间无法交换信息，甚至导致路由信息的阻塞或者产生路由环。

4.2.4 在指定网段使能 OSPF

在系统视图下使用 **ospf** 命令启动 OSPF 后，还必须指定在哪个网段上应用 OSPF。请在 OSPF 区域视图下进行下列配置。

表4-4 在指定网段使能 OSPF

操作	命令
指定网段运行 OSPF 协议	network <i>ip-address wildcard-mask</i>
取消网段运行 OSPF 协议	undo network <i>ip-address wildcard-mask</i>

一台路由器可能同时属于不同的区域（这样的路由器称作 ABR），但一个网段只能属于一个区域。

4.2.5 配置 OSPF 虚连接

OSPF 协议规定：所有非骨干区域必须与骨干区域保持连通，即 ABR 上至少有一个接口应在区域 0.0.0.0 中。如果一个区域与骨干区域 0.0.0.0 没有直接的物理连接，就必须建立虚连接来保持逻辑上的连通。

虚连接是在两台 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。它的两端必须都是 ABR，并且必须在两端同时配置。虚连接由对端路由器的 Router ID 来标识。为虚连接提供非骨干区域内部路由的区域称为运输区域（Transit Area）。虚连接在穿过转换区域的路由计算出来后被激活，相当于在两个端点之间形成一个点到点连接，这个连接与物理接口类似，可以配置接口的各参数，如 Hello 报文的发送间隔等。

虚连接的配置是在 Transit 区域进行的。

请在 OSPF 区域视图下进行下列配置。

表4-5 配置 OSPF 虚连接

操作	命令
创建并配置虚连接	vlink-peer <i>router-id</i> [hello <i>seconds</i> retransmit <i>seconds</i> trans-delay <i>seconds</i> dead <i>seconds</i> simple password md5 keyid key] *
取消创建的虚连接	undo vlink-peer <i>router-id</i>

缺省情况下，**hello** 的值为 10 秒；**retransmit** 的值为 5 秒；**trans-delay** 的值为 1 秒；**dead** 的值为 40 秒。

将虚连接看做“逻辑通道”是因为：两个 ABR 之间的 OSPF 路由器只对报文进行透明转发（由于协议报文的地址不是这些路由器，所以这些报文对于他们而言是透明的，只是当作普通的 IP 报文转发），两台 ABR 之间直接传递路由信息。这

里的路由信息是指由 ABR 生成的 Type3 LSAs，区域内的路由器同步方式没有因此改变。

4.2.6 配置 OSPF 网络类型

OSPF 以本路由器邻接网络的拓扑结构为基础计算路由。每台路由器将自己邻接的网络拓扑描述出来，传递给所有其它的路由器。

根据链路层协议类型，OSPF 将网络分为四种类型：

- 广播类型：链路层协议是 Ethernet、FDDI 等。
- 非广播多路访问 Non Broadcast MultiAccess (NBMA) 类型：链路层协议是帧中继、ATM 或 X.25 时。
- 点到多点 Point-to-Multipoint (p2mp) 类型：没有一种链路层协议会被缺省的认为是 Point-to-Multipoint 类型。点到多点是由其它网络类型强制更改的。常见的做法是将非全连通的 NBMA 改为点到多点的网络。
- 点到点 Point-to-Point (p2p) 类型：链路层协议是 PPP 或 LAPB。

NBMA 网络是指非广播、多点可达的网络，典型的有帧中继、ATM。可通过配置轮询间隔来指定路由器在与相邻路由器构成邻接关系之前发送轮询 Hello 报文的时间周期。

在没有多址访问能力的广播网上，可将接口配置成 **nbma** 方式。

若在 NBMA 网络中并非所有路由器之间都直接可达时，可将接口配置成 **p2mp** 方式。

若该路由器在 NBMA 网络中只有一个对端，则也可将接口类型改为 **p2p** 方式。

NBMA 与 p2mp 之间的区别：

- 在 OSPF 协议中 NBMA 是指那些全连通的、非广播、多点可达网络。而点到多点的网络，则并不需要一定是全连通的。
- 在 NBMA 上需要选举 DR 与 BDR，而在点到多点网络中没有 DR 与 BDR。
- NBMA 是一种缺省的网络类型，例如：如果链路层协议是 ATM，OSPF 会缺省的认为该接口的网络类型是 NBMA（不论该网络是否全连通）。点到多点不是缺省的网络类型，没有哪种链路层协议会被认为是点到多点，点到多点是由其它的网络类型强制更改的。最常见的做法是将非全连通的 NBMA 改为点到多点的网络。
- NBMA 用单播发送报文，需要手工配置邻居。点到多点采用多播方式发送报文。

请在接口视图下进行下列配置。

表4-6 配置 OSPF 接口的网络类型

操作	命令
配置接口的网络类型	ospf network-type { broadcast nbma p2mp p2p }
恢复接口缺省的网络类型	undo ospf network-type

缺省情况下，OSPF 根据链路层类型得出网络类型。如果用户为接口配置了新的网络类型，原接口的网络类型自动取消。

4.2.7 配置邻接点

对于接口类型为 NBMA 的网络，由于无法通过广播 Hello 报文的形式发现相邻路由器，必须手工为其指定相邻路由器的 IP 地址，并说明该相邻路由器是否有选举权。请在 OSPF 视图下进行下列配置。

表4-7 配置邻接点

操作	命令
配置 NBMA 接口的邻接点	peer ip-address [dr-priority dr-priority-number]
取消配置 NBMA 接口的邻接点	undo peer ip-address

缺省情况下，NBMA 接口的邻接点优先级的取值为 1。

使用 **ospf dr-priority** 命令和使用 **peer** 命令设置的优先级具有不同的用途：

- **ospf dr-priority** 命令设置的优先级用于实际的 DR 选举；
- **peer** 命令设置的优先级用于表示邻居是否具有选举权。如果在配置邻居时将优先级指定为 0，则本地路由器认为该邻居不具备选举权，不向该邻居发送 Hello 报文，这种配置可以减少在 DR 和 BDR 选举过程中网络上的 Hello 报文数量。但如果本地路由器是 DR 或 BDR，它也会向优先级为 0 的邻居发送 Hello 报文，以建立邻接关系。

4.2.8 配置 OSPF 的路由引入

1. 引入其它协议的路由

防火墙上各动态路由协议之间可以互相共享路由信息，由于 OSPF 的特性，其它的路由协议发现的路由总被当作自治系统外部的路由信息处理。可以指定路由的花费类型、花费值和标记以覆盖缺省的路由接收参数。

OSPF 使用 4 类不同的路由，按优先顺序排列如下：

- 区域内路由
- 区域间路由

- 第一类外部路由
- 第二类外部路由

区域内和区域间路由描述自治系统内部的网络结构；外部路由则描述了如何选择到自治系统以外目的地的路由。

第一类外部路由是指接收的是 IGP 路由（例如 RIP, Static），由于这类路由的可信程度较高，所以，计算出的外部路由的花费与自治系统内部的路由花费的数量级相同，并且与 OSPF 自身路由的花费具有可比性，即：到第一类外部路由的花费值 = 本路由器到相应的 ASBR 的花费值 + ASBR 到该路由目的地址的花费值。

第二类外部路由是指接收的是 EGP 路由，由于这类路由的可信度比较低，所以 OSPF 协议认为，从 ASBR 到自治系统之外的花费远远大于在自治系统之内到达 ASBR 的花费，计算路由花费时主要考虑前者。即，到第二类外部路由的花费值 = ASBR 到该路由目的地址的花费值。如果该值相等，再考虑本路由器到相应的 ASBR 的花费值。

请在 OSPF 视图下进行下列配置。

表4-8 引入其它协议的路由

操作	命令
引入其它协议的路由信息	import-route protocol [allow-ibgp] [cost value] [type { 1 2 }] [tag value] [route-policy route-policy-name]
取消引入其它协议的路由信息	undo import-route protocol

缺省情况下，OSPF 将不引入其它协议的路由信息。当配置引入其它协议的路由信息时，缺省情况下，cost 为 1，type 为 2，tag 为 1。

当 *protocol* 为 BGP 时，**allow-ibgp** 为可选关键字。**import-route bgp** 表示只引入 EBGp 路由，**import-route bgp allow-ibgp** 表示将 IBGP 路由也引入，该配置危险，请慎用！

可引入的路由包括 **direct**、**static**、RIP 与 BGP，也可以引入其它进程的 OSPF 路由。

2. 配置 OSPF 引入外部路由的参数

当 OSPF 将其它路由协议发现的路由信息引入到本自治系统中时，还需要配置一些额外的参数，如引入路由的缺省花费和缺省标记等。路由标记可以用来标识协议相关的信息，如 OSPF 接收 BGP 时用来区分自治系统的编号。

请在 OSPF 视图下进行下列配置。

表4-9 配置 OSPF 引入外部路由的参数

操作	命令
配置 OSPF 引入外部路由的最小时间间隔	default interval seconds
恢复引入外部路由最小时间间隔的缺省值	undo default interval
配置 OSPF 每次引入路由的数量上限	default limit routes
恢复每次引入外部路由数量上限的缺省值	undo default limit
配置 OSPF 在接收外部路由时缺省的花费值	default cost value
恢复 OSPF 在接收外部路由时花费的缺省值	undo default cost
配置 OSPF 在接收外部路由时缺省的标记值	default tag tag
恢复 OSPF 在接收外部路由时标记的缺省值	undo default tag
配置 OSPF 在接收外部路由时缺省的类型	default type { 1 2 }
恢复 OSPF 接收外部路由类型的缺省值	undo default type

缺省情况下，引入外部路由时的 **cost** 为 1，**tag** 为 1，路由的类型为 **Type 2**；引入外部路由的时间间隔为 1 秒；每次可引入的外部路由上限为 1000 条。

4.2.9 在 OSPF 中生成缺省路由

缺省情况下，普通的 OSPF 区域（骨干区域和非骨干区域）中是没有缺省路由的，**import-route** 命令也无法向 OSPF 路由域中引入缺省路由。

命令 **default-route-advertise** 可以在 OSPF 路由域中生成并发布缺省路由，使用这条命令时，需要了解以下几点：

- 在普通 OSPF 区域的 ASBR 上执行 **default-route-advertise** 命令，将生成一条 **Type-5 LSA** 向 OSPF 路由域内发布缺省路由；
- 在 **NSSA** 区域的 ASBR 或 ABR 上执行此命令，将生成一条 **Type-7 LSA** 向 **NSSA** 区域内发布缺省路由；
- 此命令对于 **Stub** 区域或完全 **Stub** 区域无效；
- 缺省情况下，对于 ASBR，只有当路由表中已经存在一条缺省路由时，OSPF 才会生成相应的 **Type-5 LSA** 或 **Type-7 LSA**；
- 发布缺省路由的 **Type-5 LSA** 或 **Type-7 LSA** 的扩散范围与普通的 **Type-5 LSA** 或 **Type-7 LSA** 相同。

请在 OSPF 视图下进行下列配置。

表4-10 在 OSPF 中生成缺省路由

操作	命令
在 OSPF 中生成缺省路由	default-route-advertise [always cost value type value route-policy route-policy-name] *
取消生成的缺省路由	undo default-route-advertise [always cost type route-policy] *

缺省情况下，OSPF 中没有缺省路由。

如果在生成缺省路由时使用了参数 **always**，则不论路由表中是否存在缺省路由，OSPF 都将生成一条 Type-5 或 Type-7 LSA。这个参数只对 ASBR 有效，应谨慎使用。

由于 OSPF 在进行 SPF 运算时不计算自己生成的 LSA，所以，本路由器上的 OSPF 路由中并不存在缺省路由。为保证路由信息的正确性，应只在那些与外部网络相连的路由器上配置引入缺省路由。

说明：

在 OSPF 路由器上配置 **default-route-advertise** 命令后，这台路由器就成为 ASBR，这一点与在 OSPF 路由器上配置 **import-route** 命令的效果类似。

对于 NSSA 区域的 ABR 或 ASBR，**default-route-advertise** 命令的效果与 **nssa default-route-advertise** 相同。

4.2.10 配置 OSPF 的路由过滤

请在 OSPF 视图下进行下列配置。

1. 对接收的路由进行过滤

OSPF 接收到 LSAs 后，可以根据一定的过滤条件来决定是否将计算后得到的路由信息加入路由表中。

表4-11 配置 OSPF 对引入路由的过滤

操作	命令
配置对接收路由信息进行过滤	filter-policy { acl-number ip-prefix ip-prefix-name gateway ip-prefix-name } import
取消对接收路由信息进行过滤	undo filter-policy { acl-number ip-prefix ip-prefix-name gateway ip-prefix-name } import

**注意：**

此命令仅能阻止路由信息被加入到路由表中，但相关的 LSAs 仍然被通告到其它邻居。

2. 对引入的路由进行过滤

filter-policy export 配置 ASBR 路由器对引入到 OSPF 的外部路由进行过滤，实际上是对向外发布的引入路由的 LSA 进行过滤，该命令只对 ASBR 路由器有效。

表4-12 配置 OSPF 对发布路由的过滤

操作	命令
配置 OSPF 对向外发布的引入路由的 LSA 进行过滤	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } export [<i>routing-protocol</i>]
取消 OSPF 对向外发布的引入路由的 LSA 进行过滤	undo filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } export [<i>routing-protocol</i>]

缺省情况下，OSPF 不对引入或发布的路由信息进行过滤。

**说明：**

filter-policy import 命令只对从邻居收到的本进程 OSPF 路由进行过滤，没有通过过滤的路由将不被加入路由表。

filter-policy export 命令只对本机使用 **import-route** 引入的路由起作用。如果仅配置了 **filter-policy export**，而没有配置 **import-route** 命令引入其它外部路由（包括不同进程的 OSPF 路由），**filter-policy export** 不起作用，因为 OSPF 是通过 LSA 发布路由信息，不是通过路由表。

如果在 **filter-policy export** 命令中没有指定对哪种类型的路由过滤，则对本机使用 **import-route** 引入的所有类型的路由有效。

4.2.11 配置 OSPF 的路由聚合

1. 配置 OSPF 区域路由聚合

路由聚合是指：具有相同前缀的路由信息，ABR 可以将它们聚合在一起，只发布一条路由到其它区域。一个区域可以配置多条聚合网段，这样 OSPF 可以对多个网段进行聚合。ABR 向其它区域发送路由信息时，以网段为单位生成 Type 3 LSA。如果该区域中存在一些连续的网段，则可以使用 **abr-summary** 命令将这些连续的网段聚合成一个网段。这样 ABR 只发送一条聚合后的 LSA，所有落入本命令指定的聚合网段范围的 LSA 将不再会被单独发送出去，这样可减少其它区域中 LSDB 的规模。

如果该网段范围用关键字 **not-advertise** 限定，则到这一网段路由的摘要信息将不会被广播出去。这个网段由 IP 地址/掩码标识。

需要注意的是：路由聚合只有在 ABR 上配置才会有效。

请在 OSPF 区域视图下进行下列配置。

表4-13 配置 OSPF 区域路由聚合

操作	命令
配置 OSPF 区域路由聚合	abr-summary <i>ip-address mask</i> [advertise not-advertise]
取消 OSPF 区域路由聚合	undo abr-summary <i>ip-address mask</i>

缺省情况下，区域边界路由器不对路由聚合。

2. 配置 OSPF 引入路由聚合

OSPF 支持对引入路由进行聚合。

请在 OSPF 视图下进行下列配置。

表4-14 配置 OSPF 引入路由聚合

操作	命令
配置 OSPF 对引入路由进行聚合	asbr-summary <i>ip-address mask</i> [not-advertise tag value]
取消 OSPF 对引入路由进行聚合	undo asbr-summary <i>ip-address mask</i>

缺省情况下，不对引入路由进行聚合。当配置了路由聚合时，缺省情况下通告聚合路由，tag 值为 1。

配置引入路由聚合后，如果本地路由器是自治系统边界路由器 ASBR，将对引入的聚合地址范围内的 Type-5 LSA 进行聚合，当配置了 NSSA 区域时，还要对引入的聚合地址范围内的 Type-7 LSA 进行聚合。

如果本地路由器是区域边界路由器 ABR，且是 NSSA 区域的转换路由器，则对由 Type-7 LSA 转化成的 Type-5 LSA 进行聚合处理，对于不是 NSSA 区域转换路由器的则不进行聚合处理。

4.2.12 配置 OSPF 优先级

由于防火墙上可能同时运行多个动态路由协议，就存在各个路由协议之间路由信息共享和选择的问题。系统为每一种路由协议设置一个优先级，在不同协议发现同一条路由时，优先级数值小的路由将被优选。

请在 OSPF 视图下进行下列配置。

表4-15 配置 OSPF 路由的优先级

操作	命令
配置 OSPF 协议在各路由协议之间的优先级	preference [ase] preference
恢复协议缺省优先级	undo preference [ase]

缺省情况下，OSPF 协议的优先级为 10；引入外部路由协议的优先级为 150。

4.2.13 配置 OSPF 定时器

1. 配置 Hello 报文发送时间间隔

Hello 报文是一种最常用的报文，它周期性地被发送至邻居路由器，用于发现与维持邻居关系、选举 DR 与 BDR。用户可对发送 Hello 报文的时间间隔进行设置。

根据 RFC2328 的规定，要保持网络邻居间的 hello 时钟的时间间隔的一致性。需要注意的是，Hello 时钟的值与路由收敛速度、网络负荷大小成反比。

请在接口视图下进行下列配置。

表4-16 设置 Hello 报文发送时间间隔

操作	命令
配置接口发送 hello 报文的时间间隔	ospf timer hello seconds
恢复接口发送 hello 报文时间间隔的缺省值	undo ospf timer hello
在 NBMA 接口上配置发送轮询报文的时间间隔	ospf timer poll seconds
恢复发送轮询报文间隔的缺省值	undo ospf timer poll

缺省情况下，**p2p**、**broadcast** 类型接口发送 Hello 报文的时间间隔的值为 10 秒；**p2mp**、**nbma** 类型接口发送 Hello 报文的时间间隔的值为 30 秒。

缺省情况下，发送轮询 Hello 报文的时间间隔为 120 秒。轮询时间间隔至少应为 Hello 报文间隔的 3 倍。

2. 配置相邻路由器间失效时间

在一定时间间隔内，如果路由器未收到对方的 Hello 报文，则认为对端路由器失效，这个时间间隔被称为相邻路由器间的失效时间。

请在接口视图下进行下列配置。

表4-17 设置相邻路由器间失效时间

操作	命令
配置相邻路由器间失效时间	ospf timer dead seconds
恢复相邻路由器间失效时间的缺省值	undo ospf timer dead

缺省情况下, **p2p**、**broadcast** 类型接口相邻路由器间失效时间的值为 40 秒; **p2mp**、**nbma** 类型接口相邻路由器间失效时间的值为 120 秒。

需要注意的是: 在用户修改了网络类型后, Hello 报文间隔与失效时间都将恢复缺省值。

3. 配置邻接路由器重传 LSA 的间隔

当一台路由器向它的邻居发送一条 LSA 后, 需要等到对方的确认报文。若在 **retransmit** 时间内没有收到对方的确认报文, 就会向邻居重传这条 LSA。用户可对 **retransmit** 的值进行设置。

请在接口视图下进行下列配置。

表4-18 设置邻接路由器重传 LSA 的间隔

操作	命令
配置相邻路由器重传 LSA 的时间间隔	ospf timer retransmit interval
恢复相邻路由器重传 LSA 的时间间隔缺省值	undo ospf timer retransmit

缺省情况下, 相邻路由器重传 LSA 的时间间隔的值为 5 秒。

interval 的值必须大于一个报文在两台路由器之间传送一个来回的时间。

需要注意的是: 相邻路由器重传 LSA 时间间隔的值不要设置得太小, 否则将会引起不必要的重传。

4.2.14 配置选举 DR 时的优先级

广播网络或 NBMA 类型的网络需要选举指定路由器 DR (Designated Router) 和备份指定路由器 BDR (Backup Designated Router)。

路由器接口的优先级 **Priority** 将影响接口在选举 DR 时所具有资格。优先级为 0 的路由器不会被选举为 DR 或 BDR。

DR 由本网段中所有路由器共同选举。**Priority** 大于 0 的路由器都可作为“候选者”, 选票就是 Hello 报文, OSPF 路由器将自己选出的 DR 写入 Hello 报文中, 发给网段上的其它路由器。当同一网段的两台路由器都宣布自己是 DR 时, **Priority** 高的胜出。如果 **Priority** 相等, 则 Router ID 大的胜出。

如果 DR 失效，则网络中的路由器必须重新选举 DR，并与新的 DR 同步，为了缩短这个过程，OSPF 提出了 BDR（Backup Designated Router，备份指定路由器）的概念，与 DR 同时被选举出来。BDR 也与本网段内的所有路由器建立邻接关系并交换路由信息。DR 失效后，BDR 立即成为 DR，由于不需要重新选举，并且邻接关系已经建立，所以这个过程可以很快完成。这时，还需要选举出一个新的 BDR，这时不会影响路由的计算。

需要说明的是：

- 当接口优先级为 0 时，无论什么情况下都不能成为 DR/BDR，这可能造成网络上没有 DR 或 BDR。
- DR 并不一定是网段中 Priority 最大的路由器；同理，BDR 也并不一定就是 Priority 第二大的路由器。若 DR、BDR 已经选举完毕，即使有一台 Priority 值更大的路由器加入，它也不会成为该网段中的 DR。
- DR 是网段中的概念，是针对路由器的接口而言的。某台路由器在一个接口上可能是 DR，在另一个接口上可能是 BDR，或者是 DROther。
- 只有在广播或 NBMA 类型的接口时才会选举 DR，在点到点或点到多点类型的接口上不需要选举 DR。在广播网络或 NBMA 网络上，如果 OSPF 收到的 hello 报文中没有人宣称自己是 DR，则将进入选举过程；如果多个 OSPF 宣称自己是 DR/BDR，也将进入选举过程；如果已经有人宣称自己是 DR/BDR，则新加入者接受已有的 DR/BDR，无论它的优先级是多少；当 DR 失败时，BDR 将变为 DR，再选举出新的 BDR。

请在接口视图下进行下列配置。

表4-19 设置接口在选举 DR 时的优先级

操作	命令
设置接口在选举 DR 时的优先级	ospf dr-priority <i>priority_num</i>
恢复接口的缺省优先级	undo ospf dr-priority

缺省情况下，接口在选举 DR 时的优先级为 1，取值范围为 0~255。

4.2.15 配置接口发送报文的开销

用户可以在不同接口上配置发送报文的开销，从而影响路由的计算。

请在接口视图下进行下列配置。

表4-20 设置接口发送报文的开销

操作	命令
设置接口发送报文的开销	ospf cost value
将接口发送报文的开销恢复为缺省值	undo ospf cost

缺省情况下，OSPF 根据接口的速率自动计算发送报文的开销。

4.2.16 配置 OSPF 的 SPF 计算间隔

当 OSPF 的链路状态数据库 LSDB 发生改变时，需要重新计算最短路径。如果每次改变都立即计算最短路径，将占用大量资源，并会影响路由器的效率。通过调节 SPF（Shortest Path First）的计算间隔时间，可以抑制由于网络频繁变化导致占用过多资源。

请在 OSPF 视图下进行下列配置。

表4-21 设置 SPF 计算间隔

操作	命令
设置 SPF 计算间隔	spf-schedule-interval seconds
恢复 SPF 计算间隔	undo spf-schedule-interval

缺省情况下，SPF 时间间隔为 5 秒钟。

4.2.17 配置发送链路状态更新报文所需时间

链路状态更新报文（LSU）中的链路状态广播（LSA）的老化时间在传送之前要增加延迟时间。该参数的设置主要考虑到接口上发送报文所需的时间，在低速网络上，该项配置尤为重要。

请在接口视图下进行下列配置。

表4-22 配置发送 LSU 报文所需时间

操作	命令
配置 LSU 报文的传输延迟时间	ospf trans-delay seconds
恢复 LSU 报文的传输延迟时间的缺省值	undo ospf trans-delay

缺省情况下，传输延迟时间为 1 秒。

4.2.18 配置接口发送 DD 报文时是否填充 MTU 值

运行 OSPF 协议的路由器在进行数据库同步时，使用 DD（Database Description）报文描述自己的 LSDB。

用户可以使用本命令手工设定指定接口在发送时填写 DD 报文中的 MTU 值域，设定的 MTU 值是接口的实际 MTU 值。

请在接口视图下进行下列配置。

表4-23 配置接口发送 DD 报文时是否填 MTU 值

操作	命令
使能接口发送 DD 报文时填充 MTU 值	ospf mtu-enable
禁止接口发送 DD 报文时填充 MTU 值	undo ospf mtu-enable

缺省情况下，接口发送 DD 报文时不填充 MTU 值，即 DD 报文中的 MTU 值为 0。

4.2.19 配置 OSPF 等价路由的最大个数

请在 OSPF 视图下进行下面配置。

表4-24 配置 OSPF 等价路由的最大个数

操作	命令
配置 OSPF 等价路由的最大个数	multi-path-number <i>number</i>
恢复 OSPF 等价路由最大个数的缺省值	undo multi-path-number

缺省情况下，OSPF 等价路由最大个数为 3。

4.2.20 配置 OSPF 认证

1. 配置 OSPF 区域支持报文验证

在 OSPF 中，一个区域中所有的路由器的验证类型必须一致（不要求验证、要求明文验证或者要求 MD5 密文验证），但每条链路上的密码可以是不同的。使用命令 **authentication-mode simple** 为该区域配置明文验证口令；使用命令 **authentication-mode md5** 为该区域配置 MD5 密文验证字口令。

请在 OSPF 区域视图下进行下列配置。

表4-25 配置 OSPF 区域要求报文验证

操作	命令
配置区域要求报文验证	authentication-mode { simple md5 }
配置区域不要求报文验证	undo authentication-mode

缺省情况下，区域不要求报文验证。

2. 配置 OSPF 报文的认证

OSPF 支持在相邻路由器之间支持明文验证或 MD5 密文验证。

请在接口视图下进行下列配置。

表4-26 配置 OSPF 报文的认证

操作	命令
配置接口使用报文明文验证字	ospf authentication-mode simple <i>password</i>
取消接口使用报文明文验证口令	undo ospf authentication-mode simple
配置接口使用报文 MD5 密文验证字	ospf authentication-mode md5 <i>key_id</i> <i>key</i>
取消接口使用报文 MD5 密文验证	undo ospf authentication-mode md5

缺省情况下，接口未配置任何明文或 MD5 验证字。

4.2.21 配置接口的工作状态

如果要使 OSPF 路由信息不被某一网络中的路由器获得，可禁止在相应接口上发送 OSPF 报文。

不同的进程可以对同一接口禁止发送 OSPF 报文，但 **silent-interface** 命令只对本进程已经使能的 OSPF 接口起作用，不对其它进程的接口起作用。

请在 OSPF 视图下进行下列配置。

表4-27 禁止/允许接口发送 OSPF 报文

操作	命令
禁止接口发送 OSPF 报文	silent-interface <i>interface-type interface-number</i>
允许接口发送 OSPF 报文	undo silent-interface <i>interface-type interface-number</i>

缺省情况下，允许所有接口收发 OSPF 报文。

将运行 OSPF 协议的接口指定为 Silent 状态后，该接口的直连路由仍可以发布出去，但接口的 OSPF 报文将被阻塞，接口上无法建立邻居关系。这样可以增强 OSPF 的组网适应能力，减少系统资源的消耗。

4.2.22 配置 OSPF 的 STUB 区域

Stub 区域是一类特殊的 OSPF 区域，这类区域不接收或扩散 Type-5 的 LSA（AS-external-LSAs）。对于产生大量 Type-5 LSA 的网络，这种处理方式能够有效减小 Stub 区域内路由器的 LSDB 规模，并缓解 SPF 计算对路由器资源的占用。通常情况下，Stub 区域位于自治系统边界。

为保证 Stub 区域去往自治系统外的报文能被正确转发，Stub 区域的 ABR 将通过 Summary-LSA 向本区域内发布一条缺省路由，并且只在本区域扩散。

说明：

ABR 通过 Summary-LSA（Type-3 LSA）向区域内发布的缺省路由是区域间缺省路由。

配置 Stub 区域需要注意下列几点：

- 骨干区域不能配置成 Stub 区域。
- Stub 区域不能用作传输区域，即，虚连接不能穿过 Stub 区域。
- 如果想将一个区域配置成 Stub 区域，则该区域中的所有路由器必须都要配置该属性。
- 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。

请在 OSPF 区域视图下进行下列配置。

表4-28 配置 OSPF 的 Stub 区域

操作	命令
配置一个区域为 Stub 区域	stub [no-summary]
取消配置的 Stub 区域	undo stub
配置发送到 Stub 区域的缺省路由的花费值	default-cost value
恢复发送到 Stub 区域的缺省路由的缺省花费值	undo default-cost

缺省情况下，无 Stub 区域；发送到 Stub 区域的缺省路由的花费值为 1。

需要注意的是：参数 **no-summary** 只能在 ABR 上配置，如果在配置 Stub 区域的 ABR 时使用了这一参数，则此 ABR 只向区域内发布一条缺省路由的 Summary-LSA，不生成任何其它 Summary-LSAs。这种既没有 AS-external-LSAs，也没有 Summary-LSAs 的 Stub 区域，又称为完全 Stub 区域。

命令 **default-cost** 用于 Stub 区域的 ABR，配置 ABR 发送到 Stub 区域的缺省路由的花费值。

4.2.23 配置 OSPF 的 NSSA 区域

从前一节的描述中我们可以了解到，Stub 区域中没有任何 AS 外部路由信息，通过缺省路由保证到外部目的地的可达性。为了在保持 Stub 区域优点的同时提高组网的灵活性，RFC1587（OSPF NSSA Option）定义了一种新的区域类型：NSSA 区域（Not-So-Stubby Area），这种区域能够以受限方式引入 AS 外部路由。

NSSA 实际是 Stub 区域的扩展，它与 Stub 区域有许多相似之处。配置 NSSA 区域时，也需要注意：

- 骨干区域不能配置成 NSSA 区域；
- NSSA 区域不能用作传输区域，即，虚连接不能穿过 NSSA 区域；
- 如果要将一个区域配置成 NSSA 区域，则该区域中的所有路由器都必须配置此属性；

与 Stub 区域的一个不同是：NSSA 区域内可以存在 ASBR。

NSSA 区域中的 AS 外部路由信息使用一类新的 LSA：Type-7 LSA。Type-7 LSA 与 Type-5 LSA 非常相似，它们的区别在本章“4.1.5 OSPF 的 LSA 类型”已经介绍过。

下面以图 4-3 为例，介绍 AS 外部路由信息在 NSSA 区域的传播情况。图 4-3 中，运行 OSPF 进程 100 的自治系统包括 3 个区域：区域 0 是骨干区域，区域 1 是普通的 OSPF 非骨干区域，区域 2 是 NSSA 区域。

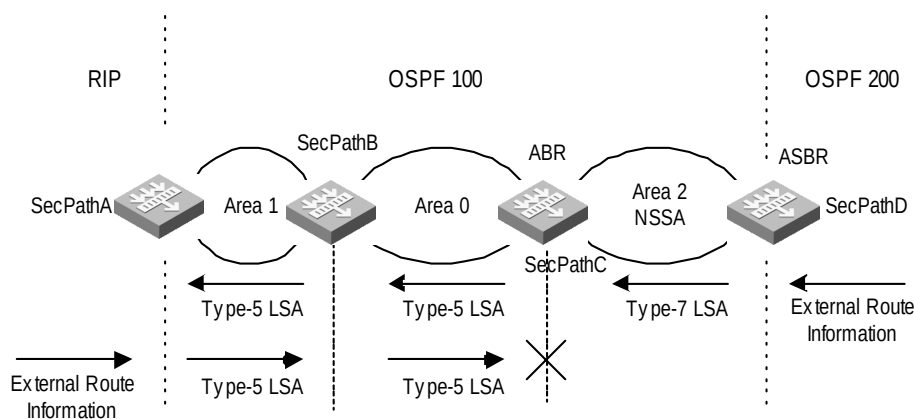


图4-3 NSSA 区域

区域 2 的 NSSA ASBR 引入 AS 外部路由信息（OSPF 进程 200 的路由信息）后，生成 Type-7 LSA 发布到区域 2 内传播，当 Type-7 LSA 到达 NSSA ABR 后，由 ABR 转换成 Type-5 LSA 传播到整个自治系统。区域 1 的 ASBR 引入 AS 外部路由信息（RIP 路由信息）后，产生 Type-5 LSA 在 OSPF 自治系统中传播，但由于区域 2 是 NSSA 区域，所以 RIP 路由信息不会到达区域 2。

请在 OSPF 区域视图下进行下列配置。

表4-29 配置 OSPF 的 NSSA 区域参数

操作	命令
配置一个区域为 NSSA 区域	nssa [default-route-advertise no-import-route no-summary] *
取消配置的 NSSA 区域	undo nssa
配置发送到 NSSA 区域的缺省路由的花费值	default-cost cost
恢复发送到 NSSA 区域的缺省路由的花费缺省值	undo default-cost

缺省情况下，不配置 NSSA 区域；发送到 NSSA 区域缺省路由的花费值为 1。

对于 OSPF 自治系统的 ASBR，如果它也是 NSSA 区域的 ABR，通常不需要将同样的外部路由信息以 Type-5 和 Type-7 LSAs 引入两次，这种情况下，可以使用参数 **no-import-route**，禁止将 AS 外部路由以 Type-7 LSA 的方式发布到 NSSA 区域。

由于 NSSA 区域获得的 AS 外部路由信息是受限的，因此，NSSA 区域的 ABR 需要通过 Type-7 LSA 向本区域内发布一条缺省路由，保证去往自治系统外的报文能被正确转发，需要注意的是：NSSA 区域的 ABR 发布的缺省路由信息不会转换成 Type-5 LSA，而 NSSA 区域内的 ASBR 发布的缺省路由信息则可以转换成 Type-5 LSA。

参数 **default-route-advertise** 用来产生发布缺省路由的 Type-7 LSA，这个参数只能用于 NSSA 的 ASBR 或 ABR：

- 在 NSSA 的 ABR 上配置时，不论系统的路由表中是否存在缺省路由 0.0.0.0，都会产生 Type-7 LSA 缺省路由；
- 在 NSSA 的 ASBR 上配置时，只有当路由表中存在缺省路由 0.0.0.0，才会产生 Type-7 LSA 缺省路由。

参数 **no-summary** 的用法与在 Stub 区域的配置相同，只能在 NSSA 区域的 ABR 配置。使用此参数后，NSSA ABR 只通过 Type-3 的 Summary-LSA 向区域内发布一条缺省路由，不再向区域内发布任何其它 Summary-LSAs，这种区域又称为 NSSA 完全 Stub 区域。

📖 说明：

参数 **default-route-advertise** 通过生成 Type-7 LSA 向 NSSA 区域内发布的缺省路由是自治系统外部缺省路由；

参数 **no-summary** 通过 Type-3 LSA 向 NSSA 完全 Stub 区域发布的缺省路由是区域间缺省路由。

命令 **default-cost** 用于 NSSA 区域的 ABR，配置 ABR 发送到 NSSA 区域的缺省路由的花费值。

4.2.24 配置 OSPF 与网管系统的配合

1. 配置 OSPF MIB 绑定

当启动了多个 OSPF 进程时，可以配置 OSPF MIB 对哪个进程进行处理，即绑定在哪个进程。

请在系统视图下进行下列配置。

表4-30 配置 OSPF MIB 绑定

操作	命令
配置 OSPF MIB 绑定	ospf mib-binding <i>process-id</i>
取消缺省的 OSPF MIB 绑定	undo ospf mib-binding

缺省情况下，MIB 绑定在第一个启动的 OSPF 进程上。

2. 配置 OSPF TRAP 功能

可以配置 OSPF 发送多种 SNMP Trap 报文，并可以通过进程号指定某个 OSPF 进程发送 SNMP Trap 报文。

请在系统视图下进行下列配置。

表4-31 配置 OSPF TRAP 功能

操作	命令
使能 OSPF 的 Trap 功能	snmp-agent trap enable ospf [<i>process-id</i>] [<i>ifstatechange</i> <i>virifstatechange</i> <i>nbrstatechange</i> <i>virnbrstatechange</i> <i>ifcfcgerror</i> <i>virifcfcgerror</i> <i>ifauthfail</i> <i>virifauthfail</i> <i>ifrxbadpkt</i> <i>virifrxbadpkt</i> <i>txretransmit</i> <i>viriftxretransmit</i> <i>originatelsa</i> <i>maxagelsa</i> <i>lsdboverflow</i> <i>lsdbapproachoverflow</i>]
取消 OSPF 的 Trap 功能	undo snmp-agent trap enable ospf [<i>process-id</i>] [<i>ifstatechange</i> <i>virifstatechange</i> <i>nbrstatechange</i> <i>virnbrstatechange</i> <i>ifcfcgerror</i> <i>virifcfcgerror</i> <i>ifauthfail</i> <i>virifauthfail</i> <i>ifrxbadpkt</i> <i>virifrxbadpkt</i> <i>txretransmit</i> <i>viriftxretransmit</i> <i>originatelsa</i> <i>maxagelsa</i> <i>lsdboverflow</i> <i>lsdbapproachoverflow</i>]

缺省情况下，OSPF 的 Trap 功能是禁止的，即 OSPF 进程不发送 Trap 报文。如果配置时不指定进程号，将对所有 OSPF 进程生效。

关于 SNMP Trap 的详细配置，请参考本手册的“基础配置”部分。

4.2.25 重启 OSPF

如果对防火墙先执行 **undo ospf**，再执行 **ospf** 来重启 OSPF 进程，防火墙上原来的 OSPF 配置会丢失。而使用 **reset ospf all** 命令，可以在不丢失原有 OSPF 配置的前提下重启 OSPF。

请在用户视图下进行下列配置。

表4-32 配置重启 OSPF 进程

操作	命令
重启 OSPF 进程	reset ospf [statistics] { all <i>process-id</i> }

重启防火墙的 OSPF 进程，可以立即清除无效的 LSA、使改变的 Router ID 立即生效、或者进行 DR、BDR 的重新选举。

如果不指定 OSPF 进程号，将重启所有 OSPF 进程。

4.3 OSPF 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 OSPF 的运行情况，用户可以通过查看显示信息验证配置的效果。

在用户视图下执行 **debugging** 命令可对 OSPF 进行调试。

表4-33 OSPF 显示和调试

操作	命令
查看 OSPF 路由进程的信息	display ospf [<i>process-id</i>] brief
查看 OSPF 统计信息	display ospf [<i>process-id</i>] cumulative
查看 OSPF 的 LSDB 信息	display ospf [<i>process-id</i>] lsdb [brief asbr ase network nssa router summary] [<i>ip-address</i>] [originate-router <i>ip-address</i> self-originate]
查看 OSPF 邻接点信息	display ospf [<i>process-id</i>] peer [brief statistics]
查看 OSPF 下一跳信息	display ospf [<i>process-id</i>] nexthop
查看 OSPF 路由表信息	display ospf [<i>process-id</i>] routing
查看 OSPF 虚连接信息	display ospf [<i>process-id</i>] vlink
查看 OSPF 请求列表	display ospf [<i>process-id</i>] request-queue
查看 OSPF 重传列表	display ospf [<i>process-id</i>] retrans-queue
查看 OSPF 到 ABR 及 ASBR 的路由信息	display ospf [<i>process-id</i>] abr-asbr
查看 OSPF 的引入路由聚合信息	display ospf [<i>process-id</i>] asbr-summary [<i>ip-address mask</i>]
查看 OSPF 接口信息	display ospf [<i>process-id</i>] interface [<i>interface-type interface-number</i>]
查看 OSPF 错误信息	display ospf [<i>process-id</i>] error
查看 OSPF 的调试信息开关状态	display debugging ospf

操作	命令
打开该 OSPF 进程下的邻接状态变化的输出开关（OSPF 视图）	log-peer-change
关闭该 OSPF 进程下的邻接状态变化的输出开关（OSPF 视图）	undo log-peer-change
打开 OSPF 报文调试信息开关	debugging ospf [process-id] packet [ack dd hello request update] [interface interface-type interface-number]
关闭 OSPF 报文调试信息开关	undo debugging ospf [process-id] packet [ack dd hello request update] [interface interface-type interface-number]
打开 OSPF 事件调试信息	debugging ospf [process-id] event
关闭 OSPF 事件调试信息	undo debugging ospf [process-id] event
打开 OSPF LSA 报文调试信息开关	debugging ospf [process-id] lsa-originate
关闭 OSPF LSA 报文调试信息开关	undo debugging ospf [process-id] lsa-originate
打开 OSPF 的 SPF 调试信息开关	debugging ospf [process-id] spf
关闭 OSPF 的 SPF 调试信息开关	undo debugging ospf [process-id] spf

4.4 OSPF 典型配置举例



注意：

在配置用例中，只列出了与 OSPF 配置相关的命令。

4.4.1 OSPF 典型配置举例

1. 组网需求

SecPathA 与 SecPathB 通过以太网口相连，SecPathB 与 SecPathC 通过以太网口相连；SecPathA 属于 area0，SecPathC 属于 area1，SecPathB 同时属于 area0 和 area1。

2. 组网图

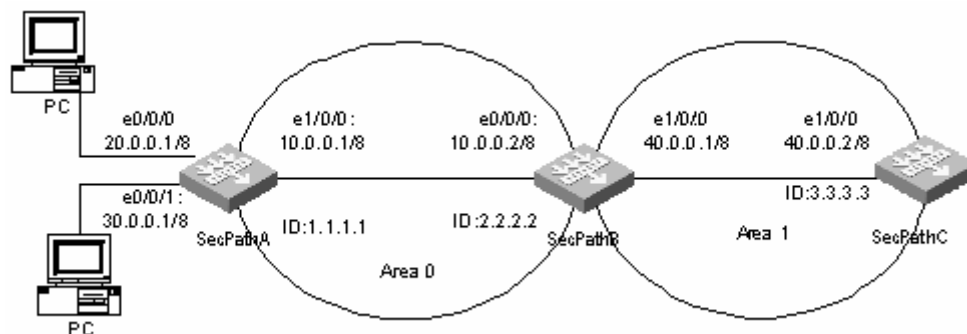


图4-4 OSPF 典型配置举例

3. 配置步骤

(1) 配置 SecPathA

```
[H3C] router id 1.1.1.1
[H3C] interface ethernet1/0/0
[H3C-ethernet1/0/0] ip address 10.0.0.1 255.0.0.0
[H3C-ethernet1/0/0] interface ethernet0/0/0
[H3C-ethernet0/0/0] ip address 20.0.0.1 255.0.0.0
[H3C-ethernet0/0/0] interface ethernet0/0/1
[H3C-ethernet0/0/1] ip address 30.0.0.1 255.0.0.0
[H3C-ethernet0/0/1] quit
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 10.0.0.1 0.255.255.255
[H3C-ospf-1-area-0.0.0.0] network 20.0.0.1 0.255.255.255
[H3C-ospf-1-area-0.0.0.0] network 30.0.0.1 0.255.255.255
```

(2) 配置 SecPathB

```
[H3C] router id 2.2.2.2
[H3C] interface ethernet0/0/0
[H3C-ethernet0/0/0] ip address 10.0.0.2 255.0.0.0
[H3C-ethernet0/0/0] interface ethernet 1/0/0
[H3C-ethernet1/0/0] ip address 40.0.0.1 255.0.0.0
[H3C-ethernet1/0/0] quit
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 10.0.0.2 0.255.255.255
[H3C-ospf-1-area-0.0.0.0] area 1
[H3C-ospf-1-area-0.0.0.1] network 40.0.0.1 0.255.255.255
```

(3) 配置 SecPathC

```
[H3C] router id 3.3.3.3
```



```
[H3C] interface ethernet 1/0/0
[H3C-ethernet1/0/0] ip address 40.0.0.2 255.0.0.0
[H3C-ethernet1/0/0] quit
[H3C] ospf
[H3C-ospf-1] area 1
[H3C-ospf-1-area-0.0.0.1] network 40.0.0.2 0.255.255.255
```

在 SecPathA 与 SecPathC 上执行 **display ip routing-table**，发现二者通过 OSPF 获得了到对方的路由（即都有 10.0.0.0/8，20.0.0.0/8，30.0.0.0/8，40.0.0.0/8 网段的路由）。

4.4.2 配置 OSPF 多进程

1. 组网需求

在 SecPathA 的接口 Ethernet1/0/0 上启动 OSPF 进程 100，接口位于区域 0。

在 SecPathB 的接口 Ethernet1/0/0 上启动 OSPF 进程 100，接口 Ethernet2/0/0 上启动 OSPF 进程 200，分别处于相应进程的区域 0。

在 SecPathC 的接口 Ethernet2/0/0 上启动 OSPF 进程 200，处于区域 0。

SecPathA 和 SecPathB 之间可以建立邻居关系，SecPathB 和 SecPathC 之间可以建立邻居关系。

2. 组网图

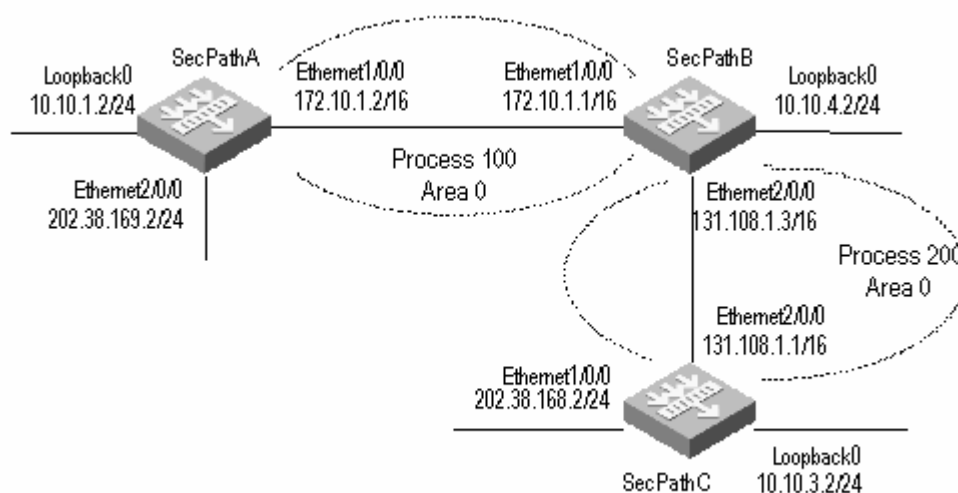


图4-5 OSPF 多进程组网图

3. 配置步骤

配置 SecPathA:

```
[H3C] interface ethernet 1/0/0
```

```
[H3C-Ethernet1/0/0] ip address 172.10.1.2 255.255.0.0
[H3C-Ethernet1/0/0] quit
[H3C] router id 10.10.1.2
[H3C] ospf 100
[H3C-ospf-100] area 0
[H3C-ospf-100-area-0.0.0.0] network 172.10.0.0 0.0.255.255

# 配置 SecPathB:

[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 172.10.1.1 255.255.0.0
[H3C-Ethernet1/0/0] quit
[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 131.108.1.3 255.255.0.0
[H3C-Ethernet2/0/0] quit
[H3C] ospf 100 router-id 10.10.2.2
[H3C-ospf-100] area 0
[H3C-ospf-100-area-0.0.0.0] network 172.10.0.0 0.0.255.255
[H3C-ospf-100] quit
[H3C] ospf 200 router-id 10.10.4.2
[H3C-ospf-200] area 0
[H3C-ospf-200-area-0.0.0.0] network 131.108.0.0 0.0.255.255

# 配置 SecPathC:

[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 131.108.1.1 255.255.0.0
[H3C-Ethernet2/0/0] quit
[H3C] router id 10.10.3.2
[H3C] ospf 200
[H3C-ospf-200] area 0
[H3C-ospf-200-area-0.0.0.0] network 131.108.0.0 0.0.255.255
```

在 SecPathB 上使用 **display ospf peer** 命令查看邻居的建立情况，可以看到 SecPathB 与 SecPathA 在 OSPF 进程 100 中建立邻居关系，SecPathB 与 SecPathC 在 OSPF 进程 200 中建立邻居关系，SecPathA 和 SecPathC 不能通过 OSPF 学到对方的路由。

4.4.3 配置 OSPF 优先级的“DR”选择

1. 组网需求

在下图中，SecPathA 的优先级为 100，它是网络上的最高优先级，所以 SecPathA 被选为 DR；SecPathC 的优先级第二高，被选为 BDR；SecPathB 的优先级为 0，这意味着它将无法成为 DR；SecPathD 没有配置优先级，取缺省值 1。

2. 组网图

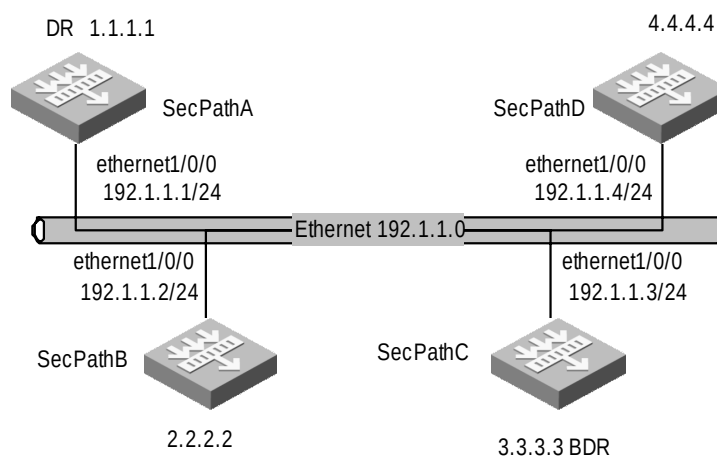


图4-6 配置 OSPF 优先级的“DR”选择组网图

3. 配置步骤

配置 SecPathA:

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 192.1.1.1 255.255.255.0
[H3C-Ethernet1/0/0] ospf dr-priority 100
[H3C-Ethernet1/0/0] quit
[H3C] router id 1.1.1.1
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
```

配置 SecPathB:

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 192.1.1.2 255.255.255.0
[H3C-Ethernet1/0/0] ospf dr-priority 0
[H3C-Ethernet1/0/0] quit
[H3C] router id 2.2.2.2
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
```

配置 SecPathC:

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 192.1.1.3 255.255.255.0
[H3C-Ethernet1/0/0] ospf dr-priority 2
[H3C-Ethernet1/0/0] quit
[H3C] router id 3.3.3.3
```

```
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255

# 配置 SecPathD:

[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 192.1.1.4 255.255.255.0
[H3C-Ethernet1/0/0] quit
[H3C] router id 4.4.4.4
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
```

在 SecPathA 上运行 **display ospf peer** 来显示 OSPF 邻居，注意 SecPathA 有三个邻居。

每个邻居的状态都是 **full**，这意味着 SecPathA 与它的每个邻居都形成了邻接（SecPathA 和 C 必须与网络中的所有 SecPath 形成邻接，才能分别充当网络的 DR 和 BDR）。SecPathA 是网络中的 DR，而 SecPathC 是 BDR。其它所有的邻居都是 DRother（这意味着它们既不是 DR，也不是 BDR）。

将 SecPathB 的优先级改为 200：

```
[H3C-Ethernet1/0/0] ospf dr-priority 200
```

在 SecPathA 上运行 **display ospf peer** 来显示 OSPF 邻居，注意 SecPathB 的优先级变为 200；但它并不是 DR。

只有当现在的 DR 不在网络上了后，DR 才会改变。关掉 SecPathA，在 SecPathD 上运行 **display ospf peer** 命令可显示邻居，注意本来是 BDR 的 SecPathC 成为了 DR，并且 SecPathB 现在也是 BDR。

关掉所有的防火墙再重新启动，这个操作会带来一个新的 DR/BDR 选择。SecPathB 就被选为 DR（优先级为 200），SecPathA 成为了 BDR（优先级为 100）。

4.4.4 配置 OSPF 虚链路

1. 组网需求

在下图中，区域 2 没有与区域 0 直接相连。区域 1 被用作运输区域（Transit Area）来连接区域 2 和区域 0。SecPathB 和 SecPathC 之间配置一条虚链路。

2. 组网图

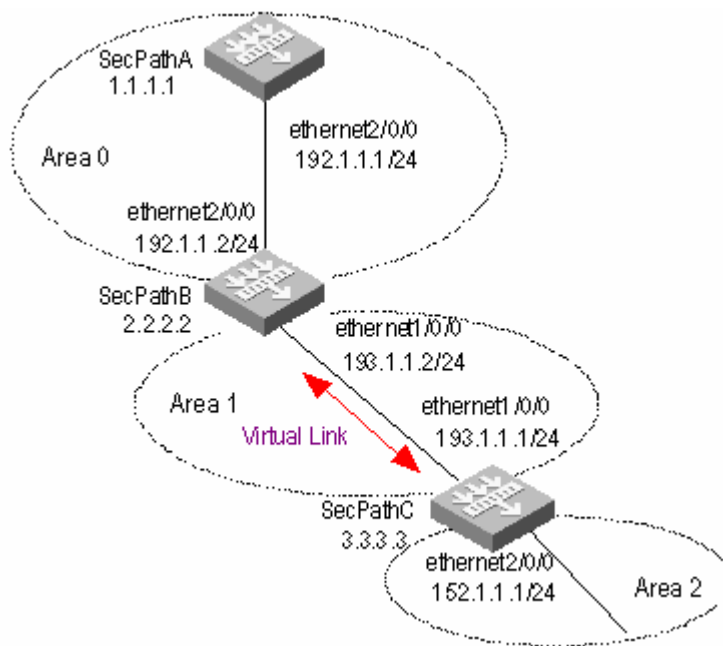


图4-7 配置 OSPF 虚链路的组网图

3. 配置步骤

配置 SecPathA:

```
[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 192.1.1.1 255.255.255.0
[H3C-Ethernet2/0/0] quit
[H3C] router id 1.1.1.1
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
```

配置 SecPathB:

```
[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 192.1.1.2 255.255.255.0
[H3C-Ethernet2/0/0] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 193.1.1.2 255.255.255.0
[H3C-Ethernet1/0/0] quit
[H3C] router id 2.2.2.2
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[H3C-ospf-1-area-0.0.0.0] quit
[H3C-ospf-1] area 1
```

```
[H3C-ospf-1-area-0.0.0.1] network 193.1.1.0 0.0.0.255
[H3C-ospf-1-area-0.0.0.1] vlink-peer 3.3.3.3

# 配置 SecPathC:

[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 152.1.1.1 255.255.255.0
[H3C-Ethernet2/0/0] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 193.1.1.1 255.255.255.0
[H3C-Ethernet1/0/0] quit
[H3C] router id 3.3.3.3
[H3C] ospf
[H3C-ospf-1] area 1
[H3C-ospf-1-area-0.0.0.1] network 193.1.1.0 0.0.0.255
[H3C-ospf-1-area-0.0.0.1] vlink-peer 2.2.2.2
[H3C-ospf-1-area-0.0.0.1] quit
[H3C-ospf-1] area 2
[H3C-ospf-1-area-0.0.0.2] network 152.1.1.0 0.0.0.255
```

4.4.5 配置 OSPF 邻居认证

1. 组网需求

在下图中，SecPathA 与 SecPathB 交换路由更新信息时采用纯文本认证，而在与 SecPathC 交换路由更新时使用 MD5 密文认证。

SecPathA 的以太网接口与 SecPathB 的以太网接口在 OSPF 区域 0 内。SecPathA 的 Ethernet 口与 SecPathC 的 Ethernet 口都在区域 1 内，它们都为区域 1 配置了 MD5 认证。

2. 组网图

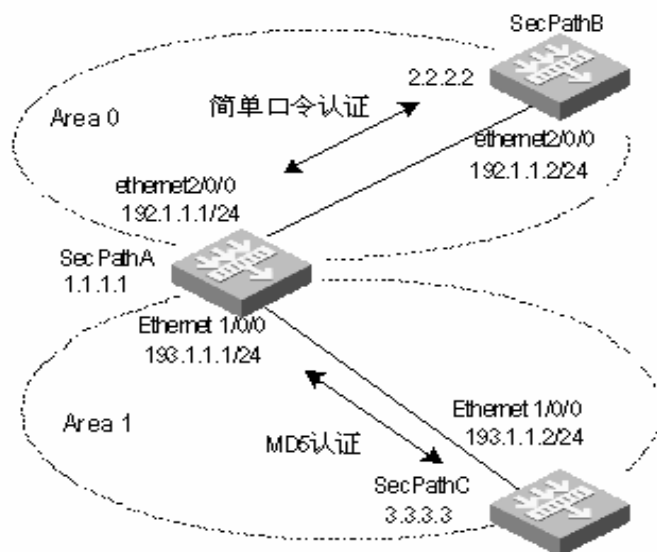


图4-8 配置 OSPF 邻居认证的组网图

3. 配置步骤

配置 SecPathA:

配置接口 Ethernet1/0/0 的网段 193.1.1.0 所在的区域 1 支持 MD5 密文验证，验证字标识符为 1，验证字为 password。

配置接口 ethernet 2/0/0 的网段 192.1.1.0 所在的区域 0 支持明文验证，验证字为 password。

```
[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 192.1.1.1 255.255.255.0
[H3C-Ethernet2/0/0] ospf authentication-mode simple password
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 193.1.1.1 255.255.255.0
[H3C-Ethernet1/0/0] ospf authentication-mode md5 1 password
[H3C] router id 1.1.1.1
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[H3C-ospf-1-area-0.0.0.0] authentication-mode simple
[H3C-ospf-1-area-0.0.0.0] quit
[H3C-ospf-1] area 1
[H3C-ospf-1-area-0.0.0.1] network 193.1.1.0 0.0.0.255
[H3C-ospf-1-area-0.0.0.1] authentication-mode md5
```

配置 SecPathB:

```
[H3C] interface ethernet 2/0/0
```

```
[H3C-Ethernet2/0/0] ip address 192.1.1.2 255.255.255.0
[H3C-Ethernet2/0/0] ospf authentication-mode simple password
[H3C] router id 2.2.2.2
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[H3C-ospf-1-area-0.0.0.0] authentication-mode simple
```

配置 SecPathC:

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 193.1.1.2 255.255.255.0
[H3C-Ethernet1/0/0] ospf authentication-mode md5 1 password
[H3C] router id 3.3.3.3
[H3C] ospf
[H3C-ospf-1] area 1
[H3C-ospf-1-area-0.0.0.1] network 193.1.1.0 0.0.0.255
[H3C-ospf-1-area-0.0.0.1] authentication-mode md5
```

4.4.6 配置 OSPF 的 STUB 区

1. 组网需求

SecPathA 与 SecPathB 通过以太网口相连，SecPathB 与 SecPathC 通过以太网口相连；SecPathA 属于 area0，SecPathC 属于 area1，SecPathB 同时属于 area0 和 area1。将 area1 配置为 STUB 区。

2. 组网图

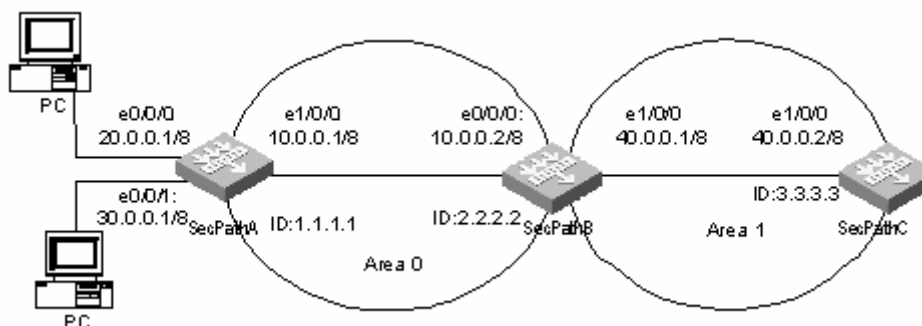


图4-9 配置 OSPF 的 STUB 区

3. 配置步骤

(1) 配置 SecPathA

```
[H3C] router id 1.1.1.1
[H3C] interface ethernet1/0/0
[H3C-ethernet1/0/0] ip address 10.0.0.1 255.0.0.0
```



```
[H3C-ethernet1/0/0] interface ethernet0/0/0
[H3C-ethernet0/0/0] ip address 20.0.0.1 255.0.0.0
[H3C-ethernet0/0/0] interface ethernet0/0/1
[H3C-ethernet0/0/1] ip address 30.0.0.1 255.0.0.0
[H3C-ethernet0/0/1] quit
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 10.0.0.1 0.255.255.255
[H3C-ospf-1-area-0.0.0.0] network 20.0.0.1 0.255.255.255
[H3C-ospf-1-area-0.0.0.0] network 30.0.0.1 0.255.255.255
```

(2) 配置 SecPathB

```
[H3C] router id 2.2.2.2
[H3C] interface ethernet0/0/0
[H3C-ethernet0/0/0] ip address 10.0.0.2 255.0.0.0
[H3C-ethernet0/0/0] interface ethernet 1/0/0
[H3C-ethernet1/0/0] ip address 40.0.0.1 255.0.0.0
[H3C-ethernet1/0/0] quit
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 10.0.0.2 0.255.255.255
[H3C-ospf-1-area-0.0.0.0] area 1
[H3C-ospf-1-area-0.0.0.1] network 40.0.0.1 0.255.255.255
[H3C-ospf-1-area-0.0.0.1] stub
```

(3) 配置 SecPathC

```
[H3C] router id 3.3.3.3
[H3C] interface ethernet 1/0/0
[H3C-ethernet1/0/0] ip address 40.0.0.2 255.0.0.0
[H3C-ethernet1/0/0] quit
[H3C] ospf
[H3C-ospf-1] area 1
[H3C-ospf-1-area-0.0.0.1] network 40.0.0.2 0.255.255.255
[H3C-ospf-1-area-0.0.0.1] stub
```

此时 SecPathC 上除了 OSPF 发现的区间路由外，还应有一条缺省路由 0.0.0.0/0。

若将 ABR 路由器 B 上的 **stub** 命令改为 **stub nosummary**，则 area1 变为完全 STUB 区，SecPathC 上不再包含任何区间路由，只包含一条默认路由。

4.5 OSPF 故障诊断与排除

故障之一：如果按前述步骤配置了 OSPF，但路由器 OSPF 却不能正常运行。

故障排除：可按如下步骤进行检查。

- (1) 局部故障排除：首先检查两台直接相连的路由器之间协议运行是否正常，正常的标志是两台路由器之间 **peer** 状态机达到 **FULL** 状态。（注：在广播和 NBMA 网络上，两台接口状态是 **DR/Other** 的路由器之间 **peer** 状态机并不达到 **FULL** 状态，而是 **2 way** 状态。DR、BDR 与其它所有路由器之间达到 **FULL** 状态）
- 使用 **display ospf peer** 命令查看区域邻居的信息。
 - 查看接口上 OSPF 信息可用 **display ospf interface** 命令。
 - 检查物理连接及下层协议是否正常运行。可通过 **Ping** 命令测试，若从本地路由器 **Ping** 对端路由器不通，则表明物理连接和下层协议有问题。
 - 如果物理连接和下层协议正常，则检查在接口上配置的 **OSPF** 参数，必须保证与和该接口相邻的路由器的参数一致。区域（Area）号必须相同；网段与掩码也必须一致（点到点与虚连接的网段与掩码可以不同）。
 - 检查在同一接口上 **dead-interval** 值应至少为 **hello-interval** 值的 4 倍，且与对端的配置保持一致。
 - 若网络的类型为 **NBMA**，则必须手工指定 **Peer**。使用 **peer ip-address** 命令。
 - 若网络类型为广播网或 **NBMA**，至少有一个接口的 **priority** 应大于零。
 - 如果一个 **Area** 配置成 **stub** 区域，则在与这个区域相连的所有路由器中都将该区域配置成 **stub** 区域。
 - 相邻的两台路由器接口类型必须一致。
 - 若配置了两个以上的区域，则至少有一个区域应配成骨干区域（即 **Area** 号为 0）。
 - 应保证骨干区域与所有的区域相连接。
 - 虚连接不能穿越 **Stub** 区域。
- (2) 全局故障排除：如果上述步骤无误，但 **OSPF** 仍不能发现远端路由，则检查如下配置。
- 若一台路由器配置了两个以上的区域，则至少有一个区域应配成骨干区域。

如下图所示：SecPathA 和 RTD 上只配置了一个区域，SecPathB（area0，area1）和 SecPathC（area1，area2）分别配置了两个区域，其中 SecPathB 中有一个区域为 0，符合要求，但 SecPathC 中的两个区域都不为 0，则必须在 SecPathC 与 SecPathB 之间配置一条虚连接。保证 area 2 与 area 0（骨干区域）相连接。

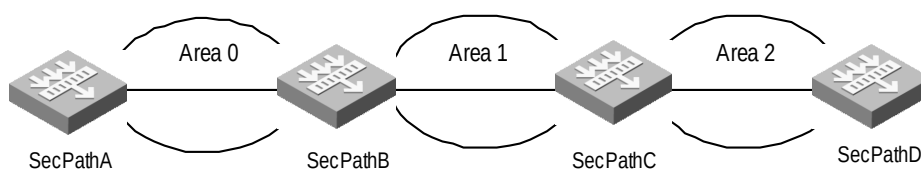


图4-10 OSPF 区域示意图

- 虚连接不能穿越 stub 区域，骨干区域（area 0）也不能配置成 Stub 区域。即如果 SecPathB 与 SecPathC 之间配置了一条虚连接，则 area 1 不能配置成 stub 区域，area 0 也不能配置成 stub 区域，上图中只有 area 2 可以配置成 stub 区域。
- 在 Stub 区域内的路由器不能接收外部路由。
- 骨干区域必须保证各个节点的连接。

第5章 BGP 配置

 说明：

BGP 中有关 VPN 实例及 VPNv4 的具体参数解释及举例，请参见本手册的“VPN”部分。

5.1 BGP 简介

BGP（Border Gateway Protocol）是一种自治系统间的动态路由发现协议。

BGP 协议早期发布的三个版本分别是 BGP-1（请参阅 RFC1105）、BGP-2（请参阅 RFC1163）和 BGP-3（请参阅 RFC1267），当前使用的版本是 BGP-4（请参阅 RFC1771）。BGP-4 适用于分布式结构，并支持无类域间路由 CIDR（Classless Inter-Domain Routing）。利用 BGP 还可以实施用户配置的策略。BGP-4 为 Internet 外部路由协议标准，广泛应用于 ISP 之间。

BGP 特性描述如下：

- BGP 是一种外部网关路由协议，与 OSPF、RIP 等内部网关路由协议不同，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好的路由。
- 通过在 BGP 路由中携带 AS 路径信息，可以彻底解决路由循环问题。
- 使用 TCP 作为其传输层协议，提高了协议的可靠性。
- BGP-4 支持无类域间路由 CIDR。这是较 BGP-3 的一个重要改进。CIDR 以一种全新的方法看待 IP 地址，不再区分 A 类网、B 类网及 C 类网。例如一个非法的 C 类网络地址 192.213.0.0（255.255.0.0）采用 CIDR 表示法 192.213.0.0/16 就成为一个合法的超级网络，其中/16 表示子网掩码由从地址左端开始的 16 比特构成。CIDR 的引入简化了路由聚合（Routes Aggregation），路由聚合实际上是合并几个不同路由的过程，这样从通告几条路由变为通告一条路由，减小了路由表规模。
- 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。
- 出于管理和安全方面的考虑，每个自治系统都希望能够对进出自治系统的路由进行控制，BGP-4 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，并且易于扩展以支持网络新的发展。

BGP 系统作为高层协议运行在一个特定的路由器上。系统初启时 BGP 路由器通过发送整个 BGP 路由表与对等体交换路由信息，之后只交换更新消息（update message）。系统在运行过程中，是通过接收和发送 keep-alive 消息来检测相互之间的连接是否正常的。

发送 BGP 消息的路由器称为 BGP 发言人（speaker），它不断的接收或产生新路由信息，并将它广告（advertise）给其它的 BGP 发言人。当 BGP 发言人收到来自其它自治系统的新路由通告时，如果该路由比当前已知路由好、或者当前还没有该路由，它就把这个路由通告给自治系统内所有其它的 BGP 发言人。一个 BGP 发言人也同它交换消息的其它的 BGP 发言人称为对等体（peer），若干相关的对等体可以构成对等体组（group）。

BGP 在路由器上以下列两种方式运行：

- IBGP（Internal BGP）
- EBGp（External BGP）

当 BGP 运行于同一自治系统（AS）内部时，被称为 IBGP；当 BGP 运行于不同自治系统之间时，称为 EBGp。

BGP 协议机的运行是通过消息驱动的，其消息共可分为四类：

- open message
- update message
- notification message
- keep-alive message

Open message 是连接建立后发送的第一个消息，它用于建立 BGP 对等体间的连接关系。Notification message 是错误通告消息。Keep-alive message 是用于检测连接有效性的消息。Update message 是 BGP 系统中最重要的信息，用于在对等体之间交换路由信息，它最多由三部分构成：不可达路由（unreachable）、路径属性（path attributes）、网络可达性信息 NLRI（network layer reach/reachable information）。

5.2 BGP 的配置

BGP 的配置包括：

- 启动 BGP
- 指定 BGP 要通告的网络路由
- 配置 BGP 对等体组
- 配置 BGP 定时器
- 配置本地优先级
- 配置自治系统的 MED 值

- 比较来自于不同 AS 邻居的 MED 值
- 配置 BGP 团体属性
- 配置 BGP 路由聚合
- 配置 BGP 协议的优先级
- 配置 BGP 路由反射器
- 配置自治系统联盟属性
- 配置 BGP 路由衰减
- 配置 BGP 与 IGP 的交互
- 配置 BGP 路由过滤
- 定义访问列表、AS 路径列表和 Route-policy
- 配置 BGP 负载分担
- 复位 BGP 连接

5.2.1 启动 BGP

启动 BGP 时应指定本地的自治系统号。启动 BGP 后，防火墙监听相邻路由器的 BGP 连接请求。要使防火墙主动向相邻路由器发出 BGP 连接请求，请参照 **peer** 命令的配置。关闭 BGP 时，BGP 将切断所有已经建立的 BGP 连接。

请在系统视图下进行下列配置。

表5-1 启动/关闭 BGP

操作	命令
启动 BGP，进入 BGP 视图	bgp <i>as-number</i>
关闭 BGP	undo bgp [<i>as-number</i>]

缺省情况下，系统不运行 BGP。

5.2.2 指定 BGP 要通告的网络路由

请在 BGP 视图下进行下列配置。

表5-2 指定 BGP 通告的网络

操作	命令
配置本地 BGP 通告的网络	network <i>ip-address</i> [<i>address-mask</i>] [route-policy <i>route-policy-name</i>]
取消本地 BGP 通告的网络	undo network <i>ip-address</i> [<i>address-mask</i>] [route-policy <i>route-policy-name</i>]

缺省情况下，本地 BGP 不通告任何网络。

使用 **network** 命令通告网络时，路由表中必须已经存在到此网络的精确匹配的路由。

例如，要将网络 172.16.1.0/24 通告到 BGP 对等体，必须使用命令 **network 172.16.1.0 255.255.255.0** 进行通告，且当前路由表中也必须已经存在到网络 172.16.1.0/24 的精确匹配的路由。

5.2.3 配置 BGP 对等体组

交换 BGP 报文的 BGP 发言者形成对等体。BGP 对等体不能够脱离对等体组而独立存在，即对等体必须隶属于某一个特定的对等体组。在配置 BGP 对等体时，必须首先配置对等体组，然后再将对等体加入该对等体组中。

当对等体组的配置变化时，每个组员的配置也相应变化。对某些属性可以指定组员的 IP 地址进行配置，从而使指定组员在这些属性上不受对等体组配置的影响。

下列各项配置均在 BGP 视图下进行。

1. 配置对等体组

在配置 BGP 对等体之前，必须首先配置对等体所隶属的对等体组。

表5-3 配置对等体组

操作	命令
创建一个对等体组	group group-name [internal external]
删除指定的对等体组	undo group group-name

在配置对等体组时需要指定对等体组的类型。**internal** 类型的对等体组包含的都是 IBGP 对等体；**external** 类型的对等体都是 EBGP 对等体或者联盟 EBGP 对等体。

配置时，如果不指定对等体组的类型，缺省为 **internal**。

2. 指定对等体组的自治系统号

可以为类型为 **external** 的对等体组指定自治系统号，**internal** 类型的对等体组无需配置自治系统号。如果为对等体组指定了自治系统号，那么，加入该对等体组的所有对等体都继承了该对等体组的自治系统号。

表5-4 为对等体组指定自治系统号

操作	命令
为对等体组指定自治系统号	peer group-name as-number as-number
删除指定的对等体组的自治系统号	undo peer group-name as-number

如果对等体组中已经加入了对等体，那么，不能够为该对等体组指定自治系统号；删除对等体组的自治系统号时，会删除对等体组中的所有对等体。

3. 向对等体组中加入组员

BGP 的对等体不能够脱离对等体组而独立存在，在配置对等体的同时必须指定其所属的对等体组，同时可以指定对等体的自治系统号。

表5-5 向对等体组中加入组员

操作	命令
在对等体组中创建一个对等体	peer <i>peer-address</i> group <i>group-name</i> [as-number <i>as-number</i>]
从对等体组中删除一个对等体	undo peer <i>peer-address</i>

加入对等体组的配置类型为 **internal**，则命令中不能够指定自治系统号参数。加入的对等体为 **IBGP** 对等体。

加入对等体组的配置类型为 **external**，如果对等体组没有指定自治系统号，那么对等体加入对等体组的同时必须同时指定该对等体的自治系统号；如果对等体组已经配置了自治系统号，对等体将继承对等体组的自治系统号，无需再为对等体指定。

4. 配置对等体（组）描述信息

为便于了解对等体的特征，可以为 BGP 对等体（组）配置描述信息。

表5-6 配置对等体（组）描述信息

操作	命令
配置对等体（组）描述信息	peer { <i>peer-address</i> <i>group-name</i> } description <i>description-line</i>
删除对等体（组）描述信息	undo peer { <i>peer-address</i> <i>group-name</i> } description

缺省情况下，BGP 对等体（组）无描述信息。

5. 配置允许同不直接相连网络上的 EBGP 对等体组建立连接

通常情况下，EBGP 对等体之间必须是物理上直接相连的，如果无法满足，可使用以下命令进行配置。

表5-7 配置允许同不直接相连网络上的 EBGP 对等体组建立连接

操作	命令
配置允许同不直接相连网络上的 EBGP 对等体组建立连接	peer <i>group-name</i> ebgp-max-hop [<i>tth</i>]
配置只允许同直接相连网络上的 EBGP 对等体组建立连接	undo peer <i>group-name</i> ebgp-max-hop

缺省情况下，只允许同直接相连网络上的对等体组建立连接。*ttl* 为最大跳数，缺省值为 64，范围为 1~255。

6. 配置指定对等体（组）的定时器

使用 **peer timer** 命令可以对指定的 BGP 对等体（组）配置定时器，包括指定 **keepalive** 报文发送时间间隔和保持定时器，它的优先级高于对所有 BGP 邻居配置定时器使用的 **timer** 命令。

表5-8 配置指定对等体（组）的定时器

操作	命令
配置指定对等体（组）的 keepalive 时间间隔与保持定时器	peer { group-name peer-address } timer keep-alive keepalive-interval hold holdtime-interval
恢复指定对等体（组）的 keepalive 时间间隔与保持定时器的缺省值	undo peer { group-name peer-address } timer

缺省情况下，**keepalive** 报文的发送时间间隔为 60 秒，保持定时器为 180 秒。

7. 配置向对等体组发送路由更新报文的时间间隔

表5-9 配置向对等体组发送路由更新报文的时间间隔

操作	命令
配置向对等体组发送路由更新报文的时间间隔	peer group-name route-update-interval seconds
恢复向对等体组发送路由更新报文的缺省时间间隔	undo peer group-name route-update-interval

缺省情况下，向 **IBGP** 对等体组发送路由更新报文的时间间隔为 5 秒，向 **EBGP** 对等体组发送路由更新报文的时间间隔为 30 秒。

8. 配置将团体属性传给对等体组

表5-10 配置将团体属性传给对等体组

操作	命令
配置将团体属性传给对等体组	peer group-name advertise-community
不将团体属性传给对等体组	undo peer group-name advertise-community

9. 配置对等体组为路由反射器的客户

表5-11 配置对等体组为路由反射器的客户

操作	命令
配置对等体组为路由反射器客户	peer group-name reflect-client
取消对等体组作为路由反射器客户	undo peer group-name reflect-client

只能将配置类型为 **internal** 的对等体组配置成反射器客户。

缺省情况下，自治系统中的所有 IBGP 必须是全连接的，且邻居间不通告学到的 IBGP 路由，以防止产生路由环。

关于路由反射器，请参考“配置 BGP 路由反射器”一节的内容。

10. 配置向对等体组发送缺省路由

表5-12 配置向对等体组发送缺省路由

操作	命令
配置向对等体组发送缺省路由	peer group-name default-route-advertise
取消向对等体组发送缺省路由	undo peer group-name default-route-advertise

缺省情况下，防火墙不向对等体发送缺省路由。使用该命令时，不要求在 BGP 路由表中存在缺省路由，而是无条件地向对等体发送一个下一跳为自身的缺省路由。

11. 配置在发布路由时将自身地址作为下一跳

BGP 路由器向对等体组发布路由时，可使用自身地址作为下一跳。

表5-13 配置在发布路由时将自身地址作为下一跳

操作	命令
配置发布路由时将自身地址作为下一跳	peer group-name next-hop-local
取消发布路由时将自身地址作为下一跳	undo peer group-name next-hop-local

缺省情况下，防火墙向 IBGP 对等体发布从 EBGP 对等体学到的路由时不把自身地址作为下一跳。

12. 配置传送 BGP 更新报文时不携带私有自治系统号

一般情况下，BGP 在发送更新报文时都携带该自治系统号（可能是公有的 AS 号，也可能是私有的 AS 号），为使某些出口路由器在发送更新报文时忽略掉私有 AS 号，可配置发送 BGP 更新报文时不携带私有自治系统号。

表5-14 配置发送 BGP 更新报文时不携带私有自治系统号

操作	命令
配置发送 BGP 更新报文时不携带私有自治系统号	peer group-name public-as-only
配置发送 BGP 更新报文时携带私有自治系统号	undo peer group-name public-as-only

缺省情况下，发送 BGP 更新报文时，携带私有自治系统号。

13. 指定路由更新报文的源接口

为使接口在出现问题时仍能发送更新报文，可配置允许内部 BGP 会话使用任何可与对端建立 TCP 连接的接口，通常使用 Loopback 接口。

表5-15 配置路由更新报文的源接口

操作	命令
配置路由更新报文的源接口	peer { peer-address group-name } connect-interface interface-type interface-number
取消路由更新报文源接口的设置	undo peer { peer-address group-name } connect-interface

缺省情况下，BGP 使用最佳路由更新报文的源接口。

14. 配置激活/去激活对等体（组）

BGP 发言者与对被去激活的对等体或对等体组之间不交换路由信息。

表5-16 激活/去激活对等体（组）

操作	命令
激活对等体/对等体组	peer { group-name peer-address } enable
去激活对等体/对等体组	undo peer { group-name peer-address } enable

缺省情况下，对等体或对等体组是激活的。

MD5 认证命令可以在 BGP 视图或 MBGP 的 VPN-instance 地址族视图下配置。当在 BGP 视图下配置时，对 MBGP 的组播扩展和 MBGP 的 VPN 扩展同样有效，因为这三者使用同一条 TCP 连接。

15. 配置 BGP 的 MD5 认证

BGP 对等体/对等体组之间需要建立并保持 TCP 连接，为提高 BGP 的安全性，可以配置在建立 TCP 连接时进行 MD5 认证。如果认证失败，则不能建立 TCP 连接。BGP 的 MD5 认证功能并不对 BGP 报文进行认证，它只是为 TCP 连接设置一个 MD5 认证密码，由 TCP 完成认证。

表5-17 配置 BGP 的 MD5 认证

操作	命令
配置对等体/对等体组的 MD5 认证	peer { group-name peer-address } password { cipher simple } password
取消 MD5 认证	undo peer { group-name peer-address } password

缺省情况下，BGP 在建立 TCP 连接时，不进行 MD5 认证。

16. 配置禁止 BGP 对等体/对等体组发起或接收 BGP 连接

表5-18 禁止 BGP 对等体/对等体组发起或接收 BGP 连接

操作	命令
禁止 BGP 对等体/对等体组发起或接收 BGP 连接	peer { group-name peer-address } shutdown
恢复缺省设置	undo peer { group-name peer-address } shutdown

缺省情况下，允许对等体/对等体组发起或接收 BGP 连接。

5.2.4 配置 BGP 对等体/对等体组的路由过滤

请在 BGP 视图下进行下面配置。

1. 指定对等体/对等体组的路由策略

对等体组的成员必须与所在的组使用相同的出方向路由更新策略，但入方向的策略可以不同。即，对外发布路由时，一个对等体组遵循的策略是相同的，而在接收路由时，各对等体可以选择自己的策略。

表5-19 指定对等体/对等体组的路由策略

操作	命令
配置 BGP 对从对等体/对等体组接收到的路由应用路由策略	peer { group-name peer-address } route-policy policy-name import
取消该路由策略	undo peer { group-name peer-address } route-policy policy-name import
配置 BGP 对向对等体组发送的路由应用路由策略	peer group-name route-policy policy-name export
取消该路由策略	undo peer group-name route-policy policy-name export

缺省情况下，不对接收及发送的路由应用路由策略。

2. 配置对等体/对等体组的基于 IP 访问控制列表的路由过滤策略

表5-20 配置对等体/对等体组的基于 IP 访问控制列表的路由过滤策略

操作	命令
配置 BGP 基于访问控制列表过滤从对等体/对等体组收到的路由	peer { group-name peer-address } filter-policy acl-number import
取消对接收路由的过滤	undo peer { group-name peer-address } filter-policy acl-number import
配置 BGP 基于访问控制列表过滤向对等体组发布的路由	peer group-name filter-policy acl-number export
取消对发布路由的过滤	undo peer group-name filter-policy acl-number export

缺省情况下，不对接收及发布的路由进行过滤。

3. 配置对等体/对等体组的基于 AS 路径列表的路由过滤策略

表5-21 配置对等体/对等体组的基于 AS 路径列表的过滤策略

操作	命令
配置 BGP 基于 AS 路径列表过滤从对等体/对等体组收到的路由	peer { group-name peer-address } as-path-acl number import
取消对接收路由的过滤	undo peer { group-name peer-address } as-path-acl number import
配置 BGP 基于 AS 路径列表过滤向对等体组发布的路由	peer group-name as-path-acl number export
取消对发布路由的过滤	undo peer group-name as-path-acl number export

缺省情况下，不对接收及发布的路由进行过滤。

4. 配置对等体/对等体组的基于前缀列表的路由过滤策略

表5-22 配置对等体/对等体组的基于前缀列表的路由过滤策略

操作	命令
配置 BGP 基于地址前缀列表过滤从对等体/对等体组收到的路由	peer { group-name peer-address } ip-prefix prefixname import
取消对接收路由的过滤	undo peer { group-name peer-address } ip-prefix prefixname import
配置 BGP 基于地址前缀列表过滤向对等体组发布的路由	peer group-name ip-prefix prefixname export
取消对发布路由的过滤	undo peer group-name ip-prefix prefixname export

缺省情况下，不对接收及发布的路由进行过滤。

5.2.5 取消 IGP 和 IBGP 路由同步

请在 BGP 视图下进行下面配置。

表5-23 配置取消 IGP 和 IBGP 路由同步

操作	命令
配置取消 IGP 和 IBGP 路由同步	undo synchronization

5.2.6 配置 BGP 定时器

当对等体间建立了 BGP 连接后，它们定时向对端发送 Keepalive Message，以防止路由器认为 BGP 连接已中断。若路由器在设定的连接保持时间（Holdtime）内未收到对端的 Keepalive Message 或任何其它类型的报文，则认为此 BGP 连接已经被中断，从而断开此 BGP 连接，并对从此 BGP 连接收到的路由进行相应的处理。因此，发送 Keepalive Message 的间隔时间和 BGP 连接保持时间是 BGP 机制中两个非常重要的参数。

BGP 路由器和它的对等体在建立 BGP 连接时，需要进行协商，协商得到的保持时间为该 BGP 路由器的保持时间和对等体的保持时间中时间较小的那个。如果保持时间协商结果为 0，则不发送 keepalive Message，且不再检测 Holdtime 是否超时。

请在 BGP 视图下进行下列配置。

表5-24 配置 BGP 定时器

操作	命令
配置 BGP 定时器	timer keep-alive keepalive-interval hold holdtime-interval
恢复定时器的缺省值	undo timer

合理的最小 Hold-time 为 keepalive message 发送间隔的三倍。如果配置 Holdtime 不为 0，则至少为 3 秒。

缺省情况下，发送 keepalive 的时间间隔为 60 秒；保持定时器时间为 180 秒。

5.2.7 配置本地优先级

可通过配置不同的本地优先级来影响 BGP 的路由选择。当一个运行 BGP 的路由器通过不同的 IBGP 对等体得到目的地相同、下一跳不同的路由时，将选取本地优先级最高的路由。

请在 BGP 视图下进行下列配置。

表5-25 配置本地优先级

操作	命令
配置本地优先级	default local-preference value
恢复缺省的本地优先级	undo default local-preference

本地优先级只在 IBGP 对等体之间交换 Update 报文时发送，不发送到本自治系统之外。

缺省情况下，本地优先级的值为 100。

说明：

在配置完缺省的本地优先级后，只有在此之后接收和发送路由时才会触发 BGP 对路径的重新优选。若要立即或对已有的路由进行重新优选，需要使用 **refresh bgp all import** 或 **reset bgp all** 命令。

5.2.8 配置自治系统的 MED 值

多出口区分 MED（Multi-Exit Discriminators）属性是路由的外部路由权（Cost），它在自治系统之间交换，但进入自治系统的 MED 不会再发送到该自治系统以外。

自治系统使用本地优先级属性来进行出自治系统的路由选择；而 MED 属性用于判断进入自治系统的最佳路由，当一个运行 BGP 的路由器通过不同的 EBGP 对等体得到目的地相同、下一跳不同的多条路由时，在其它条件相同的情况下，将选择 MED 值较小者作为自治系统的优选路由。

请在 BGP 视图下进行下列配置。

表5-26 配置系统的 MED 值

操作	命令
配置系统的 MED 值	default med med-value
恢复系统缺省的 MED 值	undo default med

上述配置只比较来自同一 AS 中的不同 EBGP 对等体的路由的 MED 值，如果要比较来自不同自治系统的对等体的路由的 MED 值，需要配置 **compare-different-as-med** 命令。

缺省情况下，MED 值为 0。

5.2.9 比较来自不同 AS 邻居路径的 MED 值

该命令用于选择最佳路径。在其它条件相同的情况下，MED 较小的路由被优选作为自治系统的外部路由。

请在 BGP 视图下进行下列配置。

表5-27 比较来自不同 AS 邻居路径的 MED 值

操作	命令
比较来自不同 AS 邻居路径的 MED 值	compare-different-as-med
禁止比较来自不同 AS 邻居路径的 MED 值	undo compare-different-as-med

缺省情况下，不允许比较来自不同 AS 邻居路径的 MED 属性值。

除非能够确认不同的自治系统采用了同样的 IGP 和路由选择方式，否则不要使用该配置。

5.2.10 配置 BGP 团体属性

团体属性是一个可选过渡属性，某些团体属性是公认的，具有全球意义，一般称为标准的团体属性，某些则是用于特殊用途，用户也可以定义扩展的团体属性。

团体属性列表是标识一个团体信息的列表，可分为标准团体访问列表（Standard-community-list）与扩展团体访问列表（Extended-community-list）两种。

此外，一条路由也可以有一个以上的团体属性。在一条路由中多个团体属性的发言者可以按照一个、几个或全部属性操作。防火墙在传递路由到其它对等体之前可以选择是否改变团体属性。

请在系统视图下进行下列配置。

表5-28 配置团体属性

操作	命令
配置标准团体列表	ip community-list <i>standard-community-list-number</i> { permit deny } [<i>aa:nn</i>] [internet] [no-export-subconfed] [no-advertise] [no-export]
配置扩展团体列表	ip community-list <i>extended-community-list-number</i> { permit deny } <i>as-regular-expression</i>
取消配置的团体列表	undo ip community-list { <i>standard-community-list-number</i> <i>extended-community-list-number</i> }

缺省情况下，未配置 BGP 团体属性。

标准团体访问列表的取值范围为 1~99，扩展团体访问列表的取值为 100~199。

5.2.11 配置 BGP 路由聚合

BGP 支持 CIDR 路由，支持路由聚合。BGP 路由聚合有两种方式：自动聚合 **summary** 与手动聚合 **aggregate**。自动聚合 **summary** 是对 BGP 引入的 IGP 子网路由进行聚合。配置 **summary** 后，BGP 将不能接收从 IGP 引入的子网路由。手动聚合 **aggregate** 是对 BGP 本地路由进行的聚合。在手动聚合方式下可配置一系列参数。通常情况下，手动聚合的优先级要比自动聚合的优先级高。

请在 BGP 视图下进行下列配置。

表5-29 配置 BGP 路由聚合

操作	命令
配置子网路由自动聚合功能	summary
取消子网路由自动聚合功能	undo summary
配置本地路由聚合功能	aggregate address mask [as-set] [detail-suppressed] [suppress-policy route-policy-name] [origin-policy route-policy-name] [attribute-policy route-policy-name]
取消本地路由聚合功能	undo aggregate address mask [as-set] [detail-suppressed] [suppress-policy route-policy-name] [origin-policy route-policy-name] [attribute-policy route-policy-name]

缺省情况下，BGP 不对子网及本地路由进行聚合。

5.2.12 配置 BGP 协议的优先级

每一种路由协议都有自己的优先级（**preference**），协议的优先级将最后决定路由策略采用哪种路由协议获取的路由作为最佳路由。优先级的数值越大，其实际的优先级越低。BGP 有三种路由：从外部对等体学到的路由，从内部对等体学到的路由及本地产生的路由。这三种路由的优先级可以是不同的，可以分别针对这三种路由手工设定 BGP 的优先级。

支持为不同的子地址族设置不同的 BGP 优先级，目前支持单播地址族和组播地址族。

请在 BGP 视图下进行下列配置。

表5-30 设定协议的优先级

操作	命令
设定 BGP 协议的优先级	preference value1 value2 value3
恢复 BGP 协议优先级的缺省值	undo preference

value1 为从 EBGP 邻居收到的路由的优先级, *value2* 为从 IBGP 邻居收到的路由的优先级, *value3* 为本地产生的路由的优先级, 取值范围均为 1~256。缺省情况下, *value1*、*value2*、*value3* 的值分别为 256、256、130。

5.2.13 配置 BGP 路由反射器

为保证 IBGP 对等体之间的连通性, IBGP 对等体之间需要建立全闭合网。在某些网络中, IBGP 对等体数目很多, 内部 BGP 网络变得非常大, 建立全闭合网开销很大。这就要求使用新的对等技术。路由反射器概念的基本思想是: 指定一个集中路由器作为内部对话的焦点。多个 BGP 路由器可以与一个中心点对等化, 然后多个路由反射器再进行对等化。

路由反射器作为其它路由器的集中点, 其它路由器就称为客户机。客户机与路由反射器对等并与其交换选路信息。路由反射器会依次在客户机之间传递 (或称反射) 信息。

在下图中, SecPathA 从外部对等体收到一个更新信息并把它传递到 SecPathC。SecPathC 被配置成路由反射器, 它有两个客户机: SecPathA 和 SecPathB。

SecPathC 把更新信息从客户机 SecPathA 反射给客户机 SecPathB。在这种配置下, 实际并不需要 SecPathA 和 SecPathB 之间的对等对话, 因为路由反射器会把 BGP 信息转给 SecPathB。

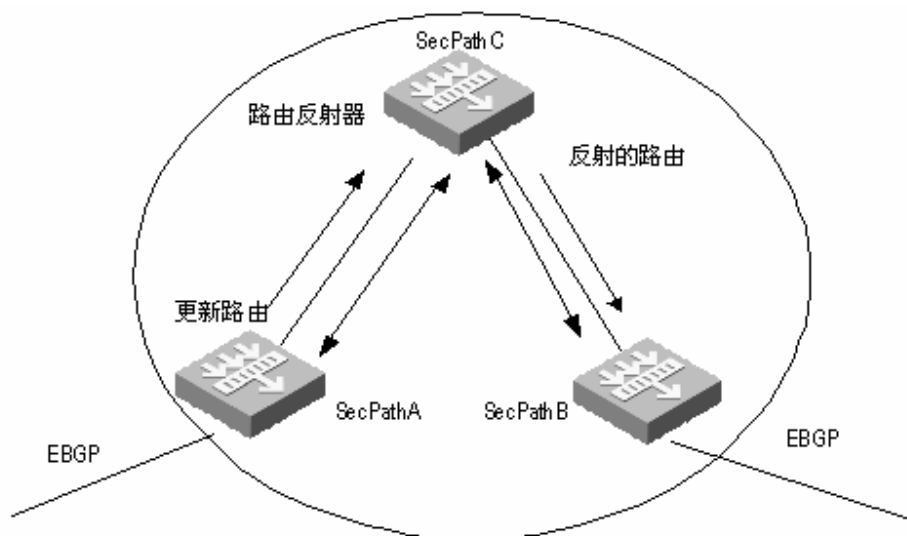


图5-1 路由反射器示意图

反射器是可以完成路由反射功能的路由器。路由反射器的 IBGP 对等体分为两类: 客户机和非客户机。一个路由反射器和它的客户机构成一个群 (Cluster)。在自治系统中不属于这个群的其它所有对等体就是非客户机。路由反射器的指定和客户机的加入是由命令 **peer reflect-client** 实现的。

非客户机与路由反射器之间，以及非客户机互相之间必须组成闭合网，因为它们遵循 IBGP 闭合网的基本规则。客户机不应与其相关群之外的 IBGP 建立对等。路由反射功能只在路由反射器上完成，所有的客户机和非客户机都是常规的 BGP 对等体，与路由反射器的功能无关。客户机所以被看成是客户机仅仅是因为路由反射器把它们列为客户机。

1. 配置客户到客户的路由反射

请在 BGP 视图下进行下列配置。

表5-31 配置客户到客户的路由反射

操作	命令
允许客户到客户的路由反射	reflect between-clients
禁止客户到客户的路由反射	undo reflect between-clients

缺省情况下，允许客户到客户的路由反射。

2. 配置路由反射器

通常一个群中有一个路由反射器，该群由路由反射器的路由器 ID 来识别。

请在 BGP 视图下进行下列配置。

表5-32 配置路由反射器的群 ID

操作	命令
配置路由反射器的群 ID	reflector cluster-id { cluster-id address }
取消路由反射器的群 ID	undo reflector cluster-id

3. 两种在自治系统内部避免循环的措施

随着路由反射器的引入，就有自治系统内产生选路循环的可能性。离开一个群的选路更新报文可能会试图回到这个群中。传统的 AS 路径方法不能探测到 AS 内部的循环，因为选路更新报文尚未离开 AS。BGP 在配置路由反射器时，提供了下述两种在 AS 内部避免循环的措施：

(1) 配置路由反射器的始发者 ID

始发者 ID（Originator_ID）如果配置不当，更新报文回到始发者，始发者会放弃它。此项参数无须配置，在启动 BGP 时自动配置。

(2) 配置路由反射器的群 ID

5.2.14 配置 BGP 自治系统联盟属性

联盟是处理 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 对等体全连接，并同联盟中其它的子自治系统建立连接。

联盟的缺陷是：从非联盟向联盟方案转变时，要求路由器重新进行配置，逻辑拓扑基本上也要改变；而且，若没有手工设置的 BGP 策略，通过联盟的选路有可能次优路径。

1. 配置联盟 ID

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。

请在 BGP 视图下进行下列配置。

表5-33 配置联盟的 ID

操作	命令
配置联盟的 ID	confederation id <i>as-number</i>
取消联盟的 ID	undo confederation id

缺省情况下，未配置联盟的 ID 号。

在配置联盟的 ID 号时，不能够与已经存在的自治系统号相同。

2. 配置属于联盟的子自治系统

请先配置联盟 ID，再配置属于联盟的子自治系统。一个联盟最多可包括 32 个子自治系统。配置属于联盟的子自治系统时使用的 *as-number* 联盟内部有效。

请在 BGP 视图下进行下列配置。

表5-34 配置属于联盟的子自治系统

操作	命令
配置属于联盟的子自治系统	confederation peer-as <i>as-number-1</i> [... <i>as-number-n</i>]
删除属于联盟的子自治系统	undo confederation peer-as [<i>as-number-1</i>] [... <i>as-number-n</i>]

缺省情况下，未配置属于联盟的子自治系统。

配置联盟子自治系统号时，所配置的子自治系统号不能够与没有配置对等体组自治系统号下的某个对等体的自治系统号相同。

3. 配置可同非标准兼容的自治系统联盟属性

如果需要与实现机制不同于 RFC1965 的设备互通，必须对联盟中所有的此类路由器进行配置。

请在 BGP 视图下进行下列配置。

表5-35 配置可同非标准兼容的自治系统联盟属性

操作	命令
配置可同非标准兼容的自治系统联盟属性	confederation nonstandard
撤消同非标准兼容的自治系统联盟	undo confederation nonstandard

缺省情况下，配置的联盟与 RFC1965 一致。

5.2.15 配置 BGP 路由衰减

路由不稳定性的主要可能原因是以前存在于路由表的一条路由间歇性的消失和重现，这种情况称为摆动（flapping）。摆动发生时，update 报文在网络上反复传播，会占用极大的带宽和路由器的处理时间，应尽力避免这种情况的发生。控制路由不稳定的技术是路由衰减。

衰减把路由分为稳定和不稳定两类，不稳定的路由应该被抑制（不被通告）。路由的历史表现是评估未来稳定性的基础。每当路由发生摆动，就给与惩罚，当惩罚达到一个预定的门限时，路由被抑制。随着时间推移，惩罚值按照幂函数递减，下降到一个门限时，路由解除抑制，被重新通告。

请在 BGP 视图下进行下列配置。

表5-36 配置 BGP 路由衰减

操作	命令
配置 BGP 路由衰减	dampening [<i>half-life-reachable</i> <i>half-life-unreachable</i> <i>reuse suppress ceiling</i>] [route-policy <i>route-policy-name</i>]
清除路由摆动衰减信息及解除对已抑制路由的抑制（用户视图）	reset bgp dampening [<i>network-address</i> [<i>mask</i>]]
取消 BGP 路由衰减	undo dampening

缺省情况下，未配置 BGP 路由衰减。

需要注意的是：命令中各参数相互依存，若配置了任何一个，那么也必须指定其它参数。

dampening 命令只对从 EBGP 邻居学到的路由进行衰减，对 IBGP 路由不进行衰减。

5.2.16 配置 BGP 与 IGP 的交互

BGP 可以向其它的自治系统发送本自治系统的内部网络的信息。为了达到此目的，可以将防火墙通过 IGP 路由协议得到的关于本系统内部的网络信息通过 BGP 发送出去。

请在 BGP 视图下进行下列配置。

表5-37 引入 IGP 协议的路由信息

操作	命令
配置 BGP 引入 IGP 协议的路由	import-route <i>protocol</i> [<i>process-id</i>] [<i>med med</i>] [<i>route-policy route-policy-name</i>]
取消 BGP 引入 IGP 协议的路由	undo import-route <i>protocol</i> [<i>process-id</i>]
将本地的默认路由引入 BGP 中	default-route imported
禁止将本地的默认路由引入 BGP 中	undo default-route imported

缺省情况下，BGP 将不引入其它协议的路由。

protocol 指定可引入的源路由协议，目前可为 direct、static、rip、ospf、ospf-ase 和 ospf-nssa。

有关引入路由信息的详细描述请参见 6.2.1 配置路由过滤。

5.2.17 配置本地 AS 号的重复次数

该命令可配置本地 AS 号的重复次数。

请在 BGP 视图下进行下列配置。

表5-38 配置 as-path 的重复次数

操作	命令
配置本地 AS 号的重复次数	peer { <i>group-name</i> <i>peer-address</i> } allow-as-loop [<i>number</i>]
取消配置本地 AS 号的重复次数	undo peer { <i>group-name</i> <i>peer-address</i> } allow-as-loop

缺省情况下，*number* 取值为 3。

5.2.18 定义访问控制列表、AS 路径列表和 Route-policy

访问控制列表（ACL）、AS 路径列表和 Route-policy 均可以作为 BGP 过滤的条件。

1. 定义访问控制列表

请参见本手册的“安全”部分。

2. 定义 AS 路径列表

BGP 的路由信息中包含一个自治系统路径域，称为 AS 路径属性。可以使用 **as-path-acl** 匹配 BGP 路由信息的自治系统路径域，过滤掉不符合条件的路由信息。对于相同的列表号，用户可以定义多条 **as-path-acl**，即一个列表号代表一组 **as-path** 访问列表。每个 AS 路径列表是用数字来标识的。

请在系统视图下进行下列配置。

表5-39 配置 AS 路径列表

操作	命令
配置 AS 路径列表	ip as-path-acl <i>aspath-acl-number</i> { permit deny } <i>as-regular-expression</i>
取消定义的 AS 路径列表	undo ip as-path-acl <i>aspath-acl-number</i>

缺省情况下，未定义 AS 路径列表。

在匹配过程中，AS 访问列表号 *aspath-acl-number* 之间是一种“或”的关系，即路由信息通过这组列表中一条就意味着通过由该列表号标识的这组 **as-path** 列表的过滤。

3. 定义 Route-policy

第一步：定义 Route-policy，请参见 6.2.2 通过 Route-policy 实现路由策略。

第二步：定义匹配规则，请参见 6.2.2 通过 Route-policy 实现路由策略。

第三步：定义赋值规则，请参见 6.2.2 通过 Route-policy 实现路由策略。

5.2.19 配置 BGP 路由过滤

1. 配置 BGP 对接收的路由信息进行过滤

请在 BGP 视图下进行下列配置。

可对 BGP 引入的路由进行过滤，只有满足某些条件的路由才能被 BGP 引入。

表5-40 配置对引入路由的过滤

操作	命令
配置对引入的路由进行过滤	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> [<i>gateway ip-prefix-name</i>] } import
取消对引入的路由进行过滤	undo filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> [<i>gateway ip-prefix-name</i>] } import

更详细描述请参见 6.2.1 配置路由过滤。

2. 配置 BGP 对发布的路由信息进行过滤

可对 BGP 发布的路由进行过滤，只有满足某些条件的路由才能被 BGP 发布。

请在 BGP 视图下进行下列配置。

表5-41 配置 BGP 对发布路由的过滤

操作	命令
配置对发布的路由进行过滤	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } export [<i>protocol</i>]
取消对发布的路由进行过滤	undo filter-policy <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } export [<i>protocol</i>]

缺省情况下，BGP 不对接收和发布的路由信息进行过滤。

当在此命令中指定 *protocol* 时，可用于过滤从指定路由协议引入的路由，目前可包括：**direct**、**static**、**rip**、**ospf**、**ospf-ase** 和 **ospf-nssa**。

更详细的描述请参见 6.2.1 配置路由过滤。

5.2.20 复位 BGP 连接

用户改变 BGP 的策略或协议配置后，可以重置当前 BGP 连接，使新的配置生效。

请在用户视图下进行下列配置。

表5-42 复位 BGP 的连接

操作	命令
复位 BGP 与特定对等体间的连接	reset bgp <i>peer-address</i> [vpn-instance <i>vpn-instance-name</i>]
复位所有的 BGP 连接	reset bgp all [vpn-instance <i>vpn-instance-name</i>]
复位指定对等体组中的所有成员的 BGP 连接	reset bgp group <i>group-name</i> [vpn-instance <i>vpn-instance-name</i>]

5.2.21 配置 BGP 路由刷新

用户改变 BGP 的策略或协议配置后，可以使用 BGP 路由刷新功能，在无需重置 BGP 连接的情况下使新的配置生效。

请在用户视图下进行下列配置。

表5-43 配置 BGP 路由刷新

操作	命令
配置 BGP 路由刷新	refresh bgp { all <i>peer-address</i> group <i>group-name</i> } { import export }

5.3 BGP 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 BGP 的运行情况，用户可以通过查看显示信息验证配置的效果。在用户视图下执行 **debugging** 命令可对 BGP 进行调试。

表5-44 BGP 显示和调试

操作	命令
查看 BGP 路由表中的信息	display bgp [multicast vpn4 { all <i>route-distinguisher route-distinguisher</i> <i>vpn-instance vpn-instance-name</i> }] routing [<i>ip-address mask</i>]
查看 BGP 路由表中的路由统计信息	display bgp [multicast vpn4 { all <i>route-distinguisher route-distinguisher</i> <i>vpn-instance vpn-instance-name</i> }] routing statistic
查看 BGP 中 AS 路径列表信息	display ip as-path-acl [<i>aspath-acl-number</i>]
查看团体列表信息	display ip community-list [<i>stand-comm-list-number</i> <i>ext-comm-list-number</i>]
查看 CIDR 路由	display bgp [multicast vpn4 { all <i>route-distinguisher route-distinguisher</i> <i>vpn-instance vpn-instance-name</i> }] routing cidr
查看指定 BGP 团体的路由信息	display bgp [multicast vpn4 { all <i>route-distinguisher route-distinguisher</i> <i>vpn-instance vpn-instance-name</i> }] routing community [<i>aa:nn</i>] [no-export-subconfed] [no-advertise] [no-export] [whole-match]
查看指定 BGP 团体列表允许的路由	display bgp [multicast vpn4 { all <i>route-distinguisher route-distinguisher</i> <i>vpn-instance vpn-instance-name</i> }] routing community-list <i>community-list-number</i> [whole-match]
查看 BGP 衰减的路由	display bgp routing dampened
显示 BGP 对等体通告或者收到的路由信息	display bgp [multicast vpn4 { all <i>route-distinguisher route-distinguisher</i> <i>vpn-instance vpn-instance-name</i> }] routing peer <i>peer-address</i> { advertised received }

操作	命令
显示从 peer 收到的衰减路由信息	display bgp [multicast] routing peer <i>peer-address</i> dampened [statistic <i>ip-address</i>]
显示从 peer 收到的匹配正则表达式的路由信息	display bgp [multicast vpn4 { all route-distinguisher <i>route-distinguisher</i> vpn-instance <i>vpn-instance-name</i> }] routing peer <i>peer-address</i> regular-expression <i>text</i>
查看与指定 as-path-acl 相匹配的路由	display bgp [multicast vpn4 { all route-distinguisher <i>route-distinguisher</i> vpn-instance <i>vpn-instance-name</i> }] routing as-path-acl <i>aspath-acl-number</i>
查看路由摆动统计信息	display bgp routing flap-info [regular-expression <i>as-regular-expression</i> as-path-acl <i>aspath-acl-number</i> address [<i>mask</i> longer-prefix-list]]
查看源 AS 不一致的路由	display bgp [multicast vpn4 { all route-distinguisher <i>route-distinguisher</i> vpn-instance <i>vpn-instance-name</i> }] routing different-origin-as
查看对等体信息	display bgp [multicast vpn4 { all route-distinguisher <i>route-distinguisher</i> vpn-instance <i>vpn-instance-name</i> }] peer [[<i>peer-address</i>] verbose]
查看已经配置的路由信息	display bgp [multicast vpn4 { all route-distinguisher <i>route-distinguisher</i> vpn-instance <i>vpn-instance-name</i> }] network
查看 AS 路径信息	display bgp paths <i>as-regular-expression</i>
查看对等体组信息	display bgp [multicast vpn4 { all route-distinguisher <i>route-distinguisher</i> vpn-instance <i>vpn-instance-name</i> }] group [<i>group-name</i>]
查看匹配 AS 正则表达式的 AS 路径	display bgp [multicast vpn4 { all route-distinguisher <i>route-distinguisher</i> vpn-instance <i>vpn-instance-name</i> }] routing regular-expression <i>as-regular-expression</i>
查看配置的 Route-policy 信息	display route-policy [<i>route-policy-name</i>]
打开 BGP 邻接状态变化的输出开关(BGP 视图)	log-peer-change
关闭 BGP 邻接状态变化的输出开关(BGP 视图)	undo log-peer-change
打开/关闭 BGP 所有报文调试信息开关	[undo] debugging bgp all
打开/关闭 BGP 事件调试信息开关	[undo] debugging bgp event
打开/关闭 BGP 一般运行信息调试开关	[undo] debugging bgp normal
打开/关闭 BGP Keepalive 调试信息开关	[undo] debugging bgp keepalive [receive send] [verbose]

操作	命令
打开/关闭 MBGP Update 报文调试信息开关	<code>[undo] debugging bgp mp-update [receive send] [verbose]</code>
打开/关闭 BGP Open 调试信息开关	<code>[undo] debugging bgp open [receive send] [verbose]</code>
打开/关闭 BGP 包调试信息开关	<code>[undo] debugging bgp packet [receive send] [verbose]</code>
打开/关闭 BGP 路由更新调试信息开关	<code>[undo] debugging bgp route-refresh [receive send] [verbose]</code>
打开/关闭 BGP Update 报文调试信息开关	<code>[undo] debugging bgp update [receive send] [verbose]</code>
清除路由的摆动统计信息	<code>reset bgp flap-info [regular-expression as-regular-expression as-path-acl aspath-acl-number address [mask]]</code>
清除指定目的地址的路由的摆动统计信息	<code>reset bgp peer-address flap-info</code>

5.4 BGP 典型配置举例

5.4.1 配置自治系统联盟属性



注意：

配置用例中，只列出了与 BGP 配置相关的命令。

1. 组网需求

下图将自治系统 100 划分为 3 个子自治系统 1001, 1002, 1003, 配置 EBGp、联盟 EBGp 和 IBGP。

2. 组网图

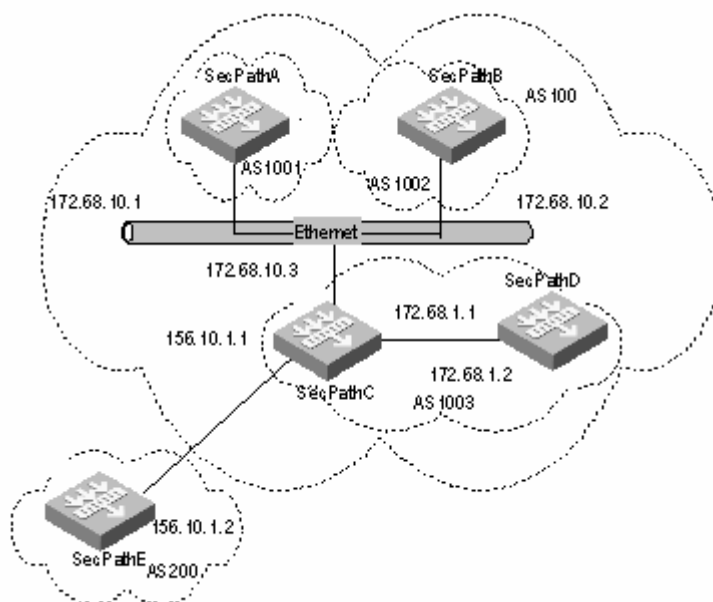


图5-2 配置自治系统联盟组网图

3. 配置步骤

配置 SecPathA:

```
[H3C] bgp 1001
[H3C-bgp] confederation id 100
[H3C-bgp] confederation peer-as 1002 1003
[H3C-bgp] group confed1002 external
[H3C-bgp] peer confed1002 as-number 1002
[H3C-bgp] group confed1003 external
[H3C-bgp] peer confed1003 as-number 1003
[H3C-bgp] peer 172.68.10.2 group confed1002
[H3C-bgp] peer 172.68.10.3 group confed1003
```

配置 SecPathB:

```
[H3C] bgp 1002
[H3C-bgp] confederation id 100
[H3C-bgp] confederation peer-as 1001 1003
[H3C-bgp] group confed1001 external
[H3C-bgp] peer confed1001 as-number 1001
[H3C-bgp] group confed1003 external
[H3C-bgp] peer confed1003 as-number 1003
[H3C-bgp] peer 172.68.10.1 group confed1001
[H3C-bgp] peer 172.68.10.3 group confed1003
```

配置 SecPathC:

```

[H3C] bgp 1003
[H3C-bgp] confederation id 100
[H3C-bgp] confederation peer-as 1001 1002
[H3C-bgp] group confed1001 external
[H3C-bgp] peer confed1001 as-number 1001
[H3C-bgp] group confed1002 external
[H3C-bgp] peer confed1002 as-number 1002
[H3C-bgp] peer 172.68.10.1 group confed1001
[H3C-bgp] peer 172.68.10.2 group confed1002
[H3C-bgp] group ebgp200 external
[H3C-bgp] peer 156.10.1.2 group ebgp200 as-number 200
[H3C-bgp] group ibgp1003 internal
[H3C-bgp] peer 172.68.1.2 group ibgp1003

```

5.4.2 配置 BGP 路由反射器

1. 组网需求

SecPathB 接收了一个经过 EBGP 的更新报文并将之传给 SecPathC。SecPathC 被配置为路由反射器，它有两个客户：SecPathB 和 SecPathD。SecPathB 和 SecPathD 间不需一个 IBGP 连接，当 SecPathC 接收了来自 SecPathB 的路由更新时，它将此信息反射给 SecPathD，反之亦然。

2. 组网图

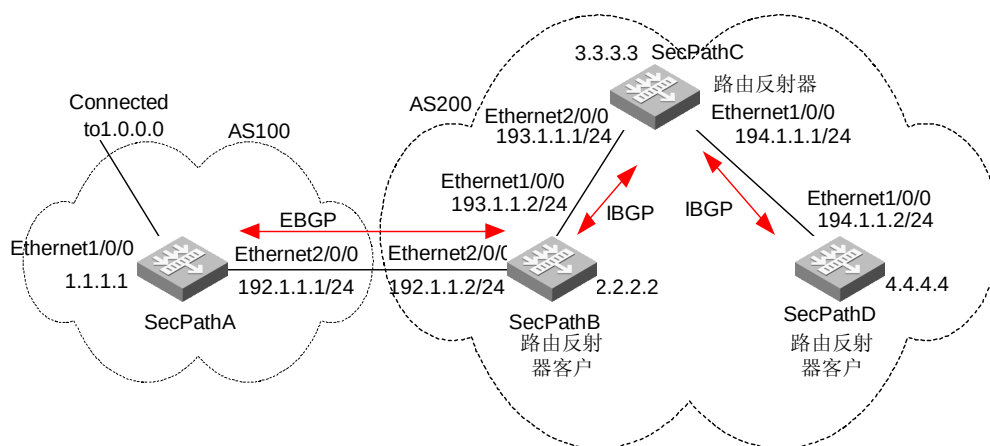


图5-3 配置 BGP 路由反射器组网图

3. 配置步骤

配置 SecPathA:

```

[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 192.1.1.1 255.255.255.0
[H3C-Ethernet2/0/0] interface ethernet 1/0/0

```

```
[H3C-Ethernet1/0/0] ip address 1.1.1.1 255.0.0.0
[H3C-Ethernet1/0/0] quit
[H3C] bgp 100
[H3C-bgp] group ex external
[H3C-bgp] peer 192.1.1.2 group ex as-number 200
[H3C-bgp] network 1.0.0.0 255.0.0.0
```

配置 SecPathB:

```
[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 192.1.1.2 255.255.255.0
[H3C-Ethernet2/0/0] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 193.1.1.2 255.255.255.0
[H3C-Ethernet1/0/0] quit
[H3C] bgp 200
[H3C-bgp] group ex external
[H3C-bgp] peer 192.1.1.1 group ex as-number 100
[H3C-bgp] group in internal
[H3C-bgp] peer 193.1.1.1 group in
```

配置 SecPathC:

```
[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 193.1.1.1 255.255.255.0
[H3C-Ethernet2/0/0] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 194.1.1.1 255.255.255.0
[H3C-Ethernet1/0/0] quit
[H3C] bgp 200
[H3C-bgp] group rr internal
[H3C-bgp] reflect between-clients
[H3C-bgp] peer rr reflect-client
[H3C-bgp] peer 193.1.1.2 group rr
[H3C-bgp] peer 194.1.1.2 group rr
```

配置 SecPathD:

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 194.1.1.2 255.255.255.0
[H3C-Ethernet1/0/0] quit
[H3C] bgp 200
[H3C-bgp] group in internal
[H3C-bgp] peer 194.1.1.1 group in
```

在 SecPathB 上用命令 **display bgp routing**，可以看到 SecPathB 已知道网络 1.0.0.0 的存在。

在 SecPathD 上用命令 **display bgp routing**，可以看到 SecPathD 也知道网络 1.0.0.0 的存在。

5.4.3 配置 BGP 路径选择

1. 组网需求

本例说明怎样通过 BGP 属性的使用来管理路由选择。

所有防火墙都配置 BGP，AS200 中的 IGP 使用 OSPF。

SecPathA 在 AS100 中，SecPathB、SecPathC 和 SecPathD 在 AS200 中。SecPathA 与 SecPathB 和 SecPathC 之间运行 EBGP。SecPathB 和 SecPathC 与 SecPathD 之间运行 IBGP。

2. 组网图

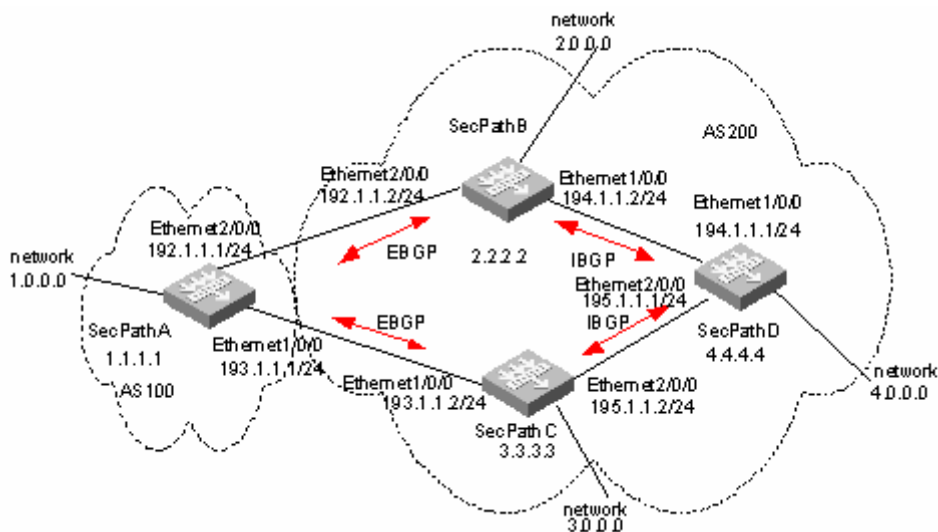


图5-4 配置 BGP 路径选择的组网图

3. 配置步骤

配置 SecPathA:

```
[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 192.1.1.1 255.255.255.0
[H3C-Ethernet2/0/0] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 193.1.1.1 255.255.255.0
[H3C-Ethernet1/0/0] quit
[H3C] bgp 100
[H3C-bgp] network 1.0.0.0
[H3C-bgp] group ex192 external
[H3C-bgp] peer 192.1.1.2 group ex192 as-number 200
[H3C-bgp] group ex193 external
[H3C-bgp] peer 193.1.1.2 group ex193 as-number 200
[H3C-bgp] quit
```

配置 SecPathA 的 MED 属性

增加访问列表到 SecPathA 上，允许网络 1.0.0.0

```
[H3C] acl number 2001
```

```
[H3C-acl-basic-2001] rule permit source 1.0.0.0 0.255.255.255
```

定义两个 Route-policy，一个名为 apply_med_50，另一个名为 apply_med_100，第一个 Route-policy 为网络 1.0.0.0 设置的 MED 属性为 50，第二个 Route-policy 设置的 MED 属性为 100。

```
[H3C] route-policy apply_med_50 permit node 10
```

```
[H3C-route-policy] if-match acl 2001
```

```
[H3C-route-policy] apply cost 50
```

```
[H3C-route-policy] quit
```

```
[H3C] route-policy apply_med_100 permit node 10
```

```
[H3C-route-policy] if-match acl 2001
```

```
[H3C-route-policy] apply cost 100
```

```
[H3C-route-policy] quit
```

应用 apply_med_50 到邻居 SecPathC（193.1.1.2）出口路由更新上，应用 apply_med_100 到邻居 SecPathB（192.1.1.2）的出口路由更新上。

```
[H3C] bgp 100
```

```
[H3C-bgp] peer ex193 route-policy apply_med_50 export
```

```
[H3C-bgp] peer ex192 route-policy apply_med_100 export
```

配置 SecPathB:

```
[H3C] interface ethernet 2/0/0
```

```
[H3C-Ethernet2/0/0] ip address 192.1.1.2 255.255.255.0
```

```
[H3C-Ethernet2/0/0] interface ethernet 1/0/0
```

```
[H3C-Ethernet1/0/0] ip address 194.1.1.2 255.255.255.0
```

```
[H3C-Ethernet1/0/0] quit
```

```
[H3C] ospf
```

```
[H3C-ospf-1] area 0
```

```
[H3C-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
```

```
[H3C-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
```

```
[H3C] bgp 200
```

```
[H3C-bgp] undo synchronization
```

```
[H3C-bgp] group ex external
```

```
[H3C-bgp] peer 192.1.1.1 group ex as-number 100
```

```
[H3C-bgp] group in internal
```

```
[H3C-bgp] peer 194.1.1.1 group in
```

配置 SecPathC:

```
[H3C] interface ethernet 1/0/0
```

```
[H3C-Ethernet1/0/0] ip address 193.1.1.2 255.255.255.0
```

```
[H3C-Ethernet1/0/0] interface ethernet 2/0/0
```

```
[H3C-Ethernet2/0/0] ip address 195.1.1.2 255.255.255.0
```



```
[H3C-Ethernet2/0/0] quit
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 193.1.1.0 0.0.0.255
[H3C-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[H3C] bgp 200
[H3C-bgp] group ex external
[H3C-bgp] peer 193.1.1.1 group ex as-number 100
[H3C-bgp] group in internal
[H3C-bgp] peer 195.1.1.1 group in
```

配置 SecPathD:

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 194.1.1.1 255.255.255.0
[H3C-Ethernet1/0/0] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 195.1.1.1 255.255.255.0
[H3C-Ethernet2/0/0] quit
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[H3C-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[H3C-ospf-1-area-0.0.0.0] network 4.0.0.0 0.255.255.255
[H3C] bgp 200
[H3C-bgp] group ex external
[H3C-bgp] peer ex as-number 200
[H3C-bgp] peer 195.1.1.2 group ex
[H3C-bgp] peer 194.1.1.2 group ex
```

为使配置生效，需要使用 **reset bgp all** 命令复位所有的 BGP 邻居。

通过上述配置后，由于 SecPathC 学到的路由 1.0.0.0 的 MED 属性比 SecPathB 学到的更小，SecPathD 优选来自 SecPathC 的路由 1.0.0.0。

如果在配置 SecPathA 时，不配置 SecPathA 的 MED 属性，而在 SecPathC 上配置本地优先级如下：

在 SecPathC 上加上访问列表 2001，允许网络 1.0.0.0

```
[H3C] acl number 2001
[H3C-acl-basic-2001] rule permit source 1.0.0.0 0.255.255.255
```

定义名为 localpref 的路由策略，设置匹配 access list 2001（访问列表 2001）的路由的本地优先级为 200，不匹配的为 100。

```
[H3C] route-policy localpref permit node 10
[H3C-route-policy] if-match acl 2001
[H3C-route-policy] apply local-preference 200
[H3C-route-policy] quit
```

```
[H3C] route-policy localpref permit node 20
[H3C-route-policy] apply local-preference 100
[H3C] quit
```

应用此路由策略到来自 BGP 邻居 193.1.1.1（SecPathA）上。

```
[H3C] bgp 200
[H3C-bgp] peer 193.1.1.1 route-policy localpref import
```

此时，由于 SecPathC 学到的路由 1.0.0.0 的 Local preference 属性值为 200，比 SecPathB 学到的路由 1.0.0.0 的 Local preference 属性值（SecPathB 没有配置 Local preference 属性，默认为 100）更大，SecPathD 依然优选来自 SecPathC 的路由 1.0.0.0。

5.5 BGP 故障诊断与排除

故障之一：邻居关系不能建立（无法进入 Established 状态）。

故障排除：BGP 邻居的建立需要能够使用 179 端口建立 TCP 会话，以及能够正确交换 Open 报文。可按照以下步骤进行检查：

- 检查邻居的 AS 号配置是否正确。
- 检查邻居的 IP 地址是否正确。
- 如果使用 Loopback 接口，检查是否配置了 **connect-interface loopback**。缺省情况下，防火墙使用最佳本地接口建立 TCP 连接，而不会用 loopback 接口。
- 如果是物理上非直连的 EBGP 邻居，检查是否配置了 **peer ebgp-max-hop**。
- 使用 ping 命令检查 TCP 连接是否正常，由于一台防火墙可能有多个接口能够到达对端，应使用扩展的 **ping -a ip-address** 命令指定发送 ping 包的源 IP 地址。
- 如果 Ping 不通，使用 **display ip routing-table** 命令检查路由表中是否存在到邻居的可用路由。
- 如果能 Ping 通，检查是否配置了禁止 TCP 端口 179 的 ACL，如果有，取消对 179 端口的禁止。

5.6 MBGP 简介

5.6.1 MBGP 概述

正如本章开始所介绍的，BGP 作为事实上的外部网关协议，广泛应用于自治系统间的互联。传统的 BGP-4 只能管理 IPv4 的路由信息，对于使用其它网络层协议（如 IPv6 等）的应用，在跨自治系统传播时就会受到一定的限制。

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 MBGP（Multiprotocol Extensions for BGP-4，BGP-4 的多协议扩展），目前的 MBGP 标准是 RFC2858。

MBGP 是向后兼容的，也就是说，支持 BGP 扩展的路由器与不支持 BGP 扩展的路由器可以互通。

5.6.2 MBGP 的扩展属性

BGP-4 使用的报文中，与 IPv4 相关的三条信息都由 Update 报文携带，这三条信息分别是：NLRI（Network Layer Reachability Information，网络层可达性信息）、路径属性中的 Next_Hop（下一跳的 IP 地址）、路径属性中的 Aggregator（该属性中包含形成聚合路由的 BGP 发言者的 IP 地址）。

因特网上实际运行的 BGP 发言者通常都具有一个 IPv4 的地址，因此，BGP-4 只需要将特定网络层协议的信息反映到 NLRI 及路由属性中的 Next_Hop 即可实现对多种网络层协议的支持。

MBGP 中引入了两个新的路径属性：

- **MP_REACH_NLRI**: Multiprotocol Reachable NLRI，多协议可达 NLRI。用于发布可达路由及下一跳信息。
- **MP_UNREACH_NLRI**: Multiprotocol Unreachable NLRI，多协议不可达 NLRI。用于撤销不可达路由。

这两种属性都是可选非过渡（optional non-transitive）的，因此，不提供多协议能力的 BGP 发言者将忽略这两个属性的信息，不把它们传递给其它邻居。

5.6.3 安全网关的 MBGP 应用

安全网关采用地址族（Address Family）来区分不同的网络层协议，关于地址族的一些取值可以参考 RFC1700。

安全网关提供多种 MBGP 扩展应用，包括对组播的扩展、对 BGP/MPLS VPN 的扩展等，不同的扩展应用需在各自的地址族视图下进行。

MBGP 在 BGP/MPLS VPN 中的应用请参见本手册的“VPN”部分中的“BGP/MPLS VPN 配置”章节。

5.7 MBGP 配置

MBGP 是对 BGP 的扩展，BGP 的很多概念和配置原理在 MBGP 中也同样适用。

在配置 MBGP 时，首先需要启动 BGP，再进入相应的地址族视图，配置不同的扩展应用的相关参数。

在配置 MBGP 对等体/对等体组时，首先在 BGP 视图下配置对等体或对等体组的 AS 号，再进入相应的地址族视图下激活该应用的对等体/对等体组关系。

BGP 视图下的部分命令在 MBGP 的地址族视图下也存在，但如果在 MBGP 的地址族视图下配置，则这些命令仅对相应的应用有效。

MBGP 地址族视图下的、与特定应用相关的命令不在本章进行介绍，相应的内容可参见本手册的“VPN”部分中的“BGP/MPLS VPN 配置”章节。

MBGP 的通用配置包括：

- 配置地址族
- 激活对等体组

5.7.1 配置地址族

在介绍了 MBGP 后，有时用 IPv4 单播地址族视图来指示通常意义上的 BGP 视图。请在 BGP 视图下进行下列配置。

表5-45 配置地址族

操作	命令
进入 MBGP 的组播地址族视图	ipv4-family multicast
删除 MBGP 的组播地址族配置	undo ipv4-family multicast
进入 MBGP 的 vpn-instanc 地址族视图	ipv4-family vpn-instance <i>vpn-instance-name</i>
删除 MBGP 的 vpn-instanc 地址族配置	undo ipv4-family vpn-instance <i>vpn-instance-name</i>
进入 MBGP 的 VPNv4 地址族视图	ipv4-family vpnv4 [unicast]
删除 MBGP 的 VPNv4 地址族配置	undo ipv4-family vpnv4 [unicast]

执行 **undo** 命令后，将退回到 BGP 视图，并删除相应的 MBGP 扩展应用配置。

5.7.2 激活对等体/对等体组

BGP 发言者之间交换路由信息，必须首先将单播地址族下的某个对等体组激活，然后，再将单播地址族下已经存在的对等体加入到这个激活的对等体组中。

请在地址族视图下进行下列配置。

表5-46 激活对等体/对等体组

操作	命令
激活指定对等体组	peer group-name enable
去掉已激活的指定对等体组	undo peer group-name enable

操作	命令
将对等体加入激活的对等体组中	peer peer-address group group-name
将对等体从激活的对等体组中删除	undo peer peer-address

缺省情况下，只有 BGP 的 IPv4 单播地址族的对等体组才是激活的，其它类型的对等体或对等体组都是没有激活的，不能交换路由信息。

5.8 MBGP 典型配置举例

MBGP 主要应用于对一些新业务的扩展，其本身的配置与 BGP 很相似，下面的例子与“BGP 典型配置举例”中的例子在组网和配置上都基本一致，主要的不同在于进入 MBGP 的地址族视图，以及激活 MBGP 对等体。

5.8.1 配置 MBGP 路由反射器

1. 组网需求

安全网关 SecPathA、SecPathB、SecPathC 和 SecPathD 上都配置 MBGP 的组播扩展应用，SecPathA 和 SecPathB 是 EBGP 对等体，SecPathC 和 SecPathB、SecPathC 和 SecPathD 是 IBGP 对等体。

SecPathB 接收了一个来自 SecPathA 的 EBGP 更新报文并将之传给 SecPathC。SecPathC 被配置为路由反射器，它有两个客户：SecPathB 和 SecPathD。当 SecPathC 接收到来自 SecPathB 的 EBGP 更新报文时，它将此信息反射给 SecPathD，SecPathB 和 SecPathD 间不需要建立 IBGP 连接，因为 SecPathC 将反射信息给 SecPathD。

2. 组网图

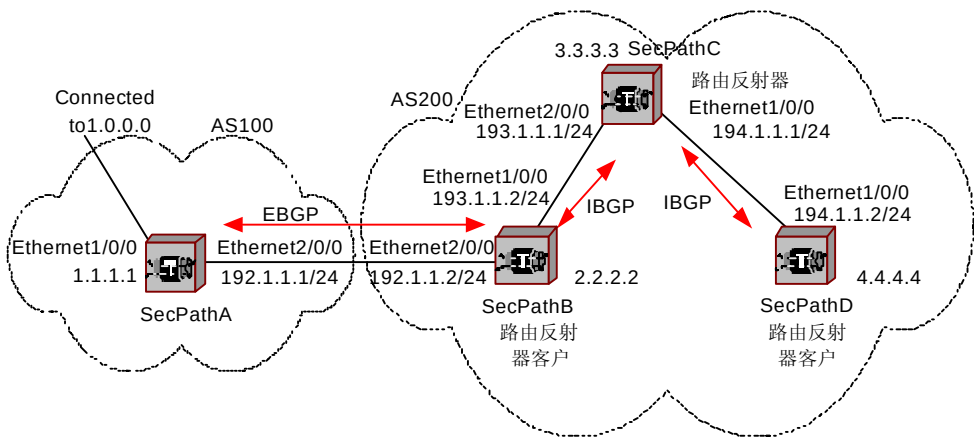


图5-5 配置 MBGP 路由反射器的组网图

3. 配置步骤

(1) 配置 SecPathA

配置接口。

```
[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 192.1.1.1 255.255.255.0
[H3C-Ethernet2/0/0] quit
```

配置 SecPathA 的 MBGP。

```
[H3C] bgp 100
[H3C-bgp] group ex external
[H3C-bgp] peer 192.1.1.2 group ex as-number 200
[H3C-bgp] ipv4-family multicast
[H3C-bgp-af-mul] peer ex enable
[H3C-bgp-af-mu] peer 192.1.1.2 group ex
[H3C-bgp-af-mu] network 1.0.0.0 255.0.0.0
```

(2) 配置 SecPathB

配置接口。

```
[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 192.1.1.2 255.255.255.0
[H3C-Ethernet2/0/0] quit
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 193.1.1.2 255.255.255.0
[H3C-Ethernet1/0/0] quit
```

配置 OSPF。

```
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 193.1.1.0 0.0.0.255
[H3C-ospf-1-area-0.0.0.0] quit
[H3C-ospf-1] quit
```

配置 SecPathB 的 MBGP。

```
[H3C] bgp 200
[H3C-bgp] group ex external
[H3C-bgp] peer 192.1.1.1 group ex as-number 100
[H3C-bgp] group in internal
[H3C-bgp] peer in next-hop-local
[H3C-bgp] peer 193.1.1.1 group in
[H3C-bgp] import-route ospf
[H3C-bgp] import-route direct
[H3C-bgp] ipv4-family multicast
[H3C-bgp-af-mul] peer in next-hop-local
```

```
[H3C-bgp-af-mul] peer ex enable
[H3C-bgp-af-mul] peer in enable
[H3C-bgp-af-mul] peer 192.1.1.1 group ex
[H3C-bgp-af-mul] peer 193.1.1.1 group in
```

(3) 配置 SecPathC

配置接口。

```
[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 193.1.1.1 255.255.255.0
[H3C-Ethernet2/0/0] quit
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 194.1.1.1 255.255.255.0
[H3C-Ethernet1/0/0] quit
```

配置 OSPF。

```
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[H3C-ospf-1-area-0.0.0.0] network 193.1.1.0 0.0.0.255
[H3C-ospf-1-area-0.0.0.0] quit
[H3C-ospf-1] quit
```

配置 SecPathC 的 MBGP。

```
[H3C] bgp 200
[H3C-bgp] group in internal
[H3C-bgp] peer 193.1.1.2 group in
[H3C-bgp] peer 194.1.1.2 group in
[H3C-bgp] peer in reflect-client
[H3C-bgp] ipv4-family multicast
[H3C-bgp-af-mul] peer in enable
[H3C-bgp-af-mul] peer in reflect-client
[H3C-bgp-af-mul] peer 193.1.1.2 group in
[H3C-bgp-af-mul] peer 194.1.1.2 group in
```

(4) 配置 SecPathD

配置接口。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 194.1.1.2 255.255.255.0
[H3C-Ethernet1/0/0] quit
```

配置 OSPF。

```
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
```

```
[H3C-ospf-1-area-0.0.0.0] quit
[H3C-ospf-1] quit
```

配置 SecPathD 的 MBGP:

```
[H3C] bgp 200
[H3C-bgp] group in internal
[H3C-bgp] peer 194.1.1.1 group in
[H3C-bgp] ipv4-family multicast
[H3C-bgp-af-mul] peer in enable
[H3C-bgp-af-mul] peer 194.1.1.1 group in
```

在 SecPathB 上用 `display bgp multicast routing` 查看 BGP 路由表。注意: SecPathB 已知道了网络 1.0.0.0 的存在。

在 SecPathD 上用 `display bgp multicast routing` 查看 BGP 路由表。注意: SecPathD 也知道网络 1.0.0.0 的存在。

第6章 IP 路由策略配置

6.1 IP 路由策略简介

防火墙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，比如只接收或发布一部分满足给定条件的路由信息；一种路由协议（如 **RIP**）可能需要引入（**import**）其它的路由协议（如 **OSPF**）发现的路由信息，从而丰富自己的路由知识；防火墙在引入其它路由协议的路由信息时，可能需要只引入一部分满足条件的路由信息，并对所引入的路由信息的某些属性进行设置，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。

在防火墙中，提供了 **Route-policy**、**acl**、**as-path**、**community-list** 和 **ip-prefix** 五种过滤器供路由协议引用。下面对各种过滤器逐个进行介绍。

1. Route-policy

用于匹配给定路由信息的某些属性，并在条件满足后对该路由信息的某些属性进行设置。

一个 **Route-policy** 可以由多个节点（**node**）构成，每个节点是进行匹配测试的一个单元，节点间依据顺序号（**node-number**）进行匹配。每个节点可以由一组 **if-match** 和 **apply** 子句组成。**if-match** 子句定义匹配规则，匹配对象是路由信息的一些属性。同一节点中的不同 **if-match** 子句是“与”的关系，只有满足节点内所有 **if-match** 子句指定的匹配条件，才能通过该节点的匹配测试。**apply** 子句指定动作，也就是在通过节点的匹配测试后所执行的动作——对路由信息的一些属性进行设置。

一个 **Route-policy** 的不同节点间是“或”的关系，系统依次检查 **Route-policy** 的各个节点，如果通过了 **Route-policy** 的某一节点，就意味着通过该 **Route-policy** 的匹配测试（不进入下一个节点的测试）。

2. 访问控制列表（ACL）

访问控制列表分为四类：高级访问控制列表、基本访问控制列表、基于接口的访问控制列表和 **MAC** 地址过滤列表。

在对路由信息过滤时，一般使用基本访问控制列表和高级访问控制列表。若使用基本访问控制列表，在定义访问列表时指定一个源 **IP** 地址或子网的范围，用于匹配路

由信息的源地址。如使用高级访问列表，则可以使用协议类型、源/目的地址或端口号等多种参数匹配路由信息。

ACL 的有关配置请参见本手册“安全”部分的防火墙配置。

3. 前缀列表（ip-prefix）

前缀列表 **ip-prefix** 的作用类似于 **ACL**，但比它更为灵活，且更易于为用户理解。**ip-prefix** 在应用于路由信息的过滤时，其匹配对象为路由信息的目的地址信息域；另外在 **ip-prefix** 中，用户可以指定 **gateway** 选项，指明只接收某些路由器发布的路由信息。

一个 **ip-prefix** 由前缀列表名标识。每个前缀列表可以包含多个表项，每个表项可以独立指定一个网络前缀形式的匹配范围，并用一个 **index-number** 来标识，**index-number** 指明了在 **ip-prefix** 中进行匹配检查的顺序。

在匹配的过程中，防火墙按升序依次检查由 **index-number** 标识的各个表项，只要有某一表项满足条件，就意味着通过该 **ip-prefix** 的过滤（不会进入下一个表项的测试）。

4. 自治系统路径信息访问列表（as-path-acl）

自治系统路径信息访问列表 **as-path** 仅用于 **BGP**。**BGP** 的路由信息包中包含一个自治系统路径域（在 **BGP** 交换路由信息的过程中，路由信息经过的自治系统路径会记录在这个域中），**as-path** 就是针对自治系统路径域指定匹配条件。

有关 **as-path** 的配置请用户参见“第 5 章 BGP 配置”中的 **ip as-path-acl** 命令。

5. 团体属性列表（community-list）

团体属性列表 **community-list** 仅用于 **BGP**。在 **BGP** 的路由信息包中，包含一个 **community** 属性域，用来标识一个团体。**community-list** 就是针对团体属性域指定匹配条件。

有关 **community-list** 的配置请用户参见“第 5 章 BGP 配置”中的 **ip community-list** 命令。

6.2 IP 路由策略配置

路由策略可以通过两种方式来实现，一是通过过滤列表，如 **ACL**、**ip-prefix**、**as-path-acl**、**community-list** 等，直接实现路由或路由属性的过滤；另一种是通过配置 **Route-policy**，对满足匹配条件的路由的属性进行设置。

本章中的配置包括：

(1) 配置路由过滤

- 定义地址前缀列表或 **ACL**
- 配置对接收到的路由进行过滤

- 引入其它路由协议发现的路由（仅 OSPF 路由过滤需要配置）
- 配置对发布的路由（对 OSPF 指引入路由）进行过滤

(2) 通过 Route-policy 实现路由策略

- 定义 Route-policy
- 定义 Route-policy 的 **if-match** 子句
- 定义 Route-policy 的 **apply** 子句
- 通过 Route-policy 对引入的路由进行过滤

有关BGP通过as-path-acl, community-list实现的路由过滤，请参见 第 5 章 BGP配置。

6.2.1 配置路由过滤

1. 定义过滤条件

(1) 定义地址前缀列表

一个 **ip-prefix** 由前缀列表名标识。每个前缀列表可以包含多个表项，每个表项可以独立指定一个网络前缀形式的匹配范围，并用一个 *index-number* 来标识，*index-number* 指明了在 **ip-prefix** 中进行匹配检查的顺序。

请在系统视图下进行下列配置。

表6-1 定义地址前缀列表

操作	命令
定义地址前缀列表	ip ip-prefix <i>ip-prefix-name</i> [index <i>index-number</i>] { permit deny } <i>network len</i> [greater-equal <i>greater-equal</i> less-equal <i>less-equal</i>] *
取消地址前缀列表	undo ip ip-prefix <i>ip-prefix-name</i> [index <i>index-number</i> permit deny]

在匹配的过程中，防火墙按升序依次检查由 *index-number* 标识的各个表项，只要有某一表项满足条件，就意味着通过该 **ip-prefix** 的过滤（不会进入下一个表项的测试）。

需要注意的是：

- 如果定义了一个以上的前缀列表表项，那么至少应该有一个表项的匹配模式是 **permit** 模式。
- **deny** 模式的表项可以先被定义以快速的过滤掉不符合条件的路由信息，但如果所有表项都是 **deny** 模式，则任何路由都不会通过该地址前缀列表的过滤。
- 可以在定义了多条 **deny** 模式的表项后定义一条 **permit 0.0.0.0/0 greater-equal 0 less-equal 32** 的表项以允许其它所有路由信息通过。

例如，按如下配置可以保证仅过滤掉 10.1.0.0, 10.2.0.0, 10.3.0.0 三个网段的路由，而其它网段的路由信息可以通过。

```
[H3C] ip ip-prefix 1 deny 10.1.0.0 16
[H3C] ip ip-prefix 1 deny 10.2.0.0 16
[H3C] ip ip-prefix 1 deny 10.3.0.0 16
[H3C] ip ip-prefix 1 permit 0.0.0.0 0 greater-equal 0 less-equal 32
```

(2) 定义访问控制列表

请参见本手册的“安全”部分。

2. 配置对接收的路由进行过滤

请在路由协议视图下进行下列配置。

定义一条策略规则，通过对一个 ACL 或地址前缀列表的引用实现在接收路由过程中对不满足条件的路由信息进行过滤。**gateway** 指定只接收来自特定邻居路由器的更新报文。

表6-2 配置对接收路由的过滤

操作	命令
配置对接收的指定地址发布的路由信息进行过滤	filter-policy gateway <i>ip-prefix-name</i> import
取消对接收的指定地址发布的路由信息进行过滤	undo filter-policy gateway <i>ip-prefix-name</i> import
配置对接收的全局路由信息进行过滤	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> [gateway] } import
取消对接收的全局路由信息进行过滤	undo filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> [gateway] } import

filter-policy import 是对接收到的本路由协议（由所在的协议视图决定）的路由进行过滤，并阻止其将路由信息加入到路由表中。当在一个进行路由导入的路由器上使用此命令时，它不能用来阻止从其它路由协议引入的路由，因为在这之前此路由条目已经出现在路由表中。

对于链路状态协议来说，它只能阻止将路由条目加入到路由表中，无法对 LSA 进行过滤，所以相关的 LSA 还会被通告到邻居。

RIP 和 BGP 协议是对邻居发来的路由表直接过滤。

3. 引入其它路由协议发现的路由信息

路由协议可以引入其它路由协议发现的路由来丰富自己的路由知识。在引入其它协议路由信息时，可以通过 **Route-policy** 来进行路由信息的过滤，实现有选择的引入。进行引入操作的目标路由协议如果不能直接引用原路由协议的路由权值，需要为引入的路由指定一个路由权以满足本协议的要求。

请在路由协议视图下进行下列配置。

表6-3 引入其它协议路由

操作	命令
设置引入其它协议的路由	import-route <i>protocol</i> [med <i>med</i> cost <i>cost</i>] [tag <i>value</i>] [type { 1 2 }]
取消引入其它协议的路由的设置	undo import-route <i>protocol</i>

缺省情况下，不引入其它协议的路由信息。

说明：

在不同的路由协议视图下，可选的参数也有所区别，具体情况请分别参考手册中相应路由协议的 **import-route** 命令。

4. 配置对发布的路由进行过滤

定义一条有关路由发布的策略规则，通过对一个 ACL 或地址前缀列表的引用实现在路由发布的过程中过滤不满足条件的路由信息，通过指定 *routing-process* 实现仅过滤发布的 *routing-process* 的路由信息。

请在路由协议视图下进行下列配置。

表6-4 配置对发布路由的过滤

操作	命令
配置对发布路由的过滤	filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } export [<i>routing-process</i>]
取消对发布路由的过滤	undo filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } export [<i>routing-process</i>]

filter-policy export 对于 OSPF 来说，是对引入的路由进行过滤，要与 **import-route** 命令结合使用，否则失效。当指定 *routing-process* 时，可以对特定类型的引入路由信息进行过滤。如果没有指定，则对所有引入的路由进行过滤。

对 RIP 和 BGP 来说，即使没有 **import-route** 命令，它也会对路由表过滤，可以看作是对发布的路由进行过滤。

目前，路由策略支持将如下协议发现的路由接收到路由表中：

- **direct**: 本机接口直接相连的网段（或主机）路由。
- **static**: 静态配置的路由。
- **rip**: RIP 发现的路由。
- **ospf**: OSPF 协议发现的路由。
- **ospf-ase**: OSPF 协议发现的外部路由。
- **ospf-nssa**: OSPF 协议发现的 NSSA 区域路由。

- **bgp**: BGP 获得的路由。
- 缺省情况下，不对接收与发布的路由进行过滤。

6.2.2 通过 Route-policy 实现路由策略

1. 定义 Route-policy

一个 **Route-policy** 可由多个节点构成，每个节点是进行匹配检查的一个单元，节点间依据顺序号 *sequence-number* 标识检查顺序。

请在系统视图下进行下列配置。

表6-5 定义 Route-policy

操作	命令
进入路由策略视图	route-policy <i>route-policy-name</i> { permit deny } node <i>node-number</i>
删除指定的 Route-policy	undo route-policy <i>route-policy-name</i> [permit deny node <i>node-number</i>]

permit 指定所定义的 **Route-policy** 节点的匹配模式为允许模式。当路由项满足该节点的所有 **if-match** 子句时，认为通过该节点的过滤，并执行该节点的 **apply** 子句，不进入下一个节点的测试；如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。

deny 指定所定义的 **Route-policy** 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** 子句时被拒绝通过该节点，不进入下一个节点的测试；如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。

不同节点间是“或”的关系，即防火墙依次检查 **Route-policy** 的各个节点，通过 **Route-policy** 的某一节点，就意味着通过该 **Route-policy** 过滤。

缺省情况下，未定义 **Route-policy**。

需要注意的是：如果定义了一个以上的 **Route-policy** 节点，**Route-policy** 的各个节点中至少应该有一个节点的匹配模式是 **permit**。当一个 **Route-policy** 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 **Route-policy**。当 **Route-policy** 的所有节点都是 **deny** 模式时，所有路由信息都不会通过该 **Route-policy**。

2. 定义 Route-policy 的 if-match 子句

if-match 子句定义匹配准则，也就是路由信息通过当前 **Route-policy** 所需满足的过滤条件，匹配对象是路由信息的一些属性。

请在路由策略视图下进行下列配置。

表6-6 定义匹配条件

操作	命令
匹配 BGP 路由信息的 AS 路径域	if-match as-path <i>aspath-acl-number</i>
取消匹配 BGP 路由信息的 AS 路径域	undo if-match as-path
匹配 BGP 路由信息的团体属性	if-match community { <i>standard-community-number</i> [whole-match] <i>extended-community-number</i> }
取消匹配 BGP 路由团体属性	undo if-match community
匹配路由信息的目的地址	if-match { acl <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> }
取消匹配路由信息的目的地址	undo if-match { acl ip-prefix }
匹配路由信息下一跳接口	if-match interface <i>interface-type number</i>
取消匹配路由信息下一跳接口	undo if-match interface
匹配路由信息的下一跳	if-match ip next-hop { acl <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> }
取消匹配路由信息的下一跳	undo if-match ip next-hop [ip-prefix]
匹配路由信息的路由权值	if-match cost <i>value</i>
取消匹配路由信息的路由权值	undo if-match cost
匹配 OSPF 路由信息的标记域	if-match tag <i>value</i>
取消匹配 OSPF 路由的标记域	undo if-match tag

缺省情况下，不进行任何匹配。

需要注意：

- (1) 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 **match** 才算满足节点的匹配，可以执行 **apply** 子句的动作。
- (2) 如不指定 **if-match** 子句，则所有路由信息都会通过该节点的过滤。

3. 定义 Route-policy 的 apply 子句

apply 子句指定动作，也就是在满足由 **if-match** 子句指定的过滤条件后所执行的一些配置命令，对路由的一些属性进行修改。

请在路由策略视图下进行下列配置。

表6-7 定义 apply 子句

操作	命令
在 BGP 路由信息的 as-path 系列前加入指定的 AS 号	apply as-path <i>as-number-1</i> [<i>as-number-2</i> [<i>as-number-3</i> ...]]
取消在 BGP 路由信息的 as-path 系列前加入指定的 AS 号的设置	undo apply as-path
在 BGP 路由信息中设置团体属性	apply community { { <i>aa:nn</i> no-export-subconfed no-advertise no-export } [additive] additive none }
取消所设置的 BGP 路由信息中的团体属性	undo apply community
设置 BGP 路由信息的本地优先级	apply local-preference <i>localpref</i>
取消 BGP 路由信息的本地优先级	undo apply local-preference
设置路由信息的路由权值	apply cost <i>value</i>
取消路由信息的路由权值	undo apply cost
设置路由信息的路由权类型	apply cost-type [internal external]
取消路由信息的路由权类型	undo apply cost-type
设置 BGP 路由信息的路由源	apply origin { igp egp <i>as-number</i> incomplete }
取消 BGP 路由信息的路由源	undo apply origin
设置 OSPF 路由信息的标记域	apply tag <i>value</i>
取消 OSPF 路由信息的标记域	undo apply tag

缺省情况下，不进行任何设置。

请注意：如果满足 Route-policy 中指定的匹配条件，并且在向 EBGp 同伴通告 IGP 路由时通告了 **apply cost-type internal** 配置的 MED 值，那么该值将作为 IGP 路由的 MED 值。用 **apply cost-type internal** 所配置的优先级低于 **apply cost** 命令，高于 **default med** 命令。

4. 应用 Route-policy

请在路由协议视图下进行下列配置。

表6-8 引入其它协议路由

操作	命令
设置引入其它协议的路由	import-route <i>protocol</i> [med <i>med</i> cost <i>cost</i>] [tag <i>value</i>] [type { 1 2 }] route-policy <i>route-policy-name</i>
取消引入其它协议的路由的设置	undo import-route <i>protocol</i>

缺省情况下，不引入其它协议的路由信息。

说明：

在不同的路由协议视图下，可选的参数也有所区别，具体情况请分别参考手册中相应路由协议的 **import-route** 命令。

对于 BGP，还可以通过配置对等体组的 Route-policy 策略控制从对等体（组）收到的路由或向对等体组通告的路由。对等体组的成员不能配置不同于对等体组的出方向路由更新策略，但可以配置不同的入口策略。

表6-9 配置对等体的 Route-policy 策略

操作	命令
配置对等体的 Route-policy 策略	peer { <i>group-name</i> <i>peer-address</i> } route-policy <i>route-policy-name</i> import
取消对等体的 Route-policy 策略	undo peer { <i>group-name</i> <i>peer-address</i> } route-policy <i>policy-name</i> import

6.3 IP 路由策略显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示路由策略的配置情况，用户可以通过查看显示信息验证配置的效果。

表6-10 路由策略显示和调试

操作	命令
查看 Route-policy	display route-policy [<i>route-policy-name</i>]
查看 BGP 中 AS 过滤的路径信息	display ip as-path-acl [<i>aspath-acl-number</i>]
查看地址前缀列表信息	display ip ip-prefix [<i>ip-prefix-name</i>]

6.4 路由策略典型配置举例

6.4.1 配置引入其它协议的路由信息

1. 组网需求

本例说明了一种 OSPF 协议有选择地引入 RIP 协议路由的情况。

防火墙连接了一所大学的校园网和一个地区性网络。校园网使用 RIP 作为其内部路由协议，地区性网络使用 OSPF 路由协议，防火墙需要将校园网中的某些路由信息在地区性网络中发布。为实现这一功能，防火墙上的 OSPF 协议在引入 RIP 协议路

由信息时通过对一个路由策略的引用实现路由过滤的功能。该路由策略由两个节点组成，实现 192.1.0.0/24 和 128.2.0.0/16 的路由信息以不同的路由权值被 OSPF 协议发布。

2. 组网图

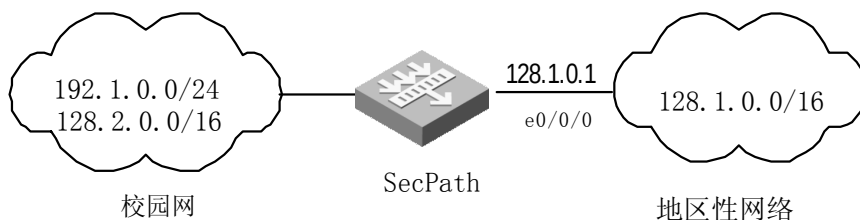


图6-1 配置 OSPF 引入 RIP 协议路由的组网图

3. 配置步骤

定义地址前缀列表。

```
[H3C] ip ip-prefix p1 permit 192.1.0.0 24
[H3C] ip ip-prefix p2 permit 128.2.0.0 16
```

配置路由策略。

```
[H3C] route-policy r1 permit node 10
[H3C-route-policy] if-match ip-prefix p1
[H3C-route-policy] apply cost 120
[H3C-route-policy] quit
[H3C] route-policy r1 permit node 20
[H3C-route-policy] if-match ip-prefix p2
[H3C-route-policy] apply cost 100
[H3C-route-policy] quit
```

配置 OSPF 协议（若要使 OSPF 成功引入 RIP 路由，还需在安全网关上对 RIP 进行相应配置，RIP 配置略）。

```
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 128.1.0.0 0.0.0.255
[H3C-ospf-1-area-0.0.0.0] quit
[H3C-ospf-1] import-route rip route-policy r1
[H3C-ospf-1] interface ethernet 0/0/0
[H3C-Ethernet0/0/0] ip address 128.1.0.1 255.255.255.0
```

6.4.2 配置过滤发布的路由信息

1. 组网需求

本例说明了 RIP 协议有选择地发布路由信息的情况。

防火墙连接了校园网 A 和校园网 B，它们都使用 RIP 作为内部路由协议，防火墙仅将校园网 A 中的 192.1.1.0/24 和 192.1.2.0/24 两个网段的路由发布到校园网 B 中去。为实现这一功能，防火墙上的 RIP 协议使用一条 **filter-policy** 命令过滤发布的路由信息，通过对一个地址前缀列表的引用来实现对发布路由进行过滤的功能。

2. 组网图

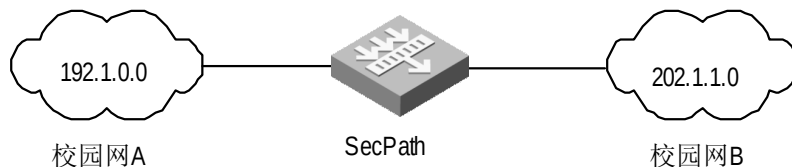


图6-2 配置过滤发布路由信息的组网图

3. 配置步骤

配置地址前缀列表。

```
[H3C] ip ip-prefix p1 permit 192.1.1.0 24
```

```
[H3C] ip ip-prefix p1 permit 192.1.2.0 24
```

配置 RIP 协议。

```
[H3C] rip
```

```
[H3C-rip] network 192.1.0.0
```

```
[H3C-rip] network 202.1.1.0
```

```
[H3C-rip] filter-policy ip-prefix p1 export
```

6.4.3 配置过滤接收的路由信息

1. 组网需求

- SecPathA 与 SecPathB 通信，都运行 OSPF 协议。
- 对 SecPathA 上的 OSPF 路由进程进行配置，引入三条静态路由。
- 通过在 SecPathB 上配置路由过滤规则，使接收到的三条静态路由部分可见，部分被屏蔽掉——20.0.0.0 和 40.0.0.0 网段的路由是可见的，30.0.0.0 网段的路由则被屏蔽。

2. 组网图

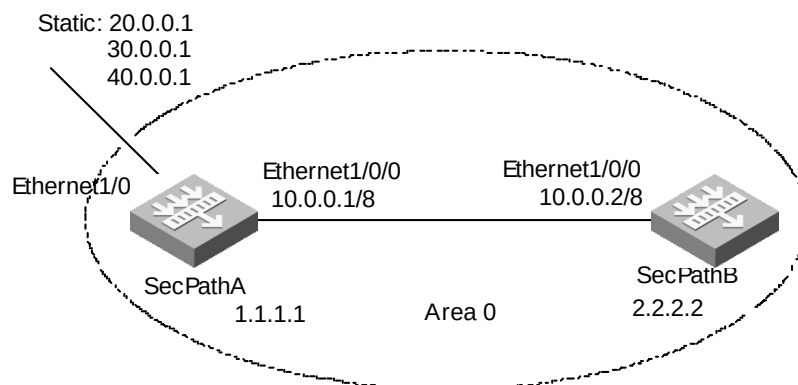


图6-3 过滤接收的路由信息组网图

3. 配置步骤

(1) 配置 SecPathA:

配置接口 Ethernet1/0/0 的 IP 地址。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 10.0.0.1 255.0.0.0
[H3C-Ethernet1/0/0] quit
```

配置三条静态路由。

```
[H3C] ip route-static 20.0.0.1 32 ethernet 1/0/1
[H3C] ip route-static 30.0.0.1 32 ethernet 1/0/1
[H3C] ip route-static 40.0.0.1 32 ethernet 1/0/1
```

启动 OSPF 协议，指定该接口所属区域号。

```
[H3C] router id 1.1.1.1
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 10.0.0.0 0.0.0.255
```

引入静态路由。

```
[H3C-ospf-1] import-route static
```

(2) 配置 SecPathB:

配置接口 Ethernet1/0/0 的 IP 地址。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 10.0.0.2 255.0.0.0
[H3C-Ethernet1/0/0] quit
```

配置访问控制列表。

```
[H3C] acl number 2001
```

```
[H3C-acl-basic-2001] rule deny source 30.0.0.0 0.255.255.255
```

```
[H3C-acl-basic-2001] rule permit source any
```

启动 OSPF 协议，指定该接口所属区域号。

```
[H3C] router id 2.2.2.2
```

```
[H3C] ospf
```

```
[H3C-ospf-1] area 0
```

```
[H3C-ospf-1-area-0.0.0.0] network 10.0.0.0 0.0.0.255
```

配置 OSPF 对接收的外部路由进行过滤。

```
[H3C-ospf-1] filter-policy 2001 import
```

6.4.4 通过配置 BGP 的 cost 属性来选择路径

1. 组网需求

本例说明怎样通过 BGP 属性的使用来管理路由选择。

所有路由器都配置 BGP，AS200 中的 IGP 使用 OSPF。

SecPathA 在 AS100 中，SecPathB、SecPathC 和 SecPathD 在 AS200 中。SecPathA 与 SecPathB 和 SecPathC 之间运行 EBGP。SecPathB 和 SecPathC 与 SecPathD 之间运行 IBGP。

2. 组网图

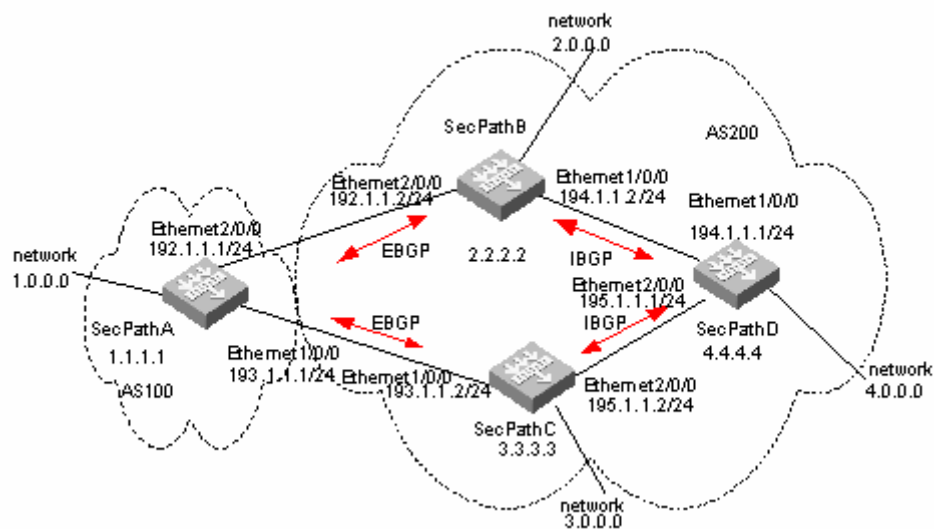


图6-4 配置 BGP 路径选择的组网图

3. 配置步骤

配置 SecPathA:

```
[H3C] interface ethernet 2/0/0
```

```
[H3C-Ethernet2/0/0] ip address 192.1.1.1 255.255.255.0
[H3C-Ethernet2/0/0] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 193.1.1.1 255.255.255.0
[H3C-Ethernet1/0/0] quit
[H3C] bgp 100
[H3C-bgp] network 1.0.0.0
[H3C-bgp] group ex192 external
[H3C-bgp] peer 192.1.1.2 group ex192 as-number 200
[H3C-bgp] group ex193 external
[H3C-bgp] peer 193.1.1.2 group ex193 as-number 200
[H3C-bgp] quit

# 配置 SecPathA 的 MED 属性

# 增加访问列表到 SecPathA 上，允许网络 1.0.0.0

[H3C] acl number 2001
[H3C-acl-basic-2001] rule permit source 1.0.0.0 0.255.255.255

# 定义两个 Route-policy，一个名为 apply_med_50，另一个名为 apply_med_100，
第一个 Route-policy 为网络 1.0.0.0 设置的 MED 属性为 50，第二个 Route-policy
设置的 MED 属性为 100。

[H3C] route-policy apply_med_50 permit node 10
[H3C-route-policy] if-match acl 2001
[H3C-route-policy] apply cost 50
[H3C-route-policy] quit
[H3C] route-policy apply_med_100 permit node 10
[H3C-route-policy] if-match acl 2001
[H3C-route-policy] apply cost 100
[H3C-route-policy] quit

# 应用 apply_med_50 到邻居 SecPathC（193.1.1.2）出口路由更新上，应用
apply_med_100 到邻居 SecPathB（192.1.1.2）的出口路由更新上。

[H3C] bgp 100
[H3C-bgp] peer ex193 route-policy apply_med_50 export
[H3C-bgp] peer ex192 route-policy apply_med_100 export

# 配置路由器 SecPathB:

[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 192.1.1.2 255.255.255.0
[H3C-Ethernet2/0/0] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 194.1.1.2 255.255.255.0
[H3C-Ethernet1/0/0] quit
[H3C] ospf
[H3C-ospf-1] import-route bgp
[H3C-ospf-1] area 0
```

```
[H3C-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[H3C-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[H3C] bgp 200
[H3C-bgp] undo synchronization
[H3C-bgp] group ex external
[H3C-bgp] peer 192.1.1.1 group ex as-number 100
[H3C-bgp] group in internal
[H3C-bgp] peer 194.1.1.1 group in
[H3C-bgp] import-route ospf
```

配置 SecPathC:

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 193.1.1.2 255.255.255.0
[H3C-Ethernet1/0/0] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 195.1.1.2 255.255.255.0
[H3C-Ethernet2/0/0] quit
[H3C] ospf
[H3C-ospf-1] import-route bgp
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 193.1.1.0 0.0.0.255
[H3C-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[H3C] bgp 200
[H3C-bgp] group ex external
[H3C-bgp] peer 193.1.1.1 group ex as-number 100
[H3C-bgp] group in internal
[H3C-bgp] peer 195.1.1.1 group in
[H3C-bgp] import-route ospf
```

配置 SecPathD:

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 194.1.1.1 255.255.255.0
[H3C-Ethernet1/0/0] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 195.1.1.1 255.255.255.0
[H3C-Ethernet2/0/0] quit
[H3C] ospf
[H3C-ospf-1] import-route bgp
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[H3C-osp-1f-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[H3C-ospf-1-area-0.0.0.0] network 4.0.0.0 0.255.255.255
[H3C] bgp 200
[H3C-bgp] group in internal
[H3C-bgp] peer 195.1.1.2 group in as-number 200
[H3C-bgp] peer 194.1.1.2 group in as-number 200
```

```
[H3C-bgp] import-route ospf
```

为使配置生效，需要使用 **reset bgp all** 命令复位所有的 BGP 邻居。

通过上述配置后，由于 SecPathC 学到的路由 1.0.0.0 的 MED 属性比 SecPathB 学到的更小，SecPathD 优选来自 SecPathC 的路由 1.0.0.0。

如果在配置 SecPathA 时，不配置 SecPathA 的 MED 属性，而在 SecPathC 上配置本地优先级如下：

在 SecPathC 上加上访问列表 2001，允许网络 1.0.0.0

```
[H3C] acl number 2001
```

```
[H3C-acl-basic-2001] rule permit source 1.0.0.0 0.255.255.255
```

定义名为 localpref 的路由策略，设置匹配 acl 2001 的路由的本地优先级为 200，不匹配的为 100。

```
[H3C] route-policy localpref permit node 10
```

```
[H3C-route-policy] if-match acl 2001
```

```
[H3C-route-policy] apply local-preference 200
```

```
[H3C-route-policy] route-policy localpref permit node 20
```

```
[H3C-route-policy] apply local-preference 100
```

```
[H3C] quit
```

应用此路由策略到来自 BGP 邻居 193.1.1.1（SecPathA）的路由信息上。

```
[H3C] bgp 200
```

```
[H3C-bgp] peer 193.1.1.1 route-policy localpref import
```

此时，由于 SecPathC 学到的路由 1.0.0.0 的 Local preference 属性值为 200，比 SecPathB 学到的路由 1.0.0.0 的 Local preference 属性值（SecPathB 没有配置 Local preference 属性，默认为 100）更大，SecPathD 依然优选来自 SecPathC 的路由 1.0.0.0。

6.4.5 基于 BGP next-hop/as-path/origin/local-preference 属性的路由策略配置举例

1. 组网需求

SecPathA 和 SecPathB 在 AS300，SecPathD 在 AS100，SecPathC 在 AS200。配置 SecPathA 与 D、SecPathB 与 C、SecPathC 与 D 均为 EBGP peer。SecPathA 与 B 为 IBGP peer；SecPathA 与 B 间的 IGP 协议为 RIP。

2. 组网图

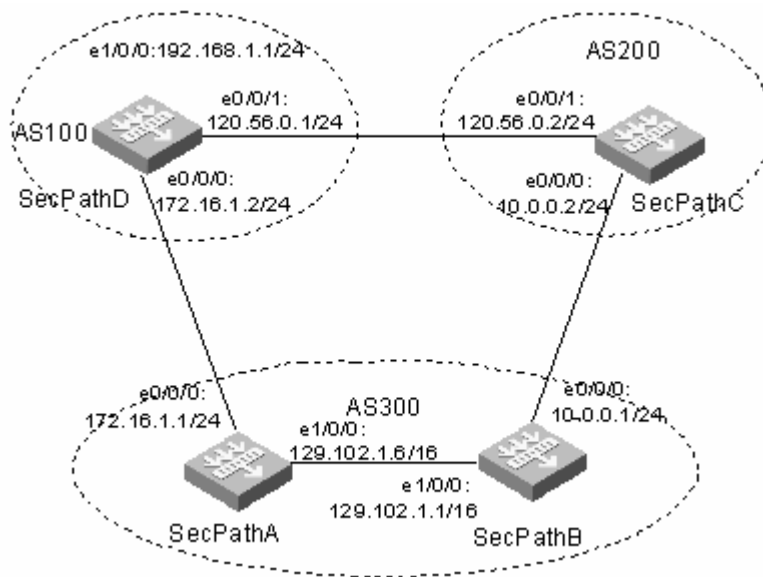


图6-5 基于 BGP next-hop/as-path/origin/local-preference 属性的路由策略配置举例

3. 配置步骤

(1) 配置 SecPathA:

配置接口 IP 地址。

```
[H3C] interface ethernet 0/0/0
[H3C-Ethernet0/0/0] ip address 172.16.1.1 255.255.255.0
[H3C-Ethernet0/0/0] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 129.102.1.6 255.255.0.0
[H3C-Ethernet1/0/0] quit
```

配置 RIP 协议。

```
[H3C] rip
[H3C-rip] network 129.102.0.0
[H3C-rip] quit
```

配置 BGP 内部邻居和外部邻居。

```
[H3C] bgp 300
[H3C-bgp] undo synchronization
[H3C-bgp] import-route rip
[H3C-bgp] group ex100 external
[H3C-bgp] peer 172.16.1.2 group ex100 as-number 100
[H3C-bgp] group in300 internal
[H3C-bgp] peer 129.102.1.1 group in300
```

(2) 配置 SecPathB:

```
[H3C] interface ethernet 0/0/0
```

```
[H3C-Ethernet0/0/0] ip address 10.0.0.1 255.255.255.0
[H3C-Ethernet0/0/0] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 129.102.1.1 255.255.0.0
[H3C-Ethernet1/0/0] quit
[H3C] rip
[H3C-rip] network 129.102.0.0
[H3C-rip] quit
[H3C] bgp 300
[H3C-bgp] import-route rip
[H3C-bgp] undo synchronization
[H3C-bgp] group in300 internal
[H3C-bgp] peer 129.102.1.6 group in300
[H3C-bgp] group ex200 external
[H3C-bgp] peer 10.0.0.2 group ex200 as-number 200
```

(3) 配置 SecPathC:

```
[H3C] interface ethernet 0/0/0
[H3C-Ethernet0/0/0] ip address 10.0.0.2 255.255.255.0
[H3C-Ethernet0/0/0] interface ethernet 0/0/1
[H3C-Ethernet0/0/1] ip address 120.56.0.2 255.255.255.0
[H3C-Ethernet0/0/1] quit
[H3C] bgp 200
[H3C-bgp] group ex100 external
[H3C-bgp] peer 120.56.0.1 group ex100 as-number 100
[H3C-bgp] group ex300 external
[H3C-bgp] peer 10.0.0.1 group ex300 as-number 300
```

(4) 配置 SecPathD:

```
[H3C] interface ethernet 0/0/0
[H3C-Ethernet0/0/0] ip address 172.16.1.2 255.255.255.0
[H3C-Ethernet0/0/0] interface ethernet 0/0/1
[H3C-Ethernet0/0/1] ip address 120.56.0.1 255.255.255.0
[H3C-Ethernet0/0/1] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 192.168.1.1 255.255.255.0
[H3C-Ethernet1/0/0] quit
[H3C] bgp 100
[H3C-bgp] network 192.168.1.0
[H3C-bgp] group ex300 external
[H3C-bgp] peer 172.16.1.1 group ex300 as-number 300
[H3C-bgp] group ex200 external
[H3C-bgp] peer 120.56.0.2 group ex200 as-number 200
[H3C-bgp] quit
[H3C] quit
```

完成上面配置在 SecPathA 和 SecPathB 上执行 **display bgp routing**，可以看到 192.168.1.0 的路由下一跳为 172.16.1.2，Origin 属性为 igp。

- 如在 SecPathD 上增加 as-path

```
[H3C] bgp 100
[H3C-bgp] peer ex300 route-policy AS300 export
[H3C-bgp] quit
[H3C] route-policy AS300 permit node 10
[H3C-route-policy] if-match acl 2001
[H3C-route-policy] apply as-path 300
[H3C-route-policy] quit
[H3C] acl number 2001 match-order auto
[H3C-acl-basic-2001] rule permit source any
[H3C-acl-basic-2001] quit
[H3C] quit
```

观察到 192.168.1.0 的路由下一跳变为 10.0.0.2，as-path 为 200, 100，原来的到 AS300 的路由被过滤掉了。

- 如在 SecPathA 上指定下一跳地址

```
[H3C] bgp 300
[H3C-bgp] peer ex100 route-policy AS100 import
[H3C-bgp] quit
[H3C] route-policy AS100 permit node 10
[H3C-route-policy] if-match acl 2001
[H3C-route-policy] apply ip-address next-hop 10.0.0.2
[H3C-route-policy] quit
[H3C] acl number 2001
[H3C-acl-basic-2001] rule permit source 192.168.1.0 0.0.0.255
[H3C-acl-basic-2001] quit
[H3C] quit
```

观察到 192.168.1.0 的路由下一跳变为 10.0.0.2。

- 如在 SecPathD 上设置 Origin 属性

```
[H3C] bgp 100
[H3C-bgp] peer ex300 route-policy AS300 export
[H3C] quit
[H3C] route-policy AS300 permit node10
[H3C-route-policy] if-match acl 2001
[H3C-route-policy] apply origin Incomplete
[H3C-route-policy] quit
[H3C] acl number 2001 match-order auto
[H3C-acl-2001] rule permit source 192.168.1.0
[H3C-acl-2001] quit
```

```
[H3C] quit
```

此时 Origin 属性变为 Incomplete。

- 如在 SecPathB 上配置 local-preference 属性

```
[H3C] bgp 200
```

```
[H3C-bgp] peer ex200 route-policy AS200 export
```

```
[H3C-bgp] quit
```

```
[H3C] route-policy AS200 permit node10
```

```
[H3C-route-policy] if-match acl 2001
```

```
[H3C-route-policy] apply local-preference 150
```

```
[H3C-route-policy] quit
```

```
[H3C] acl number 2001 match-order auto
```

```
[H3C-acl-2001] rule permit ip destination 192.168.1.0
```

```
[H3C-acl-2001] quit
```

```
[H3C] quit
```

观察到 192.168.1.0 的路由下一跳变为 10.0.0.2。

6.5 路由策略故障诊断与排错

故障一：路由协议运行正常的情况下无法实现路由信息过滤。

故障排除：检查如下几种错误：

- Route-policy 的各个节点中至少应该有一个节点的匹配模式是 **permit** 模式。
当一个 Route-policy 用于路由信息过滤时，如果某路由信息没有通过任一节点的过滤，则认为该路由信息没有通过该 Route-policy 的过滤。当 Route-policy 的所有节点都是 **deny** 模式时，所有路由信息都不会通过该 Route-policy 的过滤。
- 地址前缀列表的各个表项中至少应该有一个表项的匹配模式是 **permit** 模式。
deny 模式的表项可以先被定义以快速的过滤掉不符合条件的路由信息，但如果所有表项都是 **deny** 模式，则任何路由都不会通过该地址前缀列表的过滤。
可以在定义了多条 **deny** 模式的表项后定义一条 **permit 0.0.0.0 0 less-equal 32** 的表项以允许其它所有路由信息通过（如果不指定 **less-equal 32** 将只匹配缺省路由）。

第7章 路由容量配置

7.1 路由容量配置简介

7.1.1 概述

在大型组网应用中，路由表中的路由数量往往非常大，尤其是 OSPF 路由和 BGP 路由。路由信息通常是存储在路由器的内存中，当路由表规模不断增大时，路由器的内存使用量也将不断增加。但路由器总的内存大小并不会改变（除非进行硬件升级，而升级也不能保证解决所有问题）。当设备内存被耗尽时，设备将不能正常工作。

为了解决这种矛盾，Comware 提供了一种对路由表规模进行控制的机制，通过监控系统当前空闲内存的大小，决定是否继续向路由表中增加新的路由以及是否保持路由协议的连接。

 说明：

需要注意的是，通常情况下使用系统的默认值就可以满足要求，不建议用户自行改变配置，以避免配置不当导致系统的稳定性和可用性降低。

7.1.2 防火墙实现的路由容量限制

造成路由表规模过于庞大的通常是 BGP 路由项和 OSPF 路由项，因此，防火墙的路由容量限制只对这两类路由有效，静态路由和其它动态路由协议不受影响。

当防火墙的空闲内存大小降低到设定的内存下限时，BGP 和 OSPF 连接将被断开，相应的路由项从路由表中删除，从而释放占用的内存。系统定期检查空闲内存的大小，当发现空闲内存恢复到安全值后，再重新恢复 BGP 和 OSPF 连接。

7.2 路由容量配置

路由容量配置包括：

- 设置/恢复防火墙内存的下限与安全值
- 禁止防火墙自动恢复断开的路由协议
- 使能防火墙自动恢复断开的路由协议

7.2.1 配置防火墙内存的下限与安全值

当防火墙的空闲内存大小等于或低于下限值时，BGP 和 OSPF 连接将被断开。

当防火墙中的空闲内存大小降低到安全值，但还没有到达下限值时，通过 **disply memory limit** 命令可以看到防火墙进入一种紧急状态（Exigent）。

如果使能了自动恢复功能，当防火墙中的空闲内存大小恢复到超过安全值时，断开的 BGP 和 OSPF 连接将重新建立。

请在系统视图下进行下列配置。

表7-1 设置防火墙内存的下限与安全值

操作	命令
设置防火墙内存的下限与安全值	memory { safety safety-value limit limit-value }*
将防火墙内存的下限与安全值恢复为缺省值	undo memory { safety limit }

safety-value 和 *limit-value* 的缺省值由内存大小决定。

 说明：

请注意，在配置时，*safety-value* 必须大于 *limit-value*。

7.2.2 禁止防火墙的自动恢复连接功能

如果禁止了自动恢复功能，则即使空闲内存已经超过了安全值，断开的 BGP 和 OSPF 连接也不会恢复，因此，请不要轻易使用该功能。

请在系统视图下进行下列配置。

表7-2 禁止防火墙的自动恢复连接功能

操作	命令
禁止自动恢复功能	memory auto-establish disable

缺省情况下，使能防火墙的自动恢复功能。

7.2.3 使能防火墙的自动恢复连接功能

请在系统视图下进行下列配置。

表7-3 使能防火墙的自动恢复连接功能

操作	命令
使能防火墙的自动恢复功能	memory auto-establish enable

缺省情况下，使能防火墙的自动恢复功能。

7.3 路由容量显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后的路由容量信息，用户可以通过查看显示信息验证配置的效果。

表7-4 路由容量显示和调试

操作	命令
查看路由容量相关的内存设置和状态信息	display memory [limit]

目 录

第 1 章 MPLS体系结构	1-1
1.1 MPLS概述	1-1
1.2 基本概念	1-1
1.2.1 转发等价类（FEC）	1-1
1.2.2 标签	1-1
1.2.3 标签分发协议（LDP）	1-4
1.3 MPLS体系结构	1-4
1.3.1 MPLS网络结构	1-4
1.3.2 LSP的建立	1-4
1.3.3 LSP隧道与分层	1-5
1.3.4 标签报文的转发	1-5
1.4 LDP协议介绍	1-6
1.4.1 LDP基本概念	1-6
1.4.2 LDP工作过程	1-7
1.4.3 LDP基本操作	1-8
1.4.4 LDP环路检测	1-10
1.4.5 基于约束路由的LDP	1-10
1.5 MPLS与其他协议间的关系	1-10
1.5.1 MPLS与路由协议的关系	1-10
1.5.2 RSVP对MPLS的扩展	1-10
1.6 MPLS应用	1-11
1.6.1 基于MPLS的VPN	1-11
1.6.2 基于MPLS的流量工程	1-12
1.6.3 基于MPLS的QoS	1-12
第 2 章 MPLS配置	2-1
2.1 MPLS配置概述	2-1
2.2 MPLS基本配置	2-1
2.2.1 配置MPLS LSR ID	2-2
2.2.2 进入MPLS视图	2-2
2.2.3 配置拓扑驱动建立LSP的建立策略	2-2
2.2.4 配置静态LSP	2-3
2.2.5 配置MPLS的IP TTL复制功能	2-3
2.2.6 配置MPLS使用IP路由返回ICMP响应报文	2-4
2.3 LDP协议配置	2-5
2.3.1 使能LDP协议	2-5
2.3.2 在接口上使能LDP协议	2-6

2.3.3 配置LDP扩展发现模式	2-6
2.3.4 配置会话参数	2-7
2.3.5 配置远程LDP对等体会话参数.....	2-8
2.3.6 配置环路检测	2-8
2.3.7 配置LDP验证方式	2-9
2.4 MPLS的显示与调试.....	2-10
2.4.1 MPLS的显示与调试	2-10
2.4.2 LDP协议的显示与调试	2-12
2.5 MPLS典型配置举例.....	2-13
2.6 MPLS配置的故障排除	2-16

第1章 MPLS 体系结构

1.1 MPLS 概述

MPLS（Multiprotocol Label Switching）是多协议标签交换的简称，它用短而定长的标签来封装网络层分组。MPLS 从各种链路层（如 PPP、ATM、帧中继、以太网等）得到链路层服务，又为网络层提供面向连接的服务。MPLS 能从 IP 路由协议和控制协议中得到支持，同时，还支持基于策略的约束路由，它路由功能强大、灵活，可以满足各种新应用对网络的要求。这种技术起源于 IPv4，但其核心技术可扩展到多种网络协议（IPv6、IPX 等）。

MPLS 最初是为提高路由器的转发速度而提出一个协议，但是，它的用途已不仅仅局限于此，而是广泛地应用于流量工程（Traffic Engineering）、VPN、QoS 等方面，从而日益成为大规模 IP 网络的重要标准。

1.2 基本概念

1.2.1 转发等价类（FEC）

FEC（Forwarding Equivalence Class）是 MPLS 中的一个重要概念。MPLS 实际上是一种分类转发技术，它将具有相同转发处理方式（目的地相同、使用转发路径相同、具有相同的服务等级等）的分组归为一类，称为转发等价类。一般来说，划分分组的 FEC 是根据他的网络层目的地址。属于相同转发等价类的分组在 MPLS 网络中将获得完全相同的处理。

1.2.2 标签

1. 标签的定义

标签为一个长度固定、具有本地意义的短标识符，用于标识一个 FEC（Forwarding Equivalence Class）。当分组到达 MPLS 网络入口时，它将按一定规则被划归不同的 FEC，根据分组所属的 FEC，将相应的标签封装在分组中，这样，在网络中，按标签进行分组转发即可。

2. 标签的结构

标签的结构如 图 1-1所示。

Label	Exp	S	TTL

图1-1 标签的结构

标签位于链路层包头和网络层分组之间，长度为 4 个字节。标签共有 4 个域：

Label: 标签值字段，长度为 20bits，用于转发的指针。

Exp: 3bits，保留，协议中没有明确规定，通常用于 COS。

S: 1bit，MPLS 支持标签的分层结构，即多重标签。值为 1 时表明为最底层标签。

TTL: 8bits，和 IP 分组中的 TTL 意义相同。

3. 标签的操作

(1) 标签映射

标签映射分为两种，一种是入口路由器处的标签映射，另一种是 MPLS 域内的标签映射。

入口路由器处的标签映射为 ingress LSR 依据一定的原则对输入分组进行划分，得到多个 FEC，接着将有关标签与这些 FEC 进行映射，并记录在相应的数据库 LIB（Label Information Base）中。简单地说，就是将一个标签指派给 FEC，就称为“标签映射”。

MPLS 域内的标签映射又称为输入标签映射 ILM（Incoming Label Map），即将每个输入标签映射到一系列 NHLFE（Next Hop Label Forwarding Entry）上，然后，根据映射结果，将分组沿各通路进行转发。

(2) 标签的封装

标签在各种介质中的封装如下图所示：

以太网 /SONET /SDH分组	以太网报头 /PPP报头	标签	三层数据
帧模式 ATM分组	ATM报头	标签	三层数据
信元模式的 ATM分组	VPI/VCI		三层数据

图1-2 标签在分组中的封装位置

对于以太网、PPP 的分组，标签堆栈象“垫层”一样，位于二层报头与数据之间，对于 ATM 信元模式的分组，借用 VPI/VCI 来作为标签使用。

(3) 标签分配和分发

标签分发是为某 FEC 建立相应标签交换路径 LSP 的过程。

在 MPLS 体系中，将特定标签分配给特定 FEC（即标签绑定）的决定由下游 LSR 作出，下游 LSR 随后通知上游 LSR。即标签由下游指定，分配的标签按照从下游到上游的方向分发。

MPLS 中使用的标签分发方式有两种：下游自主标签分发方式（DU，Downstream Unsolicited）和下游按需标签分发方式（DoD，Downstream On Demand）。

- 对于一个特定的 FEC，LSR 无须从上游获得标签请求消息即进行标签分配与分发的方式，称为下游自主标签分配。
- 对于一个特定的 FEC，LSR 获得标签请求消息之后才进行标签分配与分发的方式，称为下游按需标签分配。

具有标签分发邻接关系的上游 LSR 和下游 LSR 之间，必须对使用哪种标签分发方式达成一致。

LSR 将标签分发给其对等体时，可以采用 LDP 消息进行传送，也可以将标签搭载在其他路由协议消息上。

说明：

上游和下游是相对而言的，对于一个报文转发过程来说，发送方的路由器是上游 LSR，接收方是下游 LSR。

(4) 标签分配控制方式

标签分配控制方式分为两种：独立（Independent）标签分配控制方式和有序（ordered）标签分配控制方式。

当使用独立标签分配控制方式时，每个 LSR 可以在任意时间向和它连接的 LSR 通告标签映射。

当使用有序标签分配控制方式时，只有当 LSR 收到某一特定 FEC 下一跳的特定标签映射消息或者 LSR 是 LSP 的出口节点时，LSR 才可以向上游发送标签映射消息。

(5) 标签保持方式

标签保持方式分为两种：自由标签保持方式和保守标签保持方式。

假设两台路由器 Ru，Rd，对于特定的一个 FEC，如果 LSR Ru 收到了来自 LSR Rd 的标签绑定，当 Rd 不是 Ru 的下一跳时，如果 Ru 保存该绑定，则称 Ru 使用的是自由标签保持方式；如果 Ru 丢弃该绑定，则称 Ru 使用的是保守标签保持方式。

当要求 LSR 能够迅速适应路由变化时，可使用自由标签保持方式；当要求 LSR 中保存较少的标签数量时，可使用保守标签保持方式。

1.2.3 标签分发协议（LDP）

标签分发协议 LDP（Label Distribution Protocol）是 MPLS 中的信令控制协议，是控制 LSR 之间交换标签与 FEC 绑定，协调 LSR 间工作的一系列规程。

1.3 MPLS 体系结构

1.3.1 MPLS 网络结构

MPLS 网络的基本构成单元是标签交换路由器 LSR（Label Switching Router），主要运行 MPLS 控制协议和第三层路由协议，并负责与其他 LSR 交换路由信息来建立路由表，实现 FEC 和 IP 分组头的映射，建立 FEC 和标签之间的绑定，分发标签绑定信息，建立和维护标签转发表等工作。

由 LSR 构成的网络叫做 MPLS 域，位于区域边缘的 LSR 称为边缘 LSR（LER，Labeled Edge Router），主要完成连接 MPLS 域和非 MPLS 域以及不同 MPLS 域的功能，并实现对业务的分类、分发标签（作为出口 LER）、剥去标签等。其中入口 LER 叫 Ingress，出口 LER 叫 Egress。

位于区域内部的 LSR 则称为核心 LSR，核心 LSR 可以是支持 MPLS 的路由器，也可以是支持 MPLS 标签交换的 LSR，它提供标签分发、交换功能（Label Swapping）。带标签的分组沿着由一系列 LSR 构成的标签交换路径 LSP（Label Switched Path）传送。

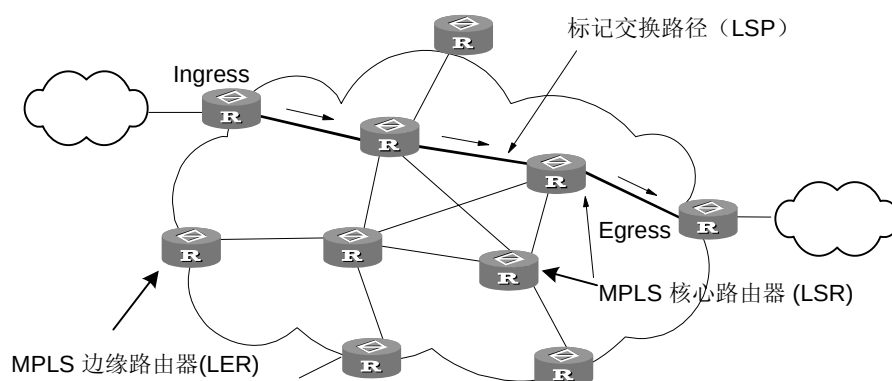


图1-3 MPLS 基本原理

1.3.2 LSP 的建立

LSP 的建立其实就是将 FEC 和标签进行绑定，并将这种绑定通告 LSP 上相邻 LSR 的过程。这个过程是通过标签分发协议 LDP 来实现的。LDP 规定了 LSR 间的消息交互过程和消息结构，以及路由选择方式。有关 LDP 的详细描述，请参见下一节。

1.3.3 LSP 隧道与分层

1. LSP 隧道

MPLS 支持 LSP 隧道技术。在一条 LSP 路径上，LSR Ru 和 LSR Rd 互为上下游，但 LSR Ru 和 LSR Rd 之间的路径，可能并不是路由协议所提供路径的一部分，MPLS 允许在 LSR Ru 和 LSR Rd 间建立一条新的 LSP 路径 $\langle Ru \ R1...Rn \ Rd \rangle$ ，LSR Ru 和 LSR Rd 分别为这条 LSP 的起点和终点。LSR Ru 和 LSR Rd 间的 LSP 就是 LSP 隧道，它避免了传统的网络层封装隧道。当隧道经由的路由和逐跳与从路由协议取得的路由一致时，这种隧道叫逐跳路由隧道；若不一致，则这种隧道叫显式路由隧道。

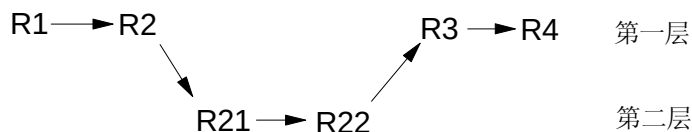


图1-4 LSP 隧道

在上图中，LSP $\langle R2 \ R21 \ R22 \ R3 \rangle$ 就是 R2、R3 间的一条隧道。

2. 多层标签栈

在 MPLS 中，分组可以携带多个标签，这些标签在分组中以“堆栈”的形式存在，对堆栈的操作按“后进先出”的原则，决定如何转发分组的标签始终是栈顶标签。标签入栈是指向输出分组中加入一个标签，使标签栈的深度加 1，同时，分组的当前标签就变为此新加入的标签；标签出栈是指从分组中去掉一个标签，使标签栈的深度减 1，同时，分组的当前标签将变为原来处于下一层的标签。

在 LSP 隧道中会使用多层标签栈。当分组在 LSP 隧道中传送时，分组的标签就会有多层。在每一隧道的入口和出口处，要进行标签栈的入栈和出栈操作，每发生一次入栈操作，标签就会增加一层。MPLS 对标签栈的深度没有限制。

标签栈按照“后进先出”方式组织标签，MPLS 从栈顶开始处理标签。

若一个分组的标签栈深度为 m ，则位于栈底的标签为 1 级标签，位于栈顶的标签为 m 级标签。未打标签的分组可看作标签栈为空（即标签栈深度为零）的分组。

1.3.4 标签报文的转发

在 Ingress，将进入网络的分组根据其特征划分成转发等价类 FEC。一般根据 IP 地址前缀或者主机地址来划分 FEC。属于相同 FEC 的分组在 MPLS 区域中将经过相同的路径（即 LSP）。LSR 对到来的 FEC 分组分配一个短而定长的标签，然后从相应的接口转发出去。

在 LSP 沿途的 LSR 上，都已建立了输入/输出标签的映射表（该表的元素叫下一跳标签转发条目，简称 NHLFE，Next Hop Label Forwarding Entry）。对于接收到的标签分组，LSR 只需根据标签从表中找到相应的 NHLFE，并用新的标签来替换

原来的标签, 然后, 对标签分组进行转发, 这个过程叫输入标签映射 ILM (Incoming Label Map)。

MPLS 在网络入口处指定特定分组的 FEC, 后续 P 路由器只需简单的转发即可, 比常规的网络层转发要简单得多, 转发速度得以提高。

 说明:

TTL 处理:

标签化分组时必须将原 IP 分组中的 TTL 值拷贝到标签中的 TTL 域。LSR 在转发标签化分组时, 要对栈顶标签的 TTL 域作减一操作。标签出栈时, 再将栈顶的 TTL 值拷贝回 IP 分组或下层标签。

但是, 当 LSP 穿越由 ATM-LSR 或 FR-LSR 构成的非 TTL LSP 段时, 域内的 LSR 无法处理 TTL 域。这时, 需要在进入非 TTL LSP 段时对 TTL 进行统一处理, 即一次性减去反映该非 TTL LSP 段长度的值。

1.4 LDP 协议介绍

LDP 协议规定标签分发过程中的各种消息以及相关的处理进程。

通过 LDP, LSR 可以把网络层的路由信息直接映射到数据链路层的交换路径上, 进而建立起网络层上的 LSP。LSP 既可以建立在两个相邻的 LSR 之间, 也可以终止于网络出口节点, 从而在网络中所有中间节点上都使用标签交换。

1.4.1 LDP 基本概念

1. LDP 对等体

LDP 对等体是指相互之间存在 LDP 会话、使用 LDP 来交换标签/FEC 映射关系的两个 LSR。

两个 LDP 对等体可以同时通过一个 LDP 会话获得对方的标签映射消息, 即, LDP 协议是双向的。

2. LDP 会话

LDP 会话用于在 LSR 之间交换标签映射、释放等消息。LDP 会话可以分为两种类型:

- 本地 LDP 会话 (Local LDP Session): 建立会话的两个 LSR 之间是直连的;
- 远端 LDP 会话 (Remote LDP Session): 建立会话的两个 LSR 之间是非直连的;

3. LDP 消息

LDP 协议主要使用四种消息:

- 发现（Discovery）消息：用于通告和维护网络中 LSR 的存在；
- 会话（Session）消息：用于建立、维护和终止 LDP 对等体之间的会话连接；
- 通告（Advertisement）消息：用于创建、改变和删除标记—FEC 绑定；
- 通知（Notification）消息：用于提供建议性的消息和差错通知。

4. 标签空间与 LDP 标识符

LDP 对等体之间分配标签的范围称为标签空间。可以为 LSR 的每个接口指定一个标签空间，也可以整个 LSR 使用一个标签空间。

LDP 标识符用于标识特定 LSR 的标签空间范围，是一个六字节的数值，格式如下：

<IP 地址>: <标签空间序号>

其中，四字节的 IP 地址是 LSR 的 IP 地址，标签空间序号占两字节。

1.4.2 LDP 工作过程

下图为 LDP 标签分发示意。

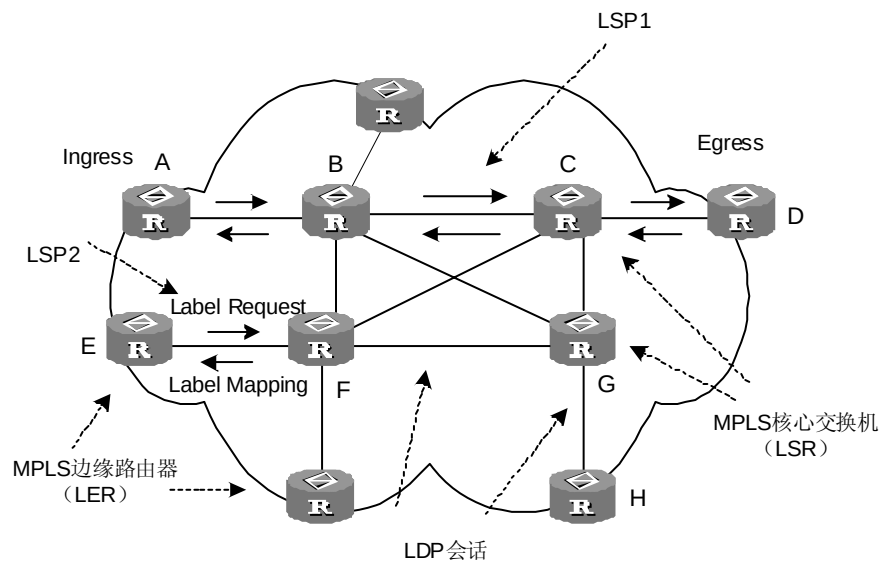


图1-5 标签分发过程

在一条 LSP 上，沿数据传送的方向，相邻的 LSR 分别称为上游 LSR 和下游 LSR。例如，在上图中的 LSP1，LSR B 为 LSR C 的上游 LSR。

标签的分发过程有下游按需标签分发 DoD 和下游自主标签分发 DU 两种模式，它们的主要区别在于标签映射的发布是上游请求还是下游主动发布。下面分别描述这两种模式的标签分发过程：

(1) DoD（downstream-on-demand）模式

上游 LSR 向下游 LSR 发送标签请求消息（包含 FEC 的描述信息），下游 LSR 为此 FEC 分配标签，并将绑定的标签通过标签映射消息反馈给上游 LSR。

下游 LSR 何时反馈标签映射消息，取决于该 LSR 采用独立标签控制方式还是有序标签控制方式。采用有序标签控制方式时，只有收到它的下游返回的标签映射消息后，才向其上游发送标签映射消息；采用独立标签控制方式时，不管有没有收到它的下游返回的标签映射消息，都立即向其上游发送标签映射消息。

上游 LSR 一般是根据其路由表中的信息来选择下游 LSR。在图 1-5 中，LSP1 沿途的 LSR 都采用有序标签控制方式，LSP2 上的 LSR F 则采用独立标签控制方式。

(2) DU (downstream unsolicited) 模式

下游 LSR 在 LDP 会话建立成功后，主动向其上游 LSR 发布标签映射消息。上游 LSR 保存标签映射信息，并根据路由表信息来处理收到的标签映射信息。

1.4.3 LDP 基本操作

按照先后顺序，LDP 的操作主要包括以下四个阶段：

- 发现阶段
- 会话建立与维护
- LSP 建立与维护
- 会话撤销

1. 发现阶段

在这一阶段，希望建立会话的 LSR 向相邻 LSR 周期性地发送 Hello 消息，通知相邻节点本地对等关系。通过这一过程，LSR 可以自动发现它的 LDP 对等体，而无需进行手工配置。

LDP 有两种发现机制：

- 基本发现机制

基本发现机制用于发现本地的 LDP 对等体，即通过链路层直接相连的 LSR，建立本地 LDP 会话。

这种方式下，LSR 向特定端口周期性发送 LDP 链路 hello 消息，并携带特定端口所属标签空间的 LDP 标识符以及其它相关信息。如果 LSR 在特定端口收到 LDP 链路 hello 消息，则表明可能存在一个可达的对等 LSR。通过 hello 消息携带的信息，LSR 还可获知在特定端口使用的标签空间。

- 扩展发现机制

扩展发现机制用于发现远端的 LDP 对等体，即不通过链路层直接相连的 LSR，建立远端 LDP 会话。

这种方式下，LSR 向某一特定 IP 地址周期地发送 LDP 目标 hello 消息 (targeted hello)。

LDP 目标 hello 消息以 UDP 分组的形式发往特定地址的知名 LDP 发现端口，LSR 发送的 LDP 目标消息带有 LSR 希望使用的标签空间和其它可选信息。

2. 会话建立与维护

对等关系建立之后，LSR 开始建立会话。这一过程又可分为两步：

- 首先建立传输层连接，即，在 LSR 之间建立 TCP 连接；
- 随后对 LSR 之间的会话进行初始化，协商会话中涉及的各种参数，如 LDP 版本、标签分发方式、定时器值、标签空间等。

3. LSP 建立与维护

LSP 的建立过程实际就是将 FEC 和标签进行绑定，并将这种绑定通告 LSP 上相邻 LSR。这个过程是通过 LDP 实现的，主要步骤如下：

- (1) 当网络的路由改变时，如果有一个边缘节点发现自己的路由表中出现了新的目的地地址，并且这一地址不属于任何现有的 FEC，则该边缘节点需要为这一目的地地址建立一个新的 FEC。边缘 LSR 决定该 FEC 将要使用的路由，向其下游 LSR 发起标签请求消息，并指明是要为哪个 FEC 分配标签；
- (2) 收到标签请求消息的下游 LSR 记录这一请求消息，根据本地的路由表找出对应该 FEC 的下一跳，继续向下游 LSR 发出标签请求消息；
- (3) 当标签请求消息到达目的节点或 MPLS 网络的出口节点时，如果这些节点尚有可供分配的标签，并且判定上述标签请求消息合法，则该节点为 FEC 分配标签，并向上游发出标签映射消息，标签映射消息中包含分配的标签等信息；
- (4) 收到标签映射消息的 LSR 检查本地存储的标签请求消息状态。对于某一 FEC 的标签映射消息，如果数据库中记录了相应的标签请求消息，LSR 将为该 FEC 进行标签分配，并在其标签转发表中增加相应的条目，然后向上游 LSR 发送标签映射消息；
- (5) 当入口 LSR 收到标签映射消息时，它也需要在标签转发表中增加相应的条目。这时，就完成了 LSP 的建立，接下来就可以对该 FEC 对应的数据分组进行标签转发了。

4. 会话撤销

LDP 通过检测会话连接上传输的 LDP PDU 来判断会话的完整性。

LSR 为每个会话建立一个“生存状态”定时器，每收到一个 LDP PDU 时刷新该定时器。如果在收到新的 LDP PDU 之前定时器超时，LSR 认为会话中断，对等关系失效。LSR 将关闭相应的传输层连接，终止会话进程。

1.4.4 LDP 环路检测

在 MPLS 域中建立 LSP 也要防止产生环路，LDP 环路检测机制可以检测 LSP 环路的出现，并避免标签请求等消息发生环路。

LDP 环路检测有两种方式：

1. 最大跳数

在传递标签绑定的消息中包含跳数信息，每经过一跳该值就加一。当该值超过规定的最大值时认为出现环路，终止 LSP 的建立过程。

2. 路径向量

在传递标签绑定的消息中记录路径信息，每经过一跳，相应的 LSR 就检查自己的 ID 是否在此记录中。如果没有，将自己的 ID 添加到该记录中；如果有，说明出现了环路，终止 LSP 的建立过程。

1.4.5 基于约束路由的 LDP

MPLS 还支持基于约束路由的 LDP 机制（CR-LDP，Constrain-based Routing LDP）。所谓 CR-LDP，就是入口节点在发起建立 LSP 时，在标签请求消息中对 LSP 路由附加了一定的约束信息。这些约束信息可以是对沿途 LSR 的精确指定，即逐一指定 LSP 上的 LSR，此时叫严格的显式路由；也可以是对选择下游 LSR 的模糊限制，即只指定 LSP 上的个别 LSR，此时叫松散的显式路由。

1.5 MPLS 与其他协议间的关系

1.5.1 MPLS 与路由协议的关系

LDP 通过逐跳方式建立 LSP 时，要利用沿途各 LSR 路由转发表中的信息来确定下一跳，而路由转发表中的信息一般是通过 IGP、BGP 等路由协议收集的。但是，LDP 并不直接和各种路由协议有关联，只是间接使用路由信息。

另一方面，虽然 LDP 是专门用来实现标签分发的协议，但 LDP 并不是唯一的标签分发协议。对 BGP、RSVP 等已有协议进行扩展，也可以支持 MPLS 标签的分发。MPLS 的一些应用也需要对某些路由协议进行扩展。例如，基于 MPLS 的 VPN 应用就需要对 BGP 协议进行扩展，以便 BGP 协议能传播 VPN 的路由信息；基于 MPLS 的流量工程 TE（Traffic Engineering）需要对 OSPF 或 IS-IS 协议进行扩展，以便携带链路状态信息。

1.5.2 RSVP 对 MPLS 的扩展

资源预留协议 RSVP（Resource Reservation Protocol）经扩展后可以支持 MPLS 标签的分发，同时，在传送标签绑定消息时，还能携带资源预留的信息。通过这种

方法建立的 LSP 可以具有资源预留功能，即沿途的 LSR 可以为该 LSP 分配一定的资源，使在此 LSP 上传送的业务得到保证。

RSVP 协议的扩展主要是在其 Path 消息和 Resv 消息中增加新的对象，这些新对象除了可以携带标签绑定信息外，还可以携带对沿途 LSR 寻径时的限制信息，从而支持 LSP 约束路由的功能。扩展的 RSVP 协议还支持快速重路由，即在一定条件下 LSP 需要改变时，可以在不中断用户业务的同时，将原来的业务流重新路由到新建立的 LSP 上。

1.6 MPLS 应用

1.6.1 基于 MPLS 的 VPN

传统的 VPN 一般是通过 GRE、L2TP、PPTP 等隧道协议来实现私有网络间数据流在公网上的传送。LSP 本身就是公网上的隧道，用 MPLS 来实现 VPN 有天然的优势。基于 MPLS 的 VPN 就是通过 LSP 将私有网络在地域上的不同分支联结起来，形成一个统一的网络。基于 MPLS 的 VPN 还支持不同 VPN 间的互通。

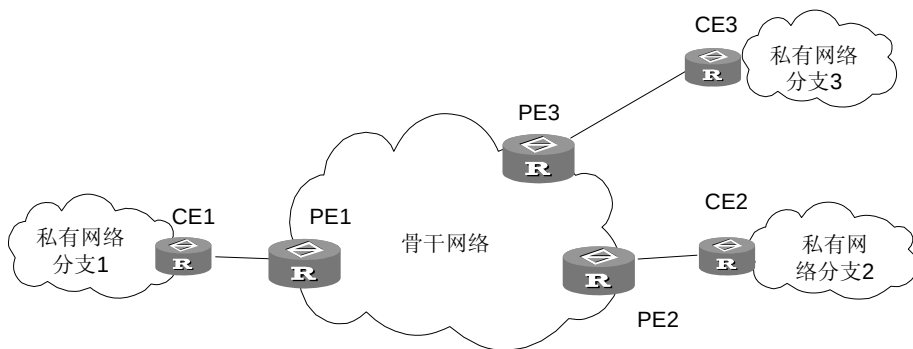


图1-6 基于 MPLS 的 VPN

图 1-6给出了基于MPLS的VPN的基本结构。CE（Customer Edge）是用户边缘设备，可以是路由器，也可以是交换机，甚至是一台主机；PE（Provider Edge）是服务商边缘路由器，位于骨干网络；PE负责对VPN用户进行管理、建立各PE间LSP连接、同一VPN用户各分支间路由分派。

PE 间的私有网络路由分派通常是用扩展的 BGP 协议实现的。基于 MPLS 的 VPN 支持不同 VPN 间 IP 地址复用和不同 VPN 间互通，和传统的路由相比，VPN 路由中需要增加分支和 VPN 的标识信息，这就需要对 BGP 协议进行扩展才能携带 VPN 的路由信息。

1.6.2 基于 MPLS 的流量工程

1. 流量工程的作用

网络拥塞是影响骨干网络性能的主要问题。拥塞的原因一般是网络资源不足，或者网络资源的负载不均衡，导致局部拥塞。流量工程用来解决由负载不均衡导致的拥塞。流量工程通过动态监控网络的流量和网络单元的负载，实时调整流量管理参数、路由参数和资源约束参数等，使网络运行状态迁移到理想状态，优化网络资源的使用，从而避免由于负载不均衡引起的拥塞。

2. 用 MPLS 来实现流量工程的优点

现有的 IGP 协议都是拓扑驱动的，只考虑网络静态的连接情况，不能反映带宽和流量特性等动态状况，这正是导致网络负载不均衡的主要原因。而 MPLS 具有的一系列不同于 IGP 的特性，正是实现流量工程所需要的：MPLS 支持异于路由协议路径的显式 LSP 路由；LSP 较传统单个 IP 分组转发更便于管理和维护；基于约束路由的 LDP 可以实现流量工程的各种策略；基于 MPLS 的流量工程的系统开销较其它实现方式更低等等。

3. 基于 MPLS 的流量工程的实现

用 MPLS 来实现流量工程时，先要根据物理网络的拓扑生成 MPLS 导出图，即由 LSR、连接 LSR 的 LSP、LSP 属性这三种元素构成的派生拓扑图。同时，将通过 MPLS 域的数据划分成若干主干流（Traffic Trunk）。主干流一般定义为在 MPLS 域中经过相同 Ingress 和 Egress 的所有单向流量。主干流有许多属性，包括流量参数、路径选择和维护方式、优先级、可抢占性、资源亲和度等。对资源也定义了一些属性，如资源级别、最大分配复用度等。然后，以主干流的属性、资源的属性、网络的状态信息为生成约束路由的策略，来找出主干流的路径。主干流的路径可以根据网络状态的变化动态调整。

1.6.3 基于 MPLS 的 QoS

为了能够在 IP 网络上支持语音，视频等实时业务，需要有 QoS 的支持，以便保证重要的、敏感或者实时性较强的数据流在网络中得到优先处理。H3C 的产品支持基于 MPLS 的 Diff-serv 特性，在保证网络高效利用率的同时，又能根据不同数据流的优先级实现差别服务，从而为语音，视频数据流提供有带宽保证的、低延时、低丢包率的服务。由于目前全网实施流量工程的难度比较大，因此，在实际的组网方案中，往往倾向于使用差分服务模型来实施 QoS。

Diff-Serv 的基本机制是：在网络边缘，根据业务的服务质量要求，将该业务映射到一定的业务类别中，利用 IP 分组中的 DS 字段（由 TOS 域而来）唯一的标记该类业务，然后，骨干网络中的各节点根据该字段对各种业务采取预先设定的服务策略，保证相应的服务质量。Diff-Serv 的这种对服务质量的分类和标签机制和 MPLS

的标签分配十分相似，事实上，基于 MPLS 的 Diff-Serv 就是通过将 DS 的分配融入 MPLS 的标签分配过程来实现的。

Diff-Serv 对不同的服务类别规定了一致的处理方法，包括队列选择、排队、丢弃等操作，这些处理组合就叫 PHB (Per Hop Behavior)。同时，属于同一 PHB 的分组又可以有不同的丢弃优先级。PHB 和丢弃优先级信息通过为分组分配不同的 DS 编码来表示，这些 DS 编码又称 DSCP (Diff-Serv Code Point)。关于 Diff-Serv 的详细介绍，请参见本手册的“QoS”部分。

为了支持基于 Diff-Serv 模型的端到端的 QoS 服务，提供如下几种技术手段：

- 基于流量的 IP 优先级分类

IP 优先级分类在网络边缘进行，利用 IPv4 包头的 Type-of-Service 3 个比特对每一个 IP 包依据其地址进行优先级分类。在核心利用不同的队列技术对不同等级的流量进行不同的处理，使得不同的服务级别得到体现。为实现语音、图象、数据流的差分服务，对不同的业务流在进行标签交换时，即 PE 在给报文加 Label 时，会把 IP 报文携带的 TOS 值映射到标签的 CoS 域，这样，原来由 IP 携带的类型信息，现在由标签携带。在 PE 路由器之间，根据标签的 CoS 域，进行有差别的调度 (PQ、CQ、WFQ、CBQ 等)。

- 用 TP 实现承诺带宽及限制带宽的功能

在 PE 上与 CE 相连的链路上配置 TP (Traffic Policing) 可以实现该功能。同时，TP 还提供了承诺的带宽和限制带宽的功能。

- 用 WRED 进行拥塞避免

WRED 在网络的瓶颈处监视并缓解网络的拥塞。一般在接入层出现拥塞的概率比较大。WRED 监视网络的负载，当拥塞刚开始出现时，它就开始有选择地丢弃一些包以降低流量。WRED 丢包的策略为：低优先级的流先丢，以保证高优先级的流可以顺利通过。在可能发生拥塞的端口运行 WRED，是避免拥塞的较好选择。

在具体实现中，为了达到最好的效率，需要对任务进行分工。因为 QoS 是一个需要消耗很多处理器资源的应用，所以，这一任务应分配在边缘和核心路由器上运行，以减少对单独路由器的压力。

综上所述，实现基于 CoS 的差分服务结构需要 4 个步骤：

- MPLS 边缘路由器上实现入口的带宽限制和完成入口流量的分类。
- 边缘设备也需要承担带宽管理的工作，采用 TP。
- MPLS 核心路由器完成 CoS 的管理工作，进行有差别的服务质量保证。
- 出口设备，像入口设备一样，完成带宽限制工作。入口、出口设备对带宽的限制保护了网络免于拥塞，使得网络具有很高的可扩展性。

详细内容请参见本手册的“QoS”部分。

第2章 MPLS 配置

2.1 MPLS 配置概述

MPLS 提供了比较完全的 MPLS 基本能力：

- 基本 MPLS 转发

Comware 支持基本 MPLS 转发功能。除标签报文的转发之外，还提供了 TTL 处理等功能。

- LDP 会话建立和 LSP 路径维护

支持 LDP 会话；支持最大跳数和路径向量两种方式的环路检测；提供静态 LSP 的建立、删除功能。

支持松散和严格的显式路由；可以人工指定 LSP 路径。

Comware 除提供 MPLS 基本功能外，还提供了性能监视和故障检测工具。

要使一台安全网关具有基本的 MPLS 功能，一般的配置过程如下：

- (1) 配置 LSR 的标识 ID
- (2) 使能 MPLS
- (3) 使能 LDP 协议
- (4) 进入接口模式，使能接口的 LDP 功能。

经过上述的基本配置，安全网关即可提供 MPLS 转发和 LDP 信令功能。

如果要修改一些缺省参数，或者实现一些特殊的 MPLS 功能，如手工建立 LSP、建立显式路由等，则可以根据配置列表提供的方法来配置。有些复杂的功能，可能需要多个配置的组合才能实现。

2.2 MPLS 基本配置

MPLS 基本配置中必须的配置项包括：

- 配置 MPLS LSR ID
- 使能 MPLS，并进入 MPLS 视图

MPLS 基本配置中可选的配置项包括：

- 配置拓扑驱动建立 LSP 的建立策略
- 配置静态 LSP
- 配置上报统计信息的间隔时间

2.2.1 配置 MPLS LSR ID

在配置其他 MPLS 命令之前，必须首先为 LSR 配置 ID。LSR ID 一般采用 IP 地址的格式，并且要保证域内唯一。

请在系统视图下进行下列配置。

表2-1 配置 MPLS LSR ID

操作	命令
指定 LSR 的 LSR ID	mpls lsr-id <i>ip-address</i>
删除 LSR 的 LSR ID	undo mpls lsr-id

缺省未指定 LSR ID。

2.2.2 进入 MPLS 视图

在系统视图下，**mpls** 命令用来进入 MPLS 视图。在进入 MPLS 视图后，可以进行 MPLS 相关配置。

表2-2 进入 MPLS 视图

操作	命令
进入 MPLS 视图	mpls
在全局下关闭 MPLS 功能	undo mpls

然后，在接口视图下，**mpls** 命令用来使能接口的 MPLS 能力。

在不支持广播报文的链路层协议，如 X.25、帧中继、ATM 上，必须要使用命令 **protocol ip { ip-address [ip-mask] | default | inarp [minutes] } [broadcast]** 配置 **broadcast** 属性，以支持广播和组播报文的传递。

2.2.3 配置拓扑驱动建立 LSP 的建立策略

配置拓扑驱动建立 LSP 的建立策略，指定过滤策略为 all 和 ip-prefix 策略。

请在 MPLS 视图下进行下列配置。

表2-3 配置拓扑驱动建立 LSP 的建立策略

操作	命令
配置拓扑驱动建立 LSP 的建立策略	lsp-trigger { all ip-prefix ip-prefix }
取消参数所指定的过滤条件，任何路由都不允许触发建立 LSP	undo lsp-trigger { all ip-prefix [ip-prefix] }

2.2.4 配置静态 LSP

可以手工设置某 LSR 为一条 LSP 上的一个节点，并可以对该 LSP 上承载的数据流进行限制。根据在 MPLS 域中的不同位置，LSR 有三种节点情况：入节点（Ingress）、中间节点（Transit）、出节点（Egress）。值得注意的是，必须对指定 LSP 沿途的 LSR 均作了相应配置，这条 LSP 才能正常工作。

undo static-lsp 用于删除一个用手工方式建立的 LSP。

请在 MPLS 视图下进行下列配置。

表2-4 设置本 LSR 为指定 LSP 的节点

操作	命令
设置本 LSR 为指定 LSP 的入口节点	static-lsp ingress <i>lsp-name</i> { destination <i>dest-addr</i> { <i>addr-mask</i> <i>mask-length</i> } } { nexthop <i>next-hop-addr</i> outgoing-interface <i>interfac-type</i> <i>interfac-num</i> } out-label <i>out-label-value</i>
	undo static-lsp ingress <i>lsp-name</i>
设置本 LSR 为指定 LSP 的中间节点	static-lsp transit <i>lsp-name</i> incoming-interface <i>interface-type</i> <i>interface-num</i> } in-label <i>in-label-value</i> { nexthop <i>next-hop-addr</i> outgoing-interface <i>interface-type</i> <i>interface-num</i> } out-label <i>out-label-value</i>
	undo static-lsp transit <i>lsp-name</i>
设置本 LSR 为指定 LSP 的出口节点	static-lsp egress <i>lsp-name</i> incoming-interface <i>interfac-type</i> <i>interfac-num</i> in-label <i>in-label-value</i>
	undo static-lsp egress <i>lsp-name</i>

2.2.5 配置 MPLS 的 IP TTL 复制功能

MPLS 标签中包含一个 8 位的 TTL 域，其含义与 IP 头中的 TTL 域相同。TTL 除了用于防止产生路由环路外，也用于实现 tracer 功能。

根据 RFC3031 中的描述，LSR 节点在对分组打标签时，需要将原 IP 分组或上层标签中的 TTL 值拷贝到新增加标签的 TTL 域。LSR 在转发标签分组时，对栈顶标签的 TTL 域作减一操作。标签出栈时，再将栈顶的 TTL 值拷贝回 IP 分组或下层标签。

如果 LSP 穿越由 ATM-LSR 或 FR-LSR 构成的非 TTL LSP 段时，由于域内的 LSR 无法处理 TTL 域，需要在进入非 TTL LSP 段时，对 TTL 进行统一处理。即，一次性减去反映该非 TTL LSP 段长度的值。

在 MPLS VPN 应用中，出于网络安全的考虑，MPLS 骨干网络的结构可能需要隐藏，这种情况下，对于私网报文，Ingress 节点上就不能使用 TTL 的复制功能。

请在 MPLS 视图下进行下列配置。

表2-5 配置 MPLS 的 IP TTL 复制功能

操作	命令
对报文使能 MPLS 的 IP TTL 复制功能	ttl propagate { public vpn }
对报文禁止 MPLS 的 IP TTL 复制功能	undo ttl propagate { public vpn }

缺省情况下，对公网报文使能 MPLS 的 IP TTL 复制功能，对 VPN 报文则不使能此功能。

在 Ingress 节点使能 IP TTL 复制功能后，报文在 LSP 中经过的每一跳都体现为 IP TTL 逐跳递减，tracert 的结果将反映报文实际经过的路径；

如果不在 Ingress 节点使能 TTL 复制功能，则报文在 LSP 中经过的跳数不会导致 IP TTL 递减，tracert 的结果不包括 MPLS 骨干网络中每一跳，就好像 Ingress 路由器与 Egress 路由器是直连的。

关于 MPLS 的 IP TTL 复制功能，需要注意以下几点：

- 在 MPLS 域内部，MPLS 报文多层标签之间的 TTL 值总是互相复制。
- MPLS 的 IP TTL 复制功能对本地发送报文没有影响，本地发送报文都将进行 TTL 复制，从而保证本地管理员能够使用 **tracert** 检测网络。
- 在 Egress 节点使能 IP TTL 复制功能后，系统将 MPLS 标签的 TTL 域值复制到 IP 头的 TTL 域，作为 IP 头的 TTL 值，并执行减一操作。
- 如果在 Ingress 路由器上配置 **ttl propagate vpn** 命令使能对 VPN 报文的 IP TTL 复制功能，则必须在 Egress 路由器上也使能对 VPN 报文的 IP TTL 复制功能。反之，如果不使能则都不使能。否则，tracert 的结果不能真实的反映网络的情况。建议在所有相关 PE 上都使能此功能，以保证从不同的 PE 执行 tracert 得到的结果一致。
- 所有的 P 路由器都不需要配置 **ttl propagate**。

2.2.6 配置 MPLS 使用 IP 路由返回 ICMP 响应报文

在 MPLS VPN 网络中，P 路由器无法对 MPLS 承载的 IP 报文进行路由。当 MPLS 报文的 TTL 超时，ICMP 响应报文将按照 LSP 继续传送，到达 LSP 终点路由器后，再根据 IP 路由转发 ICMP 响应报文。这种处理方式增加了网络流量和报文转发的不确定性。

对于仅有一层标签的 MPLS 报文，可以配置当 TTL 超时，直接使用 IP 路由返回 ICMP 响应报文。

请在 MPLS 视图下进行下列配置。

表2-6 配置 MPLS 使用 IP 路由返回 ICMP 响应报文

操作	命令
使用 IP 路由返回 ICMP 响应报文	ttl expiration pop
使用 LSP 返回 ICMP 响应报文	undo ttl expiration pop

缺省情况下, 对于一层标签的 MPLS TTL 超时报文, 将根据本地 IP 路由返回 ICMP 报文。

对于 ASBR 路由器以及 HoVPN 组网应用中的 SPE（包括嵌套应用中的 SPE），其承载 VPN 报文的 MPLS 报文也可能只有一层标签, 这种情况下, 如果希望对 VPN 私网进行 **tracert** 操作以查看公网路由器的转发路径, 需要进行两部分配置:

- (1) 在所有相关 PE 上配置 **ttl propogate vpn** 命令;
- (2) 在 ASBR 和 SPE 上配置 **undo ttl expiration pop** 命令, 以保证 ICMP 响应报文按照原 LSP 转发。

2.3 LDP 协议配置

LDP 协议配置中必须的配置包括:

- 使能 LDP 协议
- 在接口上使能 LDP 协议

LDP 协议配置中可选的配置包括:

- 配置 LDP 扩展发现模式
- 在出口节点配置倒数第二跳的标签
- 配置会话参数
- 配置环路检测
- 配置 LDP 的验证方式

2.3.1 使能 LDP 协议

要进行 LDP 的配置, 首先要使能 LDP 协议。

请在系统视图下进行下列配置。

表2-7 使能/去使能 LDP 协议

操作	命令
使能 LDP 协议	mpls ldp
禁止 LDP 协议	undo mpls ldp

缺省情况下 LDP 协议未激活。

2.3.2 在接口上使能 LDP 协议

要使接口具有 LDP 功能，必须在该接口模式下，对接口进行 LDP 使能。使能后的接口即开始建立 LDP 会话，在拓扑驱动方式时，开始建立 LSP。

禁止端口 LDP 功能，会导致接口下的所有 LDP 会话中断，基于这些会话的所有 LSP 也将被删除，建议用户谨慎使用此命令。

请在接口视图下进行下列配置。

表2-8 接口 LDP 使能

操作	命令
允许接口 LDP 功能	mpls ldp enable
禁止接口 LDP 功能	mpls ldp disable

缺省情况下禁止接口的 LDP 功能。

2.3.3 配置 LDP 扩展发现模式

配置 **remote-peer**，主要用于扩展发现模式，以便与链路不直接相连的对等体建立会话。

1. 进入 remote-peer 模式

请在系统视图下进行下列配置。

表2-9 进入扩展发现模式

操作	命令
进入扩展发现模式	mpls ldp remote-peer index
删除相应的 remote-peer	undo mpls ldp remote-peer index

无缺省的 remote-peer。

2. 配置 remote-peer 的地址

可以指定 **remote-peer** 的任何一个使能了 LDP 的接口地址或发布了路由的 LSR 的 loopback 地址，作为 **remote-peer** 的地址。

请在 **remote-peer** 视图下进行下列配置。

表2-10 配置 remote-peer 的地址

操作	命令
配置 remote-peer 的地址	remote-ip <i>ip-address</i>

无缺省的 remote-peer。

2.3.4 配置会话参数

1. 配置会话保持时间

接口上的 LDP 实体周期性的发出 Hello 报文，来发现 LDP 对等体，已经建立的 LDP 会话，也必须靠定期的消息来维持其存在（如果没有 LDP 消息报文，则须发送 Keepalive 报文）。



注意：

修改 holdtime 参数，不会改变原有会话的值，所做的修改将会作用于后续建立的会话。这里的会话指的是链路会话，而非 remote 会话。

请在接口视图下进行下列配置。

表2-11 配置会话保持时间

操作	命令
配置会话保持时间	mpls ldp timer { session-hold session-holdtime hello hello-holdtime }
恢复会话保持时间为缺省值	undo mpls ldp timer { session-hold hello }

session-holdtime 的缺省值为 60 秒，*hello-holdtime* 的缺省值为 15 秒。

2. 配置 hello 消息中的传输地址

这里的传输地址就是 hello 消息的传输地址 TLV 中携带的地址。通常情况下，传输地址为本 LSR 的 MPLS LSR ID，但是，有些应用需要灵活的配置。

请在接口视图下进行下列配置。

表2-12 配置 hello 传输地址

操作	命令
配置 hello 传输地址	mpls ldp transport-ip { interface ip-address }
恢复 hello 传输地址为默认值	undo mpls ldp transport-ip

缺省传输地址为本 LSR 的 MPLS LSR ID。

当两个 LSR 邻居之间有多条链路直接相连并且都使能 mpls ldp 时，要求使能 mpls ldp 的多个链路必须配置相同的传输地址，建议采用缺省的 lsr-id 作为传输地址，否则将可能导致 ldp 会话无法稳定建立。

2.3.5 配置远程 LDP 对等体会话参数

1. 配置 hello 计时器参数

请在 remote-peer 视图下进行下列配置。

表2-13 配置 hello 计时器参数

操作	命令
配置 hello 报文间隔和保持时间	mpls ldp timer targeted-hello { interval time holdtime time }
恢复 hello 报文间隔和保持时间为缺省值	undo mpls ldp timer targeted-hello { interval holdtime }

缺省情况下，hello 报文间隔为 13 秒，保持时间为 45 秒。

2. 配置会话保持计时器参数

请在 remote-peer 视图下进行下列配置。

表2-14 配置会话保持计时器参数

操作	命令
配置会话 keepalive 报文间隔和保持时间	mpls ldp timer targeted-session-hold { interval time holdtime time }
恢复会话 keepalive 报文间隔和保持时间为缺省值	undo mpls ldp timer targeted-session-hold { interval holdtime }

缺省情况下，keepalive 报文间隔为 24 秒，保持时间为 60 秒。

2.3.6 配置环路检测

1. 环路检测使能

用于控制在 LDP 信令过程中是否使用环路检测功能，环路检测有最大跳数和路径向量两种方式。

最大跳数方式是在传递标签绑定的消息中包含跳数信息，每经过一跳，该值就加一，当该值超过规定的最大值时，就认为出现了环路，从而终止 LSP 的建立过程。

路径向量方式是在传递标签绑定的消息中记录路径信息，每经过一跳，相应的路由器就检查自己的 ID 是否在此记录中，如果没有，就将自己的 ID 添加到该记录中，若有，就说明出现了环路，终止 LSP 的建立过程。

请在系统视图下进行下列配置。

表2-15 环路检测使能

操作	命令
允许进行环路检测	mpls ldp loop-detect
禁止进行环路检测	undo mpls ldp loop-detect

缺省为不允许环路检测。

2. 设置环路检测最大跳数

当环路检测采用最大跳数方式时，可以规定跳数的最大值，达到该最大值即认为出现了环路，LSP 建立失败。

请在系统视图下进行下列配置。

表2-16 设置环路检测最大跳数

操作	命令
设置环路检测的最大跳数	mpls ldp hops-count <i>hop-number</i>
恢复最大跳数的缺省值	undo mpls ldp hops-count

缺省的最大值为 32。

3. 设置路径向量的最大值

当环路检测采用路径向量方式时，也需要规定 LSP 路径的最大值。这样，在以下条件之一时，即认为出现了环路，LSP 建立失败：

- (1) 路径向量记录表中已有本 LSR 的记录
- (2) 路径的跳数达到这里设定的最大值

请在系统视图下进行下列配置。

表2-17 设置路径向量的最大值

操作	命令
设置路径向量的最大跳数	mpls ldp path-vectors <i>pv-number</i>
恢复路径向量最大跳数的缺省值	undo mpls ldp path-vectors

路径向量最大跳数的缺省值为 32。

2.3.7 配置 LDP 验证方式

请在接口视图或 **remote-peer** 视图下进行下列配置。

表2-18 配置 LDP 验证方式

操作	命令
配置 LDP 验证方式	mpls ldp password { cipher simple } password
取消 LDP 的验证	undo mpls ldp password

2.4 MPLS 的显示与调试

2.4.1 MPLS 的显示与调试

MPLS 提供了丰富的显示与调试命令，可以监控 LDP 会话状态、隧道配置情况、所有 LSP 及其状态等，是调试、诊断的有力工具。

1. 显示静态 LSP

在完成上述配置后，在所有视图下，执行 **display** 命令，可以显示全部或单个静态 LSP 的运行情况，通过查看显示信息，验证配置的效果。

表2-19 显示静态 LSP 的信息

操作	命令
显示静态 LSP 的信息	display mpls static-lsp [verbose] [include text]

2. 显示/清除 MPLS 统计数据

在所有视图下执行 **display** 命令，在用户视图下执行 **reset** 命令，可以显示/清除全部或单个 LSP 的统计信息。

表2-20 显示/清除 MPLS 统计数据

操作	命令
显示 MPLS 统计数据	display mpls statistics { interface { all interface-type interface-type interface-num } } { lsp [lsp-index name all name lsp-name] }
清除 MPLS 统计数据	reset mpls statistics { interface { all interface-type interface-type interface-num } lsp { lsp-index all name lsp-name } }

3. 显示/清除 MPLS 快速转发信息

在所有视图下执行 **display** 命令，在用户视图下执行 **reset** 命令，可以显示/清除 MPLS 快速转发信息。

表2-21 显示/清除 MPLS 快速转发信息

操作	命令
显示 MPLS 快速转发信息	display mpls fast-forwarding cache
清除 MPLS 快速转发信息	reset mpls fast-forwarding cache

4. 显示使能 MPLS 的接口信息

在完成上述配置后，在所有视图下执行 **display** 命令，可以显示所有使能了 MPLS 能力的接口的相关信息，通过查看显示信息，验证配置的效果。

表2-22 显示使能了 MPLS 的接口信息

操作	命令
显示使能 MPLS 的接口信息	display mpls interface

5. 显示 LSP 的信息

在所有视图下执行下列命令，可以显示 MPLS LSP 的相关信息。

表2-23 显示 MPLS LSP 的相关信息

操作	命令
显示 LSP 的信息	display mpls lsp [verbose] [include text]

6. MPLS 的调试信息

在用户视图下，执行 **debugging** 命令，可对所有使能了 MPLS 能力的接口的相关信息调试。

打开调试开关对安全网关性能有一定影响，建议慎用此命令。该命令的 **undo** 形式关闭相应的调试开关。

表2-24 打开 MPLS 的调试信息开关

操作	命令
打开 MPLS 的各种调试信息的开关	debugging mpls lspm { all packet event process agent interface policy vpn }
关闭 MPLS 的各种调试信息的开关	undo debugging mpls lspm { all packet event process agent interface policy vpn }
复位接口上某一个指定的 LDP 会话	mpls ldp reset-session peer-address

7. MPLS 的 trap 信息

使能 MPLS 的 LSP/LDP 建立过程的 TRAP 功能。

请在系统视图下进行操作。

表2-25 使能 MPLS 的 TRAP 功能

操作	命令
使能 MPLS 的 LDP TRAP 功能	snmp-agent trap enable ldp
去使能 MPLS 的 LDP TRAP 功能	undo snmp-agent trap enable ldp
使能 MPLS 的 LSP TRAP 功能	snmp-agent trap enable lsp
去使能 MPLS 的 LSP TRAP 功能	undo snmp-agent trap enable lsp

2.4.2 LDP 协议的显示与调试

1. LDP 协议的显示命令

Comware 提供了丰富的 MPLS 监控操作命令，可以监控 LSR 状态、LDP 会话状态、接口状态、对等体状态等，是调试、诊断的有力工具。

在完成上述配置后，在所有视图下，执行 **display** 命令，可以显示配置后 LDP 的运行情况，通过查看显示信息，验证配置的效果。

表2-26 LDP 监控命令

操作	命令
显示 LD 协议信息	display mpls ldp
显示 LDP 的 buffer 信息	display mpls ldp buffer-info
显示 LDP 使能的接口信息	display mpls ldp interface
显示 LDP 保存的标签信息	display mpls ldp lsp
显示 LDP 会话的所有对等体信息	display mpls ldp peer
显示 LDP 会话的远端对等体信息	display mpls ldp remote
显示 LDP 会话状态和参数	display mpls ldp session

2. 诊断命令

在用户视图下，执行 **debugging** 命令，可对 LDP 的各种消息进行调试。

表2-27 MPLS 诊断

操作	命令
打开 MPLS 诊断开关	debugging mpls ldp { { all main advertisement session pdu notification } [interface <i>interface-type</i> <i>interface-number</i>] remote }
关闭 MPLS 诊断开关	undo debugging mpls ldp { { all main advertisement session pdu notification remote } [interface <i>interface-type</i> <i>interface-number</i>] remote }

all: 显示所有和 LDP 相关的调试信息。

main: 显示 LDP 主任务的调试信息。

advertisement: 显示处理 LDP 通告消息过程中的调试信息。

session: 显示处理 LDP 会话过程中的调试信息。

pdu: 显示处理 PDU 数据包过程中的调试信息。

notification: 显示处理通知消息过程中的调试信息。

remote: 显示所有 remote peer 的调试信息。

2.5 MPLS 典型配置举例

1. 组网需求

图 2-1给出一个由四台安全网关组成的网络，其中SecPathB和SecPathC间通过SDH连接，SecPathB和SecPathA、SecPathD间通过以太网连接。

四台安全网关均支持 MPLS，任意安全网关之间都可以建立 LSP，运行的路由协议为 OSPF。LDP 利用 OSPF 的路由信息建立 LSP。

2. 组网图

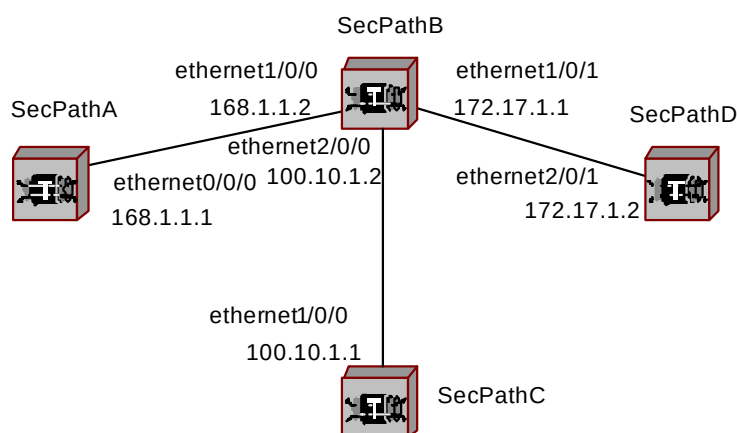


图2-1 组网图

3. 配置步骤

(1) SecPathA 上的配置

配置 SecPathA 的 LSR ID, 并使能 MPLS 及 LDP

```
[H3C] mpls lsr-id 168.1.1.1
```

```
[H3C] mpls
```

```
[H3C] mpls ldp
```

配置以太网接口的 IP 地址, 并对接口使能 MPLS 及 LDP

```
[H3C] interface ethernet 0/0/0
```

```
[H3C-Ethernet0/0/0] ip address 168.1.1.1 255.255.0.0
```

```
[H3C-Ethernet0/0/0] mpls
```

```
[H3C-Ethernet0/0/0] mpls ldp enable
```

在 SecPathA 与 SecPathB 相连的接口上运行 OSPF

```
[H3C] router id 168.1.1.1
```

```
[H3C] ospf
```

```
[H3C-ospf-1] area 0
```

```
[H3C-ospf-1-area-0.0.0.0] network 168.1.0.0 0.0.255.255
```

(2) SecPathB 上的配置

配置 SecPathB 的 LSR ID, 并使能 MPLS 及 LDP

```
[H3C] mpls lsr-id 172.17.1.1
```

```
[H3C] mpls
```

```
[H3C] mpls ldp
```

配置以太网接口 1/0/0 的 IP 地址, 并对接口使能 MPLS 及 LDP

```
[H3C] interface ethernet 1/0/0
```

```
[H3C-Ethernet1/0/0] ip address 168.1.1.2 255.255.0.0
```

```
[H3C-Ethernet1/0/0] mpls
```

```
[H3C-Ethernet1/0/0] mpls ldp enable
```

配置以太网接口 1/0/1, 并对接口使能 MPLS 及 LDP

```
[H3C] interface ethernet 1/0/1
```

```
[H3C-Ethernet1/0/1] ip address 172.17.1.1 255.255.0.0
```

```
[H3C-Ethernet1/0/1] mpls
```

```
[H3C-Ethernet1/0/1] mpls ldp enable
```

配置以太网接口 2/0/0, 并对接口使能 MPLS 及 LDP

```
[H3C] interface ethernet 2/0/0
```

```
[H3C-Ethernet2/0/0] ip address 100.10.1.2 255.255.255.0
```

```
[H3C-Ethernet2/0/0] mpls
```

```
[H3C-Ethernet2/0/0] mpls ldp enable
```

```
[H3C-Ethernet2/0/0] quit
```

分别在 SecPathB 与 SecPathA、SecPathD、SecPathC 相连的接口上运行 OSPF

```
[H3C] router id 172.17.1.1
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 168.1.0.0 0.0.255.255
[H3C-ospf-1-area-0.0.0.0] network 172.17.0.0 0.0.255.255
[H3C-ospf-1-area-0.0.0.0] network 100.10.1.0 0.0.0.255
[H3C-ospf-1-area-0.0.0.0] quit
```

(3) SecPathC 上的配置

配置 loopback 接口。

```
[H3C] interface LoopBack0
[H3C-LoopBack0] ip address 172.16.1.2 255.255.255.255
[H3C-LoopBack0] quit
```

配置 OSPF。

```
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 172.16.1.2 0.0.0.0
```

配置 SecPathC 的 LSR ID，并使能 MPLS 及 LDP

```
[H3C] mpls lsr-id 172.16.1.2
[H3C] mpls
[H3C] mpls ldp
```

配置 Ethernet 接口 1/0/0 的 IP 地址，并对接口使能 MPLS 及 LDP

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 100.10.1.1 255.255.255.0
[H3C-Ethernet1/0/0] mpls
[H3C-Ethernet1/0/0] mpls ldp enable
[H3C-Ethernet1/0/0] quit
```

在 SecPathC 与 SecPathB 相连的接口上运行 OSPF

```
[H3C] router id 172.16.1.2
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 100.10.1.0 0.0.0.255
```

(4) SecPathD 上的配置

配置 SecPathD 的 LSR ID，并使能 MPLS 及 LDP

```
[H3C] mpls lsr-id 172.17.1.2
[H3C] mpls
[H3C] mpls ldp
```

配置以太网接口 2/0/1 的 IP 地址，并对接口使能 MPLS 及 LDP

```
[H3C] interface ethernet 2/0/1
[H3C-Ethernet2/0/1] ip address 172.17.1.2 255.255.0.0
[H3C-Ethernet2/0/1] mpls
[H3C-Ethernet2/0/1] mpls ldp enable

# 在 SecPathD 与 SecPathB 相连的接口上运行 OSPF

[H3C] router id 172.17.1.2
[H3C] ospf
[H3C-ospf-1] area 0
[H3C-ospf-1-area-0.0.0.0] network 172.17.0.0 0.0.255.255
```

2.6 MPLS 配置的故障排除

故障现象：接口使能 LDP 协议后，不能与对端建立会话。

故障排除：

原因之一：环路检测配置不同。

解决方法：检查本地和对端的配置，是否一端配了环路检测，而另一端没有配，如果是这样，就会导致会话协商不通过。

原因之二：如果本机得不到对方的 LSR ID 的路由，就不能建立 TCP 连接，会话就不可能建立。

解决方法：建立会话时默认的传输地址是 MPLS LSR ID，本机必须将 LSR ID 的路由（一般为 loopback 地址）发布出去，同时，要学到对端的 LSR ID 的路由。

目 录

第 1 章 VPN概述	1-1
1.1 VPN简介	1-1
1.1.1 VPN的特点	1-1
1.1.2 VPN的优势	1-1
1.1.3 VPN网络结构.....	1-2
1.2 VPN的基本技术.....	1-2
1.2.1 VPN基本组网应用	1-2
1.2.2 VPN的原理	1-3
1.3 VPN的分类.....	1-5
第 2 章 L2TP协议配置	2-1
2.1 L2TP协议简介	2-1
2.1.1 VPDN概述	2-1
2.1.2 L2TP协议介绍	2-1
2.2 LAC配置	2-6
2.2.1 启用L2TP	2-7
2.2.2 创建L2TP组	2-8
2.2.3 设置发起L2TP连接请求及LNS地址	2-8
2.2.4 设置本端名称.....	2-9
2.2.5 启用隧道验证及设置密码.....	2-9
2.2.6 配置将AVP数据隐含	2-10
2.2.7 设置通道Hello报文发送时间间隔.....	2-10
2.2.8 设置用户名、密码及配置用户验证	2-11
2.2.9 强制断开L2TP连接	2-12
2.2.10 开启或关闭流控功能.....	2-12
2.2.11 配置L2TP会话超时时间	2-13
2.2.12 配置L2TP Tunnel连接保持功能.....	2-13
2.2.13 配置LAC作为客户端	2-14
2.3 LNS配置	2-15
2.3.1 启用L2TP.....	2-16
2.3.2 启用/禁止L2TP多域功能.....	2-16
2.3.3 创建L2TP组	2-17
2.3.4 创建虚拟模板接口.....	2-17
2.3.5 设置接收呼叫的虚拟模板接口、通道对端名称和域名	2-18
2.3.6 设置本端名称.....	2-18
2.3.7 启用隧道验证及设置密码.....	2-19
2.3.8 配置将AVP数据隐含	2-19

2.3.9 设置通道Hello报文发送时间间隔	2-20
2.3.10 强制本端CHAP验证	2-20
2.3.11 强制LCP重新协商	2-21
2.3.12 设置本端地址及分配的地址池	2-22
2.3.13 设置用户名、密码及配置用户验证	2-22
2.3.14 强制断开L2TP连接	2-22
2.3.15 开启或关闭流控功能	2-23
2.3.16 配置L2TP会话超时时间	2-23
2.3.17 配置L2TP支持EAD	2-24
2.4 L2TP显示和调试	2-24
2.5 L2TP典型配置举例	2-25
2.5.1 NAS-Initialized VPN	2-25
2.5.2 Client-Initialized VPN	2-27
2.5.3 L2TP多域组网应用	2-28
2.5.4 LAC作为客户端典型应用	2-31
2.5.5 复杂的组网情况	2-33
2.6 L2TP故障诊断与排错	2-33
第 3 章 GRE协议配置	3-1
3.1 GRE协议简介	3-1
3.2 GRE配置	3-4
3.2.1 创建虚拟Tunnel接口	3-4
3.2.2 设置Tunnel接口报文的封装模式	3-4
3.2.3 指定Tunnel的源端	3-5
3.2.4 指定Tunnel的目的端	3-5
3.2.5 设置Tunnel接口的网络地址	3-6
3.2.6 设置Tunnel两端进行端到端校验	3-6
3.2.7 设置Tunnel接口的识别关键字	3-7
3.2.8 配置通过Tunnel的路由	3-7
3.2.9 配置keepalive功能	3-7
3.3 GRE显示和调试	3-8
3.4 GRE典型配置举例	3-8
3.5 GRE故障诊断与排除	3-10
第 4 章 IPsec配置	4-1
4.1 IPsec概述	4-1
4.1.1 IPsec协议简介	4-1
4.1.2 加密卡简介	4-2
4.1.3 IPsec基本概念	4-2
4.1.4 IPsec多实例简介	4-6
4.1.5 IPsec在Comware上的实现	4-6
4.2 IPsec配置	4-7

4.2.1 定义访问控制列表.....	4-8
4.2.2 定义安全提议.....	4-9
4.2.3 创建安全策略.....	4-12
4.2.4 配置安全策略模板.....	4-20
4.2.5 在接口上应用安全策略组.....	4-21
4.2.6 配置取消对next payload域的检查	4-21
4.2.7 配置IPsec分片报文缓存处理	4-22
4.2.8 加密卡可选配置	4-23
4.3 IPsec显示与调试.....	4-25
4.3.1 Comware主体软件IPsec的显示与调试.....	4-25
4.3.2 加密卡IPsec的显示与调试.....	4-27
4.4 IPsec典型配置案例	4-29
4.4.1 采用manual方式建立安全联盟的配置	4-29
4.4.2 采用isakmp方式建立安全联盟的配置	4-32
4.4.3 使用加密卡进行加/解密和认证	4-35
4.4.4 防火墙与VRRP备份组虚地址之间建立SA配置举例	4-38
4.4.5 IPsec/IKE多实例配置举例	4-43
4.5 IPsec排错	4-47
第 5 章 IKE配置.....	5-1
5.1 IKE协议简介	5-1
5.1.1 IKE协议概述	5-1
5.1.2 IKE配置前准备工作	5-3
5.2 IKE的配置	5-3
5.2.1 IKE主要配置	5-3
5.2.2 配置本端防火墙的名称	5-4
5.2.3 定义IKE安全提议	5-4
5.2.4 配置IKE对等体.....	5-7
5.2.5 配置Keepalive定时器	5-10
5.2.6 配置IKE禁止DH硬件加速	5-12
5.3 IKE显示与调试	5-12
5.4 IKE典型配置案例.....	5-13
5.4.1 IKE典型配置组网应用.....	5-13
5.4.2 IKE野蛮模式及NAT穿越的组网应用	5-14
5.5 IKE故障诊断与排错	5-17
第 6 章 动态VPN	6-1
6.1 DVPN简介	6-1
6.1.1 概述	6-1
6.1.2 DVPN基本概念介绍.....	6-1
6.1.3 基本工作原理.....	6-2
6.1.4 基本网络结构.....	6-4

6.1.5 传统VPN与DVPN的比较	6-4
6.2 DVPN的配置	6-7
6.2.1 基本配置	6-8
6.2.2 配置Tunnel接口属性	6-11
6.2.3 配置dvpn-class	6-14
6.2.4 配置dvpn-policy	6-16
6.2.5 动态VPN的显示和调试	6-19
6.3 DVPN典型组网应用	6-20
6.3.1 DVPN穿越NAT典型配置组网	6-20
6.3.2 DVPN和GRE配合使用典型组网	6-24
第 7 章 BGP/MPLS VPN配置	7-1
7.1 BGP/MPLS VPN概述	7-1
7.1.1 BGP/MPLS VPN模型	7-1
7.1.2 BGP/MPLS VPN的实现	7-4
7.1.3 多角色主机特性简介	7-5
7.1.4 OSPF VPN扩展	7-6
7.1.5 跨域VPN	7-9
7.2 BGP/MPLS VPN配置	7-12
7.2.1 CE的配置	7-13
7.2.2 PE的配置	7-14
7.2.3 配置P	7-27
7.3 BGP/MPLS VPN显示与调试	7-27
7.4 BGP/MPLS VPN典型配置举例	7-28
7.4.1 BGP/MPLS VPN综合组网举例	7-28
7.4.2 采用GRE隧道的BGP/MPLS VPN配置举例	7-34
7.4.3 Extranet组网举例	7-36
7.4.4 Hub&Spoke组网举例	7-41
7.4.5 CE双归属组网举例	7-46
7.4.6 多角色主机组网举例	7-51
7.4.7 OSPF多实例sham link配置举例	7-53
7.4.8 OSPF 多实例 CE配置举例	7-58
7.4.9 跨域VPN组网举例-OptionA	7-59
7.4.10 跨域VPN组网举例-OptionB	7-71
7.4.11 跨域VPN组网举例-OptionC	7-78

第1章 VPN 概述

1.1 VPN 简介

虚拟私有网（Virtual Private Network）简称 VPN，是近年来随着 Internet 的广泛应用而迅速发展起来的一种新技术，用以实现在公用网络上构建私人专用网络。“虚拟”主要指这种网络是一种逻辑上的网络。

伴随企业和公司的不断扩张，员工出差日趋频繁，驻外机构及客户群分布日益分散，合作伙伴日益增多，越来越多的现代企业迫切需要利用公共 Internet 资源来进行促销、销售、售后服务、培训、合作及其它咨询活动，这为 VPN 的应用奠定了广阔市场。

1.1.1 VPN 的特点

- VPN 有别于传统网络，它并不实际存在，而是利用现有公共网络，通过资源配置而成的虚拟网络，是一种逻辑上的网络。
- VPN 只为特定的企业或用户群体所专用。从 VPN 用户角度看来，使用 VPN 与传统专网没有区别。VPN 作为私有专网，一方面与底层承载网络之间保持资源独立性，即在一般情况下，VPN 资源不会被承载网络中的其它 VPN 或非该 VPN 用户的网络成员所使用；另一方面，VPN 提供足够安全性，确保 VPN 内部信息不受外部的侵扰。
- VPN 不是一种简单的高层业务。该业务建立专网用户之间的网络互联，包括建立 VPN 内部的网络拓扑、路由计算、成员的加入与退出等，因此 VPN 技术就比各种普通的点对点的机制要复杂得多。

1.1.2 VPN 的优势

- 在远端用户、驻外机构、合作伙伴、供应商与公司总部之间建立可靠的安全连接，保证数据传输的安全性。这一优势对于实现电子商务或金融网络与通讯网络的融合将有特别重要的意义。
- 利用公共网络进行信息通讯，一方面使企业以明显更低的成本连接远地办事机构、出差人员和业务伙伴，另一方面极大的提高了网络的资源利用率，有助于增加 ISP（Internet Service Provider，Internet 服务提供商）的收益。
- 只需要通过软件配置就可以增加、删除 VPN 用户，无需改动硬件设施。这使得 VPN 的应用具有很大灵活性。

- 支持驻外 VPN 用户在任何时间、任何地点的移动接入，这将满足不断增长的移动业务需求。
- 构建具有服务质量保证的 VPN（如 MPLS VPN），可为 VPN 用户提供不同等级的服务质量保证，通过收取不同的业务使用费用可获得更多的利润。

1.1.3 VPN 网络结构

VPN 是由若干 Site 组成的集合。Site 可以同时属于不同的 VPN，但是必须遵循如下规则：两个 Site 只有同时属于一个 VPN 定义的 Site 集合，才具有 IP 连通性。按照 VPN 的定义，一个 VPN 中的所有 Site 都属于一个企业，称为 Intranet；如果 VPN 中的 Site 分属不同的企业，则称为 Extranet。

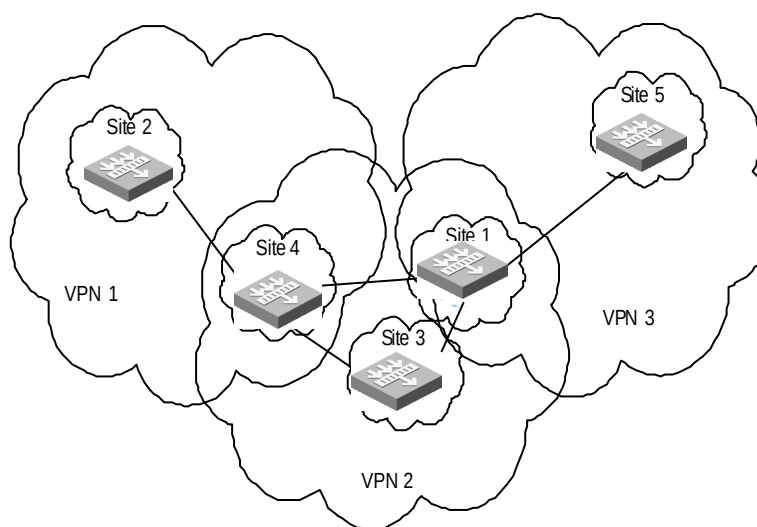


图1-1 VPN 组成示意图

上图显示了有 5 个 Site 分别构成了 3 个 VPN：

- VPN1---Site2、Site4
- VPN2---Site1、Site3、Site4
- VPN3---Site1、Site5

1.2 VPN 的基本技术

1.2.1 VPN 基本组网应用

以某企业为例，通过VPN建立的企业内部网如图 1-2所示：

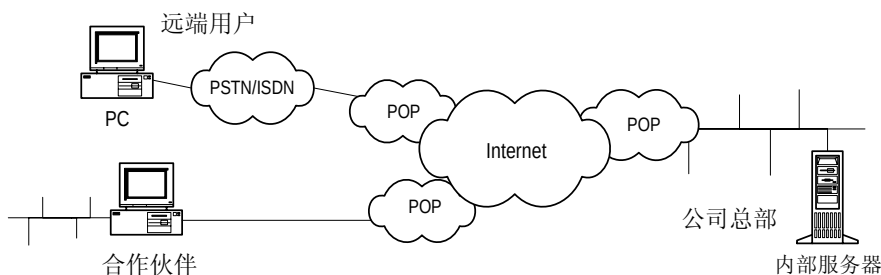


图1-2 VPN 组网示意图

从上图可以看出，企业内部资源享用者通过 PSTN/ISDN 网或局域网就可以连入本地 ISP 的 POP（Point of Presence）服务器，从而访问公司内部资源。而利用传统的 WAN 组建技术，相互之间要有专线相连才可以达到同样的目的。虚拟网组成后，远端用户和外地客户甚至不必拥有本地 ISP 的上网权限就可以访问企业内部资源，这对于流动性很大的出差员工和分布广泛的客户来说是很有意义的。

企业开设 VPN 业务所需的设备很少，只需在资源共享处放置一台支持 VPN 的服务器（如一台 Windows NT 服务器或支持 VPN 的路由器）就可以了。资源享用者通过 PSTN/ISDN 网或局域网连入本地 POP 服务器后，直接呼叫企业的远程服务器（VPN 服务器），呼叫接续过程由 ISP 的接入服务器（Access Server）与 VPN 服务器共同完成。

1.2.2 VPN 的原理

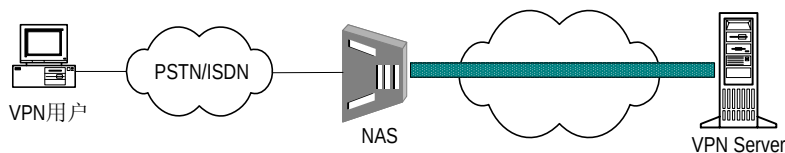


图1-3 VPN 接入示意图

如上图所示，VPN 用户通过 PSTN/ISDN 网拨入 ISP 的 NAS（Network Access Server）服务器，NAS 服务器通过用户名或接入号码识别出该用户为 VPN 用户后，就和用户的目的 VPN 服务器建立一条连接，称为隧道（Tunnel），然后将用户数据包封装成 IP 报文后通过该隧道传送给 VPN 服务器，VPN 服务器收到数据包并拆封后就可以读到真正有意义的报文了。反向的处理也一样。隧道两侧可以对报文进行加密处理，使 Internet 上的其它用户无法读取，因而是安全可靠的。对用户来说，隧道是其 PSTN/ISDN 链路的逻辑延伸，操作起来和实际物理链路相同。

隧道可以通过隧道协议来实现。根据是在 OSI 模型的第二层还是第三层实现隧道，隧道协议分为第二层隧道协议和第三层隧道协议。

1. 第二层隧道协议

第二层隧道协议是将整个 PPP 帧封装在内部隧道中。现有的第二层隧道协议有：

- **PPTP (Point-to-Point Tunneling Protocol)**: 点到点隧道协议, 由微软、Ascend 和 3Com 等公司支持, 在 Windows NT 4.0 以上版本中支持。该协议支持点到点 PPP 协议在 IP 网络上的隧道封装, PPTP 作为一个呼叫控制和管理协议, 使用一种增强的 GRE (Generic Routing Encapsulation, 通用路由封装) 技术为传输的 PPP 报文提供流控和拥塞控制的封装服务。
- **L2F (Layer 2 Forwarding)** 协议: 二层转发协议, 由北方电信等公司支持。L2F 协议支持对更高级协议链路层的隧道封装, 实现了拨号服务器和拨号协议连接在物理位置上的分离。
- **L2TP (Layer 2 Tunneling Protocol)**: 二层隧道协议, 由 IETF 起草, 微软等公司参与, 结合了上述两个协议的优点, 为众多公司所接受, 并且已经成为标准 RFC。L2TP 既可用于实现拨号 VPN 业务, 也可用于实现专线 VPN 业务。

2. 第三层隧道协议

第三层隧道协议的起点与终点均在 ISP 内, PPP 会话终止在 NAS 处, 隧道内只携带第三层报文。现有的第三层隧道协议主要有:

- **GRE (Generic Routing Encapsulation)** 协议: 这是通用路由封装协议, 用于实现任意一种网络层协议在另一种网络层协议上的封装。
- **IPsec (IP security)** 协议: IPsec 协议不是一个单独的协议, 它给出了 IP 网络上数据安全的一整套体系结构, 包括 AH (Authentication Header)、ESP (Encapsulating Security Payload)、IKE (Internet Key Exchange) 等协议。

GRE 和 IPsec 主要用于实现专线 VPN 业务。

3. 第二、三层隧道协议之间的异同

第三层隧道与第二层隧道相比, 优势在于它的安全性、可扩展性与可靠性。从安全性的角度看, 由于第二层隧道一般终止在用户侧设备上, 对用户网的安全及防火墙技术提出十分严峻的挑战; 而第三层隧道一般终止在 ISP 网关上, 因此一般情况下不会对用户网的安全技术提出较高要求。

从扩展性的角度看, 第二层隧道内封装了整个 PPP 帧, 这可能产生传输效率问题。其次, PPP 会话贯穿整个隧道并终止在用户侧设备上, 导致用户侧网关必须要保存大量 PPP 会话状态与信息, 这将对系统负荷产生较大的影响, 也会影响到系统的扩展性。此外, 由于 PPP 的 LCP 及 NCP 协商都对时间非常敏感, 这样隧道的效率降低会造成 PPP 对话超时等等一系列问题。相反, 第三层隧道终止在 ISP 的网关内, PPP 会话终止在 NAS 处, 用户侧网关无需管理和维护每个 PPP 对话的状态, 从而减轻了系统负荷。

一般地，第二层隧道协议和第三层隧道协议都是独立使用的，如果合理地将这两层协议结合起来使用，将可能为用户提供更好的安全性（如将 L2TP 和 IPsec 协议配合使用）和更佳的性能。

1.3 VPN 的分类

IP VPN 是指利用 IP 设施（包括公用的 Internet 或专用的 IP 骨干网）实现 WAN 设备专线业务（如远程拨号、DDN 等）的仿真。IP VPN 可有以下几种分类方法：

1. 按运营模式划分

(1) CPE-based VPN（Customer Premises Equipment based VPN）

用户不但要安装价格昂贵的设备及专门认证工具，还要负责繁杂的 VPN 维护（如通道维护、带宽管理等）。这种方式组网复杂度高、业务扩展能力弱。

(2) Network-based VPN（NBIP-VPN）

将 VPN 的维护等外包给 ISP 实施（也允许用户在一定程度上进行业务管理和控制），并且将其功能特性集中在网络侧设备处实现，这样可以降低用户投资、增加业务灵活性和扩展性，同时也可为运营商带来新的收入。

2. 按业务用途划分

(1) Intranet VPN（企业内部虚拟专网）

Intranet VPN 通过公用网络进行企业内部各个分布点互联，是传统的专线网或其它企业网的扩展或替代形式。

(2) Access VPN（远程访问虚拟专网）

Access VPN 向出差流动员工、远程办公人员和远程小办公室提供了通过公用网络与企业的 Intranet 和 Extranet 建立私有的网络连接。Access VPN 的结构有两种类型，一种是由用户发起（Client-initiated）的 VPN 连接，另一种是由接入服务器发起（NAS-initiated）的 VPN 连接。

(3) Extranet VPN（扩展的企业内部虚拟专网）

Extranet VPN 是指利用 VPN 将企业网延伸至供应商、合作伙伴与客户处，使不同企业间通过公网来构筑 VPN。

3. 按组网模型划分

(1) 虚拟租用线（VLL）

VLL（Virtual Leased Line）是对传统租用线业务的仿真，通过使用 IP 网络对租用线进行模拟，提供非对称、低成本的“DDN”业务。从虚拟租用线两端的用户来看，该虚拟租用线近似于过去的租用线。

(2) 虚拟专用拨号网络 (VPDN)

VPDN (Virtual Private Dial Network) 是指利用公共网络 (如 ISDN 和 PSTN) 的拨号功能及接入网来实现虚拟专用网, 从而为企业、小型 ISP、移动办公人员提供接入服务。

(3) 虚拟专用 LAN 网段 (VPLS) 业务

VPLS (Virtual Private LAN Segment) 借助 IP 公共网络实现 LAN 之间通过虚拟专用网段互连, 是局域网在 IP 公共网络上的延伸。

(4) 虚拟专用路由网 (VPRN) 业务

VPRN (Virtual Private Routing Network) 借助 IP 公共网络实现总部、分支机构和远端办公室之间通过网络管理虚拟路由器进行互连, 业务实现包括两类: 一种是使用传统 VPN 协议 (如 IPsec、GRE 等) 实现的 VPRN, 另外一种为 MPLS 方式的 VPRN。

4. 按实现层次划分

(1) L3VPN: 包括 BGP/MPLS VPN、IPsec VPN、GRE VPN、DVPN 等。

(2) L2VPN: 包括 Martini 方式的 MPLS L2VPN、Kompalla 方式的 MPLS L2VPN、SVC 方式 MPLS L2VPN、VPLS 以及静态 CCC 配置。

(3) VPDN: L2TP、PPTP 等。

第2章 L2TP 协议配置

2.1 L2TP 协议简介

2.1.1 VPDN 概述

VPDN (Virtual Private Dial Network, 虚拟私有拨号网) 是指利用公共网络 (如 ISDN 和 PSTN) 的拨号功能及接入网来实现虚拟专用网, 从而为企业、小型 ISP、移动办公人员提供接入服务。

VPDN 采用专用的网络加密通信协议, 在公共网络上为企业建立安全的虚拟专网。企业驻外机构和出差人员可从远程经由公共网络, 通过虚拟加密隧道实现和企业总部之间的网络连接, 而公共网络上其它用户则无法穿过虚拟隧道访问企业网内部的资源。

VPDN 有下列两种实现方式:

- (1) NAS 通过隧道协议, 与 VPDN 网关建立通道的方式。这种方式将客户的 PPP 连接直接连到企业的网关上, 目前可使用的协议有 L2F 与 L2TP。其好处在于: 对用户是透明的, 用户只需要登录一次就可以接入企业网络, 由企业网进行用户认证和地址分配, 而不占用公共地址, 用户可使用各种平台上网。这种方式需要 NAS 支持 VPDN 协议, 需要认证系统支持 VPDN 属性, 网关一般使用路由器或 VPN 专用服务器。
- (2) 客户机与 VPDN 网关建立隧道的方式。这种方式由客户机先建立与 Internet 的连接, 再通过专用的客户软件 (如 Win2000 支持的 L2TP 客户端) 与网关建立通道连接。其好处在于: 用户上网的方式和地点没有限制, 不需 ISP 介入。缺点是: 用户需要安装专用的软件。

VPDN 隧道协议可分为 PPTP、L2F 和 L2TP 三种, 目前使用最广泛的是 L2TP。

2.1.2 L2TP 协议介绍

1. 协议背景

PPP 协议定义了一种封装技术, 可以在二层的点到点链路上传输多种协议数据包, 这时, 用户与 NAS 之间运行 PPP 协议, 二层链路端点与 PPP 会话点驻留在相同硬件设备上。

L2TP 协议提供了对 PPP 链路层数据包的通道 (Tunnel) 传输支持, 允许二层链路端点和 PPP 会话点驻留在不同设备上, 并且采用包交换网络技术进行信息交互, 从

而扩展了 PPP 模型。L2TP 协议结合了 L2F 协议和 PPTP 协议的各自优点，成为 IETF 有关二层隧道协议的工业标准。

2. 典型 L2TP 组网应用

使用L2TP协议构建的VPDN应用的典型组网如 图 2-1所示。

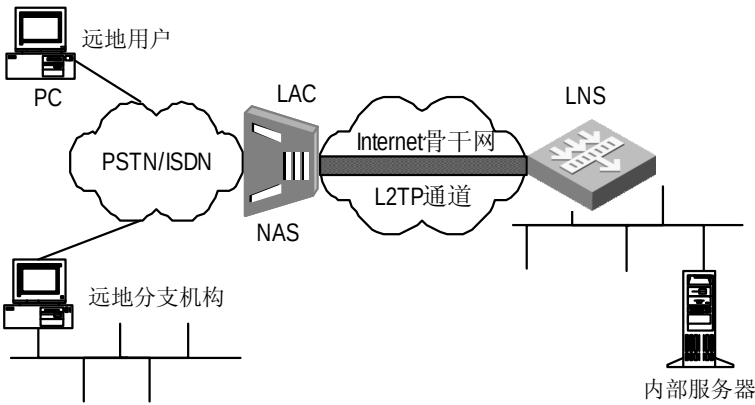


图2-1 应用 L2TP 构建的 VPDN 服务

其中，LAC 表示 L2TP 访问集中器（L2TP Access Concentrator），是附属在交换网络上的具有 PPP 端系统和 L2TP 协议处理能力的设备。LAC 一般是一个网络接入服务器 NAS，主要用于通过 PSTN/ISDN 网络为用户提供接入服务。LNS 表示 L2TP 网络服务器（L2TP Network Server），是 PPP 端系统上用于处理 L2TP 协议服务器端部分的设备。

LAC 位于 LNS 和远端系统（远地用户和远地分支机构）之间，用于在 LNS 和远端系统之间传递信息包，把从远端系统收到的信息包按照 L2TP 协议进行封装并送往 LNS，将从 LNS 收到的信息包进行解封装并送往远端系统。LAC 与远端系统之间可以采用本地连接或 PPP 链路，VPDN 应用中通常为 PPP 链路。LNS 作为 L2TP 隧道的另一侧端点，是 LAC 的对端设备，是被 LAC 进行隧道传输的 PPP 会话的逻辑终止端点。

3. L2TP 协议的技术细节

(1) L2TP 协议结构

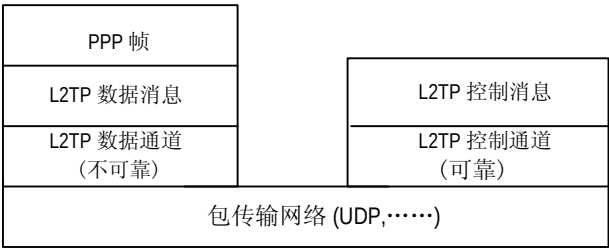


图2-2 L2TP 协议结构

上图所示 L2TP 协议结构描述了 PPP 帧和控制通道以及数据通道之间的关系。PPP 帧在不可靠的 L2TP 数据通道上进行传输，控制消息在可靠的 L2TP 控制通道内传输。

通常 L2TP 数据以 UDP 报文的形式发送。L2TP 注册了 UDP 1701 端口，但是这个端口仅用于初始的隧道建立过程中。L2TP 隧道发起方任选一个空闲的端口（未必是 1701）向接收方的 1701 端口发送报文；接收方收到报文后，也任选一个空闲的端口（未必是 1701），给发送方的指定端口回送报文。至此，双方的端口选定，并在隧道保持连通的时间段内不再改变。

(2) 隧道和会话的概念

在一个 LNS 和 LAC 对之间存在着两种类型的连接，一种是隧道（Tunnel）连接，它定义了一个 LNS 和 LAC 对；另一种是会话（Session）连接，它复用在隧道连接之上，用于表示承载在隧道连接中的每个 PPP 会话过程。在同一对 LAC 和 LNS 之间可以建立多个 L2TP 隧道，隧道由一个控制连接和一个或多个会话（Session）组成。会话连接必须在隧道建立（包括身份保护、L2TP 版本、帧类型、硬件传输类型等信息的交换）成功之后进行，每个会话连接对应于 LAC 和 LNS 之间的一个 PPP 数据流。控制消息和 PPP 数据报文都在隧道上传输。

L2TP 使用 Hello 报文来检测隧道的连通性。LAC 和 LNS 定时向对端发送 Hello 报文，若在一段时间内未收到 Hello 报文的应答，该隧道连接将被断开。

(3) 控制消息和数据消息的概念

L2TP 中存在两种消息：控制消息和数据消息。控制消息用于隧道和会话连接的建立、维护以及传输控制；数据消息则用于封装 PPP 帧并在隧道上传输。控制消息的传输是可靠传输，并且支持对控制消息的流量控制和拥塞控制；而数据消息的传输是不可靠传输，若数据报文丢失，不予重传，不支持对数据消息的流量控制和拥塞控制。

控制消息和数据消息共享相同的报文头。L2TP 报文头中包含隧道标识符（Tunnel ID）和会话标识符（Session ID）信息，用来标识不同的隧道和会话。隧道标识相同、会话标识不同的报文将被复用在一条隧道上，报文头中的隧道标识符与会话标识符由对端分配。

4. 两种典型的 L2TP 隧道模式

远端系统或 LAC 客户端（运行 L2TP 协议的主机）与 LNS 之间的隧道模式如图 2-3 所示：

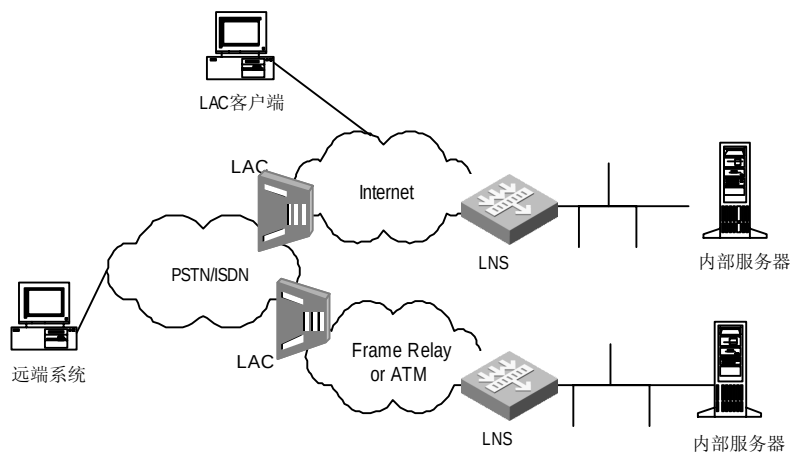


图2-3 两种典型的 L2TP 隧道模式

- (1) 由远程拨号用户发起。远程系统通过 PSTN/ISDN 拨入 LAC，由 LAC 通过 Internet 向 LNS 发起建立通道连接请求。拨号用户地址由 LNS 分配；对远程拨号用户的验证与计费既可由 LAC 侧的代理完成，也可在 LNS 侧完成。
- (2) 直接由 LAC 客户（指可在本地支持 L2TP 协议的用户）发起。LAC 客户拥有公网地址后，可直接向 LNS 发起通道连接请求，无需再经过一个单独的 LAC 设备。此时，LAC 客户的私网地址分配由 LNS 来完成。

5. L2TP 隧道会话的建立过程

L2TP 应用的典型组网如下图所示：

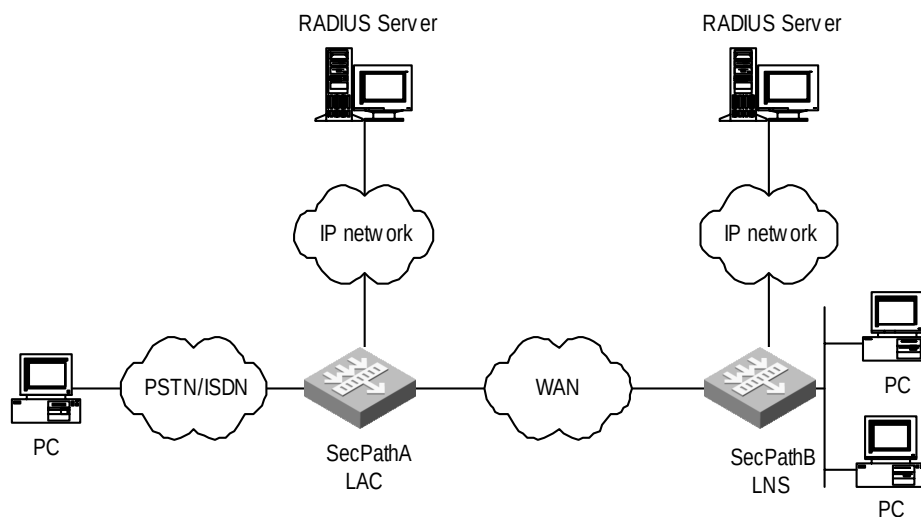


图2-4 L2TP 应用的典型组网

L2TP 隧道的呼叫建立流程可如下图所示：

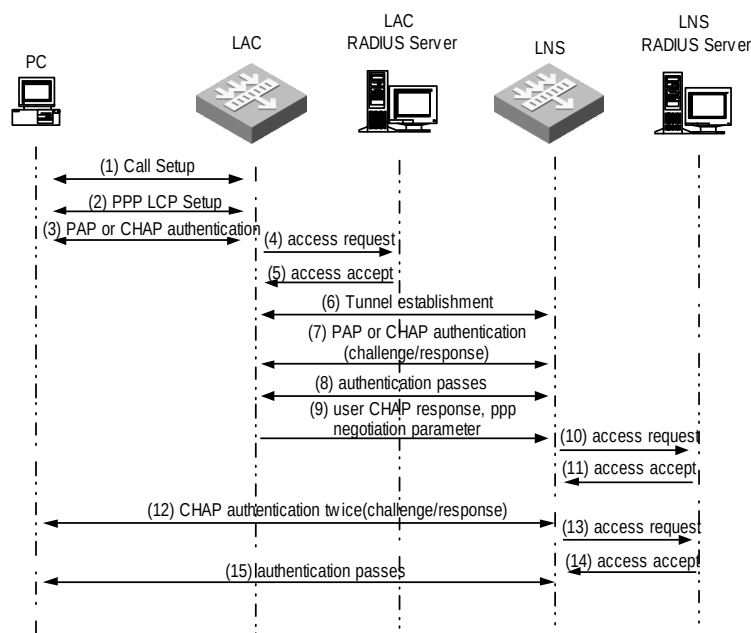


图2-5 L2TP 隧道的呼叫建立流程

L2TP 隧道的呼叫建立流程过程为：

- (1) 用户端 PC 机发起呼叫连接请求；
- (2) PC 机和 LAC 端进行 PPP LCP 协商；
- (3) LAC 对 PC 机提供的用户信息进行 PAP 或 CHAP 认证；
- (4) LAC 将认证信息（用户名、密码）发送给 RADIUS 服务器进行认证；
- (5) RADIUS 服务器认证该用户，如果认证通过则返回该用户对应的 LNS 地址等相关信息，并且 LAC 准备发起 Tunnel 连接请求；
- (6) LAC 端向指定 LNS 发起 Tunnel 连接请求；
- (7) LAC 端向指定 LNS 发送 CHAP challenge 信息，LNS 回送该 challenge 响应消息 CHAP response，并发送 LNS 侧的 CHAP challenge，LAC 返回该 challenge 的响应消息 CHAP response；
- (8) 隧道验证通过；
- (9) LAC 端将用户 CHAP response、response identifier 和 PPP 协商参数传送给 LNS；
- (10) LNS 将接入请求信息发送给 RADIUS 服务器进行认证；
- (11) RADIUS 服务器认证该请求信息，如果认证通过则返回响应信息；
- (12) 若用户在 LNS 侧配置强制本端 CHAP 认证，则 LNS 对用户进行认证，发送 CHAP challenge，用户侧回应 CHAP response；
- (13) LNS 再次将接入请求信息发送给 RADIUS 服务器进行认证；

- (14) RADIUS 服务器认证该请求信息，如果认证通过则返回响应信息；
- (15) 验证通过，用户访问企业内部资源。

6. L2TP 协议的特点

- 灵活的身份验证机制以及高度的安全性

L2TP 协议本身并不提供连接的安全性，但它可依赖于 PPP 提供的认证（比如 CHAP、PAP 等），因此具有 PPP 所具有的所有安全特性。L2TP 可与 IPsec 结合起来实现数据安全，这使得通过 L2TP 所传输的数据更难被攻击。L2TP 还可根据特定的网络安全要求在 L2TP 之上采用通道加密技术、端对端数据加密或应用层数据加密等方案来提高数据的安全性。

- 多协议传输

L2TP 传输 PPP 数据包，这样就可以在 PPP 数据包内封装多种协议。

- 支持 RADIUS 服务器的验证

LAC 端将用户名和密码发往 RADIUS 服务器进行验证申请，RADIUS 服务器负责接收用户的验证请求，完成验证。

- 支持内部地址分配

LNS 可放置于企业网的防火墙之后，它可以对远端用户的地址进行动态的分配和管理，可支持私有地址应用（RFC1918）。为远端用户所分配的地址不是 Internet 地址而是企业内部的私有地址，这样方便了地址的管理并可以增加安全性。

- 网络计费的灵活性

可在 LAC 和 LNS 两处同时计费，即 ISP 处（用于产生帐单）及企业网关（用于付费及审计）。L2TP 能够提供数据传输的出入包数、字节数以及连接的起始、结束时间等计费数据，可根据这些数据方便地进行网络计费。

- 可靠性

L2TP 协议支持备份 LNS，当一个主 LNS 不可达之后，LAC 可以重新与备份 LNS 建立连接，这样，增加了 VPN 服务的可靠性和容错性。

下面从 LAC、LNS 两侧分别介绍 L2TP 的配置。

2.2 LAC 配置

在 L2TP 的配置中，LAC 端和 LNS 端的配置有所不同，下面先介绍一下 LAC 端的配置。在各项配置任务中，必须先启动 L2TP、创建 L2TP 组，然后再进行其它功能特性的配置。PPP 配置相关命令的详细介绍请参看相关章节。

LAC 侧要进行的配置包括：

- 启用 L2TP（必选）
- 创建 L2TP 组（必选）
- 设置发起 L2TP 连接请求及 LNS 地址（必选）
- 设置本端名称（可选）
- 启用通道验证及设置密码（可选）
- 配置将 AVP 数据隐含（可选）
- 设置通道 Hello 报文发送时间间隔（可选）
- 设置用户名、密码及配置用户验证（必选）
- 强制断开 L2TP 连接（可选）
- 开启或关闭流控功能（可选）
- 配置 L2TP 会话超时时间（可选）
- 配置 L2TP Tunnel 连接保持功能（可选）
- 配置 LAC 作为客户端（可选）

2.2.1 启用 L2TP

只有启用 L2TP 后，防火墙上的 L2TP 功能才能正常发挥作用；如果禁止 L2TP，则即便配置了 L2TP 的参数，防火墙也不会提供相关功能。

这些配置在 LAC 侧必须配置。

请在系统视图下进行下列配置。

表2-1 启用/禁止 L2TP

操作	命令
启用 L2TP	l2tp enable
禁止 L2TP	undo l2tp enable

缺省情况下，L2TP 功能是被禁止的。

说明：

当成功建了隧道或者由于验证不成功而导致不能建立隧道时，此时在 LAC 端禁用 L2TP 功能然后再启用 L2TP 功能，若不能建立隧道：

- 对于 LAC 作为客户端的情况，需在 LAC 端的虚拟模板接口下执行 **undo l2tp-auto-client enable**，再执行 **l2tp-auto-client enable**，即可建立隧道。
- 对于 LAC 不作为客户端，即由远程用户发拨入 LAC 的情况，在远程用户端需重新连接以建立隧道。

2.2.2 创建 L2TP 组

为了进行 L2TP 的相关参数配置，还需要增加 L2TP 组，这不仅可以在防火墙上灵活的配置 L2TP 各项功能，而且方便地实现了 LAC 和 LNS 之间一对一、一对多的组网应用。L2TP 组在 LAC 和 LNS 上独立编号，只需要保证 LAC 和 LNS 之间关联的 L2TP 组的相关配置（如接收的通道对端名称、发起 L2TP 连接请求及 LNS 地址等）保持对应关系即可。

这些配置在 LAC 侧必须配置。

请在系统视图下进行下列配置。

表2-2 创建/删除 L2TP 组

操作	命令
创建 L2TP 组	l2tp-group <i>group-number</i>
删除 L2TP 组	undo l2tp-group <i>group-number</i>

在创建 L2TP 组后，就可以在 L2TP 组视图下进行和该 L2TP 组相关的其它配置了，如本端名称、发起 L2TP 连接请求及 LNS 地址等。

缺省情况下，未创建任何 L2TP 组。

2.2.3 设置发起 L2TP 连接请求及 LNS 地址

防火墙需要满足一定的条件才会向其它设备（如防火墙、路由器或 LNS 服务器）发出建立 L2TP 连接的请求。通过配置对接入用户信息的判别条件，并指定相应的 LNS 端的 IP 地址，防火墙可以鉴定用户是否为 VPN 用户，并决定是否向 LNS 发起连接。最多可以设置五个 LNS，即允许存在备用 LNS。正常运行时，防火墙（LAC）按照 LNS 配置的先后顺序，依次向对端（LNS）进行 L2TP 连接请求，直到某个 LNS 接受连接请求，该 LNS 就成为 L2TP 隧道的对端。发起 L2TP 连接请求的触发条件共支持两种：完整的用户名（fullusername）和带特定域名的用户（domain）。

请在 L2TP 组视图下进行下列配置。

表2-3 设置发起 L2TP 连接请求及 LNS 地址

操作	命令
配置鉴别用户是否是 VPN 用户的方式，并设置对应的 LNS 的 IP 地址。	start l2tp { ip <i>ip-addr</i> [ip <i>ip-addr</i>] [ip <i>ip-addr</i>] ... } { domain <i>domain-name</i> fullusername <i>user-name</i> }
取消连接请求配置	undo start

上述参数无缺省值，可根据实际情况进行配置，但必须配置一种触发条件，方可发出 L2TP 连接的请求。

当发起隧道连接请求时，系统先根据完整的用户名查看是否存在根据此用户名指定的 L2TP 组；如果没有找到，再根据域名进行查找。

 说明：

- 当配置多个 LNS 时，因客户端 PPP 的超时时间不同，可能会导致不能与后续几个 IP 地址（备份 LNS）建立连接，故建议最多配置两个 LNS。
- 防火墙可以同时作为 LAC 和 LNS，当既作为 LAC 又作为 LNS 时，必须使用不同的用户名，否则会导致 L2TP 功能异常。

2.2.4 设置本端名称

用户可在 LAC 侧配置本端通道名称。LAC 侧通道名称要与 LNS 侧配置的接收通道对端名称保持一致。

这些配置在 LAC 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-4 设置本端名称

操作	命令
设置本端名称	tunnel name name
恢复本端名称为默认值	undo tunnel name

缺省情况下，本端名称为防火墙的主机名。

 说明：

LNS 根据 LAC 的 tunnel 名来选择其本端的 L2TP 组，如果 tunnel 名相同，LNS 将以第一个符合配置的组建立隧道。所以若要建立多条隧道，需要配置不同的 tunnel 名。

2.2.5 启用隧道验证及设置密码

用户可根据实际需要，决定是否在创建隧道连接之前启用隧道验证。隧道验证请求可由 LAC 或 LNS 任何一侧发起。只要有一方启用了隧道验证，则只有在对端也启用了隧道验证，两端密码完全一致并且不为空的情况下，隧道才能建立；否则本端将自动将隧道连接断开。若隧道两端都配置了禁止隧道验证，隧道验证的密码一致与否将不起作用。

这些配置在 LAC 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-5 设置通道验证及密码

操作	命令
启用隧道验证	tunnel authentication
禁止隧道验证	undo tunnel authentication
设置隧道验证的密码	tunnel password { simple cipher } password
恢复隧道验证的密码为缺省值	undo tunnel password

缺省情况下，启用隧道验证，隧道验证的密码为空。为了保证通道安全，建议用户最好不要禁用隧道验证的功能。

2.2.6 配置将 AVP 数据隐含

L2TP 协议使用 AVP（Attribute Value Pair，属性值对）来传递和协商 L2TP 的一些参数属性等。在缺省情况下，AVP 是采用明文形式传输的。为了保证安全，用户可以通过下面的配置，将这些 AVP 隐藏起来传输。隐含 AVP 功能必须是两端都使用隧道验证的情况下才起作用。

这些配置在 LAC 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-6 配置将 AVP 数据隐含

操作	命令
配置将 AVP 数据隐含的传输方式	tunnel avp-hidden
恢复 AVP 的缺省传输方式	undo tunnel avp-hidden

缺省情况下，AVP 是采用明文形式传输的。

2.2.7 设置通道 Hello 报文发送时间间隔

为了检测 LAC 和 LNS 之间通道的连通性，LAC 和 LNS 会定期向对端发送 Hello 报文，接收方接收到 Hello 报文后会进行响应。当 LAC 或 LNS 在指定时间间隔内未收到对端的 Hello 响应报文时，重复发送，如果重复发送超过 3 次都没有收到对端的响应信息则认为 L2TP 隧道已经断开，需要在 LAC 和 LNS 之间重新建立隧道连接。

这项配置在 LAC 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-7 设置通道 Hello 报文发送时间间隔

操作	命令
设置通道 Hello 报文发送时间间隔	tunnel timer hello <i>hello-interval</i>
恢复通道 Hello 报文发送时间间隔	undo tunnel timer hello

缺省情况下，通道 Hello 报文的发送时间间隔为 60 秒。如果 LAC 侧不进行此项配置，LAC 将采用此缺省值为周期向对端发送 Hello 报文。

2.2.8 设置用户名、密码及配置用户验证

在 LAC 侧配置 AAA 认证时，如果选择了 local（本地认证）方式，则需要在 LAC 侧配置本地用户名和口令。

LAC 通过检查远程拨入用户名与口令是否与本地注册用户名/口令相符合来进行用户身份验证，以检查用户是否为合法 VPN 用户。验证通过后才能发起建立通道连接请求，否则将该用户转入其它类型的服务。

这些配置在 LAC 侧必须配置。

1. 配置用户名、密码

表2-8 配置用户名、密码

操作	命令
设置用户名（系统视图）	local-user <i>username</i>
取消当前设置（系统视图）	undo local-user <i>username</i>
配置本地用户口令（本地用户视图）	password { simple cipher } <i>password</i>

缺省情况下，LAC 侧未配置本地用户名和口令。

2. 配置 PPP 用户验证类型

请在虚拟模板接口视图下进行下列配置。

表2-9 配置/取消用户验证类型

操作	命令
配置对 PPP 用户进行验证	ppp authentication-mode { chap pap } [call-in] [domain <i>isp-name</i>]
取消对 PPP 用户进行验证	undo ppp authentication-mode

缺省情况下，未配置用户验证。配置本地验证的接口应该是接入用户的接口。

3. 配置 PPP 域用户及认证方案

表2-10 配置 PPP 域用户及认证方案

操作	命令
创建 ISP 域并进入域视图（系统视图）	domain { <i>isp-name</i> default { disable enable <i>isp-name</i> } }
删除指定的 ISP 域（系统视图）	undo domain <i>isp-name</i>
配置 PPP 域用户的认证方法（ISP 域视图）	scheme local

2.2.9 强制断开 L2TP 连接

当用户数为零、网络发生故障或当管理员主动要求时，都会产生断开连接的过程。LAC 和 LNS 任何一端都可主动发起断开连接的请求，连接断开后，该通道上的所有控制连接与会话连接也将被清除；当有新用户拨入时，还可重新建立连接。

这些配置在 LAC 端为可选配置。

请在用户视图下进行下列配置。

表2-11 强制断开连接

操作	命令
强制断开一个隧道连接	reset l2tp tunnel { <i>name remote-name</i> <i>id tunnel-id</i> }
强制断开一个会话连接	reset l2tp session <i>session-id</i>
强制断开该用户的连接	reset l2tp user <i>user-name</i>

2.2.10 开启或关闭流控功能

该配置任务可以开启或关闭 L2TP 的通道流控功能，达到流控目的。

这些配置在 LAC 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-12 开启或关闭流控功能

操作	命令
开启流控功能	tunnel flow-control
关闭流控功能	undo tunnel flow-control

缺省情况下，关闭通道流控功能。

2.2.11 配置 L2TP 会话超时时间

通常情况下，当 L2TP 的一个会话在一段时间内没有数据收发时，系统就会自动挂断这个会话。

用户可以根据需要设置会话的超时时间，甚至可以设置永不超时（即不自动挂断）。

请在 L2TP 组视图下进行下列配置。

表2-13 配置 L2TP 会话超时时间

操作	命令
配置 L2TP 会话超时时间	session idle-time seconds
配置 L2TP 会话不超时	undo session idle-time

缺省情况下，L2TP 会话不超时。

2.2.12 配置 L2TP Tunnel 连接保持功能

通常情况下，只有当 PPP 用户发起 L2TP 会话请求之后，LAC 才会与 LNS 建立 tunnel，并且当所有 PPP 会话（session）都断开之后，此 tunnel 也会自动拆除。

对于要求快速建立连接的应用，需要事先建立好 tunnel，一旦有 PPP 会话请求，系统可以立即建立一个会话。这就要求 LAC 与 LNS 之间总是保持一个 tunnel 连接，即使该 tunnel 上没有会话也不会被拆除。

请在 L2TP 组视图下进行下列配置。

表2-14 配置 Tunnel 连接保持功能

操作	命令
配置 Tunnel 连接保持功能	tunnel keepstanding
取消 Tunnel 连接保持功能	undo tunnel keepstanding

缺省情况下，取消 Tunnel 连接保持功能。

说明：

Tunnel 连接保持功能必须在 LAC 和 LNS 上同时配置。

配置好以上条件之后，运行 **start l2tp tunnel** 命令，以发送 tunnel 连接请求。每执行一次该命令，则发送一次连接请求。

请在 L2TP 组视图下执行下列命令。

表2-15 启动 tunnel 连接

操作	命令
启动 tunnel 连接	start l2tp tunnel

2.2.13 配置 LAC 作为客户端

通常情况下，L2TP 的客户端是拨号连接到 LAC 的用户主机。此时用户与 LAC 的连接总是 PPP 连接。

如果使用 LAC 同时作为客户端，那么用户与 LAC 之间的连接就不受限于 PPP 连接，而只要是一个 IP 连接就可以了，这样 LAC 能够将用户的 IP 报文转发到 LNS。

使用 LAC 同时作为客户端，是在 LAC 上建立一个虚拟的 PPP 用户，该用户与 LNS 保持一个常连接。其它所有实际用户的 IP 报文都是通过此虚拟用户转发给 LNS 的。

使用 LAC 同时作为客户端的配置是在配置 LAC 的基础上增加如下配置：

- 创建一个虚模板接口
- 配置虚模板接口参数，包括 IP 地址、PPP 验证方法及 PPP 验证的用户名、密码。
- 配置虚用户建立 L2TP 隧道

说明：

配置 LAC 作为客户端应同时配置 L2TP Session 不超时，否则当没有实际用户数据流时，虚拟用户的会话会因超时而挂断。

1. 创建虚拟模板接口

请在系统视图下进行下列配置。

表2-16 创建/删除虚拟模板接口

操作	命令
创建虚拟模板接口	interface virtual-template <i>virtual-template-number</i>
删除虚拟模板接口	undo interface virtual-template <i>virtual-template-number</i>

2. 配置虚拟模板接口参数

请在虚拟模板接口视图下进行下列配置。

表2-17 配置虚拟模板接口参数

操作	命令
配置虚拟模板接口 IP 地址	ip address { <i>address mask</i> ppp-negotiate unnumbered interface interface-type interface-number }
配置 PPP 验证方式	ppp authentication-mode { pap chap }
配置 CHAP 验证用户名	ppp chap user <i>user-name</i>
配置 CHAP 验证密码	ppp chap password { simple cipher } <i>password</i>
配置 PAP 验证用户名、密码	ppp pap local-user <i>user-name</i> password { simple cipher } <i>password</i>

3. 配置虚用户建立 L2TP 隧道

请在虚拟模板接口视图下进行下列配置。

表2-18 配置虚用户建立 L2TP 隧道

操作	命令
配置虚用户建立 L2TP 隧道	l2tp-auto-client enable
取消虚用户建立 L2TP 隧道	undo l2tp-auto-client enable

缺省情况下，未配置虚用户建立 L2TP 隧道。

2.3 LNS 配置

在 LNS 的各项配置任务中，必须先启动 L2TP、创建 L2TP 组，然后再进行其它功能特性的配置。PPP 和虚拟模板接口（Virtual-Template）的相关命令的详细介绍，请参看相关章节。

LNS 主要配置包括：

- 启用 L2TP（必选）
- 启用/禁止 L2TP 多域功能（可选）
- 创建 L2TP 组（必选）
- 创建虚接口模板（必选）
- 设置接收呼叫的虚拟模板接口、通道对端名称和域名（必选）
- 设置本端名称(可选)
- 配置隧道验证及设置密码(可选)
- 配置将 AVP 数据隐含(可选)
- 设置通道 Hello 报文发送时间间隔(可选)

- 强制本端 CHAP 验证(可选)
- 强制 LCP 重新协商(可选)
- 设置本端地址(必选)及分配的地址池(可选)
- 设置用户名、密码及配置用户验证(可选)
- 强制挂断通道(可选)
- 开启或关闭流控功能(可选)
- 配置 L2TP 会话超时时间（可选）

2.3.1 启用 L2TP

只有启用 L2TP 后，防火墙上的 L2TP 功能才能正常发挥作用；如果禁止 L2TP，则即便配置了 L2TP 的参数，防火墙也不会提供相关功能。

这些配置在 LNS 侧必须配置。

请在系统视图下进行下列配置。

表2-19 启用/禁止 L2TP

操作	命令
启用 L2TP	l2tp enable
禁止 L2TP	undo l2tp enable

缺省情况下，L2TP 功能是被禁止的。

2.3.2 启用/禁止 L2TP 多域功能

只有启用L2TP多域功能，防火墙才能为多个企业做LNS，L2TP多域功能的实现丰富了VPN组网方式。在“2.5.3 L2TP多域组网应用”中有简单配置步骤描述。

在 L2TP 多域应用中，这些配置在 LNS 侧必须配置。

请在系统视图下进行下列配置。

表2-20 启用/禁止 L2TP 多域功能

操作	命令
启用 L2TP 多域功能	l2tpmoreexam enable
禁止 L2TP 多域功能	undo l2tpmoreexam enable

缺省情况下，L2TP 多域功能是被禁止的。

2.3.3 创建 L2TP 组

为了进行 L2TP 的相关参数配置，还需要增加 L2TP 组，这不仅可以在防火墙上灵活的配置 L2TP 各项功能，而且方便地实现了 LAC 和 LNS 之间一对一、一对多的组网应用。L2TP 组在 LAC 和 LNS 上独立编号，只需要保证 LAC 和 LNS 之间关联的 L2TP 组的相关配置（如接收的通道对端名称、发起 L2TP 连接请求及 LNS 地址等）保持对应关系即可。

这些配置在 LNS 侧必须配置。

请在系统视图下进行下列配置。

表2-21 创建/删除 L2TP 组

操作	命令
创建 L2TP 组	l2tp-group <i>group-number</i>
删除 L2TP 组	undo l2tp-group <i>group-number</i>

在创建了 L2TP 组后，就可以在 L2TP 组视图下进行和该 L2TP 组相关的其它配置了，如本端名称、接收的通道对端名称等。

缺省情况下，未创建任何 L2TP 组。

2.3.4 创建虚拟模板接口

虚拟模板接口主要用于配置防火墙在运行过程中动态创建的虚接口的工作参数。

这些配置在 LNS 侧必须配置。

请在系统视图下进行下列配置。

表2-22 创建/删除虚接口模板

操作	命令
创建虚接口模板	interface virtual-template <i>virtual-template-number</i>
删除虚接口模板	undo interface virtual-template <i>virtual-template-number</i>

缺省情况下，未创建虚拟模板接口。

说明：

若虚拟模板接口下配置了地址借用，并且被借用的接口被某个业务占用，将会导致该接口下的 L2TP 功能异常。

2.3.5 设置接收呼叫的虚拟模板接口、通道对端名称和域名

LNS 可以使用不同的虚拟模板接口接收不同的 LAC 创建隧道的请求。在接收到 LAC 发来的创建隧道请求后，LNS 需要检查 LAC 的名称是否与合法通道对端名称相符合，从而决定是否允许通道对方进行隧道的创建。

这些配置在 LNS 侧必须配置。

请在 L2TP 组视图下进行下列配置。

表2-23 设置/取消接收的通道对端名称

操作	命令
设置通道对端的名称（L2TP 组不为 1）	allow l2tp virtual-template <i>virtual-template-number remote</i> <i>remote-name [domain domain-name]</i>
设置通道对端的名称（L2TP 组为 1）	allow l2tp virtual-template <i>virtual-template-number [remote</i> <i>remote-name] [domain domain-name]</i>
取消通道对端的名称	undo allow

当 L2TP 组号为 1 时（缺省的 L2TP 组号），可以不指定通道对端名 *remote-name*。如果在 L2TP 组 1 的视图下，仍指定对端名称，则 L2TP 组 1 不作为缺省的 L2TP 组。

说明：

- 只有组号为 1 的 L2TP 组才可以设置成缺省的组。
- 当 L2TP 组号为 1 时（缺省的 L2TP 组号），任何名称的设备都能发起隧道请求。
- “start”命令和“allow”命令是互斥的，配了一条命令之后另一条就自动失效。
- 当使用 PPPoE Client 触发 LAC 到 LNS 的隧道连接时，建议将 LNS 侧的虚拟模板接口的 MTU 值设置减小到 1480 字节。
- 防火墙可以同时作为 LAC 和 LNS，当既作为 LAC 又作为 LNS 时，必须使用不同的用户名，否则会导致 L2TP 功能异常。

2.3.6 设置本端名称

用户可在 LNS 侧配置本端通道名称。

这些配置在 LNS 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-24 设置本端名称

操作	命令
设置本端名称	tunnel name <i>name</i>
恢复本端名称为默认值	undo tunnel name

缺省情况下，本端名称为防火墙的主机名。

2.3.7 启用隧道验证及设置密码

用户可根据实际需要决定是否在创建隧道连接之前启用隧道验证。隧道验证请求可由 LAC 或 LNS 任何一侧发起。只要有一方启用了隧道验证，则只有在对端也启用了隧道验证，两端密码完全一致并且不为空的情况下，隧道才能建立；否则本端将自动将隧道连接断开。若隧道两端都配置了禁止隧道验证，隧道验证的密码一致与否将不起作用。

这些配置在 LNS 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-25 设置通道验证及密码

操作	命令
启用通道验证	tunnel authentication
禁止通道验证	undo tunnel authentication
设置通道验证的密码	tunnel password { simple cipher } <i>password</i>
取消通道验证的密码	undo tunnel password

缺省情况下，启用隧道验证，隧道验证的密码为空。为了保证通道安全，建议用户最好不要禁用隧道验证的功能。

2.3.8 配置将 AVP 数据隐含

L2TP 协议使用 AVP（Attribute Value Pair，属性值对）来传递和协商 L2TP 的一些参数属性等。在缺省情况下，AVP 是采用明文形式传输的。为了保证安全，用户可以通过下面的配置，将这些 AVP 隐藏起来传输。隐含 AVP 功能必须是两端都使用隧道验证的情况下才起作用。

这些配置在 LNS 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-26 配置将 AVP 数据隐含

操作	命令
配置将 AVP 数据隐含的传输方式	tunnel avp-hidden
恢复 AVP 的缺省传输方式	undo tunnel avp-hidden

缺省情况下，AVP 是采用明文形式传输的。

2.3.9 设置通道 Hello 报文发送时间间隔

为了检测 LAC 和 LNS 之间通道的连通性，LAC 和 LNS 会定期向对端发送 Hello 报文，接收方接收到 Hello 报文后会进行响应。当 LAC 或 LNS 在指定时间间隔内未收到对端的 Hello 响应报文时，重复发送，如果重复发送超过 3 次都没有收到对端的响应信息则认为 L2TP 隧道已经断开，需要在 LAC 和 LNS 之间重新建立隧道连接。

这些配置在 LNS 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-27 设置通道 Hello 报文发送时间间隔

操作	命令
设置通道 Hello 报文发送时间间隔	tunnel timer hello <i>hello-interval</i>
恢复通道 Hello 报文发送时间间隔	undo tunnel timer hello

缺省情况下，通道 Hello 报文的发送时间间隔为 60 秒。如果用户不进行此项配置，LNS 将采用此缺省值为周期向对端发送 Hello 报文。

2.3.10 强制本端 CHAP 验证

当 LAC 对用户进行代理验证后，LNS 可再次对用户进行验证。此时将对用户进行两次验证，第一次发生在 LAC 侧，第二次发生在 LNS 侧，只有两次验证全部成功后，L2TP 通道才能建立。

在 L2TP 组网中，LNS 侧对用户的验证方式有三种：代理验证、强制 CHAP 验证和 LCP 重协商。

这三种验证方式中，LCP 重协商的优先级最高，如果在 LNS 上同时配置 LCP 重协商和强制 CHAP 验证，L2TP 将使用 LCP 重协商，采用相应的虚拟模板接口上配置的验证方式。

如果只配置强制 CHAP 验证，则 LNS 对用户进行 CHAP 验证。强制 CHAP 验证配置在 LNS 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-28 强制本端 CHAP 验证

操作	命令
强制本端 CHAP 验证	mandatory-chap
取消本端 CHAP 验证	undo mandatory-chap

如果既不配置 LCP 重协商，也不配置强制 CHAP 验证，则 LNS 对用户进行的是代理验证。在这种情况下，LAC 将它从用户得到的所有验证信息及 LAC 端本身配置的验证方式发送给 LNS，如果虚拟模板接口未配置验证方式，LNS 侧会默认通过 LAC 侧对用户的验证结果。

在 LNS 使用代理验证时，如果虚拟模板接口配置的验证方式为 PAP，并且验证通过，则允许建立会话。如果虚拟模板接口配置的验证方式为 CHAP，而 LAC 端配置的验证方式为 PAP，则由于 LNS 要求的 CHAP 验证级别高于 LAC 能够提供的 PAP 验证，验证将无法通过，会话也就不能正确建立。

缺省情况下，不进行强制 CHAP 验证。

2.3.11 强制 LCP 重新协商

对由 NAS 发起的 VPN 服务请求（NAS-Initialized VPN），在 PPP 会话开始时，用户先和 NAS（网络接入服务器）进行 PPP 协商。若协商通过，则由 NAS 初始化 L2TP 通道连接，并将用户信息传递给 LNS，由 LNS 根据收到的代理验证信息，判断用户是否合法。

但在某些特定的情况下（如需在 LNS 侧也要进行验证与计费），需要强制 LNS 与用户间重新进行 LCP 协商，此时将忽略 NAS 侧的代理验证信息。

强制 LCP 重新协商配置在 LNS 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-29 强制/取消 LCP 重新协商

操作	命令
强制 LCP 重新协商	mandatory-lcp
取消 LCP 重新协商	undo mandatory-lcp

缺省情况下，不进行 LCP 重新协商。

启用 LCP 重协商后，如果相应的虚拟模板接口上不配置验证，则 LNS 将不对接入用户进行二次验证（这时用户只在 LAC 侧接受一次验证），直接将全局地址池的地址给 client 端。

2.3.12 设置本端地址及分配的地址池

当 LAC 与 LNS 之间的 L2TP 隧道连接建立之后，LNS 需要从地址池中为 VPN 用户分配 IP 地址。在指定地址池之前，需要在系统视图或域视图下用 **ip pool** 命令先定义一个地址池（关于 **ip pool** 命令的详细描述请参见本手册的“安全”部分）。若 LNS 采用代理验证或强制 CHAP 验证，系统将使用域视图下的地址池给用户分配 IP 地址；若 LNS 采用 LCP 重新协商方式并进行验证时，系统将使用域地址池给用户分配 IP 地址；若 LNS 采用 LCP 重新协商方式并不对用户进行验证时，系统将使用全局地址池给用户分配 IP 地址。

配置本端在 LNS 侧为必选配置，分配的地址池配置为可选配置。

请在虚拟模板接口视图下进行下列配置。

表2-30 设置本端地址及分配的地址池

操作	命令
设置本端 IP 地址	ip address X.X.X.X netmask
取消本端 IP 地址	undo ip address X.X.X.X netmask
指定给对方分配地址所用的地址池	remote address { pool pool-number X.X.X.X }
删除给对方分配地址所用的地址池	undo remote address

当为对方指定分配地址所用的地址池时，如果关键字 **pool** 后面没有输入具体的 **pool-number** 值，则表示从缺省地址池来分配地址。

缺省情况下，从地址池 0（缺省地址池）中给对方分配地址。

2.3.13 设置用户名、密码及配置用户验证

在 LNS 侧，如果配置了强制 CHAP 认证，则需要在 LNS 侧配置本地注册用户名和口令。

LNS 通过检查远程拨入用户名与口令是否与本地注册用户名/口令相符合来进行用户身份验证，以检查用户是否为合法 VPN 用户。验证通过后就可以进行 VPN 用户和 LNS 的通信，否则将通知 L2TP 清除这个 L2TP 连接。

这些配置在 LNS 侧为可选配置。具体配置方法请参考 2.2.8 设置用户名、密码及配置用户验证。

2.3.14 强制断开 L2TP 连接

当用户数为零、网络发生故障或当管理员主动要求时，都会产生断开连接的过程。LAC 和 LNS 任何一端都可主动发起断开连接的请求，连接断开后，该通道上的所有控制连接与会话连接也将被清除；当有新用户拨入时，还可重新建立连接。

这些配置在 LNS 端为可选配置。

请在用户视图下进行下列配置。

表2-31 强制断开连接

操作	命令
强制断开一个隧道连接	reset l2tp tunnel { name <i>remote-name</i> id <i>tunnel-id</i> }
强制断开一个会话连接	reset l2tp session <i>session-id</i>
强制断开该用户的连接	reset l2tp user <i>user-name</i>

2.3.15 开启或关闭流控功能

该配置任务可以开启或关闭 L2TP 简单的通道流控功能，达到流控目的。

这些配置在 LNS 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-32 开启或关闭流控功能

操作	命令
开启流控功能	tunnel flow-control
关闭流控功能	undo tunnel flow-control

缺省情况下，关闭通道流控功能。

2.3.16 配置 L2TP 会话超时时间

通常情况下，当 L2TP 的一个会话在一段时间内没有数据收发时，系统就会自动挂断这个会话。

用户可以根据需要设置会话的超时时间，甚至可以设置永不超时（即不自动挂断）。

请在 L2TP 组视图下进行下列配置。

表2-33 配置 L2TP 会话超时时间

操作	命令
配置 L2TP 会话超时时间	session idle-time <i>seconds</i>
配置 L2TP 会话不超时	undo session idle-time

缺省情况下，L2TP 会话不超时。

2.3.17 配置 L2TP 支持 EAD

PPP 用户通过接入认证后，EAD（Endpoint Admission Defense，端点准入防御）服务器将对其进行安全认证。如果认证通过，用户可以正常访问网络资源，如果认证不通过，用户则只能访问隔离区的资源。

表2-34 配置 L2TP 支持 EAD

配置步骤	命令	说明
进入 VT（虚拟模板）接口视图	interface virtual-template number	-
配置开启 PPP 访问控制功能	ppp access-control enable	必选 缺省情况下，关闭 PPP 的访问控制功能
设置 VT 接口下 PPP 用户的包过滤防火墙的分片匹配模式	ppp access-control match-fragments { normally exactly }	可选 缺省情况下，分片匹配模式为 normally
显示 VT 接口下 PPP 用户的访问控制统计信息	display ppp access-control { interface type number }	-

2.4 L2TP 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 L2TP 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **debugging** 命令可对 L2TP 进行调试。

表2-35 L2TP 的显示和调试

操作	命令
显示当前的 L2TP 用户的信息	display l2tp user
显示当前的 L2TP 通道的信息	display l2tp tunnel
显示当前的 L2TP 会话的信息	display l2tp session
打开所有的 L2TP 调试信息开关	debugging l2tp all
关闭所有的 L2TP 调试信息开关	undo debugging l2tp all
打开 L2TP 控制报文调试开关	debugging l2tp control
关闭 L2TP 控制报文调试开关	undo debugging l2tp control
打开 PPP 报文内容的调试开关	debugging l2tp dump
关闭 PPP 报文内容的调试开关	undo debugging l2tp dump
打开 L2TP 错误信息的调试开关	debugging l2tp error

操作	命令
关闭 L2TP 错误信息的调试开关	undo debugging l2tp error
打开 L2TP 的事件调试信息开关	debugging l2tp event
关闭 L2TP 的事件调试信息开关	undo debugging l2tp event
打开隐藏 AVP 的调试信息开关	debugging l2tp hidden
关闭隐藏 AVP 的调试信息开关	undo debugging l2tp hidden
打开 L2TP 数据报文调试开关	debugging l2tp payload
关闭 L2TP 数据报文调试开关	undo debugging l2tp payload
打开 L2TP 时间戳信息调试开关	debugging l2tp time-stamp
关闭 L2TP 时间戳信息调试开关	undo debugging l2tp timestamp

2.5 L2TP 典型配置举例

L2TP 的呼叫可以由 NAS（网络接入服务器）主动发起，也可以由客户端发起。下面将分别针对这两种情况举例说明。

2.5.1 NAS-Initialized VPN

1. 组网需求

VPN 用户访问公司总部过程如下：

- 用户以普通的上网方式进行拨号上网。
- 在接入服务器（NAS）处对此用户进行验证，发现是 VPN 用户，则由接入服务器向 LNS 发起隧道连接请求。
- 在接入服务器与 LNS 隧道建立后，接入服务器把与 VPN 用户已经协商的内容作为报文内容传给 LNS。
- LNS 再根据预协商的内容决定是否接受此连接。
- 用户与公司总部间的通信都通过接入服务器与 LNS 之间的隧道进行传输。

2. 组网图

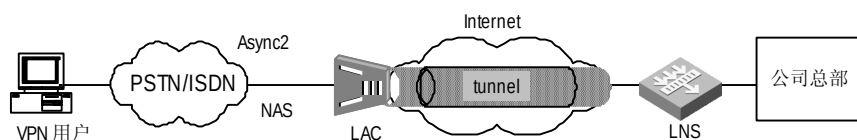


图2-6 NAS-Initialized VPN 组网图

3. 配置步骤

(1) 用户侧的配置

在用户侧，在拨号网络窗口中输入 VPN 用户名 `vpdnuser`，口令 `Hello`，拨入号码为 170。在拨号后弹出的拨号终端窗口中输入 RADIUS 验证的用户名 `username` 和口令 `userpass`。

(2) NAS 侧的配置

在 NAS 上配置拨入号码为 170。

在 RADIUS 服务器上设置一个用户名为 `username`、口令为 `userpass` 的 VPN 用户，并设置相应的 LNS 侧设备的 IP 地址（本例中 LNS 侧与通道相连接的以太口的 IP 地址为 202.38.160.2）。

将本端的设备名称定义为 LAC，需要进行通道验证，通道验证密码为 `tunnelpwd`。

(3) 防火墙（LNS 侧）的配置

设置用户名及口令（应与用户侧的设置一致）。

```
[H3C] local-user vpdnuser
```

```
[H3C-luser-vpdnuser] password simple Hello
```

```
[H3C-luser-vpdnuser] service-type ppp
```

对 VPN 用户采用本地验证。

```
[H3C] domain system
```

```
[H3C-isp-system] scheme local
```

```
[H3C-isp-system] ip pool 1 192.168.0.2 192.168.0.100
```

启用 L2TP 服务，并设置一个 L2TP 组。

```
[H3C] l2tp enable
```

```
[H3C] l2tp-group 1
```

配置虚模板 Virtual-Template 的相关信息。

```
[H3C] interface virtual-template 1
```

```
[H3C-virtual-template1] ip address 192.168.0.1 255.255.255.0
```

```
[H3C-virtual-template1] ppp authentication-mode chap domain system
```

```
[H3C-virtual-template1] remote address pool 1
```

配置 LNS 侧接收的通道对端名称。

```
[H3C] l2tp-group 1
```

```
[H3C-l2tp1] allow l2tp virtual-template 1 remote LAC
```

启用通道验证并设置通道验证密码。

```
[H3C-l2tp1] tunnel authentication
```

```
[H3C-l2tp1] tunnel password simple tunnelpwd
```

2.5.2 Client-Initialized VPN

1. 组网需求

VPN 用户访问公司总部过程如下：

用户首先连接 Internet，之后，直接由用户向 LNS 发起 Tunnel 连接的请求。

在 LNS 接受此连接请求之后，VPN 用户与 LNS 之间就建立了一条虚拟的 Tunnel。

用户与公司总部间的通信都通过 VPN 用户与 LNS 之间的 Tunnel 进行传输。

2. 组网图

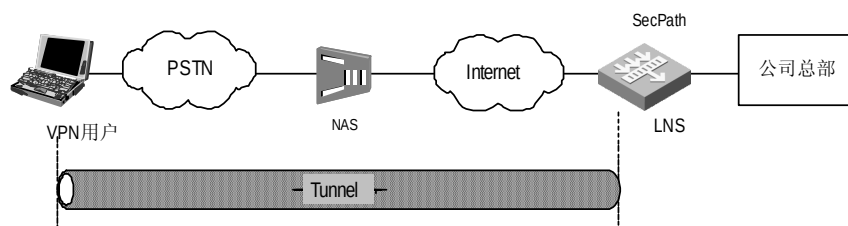


图2-7 Client-Initialized VPN 组网图

3. 配置步骤

(1) 用户侧的配置

在用户侧主机上必须装有 L2TP 的客户端软件，如 WinVPN Client，并且用户通过拨号方式连接到 Internet。然后再进行如下配置（设置的过程与相应的客户端软件有关，以下为设置的内容）：

在用户侧设置 VPN 用户名为 vpdnuser，口令为 Hello。

将 LNS 的 IP 地址设为防火墙的 Internet 接口地址（本例中 LNS 侧与通道相连接的以太口的 IP 地址为 202.38.160.2）。

修改连接属性，将采用的协议设置为 L2TP，将加密属性设为自定义，并选择 CHAP 验证，进行通道验证，通道的密码为：tunnelpwd。

(2) 防火墙（LNS 侧）的配置

设置用户名及口令（应与用户侧的设置一致）。

```
[H3C] local-user vpdnuser
[H3C-luser-vpdnuser] password simple Hello
[H3C-luser-vpdnuser] service-type ppp

# 对 VPN 用户采用本地验证。

[H3C] domain system
[H3C-isp-system] scheme local
[H3C-isp-system] ip pool 1 192.168.0.2 192.168.0.100

# 启用 L2TP 服务，并设置一个 L2TP 组。
```

```
[H3C] l2tp enable
[H3C] l2tp-group 1
# 配置虚模板 Virtual-Template 的相关信息。

[H3C] interface virtual-template 1
[H3C-virtual-template1] ip address 192.168.0.1 255.255.255.0
[H3C-virtual-template1] ppp authentication-mode chap domain system
[H3C-virtual-template1] remote address pool 1
# 配置 LNS 侧接收的通道对端名称。

[H3C] l2tp-group 1
[H3C-l2tp1] allow l2tp virtual-template 1
# 启用通道验证并设置通道验证密码。

[H3C-l2tp1] tunnel authentication
[H3C-l2tp1] tunnel password simple tunnelpwd
```

2.5.3 L2TP 多域组网应用

1. 组网需求

企业中拥有两个域，PC1 为企业中 263.net 域的用户，PC2 为企业中 163.net 域的用户。一般情况下，用户无法通过 Internet 直接访问企业内部的网络。通过建立 VPN 并支持多域，不同域的用户将从 LNS 获得不同范围的地址，并可以访问企业内部网络。

2. 组网图

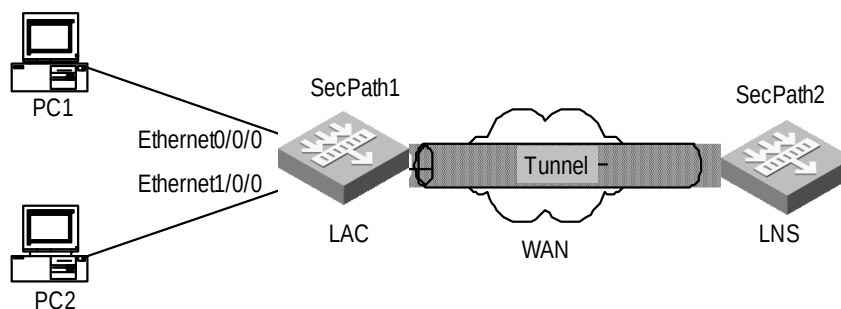


图2-8 L2TP 支持多域组网图

3. 配置步骤

(1) 用户侧的配置

建一拨号网络，接收由 LNS 服务器端分配的地址。

对于 PC1 而言，在弹出的拨号终端窗口中输入用户名 vpdn1@263.net，口令为 11111（此用户名与口令已在 LNS 中注册）。

对于 PC2 而言, 在弹出的拨号终端窗口中输入用户名 vpdn2@163.net, 口令为 22222 (此用户名与口令已在 LNS 中注册)。

(2) SecPath1 (LAC 侧) 的配置

(本例中 LAC 侧的 Ethernet0/0/0 和 Ethernet1/0/0 是用户接入接口, Ethernet0/0/1 的 IP 地址为 202.38.160.1, LNS 侧与通道相连接的 IP 地址为 202.38.160.2)。

设置用户名及口令。

```
<H3C> system-view
[H3C] local-user vpdn1
[H3C-luser-vpdn1] password simple 11111
[H3C-luser-vpdn1] service-type ppp
[H3C-luser-vpdn1] quit
[H3C] local-user vpdn2
[H3C-luser-vpdn2] password simple 22222
[H3C-luser-vpdn2] service-type ppp
[H3C-luser-vpdn2] quit
```

配置域用户采用本地认证。

```
[H3C] domain 263.net
[H3C-isp-263.net] scheme local
[H3C-isp-263.net] quit
[H3C] domain 163.net
[H3C-isp-163.net] scheme local
[H3C-isp-163.net] quit
```

在 Ethernet0/0/0 和 Ethernet1/0/0 接口上配置 PPPoE server。

```
[H3C] interface Ethernet0/0/0
[H3C-Ethernet0/0/0] pppoe-server bind Virtual-Template 100
[H3C-Ethernet0/0/0] interface Ethernet1/0/0
[H3C-Ethernet1/0/0] pppoe-server bind Virtual-Template 101
```

在 Ethernet0/0/1 接口上配置 IP 地址。

```
[H3C-Ethernet0/0/0] interface Ethernet0/0/1
[H3C-Ethernet0/0/1] ip address 202.38.160.1 255.255.255.0
```

在虚模板上启动 CHAP 认证。

```
[H3C-Ethernet0/0/1] interface Virtual-Template 100
[H3C-Virtual-Template100] ppp authentication-mode chap domain 263.net
[H3C-Virtual-Template100] interface Virtual-Template 101
[H3C-Virtual-Template101] ppp authentication-mode chap domain 163.net
[H3C-Virtual-Template101] quit
```

设置两个 L2TP 组并配置相关属性。

```
[H3C] l2tp enable
```

```
[H3C] l2tp-group 1
[H3C-l2tp1] tunnel name LAC
[H3C-l2tp1] start l2tp ip 202.38.160.2 domain 263.net
[H3C-l2tp1] l2tp-group 2
[H3C-l2tp2] tunnel name LAC
[H3C-l2tp2] start l2tp ip 202.38.160.2 domain 163.net
```

启用通道验证并设置通道验证密码。

```
[H3C-l2tp2] tunnel authentication
[H3C-l2tp2] tunnel password simple 12345
[H3C-l2tp2] quit
[H3C] l2tp-group 1
[H3C-l2tp1] tunnel authentication
[H3C-l2tp1] tunnel password simple 12345
```

(3) SecPath2 (LNS 侧) 的配置。

```
<H3C> system-view
[H3C] l2tp enable
[H3C] l2tpmoreexam enable
```

创建两个用户名及口令

```
[H3C] local-user vpdn1
[H3C-luser-vpdn1] password simple 11111
[H3C-luser-vpdn1] service-type ppp
[H3C-luser-vpdn1] quit
[H3C] local-user vpdn2
[H3C-luser-vpdn2] password simple 22222
[H3C-luser-vpdn2] service-type ppp
[H3C-luser-vpdn2] quit
```

创建两个地址池。

```
[H3C] domain 163.net
[H3C-isp-163.net] scheme local
[H3C-isp-163.net] ip pool 1 202.38.161.10 202.38.161.100
[H3C-isp-163.net] quit
[H3C] domain 263.net
[H3C-isp-263.net] scheme local
[H3C-isp-263.net] ip pool 1 202.38.162.10 202.38.162.100
[H3C-isp-263.net] quit
```

创建两个相应的 virtual template。

```
[H3C] interface virtual-template 1
[H3C-Virtual-Template1] ip address 202.38.161.1 255.255.255.0
[H3C-Virtual-Template1] remote address pool 1
[H3C-Virtual-Template1] ppp authentication-mode chap domain 163.net
```

```
[H3C-Virtual-Template1] interface virtual-template 2
[H3C-Virtual-Template2] ip address 202.38.162.2 255.255.255.0
[H3C-Virtual-Template2] remote address pool 1
[H3C-Virtual-Template2] ppp authentication-mode chap domain 263.net
[H3C-Virtual-Template2] quit
```

创建两个相应的 L2TP-group 组。

```
[H3C] l2tp-group 3
[H3C-l2tp3] tunnel authentication
[H3C-l2tp3] allow l2tp virtual-template 1 remote LAC domain 163.net
[H3C-l2tp3] tunnel password simple 12345
[H3C-l2tp3] quit
[H3C] l2tp-group 4
[H3C-l2tp4] tunnel authentication
[H3C-l2tp4] allow l2tp virtual-template 2 remote LAC domain 263.net
[H3C-l2tp4] tunnel password simple 12345
```

上述配置中，如果 LNS 端需要采用 RADIUS 验证，请修改 AAA 配置即可。

2.5.4 LAC 作为客户端典型应用

1. 组网需求

LAC 同时作为 L2TP 客户端，与 LNS 建立常连接。并将所有私有网络的数据转发给 LNS。

2. 组网图

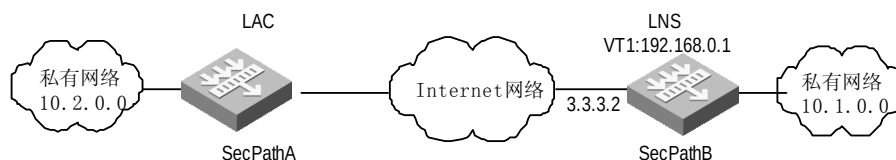


图2-9 LAC 作为客户端应用组网图

3. 配置步骤

说明：

本例假设公网地址和路由都已正确配置。此处只说明了 VPN 相关配置。

(1) LAC 的典型配置

设置用户名及口令。

```
[H3C] local-user vpdnuser
```

```
[H3C-luser-vpdnuser] password simple Hello
[H3C-luser-vpdnuser] service-type ppp
[H3C-luser-vpdnuser] quit
# 启用 L2TP 服务，并设置一个 L2TP 组。

[H3C] l2tp enable
[H3C] l2tp-group 1
# 配置 LAC 侧本端名称，配置对端 LNS 的 IP 地址。

[H3C-l2tp1] tunnel name LAC
[H3C-l2tp1] start l2tp ip 3.3.3.2 fullusername vpdnuser
# 启用通道验证并设置通道验证密码。

[H3C-l2tp1] tunnel authentication
[H3C-l2tp1] tunnel password simple tunnelpwd
[H3C-l2tp1] quit
# 配置虚模板 Virtual-Template 的相关信息。

[H3C] interface virtual-template 1
[H3C-virtual-template1] ip address ppp-negotiate
[H3C-virtual-template1] ppp authentication-mode pap
[H3C-virtual-template1] ppp pap local-user vpdnuser password simple Hello
[H3C-virtual-template1] quit
# 配置私网路由。

[H3C] ip route-static 10.1.0.0 16 virtual-template 1
(2) LNS 的典型配置
# 设置用户名及口令。

[H3C] local-user vpdnuser
[H3C-luser-vpdnuser] password simple Hello
[H3C-luser-vpdnuser] service-type ppp
# 配置 Ethernet0/0/1 接口。

[H3C] interface Ethernet0/0/1
[H3C-Ethernet0/0/1] ip address 3.3.3.2 255.255.0.0
[H3C-Ethernet0/0/1] quit
# 配置域及地址池。

[RouterB] domain system
[H3C-isp-system] scheme local
[H3C-isp-system] ip pool 1 192.168.0.2 192.168.0.10
[H3C-isp-system] quit
# 启用 L2TP 服务，并设置一个 L2TP 组。

[H3C] l2tp enable
```



```
[H3C] l2tp-group 1
# 配置虚模板 Virtual-Template 的相关信息。

[H3C] interface virtual-template 1
[H3C-virtual-template1] ip address 192.168.0.1 255.255.255.0
[H3C-virtual-template1] remote address pool 1
[H3C-virtual-template1] ppp authentication-mode pap
[H3C-virtual-template1] quit
# 配置 LNS 侧接收的通道对端名称。

[H3C] l2tp-group 1
[H3C-l2tp1] allow l2tp virtual-template 1 remote LAC
# 启用通道验证并设置通道验证密码。

[H3C-l2tp1] tunnel authentication
[H3C-l2tp1] tunnel password simple tunnelpwd
[H3C-l2tp1] quit
# 配置私网路由。

[H3C] ip route-static 10.2.0.0 16 virtual-template1
```

(3) 启动 L2TP 连接

在 SecPath A 的虚模板接口视图下执行启动 L2TP 连接命令

```
[H3C] interface virtual-template 1
[H3C-virtual-template1] l2tp-auto-client enable
```

 说明:

LAC 和 LNS 连接的私网主机应分别以 LAC 和 LNS 为网关。

2.5.5 复杂的组网情况

防火墙支持同时作为 LAC 及 LNS，并支持同时有多路用户呼入；只要内存及线路不受限制，L2TP 可以同时接收和发起多个呼叫。这些复杂组网的需求及配置可以综合参考以上的几种组网情况，综合应用。

特别需要注意的是静态路由的配置，许多应用是依靠路由来发起的。

2.6 L2TP 故障诊断与排错

VPN 创建连接的过程比较复杂，这里就几种常见的情况进行分析。在进行 VPN 排错之前，请先确认 LAC 与 LNS 都已在公共网上，并实现正确连通。

故障之一：用户登录失败

故障排除：用户登录失败主要有以下几种原因。

- Tunnel 建立失败，Tunnel 不能建立的原因有：
 - (1) 在 LAC 端，LNS 的地址设置不正确。
 - (2) LNS（通常为防火墙、路由器）端没有设置可以接收该隧道对端的 L2TP 组，具体可以查看 **allow** 命令的说明。
 - (3) Tunnel 验证不通过，如果配置了验证，应该保证双方的隧道密码一致。
 - (4) 如果是本端强制挂断了连接，而由于网络传输等原因，对端还没有收到相应的 **Disconnect** 报文，此时立即发起了一个隧道连接，连接将不能成功，因为对方必须相隔一定的时间才能侦测到链路被挂断。
- PPP 协商不通过，可能原因有：
 - (1) LAC 端设置的用户名与密码有误，或者是 LNS 端没有设置相应的用户。
 - (2) LNS 端不能分配地址，比如地址池设置的较小，或没有进行设置。
 - (3) 密码验证类型不一致。如 Windows 2000 所创建的 VPN 连接缺省的验证类型为 **MSCHAP**，如果对端不支持 **MSCHAP**，建议改为 **CHAP**。

故障之二：数据传输失败，在建立连接后数据不能传输，如 **Ping** 不通对端。

故障排除：可能有如下原因。

- 用户设置的地址有误：一般情况下，由 LNS 分配地址，而用户也可以指定自己的地址。如果指定的地址和 LNS 所要分配的地址不属于同一个网段，就会发生这种情况，建议由 LNS 统一分配地址。
- 网络拥挤：Internet 主干网产生拥挤，丢包现象严重。L2TP 是基于 UDP（用户数据报文）进行传输的，UDP 不对报文进行差错控制；如果是在线路质量不稳定的情况下进行 L2TP 应用，有可能会产生 **Ping** 不通对端的情况。

第3章 GRE 协议配置

3.1 GRE 协议简介

1. 协议简介

GRE（Generic Routing Encapsulation，通用路由封装）协议是对某些网络层协议（如 IP 和 IPX）的数据报进行封装，使这些被封装的数据报能够在另一个网络层协议（如 IP）中传输。GRE 是 VPN（Virtual Private Network）的第三层隧道协议，在协议层之间采用了一种被称之为 Tunnel（隧道）的技术。Tunnel 是一个虚拟的点连点的连接，在实际中可以看成仅支持点对点连接的虚拟接口。这个接口提供了一条通路使封装的数据报能够在这个通路上传输，并且在一个 Tunnel 的两端分别对数据报进行封装及解封装。

一个报文要想在 Tunnel 中传输，必须要经过加封装与解封装两个过程，下面以图 3-1 的网络为例说明这两个过程：

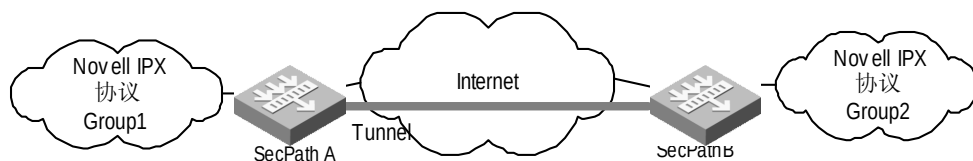


图3-1 IPX 网络通过 GRE 隧道互连

(1) 加封装过程

连接 Novell group1 的接口收到 IPX 数据报后首先交由 IPX 协议处理，IPX 协议检查 IPX 报头中的目的地址域来确定如何路由此包。若报文的目的地址被发现要路由经过网号为 1f 的网络（Tunnel 的虚拟网号），则将此报文发给网号为 1f 的 Tunnel 端口。Tunnel 口收到此包后进行 GRE 封装，然后交给 IP 模块处理，在封装 IP 报文头后，根据此包的目的地址及路由表交由相应的网络接口处理。

(2) 解封装的过程

解封装过程和加封装的过程相反。从 Tunnel 接口收到的 IP 报文，通过检查目的地址，当发现目的地就是此防火墙时，系统剥掉此报文的 IP 报头，交给 GRE 协议模块处理（进行检验密钥、检查校验和及报文的序列号等）。GRE 协议模块完成相应的处理后，剥掉 GRE 报头，再交由 IPX 协议模块处理。IPX 协议模块象对待一般数据报一样对此数据报进行处理。

一个需要封装和路由的数据报，称之为净荷（Payload）。系统收到这个净荷，首先净荷被加上 GRE 封装，成为 GRE 报文；再被封装在 IP 报文中，这样就可完全由

IP 层负责此报文的向前传输（Forwarded）。人们常把这个负责向前传输 IP 协议称为传输协议（Delivery Protocol 或者 Transport Protocol）。

封装好的报文的形式如下图所示。

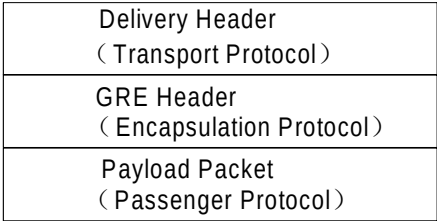


图3-2 封装好的 Tunnel 报文格式

举例来说，一个封装在 IP Tunnel 中的 IPX 传输报文的格式如下。

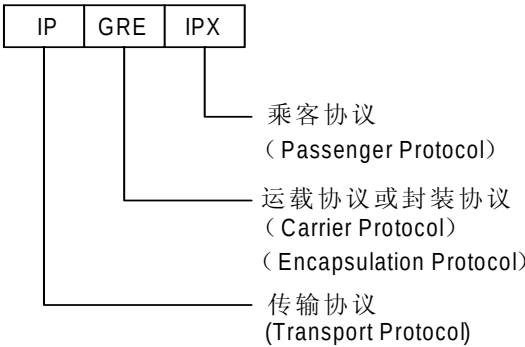


图3-3 Tunnel 中传输报文的格式

2. 应用范围

GRE 主要能实现以下几种服务类型：

- (1) 多协议的本地网通过单一协议的骨干网传输

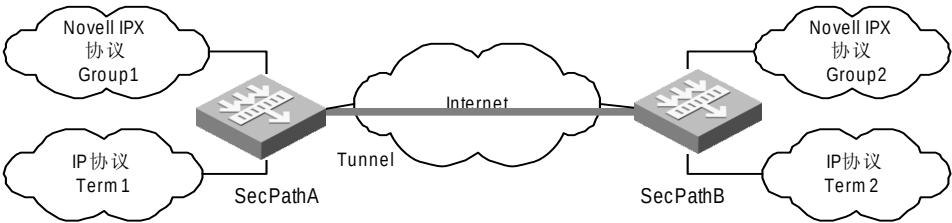


图3-4 多协议本地网通过单一协议骨干网传输

上图中，Group1 和 Group2 是运行 Novell IPX 协议的本地网，Term1 和 Term2 是运行 IP 协议的本地网。通过在 SecPath A 和 SecPath B 之间采用 GRE 协议封装的隧道（Tunnel），Group1 和 Group2、Team1 和 Team2 可以互不影响地进行通信。

(2) 扩大了步跳数受限协议（如 IPX）的网络的工作范围

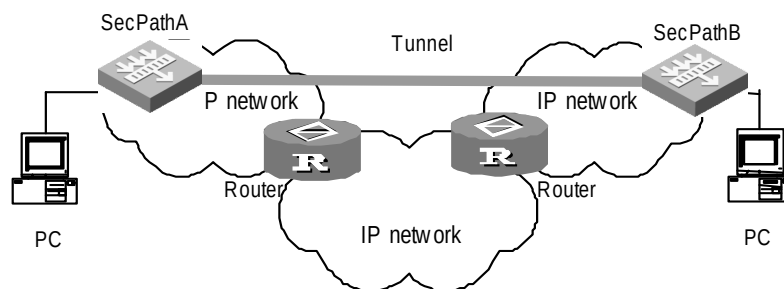


图3-5 扩大网络工作范围

若上图中的两台终端之间的步跳数超过 15，它们将无法通信。而通过在网络中使用隧道（Tunnel）可以隐藏一部分步跳，从而扩大网络的工作范围。

(3) 将一些不能连续的子网连接起来，用于组建 VPN

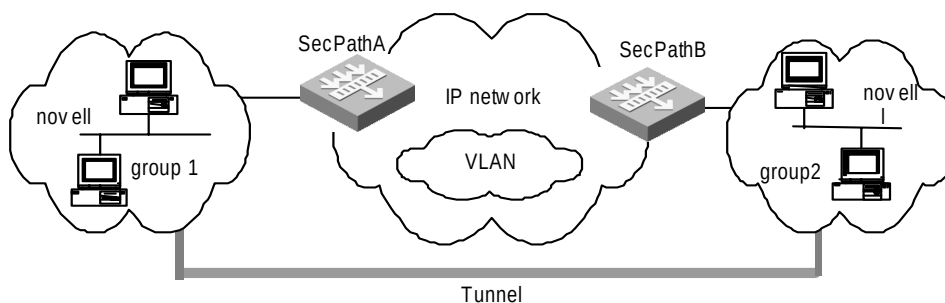


图3-6 Tunnel 连接不连续子网

运行 Novell IPX 协议的两个子网 group1 和 group2 分别在不同的城市，通过使用隧道可以实现跨越广域网的 VPN。

(4) 与 IPsec 结合使用

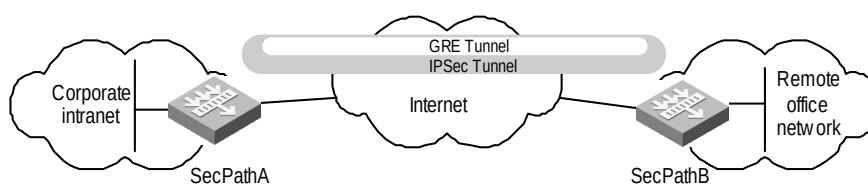


图3-7 GRE-IPsec 隧道应用

对于诸如路由协议、语音、视频等数据先进行 GRE 封装，然后再对封装后的报文进行 IPsec 的加密处理。

另外，GRE 还支持由用户选择记录 Tunnel 接口的识别关键字，和对封装的报文进行端到端校验。

由于 GRE 收发双方加封装、解封装处理以及由于封装造成的数据量增加等因素的影响，这就导致使用 GRE 会造成防火墙的数据转发效率有一定程度的下降。

3.2 GRE 配置

在各项配置中，必须先创建虚拟 Tunnel 接口，才能在虚拟 Tunnel 接口上进行其它功能特性的配置。当删除虚拟 Tunnel 接口后，该接口上的所有配置也将被删除。

GRE 主要配置包括：

- 创建虚拟 Tunnel 接口（必选）
- 设置 Tunnel 接口报文的封装模式（可选）
- 指定 Tunnel 的源端（必选）
- 指定 Tunnel 的目的端（必选）
- 设置 Tunnel 接口的网络地址（必选）
- 设置 Tunnel 两端进行端到端校验（可选）
- 设置 Tunnel 接口的识别关键字（可选）
- 配置通过 Tunnel 的路由（可选）

3.2.1 创建虚拟 Tunnel 接口

创建虚拟 Tunnel 接口，从而在该接口上进行 GRE 其它参数的配置。这些配置在 Tunnel 两端必须配置。

请在系统视图下进行下列配置。

表3-1 创建虚拟 Tunnel 接口

操作	命令
创建虚拟 Tunnel 接口	interface tunnel number
删除虚拟 Tunnel 接口	undo interface tunnel number

缺省情况下，不创建虚拟 Tunnel 接口。

number 为设定的接口号，范围 0~1023，但实际可建的 Tunnel 数目将受到接口总数及内存状况的限制。

3.2.2 设置 Tunnel 接口报文的封装模式

设置 Tunnel 接口的封装协议和传输协议。这些配置在 Tunnel 两端为可选配置，如果配置则必须确保 Tunnel 两端的封装模式相同。

请在 Tunnel 视图下进行下列配置。

表3-2 设置 Tunnel 接口报文的封装模式

操作	命令
设置 Tunnel 接口报文的封装模式	tunnel-protocol gre

缺省情况下，Tunnel 接口报文的封装模式为 GRE。

3.2.3 指定 Tunnel 的源端

在创建 Tunnel 接口后，还要指明 Tunnel 通道的源端地址，即发出 GRE 报文的实际接口地址。Tunnel 的源端地址与目的端地址唯一标识了一个通道。这些配置在 Tunnel 两端必须配置，且两端地址互为源地址和目的地址。

请在 Tunnel 接口视图下进行下列配置。

表3-3 设置 Tunnel 接口的源端地址

操作	命令
设置 Tunnel 接口的源端地址	source { <i>ip-addr</i> <i>interface-type interface-num</i> }
删除 Tunnel 接口的源端地址	undo source

说明：

- 不能对两个或两个以上使用同种封装协议的 Tunnel 接口配置完全相同的源地址和目的地址。
- 使用命令 **source** 设置的是实际的物理接口地址或实际物理接口，为支持动态路由协议，还需要设置 Tunnel 接口的网络地址。在 Tunnel 接口视图下通过命令 **ip address** 可完成这一设置。

3.2.4 指定 Tunnel 的目的端

在创建 Tunnel 接口后，还要指明 Tunnel 通道的目的端地址，即接收 GRE 报文的实际物理接口的 IP 地址。Tunnel 的源端地址与目的端地址唯一标识了一个通道。这些配置在 Tunnel 两端必须配置，且两端地址互为源地址和目的地址。

请在 Tunnel 接口视图下进行下列配置。

表3-4 设置 Tunnel 接口的目的端地址

操作	命令
设置 Tunnel 接口的目的端地址	destination <i>ip-addr</i>
删除 Tunnel 接口的目的端地址	undo destination

 说明：

使用命令 **destination** 设置的是实际的物理接口的 IP 地址，为支持动态路由协议，还需要设置 Tunnel 接口的网络地址。

3.2.5 设置 Tunnel 接口的网络地址

Tunnel 接口的网络地址可以不是申请得到的网络地址。用户设置通道两端的网络地址应该位于同一网段上。这些配置在 Tunnel 两端都必须配置，并且确保地址在同一网段。

请在 Tunnel 接口视图下进行下列设置。

表3-5 设置 Tunnel 接口的网络地址

操作	命令
设置 Tunnel 接口的 IP 地址	ip address { ip-addr mask unnumbered interface interface-type interface-number }
删除 Tunnel 接口的 IP 地址	undo ip address

缺省情况下，未设置 Tunnel 接口的网络地址。

3.2.6 设置 Tunnel 两端进行端到端校验

在 RFC 1701 中规定：若 GRE 报文头中的 Checksum 位置位，则校验和有效。发送方将根据 GRE 头及 payload 信息计算校验和，并将包含校验和的报文发送给对端。接收方对接收到的报文计算校验和，并与报文中的校验和比较，如果一致则对报文进一步处理，否则丢弃。

隧道两端可以根据实际应用需要，配置校验和或禁止校验和。如果本端配置了校验和而对端没有配置，则本端将不会对接收到的报文进行校验和检查，但对发送的报文计算校验和；相反，如果本端没有配置校验和而对端已配置，则本端将对从对端发来的报文进行校验和检查，但对发送的报文不计算校验和。

请在 Tunnel 接口视图下进行下列配置。

表3-6 设置 Tunnel 两端进行端到端校验

操作	命令
设置 Tunnel 两端进行端到端校验	gre checksum
禁止 Tunnel 两端进行端到端校验	undo gre checksum

缺省情况下，禁止 Tunnel 两端进行端到端校验。

3.2.7 设置 Tunnel 接口的识别关键字

在 RFC 1701 中规定：若 GRE 报文头中的 KEY 字段置位，则收发双方将进行通道识别关键字的验证，只有 Tunnel 两端设置的识别关键字完全一致时才能通过验证，否则将报文丢弃。

请在 Tunnel 接口视图下进行配置。

表3-7 设置 Tunnel 接口的识别关键字

操作	命令
设置 Tunnel 接口的识别关键字	gre key <i>key-number</i>
删除 Tunnel 接口的识别关键字	undo gre key

key-number 可取值 0~4294967295 之间的整数。

缺省情况下，Tunnel 不使用识别关键字。

3.2.8 配置通过 Tunnel 的路由

在隧道的源端和目的端上都必须存在经过 Tunnel 转发的路由，这样需要进行 GRE 封装的报文才能正确转发。可以配置静态路由，也可以配置动态路由。

1. 静态路由配置

可以手工配置一条到达目的地址（不是 Tunnel 的目的端地址，而是未进行 GRE 封装的报文的目的地址）的路由，下一跳是对端 Tunnel 接口的地址。在 Tunnel 的两端都要进行此项配置。配置的详细情况请参见本手册的“路由协议”部分，配置命令的详细解释请参见相应的命令手册。

2. 动态路由配置

如果在防火墙上运行了动态路由协议，只需在 Tunnel 接口上和与私网相连的防火墙接口上使能该动态路由协议即可，在 Tunnel 的两端都必须进行此项配置。配置的详细情况请参见本手册的“路由协议”部分，配置命令的详细解释请参见相应的命令手册。

3.2.9 配置 keepalive 功能

请在 Tunnel 接口视图下进行配置。

表3-8 配置 keepalive 功能

操作	命令
使能 GRE 的 keepalive 功能	keepalive [<i>seconds</i> [<i>times</i>]]
关闭 GRE 的 keepalive 功能	undo keepalive

缺省情况下，不启用 GRE 的 keepalive 功能。*seconds* 缺省为 10 秒。*times* 缺省为 3 次。

配置了 GRE 的 keepalive 的功能后，防火墙会从 Tunnel 口定期发送 GRE 的 keepalive 报文。如果超时时间内对端没有回应，则本端防火墙重新发送 keepalive 报文。如果超过最大传送次数后仍然没有接受到对端的回应，则本端 Tunnel 口的协议状态将变为 down。

3.3 GRE 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 GRE 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **debugging** 命令可对 GRE 进行调试。

表3-9 GRE 的显示和调试

操作	命令
显示 Tunnel 接口的工作状态	display interface tunnel <i>number</i>
打开 Tunnel 调试信息	debugging tunnel

3.4 GRE 典型配置举例

1. 组网需求

运行 IP 协议的两个子网 Group1 和 Group2，通过在 SecPath1 和 SecPath2 之间使用三层隧道协议 GRE 实现互联。

2. 组网图

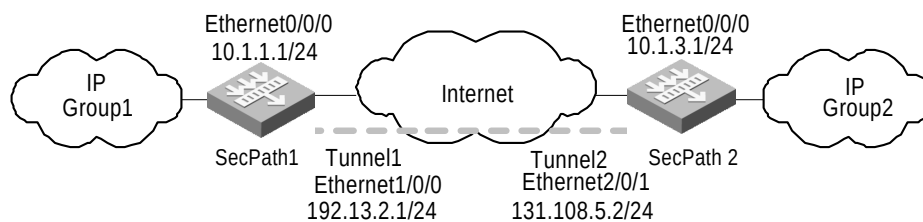


图3-8 GRE 应用组网图

3. 配置步骤

(1) 配置 SecPath1

配置接口 Ethernet0/0/0。

```
[H3C] interface ethernet 0/0/0
[H3C-Ethernet0/0/0] ip address 10.1.1.1 255.255.255.0
[H3C-Ethernet0/0/0] quit
```

配置接口 Ethernet1/0/0（隧道的实际物理接口）。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 192.13.2.1 255.255.255.0
[H3C-Ethernet1/0/0] quit
```

创建 Tunnel1 接口。

```
[H3C] interface tunnel 1
```

配置 Tunnel1 接口的 IP 地址。

```
[H3C-Tunnel1] ip address 10.1.2.1 255.255.255.0
```

配置 Tunnel 封装模式。

```
[H3C-Tunnel1] tunnel-protocol gre
```

配置 Tunnel1 接口的源地址（Ethernet1/0/0 的 IP 地址）。

```
[H3C-Tunnel1] source 192.13.2.1
```

配置 Tunnel1 接口的目的地址（SecPath2 的 Ethernet2/0/1 的 IP 地址）。

```
[H3C-Tunnel1] destination 131.108.5.2
[H3C-Tunnel1] quit
```

配置从 SecPath1 经过 Tunnel1 接口到 Group2 的静态路由。

```
[H3C] ip route-static 10.1.3.0 255.255.255.0 tunnel 1
```

(2) 配置 SecPath2

配置接口 Ethernet0/0/0。

```
[H3C] interface ethernet 0/0/0
[H3C-Ethernet0/0/0] ip address 10.1.3.1 255.255.255.0
```

```
[H3C-Ethernet0/0/0] quit
# 配置接口 Ethernet2/0/1（隧道的实际物理接口）。

[H3C] interface ethernet 2/0/1
[H3C-Ethernet2/0/1] ip address 131.108.5.2 255.255.255.0
[H3C-Ethernet2/0/1] quit

# 创建 Tunnel2 接口。

[H3C] interface tunnel 2
# 配置 Tunnel2 接口的 IP 地址。

[H3C-Tunnel2] ip address 10.1.2.2 255.255.255.0
# 配置 Tunnel 封装模式。

[H3C-Tunnel2] tunnel-protocol gre
# 配置 Tunnel2 接口的源地址（Ethernet2/0/1 的 IP 地址）。

[H3C-Tunnel2] source 131.108.5.2
# 配置 Tunnel2 接口的目的地址（SecPath1 的 Ethernet1/0/0 的 IP 地址）。

[H3C-Tunnel2] destination 192.13.2.1
[H3C-Tunnel2] quit
# 配置从 SecPath2 经过 Tunnel2 接口到 Group1 的静态路由。

[H3C] ip route-static 10.1.1.0 255.255.255.0 tunnel 2
```

3.5 GRE 故障诊断与排除

GRE 的配置相对比较简单，但要注意配置的一致性，大部分的错误都可以通过使用调试命令 **debugging tunnel** 定位。这里仅就一种错误进行分析，如图 3-9 所示。

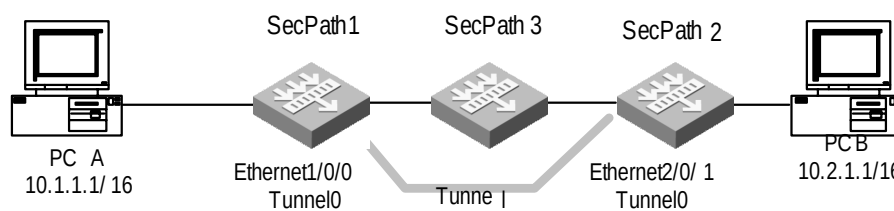


图3-9 GRE 排错示例

故障之一：Tunnel 两端接口配置正确且 Tunnel 两端可以 ping 通，但 PC A 和 PC B 之间却无法 ping 通。

故障排除：可以按照如下步骤进行。

- 在任一视图下，在 SecPath1 和 SecPath2 分别执行 **display ip routing-table** 命令，观察在 SecPath1 是否有经过 Tunnel0 接口到 10.2.0.0/16 的路由；在 SecPath2 是否有经过 Tunnel0 接口到 10.1.0.0/16 的路由。
- 如果在上一步的输出中发现缺少相应的静态路由，在系统视图下使用 **ip route-static** 命令添加。以 SecPath1 为例，配置如下：

```
[H3C] ip route-static 10.2.0.0 255.255.0.0 tunnel 0
```

第4章 IPsec 配置

4.1 IPsec 概述

4.1.1 IPsec 协议简介

IPsec（IP security）协议族是 IETF 制定的一系列协议，它为 IP 数据报提供了高质量的、可互操作的、基于密码学的安全功能。特定的通信方之间在 IP 层通过加密与数据源验证等方式，来保证数据报在网络上传输时的私有性、完整性、真实性和防重放。

 说明：

私有性（Confidentiality）指对用户数据进行加密保护，用密文的形式传送。

完整性（Data integrity）指对接收的数据进行验证，以判定报文是否被篡改。

真实性（Data origin authentication）指验证数据源，以保证数据来自真实的发送者。

防重放（Anti-replay）指防止恶意用户通过重复发送捕获到的数据包所进行的攻击，即接收方会拒绝旧的或重复的数据包。

IPsec 通过 AH（Authentication Header，认证头）和 ESP（Encapsulating Security Payload，封装安全载荷）这两个安全协议来实现上述目标。IPsec 还可以通过 IKE（Internet Key Exchange，Internet 密钥交换协议）为 IPsec 提供自动协商交换密钥、建立和维护安全联盟的服务，以简化 IPsec 的使用和管理。

- AH 是报文头验证协议，主要提供的功能有数据源验证、数据完整性校验和防报文重放；然而，AH 并不加密所保护的数据报。
 - ESP 是封装安全载荷协议，它除提供 AH 协议的所有功能之外（数据完整性校验不包括 IP 头），还提供对 IP 报文的加密功能。
-

 说明：

AH 和 ESP 可以单独使用，也可以同时使用。对于 AH 和 ESP，都有两种操作模式：传输模式和隧道模式。工作模式将在后文介绍。

- IKE 用于协商 AH 和 ESP 所使用的密码算法，并自动地进行安全联盟的建立与密钥交换。

 说明：

IKE 协商并不是必须的，IPsec 所使用的策略和算法等也可以手工协商。关于两种协商方式的比较，将在后文介绍。

4.1.2 加密卡简介

在实际应用中，IPsec 对报文的处理包括 ESP 协议处理和 AH 协议处理。为了确保信息的安全，加密/解密、认证的算法一般比较复杂。防火墙的 IPsec 软件进行加密/解密算法将占用大量的 CPU 资源，从而影响了防火墙的整体处理效率。因此，对于模块化的防火墙，可以使用加密卡（模块化硬件插卡），以硬件方式完成数据的 IPsec 运算，消除了 Comware 主体软件处理 IPsec 对整体性能的影响，提高了防火墙的工作效率，同时也提高了 IPsec 的处理效率。

- (1) 加密卡进行加/解密处理的过程是：防火墙将需要加/解密处理的数据发给加密卡，加密卡对数据进行加/解密运算并给数据添加/删除加密帧头，然后加密卡将处理后的数据发送回防火墙，再由防火墙进行转发处理。
- (2) 在使用加密卡进行 IPsec 处理的过程中，若处理某特定数据流的加密卡状态异常时，加密卡将无法进行 IPsec 的处理。此时，若已经打开主机备份处理开关，并且 Comware 主体软件 IPsec 模块支持该加密卡使用的加密/认证算法，则 Comware 主体软件 IPsec 模块将代替加密卡对数据进行 IPsec 处理，从而实现了加密卡的备份功能。但加密卡之间无法互做备份。

 说明：

加密卡与 Comware 主体软件 IPsec 模块对数据的处理机制完全相同，区别仅仅在于 Comware 主体软件是通过软件实现 IPsec 处理的，而加密卡是通过硬件实现 IPsec 处理的。

4.1.3 IPsec 基本概念

1. 安全联盟

IPsec 在两个端点之间提供安全通信，端点被称为 IPsec 对等体。

IPsec 能够允许系统、网络的用户或管理员控制对等体间安全服务的粒度。例如，某个组织的安全策略可能规定来自特定子网的数据流应同时使用 AH 和 ESP 进行保护，并使用 3DES（Triple Data Encryption Standard，三重数据加密标准）进行加密；另一方面，策略可能规定来自另一个站点的数据流只使用 ESP 保护，并仅使用 DES 加密。通过 SA（Security Association，安全联盟），IPsec 能够对不同的数据流提供不同级别的安全保护。

安全联盟是 IPsec 的基础，也是 IPsec 的本质。SA 是通信对等体间对某些要素的约定，例如，使用哪种协议（AH、ESP 还是两者结合使用）、协议的操作模式（传输模式和隧道模式）、加密算法（DES 和 3DES）、特定流中保护数据的共享密钥以及 SA 的生存周期等。

安全联盟是单向的，在两个对等体之间的双向通信，最少需要两个安全联盟来分别对两个方向的数据流进行安全保护。同时，如果希望同时使用 AH 和 ESP 来保护对等体间的数据流，则分别需要两个 SA，一个用于 AH，另一个用于 ESP。

安全联盟由一个三元组来唯一标识，这个三元组包括 SPI（Security Parameter Index，安全参数索引）、目的 IP 地址、安全协议号（AH 或 ESP）。SPI 是为唯一标识 SA 而生成的一个 32 比特的数值，它在 AH 和 ESP 头中传输。

安全联盟具有生存周期。生存周期的计算包括两种方式：

- 以时间为限制，每隔指定长度的时间就进行更新；
- 以流量为限制，每传输指定的数据量（字节）就进行更新。

2. IPsec 协议的操作模式

IPsec 协议有两种操作模式：传输模式和隧道模式。SA 中指定了协议的操作模式。

在传输模式下，AH 或 ESP 被插入到 IP 头之后但在所有传输层协议之前，或所有其他 IPsec 协议之前。在隧道模式下，AH 或 ESP 插在原始 IP 头之前，另外生成一个新头放到 AH 或 ESP 之前。不同安全协议在传输模式和隧道模式下的数据封装形式（传输协议以 TCP 为例）如下图所示：

模式 协议	transport						tunnel					
AH	IP Header	AH	TCP Header	data			new IP Header	AH	raw IP Header	TCP Header	data	
ESP	IP Header	ESP	TCP Header	data	ESP Tail	ESP Auth data	new IP Header	ESP	raw IP Header	TCP Header	data	ESP Tail ESP Auth data
AH-ESP	IP Header	AH	ESP	TCP Header	data	ESP Tail ESP Auth data	new IP Header	AH	ESP	raw IP Header	TCP Header	data ESP Tail ESP Auth data

图4-1 安全协议数据封装格式

从安全性来讲，隧道模式优于传输模式。它可以完全地对原始 IP 数据报进行验证和加密；此外，可以使用 IPsec 对等体的 IP 地址来隐藏客户机的 IP 地址。从性能来讲，隧道模式比传输模式占用更多带宽，因为它有一个额外的 IP 头。因此，到底使用哪种模式需要在安全性和性能间进行权衡。

3. 验证算法与加密算法

(1) 验证算法

AH 和 ESP 都能够对 IP 报文的完整性进行验证, 以判别报文在传输过程中是否被篡改。验证算法的实现主要是通过杂凑函数。杂凑函数是一种能够接受任意长的消息输入, 并产生固定长度输出的算法, 该输出称为消息摘要。IPsec 对等体计算摘要, 如果两个摘要是相同的, 则表示报文是完整未经篡改的。一般来说 IPsec 使用两种验证算法:

- MD5: MD5 通过输入任意长度的消息, 产生 128bit 的消息摘要。
- SHA-1: SHA-1 通过输入长度小于 2 的 64 次方比特的消息, 产生 160bit 的消息摘要。

SHA-1 的摘要长于 MD5, 因而是更安全的。

(2) 加密算法

ESP 能够对 IP 报文内容进行加密保护, 防止报文内容在传输过程中被窥探。加密算法实现主要通过对称密钥系统, 它使用相同的密钥对数据进行加密和解密。Comware 中的 IPsec 实现了三种加密算法:

- DES (Data Encryption Standard): 使用 56bit 的密钥对每个 64bit 的明文块进行加密。
- 3DES (Triple DES): 使用三个 56bit 的 DES 密钥 (共 168bit 密钥) 对明文进行加密。
- AES (Advanced Encryption Standard): Comware 实现了 128bit、192bit 和 256bit 密钥长度的 AES 算法。

4. 协商方式

有两种协商方式建立安全联盟, 一种是手工方式 (**manual**), 一种是 IKE 自动协商 (**isakmp**) 方式。前者配置比较复杂, 创建安全联盟所需的全部信息都必须手工配置, 而且 IPsec 的一些高级特性 (例如定时更新密钥) 不被支持, 但优点是可以不依赖 IKE 而单独实现 IPsec 功能。而后者则相对比较简单, 只需要配置好 IKE 协商安全策略的信息, 由 IKE 自动协商来创建和维护安全联盟。

当与之进行通信的对等体设备数量较少时, 或是在小型静态环境中, 手工配置安全联盟是可行的。对于中、大型的动态网络环境中, 推荐使用 IKE 协商建立安全联盟。

5. IPsec DPD

IPsec DPD (IPsec Dead Peer Detection on-demand) 为按需型 IPsec/IKE 安全隧道对端状态探测功能。启动 DPD 功能后, 当接收端长时间收不到对端的报文时, 能够触发 DPD 查询, 主动向对端发送请求报文, 对 IKE Peer 是否存在进行检测。与

IPsec 中原有的周期性 Keepalive 功能相比，DPD 具有产生数据流量小、检测及时、隧道恢复快的优点。

在防火墙与 VRRP 备份组的虚地址之间建立 ISAKMP SA 的应用方案中，DPD 功能保证了 VRRP 备份组中主备切换时安全隧道能够迅速自动恢复。解决了 VRRP 备份组主备切换使安全隧道通信中断的问题，扩展了 IPsec 的应用范围，提高了 IPsec 协议的健壮性。

该功能符合 RFC3706、RFC2408。

(1) 定时器

IPsec DPD 在发送和接收 DPD 报文中使用了两个定时器：intervaltime 和 timeout。

- **intervaltime**：触发 DPD 查询的间隔时间，该时间指明隔多久没有收到对端 IPsec 报文时触发 DPD 查询。
- **timeout**：等待 DPD 应答报文超时时间。

(2) 运行机制

- **发送端**

当启动了 DPD 功能以后，如在 intervaltime 定时器指定的时间间隔内没有收到对端的 IPsec 报文，且本端欲向对端发送 IPsec 报文时，DPD 向对端发送 DPD 请求，并等待应答报文。如果超过 timeout 定时器设定的超时时间仍然未收到正确的应答报文，DPD 记录失败事件 1 次。当失败事件达到 3 次时，删除 ISAKMP SA 和相应的 IPsec SA。

对于路由器与 VRRP 备份组虚地址之间建立的 IPsec SA，连续 3 次失败后，安全隧道同样会被删除，但是当有符合安全策略的报文重新触发安全联盟协商时，会重新建立起安全隧道。切换时间的长短与 timeout 定时器的设置有关，定时器设定的超时时间越短，通信中断时间越短（注意：超时时间过短会增加网络开销，一般情况下采用缺省值即可）。

- **接收端**

收到请求报文后，发送响应报文。



注意：

如果 IPsec SA 对应的 IKE SA 已经更新，当触发 DPD 查询时，DPD 查询功能将失效，并且 IPsec SA 将被删除。当后续报文再触发 IKE 协商，并建立与更新后的 IKE SA 对应的 IPsec SA 后，DPD 功能才能生效。

4.1.4 IPsec 多实例简介

目前 IPsec 实现了 MPLS PE 与 CE 之间绑定接口的 IPsec 多实例功能，即 IPsec 隧道建立在 PE 和 CE 之间，且 PE 使用不同接口连接不同的 CE，故属于不同的 VPN 的 CE 可以分别与 PE 建立 IPsec 隧道，从而使组网更加灵活。

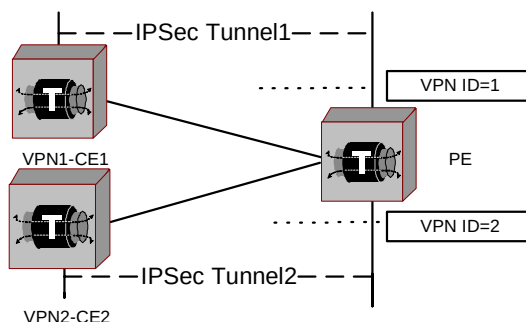


图4-2 IPsec 多实例应用示意图

报文处理过程如下：

- 当 PE 设备向 CE 转发 IP 报文时，根据报文中的 VPN ID 来确定该报文属于哪一个 VPN，然后查找相应的 VPN 路由表，并将报文转发到相应的出接口。此时若在出接口上配置了 ipsec policy，则对匹配 ACL 的报文进行加密传输，发往 CE。
- 当 PE 收到 IPsec 报文时首先进行解密处理（非 IPsec 报文则跳过这一步），然后根据报文中的 VPN ID 来确定该报文属于哪一个 VPN，通过查找相应的 VPN 路由表确定该报文的地址是本机还是非本机，若为本机报文，则交由 IP 层处理（可能转发给另一个同属于一个 VPN 的 CE）；若为非本机报文，则按 VPN 路由表指示进行标签封装。

4.1.5 IPsec 在 Comware 上的实现

Comware 实现了上述所介绍的 IPsec 的全部内容。

其实现方式是基于下列思路：通过 IPsec，对等体之间（此处是指 Comware 所在防火墙及其对端）能够对不同的数据流实施不同的安全保护（验证、加密或两者同时使用）。其中数据流的区分通过配置 ACL 来进行；安全保护所用到的安全协议、验证算法和加密算法、操作模式等通过配置安全提议来进行；数据流和安全提议的关联（即定义对何种数据流实施何种保护）、SA 的协商方式、对等体 IP 地址的设置（即保护路径的起/终点）、所需要的密钥和 SA 的生存周期等通过配置安全策略来进行；最后在防火墙的接口上实施安全策略即完成了 IPsec 的配置。

具体介绍如下：

(1) 定义被保护的数据流

数据流是一组流量（traffic）的集合，由源地址/掩码、目的地址/掩码、IP 报文承载的协议号、源端口号、目的端口号等来规定。一个数据流用一个 ACL 来定义，所有匹配一个访问控制列表规则的流量，在逻辑上作为一个数据流。一个数据流可以小到是两台主机之间单一的 TCP 连接；也可以大到是两个子网之间所有的流量。IPsec 能够对不同的数据流施加不同的安全保护，因此 IPsec 配置的第一步就是定义数据流。

(2) 定义安全提议

安全提议规定了对要保护的数据流所采用的安全协议、验证或加密算法、操作模式（即报文的封装方式）等。

Comware 支持的 AH 和 ESP 安全协议，两者既可单独使用，也可结合使用。其中，AH 支持 MD5 和 SHA-1 验证算法；ESP 协议支持 MD5、SHA-1 验证算法和 DES、3DES、AES 加密算法。Comware 支持的操作模式包括传输模式和隧道模式。

对同一数据流，对等体两端必须设置相同的协议、算法和操作模式。另外，对于两个防火墙（例如 SecPath 防火墙间）实施 IPsec，建议采用隧道模式，以隐藏实际通信的源和目的 IP 地址。

因此，请先根据需要配置好一个安全提议，以便下一步将数据流和安全提议相关联。

(3) 定义安全策略或安全策略组

安全策略规定了对什么样的数据流采用什么样的安全提议。一条安全策略由“名字”和“顺序号”共同唯一确定。安全策略分为手工安全策略和 IKE 协商安全策略。前者需要用户手工配置密钥、SPI 等参数，在隧道模式下还需要手工配置安全隧道两个端点的 IP 地址；后者则由 IKE 自动协商生成这些参数。

安全策略组是所有具有相同名称、不同顺序号的安全策略的集合。在同一个安全策略组中，顺序号越小的安全策略，优先级越高。

(4) 接口实施安全策略

在接口上应用安全策略组，安全策略组中的所有安全策略同时应用在这个接口上，从而实现对流经这个接口的不同的数据流进行不同的安全保护。

4.2 IPsec 配置

1. IPsec 主要配置

(1) 配置访问控制列表

(2) 定义安全提议

- 创建安全提议（包括 IPsec 安全提议和加密卡安全提议两种类型）
- 指定加密卡安全提议使用的加密卡（仅用于加密卡）

- 选择安全协议
- 选择安全算法
- 选择报文封装形式

(3) 创建安全策略

包括手工创建安全策略和用 IKE 创建安全策略。

手工创建安全策略：

- 手工创建安全策略
- 在安全策略中引用安全提议
- 在安全策略中引用访问控制列表
- 配置隧道的起点和终点
- 配置安全联盟的 SPI
- 配置安全联盟使用的密钥

用 IKE 创建安全策略：

- 用 IKE 创建安全策略
- 在安全策略中引用安全提议
- 在安全策略中引用访问控制列表
- 在安全策略中引用 IKE 对等体
- 配置安全联盟生存周期（可选）
- 配置协商时使用的 PFS 特性（可选）

在安全策略中可以根据需要引用 IPsec 安全提议或加密卡安全提议。

(4) 配置安全策略模板（可选）

(5) 在接口上应用安全策略

(6) 配置取消对 next payload 域的检查（可选）

2. 加密卡可选配置

- (1) 使能加密卡
- (2) 使能 Comware 主体软件备份
- (3) 配置加密卡快转功能
- (4) 配置加密卡的简单网管操作

4.2.1 定义访问控制列表

IPsec 使用高级访问控制列表来判断哪些报文需要受到保护，哪些则不需要。用于 IPsec 的高级访问控制列表的作用不同于在防火墙中所介绍的高级访问控制列表。一般的高级访问控制列表是用来决定一个接口上哪些数据可通过，哪些要被拒绝；

而 IPsec 是根据高级访问控制列表中的规则来确定哪些报文需要安全保护，哪些报文不需要安全保护，故用于 IPsec 的高级访问控制列表可称为加密访问控制列表。加密访问控制列表匹配（**permit**）的报文将被保护，加密访问控制列表拒绝（**deny**）的报文将不被保护。加密访问控制列表既可用于加密入口数据流，也可用于加密出口数据流。

访问控制列表的具体配置请参见本手册的“安全”部分。

发起方的访问控制列表的镜像应该为接收方的访问控制列表的子集，或者双方的访问控制列表互为镜像，这样协商才能成功。建议用户将本端和对端的访问控制列表配置成互为镜像，例如：

本端：

```
acl number 3101
rule 1 permit ip source 173.1.1.0 0.0.0.255 destination 173.2.2.0 0.0.0.255
```

对端：

```
acl number 3101
rule 1 permit ip source 173.2.2.0 0.0.0.255 destination 173.1.1.0 0.0.0.255
```

 说明：

IPsec 对访问控制列表（ACL）中 **permit** 的数据流进行保护，因此建议用户精确地配置 ACL，只对确实需要 IPsec 保护的数据流配置 **permit**，避免盲目地使用关键字 **any**。

当用户使用 **display acl all** 命令来浏览防火墙的访问控制列表，所有高级 IP 访问控制列表都将显示在命令的输出中，即同时包括了用于通信过滤和用于加密的高级 IP 访问控制列表，该命令的输出信息不区分这两种不同用途的高级访问控制列表。

4.2.2 定义安全提议

安全提议保存 IPsec 需要使用的特定安全性协议以及加密/验证算法，为 IPsec 协商安全联盟提供各种安全参数。为了能够成功的协商 IPsec 的安全联盟，两端必须使用相同的安全提议。

安全提议的配置包括：

- 创建安全提议
- 指定加密卡安全提议使用的加密卡（仅适用于加密卡）
- 设置安全协议对 IP 报文的封装模式
- 选择安全协议
- 选择安全算法

1. 创建安全提议

安全提议是用于实施 IPsec 保护而采用的安全协议、算法、报文封装形式的一个组合。一条安全策略通过引用一个或多个安全提议来确定采用的安全协议、算法和报文封装形式。在安全策略引用一个安全提议之前，这个安全提议必须已经建立。

可对安全提议进行修改，但对已协商成功的安全联盟，新修改的安全提议并不起作用，即安全联盟仍然使用原来的安全提议（除非使用 **reset ipsec sa** 或 **reset encrypt-card sa** 命令重置），只有新协商的安全联盟将使用新的安全提议。

请在系统视图下进行下列配置。

表4-1 配置安全提议

操作	命令
创建安全提议并进入安全提议视图（适用于 Comware 主体软件 IPsec）	ipsec proposal <i>proposal-name</i>
删除安全提议（适用于 Comware 主体软件 IPsec）	undo ipsec proposal <i>proposal-name</i>
创建加密卡安全提议并进入加密卡安全提议视图（适用于加密卡）	ipsec card-proposal <i>proposal-name</i>
删除加密卡安全提议（适用于加密卡）	undo ipsec card-proposal <i>proposal-name</i>

缺省情况下，未配置安全提议。

2. 指定加密卡安全提议使用的加密卡（仅适用于加密卡）

当使用加密卡进行数据处理时，需要在加密卡安全提议模式下指定使用加密卡的槽位号。同一块加密卡可以在不同的加密卡安全提议中使用。在系统视图下，使用 **ipsec card-proposal** *proposal-name* 命令进入加密卡提议视图，然后在加密卡提议视图下，指定加密卡安全提议使用的加密卡。

表4-2 指定加密卡安全提议使用的加密卡的槽位

操作	命令
进入加密卡提议视图	ipsec card-proposal <i>proposal-name</i>
指定加密卡安全提议使用的加密卡	use encrypt-card <i>slot-id</i>
取消加密卡安全提议使用的加密卡	undo use encrypt-card

缺省情况下，加密卡安全提议没有使用任何加密卡。

3. 选择报文封装形式

在安全提议中需要指定报文封装模式，安全隧道的两端所选择的 IP 报文封装模式必须一致。

请在安全提议视图或加密卡安全提议视图下进行下列配置。

表4-3 选择报文封装形式

操作	命令
设置安全协议对 IP 报文的封装形式	encapsulation-mode { transport tunnel }
恢复缺省报文封装形式	undo encapsulation-mode

通常，在两个防火墙（路由器）之间，总是使用隧道模式。而在两台主机之间的通讯，或者是一台主机和一个防火墙之间的通讯选择传输模式。

缺省情况下采用 **tunnel**，即隧道模式。

4. 选择安全协议

安全提议中需要选择所采用的安全协议。目前可选的安全协议有 **AH** 和 **ESP**，也可指定同时使用 **AH** 与 **ESP**。安全隧道两端所选择的安全协议必须一致。

请在安全提议或加密卡安全提议视图下进行下列配置。

表4-4 选择安全协议

操作	命令
设置安全提议采用的安全协议	transform { ah ah-esp esp }
恢复缺省的安全协议	undo transform

缺省情况下采用 **esp**，即 RFC 2406 规定的 ESP 协议。

5. 选择安全算法

不同的安全协议可以采用不同的验证算法和加密算法。目前，**AH** 支持 MD5 和 SHA-1 验证算法；**ESP** 协议支持 MD5、SHA-1 验证算法和 DES、3DES、AES 加密算法。

请在安全提议或加密卡安全提议视图下进行下列配置。

表4-5 选择安全算法

操作	命令
设置 ESP 协议采用的加密算法	esp encryption-algorithm { 3des des aes }
设置 ESP 协议不对报文进行加密	undo esp encryption-algorithm
设置 ESP 协议采用的验证算法	esp authentication-algorithm { md5 sha1 }
设置 ESP 协议不对报文进行验证	undo esp authentication-algorithm
设置 AH 协议采用的验证算法	ah authentication-algorithm { md5 sha1 }
恢复 AH 协议缺省的验证算法	undo ah authentication-algorithm

ESP 协议允许对报文同时进行加密和验证，或只加密，或只验证。注意，**undo esp authentication-algorithm** 命令不是恢复验证算法为缺省算法，而是设置验证算法为空，即不验证。当加密算法为空时，**undo esp authentication-algorithm** 命令失效。AH 协议没有加密的功能，只对报文进行验证。**undo ah authentication-algorithm** 命令用来恢复 AH 协议缺省验证算法（md5）。在安全隧道的两端设置的安全策略所引用的安全提议必须设置成采用同样的验证算法和/或加密算法。

Comware 主体软件及加密卡中 ESP 协议支持的安全加密算法有三种：**des**、**3des** 和 **aes**；支持的安全认证算法有 **hmac-md5** 和 **hmac-sha1**。

Comware 主机软件及加密卡中 AH 协议支持的认证算法有 **hmac-md5** 和 **hmac-sha1** 两种。

缺省情况下，ESP 协议采用的加密算法是 **des**，采用的验证算法是 **md5**；AH 协议采用的验证算法是 **md5**。

 说明：

必须首先通过 **transform** 命令选择了相应的安全协议后，该安全协议所需的安全算法才可配置。例如，如果使用 **transform** 命令选择了 **esp**，那么只有 ESP 所需的安全算法才可配置，而 AH 所需的安全算法则不能配置。

4.2.3 创建安全策略

安全策略规定了对什么样的数据流采用什么样的安全提议。安全策略分为手工安全策略和 IKE 协商安全策略，前者需要用户手工配置密钥、SPI 等参数，在隧道模式下还需要手工配置安全隧道两个端点的 IP 地址；后者则由 IKE 自动协商生成这些参数。

 说明：

本节将全面介绍安全策略的各项配置，包括手工协商方式所需的配置和 IKE 协商所需的配置。对于仅用于某种协商方式下的配置，会特别标明；没有特别标明的配置项，则表示手工方式和 IKE 协商方式下均需配置。

1. 手工创建安全策略

(1) 手工创建安全策略

一旦安全策略已经创建，就不能再修改它的协商方式。例如：创建了 **manual** 方式的安全策略，就不能修改成 **isakmp** 方式，而必须先删除这条安全策略然后再重新创建。

请在系统视图下进行下列配置。

表4-6 创建安全策略

操作	命令
用手工方式创建安全联盟的安全策略	ipsec policy <i>policy-name seq-number manual</i>
修改安全联盟的安全策略	ipsec policy <i>policy-name seq-number manual</i>
删除安全策略	undo ipsec policy <i>policy-name [seq-number]</i>

具有相同名称、不同顺序号的安全策略共同构造一个安全策略组，在一个安全策略组中最大可以设置 500 条安全策略。并且，所有安全策略的总数也不能超过 500。在一个安全策略组中，顺序号越小的安全策略，优先级越高。

缺省情况下，没有安全策略存在。

(2) 配置在安全策略中引用安全提议

安全策略通过引用安全提议来确定采用的安全协议、算法和报文封装形式。在引用一个安全提议之前，这个安全提议必须已经建立。

请在安全策略视图下进行下列配置。

表4-7 在安全策略中应用安全提议

操作	命令
设置安全策略所引用的安全提议	proposal <i>proposal-name1</i> [<i>proposal-name2... proposal-name6</i>]
取消安全策略引用的安全提议	undo proposal [<i>proposal-name</i>]

通过手工（**manual**）方式建立安全联盟，一条安全策略只能引用一个安全提议，并且如果已经设置了安全提议，必须先取消原先的安全提议才能设置新的安全提议。在安全隧道的两端设置的安全策略所引用的安全提议必须设置成采用同样的安全协议、算法和报文封装形式。

(3) 配置在安全策略中引用的访问控制列表

安全策略引用访问控制列表，IPsec 根据该访问控制列表中的规则来确定哪些报文需要安全保护，哪些报文不需要安全保护。访问控制列表匹配（**permit**）的报文被保护，访问控制列表拒绝（**deny**）的报文不被保护。

请在安全策略视图下进行下列配置。

表4-8 设置安全策略引用的访问控制列表

操作	命令
设置安全策略引用的访问控制列表	security acl <i>acl-number</i>
取消安全策略引用的访问控制列表	undo security acl

一条安全策略只能引用一条访问控制列表，如果设置安全策略引用了多于一个访问控制列表，最后配置的那条访问控制列表才有效。

对于手工方式创建的安全策略，只支持保护访问控制列表下的一条规则，即只有最先匹配此访问控制列表的报文被保护，后续匹配此访问控制列表中其它规则的报文不会被保护。

(4) 配置隧道的起点与终点

通常人们把应用安全策略的通道称为“安全隧道”。安全隧道是建立在本端和对端网关之间，所以必须正确设置本端地址和对端地址才能成功地建立起一条安全隧道。请在安全策略视图下进行下列配置。

表4-9 配置隧道的起点与终点

操作	命令
设置安全策略的本端地址	tunnel local <i>ip-address</i>
删除在安全策略中设定的本端地址	undo tunnel local
设置安全策略的对端地址	tunnel remote <i>ip-address</i>
删除安全策略中设置的对端地址	undo tunnel remote [<i>ip-address</i>]

对于 **manual** 方式的安全策略，必须正确设置本端地址和对端地址才能成功地建立一条安全隧道，而 **isakmp** 方式的安全策略则不需要配置本端和对端地址，通过安全联盟自动协商可以获得。

(5) 配置安全联盟的 SPI

此配置任务仅用于 **manual** 方式的安全策略。用下列命令手工配置安全联盟的 SPI，实现手工创建安全联盟（对于 **isakmp** 方式的安全策略，不需要手工配置，IKE 将自动协商安全联盟的 SPI 并创建安全联盟）。

请在安全策略视图下进行下列配置。

表4-10 配置安全联盟的 SPI

操作	命令
配置安全联盟的 SPI	sa spi { inbound outbound } { ah esp } <i>spi-number</i>
删除安全联盟的 SPI	undo sa spi { inbound outbound } { ah esp }

在为系统配置安全联盟时，必须分别设置 **inbound** 和 **outbound** 两个方向的安全联盟的参数。

在安全隧道的两端设置的安全联盟参数必须是完全匹配的。本端的入方向安全联盟的 SPI 必须和对端的出方向安全联盟的 SPI 一样；本端的出方向安全联盟的 SPI 必须和对端的入方向安全联盟的 SPI 一样。

(6) 配置安全联盟使用的密钥

此配置任务仅用于 **manual** 方式的安全策略，用如下命令手工输入安全联盟的密钥（对于采用 **isakmp** 协商方式的安全策略，无需手工配置密钥，IKE 将自动协商安全联盟的密钥）。

请在安全策略视图下进行下列配置。

表4-11 配置安全联盟使用的密钥

操作	命令
配置协议的验证密钥 (以 16 进制方式输入)	sa authentication-hex { inbound outbound } { ah esp } hex-key
配置协议的密钥 (以字符串方式输入)	sa string-key { inbound outbound } { ah esp } string-key
配置 ESP 协议的加密密钥 (以 16 进制方式输入)	sa encryption-hex { inbound outbound } esp hex-key
删除设置的安全联盟的参数	undo sa string-key { inbound outbound } { ah esp } undo sa authentication-hex { inbound outbound } { ah esp } undo encryption-hex { inbound outbound } esp

在安全隧道的两端设置的安全联盟参数必须是完全匹配的。本端的入方向安全联盟的 SPI 及密钥必须和对端的出方向安全联盟的 SPI 及密钥一样；本端的出方向安全联盟的 SPI 及密钥必须和对端的入方向安全联盟的 SPI 及密钥一样。

如果分别以两种方式输入了密钥，则最后设定的密钥有效。在安全隧道的两端，应当以相同的方式输入密钥。如果一端以字符串方式输入密钥，另一端以 16 进制方式输入密钥，则不能正确地建立安全隧道。

2. 用 IKE 创建安全策略

IKE 创建安全策略的配置包括：

- 用 IKE 创建安全策略
- 配置安全策略中引用的安全提议
- 配置安全策略引用的访问控制列表
- 配置安全策略引用的 IKE 对等体
- 配置安全联盟的生存时间（可选）
- 配置协商时使用的 PFS 特性（可选）
- 配置 IPsec DPD（可选）

(1) 用 IKE 创建安全策略

请在系统视图下进行下列配置。

表4-12 创建安全策略

操作	命令
用 IKE 创建安全策略，进入安全策略视图	ipsec policy <i>policy-name</i> <i>seq-number</i> isakmp
用 IKE 并采用策略模板动态创建安全策略	ipsec policy <i>policy-name</i> <i>seq-number</i> isakmp [template <i>template-name</i>]
修改通过 IKE 协商建立的安全策略	ipsec policy <i>policy-name</i> <i>seq-number</i> isakmp
删除安全策略	undo ipsec policy <i>policy-name</i> [<i>seq-number</i>]

若采用策略模板动态创建安全策略，则必须预先定义策略模板，策略模板的定义请参见 4.2.4 配置安全策略模板。

(2) 配置在安全策略中引用安全提议

安全策略通过引用安全提议来确定采用的安全协议、算法和报文封装形式。在引用一个安全提议之前，这个安全提议必须已经建立。

请在安全策略视图下进行下列配置。

表4-13 在安全策略中应用安全提议

操作	命令
设置安全策略所引用的安全提议	proposal <i>proposal-name1</i> [<i>proposal-name2</i> ... <i>proposal-name6</i>]
取消安全策略引用的安全提议	undo proposal [<i>proposal-name</i>]

通过 IKE (**isakmp**) 协商建立安全联盟，一条安全策略最多可以引用六个安全提议，IKE 协商将在安全隧道的两端搜索能够完全匹配的安全提议。如果 IKE 在两端找不到完全匹配的安全提议，则安全联盟不能建立，需要被保护的报文将被丢弃。

(3) 配置在安全策略中引用的访问控制列表

安全策略引用访问控制列表，IPsec 根据该访问控制列表中的规则来确定哪些报文需要安全保护，哪些报文不需要安全保护：访问控制列表匹配 (**permit**) 的报文被保护，访问控制列表拒绝 (**deny**) 的报文不被保护。

请在安全策略视图下进行下列配置。

表4-14 设置安全策略引用的访问控制列表

操作	命令
设置安全策略引用的访问控制列表	security acl <i>acl-number</i>
取消安全策略引用的访问控制列表	undo security acl

一条安全策略只能引用一条访问控制列表，如果设置安全策略引用了多于一个访问控制列表，最后配置的那条访问控制列表才有效。

(4) 配置在安全策略中引用 IKE 对等体

对于 IKE 协商方式，无需像手工方式那样配置对等体、SPI 和密钥等参数，IKE 将自动协商它们，因而仅需要将安全策略和 IKE Peer 关联即可。在引用一个 IKE 对等体之前，该 IKE 对等体必须已经建立。

请在安全策略视图下进行下列配置。

表4-15 设置安全策略引用的访问控制列表

操作	命令
在安全策略中引用 IKE 对等体。	ike-peer <i>peer-name</i>
取消在安全策略中引用 IKE 对等体。	undo ike-peer [<i>peer-name</i>]

说明：

本章仅介绍了 IPsec 对 IKE Peer 的引用，实际在 IKE Peer 视图下还需要进行一些 IKE 相关参数的设置，包括 IKE 的协商模式、ID 类型、NAT 穿越、共享密钥、对端地址和对端名称等。有关 IKE Peer 的配置，请参考下一章的内容。

(5) 配置安全联盟的生存周期（可选）

(a) 配置全局的安全联盟生存周期

所有在安全策略视图下没有单独配置生存周期的安全联盟，都采用全局生存周期。IKE 为 IPsec 协商建立安全联盟时，对于 IKE 第 1 阶段，安全联盟的生存周期由发起方决定；对于 IKE 第 2 阶段，采用本地设置的和对端提议的生存周期中较小的一个。

有两种类型的生存周期：“基于时间”的生存周期和“基于流量”的生存周期。无论哪一种类型的生存周期先到期，安全联盟都会失效。安全联盟快要失效前，IKE 将为 IPsec 协商建立新的安全联盟，这样在旧的安全联盟失效时新的安全联盟就已经准备好。

请在系统视图下进行下列配置。

表4-16 配置全局的安全联盟生存周期

操作	命令
设置全局的安全联盟（SA）生存周期	ipsec sa global-duration { traffic-based <i>kilobytes</i> time-based <i>seconds</i> }
恢复全局的安全联盟（SA）生存周期为缺省值	undo ipsec sa global-duration { traffic-based time-based }

改变全局生存周期，不会影响单独配置了自己的生存周期的安全策略，也不会对已经建立的安全联盟产生影响，但是在以后的 IKE 协商中会用于建立新的安全联盟。

生存周期只对通过 **isakmp** 方式建立的安全联盟有效，对通过 **manual** 方式建立的安全联盟没有生存周期的限制，即手工建立的安全联盟永远不会失效。

(b) 配置安全联盟的生存周期

为安全策略设置单独的安全联盟生存周期，如果没有单独设置生存周期，则采用设定的全局生存周期。

IKE 为 IPsec 协商建立安全联盟时，对于 IKE 第 1 阶段，安全联盟的生存周期由发起方决定；对于 IKE 第 2 阶段，采用本地设置的和对端提议的生存周期中较小的一个。

请在安全策略视图下进行下列配置。

表4-17 配置安全联盟生存周期

操作	命令
设置安全策略安全联盟的生存周期	sa duration { traffic-based kilobytes time-based seconds }
恢复使用设定的全局生存周期	undo sa duration { traffic-based time-based }

改变生存周期，不会影响已经建立的安全联盟，但是在以后的 IKE 协商中会用于建立新的安全联盟。

(6) 配置协商时使用的 PFS 特性（可选）

PFS（Perfect Forward Secrecy，完善的前向安全性）是一种安全特性，指一个密钥被破解，并不影响其他密钥的安全性，因为这些密钥间没有派生关系。此特性是通过在 IKE 阶段 2 的协商中增加密钥交换来实现的。

请在安全策略视图下进行下列配置。

表4-18 设置协商时使用的 PFS 特性

操作	命令
设置协商时使用的 PFS 特性	pfs { dh-group1 dh-group2 dh-group5 dh-group14 }
设置在协商时不使用 PFS 特性	undo pfs

IKE 在使用此安全策略发起一个协商时，进行一个 PFS 交换。如果本端指定了 PFS，对端在发起协商时必须是 PFS 交换。本端和对端指定的 DH 组必须一致，否则协商会失败。

group1、**group2**、**group5**、**group14** 能够依次提供更高的安全性，但是需要更长的计算时间。

缺省情况下，不使用 PFS 特性。

(7) 配置 IPsec DPD (可选)

- 创建 DPD 结构

请在系统视图下进行下面配置。

表4-19 创建 DPD 结构并进入 DPD 结构视图

操作	命令
创建 DPD 结构并进入 DPD 结构视图	ike dpd dpd-name
删除一个 DPD 结构	undo ike dpd dpd-name

DPD 数据结构（简称为 DPD 结构）用于配置 DPD 查询参数，包括 DPD 查询时间间隔及等待 DPD 应答报文超时时间间隔。该数据结构可以被多个 IKE Peer 引用，这样用户不必针对接口一一进行重复配置。如果 DPD 结构已经被 IKE Peer 引用，则不能删除。

- 配置定时器

请在 DPD 结构视图下进行下面配置。

表4-20 配置定时器

操作	命令
配置触发 DPD 查询的时间间隔	interval-time seconds
恢复触发 DPD 查询的时间间隔的缺省值	undo interval-time
配置等待 DPD 应答报文的超时时间	time-out seconds
恢复等待 DPD 应答报文超时时间为缺省值	undo time-out

缺省情况下，DPD 查询的时间间隔为 10 秒，等待 DPD 应答报文的超时时间为 5 秒。

- 为 IKE Peer 指定 DPD 结构

请在 IKE Peer 视图下进行下面配置。

表4-21 为 IKE Peer 指定 DPD 结构

操作	命令
为 IKE Peer 指定 DPD 结构	dpd dpd-name
取消 IKE Peer 的 DPD 结构	undo dpd

4.2.4 配置安全策略模板

在采用 IKE 方式创建安全策略时，除直接在安全策略视图下配置安全策略外，还可以通过引用安全策略模板来创建安全策略。在这种情况下，我们应先在安全策略模板中配置好所有的安全策略。

安全策略模板的配置与普通的安全策略配置相似，首先创建一个策略模板，然后配置模板的参数。

请在系统视图下进行下列配置。

表4-22 创建安全策略模板

操作	命令
创建/修改 IPsec 安全策略模板	ipsec policy-template <i>template-name</i> <i>seq-number</i>
删除安全策略模板	undo ipsec policy-template <i>policy-template-name</i> [<i>seq-number</i>]

执行上面的创建命令，会进入 IPsec 策略模板视图，在此视图下，可以配置策略模板的参数。

说明：

安全策略模板可配置的参数与 isakmp 方式的 IPsec 安全策略相同，只是很多参数是可选的。必须配置的参数只有 IPsec 安全提议和 IKE 对等体（在 IKE 对等体中无需配置对方的 IP 地址），而保护的数据流、PFS 特性可以不配置。但需要注意的是，如果配置了这些参数中的一个或几个，则在协商时这些参数必须匹配。

在策略模板配置完成后，还需要使用如下命令引用所定义的策略模板：

表4-23 引用安全策略模板

操作	命令
引用 IPsec 安全策略模板	ipsec policy <i>policy-name</i> <i>seq-number</i> isakmp template <i>template-name</i>

当某一个安全策略引用了安全策略模板后，就不能够再进入其安全策略视图下配置或修改安全策略了，只能进入安全策略模板视图下配置或修改。



注意：

不能用应用策略模板的安全策略来发起安全联盟的协商，但可以响应协商。

4.2.5 在接口上应用安全策略组

为使定义的安全联盟生效，应在每个要加密的出站数据、解密的入站数据所在接口（逻辑的或物理的）上应用一个安全策略组，由这个接口根据所配置的安全策略组和对端加密防火墙配合进行报文的加密处理。当安全策略组被从接口上删除后，此接口便不再具有 IPsec 的安全保护功能。

请在接口视图下进行下列配置。

表4-24 应用安全策略组

操作	命令
应用安全策略组	ipsec policy <i>policy-name</i>
取消应用的安全策略组	undo ipsec policy [<i>policy-name</i>]

一个接口只能应用一个安全策略组，一个安全策略组可以应用到多个接口上。但手工方式配置的安全策略只能应用到一个接口。

当从一个接口发送报文时，将按照从小到大的顺序号查找安全策略组中每一条安全策略。如果报文匹配了一条安全策略引用的访问控制列表，则使用这条安全策略对报文进行处理；如果报文没有匹配安全策略引用的访问控制列表，则继续查找下一条安全策略；如果报文对所有安全策略引用的访问控制列表都不匹配，则报文直接被发送（IPsec 不对报文加以保护）。

防火墙实现的 IPsec 安全策略除了可以应用到串口、以太网口等实际物理接口上之外，还能够应用到 Tunnel、Virtual Template 等虚接口上。这样就可以根据实际组网要求，在如 GRE、L2TP 等隧道上应用 IPsec。

当在所有接口上都删除了安全策略后，才会删除所有的 IKE SA，否则需要手工删除或等到 IKE SA 超时。

4.2.6 配置取消对 next payload 域的检查

Next payload 是指在 IKE 协商报文（由几个 payload 组装而成）的最后一个 payload 的通用头中 Next Payload 域。按协议规定该域必须为 0，但某些公司的设备会将该域赋其它值，为增强设备的互通性，可以通过以下命令取消 IPsec 协商过程对该域的检查。

表4-25 配置取消对 next payload 域的检查

操作	命令
配置在 IPsec 协商过程中取消对最后一个 payload 的 next payload 域的检查	ike next-payload check disabled
恢复缺省设置	undo ike next-payload check disabled

缺省情况下，检查 next payload 域。

4.2.7 配置 IPsec 分片报文缓存处理

当接口上配置 IPsec 安全策略时，接口上发送和接收的报文都需要与安全策略中的 ACL 进行匹配，然后进行 IPsec 相关处理。

当报文为分片报文时，后续分片因为不含有端口等信息无法正确匹配安全策略。

- 当分片报文顺序到达时，即首片报文先于非首片报文到达时，首片报文会创建分片表项，并且匹配安全策略后填写分片表项内容。后续非首片报文匹配分片表项后，进行 IPsec 相关处理。
- 当非首片报文先于首片报文到达时，由于无法找到分片表项进行匹配，需要等待首片。IPsec 缓存分片报文机制将缓存等待中的非首片报文，等待首片报文到达之后再进行处理。

1. 配置 IPsec 分片报文缓存机制

请在系统视图下进行下面配置。

表4-26 配置 IPsec 分片报文缓存机制

操作	命令
使能入方向的 IPsec 分片报文缓存机制	ipsec fragment-chain inbound enable
关闭入方向的 IPsec 分片报文缓存机制	ipsec fragment-chain inbound disable
使能出方向的 IPsec 分片报文缓存机制	ipsec fragment-chain outbound enable
关闭出方向的 IPsec 分片报文缓存机制	ipsec fragment-chain outbound disable

缺省情况下，关闭 IPsec 分片报文缓存机制，即非首片报文先于首片报文到达时，非首片报文将被丢弃。

2. 配置 IPsec 分片报文缓存超时时间

请在系统视图下进行下面配置。

表4-27 配置 IPsec 分片报文缓存超时时间

操作	命令
配置 IPsec 分片报文缓存超时时间	ipsec fragment-chain timeout seconds

缺省情况下，IPsec 分片报文缓存超时时间为 3 秒。

4.2.8 加密卡可选配置

加密卡的主要配置与 IPsec 的配置过程相同，请参见本章的前面各节，以下为加密卡的可选配置，请根据需要进行选配。

1. 进入加密卡接口视图并且使能加密卡

当防火墙上有多块加密卡在并行工作时，可以通过 **undo shutdown** 和 **shutdown** 命令灵活的管理各加密卡。根据应用的需要可以将该加密卡设置为不可用状态（禁止该加密卡进行数据处理）或可用状态，便于维护管理和调试。对处于 **shutdown** 状态下的加密卡执行 **undo shutdown** 命令将复位并初始化该加密卡。

可以通过 **interface encrypt** 命令进入相应槽位的加密卡，并且在加密卡视图下完成使能/禁止加密卡的操作。

请在系统视图下完成下面配置。

表4-28 进入加密卡接口视图

操作	命令
进入加密卡接口视图	interface encrypt slot-id

请在加密卡接口视图下进行下列配置。

表4-29 使能/禁止加密卡

操作	命令
使能加密卡	undo shutdown
禁用加密卡	shutdown

缺省情况下，使能所有加密卡。

2. 使能 Comware 主体软件备份

对于应用于加密卡侧的安全联盟，只要该加密卡工作状态正常，IPsec 处理就由状态正常的加密卡进行处理。当该加密卡状态异常时，则无法完成 IPsec 处理。此时如果已经开启主机备份处理开关，并且 Comware 主体软件 IPsec 模块支持该安全联盟所使用的加密/认证算法，则由 Comware 主体软件 IPsec 模块替代加密卡进行 IPsec 处理；若 Comware 主体软件 IPsec 模块不支持该安全联盟使用的算法，则报文被丢弃。

请在系统视图下进行下列配置。

表4-30 使能/禁用主机备份处理

操作	命令
使能主机备份处理	encrypt-card backuped
禁用主机备份处理	undo encrypt-card backuped

缺省情况下，禁用主机备份处理。

3. 配置加密卡快转功能

加密卡快转指的是对于[SourIP, SourPort, DestIP, DestPort, Prot] 五元组相同的一系列报文，防火墙在接收或发送第一个报文时就会创建一个快转表项，之后符合此表项的所有报文都会直接被发往加密卡进行加密或解密，然后再由加密卡发往目的出口。这样省去了对每个报文逐一进行从 IP 到 IPsec 的处理，加速了处理过程。

请在系统视图下进行如下配置。

表4-31 配置加密卡快转功能

操作	命令
使能加密卡快转功能	encrypt-card fast-switch
关闭加密卡快转功能	undo encrypt-card fast-switch

缺省情况下，关闭加密卡快转功能。



注意：

开启加密卡快转功能后，经过加密卡快转的报文将不进行 ACL 的统计计数。

4. 配置加密卡的简单网管操作

为了更加便于管理和维护，加密卡支持通过 SNMP 协议远程管理。通过与防火墙的网管功能结合，可以在网管终端查询加密卡的状态并监控 trap 信息。其中可监控的 trap 信息包括加密卡的复位信息、状态变迁信息以及报文处理过程中的异常丢包信息等。

该命令在系统视图下进行如下配置。

表4-32 使能/关闭加密卡 trap 信息开关

操作	命令
使能加密卡 trap 信息开关	snmp-agent trap enable encrypt-card
关闭加密卡 trap 信息开关	undo snmp-agent trap enable encrypt-card

缺省情况下，加密卡 trap 信息开关是打开的。

4.3 IPsec 显示与调试

4.3.1 Comware 主体软件 IPsec 的显示与调试

1. IPsec 显示与调试

IPsec 提供以下命令显示安全联盟、安全联盟生存周期、安全提议、安全策略的信息以及 IPsec 处理的报文的统计信息。

display 命令可在所有视图下进行操作，**debugging** 命令只能在用户视图下操作。

表4-33 IPsec 显示与调试

操作	命令
显示安全联盟的相关信息	display ipsec sa [<i>brief</i> <i>remote ip-address</i> <i>policy policy-name</i> [<i>seq-number</i>] <i>duration</i>]
显示 IPsec 的隧道信息	display ipsec tunnel
显示 IPsec 处理报文的统计信息	display ipsec statistics
显示安全提议的信息	display ipsec proposal [<i>proposal-name</i>]
显示安全策略的信息	display ipsec policy [<i>brief</i> <i>name policy-name</i> [<i>seq-number</i>]]
显示安全策略模板的信息	display ipsec policy-template [<i>brief</i> <i>name policy-name</i> [<i>seq-number</i>]]
显示 IPsec 分片报文的缓存信息	display ipsec fragment buffer-chain
显示 IPsec 分片报文的统计信息	display ipsec fragment statistics
显示 DPD 的配置信息	display ike dpd [<i>dpd-name</i>]
打开 IPsec 的调试功能	debugging ipsec { <i>all</i> <i>sa</i> <i>packet</i> [<i>policy policy-name</i> [<i>seq-number</i>] <i>parameters ip-address protocol spi-number</i>] <i>fragment</i> <i>misc</i> }
禁止 IPsec 的调试功能	undo debugging ipsec { <i>all</i> <i>sa</i> <i>packet</i> [<i>policy policy-name</i> [<i>seq-number</i>] <i>parameters ip-address protocol spi-number</i>] <i>fragment</i> <i>misc</i> }
打开 DPD 的调试功能	debugging ike dpd
禁止 DPD 的调试功能	undo debugging ike dpd

2. 清除 IPsec 的报文统计信息

此配置任务清除 IPsec 的报文统计信息，所有的统计信息都被设置成 0。

请在用户视图下进行下列操作。

表4-34 清除 IPsec 的报文统计信息

操作	命令
清除 IPsec 的报文统计信息	reset ipsec statistics

3. 清除 IPsec 分片报文统计信息

此配置任务清除 IPsec 分片报文统计信息，所有的统计信息都被设置成零。

请在用户视图下进行下列操作。

表4-35 清除 IPsec 分片报文统计信息

操作	命令
清除 IPsec 分片报文统计信息	reset ipsec fragment statistics

4. 清除 IPsec 分片报文缓存队列

此配置清除 IPsec 缓存队列中分片报文，所有缓存队列中的分片报文将被丢弃。

请在用户视图下进行下列操作。

表4-36 清除 IPsec 分片报文缓存队列

操作	命令
清除 IPsec 缓存队列中的分片报文	reset ipsec fragment buffer-chain

5. 删除安全联盟

此配置任务删除已经建立的安全联盟（无论是手工建立的还是通过 IKE 协商建立的）。如果未指定参数，则删除所有的安全联盟。

请在用户视图下进行下列操作。

表4-37 删除安全联盟

操作	命令
删除安全联盟	reset ipsec sa [<i>remote ip-address</i> <i>policy policy-name</i> [<i>seq-number</i>]] parameters <i>ip-address protocol spi-number</i>]

对于通过 IKE 协商建立的安全联盟，被删除后如果有报文重新触发 IKE 协商，IKE 将重新协商建立安全联盟。

对于手工建立的安全联盟，被删除后系统会根据手工设置的参数立即创建新的安全联盟。

如果指定参数 **parameters**, 由于安全联盟是成对出现的, 删除了一个方向安全联盟, 另一个方向安全联盟也随之被删除。

4.3.2 加密卡 IPsec 的显示与调试

1. 加密卡 IPsec 的显示与调试

加密卡可以提供下面的命令用来显示安全联盟信息、统计信息、系统日志、接口信息以及主机备份信息。

display 命令可在所用视图下操作, 而 **debugging** 命令则只能在用户视图下操作。具体显示和调试命令如下表所示:

表4-38 加密卡的显示和调试命令

操作	命令
显示加密卡的接口信息	display interface encrypt [<i>slot-id</i>]
显示加密卡的快转表项	display encrypt-card fast-switch
打开加密卡侧 Comware 主体测试软件的调试开关	debugging encrypt-card host { all packet sa command error misc }
禁止加密卡侧 Comware 主体测试软件的调试开关	undo debugging encrypt-card host { all packet sa command error misc }

2. 清除加密卡的统计信息

此配置命令清除加密卡上的统计信息。

请在用户视图下进行下列配置。

表4-39 清除加密卡的统计信息

操作	命令
清除加密卡的统计信息	reset counters interface encrypt [<i>slot-id</i>]

3. 清除加密卡侧的安全联盟

此配置命令清除加密卡侧已配置的安全联盟, 无论是手工创建的还是 IKE 协商创建的。

请在用户视图下进行下列配置。

表4-40 清除加密卡侧的安全联盟

操作	命令
清除加密卡侧联盟	reset encrypt-card sa [<i>slot-id</i>]

 说明:

目前的加密卡尚不支持此命令。

4. 清除加密卡侧的报文统计信息

此命令用来清除加密卡侧所有的统计信息的计数器，其中包括数据包统计、字节数统计、丢包统计、认证失败统计、错误 SA 统计、非法加密卡安全提议统计、非法协议统计等信息。

请在用户视图下进行下面配置。

表4-41 清除加密卡报文统计信息

操作	命令
清除加密卡侧报文统计信息	reset encrypt-card statistics [slot-id]

 说明:

目前的加密卡尚不支持此命令。

5. 清除加密卡系统日志信息

此命令用来清除加密卡侧的日志统计信息。加密卡的日志中记录了到清除命令下发前对加密卡所做的关键操作的信息。

请在用户视图下进行下面配置。

表4-42 清除加密卡日志统计信息

操作	命令
清除加密卡侧日志信息	reset encrypt-card syslog [slot-id]

 说明:

目前的加密卡尚不支持此命令。

6. 清除加密卡的快速转发信息

此命令用来清除加密卡侧的快速转发表项信息。

请在用户视图下进行下面配置。

表4-43 清除加密卡的快速转发信息

操作	命令
清除加密卡的快速转发信息	reset encrypt-card fast-switch

4.4 IPsec 典型配置案例

4.4.1 采用 manual 方式建立安全联盟的配置

1. 组网需求

在 SecPath A 和 SecPathB 之间建立一个安全隧道，对 PC A 代表的子网（10.1.1.x）与 PC B 代表的子网（10.1.2.x）之间的数据流进行安全保护。安全协议采用 ESP 协议，加密算法采用 DES，验证算法采用 SHA1-HMAC-96。

2. 组网图

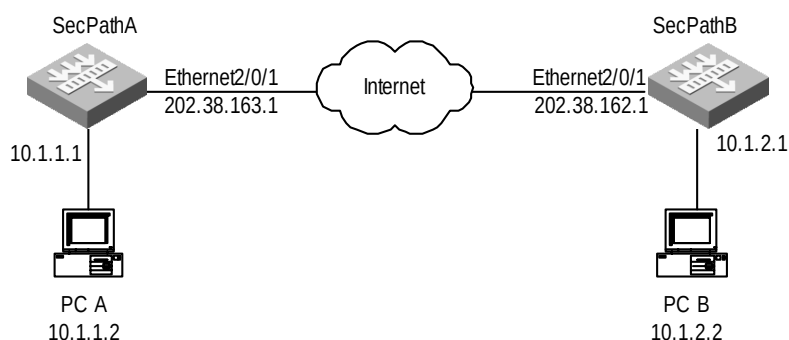


图4-3 IPsec 配置组网图

3. 配置步骤

(1) 配置 SecPathA

配置一个访问控制列表，定义由子网 10.1.1.x 去子网 10.1.2.x 的数据流。

```
[H3C] acl number 3101
[H3C-acl-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination
10.1.2.0 0.0.0.255
[H3C-acl-adv-3101] rule deny ip source any destination any
```

配置到 PC B 的静态路由。

```
[H3C] ip route-static 10.1.2.0 255.255.255.0 202.38.162.1
```

创建名为 tran1 的安全提议。

```
[H3C] ipsec proposal tran1
```

报文封装形式采用隧道视图。

```
[H3C-ipsec-proposal-tran1] encapsulation-mode tunnel
# 安全协议采用 ESP 协议。

[H3C-ipsec-proposal-tran1] transform esp
# 选择算法。

[H3C-ipsec-proposal-tran1] esp encryption-algorithm des
[H3C-ipsec-proposal-tran1] esp authentication-algorithm sha1
# 退回到系统视图。

[H3C-ipsec-proposal-tran1] quit
# 创建一条安全策略，协商方式为 manual。

[H3C] ipsec policy map1 10 manual
# 引用访问控制列表。

[H3C-ipsec-policy-manual-map1-10] security acl 3101
# 引用安全提议。

[H3C-ipsec-policy-manual-map1-10] proposal tran1
# 设置对端地址。

[H3C-ipsec-policy-manual-map1-10] tunnel remote 202.38.162.1
# 设置本端地址。

[H3C-ipsec-policy-manual-map1-10] tunnel local 202.38.163.1
# 设置 SPI。

[H3C-ipsec-policy-manual-map1-10] sa spi outbound esp 12345
[H3C-ipsec-policy-manual-map1-10] sa spi inbound esp 54321
# 设置密钥。

[H3C-ipsec-policy-manual-map1-10] sa string-key outbound esp abcdefg
[H3C-ipsec-policy-manual-map1-10] sa string-key inbound esp gfedcba
[H3C-ipsec-policy-manual-map1-10] quit
# 配置 Ethernet2/0/1。

[H3C] interface ethernet 2/0/1
[H3C-Ethernet2/0/1] ip address 202.38.163.1 255.0.0.0
# 应用安全策略组。

[H3C-Ethernet2/0/1] ipsec policy map1
```

(2) 配置 SecPathB

配置一个访问控制列表，定义由子网 10.1.2.x 去子网 10.1.1.x 的数据流。

```
[H3C] acl number 3101
[H3C-acl-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination
10.1.1.0 0.0.0.255
```

```
[H3C-acl-adv-3101] rule deny ip source any destination any
[H3C-acl-adv-3101] quit
# 配置到 PC A 的静态路由。

[H3C] ip route-static 10.1.1.0 255.255.255.0 202.38.163.1
# 创建名为 tran1 的安全提议。

[H3C] ipsec proposal tran1
# 报文封装形式采用隧道模式。

[H3C-ipsec-proposal-tran1] encapsulation-mode tunnel
# 安全协议采用 ESP 协议。

[H3C-ipsec-proposal-tran1] transform esp
# 选择算法。

[H3C-ipsec-proposal-tran1] esp encryption-algorithm des
[H3C-ipsec-proposal-tran1] esp authentication-algorithm sha1
# 退回到系统视图。

[H3C-ipsec-proposal-tran1] quit
# 创建一条安全策略，协商方式为 manual。

[H3C] ipsec policy use1 10 manual
# 引用访问控制列表。

[H3C-ipsec-policy-manual-use1-10] security acl 3101
# 引用安全提议。

[H3C-ipsec-policy-manual-use1-10] proposal tran1
# 设置对端地址。

[H3C-ipsec-policy-manual-use1-10] tunnel remote 202.38.163.1
# 设置本端地址。

[H3C-ipsec-policy-manual-use1-10] tunnel local 202.38.162.1
# 设置 SPI。

[H3C-ipsec-policy-manual-use1-10] sa spi outbound esp 54321
[H3C-ipsec-policy-manual-use1-10] sa spi inbound esp 12345
# 设置密钥。

[H3C-ipsec-policy-manual-use1-10] sa string-key outbound esp gfedcba
[H3C-ipsec-policy-manual-use1-10] sa string-key inbound esp abcdefg
[H3C-ipsec-policy-manual-use1-10] quit
# 配置 Ethernet2/0/1。

[H3C] interface ethernet 2/0/1
```

配置的 IP 地址。

```
[H3C-Ethernet2/0/1] ip address 202.38.162.1 255.0.0.0
```

应用安全策略组。

```
[H3C-Ethernet2/0/1] ipsec policy use1
```

以上配置完成后, SecPathA 和 SecPathB 之间的安全隧道就建立好了, 子网 10.1.1.x 与子网 10.1.2.x 之间的数据流将被加密传输。

4.4.2 采用 isakmp 方式建立安全联盟的配置

1. 组网需求

如上例图所示, 在 SecPathA 和 SecPathB 之间建立一个安全隧道, 对 PC A 代表的子网 (10.1.1.x) 与 PC B 代表的子网 (10.1.2.x) 之间的数据流进行安全保护。安全协议采用 ESP 协议, 加密算法采用 DES, 验证算法采用 SHA1-HMAC-96。

2. 组网图

见图 4-3。

3. 配置步骤

(1) 配置 SecPathA

配置一个访问控制列表, 定义由子网 10.1.1.x 去子网 10.1.2.x 的数据流。

```
[H3C] acl number 3101
```

```
[H3C-acl-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination  
10.1.2.0 0.0.0.255
```

```
[H3C-acl-adv-3101] rule deny ip source any destination any
```

配置到 PC B 的静态路由。

```
[H3C] ip route-static 10.1.2.0 255.255.255.0 202.38.162.1
```

创建名为 tran1 的安全提议。

```
[H3C] ipsec proposal tran1
```

报文封装形式采用隧道模式。

```
[H3C-ipsec-proposal-tran1] encapsulation-mode tunnel
```

安全协议采用 ESP 协议。

```
[H3C-ipsec-proposal-tran1] transform esp
```

选择算法。

```
[H3C-ipsec-proposal-tran1] esp encryption-algorithm des
```

```
[H3C-ipsec-proposal-tran1] esp authentication-algorithm sha1
```

退回到系统视图。

```
[H3C-ipsec-proposal-tran1] quit
# 配置 IKE 对等体。

[H3C] ike peer peer
[H3C-ike-peer-peer] pre-shared-key abcde
[H3C-ike-peer-peer] remote-address 202.38.162.1
# 创建一条安全策略，协商方式为 isakmp。

[H3C] ipsec policy map1 10 isakmp
# 引用安全提议。

[H3C-ipsec-policy-isakmp-map1-10] proposal tran1
# 引用访问控制列表。

[H3C-ipsec-policy-isakmp-map1-10] security acl 3101
# 引用 IKE 对等体。

[H3C-ipsec-policy-isakmp-map1-10] ike-peer peer
# 退回到系统视图。

[H3C-ipsec-policy-isakmp-map1-10] quit
# 进入配置视图。

[H3C] interface ethernet 2/0/1
# 配置的 IP 地址。

[H3C-Ethernet2/0/1] ip address 202.38.163.1 255.0.0.0
# 应用安全策略组。

[H3C-Ethernet2/0/1] ipsec policy map1
# 退回到系统视图。

[H3C-Ethernet2/0/1] quit
```

(2) 配置 SecPathB:

```
# 配置一个访问控制列表，定义由子网 10.1.2.x 去子网 10.1.1.x 的数据流。

[H3C] acl number 3101
[H3C-acl-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination
10.1.1.0 0.0.0.255
[H3C-acl-adv-3101] rule deny ip source any destination any
# 配置到 PC A 的静态路由。

[H3C] ip route-static 10.1.1.0 255.255.255.0 202.38.163.1
# 创建名为 tran1 的安全提议。

[H3C] ipsec proposal tran1
# 报文封装形式采用隧道模式。
```

```
[H3C-ipsec-proposal-tran1] encapsulation-mode tunnel
# 安全协议采用 ESP 协议。

[H3C-ipsec-proposal-tran1] transform esp
# 选择算法。

[H3C-ipsec-proposal-tran1] esp encryption-algorithm des
[H3C-ipsec-proposal-tran1] esp authentication-algorithm sha1
# 退回到系统视图。

[H3C-ipsec-proposal-tran1] quit
# 配置 IKE 对等体。

[H3C] ike peer peer
[H3C-ike-peer-peer] pre-shared-key abcde
[H3C-ike-peer-peer] remote-address 202.38.163.1
# 创建一条安全策略，协商方式为 isakmp。

[H3C] ipsec policy use1 10 isakmp
# 引用访问控制列表。

[H3C-ipsec-policy-isakmp-use1-10] security acl 3101
# 引用安全提议。

[H3C-ipsec-policy-isakmp-use1-10] proposal tran1
# 引用 IKE 对等体。

[H3C-ipsec-policy-isakmp-map1-10] ike-peer peer
# 退回到系统视图。

[H3C-ipsec-policy-isakmp-use1-10] quit
# 进入配置视图。

[H3C] interface ethernet 2/0/1
# 配置的 IP 地址。

[H3C-Ethernet2/0/1] ip address 202.38.162.1 255.0.0.0
# 应用安全策略组。

[H3C-Ethernet2/0/1] ipsec policy use1
# 退回到系统视图。

[H3C-Ethernet2/0/1] quit
```

以上配置完成后，SecPathA 和 SecPathB 之间如果有子网 10.1.1.x 与子网 10.1.2.x 之间的报文通过，将触发 IKE 进行协商建立安全联盟。IKE 协商成功并创建了安全联盟后，子网 10.1.1.x 与子网 10.1.2.x 之间的数据流将被加密传输。

4.4.3 使用加密卡进行加/解密和认证

1. 组网需求

在 SecPathA 和 SecPathB 之间建立一个安全隧道对 PC A 代表的子网(10.1.1.0/24) 与 PC B 代表的子网 (10.1.2.0/24) 之间的数据流进行安全保护。使用手工方式建立安全联盟, 安全协议采用 ESP 协议, 加密算法采用 DES, 认证算法采用 sha1-hmac-96。

2. 组网图

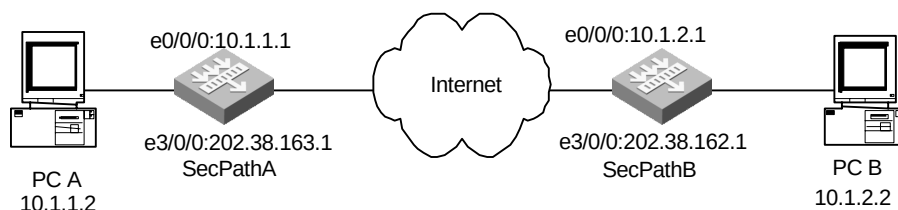


图4-4 使用加密卡建立安全隧道组网图

3. 配置步骤

(1) 配置 SecPathA

配置一个访问列表, 定义由子网 10.1.1.0/24 去子网 10.1.2.0/24 的数据流。

```
[H3C] acl number 3001
[H3C-acl-adv-3001] rule permit ip source 10.1.1.0 0.0.0.255 destination
10.1.2.0 0.0.0.255
[H3C-acl-adv-3001] rule deny ip source any destination any
```

创建名为 trans1 的加密卡安全提议

```
[H3C] ipsec card-proposal tran1
```

指定 trans1 加密卡安全提议使用的加密卡槽位为 1/0/0

```
[H3C-ipsec-card-proposal-tran1] use encrypt-card 1/0/0
```

报文封装形式采用隧道模式。

```
[H3C-ipsec-card-proposal-tran1] encapsulation-mode tunnel
```

安全协议采用 ESP 协议。

```
[H3C-ipsec-card-proposal-tran1] transform esp
```

选择算法。

```
[H3C-ipsec-card-proposal-tran1] esp encryption-algorithm des
```

```
[H3C-ipsec-card-proposal-tran1] esp authentication-algorithm sha1-hmac-96
```

退回到系统视图。

```
[H3C-ipsec-card-proposal-tran1] quit
```



```
# 创建一条安全策略，协商方式为 manual。

[H3C] ipsec policy policy1 10 manual

# 引用访问列表。

[H3C-ipsec-policy-policy1-10] security acl 3001

# 设置对端地址。

[H3C-ipsec-policy-policy1-10] tunnel remote 202.38.162.1

# 设置本端地址。

[H3C-ipsec-policy-policy1-10] tunnel local 202.38.163.1

# 引用加密卡安全提议。

[H3C-ipsec-policy-policy1-10] proposal tran1

# 设置 SPI。

[H3C-ipsec-policy-policy1-10] sa spi outbound esp 12345
[H3C-ipsec-policy-policy1-10] sa spi inbound esp 54321

# 设置密钥。

[H3C-ipsec-policy-policy1-10] sa string-key outbound esp abcdefg
[H3C-ipsec-policy-policy1-10] sa string-key inbound esp gfedcba

# 退回到系统视图。

[H3C-ipsec-policy-policy1-10] quit

# 进入以太网口视图，配置 IP 地址。

[H3C-Ethernet0/0/0] ip address 10.1.1.1 255.255.255.0
[H3C-Ethernet0/0/0] quit

# 进入以太网口视图，配置 IP 地址。

[H3C] interface ethernet 3/0/0
[H3C-Ethernet3/0/0] ip address 202.38.163.1 255.255.255.0

# 退回到系统视图，配置去 10.1.2.0/24 网段的静态路由。

[H3C-Ethernet3/0/0] quit
[H3C] ip route-static 10.1.2.0 255.255.255.0 202.38.162.1

# 在以太网口上应用安全策略库。

[H3C-Ethernet3/0/0] ipsec policy policy1
```

(2) 配置 SecPathB

```
# 配置一个访问列表，定义由子网 10.1.2.0/24 去子网 10.1.1.0/24 的数据流。

[H3C] acl number 3000
[H3C-acl-adv-3000] rule permit ip source 10.1.2.0 0.0.0.255 destination
10.1.1.0 0.0.0.255
[H3C-acl-adv-3000] rule deny ip source any destination any
```

```
# 创建名为 tran1 的加密卡安全提议。

[H3C] ipsec card-proposal tran1
# 指定 trans1 加密卡安全提议使用的加密卡的槽位号 1/0/0。

[H3C] use encrypt-card 1/0/0
# 报文封装形式采用隧道模式。

[H3C-ipsec-card-proposal-tran1] encapsulation-mode tunnel
# 安全协议采用 ESP 协议。

[H3C-ipsec-card-proposal-tran1] transform esp
# 选择算法。

[H3C-ipsec-card-proposal-tran1] esp encryption-algorithm des
[H3C-ipsec-card-proposal-tran1] esp authentication-algorithm sha1-hmac-96
# 退回到系统视图。

[H3C-ipsec-card-proposal-tran1] quit
# 创建一条安全策略，协商方式为 manual。

[H3C] ipsec policy map1 10 manual
# 引用访问列表。

[H3C-ipsec-policy-map1-10] security acl 3000
# 设置对端地址。

[H3C-ipsec-policy-map1-10] tunnel remote 202.38.163.1
# 设置本端地址。

[H3C-ipsec-policy-map1-10] tunnel local 202.38.162.1
# 引用加密卡安全提议。

[H3C-ipsec-policy-map1-10] proposal tran1
# 设置 SPI。

[H3C-ipsec-policy-map1-10] sa spi outbound esp 54321
[H3C-ipsec-policy-map1-10] sa spi inbound esp 12345
# 设置密钥。

[H3C-ipsec-policy-map1-10] sa string-key outbound esp gfedcba
[H3C-ipsec-policy-map1-10] sa string-key inbound esp abcdefg
# 退回到系统视图。

[H3C-ipsec-policy-map1-10] quit
# 进入以太网口视图，配置 IP 地址。

[H3C-Ethernet0/0/0] ip address 10.1.2.1 255.255.255.0
[H3C-Ethernet0/0/0] quit
```

进入以太网口视图，配置 IP 地址。

```
[H3C] interface ethernet 3/0/0
```

```
[H3C-Ethernet3/0/0] ip address 202.38.162.1 255.255.255.0
```

退回到系统视图，配置去 10.1.1.x 网段的静态路由。

```
[H3C-Ethernet3/0/0] quit
```

```
[H3C] ip route-static 10.1.1.0 255.255.255.0 202.38.163.1
```

在以太网口上应用安全策略库。

```
[H3C-Ethernet3/0/0] ipsec policy map1
```

4.4.4 防火墙与 VRRP 备份组虚地址之间建立 SA 配置举例

1. 组网需求

总公司把 SecPathA 和 SecPathB 组成的 VRRP 备份组作为自己的缺省网关。SecPathC 与 VRRP 备份组的虚地址之间建立 IPsec SA，保护总公司与分公司之间的数据流。RouterA、RouterB 为运营商的接入路由器，这里不作重点说明。

2. 组网图

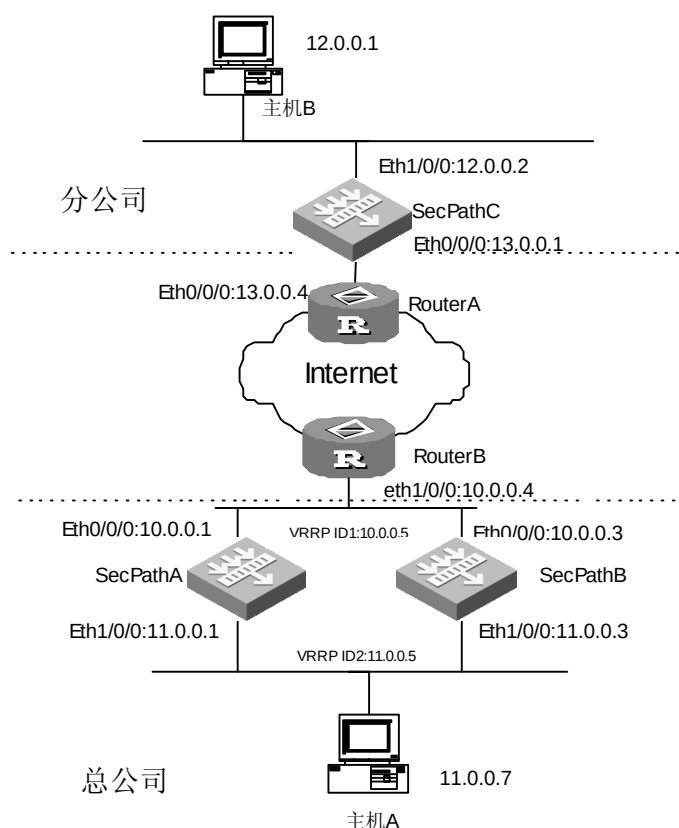


图4-5 防火墙与 VRRP 备份组虚地址之间建立 SA 配置举例

3. 配置步骤

(1) 配置 SecPathA

配置 SecPathA 为 VRRP 备份组的 Master。

```
<H3C> system
[H3C] vrrp ping-enable
[H3C] interface ethernet0/0/0
[H3C-Ethernet0/0/0] ip address 10.0.0.1 255.255.255.0
[H3C-Ethernet0/0/0] vrrp vrid 1 virtual-ip 10.0.0.5
[H3C-Ethernet0/0/0] vrrp vrid 1 priority 120
[H3C-Ethernet0/0/0] vrrp vrid 1 preempt-mode timer delay 5
[H3C-Ethernet0/0/0] interface ethernet1/0/0
[H3C-Ethernet1/0/0] ip address 11.0.0.1 255.255.255.0
[H3C-Ethernet1/0/0] vrrp vrid 2 virtual-ip 11.0.0.5
[H3C-Ethernet1/0/0] vrrp vrid 2 priority 120
[H3C-Ethernet1/0/0] vrrp vrid 2 preempt-mode timer delay 5
[H3C-Ethernet1/0/0] quit
```

配置 IPsec 保护的数据流。

```
[H3C] acl number 3101
[SecPathA-acl-adv-3101] rule 0 permit ip source 11.0.0.0 0.0.0.255 destination
12.0.0.0 0.0.0.255
[H3C-acl-adv-3101] rule deny ip source any destination any
[H3C-acl-adv-3101] quit
```

配置到主机 B 的静态路由。

```
[H3C] ip route-static 0.0.0.0 0.0.0.0 10.0.0.4 preference 60
```

配置 IPsec DPD。

```
[H3C] ike dpd dpd1
[H3C-ike-dpd-dpd1] interval-time 10
[H3C-ike-dpd-dpd1] time-out 5
[H3C-ike-dpd-dpd1] quit
```

创建名为 tran1 的安全提议（内容略）。

```
[H3C] ipsec proposal tran1
```

配置 IKE 对等体。

```
[H3C] ike peer peer
[H3C-ike-peer-peer] pre-shared-key abcde
[H3C-ike-peer-peer] remote-address 13.0.0.1
[H3C-ike-peer-peer] local-address 10.0.0.5
[H3C-ike-peer-peer] dpd dpd1
[H3C-ike-peer-peer] quit
```

创建一条安全策略，协商方式为 isakmp。

```
[H3C] ipsec policy map1 10 isakmp
[H3C-ipsec-policy-isakmp-map1-10] proposal tran1
[H3C-ipsec-policy-isakmp-map1-10] security acl 3101
[H3C-ipsec-policy-isakmp-map1-10] ike-peer peer
[H3C-ipsec-policy-isakmp-map1-10] quit
```

在接口上应用安全策略组。

```
[H3C] interface ethernet 0/0/0
[H3C-ethernet0/0/0] ipsec policy map1
[H3C-ethernet0/0/0] quit
```

(2) 配置 SecPathB

配置 RouterB 为 VRRP 备份组的 Slave（缺省优先级为 100，低于 RouterA 的优先级）。

```
<H3C> system
[H3C] vrrp ping-enable
[H3C] interface ethernet 0/0/0
[H3C-Ethernet0/0/0] ip address 10.0.0.3 255.255.255.0
[H3C-Ethernet0/0/0] vrrp vrid 1 virtual-ip 10.0.0.5
[H3C-Ethernet0/0/0] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 11.0.0.3 255.255.255.0
[H3C-Ethernet1/0/0] vrrp vrid 2 virtual-ip 11.0.0.5
[H3C-Ethernet1/0/0] quit
```

配置 IPsec 保护的数据流。

```
[H3C] acl number 3101
[H3C-acl-adv-3101] rule 0 permit ip source 11.0.0.0 0.0.0.255 destination
12.0.0.0 0.0.0.255
[H3C-acl-adv-3101] rule deny ip source any destination any
[H3C-acl-adv-3101] quit
```

配置到主机 B 的静态路由。

```
[H3C] ip route-static 0.0.0.0 0.0.0.0 10.0.0.4 preference 60
```

配置 IPsec DPD。

```
[H3C] ike dpd dpd1
[H3C-ike-dpd-dpd1] interval-time 10
[H3C-ike-dpd-dpd1] time-out 5
[H3C-ike-dpd-dpd1] quit
```

创建名为 tran1 的安全提议（内容略）。

```
[H3C] ipsec proposal tran1
```

配置 IKE 对等体。

```
[H3C] ike peer peer
[H3C-ike-peer-peer] pre-shared-key abcde
[H3C-ike-peer-peer] remote-address 13.0.0.1
[H3C-ike-peer-peer] local-address 10.0.0.5
[H3C-ike-peer-peer] dpd dpd1
[H3C-ike-peer-peer] quit
# 创建一条安全策略，协商方式为 isakmp。
[H3C] ipsec policy map1 10 isakmp
[H3C-ipsec-policy-isakmp-map1-10] proposal tran1
[H3C-ipsec-policy-isakmp-map1-10] security acl 3101
[H3C-ipsec-policy-isakmp-map1-10] ike-peer peer
[H3C-ipsec-policy-isakmp-map1-10] quit
```

在接口上应用安全策略组。

```
[H3C] interface ethernet 0/0/0
[H3C-Ethernet0/0/0] ipsec policy map1
[H3C-Ethernet0/0/0] quit
```

(3) 配置 SecPathC

配置 IPsec 保护的数据流。

```
[H3C] acl number 3101
[H3C-acl-adv-3101] rule 0 permit ip source 12.0.0.0 0.0.0.255 destination
11.0.0.0 0.0.0.255
[H3C-acl-adv-3101] rule deny ip source any destination any
[H3C-acl-adv-3101] quit
```

配置到主机 A 的静态路由。

```
[H3C] ip route-static 0.0.0.0 0.0.0.0 13.0.0.4 preference 60
```

配置 IPsec DPD。

```
[H3C] ike dpd dpd1
[H3C-ike-dpd-dpd1] interval-time 10
[H3C-ike-dpd-dpd1] time-out 5
[H3C-ike-dpd-dpd1] quit
```

创建名为 tran1 的安全提议（内容略）。

```
[H3C] ipsec proposal tran1
```

配置 IKE 对等体。

```
[H3C] ike peer peer
[H3C-ike-peer-peer] pre-shared-key abcde
[H3C-ike-peer-peer] remote-address 10.0.0.5
[H3C-ike-peer-peer] local-address 13.0.0.1
[H3C-ike-peer-peer] dpd dpd1
```

```
[H3C-ike-peer-peer] quit
```

创建一条安全策略，协商方式为 isakmp。

```
[H3C] ipsec policy map1 10 isakmp
[H3C-ipsec-policy-isakmp-map1-10] proposal tran1
[H3C-ipsec-policy-isakmp-map1-10] security acl 3101
[H3C-ipsec-policy-isakmp-map1-10] ike-peer peer
[H3C-ipsec-policy-isakmp-map1-10] quit
```

在接口上应用安全策略组。

```
[H3C] interface ethernet 0/0/0
[H3C-Ethernet0/0/0] ip address 13.0.0.1 255.0.0.0
[H3C-Ethernet0/0/0] ipsec policy map1
[H3C-Ethernet0/0/0] quit
```

配置以太网口。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 12.0.0.2 255.255.255.0
```

在主机 B 上 **ping -c 500 11.0.0.7** (PC A)，然后在 SecPathA 和 SecPathC 上执行 **display ike sa**、**display ipsec sa** 命令，显示已经建立了安全联盟。

然后在 SecPathA 的 Ethernet 0/0/0 上执行 **shutdown** 命令，在 SecPathC 上通过执行 **debugging ike dpd** 命令，发现连续 3 次发送 DPD 查询报文，并连续 3 次超时没有收到响应报文，最后显示删除该 Peer 下所有 SA（此时 VRRP 备份组正在主备切换），十几秒后，安全隧道重新恢复。调试信息如下：

```
<H3C> debugging ike dpd
```

（连续三次没有收到对端响应，删除 SA）

```
H3C IKE/8/DEBUG:REQUEST(send dpd request): send a message (seqno:-12903966)
H3C IKE/8/DEBUG:REQUEST: wait for response timeout
H3C IKE/8/DEBUG:REQUEST(send dpd request): send a message (seqno:-1917909230)
H3C IKE/8/DEBUG:REQUEST: wait for response timeout
H3C IKE/8/DEBUG:REQUEST(send dpd request): send a message (seqno:-1183268982)
H3C IKE/8/DEBUG:REQUEST: wait for response timeout
H3C IKE/8/DEBUG:REQUEST: there are three fail and all SAs associated were
deleted
```

（收到对端响应，对端主备切换已经完成）

```
H3C IKE/8/DEBUG:REQUEST(send dpd request): send a message (seqno:1382148220)
H3C IKE/8/DEBUG:REQUEST(recv dpd response): received a message
(seqno:1382148220)
H3C IKE/8/DEBUG:RESPONSE(recv dpd request): received a message
(seqno:1382148220)
H3C IKE/8/DEBUG:RESPONSE(send dpd response): send a message
```

(seqno:1382148220)

4.4.5 IPsec/IKE 多实例配置举例

1. 组网需求

CE1、CE3 属于 VPN1，CE1 与 PE1 间通过 IPsec/IKE 隧道相连。CE2、CE4 属于 VPN2，CE2 与 PE1 间通过 IPsec/IKE 隧道相连。

2. 组网图

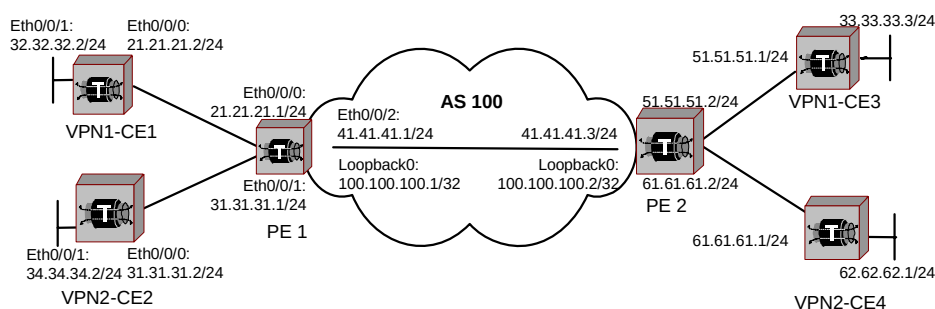


图4-6 IPsec/IKE 多实例配置举例组网图

3. 配置步骤

(1) 配置 CE1

```
<CE1> system-view
```

配置 IKE peer。

```
[CE1] ike peer test
```

```
[CE1-ike-peer-test] pre-shared-key H3C
```

```
[CE1-ike-peer-test] remote-address 21.21.21.1
```

```
[CE1-ike-peer-test] quit
```

配置安全提议（略）。

```
[CE1] ipsec proposal prop
```

配置安全策略。

```
[CE1] ipsec policy map 1 isakmp
```

```
[CE1-ipsec-policy-isakmp-map-1] security acl 3000
```

```
[CE1-ipsec-policy-isakmp-map-1] ike-peer test
```

```
[CE1-ipsec-policy-isakmp-map-1] proposal prop
```

```
[CE1-ipsec-policy-isakmp-map-1] quit
```

以太网接口，并在接口上应用安全策略。

```
[CE1] interface Ethernet0/0/0
```

```
[CE1-Ethernet0/0/0] ip address 21.21.21.2 255.255.255.0
```

```
[CE1-Ethernet0/0/0] ipsec policy map
```



```
[CE1-Ethernet0/0/0] quit
[CE1] interface Ethernet0/0/1
[CE1-Ethernet0/0/1] ip address 32.32.32.1 255.255.255.0
[CE1-Ethernet0/0/1] quit
# 配置 IPsec 保护的数据流。

[CE1] acl number 3000
[CE1-acl-adv-3000] rule 0 permit ip source 21.21.21.0 0.0.0.255 destination
51.51.51.0 0.0.0.255
[CE1-acl-adv-3000] quit
# 配置静态路由。

[CE1] ip route-static 0.0.0.0 0.0.0.0 21.21.21.1 preference 60
[CE1] ip route-static 33.33.33.0 255.255.255.0 21.21.21.1 preference 60

(2) 配置 PE1
<PE1> system-view
# 配置 MPLS 基本能力。

[PE1] mpls lsr-id 100.100.100.1
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
# 配置 vpn-instance vrf1。

[PE1] ip vpn-instance vrf1
[PE1-vpn-vrf1] route-distinguisher 100:1
[PE1-vpn-vrf1] vpn-target 100:1 export-extcommunity
[PE1-vpn-vrf1] vpn-target 100:1 import-extcommunity
[PE1-vpn-vrf1] quit
# 配置 vpn-instance vrf2。

[PE1] ip vpn-instance vrf2
[PE1-vpn-vrf2] route-distinguisher 100:2
[PE1-vpn-vrf2] vpn-target 100:2 export-extcommunity
[PE1-vpn-vrf2] vpn-target 100:2 import-extcommunity
[PE1-vpn-vrf2] quit
# 配置 IKE peer test1。

[PE1] ike peer test1
[PE1-ike-peer-test1] pre-shared-key H3C
[PE1-ike-peer-test1] remote-address 21.21.21.2
[PE1-ike-peer-test1] quit
# 配置 IKE peer test2。

[PE1] ike peer test2
```

```
[PE1-ike-peer-test2] pre-shared-key H3C
[PE1-ike-peer-test2] remote-address 31.31.31.2
[PE1-ike-peer-test2] quit
# 配置安全提议（内容略）。

[PE1] ipsec proposal prop1
[PE1] ipsec proposal prop2
# 配置安全策略。

[PE1] ipsec policy map1 1 isakmp
[PE1-ipsec-policy-isakmp-map-1] security acl 3000
[PE1-ipsec-policy-isakmp-map-1] ike-peer test1
[PE1-ipsec-policy-isakmp-map-1] proposal prop
[PE1-ipsec-policy-isakmp-map-1] quit
[PE1] ipsec policy map2 1 isakmp
[PE1-ipsec-policy-isakmp-map-2] security acl 3001
[PE1-ipsec-policy-isakmp-map-2] ike-peer test2
[PE1-ipsec-policy-isakmp-map-2] proposal prop2
# 在接口上绑定 vpn-instance 并应用安全策略。

[PE1] interface Ethernet0/0/0
[PE1-Ethernet0/0/0] ip binding vpn-instance vrf1
[PE1-Ethernet0/0/0] ip address 21.21.21.1 255.255.255.0
[PE1-Ethernet0/0/0] ipsec policy map1
[PE1-Ethernet0/0/0] quit
[PE1] interface Ethernet0/0/1
[PE1-Ethernet0/0/1] ip binding vpn-instance vrf2
[PE1-Ethernet0/0/1] ip address 31.31.31.1 255.255.255.0
[PE1-Ethernet0/0/1] ipsec policy map2
[PE1-Ethernet0/0/1] quit
# 在接口 Ethernet0/0/2 上启动 MPLS。

[PE1] interface Ethernet0/0/2
[PE1-Ethernet0/0/2] ip address 41.41.41.1 255.255.255.0
[PE1-Ethernet0/0/2] mpls
[PE1-Ethernet0/0/2] mpls ldp enable
[PE1-Ethernet0/0/2] quit
# 配置接口 LoopBack0。

[PE1] interface LoopBack0
[PE1-LoopBack0] ip address 100.100.100.1 255.255.255.255
# 配置 IPsec 保护的数据流。

[PE1] acl number 3000
[PE1-acl-adv-3000] rule 0 permit ip source 51.51.51.0 0.0.0.255 destination
```

```
21.21.21.0 0.0.0.255
[PE1-acl-adv-3000] quit
[PE1] acl number 3001
[PE1-acl-adv-3001] rule 0 permit ip source 61.61.61.0 0.0.0.255 destination
31.31.31.0 0.0.0.255
[PE1-acl-adv-3001] quit
```

在 PE1 与 PE2 之间建立 MP-IBGP 邻居,并在 VPNv4 地址族视图下激活 MP-IBGP 对等体。

```
[PE1] bgp 100
[PE1-bgp] undo synchronization
[PE1-bgp] group g1 internal
[PE1-bgp] peer 100.100.100.2 group g1
[PE1-bgp] peer 100.100.100.2 connect-interface LoopBack0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer g1 enable
[PE1-bgp-af-vpn] peer 100.100.100.2 group g1
[PE1-bgp-af-vpn] quit
```

配置引入 CE1、CE2 的私网路由。

```
[PE1-bgp] ipv4-family vpn-instance vrf1
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] undo synchronization
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] ipv4-family vpn-instance vrf2
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] undo synchronization
[PE1-bgp-af-vpn-instance] quit
```

在 PE1 与 PE2 相连的接口及环回接口上启用 OSPF, 实现 AS 内部的互通。

```
[PE1] ospf 1
[PE1-ospf-1] area 0.0.0.0
[PE1-ospf-1] network 41.41.41.0 0.0.0.255
[PE1-ospf-1] network 100.100.0.0 0.0.255.255
[PE1-ospf-1] quit
```

配置私网静态路由。

```
[PE1] ip route-static vpn-instance vrf1 32.32.32.0 255.255.255.0 21.21.21.2
preference 60
```

CE2, CE3 和 CE4 的配置与 CE1 相似; PE2 的配置与 PE1 对称。

4.5 IPsec 排错

故障之一：初次在接口上应用 IPsec 策略，收发端可正常加解密数据流；关闭掉 IPsec 功能后，收发端仍可正常通信；再次应用 IPsec 策略后，报文不能进行 IPsec 处理，无法 PING 通对端。

故障排除：此问题一般出现在通信发起端直接在安全策略视图下配置安全策略，而被连接端通过引用安全策略模板来创建安全策略的情况下。当第一次使用 IPsec 的时候，两端可以通是正常的。但是当第二次不使用 IPsec 功能时，就会在通信被连接端建立一个快转表项。当第三次又使用 IPsec 的时候，由于这个快转表项的存在，从而导致报文不能进入 IPsec 处理。因此，当第三次使用 IPsec 之前，通信两端使用 **reset ip fast-forwarding cache** 命令清除一下快速转发缓冲区中的内容，就可以恢复正常通信了。

第5章 IKE 配置

5.1 IKE 协议简介

5.1.1 IKE 协议概述

在实施 IPsec 的过程中，可以使用 IKE（Internet Key Exchange）协议来建立安全联盟，该协议建立在由 ISAKMP（Internet Security Association and Key Management Protocol，Internet 安全联盟和密钥管理协议）定义的框架上。IKE 为 IPsec 提供了自动协商交换密钥、建立安全联盟的服务，能够简化 IPsec 的使用和管理。

网络安全包括两层含义：其一是内部网的安全，其二是在公共网络中进行数据交换的安全。实现前者的手段有防火墙、地址转换（NAT）等。后者如正在兴起的 IPsec（IP security），IPsec 提供了在 IP 层对报文实施加密的保护手段。IPsec 的安全联盟可以通过手工配置的方式建立，但是当网络中结点增多时，手工配置将非常困难，而且难以保证安全性。这时就要使用 IKE 自动地进行安全联盟的建立与密钥交换。

IKE 具有一套自我保护机制，可以在不安全的网络上安全地分发密钥、验证身份、建立 IPsec 安全联盟。

IKE 的安全机制包括：

- **DH（Diffie-Hellman）交换及密钥分发。**Diffie-Hellman 算法是一种公共密钥算法。通信双方在不传送密钥的情况下通过交换一些数据，计算出共享的密钥。加密的前提是交换加密数据的双方必须要有共享的密钥。IKE 的精髓在于它永远不在不安全的网络上直接传送密钥，而是通过一系列数据的交换，最终计算出双方共享的密钥。即使第三者（如黑客）截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥。
- **完善的前向安全性（Perfect Forward Secrecy，PFS）。**PFS 特性是一种安全特性，指一个密钥被破解，并不影响其他密钥的安全性，因为这些密钥间没有派生关系。对于 IPsec，是通过在 IKE 阶段 2 协商中增加一次密钥交换来实现的。
- **身份验证。**身份验证确认通信双方的身份。对于 pre-shared key 验证方法，验证字用来作为一个输入产生密钥，验证字不同是不可能在双方产生相同的密钥的。验证字是验证双方身份的关键。
- **身份保护。**身份数据在密钥产生之后加密传送，实现了对身份数据的保护。

IKE 使用了两个阶段为 IPsec 进行密钥协商并建立安全联盟：第一阶段，通信各方彼此间建立了一个已通过身份验证和安全保护的通道，此阶段的交换建立了一个 ISAKMP 安全联盟，即 ISAKMP SA；第二阶段，用在第一阶段建立的安全通道为 IPsec 协商安全服务，即为 IPsec 协商具体的安全联盟，建立 IPsec SA。IPsec SA 用于最终的 IP 数据安全传送。

从下图我们可以看出 IKE 和 IPsec 的关系。

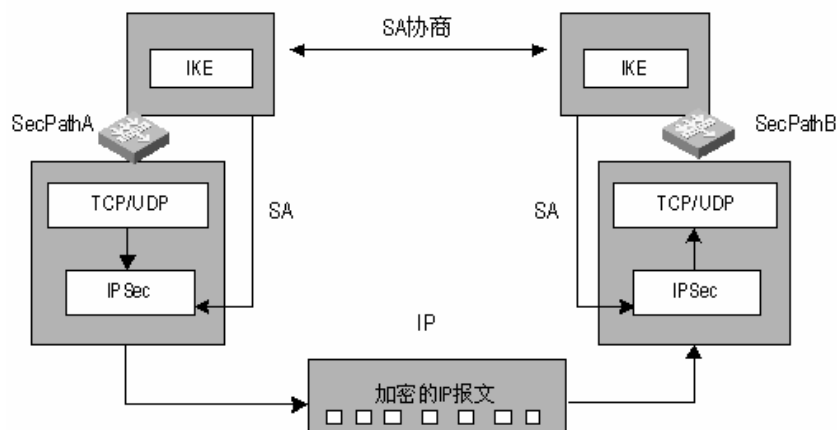


图5-1 IKE 和 IPsec 的关系图

1. IKE 野蛮模式

为了使 IKE 支持目前广泛应用的通过 ADSL 及拨号方式构建 VPN 的方案中的特殊情况——即局端设备的 IP 地址为固定分配的，用户端设备的 IP 地址为动态获取的情况，在 IKE 阶段的协商模式中增加了 IKE 野蛮模式，它可以选择根据协商发起端的 IP 地址或者 ID 来查找对应的身份验证字，并最终完成协商。IKE 野蛮模式相对于主模式来说更加灵活，能够支持协商发起端为动态 IP 地址的情况。

2. NAT 穿越

在 IPsec/IKE 组建的 VPN 隧道中，若存在 NAT 网关设备，且 NAT 网关设备对 VPN 业务数据流进行了 NAT 转换的话，则必须配置 IPsec/IKE 的 NAT 穿越功能。该功能删去了 IKE 协商过程中对 UDP 端口号的验证过程，同时实现了对 VPN 隧道中 NAT 网关设备的发现功能，即如果发现 NAT 网关设备，则将在之后的 IPsec 数据传输中使用 UDP 封装（即将 IPsec 报文封装到 IKE 协商所使用的 UDP 连接隧道里）的方法，避免了 NAT 网关对 IPsec 报文进行篡改（NAT 网关设备将只能够修改最外层的 IP 和 UDP 报文头，对 UDP 报文封装的 IPsec 报文将不作修改），从而保证了 IPsec 报文的完整性（IPsec 数据加密解密验证过程中要求报文原封不动地被传送到接收端）。目前仅在野蛮模式下支持 NAT 穿越，主模式不支持。

以上两个特性在 ADSL+IPsec 的组网方式中一般结合使用，解决了在企业网宽带接入方式下 IP 地址不固定、公网中需要穿越 NAT 等问题，为企业网以 ADSL 宽带接入替代原有的专线方式提供了安全的解决方案。

3. IKE 多实例

IKE 多实例实现了不同 CE 与 PE 进行 IKE 报文协商的功能，并配合 IPsec 共同实现了 PE 与 CE 之间绑定了接口的 IPsec/IKE 多实例功能。

当 CE 端发起 IKE 协商时，IP 报文中携带的 VPN 实例信息随之传给 PE，PE 从接收到的协商报文中获取 VPN 实例信息，并在协商过程中保存 VPN ID；当 PE 往 CE 端发送协商报文时，在 IP 报文中填入此 VPN ID 号，然后发给 IP 层进行处理，由 IP 层根据 VPN 路由表，将报文转发到对应的 CE。

5.1.2 IKE 配置前准备工作

进行 IKE 配置之前，用户需要确定以下几个因素，以便配置过程的顺利进行：

- 确定 IKE 交换过程中算法的强度，即确定安全保护的强度（包括身份验证方法、加密算法、验证算法、DH 组）：不同的算法的强度不同，强度越高的算法，受保护数据越难被破解，但消耗的计算资源越多。一般来说，密钥越长的算法强度越高。
- 确定通信双方预先约定的身份验证字。

5.2 IKE 的配置

5.2.1 IKE 主要配置

- (1) 配置本端防火墙的名称
- (2) 定义 IKE 安全提议
 - 创建 IKE 安全提议
 - 选择加密算法
 - 选择验证方法
 - 选择验证算法
 - 选择 Diffie-Hellman 组标识
 - 配置 ISAKMP SA 生存周期（可选）
- (3) 配置 IKE 对等体
 - 创建 IKE 对等体
 - 配置 IKE 协商模式
 - 配置身份验证字
 - 配置本端防火墙的 ID 类型
 - 配置 IKE 协商过程中使用的 IP 地址
 - 配置 NAT 穿越功能

- 配置 IKE 对等体的子网类型
- (4) 配置 Keepalive 定时器参数
- 配置发送 Keepalive 报文的时间间隔
 - 配置等待 Keepalive 报文的超时时间

5.2.2 配置本端防火墙的名称

当 IKE 协商的发起端使用网关名字进行协商时（即配置了 **id-type name**），本端需要配置命令 **ike local-name**。

请在系统视图下进行下列配置。

表5-1 配置本端防火墙的名称

操作	命令
配置本端防火墙的名称	ike local-name <i>id</i>
恢复本端防火墙设备的缺省名称	undo ike local-name

5.2.3 定义 IKE 安全提议

1. 创建 IKE 安全提议

IKE 提议定义了一套属性数据来描述 IKE 协商怎样进行安全通信。配置 IKE 提议包括创建 IKE 提议、选择加密算法、选择验证方法、选择验证算法、选择 Diffie-Hellman 组标识和设置安全联盟生存周期。

对于主模式，用户可以按照优先级创建多条 IKE 提议，但是协商双方必须至少有一条匹配的 IKE 提议才能协商成功。对于野蛮模式，发起方只会选择优先级最高的安全提议与对方进行协商，如果响应方有匹配的安全提议，则协商成功，否则协商将失败，即发起方不会再使用其它低优先级的安全提议发起协商。

此配置任务定义一个 IKE 提议。配置的 IKE 提议将被用来建立安全通道。

请在系统视图下进行下列配置。

表5-2 创建 IKE 提议

操作	命令
创建 IKE 安全提议	ike proposal <i>proposal-number</i>
删除 IKE 安全提议	undo ike proposal <i>proposal-number</i>

执行 **ike proposal** 命令会进入 IKE 提议视图。在 IKE 提议视图下可以配置加密算法、验证算法、组标识、生存周期和验证方法。

proposal-number 为 IKE 提议序号，取值为 1~100。该序号同时表示优先级，数值越小，优先级越高。可以为进行 IKE 协商的每一端配置多条提议，在协商时将从优先级最高的提议开始匹配一条双方都相同的提议，匹配的原则是：协商双方具有相同的加密算法、验证算法、验证方法和 DH 组标识。

系统提供一条缺省的 IKE 提议，具有最低的优先级，此缺省提议具有缺省的加密算法、验证算法、组标识、生存周期和验证方法。

IKE 提议需要定义参数见下文。

2. 选择加密算法

此配置任务指定一个 IKE 提议使用的加密算法。

请在 IKE 提议视图下进行下列配置。

表5-3 选择加密算法

操作	命令
选择加密算法	encryption-algorithm { des-cbc 3des-cbc aes-cbc }
设置加密算法为缺省值	undo encryption-algorithm

缺省情况下使用 CBC 模式的 56-bit DES 加密算法。

3. 选择验证方法

当前 IKE 认证算法只有两种选择：预共享密钥(*pre-share-key*)和 PKI(*rsa-signature*)方法。

请在 IKE 提议视图下进行下列配置。

表5-4 选择验证方法

操作	命令
选择验证方法	authentication-method { pre-share rsa-signature }
设置验证方法为缺省值	undo authentication-method

缺省情况下，使用预共享密钥验证方法。

 说明：

- 关于 PKI 的配置，请参考本手册中的“PKI 配置”。
- 在 IKE 协商中，如果发起方使用 RSA 数字签名验证方式，那么在 IKE 对等体（IKE Peer）中配置的 **id-type**，**remote-name** 将不生效，响应方只会根据 IKE 对等体中的 **remote-address** 来选择 IKE Peer，故当使用 RSA 数字签名验证方式时，发起方和响应方都要具体指定 **remote-address**，若未配置 **remote-address**，则默认为匹配所有地址。

4. 选择验证算法

此配置任务指定一个 IKE 提议使用的验证算法。

请在 IKE 提议视图下进行下列配置。

表5-5 选择验证算法

操作	命令
选择验证算法	authentication-algorithm { md5 sha }
设置验证算法为缺省值	undo authentication-algorithm

缺省情况下，使用 SHA-1 验证算法。

5. 选择 Diffie-Hellman 组标识

此配置任务指定一个 IKE 提议使用的 Diffie-Hellman 组标识。

请在 IKE 提议视图下进行下列配置。

表5-6 选择 DH 组标识

操作	命令
选择 Diffie-Hellman 组标识	dh { group1 group2 group5 group14 }
设置 Diffie-Hellman 组标识为缺省值	undo dh

缺省情况下指定为 **group1**，即 768-bit 的 Diffie-Hellman 组。

6. 配置 ISAKMP SA 生存周期

此配置任务指定一个 IKE 提议使用的 ISAKMP SA 生存周期。

请在 IKE 提议视图下进行下列配置。

表5-7 设置 ISAKMP SA 生存周期

操作	命令
设置 ISAKMP SA 生存周期	sa duration seconds
设置生存周期为缺省值	undo sa duration

如果 **duration** 时间超时，ISAKMP SA 将自动更新。生存周期可以设定为 60 到 604800 秒之间的一个值。因为 IKE 协商需要进行 DH 计算，在低端防火墙上需要经过较长的时间，为使 ISAKMP SA 的更新不影响安全通信，建议设置 **duration** 大于 10 分钟。

SA 在设定的生存周期超时前会提前协商另一个 SA 来替换旧的 SA。在新的 SA 还没有协商完之前，依然使用旧的 SA；在新的 SA 建立后，将立即使用新的 SA，而旧的 SA 在生存周期超时时被自动清除。

缺省情况下，ISAKMP SA 生存周期为 86400 秒（一天）。

5.2.4 配置 IKE 对等体

1. 创建 IKE 对等体

请在系统视图下进行下列配置。

表5-8 配置 ike 对等体

操作	命令
配置一个 IKE 对等体并进入 ike peer 视图	ike peer peer-name
删除一个 IKE 对等体	undo ike peer peer-name

2. 配置 IKE 协商模式

请在 ike-peer 视图下进行下列配置。

表5-9 配置协商模式

操作	命令
配置 IKE 阶段的协商模式。	exchange-mode { aggressive main }
恢复 IKE 阶段缺省的协商模式。	undo exchange-mode

缺省情况下使用主模式。

说明：

- 当安全隧道一端的 IP 地址为动态获取时，必须将 IKE 阶段的协商模式配置为野蛮模式。
- 当响应方使用策略模板接受发起方的协商请求时，会根据发起方的协商模式而进行选择。

3. 配置身份验证字

请在 `ike-peer` 视图下进行下列配置。

表5-10 配置身份验证字

操作	命令
配置 IKE 阶段协商所使用的身份验证字	<code>pre-shared-key key</code>
取消 IKE 阶段协商所使用的身份验证字	<code>undo pre-shared-key</code>

4. 配置 IKE 协商过程中使用的 ID 类型

请在 `ike-peer` 视图下进行下列配置。

表5-11 配置 IKE 协商过程中使用的 ID 类型

操作	命令
选择 IKE 阶段的协商过程中使用 ID 的类型	<code>id-type { ip name }</code>
恢复 IKE 阶段的协商过程中使用的 ID 类型的缺省设置	<code>undo id-type</code>

缺省情况下使用 IP 地址作为 IKE 协商过程中使用的 ID 类型。

在主模式方式下只能使用 IP 地址作为 IKE 协商过程中使用的 ID。在野蛮模式下，可以选择 IP 地址或者名称来作为 IKE 协商过程中使用的 ID。

5. 指定对端防火墙设备的 ID

当 IKE 协商的发起端使用网关名字进行协商时（即配置了 `id-type name`），发起端会发送自己的名称给对端来标识自己的身份，而对端使用 `remote-name name` 来验证发起端，故此时 `name` 应与发起端网关上使用 `ike local-name` 命令所配的名字保持一致。

请在 `ike-peer` 视图下进行下列配置。

表5-12 指定对端设备的名称

操作	命令
指定对端设备的名称	remote-name <i>name</i>
删除对端设备的名称	undo remote-name

6. 配置本端及对端设备的 IP 地址

当 IKE 协商的发起端使用地址进行协商时（即配置了 **id-type ip**），发起端会发送自己的 IP 地址给对端来标识自己的身份，而响应端使用 **remote-address low-ip-address [high-ip-address]** 来验证发起端。若响应端只配置了 **low-ip-address** 时，**low-ip-address** 应与发起端上 **local-address** 命令所配的 IP 地址保持一致；若响应端配置了 **low-ip-address** 和 **high-ip-address**，即配置了一个地址范围时，此地址范围应包含发起端上 **local-address** 命令所配置的 IP 地址。IKE 协商的发起端不能配置 **remote-address** 为地址范围。

请在 **ike-peer** 视图下进行下列配置。

表5-13 配置防火墙和对端设备的 IP 地址

操作	命令
配置本端防火墙的 IP 地址	local-address <i>ip-address</i>
删除本端防火墙的 IP 地址	undo local-address
配置对端设备的 IP 地址	remote-address <i>low-ip-address [high-ip-address]</i>
删除对端设备的 IP 地址	undo remote-address

一般情况下命令 **local-address** 不需要配置，只有当用户需要指定特殊的本端网关地址时（如指定 **loopback** 接口地址）才需要配置这条命令。

7. 配置 NAT 穿越功能

在 IPsec/IKE 组建的 VPN 隧道中，若存在 NAT 防火墙设备，则必须配置 IPsec/IKE 的 NAT 穿越功能。

请在 **ike-peer** 视图下进行下列配置。

表5-14 配置 IKE/IPsec 的 NAT 穿越功能

操作	命令
配置 IKE/IPsec 的 NAT 穿越功能	nat-traversal
取消 IKE/IPsec 的 NAT 穿越功能	undo nat-traversal

为了节省 IP 地址空间，ISP 经常会在公网中加入 NAT 网关，以便于将私有 IP 地址分配给用户，此时可能会导致 IPsec/IKE 隧道的两端一端为公网地址，另一端为私网地址，所以必须在隧道两端配置 NAT 穿越，保证隧道能够正常协商建立。

8. 配置子网类型

这两条命令仅在与 NETSCREEN 的设备互通时使用。

请在 `ike-peer` 视图下进行下列配置。

表5-15 配置 IKE 对等体的子网类型

操作	命令
配置本端网关的子网类型	local { multi-subnet single-subnet }
恢复缺省的子网类型	undo local
配置对端网关的子网类型	peer { multi-subnet single-subnet }
恢复缺省的子网类型	undo peer

缺省情况下，本端和对端的子网类型为 **single-subnet**。

5.2.5 配置 Keepalive 定时器

1. 配置发送 Keepalive 报文的时间间隔

配置通过 ISAKMP SA 向对端发送 Keepalive 报文的时间间隔。

请在系统视图下进行下列配置。

表5-16 设置发送 Keepalive 报文的时间间隔

操作	命令
设置 ISAKMP SA 向对端发送 Keepalive 报文的时间间隔	ike sa keepalive-timer interval seconds
设置使该功能失效	undo ike sa keepalive-timer interval

IKE 通过此报文维护该条 ISAKMP SA 的链路状态。一般在对端使用命令 **ike sa keepalive-timer timeout** 配置了超时时间时，必须在本端配置此 Keepalive 报文发送时间间隔。当对端在配置的超时时间到后，如果对端的 ISAKMP SA 无 TIMEOUT 标记，则将其标记为 TIMEOUT，当对端再收到本端 keepalive-timer 时间到后发送的 keepalive 报文，将清除 TIMEOUT 标记；如果对端的 ISAKMP SA 已带有 TIMEOUT 标记，说明在超时时间内未收到 Keepalive 报文，则删除该 ISAKMP SA 以及对应的 IPsec SA。所以在配置时需使配置的超时时间比 Keepalive 报文发送时间长。

缺省情况下，此功能无效。

2. 配置等待 Keepalive 报文的超时时间

配置一个 ISAKMP SA 等待 Keepalive 报文的超时时间。

请在系统视图下进行下列配置。

表5-17 设置等待 Keepalive 报文的超时时间

操作	命令
设置 ISAKMP SA 等待 Keepalive 报文的超时时间	ike sa keepalive-timer timeout seconds
设置使该功能失效	undo ike sa keepalive-timer timeout

IKE 通过此报文维护该条 ISAKMP SA 的链路状态。当对端在配置的超时时间到后，如果对端的 ISAKMP SA 无 TIMEOUT 标记，则将其标记为 TIMEOUT，当对端再收到本端 keepalive-timer 时间到后发送的 keepalive 报文，将清除 TIMEOUT 标记；如果对端的 ISAKMP SA 已带有 TIMEOUT 标记，说明在超时时间内未收到 Keepalive 报文，则删除该 ISAKMP SA 以及对应的 IPsec SA。所以在配置时需使配置的超时时间比 Keepalive 报文发送时间长。

在网络上一般不会出现超过连续三次的报文丢失，所以配置超时时间时可以采用对端配置的 Keepalive 报文发送时间间隔的三倍。

缺省情况下，此功能无效。

3. 配置发送 NAT Keepalive 报文的时间间隔

配置 IKE 对等体发送 NAT Keepalive 报文的时间间隔。

表5-18 配置发送 NAT Keepalive 报文的时间间隔

操作	命令
配置 IKE 对等体发送 NAT Keepalive 报文的时间间隔	ike sa nat-keepalive-timer interval seconds
恢复发送 NAT Keepalive 报文的时间间隔为缺省值	undo ike sa nat-keepalive-timer interval

缺省情况下，发送 NAT Keepalive 报文的时间间隔为 20 秒。

NAT Keepalive 报文是一个使用 UDP 封装的未加密的报文。通过发送 NAT Keepalive 报文，在 NAT 网关设备上可以保持 IKE 对等体之间的 NAT 动态映射有效。NAT Keepalive 报文并不用来检测对等体的状态。当配置此命令时，需要确保配置的时间小于 NAT 转换的超时时间。

5.2.6 配置 IKE 禁止 DH 硬件加速

防火墙支持 DH 硬件加速。如果加密卡出现故障，可以使用该命令切换到软件处理流程上。

请在系统视图下进行下列配置。

表5-19 配置 IKE DH 硬件加速

操作	命令
禁止 DH 硬件加速	ike encrypt-card dh-computation disabled
使能 DH 硬件加速	undo ike encrypt-card dh-computation disabled

缺省情况下，IKE 使用 DH 硬件加速。

说明：

禁止 DH 硬件加速后，IKE 流程中的 DH 交换会切换到纯软件流程，故性能会有所下降。

5.3 IKE 显示与调试

IKE 提供以下命令显示当前所有安全联盟的状态和每个 IKE 提议配置的参数。**display** 命令可在所有视图下进行下列操作，**debugging** 和 **reset** 命令只能在用户视图下操作。

表5-20 IKE 显示与调试

操作	命令
显示当前已建立的安全通道	display ike sa [verbose [connection-id id remote-address ip-address]]
显示每个 IKE 提议配置的参数	display ike proposal
显示 IKE 对等体的配置信息	display ike peer [peer-name]
删除安全隧道	reset ike sa [connection-id]
打开 IKE 的调试信息	debugging ike { all error exchange message misc transport }
关闭 IKE 的调试信息	undo debugging ike { all error exchange message misc transport }

在删除指定的安全通道时，需要指定 SA 的 *connection-id*，通过命令 **display ike sa** 可以显示目前的安全联盟的 *connection-id* 信息。针对同一个安全通道（即相同的对端），分别有阶段 1 的信息和阶段 2 的信息。

删除本地的安全联盟时，如果阶段 1 的 ISAKMP SA 还存在，将在此安全联盟的保护下向对端发送删除消息，通知对方清除安全联盟数据库。

如果未指定 *connection-id*，所有的阶段 1 的 SA 都会被删除。

安全通道与安全联盟是完全不同的两个概念，安全通道是一个两端可以互通的通道，而 IPsec SA 则是一个单向的连接，所以安全通道是由一对或几对安全联盟组成的。

5.4 IKE 典型配置案例

5.4.1 IKE 典型配置组网应用

1. 组网需求

- 主机 1 与 2 之间进行安全通信，在 SecPathA 与 SecPathB 之间使用 IKE 自动协商建立安全通道。
- 在 SecPathA 上配置一条 IKE 提议，其优先级为 10，网关 B 使用缺省的 IKE 提议。
- 为使用 pre-shared key 验证方法的提议配置验证字。

2. 组网图

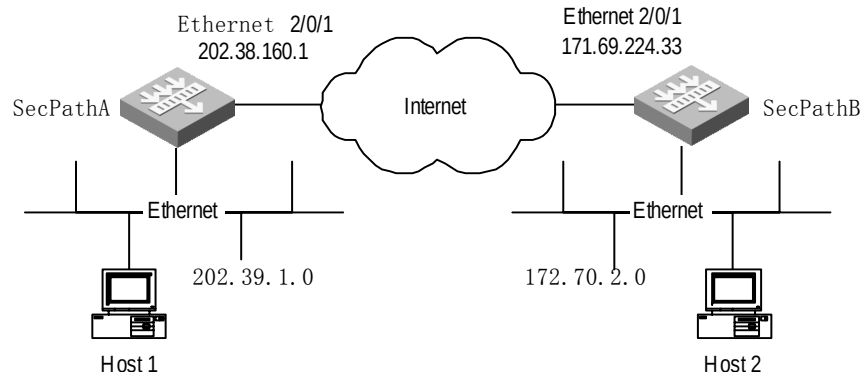


图5-2 IKE 配置举例组网图

3. 配置步骤

(1) 配置 SecPathA

配置 IKE 对等体。

```
[H3C] ike peer peer
[H3C-ike-peer-peer] pre-shared-key abcde
[H3C-ike-peer-peer] remote-address 171.69.224.33
```

配置一条 IKE 提议 10。

```
[H3C] ike proposal 10
```

指定 IKE 提议使用的验证算法为 MD5。

```
[H3C-ike-proposal-10] authentication-algorithm md5
```

使用 pre-shared key 验证方法。

```
[H3C-ike-proposal-10] authentication-method pre-share
```

设置 ISAKMP SA 生存周期 5000 秒。

```
[H3C-ike-proposal-10] sa duration 5000
```

(2) 配置 SecPathB

配置 IKE 对等体。

```
[H3C] ike peer peer
```

```
[H3C-ike-peer-peer] pre-shared-key abcde
```

```
[H3C-ike-peer-peer] remote address 202.38.160.1
```

以上配置可以保证网关 A 和 B 之间进行 IKE 协商。由于网关 A 配置的提议是 proposal 10, 使用 authentication-algorithm md5, 但网关 B 上只有一条缺省的 IKE 提议, 默认是 authentication-algorithm sha。在进行提议匹配的时候, 从优先级最高的提议开始, 因为网关 B 上没有和网关 A 上提议 10 相匹配的提议, 所以双方能够匹配的只有缺省的 IKE 提议。另外, 在进行提议匹配的时候, duration 是不用进行匹配的, 生存周期由 IKE 协商发起方决定。

关于 IPsec 的相应配置请参考 IPsec 配置举例。

5.4.2 IKE 野蛮模式及 NAT 穿越的组网应用

1. 组网需求

- SecPathA 的 Ethernet0/0/0 口为公网固定 IP 地址, SecPathB 为动态获取 IP 地址。
- 由于 SecPathB 要通过运营商的 NAT 设备才能上公网, 所以分公司要和总部建立起 IPSEC 连接必须具备 IKE 野蛮模式及 NAT 穿越功能。
- 为了保证信息安全采用 IPsec/IKE 方式创建安全隧道。

2. 组网图

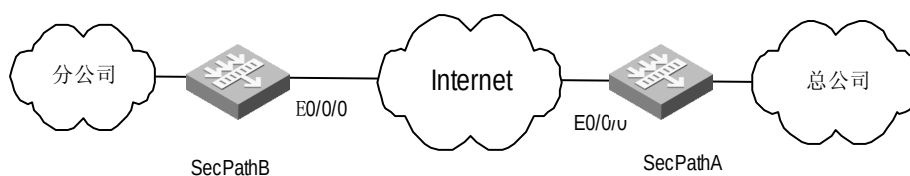


图5-3 IKE 野蛮模式及 NAT 穿越的典型配置案例

3. 配置步骤

(1) 配置 SecPathA

配置本端防火墙设备的名字。

```
[H3C] ike local-name SecPathA
```

配置 acl。

```
[H3C] acl number 3101 match-order auto
```

```
[H3C-acl-adv-3101] rule permit ip source any destination any
```

配置 IKE 对等体 peer。

```
[H3C] ike peer peer
```

```
[H3C-ike-peer-peer] exchange-mode aggressive
```

```
[H3C-ike-peer-peer] pre-shared-key abc
```

```
[H3C-ike-peer-peer] id-type name
```

```
[H3C-ike-peer-peer] remote-name SecPathB
```

```
[H3C-ike-peer-peer] nat traversal
```

创建 IPsec 安全提议 prop。

```
[H3C] ipsec proposal prop
```

```
[H3C-ipsec-proposal-prop] encapsulation-mode tunnel
```

```
[H3C-ipsec-proposal-prop] transform esp
```

```
[H3C-ipsec-proposal-prop] esp encryption-algorithm des
```

```
[H3C-ipsec-proposal-prop] esp authentication-algorithm sha1
```

创建安全策略 policy 并指定通过 IKE 协商建立安全联盟。

```
[H3C] ipsec policy policy 10 isakmp
```

配置安全策略 policy 引用 ike 对等体 peer。

```
[H3C-ipsec-policy-isakmp-policy-10] ike-peer peer
```

配置安全策略 policy 引用访问控制列表 3101。

```
[H3C-ipsec-policy-isakmp-policy-10] security acl 3101
```

配置安全策略 policy 引用 IPsec 安全提议 prop。

```
[H3C-ipsec-policy-isakmp-policy-10] proposal prop
```

进入 E0/0/0 并配置 IP 地址。

```
[H3C] interface Ethernet0/0/0
```

```
[H3C-Ethernet0/0/0] ip address 100.0.0.1 255.255.0.0
```

配置 E0/0/0 引用安全策略组 policy。

```
[H3C-Ethernet0/0/0] ipsec policy policy
```

(2) 配置 SecPathB

配置本端防火墙设备的名字。

```
[H3C] ike local-name SecPathB
# 配置 acl。

[H3C] acl number 3101 match-order auto
[H3C-acl-adv-3101] rule permit ip source any destination any
# 配置 IKE 对等体 peer。

[H3C] ike peer peer
[H3C-ike-peer-peer] exchange-mode aggressive
[H3C-ike-peer-peer] pre-shared-key abc
[H3C-ike-peer-peer] id-type name
[H3C-ike-peer-peer] remote-name SecPathA
[H3C-ike-peer-peer] remote-address 100.0.0.1
[H3C-ike-peer-peer] nat traversal
# 创建 IPsec 安全提议 prop。

[H3C] ipsec proposal prop
[H3C-ipsec-proposal-prop] encapsulation-mode tunnel
[H3C-ipsec-proposal-prop] transform esp
[H3C-ipsec-proposal-prop] esp encryption-algorithm des
[H3C-ipsec-proposal-prop] esp authentication-algorithm sha1
# 创建安全策略 policy 并指定通过 IKE 协商建立安全联盟。

[H3C] ipsec policy policy 10 isakmp
# 配置安全策略 policy 引用 ike 对等体 peer。

[H3C-ipsec-policy-isakmp-policy-10] ike-peer peer
# 配置安全策略 policy 引用访问控制列表 3101。

[H3C-ipsec-policy-isakmp-policy-10] security acl 3101
# 配置安全策略 policy 引用 IPsec 安全提议 prop。

[H3C-ipsec-policy-isakmp-policy-10] proposal prop
# 进入 E0/0/0 并配置接口动态协商 IP 地址。

[H3C-Ethernet0/0/0] pppoe-client dial-bundle-number 1
# 配置拨号接口。

[H3C] dialer-rule 1 ip permit
[H3C] interface dialer 1
[H3C-Dialer1] link-protocol ppp
[H3C-Dialer1] ppp pap local-user aaa password simple aaa
[H3C-Dialer1] mtu 1450
[H3C-Dialer1] ip address ppp-negotiate
[H3C-Dialer1] dialer user 12
[H3C-Dialer1] dialer-group 1
```

```
[H3C-Dialer1] dialer bundle 1
# 配置 Dialer1 引用安全策略组 policy。
[H3C-Dialer1] ipsec policy policy
```

5.5 IKE 故障诊断与排错

配置参数建立 IPsec 安全通道时，可以打开 IKE 的 Error 调试开关，帮助我们查找配置问题。其命令是：

```
<H3C> debugging ike error
```

故障之一：非法用户身份信息

故障排除：用户身份信息是发起 IPsec 通信的用户用来标识自己的数据。在实际应用中我们可以通过用户身份标识实现对不同的数据流建立不同的安全通道进行保护。目前我们是通过用户的 IP 地址来标识用户。

可以看到调试信息：

```
got NOTIFY of type INVALID_ID_INFORMATION
```

或者

```
drop message from A.B.C.D due to notification type INVALID_ID_INFORMATION
```

检查协商两端接口上配置的安全策略中的 ACL 内容是否相容。建议用户将两端的 ACL 配置成互为镜像的。ACL 镜像的含义请参考 IPsec 配置中“配置访问控制列表”内容。

故障之二：提议不匹配

故障排除：

可以看到调试信息：

```
got NOTIFY of type NO_PROPOSAL_CHOSEN
```

或者：

```
drop message from A.B.C.D due to notification type NO_PROPOSAL_CHOSEN
```

协商双方没有可以匹配的提议。对于阶段 1，检查 IKE proposal 是否有与对方匹配的。对于阶段 2 协商，检查双方接口上应用的 IPsec 安全策略的参数是否匹配，引用的 IPsec 安全提议的协议、加密算法和验证算法是否有匹配的。

故障之三：无法建立安全通道

故障排除：实际应用中有时会发现在不稳定的网络状态下，安全通道无法建立或者存在安全通道却无法通信，而且检查双方的 ACL 的配置正确，也有匹配的提议。

这种情况一般是安全通道建立好以后，有一方的设备重启造成的。解决办法：

- 使用 **display ike sa** 命令检查双方是否都已建立阶段 1 的 SA。

- 使用 **display ipsec sa policy** 命令查看接口上的安全策略是否已建立了 IPsec SA。
- 根据以上两步的结果查看，如果有一方存在的 SA 在另一方不存在的情况，使用 **reset ike sa** 命令清除错误存在的 SA，重新发起协商。

第6章 动态 VPN

6.1 DVPN 简介

6.1.1 概述

DVPN（Dynamic Virtual Private Network）动态虚拟私有网络技术，通过动态获取对端的信息建立 VPN 连接。DVPN 提出了 NBMA 类型的隧道机制，使用 Tunnel 逻辑接口作为 DVPN 隧道的端点，完成 DVPN 报文的封装和发送，同时通过 Tunnel 接口完成私网路由的动态学习。DVPN 采用了 Client 和 Server 的方式解决了传统 VPN 的缺陷，Client 通过在 Server 注册，将 Client 自己的信息在 Server 上进行保存，这样 Client 可以通过 Server 的重定向功能得到其它 Client 的信息，从而可以在 Client 之间建立独立的 Session（会话，进行数据传输的通道）。当多个 DVPN 接入设备通过向共同的 Server 进行注册，构建一个 DVPN 域，就实现了各个 DVPN 接入设备后面的网络的 VPN 互联。

6.1.2 DVPN 基本概念介绍

1. DVPN 域

所有通过 DVPN 实现互连的私有网络以及网络中的防火墙、路由器设备共同构成 DVPN 域。

2. DVPN 接入设备

在网络中用来构建 DVPN 动态虚拟私有网络的防火墙、路由器设备，所有支持 DVPN 特性的防火墙、路由器都可以作为 DVPN 接入设备。

3. Server 设备

DVPN 域中，承担 Server 功能的 DVPN 接入设备。所有的其他 DVPN 接入设备必须在 Server 上进行注册后才能接入 DVPN 域中。

4. Client 设备

DVPN 域中作为 Client 的 DVPN 接入设备。Client 设备必须在指定的 Server 设备上完成注册才能接入 DVPN 域。

5. DVPN ID

一个 DVPN 域的唯一标识。在同一台 DVPN 接入设备上，不同的 DVPN 域 ID 不同。

6. Map

Client 设备在 Server 设备上注册时，在 Client 和 Server 之间将建立一个注册通道，称为 Map。Map 在 Client 设备完成注册后仍然存在，直到 Client 设备退出 DVPN 域或退出网络。

7. Session

DVPN 网络数据通讯隧道。所有的数据报文都通过会话隧道进行传递。在 DVPN 域中的两个接入设备之间可以建立一个 Session，实现私有网络的直接互联。

8. Redirect

报文重定向机制。当两个 Client 之间还没有建立 Session 时，他们的数据通讯需要通过 Server 进行转发。Server 在转发时将判断这两个 Client 之间是否可以建立独立的 Session，如果可以，Server 将发送重定向报文给发起数据通信的源 Client，重定向报文中包含了目的 Client 的信息。

9. 主动端和被动端

Session 会话中，Session 两端会协商确定一个主动端和一个被动端，Client 和 Server 之间的 Session 会话，Client 端为 Session 的主动端，Server 为 Session 的被动端；Client 之间的 Session 会话，发起会话建立请求的 Client 为主动端，另一个为 Session 的被动端。

6.1.3 基本工作原理

DVPN 在各个接入设备之间运行 DVPN 私有协议，Server 设备记录着所有已经注册成功的 Client 的信息，Client 设备记录所有已经建立数据通道的 Session 信息。表项内容包括：目标设备的私网地址（Tunnel 接口地址），目标设备的公网地址（WAN 接口的公网 IP 地址），目标设备的 UDP 端口号（采用 UDP 协议时），还有会话通路状态标识等。下面对 Server 与 Client 之间的交互过程作以简单说明：

1. 注册阶段

当 Client 端配置好接口属性，指定了 Server 地址，并且接口状态 UP 后，将向 Server 端发起注册协商，注册协商过程要完成算法协商、密钥协商、身份验证（可选）、信息注册、策略的发布等。

注册协商过程，Client 设备和 Server 设备之间会创建一个 Map，所有的注册协商通过 Map 完成。在整个 Client 生命周期中，Client 和 Server 各自存在一个对应的 Map。只有 Client 退出 DVPN 域，Map 才会被删除。如果 Client 端删除注册使用的 Map，Client 会释放所有的资源（包括所有的 Session 通道），回到初始化状态。

具体的注册过程可以参见下面的流程图，在注册过程中如果出现错误，注册过程会停止，并且返回到初始状态。

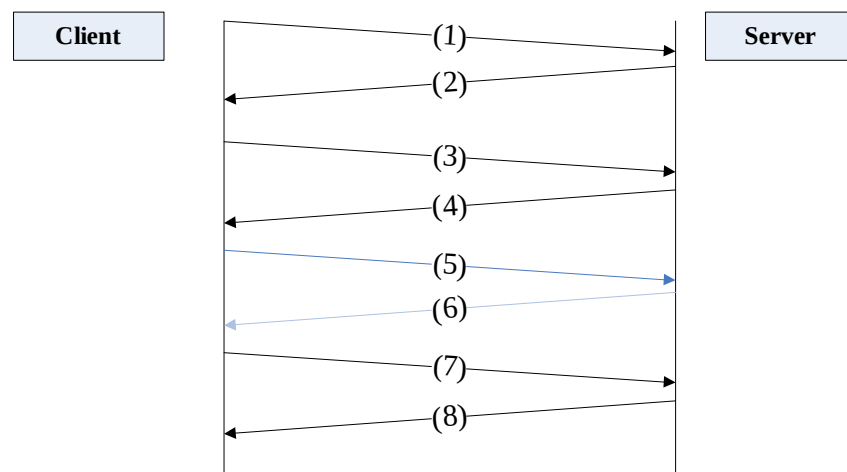


图6-1 DVPN 注册过程

- (1) Client 向 Server 发送算法协商请求消息；
- (2) Server 向 Client 发送算法协商回应报文；
- (3) Client 向 Server 发送密钥协商的请求消息和对 Server 的认证请求消息；
- (4) Server 向 Client 发送密钥协商的回应消息和对 Client 的认证消息，以及回应 Client 的认证请求消息；
- (5) Client 向 Server 发送自己的身份认证消息；
- (6) Server 向 Client 发送身份认证的结果信息；
- (7) Client 向 Server 发送注册请求信息，主要包含 Client 的所有信息；
- (8) Server 回应 Client 的注册请求信息，主要包含所有的数据加密策略，密钥信息，以及 VPN ID 信息等。

2. 会话建立阶段

Client 注册成功后，会立即和 Server 建立会话 Session，通过会话完成实际数据的 DVPN 转发。

若 Server 端接收到的目的地址并非发往本地私网地址的数据报文，而是发往 VPN 网络中的另一个节点的报文，则 Server 转发该数据报文，同时向该数据报文的源节点发送下一跳重定向通告（Redirect），通知源 Client 所要到达目的地之的下一跳的相关信息。此时收到重定向报文的 Client 立即向对端 Client 发送会话建立请求，经过会话协商，在两个 Client 之间建立独立的 Session 会话通道（同时协商该 Session 的 IPsec SA）。这两个 Client 之间的数据可以直接通过该 Session 会话通道进行数据转发，而不需要通过 Server 进行转发了。

当删除 Session 时，会判断该 Session 是否为注册 Map 创建的 Session，如果没有对应的 Map 则直接删除 Session，否则需要删除 Session 对应的 Map。

6.1.4 基本网络结构

DVPN 采用 Client/Server 模式，对于同一个 DVPN 域的 N 个接入设备中，必须设置一个为 Server 工作方式（使用固定的公网 IP 地址），其他设置为 Client 方式，并在每一个 Client 端手工配置 Server 的信息。当每个 Client 到 Server 注册成功之后，Client 和 Server 之间就自动地建立了 Session 隧道（会话）。在网络运行中，Server 可以根据需要向 Client 发送 Redirect（重定向）报文。Client 在接收到重定向报文后，从中得到其他 Client 的信息，在 Client 之间建立 Session 隧道，实现 DVPN 域中的全连接。

建立隧道的方式采用 UDP DVPN 封装格式，对 DVPN 控制报文、需要转发的数据报文，使用 UDP 进行封装。所以 UDP DVPN 可以自由地穿过 NAT 网关建立 DVPN 隧道，满足 Client 为私有 IP 地址时的需求。

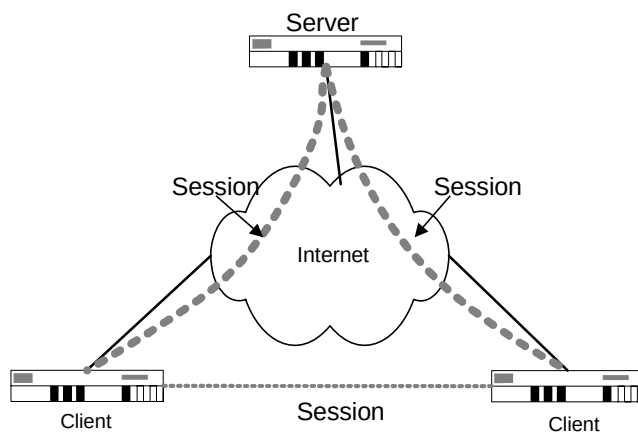


图6-2 动态 VPN 基本网络结构

6.1.5 传统 VPN 与 DVPN 的比较

1. 传统 VPN 存在的弊端

在现有的 VPN 组网方案中，三层 VPN（Virtual Private Network）一般采用 GRE 或 MPLS/BGP VPN 两种方式。两种 VPN 虽然存在各自的优点，但是在实际的应用中都存在以下弊端：

- 组网及配置复杂。三层 VPN 技术都采用的是点到点的隧道方案，当接入点数量为 N，且需要建立一个全联通的 VPN 网络时，整个网络需要手工配置 $N \times (N-1) / 2$ 个点到点的 VPN 隧道连接。
- 可维护性及可扩展性差。对于一个已经组建好的 VPN 网络，若需要增加节点或修改某个节点的配置，那么其他所有节点都必须针对这个节点修改本地配置，维护成本较高。

- GRE 还存在无法穿透 NAT 网关的缺陷。GRE 方式建立 VPN 隧道，如果出口有 NAT 网关，那么就必须要一个公网地址直接对应一个内部地址来解决，需要大量的公网 IP 地址，这导致了 GRE 不能够应用于 NAT 网关内部。IPsec 构建的 VPN 在原来的版本也是没有办法穿越 NAT 网关，目前通过将 IPsec 报文封装在 UDP 报文中进行发送，实现了 NAT 网关的穿越。
- GRE 无法适用于动态 IP 的情况。GRE 方式建立 VPN 隧道依赖于固定的 IP 地址，根本无法为拨号用户建立 VPN。
- L2TP 和 GRE 没有能够提供对传输的数据的加密保护，IPsec 对通过 IPsec VPN 进行转发的数据提供了最安全的保护。
- IPsec 在动态路由的支持存在一定的缺陷，IPsec 的 VPN 隧道是基于数据流的，而不像 GRE 和 L2TP 基于接口建立 VPN。在实现两个私有网络互联以后，两个私有网络之间没有办法实现路由的学习，这样给网络的动态规划带来了一定的问题。

2. DVPN 的特点

DVPN 不但继承了传统 VPN 的各种优点，更大程度上解决了传统 VPN 目前还没有解决的问题。配置简单、网络规划简单、功能强大，比传统的 VPN 更加符合目前以及未来的网络应用。其特点如下：

- 配置简单。一个 DVPN 接入设备可以通过一个 Tunnel 逻辑接口和多个 DVPN 接入设备建立会话通道，而不用为每一个通道配置一个逻辑的接口作为隧道的端点，大大的简化了配置的复杂度，提高了网络的可维护性和易扩充性。如果需要在已有的 DVPN 域中加入一个新的私有网络，只需要在 DVPN 的 Client 接入设备上配置需要加入的 DVPN 域的 Server 信息，新的 DVPN Client 就可以成功的添加到 DVPN 域中。
- 自由穿越 NAT 网关技术。采用 UDP 方式的 DVPN。由于使用了 UDP 报文进行封装，可以自由穿越 NAT 网关。解决内网 DVPN 接入设备和公网 DVPN 接入设备之间的 VPN 连接，使 NAT 网关内部的私有网络和 NAT 网关外部的私有网络共同构建一个虚拟私有网络。
- 支持依赖动态 IP 地址构建 VPN。当在一个 DVPN 域内部构建隧道时，只需要指定相应的 Server 的 IP 地址，并不关心自己当前使用的 IP 地址是多少，更加适应如普通拨号、xDSL 拨号等使用动态 IP 地址的组网应用。

- 支持自动建立隧道技术。DVPN 中的 Server 维护着一个 DVPN 域中所有接入设备的信息，DVPN 域中的 Client 可以通过 Server 的重定向功能自动获得需要进行通信的其它 Client 的信息，并最终在两个 Client 之间自动建立会话隧道 (Session)。作为 Client 的 DVPN 接入设备只需配置自己的相关信息和 Server 的信息，不需要知道其他 Client 的信息，极大地减少了网络的维护管理工作。
- 注册过程加密技术。在 Client 向 Server 进行注册的过程中，需要先完成算法套件以及各种密钥的协商。使用协商出来的算法对注册过程中的关键信息（例如用户名、密码等）进行加密保护，还可以对注册的报文进行合法性检测，保证关键注册信息的安全性。
- 身份认证技术。在 Client 向 Server 进行注册的过程中，Client 可以根据配置需要对 Server 的身份使用 pre-shared-key 进行验证，保证 Client 接入一个合法的 Server；同时 Server 可以根据需要使用 AAA 对需要接入到 DVPN 域的 Client 进行身份验证，保证只有通过身份验证的 Client 才可以接入到 DVPN 域。
- 策略的统一管理技术。Client 在 Server 端注册成功后，Server 会将 DVPN 域中的策略发布给该 Client。策略主要包括会话协商使用的算法套件、会话的保活时间、会话的空闲超时时间、IPsec 使用的加密验证算法、IPsec SA 的重协商时间等。在整个 DVPN 域中，所有的 Session 会使用相同的策略。
- 会话协商过程中的加密技术。在 Session 协商过程中，所有的会话的控制报文都会使用 Server 发布的算法套件进行 IPsec 加密保护。即在建立 Session 的会话协商过程中，根据 Server 发布数据的加密验证算法，为 Session 的数据通信协商 IPsec SA。协商过程使用 DH (Diffie-Hellman) 进行 SA 的密钥协商。对于需要通过该 Session 进行转发的数据，如果需要加密处理，则通过 IPsec 使用 Session 协商出来的 IPsec SA 对报文进行加密处理后，通过 DVPN 进行转发，实现了转发数据报文的安全性。Session 的 IPsec SA 支持重协商功能，可以根据需要指定进行 IPsec SA 重协商的时间，进一步保证数据的安全性。
- 支持多个 VPN 域。DVPN 允许用户在一台 DVPN 设备上支持多个 VPN 域。即一台防火墙不仅可以属于 VPN A，也可以属于 VPN B；同一设备可以在 VPN A 中作为 Client 设备，同时还在 VPN B 中作为 Server 设备使用。在同一台 DVPN 设备上最多可以支持 200 个 DVPN 域，可以同时作为 200 个 DVPN 域的 Server 设备。大大提高了组网的灵活性，也可以更加充分的使用网络设备资源，减少了用户的投资。在实际的组网中为了保证各个 DVPN 域之间的隔离，如果在同一台 DVPN 设备上支持多个 DVPN 域，需要通过私网路由来实现不同 DVPN 域的隔离。

- 动态路由的支持。DVPN 可以对需要通过 Tunnel 接口发送的路由报文，通过所有的 Session 会话进行广播，从而实现整个 DVPN 域内的路由自动学习。实际应用中，DVPN 配合动态路由协议，可以简化对需要接入到 DVPN 域的各个私有网络的规划，简化整个网络的配置，提高网络的维护性和自动化。

6.2 DVPN 的配置

DVPN 的配置包括两方面，一是配置 Client，二是配置 Server。

1. Client 端的配置

Client 端的配置包括基本配置、Tunnel 接口属性配置和 dvpn-class 配置。

(1) 基本配置

- 使能/禁止 DVPN 功能
- 配置 Client 注册的时间间隔
- 配置 Client 注册次数
- 配置 Client 的 dumb 时间

(2) 配置 Tunnel 接口属性

- 配置 Tunnel 接口的报文封装格式 UDP DVPN
- 配置 Tunnel 接口的接口类型（设置为 Client）
- 配置 Tunnel 接口的源端（源地址或者源接口）
- 配置 Tunnel 接口使用的 dvpn-class
- 配置 Tunnel 接口所属的 DVPN 域
- 配置 Client 向 Server 注册时的类型（可选）
- 配置 IPsec 加密的数据流

(3) dvpn-class 配置步骤

dvpn-class 视图下的命令用来配置 Client 设备需要接入的 Server 信息参数、以及注册过程中协商使用的信息。配置的内容包括：

- 创建并进入 dvpn-class 视图
- 配置指定 Server 的公网 IP 地址
- 配置指定 Server 的私网 IP 地址（可选）
- 配置注册过程使用的算法套件（可选，默认为 des-md5-dh1）
- 配置 Client 对 Server 的身份验证方法（可选，默认 NONE）
- 配置 Client 对 Server 验证使用的 pre-shared-key（可选，验证 Server 时需要配置）

- 配置 Client 注册使用的用户信息（可选，如果 Server 需要对 Client 进行身份认证，需要配置用户信息）

2. Server 端的配置

Server 端配置包括基本配置、配置 Tunnel 接口属性和配置 DVPN 的策略套件。DVPN 的策略套件是在 dvpn-policy 视图下配置的。具体配置步骤如下：

(1) 基本配置

- 使能/禁止 DVPN 功能
- 配置 Map 的老化时间
- 配置对 Client 的验证方式
- 配置 Server 的 pre-shared-key

(2) 配置 Tunnel 接口属性

- 配置 Tunnel 接口的报文封装格式 UDP DVPN
- 配置 Tunnel 接口的接口类型（设置为 Server）
- 配置 Tunnel 接口所属的 DVPN 域
- 配置 Tunnel 接口的源端（源地址或者源接口）
- 配置 DVPN 域的统一策略（可选）
- 配置 IPsec 加密的数据流

(3) 配置 DVPN 策略套件

- 创建并进入 dvpn-policy 视图
- 配置 Server 对 Client 的验证方式（可选，默认 NONE）
- 配置指定 Session 的算法套件（可选，默认为 des-md5-dh1）
- 配置指定 Session 的空闲超时时间（可选，默认 300 秒）
- 配置指定 Session 的 Keepalive 时间（可选，默认 10 秒）
- 配置指定 Session 建立请求的时间间隔（可选，默认 10 秒）
- 配置 IPsec 的算法套件（可选，默认为 des-md5-dh1）
- 配置指定 IPsec SA 的重协商时间（可选，默认 3600 秒）

由于 Client 端和 Server 端有许多重复的配置，所以下面将从全局配置、Tunnel 接口配置、dvpn-class 配置、以及 dvpn-policy 四个方面进行介绍配置步骤。

6.2.1 基本配置

1. 使能/禁止 DVPN 功能

通过该命令控制设备是否支持 DVPN 功能。如果 Server 禁止 DVPN 功能，已经建立的 DVPN 会话会等待超时以后进行删除，而不会立即删除。

请在 Client 和 Server 端的系统视图下进行下列配置。

表6-1 使能/禁止 DVPN 配置

操作	命令
使能 DVPN 功能	dvpn service enable
禁止 DVPN 功能	undo dvpn service enable

缺省情况下，系统关闭 DVPN 功能。

2. 配置 Server 的 pre-shared-key

通过该命令可以在 Server 上配置身份验证信息（即 pre-shared-key）。在 Client 需要对 Server 进行身份验证时，Client 需要指定需要接入的 Server 的 pre-shared-key，而且和 Server 的 pre-shared-key 必须一致。

请在 Server 端的系统视图下进行下列配置。

表6-2 配置 Server 的 pre-shared-key

操作	命令
配置 Server 的 pre-shared-key	dvpn server pre-shared-key key
删除 Server 的 pre-shared-key	undo dvpn server pre-shared-key

缺省情况下，系统没有配置 pre-shared-key。

3. 配置对 Client 的验证方式

服务器支持对需要接入 DVPN 的客户端进行身份验证，目前支持的验证方式有 PAP、CHAP、NONE。通过该命令可以在 Server 端指定对 Client 进行身份验证的方式，当 Client 进行 DVPN 接入时，如果没有配置相应的策略，则会使用该命令指定的验证方式对 Client 进行身份验证。

请在 Server 端的系统视图下进行下列配置。

表6-3 配置对 client 的验证方式

操作	命令
配置对 Client 的身份认证方式	dvpn server authentication-client method { none { chap pap } [domain isp-name] }

缺省情况下，不对 Client 进行身份验证。

4. 配置 Map 的老化时间

对于注册不成功的 Map，可以通过在 Server 端配置 Map 的老化时间进行删除。如果 Client 已经注册成功，Map 会和创建的 Session 同时存在。

请在系统视图下进行下列配置。

表6-4 配置 Map 的老化时间

操作	命令
配置 Map 的老化时间	dvpn server map age-time time
恢复 Map 的老化时间为默认值	undo dvpn server map age-time

缺省情况下，Map 的老化时间为 30 秒。

5. 配置 Client 注册的时间间隔

Client 在向 Server 进行注册时，可以连续多次向 Server 发起注册，如果一次注册失败，则 Client 经过一定的注册时间间隔后，会再次向 Server 进行注册。时间间隔可以在 Client 端进行配置。

请在 Client 端的系统视图下进行下列配置。

表6-5 配置 Client 注册的时间间隔

操作	命令
配置 Client 注册的时间间隔	dvpn client register-interval time-interval
恢复 Client 注册时间间隔为缺省值	undo dvpn client register-interval

缺省情况下，Client 注册的时间间隔为 10 秒。

6. 配置 Client 注册次数

Client 在向 Server 进行注册时，如果注册失败可以连续多次向 Server 发起注册，如果超过最大允许注册次数，则 Client 会进入 dumb 状态。可以通过在 Client 端配置下面的命令来设置一次注册最大的尝试次数。

请在 Client 端的系统视图下进行下列配置。

表6-6 配置 Client 注册次数

操作	命令
配置 Client 注册次数	dvpn client register-retry times
恢复 Client 注册次数为缺省值	undo dvpn client register-retry

缺省情况下，Client 注册次数为 3 次。



注意：

处于 dumb 状态的 Client 不会向 Server 进行注册。

7. 配置 Client 的 dumb 时间

Client 在向 Server 进行注册时，连续多次向 Server 发起注册，当 Client 注册失败的次数超过最大允许注册次数时，则 Client 会进入 dumb 状态。处于 dumb 状态的 Client 不会向 Server 进行注册，只有经过了 dumb 时间，Client 才会重新向 Server 进行注册。

请在 Client 端的系统视图下进行下列配置。

表6-7 配置 Client 的 dumb 时间

操作	命令
配置 Client 的 dumb 时间	dvpn client register-dumb time
恢复 Client 的 dumb 时间为默认值	undo dvpn client register-dumb

缺省情况下，Client 的 dumb 时间为 300 秒。

6.2.2 配置 Tunnel 接口属性

1. 配置 Tunnel 接口的封装格式

在配置 DVPN 其他参数前，请务必在 Tunnel 接口上封装 UDP DVPN。

请在 Client 和 Server 端的 Tunnel 接口视图下进行下列配置。

表6-8 设置 Tunnel 接口报文的封装模式

操作	命令
设置 Tunnel 接口报文的封装格式	tunnel-protocol udp dvpn

缺省情况下，封装为 GRE 方式。

2. 配置 Tunnel 接口的类型

Server 端应选择 **Server**，Client 端应选择 **Client**。

请在 Client 端和 Server 端的 Tunnel 接口视图下进行下列配置。

表6-9 设置 Tunnel 接口的类型

操作	命令
配置 Tunnel 接口的类型	dvpn interface-type { client server }
恢复 Tunnel 接口的缺省类型	undo dvpn interface-type

缺省情况下，Tunnel 接口为 **client** 类型。

3. 配置 DVPN 客户端的注册类型

本命令仅在 Client 端使用。当客户端向服务器进行注册时，客户端可以请求服务器转发由此客户端发送的数据包，并且还可以通告服务器不允许将本客户端的注册信息发布给其他客户端。

请在 Client 端的 Tunnel 接口视图下进行下列配置。

表6-10 配置 DVPN 客户端的注册类型

操作	命令
配置 DVPN 客户端的注册类型	dvpn register-type { forward undistributed } *
取消 DVPN 客户端所配置的注册类型	undo dvpn register-type { forward undistributed } *

缺省情况下，并未配置客户端的注册类型。

4. 配置 Tunnel 接口所属的 DVPN 域

本命令用来配置 Tunnel 接口所属的 DVPN 域的标识，属于同一 DVPN 域的 Tunnel 接口应配置相同的 dvpn-id。

请在 Client 端和 Server 端的 Tunnel 接口视图下进行下列配置。

表6-11 配置 Tunnel 接口所属的 VPN

操作	命令
配置 Tunnel 接口所属的 VPN	dvpn dvpn-id dvpn-id
删除 Tunnel 接口所属的 VPN	undo dvpn dvpn-id

缺省情况下，Tunnel 接口没有配置 DVPN 域标识。

5. 配置 Tunnel 接口的源端

Tunnel 接口的源端地址或源接口，即发出 DVPN 报文的接口地址。Tunnel 的源端地址与目的端地址唯一标识了一个通道。这些配置在 Server 及 Client 两端必须配置，且两端地址互为源地址和目的地址。

请在 Client 和 Server 端的 Tunnel 接口视图下进行下列配置。

表6-12 设置 Tunnel 接口的源端地址

操作	命令
设置 Tunnel 接口的源端地址或源接口	source { X.X.X.X interface-type interface-num }
删除 Tunnel 接口的源端地址或源接口	undo source

6. 配置 Tunnel 接口使用的 dvpn-class

本命令仅在 Client 端使用。在 Client 端的 dvpn-class 视图下配置好 Server 的各种参数属性，然后使用下面命令引用相应的 dvpn-class-name。

请在 Client 端的 Tunnel 接口视图下进行下列配置。

表6-13 配置 Tunnel 接口使用的 dvpn-class

操作	命令
配置 Tunnel 接口使用的 dvpn-class 名称	dvpn server dvpn-class-name
删除 Tunnel 接口使用的 dvpn-class 名称	undo dvpn server dvpn-class-name

缺省情况下，接口没有应用 dvpn-class。

7. 配置 Tunnel 接口使用的 dvpn-policy

本命令仅在 Server 端使用。在 Server 端的 dvpn-policy 视图下配置好策略的各种参数，然后可以使用下面命令将策略应用到 DVPN 域中。

请在 Server 端的 Tunnel 接口视图下进行下列配置。

表6-14 配置 Tunnel 接口的 dvpn-policy

操作	命令
配置 Tunnel 接口的 dvpn-policy	dvpn policy dvpn-policy-name
删除 Tunnel 接口的 dvpn-policy	undo dvpn policy dvpn-policy-name

缺省情况下，接口没有应用 dvpn-policy。

8. 配置 IPsec 加密的数据流

dvpn security acl 需要与 **acl** 以及 **rule** 命令配合使用，当 **rule** 命令匹配的关键字为 **deny** 时，表示对于 **rule** 命令 **deny** 掉的数据报文不进行 IPsec 加密，若 **rule** 命令匹配的关键字为 **permit**，对于该配置则无实际意义。

请在 Tunnel 接口视图下进行下列配置。

表6-15 配置 IPsec 加密数据流

操作	命令
配置 IPsec 加密的数据流	dvpn security acl acl-number
删除 IPsec 加密的数据流	undo dvpn security acl

缺省情况下，对接口的所有数据进行 IPsec 加密。

6.2.3 配置 dvpn-class

在 dvpn-class 视图下主要用来配置指定 Server 的相关信息，主要包括私网 IP 地址、公网 IP 地址、用户名等，用于 Client 在指定 Server 上进行注册，以下配置在 Client 端进行配置，应与 Server 端的实际配置保持一致。

1. 创建并进入 dvpn-class 视图

可以通过下面的命令创建并进入 dvpn-class 视图，或者删除已经存在的 dvpn-class。如果当前 dvpn-class 正在被 Dvpn 使用，则不能直接进行删除。

请在系统视图下进行下列配置。

表6-16 创建 dvpn-class 视图

操作	命令
创建并进入 dvpn-class 视图	dvpn class <i>dvpn-class-name</i>
删除 dvpn-class 视图	undo dvpn class <i>dvpn-class-name</i>

缺省情况下，没有配置任何 dvpn-class。

2. 配置指定 Server 的公网 IP 地址

这里的公网 IP 地址指 Server 提供的固定的公有 IP 地址。

请在 dvpn-class 视图下进行下列配置。

表6-17 配置 Server 端的公网 IP 地址

操作	命令
配置 Server 的公网 IP 地址	public-ip <i>ip-address</i>
删除 Server 的公网 IP 地址	undo public-ip

缺省情况下，没有指定 Server 的公网 IP 地址。

3. 配置指定 Server 的私网 IP 地址

这里的私网 IP 地址指 Server 接入 DVPN 域的 Tunnel 接口的 IP 地址。

请在 dvpn-class 视图下进行下列配置。

表6-18 配置 Server 端的私网 IP 地址

操作	命令
配置 Server 的私网 IP 地址	private-ip <i>ip-address</i>
删除 Server 的私网 IP 地址	undo private-ip

缺省情况下，没有指定 Server 的私网 IP 地址。

4. 配置注册过程的算法套件

DVPN 的注册控制报文的报文内容必须进行加密保护，通过注册过程的算法套件确定注册报文的加密算法、验证算法以及密钥协商算法。

请在 `dvpn-class` 视图下进行下列配置。

表6-19 配置注册过程的算法套件

操作	命令
配置注册过程的算法套件	algorithm-suite <i>suite-number</i>
恢复缺省的注册过程的算法套件	undo algorithm-suite

缺省情况下，注册过程的算法套件为 1，即 DES-MD5-GROUP1。其他的算法套件请参考命令手册的相关内容。

5. 配置 Client 对 Server 的验证方式

客户端对其需要接入的服务器端可使用 `pre-shared-key` 进行身份验证方式。

请在 `dvpn-class` 视图下进行下列配置。

表6-20 配置 Client 对 Server 的验证方式

操作	命令
配置使用 <code>pre-shared-key</code> 进行身份认证	authentication-server method pre-share
配置不对 Server 进行身份认证	authentication-server method none

缺省情况下，Client 不对 Server 进行身份验证。

6. 配置用于验证 Server 的 pre-shared-key

该命令用于在 Client 端配置 `pre-shared-key`，要求和其接入的 Server 端的 `pre-shared-key` 一致，Client 才可以在 Server 上注册成功。

请在 `dvpn-class` 视图下进行下列配置。

表6-21 配置 Server 的 pre-shared-key

操作	命令
配置用于验证 Server 的 pre-shared-key	pre-shared-key <i>key</i>
删除用于验证 Server 的 pre-shared-key	undo pre-shared-key

缺省情况下，没有配置 `pre-shared-key`。

7. 配置 Client 的用户名和密码

用户名和密码在 Client 注册到 Server 时使用，如果 Server 需要对接入的 Client 进行身份认证，则 Client 必须在 `dvpn-class` 配置用户信息。

请在 `dvpn-class` 视图下进行下列配置。

表6-22 配置 Client 的用户名和密码

操作	命令
配置 Client 端的用户名和密码	<code>local-user username password { simple cipher } password</code>
删除 Client 端的用户名和密码	<code>undo local-user</code>

缺省情况下，没有配置用户名和密码。

6.2.4 配置 dvpn-policy

在 `dvpn-policy` 视图下主要用来配置指定 DVPN 的策略信息，主要包括会话的算法、数据 IPsec 的算法、以及各种时间参数等。Client 在 Server 上注册成功后，Server 会对注册成功的 Client 发送 DVPN 引用的策略。



注意：

如果要修改并应用已经配置好的策略，必须重起防火墙或 `shutdown/undo shutdown` 隧道接口，否则新的策略不会生效。

1. 创建并进入 dvpn-policy 视图

当 `dvpn-policy` 视图已经存在，可以通过下面的命令进入 `dvpn-policy` 视图，或者删除已经存在的 `dvpn-policy`。如果 `dvpn-policy` 正在被 DVPN 使用，则不能直接进行删除。

请在系统视图下进行下列配置。

表6-23 创建并进入 dvpn-policy 视图

操作	命令
创建并进入 <code>dvpn-policy</code> 视图	<code>dvpn policy dvpn-policy-name</code>
删除 <code>dvpn-policy</code> 视图	<code>undo dvpn policy dvpn-policy-name</code>

缺省情况下，没有配置任何 `dvpn-policy`。

2. 配置 Server 对 Client 的验证方式

服务器支持对需要接入的 DVPN 客户端进行身份验证，目前支持的验证方式有 PAP、CHAP、none。

请在 `dvpn-policy` 视图下进行下列配置。

表6-24 配置对 client 的验证方式

操作	命令
配置对 Client 的身份认证方式	authentication-client method { none { chap pap } [domain <i>isp-name</i>] }

缺省情况下，不对 Client 进行身份验证。

3. 配置指定 Session 的加密算法套件

DVPN 会话协商的控制报文支持 DES、3DES、AES 加密算法和 MD5、SHA1 验证算法，以及 DH-group1、DH-group2 密钥协商算法。通过下面的命令可以选择会话控制报文使用的算法。

请在 `dvpn-policy` 视图下进行下列配置。

表6-25 配置会话的加密算法套件

操作	命令
配置会话的加密算法套件	session algorithm-suite <i>suite-number</i>
恢复会话的加密算法套件为缺省值	undo session algorithm-suite

缺省情况下，会话控制报文的算法套件为 1，即 DES 加密算法、MD5 验证算法和 DH-group1 密钥协商算法。

4. 配置指定 Session 的空闲超时时间

会话在空闲超时时间内没有接收到任何的数据报文，则会话空闲超时断开。

请在 `dvpn-policy` 视图下进行下列配置。

表6-26 配置会话的空闲超时时间

操作	命令
配置会话的空闲超时时间	session idle-time <i>time-interval</i>
恢复会话的空闲超时时间为缺省值	undo session idle-time

缺省情况，会话的空闲超时时间为 300 秒。

5. 配置指定 Session 的 Keepalive 时间

会话在建立成功后，会话的主动端会定时的发送 **keepalive** 报文探测会话连接是否正常。当会话连接有数据报文发送时，就不需要发送 **keepalive** 报文。

请在 **dvpn-policy** 视图下进行下列配置。

表6-27 配置会话的保活时间

操作	命令
配置会话的保活时间	session keepalive-interval <i>time-interval</i>
恢复会话的保活时间为缺省值	undo session keepalive-interval

缺省情况，会话的保活时间为 10 秒。

6. 配置指定 Session 建立的时间间隔

会话在建立过程中，发起会话建立请求的主动端，如果建立不成功，会在会话建立请求时间间隔以后再进行会话建立请求。如果连续三次发送会话建立请求都没能成功建立会话通道，则认为会话建立失败。

请在 **dvpn-policy** 视图下进行下列配置。

表6-28 配置会话建立请求时间间隔

操作	命令
配置会话建立请求的时间间隔	session setup-interval <i>time-interval</i>
恢复会话建立请求的时间间隔为缺省值	undo session setup-interval

缺省情况，会话建立请求时间间隔为 10 秒。

7. 配置 IPsec 的算法套件

DVPN 的数据报文使用 IPsec 进行数据的加密保护，目前 IPsec 支持 DES、3DES、AES 加密算法和 MD5、SHA1 验证算法。通过下面的命令可以选择 IPsec SA 处理转发数据使用的算法套件。

请在 **dvpn-policy** 视图下进行下列配置。

表6-29 配置 IPsec 的算法套件

操作	命令
配置 IPsec SA 的算法套件	data algorithm-suite <i>suite-number</i>
恢复 IPsec SA 的算法套件为缺省值	undo data algorithm-suite

缺省情况下，数据报文的算法套件为 1，即 DES 加密算法、MD5 验证算法。

8. 配置指定 IPsec SA 的生存周期

DVPN 策略可以指定数据加密使用的 IPsec SA 的生存周期。请在 `dvpn-policy` 视图下进行下列配置。

表6-30 配置 IPsec SA 的生存周期

操作	命令
配置 IPsec SA 的生存周期	data ipsec-sa duration time-based <i>time-interval</i>
恢复 IPsec SA 的生存周期为缺省值	undo data ipsec-sa duration time-based

缺省情况下，IPsec SA 的生存周期为 3600 秒。

6.2.5 动态 VPN 的显示和调试

完成上述配置后，在所有视图下执行 **display** 命令可以查看 DVPN 配置后的运行情况。

在用户视图下执行 **reset** 命令可以清除该运行情况。

在用户视图下执行 **debugging** 命令可以对 DVPN 进行调试。

表6-31 动态 VPN 的显示和调试

操作	命令
DVPN 的调试开关	[undo] debugging dvpn { all error event { all register session misc } hexadecimal packet { all control data ipsec } }
显示系统 DVPN 的全局信息或 DVPN 域信息	display dvpn info { dvpn-id <i>dvpn-id</i> global }
显示 DVPN 的 Map 信息	display dvpn map { all dvpn-id <i>vpn-id</i> public-ip <i>public-ip</i> }
显示 DVPN 的会话信息	display dvpn session { all dvpn-id <i>dvpn-id</i> [private-ip <i>private-ip</i>] }
显示 DVPN 的 IPsec SA 信息	display dvpn ipsec-sa { all dvpn-id <i>dvpn-id</i> [private-ip <i>private-ip</i>] }
显示 DVPN 在线用户信息	display dvpn online-user
清除 DVPN 接入	reset dvpn all <i>dvpn-id</i>
删除 DVPN 的 map	reset dvpn map <i>public-ip</i> port [<i>client-id</i>]
删除 DVPN 的会话	reset dvpn session <i>dvpn-id</i> <i>private-ip</i>
清除 DVPN 的统计信息	reset dvpn statistics

 说明:

如果在修改 `dvpn policy` 后想应用新的策略，必须重起防火墙或 **shutdown/undo shutdown** 隧道接口，**reset** 命令不会应用新的 `policy`。

6.3 DVPN 典型组网应用

6.3.1 DVPN 穿越 NAT 典型配置组网

1. 组网需求

如下图所示，总部和两个分支机构分支 A 和分支 B 分别建立 DVPN 连接，其中分支一的私有网络需要通过 NAT 转换与总部私有网络连接，需要实现 DVPN 的 NAT 穿越。

- 在注册和会话过程中需要使用缺省的算法套件 1，即加密算法为 DES、验证算法为 MD5，使用 DH-group1 算法进行密钥协商。
- 数据传输采用 IPsec 进行加密保护，也使用缺省的算法套件 1，即加密算法为 DES、验证算法为 MD5，使用 DH-group1 算法进行密钥协商。

2. 组网图

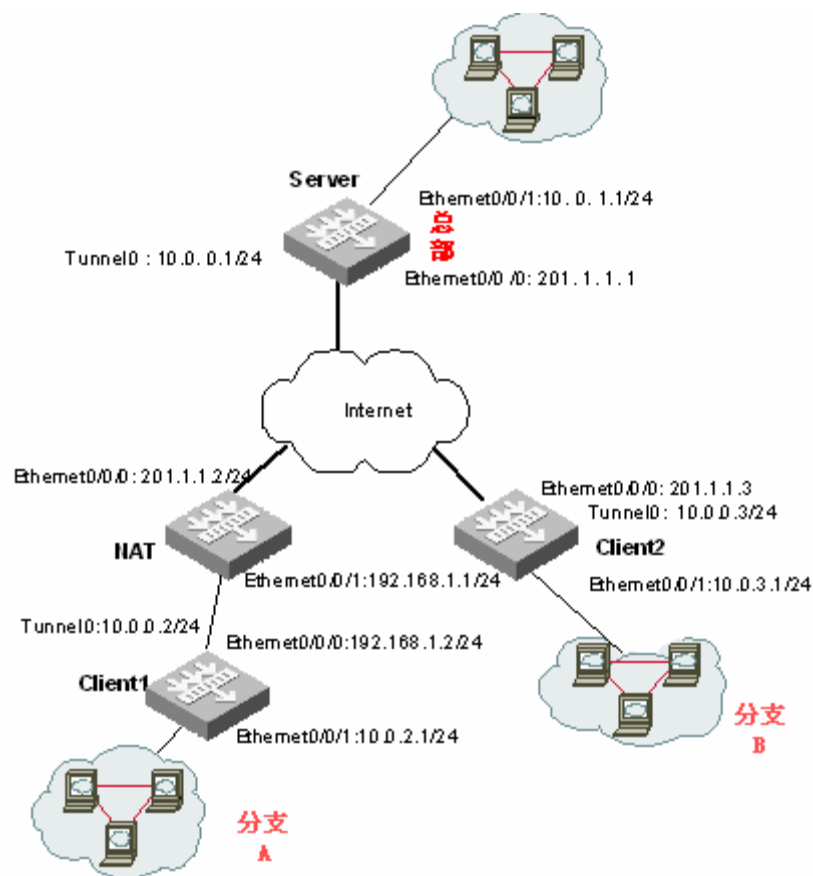


图6-3 DVPN 和 NAT 配合使用典型组网图

3. 配置步骤

(1) 配置 Server

配置 Ethernet0/0/0 接口。

```
[Server] interface Ethernet0/0/0
[Server-Ethernet0/0/0] ip address 201.1.1.1 255.255.255.0
[Server-Ethernet0/0/0] quit
```

配置 Ethernet0/0/1 接口。

```
[Server] interface Ethernet0/0/1
[Server-Ethernet0/0/1] ip address 10.0.1.1 255.255.255.0
[Server-Ethernet0/0/1] quit
```

配置 DVPN policy，且策略中的配置均使用缺省值。

```
[Server] dvpn policy testpolicy
[Server-Policy-testpolicy] quit
```

配置 Tunnel0 接口。

```
[Server] interface tunnel 0
```

```
[Server-Tunnel0] tunnel-protocol udp dvpn
[Server-Tunnel0] dvpn interface-type server
[Server-Tunnel0] ip address 10.0.0.1 255.255.255.0
[Server-Tunnel0] source Ethernet0/0/0
[Server-Tunnel0] dvpn dvpn-id 1
[Server-Tunnel0] dvpn policy testpolicy
[Server-Tunnel0] quit
```

配置路由信息。

```
[Server] ip route-static 10.0.2.0 255.255.255.0 10.0.0.2
[Server] ip route-static 10.0.3.0 255.255.255.0 10.0.0.3
```

(2) 配置 NAT 设备

配置 Ethernet0/0/0 接口。

```
[Nat] interface Ethernet0/0/0
[Nat-Ethernet0/0/0] ip address 201.1.1.2 255.255.255.0
[Nat-Ethernet0/0/0] nat outbound 3000
[Nat-Ethernet0/0/0] quit
```

配置 Ethernet0/0/1 接口。

```
[Nat] interface Ethernet0/0/1
[Nat-Ethernet0/0/1] ip address 192.168.1.1 255.255.255.0
[Nat-Ethernet0/0/1] quit
```

配置 ACL。

```
[Nat] acl number 3000
[Nat-Acl-Adv-3000] rule permit ip
```

配置静态路由。

```
[Nat] ip route-static 10.0.2.0 255.255.255.0 192.168.1.2
```

(3) 配置 Client1

配置 Ethernet0/0/0 接口。

```
[Client1] interface Ethernet0/0/0
[Client1-Ethernet0/0/0] ip address 192.168.1.2 255.255.255.0
[Client1-Ethernet0/0/0] quit
```

配置 Ethernet0/0/1 接口。

```
[Client1] interface Ethernet0/0/1
[Client1-Ethernet0/0/1] ip address 10.0.2.1 255.255.255.0
[Client1-Ethernet0/0/1] quit
```

配置 dvpn-class。

```
[Client1] dvpn class testserver
[Client1-class-testserver] public-ip 201.1.1.1
```

```
[Client1-class-testserver] quit
```

配置 Tunnel0 接口属性。

```
[Client1] interface tunnel 0
```

```
[Client1-Tunnel0] ip address 10.0.0.2 255.255.255.0
```

```
[Client1-Tunnel0] tunnel-protocol udp dvpn
```

```
[Client1-Tunnel0] source Ethernet0/0/0
```

```
[Client1-Tunnel0] dvpn interface-type client
```

```
[Client1-Tunnel0] dvpn server testserver
```

```
[Client1-Tunnel0] dvpn dvpn-id 1
```

```
[Client1-Tunnel0] quit
```

配置静态路由。

```
[Client1] ip route-static 10.0.1.0 255.255.255.0 10.0.0.1
```

```
[Client1] ip route-static 10.0.3.0 255.255.255.0 10.0.0.3
```

```
[Client1] ip route-static 201.1.1.0 255.255.255.0 192.168.1.1
```

(4) 配置 Client2

配置 Ethernet0/0/0 接口。

```
[Client2] interface Ethernet0/0/0
```

```
[Client2-Ethernet0/0/0] ip address 201.1.1.3 255.255.255.0
```

```
[Client2-Ethernet0/0/0] quit
```

配置 Ethernet0/0/1 接口。

```
[Client2] interface Ethernet0/0/1
```

```
[Client2-Ethernet0/0/1] ip address 10.0.3.1 255.255.255.0
```

```
[Client2-Ethernet0/0/1] quit
```

配置 dvpn-class。

```
[Client2] dvpn class testserver
```

```
[Client2-class-testserver] public-ip 201.1.1.1
```

```
[Client2-class-testserver] quit
```

配置 Tunnel0 接口属性。

```
[Client2] interface tunnel 0
```

```
[Client2-Tunnel0] ip address 10.0.0.3 255.255.255.0
```

```
[Client2-Tunnel0] tunnel-protocol udp dvpn
```

```
[Client2-Tunnel0] source Ethernet0/0/0
```

```
[Client2-Tunnel0] dvpn interface-type client
```

```
[Client2-Tunnel0] dvpn server testserver
```

```
[Client2-Tunnel0] dvpn dvpn-id 1
```

```
[Client2-Tunnel0] quit
```

配置静态路由。

```
[Client2] ip route-static 10.0.1.0 255.255.255.0 10.0.0.1
```

```
[Client2] ip route-static 10.0.2.0 255.255.255.0 10.0.0.2
```

6.3.2 DVPN 和 GRE 配合使用典型组网

1. 组网需求

如下图所示，总部需要与分支 A 通过 DVPN 构建虚拟私有网络，与分支 B 通过 GRE 构建虚拟私有网络，这样总部与分支 A 及分支 B 共同构建一个大的 VPN 网络。在该网络中需要实现：

- Server 对接入 DVPN 的 Client1 进行身份认证；
- Client1 对需要接入的 Server 也进行身份认证。

2. 组网图

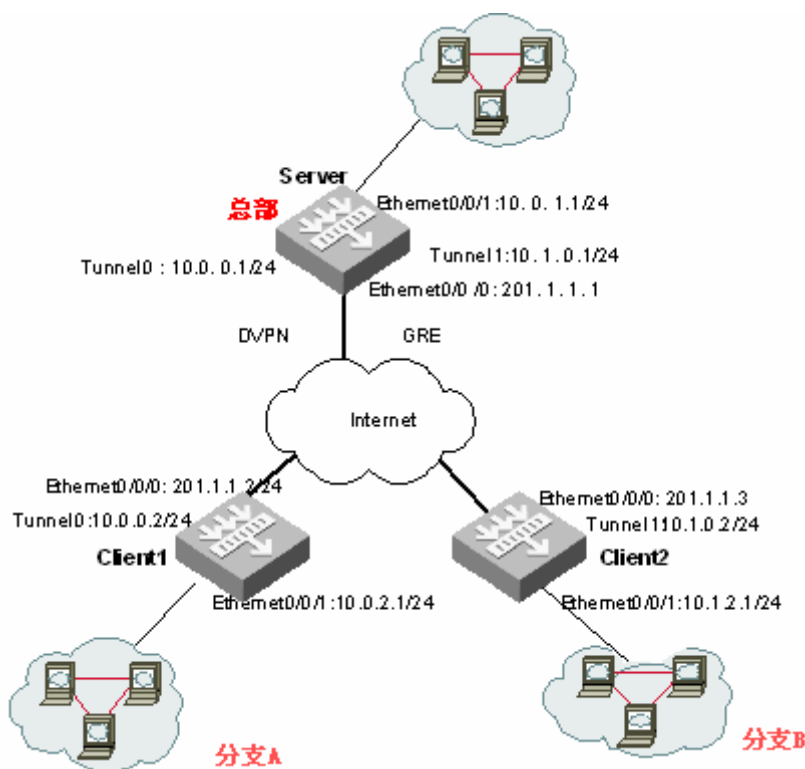


图6-4 DVPN 和 GRE 配合使用典型组网图

3. 配置步骤

(1) 配置 Server

配置 Ethernet0/0/0 接口。

```
[Server] interface Ethernet0/0/0
[Server-Ethernet0/0/0] ip address 201.1.1.1 255.255.255.0
[Server-Ethernet0/0/0] quit
```

配置 Ethernet0/0/1 接口。

```
[Server] interface Ethernet0/0/1
[Server-Ethernet0/0/1] ip address 10.0.1.1 255.255.255.0
[Server-Ethernet0/0/1] quit

# 配置 Server 的身份 pre-shared-key。

[Server] dvpn server pre-shared-key 123456

# 配置 DVPN 使用的验证域使用本地验证。

[Server] domain dvpn
[Server-isp-dvpn] scheme local
[Server-isp-dvpn] quit

# 配置 DVPN policy。

[Server] dvpn policy testpolicy
[Server-Policy-testpolicy] authentication-client method chap domain dvpn
[Server-Policy-testpolicy] data algorithm-suite 7
[Server-Policy-testpolicy] session algorithm-suite 12
[Server-Policy-testpolicy] quit

# 配置 DVPN 本地用户。

[Server] local-user dvpnuser
[Server-luser-dvpnuser] password simple dvpnuser
[Server-luser-dvpnuser] service-type dvpn
[Server-luser-dvpnuser] quit

# 配置 DVPN 使用的 Tunnel0 接口。

[Server] interface tunnel 0
[Server-Tunnel0] tunnel-protocol udp dvpn
[Server-Tunnel0] dvpn interface-type server
[Server-Tunnel0] ip address 10.0.0.1 255.255.255.0
[Server-Tunnel0] source Ethernet0/0/0
[Server-Tunnel0] dvpn dvpn-id 1
[Server-Tunnel0] dvpn policy testpolicy
[Server-Tunnel0] quit

# 配置 GRE 使用的 Tunnel1 接口。

[Server] interface tunnel 1
[Server-Tunnel1] ip address 10.1.0.1 255.255.255.0
[Server-Tunnel1] destination 201.1.1.3
[Server-Tunnel1] source Ethernet0/0/0
[Server-Tunnel1] quit

# 配置路由信息。

[Server] ip route-static 10.1.2.0 255.255.255.0 tunnel1
[Server] ip route-static 10.0.2.0 255.255.255.0 10.0.0.2
```

(2) 配置 Client1

配置 Ethernet0/0/0 接口。

```
[Client1] interface Ethernet0/0/0
[Client1-Ethernet0/0/0] ip address 201.1.1.2 255.255.255.0
[Client1-Ethernet0/0/0] quit
```

配置 Ethernet0/0/1 接口。

```
[Client1] interface Ethernet0/0/1
[Client1-Ethernet0/0/1] ip address 10.0.2.1 255.255.255.0
[Client1-Ethernet0/0/1] quit
```

配置 dvpn-class。

```
[Client1] dvpn class testserver
[Client1-class-testserver] public-ip 201.1.1.1
[Client1-class-testserver] authentication-server method pre-share
[Client1-class-testserver] pre-shared-key 123456
[Client1-class-testserver] local-user dvpnuser@dvpn password simple dvpnuser
[Client1-class-testserver] quit
```

配置 Tunnel0 接口属性。

```
[Client1] interface tunnel 0
[Client1-Tunnel0] ip address 10.0.0.2 255.255.255.0
[Client1-Tunnel0] tunnel-protocol udp dvpn
[Client1-Tunnel0] source Ethernet0/0/0
[Client1-Tunnel0] dvpn interface-type client
[Client1-Tunnel0] dvpn server testserver
[Client1-Tunnel0] dvpn dvpn-id 1
[Client1-Tunnel0] quit
```

配置静态路由。

```
[Client1] ip route-static 10.0.1.0 255.255.255.0 10.0.0.1
[Client1] ip route-static 10.1.2.0 255.255.255.0 10.0.0.1
```

(3) 配置 Client2

配置 Ethernet0/0/0 接口。

```
[Client2] interface Ethernet0/0/0
[Client2-Ethernet0/0/0] ip address 201.1.1.3 255.255.255.0
[Client2-Ethernet0/0/0] quit
```

配置 Ethernet0/0/1 接口。

```
[Client2] interface Ethernet0/0/1
[Client2-Ethernet0/0/1] ip address 10.1.2.1 255.255.255.0
[Client2-Ethernet0/0/1] quit
```

配置 Tunnel0 接口属性。


```
[Client2] interface tunnel 0
[Client2-Tunnel0] ip address 10.1.0.2 255.255.255.0
[Client2-Tunnel0] source Ethernet0/0/0
[Client2-Tunnel0] destination 201.1.1.1
[Client2-Tunnel0] quit

# 配置静态路由。

[Client2] ip route-static 10.0.1.0 255.255.255.0 10.1.0.1
[Client2] ip route-static 10.0.2.0 255.255.255.0 10.1.0.1
```

第7章 BGP/MPLS VPN 配置

7.1 BGP/MPLS VPN 概述

传统 VPN 使用第二层隧道协议（L2TP、L2F 和 PPTP 等）或者第三层隧道技术（IPsec、GRE 等），获得了很大成功，被广泛应用。但是，随着 VPN 范围的扩大，传统 VPN 在可扩展性和可管理性等方面的缺陷越来越突出。

通过 MPLS（Multiprotocol Label Switching，多协议标签交换）技术可以非常容易地实现基于 IP 技术的 VPN 业务，而且可以满足 VPN 可扩展性和管理的需求。利用 MPLS 构造的 VPN，通过配置，可将单一接入点形成多种 VPN，每种 VPN 代表不同的业务，使网络能以灵活方式传送不同类型的业务。

Comware 目前提供比较完全的 BGP/MPLS VPN 组网能力：

- 地址隔离，允许不同 VPN 之间和 VPN 与公网之间的地址重叠。
- 支持 MP-BGP 协议穿越公网发布 VPN 的路由消息，构建 BGP/MPLS VPN。
- 通过 MPLS LSP 转发 VPN 的数据流。
- 提供了 MPLS VPN 的性能监视和故障检测工具。

7.1.1 BGP/MPLS VPN 模型

1. BGP/MPLS VPN 模型

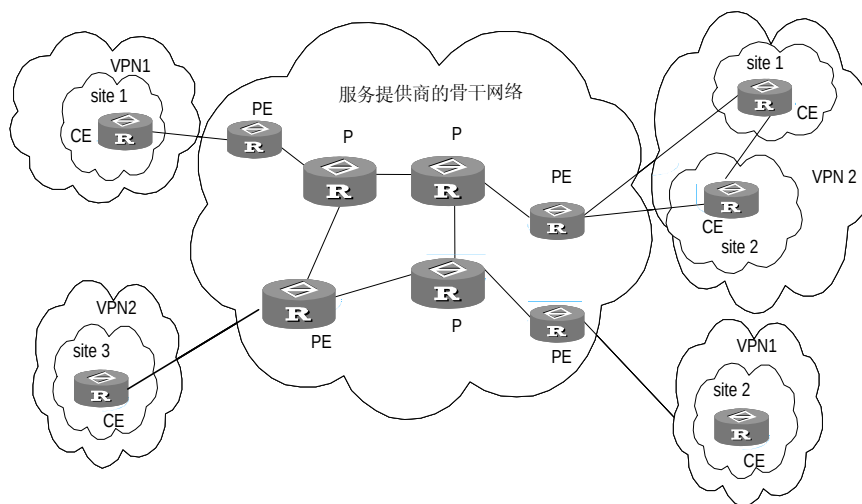


图7-1 MPLS VPN 模型

如上图所示，MPLS VPN 模型中，包含三个组成部分：CE、PE 和 P。

- **CE (Customer Edge) 设备**: 是用户网络边缘设备, 有接口直接与服务提供商相连, 可以是路由器或是交换机等。CE “感知”不到 VPN 的存在。
- **PE (Provider Edge) 路由器**: 即运营商边缘路由器, 是运营商网络的边缘设备, 与用户的 CE 直接相连。MPLS 网络中, 对 VPN 的所有处理都发生在 PE 路由器上。
- **P (Provider) 路由器**: 运营商网络中的骨干路由器, 不和 CE 直接相连。P 路由器需要支持 MPLS 能力。

CE 和 PE 的划分主要是从运营商与用户的管理范围来划分的, CE 和 PE 是两者管理范围的边界。安全网关可以用于 CE 或 PE 设备。

2. BGP/MPLS VPN 中的基本概念

(1) vpn-instance

vpn-instance 是 MPLS VPN 中实现 VPN 路由的重要概念。在 MPLS VPN 的实现中, 每个 Site 在 PE 上对应一个专门的 vpn-instance (vpn-instance 通过与接口绑定实现与 Site 的关联)。如果一个 Site 中的用户同时属于多个 VPN, 则该 Site 对应的 vpn-instance 中将包括所有这些 VPN 的信息。

具体来说, vpn-instance 的信息中包括: 标签转发表、IP 路由表、与 vpn-instance 绑定的接口以及 vpn-instance 的管理信息 (包括 RD、路由过滤策略 VPN Target、成员接口列表等)。可以认为, 它综合了该 Site 的 VPN 成员关系和路由规则。

PE 负责更新和维护 vpn-instance 与 VPN 的关联关系。为了避免数据泄漏出 VPN 之外, 同时防止 VPN 之外的数据进入, 在 PE 上, 每个 vpn-instance 有一套相对独立的路由表和标签转发表, 报文转发信息存储在该 vpn-instance 的 IP 路由表和标签转发表中。

(2) MP-BGP

MP-BGP (multiprotocol extensions for BGP-4, 请参见 RFC2283) 在 PE 路由器之间传播 VPN 组成信息和路由。MP-BGP 向下兼容, 既可以支持传统的 IPv4 地址族, 又可以支持其他地址族 (比如 VPN-IPv4 地址族)。使用 MP-BGP 确保 VPN 的私网路由只在 VPN 内发布, 并实现 MPLS VPN 成员间的通信。

(3) VPN-IPv4 地址族

由于 VPN 网络是一个私用网络, 不同的 Site 可以使用相同的 IP 地址来表示。而 PE 路由器之间使用 MP-IBGP 来发布与之相连的 CE 的路由时, 是假定 IP 地址是全球唯一的, 二者之间不同的含义会导致路由错误。为了解决这个问题, 在发布路由之前 MP-BGP 需要实现 IPv4 地址到 VPN-IPv4 地址族的转换, 使之成为全球唯一的地址 (故 PE 路由器需要支持 MP-BGP)。

一个 VPN-IPv4 地址有 12 个字节, 开始是 8 字节的 RD (Route Distinguisher, 路由识别符), 下面是 4 字节的 IPv4 地址。服务提供商可以独立地分配 RD, 但是,

需要把他们专用的 AS（Autonomous System—自治系统）号作为 RD 的一部分。通过这样的处理以后，即使 VPN-IPv4 地址中包含的 4 字节 IPv4 地址重叠，VPN-IPv4 地址仍可以保持全局唯一。RD 纯粹是为了区别不同的路由，仅在运营商网络内部使用，RD 为零的 VPN-IPv4 地址相当于普通的 IPv4 地址。

PE 从 CE 接收的路由是 IPv4 路由，需要引入 vpn-instance 路由表中，此时需要附加一个 RD。在我们的实现中，为来自于同一个用户 Site 的所有路由设置相同的 RD。

3. VPN Target 属性

VPN Target 属性是 MP-BGP 扩展团体属性之一，主要用来限制 VPN 路由信息发布和接收。它标识了可以使用某路由的 Site 的集合，即该路由可以被哪些 Site 所接收，通过它，可以明确每一个 PE 路由器可以接收哪些 Site 传送来的路由。与 VPN Target 中指明的 Site 相连的 PE 路由器，都会接收到具有这种属性的路由。

PE 路由器存在两个 VPN Target 属性集合：一个集合称为 Export Targets，在发布本地路由到远端 PE 路由器时，附加到从某个直连的 Site 上接收到的路由上；另一个集合称为 Import Targets，在接收远端 PE 发布的路由时，决定哪些路由可以引入此 Site 的 VPN 路由表中。

当通过匹配路由所携带的 VPN Target 属性来过滤 PE 路由器接收的路由信息时，如果该路由携带的 Export VPN Target 集合与接收路由的 PE 的 Import VPN Target 集合存在相同项，则该路由被安装到 VPN 路由表中，进行适当处理后发布给相连的 CE；如果该路由携带的 Export VPN Target 集合与接收路由的 PE 的 Import VPN Target 集合没有相同项，则该路由被拒绝。

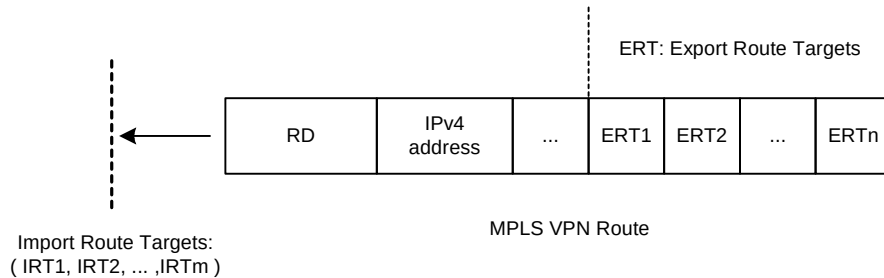


图7-2 通过匹配 VPN Target 属性过滤路由

说明：

通过 VPN Target 属性来过滤 PE 路由器接收的路由信息，使得其他 VPN 的路由不会出现在本 VPN 路由表中（在 VPN 之间不需互通的情况下），所以，CE 发送的数据只会在所属的 VPN 内转发，不会被转发到外部。

7.1.2 BGP/MPLS VPN 的实现

BGP/MPLS VPN 的主要原理是：利用 BGP 在运营商骨干网上传播 VPN 的私网路由信息，用 MPLS 来转发 VPN 业务流。

下面从 VPN 路由信息的发布和 VPN 报文转发两个方面介绍 BGP/MPLS VPN 的实现。

1. VPN 路由信息发布

(1) CE 到 PE 间的路由信息交换

PE 可以通过静态路由、RIP（应支持多实例）、OSPF（应支持多实例）或 EBGPP 学习到与它相连的 CE 的路由信息，并将此路由安装到 VPN-instance 中。

(2) 入口 PE 到出口 PE 的路由信息交换

入口 PE 路由器利用 MP-IBGP 穿越公网，把它从 CE 学习到的路由信息发布给出口 PE（带着 MPLS 标签），同时，获得出口 PE 学习到的 CE 路由信息。

PE 之间通过 IGP（如 RIP、OSPF）来保证 VPN 内部节点之间的连通性，故应在所有互联接口及 loopback 接口上运行 IGP。

(3) PE 之间的 LSP 建立

为了使用 MPLS LSP 转发 VPN 的数据流量，一定在 PE 之间建立公网 LSP。从 CE 接收报文并建立私网标签栈的 PE 路由器是 ingress LSR，BGP 的下一跳（即出口 PE 路由器）是 egress LSR。可以使用 LDP 建立尽力转发的 LSP，也可以使用 RSVP 建立支持特定 QoS 的 LSP 或基于流量工程的 LSP。使用 LDP 建立 LSP 将在 PE 之间形成全连接的 LSP，本章只讨论这种情况。

(4) PE 到 CE 间的路由信息交换

CE 可以通过静态路由、RIP、OSPF、或 EBGPP，从相连的 PE 上学习远端的 VPN 路由。

经过以上的步骤，CE 之间将建立可达的路由，完成 VPN 私网路由信息在公网上的传播。

2. VPN 报文的转发

VPN 报文在入口 PE 路由器上形成两层标签栈：

内层标签，也称 MPLS 标签，是由出口 PE 向入口 PE 发布路由时分配的（安装在 VPN 转发表中），在标签栈中处于栈底位置。当从公网上发来的 VPN 报文到达出口 PE 时，根据标签查找 MPLS 转发表就可以从指定的接口将报文发送到指定的 CE 或者 Site。

外层标签, 也称 LSP 的初始化标签, 指示了从入口 PE 到出口 PE 的一条 LSP, 在标签栈中处于栈顶位置。VPN 报文利用这层标签的交换, 就可以沿着 LSP 到达对端 PE。

以下图为例:

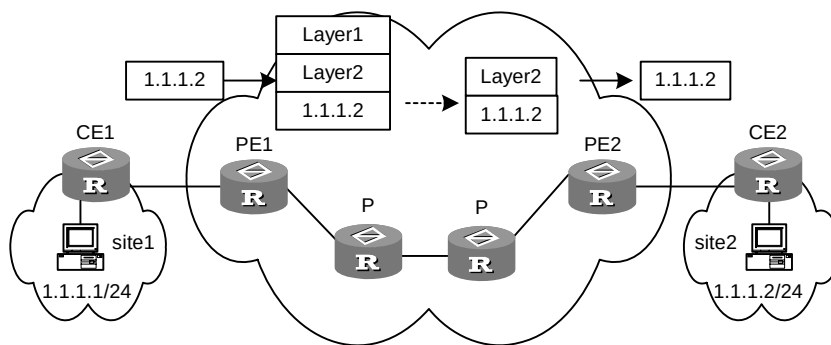


图7-3 VPN 报文转发示意图

- (1) Site1 发出一个目的地址为 1.1.1.2 的 IPv4 报文到达 CE1, CE1 查找 IP 路由表, 根据匹配的表项将 IPv4 报文发送至 PE1。
- (2) PE1 根据报文到达的接口及目的地址查找 VPN-instance 表项, 获得内层标签、外层标签、BGP 下一跳 (PE2)、输出接口等。进行标签封装后, PE1 通过输出接口转发 MPLS 报文到 LSP 上的第一个 P。
- (3) LSP 上的每一个 P 路由器利用交换报文的外层标签转发 MPLS 报文, 直到报文传送到倒数第二跳路由器, 即到 PE2 前的 P 路由器。倒数第二跳路由器将外层标签弹出, 并转发 MPLS 报文到 PE2。
- (4) PE2 根据内层标签和目的地址查找 VPN 转发表, 确定标签操作和报文的出接口, 最终弹出内层标签并由出接口转发 IPv4 报文至 CE2。
- (5) CE2 查找路由表, 根据正常的 IPv4 报文转发过程将报文传送到 Site2。

7.1.3 多角色主机特性简介

从 CE 进入 PE 的报文的 VPN 属性由入接口绑定的 VPN 决定, 这样, 就实质上决定了由同一个入接口经过 PE 转发的所有 CE 设备必须都属于同一个 VPN。但是, 在实际组网环境中, 存在一个 CE 设备经过一个物理接口访问多个 VPN 的需求, 这种需求也许可以通过设置不同的逻辑接口来实现, 但是这种折中的解决方式会增加额外的配置负担, 使用起来也有很大的局限性。为了解决该问题, 利用多角色主机的构思, 通过配置针对 IP 地址的策略路由来区分报文对不同 VPN 的访问, 而从 PE 到 CE 的下行数据流, 是通过静态路由来实现的, 多角色主机情形下的静态路由跟普通的不一樣, 是通过一个 VPN 里面的静态路由指定其他 VPN 中的接口作为出接口来实现的, 从而达到在一个逻辑接口访问多个 VPN 的目的。

7.1.4 OSPF VPN 扩展

1. OSPF 多实例

OSPF 是目前应用最为广泛的 IGP 路由协议之一，因此许多 VPN 将会使用 OSPF 作为其内部路由协议。如果在 PE-CE 链路上也使用 OSPF 将会非常便利：CE 路由器只需要支持 OSPF 协议，不需要支持更多的协议；同时，网络管理员也只需要了解 OSPF 协议；另外，如果客户需要将传统的 OSPF 骨干区域转换为 BGP/MPLS VPN 服务，那么在 PE 和 CE 之间使用 OSPF 可以简化这种转换。

为了在 BGP/MPLS VPN 应用中将 OSPF 作为 PE-CE 间的路由协议，此时，PE 路由器必须支持同时运行多个 OSPF 实例，此时，每一个 OSPF 实例与一个 VPN-Instance 相对应，拥有自己独立的接口、路由表，并且使用 BGP/OSPF 交互通过 MPLS 网络传送 VPN 的路由信息。

下面具体介绍在 PE-CE 间配置 OSPF 需要了解的知识。

(1) PE 和 CE 间的 OSPF 区域配置

PE 与 CE 之间的 OSPF 区域可以是非骨干区域，也可以是骨干区域。

在 OSPF VPN 扩展应用中，MPLS VPN 骨干网被看作是骨干区域 area 0。由于 OSPF 要求骨干区域连续，因此，所有 VPN 节点的 area 0 必须与 MPLS VPN 骨干网相连。

即：如果 VPN 节点存在 OSPF area 0，则 CE 接入的 PE 必须通过 area 0 与这个 VPN 节点的骨干区域相连（可以通过 Virtual-link 实现逻辑上的连通）。

(2) BGP/OSPF 交互

在 PE-CE 间运行 OSPF 后，PE 与 PE 通过 BGP 发布 VPN 路由，PE 通过 OSPF 向 CE 发布 VPN 路由。

以下图为例，PE1 和 PE2 通过 MPLS 骨干网相连，CE11、CE21 和 CE22 都属于 VPN1。假设图中所有路由器属于同一个自治系统，即，CE11、CE21、CE22 属于同一个 OSPF 域（OSPF domain）。

VPN1 路由的发布过程大致可以描述为：首先在 PE1 上将 CE11 的 OSPF 路由引入 BGP；然后通过 BGP 将这些 VPN 路由发布给 PE2；在 PE2 上将 BGP 的 VPN 路由引入到 OSPF，再发布给 CE21 和 CE22。

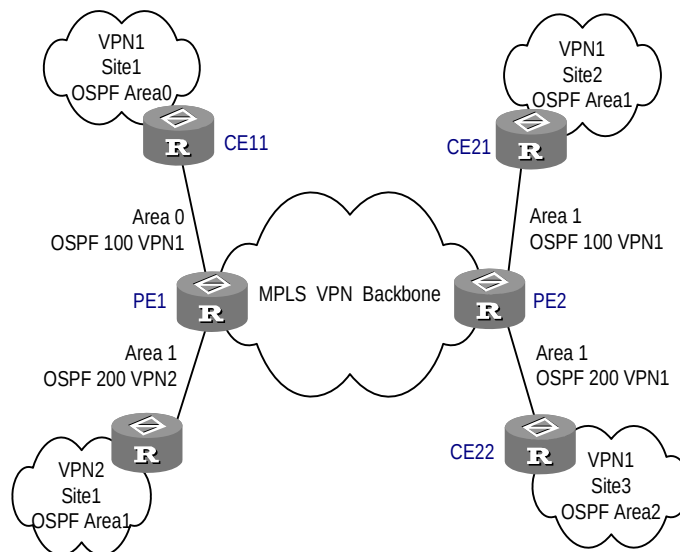


图7-4 OSPF 在 VPN 中的使用

如果使用标准的 BGP/OSPF 交互过程, PE2 将把 BGP VPN 路由通过 Type5 LSAs, 即 ASE LSAs, 发布给 CE21 和 CE22。但 CE11 与 CE21、CE22 是同一个 OSPF 域, 它们之间的路由发布应该使用 Type3 LSAs, 即区域间路由。

为了避免上述情况的发生, PE 使用一种经过修改的 BGP/OSPF 交互过程 (简称为 BGP/OSPF 互操作功能), 发布从一个 Site 到另一个 Site 的路由, 并区分这种路由与真正的 AS-External 路由。这一过程需要 BGP 使用扩展团体属性, 携带可以标识 OSPF 属性的信息。

在 Comware 的实现中, 要求每个 OSPF 域有一个可配置的域 ID (Domain ID)。一般建议: 与每个 VPN 实例相关的网络中的所有 OSPF 实例要么配置一个相同的域 ID, 要么都使用缺省的 0 作为域 ID。这样在收到 BGP 的 VPN 路由时, 域 ID 相同的是来自同一 VPN 实例的路由。

(3) 路由环的检测

假设 PE 与 CE 之间通过 OSPF 骨干区域相连, 且同一个 VPN 节点 (Site) 连接到不同的多个 PE。这种情况下, 当一个 PE 通过 LSA 向 VPN 节点发布从 MPLS/BGP 学的 BGP VPN 路由时, LSA 可能被另一个 PE 接收到, 造成路由环。

为了防止产生路由环, 对于从 MPLS/BGP 学到的 BGP VPN 路由, 无论 PE 与 CE 间是否通过 OSPF 骨干区域相连, PE 在生成 Type3 LSA 时, 都会设置标志位 DN。PE 路由器的 OSPF 进程在进行路由计算时, 忽略 DN 置位的 Type3 LSAs。

如果 PE 需要向 CE 发布一条来自其它 OSPF 域的路由, 则 PE 应表明自己是 ASBR, 并将该路由作为 Type5 LSA 发布。为 OSPF 实例配置的 VPN Route Tag 包含在 Type5 或 Type7 的 LSA 中。PE 路由器的 OSPF 进程在进行路由计算时, 如果 Type5 或 Type7 的 LSA 的 tag 值与 PE 路由器上配置的 route tag 相同, 则忽略此 LSA。

2. Multi-VPN-Instance CE

支持 OSPF 多实例后，在一个路由器上可以运行多个 OSPF 进程，不同的进程可以绑定不同的 VPN-Instance。在实际应用中，可以针对每种业务建立一个 OSPF 实例，采用 OSPF 多实例实现不同业务传输的完全隔离，低成本地解决传统局域网的安全性问题，极大的满足客户的需求。而 OSPF 多实例通常是运行在 PE 路由器上的，对于这种在局域网中运行 OSPF 多实例的路由器，通常也称之为 Multi-VPN-Instance CE。目前，局域网不同业务的隔离一般是通过交换机的 VLAN 功能实现的。OSPF Multi-VPN-Instance CE 提供了在路由器上实现业务隔离的方案。

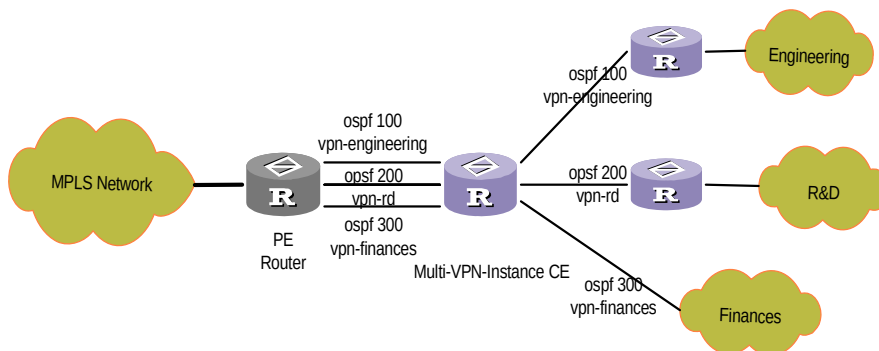


图7-5 Multi-VPN-Instance CE 在解决传统局域网安全性中的应用

3. Sham link

如下图所示，在 OSPF 的 PE-CE 连接中，假设同一个 OSPF 区域中有两个 Site 连接到不同的 PE，两个 Site 之间存在一条区域内的 OSPF 链路（这种链路称为 backdoor），并且这两个 Site 属于同一个 VPN。这种情况下，通过 PE 连接两个 Site 的路由将作为区域间路由 (Inter-Area Route)，由于其优先级低于经过 backdoor 链路的区域内路由 (Intra-Area Route)，不会被 OSPF 优选。

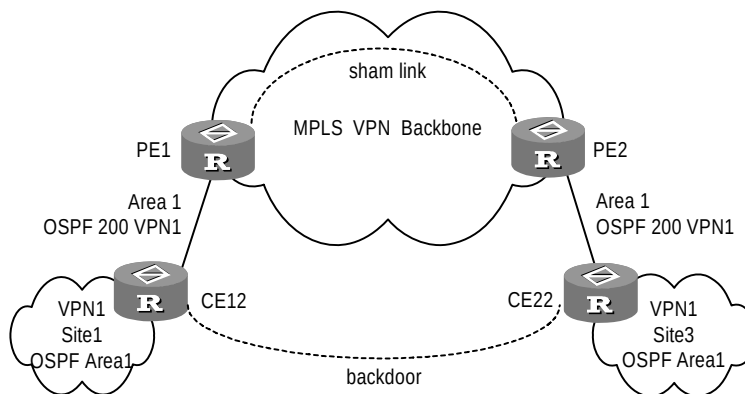


图7-6 sham link 应用示意图

某些情况下，可能需要优先使用经过 MPLS VPN 骨干网的路由，这时，可以在 PE 路由器之间建立 sham link 链路，使经过 MPLS VPN 骨干网的路由也成为 OSPF 区域内路由。

sham link 作为区域内的一条 unnumbered 点到点链路，包含在 Type1 LSA 中发布。用户可以通过调整度量值 metric 在 sham link 和 backdoor 之间进行选路。

sham link 被看成是两个 VPN 实例之间的链路，每个 VPN 实例中必须有一个 sham link 的端点地址，它是 PE 路由器上 VPN 地址空间中的一个有 32 位掩码的 loopback 接口地址。同一个 OSPF 进程的 sham link 可以共用端点地址，但不同 OSPF 进程不能拥有两条端点地址完全相同的 sham link。

sham link 的端点地址被 BGP 作为 VPN-IPv4 地址发布。如果路由经过了 sham link，它就不能再以 VPN-IPv4 路由的形式被引入到 BGP。

sham link 可以在任何区域配置。在 Comware 中，sham link 需要手工配置。并且，本端 VPN 实例中必须有到 sham link 目的地址的路由。

7.1.5 跨域 VPN

实际组网应用中，某用户一个 VPN 的多个 Site 可能会连接到使用不同 AS 号的多个服务提供商，或者连接到一个服务提供商的多个 AS。这种 VPN 跨越多个自治系统的应用方式被称为跨域 VPN (Multi-AS BGP/MPLS VPN)。

RFC2547bis 中提出了三种跨域 VPN 解决方案，分别是：

- VPN-INSTANCE-to-VPN-INSTANCE: ASBR 间使用子接口管理 VPN 路由，也称为 Inter-Provider Backbones Option A;
- EBGp Redistribution of labeled VPN-IPv4 routes: ASBR 间通过 MP-EBGP 发布标签 VPN-IPv4 路由，也称为 Inter-Provider Backbones Option B;
- Multihop EBGp redistribution of labeled VPN-IPv4 routes: PE 间通过 Multi-hop MP-EBGP 发布标签 VPN-IPv4 路由，也称为 Inter-Provider Backbones Option C。

Comware 支持上述三种解决方案。

1. ASBR 间使用子接口管理 VPN 路由

这种方式下，两个 AS 的 PE 路由器直接相连，PE 路由器同时也是各自所在自治系统的边界路由器 ASBR。

作为 ASBR 的 PE 之间通过多个子接口相连，两个 PE 都把对方作为自己的 CE 设备对待，使用传统的 EBGp 方式向对端发布 IPv4 路由。每个子接口对应一个 VPN，需要将 ASBR 的子接口绑定在对应的 vpn-instance 下，但不需要使能 MPLS。报文在 AS 内部作为 VPN 报文，采用两层标签转发方式；在 ASBR 之间则采用普通 IP 转发方式。

理想情况下，每个跨域的 VPN 都有一对子接口，用来交换 VPN 路由信息。

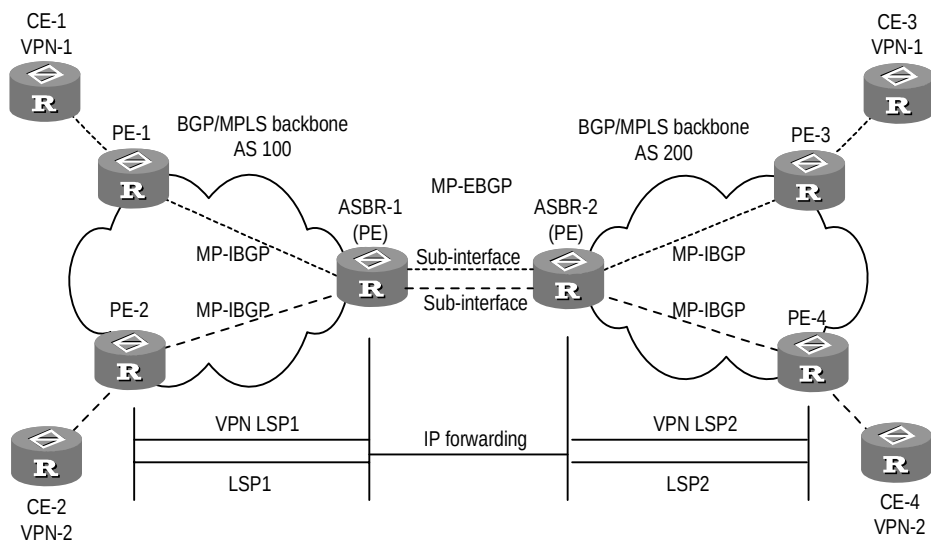


图7-7 ASBR 间使用子接口管理 VPN 路由组网图

使用子接口实现跨域 VPN 的优点是实现简单：两个作为 ASBR 的 PE 之间不需要为跨域进行特殊配置。

缺点是可扩展性差：作为 ASBR 的 PE 需要管理所有 VPN 路由，为每个 VPN 创建 VPN 实例。这将导致 PE 上的 VPN-IPv4 路由数量过于庞大。并且，为每个 VPN 单独创建子接口也提高了对 PE 设备的要求。

2. ASBR 间通过 MP-EBGP 发布标签 VPN-IPv4 路由

这种方式下，两个 ASBR 通过 MP-EBGP 交换它们从各自 AS 的 PE 路由器接收的标签 VPN-IPv4 路由。

路由发布过程可分为以下步骤：

- (1) AS100 内的 PE 先通过 MP-IBGP 方式把标签 VPN-IPv4 路由发布给 AS100 的边界路由器 PE，或发布给为 ASBR PE 反射路由的路由反射器；
- (2) 作为 ASBR 的 PE 通过 MP-EBGP 方式把标签 VPN-IPv4 路由发布给 AS200 的 PE（也是 AS200 的边界路由器）；
- (3) AS200 的 ASBR PE 再通过 MP-IBGP 方式把标签 VPN-IPv4 路由发布给 AS200 内的 PE，或发布给为 PE 反射路由的路由反射器。

这种方式的 ASBR 需要对标签 VPN-IPv4 路由进行特殊处理，因此也称为 ASBR 扩展方式。

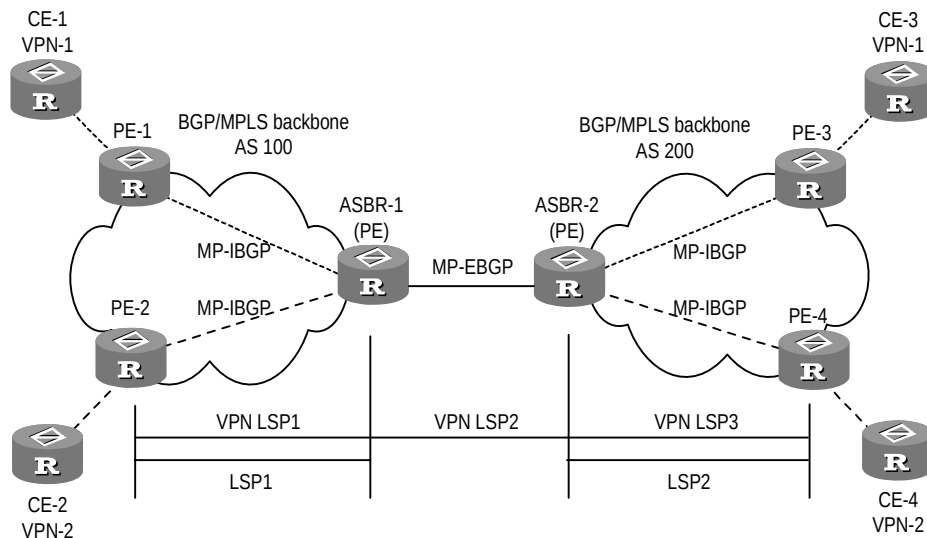


图7-8 ASBR 间通过 MP-EBGP 发布标签 VPN-IPv4 路由组网图

在可扩展性方面，通过 MP-EBGP 发布标签 VPN-IPv4 路由优于 ASBR 间通过子接口管理 VPN。

采用 MP-EBGP 方式时，需要注意：

- ASBR 之间不对接收的 VPN-IPv4 路由进行 VPN Target 过滤，因此，交换 VPN-IPv4 路由的各 AS 服务提供商之间需要就这种路由交换达成信任协议；
- VPN-IPv4 路由交换仅发生在私网对等点之间，不能与公网交换 VPN-IPv4 路由，也不能与没有达成信任协议的 MP-EBGP 对等体交换 VPN-IPv4 路由。

3. PE 间通过 Multi-hop MP-EBGP 发布标签 VPN-IPv4 路由

前面介绍的两种方式都需要 ASBR 参与 VPN-IPv4 路由的维护和发布。当每个 AS 都有大量的 VPN 路由需要交换时，ASBR 就很可能成为阻碍网络进一步扩展的瓶颈。解决上述可扩展性问题的方案是：ASBR 不维护或发布 VPN-IPv4 路由，PE 之间直接交换 VPN-IPv4 路由。

两个 ASBR 通过 MP-IBGP 向各自 AS 内的 PE 路由器发布标签 IPv4 路由。

ASBR 上不保存 VPN-IPv4 路由，相互之间也不通告 VPN-IPv4 路由。

ASBR 保存 AS 内 PE 的 32 位掩码带标签的 IPv4 路由，并通告给其它 AS 的对等体。过渡自治系统中的 ASBR 也通告带标签的 IPv4 路由。这样，在入口 PE 和出口 PE 之间建立起一条 LSP。

不同 AS 的 PE 之间建立 Multihop 方式的 EBGP 连接，交换 VPN-IPv4 路由。

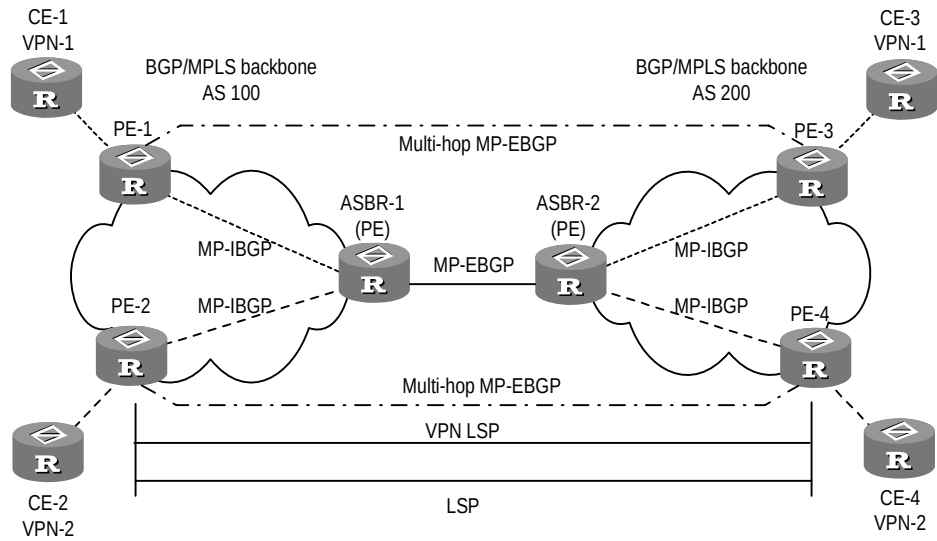


图7-9 PE 间通过 Multi-hop MP-EBGP 发布标签 VPN-IPv4 路由组网图

为提高可扩展性，可以在每个AS中指定一个路由反射器RR（Route Reflector），由RR保存所有VPN-IPv4 路由，与AS的PE交换VPN-IPv4 路由信息。两个AS的RR之间建立跨域VPNv4 连接，通告VPN-IPv4 路由。如图 7-10所示：

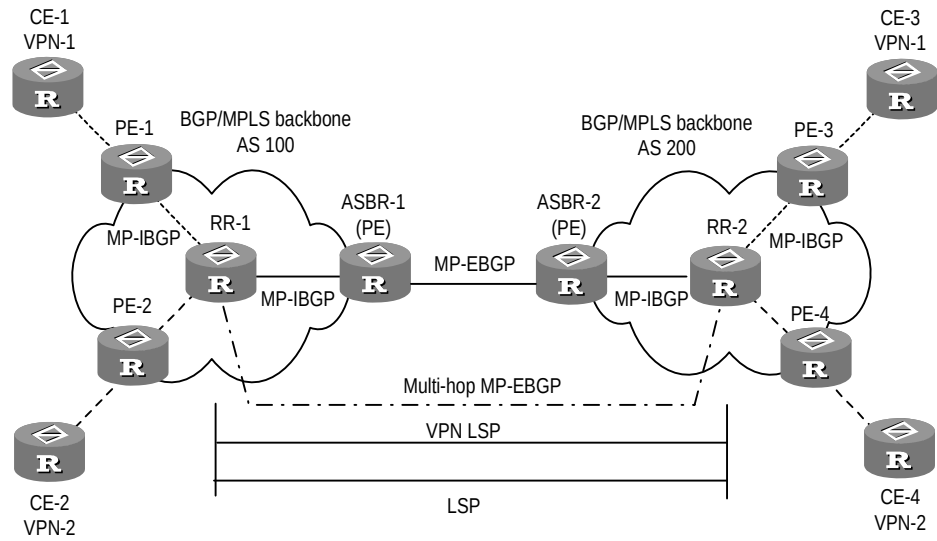


图7-10 采用 RR 的跨域 VPN OptionC 方式组网图

7.2 BGP/MPLS VPN 配置

要实现 BGP/MPLS VPN 的功能一般需要完成以下步骤：在 PE、CE、P 上配置基本信息；然后建立 PE 到 PE 的具有 IP 能力的逻辑或物理的链路；发布、更新 VPN 信息。

1. CE 设备

CE 设备的配置比较简单，只需配置静态路由、RIP、OSPF 或 EBGP 等，与相连的 PE 交换 VPN 路由信息。不需要配置 MPLS。

2. PE 设备

PE 设备的配置比较复杂，完成 MPLS/BGP VPN 的核心功能，大致可分为以下几个部分：

- 配置 MPLS 基本能力，与 P 设备和其它 PE 设备共同维护 LSP；
- 配置 BGP/MPLS VPN Site，即有关 vpn-instance 的配置；
- 配置静态路由、RIP、OSPF 或 MP-EBGP，与 CE 交换 VPN 路由信息；
- 配置 IGP，实现 PE 内部的互通；
- 配置 MP-IBGP，在 PE 之间交换 VPN 路由信息。

3. P 设备

P 设备的配置比较简单，主要是配置 MPLS 基本能力，提供 MPLS 转发能力和对 LDP 的支持。

下面 CE 对、PE、P 的配置进行分析。

7.2.1 CE 的配置

CE 作为用户端设备，仅需要做一些基本的配置，使之能够实现与 PE 设备进行路由信息的交换。目前可选择的路由交换方式有：静态路由、RIP、OSPF、EBGP、VLAN 子接口等。

1. 在 CE 上配置静态路由

如选择静态路由作为 CE-PE 间的路由交换方式，则应在 CE 上配置一条指向 PE 端的私网静态路由。

请在系统视图下进行下列配置。

表7-1 定义/清除 vpn-instance 路由表的静态路由

操作	命令
创建一条指定的 vpn-instance 的静态路由	ip route-static <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } { <i>interface-type</i> <i>interface-number</i> <i>gateway-address</i> } [<i>preference preference-value</i>] [reject blackhole]
删除一条指定的 vpn-instance 的静态路由	undo ip route-static <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } [<i>interface-type</i> <i>interface-number</i> <i>gateway-address</i>] [<i>preference preference-value</i>]

每个静态路由都有缺省的优先值 60。配置静态路由时，可以指定一条静态路由的优先级。

2. 在 CE 上配置 RIP

如选择 RIP 作为 CE-PE 间的路由交换方式，则应在 CE 上配置 RIP。有关 RIP 配置步骤的详细说明，请参阅本手册的“路由协议”部分中的 RIP 配置章节。

3. 在 CE 上配置 OSPF

如选择 OSPF 作为 CE-PE 间的路由交换方式，则应在 CE 上配置 OSPF。OSPF 的一般配置方法请参见本手册的“路由协议”部分。

4. 在 CE 上配置 EBGp

如选择 BGP 作为 CE-PE 间的路由交换方式，则应在 CE 上配置 EBGp 对等体，并应引入直连路由、静态路由及其他 IGP 路由，以便 BGP 能够将 VPN 路由全部发布给 PE。

7.2.2 PE 的配置

1. MPLS 基本能力配置

MPLS 基本能力配置包括配置 MPLS 的 LSR ID，全局使能 MPLS 并在所使用的接口视图下使能 MPLS。

具体配置请参考 MPLS 基本配置部分。

2. 定义 VPN 实例

(1) 创建并进入 VPN 实例视图

vpn-instance 在实现中与 Site 关联，一个 Site 的 VPN 成员关系和路由规则等均在 vpn-instance 的配置下体现。

该命令用来创建新的 vpn-instance 或进入已有的 VPN 实例视图。如果该 vpn-instance 已存在，则直接进入该 vpn-instance 的视图下，进行相应的配置。

请在系统视图下进行下列配置。

表7-2 创建并进入 VPN 实例视图

操作	命令
创建并进入 VPN 实例视图	ip vpn-instance <i>vpn-instance-name</i>
删除 vpn-instance	undo ip vpn-instance <i>vpn-instance-name</i>

缺省情况下，没有定义 vpn-instance。

(2) 配置 VPN-instance 的 RD

在 PE 上配置 RD，当从 CE 学习到的一条 VPN 路由引入 BGP 时，MP-BGP 将 RD 附加到 IPv4 前面，使之转换为 VPN IPv4 地址，使原来在 VPN 中的全局不唯一的 IPv4 地址成为全局唯一的 VPN IPv4 地址，以便在 VPN 中实现正确的路由。

请在 VPN 实例视图下进行下列配置。

表7-3 配置 VPN-instance 的 RD

操作	命令
配置 VPN-instance 的 RD	route-distinguisher <i>route-distinguisher</i>

参数无缺省值，一个 vpn-instance 只有配置了 RD 才能起作用。在配置 RD 之前，除了描述信息以外，不能配置 vpn-instance 的其他任何参数。

(3) 为 vpn-instance 配置描述信息

为 VPN 实例配置描述信息，请在 VPN 实例视图下进行下列配置。

表7-4 为 vpn-instance 配置描述信息

操作	命令
为 vpn-instance 配置描述信息	description <i>vpn-instance-description</i>
删除 vpn-instance 描述信息	undo description

(4) 配置 vpn-instance 的 vpn-target 属性

VPN-target 用来控制 VPN 路由信息的发布，该属性是 BGP 的扩展团体属性。

VPN 路由的发布控制过程如下：

- 当从 CE 学习到的一条 VPN 路由引入 BGP 时，BGP 为它关联一个 VPN-Target 扩展团体属性列表，通常，这个列表是与 CE 相关联的 VPN-instance 的输出路由属性列表。
- VPN-instance 根据 VPN-target 中 **import-extcommunity** 定义输入路由属性列表，定义可被接受并引入此 VPN-instance 的路由范围。
- VPN-instance 根据 VPN-target 中的 **export-extcommunity** 对向外发布的路由进行 VPN-Target 属性的修改。

像 RD 一样，一个扩展团体或者是由一个自治系统号和一个任意的数组成，或者是由一个 IP 地址和一个任意的数组成。有以下两种格式：

与自治系统号 (ASN) 相关，形式为 16 位自治系统号(ASN)：32 位用户自定义数，例如：100:1。

与 IP 地址相关，形式为 32 位 IP 地址：16 位用户自定义数，例如：172.1.1.1:1。

请在 VPN 实例视图下进行下列配置。

表7-5 为 vpn-instance 创建 vpn-target 扩展团体

操作	命令
为 vpn-instance 创建 vpn-target 扩展团体	vpn-target <i>vpn-target-extcommunity</i> [import-extcommunity export-extcommunity both]
从 vpn-instance 关联的 vpn-target 列表中删除指定的 vpn-target 属性	undo vpn-target <i>vpn-target-extcommunity</i> [import-extcommunity export-extcommunity both]

系统缺省值为 **both**。一情况下 VPN 中的所有 Site 都可以互通，此时 **import-extcommunity** 和 **export-extcommunity** 属性相同，配 **both** 即可。

一条命令最多只能配置 16 个 vpn-target；一个 vpn-instance 最多只能配置 256 个 vpn-target。

(5) 限制一个 vpn-instance 中最大路由数

该命令可以限制一个 vpn-instance 中最大路由数，防止从一个 Site 引入的路由数量过多。

请在 VPN 实例视图下进行下列配置。

表7-6 限制一个 vpn-instance 中最大路由数

操作	命令
限制一个 vpn-instance 中最大路由数	routing-table limit <i>threshold-value</i> { <i>warn-threshold</i> syslog-alert }
取消最大路由数限制	undo routing-table limit

说明：

改变 VPN-instance 的路由数目限制，不会影响已存在的路由表，如果需要新配置的路由限制立即生效，应重建相应的路由协议，或对相关接口进行 **shutdown/undo shutdown** 的操作。

(6) 将接口（含 VLAN 子接口）与 vpn-instance 关联

vpn-instance 通过与接口绑定实现与直接连接的 Site 相关联。当 Site 发来的报文经此接口进入 PE，即可查找相应的 vpn-instance 获得路由信息（包括下一条、标签、输出接口等信息）。同理，当 CE 通过 VLAN 子接口连接到 PE 时，应在 VLAN 子接口下将子接口与 vpn-instance 关联。

该命令将一个 vpn-instance 与一个接口关联起来。

请在接口或子接口视图进行下列配置。

表7-7 将接口或子接口与 vpn-instance 关联

操作	命令
将接口或子接口与 vpn-instance 关联	ip binding vpn-instance <i>vpn-instance-name</i>
取消接口或子接口与 vpn-instance 关联	undo ip binding vpn-instance <i>vpn-instance-name</i>

**注意：**

在实施接口或子接口与 vpn-instance 的绑定时，需要在接口或子接口上先执行 **ip binding vpn-instance** 命令，再配置 IP 地址，否则，已经配置的 IP 地址会因为执行 **ip binding vpn-instance** 命令而被删除。

3. 配置 PE 与 CE 间进行路由交换

目前 PE 与 CE 间的路由交换方式有：静态路由、RIP、OSPF、EBGP、VLAN 子接口等。

(1) 在 PE 上配置静态路由

可以在 PE 上配置一条指向 CE 端的静态路由，使 PE 通过静态路由的方式向 CE 学习 VPN 路由。

请在系统视图下进行下列配置。

表7-8 定义/清除 vpn-instance 路由表的静态路由

操作	命令
创建一条指定的 vpn-instance 的静态路由	ip route-static vpn-instance <i>vpn-instance-name1</i> <i>vpn-instance-name2</i> ... <i>destination-address</i> { <i>mask</i> <i>mask-length</i> } { <i>interface-type</i> <i>interface-number</i> [<i>nexthop-address</i>] vpn-instance <i>vpn-nexthop-name</i> <i>vpn-nexthop-address</i> <i>nexthop-address</i> [public] } [preference <i>preference-value</i>] [reject blackhole]
删除一条指定的 vpn-instance 的静态路由	undo ip route-static vpn-instance <i>vpn-instance-name1</i> <i>vpn-instance-name2</i> ... <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } { <i>interface-type</i> <i>interface-number</i> [vpn-instance <i>vpn-nexthop-name</i> <i>vpn-nexthop-address</i> <i>nexthop-address</i> [public] } [preference <i>preference-value</i>]

每个静态路由都有缺省的优先值 60。配置静态路由时，可以指定一条静态路由的优先级。

(2) 在 PE 上配置 RIP 多实例

在 PE 和 CE 之间配置 RIP 时，需要在 PE 上指定 RIP 实例的运行环境。使用该命令进入路由实例的配置视图，并在此视图下配置 RIP 路由实例的引入、发布等。

请在 RIP 视图下进行下列配置。

表7-9 配置 PE、CE 间的 RIP 路由协议实例

操作	命令
创建 PE、CE 间的 RIP 路由协议实例	ipv4-family [unicast] vpn-instance <i>vpn-instance-name</i>
取消 PE、CE 间的 RIP 路由协议实例	undo ipv4-family [unicast] vpn-instance <i>vpn-instance-name</i>

然后配置 RIP 多实例引入 IBGP 路由。

有关 RIP 配置步骤的详细说明，请参阅本手册的“路由协议”部分中的 RIP 配置章节。

(3) 在 PE 上配置 EBGp

PE 与 CE 之间运行 EBGp，应在 MP-BGP 的 VPN-instance 视图下，为每个 VPN 配置邻居，并引入 CE 的 IGP 路由。

第一步：配置对等体组

请在配置 VPN-instance 视图下配置对等体所隶属的对等体组。

表7-10 配置对等体组

操作	命令
创建一个对等体组	group group-name [internal external]
删除指定的对等体组	undo group group-name

配置时，如果不指定对等体组的配置类型，缺省为 **internal**。因为当 PE、CE 选用 BGP 进行路由交换时，一般属于不同的 AS，此时，应选用 **external**，建立 EBGp 对等体。

第二步：指定邻居 AS 号并向对等体组中加入组员

在 PE 和 CE 之间可以通过 EBGp 来交换路由信息，应为每个对应 CE 的 vpn-instance 分别指定邻居的 AS 号。

请在 MP-BGP 的 vpn-instance 视图下进行下列配置。

表7-11 配置指定同伴的 AS 号

操作	命令
配置指定邻居的 AS 号	peer group-name as-number as-number peer peer-address group group-name [as-number as-number]
删除邻居的 AS 号	undo peer { group-name as-number peer-address }

第三步：配置 MP-BGP 引入 IGP 路由

为了正确地在公网上传播 VPN 路由信息，PE 必须将与它直接相连的 CE 的 VPN 路由引入自己的 MBGP 路由表中，以发布给建立了 BGP 邻居关系的其它 PE。

举例来讲：如果 PE 与 CE 间使用静态路由，则 PE 需要在 MBGP 的 VPN-instance 视图下引入静态路由（`import-route static`）；如果 PE 与 CE 间运行 RIP，则 PE 需要在 MBGP 的 VPN-instance 视图下引入 RIP 路由（`import-route rip`），如果 PE 与 CE 之间运行 BGP，则 MBGP 直接引入直连路由即可。

请在 MBGP 的 VPN-instance 视图下进行下列配置。

表7-12 引入 IGP 协议的路由信息

操作	命令
配置 BGP 引入 IGP 协议的路由	<code>import-route protocol [process-id] [med med]</code>
取消 BGP 引入 IGP 协议的路由	<code>undo import-route protocol</code>

第四步：配置 BGP 的同步方式为不同步

请在 MBGP 的 VPN-instance 视图下进行下列配置。

表7-13 配置允许 BGP 与 IGP 不同步

操作	命令
配置允许 BGP 与 IGP 不同步	<code>undo synchronization</code>

目前，不同步方式为缺省配置。

第五步：Hub&Spoke 组网中允许路由环路配置（选配）。

一般来说，配置 PE-CE 的步骤通过指定邻居 AS 号后就可以完成，其余的配置保留系统默认值即可。

在标准 BGP 情况下，BGP 是通过 AS 号来检测路由循环，避免产生路由环路。但在 Hub&Spoke 组网方式下，如果在 PE 和 CE 之间运行 EBGP 协议，当 PE 将路由信息通告给 CE 时带上本自治系统的 AS 号。然后再从 CE 接收路由更新时，路由更新消息中就会带有本自治域系统的 AS 号，这样 PE 就不会接收这条路由更新信息。

通过配置 `peer allow-as-loop` 可以使 PE 仍然接收从 CE 发送的包含本 AS 号的路由更新信息。

请在 IPv4 地址族子视图下进行下列配置。

表7-14 配置允许/禁止路由环路

操作	命令
配置允许路由环路	peer { group-name peer-address } allow-as-loop [number]
配置禁止路由环路	undo peer { group-name peer-address } allow-as-loop

默认情况下，对于接收到的路由更新信息不允许产生环路信息。

第六步：配置 BGP 相关特性。

4. 配置 PE-PE 间进行路由交换

在 PE 上配置 MP-IBGP 协议，使得 PE 之间能够交互 VPN-IPv4 路由。

下列各项配置可在 BGP 视图或 VPN 实例视图下进行。

(1) 配置 IBGP

一般情况下，需要配置以下各项：

第一步：配置 BGP 的同步方式为不同步

第二步：配置 BGP 邻居

注意，应用 loopback 接口建立 BGP 的邻居关系，且子网掩码应为 32 位。

第三步：配置允许内部 BGP 会话使用任何可操作的 TCP 连接接口

一般情况下，BGP 是使用最佳本地地址进行 TCP 连接的；但为使接口在出现问题时该 TCP 连接还有效，可配置允许内部 BGP 会话使用任何可与对端建立 TCP 连接的接口，这条命令通常与 Loopback 接口一起配置。

表7-15 配置允许内部 BGP 会话使用任何可操作的 TCP 连接接口

操作	命令
配置允许内部 BGP 会话使用任何可操作的 TCP 连接的接口	peer { peer-address group-name } connect-interface interface-type interface-number
恢复使用最佳本地地址进行 TCP 连接	undo peer { peer-address group-name } connect-interface

BGP 可以使用指定接口和对端建立 BGP 邻居，一般来说都是指定 LoopBack 环回接口。因为这个接口永远处于 up 状态，可以减少由于网络震荡带来的冲击。

(2) 配置 MP-IBGP

第一步：进入协议地址族视图

请在 BGP 视图下进行下列配置。

表7-16 配置 vpnv4 地址族

操作	命令
进入 MBGP 的 vpnv4 视图	ipv4-family vpnv4 [unicast]
删除 MBGP 的 VPNv4 地址族视图的配置	undo ipv4-family vpnv4 [unicast]

第二步：配置 MBGP 邻居。

在 MBGP 的 vpnv4 视图下配置 MBGP 的 **internal** 邻居。

第三步：配置激活对等体（组）。

由于缺省情况下，BGP 邻居处于激活状态，MBGP 邻居处于非激活状态。用户应在 vpnv4 视图下激活 MBGP 邻居。

第四步：配置在发布路由时将自身地址作为下一跳（可选）

该配置命令缺省为没有配置，在跨域 VPN 配置 B 方式下，对域内的 IBGP 对等体必需要配置该命令。

请在 MBGP 的 vpnv4 视图下进行下列配置。

表7-17 配置在发布路由时将自身地址作为下一跳

操作	命令
配置发布路由时将自身地址作为下一跳	peer group-name next-hop-local
取消发布路由时将自身地址作为下一跳	undo peer group-name next-hop-local

第五步：配置传送 BGP 更新报文时不携带私有自治系统号（可选）

请在 MBGP 的 vpnv4 视图下进行下列配置。

表7-18 配置发送 BGP 更新报文时不携带私有自治系统号

操作	命令
配置发送 BGP 更新报文时不携带私有自治系统号	peer group-name public-as-only
配置发送 BGP 更新报文时携带私有自治系统号	undo peer group-name public-as-only

5. OSPF VPN 扩展配置

本节介绍 OSPF VPN 扩展的三种应用配置，包括：

- 在 PE-CE 间运行 OSPF
- 配置 Multi-VPN-Instance CE
- 配置 sham link

(1) 在 PE 上配置 OSPF 多实例

在 PE 上运行 OSPF 与 CE 交换路由信息，需要 OSPF 支持多实例配置。其他配置，如 MPLS 基本配置、vpn-instance 的配置不变。需要注意的是，在 vpn-instance 下应引入 OSPF 路由及直连路由，在 OSPF 下也应引入 BGP 路由。这里对 OSPF 多实例的配置进行详细描述。

第一步：配置 OSPF 进程。

请在系统视图下进行下列配置。

表7-19 配置 OSPF 进程

操作	命令
配置一个 OSPF 进程	ospf process-id [router-id router-id-number] [vpn-instance vpn-instance-name]
删除一个 OSPF 进程	undo ospf process-id

缺省进程号为 1。



注意：

一个 OSPF 进程只能属于一个 vpn 实例，一个实例可以包含多个 OSPF 进程。缺省状态下 OSPF 进程属于公网。

第二步：配置 domain-id。

Domain ID 用来标识不同的 OSPF 路由自治域，同一个 OSPF 路由域需要配置相同的 Domain ID。每个进程只能配置一个 domain-id，不同的进程之间可配置相同的 domain-id，也可配置不同的 domain-id。

表7-20 配置 domain-id

操作	命令
配置 domain-id	domain-id { id-number id-addr }
恢复缺省值	undo domain-id

id-number 缺省为 0，id-addr 缺省为 0.0.0.0。

一般建议：与每个 VPN 实例相关的网络中的所有 OSPF 实例要么配置一个相同的 Domain ID，要么都使用缺省的 0 作为 Domain ID。



注意：

执行这个命令后，不会马上起作用，只有在 reset ospf 后才会起作用。

第三步：配置标识 VPN 引入路由的 tag 值（可选）。

如果同一个 VPN site 链接了多个 PE，那么从 MPLS/BGP 学到的路由，被一个 PE 通过 5 类或 7 类 LSA 向 VPN site 发布时，可能被另一个 PE 收到，造成路由环。为了防止路由环，在这种情况下应配置 Route-tag，且同一 VPN 域的 PE 最好配置相同的 route-tag。

请在 OSPF 视图下进行下列配置。



注意：

配置 route-tag 后，不会马上起作用，只有在 reset ospf 后才会起作用。

表7-21 配置标识 VPN 引入路由的 tag 值

操作	命令
配置标识 VPN 引入路由的 tag 值	route-tag tag-number
恢复缺省值	undo route-tag

tag-number 用来标识 VPN 引入路由的 tag 值，取默认值时前面两个字节为固定的 0xD000，后面的两个字节为本端 BGP 的 AS 号，比如本端 BGP AS 号为 100，则其默认的 tag 十进制值为 3489661028。该值的取值范围为 0~4294967295 的整数。

(2) 配置安全网关成为多实例 CE

当需要在 CE 安全网关上隔离不同 VPN 之间的业务时，应配置 OSPF 多实例。此时的 CE 称为 Multi-VPN-Instance CE。

如果在 CE 安全网关上配置 OSPF 进程绑定 VPN 实例后，则必须在 OSPF 协议视图配置如下命令。

表7-22 配置安全网关变为 Multi-VPN-Instance CE

操作	命令
配置安全网关变为 Multi-VPN-Instance CE	vpn-instance-capability simple
取消配置	undo vpn-instance-capability

(3) 配置 sham link

当两个 CE 之间存在 backdoor 链路（即不是通过 MPLS 骨干网络的 OSPF 链路），此时，又希望数据通过 MPLS 骨干传送时，就需要在两个 PE 之间配置 sham link。在 VPN PE 间配置 sham link，将其视为 OSPF 区域内的一条 link。其中，源地址和目的地址均为 32 位掩码的 loopback 接口地址，且该 loopback 接口需在 VPN 实例中绑定，并通过 BGP 引入直连路由引入到 BGP 中。

请在 OSPF 区域视图下配置下面命令。

表7-23 配置 sham link

操作	命令
配置 sham link	sham-link <i>source-addr destination-addr</i> [cost <i>cost-value</i>] [simple password md5 <i>keyid key</i>] [dead <i>seconds</i>] [hello <i>seconds</i>] [retransmit <i>seconds</i>] [trans-delay <i>seconds</i>]
删除 sham link	undo sham-link <i>source-addr destination-addr</i>

其中，**cost** 的缺省值为 1，**dead** 的缺省值为 40 秒，**hello** 的缺省值为 10 秒，**retransmit** 的缺省值为 5 秒，**trans-delay** 的缺省值为 1 秒。

6. 多角色主机特性配置

PE-PE 间进行路由交换配置完成后，必须在 PE 上进行如下配置，才能够实现与之相连的 Site 的多角色应用。

第一步：在 PE 上配置 vpn-instance。

在多角色主机应用中，一个 Site 经一个物理接口接入到 PE，但可以访问多个 VPN，故需要在 PE 上配置多个 vpn-instance，仅将可以直接访问的 VPN 与连接 Site 的接口绑定即可。vpn-instance 的配置，请参考 2. 定义 VPN 实例。

第二步：配置策略路由。

在策略路由使能后满足 route-policy 的条件情况下，指定报文依次在已经配置的 vpn-name1, vpn-name2, vpn-name3, vpn-name4, vpn-name5, vpn-name6 中查找私网转发路由并进行相应的转发。

请在 route-policy 视图下进行下列配置。

表7-24 在指定 VPN 实例中查找私网转发路由并进行相应的转发

操作	命令
在指定 VPN 实例中查找私网转发路由并进行相应的转发	apply access-vpn <i>vpn-instance</i> [<i>vpn-name1 vpn-name2 ...</i>]
取消在指定 VPN 实例中的查找	undo apply access-vpn <i>vpn-instance</i> [<i>vpn-name1 vpn-name2 ...</i>]

第三步：配置到一个私网的静态路由。

通过配置静态路由，指定其他 VPN 中的接口作为出接口，从而使从 PE 返回到 CE 的下行报文，能够直接返回 Site。

请在系统视图下配置下列命令。

表7-25 配置到一个私网的静态路由

操作	命令
用于配置到一个私网的静态路由	ip route-static vpn-instance <i>vpn-instance-name1</i> <i>vpn-instance-name2</i> ... <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } { <i>interface-type</i> <i>interface-number</i> [vpn-instance <i>vpn-nexthop-name</i> <i>vpn-nexthop-address</i>] } [preference <i>preference-value</i>] [reject blackhole]
取消静态路由的配置	undo ip route-static vpn-instance <i>vpn-instance-name1</i> <i>vpn-instance-name2</i> ... <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } { <i>interface-type</i> <i>interface-number</i> [vpn-instance <i>vpn-nexthop-name</i> <i>vpn-nexthop-address</i>] } [preference <i>preference-value</i>] [reject blackhole]

7. 配置跨域 VPN

PE-PE 间进行路由交换配置完成后，再进行如下配置才能实现跨域的 MPLS VPN。

(1) 配置 VPN-Target 过滤

缺省情况下，PE 对收到的 VPNv4 路由进行 VPN-target 过滤。通过过滤的路由会被加入到路由表中，没有通过过滤的路由将被丢弃。

当 PE 同时作为 ASBR 时，它需要保存所有 VPNv4 路由信息，以通告给其它 ASBR。这种情况下，PE 应接收所有 VPNv4 路由信息，不对它们路由进行 VPN-target 过滤，即 ASBR-PE 之间只要是 peer 的路由都接受，不区分 VPN-target。

请在 BGP-VPNv4 子地址族视图下进行下列配置。

表7-26 配置 VPN-Target 过滤

操作	命令
允许对 VPNv4 路由进行 VPN-Target 过滤	policy vpn-target
不对 VPNv4 路由进行 VPN-Target 过滤	undo policy vpn-target

undo policy vpn-target 只用在 PE 同时作为 ASBR 时，且为跨域 VPN 的 OptionB 方式。

(2) 配置对公网路由的标签处理

在 Multihop MP-EBGP 方式的跨域 VPN 解决方案中，需要建立一条跨域的 VPN LSP，相关 PE、ASBR 之间发布公网路由时需要携带 MPLS 标签信息。

对公网路由分配 MPLS 标签是通过路由策略控制的，只对满足某些条件的路由分配标签，其它路由还是普通 IPv4 路由。

请在 Route-policy 视图下进行下列配置。

表7-27 配置对公网路由的标签处理

操作	命令
为满足 Route-policy 匹配条件的公网路由分配 MPLS 标签	apply mpls-label
取消为公网路由分配 MPLS 标签	undo apply mpls-label
配置只收发带 MPLS 标签的公网路由	if-match mpls-label
取消收发带 MPLS 标签的公网路由	undo if-match mpls-label

缺省情况下，公网路由不带 MPLS 标签，没有定义 Route-policy。

携带 MPLS 标签的公网路由通过 MP-BGP 发布。根据 RFC3107 (Carrying Label Information in BGP-4) 中的描述，一条路由的标签映射信息可以通过发布这条路由的 BGP Update 消息捎带 (piggyback)。这种能力使用 BGP 的扩展属性实现，要求 BGP 对等体能够处理标签 IPv4 路由。

请在 BGP 视图下进行下列配置。

表7-28 配置标签 IPv4 路由处理能力

操作	命令
使能处理标签 IPv4 路由的能力	peer group-name label-route-capability
取消处理标签 IPv4 路由的能力	undo peer group-name label-route-capability

缺省情况下，BGP 对等体不能处理标签 IPv4 路由。

(3) 配置发布路由时不改变下一跳

通常情况下，BGP Speaker 在向 EBGp 对等体发布路由时，会将下一跳改为自己。在采用 Multihop MP-EBGP 跨域 VPN 方式，并使用路由反射器 RR (Route Reflector) 通告 VPNv4 路由的组网应用中，RR 之间通告 VPNv4 路由时，路由的下一跳不能被改变。

下列配置可在 BGP 视图、BGP-VPNv4 子地址族视图、BGP VPN 实例视图、BGP-IPv4 组播子地址族视图下进行。

表7-29 配置发布路由时不改变下一跳

操作	命令
配置向 EBGp 对等体发送路由时不改变下一跳	peer group-name next-hop-invariable
恢复缺省设置	undo peer group-name next-hop-invariable

缺省情况下，向 EBGp 对等体发送路由时，下一跳会改为 BGP Speaker。

7.2.3 配置 P

P 不需要维护 VPN 路由，但需要保证公网的连通性，并配合 PE 建立 LSP，故需要如下配置：

第一步：配置 MPLS 基本能力，并在 P 与 PE 相连的各接口上使能 LDP，以转发 MPLS 报文。具体配置请参见本手册“MPLS”部分中的 MPLS 配置

第二步：在 P 与 PE 相连的各接口上启动 OSPF 协议，并引入直连路由，实现 PE 内部的互通。具体配置请参见本手册“路由协议”的“OSPF”部分。

7.3 BGP/MPLS VPN 显示与调试

1. 从 BGP 表中显示 VPN 地址信息

在完成上述配置后，在所有视图下执行 **display** 命令，可以显示 BGP 数据库中 VPNv4 信息，通过查看显示信息，验证配置的效果。

表7-30 从 BGP 表中显示 VPN 地址信息

操作	命令
从 BGP 表中显示 VPN 地址信息	display bgp vpnv4 { all route-distinguisher rd-value vpn-instance vpn-instance-name } { group [group-name] network peer [ip-address1 verbose] routing [ip-address2 statistic] [label] [as-path-acl as-path-acl cidr community [community-number no-advertise no-export no-export-subconfed whole-match] community-list community-list [whole-match] different-origin-as peer ip-address1 [advertised received] regular-expression text }

2. 显示与 vpn-instance 相关联的 IP 路由表

在完成上述配置后，在所有视图下执行 **display** 命令可以显示与 vpn-instance 相关联的 IP 路由表中的相关信息，通过查阅该显示信息来验证配置的效果。

表7-31 显示与 vpn-instance 相关联的 IP 路由表

操作	命令
显示与 vpn-instance 相关联的 IP 路由表	display ip routing-table vpn-instance vpn-instance-name [statistics [ip-address] [verbose]]

3. 显示 vpn-instance 相关信息

在完成上述配置后，在所有视图下执行 **display** 命令可以显示 vpn-instance 相关信息，包括该 VPN 实例的 RD，描述以及与之关联的接口等信息，通过查阅该显示信息来验证配置的效果。

表7-32 显示 vpn-instance 相关信息

操作	命令
显示 vpn-instance 相关信息，包括该 VPN 实例的 RD，描述以及与之关联的接口等信息	display ip vpn-instance [<i>vpn-instance-name</i> verbose]

4. 显示涉及处理 BGP 的调试信息

在用户视图下，执行 **debugging** 命令可对 BGP 相关运行情况进行调试。

表7-33 显示涉及处理 BGP 的调试信息

操作	命令
显示涉及处理 BGP 的调试信息	debugging bgp { { keepalive mp-update open packet update route-refresh } [receive send verbose] } { all event normal }
关闭调试信息	undo debugging bgp { { keepalive mp-update open packet update route-refresh } [receive send verbose] } { all event normal }

5. 显示 MPLS I3vpn-lsp 的相关信息

表7-34 显示 MPLS I3vpn-lsp 的相关信息

操作	命令
显示 mpls I3vpn 标签交换路径的相关信息	display mpls I3vpn-lsp [verbose] [include text]
显示 mpls I3vpn 标签交换路径 vpn-instance 相关的信息	display mpls I3vpn-lsp [vpn-instance <i>vpn-instance-name</i>] [transit egress ingress] [include text verbose]

6. 显示配置的 sham link

表7-35 显示配置的 sham link

操作	命令
显示配置的 sham link	display ospf [<i>process-id</i>] sham-link

7.4 BGP/MPLS VPN 典型配置举例

7.4.1 BGP/MPLS VPN 综合组网举例

1. 组网需求

- CE1、CE3 构成 VPN-A，CE2、CE4 构成 VPN-B；

- 不同 VPN 用户之间不能互相访问。VPN-A 使用的 VPN-target 属性为 111:1, VPN-B 使用的 VPN-target 属性为 222:2;
- PE 和 P 使用 SecPath 系列安全网关, CE 为一般的中低端设备。

说明:

此案例的配置重点在于:

- CE 与 PE 之间配置 EBGp 交换 VPN 路由信息
- PE 之间配置 OSPF 实现 PE 内部的互通
- PE 之间配置 MP-IBGP 交换 VPN 路由信息

2. 组网图

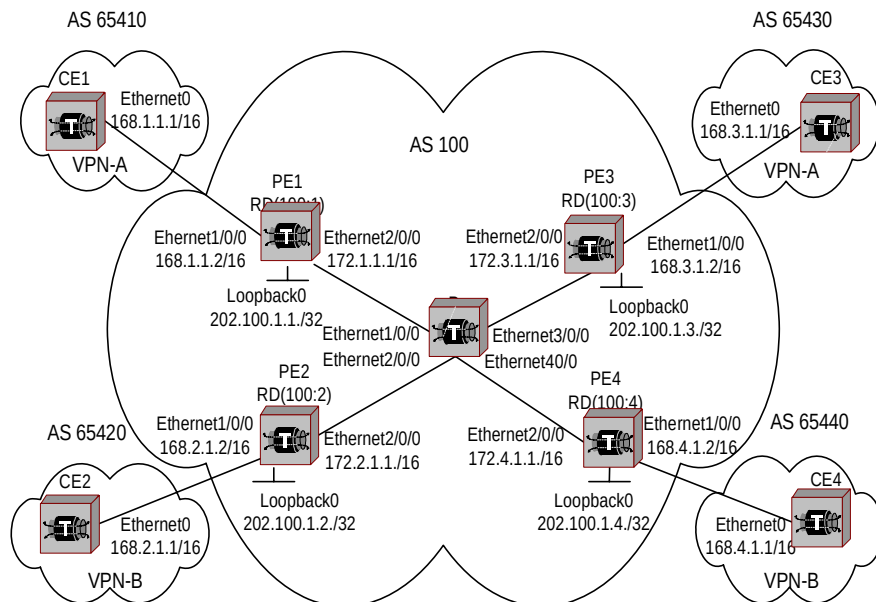


图7-11 BGP/MPLS VPN 综合组网图

3. 配置步骤

下面依次介绍各 PE、CE 和 P 上的配置。

(1) 配置 CE1

CE1 与 PE1 建立 EBGp 邻居, 引入直连路由和静态路由, 从而将 CE1 的内部 VPN 路由引入到 BGP, 进而发布给 PE1。CE1 使用接口 Ethernet0 与 PE1 相连。

```
[CE1] interface ethernet 0
[CE1-Ethernet0] ip address 168.1.1.1 255.255.0.0
[CE1-Ethernet0] quit
[CE1] bgp 65410
[CE1-bgp] group 168 external
[CE1-bgp] peer 168.1.1.2 group 168 as-number 100
```

```
[CE1-bgp] import-route direct
[CE1-bgp] import-route static
```

 说明:

另外 3 个 CE (CE2~CE4) 配置与 CE1 配置类似, 配置过程省略。

(2) 配置 PE1

在 PE1 上创建 VPN-A 的 VPN-instance, 并配置相关属性以控制 VPN 路由信息的发布。

```
[PE1] ip vpn-instance vpna
[PE1-vpn-vpna] route-distinguisher 100:1
[PE1-vpn-vpna] vpn-target 111:1 both
[PE1-vpn-vpna] quit
```

PE1 与 CE1 间建立 EBGP 邻居, 并将学到的 CE1 内部 VPN 路由引入 MBGP 的 VPN-instance 地址族。

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-af-vpn-instance] group 168 external
[PE1-bgp-af-vpn-instance] peer 168.1.1.1 group 168 as-number 65410
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] quit
```

将 PE1 与 CE1 相连的接口 Ethernet1/0/0 绑定到 VPN-A (需要注意的是, 应先配置接口与 VPN-instance 的关联后, 再配置接口的 IP 地址)。

```
[PE1] interface ethernet 1/0/0
[PE1-Ethernet1/0/0] ip binding vpn-instance vpna
[PE1-Ethernet1/0/0] ip address 168.1.1.2 255.255.0.0
[PE1-Ethernet1/0/0] quit
```

配置 LoopBack 接口 (对 PE 配置 LoopBack 接口地址时, 必须使用 32 位掩码的主机地址, 以防止此路由被聚合, 导致 LSP 不能正确处理内层标签)。

```
[PE1] interface loopback0
[PE1-LoopBack 0] ip address 202.100.1.1 255.255.255.255
[PE1-LoopBack 0] quit
```

配置 MPLS 基本能力, 并在 PE1 与 P 相连的接口上使能 MPLS 及 LDP。建立 LSP 和实现 MPLS 报文转发。

```
[PE1] mpls lsr-id 202.100.1.1
[PE1] mpls
[PE1-mpls] mpls ldp
```

```
[PE1-mpls] quit
[PE1] interface Ethernet2/0/0
[PE1-Ethernet2/0/0] ip address 172.1.1.1 255.255.0.0
[PE1-Ethernet2/0/0] mpls
[PE1-Ethernet2/0/0] mpls ldp enable
[PE1-Ethernet2/0/0] quit
```

在 PE1 与 P 相连的接口及 loopback 接口上启用 OSPF，并引入直连路由。实现 PE 内部的互通。

```
[PE1] ospf
[PE1-ospf] area 0
[PE1-ospf-area-0.0.0.0] network 172.1.0.0 0.0.255.255
[PE1-ospf-area-0.0.0.0] network 202.100.1.1 0.0.0.0
[PE1-ospf-area-0.0.0.0] quit
[PE1-ospf] import-route direct
[PE1-ospf] quit
```

在 PE 与 PE 之间建立 MP-IBGP 邻居，进行 PE 内部的 VPN 路由信息交换。并在 VPNv4 地址族视图下激活 MP-IBGP 对等体。

```
[PE1] bgp 100
[PE1-bgp] group 202 internal
[PE1-bgp] peer 202.100.1.3 group 202
[PE1-bgp] peer 202.100.1.3 connect-interface loopback0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer 202 enable
[PE1-bgp-af-vpn] peer 202.100.1.3 group 202
[PE1-bgp-af-vpn] quit
[PE1-bgp] quit
```

(3) 配置 P

配置 P 的 MPLS 基本能力，并在 P 与 PE 相连的各接口上使能 LDP，以转发 MPLS 报文。

```
[P] mpls lsr-id 172.1.1.2
[P] mpls
[P-mpls] mpls ldp
[P-mpls] quit
[P] interface Ethernet1/0/0
[P-Ethernet1/0/0] ip address 172.1.1.2 255.255.0.0
[P-Ethernet1/0/0] mpls
[P-Ethernet1/0/0] mpls ldp enable
[P-Ethernet1/0/0] interface Ethernet2/0/0
[P-Ethernet2/0/0] ip address 172.2.1.2 255.255.0.0
[P-Ethernet2/0/0] mpls
```



```
[P-Ethernet2/0/0] mpls ldp enable
[P-Ethernet2/0/0] interface Ethernet3/0/0
[P-Ethernet3/0/0] ip address 172.3.1.2 255.255.0.0
[P-Ethernet3/0/0] mpls
[P-Ethernet3/0/0] mpls ldp enable
[P-Ethernet3/0/0] interface Ethernet4/0/0
[P-Ethernet4/0/0] ip address 172.4.1.2 255.255.0.0
[P-Ethernet4/0/0] mpls
[P-Ethernet4/0/0] mpls ldp enable
[P-Ethernet4/0/0] quit
```

在 P 与 PE 相连的各接口上启动 OSPF 协议，并引入直连路由，实现 PE 内部的互通。

```
[P] ospf
[P-ospf] area 0
[P-ospf-area-0.0.0.0] network 172.1.1.0 0.0.255.255
[P-ospf-area-0.0.0.0] network 172.2.1.0 0.0.255.255
[P-ospf-area-0.0.0.0] network 172.3.1.0 0.0.255.255
[P-ospf-area-0.0.0.0] network 172.4.1.0 0.0.255.255
[P-ospf-area-0.0.0.0] quit
[P-ospf] import-route direct
```

(4) 配置 PE3

说明:

PE3 的配置过程与 PE1 相似，需要注意 PE3 上对于 VPN 路由属性的设置，以了解如何控制同一 VPN 的路由信息在 MPLS 网上的发布（相同的 VPN-target）。

在 PE3 上创建 VPN-A 的 VPN-instance，并配置相关属性以控制 VPN 路由信息的发布。

```
[PE3] ip vpn-instance vpna
[PE3-vpn-vpna] route-distinguisher 100:3
[PE3-vpn-vpna] vpn-target 111:1 both
[PE3-vpn-vpna] quit
```

PE3 与 CE3 间建立 EBGP 邻居，并将学到的 CE3 内部 VPN 路由引入 MBGP 的 VPN-instance 地址族。

```
[PE3] bgp 100
[PE3-bgp] ipv4-family vpn-instance vpna
[PE3-bgp-af-vpn-instance] group 168 external
[PE3-bgp-af-vpn-instance] peer 168.3.1.1 group 168 as-number 65430
[PE3-bgp-af-vpn-instance] import-route direct
[PE3-bgp-af-vpn-instance] quit
```

```
[PE3-bgp] quit
```

将 PE3 与 CE3 相连的接口 Ethernet1/0/0 绑定到 VPN-A。

```
[PE3] interface ethernet 1/0/0
```

```
[PE3-Ethernet1/0/0] ip binding vpn-instance vpna
```

```
[PE3-Ethernet1/0/0] ip address 168.3.1.2 255.255.0.0
```

```
[PE3-Ethernet1/0/0] quit
```

配置 LoopBack 接口。

```
[PE3] interface loopback0
```

```
[PE3-LoopBack 0] ip address 202.100.1.3 255.255.255.255
```

```
[PE3-LoopBack 0] quit
```

配置 MPLS 基本能力, 并在 PE3 与 P 相连的接口上使能 MPLS 及 LDP。建立 LSP 和实现 MPLS 报文转发。

```
[PE3] mpls lsr-id 202.100.1.3
```

```
[PE3] mpls
```

```
[PE3-mpls] mpls ldp
```

```
[PE3-mpls] quit
```

```
[PE3] interface Ethernet 2/0/0
```

```
[PE3-Ethernet2/0/0] ip address 172.3.1.1 255.255.0.0
```

```
[PE3-Ethernet2/0/0] mpls
```

```
[PE3-Ethernet2/0/0] mpls ldp enable
```

```
[PE3-Ethernet2/0/0] quit
```

在 PE3 与 P 相连的接口及 loopback 接口上启用 OSPF, 并引入直连路由。

```
[PE3] ospf
```

```
[PE3-ospf-area-0.0.0.0] network 172.3.0.0 0.0.255.255
```

```
[PE3-ospf-area-0.0.0.0] network 202.100.1.3 0.0.0.0
```

```
[PE3-ospf-area-0.0.0.0] import-route direct
```

在 PE 与 PE 之间建立 MP-IBGP 邻居, 进行 PE 内部的 VPN 路由信息交换。

```
[PE3] bgp 100
```

```
[PE3-bgp] group 202 internal
```

```
[PE3-bgp] peer 202.100.1.1 group 202
```

```
[PE3-bgp] peer 202.100.1.1 connect-interface loopback0
```

```
[PE3-bgp-af-vpn] peer 202 enable
```

```
[PE3-bgp-af-vpn] peer 202.100.1.1 group 202
```

```
[PE3-bgp-af-vpn] quit
```

(5) PE2 与 PE4 的配置

PE2 与 PE4 的配置与 PE1 和 PE3 的配置类似, 具体配置过程略。

7.4.2 采用 GRE 隧道的 BGP/MPLS VPN 配置举例

1. 组网需求

- CE-1、CE-3 构成 VPN_A，CE-2、CE-4 构成 VPN_B。
- PE 使用 SecPath 系列安全网关，PE 需要支持 MPLS 能力。P 为任意的 SecPath 系列安全网关（无须支持 MPLS 能力），CE 为一般的中低端设备。

2. 组网图

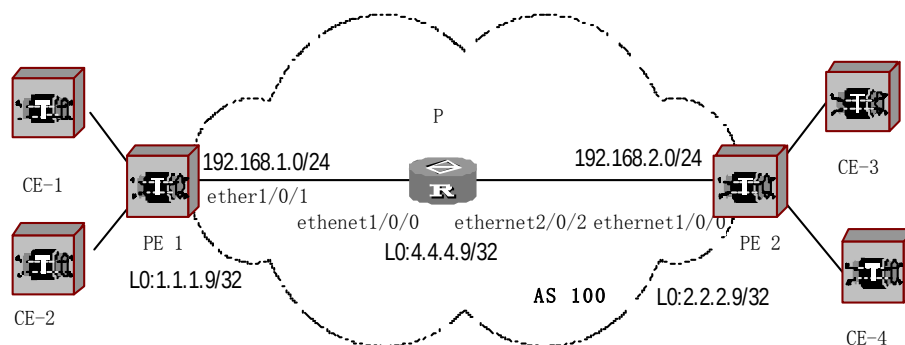


图7-12 采用 GRE 隧道的 BGP/MPLS VPN 组网图

3. 配置步骤

(1) 配置 CE1

CE1 与 PE1 建立 EBGP 邻居，引入直连路由和静态路由，从而将 CE1 的内部 VPN 路由引入到 BGP，进而发布给 PE1，CE1 使用接口 Ethernet0 与 PE1 相连。

```
[CE1] interface ethernet 0
[CE1-Ethernet0] ip address 20.1.1.1 255.255.0.0
[CE1-Ethernet0] quit
[CE1] bgp 65410
[CE1-bgp] group 20 external
[CE1-bgp] peer 20.1.1.2 group 20 as-number 100
[CE1-bgp] import-route direct
[CE1-bgp] import-route static
```

说明：

另外 3 个 CE（CE2~CE4）配置与 CE1 配置类似，配置过程省略。

(2) 配置 PE1

VPN-instance 配置。

```
[PE1] ip vpn-instance vpna
```

```
[PE1-vpn-vpna] route-distinguisher 100:1
```

```
[PE1-vpn-vpna] vpn-target 100:1 both
```

```
[PE1-vpn-vpna] quit
```

接口配置，将 PE1 与 CE1 相连的接口 Ethernet1/0/0 绑定到 VPN-A。

```
[PE1] interface loopback0
```

```
[PE1-LoopBack0] ip address 1.1.1.9 255.255.255.255
```

```
[PE1-LoopBack0] quit
```

```
[PE1] interface ethernet 1/0/0
```

```
[PE1-Ethernet1/0/0] ip binding vpn-instance vpna
```

```
[PE1-Ethernet1/0/0] ip address 20.1.1.2 255.255.0.0
```

```
[PE1-LoopBack1/0/0] quit
```

```
[PE1] interface ethernet1/0/1
```

```
[PE1-Ethernet1/0/1] ip address 192.168.1.1 255.255.255.0
```

```
[PE1-Ethernet1/0/1] quit
```

PE1 与 CE1 间建立 EBGP 邻居，并引入 VPN-instance 的接口路由。

```
[PE1] bgp 100
```

```
[PE1-bgp] ipv4-family vpn-instance vpna
```

```
[PE1-bgp-af-vpn-instance] group 20 external
```

```
[PE1-bgp-af-vpn-instance] peer 20.1.1.1 group 20 as-number 65410
```

```
[PE1-bgp-af-vpn-instance] peer 20 next-hop-local
```

```
[PE1-bgp-af-vpn-instance] import-route direct
```

```
[PE1-bgp-af-vpn-instance] quit
```

```
[PE1-bgp] quit
```

在 PE 与 PE 之间建立 MP-IBGP 邻居，进行 PE 内部的 VPN 路由信息交换，并在 VPNv4 地址族视图下激活 IBGP 对等体。

```
[PE1] bgp 100
```

```
[PE1-bgp] group 2
```

```
[PE1-bgp] peer 2.2.2.9 group 2
```

```
[PE1-bgp] peer 2.2.2.9 connect-interface loopback0
```

```
[PE1-bgp] ipv4-family vpnv4
```

```
[PE1-bgp-af-vpn] peer 2 enable
```

```
[PE1-bgp-af-vpn] peer 2.2.2.9 group 2
```

在 PE1 与 P 相连的接口及环回接口上启用 OSPF，并引入直连路由，实现 AS 内部的互通。

```
[PE1] ospf
```

```
[PE1-ospf-1] area 0
```

```
[PE1-ospf-1-area-0.0.0.0] network 192.168.1.0 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] import-route direct
```

配置 MPLS。

```
[PE1] mpls lsr-id 1.1.1.9
```

```
[PE1] mpls
```

```
[PE1-mpls] mpls ldp
```

配置 GRE 隧道。

```
[PE1] interface tunnel 1
```

```
[PE1-Tunnel1] tunnel-protocol gre
```

```
[PE1-Tunnel1] source loopback 0
```

```
[PE1-Tunnel1] destination 2.2.2.9
```

```
[PE1-Tunnel1] mpls
```

```
[PE1-Tunnel1] mpls ldp enable
```

```
[PE1-Tunnel1] mpls ldp transport-ip interface
```

 说明：

- PE2 配置与 PE1 类似，配置过程省略。
 - VPN_B 的配置与 VPN_A 的配置类似，但是要为 VPN_B 设置唯一的 route distinguisher，并且正确的设置 VPN target 属性，以确保相应的路由仅被导入到相应的 VPN instance 中。
-

(3) 配置 P

配置接口。

```
[P] interface ethernet1/0/0
```

```
[P-ethernet1/0/0] ip address 192.168.1.2 255.255.255.0
```

```
[P] interface ethernet2/0/1
```

```
[P-ethernet2/0/1] ip address 192.168.2.2 255.255.255.0
```

配置 OSPF 协议。

```
[P] ospf
```

```
[P-ospf-1] area 0
```

```
[P-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
```

```
[P-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
```

```
[P-ospf-1-area-0.0.0.0] quit
```

```
[P-ospf-1] import-route direct
```

7.4.3 Extranet 组网举例

1. 组网需求

公司 A 和公司 B 通过 VPN 互联，两个公司的总部都在城市 C，虚拟内部网号分别为 VPN1 和 VPN2。

通过 MPLS 给用户提提供 VPN 功能，两个 VPN 之间有一部分共享资源在城市 C，两个 VPN 内的用户都可以访问位于城市 C 的资源，但城市 A 和 B 的 VPN 用户不能互相访问。

由于两个公司在 PE-C 上共用一个 VPN-instance，所以两个公司使用的 IP 地址空间不能重叠。

说明：

此案例的配置重点在于：通过对不同 PE 上 VPN-target 属性的设置，控制不同城市 VPN 用户对资源的访问权限。

2. 组网图

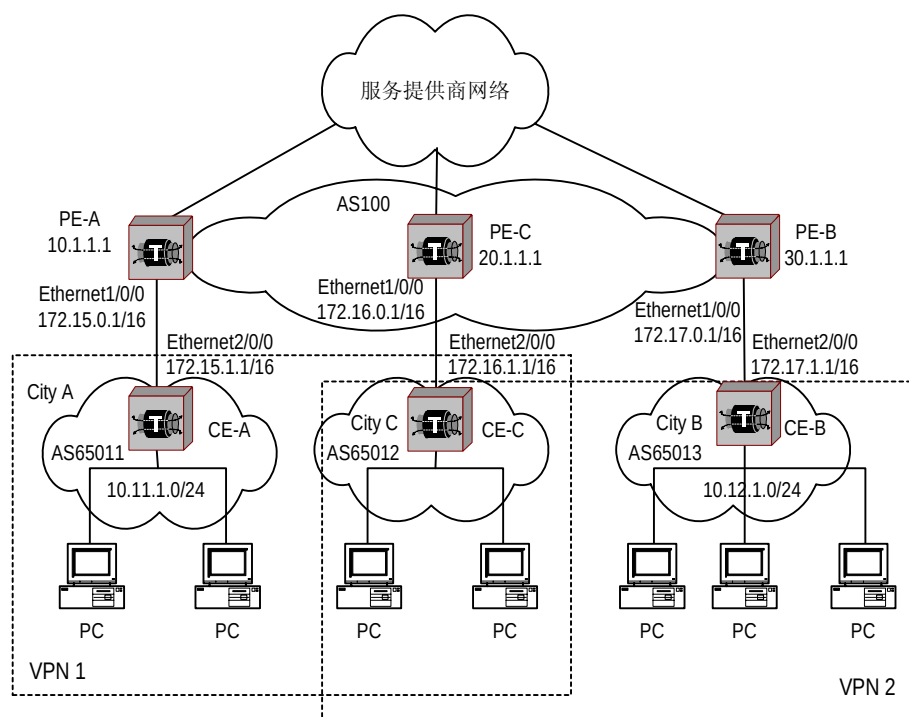


图7-13 Extranet 组网图

3. 配置步骤

说明：

本配置步骤部分省略了 PE 之间的 MPLS 基本能力配置、PE 与 P 间的配置、以及 CE 的配置。这部分的内容可以参考前一个配置举例。

(1) 配置 PE-A

在 PE-A 上创建 VPN1 的 VPN-instance，能够收发 VPN-target 为 111:1 的 VPN 路由信息。

```
[PE-A] ip vpn-instance vpn1
[PE-A-vpn-vpn1] route-distinguisher 100:1
[PE-A-vpn-vpn1] vpn-target 111:1 both
[PE-A-vpn-vpn1] quit
```

PE-A 与 CE-A 间建立 EBGP 邻居，并将学到的 CE-A 内部 VPN 路由引入 MBGP 的 VPN-instance 地址族。

```
[PE-A] bgp 100
[PE-A-bgp] ipv4-family vpn-instance vpn1
[PE-A-bgp-af-vpn-instance] group 172 external
[PE-A-bgp-af-vpn-instance] peer 172.15.1.1 group 172 as-number 65011
[PE-A-bgp-af-vpn-instance] import-route direct
[PE-A-bgp-af-vpn-instance] import-route static
[PE-A-bgp-af-vpn-instance] quit
[PE-A-bgp] quit
```

将与 CE-A 连接的接口 Ethernet1/0/0 与 VPN-instance 绑定。

```
[PE-A] interface ethernet 1/0/0
[PE-A-Ethernet1/0/0] ip binding vpn-instance vpn1
[PE-A-Ethernet1/0/0] ip address 172.15.0.1 255.255.0.0
[PE-A-Ethernet1/0/0] quit
```

配置 LoopBack 接口。

```
[PE-A] interface loopback 0
[PE-A-LoopBack0] ip address 10.1.1.1 255.255.255.255
[PE-A-LoopBack0] quit
```

配置 MPLS 基本能力。

```
[PE-A] mpls lsr-id 10.1.1.1
[PE-A] mpls
[PE-A-mpls] quit
[PE-A] mpls ldp
```

在 PE 与 PE 之间建立 MP-IBGP 邻居，进行 PE 内部的 VPN 路由信息交换。并在 VPNv4 地址族视图下激活 MP-IBGP 对等体。

```
[PE-A] bgp 100
[PE-A-bgp] group 20
[PE-A-bgp] peer 20.1.1.1 group 20
[PE-A-bgp] peer 20.1.1.1 connect-interface loopback 0
[PE-A-bgp] group 30
[PE-A-bgp] peer 30.1.1.1 group 30
[PE-A-bgp] peer 30.1.1.1 connect-interface loopback 0
[PE-A-bgp] ipv4-family vpnv4
[PE-A-bgp-af-vpn] peer 20 enable
[PE-A-bgp-af-vpn] peer 20.1.1.1 group 20
```

```
[PE-A-bgp-af-vpn] peer 30 enable
[PE-A-bgp-af-vpn] peer 30.1.1.1 group 30
[PE-A-bgp-af-vpn] quit
```

(2) 配置 PE-C

在 PE-C 上创建一个 VPN-instance，能够收发 VPN-target 为 111:1 和 222:2 的 VPN 路由信息。

```
[PE-C] ip vpn-instance vpn2
[PE-C-vpn-vpn2] route-distinguisher 100:2
[PE-C-vpn-vpn2] vpn-target 111:1
[PE-C-vpn-vpn2] vpn-target 222:2
[PE-C-vpn-vpn2] quit
```

PE-C 与 CE-C 间建立 EBGp 邻居，并将学到的 CE-C 内部 VPN 路由引入 MBGP 的 VPN-instance 地址族。

```
[PE-C] bgp 100
[PE-C-bgp] ipv4-family vpn-instance vpn2
[PE-C-bgp-af-vpn-instance] group 172 external
[PE-C-bgp-af-vpn-instance] peer 172.16.1.1 group 172 as-number 65012
[PE-C-bgp-af-vpn-instance] import-route direct
[PE-C-bgp-af-vpn-instance] import-route static
[PE-C-bgp-af-vpn-instance] quit
[PE-C-bgp] quit
```

将与 CE-C 相连的接口 Ethernet1/0/0 与 VPN-instance 绑定。

```
[PE-C] interface ethernet 1/0/0
[PE-C-Ethernet1/0/0] ip binding vpn-instance vpn2
[PE-C-Ethernet1/0/0] ip address 172.16.0.1 255.255.0.0
```

配置 LoopBack 接口。

```
[PE-C] interface loopback 0
[PE-C-LoopBack0] ip address 20.1.1.1 255.255.255.255
[PE-C-LoopBack0] quit
```

配置 MPLS 基本能力。

```
[PE-C] mpls lsr-id 20.1.1.1
[PE-C] mpls
[PE-C-mpls] quit
[PE-C] mpls ldp
```

在 PE 与 PE 之间建立 MP-IBGP 邻居，进行 PE 内部的 VPN 路由信息交换。并在 VPNv4 地址族视图下激活 MP-IBGP 对等体。

```
[PE-C] bgp 100
[PE-C-bgp] group 10
[PE-C-bgp] peer 10.1.1.1 group 10
```



```
[PE-C-bgp] peer 10.1.1.1 connect-interface loopback 0
[PE-C-bgp] group 30
[PE-C-bgp] peer 30.1.1.1 group 30
[PE-C-bgp] peer 30.1.1.1 connect-interface loopback 0
[PE-C-bgp] ipv4-family vpnv4
[PE-C-bgp-af-vpn] peer 10 enable
[PE-C-bgp-af-vpn] peer 10.1.1.1 group 10
[PE-C-bgp-af-vpn] peer 30 enable
[PE-C-bgp-af-vpn] peer 30.1.1.1 group 30
[PE-C-bgp-af-vpn] quit
```

(3) 配置 PE-B

在 PE-B 上创建 VPN2 的 VPN-instance, 能够收发 VPN-target 为 222:2 的 VPN 路由信息。

```
[PE-B] ip vpn-instance vpn3
[PE-B-vpn-vpn3] route-distinguisher 100:3
[PE-B-vpn-vpn3] vpn-target 222:2
[PE-B-vpn-vpn3] quit
```

PE-B 与 CE-B 间建立 EBGP 邻居, 并将学到的 CE-B 内部 VPN 路由引入 MBGP 的 VPN-instance 地址族。

```
[PE-B] bgp 100
[PE-B-bgp] ipv4-family vpn-instance vpn3
[PE-B-bgp-af-vpn-instance] group 172 external
[PE-B-bgp-af-vpn-instance] peer 172.17.1.1 group 172 as-number 65013
[PE-B-bgp-af-vpn-instance] import-route direct
[PE-B-bgp-af-vpn-instance] import-route static
[PE-B-bgp-af-vpn-instance] quit
[PE-B-bgp] quit
```

将与 CE-B 相连的接口 Ethernet1/0/0 与 VPN-instance 绑定。

```
[PE-B] interface ethernet 1/0/0
[PE-B-Ethernet1/0/0] ip binding vpn-instance vpn3
[PE-B-Ethernet1/0/0] ip address 172.17.0.1 255.255.0.0
[PE-B-Ethernet1/0/0] quit
```

配置 LoopBack 接口。

```
[PE-B] interface loopback 0
[PE-B-LoopBack0] ip address 30.1.1.1 255.255.255.255
[PE-B-LoopBack0] quit
```

配置 MPLS 基本能力。

```
[PE-B] mpls lsr-id 30.1.1.1
[PE-B] mpls
```

```
[PE-B-mpls] quit
```

```
[PE-B] mpls ldp
```

在 PE 与 PE 之间建立 MP-IBGP 邻居, 进行 PE 内部的 VPN 路由信息交换。并在 VPNv4 地址族视图下激活 MP-IBGP 对等体。

```
[PE-B] bgp 100
```

```
[PE-B-bgp] group 10
```

```
[PE-B-bgp] peer 10.1.1.1 group 10
```

```
[PE-B-bgp] peer 10.1.1.1 connect-interface loopback 0
```

```
[PE-B-bgp] group 20
```

```
[PE-B-bgp] peer 20.1.1.1 group 20
```

```
[PE-B-bgp] peer 20.1.1.1 connect-interface loopback 0
```

```
[PE-B-bgp] ipv4-family vpnv4
```

```
[PE-B-bgp-af-vpn] peer 10 enable
```

```
[PE-B-bgp-af-vpn] peer 10.1.1.1 group 10
```

```
[PE-B-bgp-af-vpn] peer 20 enable
```

```
[PE-B-bgp-af-vpn] peer 20.1.1.1 group 20
```

```
[PE-B-bgp-af-vpn] quit
```

7.4.4 Hub&Spoke 组网举例

1. 组网需求

Hub&Spoke 组网方式也称为中心服务器拓扑组网。中心 Site 称为 Hub-Site, 它知道同一 VPN 所有其它 Site 的路由; 不处于中心的 site 称为 Spoke-Site, 它们的流量通过 HUB-Site 到达目的地。Hub-Site 是 Spoke-Site 的中枢节点。

某银行的网络包括各分公司网络与公司总部的网络, 要求各分公司之间不能直接交换数据, 必须通过总部进行通信, 以进行统一控制。采用 Hub&Spoke 拓扑, CE2 和 CE3 为 Spoke 站点, CE1 为银行数据中心 Hub 站点, CE2 与 CE3 间的通信由 CE1 控制。

- PE1 分别与 PE2、PE3 建立 IBGP 邻居关系, 但 PE2 与 PE3 不建立 IBGP 邻居关系, 不交换 VPN 路由信息;
- 在 PE1 上创建两个 VPN-instance, 引入 VPN-target 属性为 100:1 的 VPN 路由, 对发布的 VPN 路由设置 VPN-target 属性 100:2;
- 在 PE2 上创建一个 VPN-instance, 引入 VPN-target 属性为 100:2 的 VPN 路由, 对发布的 VPN 路由设置 VPN-target 属性 100:1;
- 在 PE3 上创建一个 VPN-instance, 引入 VPN-target 属性为 100:2 的 VPN 路由, 对发布的 VPN 路由设置 VPN-target 属性 100:1。

经过以上配置, PE2 和 PE3 将只能通过 PE1 学到对方的路由。

说明：

此案例的配置重点有两个：

- 通过对不同 PE 上 VPN-target 属性的设置，控制总部与分公司之间的路由发布。
- 允许一次路由环路，使 PE 能够接收 CE 发送的含本 AS 号的路由更新。

2. 组网图

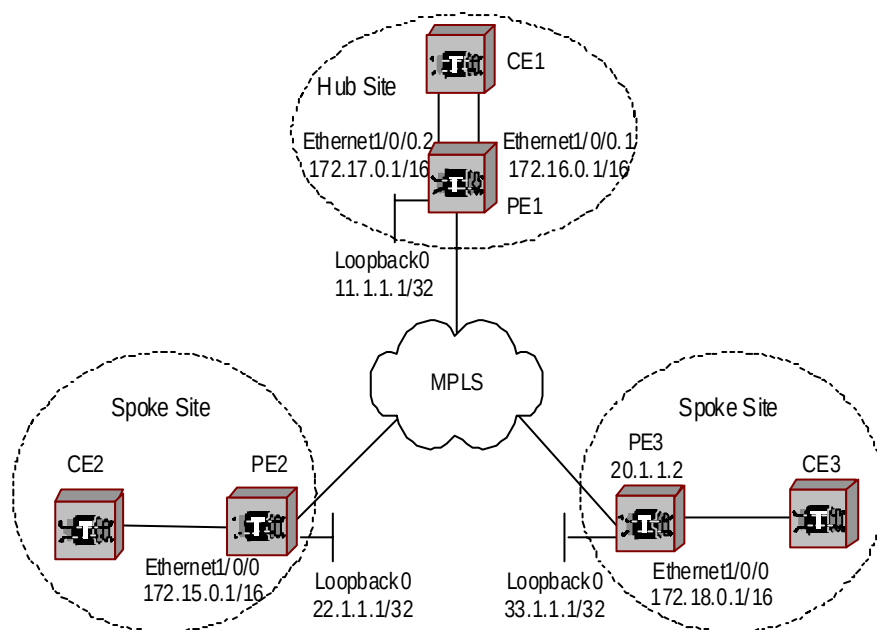


图7-14 Hub&Spoke 组网图

3. 配置步骤

说明：

本配置步骤部分省略了PE之间的MPLS基本能力配置、及CE的配置。这部分的内容可以参考 7.4.1。

(1) 配置 PE1

在 PE1 上配置两个 VPN-instance，对从 PE2 和 PE3 接收的路由加上指定的 VPN-target 属性。

```
[PE1] ip vpn-instance vpn-instance2
[PE1-vpn-vpn-instance2] route-distinguisher 100:2
[PE1-vpn-vpn-instance2] vpn-target 100:1 import-extcommunity
[PE1-vpn-vpn-instance2] quit
[PE1] ip vpn-instance vpn-instance3
[PE1-vpn-vpn-instance3] route-distinguisher 100:3
```

```
[PE1-vpn-vpn-instance3] vpn-target 100:2 export-extcommunity
[PE1-vpn-vpn-instance3] quit
```

PE1 与 CE1 间建立 EBGP 邻居，将学到的 CE1 内部 VPN 路由引入 MBGP 的 VPN-instance 地址族，并允许一次路由环路。

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpn-instance2
[PE1-bgp-af-vpn-instance] group 17216 external
[PE1-bgp-af-vpn-instance] peer 172.16.1.1 group 17216 as-number 65002
[PE1-bgp-af-vpn-instance] peer 172.16.1.1 allow-as-loop 1
[PE1-bgp-af-vpn-instance] import-route static
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] ipv4-family vpn-instance vpn-instance3
[PE1-bgp-af-vpn-instance] group 17217 external
[PE1-bgp-af-vpn-instance] peer 172.17.1.1 group 17217 as-number 65002
[PE1-bgp-af-vpn-instance] peer 172.17.1.1 allow-as-loop 1
[PE1-bgp-af-vpn-instance] import-route static
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] quit
```

将 PE1 与 CE1 相连的接口绑定到不同的 VPN-instance。以太网子接口 Ethernet1/0/0.1 绑定到 vpn-instance2，以太网子接口 Ethernet1/0/0.2 绑定到 vpn-instance3。

```
[PE1] interface ethernet 1/0/0.1
[PE1-Ethernet1/0/0.1] ip binding vpn-instance vpn-instance2
[PE1-Ethernet1/0/0.1] ip address 172.16.0.1 255.255.0.0
[PE1-Ethernet1/0/0.1] quit
[PE1] interface ethernet 1/0/0.2
[PE1-Ethernet1/0/0.2] ip binding vpn-instance vpn-instance3
[PE1-Ethernet1/0/0.2] ip address 172.17.0.1 255.255.0.0
[PE1-Ethernet1/0/0.2] quit
```

配置 LoopBack 接口。

```
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 11.1.1.1 255.255.255.255
[PE1-LoopBack0] quit
```

在 PE 与 PE 之间建立 MP-IBGP 邻居，进行 PE 内部的 VPN 路由信息交换。并在 VPNv4 地址族视图下激活 MP-IBGP 对等体。

```
[PE1] bgp 100
[PE1-bgp] group 22
[PE1-bgp] peer 22.1.1.1 group 22
```

```
[PE1-bgp] peer 22.1.1.1 connect-interface loopback 0
[PE1-bgp] group 33
[PE1-bgp] peer 33.1.1.1 group 33
[PE1-bgp] peer 33.1.1.1 connect-interface loopback 0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer 22 enable
[PE1-bgp-af-vpn] peer 22.1.1.1 group 22
[PE1-bgp-af-vpn] peer 33 enable
[PE1-bgp-af-vpn] peer 33.1.1.1 group 33
[PE1-bgp-af-vpn] quit
```

(2) 配置 PE2

在 PE2 上创建 VPN-instance，允许引入 VPN-target 属性为 100:2 的 VPN 路由，发布的 VPN 路由的 VPN-target 属性为 100:1。

```
[PE2] ip vpn-instance vpn-instance1
[PE2-vpn-vpn-instance1] route-distinguisher 100:1
[PE2-vpn-vpn-instance1] vpn-target 100:1 export-extcommunity
[PE2-vpn-vpn-instance1] vpn-target 100:2 import-extcommunity
[PE2-vpn-vpn-instance1] quit
```

PE2 与 CE2 间建立 EBGP 邻居，将学到的 CE2 内部 VPN 路由引入 MBGP 的 VPN-instance 地址族。

```
[PE2] bgp 100
[PE2-bgp] ipv4-family vpn-instance vpn-instance1
[PE2-bgp-af-vpn-instance] group 172 external
[PE2-bgp-af-vpn-instance] peer 172.15.1.1 group 172 as-number 65001
[PE2-bgp-af-vpn-instance] import-route static
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] quit
[PE2-bgp] quit
```

将 PE2 与 CE2 相连的接口绑定到 VPN-instance。

```
[PE2] interface ethernet 1/0/0
[PE2-Ethernet1/0/0] ip binding vpn-instance vpn-instance1
[PE2-Ethernet1/0/0] ip address 172.15.0.1 255.255.0.0
[PE2-Ethernet1/0/0] quit
```

配置 LoopBack 接口。

```
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 22.1.1.1 255.255.255.255
[PE2-LoopBack0] quit
```

在 PE2 与 PE1 之间建立 MP-IBGP 邻居，进行 PE 内部的 VPN 路由信息交换。并在 VPNv4 地址族视图下激活 MP-IBGP 对等体。

```
[PE2] bgp 100
[PE2] group 11
[PE2-bgp] peer 11.1.1.1 group 11
[PE2-bgp] peer 11.1.1.1 connect-interface loopback 0
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpn] peer 11 enable
[PE2-bgp-af-vpn] peer 11.1.1.1 group 11
[PE2-bgp-af-vpn] quit
[PE2-bgp] quit
```

(3) 配置 PE3

在 PE3 上创建 VPN-instance，允许引入 VPN-target 属性为 100:2 的 VPN 路由，发布的 VPN 路由的 VPN-target 属性为 100:1。

```
[PE3] ip vpn-instance vpn-instance2
[PE3-vpn-vpn-instance2] route-distinguisher 100:1
[PE3-vpn-vpn-instance2] vpn-target 100:1 export-extcommunity
[PE3-vpn-vpn-instance2] vpn-target 100:2 import-extcommunity
[PE3-vpn-vpn-instance2] quit
```

PE3 与 CE3 间建立 EBGP 邻居，将学到的 CE3 内部 VPN 路由引入 MBGP 的 VPN-instance 地址族。

```
[PE3] bgp 100
[PE3-bgp] ipv4-family vpn-instance vpn-instance1
[PE3-bgp-af-vpn-instance] group 172 external
[PE3-bgp-af-vpn-instance] peer 172.18.1.1 group 172 as-number 65001
[PE3-bgp-af-vpn-instance] import-route static
[PE3-bgp-af-vpn-instance] import-route direct
[PE3-bgp-af-vpn-instance] quit
[PE3-bgp] quit
```

将 PE3 与 CE3 相连的接口绑定到 VPN-instance。

```
[PE3] interface ethernet 1/0/0
[PE3-Ethernet1/0/0] ip binding vpn-instance vpn-instance2
[PE3-Ethernet1/0/0] ip address 172.18.0.1 255.255.0.0
[PE3-Ethernet1/0/0] quit
```

配置 LoopBack 接口。

```
[PE3] interface loopback 0
[PE3-LoopBack0] ip address 33.1.1.1 255.255.255.255
[PE3-LoopBack0] quit
```

在 PE3 与 PE1 之间建立 MP-IBGP 邻居，进行 PE 内部的 VPN 路由信息交换。并在 VPNv4 地址族视图下激活 MP-IBGP 对等体。

```
[PE3] bgp 100
```

```

[PE3-bgp] group 11
[PE3-bgp] peer 11.1.1.1 group 11
[PE3-bgp] peer 11.1.1.1 connect-interface loopback 0
[PE3-bgp] ipv4-family vpnv4
[PE3-bgp-af-vpn] peer 11 enable
[PE3-bgp-af-vpn] peer 11.1.1.1 group 11
[PE3-bgp-af-vpn] quit
[PE3-bgp] quit

```

7.4.5 CE 双归属组网举例

1. 组网需求

在对网络健壮性要求较高的应用中，可以采用 CE 双归属方式组网。

在下面的组网图中，CE1 和 CE2 分别与 PE1 和 PE2 设备相连，实现双归属；三个 PE 设备也两两相连，组成备份链路。CE3 和 CE4 不使用双归属，只与一个 PE 设备相连。

CE1 与 CE3 属于同一个 VPN；CE2 与 CE4 属于同一个 VPN。不同的 VPN 之间不能互通。

2. 组网图

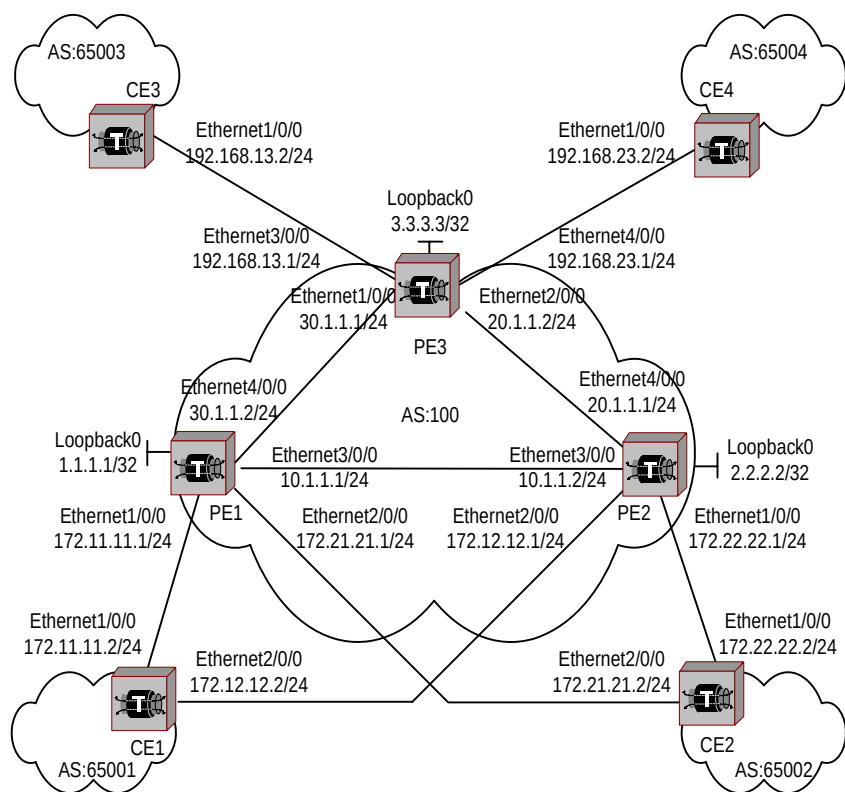


图7-15 CE 双归属组网图

3. 配置步骤

说明:

本配置步骤省略了 CE 的配置，CE 的配置可参考 7.4.1。

(1) 配置 PE1

在 PE1 上为 CE1 和 CE2 分别创建 VPN-instance1.1 和 1.2，并配置不同的 VPN-target 属性。

```
[PE1] ip vpn-instance vpn-instance1.1
[PE1-vpn-vpn-instance1.1] route-distinguisher 1.1.1.1:1
[PE1-vpn-vpn-instance1.1e] vpn-target 1.1.1.1:1
[PE1-vpn-vpn-instance1.1] vpn-target 2.2.2.2:1 import-extcommunity
[PE1-vpn-vpn-instance1.1] vpn-target 3.3.3.3:1 import-extcommunity
[PE1-vpn-vpn-instance1.1] quit
[PE1] ip vpn-instance vpn-instance1.2
[PE1-vpn-vpn-instance1.2] route-distinguisher 1.1.1.1:2
[PE1-vpn-vpn-instance1.2] vpn-target 1.1.1.1:2
[PE1-vpn-vpn-instance1.2] vpn-target 2.2.2.2:2 import-extcommunity
[PE1-vpn-vpn-instance1.2] vpn-target 3.3.3.3:2 import-extcommunity
[PE1-vpn-vpn-instance1.2] quit
```

在 PE1 与 CE1 间建立 EBGp 邻居，将 CE1 内部 VPN 路由引入 VPN-instance1.1。

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpn-instance1.1
[PE1-bgp-af-vpn-instance] group 17211 external
[PE1-bgp-af-vpn-instance] peer 172.11.11.2 group 17211 as-number 65001
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] import-route static
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] quit
```

在 PE1 与 CE2 间建立 EBGp 邻居，将 CE2 内部 VPN 路由引入 VPN-instance1.2。

```
[PE1-bgp] ipv4-family vpn-instance vpn-instance1.2
[PE1-bgp-af-vpn-instance] group 17221 external
[PE1-bgp-af-vpn-instance] peer 172.21.21.2 group 17221 as-number 65002
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] import-route static
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] quit
```

将 PE1 与 CE1 相连的接口绑定到 VPN-instance1.1；将 PE1 与 CE2 相连的接口绑定到 VPN-instance1.2


```
[PE1] interface ethernet 1/0/0
[PE1-Ethernet1/0/0] ip binding vpn-instance vpn-instance1.1
[PE1-Ethernet1/0/0] ip address 172.11.11.1 255.255.255.0
[PE1-Ethernet1/0/0] quit
[PE1] interface ethernet 2/0/0
[PE1-Ethernet2/0/0] ip binding vpn-instance vpn-instance1.2
[PE1-Ethernet2/0/0] ip address 172.21.21.1 255.255.255.0
[PE1-Ethernet2/0/0] quit
```

配置 LoopBack 接口。

```
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.1 255.255.255.255
[PE1-LoopBack0] quit
```

配置 MPLS 基本能力，并在 PE1 与 PE2、PE3 相连的接口上使能 LDP。

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls
[PE1-mpls] mpls ldp
[PE1-mpls] quit
[PE1] interface Ethernet 3/0/0
[PE1-Ethernet3/0/0] mpls
[PE1-Ethernet3/0/0] mpls ldp enable
[PE1-Ethernet3/0/0] ip address 10.1.1.1 255.255.255.0
[PE1-Ethernet3/0/0] interface Ethernet 4/0/0
[PE1-Ethernet4/0/0] mpls
[PE1-Ethernet4/0/0] mpls ldp enable
[PE1-Ethernet4/0/0] ip address 30.1.1.2 255.255.255.0
[PE1-Ethernet4/0/0] quit
```

在 PE1 与 P2、PE3 相连的接口及环回接口上启用 OSPF，实现 PE 内部的互通。

```
[PE1] router id 1.1.1.1
[PE1] ospf
[PE1-ospf] area 0
[PE1-ospf-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-area-0.0.0.0] network 30.1.1.2 0.0.0.255
[PE1-ospf-area-0.0.0.0] network 10.1.1.1 0.0.0.255
[PE1-ospf-area-0.0.0.0] quit
[PE1-ospf] quit
```

在 PE 与 PE 之间建立 MP-IBGP 邻居，进行 PE 内部的 VPN 路由信息交换。并在 VPNv4 地址族视图下激活 MP-IBGP 对等体。

```
[PE1] bgp 100
[PE1-bgp] group 2
[PE1-bgp] peer 2.2.2.2 group 2
```

```
[PE1-bgp] peer 2.2.2.2 connect-interface loopback 0
[PE1-bgp] group 3
[PE1-bgp] peer 3.3.3.3 group 3
[PE1-bgp] peer 3.3.3.3 connect-interface loopback 0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer 2 enable
[PE1-bgp-af-vpn] peer 2.2.2.2 group 2
[PE1-bgp-af-vpn] peer 3 enable
[PE1-bgp-af-vpn] peer 3.3.3.3 group 3
[PE1-bgp-af-vpn] quit
```

(2) 配置 PE2

说明:

PE2 与 PE1 的配置基本相同，以下仅对 VPN-instance 的配置进行说明，其它配置不再赘述。

在 PE2 上为 CE1 和 CE2 分别创建 VPN-instance2.1 和 2.2，并配置不同的 VPN-target 属性。

```
[PE2] ip vpn-instance vpn-instance2.1
[PE2-vpn-vpn-instance2.1] route-distinguisher 2.2.2.2:1
[PE2-vpn-vpn-instance2.1] vpn-target 2.2.2.2:1
[PE2-vpn-vpn-instance2.1] vpn-target 1.1.1.1:1 import-extcommunity
[PE2-vpn-vpn-instance2.1] vpn-target 3.3.3.3:1 import-extcommunity
[PE2-vpn-vpn-instance2.1] quit
[PE2] ip vpn-instance vpn-instance2.2
[PE2-vpn-vpn-instance2.2] route-distinguisher 2.2.2.2:2
[PE2-vpn-vpn-instance2.2] vpn-target 2.2.2.2:2
[PE2-vpn-vpn-instance2.2] vpn-target 1.1.1.1:2 import-extcommunity
[PE2-vpn-vpn-instance2.2] vpn-target 3.3.3.3:2 import-extcommunity
[PE2-vpn-vpn-instance2.2] quit
```

在 PE2 与 CE1 间建立 EBGP 邻居，将 CE1 内部 VPN 路由引入 VPN-instance2.1。

```
[PE2] bgp 100
[PE2-bgp] ipv4-family vpn-instance vpn-instance2.1
[PE2-bgp-af-vpn-instance] group 17212 external
[PE2-bgp-af-vpn-instance] peer 172.12.12.2 group 17212 as-number 65001
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] import-route static
[PE2-bgp-af-vpn-instance] quit
```

在 PE2 与 CE2 间建立 EBGP 邻居，将 CE2 内部 VPN 路由引入 VPN-instance2.2。

```
[PE2-bgp] ipv4-family vpn-instance vpn-instance2.2
```

```
[PE2-bgp-af-vpn-instance] group 17222 external
[PE2-bgp-af-vpn-instance] peer 172.22.22.2 group 17222 as-number 65002
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] import-route static
[PE2-bgp-af-vpn-instance] quit
[PE2-bgp] quit
```

将 PE2 与 CE1 相连的接口绑定到 VPN-instance2.1; 将 PE2 与 CE2 相连的接口绑定到 VPN-instance2.2

```
[PE2] interface ethernet 2/0/0
[PE2-Ethernet2/0/0] ip binding vpn-instance vpn-instance2.1
[PE2-Ethernet2/0/0] ip address 172.12.12.1 255.255.255.0
[PE2-Ethernet2/0/0] quit
[PE2] interface ethernet 1/0/0
[PE2-Ethernet1/0/0] ip binding vpn-instance vpn-instance2.2
[PE2-Ethernet1/0/0] ip address 172.22.22.1 255.255.255.0
[PE2-Ethernet1/0/0] quit
```

(3) 配置 PE3

说明:

以下仅对 PE3 的 VPN-instance 配置进行说明, 其它配置与 PE1 和 PE2 类似, 不再赘述。

在 PE3 上为 CE3 和 CE4 分别创建 VPN-instance3.1 和 3.2, 并配置不同的 VPN-target 属性。

```
[PE3] ip vpn-instance vpn-instance3.1
[PE3-vpn-vpn-instance3.1] route-distinguisher 3.3.3.3:1
[PE3-vpn-vpn-instance3.1] vpn-target 3.3.3.3:1
[PE3-vpn-vpn-instance3.1] vpn-target 1.1.1.1:1 import-extcommunity
[PE3-vpn-vpn-instance3.1] vpn-target 2.2.2.2:1 import-extcommunity
[PE3-vpn-vpn-instance3.1] quit
[PE3] ip vpn-instance vpn-instance3.2
[PE3-vpn-vpn-instance3.2] route-distinguisher 3.3.3.3:2
[PE3-vpn-vpn-instance3.2] vpn-target 3.3.3.3:2
[PE3-vpn-vpn-instance3.2] vpn-target 1.1.1.1:2 import-extcommunity
[PE3-vpn-vpn-instance3.2] vpn-target 2.2.2.2:2 import-extcommunity
[PE3-vpn-vpn-instance3.2] quit
```

在 PE3 与 CE3 间建立 EBGp 邻居, 将 CE3 内部 VPN 路由引入 VPN-instance3.1。

```
[PE3] bgp 100
[PE3-bgp] ipv4-family vpn-instance vpn-instance3.1
[PE3-bgp-af-vpn-instance] group 192 external
```

```
[PE3-bgp-af-vpn-instance] peer 192.168.13.2 group 192 as-number 65003
[PE3-bgp-af-vpn-instance] import-route direct
[PE3-bgp-af-vpn-instance] import-route static
[PE3-bgp-af-vpn-instance] quit
[PE3-bgp] quit
```

在 PE3 与 CE4 间建立 EBGP 邻居, 将 CE4 内部 VPN 路由引入 VPN-instance3.2。

```
[PE3-bgp] ipv4-family vpn-instance vpn-instance3.2
[PE3-bgp-af-vpn-instance] group 232 external
[PE3-bgp-af-vpn-instance] peer 192.168.23.2 group 232 as-number 65004
[PE3-bgp-af-vpn-instance] import-route direct
[PE3-bgp-af-vpn-instance] import-route static
[PE3-bgp-af-vpn-instance] quit
[PE3-bgp] quit
```

将 PE3 与 CE3 相连的接口绑定到 VPN-instance3.1; 将 PE3 与 CE2 相连的接口绑定到 VPN-instance3.2

```
[PE3] interface ethernet 3/0/0
[PE3-Ethernet3/0/0] ip binding vpn-instance vpn-instance3.1
[PE3-Ethernet3/0/0] ip address 192.168.13.1 255.255.255.0
[PE3-Ethernet3/0/0] quit
[PE3] interface ethernet 4/0/0
[PE3-Ethernet4/0/0] ip binding vpn-instance vpn-instance3.2
[PE3-Ethernet4/0/0] ip address 192.168.23.1 255.255.255.0
[PE3-Ethernet4/0/0] quit
```

7.4.6 多角色主机组网举例

1. 组网需求

如下图所示, 某公司通过 BGP/MPLS VPN 来提供 VPN 服务。

PE1 与 CE1 相连的 Ethernet0/0/0 接口绑定到 VPN1, PE2 与 CE2 相连的接口 Ethernet0/0/0 绑定到 VPN2。

主机 PC1 通过 CE1 接入, PC1 的 IP 地址为 100.1.1.2, 配置完成后, 它将可以访问 VPN1 和 VPN2。

说明:

此案例的配置要点在于:

通过配置静态路由和路由策略, 使 PC1 访问不同 VPN 的报文在不同的 VPN-instance 中查找路由。

2. 组网图

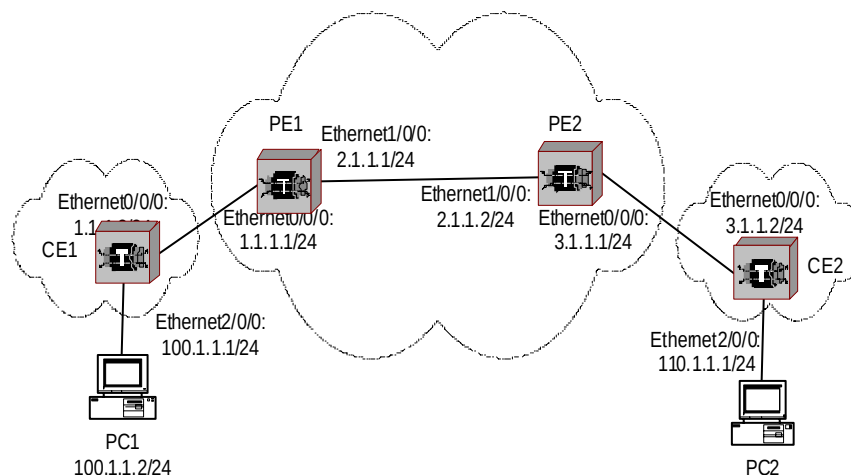


图7-16 多角色主机组网图

3. 配置步骤

(1) 配置 CE1

在 CE1 上配置一条指向 PE1 的缺省路由。

```
[CE1] ip route-static 0.0.0.0 0 1.1.1.1
```

(2) 配置 PE1

在 PE1 上为 VPN1 和 VPN2 分别创建 VPN-instance，并配置不同的 VPN-target 属性。

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-vpn1] route-distinguisher 100:1
[PE1-vpn-vpn1] vpn-target 100:1 both
[PE1-vpn-vpn1] quit
[PE1] ip vpn-instance vpn2
[PE1-vpn-vpn2] route-distinguisher 100:2
[PE1-vpn-vpn2] vpn-target 100:2 both
[PE1-vpn-vpn2] quit
```

将 PE1 与 CE1 相连的接口绑定到 VPN1。

```
[PE1] interface ethernet0/0/0
[PE1-Ethernet0/0/0] ip binding vpn-instance vpn1
[PE1-Ethernet0/0/0] ip address 1.1.1.1 255.255.255.0
[PE1-Ethernet0/0/0] quit
```

配置静态路由，使 PC1 访问 VPN2 的返回报文能够在 PE1 的 VPN-instance vpn1 中找到正确的路由，回到 PC1（相应的还需要在 PE2 配置 MBGP 引入静态路由，以便通过 MBGP 将这条路由发布给整个 VPN2）。

```
[PE1] ip route-static vpn-instance vpn2 100.1.0.0 16 vpn-instance vpn1 2.1.1.2
```

配置策略路由, 对于 PC1 发出的报文, 可以同时在 vpn1 和 vpn2 中查找私网路由并转发。

```
[PE1] acl number 101
[PE1-acl-adv-101] rule 0 permit ip vpn-instance vpn1 source 100.1.1.2 0
[PE1-acl-adv-101] quit
[PE1] route-policy aaa permit node 10
[PE1-route-policy] if-match acl 101
[PE1-route-policy] apply access-vpn vpn-instance vpn1 vpn2
[PE1-route-policy] quit
```

在接口 Ethernet0/0/0 上应用定义的策略路由。

```
[PE1] interface ethernet0/0/0
[PE1-Ethernet0/0/0] ip policy route-policy aaa
```

其他配置请参考前面的例子。

7.4.7 OSPF 多实例 sham link 配置举例

1. 组网需求

如下图所示, 一个公司通过 SecPath 系列安全网关的 OSPF 多实例功能连接到广域网, 其中 OSPF 绑定于 VPN1。PE 之间是 MPLS VPN 骨干网, PE 和 CE 之间运行 OSPF。在 PE1 和 PE2 之间配置一条 sham link, 使得 CE1 和 CE2 之间的流量不会通过 CE1 和 CE2 之间直接相连的链路(backdoor link)。

2. 组网图

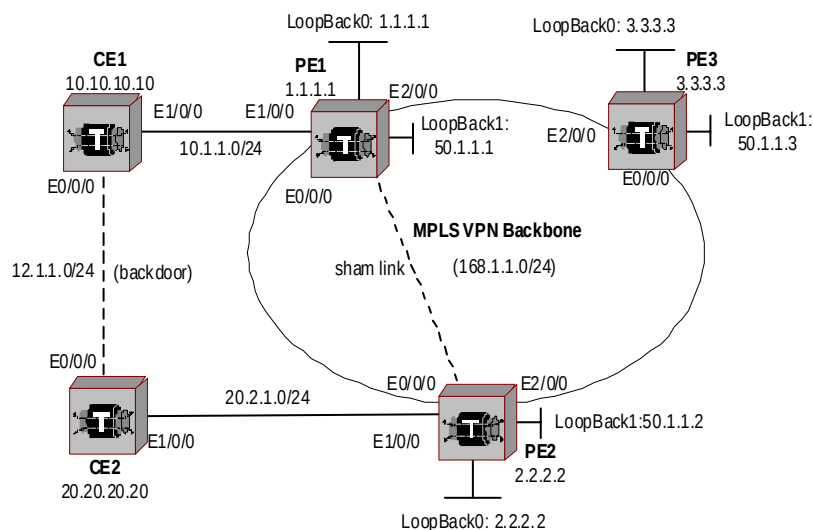


图7-17 OSPF 多实例配置案例组网图

3. 配置步骤

(1) 配置 PE1

使能 MPLS 及 LDP。

```
[PE1] mpls lsr-id 50.1.1.2
```

```
[PE1] mpls
```

```
[PE1-mpls] mpls ldp
```

配置 vpn-instance。

```
[PE1] ip vpn-instance VPN1
```

```
[PE1-vpn-VPN1] route-distinguisher 2:1
```

```
[PE1-vpn-VPN1] vpn-target 100:1 export-extcommunity
```

```
[PE1-vpn-VPN1] vpn-target 100:1 import-extcommunity
```

配置接口。

```
[PE1] interface Ethernet0/0/0
```

```
[PE1-Ethernet0/0/0] ip address 168.1.12.1 255.255.255.0
```

```
[PE1-Ethernet0/0/0] ospf cost 1
```

```
[PE1-Ethernet0/0/0] mpls
```

```
[PE1-Ethernet0/0/0] mpls ldp enable
```

```
[PE1-Ethernet0/0/0] mpls ldp transport-ip interface
```

```
[PE1] interface Ethernet1/0/0
```

```
[PE1-Ethernet1/0/0] ip binding vpn-instance VPN1
```

```
[PE1-Ethernet1/0/0] ip address 10.1.1.2 255.255.255.0
```

```
[PE1-Ethernet1/0/0] ospf cost 1
```

```
[PE1] interface Ethernet2/0/0
```

```
[PE1-Ethernet2/0/0] ip address 168.1.13.1 255.255.255.0
```

```
[PE1-Ethernet2/0/0] ospf cost 1
```

```
[PE1-Ethernet2/0/0] mpls
```

```
[PE1-Ethernet2/0/0] mpls ldp enable
```

```
[PE1-Ethernet2/0/0] mpls ldp transport-ip interface
```

```
[PE1] interface loopback0
```

```
[PE1-LoopBack0] ip binding vpn-instance VPN1
```

```
[PE1-LoopBack0] ip address 1.1.1.1 255.255.255.255
```

```
[PE1] interface loopback1
```

```
[PE1-LoopBack1] ip address 50.1.1.1 255.255.255.255
```

配置 BGP peer。

```
[PE1] bgp 100
```

```
[PE1-bgp] undo synchronization
```

```
[PE1-bgp] group fc internal
```

```
[PE1-bgp] peer 2.2.2.2 group fc
```

```
[PE1-bgp] peer 2.2.2.2 connect-interface LoopBack1
```

```
[PE1-bgp] peer 3.3.3.3 group fc
```

```
[PE1-bgp] peer 3.3.3.3 connect-interface LoopBack1
```

配置 BGP 引入 OSPF 路由及直连路由。

```
[PE1-bgp] ipv4-family vpn-instance vpn1
[PE1-bgp-af-vpn-instance] import-route ospf 100
[PE1-bgp-af-vpn-instance] import-route ospf-ase 100
[PE1-bgp-af-vpn-instance] import-route ospf-nssa 100
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] undo synchronization
```

在 MBGP 下建立 peer 并激活。

```
[PE1-bgp-af-vpn] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer fc enable
[PE1-bgp-af-vpn] peer fc advertise-community
[PE1-bgp-af-vpn] peer 2.2.2.2 group fc
[PE1-bgp-af-vpn] peer 3.3.3.3 group fc
```

绑定 OSPF 进程到 vpn-instance。

```
[PE1] ospf 100 router-id 1.1.1.1 vpn-instance VPN1
[PE1-ospf-100] import-route bgp
[PE1-ospf-100] area 0.0.0.1
[PE1-ospf-100-area-0.0.0.1] network 10.1.1.0 0.0.0.255
```

配置 sham link。

```
[PE1-ospf-100-area-0.0.0.1] sham-link 1.1.1.1 2.2.2.2
```

配置到 PE2、PE3 的静态路由。

```
[PE1] ip route-static 50.1.1.2 255.255.255.255 168.1.12.2
[PE1] ip route-static 50.1.1.3 255.255.255.255 168.1.13.3
```

(2) 配置 PE2

使能 MPLS 及 LDP。

```
[PE2] mpls lsr-id 50.0.0.1
[PE2] mpls
[PE2- mpls] mpls ldp
```

配置 vpn-instance VPN1。

```
[PE2] ip vpn-instance VPN1
[PE2-vpn-VPN1] route-distinguisher 2:1
[PE2-vpn-VPN1] vpn-target 100:1 export-extcommunity
[PE2-vpn-VPN1] vpn-target 100:1 import-extcommunity
```

配置接口。

```
[PE2] interface Ethernet0/0/0
[PE2-Ethernet0/0/0] ip address 168.1.12.2 255.255.255.0
[PE2-Ethernet0/0/0] ospf cost 1
```



```
[PE2-Ethernet0/0/0] mpls
[PE2-Ethernet0/0/0] mpls ldp enable
[PE2-Ethernet0/0/0] mpls ldp transport-ip interface
[PE2] interface Ethernet1/0/0
[PE2-Ethernet1/0/0] ip binding vpn-instance VPN1
[PE2-Ethernet1/0/0] ip address 20.1.1.2 255.255.255.0
[PE2-Ethernet1/0/0] ospf cost 1
[PE2] interface Ethernet2/0/0
[PE2-Ethernet2/0/0] ip address 168.1.23.2 255.255.255.0
[PE2-Ethernet2/0/0] ospf cost 1
[PE2-Ethernet1/0/0] mpls
[PE2-Ethernet1/0/0] mpls ldp enable
[PE2-Ethernet1/0/0] mpls ldp transport-ip interface
[PE2] interface LoopBack0
[PE2- LoopBack0] ip binding vpn-instance VPN1
[PE2- LoopBack0] ip address 2.2.2.2 255.255.255.255
[PE2] interface LoopBack1
[PE2- LoopBack1] ip address 50.1.1.2 255.255.255.255
```

配置 BGP。

```
[PE2] bgp 100
[PE2-bgp-100] undo synchronization
[PE2-bgp-100] group fc internal
[PE2-bgp-100] peer 50.1.1.1 group fc
[PE2-bgp-100] peer 50.1.1.1 connect-interface LoopBack10
[PE2-bgp-100] peer 50.1.1.3 group fc
[PE2-bgp-100] peer 50.1.1.3 connect-interface LoopBack10
```

配置 vpn-instance 引入 OSPF 及直连路由。

```
[PE2-bgp] ipv4-family vpn-instance VPN1
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] import-route ospf-nssa 100
[PE2-bgp-af-vpn-instance] import-route ospf-ase 100
[PE2-bgp-af-vpn-instance] import-route ospf 100
[PE2-bgp-af-vpn-instance] undo synchronization
```

配置 MBGP 使能 peer。

```
[PE2-bgp-af-vpn] ipv4-family vpnv4
[PE2-bgp-af-vpn] peer fc enable
[PE2-bgp-af-vpn] peer fc advertise-community
[PE2-bgp-af-vpn] peer 50.1.1.1 group fc
[PE2-bgp-af-vpn] peer 50.1.1.3 group fc
```

配置 OSPF 引入 BGP 及直连路由。

```
[PE2] ospf 100 router-id 2.2.2.2 vpn-instance VPN1
[PE2-ospf-100] import-route bgp
[PE2-ospf-100] import-route static
[PE2-ospf-100] area 0.0.0.1
[PE2-ospf-100-0.0.0.1] network 20.1.1.0 0.0.0.255
```

配置 sham link。

```
[PE2-ospf-100-0.0.0.1] sham-link 2.2.2.2 1.1.1.1
```

配置到 PE1、PE3 的静态路由。

```
[PE2] ip route-static 50.1.1.1 255.255.255.255 168.1.12.1
[PE2] ip route-static 50.1.1.3 255.255.255.255 168.1.23.3
```

(3) 配置 CE1

配置接口。

```
[CE1] interface Ethernet0/0/0
[CE1-Ethernet0/0/0] ip address 12.1.1.1 255.255.255.0
[CE1-Ethernet0/0/0] ospf cost 1
[CE1] interface Ethernet1/0/0
[CE1-Ethernet1/0/0] ip address 10.1.1.1 255.255.255.0
[CE1-Ethernet1/0/0] ospf cost 1
```

配置 OSPF。

```
[CE1] ospf 100 router-id 10.10.10.129
[CE1-ospf-100] import-route direct
[CE1-ospf-100] area 0.0.0.1
[CE1-ospf-100] network 10.1.1.0 0.0.0.255
[CE1-ospf-100] network 12.1.1.0 0.0.0.255
```

(4) 配置 CE2

配置接口。

```
[CE2] interface Ethernet0/0/0
[CE2-Ethernet0/0/0] ip address 12.1.1.2 255.255.255.0
[CE2-Ethernet0/0/0] ospf cost 1
[CE2] interface Ethernet1/0/0
[CE2-Ethernet1/0/0] ip address 20.1.1.1 255.255.255.0
[CE2-Ethernet1/0/0] ospf cost 1
```

配置 OSPF。

```
[CE2] ospf 100 router-id 20.20.20.20
[CE2-ospf-100] area 0.0.0.1
[CE2-ospf-100] network 12.1.1.0 0.0.0.255
[CE2-ospf-100] network 20.1.1.0 0.0.0.255
```

7.4.8 OSPF 多实例 CE 配置举例

1. 组网需求

在一个 VPN 内部的 CE 通过配置多个 vpn-instance 实现业务隔离。

2. 组网图

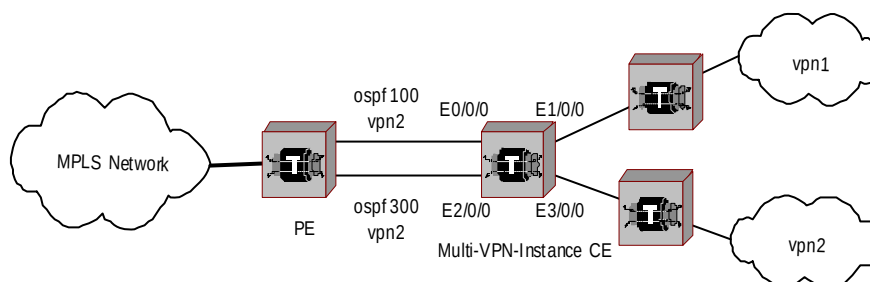


图7-18 OSPF 多实例 CE 配置举例

3. 配置步骤

配置 CE

配置实例 CE-VPN1

```
[CE] ip vpn-instance CE-VPN1
[CE-vpn-CE-VPN1] route-distinguisher 100:1
[CE-vpn-CE-VPN1] vpn-target 100:1 export-extcommunity
[CE-vpn-CE-VPN1] vpn-target 100:1 import-extcommunity
```

配置实例 CE-VPN2

```
[CE] ip vpn-instance CE-VPN2
[CE-vpn-CE-VPN2] route-distinguisher 200:1
[CE-vpn-CE-VPN2] vpn-target 200:1 export-extcommunity
[CE-vpn-CE-VPN2] vpn-target 200:1 import-extcommunity
```

配置 ethernet0/0/0

```
[CE] interface Ethernet0/0/0
[CE-Ethernet 0/0/0] ip binding vpn-instance CE-VPN1
[CE-Ethernet 0/0/0] ip address 10.1.1.2 255.255.255.0
```

配置 ethernet1/0/0

```
[CE] interface Ethernet1/0/0
[CE-Ethernet1/0/0] ip binding vpn-instance CE-VPN1
[CE-Ethernet1/0/0] ip address 10.2.1.2 255.255.255.0
[CE-Ethernet1/0/0] ospf cost 100
```

配置 ethernet2/0/0

```
[CE] interface Ethernet2/0/0
```

```
[CE-Ethernet2/0/0] ip binding vpn-instance CE-VPN2
[CE-Ethernet2/0/0] ip address 20.1.1.2 255.255.255.0

# 配置 ethernet3/0/0

[CE] interface Ethernet3/0/0
[CE-Ethernet3/0/0] ip binding vpn-instance CE-VPN2
[CE-Ethernet3/0/0] ip address 20.2.1.2 255.255.255.0

# 配置 ospf 100

[CE] ospf 100 vpn-instance CE-VPN1
[CE-ospf-100] vpn-instance-capability simple
[CE-ospf-100] area 0.0.0.0
[CE-ospf-100-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[CE-ospf-100-area-0.0.0.0] network 10.2.1.0 0.0.0.255

# 配置 ospf 200

[CE] ospf 200 vpn-instance CE-VPN2
[CE-ospf-200] vpn-instance-capability simple
[CE-ospf-200] area 0.0.0.1
[CE-ospf-100-area-0.0.0.1] network 20.1.1.0 0.0.0.255
[CE-ospf-100-area-0.0.0.1] network 20.2.1.0 0.0.0.255
```

7.4.9 跨域 VPN 组网举例-OptionA

1. 组网需求

CE1 和 CE2 属于同一个 VPN。CE1 通过 AS100 的 PE1 接入, CE2 通过 AS200 的 PE2 接入。

采用 OptionA 方式实现跨域的 BGP/MPLS VPN, 即采用 VPN-INSTANCE-to-VPN-INSTANCE 方式管理 VPN 路由。

同一个 AS 内部的 MPLS 骨干网使用 OSPF 作为 IGP。

2. 组网图

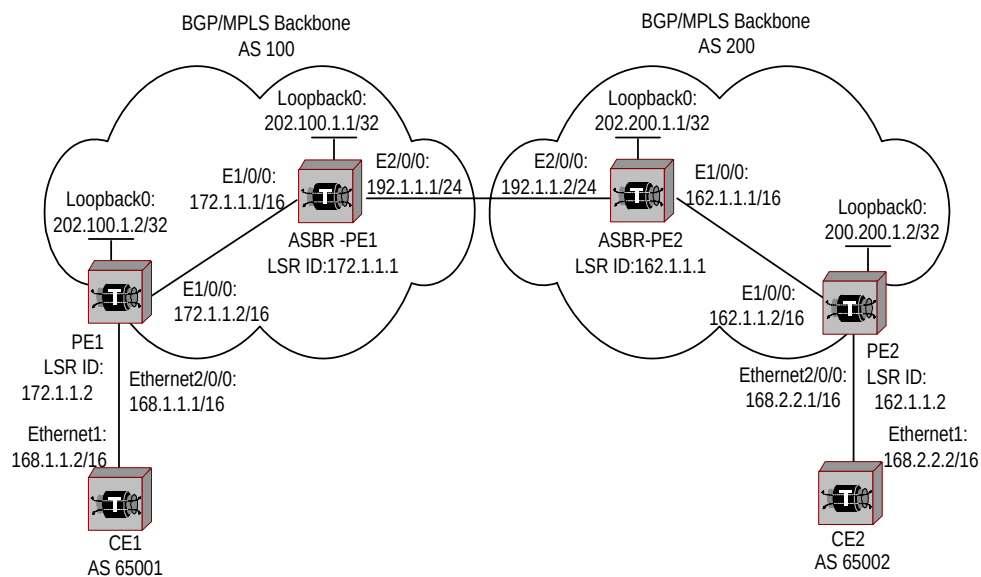


图7-19 跨域 VPN 组网图

3. 配置步骤

根据实现的功能，配置步骤可分为四个部分：

- 在 MPLS 骨干网上配置 IGP 协议 OSPF
- 在 MPLS 骨干网上配置 MPLS 基本能力
- 在 PE 上配置 VPN 实例
- 配置 MP-BGP

下面按照这四个部分的顺序进行介绍：

(1) 在 MPLS 骨干网上配置 IGP 协议 OSPF，使它们能相互学习到路由。

配置 PE1。

```
[PE1] interface loopback0
[PE1-LoopBack0] ip address 202.100.1.2 255.255.255.255
[PE1-LoopBack0] quit
[PE1] interface Ethernet1/0/0
[PE1-Ethernet1/0/0] ip address 172.1.1.2 255.255.0.0
[PE1-Ethernet1/0/0] quit
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 172.1.0.0 0.0.255.255
[PE1-ospf-1-area-0.0.0.0] network 202.100.1.2 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

配置 ASBR-PE1。

```
[ASBR-PE1] interface loopback0
[ASBR-PE1-LoopBack 0] ip address 202.100.1.1 255.255.255.255
[ASBR-PE1-LoopBack 0] quit
[ASBR-PE1] interface Ethernet1/0/0
[ASBR-PE1-Ethernet1/0/0] ip address 172.1.1.1 255.255.0.0
[ASBR-PE1-Ethernet1/0/0] quit
[ASBR-PE1] ospf
[ASBR-PE1-ospf-1] area 0
[ASBR-PE1-ospf-1-area-0.0.0.0] network 172.1.0.0 0.0.255.255
[ASBR-PE1-ospf-1-area-0.0.0.0] network 202.100.1.1 0.0.0.0
[ASBR-PE1-ospf-1-area-0.0.0.0] quit
[ASBR-PE1-ospf-1] quit
```

配置 PE2。

```
[PE2] interface loopback0
[PE2-LoopBack0] ip address 202.200.1.2 255.255.255.255
[PE2-LoopBack0] quit
[PE2] interface Ethernet1/0/0
[PE2-Ethernet1/0/0] ip address 162.1.1.2 255.255.0.0
[PE2-Ethernet1/0/0] quit
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 162.1.0.0 0.0.255.255
[PE2-ospf-1-area-0.0.0.0] network 202.200.1.2 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

配置 ASBR-PE2。

```
[ASBR-PE2] interface loopback0
[ASBR-PE2-LoopBack0] ip address 202.200.1.1 255.255.255.255
[ASBR-PE2-LoopBack0] quit
[ASBR-PE2] interface Ethernet1/0/0
[ASBR-PE2-Ethernet1/0/0] ip address 162.1.1.1 255.255.0.0
[ASBR-PE2-Ethernet1/0/0] quit
[ASBR-PE2] ospf
[ASBR-PE2-ospf-1] area 0
[ASBR-PE2-ospf-1-area-0.0.0.0] network 162.1.0.0 0.0.255.255
[ASBR-PE2-ospf-1-area-0.0.0.0] network 202.200.1.1 0.0.0.0
[ASBR-PE2-ospf-1-area-0.0.0.0] quit
[ASBR-PE2-ospf-1] quit
```

上述配置完成后, ASBR-PE 与本 AS 的 PE 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, PE 之间能学习到对方的 Loopback 地址。

ASBR-PE 与本 AS 的 PE 之间能够互相 ping 通。

以 PE1 和 ASBR-PE1 为例:

```
[PE1] display ospf peer
          OSPF Process 1 with Router ID 202.100.1.2
                Neighbors
Area 0 interface 172.1.1.2(Ethernet1/0/0)'s neighbor(s)
RouterID: 202.100.1.1      Address: 172.1.1.1
    State: Full  Mode: Nbr is Slave  Priority: 1
    DR: None   BDR: None
    Dead timer expires in 40s
    Neighbor comes up for 00:01:32
```

```
[PE1] display ip routing-table
Routing Table: public net
```

Destination/Mask	Protocol	Pre	Cost	Nexthop	Interface
127.0.0.0/8	DIRECT	0	0	127.0.0.1	InLoopBack0
127.0.0.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
172.1.0.0/16	DIRECT	0	0	172.1.1.2	Ethernet1/0/0
172.1.1.1/32	DIRECT	0	0	172.1.1.1	Ethernet1/0/0
172.1.1.2/32	DIRECT	0	0	127.0.0.1	InLoopBack0
202.100.1.1/32	OSPF	10	1563	172.1.1.1	Ethernet1/0/0
202.100.1.2/32	DIRECT	0	0	127.0.0.1	InLoopBack0

```
[PE1] ping 202.100.1.1
PING 202.100.1.1: 56 data bytes, press CTRL_C to break
  Reply from 202.100.1.1: bytes=56 Sequence=1 ttl=255 time=10 ms
  Reply from 202.100.1.1: bytes=56 Sequence=2 ttl=255 time=1 ms
  Reply from 202.100.1.1: bytes=56 Sequence=3 ttl=255 time=50 ms
  Reply from 202.100.1.1: bytes=56 Sequence=4 ttl=255 time=80 ms
  Reply from 202.100.1.1: bytes=56 Sequence=5 ttl=255 time=1 ms
--- 202.100.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/28/80 ms
```

```
[ASBR-PE1] display ospf peer
          OSPF Process 1 with Router ID 202.100.1.1
                Neighbors
```

```

Area 0 interface 172.1.1.1(Ethernet1/0/0)'s neighbor(s)
RouterID: 202.100.1.2      Address: 172.1.1.2
    State: Full  Mode: Nbr is Master  Priority: 1
    DR: None  BDR: None
    Dead timer expires in 30s
    Neighbor comes up for 00:01:49

```

```
[ASBR-PE1] display ip routing-table
```

```
Routing Table: public net
```

Destination/Mask	Protocol	Pre	Cost	NextHop	Interface
127.0.0.0/8	DIRECT	0	0	127.0.0.1	InLoopBack0
127.0.0.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
172.1.0.0/16	DIRECT	0	0	172.1.1.1	Ethernet1/0/0
172.1.1.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
172.1.1.2/32	DIRECT	0	0	172.1.1.2	Ethernet1/0/0
202.100.1.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
202.100.1.2/32	OSPF	10	1563	172.1.1.2	Ethernet1/0/0

```
[ASBR-PE1] ping 202.100.1.2
```

```

PING 202.100.1.2: 56 data bytes, press CTRL_C to break
  Reply from 202.100.1.2: bytes=56 Sequence=1 ttl=255 time=10 ms
  Reply from 202.100.1.2: bytes=56 Sequence=2 ttl=255 time=10 ms
  Reply from 202.100.1.2: bytes=56 Sequence=3 ttl=255 time=10 ms
  Reply from 202.100.1.2: bytes=56 Sequence=4 ttl=255 time=60 ms
  Reply from 202.100.1.2: bytes=56 Sequence=5 ttl=255 time=10 ms
--- 202.100.1.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 10/20/60 ms

```

(2) 在 MPLS 骨干网上配置 MPLS 基本能力, 使网络能够转发 VPN 流量。

配置 PE1 的 MPLS 基本能力, 并在与 ASBR-PE1 相连的接口上使能 LDP。

```

[PE1] mpls lsr-id 172.1.1.2
[PE1] mpls
[PE1-mpls] lsp-trigger all
[PE1-mpls] quit
[PE1] mpls ldp
[PE1] interface Ethernet1/0/0
[PE1-Ethernet1/0/0] mpls
[PE1-Ethernet1/0/0] mpls ldp enable
[PE1-Ethernet1/0/0] quit

```

配置 ASBR-PE1 的 MPLS 基本能力, 并在与 PE1 相连的接口上使能 LDP。


```
[ASBR-PE1] mpls lsr-id 172.1.1.1
[ASBR-PE1] mpls
[ASBR-PE1-mpls] lsp-trigger all
[ASBR-PE1-mpls] quit
[ASBR-PE1] mpls ldp
[ASBR-PE1] interface Ethernet1/0/0
[ASBR-PE1-Ethernet1/0/0] mpls
[ASBR-PE1-Ethernet1/0/0] mpls ldp enable
[ASBR-PE1-Ethernet1/0/0] quit
```

配置 ASBR-PE2 的 MPLS 基本能力, 并在与 PE2 相连的接口上使能 LDP。

```
[ASBR-PE2] mpls lsr-id 162.1.1.1
[ASBR-PE2] mpls
[ASBR-PE2-mpls] lsp-trigger all
[ASBR-PE2-mpls] quit
[ASBR-PE2] mpls ldp
[ASBR-PE2] interface Ethernet1/0/0
[ASBR-PE2-Ethernet1/0/0] mpls
[ASBR-PE2-Ethernet1/0/0] mpls ldp enable
[ASBR-PE2-Ethernet1/0/0] quit
```

配置 PE2 的 MPLS 基本能力, 并在与 ASBR-PE2 相连的接口上使能 LDP。

```
[PE2] mpls lsr-id 162.1.1.2
[PE2] mpls
[PE2-mpls] lsp-trigger all
[PE2-mpls] quit
[PE2] mpls ldp
[PE2] interface Ethernet1/0/0
[PE2-Ethernet1/0/0] mpls
[PE2-Ethernet1/0/0] mpls ldp enable
[PE2-Ethernet1/0/0] quit
```

上述配置完成后, 同一 AS 的 PE 和 ASBR-PE 之间应该建立起 LDP 邻居, 在各安全网关上执行 **display mpls ldp session** 命令可以看到显示结果中 Session State 项为 “Operational”。ASBR-PE1 和 ASBR-PE2 互连的接口上不需要使能 MPLS。

以 PE1 和 ASBR-PE1 上的显示为例:

```
[PE1] display mpls ldp session
Displaying information about all sessions:
  Local LDP ID: 172.1.1.2:0;   Peer LDP ID: 172.1.1.1:0
  TCP Connection: 172.1.1.2 -> 172.1.1.1
  Session State: Operational
  Session Role: Active
  Session existed time: 3 minutes 32 seconds
```

```

KeepAlive Packets Sent/Received: 11/11
Negotiated Keepalive hold time: 60 Peer PV Limit: 0
LDP Basic Discovery Source((A) means active):
Ethernet1/0/0(A)

```

```

[ASBR-PE1] display mpls ldp session
Displaying information about all sessions:
Local LDP ID: 172.1.1.1:0; Peer LDP ID: 172.1.1.2:0
TCP Connection: 172.1.1.1 <- 172.1.1.2
Session State: Operational
Session Role: Passive
Session existed time: 4 minutes 37 seconds
KeepAlive Packets Sent/Received: 14/14
Negotiated Keepalive hold time: 60 Peer PV Limit: 0
LDP Basic Discovery Source((A) means active):
Ethernet1/0/0(A)

```

(3) 在 PE 上配置 VPN 实例，并绑定到连接 CE 的接口上。

说明:

同一 AS 内的 ASBR-PE 与 PE 的 VPN 实例的 VPN-Target 应能匹配，不同 AS 的 PE 的 VPN 实例的 VPN-Target 则不需要匹配。

配置 CE1。

```

[CE1] interface ethernet 1
[CE1-Ethernet1] ip address 168.1.1.2 255.255.0.0
[CE1-Ethernet1] quit

```

在 PE1 上配置 VPN 实例，并将此实例绑定到连接 CE1 的接口。

```

[PE1] ip vpn-instance vpna
[PE1-vpn-vpn-vpna] route-distinguisher 100:2
[PE1-vpn-vpn-vpna] vpn-target 100:1 both
[PE1-vpn-vpn-vpna] quit
[PE1] interface ethernet 2/0/0
[PE1-Ethernet2/0/0] ip binding vpn-instance vpna
[PE1-Ethernet2/0/0] ip address 168.1.1.1 255.255.0.0
[PE1-Ethernet2/0/0] quit

```

在 ASBR-PE1 上配置 VPN 实例，并将此实例绑定到连接 ASBR-PE2 的接口（ASBR-PE1 认为 ASBR-PE2 是自己的 CE）。

```

[ASBR-PE1] ip vpn-instance vpna
[ASBR-PE1-vpn-vpn-vpna] route-distinguisher 100:1
[ASBR-PE1-vpn-vpn-vpna] vpn-target 100:1 both

```

```
[ASBR-PE1-vpn-vpn-vpna] quit
[ASBR-PE1] interface Ethernet 2/0/0
[ASBR-PE1-Ethernet2/0/0] ip binding vpn-instance vpna
[ASBR-PE1-Ethernet2/0/0] ip address 192.1.1.1 255.255.255.0
[ASBR-PE1-Ethernet2/0/0] quit
```

配置 CE2。

```
[CE2] interface ethernet 1
[CE2-Ethernet1] ip address 168.2.2.2 255.255.0.0
[CE2-Ethernet1] quit
```

在 PE2 上配置 VPN 实例，并将此实例绑定到连接 CE2 的接口。

```
[PE2] ip vpn-instance vpna
[PE2-vpn-instance] route-distinguisher 200:2
[PE2-vpn-instance] vpn-target 100:1 both
[PE2-vpn-instance] quit
[PE2] interface ethernet 2/0/0
[PE2-Ethernet2/0/0] ip binding vpn-instance vpna
[PE2-Ethernet2/0/0] ip address 168.2.2.1 255.255.0.0
[PE2-Ethernet2/0/0] quit
```

在 ASBR-PE2 上配置 VPN 实例，并将此实例绑定到连接 ASBR-PE1 的接口（ASBR-PE2 认为 ASBR-PE1 是自己的 CE）。

```
[ASBR-PE2] ip vpn-instance vpna
[ASBR-PE2-vpn-vpn-vpna] route-distinguisher 200:1
[ASBR-PE2-vpn-vpn-vpna] vpn-target 100:1 both
[ASBR-PE2-vpn-vpn-vpna] quit
[ASBR-PE2] interface Ethernet 2/0/0
[ASBR-PE2-Ethernet2/0/0] ip binding vpn-instance vpna
[ASBR-PE2-Ethernet2/0/0] ip address 192.1.1.2 255.255.255.0
[ASBR-PE2-Ethernet2/0/0] quit
```

上述配置完成后，在各 PE 上执行 **display ip vpn-instance verbose** 命令能正确显示 VPN 实例配置。

以 PE1 和 ASBR-PE1 上的显示为例：

```
[PE1] display ip vpn-instance verbose
VPN-Instance : vpna
  No description
  Route-Distinguisher :
    100:2
  Interfaces :
    Ethernet2/0/0
  Export-ext-communities :
    100:1
```

```
Import-ext-communities :
    100:1
[ASBR-PE1] display ip vpn-instance verbose
VPN-Instance : vpna
    No description
    Route-Distinguisher :
        100:1
    Interfaces :
        Ethernet2/0/0
    Export-ext-communities :
        100:1
    Import-ext-communities :
        100:1
```

各 PE 并能 ping 通 CE。ASBR-PE 之间也能互相 ping 通。

PE 对自己的 CE 进行 ping 测试时，需要指定目的地址所属的 VPN。

例如，从 ASBR-PE1 对 ASBR-PE2 进行 ping 测试：

```
[ASBR-PE1] ping -vpn-instance vpna 192.1.1.2
PING 192.1.1.2: 56 data bytes, press CTRL_C to break
  Reply from 192.1.1.2: bytes=56 Sequence=1 ttl=255 time=10 ms
  Reply from 192.1.1.2: bytes=56 Sequence=2 ttl=255 time=10 ms
  Reply from 192.1.1.2: bytes=56 Sequence=3 ttl=255 time=1 ms
  Reply from 192.1.1.2: bytes=56 Sequence=4 ttl=255 time=1 ms
  Reply from 192.1.1.2: bytes=56 Sequence=5 ttl=255 time=60 ms
--- 192.1.1.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/16/60 ms
```

从 CE1 对 PE1 进行 ping 测试：

```
[CE1] ping 168.1.1.1
PING 168.1.1.1: 56 data bytes, press CTRL_C to break
  Reply from 168.1.1.1: bytes=56 Sequence=1 ttl=255 time=1 ms
  Reply from 168.1.1.1: bytes=56 Sequence=2 ttl=255 time=60 ms
  Reply from 168.1.1.1: bytes=56 Sequence=3 ttl=255 time=1 ms
  Reply from 168.1.1.1: bytes=56 Sequence=4 ttl=255 time=60 ms
  Reply from 168.1.1.1: bytes=56 Sequence=5 ttl=255 time=10 ms
--- 168.1.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/26/60 ms
```

从 PE1 对 CE1 进行 ping 测试:

```
[PE1] ping -vpn-instance vpna 168.1.1.2
  PING 168.1.1.2: 56 data bytes, press CTRL_C to break
    Reply from 168.1.1.2: bytes=56 Sequence=1 ttl=255 time=10 ms
    Reply from 168.1.1.2: bytes=56 Sequence=2 ttl=255 time=10 ms
    Reply from 168.1.1.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 168.1.1.2: bytes=56 Sequence=4 ttl=255 time=50 ms
    Reply from 168.1.1.2: bytes=56 Sequence=5 ttl=255 time=10 ms
  --- 168.1.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/16/50 ms
```

(4) 配置 MP-BGP, 在 PE 之间建立 IBGP 对等体关系, 在 PE 与 CE 之间建立 EBGp 对等体关系。

配置 CE1。

```
[CE1] bgp 65001
[CE1-bgp] group 20 external
[CE1-bgp] peer 168.1.1.1 group 20 as-number 100
[CE1-bgp] quit
```

配置 PE1: 与 CE1 建立 EBGp 对等体, 与 ASBR-PE1 建立 IBGP 对等体。

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-af-vpn-instance] group 10 external
[PE1-bgp-af-vpn-instance] peer 168.1.1.2 group 10 as-number 65001
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] group 20
[PE1-bgp] peer 202.100.1.1 group 20
[PE1-bgp] peer 202.100.1.1 connect-interface loopback0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer 20 enable
[PE1-bgp-af-vpn] peer 202.100.1.1 group 20
[PE1-bgp-af-vpn] quit
[PE1-bgp] quit
```

配置 ASBR-PE1: 与 ASBR-PE2 建立 EBGp 对等体, 与 PE1 建立 IBGP 对等体。

```
[ASBR-PE1] bgp 100
[ASBR-PE1-bgp] ipv4-family vpn-instance vpna
[ASBR-PE1-bgp-af-vpn-instance] group 10 external
[ASBR-PE1-bgp-af-vpn-instance] peer 192.1.1.2 group 10 as-number 200
```

```
[ASBR-PE1-bgp-af-vpn-instance] quit
[ASBR-PE1-bgp] group 20
[ASBR-PE1-bgp] peer 202.100.1.2 group 20
[ASBR-PE1-bgp] peer 202.100.1.2 connect-interface loopback0
[ASBR-PE1-bgp] ipv4-family vpnv4
[ASBR-PE1-bgp-af-vpn] peer 20 enable
[ASBR-PE1-bgp-af-vpn] peer 202.100.1.2 group 20
[ASBR-PE1-bgp-af-vpn] quit
[ASBR-PE1-bgp] quit
```

配置 CE2。

```
[CE2] bgp 65002
[CE2-bgp] group 10 external
[CE2-bgp] peer 168.2.2.1 group 10 as-number 200
[CE2-bgp] quit
```

配置 PE2: 与 CE2 建立 EBGP 对等体, 与 ASBR-PE2 建立 IBGP 对等体。

```
[PE2] bgp 200
[PE2-bgp] ipv4-family vpn-instance vpna
[PE2-bgp-af-vpn-instance] group 10 external
[PE2-bgp-af-vpn-instance] peer 168.2.2.2 group 10 as-number 65002
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] quit
[PE2-bgp] group 20
[PE2-bgp] peer 202.200.1.1 group 20
[PE2-bgp] peer 202.200.1.1 connect-interface loopback0
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpn] peer 20 enable
[PE2-bgp-af-vpn] peer 202.200.1.1 group 20
[PE2-bgp-af-vpn] quit
[PE2-bgp] quit
```

配置 ASBR-PE2: 与 ASBR-PE1 建立 EBGP 对等体, 与 PE2 建立 IBGP 对等体。

```
[ASBR-PE2] bgp 200
[ASBR-PE2-bgp] ipv4-family vpn-instance vpna
[ASBR-PE2-bgp-af-vpn-instance] group 10 external
[ASBR-PE2-bgp-af-vpn-instance] peer 192.1.1.1 group 10 as-number 100
[ASBR-PE2-bgp-af-vpn-instance] quit
[ASBR-PE2-bgp] group 20
[ASBR-PE2-bgp] peer 202.200.1.2 group 20
[ASBR-PE2-bgp] peer 202.200.1.2 connect-interface loopback0
[ASBR-PE2-bgp] ipv4-family vpnv4
[ASBR-PE2-bgp-af-vpn] peer 20 enable
[ASBR-PE2-bgp-af-vpn] peer 202.200.1.2 group 20
```

```
[ASBR-PE2-bgp-af-vpn] quit
```

```
[ASBR-PE2-bgp] quit
```

上述配置完成后, 在各安全网关上执行 **display bgp vpnv4 all peer** 命令, 可以看到 PE 之间、PE 与 CE 之间的 BGP 对等体关系都已建立, 并达到 Established 状态。

以 PE1 和 ASBR-PE1 上的显示为例:

```
[PE1] display bgp vpnv4 all peer
```

Peer	AS-num	Ver	Queued-Tx	Msg-Rx	Msg-Tx	Up/Down	State
168.1.1.2	65001	4	0	4	7	00:03:23	Established
202.100.1.1	100	4	0	1	1	00:03:14	Established

```
[ASBR-PE1] display bgp vpnv4 all peer
```

Peer	AS-num	Ver	Queued-Tx	Msg-Rx	Msg-Tx	Up/Down	State
192.1.1.2	200	4	0	5	6	00:03:38	Established
202.100.1.2	100	4	0	1	1	00:04:17	Established

CE 之间能学习到对方的接口路由, CE1 和 CE2 能够相互 ping 通。

```
[CE1] display ip routing-table
```

```
Routing Table: public net
```

Destination/Mask	Protocol	Pre	Cost	Nexthop	Interface
127.0.0.0/8	DIRECT	0	0	127.0.0.1	InLoopBack0
127.0.0.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0
168.1.0.0/16	DIRECT	0	0	168.1.1.2	Ethernet1
168.1.1.2/32	DIRECT	0	0	127.0.0.1	InLoopBack0
168.2.0.0/16	BGP	256	0	168.1.1.1	Ethernet2/0/0

```
[PE1] display ip routing-table vpn-instance vpna
```

```
vpna Route Information
```

```
Routing Table: vpna Route-Distinguisher: 100:2
```

Destination/Mask	Protocol	Pre	Cost	Nexthop	Interface
168.1.0.0/16	DIRECT	0	0	168.1.1.1	Ethernet2/0/0
168.1.1.1/32	DIRECT	0	0	127.0.0.1	InLoopBack0

```
VPN Routing Table: Route-Distinguisher: 100:1
```

168.2.0.0/16	BGP	256	0	202.100.1.1	InLoopBack0

```
[ASBR-PE1] display ip routing-table vpn-instance vpna
```

```
vpna Route Information
```

```
Routing Table: vpna Route-Distinguisher: 100:1
```

Destination/Mask	Protocol	Pre	Cost	Nexthop	Interface
168.2.0.0/16	BGP	256	0	192.1.1.2	Ethernet2/0/0
192.1.1.0/24	DIRECT	0	0	192.1.1.1	Ethernet2/0/0

```

192.1.1.1/32      DIRECT    0    0      127.0.0.1      InLoopBack0
192.1.1.2/32      DIRECT    0    0      192.1.1.2      Ethernet2/0/0
VPN Routing Table: Route-Distinguisher: 100:2
168.1.0.0/16      BGP       256  0      202.100.1.2     InLoopBack0

```

[CE1] ping 168.2.2.2

```

PING 168.2.2.2: 56 data bytes, press CTRL_C to break
  Reply from 168.2.2.2: bytes=56 Sequence=1 ttl=251 time=140 ms
  Reply from 168.2.2.2: bytes=56 Sequence=2 ttl=251 time=130 ms
  Reply from 168.2.2.2: bytes=56 Sequence=3 ttl=251 time=130 ms
  Reply from 168.2.2.2: bytes=56 Sequence=4 ttl=251 time=70 ms
  Reply from 168.2.2.2: bytes=56 Sequence=5 ttl=251 time=130 ms
--- 168.2.2.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 70/120/140 ms

```

[CE2] ping 168.1.1.2

```

PING 168.1.1.2: 56 data bytes, press CTRL_C to break
  Reply from 168.1.1.2: bytes=56 Sequence=1 ttl=251 time=130 ms
  Reply from 168.1.1.2: bytes=56 Sequence=2 ttl=251 time=190 ms
  Reply from 168.1.1.2: bytes=56 Sequence=3 ttl=251 time=70 ms
  Reply from 168.1.1.2: bytes=56 Sequence=4 ttl=251 time=130 ms
  Reply from 168.1.1.2: bytes=56 Sequence=5 ttl=251 time=190 ms
--- 168.1.1.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 70/142/190 ms

```

7.4.10 跨域 VPN 组网举例-OptionB

1. 组网需求

CE1 和 CE2 属于同一个 VPN。CE1 通过 AS100 的 PE1 接入，CE2 通过 AS200 的 PE2 接入。

要求采用 OptionB 方式实现跨域的 BGP/MPLS VPN，即，在 ASBR 间发布标签 VPN-IPv4 路由。

同一个 AS 内部的 MPLS 骨干网使用 OSPF 作为 IGP。

2. 组网图

请参见图 7-19。

3. 配置步骤

根据实现的功能，配置步骤可分为四个部分：

- 在 MPLS 骨干网上配置 IGP 协议 OSPF
- 在 MPLS 骨干网上配置 MPLS 基本能力
- 在 PE 上配置 VPN 实例
- 配置 MP-BGP

与 OptionA 方式相比，主要的区别在于后面两个部分。

(1) 在 MPLS 骨干网上配置 IGP 协议 OSPF，使它们能相互学习到路由。

 说明：

在这一部分：

- PE1 和 PE2 上的配置与“7.4.9 跨域 VPN 组网举例-OptionA”中完全相同；
 - ASBR-PE1 和 ASBR-PE2 上增加了配置它们之间接口的 IP 地址。
-

配置 PE1。

```
[PE1] interface loopback0
[PE1-LoopBack0] ip address 202.100.1.2 255.255.255.255
[PE1-LoopBack0] quit
[PE1] interface Ethernet1/0/0
[PE1-Ethernet1/0/0] ip address 172.1.1.2 255.255.0.0
[PE1-Ethernet1/0/0] quit
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 172.1.0.0 0.0.255.255
[PE1-ospf-1-area-0.0.0.0] network 202.100.1.2 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

配置 ASBR-PE1。

```
[ASBR-PE1] interface loopback0
[ASBR-PE1-LoopBack 0] ip address 202.100.1.1 255.255.255.255
[ASBR-PE1-LoopBack 0] quit
[ASBR-PE1] interface Ethernet1/0/0
[ASBR-PE1-Ethernet1/0/0] ip address 172.1.1.1 255.255.0.0
[ASBR-PE1-Ethernet1/0/0] quit
[ASBR-PE1] interface Ethernet 2/0/0
[ASBR-PE1-Ethernet2/0/0] ip address 192.1.1.1 255.255.255.0
[ASBR-PE1-Ethernet2/0/0] quit
[ASBR-PE1] ospf
```

```
[ASBR-PE1-ospf-1] area 0
[ASBR-PE1-ospf-1-area-0.0.0.0] network 172.1.0.0 0.0.255.255
[ASBR-PE1-ospf-1-area-0.0.0.0] network 202.100.1.1 0.0.0.0
[ASBR-PE1-ospf-1-area-0.0.0.0] quit
[ASBR-PE1-ospf-1] quit
```

配置 PE2。

```
[PE2] interface loopback0
[PE2-LoopBack0] ip address 202.200.1.2 255.255.255.255
[PE2-LoopBack0] quit
[PE2] interface Ethernet1/0/0
[PE2-Ethernet1/0/0] ip address 162.1.1.2 255.255.0.0
[PE2-Ethernet1/0/0] quit
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 162.1.0.0 0.0.255.255
[PE2-ospf-1-area-0.0.0.0] network 202.200.1.2 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

配置 ASBR-PE2。

```
[ASBR-PE2] interface loopback0
[ASBR-PE2-LoopBack0] ip address 202.200.1.1 255.255.255.255
[ASBR-PE2-LoopBack0] quit
[ASBR-PE2] interface Ethernet1/0/0
[ASBR-PE2-Ethernet1/0/0] ip address 162.1.1.1 255.255.0.0
[ASBR-PE2-Ethernet1/0/0] quit
[ASBR-PE2] interface Ethernet 2/0/0
[ASBR-PE2-Ethernet2/0/0] ip address 192.1.1.2 255.255.255.0
[ASBR-PE2-Ethernet2/0/0] quit
[ASBR-PE2] ospf
[ASBR-PE2-ospf-1] area 0
[ASBR-PE2-ospf-1-area-0.0.0.0] network 162.1.0.0 0.0.255.255
[ASBR-PE2-ospf-1-area-0.0.0.0] network 202.200.1.1 0.0.0.0
[ASBR-PE2-ospf-1-area-0.0.0.0] quit
[ASBR-PE2-ospf-1] quit
```

上述配置完成后:ASBR-PE 与本 AS 的 PE 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; PE 之间能学习到对方的 Loopback 地址。

ASBR-PE 与本 AS 的 PE 之间能够互相 ping 通;ASBR-PE 之间也能够互相 ping 通。

(2) 在 MPLS 骨干网上配置 MPLS 基本能力,使网络能够转发 VPN 流量。

 说明:

在这一部分:

PE1、PE2、ASBR-PE1 和 ASBR-PE2 上的配置与 “7.4.9 跨域VPN组网举例-OptionA” 中完全相同。

配置 PE1 的 MPLS 基本能力，并在与 ASBR-PE1 相连的接口上使能 LDP。

```
[PE1] mpls lsr-id 172.1.1.2
[PE1] mpls
[PE1-mpls] lsp-trigger all
[PE1-mpls] quit
[PE1] mpls ldp
[PE1] interface Ethernet1/0/0
[PE1-Ethernet1/0/0] mpls
[PE1-Ethernet1/0/0] mpls ldp enable
[PE1-Ethernet1/0/0] quit
```

配置 ASBR-PE1 的 MPLS 基本能力，并在与 PE1 相连的接口上使能 LDP。

```
[ASBR-PE1] mpls lsr-id 172.1.1.1
[ASBR-PE1] mpls
[ASBR-PE1-mpls] lsp-trigger all
[ASBR-PE1-mpls] quit
[ASBR-PE1] mpls ldp
[ASBR-PE1] interface Ethernet1/0/0
[ASBR-PE1-Ethernet1/0/0] mpls
[ASBR-PE1-Ethernet1/0/0] mpls ldp enable
[ASBR-PE1-Ethernet1/0/0] quit
```

配置 ASBR-PE2 的 MPLS 基本能力，并在与 PE2 相连的接口上使能 LDP。

```
[ASBR-PE2] mpls lsr-id 162.1.1.1
[ASBR-PE2] mpls
[ASBR-PE2-mpls] lsp-trigger all
[ASBR-PE2-mpls] quit
[ASBR-PE2] mpls ldp
[ASBR-PE2] interface Ethernet1/0/0
[ASBR-PE2-Ethernet1/0/0] mpls
[ASBR-PE2-Ethernet1/0/0] mpls ldp enable
[ASBR-PE2-Ethernet1/0/0] quit
```

配置 PE2 的 MPLS 基本能力，并在与 ASBR-PE2 相连的接口上使能 LDP。

```
[PE2] mpls lsr-id 162.1.1.2
[PE2] mpls
[PE2-mpls] lsp-trigger all
```

```
[PE2-mpls] quit
[PE2] mpls ldp
[PE2] interface Ethernet1/0/0
[PE2-Ethernet1/0/0] mpls
[PE2-Ethernet1/0/0] mpls ldp enable
[PE2-Ethernet1/0/0] quit
```

上述配置完成后，同一 AS 的 PE 和 ASBR-PE 之间应该建立起 LDP 邻居，在各安全网关上执行 **display mpls ldp session** 命令可以看到显示结果中 Session State 项为 “Operational”。

(3) 在 PE 上配置 VPN 实例，并绑定到连接 CE 的接口上。

 说明：

与 OptionA 方式不同的是：采用 OptionB 方式时，不仅要求同一 AS 内的 ASBR-PE 与 PE 的 VPN 实例的 VPN-Target 匹配，不同 AS 的 PE 的 VPN 实例的 VPN-Target 也需要匹配。

在这一部分：

- CE1、CE2、PE1 和 PE2 上的配置与 “7.4.9 跨域 VPN 组网举例-OptionA” 中完全相同；
 - 不再需要在 ASBR-PE 上配置 VPN 实例和接口绑定。
-

配置 CE1。

```
[CE1] interface ethernet 1
[CE1-Ethernet1] ip address 168.1.1.2 255.255.0.0
[CE1-Ethernet1] quit
```

在 PE1 上配置 VPN 实例，并将此实例绑定到连接 CE1 的接口。

```
[PE1] ip vpn-instance vpna
[PE1-vpn-vpn-vpna] route-distinguisher 100:2
[PE1-vpn-vpn-vpna] vpn-target 100:1 both
[PE1-vpn-vpn-vpna] quit
[PE1] interface ethernet 2/0/0
[PE1-Ethernet2/0/0] ip binding vpn-instance vpna
[PE1-Ethernet2/0/0] ip address 168.1.1.1 255.255.0.0
[PE1-Ethernet2/0/0] quit
```

配置 CE2。

```
[CE2] interface ethernet 1
[CE2-Ethernet1] ip address 168.2.2.2 255.255.0.0
[CE2-Ethernet1] quit
```

在 PE2 上配置 VPN 实例，并将此实例绑定到连接 CE2 的接口。

```
[PE2] ip vpn-instance vpna
```

```
[PE2-vpn-instance] route-distinguisher 200:2
[PE2-vpn-instance] vpn-target 100:1 both
[PE2-vpn-instance] quit
[PE2] interface ethernet 2/0/0
[PE2-Ethernet2/0/0] ip binding vpn-instance vpna
[PE2-Ethernet2/0/0] ip address 168.2.2.1 255.255.0.0
[PE2-Ethernet2/0/0] quit
```

上述配置完成后, 在各 PE 上执行 **display ip vpn-instance verbose** 命令能正确显示 VPN 实例配置, 并能 ping 通 CE。

PE 对自己的 CE 进行 ping 测试时, 需要指定目的地址所属的 VPN。

例如, 从 PE1 对 CE1 进行 ping 测试:

```
[PE1] ping -vpn-instance vpna 168.1.1.2
```

(4) 配置 MP-BGP, 在 PE 之间建立 IBGP 对等体关系, 在 PE 与 CE 之间建立 EBGP 对等体关系。

说明:

在这一部分:

- CE1、CE2、PE1 和 PE2 上的配置与 “7.4.9 跨域 VPN 组网举例-OptionA” 中完全相同;
 - ASBR-PE1 和 ASBR-PE2 上需要进行特殊配置: 在 VPNV4 地址族中配置 **undo policy vpn-target**; 对域内的 IBGP 对等体配置 **next-hop-local**。
-

配置 CE1。

```
[CE1] bgp 65001
[CE1-bgp] group 20 external
[CE1-bgp] peer 168.1.1.1 group 20 as-number 100
[CE1-bgp] quit
```

配置 PE1: 与 CE1 建立 EBGP 对等体, 与 ASBR-PE1 建立 IBGP 对等体。

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-af-vpn-instance] group 10 external
[PE1-bgp-af-vpn-instance] peer 168.1.1.2 group 10 as-number 65001
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] group 20
[PE1-bgp] peer 202.100.1.1 group 20
[PE1-bgp] peer 202.100.1.1 connect-interface loopback0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer 20 enable
```

```
[PE1-bgp-af-vpn] peer 202.100.1.1 group 20
```

```
[PE1-bgp-af-vpn] quit
```

```
[PE1-bgp] quit
```

配置 ASBR-PE1: 与 ASBR-PE2 建立 EBGP 对等体, 与 PE1 建立 IBGP 对等体。

```
[ASBR-PE1] bgp 100
```

```
[ASBR-PE1-bgp] group 10 external
```

```
[ASBR-PE1-bgp] peer 192.1.1.2 group 10 as-number 200
```

```
[ASBR-PE1-bgp] group 20
```

```
[ASBR-PE1-bgp] peer 202.100.1.2 group 20
```

```
[ASBR-PE1-bgp] peer 202.100.1.2 connect-interface loopback0
```

```
[ASBR-PE1-bgp] ipv4-family vpnv4
```

```
[ASBR-PE1-bgp-af-vpn] peer 20 enable
```

```
[ASBR-PE1-bgp-af-vpn] peer 202.100.1.2 group 20
```

```
[ASBR-PE1-bgp-af-vpn] peer 20 next-hop-local
```

```
[ASBR-PE1-bgp-af-vpn] peer 10 enable
```

```
[ASBR-PE1-bgp-af-vpn] peer 192.1.1.2 group 10
```

```
[ASBR-PE1-bgp-af-vpn] undo policy vpn-target
```

```
[ASBR-PE1-bgp-af-vpn] quit
```

```
[ASBR-PE1-bgp] quit
```

配置 CE2。

```
[CE2] bgp 65002
```

```
[CE2-bgp] group 10 external
```

```
[CE2-bgp] peer 168.2.2.1 group 10 as-number 200
```

```
[CE2-bgp] quit
```

配置 PE2: 与 CE2 建立 EBGP 对等体, 与 ASBR-PE2 建立 IBGP 对等体。

```
[PE2] bgp 200
```

```
[PE2-bgp] ipv4-family vpn-instance vpna
```

```
[PE2-bgp-af-vpn-instance] group 10 external
```

```
[PE2-bgp-af-vpn-instance] peer 168.2.2.2 group 10 as-number 65002
```

```
[PE2-bgp-af-vpn-instance] import-route direct
```

```
[PE2-bgp-af-vpn-instance] quit
```

```
[PE2-bgp] group 20
```

```
[PE2-bgp] peer 202.200.1.1 group 20
```

```
[PE2-bgp] peer 202.200.1.1 connect-interface loopback0
```

```
[PE2-bgp] ipv4-family vpnv4
```

```
[PE2-bgp-af-vpn] peer 20 enable
```

```
[PE2-bgp-af-vpn] peer 202.200.1.1 group 20
```

```
[PE2-bgp-af-vpn] quit
```

```
[PE2-bgp] quit
```

配置 ASBR-PE2: 与 ASBR-PE1 建立 EBGP 对等体, 与 PE2 建立 IBGP 对等体。

```
[ASBR-PE2] bgp 200
[ASBR-PE2-bgp] group 10 external
[ASBR-PE2-bgp] peer 192.1.1.1 group 10 as-number 100
[ASBR-PE2-bgp] group 20
[ASBR-PE2-bgp] peer 202.200.1.2 group 20
[ASBR-PE2-bgp] peer 202.200.1.2 connect-interface loopback0
[ASBR-PE2-bgp] ipv4-family vpnv4
[ASBR-PE2-bgp-af-vpn] peer 20 enable
[ASBR-PE2-bgp-af-vpn] peer 202.200.1.2 group 20
[ASBR-PE2-bgp-af-vpn] peer 20 next-hop-local
[ASBR-PE2-bgp-af-vpn] undo policy vpn-target
[ASBR-PE2-bgp-af-vpn] peer 10 enable
[ASBR-PE2-bgp-af-vpn] peer 192.1.1.1 group 10
[ASBR-PE2-bgp-af-vpn] quit
[ASBR-PE2-bgp] quit
```

上述配置完成后, 在各安全网关上执行 **display bgp vpnv4 all peer** 命令, 可以看到 PE 之间、PE 与 CE 之间的 BGP 对等体关系都已建立, 并达到 Established 状态。

CE 之间能学习到对方的接口路由, CE1 和 CE2 能相互 ping 通。

说明: 当 PE 同时作为 ASBR 时, 它需要保存所有 VPNv4 路由信息, 以通告给其它 ASBR。这种情况下, PE 应接收所有 VPNv4 路由信息, 不对它们路由进行 VPN-target 过滤, 故必须配置 **undo policy vpn-target** 命令。

7.4.11 跨域 VPN 组网举例-OptionC

1. 组网需求

CE1 和 CE2 属于同一个 VPN。CE1 通过 AS100 的 PE1 接入, CE2 通过 AS200 的 PE2 接入。

采用 OptionC 方式实现跨域的 BGP/MPLS VPN, 即, 采用 PE 间通过 Multi-hop MP-EBGP 发布标签 VPN-IPv4 路由方式管理 VPN 路由。

2. 组网图

请参见图 7-19。

3. 配置步骤

根据实现的功能, 配置步骤可分为四个部分:

- 在 MPLS 骨干网上配置 IGP 协议 OSPF
- 在 MPLS 骨干网上配置 MPLS 基本能力
- 在 PE 上配置 VPN 实例
- 配置 MP-BGP

与 OptionA 方式相比，主要的区别在于后面两个部分。

(1) 在 MPLS 骨干网上配置 IGP 协议 OSPF，使它们能相互学习到路由。

 说明：

在这一部分：

PE1 和 PE2 上的配置与 “7.4.10 跨域 VPN 组网举例-OptionB” 中完全相同。

配置 PE1。

```
[PE1] interface loopback0
[PE1-LoopBack0] ip address 202.100.1.2 255.255.255.255
[PE1-LoopBack0] quit
[PE1] interface Ethernet1/0/0
[PE1-Ethernet1/0/0] ip address 172.1.1.2 255.255.0.0
[PE1-Ethernet1/0/0] quit
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 172.1.0.0 0.0.255.255
[PE1-ospf-1-area-0.0.0.0] network 202.100.1.2 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

配置 ASBR-PE1。

```
[ASBR-PE1] interface loopback0
[ASBR-PE1-LoopBack 0] ip address 202.100.1.1 255.255.255.255
[ASBR-PE1-LoopBack 0] quit
[ASBR-PE1] interface Ethernet1/0/0
[ASBR-PE1-Ethernet1/0/0] ip address 172.1.1.1 255.255.0.0
[ASBR-PE1-Ethernet1/0/0] quit
[ASBR-PE1] interface Ethernet 2/0/0
[ASBR-PE1-Ethernet2/0/0] ip address 192.1.1.1 255.255.255.0
[ASBR-PE1-Ethernet2/0/0] quit
[ASBR-PE1] ospf
[ASBR-PE1-ospf-1] area 0
[ASBR-PE1-ospf-1-area-0.0.0.0] network 172.1.0.0 0.0.255.255
[ASBR-PE1-ospf-1-area-0.0.0.0] network 202.100.1.1 0.0.0.0
[ASBR-PE1-ospf-1-area-0.0.0.0] quit
[ASBR-PE1-ospf-1] quit
```

配置 PE2。

```
[PE2] interface loopback0
[PE2-LoopBack0] ip address 202.200.1.2 255.255.255.255
[PE2-LoopBack0] quit
```



```
[PE2] interface Ethernet1/0/0
[PE2-Ethernet1/0/0] ip address 162.1.1.2 255.255.0.0
[PE2-Ethernet1/0/0] quit
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 162.1.0.0 0.0.255.255
[PE2-ospf-1-area-0.0.0.0] network 202.200.1.2 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit

# 配置 ASBR-PE2。

[ASBR-PE2] interface loopback0
[ASBR-PE2-LoopBack0] ip address 202.200.1.1 255.255.255.255
[ASBR-PE2-LoopBack0] quit
[ASBR-PE2] interface Ethernet1/0/0
[ASBR-PE2-Ethernet1/0/0] ip address 162.1.1.1 255.255.0.0
[ASBR-PE2-Ethernet1/0/0] quit
[ASBR-PE2] interface Ethernet 2/0/0
[ASBR-PE2-Ethernet2/0/0] ip address 192.1.1.2 255.255.255.0
[ASBR-PE2-Ethernet2/0/0] quit
[ASBR-PE2] ospf
[ASBR-PE2-ospf-1] area 0
[ASBR-PE2-ospf-1-area-0.0.0.0] network 162.1.0.0 0.0.255.255
[ASBR-PE2-ospf-1-area-0.0.0.0] network 202.200.1.1 0.0.0.0
[ASBR-PE2-ospf-1-area-0.0.0.0] quit
[ASBR-PE2-ospf-1] quit
```

上述配置完成后:ASBR-PE 与本 AS 的 PE 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;PE 之间能学习到对方的 Loopback 地址。

ASBR-PE 与本 AS 的 PE 之间能够互相 ping 通;ASBR-PE 之间也能够互相 ping 通。

(2) 在 MPLS 骨干网上配置 MPLS 基本能力,使网络能够转发 VPN 流量。

 说明:

在这一部分:

PE1、PE2 上的配置与“7.4.10 跨域VPN组网举例-OptionB”中完全相同。
ASBR-PE 之间需要配置接口的 MPLS 能力。

配置 PE1 的 MPLS 基本能力,并在与 ASBR-PE1 相连的接口上使能 LDP。

```
[PE1] mpls lsr-id 172.1.1.2
[PE1] mpls
[PE1-mpls] lsp-trigger all
```

```
[PE1-mpls] quit
[PE1] mpls ldp
[PE1] interface Ethernet1/0/0
[PE1-Ethernet1/0/0] mpls
[PE1-Ethernet1/0/0] mpls ldp enable
[PE1-Ethernet1/0/0] quit
```

配置 ASBR-PE1 的 MPLS 基本能力, 并在与 PE1 相连的接口上使能 LDP, 在与 ASBR-PE2 相连的接口上使能 MPLS。

```
[ASBR-PE1] mpls lsr-id 172.1.1.1
[ASBR-PE1] mpls
[ASBR-PE1-mpls] lsp-trigger all
[ASBR-PE1-mpls] quit
[ASBR-PE1] mpls ldp
[ASBR-PE1] interface Ethernet1/0/0
[ASBR-PE1-Ethernet1/0/0] mpls
[ASBR-PE1-Ethernet1/0/0] mpls ldp enable
[ASBR-PE1-Ethernet1/0/0] quit
[ASBR-PE1] interface Ethernet2/0/0
[ASBR-PE1-Ethernet2/0/0] mpls
[ASBR-PE1-Ethernet2/0/0] quit
```

配置 ASBR-PE2 的 MPLS 基本能力, 并在与 PE2 相连的接口上使能 LDP, 在与 ASBR-PE1 相连的接口上使能 MPLS。

```
[ASBR-PE2] mpls lsr-id 162.1.1.1
[ASBR-PE2] mpls
[ASBR-PE2-mpls] lsp-trigger all
[ASBR-PE2-mpls] quit
[ASBR-PE2] mpls ldp
[ASBR-PE2] interface Ethernet1/0/0
[ASBR-PE2-Ethernet1/0/0] mpls
[ASBR-PE2-Ethernet1/0/0] mpls ldp enable
[ASBR-PE2-Ethernet1/0/0] quit
[ASBR-PE2] interface Ethernet2/0/0
[ASBR-PE2-Ethernet2/0/0] mpls
[ASBR-PE2-Ethernet2/0/0] quit
```

配置 PE2 的 MPLS 基本能力, 并在与 ASBR-PE2 相连的接口上使能 LDP。

```
[PE2] mpls lsr-id 162.1.1.2
[PE2] mpls
[PE2-mpls] lsp-trigger all
[PE2-mpls] quit
[PE2] mpls ldp
[PE2] interface Ethernet1/0/0
```

```
[PE2-Ethernet1/0/0] mpls
[PE2-Ethernet1/0/0] mpls ldp enable
[PE2-Ethernet1/0/0] quit
```

上述配置完成后，同一 AS 的 PE 和 ASBR-PE 之间应该建立起 LDP 邻居，在各安全网关上执行 **display mpls ldp session** 命令可以看到显示结果中 Session State 项为 “Operational”。

(3) 在 PE 上配置 VPN 实例，并绑定到连接 CE 的接口上。

 说明：

在这一部分：

CE1、CE2、PE1 和 PE2 上的配置与 “7.4.10 跨域VPN组网举例-OptionB” 中完全相同。

配置 CE1。

```
[CE1] interface ethernet 1
[CE1-Ethernet1] ip address 168.1.1.2 255.255.0.0
[CE1-Ethernet1] quit
```

在 PE1 上配置 VPN 实例，并将此实例绑定到连接 CE1 的接口。

```
[PE1] ip vpn-instance vpna
[PE1-vpn-vpn-vpna] route-distinguisher 100:2
[PE1-vpn-vpn-vpna] vpn-target 100:1 both
[PE1-vpn-vpn-vpna] quit
[PE1] interface ethernet 2/0/0
[PE1-Ethernet2/0/0] ip binding vpn-instance vpna
[PE1-Ethernet2/0/0] ip address 168.1.1.1 255.255.0.0
[PE1-Ethernet2/0/0] quit
```

配置 CE2。

```
[CE2] interface ethernet 1
[CE2-Ethernet1] ip address 168.2.2.2 255.255.0.0
[CE2-Ethernet1] quit
```

在 PE2 上配置 VPN 实例，并将此实例绑定到连接 CE2 的接口。

```
[PE2] ip vpn-instance vpna
[PE2-vpn-instance] route-distinguisher 200:2
[PE2-vpn-instance] vpn-target 100:1 both
[PE2-vpn-instance] quit
[PE2] interface ethernet 2/0/0
[PE2-Ethernet2/0/0] ip binding vpn-instance vpna
[PE2-Ethernet2/0/0] ip address 168.2.2.1 255.255.0.0
[PE2-Ethernet2/0/0] quit
```

上述配置完成后, 在各 PE 上执行 **display ip vpn-instance verbose** 命令能正确显示 VPN 实例配置, 并能 ping 通 CE。

PE 对自己的 CE 进行 ping 测试时, 需要指定目的地址所属的 VPN。

例如, 从 PE1 对 CE1 进行 ping 测试:

```
[PE1] ping -vpn-instance vpna 168.1.1.2
```

(4) 配置 MP-BGP, 在 PE 之间建立 IBGP 对等体关系, 在 PE 与 CE 之间建立 EBGP 对等体关系。

说明:

在这一部分:

- CE1、CE2 的配置与 “7.4.10 跨域VPN组网举例-OptionB” 中完全相同;
 - 在以下安全网关之间配置能够交换带标签的 IPv4 路由: PE1 与 ASBR-PE1、PE2 与 ASBR-PE2、ASBR-PE1 与 ASBR-PE2;
 - ASBR-PE 向本 AS 内的 PE 发布路由时, 将下一跳改为自己;
 - 在 ASBR-PE 上配置路由策略: 对于从本 AS 内的 PE 接收的路由, 在向对端 AS 的 ASBR 发布时, 分配 MPLS 标签; 对于向本 AS 内的 PE 发布的路由, 如果是带标签的 IPv4 路由, 为其分配新的 MPLS 标签。
-

配置 CE1。

```
[CE1] bgp 65001
[CE1-bgp] group 20 external
[CE1-bgp] peer 168.1.1.1 group 20 as-number 100
[CE1-bgp] quit
```

配置 PE1: 与 CE1 建立 EBGP 对等体, 与 ASBR-PE1 建立 IBGP 对等体, 与 PE2 建立 Multihop MP-EBGP 对等体。

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-af-vpn-instance] group 10 external
[PE1-bgp-af-vpn-instance] peer 168.1.1.2 group 10 as-number 65001
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] group 20
[PE1-bgp] peer 20 label-route-capability
[PE1-bgp] peer 202.100.1.1 group 20
[PE1-bgp] peer 202.100.1.1 connect-interface loopback0
[PE1-bgp] group 30 external
[PE1-bgp] peer 30 ebgp-max-hop
[PE1-bgp] peer 200.200.1.2 group 30 as-number 200
[PE1-bgp] peer 200.200.1.2 connect-interface loopback0
```

```
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer 30 enable
[PE1-bgp-af-vpn] peer 200.200.1.2 group 30
[PE1-bgp-af-vpn] quit
[PE1-bgp] quit
```

配置 ASBR-PE1: 配置路由策略。

```
[ASBR-PE1] acl number 2001
[ASBR-PE1-acl-basic-2001] rule permit source 202.100.1.2 0
[ASBR-PE1-acl-basic-2001] rule deny source any
[ASBR-PE1-acl-basic-2001] quit
[ASBR-PE1] route-policy rtp-ebgp permit node 1
[ASBR-PE1-route-policy] if-match acl 2001
[ASBR-PE1-route-policy] apply mpls-label
[ASBR-PE1-route-policy] quit
[ASBR-PE1] route-policy rtp-ibgp permit node 10
[ASBR-PE1-route-policy] if-match mpls-label
[ASBR-PE1-route-policy] apply mpls-label
[ASBR-PE1-route-policy] quit
```

配置 ASBR-PE1: 与 ASBR-PE2 建立 EBGP 对等体, 与 PE1 建立 IBGP 对等体。

```
[ASBR-PE1] bgp 100
[ASBR-PE1-bgp] import-route ospf
[ASBR-PE1-bgp] group 10 external
[ASBR-PE1-bgp] peer 10 label-route-capability
[ASBR-PE1-bgp] peer 10 route-policy rtp-ebgp export
[ASBR-PE1-bgp] peer 192.1.1.2 group 10 as-number 200
[ASBR-PE1-bgp] group 20
[ASBR-PE1-bgp] peer 20 label-route-capability
[ASBR-PE1-bgp] peer 20 next-hop-local
[ASBR-PE1-bgp] peer 20 route-policy rtp-ibgp export
[ASBR-PE1-bgp] peer 202.100.1.2 group 20
[ASBR-PE1-bgp] peer 202.100.1.2 connect-interface loopback0
[ASBR-PE1-bgp] quit
```

配置 CE2。

```
[CE2] bgp 65002
[CE2-bgp] group 10 external
[CE2-bgp] peer 168.2.2.1 group 10 as-number 200
[CE2-bgp] quit
```

配置 PE2: 与 CE2 建立 EBGP 对等体, 与 ASBR-PE2 建立 IBGP 对等体, 与 PE1 建立 Multihop MP-EBGP 对等体。

```
[PE2] bgp 200
```

```
[PE2-bgp] ipv4-family vpn-instance vpna
[PE2-bgp-af-vpn-instance] group 10 external
[PE2-bgp-af-vpn-instance] peer 168.2.2.2 group 10 as-number 65002
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] quit
[PE2-bgp] group 20
[PE2-bgp] peer 20 label-route-capability
[PE2-bgp] peer 202.200.1.1 group 20
[PE2-bgp] peer 202.200.1.1 connect-interface loopback0
[PE2-bgp] group 30 external
[PE2-bgp] peer 30 ebgp-max-hop
[PE2-bgp] peer 202.100.1.2 group 30 as-number 100
[PE2-bgp] peer 202.100.1.2 connect-interface loopback0
[PE2-bgp] ipv4-family vpv4
[PE2-bgp-af-vpn] peer 30 enable
[PE2-bgp-af-vpn] peer 202.100.1.2 group 30
[PE2-bgp-af-vpn] quit
[PE2-bgp] quit
```

配置 ASBR-PE2: 配置路由策略。

```
[ASBR-PE2] acl number 2001
[ASBR-PE2-acl-basic-2001] rule permit source 200.200.1.2 0
[ASBR-PE2-acl-basic-2001] rule deny source any
[ASBR-PE2-acl-basic-2001] quit
[ASBR-PE2] route-policy rtp-ebgp permit node 1
[ASBR-PE2-route-policy] if-match acl 2001
[ASBR-PE2-route-policy] apply mpls-label
[ASBR-PE2-route-policy] quit
[ASBR-PE2] route-policy rtp-ibgp permit node 10
[ASBR-PE2-route-policy] if-match mpls-label
[ASBR-PE2-route-policy] apply mpls-label
[ASBR-PE2-route-policy] quit
```

配置 ASBR-PE2: 与 ASBR-PE1 建立 EBGp 对等体, 与 PE2 建立 IBGP 对等体。

```
[ASBR-PE2] bgp 200
[ASBR-PE2-bgp] import-route ospf
[ASBR-PE2-bgp] group 10 external
[ASBR-PE2-bgp] peer 10 label-route-capability
[ASBR-PE2-bgp] peer 10 route-policy rtp-ebgp export
[ASBR-PE2-bgp] peer 192.1.1.1 group 10 as-number 100
[ASBR-PE2-bgp] group 20
[ASBR-PE2-bgp] peer 20 label-route-capability
[ASBR-PE2-bgp] peer 20 next-hop-local
[ASBR-PE2-bgp] peer 20 route-policy rtp-ibgp export
```

```
[ASBR-PE2-bgp] peer 202.200.1.2 group 20
```

```
[ASBR-PE2-bgp] peer 202.200.1.2 connect-interface loopback0
```

等待所有 BGP 对等体关系建立以后，在 PE1、PE2 上可以看到对方的 IPv4 路由 200.200.1.2、202.100.1.2，使用 **display bgp routing label** 命令可以看到这两条路由带标签，可以看到从对方学到的 VPNv4 路由。

CE 之间能学习到对方的接口路由，CE1 和 CE2 能相互 ping 通。

目 录

第 1 章 网络安全介绍	1-1
1.1 Comware提供的网络安全特性简介	1-1
1.2 命令行分级保护	1-2
1.3 基于RADIUS的AAA	1-2
1.4 包过滤和防火墙	1-2
1.4.1 防火墙的概念	1-2
1.4.2 防火墙的分类	1-3
1.4.3 包过滤	1-4
1.5 交换路由信息时的安全认证	1-5
第 2 章 AAA及RADIUS/HWTACACS协议配置	2-1
2.1 简介	2-1
2.1.1 AAA概述	2-1
2.1.2 RADIUS协议概述	2-2
2.1.3 HWTACACS协议概述	2-6
2.2 AAA配置	2-9
2.2.1 创建ISP域并配置相关属性	2-9
2.2.2 创建本地用户并配置相关属性	2-14
2.3 RADIUS协议配置	2-16
2.3.1 创建RADIUS方案	2-17
2.3.2 配置RADIUS认证/授权服务器	2-17
2.3.3 配置RADIUS计费服务器及相关属性	2-18
2.3.4 设置RADIUS报文的共享密钥	2-20
2.3.5 设置RADIUS请求报文的最大传送次数	2-21
2.3.6 设置支持的RADIUS服务器的类型	2-21
2.3.7 设置RADIUS服务器的状态	2-22
2.3.8 设置发送给RADIUS服务器的用户名格式	2-22
2.3.9 设置发送给RADIUS服务器的数据流的单位	2-23
2.3.10 配置NAS发送RADIUS报文使用的源地址	2-23
2.3.11 配置RADIUS服务器的定时器	2-24
2.3.12 使能RADIUS服务器状态变为down时发送trap报文的功能	2-25
2.3.13 配置本地RADIUS认证服务器	2-25
2.4 HWTACACS协议配置	2-26
2.4.1 创建HWTACACS方案	2-27
2.4.2 配置HWTACACS认证服务器	2-27
2.4.3 配置HWTACACS授权服务器	2-28
2.4.4 配置TACACS计费服务器及相关属性	2-28

2.4.5 配置NAS发送HWTACACS报文使用的源地址	2-29
2.4.6 配置TACACS服务器的密钥	2-30
2.4.7 配置TACACS服务器的用户名格式	2-30
2.4.8 配置TACACS服务器的流量单位	2-30
2.4.9 配置TACACS服务器的定时器	2-31
2.5 TACACS支持super认证配置	2-32
2.5.1 Super认证切换权限处理过程	2-32
2.5.2 设置super认证方式	2-33
2.5.3 设置super认证方案	2-34
2.6 AAA及RADIUS/HWTACACS协议的显示和调试	2-34
2.7 AAA及RADIUS/HWTACACS协议典型配置举例	2-36
2.7.1 Telnet/SSH用户通过RADIUS服务器认证、计费的应用	2-36
2.7.2 FTP/Telnet用户本地认证配置	2-38
2.7.3 PPP用户通过TACACS服务器认证、授权、计费的应用	2-38
2.7.4 Telnet用户通过TACACS服务器认证（一次性认证）、计费的应用	2-40
2.8 AAA及RADIUS/HWTACACS协议故障的诊断与排除	2-42
2.8.1 RADIUS协议故障诊断与排除	2-42
2.8.2 HWTACACS协议故障诊断与排除	2-43
第3章 访问控制列表配置	3-1
3.1 访问控制列表简介	3-1
3.1.1 访问控制列表概述	3-1
3.1.2 访问控制列表的分类	3-1
3.1.3 访问控制列表的匹配顺序	3-1
3.1.4 访问控制列表的创建	3-2
3.1.5 基本访问控制列表	3-3
3.1.6 高级访问控制列表	3-4
3.1.7 基于接口的访问控制列表	3-11
3.1.8 基于MAC地址的访问控制列表	3-12
3.1.9 ACL对分片报文的支持	3-13
3.2 访问控制列表配置	3-14
3.2.1 配置基本访问控制列表	3-14
3.2.2 配置高级访问控制列表	3-14
3.2.3 配置基于接口的访问控制列表	3-15
3.2.4 配置基于MAC地址的访问控制列表	3-15
3.2.5 为ACL添加描述	3-16
3.2.6 为ACL规则添加注释	3-16
3.2.7 删除访问控制列表	3-16
3.2.8 使能/关闭ACL计数器	3-16
3.3 时间段配置	3-17
3.3.1 创建/删除一个时间段	3-17

3.4 访问控制列表的显示与调试.....	3-17
3.5 访问控制列表典型配置案例.....	3-18
第 4 章 地址转换（NAT）配置.....	4-1
4.1 地址转换（NAT）简介.....	4-1
4.1.1 地址转换概述.....	4-1
4.2 地址转换实现的功能.....	4-2
4.2.1 多对多地址转换及地址转换的控制.....	4-2
4.2.2 NAPT——网络地址端口转换.....	4-3
4.2.3 静态网段地址转换.....	4-4
4.2.4 双向地址转换.....	4-4
4.2.5 内部服务器.....	4-5
4.2.6 Easy IP.....	4-6
4.2.7 地址转换应用层网关.....	4-6
4.2.8 NAT限制最大TCP连接数.....	4-6
4.2.9 支持NAT多实例.....	4-6
4.3 NAT的配置.....	4-7
4.3.1 配置地址池.....	4-7
4.3.2 配置地址转换.....	4-8
4.3.3 配置内部服务器.....	4-11
4.3.4 配置地址转换应用层网关.....	4-12
4.3.5 配置内部主机通过域名区分并访问其对应的内部服务器.....	4-12
4.3.6 配置地址转换有效时间.....	4-13
4.3.7 配置NAT限制最大TCP连接数.....	4-13
4.3.8 配置报文匹配方式.....	4-15
4.3.9 配置地址转换表项的老化刷新速度.....	4-16
4.4 地址转换显示和调试.....	4-16
4.5 NAT配置举例.....	4-17
4.5.1 典型NAT配置举例.....	4-17
4.5.2 使用loopback接口地址进行地址转换典型配置举例.....	4-19
4.5.3 静态网段地址转换典型组网应用.....	4-20
4.5.4 双向地址转换配置举例.....	4-22
4.5.5 内部主机通过域名区分并访问对应的内部服务器组网应用.....	4-23
4.5.6 对单一源地址发起的连接数进行限制.....	4-24
4.6 NAT排错.....	4-25
第 5 章 防火墙配置.....	5-1
5.1 防火墙简介.....	5-1
5.1.1 ACL/包过滤防火墙简介.....	5-1
5.1.2 ASPF简介.....	5-2
5.2 包过滤防火墙配置.....	5-5
5.2.1 使能或禁止包过滤防火墙.....	5-5

5.2.2 设置防火墙缺省过滤方式.....	5-6
5.2.3 设置包过滤防火墙分片报文检测开关.....	5-6
5.2.4 配置分片报文检测的上、下门限值	5-6
5.2.5 在接口上应用访问控制列表	5-7
5.2.6 包过滤防火墙显示与调试.....	5-7
5.2.7 包过滤防火墙典型配置举例	5-8
5.2.8 包过滤防火墙分片报文处理配置举例.....	5-10
5.3 ASPF配置	5-11
5.3.1 允许防火墙	5-11
5.3.2 配置访问控制列表.....	5-11
5.3.3 定义ASPF策略.....	5-12
5.3.4 在接口上应用ASPF策略	5-13
5.3.5 配置协议超时时间.....	5-14
5.3.6 配置ASPF的会话日志功能	5-14
5.3.7 端口映射配置.....	5-15
5.3.8 ASPF显示与调试.....	5-15
5.3.9 ASPF使用注意事项	5-16
5.3.10 ASPF典型配置案例	5-16
5.4 黑名单	5-18
5.4.1 黑名单简介	5-18
5.4.2 黑名单配置	5-19
5.4.3 黑名单显示与调试.....	5-20
5.4.4 黑名单典型配置案例	5-20
5.5 MAC和IP地址绑定.....	5-21
5.5.1 MAC和IP地址绑定简介	5-21
5.5.2 MAC和IP地址绑定配置.....	5-21
5.5.3 MAC和IP地址绑定的显示与调试	5-23
5.5.4 MAC和IP地址绑定典型配置案例	5-23
5.6 安全区域配置	5-24
5.6.1 安全区域介绍.....	5-24
5.6.2 安全区域配置.....	5-24
5.6.3 安全区域的显示	5-26
第 6 章 面向对象管理	6-1
6.1 对象管理简介	6-1
6.2 对象创建.....	6-1
6.2.1 地址对象创建.....	6-1
6.2.2 域名地址对象更新.....	6-2
6.2.3 地址组对象创建	6-2
6.2.4 服务对象创建.....	6-3
6.2.5 服务组对象创建	6-3

6.2.6 流对象创建	6-4
6.2.7 时间段对象创建	6-5
6.3 流对象引用	6-5
6.3.1 包过滤中的流对象引用	6-5
6.3.2 NAT中的流对象引用	6-5
6.4 面向对象管理的显示和调试.....	6-6
第 7 章 透明防火墙	7-1
7.1 透明模式简介	7-1
7.1.1 获取地址表过程	7-1
7.1.2 转发和过滤	7-3
7.2 防火墙透明模式配置	7-5
7.2.1 配置防火墙的工作模式	7-5
7.2.2 配置防火墙系统IP地址	7-6
7.2.3 启动/禁止ARP学习功能	7-7
7.2.4 配置对未知目的MAC地址的IP报文的处理方式	7-7
7.2.5 配置基于MAC地址的访问控制列表	7-8
7.2.6 配置在接口上应用访问控制列表	7-8
7.2.7 配置MAC地址转发表的老化时间	7-9
7.2.8 配置允许通过的报文类型	7-9
7.2.9 配置VLAN ID透传	7-9
7.3 透明防火墙的显示和调试	7-10
7.4 典型配置举例	7-11
7.4.1 VLAN ID透传配置举例	7-11
第 8 章 混合模式配置	8-1
8.1 网桥简介	8-1
8.1.1 获取地址表过程	8-1
8.1.2 转发和过滤	8-3
8.2 网桥配置	8-5
8.2.1 网桥基本配置	8-6
8.2.2 配置网桥地址表	8-7
8.2.3 配置以太帧过滤	8-8
8.2.4 配置网桥路由功能	8-9
8.2.5 配置网桥组对网络层协议的桥接功能	8-10
8.2.6 配置网桥允许通过的报文类型	8-10
8.2.7 配置对未知目的MAC地址的IP报文的处理方式	8-11
8.2.8 配置VLAN ID透传	8-11
8.3 网桥的显示和调试	8-12
8.4 网桥典型配置举例	8-13
8.4.1 同时支持路由和桥接举例	8-13

8.4.2 以太网子接口上使用网桥举例	8-14
8.4.3 VLAN ID透传配置举例	8-15
第 9 章 PKI配置	9-1
9.1 PKI简介	9-1
9.1.1 概述	9-1
9.1.2 相关术语	9-2
9.1.3 主要应用	9-2
9.1.4 配置任务列表	9-3
9.2 证书申请配置	9-3
9.2.1 证书申请概述	9-3
9.2.2 进入PKI域视图	9-3
9.2.3 配置信任的CA	9-4
9.2.4 配置申请证书的服务器	9-4
9.2.5 配置实体命名空间	9-7
9.2.6 创建公、私密钥对	9-10
9.2.7 配置查询证书申请处理状态的重发间隔和次数	9-11
9.2.8 配置证书申请模式	9-11
9.2.9 手工申请证书	9-12
9.2.10 手工获取证书	9-12
9.2.11 导入证书	9-13
9.2.12 删除证书	9-13
9.3 证书验证配置	9-13
9.3.1 证书验证配置任务列表	9-13
9.3.2 配置CRL发布点位置	9-14
9.3.3 配置CRL更新周期	9-14
9.3.4 配置是否必须检查CRL	9-14
9.3.5 获取CRL	9-15
9.3.6 验证证书	9-15
9.4 显示和调试	9-16
9.5 典型配置举例	9-17
9.5.1 使用PKI证书方法进行IKE协商认证	9-17
9.6 证书故障诊断与排除	9-19
9.6.1 故障之一：获取CA的证书失败	9-19
9.6.2 故障之二：本地证书申请失败	9-19
9.6.3 故障之三：CRL获取失败	9-20
第 10 章 SSL配置	10-1
10.1 SSL简介	10-1
10.2 SSL配置	10-3
10.2.1 配置服务器端SSL策略	10-3
10.2.2 配置SSL加密卡	10-7

10.2.3 配置基于证书属性访问控制的策略	10-8
10.2.4 配置SSL Proxy服务器策略	10-11
10.2.5 配置举例：建立SSL Proxy服务器	10-14
第 11 章 Web和邮件过滤.....	11-1
11.1 Web和邮件过滤简介	11-1
11.2 配置Web过滤	11-1
11.2.1 配置Web地址过滤	11-1
11.2.2 配置Web内容过滤	11-4
11.2.3 配置SQL注入攻击防范	11-6
11.3 配置邮件过滤	11-8
11.3.1 配置邮件地址过滤	11-8
11.3.2 配置邮件主题过滤	11-10
11.3.3 配置邮件内容过滤	11-11
11.3.4 配置邮件附件过滤	11-13
11.3.5 邮件过滤功能的显示和调试	11-14
第 12 章 攻击防范与报文统计.....	12-1
12.1 攻击防范与报文统计简介	12-1
12.1.1 攻击防范简介.....	12-1
12.1.2 网络攻击的种类	12-1
12.1.3 典型的网络攻击	12-2
12.1.4 报文统计分析功能简介	12-3
12.2 攻击防范配置	12-4
12.2.1 使能/关闭ARP Flood攻击防范功能.....	12-4
12.2.2 配置ARP欺骗攻击防范功能.....	12-5
12.2.3 使能/关闭IP欺骗攻击防范功能.....	12-5
12.2.4 使能/关闭Land攻击防范功能	12-5
12.2.5 使能/关闭Smurf攻击防范功能.....	12-6
12.2.6 使能/关闭WinNuke攻击防范功能.....	12-6
12.2.7 使能/关闭Fraggle攻击防范功能	12-6
12.2.8 使能/关闭Frag Flood攻击防范功能.....	12-7
12.2.9 使能/关闭SYN Flood攻击防范功能.....	12-7
12.2.10 使能/关闭ICMP Flood攻击防范功能	12-9
12.2.11 使能/关闭UDP Flood攻击防范功能	12-10
12.2.12 使能/关闭ICMP重定向报文控制功能	12-12
12.2.13 使能/关闭ICMP不可达报文控制功能	12-12
12.2.14 使能/关闭地址扫描攻击防范功能.....	12-12
12.2.15 使能/关闭端口扫描攻击防范功能.....	12-13
12.2.16 使能/关闭源路由选项IP报文控制功能.....	12-14
12.2.17 使能/关闭路由记录选项攻击防范功能	12-14
12.2.18 使能/关闭Tracert报文控制功能.....	12-14

12.2.19 使能/关闭Ping of Death攻击防范功能	12-14
12.2.20 使能/关闭Teardrop攻击防范功能.....	12-15
12.2.21 使能/关闭TCP报文标志合法性检测功能.....	12-15
12.2.22 使能/关闭IP分片报文检测功能.....	12-16
12.2.23 使能/关闭超大ICMP报文控制功能	12-16
12.3 设置防火墙连接数量和连接速率监控的告警级别	12-16
12.4 系统统计功能的配置	12-17
12.4.1 使能/关闭系统统计功能	12-17
12.4.2 配置系统连接数监控	12-17
12.4.3 配置系统报文比率异常告警检测	12-18
12.5 域统计功能的配置	12-18
12.5.1 使能/关闭域统计功能	12-19
12.5.2 配置域连接数量监控	12-19
12.5.3 配置域连接速率监控	12-20
12.6 IP统计功能的配置	12-20
12.6.1 使能/关闭IP统计功能	12-20
12.6.2 配置IP连接数量监控	12-21
12.6.3 配置IP连接速率监控	12-22
12.7 攻击防范与报文统计显示与调试	12-22
12.7.1 攻击防范显示与调试	12-22
12.7.2 报文统计显示与调试	12-24
12.8 SMTP客户端配置	12-24
12.8.1 配置触发邮件的时间	12-24
12.8.2 配置邮件的收件人地址	12-25
12.8.3 SMTP客户端的显示和调试.....	12-25
12.9 DNS客户端配置	12-26
12.9.1 配置DNS服务器.....	12-26
12.9.2 配置DNS缓存	12-26
12.9.3 DNS客户端的显示和调试	12-26
12.10 攻击防范与报文统计典型配置举例	12-27
12.10.1 使能Land攻击防范功能	12-27
12.10.2 使能SYN Flood攻击防范功能	12-28
12.10.3 使能地址扫描攻击防范功能	12-29
12.10.4 监控基于域的连接数量	12-30
12.10.5 显示指定IP的统计信息	12-32
12.11 攻击防范故障诊断与排除	12-33
第 13 章 IDS联动.....	13-1
13.1 IDS联动功能简介	13-1
13.2 IDS联动配置.....	13-2
13.2.1 在接口下发IDS联动规则.....	13-2

13.2.2 IDS联动的显示与调试	13-2
13.3 IDS典型配置举例	13-3
第 14 章 日志维护	14-1
14.1 日志简介	14-1
14.2 Syslog日志配置	14-2
14.2.1 配置Syslog日志缓冲区的扫描时间	14-2
14.2.2 配置信息中心的日志重定向	14-2
14.3 域间流日志配置	14-3
14.3.1 配置防火墙域间流日志	14-4
14.3.2 配置防火墙流日志统计阈值	14-4
14.4 配置NAT日志	14-5
14.5 日志的清除	14-5
14.6 日志典型配置举例	14-5
14.6.1 输出攻击防范日志到日志主机	14-5
14.6.2 域间流日志配置举例	14-7
14.6.3 NAT日志配置举例	14-8

第1章 网络安全介绍

1.1 Comware 提供的网络安全特性简介

防火墙必须防范来自公网上的恶意攻击。另外，有时用户无意识但有破坏性的访问也会导致设备的性能下降，甚至无法正常工作。

Comware 提供的网络安全特性：

- 基于 RADIUS（Remote Authentication Dial-In User Service）和 HWTACACS（HUAWEI Terminal Access Controller Access Control System）的 AAA（Authentication、Authorization、Accounting）服务：与 RADIUS 和 TACACS 服务器配合实施的 AAA 服务，可以提供对接入用户的验证、授权和计费安全服务，防止非法访问。
- 验证协议：在 PPP 线路上支持 CHAP 和 PAP 验证。
- 包过滤（Packet Filter）：用访问控制列表实现，指定可以通过（或禁止通过）防火墙的报文类型。
- 应用层报文过滤 ASPF（Application Specific Packet Filter）：也称为状态防火墙，是一种高级通信过滤，它检查应用层协议信息并且监控基于连接的应用层协议状态，维护每一个连接的状态信息，并动态地决定数据包是否被允许通过防火墙或者被丢弃。
- 网络层安全（IP security, IPsec）：特定的通信方之间在 IP 层通过加密与数据源验证，来保证数据包在 Internet 上传输时的私有性、完整性和真实性。
- IKE 为 IPsec 提供了自动协商交换密钥、建立安全联盟的服务，能够简化 IPsec 的使用和管理。
- 事件日志：记录系统安全方面事件，实时跟踪非法侵入。
- 地址转换：NAT 网关将公共网络和企业内部网隔离开，在公共网络中隐藏企业内部设备的 IP 地址，阻止来自公网上的攻击。
- 动态路由协议的验证功能：确保所交换路由信息的可靠性。
- 视图分级保护：将用户分成 4 级，每级用户赋予不同的配置权限，级别低的用户不能进入更高级的视图。

本章中将详细介绍 AAA 及 RADIUS 配置、用户口令配置、防火墙和包过滤配置等；IPsec 配置，IKE 配置请参见本手册的“VPN”部分；PPP 验证协议配置请参见本手册的“用户接入”部分；日志的配置请参见本手册的“基础配置”部分；地址转换

请参见 第 4 章 地址转换（NAT）配置；动态路由协议的验证请参见本手册的“路由协议”部分。

1.2 命令行分级保护

系统命令行采用分级保护方式，命令行划分为参观级、监控级、配置级、管理级 4 个级别，只有提供了正确的登录口令，才能使用相应的命令。

1.3 基于 RADIUS 的 AAA

AAA 是验证（Authentication）、授权（Authorization）、计费（Accounting）的缩写，用来实现对用户的访问进行管理的功能。AAA 可以用多种协议来实现，这里 AAA 是基于 RADIUS 协议来实现的。

AAA 提供如下功能：

- 用户的分级管理：用户可以对系统的配置数据进行管理维护，对设备进行监控和维护等操作，而这些操作对系统的正常运行至关重要。因此要对用户进行严格分级管理，不同级别的用户有不同的权限；低级别的用户只能进行一些查看操作，只有高级用户才能进行一些如修改数据、维护设备，以及其它比较敏感的操作。
- PPP 用户的验证：建立 PPP 连接时，对用户名及密码进行验证。
- PPP 用户的地址管理和分配：建立 PPP 连接时，可以为 PPP 用户分配预先指定的 IP 地址。

第二章将详细介绍 RADIUS 协议及其配置、用户口令配置、PPP 用户地址配置。PPP 验证协议请参见本手册的“用户接入”部分。

1.4 包过滤和防火墙

1.4.1 防火墙的概念

防火墙一方面阻止来自 Internet 的对受保护网络的未授权或未验证的访问，另一方面允许内部网络的用户对 Internet 进行 Web 访问或收发 E-mail 等。防火墙也可以作为一个访问 Internet 的权限控制关口，如允许组织内的特定的人可以访问 Internet。

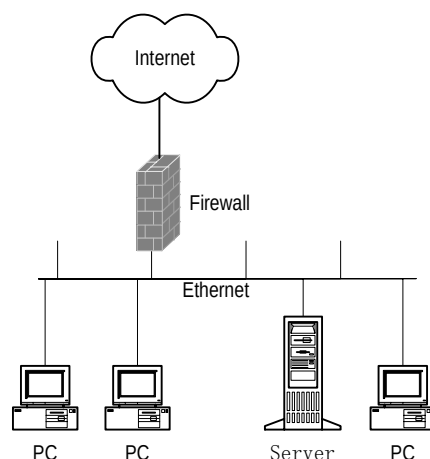


图1-1 防火墙使内部网络和 Internet 隔离

防火墙不单应用于和外部 **Internet** 的连接，也可以用于保护组织内部网络的大型机和重要资源（如数据）。对受保护数据的访问都必须经过防火墙的过滤，即使该访问是来自组织内部。

当外部网络的用户访问网内资源时，要经过防火墙；而内部网络的用户访问网外资源时，也会经过防火墙。这样，防火墙就起到了一个“警卫”的作用，可以将需要禁止的数据包在这里给丢掉。

1.4.2 防火墙的分类

一般把防火墙分为两类：网络层防火墙、应用层防火墙。网络层的防火墙主要获取数据包的包头信息，如协议号、源地址、目的地址和目的端口等，或者直接获取包头的一段数据；而应用层的防火墙则对整个信息流进行分析。

常见的防火墙有以下几种：

- 应用网关（**Application Gateway**）：检验通过此网关的所有数据包中的应用层的数据。如 **FTP** 应用网关，对于连接的 **Client** 端来说是一个 **FTP Server**，对于 **Server** 端来说是一个 **FTP Client**。连接中传输的所有 **FTP** 数据包都必须经过此 **FTP** 应用网关。
- 电路级网关（**Circuit-Level Gateway**）：此电路指虚电路。在 **TCP** 或 **UDP** 发起（**Open**）一个连接或电路之前，验证该会话的可靠性。只有在握手被验证为合法且握手完成之后，才允许数据包的传输。一个会话建立后，此会话的信息被写入防火墙维护的有效连接表中。数据包只有在它所含的会话信息符合该有效连接表中的某一条目（**Entry**）时，才被允许通过。会话结束时，该会话在表中的条目被删掉。电路级网关只对连接在会话层进行验证。一旦验证通过，在该连接上可以运行任何一个应用程序。以 **FTP** 为例，电路层网关只在一个

FTP 会话开始时，在 TCP 层对此会话进行验证。如果验证通过，则所有的数据都可以通过此连接进行传输，直至会话结束。

- 包过滤（Packet Filter）：对每个数据包按照用户所定义的项目进行过滤，如比较数据包的源地址、目的地址等是否符合规则。包过滤不管会话的状态，也不分析数据。如用户规定允许端口是 21 或者大于等于 1024 的数据包通过，则只要端口符合该条件，数据包便可以通过此防火墙。如果配置的规则比较符合实际应用的话，在这一层能够过滤掉很多有安全隐患的数据包。
- 地址转换（NAT）：地址转换又称地址代理，它实现了私有网络访问外部网络的功能。地址转换的机制就是将私有网络内主机的 IP 地址和端口替换为防火墙的外部网络地址和端口，以及从防火墙的端口转换为私有网络主机的 IP 地址和端口，即<私有地址+端口>与<公有地址+端口>之间的转换。私有地址是指内部网络或主机地址，公有地址是指在 Internet 上全球唯一的 IP 地址。

Internet 地址分配组织规定将下列的 IP 地址被保留用作私有地址：

10.0.0.0～10.255.255.255

172.16.0.0～172.31.255.255

192.168.0.0～192.168.255.255

这三个范围内的地址不会在 Internet 上被分配，可在一个单位或公司内部使用。各企业根据在预见未来内部主机和网络的数量后，选择合适的内部网络地址，不同企业的内部网络地址可以相同。如果一个公司选择上述三个范围之外的其它网段作为内部网络地址，则有可能会造成混乱。地址转换在允许内部网络的主机访问网外资源的同时，为内部主机提供“隐私”（Privacy）保护。

1.4.3 包过滤

1. 包过滤功能

包过滤一般是指对 IP 数据包的过滤。对防火墙需要转发的数据包，先获取包头信息，包括 IP 层所承载的上层协议的协议号、数据包的源地址、目的地址、源端口和目的端口等，然后和设定的规则进行比较，根据比较的结果对数据包进行转发或者丢弃。

包过滤（对 IP 数据包）所选取用来判断的元素如图 1-2 所示（图中 IP 所承载的上层协议为 TCP/UDP）。

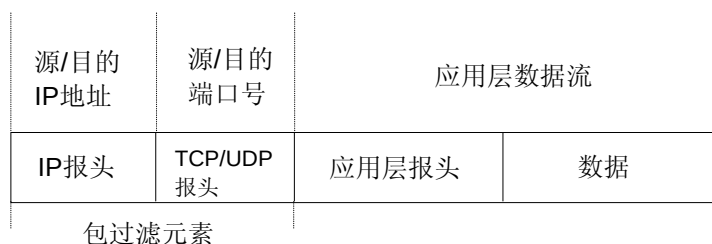


图1-2 包过滤元素示意图

大多数包过滤系统在数据本身上不做任何事，不做基于内容的筛选。

2. 访问控制列表

为了过滤数据包，需要配置一些规则，规定什么样的数据包可以通过，什么样的数据包不能通过。这些规则就是通过访问控制列表（Access Control List）体现的。

用户需要根据自己的安全策略来确定访问控制列表，并将其应用到整机或指定接口上，防火墙就会根据访问控制列表来检查所有接口或指定接口上的所有数据包，对于符合规则的报文作正常转发或丢弃处理，从而起到防火墙的作用。

1.5 交换路由信息时的安全认证

维护正确的路由转发表是路由器正常工作的基础，而路由转发表的维护是通过相邻路由器动态交换路由信息来实现的。

1. 交换路由信息时进行安全认证的必要性

在网络上，相邻的路由器需要交换大量的路由信息，不可靠的路由器可能会发送攻击网络设备的信息。如果具有路由信息认证的功能，防火墙会对收到的相邻路由器的交换路由更新报文进行认证处理，从而保证防火墙只接收可靠的路由信息。

2. 认证的实现

相互交换路由信息的路由器都共享一个口令字，口令字与路由信息报文一起发送，收到路由信息的路由器对报文进行认证，检查报文中的口令字，如果与共享口令字相同，则接受报文，否则丢弃。

认证的实现有两种方式：明文认证和 MD5 认证。明文认证以明文形式发送口令字，安全性较低。而 MD5 认证是发送加密后的口令字，MD5 认证方式安全性较高。

第2章 AAA 及 RADIUS/HWTACACS 协议配置

2.1 简介

2.1.1 AAA 概述

AAA（Authentication Authorization Accounting，认证、授权和计费）提供了一个用来对认证、授权和计费这三种安全功能进行配置的一致性框架，实际上是对网络安全的一种管理。

这里的网络安全主要是指访问控制，包括：

- 哪些用户可以访问网络服务器？
- 具有访问权的用户可以得到哪些服务？
- 如何对正在使用网络资源的用户进行计费？

针对以上问题，AAA 必须提供下列服务：

1. 认证功能

AAA 支持以下认证方式：

- 不认证：对用户非常信任，不对其进行合法检查，一般情况下不采用这种方式。
- 本地认证：将用户信息（包括本地用户的用户名、密码和各种属性）配置在宽带接入服务器上。本地认证的优点是速度快，可以为运营降低成本；缺点是存储信息量受设备硬件条件限制。
- 远端认证：支持通过 RADIUS 协议或 HWTACACS 协议进行远端认证，由宽带接入服务器作为 Client 端，与 RADIUS 服务器或 TACACS 服务器通信。对于 RADIUS 协议，可以采用标准 RADIUS 协议或扩展 RADIUS 协议，与 iTELLIN/CAMS 等设备配合完成认证。

2. 授权功能

AAA 支持以下授权方式：

- 直接授权：对用户非常信任，直接授权通过。
- 本地授权：根据宽带接入服务器上为本地用户帐号配置的相关属性进行授权。
- HWTACACS 授权：由 TACACS 服务器对用户进行授权。
- if-authenticated 授权：如果用户通过了验证，并且使用的验证方法不是 none，则对用户授权通过。

- **RADIUS 认证成功后授权：**RADIUS 协议的认证和授权是绑定在一起的，不能单独使用 RADIUS 进行授权。

3. 计费功能

AAA 支持以下计费方式：

- **不计费：**不对用户计费。
- **远端计费：**支持通过 RADIUS 服务器或 TACACS 服务器进行远端计费。

说明：

目前防火墙只支持对 PPP 用户和 Telnet 用户进行计费，但是对 Telnet 用户不能进行实时计费。

AAA 一般采用客户机/服务器结构：客户端运行于被管理的资源侧，服务器上集中存放用户信息。因此，AAA 框架具有良好的可扩展性，并且容易实现用户信息的集中管理。AAA 是一种管理框架，因此，它可以用多种协议来实现，Comware 中 AAA 是基于 RADIUS 协议或 HWTACACS 协议来实现的。

2.1.2 RADIUS 协议概述

1. 什么是 RADIUS

RADIUS 是 Remote Authentication Dial-In User Service（远程认证拨号用户服务）的简称，它是一种分布式的、客户机/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常被应用在既要求较高安全性，又要求维持远程用户访问的各种网络环境中（例如，它常被应用来管理使用串口和调制解调器的大量分散拨号用户）。RADIUS 系统是 NAS（Network Access Server）系统的重要辅助部分。

RADIUS 服务包括三个组成部分：

- **协议：**RFC2865、2866 协议基于 UDP/IP 层定义了 RADIUS 帧格式及消息传输机制，并定义了 1812 作为认证端口，1813 作为计费端口。
- **服务器：**RADIUS 服务器运行在中心计算机或工作站上，包含了相关的用户认证和网络服务访问信息。
- **客户端：**位于网络访问服务器 NAS（Network Access Server）侧，可以遍布整个网络。

RADIUS 基于客户机/服务器模型，NAS（如防火墙、路由器）作为 RADIUS 客户端，负责传输用户信息到指定的 RADIUS 服务器，然后根据从服务器返回的信息进行相应处理（如接入/挂断用户）。RADIUS 服务器负责接收用户连接请求，认证用户，然后给 NAS 返回所有需要的信息。

RADIUS 服务器通常要维护三个数据库：第一个数据库“Users”用于存储用户信息（如用户名、口令以及使用的协议、IP 地址等配置），第二个数据库“Clients”用于存储 RADIUS 客户端的信息（如共享密钥），第三个数据库“Dictionary”存储的信息用于解释 RADIUS 协议中的属性和属性值的含义。如下图所示：

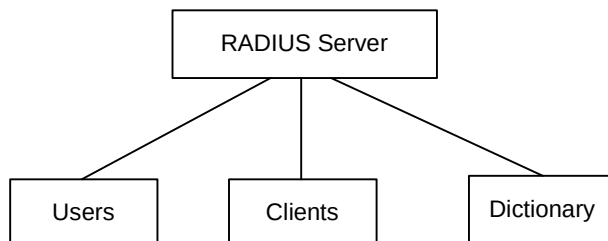


图2-1 RADIUS 服务器的组成

另外，RADIUS 服务器还能够作为其他 AAA 服务器的客户端进行代理认证或计费。RADIUS 服务器支持多种方法来认证用户，如基于 PPP 的 PAP、CHAP 认证、基于 UNIX 的 Login 等。

2. RADIUS 的基本消息交互流程

RADIUS 服务器对用户的认证过程通常需要利用 NAS 等设备的代理认证功能，RADIUS 客户端和 RADIUS 服务器之间通过共享密钥认证相互间交互的消息，用户密码采用密文方式在网络上传输，增强了安全性。RADIUS 协议合并了认证和授权过程，即响应报文中携带了授权信息。操作流程图和步骤如下所示：

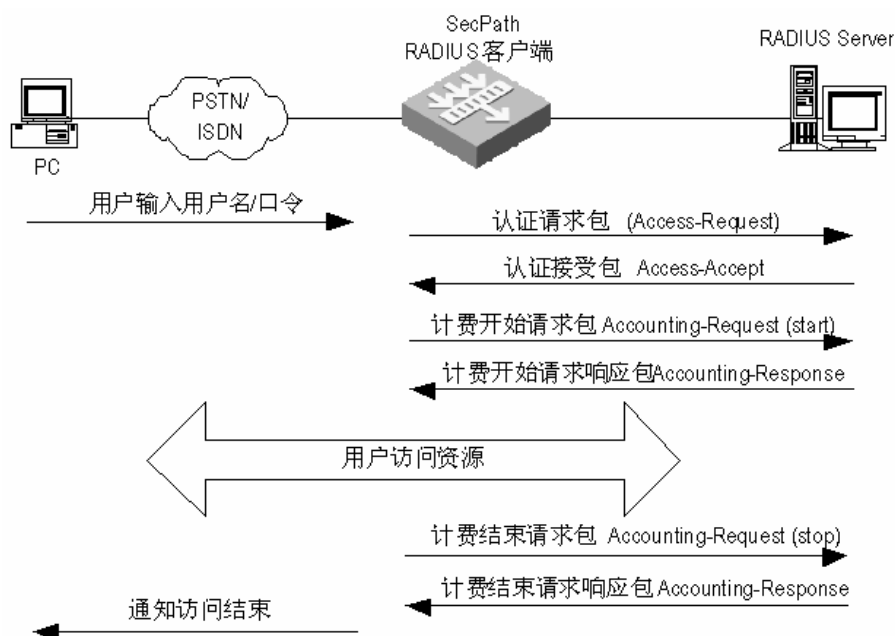


图2-2 RADIUS 的基本消息交互流程

基本交互步骤如下：

- (1) 用户输入用户名和口令；
- (2) RADIUS 客户端根据获取的用户名和口令，向 RADIUS 服务器发送认证请求包（Access-Request）。
- (3) RADIUS 服务器将该用户信息与 Users 数据库信息进行对比分析，如果认证成功，则将用户的权限信息以认证响应包（Access-Accept）发送给 RADIUS 客户端；如果认证失败，则返回 Access-Reject 响应包。
- (4) RADIUS 客户端根据接收到的认证结果接入/拒绝用户。如果可以接入用户，则 RADIUS 客户端向 RADIUS 服务器发送计费开始请求包（Accounting-Request），Status-Type 取值为 start；
- (5) RADIUS 服务器返回计费开始响应包（Accounting-Response）；
- (6) RADIUS 客户端向 RADIUS 服务器发送计费停止请求包（Accounting-Request），Status-Type 取值为 stop；
- (7) RADIUS 服务器返回计费结束响应包（Accounting-Response）。

3. RADIUS 协议的报文结构

RADIUS 采用 UDP 传输消息，通过定时器管理机制、重传机制、备用服务器机制，确保 RADIUS 服务器和客户端之间交互消息正确收发。RADIUS 报文结构如下：

Code	Identifier	Length
Authenticator		
Attribute		

图2-3 RADIUS 报文结构

其中 Identifier 域用于匹配请求包和响应包，随着 Attribute 域改变、接收到有效响应包而不断变化，而在重传时保持不变。Authenticator 域(16 字节)用于验证 RADIUS 服务器传输回来的请求，同时用于密码隐藏算法上，分为 Request Authenticator 和 Response Authenticator。

- Request Authenticator 采用 16 字节的随机码。
- Response Authenticator 是对 Code、Identifier、Request Authenticator、Length、Attribute 和共享密钥使用 MD5 算法进行运算后的结果。

(1) 由 Code 域决定 RADIUS 报文的类型，主要包括：

表2-1 Code 域主要取值的说明

Code	报文类型	报文说明
1	Access-Request 认证请求包	方向 Client->Server, Client 将用户信息传输到 Server 以判断是否接入该用户。该报文中必须包含 User-Name 属性, 可选包含 NAS-IP-Address、User-Password、NAS-Port 等属性。
2	Access-Accept 认证接受包	方向 Server->Client, 如果 Access-Request 报文中所有 Attribute 值都是可以接受的（即认证通过），则传输该类型报文。
3	Access-Reject 认证拒绝包	方向 Server->Client, 如果 Access-Request 报文中存在任何 Attribute 值无法被接受（即认证失败），则传输该类型报文。
4	Accounting-Request 计费请求包	方向 Client->Server, Client 将用户信息传输到 Server, 请求 Server 开始计费, 由该报文中的 Acct-Status-Type 属性区分计费开始请求和计费结束请求。该报文包含的属性和 Access-Request 报文大致相同。
5	Accounting-Response 计费响应包	方向 Server->Client, Server 通知 Client 侧已经收到 Accounting-Request 报文并且已经正确记录计费信息。该报文包含端口上输入/输出字节数、输入/输出包数、会话时长等信息。

(2) Attribute 域携带专门的认证、授权和计费信息，提供请求和响应报文的配置细节，该域采用（Type、Length、Value）三元组的形式提供，RFC 中定义的标准 Attribute 域大致包括：

表2-2 Attribute 域主要取值的说明

Type	属性类型	Type	属性类型
1	User-Name	23	Framed-IPX-Network
2	User-Password	24	State
3	CHAP-Password	25	Class
4	NAS-IP-Address	26	Vendor-Specific
5	NAS-Port	27	Session-Timeout
6	Service-Type	28	Idle-Timeout
7	Framed-Protocol	29	Termination-Action
8	Framed-IP-Address	30	Called-Station-Id
9	Framed-IP-Netmask	31	Calling-Station-Id
10	Framed-Routing	32	NAS-Identifier
11	Filter-ID	33	Proxy-State
12	Framed-MTU	34	Login-LAT-Service

Type	属性类型	Type	属性类型
13	Framed-Compression	35	Login-LAT-Node
14	Login-IP-Host	36	Login-LAT-Group
15	Login-Service	37	Framed-AppleTalk-Link
16	Login-TCP-Port	38	Framed-AppleTalk-Network
17	(unassigned)	39	Framed-AppleTalk-Zone
18	Reply_Message	40-59	(reserved for accounting)
19	Callback-Number	60	CHAP-Challenge
20	Callback-ID	61	NAS-Port-Type
21	(unassigned)	62	Port-Limit
22	Framed-Route	63	Login-LAT-Port

RADIUS 协议具有良好的可扩展性，协议中定义的 26 号属性（Vender-Specific）可以被方便地扩展以支持用户自己定义的扩展属性，报文结构如下图所示：

Type	Length	Vendor-ID	
Vendor-ID		type (specified)	length (specified)
specified attribute value			

图2-4 包括扩展属性的 RADIUS 报文片断

4. RADIUS 的特点

RADIUS 使用 UDP 作为传输协议，具有良好的实时性；同时也支持重传机制和备用服务器机制，从而有较好的可靠性。RADIUS 的实现比较简单，适用于大用户量时服务器端的多线程结构。正因为如此，RADIUS 协议得到了广泛的应用。

2.1.3 HWTACACS 协议概述

1. HWTACACS 特性

HWTACACS（HUAWEI Terminal Access Controller Access Control System）安全协议是在 TACACS（RFC1492）基础上进行了功能增强的一种安全协议。该协议与 RADIUS 协议类似，主要是通过 Server-Client 模式与 TACACS 服务器通信来实现多种用户的 AAA 功能，可用于 PPP 和 VPDN 接入用户及 login 用户的认证、授权和计费。

与 RADIUS 相比，HWTACACS 具有更加可靠的传输和加密特性，更加适合于安全控制。HWTACACS 协议与 RADIUS 协议的主要区别如下表：

表2-3 HWTACACS 协议和 RADIUS 协议区别

HWTACACS 协议	RADIUS 协议
使用 TCP，网络传输更可靠	使用 UDP
除了标准的 HWTACACS 报文头，对报文主体全部进行加密	只是对验证报文中的密码字段进行加密
认证和授权分离，例如，可以用一个 TACACS 服务器进行认证，另外一个 TACACS 服务器进行授权	认证和授权一起处理
适于进行安全控制	适于进行计费
支持对防火墙上的配置命令进行授权使用	不支持

HWTACACS 的典型应用是拨号用户或终端用户需要登录到防火墙上进行操作，防火墙作为 HWTACACS 的客户端，将用户名和密码发给 TACACS 服务器进行验证，验证通过并得到授权之后可以登录到防火墙上进行操作。如下图所示：

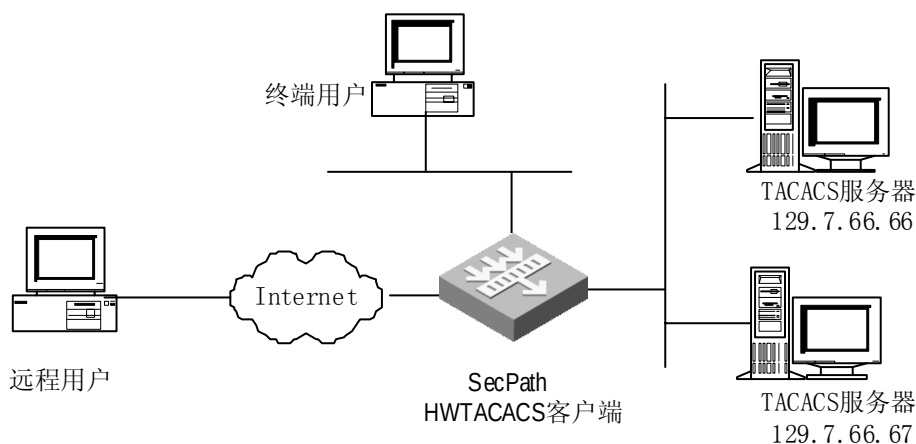


图2-5 HWTACACS 的典型应用组网图

2. HWTACACS 的基本消息交互流程

以 Telnet 用户为例，使用 HWTACACS 对用户进行认证、授权和计费。在整个过程中的基本消息交互流程如下：

- (1) 用户请求登录防火墙，TACACS 客户端收到请求之后，向 TACACS 服务器发送开始认证报文；
- (2) TACACS 服务器发送认证回应报文，请求用户名；TACACS 客户端收到回应报文后，向用户询问用户名；
- (3) TACACS 客户端收到用户名后，向 TACACS 服务器发送认证持续报文，其中包括了用户名；

- (4) TACACS 服务器发送认证回应报文，请求登录密码；TACACS 客户端收到回应报文，向用户询问登录密码；
- (5) TACACS 客户端收到登录密码后，向 TACACS 服务器发送认证持续报文，其中包括了登录密码；
- (6) TACACS 服务器发送认证回应报文，指示用户通过认证；
- (7) TACACS 客户端向 TACACS 服务器发送用户授权报文；
- (8) TACACS 服务器发送授权回应报文，指示用户通过授权；
- (9) TACACS 客户端收到授权回应成功报文，向用户输出防火墙的配置界面；
- (10) TACACS 客户端向 TACACS 服务器发送计费开始报文；
- (11) TACACS 服务器发送计费回应报文，指示计费开始报文已经收到；
- (12) 用户退出，TACACS 客户端向 TACACS 服务器发送计费结束报文；
- (13) TACACS 服务器发送计费结束报文，指示计费结束报文已经收到。

基本消息交互流程图如下：

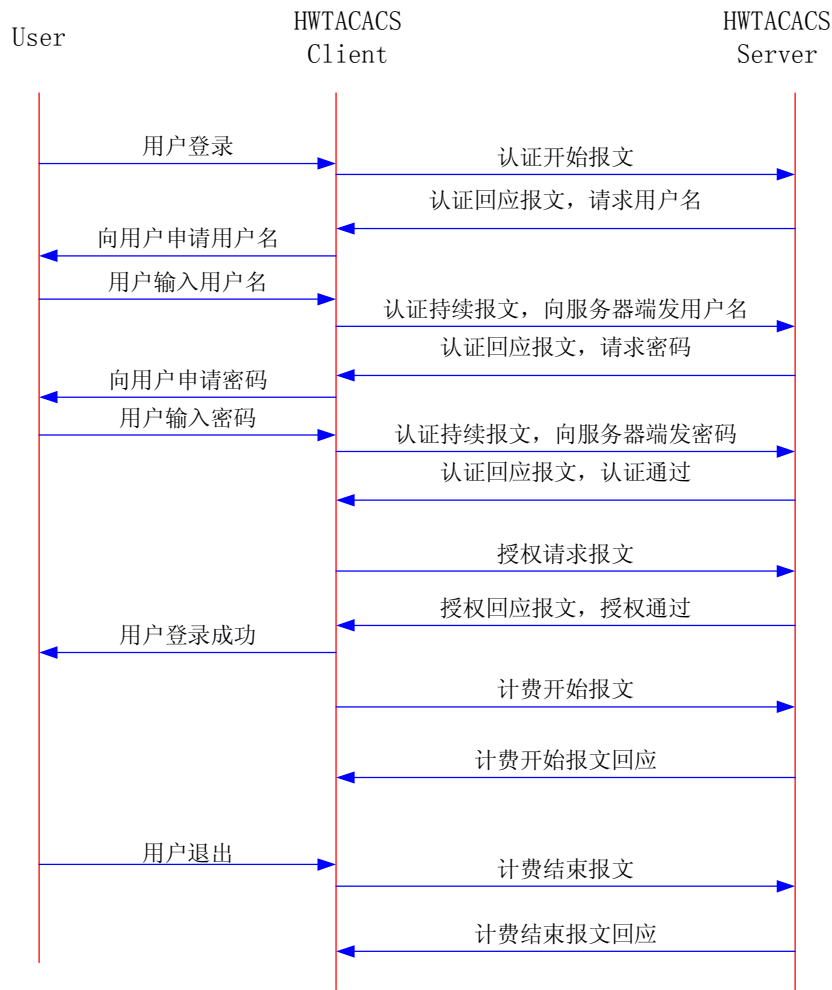


图2-6 Telnet 用户认证、授权和计费流程图

2.2 AAA 配置

AAA 的配置包括：

(1) 创建 ISP 域并配置相关属性

- 创建 ISP 域
- 配置用户使用的 AAA 方案
- 配置 ISP 域的状态
- 配置可接入用户数量的最大值
- 配置计费可选开关
- 定义本地地址池并为 PPP 用户分配 IP 地址

(2) 创建本地用户并配置相关属性（仅用于本地认证）

2.2.1 创建 ISP 域并配置相关属性

1. 创建 ISP 域

什么是 ISP（Internet Service Provider）域？简单点说，ISP 域即 ISP 用户群，一个 ISP 域即是由同属于一个 ISP 的用户构成的用户群。一般说来，在“userid@isp-name”形式（例如 myuser@mydomain.net）的用户名中，“@”后的“isp-name”（如例中的“mydomain.net”）即为 ISP 域的域名。在防火墙对用户进行接入控制时，对于用户名为“userid@isp-name”形式的 ISP 用户，系统将把“userid”作为用于身份认证的用户名，把“isp-name”作为域名。

引入 ISP 域的设置是为了支持多 ISP 的应用环境：在这种环境中，同一个接入设备接入的有可能是不同 ISP 的用户。由于各 ISP 用户的用户属性（例如用户名及密码构成、服务类型/权限等）有可能各不相同，因此有必要通过设置 ISP 域的方法把它们区别开。在 ISP 域视图下，可以为每个 ISP 域配置包括使用的 AAA 方案在内的一整套单独的 ISP 域属性。

对于 SecPath 系列防火墙来说，每个接入用户都属于一某个 ISP 域。系统中最多可以配置 16 个 ISP 域。如果某个用户在登录时没有上报 ISP 域名，则系统将把它归于缺省的 ISP 域。

请在系统视图下进行下列配置。

表2-4 创建/删除 ISP 域

操作	命令
创建 ISP 域或进入指定 ISP 域视图	domain { <i>isp-name</i> default { disable enable <i>isp-name</i> } }
删除指定的 ISP 域	undo domain <i>isp-name</i>

缺省情况下，系统中使用的域为“system”。

2. 配置域引用的 AAA 方案

用户可以通过两种方式配置认证、授权、计费方案：

(1) 认证、授权、计费捆绑方式

采用这种方式时，用户通过 **scheme** 命令指定具体的 AAA 方案。若采用 RADIUS（或 HWTACACS）方案，认证、授权、计费统一由 RADIUS（或 HWTACACS）方案中指定的 RADIUS（或 TACACS）服务器来完成，即认证、授权、计费不能分别指定不同的方案。

若采用本地认证方案，只能完成认证、授权，不能实现计费。

如果配置了 **radius-scheme radius-scheme-name local** 或 **hwtacacs-scheme hwtacacs-scheme-name local**，则 **local** 为 RADIUS 服务器或 HWTACACS 服务器没有正常响应后的备选认证方案。即当 RADIUS 服务器或 HWTACACS 服务器有效时，不使用本地认证；当 RADIUS 服务器或 HWTACACS 服务器无效时，使用本地认证。

如果 **local** 作为第一方案，那么只能采用本地认证，不能再同时采用 RADIUS、HWTACACS 或 **none** 方案。如果 **none** 作为第一方案，那么不能同时采用 RADIUS 或 HWTACACS 方案。

请在 ISP 域视图下进行下列配置。

表2-5 配置 ISP 域的相关属性

操作	命令
配置域使用的 AAA 方案	scheme { radius-scheme radius-scheme-name [local] hwtacacs-scheme hwtacacs-scheme-name [local] local none }
恢复域使用的缺省的 AAA 方案	undo scheme [radius-scheme hwtacacs-scheme none]

系统缺省使用的 AAA 方案为 **local**。



注意：

- 当对 FTP 用户进行验证时，不能使用 **none** 认证，因为 Comware 实现的 FTP 服务器不支持匿名用户登录。
- 如果配置 **scheme none**，则用户登录到系统后所拥有的级别为 level 0。

(2) 认证、授权、计费分离方式

采用这种方式时，用户可以通过 **authentication**、**authorization**、**accounting** 这三条命令分别指定认证、授权、计费方案。如：采用 RADIUS 方案进行认证、授权，

采用 HWTACACS 方案进行计费且计费可选，这样可以为用户提供更加灵活多样的组合方案。认证、授权、计费分离方式中对于 AAA 支撑的各种业务的具体实现如下：

- 对于终端用户

认证采用：RADIUS，HWTACACS，local，RADIUS-local，HWTACACS-local 或者 none。

授权采用：HWTACACS 或者 none。

计费采用：RADIUS，HWTACACS 或者 none。

用户可以参照上面的实现任意组合配置认证，授权和计费的方案。

- 对于 FTP 用户

对于 FTP 用户仅支持认证。

认证采用：RADIUS，HWTACACS，local，RADIUS-local，HWTACACS-local。

- 对于 PPP 及 L2TP 用户

认证采用：RADIUS，HWTACACS，local，RADIUS-local，HWTACACS-local 或者 none。

授权采用：HWTACACS 或者 none。

计费采用：RADIUS，HWTACACS 或者 none。

用户可以参照上面的实现任意组合配置认证、授权和计费的方案。

- 对于 DVPN 业务

当前仅支持 RADIUS、local 或者 RADIUS-local 认证、授权；支持 RADIUS 计费。

请在 ISP 域视图下进行下列配置。

表2-6 配置 ISP 域的相关属性

操作	命令
配置域使用的认证方案	authentication { radius-scheme <i>radius-scheme-name</i> [local] hwtacacs-scheme <i>hwtacacs-scheme-name</i> [local] local none }
恢复域缺省的认证方案	undo authentication
配置域使用的授权方案	authorization { hwtacacs-scheme <i>hwtacacs-scheme-name</i> none }
恢复域缺省的授权方案	undo authorization
配置域使用的计费方案	accounting { radius-scheme <i>radius-scheme-name</i> hwtacacs-scheme <i>hwtacacs-scheme-name</i> none }
删除域使用的计费方案	undo accounting

说明：

- (1) 如果在配置了认证、授权、计费分离方案的同时还配置了认证、授权、计费捆绑方案，优先使用认证、授权、计费分离方案。
- (2) 由于 RADIUS 方案与 local 方案不支持认证和授权的分离，在配置认证授权时应注意如下事项：
 - 当域中配置了 **scheme radius-scheme** 命令或者 **scheme local** 命令，且没有同时配置 **authentication** 命令时，此时如果配置了 **authorization none**，RADIUS 方案和 local 方案返回的授权信息仍然有效；如果配置了 **authorization hwtacacs**，表示使用 HWTACACS 方案进行授权。
 - 如果配置了 **scheme radius-scheme** 或者 **scheme local** 命令，且同时配置了 **authentication hwtacacs-scheme** 命令，则使用 HWTACACS 方案进行认证，并且不进行授权。

3. 配置 ISP 域的状态

每个 ISP 域有两种状态：**active** 或 **block**。当某个 ISP 域处于 **active** 状态时，允许该域下的用户请求网络服务；当某个 ISP 域处于 **block** 状态时，不允许该域下的用户请求网络服务，但是不影响已经在线的用户。一个 ISP 域在刚被创建时是处于 **active** 状态的，即在这个时候，允许任何属于该域的用户请求网络服务。

请在 ISP 域视图下进行下列配置。

表2-7 配置 ISP 域的状态

操作	命令
设置 ISP 域的状态	state { active block }

缺省情况下，当一个 ISP 域被创建以后，其状态为 **active**。

4. 配置可接入用户数量的最大值

可接入用户数的最大值用来指定该 ISP 域最多可容纳多少个接入用户。

请在 ISP 域视图下进行下列配置。

表2-8 配置可接入用户数量的最大值

操作	命令
指定可接入用户数的最大值	access-limit { disable enable max-user-number }
恢复可接入用户数到缺省设置	undo access-limit

缺省情况下，当一个 ISP 域被创建以后，其可容纳的接入用户没有数量限制。

5. 配置计费可选开关

在对用户实施计费时，当发现没有可用的计费服务器或与计费服务器通信失败时，只要用户配置了 **accounting optional**，即使无法实施计费，也不会挂断用户。

accounting optional 命令与 **scheme** 命令中的 **none** 方案的区别在于，使用此命令时，系统仍然向计费服务器发送计费信息，但不管计费服务器是否响应，能否实施计费，系统都不会挂断用户。而使用 **none** 方案时，系统就不会向计费服务器发送计费信息，当然，也不会挂断用户。如果 **scheme** 命令中指定了采用 RADIUS 或 HWTACACS 方案，但没有配置此命令，系统就会向计费服务器发送计费信息，如果计费服务器没有响应，不能实施计费，那么系统就会挂断用户。

请在 ISP 域视图下进行下列配置。

表2-9 配置计费可选开关

操作	命令
打开计费可选开关	accounting optional
关闭计费可选开关	undo accounting optional

缺省情况下，当一个 ISP 域被创建以后，计费可选开关关闭。

6. 定义地址池并为 PPP 用户分配 IP 地址

采用 PPP 方式接入的用户，可以利用 PPP 地址协商功能获得 IP 地址。有三种方法可以为 PPP 用户分配 IP 地址：

- 不配置地址池，在接口上直接给对方配置 IP 地址。
- 在系统视图下定义 IP 地址池，然后在接口视图下指定该接口给对端分配地址时使用的 IP 地址池（只能指定一个）。
- 在域视图下定义 PPP 域用户的 IP 地址池（可以定义多个），依次使用这些地址池直接给用户分配 IP 地址。

请在 ISP 域视图下进行下列配置。

表2-10 定义 PPP 域用户的 IP 地址池

操作	命令
定义为 PPP 用户分配 IP 地址的地址池	ip pool pool-number low-ip-address [high-ip-address]
删除指定的地址池	undo ip pool pool-number

缺省情况下，没有配置 IP 地址池。

下面介绍 AAA 对 PPP 用户的地址分配原则：

- (1) 对于域的用户（包括 *userid* 和 *userid@isp-name* 两种用户）分配地址的优先级如下：
 - 如果采用 RADIUS 或 TACACS 认证和授权，并且服务器给用户下发了地址，则采用服务器下发的地址。
 - 如果服务器没有下发地址，而是下发地址池，则在域视图下相应的地址池中查找地址给用户。
 - 如果上述两种方式没有分配到地址或是采用本地认证，则根据接口下的配置给用户分配地址。
 - 如果接口配置了 **remote address ip-address** 命令，并且此地址没有被使用，则给用户分配此地址。
 - 如果接口配置了 **remote address pool** 命令，则在域视图下相应的地址池中查找地址给用户分配。
 - 如果接口没有配置 **remote address** 命令，则在域视图下遍历所有的地址池查找地址给用户分配。
- (2) 对于不认证用户，采用接口下指定的地址池（即在系统视图下定义的地址池）给用户分配地址。

 说明：

对于进行认证的用户，且未使用 **remote address ip-address** 命令分配地址时，当 PPP 连接建立后，仍可以对 PPP 的地址分配方式进行修改。

2.2.2 创建本地用户并配置相关属性

当 AAA 方案选择了本地认证方案（**local**）时，应在防火墙上创建本地用户并配置相关属性。

 说明：

当用户配置了 **radius-scheme** 或 **hwtacacs-scheme** 认证方法时，应在 RADIUS 或 TACACS 服务器端进行类似的配置，此时本地配置将不起作用。

1. 创建本地用户

所谓本地用户，是指在 NAS（即防火墙）上设置的一组用户的集合。该集合以用户名为用户的唯一标识。为使某个请求网络服务的用户可以通过本地认证，需要在 NAS 的本地用户数据库中添加相应的表项。

请在系统视图下进行下列配置。

表2-11 创建/删除本地用户

操作	命令
添加本地用户	local-user <i>user-name</i>
删除本地用户或本地用户的相关属性	undo local-user <i>user-name</i> [service-type level]
删除所有本地用户或指定类型的本地用户	undo local-user all [service-type { ftp ppp ssh telnet terminal }]

缺省情况下，系统中没有任何本地用户。

2. 设置本地用户的属性

本地用户的属性包括：用户密码显示方式、用户密码、用户状态以及授权用户可以使用的业务类型等。

请在系统视图下进行下列设置。

表2-12 设置本地用户密码显示方式

操作	命令
设置所有本地用户密码的显示方式	local-user password-display-mode { cipher-force auto }
取消已设置的本地用户密码的显示方式	undo local-user password-display-mode

其中，**auto** 表示按照用户配置的密码显示方式（参考下面表格中 **password** 命令）显示，**cipher-force** 表示所有接入用户的密码显示必须采用密文方式。

请在本地用户视图下进行下列配置。

表2-13 设置/取消指定用户的相关属性

操作	命令
设置用户的密码	password { simple cipher } <i>password</i>
取消用户的密码设置	undo password
设置用户的状态	state { active block }
取消用户的状态	undo state { active block }
设置用户可以使用服务类型	service-type { telnet ssh terminal }* [level <i>level</i>]
取消用户可以使用服务	undo service-type { telnet ssh terminal }*
设置用户的优先级	level <i>level</i>
恢复缺省的优先级	undo level
授权用户可以使用 DVPN 服务	service-type dvpn
取消用户可以使用 DVPN 服务	undo service-type dvpn

操作	命令
授权 FTP 用户可以访问的目录	service-type ftp [ftp-directory directory]
恢复对 FTP 用户授权的缺省目录	undo service-type ftp [ftp-directory]
授权用户可以使用 PPP 服务	service-type ppp
取消用户可以使用 PPP 服务	undo service-type ppp

系统缺省不对用户授权任何服务。用户缺省优先级为 0。

说明：

如果配置的认证方式需要用户名和口令（包括本地认证、RADIUS 认证及 HWTACACS 认证），则用户登录系统后所能访问的命令级别由用户的优先级确定。对于使用 RSA 认证的用户，其所能访问的命令级别由用户界面的优先级确定。如果配置的认证方式不认证或采用 password 认证，则用户登录到系统后所能访问的命令级别由用户界面的优先级确定。

2.3 RADIUS 协议配置

RADIUS 协议配置是以 RADIUS 方案为单位进行的，一个 RADIUS 方案在实际组网环境中既可以是一台独立的 RADIUS 服务器，也可以是两台配置相同、但 IP 地址不同的主、备 RADIUS 服务器。由于存在上述情况，因此每个 RADIUS 方案的属性包括：主服务器的 IP 地址、备服务器的 IP 地址、共享密钥以及 RADIUS 服务器类型等。

实际上，RADIUS 协议配置仅仅定义了 NAS 和 RADIUS Server 之间进行信息交互所必须的一些参数。为了使这些参数能够生效，还必须在某个 ISP 域视图下指定该域引用配置有上述参数的 RADIUS 方案。具体配置命令的细节，请参见 2.2 AAA 配置。

RADIUS 协议的配置包括：

- 创建 RADIUS 方案
- 设置 RADIUS 认证/授权服务器
- 设置 RADIUS 计费服务器及相关属性
- 设置 RADIUS 报文的共享密钥
- 设置 RADIUS 请求报文的最大传送次数
- 设置支持的 RADIUS 服务器的类型
- 设置 RADIUS 服务器的状态
- 设置发送给 RADIUS 服务器的用户名格式
- 设置发送给 RADIUS 服务器的数据流的单位

- 配置 NAS 发送 RADIUS 报文使用的源地址
- 配置 RADIUS 服务器的定时器
- 使能 RADIUS 服务器状态变为 down 时发送 trap 报文的功能

在以上的配置任务中，创建 RADIUS 方案、配置 RADIUS 认证/授权服务器是必需的；其余任务则是可选的，用户可以根据各自的具体需求决定是否进行这些配置。

2.3.1 创建 RADIUS 方案

如前所述，RADIUS 协议的配置是以 RADIUS 方案为单位进行的。因此，在进行其它 RADIUS 协议配置之前，必须先创建 RADIUS 方案并进入其视图。

可以使用下面命令创建/删除 RADIUS 方案。

请在系统视图下进行下列配置。

表2-14 创建/删除 RADIUS 方案

操作	命令
创建 RADIUS 方案并进入其视图	radius scheme <i>radius-scheme-name</i>
删除 RADIUS 方案	undo radius scheme <i>radius-scheme-name</i>

一个 RADIUS 方案可以同时被多个 ISP 域引用。系统最多支持配置 16 个 RADIUS 方案。

缺省情况下，系统中已创建了一个名为“system”的 RADIUS 方案，其各项属性均为缺省值。



注意：

FTP、Terminal、SSH 不是 RADIUS 协议的标准属性取值，需要修改 RADIUS 服务器的属性，在属性 login-service（标准属性 15）中增加两个取值的定义：

login-service(50) = SSH

login-service（51）= FTP

login-service(52) = Terminal

修改后再启动 RADIUS 服务器方可。

2.3.2 配置 RADIUS 认证/授权服务器

可以使用下面命令设置 RADIUS 认证/授权服务器的 IP 地址和端口号。

请在 RADIUS 视图下进行下列配置。

表2-15 设置 RADIUS 认证/授权服务器的 IP 地址和端口号

操作	命令
设置主 RADIUS 认证/授权服务器的 IP 地址和端口号	primary authentication <i>ip-address</i> [<i>port-number</i>]
将主 RADIUS 认证/授权服务器的 IP 地址和端口号恢复为缺省值	undo primary authentication
设置备 RADIUS 认证/授权服务器的 IP 地址和端口号	secondary authentication <i>ip-address</i> [<i>port-number</i>]
将备 RADIUS 认证/授权服务器的 IP 地址和端口号恢复为缺省值	undo secondary authentication

RADIUS 服务器的授权信息是随认证应答报文发给 RADIUS 客户端的，故不需要指定单独的授权服务器。

在实际组网环境中，可以指定 2 台 RADIUS 服务器分别作为主、备认证/授权服务器；也可以指定一台服务器既作为主认证/授权服务器，又作为备认证/授权服务器。

2.3.3 配置 RADIUS 计费服务器及相关属性

1. 配置 RADIUS 计费服务器

可以使用下面命令设置 RADIUS 计费服务器的 IP 地址和端口号。

请在 RADIUS 视图下进行下列配置。

表2-16 设置 RADIUS 计费服务器的 IP 地址和端口号

操作	命令
设置主 RADIUS 计费服务器的 IP 地址和端口号	primary accounting <i>ip-address</i> [<i>port-number</i>]
将主 RADIUS 计费服务器的 IP 地址和端口号恢复为缺省值	undo primary accounting
设置备 RADIUS 计费服务器的 IP 地址和端口号	secondary accounting <i>ip-address</i> [<i>port-number</i>]
将备 RADIUS 计费服务器的 IP 地址和端口号恢复为缺省值	undo secondary accounting

在实际组网环境中，可以指定 2 台 RADIUS 服务器分别作为主、备计费服务器；也可以指定一台服务器既作为主计费服务器，又作为备计费服务器。

为了保证 NAS 与 RADIUS 服务器能够正常交互，在设置 RADIUS 服务器的 IP 地址和 UDP 端口之前，必须确保 RADIUS 服务器与 NAS 的路由连接正常。此外，由于 RADIUS 协议采用不同的 UDP 端口来收发认证/授权和计费报文，因此必须将认证/授权端口号和计费端口号设置得不同。RFC2138/2139 中建议的认证/授权端口号为 1812、计费端口号为 1813，但是也可以不选用 RFC 建议值（尤其是比较早期的

RADIUS Server，普遍采用 1645 作为认证/授权端口号、1646 作为计费端口号）。在使用中，请保证防火墙上的 RADIUS 服务端口设置与 RADIUS 服务器上的端口设置保持一致。

可以使用命令 **display radius scheme** 来查看 RADIUS 方案中主、备计费服务器的 IP 地址和端口号。

 说明：

在计费成功后，计费更新以及计费停止报文都会发往计费成功时使用的服务器上，即使此服务器不可用，也不会发生主备切换。只有在最开始的认证、授权、计费过程中才会发生切换，成功后将不再切换。

2. 配置计费可选开关

在对用户实施计费时，当发现没有可用的计费服务器或与计费服务器通信失败时，只要配置了 **accounting optional** 命令，即使无法实施计费，也不会挂断用户。

请在 RADIUS 视图下进行下列配置。

表2-17 配置计费可选开关

操作	命令
打开计费可选开关	accounting optional
关闭计费可选开关	undo accounting optional

缺省情况下，当一个 RADIUS 方案被创建以后，计费可选开关关闭。

3. 使能停止计费报文缓存及重传功能

由于停止计费请求报文涉及到话单结算、并最终影响收费多少，对用户和 ISP 都有比较重要的影响，因此 NAS 应该尽最大努力把它发送给 RADIUS 计费服务器。所以，如果 RADIUS 计费服务器对防火墙发出的停止计费请求报文没有响应，防火墙将其缓存在本机上，然后重新发送直到 RADIUS 计费服务器产生响应，或者在重新发送的次数达到指定的次数限制后将其丢弃。可以使用下面的命令来设置防火墙允许停止计费报文缓存功能。

请在 RADIUS 视图下进行下列配置。

表2-18 设置使能停止计费报文缓存及重传功能

操作	命令
使能停止计费报文缓存功能	stop-accounting-buffer enable
关闭停止计费报文缓存功能	undo stop-accounting-buffer enable

操作	命令
使能停止计费报文重传功能，并配置停止计费报文可以传送的最大次数	retry stop-accounting <i>retry-times</i>
恢复停止计费报文最大传送次数为缺省值	undo retry stop-accounting

缺省情况下，使能停止计费报文缓存功能，最多可以将缓存的停止计费请求报文重发 500 次。

4. 设置允许实时计费请求无响应的最大次数

RADIUS 服务器通常通过连接超时定时器来判断用户是否在线。如果 RADIUS 服务器长时间收不到 NAS 传来的实时计费报文，它会认为线路或设备故障并停止对用户计费。为了配合 RADIUS 服务器的这种特性，有必要在不可预见的故障条件下在 NAS 端尽量与 RADIUS 服务器同步切断用户连接。SecPath 系列防火墙提供对连续实时计费请求无响应次数限制的设置——在 NAS 向 RADIUS 服务器发出的实时计费请求没有得到响应的次数超过所设定的限度时，NAS 将切断用户连接。

可以使用下面的命令设置允许实时计费请求无响应的最大次数。

请在 RADIUS 视图下进行下列配置。

表2-19 设置允许实时计费请求无响应的最大次数

操作	命令
设置允许实时计费请求无响应的最大次数	retry realtime-accounting <i>retry-times</i>
恢复允许实时计费请求无响应的最大次数为缺省值	undo retry realtime-accounting

缺省情况下，最多允许 5 次实时计费请求无响应。

2.3.4 设置 RADIUS 报文的共享密钥

RADIUS 客户端（即防火墙）与 RADIUS 服务器使用 MD5 算法来加密 RADIUS 报文，双方通过设置共享密钥来验证报文的合法性。只有在密钥一致的情况下，双方才能彼此接收对方发来的报文并作出响应。

可以使用下面命令设置 RADIUS 报文的共享密钥。

请在 RADIUS 视图下进行下列配置。

表2-20 设置 RADIUS 报文的共享密钥

操作	命令
设置 RADIUS 认证/授权报文的共享密钥	key authentication <i>string</i>
恢复 RADIUS 认证/授权报文共享密钥为缺省值	undo key authentication

操作	命令
设置 RADIUS 计费报文的共享密钥	key accounting string
恢复 RADIUS 计费报文共享密钥为缺省	undo key accounting

缺省情况下，RADIUS 认证/授权报文和 RADIUS 计费报文均无共享密钥。

2.3.5 设置 RADIUS 请求报文的最大传送次数

由于 RADIUS 协议采用 UDP 报文来承载数据，因此其通信过程是不可靠的。如果 RADIUS 服务器在响应超时定时器规定的时长内没有响应 NAS，则 NAS 有必要向 RADIUS 服务器重传 RADIUS 请求报文。如果累计的传送次数超过最大传送次数而 RADIUS 服务器仍旧没有响应，则 NAS 将认为其与当前 RADIUS 服务器的通信已经中断，并将转而向其它的 RADIUS 服务器发送请求报文。

可以使用下面命令设置 RADIUS 请求报文的最大传送次数。

请在 RADIUS 视图下进行下列配置。

表2-21 设置 RADIUS 请求报文的最大传送次数

操作	命令
设置 RADIUS 请求报文的最大传送次数	retry retry-times
将 RADIUS 请求报文的最大传送次数恢复为缺省值	undo retry

缺省情况下，RADIUS 请求报文的最大传送次数为 3 次。

2.3.6 设置支持的 RADIUS 服务器的类型

可以使用下面的命令来选择支持何种 RADIUS 服务器类型。

请在 RADIUS 视图下进行下列配置。

表2-22 设置支持何种类型的 RADIUS 服务器

操作	命令
设置支持何种类型的 RADIUS 服务器	server-type { extended standard }
恢复 RADIUS 服务器类型为 standard	undo server-type

缺省情况下，system 方案中的 RADIUS 服务器的类型为 **extended**，新创建的 RADIUS 方案中的 RADIUS 服务器的类型为 **standard**。

 说明：

当使用 CAMS 服务器时，只有将 service-type 配置为 extended 后，部分参数才能生效，如服务类型、EXEC 优先级、FTP 目录等。

2.3.7 设置 RADIUS 服务器的状态

对于某个 RADIUS 方案中的主、备服务器（无论是认证/授权服务器还是计费服务器），当主服务器因故障与 NAS 的通信中断时，NAS 会主动地转而与备服务器交互报文。当主服务器恢复正常后，NAS 却不会立即恢复与其通信，而是继续与备服务器通信；直到备服务器也出现故障后，NAS 才能再转而恢复与主服务器交互报文。为了使 NAS 在主服务器故障排除后迅速恢复与其通信，需要通过下面的命令手工将主服务器的状态设为 **active**。

当主服务器与备服务器的状态都为 **active** 或都为 **block** 时，NAS 将只把报文发送到主服务器上。

请在 RADIUS 视图下进行下列配置。

表2-23 设置 RADIUS 服务器的状态

操作	命令
设置主 RADIUS 认证/授权服务器的状态	state primary authentication { block active }
设置主 RADIUS 计费服务器的状态	state primary accounting { block active }
设置备 RADIUS 认证/授权服务器的状态	state secondary authentication { block active }
设置备 RADIUS 计费服务器的状态	state secondary accounting { block active }

可以使用命令 **display radius scheme** 来确定 RADIUS 方案中的服务器的状态。

2.3.8 设置发送给 RADIUS 服务器的用户名格式

如前所述，接入用户通常以“userid@isp-name”的格式命名，“@”后面的部分为 ISP 域名，防火墙就是通过该域名来决定将用户归于哪个 ISP 域的。但是，有些较早期的 RADIUS 服务器不能接受携带有 ISP 域名的用户名，在这种情况下，有必要将用户名中携带的域名去除后再传送给 RADIUS 服务器。因此，防火墙提供下面的命令以指定发送给 RADIUS 服务器的用户名是否携带有 ISP 域名。

表2-24 设置发送给 RADIUS 服务器的用户名格式

操作	命令
设置发送给 RADIUS 服务器的用户名格式	user-name-format { with-domain without-domain }

说明：

如果指定某个 RADIUS 方案不允许用户名中携带有 ISP 域名，那么请不要在两个乃至两个以上的 ISP 域中同时设置使用该 RADIUS 方案，否则，会出现虽然实际用户不同（在不同的 ISP 域中）、但 RADIUS 服务器认为用户相同（因为传送到它的用户名相同）的错误。

缺省情况下，在 system 方案中，NAS 发送给 RADIUS 服务器的用户名不携带 ISP 域名；在新创建的 RADIUS 方案中，NAS 发送给 RADIUS 服务器的用户名携带 ISP 域名。

2.3.9 设置发送给 RADIUS 服务器的数据流的单位

防火墙提供下面的命令以指定发送给 RADIUS 服务器的数据流的单位。

表2-25 设置发送给 RADIUS 服务器的数据流的单位

操作	命令
设置发送给 RADIUS 服务器的数据流的单位	data-flow-format data { byte giga-byte kilo-byte mega-byte } packet { giga-packet kilo-packet mega-packet one-packet }
恢复发送到 RADIUS 服务器的数据流的单位为缺省设置	undo data-flow-format

缺省情况下，RADIUS 方案默认的发送数据单位为 byte，数据包的单位为 one packet。

2.3.10 配置 NAS 发送 RADIUS 报文使用的源地址

请在相应视图下进行下列配置。

表2-26 配置 NAS 发送 RADIUS 报文使用的源地址

操作	命令
配置 NAS 发送 RADIUS 报文使用的源地址（RADIUS 视图）	nas-ip ip-address
取消 NAS 发送 RADIUS 报文使用的源地址（RADIUS 视图）	undo nas-ip
配置 NAS 发送 RADIUS 报文使用的源地址（系统视图）	radius nas-ip ip-address
取消 NAS 发送 RADIUS 报文使用的源地址（系统视图）	undo radius nas-ip

这两条命令的作用相同。缺省情况下，不指定源地址，即以发送报文的接口地址作为源地址。

2.3.11 配置 RADIUS 服务器的定时器

1. 设置 RADIUS 服务器应答超时定时器

如果在 RADIUS 请求报文（认证/授权请求或计费请求）传送出去一段时间后，NAS 还没有得到 RADIUS 服务器的响应，则有必要重传 RADIUS 请求报文，以保证用户确实能够得到 RADIUS 服务。

可以使用下面命令设置 RADIUS 服务器应答超时定时器。

请在 RADIUS 视图下进行下列配置。

表2-27 设置 RADIUS 服务器应答超时定时器

操作	命令
设置 RADIUS 服务器应答超时定时器	timer seconds timer response-timeout seconds
将 RADIUS 服务器应答超时定时器恢复为缺省值	undo timer undo timer response-timeout

缺省情况下，RADIUS 服务器应答超时定时器为 3 秒。**timer** 命令与 **timer response-timeout** 命令的功能一样。

2. 配置 RADIUS 服务器的主服务器恢复激活状态时间

请在 RADIUS 视图下进行下列配置。

表2-28 配置 RADIUS 服务器的主服务器恢复激活状态时间

操作	命令
配置恢复激活时间	timer quiet minutes
恢复缺省配置	undo timer quiet

缺省情况下，主服务器恢复激活状态前需要等待 5 分钟。

3. 设置实时计费时间间隔

为了对用户实施实时计费，有必要设置实时计费的时间间隔。在设置了该属性以后，每隔设定的时间，NAS 会向 RADIUS 服务器发送一次在线用户的计费信息。

可以使用下面命令设置实时计费间隔。

请在 RADIUS 视图下进行下列配置。

表2-29 设置实时计费间隔

操作	命令
设置实时计费间隔	timer realtime-accounting minutes
将实时计费间隔恢复为缺省值	undo timer realtime-accounting

其中，*minutes* 为实时计费间隔时间，单位为分钟，其取值必须为 3 的整数倍。

实时计费间隔的取值对 NAS 和 RADIUS 服务器的性能有一定的相关性要求——取值越小，对 NAS 和 RADIUS 服务器的性能要求越高。建议当用户量比较大（≥1000）时，尽量把该间隔的值设置得大一些。以下是实时计费间隔与用户量之间的推荐比例关系：

表2-30 实时计费间隔与用户量之间的推荐比例关系

用户数	实时计费间隔（分钟）
1~99	3
100~499	6
500~999	12
≥1000	≥15

缺省情况下，实时计费间隔为 12 分钟。

2.3.12 使能 RADIUS 服务器状态变为 down 时发送 trap 报文的功能

请在系统视图下进行下列配置。

表2-31 使能 RADIUS 服务器状态变为 down 时发送 trap 报文的功能

操作	命令
使能 RADIUS 服务器状态变为 down 时发送 trap 报文的功能	radius trap { authentication-server-down accounting-server-down }
关闭 RADIUS 服务器状态变为 down 时发送 trap 报文的功能	undo radius trap { authentication-server-down accounting-server-down }

缺省情况下，关闭该功能。

2.3.13 配置本地 RADIUS 认证服务器

防火墙提供了本地简单 RADIUS 服务器端功能（包括认证和授权），称之为本地 RADIUS 认证服务器功能。

请在系统视图下进行下列配置。

表2-32 配置本地 RADIUS 认证服务器

操作	命令
配置本地 RADIUS 认证服务器	local-server nas-ip <i>ip-address</i> key <i>password</i>
取消本地 RADIUS 认证服务器的配置	undo local-server nas-ip <i>ip-address</i>

缺省情况下，系统创建了一个 NAS-IP 为 127.0.0.1、无缺省密钥的本地 RADIUS 认证服务器。

说明：

采用本地 RADIUS 认证服务器功能时，其认证/授权服务的 UDP 端口号必须为 1645，计费服务的 UDP 端口号为 1646。

用此命令配置的报文加密密钥（key password）必须和在 RADIUS 方案视图下用命令 **key authentication** 配置的认证/授权报文加密密钥一致。

包括系统缺省创建的本地 RADIUS 认证服务器在内，设备最多支持 16 个本地 RADIUS 认证服务器。

2.4 HWTACACS 协议配置

HWTACACS 的配置包括：

- 创建 HWTACACS 方案
- 配置 TACACS 认证服务器
- 配置 TACACS 授权服务器
- 配置 TACACS 计费功能
- 配置 NAS 发送 HWTACACS 报文使用的源地址
- 配置 TACACS 服务器的密钥
- 配置 TACACS 服务器的用户名格式
- 配置 TACACS 服务器的流量单位
- 配置 TACACS 服务器的定时器

说明：

与 RADIUS 的配置相比，配置 TACACS 服务器时需要注意以下几点：

- 除删除方案外，HWTACACS 的大部分属性在改变配置时都不检查当前是否有用户在使用此方案。
- HWTACAS 服务器缺省没有密钥。

在以上的配置任务中，创建 HWTACACS 方案、配置 TACACS 认证/授权服务器是必需的；其余任务则是可选的，用户可以根据各自的具体需求决定是否进行这些配置。

2.4.1 创建 HWTACACS 方案

如前所述，HWTACACS 协议的配置是以 HWTACACS 方案为单位进行的。因此，在进行其它 HWTACACS 协议配置之前，必须先创建 HWTACACS 方案并进入其视图。

请在系统视图下进行下列配置。

表2-33 创建 HWTACACS 方案

操作	命令
创建 HWTACACS 方案，并进入 HWTACACS 视图	hwtacacs scheme <i>hwtacacs-scheme-name</i>
删除 HWTACACS 方案	undo hwtacacs scheme <i>hwtacacs-scheme-name</i>

如果指定的 HWTACACS 方案名不存在，将创建一个新的 HWTACACS 方案并进入 HWTACACS 视图。

在 HWTACACS 视图下，可以对此 HWTACACS 方案进行具体配置。

系统最多支持配置 16 个 HWTACACS 方案。只有当方案没有用户使用时，才能删除该方案。

缺省情况下，没有定义 HWTACACS 方案。

2.4.2 配置 HWTACACS 认证服务器

请在 HWTACACS 视图下进行下列配置。

表2-34 配置 TACACS 认证服务器

操作	命令
配置 TACACS 主认证服务器	primary authentication <i>ip-address</i> [<i>port</i>]
删除 TACACS 主认证服务器	undo primary authentication
配置 TACACS 备认证服务器	secondary authentication <i>ip-address</i> [<i>port</i>]
删除 TACACS 备认证服务器	undo secondary authentication

主认证服务器和备用认证服务器的 IP 地址不能相同，否则将提示配置不成功。端口号缺省使用 49。

如果多次执行此命令，新的配置将覆盖原来的配置。

只有当没有活跃的用于发送认证报文的 TCP 连接使用该认证服务器时，才允许删除该服务器。删除服务器只对之后的报文有效。

2.4.3 配置 HWTACACS 授权服务器

请在 HWTACACS 视图下进行下列配置。

表2-35 配置 TACACS 授权服务器

操作	命令
配置 TACACS 主授权服务器	primary authorization <i>ip-address</i> [<i>port</i>]
删除 TACACS 主授权服务器	undo primary authorization
配置 TACACS 备授权服务器	secondary authorization <i>ip-address</i> [<i>port</i>]
删除 TACACS 备授权服务器	undo secondary authorization

说明：

对于所有类型的用户，如果配置了 TACACS 认证，但没有配置 TACACS 授权服务器，则用户无法登录。

主授权服务器和备用授权服务器的 IP 地址不能相同，否则将提示配置不成功。端口号缺省使用 49。

如果多次执行此命令，新的配置将覆盖原来的配置。

只有当没有活跃的用于发送授权报文的 TCP 连接使用该授权服务器，才允许删除该服务器。

2.4.4 配置 TACACS 计费服务器及相关属性

1. 配置 TACACS 计费服务器

请在 HWTACACS 视图下进行下列配置。

表2-36 配置 HWTACACS 计费服务器

操作	命令
配置 TACACS 主计费服务器	primary accounting <i>ip-address</i> [<i>port</i>]
删除配置的 TACACS 主计费服务器	undo primary accounting
配置 TACACS 备计费服务器	secondary accounting <i>ip-address</i> [<i>port</i>]
删除配置的 TACACS 备计费服务器	undo secondary accounting

主计费服务器和备用计费服务器的 IP 地址不能相同，否则将提示配置不成功。端口号缺省使用 49。

缺省情况下，HWTACACS 计费服务器的 IP 地址为全零。

如果多次执行此命令，新的配置将覆盖原来的配置。

只有当没有活跃、用于发送计费报文的 TCP 连接使用该计费服务器时，才允许删除该服务器。

说明：

在计费成功后，计费更新以及计费停止报文都会发往计费成功时使用的服务器上，即使此服务器不可用，也不会发生主备切换。只有在最开始的认证、授权、计费过程中才会发生切换，成功后将不再切换。

2. 使能停止计费报文缓存及重传功能

请在 HWTACACS 视图下进行下列配置。

表2-37 设置使能停止计费报文缓存及重传功能

操作	命令
使能停止计费报文缓存功能	stop-accounting-buffer enable
关闭停止计费报文缓存功能	undo stop-accounting-buffer enable
使能停止计费报文重传，并配置传送的最大次数	retry stop-accounting <i>retry-times</i>
关闭停止计费报文重传功能	undo retry stop-accounting

缺省情况下，使能停止计费报文重传功能，且允许停止计费报文传送 100 次。

2.4.5 配置 NAS 发送 HWTACACS 报文使用的源地址

请 HWTACACS 视图和系统视图下进行下列配置。

表2-38 配置 NAS 发送 HWTACACS 报文使用的源地址

操作	命令
配置 NAS 发送 HWTACACS 报文使用的源地址(HWTACACS 视图)	nas-ip <i>ip-address</i>
取消 NAS 发送 HWTACACS 报文使用的源地址(HWTACACS 视图)	undo nas-ip
配置 NAS 发送 HWTACACS 报文使用的源地址（系统视图）	hwtacacs nas-ip <i>ip-address</i>
取消 NAS 发送 HWTACACS 报文使用的源地址（系统视图）	undo hwtacacs nas-ip

缺省情况下，不指定源地址，即以发送报文的接口地址作为源地址。

2.4.6 配置 TACACS 服务器的密钥

使用 TACACS 服务器作为 AAA 服务器时，可设置密钥以提高防火墙与 TACACS 服务器通信的安全性。

请在 HWTACACS 视图下进行下列配置。

表2-39 配置 TACACS 服务器的密钥

操作	命令
配置 TACACS 计费、授权及认证服务器的密钥	key { accounting authorization authentication } string
删除配置	undo key { accounting authorization authentication }

缺省情况下，没有密钥。

2.4.7 配置 TACACS 服务器的用户名格式

用户名通常采用“userid@isp-name”格式，“@”后面的部分为域名。

如果 TACACS 服务器不接受带域名的用户名时，可以配置将用户名的域名去除后再传送给 TACACS 服务器。

请在 HWTACACS 视图下进行下列配置。

表2-40 配置 TACACS 服务器的用户名格式

操作	命令
配置用户名带域名	user-name-format with-domain
配置用户名不带域名	user-name-format without-domain

缺省情况下，发往 TACACS 服务器的用户名带域名。

2.4.8 配置 TACACS 服务器的流量单位

请在 HWTACACS 视图下进行下列配置。

表2-41 配置 TACACS 服务器的流量单位

操作	命令
配置 TACACS 服务器的流量单位	data-flow-format data { byte giga-byte kilo-byte mega-byte } data-flow-format packet { giga-packet kilo-packet mega-packet one-packet }
恢复发送到 TACACS 服务器的数据流的单位为缺省设置	undo data-flow-format { data packet }

缺省情况下，发送数据单位为 **byte**，数据包的单位为 **one packet**。。

2.4.9 配置 TACACS 服务器的定时器

1. 配置 TACACS 服务器的应答超时时间

由于 HWTACACS 是基于 TCP 实现的，因此，服务器应答超时或 TCP 超时都可能与 TACACS 服务器的连接断开。

请在 HWTACACS 视图下进行下列配置。

表2-42 配置 TACACS 服务器应答超时时间

操作	命令
配置应答超时时间	timer response-timeout seconds
恢复缺省配置	undo timer response-timeout

缺省情况下，应答超时时间为 5 秒。

2. 配置 TACACS 服务器的主服务器恢复激活状态时间

请在 HWTACACS 视图下进行下列配置。

表2-43 配置 TACACS 服务器的主服务器恢复激活状态时间

操作	命令
配置恢复激活时间	timer quiet minutes
恢复缺省配置	undo timer quiet

缺省情况下，主服务器恢复激活状态前需要等待 5 分钟。

3. 设置实时计费时间间隔

为了对用户实施实时计费，有必要设置实时计费的时间间隔。在设置了该属性以后，每隔设定的时间，NAS 会向 TACACS 服务器发送一次在线用户的计费信息。

可以使用下面命令设置实时计费间隔。

请在 HWTACACS 视图下进行下列配置。

表2-44 设置实时计费间隔

操作	命令
设置实时计费间隔	timer realtime-accounting minutes
将实时计费间隔恢复为缺省值	undo timer realtime-accounting

其中，*minutes* 为实时计费间隔时间，单位为分钟，其取值必须为 3 的整数倍。

实时计费间隔的取值对 NAS 和 TACACS 服务器的性能有一定的相关性要求——取值越小，对 NAS 和 TACACS 服务器的性能要求越高。建议当用户量比较大(≥ 1000)时，尽量把该间隔的值设置得大一些。以下是实时计费间隔与用户量之间的推荐比例关系：

表2-45 实时计费间隔与用户量之间的推荐比例关系

用户数	实时计费间隔（分钟）
1~99	3
100~499	6
500~999	12
≥ 1000	≥ 15

缺省情况下，实时计费间隔为 12 分钟。

2.5 TACACS 支持 super 认证配置

当用户以较低权限登录到防火墙上时，用户可以通过 **super level** 命令来获取更高的权限。

在进行权限级别切换时，可以通过 **super-password** 来进行认证，对于某一个级别，所有用户都是使用同一个密码，这种认证方式不够灵活且安全性不高。TACACS 支持 **super** 认证增加了 TACACS 认证，即在 TACACS 服务器上配置用户名和 **super** 密码，大大提高了设置管理的灵活性和安全性。

2.5.1 Super 认证切换权限处理过程

系统允许在每个用户界面视图下配置 **super** 认证方式。支持四种认证方式：

- **super-password**
- **scheme**
- **super-password + scheme**
- **scheme + super-password**

当用户登录到设备以后，如果用户想获得其它的权限，可以通过 **super level** 命令来改变当前用户的权限。

系统对此命令的处理有以下几种情况：

1. 用户申请的权限不大于当前权限

这种情况下，用户将直接获得申请的权限，不需要通过认证。

2. 用户申请的权限大于当前权限

这种情况下，系统的处理过程由当前用户接口下配置的 **super** 认证方式决定。

(1) 认证方式为 **super-password**

我们可以为每一个权限级别设置一个 **super-password**

- 如果对应当前用户申请的级别设置了该密码，则系统提示输入密码，如果密码输入正确，用户获得申请的权限，否则提示用户认证失败。
- 如果对应当前用户申请的级别没有设置密码，则用户将不能获得该权限。



注意：

没有设置对应级别 **super-password** 的情况下，系统处理过程与以前不同，以前在这种情况下，**console** 口用户可以直接获得该权限，其他用户不可以直接获得权限，现在所有用户都不能获得该权限！

(2) 认证方式为 **scheme**

- 如果用户登录时采用的是 **AAA** 认证方式，即登录时需输入用户名和密码，则在执行 **super level** 命令后，系统提示输入密码，然后将当前用户名和用户输入的 **super** 密码发送到 **TACACS** 服务器上认证。如果认证通过，用户获得相应权限，否则提示认证失败。
- 如果用户登录时采用的是 **none** 或者 **password** 方式，即登录时无须输入用户名。在执行 **super level** 命令后，系统提示输入用户名和 **super** 密码，然后将用户输入的用户名和密码发送到 **TACACS** 服务器上认证。如果认证通过，用户获得相应权限，否则提示认证失败。

(3) 认证方式为 **scheme + super-password**

这种情况下，系统优先采用 **scheme** 认证方式，如果此时 **scheme** 中配置的 **TACACS** 服务器不可达或者域中没有配置认证方案，将采用 **super-password** 认证方式。

(4) 认证方式为 **super-password + scheme**

这种情况下，系统优先采用 **super-password** 认证方式，如果没有设置相应级别的 **super-password**，则采用 **scheme** 认证方式。

2.5.2 设置 **super** 认证方式

请在用户界面视图下进行下列配置。

表2-46 设置 super 认证方式

操作	命令
设置 super 认证方式	super authentication-mode { super-password scheme }*
恢复 super 认证方式为缺省值	undo super authentication-mode

缺省情况下，super 认证方式为 super-password。

2.5.3 设置 super 认证方案

系统支持为每个域配置一个 super 认证方案，该方案只能是 HWTACACS 方案，不可以设置为 RADIUS 或者 local 方案。当某个 HWTACACS 方案被一个域的 super 认证方案引用时，该方案不可以被删除。若没有指定或指定的方案不存在，TACACS 认证将失败。

请在 ISP 域视图下进行下列配置。

表2-47 设置 super 认证方案

操作	命令
设置 super 认证方案	authentication super hwtacacs-scheme <i>hwtacacs-scheme-name</i>
取消 super 认证方案的配置	undo authentication super

缺省情况下，未配置 super 认证方案。

2.6 AAA 及 RADIUS/HWTACACS 协议的显示和调试

完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 AAA、RADIUS/HWTACACS 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可清除相关配置。

在用户视图下，执行 **debugging** 命令可进行调试。

表2-48 AAA 协议的显示和调试

操作	命令
显示所有或指定 ISP 域的配置信息	display domain [<i>isp-name</i>]
显示用户连接的相关信息	display connection [domain <i>isp-name</i> ip <i>ip-address</i> mac <i>mac-address</i> radius-scheme <i>radius-scheme-name</i> hwtacacs-scheme <i>hwtacacs-scheme-name</i> ucibindex <i>ucib-index</i> user-name <i>user-name</i>]

操作	命令
显示本地用户的相关信息	display local-user [domain <i>isp-name</i> service-type { dvpn telnet ssh terminal ftp ppp } state { active block } user-name <i>user-name</i>]

表2-49 RADIUS 协议的显示和调试

操作	命令
显示所有或指定 RADIUS 方案的配置信息	display radius scheme [<i>radius-scheme-name</i>]
显示 RADIUS 报文的统计信息	display radius statistics
显示缓存的没有得到响应的停止计费请求报文	display stop-accounting-buffer { radius-scheme <i>radius-scheme-name</i> session-id <i>session-id</i> time-range <i>start-time stop-time</i> user-name <i>user-name</i> }
显示本地 RADIUS 认证服务器的统计信息	display local-server statistics
打开 RADIUS 报文调试开关	debugging radius packet
关闭 RADIUS 报文调试开关	undo debugging radius packet
打开本地 RADIUS 认证服务器的调试开关	debugging local-server { all error event packet }
关闭本地 RADIUS 认证服务器的调试开关	undo debugging local-server { all error event packet }
删除那些缓存的、没有得到响应的停止计费请求报文	reset stop-accounting-buffer { radius-scheme <i>radius-scheme-name</i> session-id <i>session-id</i> time-range <i>start-time stop-time</i> user-name <i>user-name</i> }
清除 RADIUS 服务器的统计信息	reset radius statistics

表2-50 HWTACACS 协议的显示和调试

操作	命令
显示所有或指定 HWTACACS 方案的配置信息	display hwtacacs scheme [<i>hwtacacs-scheme-name</i> [statistics]]
显示缓存的没有得到响应的停止计费请求报文	display stop-accounting-buffer <i>hwtacacs-scheme hwtacacs-scheme-name</i>
打开 HWTACACS 协议调试开关	debugging hwtacacs { all error event message receive-packet send-packet }
关闭 HWTACACS 协议调试开关	undo debugging hwtacacs { all error event message receive-packet send-packet }
删除那些在防火墙上缓存的、没有得到响应的停止计费请求报文	reset stop-accounting-buffer <i>hwtacacs-scheme hwtacacs-scheme-name</i>

操作	命令
清除 TACACS 服务器的统计信息	reset hwtacacs statistics { accounting authentication authorization all }

2.7 AAA 及 RADIUS/HWTACACS 协议典型配置举例

2.7.1 Telnet/SSH 用户通过 RADIUS 服务器认证、计费的应用

说明：

SSH/Telnet 用户通过 RADIUS 服务器认证的配置方法类似，下面的描述以 Telnet 用户的远端认证为例。

1. 组网需求

如下图所示的环境中，现需要通过配置防火墙实现 RADIUS 服务器对登录防火墙的 Telnet 用户进行认证、计费。

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）与防火墙相连，服务器 IP 地址为 10.110.91.146，设置防火墙与认证 RADIUS 服务器交互报文时的共享密钥为“expert”、与计费 RADIUS 服务器交互报文时的共享密钥为“expert”。

RADIUS 服务器可使用 CAMS 服务器。使用第三方 RADIUS 服务器时，RADIUS 方案中的 server-type 可以选择 standard 类型或 extended 类型；使用 CAMS 服务器时，RADIUS 方案中的 server-type 应选择 extended 类型。在 RADIUS 服务器上设置与防火墙交互报文时的共享密钥为“expert”；设置验证及计费的端口号；添加 Telnet 用户名及登录密码。如果 RADIUS 方案中设置防火墙不从用户名中去除用户名而是一起传给 RADIUS 服务器，RADIUS 服务器上添加的 Telnet 用户名应为“userid@isp-name”形式。

2. 组网图

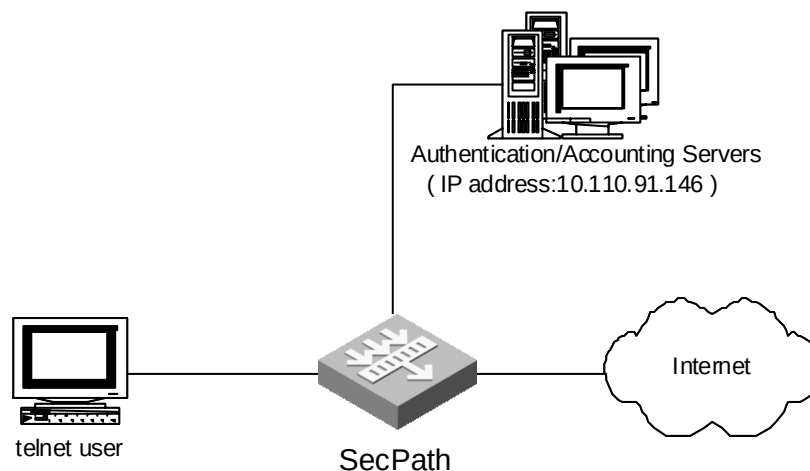


图2-7 配置 Telnet 用户的远端 RADIUS 认证

3. 配置步骤

配置 Telnet 用户采用 AAA 认证方式。

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] authentication-mode scheme
```

配置 domain。

```
[H3C] domain cams
[H3C-isp-cams] access-limit enable 10
[H3C-isp-cams] accounting optional
[H3C-isp-cams] quit
```

配置 RADIUS 方案。

```
[H3C] radius scheme cams
[H3C-radius-cams] primary authentication 10.110.91.146 1812
[H3C-radius-cams] primary accounting 10.110.91.146 1813
[H3C-radius-cams] key authentication expert
[H3C-radius-cams] key accounting expert
[H3C-radius-cams] server-type extended
[H3C-radius-cams] user-name-format with-domain
[H3C-radius-cams] quit
```

配置 domain 和 RADIUS 的关联。

```
[H3C] domain cams
[H3C-isp-cams] scheme radius-scheme cams
```

Telnet 用户登录时输入用户名 **userid@cams**，以使用 **cams** 域进行认证。

2.7.2 FTP/Telnet 用户本地认证配置

说明：

FTP 用户与 Telnet 用户通过本地认证的配置方法类似, 下面描述仅以 Telnet 用户为例。

1. 组网需求

如下图所示的环境中, 现需要通过配置防火墙实现对登录防火墙的 Telnet 用户进行本地认证。

2. 组网图

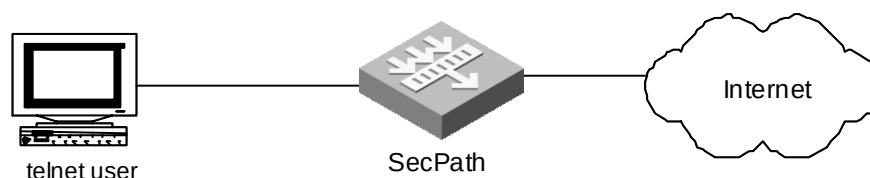


图2-8 配置 Telnet 用户的本地认证

3. 配置步骤

配置 Telnet 用户采用 AAA 认证方式。

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] authentication-mode scheme
```

创建本地用户 telnet。

```
[H3C] local-user telnet
[H3C-luser-telnet] service-type telnet
[H3C-luser-telnet] password simple pwd
[H3C] domain system
[H3C-isp-system] scheme local
```

使用 Telnet 登陆时输入用户名为 *userid@system*, 以使用 *system* 域进行认证。

2.7.3 PPP 用户通过 TACACS 服务器认证、授权、计费的应用

1. 组网需求

如下图所示的环境中, 现需要通过配置防火墙实现 TACACS 服务器对登录防火墙的 PPP 用户分配 IP 地址, 并进行认证、授权、计费。

一台 TACACS 服务器（其担当认证、授权、计费服务器的职责）与防火墙相连, 服务器 IP 地址为 10.110.91.146, 设置防火墙与认证、授权、计费 TACACS 服务器交

互报文时的共享密钥均为“expert”，设置防火墙除去用户名中的域名后再将之传给 TACACS 服务器。

在 TACACS 服务器上设置与防火墙交互报文时的共享密钥为“expert”；添加 PPP 用户名及密码。

2. 组网图

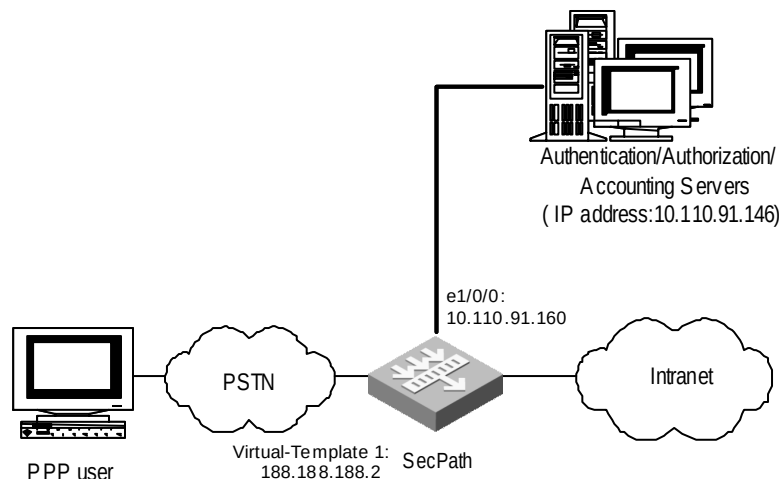


图2-9 配置 PPP 用户的远端 HWTACACS 认证

3. 配置步骤

配置 HWTACACS 方案。

```
[H3C] hwtacacs scheme hwtac
[H3C-hwtacacs-hwtac] primary authentication 10.110.91.146 49
[H3C-hwtacacs-hwtac] primary authorization 10.110.91.146 49
[H3C-hwtacacs-hwtac] primary accounting 10.110.91.146 49
[H3C-hwtacacs-hwtac] key authentication expert
[H3C-hwtacacs-hwtac] key authorization expert
[H3C-hwtacacs-hwtac] key accounting expert
[H3C-hwtacacs-hwtac] user-name-format without-domain
[H3C-hwtacacs-hwtac] quit
```

配置 domain 和 hwtacacs 的关联。

```
[H3C] domain hwtacacs
[H3C-isp-hwtacacs] scheme hwtacacs-scheme hwtac
[H3C-isp-hwtacacs] ip pool 1 200.1.1.1 200.1.1.99
[H3C-isp-hwtacacs] quit
```

配置防火墙上的虚拟模板参数。

```
[H3C] interface virtual-template 1
[H3C-Virtual-Template1] ppp authentication-mode pap domain hwtacacs
```

```
[H3C-Virtual-Template1] ip address 188.188.188.2 255.255.255.0
[H3C-Virtual-Template1] remote address pool 1
[H3C-Virtual-Template1] quit
```

配置以太网口。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 10.110.91.160 255.255.255.0
```

2.7.4 Telnet 用户通过 TACACS 服务器认证（一次性认证）、计费的应用

1. 组网需求

如下图所示的环境中，现需要通过配置防火墙实现 TACACS 服务器对登录防火墙的 Telnet 用户进行一次性认证、计费。

一台 TACACS 服务器（其担当认证、授权和计费 TACACS 服务器的职责）与防火墙相连，服务器 IP 地址为 10.110.91.146，设置防火墙与认证、授权和计费 TACACS 服务器交互报文时的共享密钥为“expert”。TACACS 服务器提供一次性口令认证功能，防火墙不从用户名中去除用户域名而是一起传给 TACACS 服务器，故 TACACS 服务器上添加的 Telnet 用户名应为“test@tacacs”。

2. 组网图

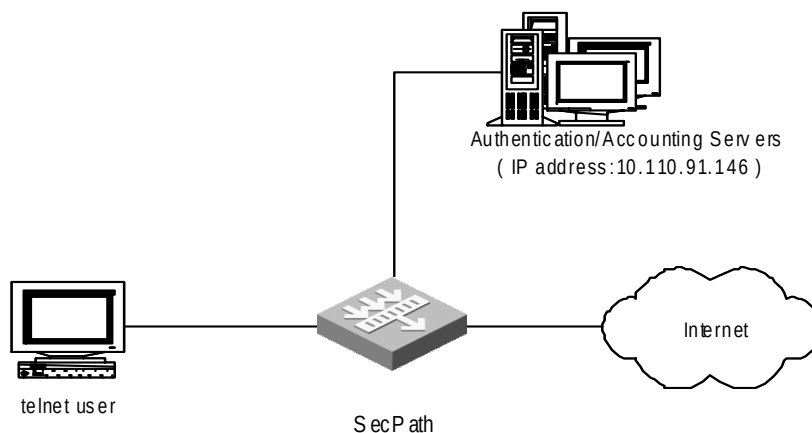


图2-10 配置 Telnet 用户的远端 TACACS 认证

3. 配置步骤

(1) 配置防火墙

配置 Telnet 用户采用 AAA 认证方式。

```
[H3C] user-interface vty0 4
[H3C-ui-vty0-4] authentication-mode scheme
```

配置 domain。

```
[H3C] domain tacacs
```

```
[H3C-isp-tacacs] access-limit enable 10
[H3C-isp-tacacs] accounting optional
[H3C-isp-tacacs] quit

# 配置 TACACS 方案。

[H3C] hwtacacs scheme system
[H3C-hwtacacs-system] primary authentication 10.110.91.146
[H3C-hwtacacs-system] primary authorization 10.110.91.146
[H3C-hwtacacs-system] primary accounting 10.110.91.146
[H3C-hwtacacs-system] key authentication expert
[H3C-hwtacacs-system] key authorization expert
[H3C-hwtacacs-system] key accounting expert
[H3C-hwtacacs-system] user-name-format with-domain
[H3C-hwtacacs-system] quit

# 配置 domain 和 HWTACACS 方案的关联。

[H3C] domain tacacs
[H3C-isp-tacacs] scheme hwtacacs-scheme system
```

(2) 配置 TACACS 服务器

- 配置 IP 地址
- 配置共享密钥
- 添加 Telnet 用户名 test@tacacs
- 启动一次性认证

(3) 登录过程

Telnet 一次性认证用户登录过程如下。

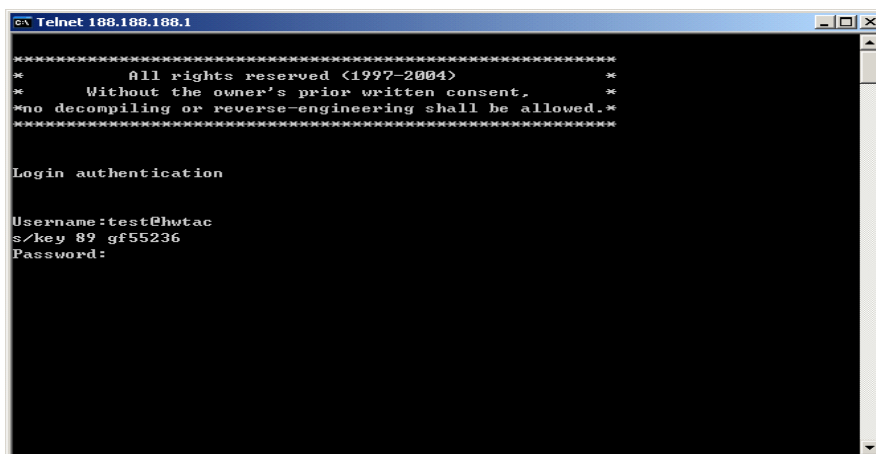


图2-11 Telnet 用户登录界面

第一步：输入用户名 test@tacacs；

第二步：根据登录界面上的提示信息“s/key 89 gf55236”，利用 winkey.exe 计算器计算登录密码；

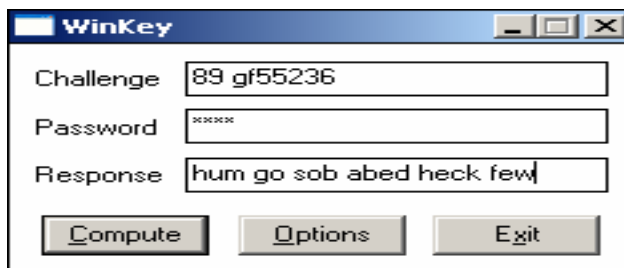


图2-12 计算登录密码

图中：

Challenge: 框输入服务器返回的提示信息“89 gf55236”；

Password: 输入用户的私有密码，例如“test”；

Response: 输出的计算结果，也就是要在登录界面上输入的密码。

第三步：在登录界面上输入计算得到的密码，即可通过认证。

2.8 AAA 及 RADIUS/HWTACACS 协议故障的诊断与排除

2.8.1 RADIUS 协议故障诊断与排除

RADIUS 协议在 TCP/IP 协议族中处于应用层，它主要规定 NAS 与 ISP 的 RADIUS 服务器间如何交互用户信息，因此它失效的可能性比较大。

- 故障之一：用户认证/授权总是失败

故障排除：

- (1) 用户名不是“userid@isp-name”的形式，或 NAS 没有指定缺省的 ISP 域——请使用正确形式的用户名或在 NAS 中设定缺省的 ISP 域。
- (2) RADIUS 服务器的数据库中没有配置该用户——检查 RADIUS 服务器的数据库以保证该用户的配置信息确实存在。
- (3) 用户侧输入的密码不正确——请保证接入用户输入正确的密码。
- (4) RADIUS 服务器和 NAS 的报文共享密钥不同——请仔细比较两端的共享密钥，确保它们相同。
- (5) NAS 与 RADIUS 服务器之间存在通信故障（可以通过在 NAS 上 ping RADIUS 服务器来检查）——请保证 NAS 与 RADIUS 服务器之间能够正常通信。

- 故障之二：RADIUS 报文无法传送到 RADIUS 服务器

故障排除：

- (1) NAS 与 RADIUS 服务器之间的通信线路不通（物理层/链路层）——请保证线路通畅。

- (2) NAS 上没有设置相应的 RADIUS 服务器 IP 地址——请保证正确设置 RADIUS 服务器的 IP 地址。
- (3) 认证/授权和计费服务的 UDP 端口设置得不正确——请保证与 RADIUS 服务器提供的端口号一致。
- 故障之三：用户认证通过并获得授权，但是不能向 RADIUS 服务器传送计费话单。

故障排除：

- (1) 计费端口号设置得不正确——请正确设置 RADIUS 计费端口号。
- (2) 计费服务器和认证/授权服务器不是同一台机器，NAS 却要求认证/授权和计费在同一个服务器（IP 地址相同）——请保证 NAS 的认证/授权和计费服务器的设置与实际情况相同。

2.8.2 HWTACACS 协议故障诊断与排除

HWTACACS 的故障现象与 RADIUS 基本相似，可以参考上面内容。

第3章 访问控制列表配置

3.1 访问控制列表简介

3.1.1 访问控制列表概述

防火墙为了过滤数据包，需要配置一系列的规则，以决定什么样的数据包能够通过，这些规则就是通过访问控制列表 ACL（Access Control List）定义的。访问控制列表是由 **permit** 和 **deny** 语句组成的一系列有顺序的规则，这些规则根据数据包的源地址、目的地址、端口号等来描述。ACL 通过这些规则对数据包进行分类，这些规则应用到防火墙接口上，防火墙根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。

3.1.2 访问控制列表的分类

按照访问控制列表的用途，可以分为四类：

- 基本的访问控制列表（basic acl）
- 高级的访问控制列表（advanced acl）
- 基于接口的访问控制列表（interface-based acl）
- 基于 MAC 的访问控制列表（mac-based acl）

访问控制列表的使用用途是依靠数字的范围来指定的，1000～1999 是基于接口的访问控制列表，2000～2999 范围的访问控制列表是基本的访问控制列表，3000～3999 范围的访问控制列表是高级的访问控制列表，4000～4999 范围的访问控制列表是基于 MAC 地址访问控制列表。

3.1.3 访问控制列表的匹配顺序

一个访问控制列表可以由多条“**permit** 和 **deny**”语句组成，每一条语句描述的规则是不同的，这些规则可能存在重复或矛盾的地方，在将一个数据包和访问控制列表的规则进行匹配的时候，到底采用哪些规则呢？就需要确定规则的匹配顺序。

有两种匹配顺序：

- 配置顺序
- 自动排序

配置顺序，是指按照用户配置 ACL 的规则的先后进行匹配。

自动排序使用“深度优先”的原则。

“深度优先”规则是把指定数据包范围最小的语句排在最前面。这一点可以通过比较地址的通配符来实现，通配符越小，则指定的主机的范围就越小。比如 129.102.1.1 0.0.0.0 指定了一台主机：129.102.1.1，而 129.102.1.1 0.0.255.255 则指定了一个网段：129.102.1.1～129.102.255.255，显然前者在访问控制规则中排在前面。具体标准为：对于基本访问控制规则的语句，直接比较源地址通配符，通配符相同的则按配置顺序；对于基于接口的访问控制规则，配置了“any”的规则排在后面，其它按配置顺序；对于高级访问控制规则，首先比较源地址通配符，相同的再比较目的地址通配符，仍相同的则比较端口号的范围，范围小的排在前面，如果端口号范围也相同则按配置顺序。

使用 **display acl** 命令就可以看出是哪条规则首先生效。显示时，列在前面的规则首先生效。

3.1.4 访问控制列表的创建

一个访问控制列表是由 **permit** 和 **deny** 语句组成的一系列的规则列表，若干个规则列表构成一个访问控制列表。在配置访问控制列表的规则之前，首先需要创建一个访问控制列表。

可以使用如下命令创建一个访问控制列表：

```
acl number acl-number [ match-order { config | auto } ]
```

使用如下的命令删除一个或所有的访问控制列表：

```
undo acl { number acl-number | all }
```

参数说明：

- **number** *acl-number*：定义一个 ACL。
- *acl-number*：访问控制规则序号。1000～1999 是基于接口的访问控制列表，2000～2999 范围的访问控制列表是基本的访问控制列表，3000～3999 范围的访问控制列表是高级的访问控制列表，4000～4999 是基于 MAC 地址的访问控制列表。
- **match-order config**：指定匹配该规则时按用户的配置顺序。
- **match-order auto**：指定匹配该规则时系统自动排序，即按“深度优先”的顺序。
- **all**：删除所有配置的 ACL。

缺省情况下匹配顺序为按用户的配置排序，即“**config**”。用户一旦指定某一条访问控制列表的匹配顺序，就不能再更改该顺序，除非把该 ACL 的内容全部删除，再重新指定其匹配顺序。

创建了一个访问控制列表之后，将进入 ACL 视图，ACL 视图是按照访问控制列表的用途来分类的，例如创建了一个编号为 3000 的 ACL，将进入高级 ACL 视图，防火墙的提示符如下所示：

[H3C-acl-adv-3000]

进入了 ACL 视图之后，就可以配置 ACL 的规则了。对于不同的 ACL，其规则是不一样的，具体的各种 ACL 的规则的配置方法将在后面小节分别介绍。

3.1.5 基本访问控制列表

基本访问控制列表只能使用源地址信息，做为定义访问控制列表的规则的元素。通过上面小节介绍的 **acl** 命令，可以创建一个基本的访问控制列表，同时进入基本访问控制列表视图，在基本访问控制列表视图下，可以创建基本访问控制列表的规则。

可以使用如下的命令定义一个基本访问控制列表的规则：

```
rule [ rule-id ] { permit | deny } [ source { sour-addr sour-wildcard | any } ]  
[ time-range time-name ] [ logging ] [ fragment ] [ vpn-instance  
vpn-instance-name ]
```

参数说明：

- **rule-id**: 可选参数，ACL 规则编号，范围为 0~65534。当指定了编号，如果与编号对应的 ACL 规则已经存在，则会部分覆盖旧的规则，相当于编辑一个已经存在的 ACL 规则。故建议用户当编辑一个已存在编号的规则时，先将旧的规则删除，再创建新的规则，否则配置结果可能与预期的效果不同。如果与编号对应的 ACL 规则不存在，则使用指定的编号创建一个新的规则。如果不指定编号，表示增加一个新规则，系统自动会为这个 ACL 规则分配一个编号，并增加新规则。
- **permit**: 允许符合条件的数据包。
- **deny**: 丢弃符合条件的数据包。
- **source**: 可选参数，指定 ACL 规则的源地址信息。如果不指定，表示报文的任何源地址都匹配。
- **sour-addr**: 数据包的源地址，点分十进制表示。
- **sour-wildcard**: 源地址通配符，点分十进制表示。
- **any**: 表示所有源地址，作用与源地址是 0.0.0.0，通配符是 255.255.255.255 相同。
- **time-range**: 可选参数，指定访问控制列表的生效时间。
- **time-name**: 访问控制列表生效的时间段名字。
- **logging**: 可选参数，是否对符合条件的数据包做日志。日志内容包括访问控制规则的序号，数据包允许或被丢弃，数据包的数目。目前支持此选项的业务只有包过滤防火墙（在接口下被 **firewall packet-filter** 命令引用）。
- **fragment**: 可选参数，指定该规则是否仅对非首片分片报文有效。当包含此参数时表示该规则仅对非首片分片报文有效。

- **vpn-instance vpn-instance-name:** 可选参数，指定报文是属于哪个 VPN 实例的。如果没有指定，该规则对所有 VPN 实例中的报文都有效；如果指定了，则表示该规则仅仅对指定的 VPN 实例中的报文有效。

对已经存在的 ACL 规则，如果采用指定 ACL 规则编号的方式进行编辑，没有配置的部分是不受影响的。例如：

先配置了一个 ACL 规则：

```
rule 1 deny source 1.1.1.1 0
```

然后再对这个 ACL 规则进行编辑：

```
rule 1 deny logging
```

这个时候，ACL 的规则则变成：

```
rule 1 deny source 1.1.1.1 0 logging
```

可以使用如下命令删除一个基本访问控制列表的规则：

```
undo rule rule-id [ source ] [ time-range ] [ logging ] [ fragment ] [ vpn-instance ]
```

参数说明：

- **rule-id:** ACL 规则编号，必须是一个已经存在的 ACL 规则编号。如果后面不指定参数，则将这个 ACL 规则完全删除。否则只是删除对应 ACL 规则的部分信息。
- **source:** 可选参数，仅仅删除编号对应的 ACL 规则的源地址部分的信息设置。
- **time-range:** 可选参数，仅仅删除编号对应的 ACL 规则在规定时间内生效的设置。
- **logging:** 可选参数，仅仅删除编号对应的 ACL 规则对符合条件的数据包做日志的设置。
- **fragment:** 可选参数，仅仅删除编号对应的 ACL 规则仅对非首片分片报文有效的设置。
- **vpn-instance:** 可选参数，仅仅删除编号对应的 ACL 规则中关于 VPN 实例的设置。

3.1.6 高级访问控制列表

高级访问控制列表可以使用数据包的源地址信息、目的地址信息、IP 承载的协议类型、针对协议的特性，例如 TCP 的源端口、目的端口，ICMP 协议的类型、代码等内容定义规则。可以利用高级访问控制列表定义比基本访问控制列表更准确、更丰富、更灵活的规则。

通过前面小节介绍的 **acl** 命令，可以创建一个高级的访问控制列表，同时进入高级访问控制列表视图，在高级访问控制列表视图下，可以创建高级访问控制列表的规则。

可以使用如下的命令定义一个高级访问控制列表规则：

```
rule [ rule-id ] { permit | deny } protocol [ source { sour-addr sour-wildcard | any } ]  
[ destination { dest-addr dest-wildcard | any } ] [ soucre-port operator port1  
[ port2 ] ] [ destination-port operator port1 [ port2 ] ] [ icmp-type { icmp-message |  
icmp-type icmp-code } ] [ dscp dscp ] [ established ] [ precedence precedence ]  
[ tos tos ] [ time-range time-name ] [ logging ] [ fragment ] [ vpn-instance  
vpn-instance-name ]
```

参数说明：

- **rule-id**: 可选参数，ACL 规则编号，范围为 0~65534。当指定了编号，如果与编号对应的 ACL 规则已经存在，则会部分覆盖旧的规则，相当于编辑一个已经存在的 ACL 规则。故建议用户当编辑一个已存在编号的规则时，先将旧的规则删除，再创建新的规则，否则配置结果可能与预期的效果不同。如果与编号对应的 ACL 规则不存在，则使用指定的编号创建一个新的规则。如果不指定编号，表示增加一个新规则，系统自动会为这个 ACL 规则分配一个编号。
- **deny**: 拒绝符合条件的数据包。
- **permit**: 允许符合条件的数据包。
- **protocol**: 用名字或数字表示的 IP 承载的协议类型。数字范围为 1~255；名称取值范围为：gre、icmp、igmp、ip、ipinip、ospf、tcp、udp。
- **source**: 可选参数，指定 ACL 规则的源地址信息。如果不配置，表示报文的任何源地址都匹配。
- **sour-addr**: 数据包的源地址，点分十进制表示。
- **sour-wildcard**: 源地址通配符，点分十进制表示。
- **destination**: 可选参数，指定 ACL 规则的目的地址信息。如果不配置，表示报文的任何目的地址都匹配。
- **dest-addr**: 数据包的目的地址，点分十进制表示。
- **dest-wildcard**: 目的地址通配符，点分十进制表示。
- **any**: 表示所有源地址或目的地址，作用与源或目的地址是 0.0.0.0，通配符是 255.255.255.255 相同。
- **icmp-type**: 可选参数，指定 ICMP 报文的类型和消息码信息，仅仅在报文协议是 ICMP 的情况下有效。如果不配置，表示任何 ICMP 类型的报文都匹配。
- **icmp-type**: ICMP 包可以依据 ICMP 的消息类型进行过滤。取值为 0~255 的数字。

- **icmp-code:** 依据 ICMP 的消息类型进行过滤的 ICMP 包也可以依据消息码进行过滤。取值为 0~255 的数字。
- **icmp-message:** ICMP 包可以依据 ICMP 消息类型名称或 ICMP 消息类型和码的名称进行过滤。
- **source-port:** 可选参数，指定 UDP 或者 TCP 报文的源端口信息，仅仅在规则指定的协议号是 TCP 或者 UDP 有效。如果不指定，表示 TCP/UDP 报文的任何源端口信息都匹配。
- **destination-port:** 可选参数，指定 UDP 或者 TCP 报文的端口信息，仅仅在规则指定的协议号是 TCP 或者 UDP 有效。如果不指定，表示 TCP/UDP 报文的任何目的端口信息都匹配。
- **operator:** 可选参数。比较源或者目的地址的端口号的操作符，名字及意义如下：lt（小于），gt（大于），eq（等于），neq（不等于），range（在范围内）。只有 range 需要两个端口号做操作数，其他的只需要一个端口号做操作数。
- **port1, port2:** 可选参数。TCP 或 UDP 的端口号，用名称或数字表示，数字的取值范围为 0~65535。
- **dscp dscp:** 指定 DSCP 字段（IP 报文中的 DS 字节）。此参数与 **precedence**、**tos** 互斥。
- **established:** 匹配所有标志为 ACK 或 RST 的 TCP 报文。包括 SYN+ACK、ACK、FIN+ACK、RST、RST+ACK 等几种报文。使用此选项时，建议关闭快速转发功能，有关快速转发的描述请参见本手册的“网络层协议”部分。
- **precedence:** 可选参数，数据包可以依据优先级字段进行过滤。取值为 0~7 的数字或名称。此参数与 **dscp** 互斥。
- **tos tos:** 可选参数，数据包可以依据服务类型字段进行过滤。取值为 0~15 的数字或名称。此参数与 **dscp** 互斥。

该 ToS 值为 ToS 字段中的第四位到第七位（从左向右数）的 4 个比特，取值范围为 0~15（如下面所示），而实际表示的值为 0~30。

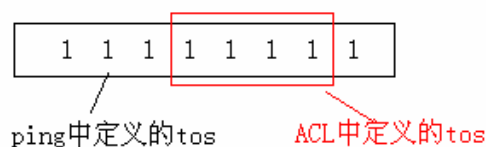


图3-1 ACL 中 ToS 参数的含义

所以，当我们在 ACL 中配置了 ToS 值（如配置为 1），然后在 ping 命令应用-tos 时，必须对其值增大 2 倍（即必须配置为 2），这样才能够通过 ping 命令测试在 ACL 中配置的 ToS 的结果。

- **logging**: 可选参数，是否对符合条件的数据包做日志。日志内容包括访问控制列表规则的序号，数据包允许或被丢弃，IP 承载的上层协议类型，源/目的地址，源/目的端口号，数据包的数目。目前支持此选项的业务只有包过滤防火墙（在接口下被 **firewall packet-filter** 命令引用）。
- **time-range time-name**: 配置这条访问控制规则生效的时间段。
- **fragment**: 指定该规则是否仅对非首片分片报文有效。当包含此参数时表示该规则仅对非首片分片报文有效。
- **vpn-instance vpn-instance-name**: 可选参数，指定报文是属于哪个 VPN 实例的。如果没有指定，该规则对所有 VPN 实例中的报文都有效；如果指定了，则表示该规则仅仅对指定的 VPN 实例中的报文有效。

对已经存在的 ACL 规则，如果采用指定 ACL 规则编号的方式进行编辑，没有配置的部分是不受影响的。例如：

先配置了一个 ACL 规则：

```
rule 1 deny ip source 1.1.1.1 0
```

然后再对这个 ACL 规则进行编辑：

```
rule 1 deny ip destination 2.2.2.1 0
```

这个时候，ACL 的规则则变成：

```
rule 1 deny ip source 1.1.1.1 0 destination 2.2.2.1 0
```

可以使用如下命令删除一个高级访问控制列表的规则：

```
undo rule rule-id [ source ] [ destination ] [ source-port ] [ destination-port ]  
[ icmp-type ] [ dscp ] [ precedence ] [ tos ] [ time-range ] [ logging ] [ fragment ]  
[ vpn-instance ]
```

参数说明：

- **rule-id**: ACL 规则编号，必须是一个已经存在的 ACL 规则编号。如果后面不指定参数，则将这个 ACL 规则完全删除。否则只是删除对应 ACL 规则的部分信息。
- **source**: 可选参数，仅仅删除编号对应的 ACL 规则的源地址部分的信息设置。
- **destination**: 可选参数，仅仅删除编号对应的 ACL 规则的目的地地址部分的信息设置。
- **source-port**: 可选参数，仅仅删除编号对应的 ACL 规则的源端口部分的信息设置，仅仅在规则的协议号是 TCP 或者 UDP 的情况下有效。

- **destination-port:** 可选参数，仅仅删除编号对应的 ACL 规则的目的端口部分的信息设置，仅仅在规则的协议号是 TCP 或者 UDP 的情况下有效。
- **icmp-type:** 可选参数，仅仅删除编号对应的 ACL 规则 ICMP 类型和消息码部分的信息设置，仅仅在规则的协议号是 ICMP 的情况下有效。
- **dscp:** 可选参数，仅仅删除编号对应的 ACL 规则的 DSCP 字段的相关设置。
- **precedence:** 可选参数，仅仅删除编号对应的 ACL 规则的 precedence 的相关设置。
- **tos:** 可选参数，仅仅删除编号对应的 ACL 规则的 tos 的相关设置。
- **time-range:** 可选参数，仅仅删除编号对应的 ACL 规则在规定时间生效的设置。
- **logging:** 可选参数，仅仅删除编号对应的 ACL 规则对符合条件的数据包做日志的设置。
- **fragment:** 可选参数，仅仅删除编号对应的 ACL 规则仅对非首片分片报文有效的设置。
- **vpn-instance:** 可选参数，仅仅删除编号对应的 ACL 规则中关于 VPN 实例的设置。

只有 TCP 和 UDP 协议需要指定端口范围。支持的操作符及其语法如下表。

表3-1 高级访问控制列表的操作符意义

操作符及语法	意义
eq portnumber	等于端口号 portnumber
gt portnumber	大于端口号 portnumber
lt portnumber	小于端口号 portnumber
neq portnumber	不等于端口号 portnumber
range portnumber1 portnumber2	介于端口号 portnumber1 和 portnumber2 之间

在指定 *portnumber* 时，对于部分常见的端口号，可以用相应的助记符来代替其实际数字，支持的助记符如下表。

表3-2 端口号助记符

协议	助记符	意义及实际值
TCP	Bgp	Border Gateway Protocol (179)
	Chargen	Character generator (19)
	Cmd	Remote commands (rcmd, 514)
	Daytime	Daytime (13)
	Discard	Discard (9)
	Domain	Domain Name Service (53)
	Echo	Echo (7)
	Exec	Exec (rsh, 512)
	Finger	Finger (79)
	Ftp	File Transfer Protocol (21)
	Ftp-data	FTP data connections (20)
	Gopher	Gopher (70)
	Hostname	NIC hostname server (101)
	Irc	Internet Relay Chat (194)
	Klogin	Kerberos login (543)
	Kshell	Kerberos shell (544)
	Login	Login (rlogin, 513)
	Lpd	Printer service (515)
	Nntp	Network News Transport Protocol (119)
	Pop2	Post Office Protocol v2 (109)
	Pop3	Post Office Protocol v3 (110)
	Smtpt	Simple Mail Transport Protocol (25)
	Sunrpc	Sun Remote Procedure Call (111)
	Syslog	Syslog (514)
	Tacacs	TAC Access Control System (49)
	Talk	Talk (517)
	Telnet	Telnet (23)
	Time	Time (37)
	Uucp	Unix-to-Unix Copy Program (540)
	Whois	Nickname (43)
	Www	World Wide Web (HTTP, 80)

协议	助记符	意义及实际值
UDP	biff	Mail notify (512)
	bootpc	Bootstrap Protocol Client (68)
	bootps	Bootstrap Protocol Server (67)
	discard	Discard (9)
	dns	Domain Name Service (53)
	dnsix	DNSIX Securit Attribute Token Map (90)
	echo	Echo (7)
	mobilip-ag	MobileIP-Agent (434)
	mobilip-mn	MobilIP-MN (435)
	nameserver	Host Name Server (42)
	netbios-dgm	NETBIOS Datagram Service (138)
	netbios-ns	NETBIOS Name Service (137)
	netbios-ssn	NETBIOS Session Service (139)
	ntp	Network Time Protocol (123)
	rip	Routing Information Protocol (520)
	snmp	SNMP (161)
	snmptrap	SNMPTRAP (162)
	sunrpc	SUN Remote Procedure Call (111)
	syslog	Syslog (514)
	tacacs-ds	TACACS-Database Service (65)
	talk	Talk (517)
	tftp	Trivial File Transfer (69)
	time	Time (37)
	who	Who(513)
	Xdmcp	X Display Manager Control Protocol (177)

- 对于 ICMP 协议可以指定 ICMP 报文类型，缺省为全部 ICMP 报文。指定 ICMP 报文类型时，可以用数字（0～255），也可以用助记符。

表3-3 ICMP 报文类型助记符

助记符	意义
echo	Type=8, Code=0
echo-reply	Type=0, Code=0
fragmentneed-DFset	Type=3, Code=4
host-redirect	Type=5, Code=1
host-tos-redirect	Type=5, Code=3
host-unreachable	Type=3, Code=1
information-reply	Type=16, Code=0
information-request	Type=15, Code=0
net-redirect	Type=5, Code=0
net-tos-redirect	Type=5, Code=2
net-unreachable	Type=3, Code=0
parameter-problem	Type=12, Code=0
port-unreachable	Type=3, Code=3
protocol-unreachable	Type=3, Code=2
reassembly-timeout	Type=11, Code=1
source-quench	Type=4, Code=0
source-route-failed	Type=3, Code=5
timestamp-reply	Type=14, Code=0
timestamp-request	Type=13, Code=0
ttl-exceeded	Type=11, Code=0

配置举例请参考命令手册。

这样，用户通过配置防火墙，添加适当的访问规则，就可以利用包过滤来对通过防火墙的 IP 包进行检查，从而过滤掉用户不希望通过防火墙的数据包，起到保护网络安全的作用。

3.1.7 基于接口的访问控制列表

基于接口的访问控制列表，是一种特殊的访问控制列表，可以根据接收报文的接口指定规则。

通过前面小节介绍的 **acl** 命令，可以创建一个基于接口的访问控制列表，同时进入基于接口的访问控制列表视图，在基于接口的访问控制列表视图下，可以创建基于接口的访问控制列表规则。

可以使用如下的命令定义一个基于接口的访问控制列表规则：

```
rule [ rule-id ] { permit | deny } interface { interface-type interface-number | any }
[ time-range time-name ] [ logging ]
```

参数说明：

- **rule-id**: 可选参数, ACL 规则编号, 范围为 0~65534。当指定了编号, 如果与编号对应的 ACL 规则已经存在, 则会部分覆盖旧的规则, 相当于编辑一个已经存在的 ACL 规则。故建议用户当编辑一个已存在编号的规则时, 先将旧的规则删除, 再创建新的规则, 否则配置结果可能与预期的效果不同。如果与编号对应的 ACL 规则不存在, 则使用指定的编号创建一个新的规则。如果不指定编号, 表示增加一个新规则, 系统自动会为这个 ACL 规则分配一个编号, 并增加新规则。
- **deny**: 丢弃符合条件的数据包。
- **permit**: 允许符合条件的数据包。
- **interface interface-type interface-number**: 指定数据包的接口信息, 即从此接口接收到的报文进行过滤。**any** 代表所有的接口。
- **logging**: 可选参数, 是否对符合条件的数据包做日志。日志内容包括访问控制列表规则的序号, 数据包允许或被丢弃, 数据包的数目。仅当 ACL 被用作包过滤防火墙时, 系统将记录日志。
- **time-range time-name**: 配置这条访问控制规则生效的时间段。

可以使用如下的命令删除一个基于接口的访问控制列表的规则:

```
undo rule rule-id [ logging ] [ time-range ]
```

参数说明:

- **rule-id**: ACL 规则编号, 必须是一个已经存在的 ACL 规则编号。
- **logging**: 可选参数, 是否对符合条件的数据包做日志。日志内容包括访问控制列表规则的序号, 数据包允许或被丢弃, 数据包的数目。目前支持此选项的业务只有包过滤防火墙（在接口下被 **firewall packet-filter** 命令引用）。
- **time-range**: 可选参数, 指定规则在一定时间段内有效。

3.1.8 基于 MAC 地址的访问控制列表

基于以太网的 MAC 地址的访问控制列表的编号取值范围是 4000~4999。

可以使用如下的命令定义一个基于 MAC 地址的访问控制列表规则:

```
rule [ rule-id ] { deny | permit } [ type type-code type-mask | isap isap-code isap-mask ] [ source-mac sour-addr sour-mask ] [ dest-mac dest-addr dest-mask ] [ time-range time-name ] [ logging ]
```

参数说明如下:

- **rule-id** 为规则号。

- **type-code** 为一个十六进制数，格式为 xxxx，用来匹配传输报文的协议类型。**type-mask** 为协议类型的通配符。关于 **type-code** 值，请参考命令手册中的相关表格。
- **lsap-code** 为一个十六进制数，格式为 xxxx，用来匹配接口上桥接报文的封装格式，**lsap-mask** 为协议类型的通配符。
- **sour-addr** 为数据帧的源 MAC 地址，格式为 xxxx-xxxx-xxxx，用来匹配一个数据帧的源地址。**sour-mask** 为源 MAC 地址的通配符。
- **dest-addr** 为报文的目的 MAC 地址，格式为 xxxx-xxxx-xxxx，用来匹配一个数据帧的目的地址。**dest-mask** 为目的 MAC 地址的通配符。
- **time-range time-name**：配置这条访问控制规则生效的时间段。
- **logging**：可选参数，是否对符合条件的报文做日志。仅当 ACL 被用作包过滤防火墙时，系统将记录日志。目前支持此选项的业务只有包过滤防火墙（在接口下被 **firewall packet-filter** 命令引用）。

可以使用如下的命令删除一个基于 MAC 地址的访问控制列表的规则：

undo rule rule-id [time-range time-name] [logging]

参数说明：

- **rule-id**：ACL 规则编号，必须是一个已经存在的 ACL 规则编号。

3.1.9 ACL 对分片报文的支持

传统的包过滤并不处理所有 IP 报文分片，而是只对第一个（首片）分片报文进行匹配处理，后续分片一律放行。这样，网络攻击者可能构造后续的分片报文进行流量攻击，就带来了安全隐患。

Comware 平台的包过滤提供了对分片报文过滤的功能，包括：对所有的分片报文进行三层（IP 层）的匹配过滤；同时，对于包含高级信息的 ACL 规则项（例如包含 TCP/UDP 端口号，ICMP 类型），提供标准匹配和精确匹配两种匹配方式。标准匹配即三层信息的匹配，匹配将忽略三层以外的信息；精确匹配则对所有的 ACL 项条件进行匹配，这就要求防火墙必须记录首片分片报文的状态以获得完整的后续分片的匹配信息。缺省的功能方式为标准匹配方式。

在 ACL 的规则配置项中，通过关键字 **fragment** 来标识该 ACL 规则仅对非首片分片报文有效，而对非分片报文和首片分片报文则忽略此规则。而不包含此关键字的配置规则项对所有报文均有效。

例如：

```
[H3C-acl-basic-2000] rule deny source 202.101.1.0 0.0.0.255 fragment
[H3C-acl-basic-2000] rule permit source 202.101.2.0 0.0.0.255
[H3C-acl-adv-3001] rule permit ip destination 171.16.23.1 0 fragment
```

```
[H3C-acl-adv-3001] rule deny ip destination 171.16.23.2 0
```

上述规则项中，所有项对非首片分片报文均有效；第一，三项对非分片和首片分片报文是被忽略的，仅仅对非首片分片报文有效。

3.2 访问控制列表配置

访问控制列表的配置包括：

- 配置基本访问控制列表
- 配置高级访问控制列表
- 配置基于接口的访问控制列表
- 配置基于 MAC 地址的访问控制列表
- 为 ACL 添加描述
- 为 ACL 规则添加注释
- 删除访问控制列表
- 使能/关闭 ACL 计数器

3.2.1 配置基本访问控制列表

请进行下列配置。

表3-4 配置基本访问控制列表

操作	命令
在系统视图下，创建一个基本访问控制列表	acl number <i>acl-number</i> [match-order { config auto }]
在基本访问控制列表视图下，配置 ACL 规则	rule [<i>rule-id</i>] { permit deny } [source { <i>sour-addr</i> <i>sour-wildcard</i> any }] [time-range <i>time-name</i>] [logging] [fragment] [vpn-instance <i>vpn-instance-name</i>] undo rule <i>rule-id</i> [source] [time-range] [logging] [fragment] [vpn-instance]

3.2.2 配置高级访问控制列表

请进行下列配置。

表3-5 配置高级访问控制列表

操作	命令
在系统视图下，创建一个高级访问控制列表	acl number <i>acl-number</i> [match-order { config auto }]

操作	命令
在高级访问控制列表视图下，配置 ACL 规则	<pre>rule [rule-id] { permit deny } protocol [source { sour-addr sour-wildcard any }] [destination { dest-addr dest-wildcard any }] [source-port operator port1 [port2]] [destination-port operator port1 [port2]] [icmp-type { icmp-type icmp-code icmp-message }] [precedence precedence] [dscp dscp] [established] [tos tos] [time-range time-name] [logging] [fragment] [vpn-instance vpn-instance-name] undo rule rule-id [source] [destination] [source-port] [destination-port] [icmp-type] [precedence] [dscp] [tos] [time-range] [logging] [fragment] [vpn-instance]</pre>

3.2.3 配置基于接口的访问控制列表

请进行下列配置。

表3-6 配置基于接口的访问控制列表

操作	命令
在系统视图下，创建一个基于接口的访问控制列表	<pre>acl number acl-number [match-order { config auto }]</pre>
在基于接口的访问控制列表视图下，配置 ACL 规则	<pre>rule { permit deny } interface { interface-type interface-number any } [time-range time-name] [logging] undo rule rule-id [time-range] [logging]</pre>

其中，**interface type number** 指定接口，即对从此接口接收到的报文进行过滤，**any** 表示所有接口。

3.2.4 配置基于 MAC 地址的访问控制列表

请进行下列配置。

表3-7 配置基于 MAC 地址的访问控制列表

操作	命令
在系统视图下，创建一个基于 MAC 地址的访问控制列表	<pre>acl number acl-number</pre>
在基于 MAC 地址的访问控制列表视图下，配置 ACL 规则	<pre>rule [rule-id] { deny permit } [type type-code type-wildcard lsap lsap-code lsap-mask] [source-mac sour-addr sour-wildcard] [dest-mac dest-addr dest-mask] [time-range time-name] [logging] undo rule rule-id [time-range] [logging]</pre>

3.2.5 为 ACL 添加描述

用户可以为 ACL 添加描述，以便记忆所配置 ACL 的用途，这对于需要管理大量和复杂的 ACL 的用户来说，极大减少了其维护和管理复杂性。

请在 ACL 视图下进行下列配置。

表3-8 为 ACL 添加描述

操作	命令
为 ACL 添加描述	description <i>text</i>
删除 ACL 的描述	undo description

描述内容最长为 127 个字符。

3.2.6 为 ACL 规则添加注释

用户可以为特定的 ACL 规则添加注释，以便记忆所配置规则的用途，极大的减少了维护和管理复杂性。

请在 ACL 视图下进行下列配置。

表3-9 为 ACL 规则添加注释

操作	命令
为 ACL 规则添加注释	rule <i>rule-id</i> comment <i>text</i>
删除 ACL 规则的注释	undo rule <i>rule-id</i> comment

注释内容最长为 127 个字符。

3.2.7 删除访问控制列表

请在系统视图下进行下列配置。

表3-10 删除访问控制列表

操作	命令
删除访问控制列表	undo acl { number <i>acl-number</i> all }

3.2.8 使能/关闭 ACL 计数器

请在系统视图下进行下列配置。

表3-11 使能/关闭 ACL 计数器

操作	命令
使能 ACL 计数器	acl counter enable
关闭 ACL 计数器	acl counter disable

缺省情况下，使能 ACL 计数器。

3.3 时间段配置

时间段的配置包括：

- 创建一个时间段

3.3.1 创建/删除一个时间段

在同一个名字下可以配置多个时间段。

请在系统视图下进行下列配置。

表3-12 配置时间段

操作	命令
创建一个时间段	time-range <i>time-name</i> { <i>start-time to end-time days-of-the-week</i> [from <i>start-time start-date</i>] [to <i>end-time end-date</i>] from <i>start-time start-date</i> [to <i>end-time end-date</i>] to <i>end-time end-date</i> }
删除一个时间段	undo time-range <i>time-name</i> [<i>start-time to end-time days-of-the-week</i> [from <i>start-time start-date</i>] [to <i>end-time end-date</i>] from <i>start-time start-date</i> [to <i>end-time end-date</i>] to <i>end-time end-date</i>]

3.4 访问控制列表的显示与调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 ACL 和时间段的运行情况，通过查看显示信息确认配置的效果。在用户视图下执行 **reset** 命令可以清除访问规则计数器。

表3-13 访问控制列表的显示与调试

操作	命令
显示配置的访问控制列表规则	display acl { all <i>acl-number</i> }
显示时间段	display time-range { all <i>time-name</i> }
清除访问规则计数器	reset acl counter { all <i>acl-number</i> }

3.5 访问控制列表典型配置案例

请参见包过滤防火墙部分典型配置案例。

第4章 地址转换（NAT）配置

4.1 地址转换（NAT）简介

4.1.1 地址转换概述

如 RFC1631 所描述，NAT（Network Address Translation，网络地址转换）是将 IP 数据报报头中的 IP 地址转换为另一个 IP 地址的过程。在实际应用中，NAT 主要用于实现私有网络访问外部网络的功能。这种通过使用少量的公有 IP 地址代表多数的私有 IP 地址的方式将有助于减缓可用 IP 地址空间枯竭的速度。

说明：

私有地址是指内部网络或主机地址，公有地址是指在 Internet 上全球唯一的 IP 地址。RFC1918 为私有网络预留出了三个 IP 地址块，如下：

A 类：10.0.0.0 ~ 10.255.255.255

B 类：172.16.0.0 ~ 172.31.255.255

C 类：192.168.0.0 ~ 192.168.255.255

上述三个范围内的地址不会在 Internet 上被分配，因而可以不必向 ISP 或注册中心申请而在公司或企业内部自由使用。

下图描述了一个基本的 NAT 应用。

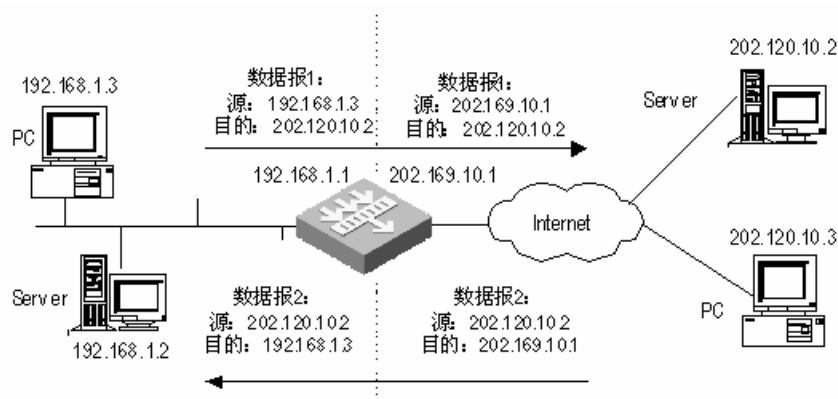


图4-1 地址转换的基本过程

NAT 服务器处于私有网络和公有网络的连接处。当内部 PC（192.168.1.3）向外部服务器（202.120.10.2）发送一个数据报 1 时，数据报将通过 NAT 服务器。NAT 进程查看报头内容，发现该数据报是发往外网的，那么它将数据报 1 的源地址字段的私有地址 192.168.1.3 换成一个可在 Internet 上选路的公有地址 202.169.10.1，并将该数据报发送到外部服务器，同时在网络地址转换表中记录这一映射；外部服务

器给内部 PC 发送应答报文 2（其初始目的地址为 202.169.10.1），到达 NAT 服务器后，NAT 进程再次查看报头内容，然后查找当前网络地址转换表的记录，用原来的内部 PC 的私有地址 192.168.1.3 替换目的地址。

上述的 NAT 过程对终端（如图中的 PC 和服务器）来说是透明的。对外部服务器而言，它认为内部 PC 的 IP 地址就是 202.169.10.1，并不知道有 192.168.1.3 这个地址。因此，NAT “隐藏”了企业的私有网络。

地址转换的优点在于，为内部主机提供了“隐私”（Privacy）保护前提下，实现了内部网络的主机通过该功能访问外部网络资源。但它也有一些缺点：

- 由于需要对数据报文进行 IP 地址的转换，涉及 IP 地址的数据报的报头不能被加密。在应用协议中，如果报文中有地址或端口需要转换，则报文不能被加密。例如，不能使用加密的 FTP 连接，否则 FTP 的 port 命令不能被正确转换。
- 网络调试变得更加困难。比如，某一台内部网络的主机试图攻击其它网络，则很难指出究竟是哪一台机器是恶意的，因为主机的 IP 地址被屏蔽了。
- 在链路的带宽低于 10Mbit/s 速率时，地址转换对网络性能基本不构成影响，此时，网络传输的瓶颈在传输线路上；当速率高于 10Mbit/s 时，地址转换将对防火墙性能产生一些影响。

4.2 地址转换实现的功能

4.2.1 多对多地址转换及地址转换的控制

从图 4-1 的地址转换过程可见，当内部网络访问外部网络时，地址转换将会选择一个合适的外部地址，替代内部网络数据报文的源地址。在上图中是选择 NAT 服务器出接口的 IP 地址（公有地址）。这样所有内部网络的主机访问外部网络时，只能拥有一个外部的 IP 地址，因此，这种情况只允许最多有一台内部主机访问外部网络，这称为“一对一地址转换”。当内部网络的主机并发的要求访问外部网络时，“一对一地址转换”仅能够实现其中一台主机的访问请求。

NAT 的一种变形实现了并发性。允许 NAT 服务器拥有多个公有 IP 地址，当第一个内部主机访问外网时，NAT 选择一个公有地址 IP1，在地址转换表中添加记录并发送数据报；当另一内部主机访问外网时，NAT 选择另一个公有地址 IP2，以此类推，从而满足了多台内部主机访问外网的请求。这称为“多对多地址转换”。

说明：

NAT 服务器拥有的公有 IP 地址数目要远少于内部网络的主机数目，因为所有内部主机并不会同时访问外网。公有 IP 地址数目的确定，应根据网络高峰期可能访问外网的内部主机数目的统计值来确定。

在实际应用中，我们可能希望某些内部的主机具有访问 Internet（外部网络）的权利，而某些主机不允许访问。即当 NAT 进程查看数据报报头内容时，如果发现源 IP 地址是为那些不允许访问网络的内部主机所拥有的，它将不进行 NAT 转换。这就是一个对地址转换进行控制的问题。

SecPath 系列防火墙可以通过定义地址池来实现多对多地址转换，同时利用访问控制列表来对地址转换进行控制的。

- 地址池：用于地址转换的一些公有 IP 地址的集合。用户应根据自己拥有的合法 IP 地址数目、内部网络主机数目以及实际应用情况，配置恰当的地址池。地址转换的过程中，将会从地址池中挑选一个地址做为转换后的源地址。
- 利用访问控制列表限制地址转换：只有满足访问控制列表条件的数据报文才可以进行地址转换。这可以有效地控制地址转换的使用范围，使特定主机能够有权利访问 Internet。

4.2.2 NAPT——网络地址端口转换

还有一种 NAT 变形——这就是 NAPT（Network Address Port Translation，网络地址端口转换），NAPT 允许多个内部地址映射到同一个公有地址上，非正式的也可称之为“多对一地址转换”或地址复用。

NAPT 映射 IP 地址和端口号，来自不同内部地址的数据报可以映射到同一外部地址，但它们被转换为该地址的不同端口号，因而仍然能够共享同一地址。也就是<私有地址+端口>与<公有地址+端口>之间的转换。

下图描述了 NAPT 的基本原理。

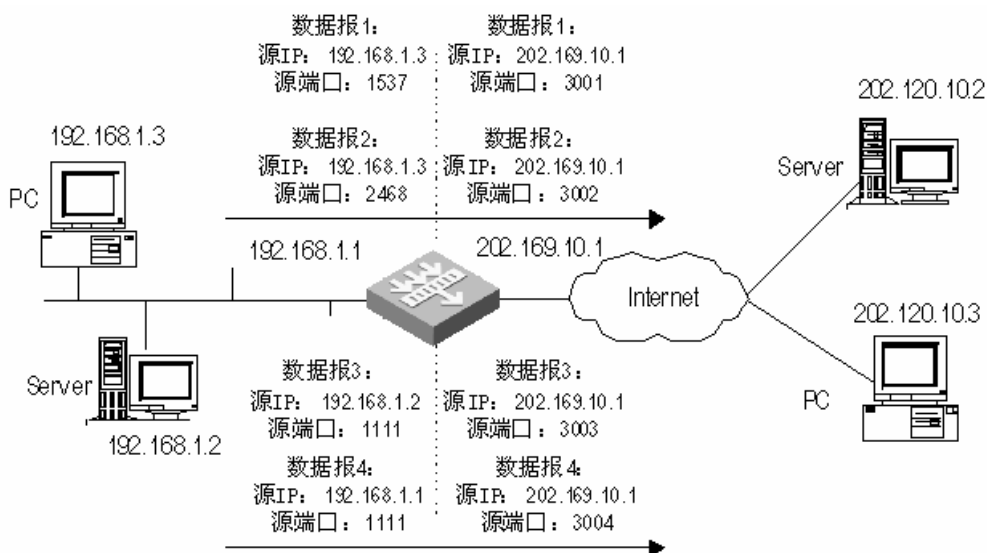


图4-2 NAPT 地址复用示意图

如图所示，四个带有内部地址的数据报到达 NAT 服务器，其中数据报 1 和 2 来自同一个内部地址但有不同的源端口号，数据报 3 和 4 来自不同的内部地址但具有相同的源端口号。通过 NAT 映射，四个数据报都被转换到同一个外部地址，但每个数据报都赋予了不同的源端口号，因而仍保留了报文之间的区别。当回应报文到达时，NAT 进程仍能够根据回应报文的目地址和端口号来区别该报文应转发到的内部主机。

4.2.3 静态网段地址转换

该特性实现了一种新的 NAT 静态地址转换方式，即将指定范围内的内部主机地址转换为指定的公网网段地址，转换过程中只对网段地址进行转换，保持主机地址不变。当内部主机访问外部网络时，如果主机地址在指定的内部主机地址范围内，会被转换为对应的公网地址；同样当通过公网网段地址对内部主机进行访问时，可以直接访问到内部主机（该公网地址在转换后在指定的内部主机地址范围内）。

通过 NAT 网段地址转换功能实现了内部主机地址和公网地址的直接映射关系，且同时提供了类似 NAT Server 的功能。

静态网段地址转换方式中公网 IP 地址与私网 IP 地址一一对应，因此比较浪费 IP 地址空间，故可以考虑与传统的静态地址转换或动态地址转换配合使用，只要不存在地址冲突即可。

4.2.4 双向地址转换

常规地址转换技术只转换报文的源地址或目的地址，而双向地址转换（Bidirectional NAT）技术可以将报文的源地址和目的地址同时转换，该技术应用于内部网络主机地址与公网上主机地址重叠的情况。如图所示：内部网络主机 PC1 和公网上主机 PC3 的地址重叠。这种情况下，内部网络主机 PC2 访问主机 PC3 的报文不会到达目的主机，而会被错误的转发到主机 PC1 上。双向 NAT 技术通过在 SecPathA 上配置重叠地址池到临时地址的映射关系（在实现常规 NAT 的基础上），将重叠地址转换为唯一的临时地址，来保证报文的正确转发。

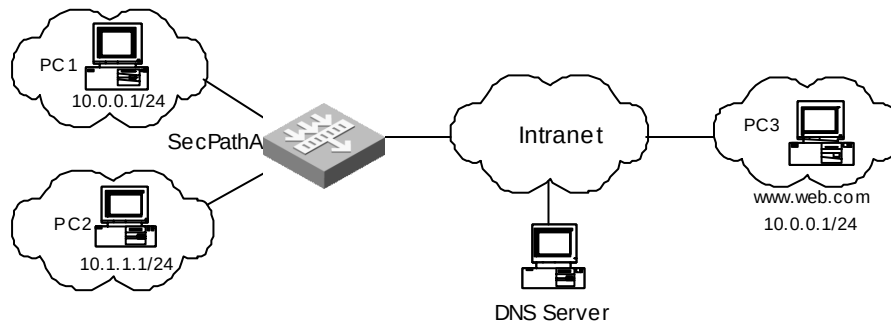


图4-3 双向地址转换应用组网图

例如，在 SecPathA 上配置双向地址转换：

第一步：配置常规 NAT（多对多地址转换）。

配置 NAT 地址池 200.0.0.1~200.0.0.100，并应用到广域网接口。

第二步：配置一组重叠地址到临时地址的映射。

10.0.0.0<—>3.0.0.0，子网掩码为 24 位。

此映射表示，重叠地址池与临时地址池一一对应，转换规则为：

临时地址 = 临时地址池首地址 + （重叠地址 - 重叠地址池首地址）

重叠地址 = 重叠地址池首地址 + （临时地址 - 临时地址池首地址）

当内部主机 PC2 直接用域名访问公网上的主机 PC3 时，报文的处理流程如下：

- (1) PC2 发送解析域名为 www.web.com 的 Web 服务器的 DNS 请求，经公网 DNS 服务器解析后，SecPathA 收到 DNS 服务器的响应报文。SecPathA 检查 DNS 响应报文载荷中的解析回来的地址 10.0.0.1，经检查该地址为重叠地址（与重叠地址池匹配），将地址 10.0.0.1 转换为对应的临时地址 3.0.0.1。之后再对 DNS 响应报文进行目的地址转换（常规 NAT 处理），发送给 PC2。
- (2) PC2 用 www.web.com 对应的临时地址 3.0.0.1 发起访问，当报文到达 SecPathA 时，先转换报文的源地址（常规 NAT 处理），再将报文的目的地地址即临时地址，转换为对应的重叠地址 10.0.0.1。
- (3) 将报文送到广域网出接口，并经广域网逐跳转发至主机 PC3。
- (4) 当 PC3 给 PC2 返回的报文到达 SecPathA 时，先检查报文的源地址 10.0.0.1，该地址为重叠地址（与重叠地址池匹配），则将源地址转换为对应的临时地址 3.0.0.1。之后再对返回报文的目的地地址进行常规 NAT 转换，并发送给 PC2。

4.2.5 内部服务器

NAT 隐藏了内部网络的结构，具有“屏蔽”内部主机的作用，但是在实际应用中，可能需要提供给外部一个访问内部主机的机会，如提供给外部一个 WWW 的服务器，或是一台 FTP 服务器。使用 NAT 可以灵活地添加内部服务器，例如，可以使用 202.169.10.10 作为 Web 服务器的外部地址；使用 202.110.10.11 作为 FTP 服务器的外部地址；甚至还可以使用 202.110.10.12:8080 这样的地址作为 Web 的外部地址；还可为外部用户提供多台同样的服务器（如提供多台 Web 服务器）。

SecPath 系列防火墙的 NAT 功能提供了内部服务器功能供外部网络访问。外部网络的用户访问内部服务器时，NAT 将请求报文内的目的地地址转换成内部服务器的私有地址。对内部服务器回应报文而言，NAT 要将回应报文的源地址（私网地址）转换成公网地址。

4.2.6 Easy IP

Easy IP 的概念很简单，当进行地址转换时，直接使用接口的公有 IP 地址作为转换后的源地址。同样它也利用访问控制列表控制哪些内部地址可以进行地址转换。

4.2.7 地址转换应用层网关

地址转换会导致许多对 NAT 敏感的应用协议无法正常工作，必须针对该协议进行特殊的处理。所谓对 NAT 敏感的协议是指该协议的某些报文的有效载荷中携带 IP 地址和（或）端口号，如果不进行特殊处理，将会严重影响后继的协议交互。

地址转换应用层网关（NAT Application Level Gateway, NAT ALG）是解决特殊协议穿越 NAT 的一种常用方式，该方法按照地址转换规则，对载荷中的 IP 地址和端口号进行替换，从而实现对该协议的透明中继。目前 Comware 的 NAT ALG 支持 PPTP、DNS、FTP、ILS、NBT、H.323 等协议。

4.2.8 NAT 限制最大 TCP 连接数

NAT 也存在着一些问题。例如，如果局域网内的某台 PC 感染病毒，它会发起大量的 TCP 连接，迅速消耗设备资源，导致设备性能下降，影响其他用户使用。NAT 限制最大 TCP 连接数特性可以避免出现这种情况。

NAT 限制最大 TCP 连接数特性通过连接数限制特性设置某种特征的 TCP 连接数上限，从而可以实现 NAT 限制最大 TCP 连接数的功能。

连接数限制的配置相当灵活，用户可以通过配置策略实现针对不同的连接进行限制。用户配置的策略包括两方面的内容：

1. 符合什么特征的报文需要被限制。

可以通过 ACL 来指定报文的特征，如基于报文的源地址、基于报文的目的地址、基于服务，用户可以根据自己的需要使用 ACL 灵活地指定。

2. 对于符合指定特征的连接如何进行限制。

用户可以通过指定上限和下限两个阈值来控制是否允许建立连接。当符合某种特征的连接数达到上限时禁止建立该种连接。当连接数降低到小于等于下限时，允许建立连接。

4.2.9 支持 NAT 多实例

NAT 多实例允许分属于不同 MPLS VPN 的用户通过同一个出口访问外部网络（Internet），同时允许不同的 VPN 用户使用相同的私网地址。当 MPLS VPN 用户访问 Internet 时，Comware 的地址转换将内部网络主机的 IP 地址和端口替换为安全网关的外部网络地址和端口，同时还记录了用户的 MPLS VPN 信息（如协议类型和路由标识符 RD 等）。报文还原时，地址转换将外部网络地址和端口还原为内部

网络主机的 IP 地址和端口，同时获知是哪一个 MPLS VPN 用户的访问。无论 PAT 方式的地址转换，还是 NO-PAT 方式的地址转换都支持多实例。

Comware 的地址转换支持内部服务器的多实例，提供给外部访问 MPLS VPN 内主机的机会。例如，VPN1 内提供 WWW 服务的主机地址是 10.110.1.1，可以使用 202.110.10.20 作为 web 服务器的外部地址，Internet 的用户使用 202.110.10.20 的地址就可以访问到 MPLS VPN1 提供的 WWW 服务。

4.3 NAT 的配置

NAT 配置包括：

- 配置地址池
- 配置 Easy IP
- 配置静态地址转换
- 配置多对多地址转换
- 配置 NAPT
- 配置内部服务器
- 配置地址转换应用层网关
- 配置内部主机通过域名区分并访问其对应的内部服务器
- 配置地址转换有效时间
- 配置最大连接数限制
- 配置报文匹配方式
- 配置地址转换表项的老化刷新速度

4.3.1 配置地址池

地址池是一些连续的 IP 地址集合，当内部数据包通过地址转换到达外部网络时，将会选择地址池中的某个地址作为转换后的源地址。

请在系统视图下进行下列配置。

表4-1 配置地址池

操作	命令
定义一个地址池	nat address-group <i>group-number</i> <i>start-addr</i> <i>end-addr</i>
删除一个地址池	undo nat address-group <i>group-number</i>

 说明：

- NAT 地址池中的地址不应包含公网主机已使用的地址，否则会造成地址冲突。
- 如果防火墙仅提供 Easy IP 功能，则不需要配置 NAT 地址池，直接使用接口地址作为转换后的 IP 地址。
- 当某个地址池已经和某个访问控制列表关联进行地址转换，是不允许删除这个地址池的。
- 地址池长度（地址池中包含的所有地址个数）不能超过 255 个地址。

4.3.2 配置地址转换

将访问控制列表和地址池关联（或接口地址）后，即可实现地址转换。这种关联指定了“具有某些特征的 IP 报文”才可以使用“这样的地址池中的地址（或接口地址）”。当内部网络有数据包要发往外部网络时，首先根据访问列表判定是否是允许的数据包，然后根据转换关联找到与之对应的地址池（或接口地址）进行转换。

访问控制列表的配置请参见 第 3 章 访问控制列表配置。

不同形式的地址转换，配置方法稍有不同。

1. Easy IP

如果地址转换命令不带 **address-group** 参数，即仅使用 **nat outbound acl-number** 命令，则实现了 **easy-ip** 的特性。地址转换时，直接使用接口的 IP 地址作为转换后的地址，利用访问控制列表控制哪些地址可以进行地址转换。

请在接口视图下进行下列配置。

表4-2 配置 Easy IP

操作	命令
配置访问控制列表和接口地址关联	nat outbound acl-number
删除访问控制列表和接口地址的关联	undo nat outbound acl-number

2. 使用指定 loopback 接口进行地址转换

请在接口视图下进行下列配置。

表4-3 使用指定 loopback 接口进行地址转换

操作	命令
配置访问控制列表和指定的 loopback 接口地址关联	nat outbound <i>acl-number</i> interface <i>interface-type</i> <i>interface-number</i>
删除访问控制列表和指定 loopback 接口地址的关联	undo nat outbound <i>acl-number</i> interface <i>interface-type</i> <i>interface-number</i>

匹配访问控制列表的数据报文的源地址将转换为指定的 loopback 接口的 IP 地址。

3. 配置静态地址转换表

(1) 配置一对一静态地址转换表

请在系统视图下进行下列配置。

表4-4 配置一对一地址转换

操作	命令
配置从内部地址到外部地址的一对一转换	nat static <i>ip-addr1</i> <i>ip-addr2</i>
删除已经配置得 NAT 一对一转换	undo nat static <i>ip-addr1</i> <i>ip-addr2</i>

(2) 配置静态网段地址转换表

使用静态网段地址转换时，只进行网段地址的转换，而保持主机地址不变。

请在系统视图下进行下列配置。

表4-5 配置网段地址静态转换表

操作	命令
配置从内部地址到外部地址的静态网段地址转换表	nat static inside ip <i>inside-address</i> global ip <i>global-address</i> nat static inside ip <i>inside-start-address</i> <i>inside-end-address</i> global ip <i>global-address</i> <i>mask</i>
删除已经配置的 NAT 网段地址转换表	undo nat static inside ip <i>inside-address</i> undo nat static inside ip <i>inside-address</i> global ip <i>global-address</i> undo nat static inside ip <i>inside-start-address</i> <i>inside-end-address</i> [global ip <i>global-address</i> <i>mask</i>]

nat static inside 和 **nat static** 会分别创建两种不同的 NAT 静态表项，在具体的配置中，两种 NAT 静态表项不存在冲突即可。

**注意：**

在配置静态网段地址转换时，应该确保转换后的地址不会被网络拓扑中的其他设备使用。

(3) 使静态转换表项在接口上生效

请在接口视图下进行下列配置。

表4-6 使静态转换表项在接口上生效

操作	命令
使已经配置的 NAT 静态转换表项在接口上生效	nat outbound static
禁止在接口上配置的 NAT 静态转换表项生效	undo nat outbound static

4. 配置多对多地址转换

将访问控制列表和地址池关联后，即可实现多对多地址转换。

请在接口视图下进行下列配置。

表4-7 配置多对多地址转换

操作	命令
配置访问控制列表和地址池关联	nat outbound acl-number address-group group-number [no-pat]
删除访问控制列表和地址池的关联	undo nat outbound acl-number address-group group-number [no-pat]

5. 配置 NAPT

将访问控制列表和 NAT 地址池关联时，如果选择 **no-pat** 参数，则表示只转换数据包的 IP 地址而不使用端口信息，即不使用 NAPT 功能；如果不选择 **no-pat** 参数，则启用 NAPT 功能。缺省情况是启用。

请在接口视图下进行下列配置。

表4-8 配置 NAPT

操作	命令
配置访问控制列表和地址池关联	nat outbound acl-number [address-group group-number]
删除访问控制列表和地址池的关联	undo nat outbound acl-number [address-group group-number]

6. 配置双向地址转换

请在系统视图下进行下面配置。

表4-9 配置双向地址转换

操作	命令
配置重叠地址池到临时地址池的映射	nat overlapaddress <i>number</i> <i>overlappool-startaddress</i> <i>temppool-startaddress</i> { pool-length <i>pool-length</i> address-mask <i>mask</i> }
删除重叠地址池到临时地址池的映射	undo nat overlapaddress <i>number</i>

7. 配置 NAT 多实例

无论 Easy IP、多对多地址转换，还是 NAPT，都可以支持 NAT 多实例的配置。只要在访问控制列表的规则 **rule** 中配置 **vpn-instance** *vpn-instance-name*，指明那些 MPLS VPN 用户需要进行地址转换，即可以实现对 MPLS VPN 的支持。

4.3.3 配置内部服务器

通过配置内部服务器，可将相应的外部地址、端口等映射到内部的服务器上，提供了外部网络可访问内部服务器的功能。内部服务器与外部网络的映射表是由 **nat server** 命令配置的。

用户需要提供的信息包括：外部地址、外部端口、内部服务器地址、内部服务器端口以及服务协议类型。

防火墙支持使用接口地址作为 NAT Server 的公网地址。当路由器的公网接口通过拨号或 DHCP 方式获取公网地址时，其 NAT Server 的公网地址可以动态更新，方便用户配置。

当内部服务器位于 MPLS VPN 时，还应指定所属的 *vpn-instance-name*。如果不设置该值，表示内部服务器属于一个普通的私网，不属于某一个 MPLS VPN。

请在接口视图下进行下列配置。

表4-10 配置内部服务器

操作	命令
配置内部服务器	nat server [vpn-instance <i>vpn-instance-name</i>] protocol <i>pro-type</i> global { <i>global-addr</i> current-interface interface <i>type number</i> } [<i>global-port</i>] inside <i>host-addr</i> [<i>host-port</i>] nat server [vpn-instance <i>vpn-instance-name</i>] protocol <i>pro-type</i> global { <i>global-addr</i> current-interface interface <i>type number</i> } <i>global-port1 global-port2</i> inside <i>host-addr1 host-addr2 host-port</i>

操作	命令
删除内部服务器	<pre>undo nat server [vpn-instance vpn-instance-name] protocol pro-type global { global-addr current-interface interface type number } [global-port] inside host-addr [host-port] undo nat server [vpn-instance vpn-instance-name] protocol pro-type global { global-addr current-interface interface type number } global-port1 global-port2 inside host-addr1 host-addr2 host-port</pre>



注意：

- *global-port* 和 *inside-port* 只要有一个定义了 any，则另一个要么不定义，要么是 any。
- 如果 *global-port* 和 *inside-port* 都为 0、any 或未配置的话，则内网服务器可以通过该配置访问公网，但发起访问的协议必须与配置的协议相同。
- 当使用端口范围配置 FTP 服务器的 NAT Server 时，内部端口号不能配置为 20 和 21；当不使用端口范围配置 FTP 服务器的 NAT Server 时，内部端口号不能配置为 20。
- 由于 TFTP 协议的特殊性，当配置 TFTP 服务器的 NAT Server 时，还应对内部的 TFTP 服务器配置相应的 **nat outbound** 命令。

4.3.4 配置地址转换应用层网关

请在系统视图下进行下面配置

表4-11 配置地址转换应用层网关

操作	命令
配置地址转换应用层网关	nat alg { dns ftp h323 ils msn nbt pptp tns }
禁用地址转换应用层网关功能	undo nat alg { dns ftp h323 ils msn nbt pptp tns }

缺省情况下，使能地址转换应用层网关功能。

4.3.5 配置内部主机通过域名区分并访问其对应的内部服务器

当内部网络无 DNS 服务器，但存在类型不同的多台内部服务器（如 FTP、WWW 等），且内部主机希望通过不同域名区分并访问其对应的内部服务器时，请在系统视图下进行下面配置。

表4-12 配置内部主机通过域名区分并访问其对应的内部服务器

操作	命令
配置一条域名到外部 IP 地址、端口号、协议类型的映射	nat dns-map <i>domain-name</i> <i>global-addr</i> <i>global-port</i> [tcp udp]
删除一条域名到外部 IP 地址、端口号、协议类型的映射。	undo nat dns-map <i>domain-name</i>

系统最多允许配置 64 条映射。

4.3.6 配置地址转换有效时间

由于地址转换所使用的 HASH 表不能永久存在，该命令支持用户可为 TCP、UDP、ICMP 协议分别设置 HASH 表有效的时间，若在设定的时间内未使用该 HASH 表，将失效。举例来说，某个 IP 地址为 10.110.10.10 的用户利用端口 2000 进行了一次对外 TCP 连接，地址转换为它分配了相应的地址和端口，但是若在一定时间内他一直未使用这个 TCP 连接，系统将把这个连接删除。

请在系统视图下进行下列配置。

表4-13 配置地址转换的有效时间

操作	命令
配置地址转换有效时间	nat aging-time { default { dns ftp-ctrl ftp-data icmp pptp tcp tcp-fin tcp-syn udp } <i>seconds</i> }

参数 **default** 表示采用系统缺省的地址转换有效时间。

缺省情况下，DNS 协议地址转换有效时间为 60 秒，FTP 协议控制链路地址转换有效时间为 7200 秒，FTP 协议数据链路地址转换有效时间为 300 秒，PPTP 协议地址转换有效时间为 86400 秒，TCP 地址转换有效时间为 86400 秒，TCP 协议 FIN、RST 或 SYN 连接地址转换有效时间为 60 秒，UDP 地址转换有效时间为 300 秒，ICMP 地址转换有效时间为 60 秒。ALG 的默认老化时间和对应的应用有关，同时为防止攻击，首包老化时间设置为 5 秒。

4.3.7 配置 NAT 限制最大 TCP 连接数

1. 使能连接数限制功能

请在系统视图下进行下列配置。

表4-14 使能连接数限制功能

操作	命令
使能连接数限制功能	connection-limit enable
关闭连接数限制功能	undo connection-limit enable

缺省情况下，关闭连接数限制功能。

2. 设置缺省的连接数限制行为

当系统在未查找到连接数限制策略时，可以设置缺省行为，即是否进行连接数限制。请在系统视图下进行下列配置。

表4-15 设置缺省的连接数限制行为

操作	命令
设置缺省的连接数限制行为	connection-limit default { permit deny }

缺省情况下，未查找到连接数限制策略时不对连接数进行限制。

3. 设置连接数限制的缺省阈值

请在系统视图下进行下列配置。

表4-16 设置连接数限制的缺省阈值

操作	命令
设置连接数限制的缺省阈值	connection-limit default amount { upper-limit upper-limit lower-limit lower-limit }*
取消设置的阈值	undo connection-limit default amount { upper-limit lower-limit }*

缺省情况下，上限为 50，下限为 20。

4. 创建连接数限制策略

请在系统视图下进行下列配置。

表4-17 创建连接数限制策略

操作	命令
创建连接数限制策略并进入连接数限制策略视图	connection-limit policy policy-number
删除连接数限制策略	undo connection-limit policy { policy-number all }

缺省情况下，未创建连接数限制策略。

5. 定义连接数限制策略的规则

请在连接数限制策略视图下进行下列配置。

表4-18 定义连接数限制策略的规则

操作	命令
定义连接数限制策略的规则	limit <i>limit-id</i> acl <i>acl-number</i> [{ per-source per-destination per-service }* amount <i>upper-limit</i> <i>lower-limit</i>]
删除连接数限制策略的规则	undo limit <i>limit-id</i>

缺省情况下，未定义连接数限制策略的规则。

说明：

- 通过定义连接限制策略规则的 ACL，不但可以限制 TCP 连接数量，也可以限制非 TCP 流量（如：UDP、ICMP）。如果只对 TCP 连接进行限制，需要在 ACL 中明确指定。
- 在实际应用中，需要合理设置 TCP 连接的上限值和下限值，否则会影响正常业务。

6. 绑定连接数限制策略

配置完连接数限制策略后，需将其与 NAT 功能绑定才能生效。

请在系统视图下进行下列配置。

表4-19 绑定连接数限制策略

操作	命令
绑定连接数限制策略	nat connection-limit-policy <i>policy-number</i>
取消绑定连接数限制策略	undo nat connection-limit-policy <i>policy-number</i>

缺省情况下，未绑定连接数限制策略。

4.3.8 配置报文匹配方式

可以通过如下配置改变报文的匹配方式。

请在系统视图下进行下列配置。

表4-20 配置报文匹配方式

操作	命令
配置报文匹配方式为五元组匹配	nat match factor-all
配置报文匹配方式为三元组匹配	undo nat match factor-all

缺省情况下，报文匹配方式为五元组匹配。

当匹配方式为三元组匹配时，创建的 UDP 协议的 NAT 表项将不包括目的地址和目的端口。

4.3.9 配置地址转换表项的老化刷新速度

地址转换表项的老化刷新速度可以在一定范围内调整。

请在系统视图下进行下列配置。

表4-21 配置地址转换表项的老化刷新速度

操作	命令
配置地址转换表项的老化刷新速度	nat session refresh-speed level <i>level-value</i>
恢复缺省的地址转换表项的老化刷新速度	undo nat session refresh-speed

参数 *level-value* 表示老化刷新速度的等级，取值范围为 1~5，级别越高速度越快。

默认情况下，SecPath F1000 的等级为 2，SecBlade 的等级为 3，其它 SecPath 安全网关设备的等级为 1。

4.4 地址转换显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示地址转换配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可以清除该运行情况。

在用户视图下，执行 **debugging** 命令可以对地址转换进行调试。

表4-22 地址转换显示和调试

操作	命令
查看地址转换的状况	display nat { address-group aging-time all outbound server statistics static session [vpn-instance <i>vpn-instance-name</i>] [source { global <i>global-addr</i> inside <i>inside-addr</i> }] }

操作	命令
显示连接数限制信息	display connection-limit statistics [source <i>source-addr</i> { <i>source-mask</i> <i>source-mask-len</i> }] [destination <i>destination-addr</i> { <i>destination-mask</i> <i>destination-mask-len</i> }] [destination-port { { <i>eq</i> <i>neq</i> <i>gt</i> <i>lt</i> } <i>destination-port</i> range <i>destination-port1</i> <i>destination-port2</i> }] [vpn-instance <i>vpn-name</i>]
显示连接数限制策略	display connection-limit policy { <i>policy-number</i> all }
显示与 NAT 相关的连接数限制信息	display nat connection-limit [source <i>source-addr</i> { <i>source-mask</i> <i>source-mask-len</i> }] [destination <i>destination-addr</i> { <i>destination-mask</i> <i>destination-mask-len</i> }] [destination-port { { <i>eq</i> <i>neq</i> <i>gt</i> <i>lt</i> } <i>destination-port</i> range <i>destination-port1</i> <i>destination-port2</i> }] [vpn-instance <i>vpn-name</i>]
打开 NAT 的调试开关	debugging nat { <i>alg</i> <i>event</i> <i>packet</i> } [interface <i>interface-type</i> <i>interface-number</i>]
关闭 NAT 的调试开关	undo debugging nat { <i>alg</i> <i>event</i> <i>packet</i> } [interface <i>interface-type</i> <i>interface-number</i>]
打开连接数限制的调试开关	debugging connection-limit
关闭连接数限制的调试开关	undo debugging connection-limit
清除地址转换映射表	reset nat { <i>log-entry</i> <i>session</i> }

4.5 NAT 配置举例

4.5.1 典型 NAT 配置举例

1. 组网需求

如下图所示，一个公司通过 SecPath 防火墙的地址转换功能连接到广域网。要求该公司能够通过防火墙 Ethernet3/0/0 访问 Internet，公司内部对外提供 WWW、FTP 和 SMTP 服务，而且提供两台 WWW 的服务器。公司内部网址为 10.110.0.0/16。其中，内部 FTP 服务器地址为 10.110.10.1，内部 WWW 服务器 1 地址为 10.110.10.2，内部 WWW 服务器 2 地址为 10.110.10.3，内部 SMTP 服务器地址为 10.110.10.4，并且希望可以对外提供统一的服务器的 IP 地址。内部 10.110.10.0/24 网段可以访问 Internet，其它网段的 PC 机则不能访问 Internet。外部的 PC 可以访问内部的服务器。公司具有 202.38.160.100 至 202.38.160.105 六个合法的 IP 地址。选用 202.38.160.100 作为公司对外的 IP 地址，WWW 服务器 2 对外采用 8080 端口。

2. 组网图

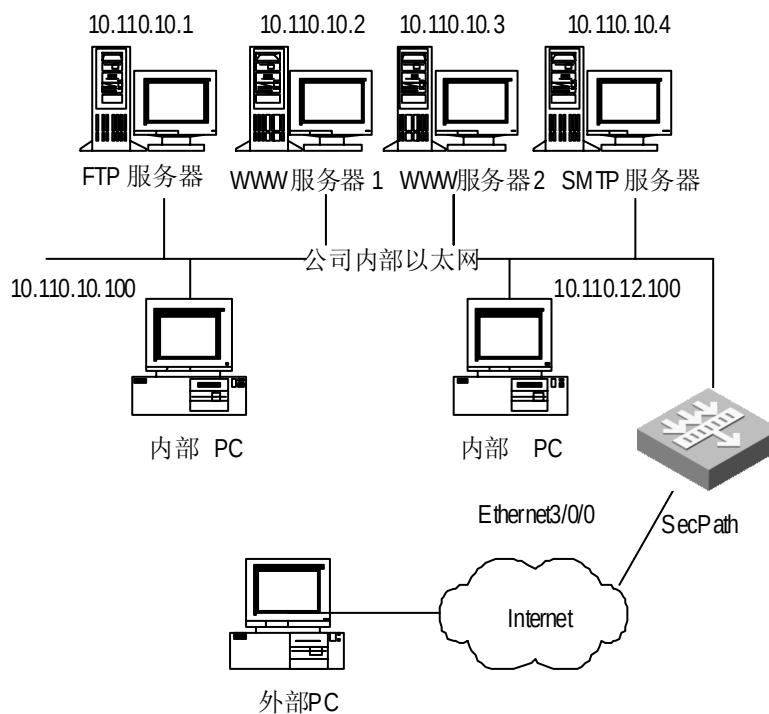


图4-4 地址转换配置案例组网图

3. 配置步骤

配置地址池和访问控制列表，允许 10.110.10.0/24 网段进行地址转换。

```
[H3C] nat address-group 1 202.38.160.101 202.38.160.105
[H3C] acl number 2001
[H3C-acl-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[H3C-acl-basic-2001] rule deny source 10.110.0.0 0.0.255.255
[H3C-acl-basic-2001] quit
[H3C] interface Ethernet3/0/0
[H3C-Ethernet3/0/0] nat outbound 2001 address-group 1
```

设置内部 FTP 服务器。

```
[H3C-Ethernet3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.1 ftp
```

设置内部 WWW 服务器 1。

```
[H3C-Ethernet3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.2 www
```

设置内部 WWW 服务器 2。

```
[H3C-Ethernet3/0/0] nat server protocol tcp global 202.38.160.100 8080 inside
10.110.10.3 www
```

设置内部 SMTP 服务器。

```
[H3C-Ethernet3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.4 smtp
```

4.5.2 使用 loopback 接口地址进行地址转换典型配置举例

1. 组网需求

如下图所示，公司通过 SecPath 防火墙的 Ethernet3/0/0 接口访问 internet，内部 10.110.10.0/24 网段可以访问 Internet，其它网段的 PC 机则不能访问 Internet，内部 10.110.10.0/24 网段使用 loopback 接口 IP 地址 202.38.160.106 做为地址转换后 IP 地址。公司内部对外提供 WWW、FTP 和 SMTP 服务，三个服务器对外使用统一的服务器 IP 地址 202.38.160.100。

2. 组网图

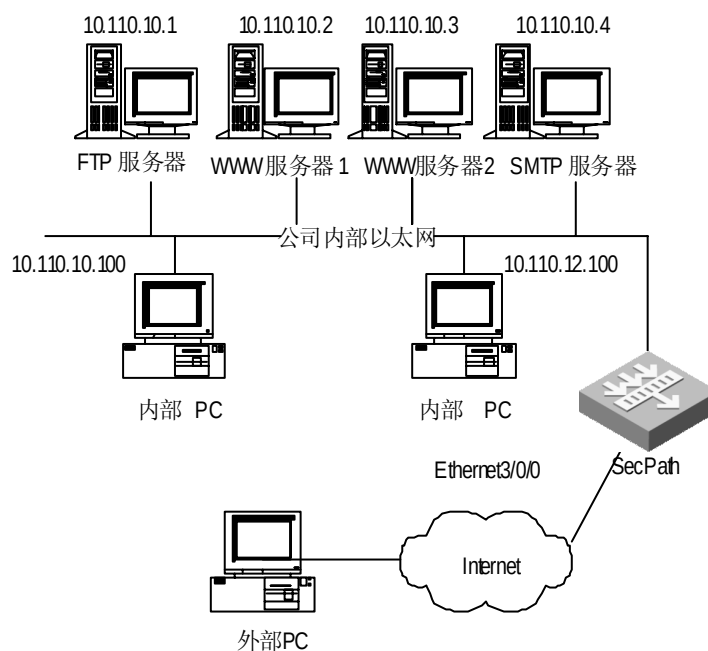


图4-5 地址转换配置举例组网图

3. 配置步骤

配置访问控制列表。

```
[H3C] acl number 2001
[H3C-acl-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[H3C-acl-basic-2001] rule deny source 10.110.0.0 0.0.255.255
[H3C-acl-basic-2001] quit
```

配置 loopback 接口

```
[H3C] interface loopback0
```

```
[H3C-LoopBack0] ip address 202.38.160.106 32
[H3C-LoopBack0] quit
# 设置内部 FTP 服务器。

[H3C] interface Ethernet3/0/0
[H3C-Ethernet3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.1 ftp
# 设置内部 WWW 服务器 1。

[H3C-Ethernet3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.2 www
# 设置内部 WWW 服务器 2。

[H3C-Ethernet3/0/0] nat server protocol tcp global 202.38.160.100 8080 inside
10.110.10.3 www
# 设置内部 SMTP 服务器。

[H3C-Ethernet3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.4 smtp
# 配置使用 loopback 接口作为转换后的 IP 地址。

[H3C-Ethernet3/0/0] nat outbound 2001 interface loopback 0
```

4.5.3 静态网段地址转换典型组网应用

1. 组网需求

私网 A 的网络地址为 10.1.1.0/24 网段，私网 B 的网络地址也为 10.1.1.0/24 网段。假设 PC1 的地址为 10.1.1.2，PC2 的地址也是 10.1.1.2。SecPathA 的广域网接口 IP 地址为 201.1.1.1/24，SecPathB 的广域网接口 IP 地址为 201.2.2.2/24。SecPathA 和 SecPathB 上配置网段地址转换，将私网 A 的网络地址 10.1.1.0/24 转换为 211.2.1.0/24，将私网 B 的网络地址 10.1.1.0/24 转换为 211.2.2.0/24。在 SecPathA 和 SecPathB 上配置动态路由，保证 SecPathA 到 211.2.2.0/24 的路由及 SecPathB 到 211.2.1.0/24 的路由可达。

要求能够实现私网对公网的访问，而且实现私网 A 的 PC1 可以通过 PC2 在 SecPathB 上的公网地址 211.2.2.2 访问到 PC2；同样私网 B 的 PC2 可以通过 PC1 在 SecPathA 上的公网地址 211.2.1.2 访问到 PC1。

2. 组网应用

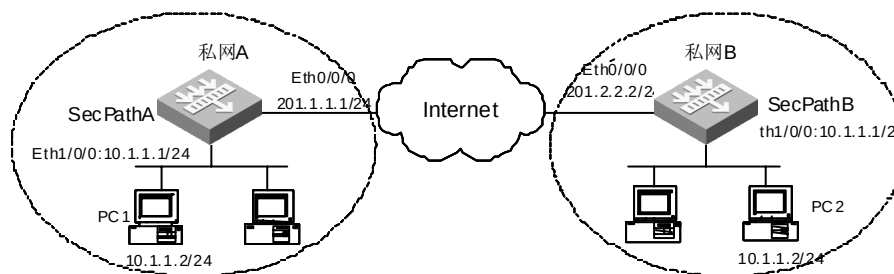


图4-6 静态网段地址转换应用组网图

3. 配置步骤

(1) 配置 SecPathA

配置网段地址静态转换。

```
[H3C] nat static inside ip 10.1.1.1 10.1.1.254 global ip 211.2.1.0 255.255.255.0
```

配置网段地址转换在接口 Ethernet0/0/0 上生效。

```
[H3C] interface Ethernet0/0/0
[H3C-Ethernet0/0/0] ip address 201.1.1.1 255.255.255.0
[H3C-Ethernet0/0/0] nat outbound static
[H3C-Ethernet0/0/0] quit
```

配置 Ethernet1/0/0 接口。

```
[H3C] interface Ethernet1/0/0
[H3C-Ethernet1/0/0] ip address 10.1.1.1 255.255.255.0
```

配置动态路由，保证到 211.2.2.0 网段的路由可达（略）。

(2) 配置 SecPathB

配置网段地址静态转换。

```
[H3C] nat static inside ip 10.1.1.1 10.1.1.254 global ip 211.2.2.0 255.255.255.0
```

配置网段地址转换在接口 Ethernet0/0/0 上生效。

```
[H3C] interface Ethernet0/0/0
[H3C-Ethernet0/0/0] ip address 201.2.2.2 255.255.255.0
[H3C-Ethernet0/0/0] nat outbound static
[H3C-Ethernet0/0/0] quit
```

配置 Ethernet1/0/0 接口。

```
[H3C] interface ethernet1/0/0
[H3C-Ethernet1/0/0] ip address 10.1.1.1 255.255.255.0
```

配置动态路由，保证到 211.2.1.0 网段的路由可达（略）。

4.5.4 双向地址转换配置举例

1. 组网需求

公司内部局域网使用 10.0.0.0/24 和 10.1.1.0/24 网段地址。当 PC1 的 IP 地址 10.0.0.1 与公网上主机 PC3 的 IP 地址相同时，要求 PC1、PC2 可以用域名 www.web.com 或 IP 地址 3.0.0.1/24 访问 PC3。

2. 组网图

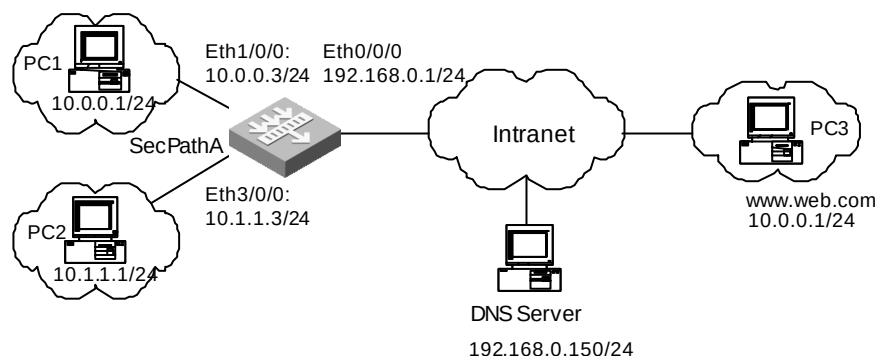


图4-7 双向地址转换配置举例组网图

3. 配置步骤

配置 NAT 地址池。

```
[H3C] nat address-group 1 2.0.0.1 2.0.0.200
```

配置双向 NAT 映射。

```
[H3C] nat overlapaddress 3 10.0.0.0 3.0.0.0 address-mask 24
```

配置访问控制列表。

```
[H3C] acl number 2000
```

```
[H3C-acl-basic-2000] rule 0 permit source 10.0.0.0 0.0.0.255
```

```
[H3C-acl-basic-2000] rule 1 permit source 10.1.1.0 0.0.0.255
```

```
[H3C-acl-basic-2000] quit
```

在广域网接口上绑定 NAT outbound。

```
[H3C] interface ethernet0/0/0
```

```
[H3C-Ethernet0/0/0] ip address 192.168.0.1 255.255.255.0
```

```
[H3C-Ethernet0/0/0] nat outbound 2000 address-group 1
```

```
[H3C-Ethernet0/0/0] quit
```

配置局域网口 IP 地址。

```
[H3C] interface ethernet 1/0/0
```

```
[H3C-Ethernet1/0/0] ip address 10.0.0.3 255.255.255.0
```



```
[H3C-Ethernet1/0/0] interface ethernet 3/0/0
[H3C-Ethernet3/0/0] ip address 10.1.1.3 255.255.255.0
[H3C-Ethernet3/0/0] quit
```

4.5.5 内部主机通过域名区分并访问对应的内部服务器组网应用

1. 组网需求

某公司内部网络位于 10.0.0.0/8 网段，提供 FTP 及 WWW 内部服务器，域名分别为 www.zc.com 和 ftp.zc.com，域名可以被外部 DNS 服务器正确解析。连接外部网络的接口 Ethernet0/0/0 的 IP 地址为 1.1.1.1/8。通过配置 NAT 的 DNS 映射功能，使得内部主机在无 DNS 服务器的情况下也可以通过域名来访问内部服务器。

2. 组网图

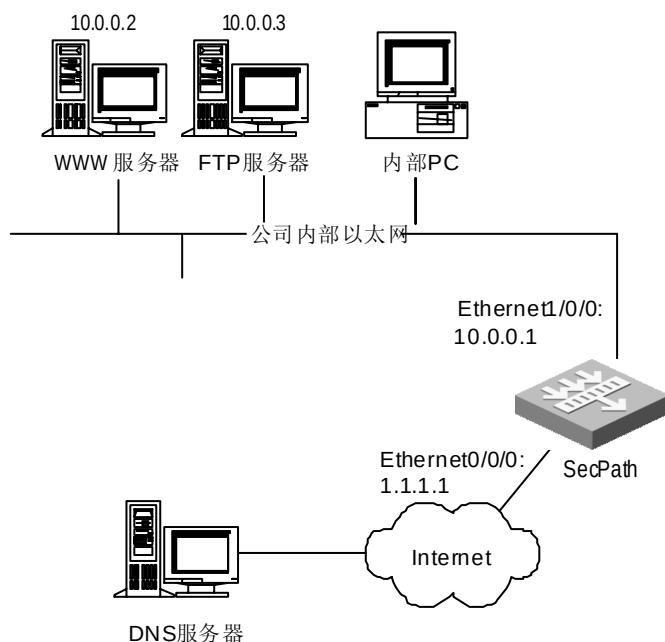


图4-8 内部主机通过域名区分并访问对应的内部服务器

3. 配置步骤

在 Ethernet0/0/0 接口上配置 FTP 及 WWW 内部服务器。

```
[H3C] interface ethernet0/0/0
[H3C-Ethernet0/0/0] ip address 1.1.1.1 255.0.0.0
[H3C-Ethernet0/0/0] nat outbound 2000
[H3C-Ethernet0/0/0] nat server protocol tcp global 1.1.1.1 www inside 10.0.0.2
www
[H3C-Ethernet0/0/0] nat server protocol tcp global 1.1.1.1 ftp inside 10.0.0.3
ftp
[H3C-Ethernet0/0/0] quit
```

配置访问控制列表，允许 10.0.0.0/8 网段访问 Internet。

```
[H3C] acl number 2000
```

```
[H3C-acl-basic-2000] rule 0 permit source 10.0.0.0 0.0.0.255
```

```
[H3C-acl-basic-2000] rule 1 deny
```

配置 ethernet1/0/0。

```
[H3C] interface ethernet1/0/0
```

```
[H3C-Ethernet1/0/0] ip address 10.0.0.1 255.0.0.0
```

此时外部主机可以通过域名 **www.zc.com** 和 **ftp.zc.com** 访问其对应的内部服务器。
加上如下配置后，内部主机也可以通过域名 **www.zc.com** 和 **ftp.zc.com** 访问其对应的内部服务器。

配置域名与外部地址、端口号、协议类型之间的映射。

```
[H3C] nat dns-map www.zc.com 1.1.1.1 80 tcp
```

```
[H3C] nat dns-map ftp.zc.com 1.1.1.1 21 tcp
```

4.5.6 对单一源地址发起的连接数进行限制

1. 组网需求

如图 4-9 所示，防火墙的 Ethernet1/0 接口连接了局域网 192.168.1.0/24，Ethernet1/1 连接到 Internet，在防火墙上配置了 NAT 以实现局域网内的 PC 都能访问 Internet。

为了限制局域网内主机对外发起的连接数，以免影响局域网其他 PC 正常访问 Internet，在防火墙上配置 NAT 限制最大 TCP 连接数特性，对单一源地址发起的连接数进行限制，连接数上限为 10，下限为 1。

2. 组网图

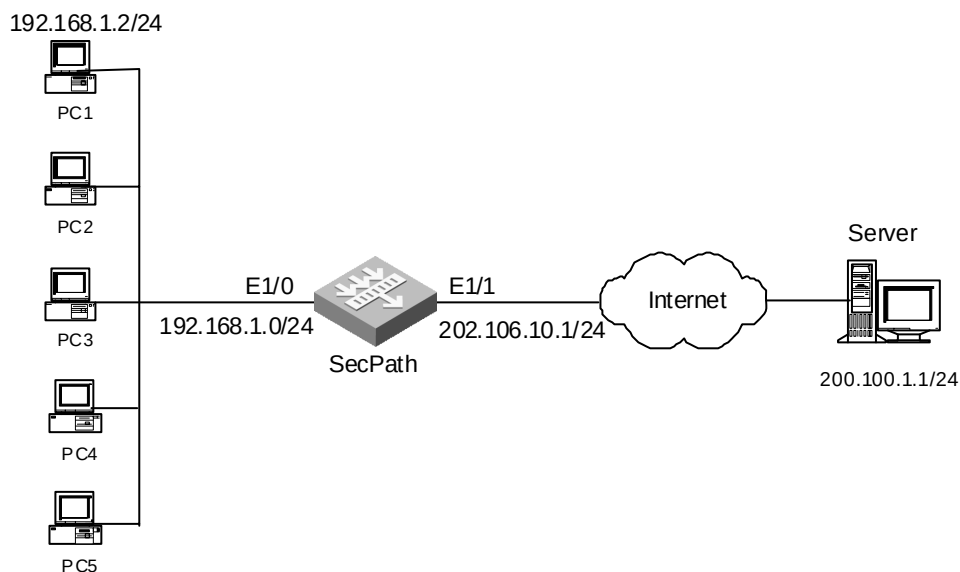


图4-9 NAT 限制最大 TCP 连接数组网图

3. 配置步骤

在防火墙上配置局域网用户通过 NAT 访问 Internet。

略，具体配置请参见本手册的典型 NAT 配置举例。

创建 ACL 并配置规则，来匹配源 IP 地址为 192.168.1.2/24 的数据。

```
<H3C> system-view
[H3C] acl number 3000
[H3C-acl-adv-3000] rule 0 permit tcp source 192.168.1.2 0
[H3C-acl-adv-3000] quit
```

创建连接数限制策略，并配置子规则，对单一源地址发起的连接数进行限制。

```
[H3C] connection-limit enable
[H3C] connection-limit policy 0
[H3C-connection-limit-policy-0] limit 0 acl 3000 per-source amount 10 1
[H3C-connection-limit-policy-0] quit
```

NAT 引用连接数限制策略 0。

```
[H3C] nat connection-limit-policy 0
```

4.6 NAT 排错

故障之一：地址转换不正常。

故障排除：打开 NAT 的 Debug 开关，具体操作请参见 **debugging** 命令中的 **debugging nat**。根据防火墙上的 Debug 调试信息，初步定位错误，然后使用其它命令作进一步的判断。调试时，注意观察转换后的源地址，要保证这个地址是希望转换的地址，否则可能会是地址池配置错误。同时要注意想要访问的网络必须要有回到地址池中地址段的路由。注意防火墙以及地址转换本身的访问控制列表对地址转换造成的影响，同时注意路由的配置。

故障之二：内部服务器工作不正常。

故障排除：如果外部主机不能正常访问内部服务器，请检查是否是内部服务器主机的配置有错或防火墙上对内部服务器的配置有错，如对内部服务器的IP地址指定错误等等。同时也有可能是防火墙禁止了外部主机对内部网络的访问，可以用**display acl**命令来查看，请参见 第5章 防火墙配置。

第5章 防火墙配置

5.1 防火墙简介

在大厦构造中，防火墙被设计用来防止火从大厦的一部分传播到另一部分。网络的防火墙服务于类似目的：防止 Internet 的危险传播到您的内部网络。

防火墙一方面阻止来自 Internet 对受保护网络的未授权或未认证的访问，另一方面允许内部网络的用户对 Internet 进行 Web 访问或收发 E-mail 等。防火墙也可以作为一个访问 Internet 的权限控制关口，如允许内部网络的特定用户访问 Internet。现在的许多防火墙同时还具有一些其他特点，如进行身份鉴别，对信息进行安全（加密）处理等。

防火墙不单用于对 Internet 的连接，也可以用来在组织网络内部保护大型机和重要的资源（如数据）。对受保护数据的访问都必须经过防火墙的过滤，即使网络内部用户要访问受保护的数据，也要经过防火墙。

当外部网络的用户访问网内资源时，要经过防火墙；而内部网络的用户访问网外资源时，也会经过防火墙。这样，防火墙就起到了一个“警卫”的作用，可以将需要禁止的数据包在这里给丢掉。

Comware中的防火墙主要是指基于访问控制列表（ACL）的包过滤（以下简称ACL/包过滤）、基于应用层的包过滤（以下简称状态防火墙ASPF）和地址转换。有关地址转换请参见第4章 地址转换（NAT）配置，本章以下部分将重点介绍ACL/包过滤防火墙和状态防火墙。

5.1.1 ACL/包过滤防火墙简介

1. ACL/包过滤概述

ACL/包过滤应用在防火墙中，就为防火墙增加了对数据包的过滤功能。ACL/包过滤实现对 IP 数据包的过滤，对防火墙需要转发的数据包，先获取数据包的包头信息，包括 IP 层所承载的上层协议的协议号，数据包的源地址、目的地址、源端口和目的端口等，然后和设定的 ACL 规则进行比较，根据比较的结果决定对数据包进行转发或者丢弃。

2. 包过滤对分片报文过滤的支持

Comware 平台 ACL/包过滤提供了对分片报文检测过滤的支持。包过滤防火墙将检测报文类型（非分片报文、首片分片报文、非首片分片报文），获得报文的三层（IP 层）信息（基本 ACL 规则和不含三层以外信息的高级 ACL 规则）及三层以外的信息（包含三层以外信息的高级 ACL 规则）用于匹配，并获得配置的 ACL 规则。

对于配置了精确匹配过滤方式的高级 ACL 规则，包过滤防火墙需要记录每一个首片分片的三层以外的信息，当后续分片到达时，使用这些保存的信息对 ACL 规则的每一个匹配条件进行精确匹配。

应用精确匹配过滤后，包过滤防火墙的执行效率会略微降低，配置的匹配项目越多，效率降低越多，可以配置门限值来限制防火墙最大处理的数目。

有关标准匹配及精确匹配的概念参见 第3章 访问控制列表配置。

5.1.2 ASPF 简介

ACL/包过滤防火墙为静态防火墙，目前存在如下问题：

- 对于多通道的应用层协议（如 FTP, H.323 等），部分安全策略配置无法预知。
- 无法检测某些来自于应用层的攻击行为（如 TCP SYN、Java Applet、ActiveX 等）。

故提出了状态防火墙——ASPF 的概念。ASPF（Application Specific Packet Filter）是针对应用层及传输层的包过滤，即基于状态的报文过滤。ASPF 能够实现的应用层协议检测包括：FTP、HTTP、SMTP、RTSP、H.323（Q.931, H.245, RTP/RTCP）、SNMP、SQLNET 检测；能够实现的传输层协议检测包括：通用 TCP/UDP 检测。

ASPF 的主要功能如下：

- 能够检查应用层协议信息，如报文的协议类型和端口号等信息，并且监控基于连接的应用层协议状态。对于所有连接，每一个连接状态信息都将被 ASPF 维护并用于动态地决定数据包是否被允许通过防火墙进入内部网络，以便阻止恶意的入侵。
- 能够检测传输层协议信息（即通用 TCP 和 UDP 协议检测），能够根据源、目的地址及端口号决定 TCP 或 UDP 报文是否可以通过防火墙进入内部网络。

ASPF 的其它功能：

- DoS（Denial of Service，拒绝服务）攻击的检测和防范。
- ASPF 不仅能够根据连接的状态对报文进行过滤还能够对应用层报文的内容加以检测，提供对不可信站点的 Java Blocking（Java 阻断）和 ActiveX Blocking（ActiveX 阻断）功能。
- 增强的会话日志功能。可以对所有的连接进行记录，包括记录连接的时间、源地址、目的地址、使用的端口和传输的字节数。
- 支持应用协议端口映射 PAM（Port to Application Map），允许用户自定义应用层协议使用非通用端口。

在网络边界，ASPF 和普通的静态防火墙协同工作，能够为企业内部网络提供更全面的、更符合实际需求的安全策略。

1. 基本概念

- Java Blocking 和 ActiveX Blocking

Java Blocking 是对通过 HTTP 协议传输的 Java Applet 小程序进行阻断。当配置了 Java Blocking 时，用户为试图在 web 页面中获取包含 Java Applet 的程序而发送的请求指令将会被 ASPF 阻断过滤。当配置了 ActiveX Blocking 时，ASPF 将会对通过 HTTP 协议传输的 ActiveX 控件进行阻断，防止用户安装不安全的或恶意的控件。

- 端口映射

应用层协议使用通用的端口号进行通信。端口映射允许用户对不同的应用定义一组新的端口号。端口映射提供了一些机制来维护和使用用户定义的端口配置信息。

PAM 支持两类映射机制：通用端口映射和基于基本访问控制列表（ACL）的主机端口映射。通用端口映射是将用户自定义端口号和应用层协议建立映射关系，例如：将 8080 端口映射为 HTTP 协议，这样所有目标端口是 8080 的 TCP 报文被认为是 HTTP 报文。基于基本访问控制列表的主机端口映射是对去往/来自某些特定主机的报文建立自定义端口号和应用协议的映射，例如：将目的地址为 10.110.0.0 网段的使用 8080 端口的 TCP 报文映射为 HTTP 报文。主机的范围可由基本的 ACL 指定。

- 单通道协议/多通道协议

单通道协议：从会话建立到删除的全过程中，只有一个通道参与数据交互，例如 SMTP，HTTP。

多通道协议：包含一个控制通道和若干其它控制或数据通道，即控制信息的交互和数据的传送是在不同的通道上完成的，例如 FTP，RTSP。

- 内部接口和外部接口

如果防火墙连接了内部网和 Internet，并且防火墙要通过部署 ASPF 来保护内部网的服务器，则防火墙上与内部网连接的接口就是内部接口，与 Internet 相连的接口就是外部接口。

当 ASPF 应用于防火墙外部接口的出方向时，可以在防火墙上为内部网用户访问 Internet 的返回报文打开一个临时通道。

2. 应用层协议检测的基本原理

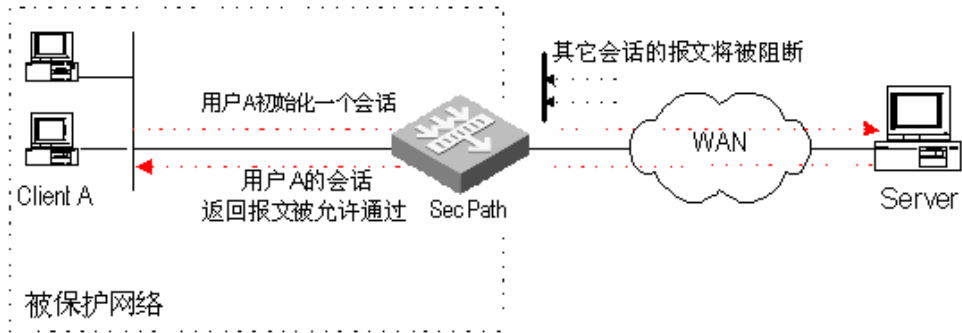


图5-1 应用层协议检测的基本原理

如上图所示，为了保护内部网络，一般情况下需要在防火墙上配置静态访问控制列表，以便允许内部网的主机访问外部网络，同时拒绝外部网络的主机访问内部网络。但静态访问控制列表会将用户发起连接后返回的报文过滤掉，导致连接无法正常建立。当在防火墙上配置了应用层协议检测后，ASPF可以检测每一个应用层的会话，并创建一个状态表和一个临时访问控制表（TACL）。状态表在检测到第一个外发报文时创建，用于维护一次会话中某一时刻会话所处的状态，并检测会话状态的转换是否正确。临时访问控制列表的表项在创建状态表项的时候同时创建，会话结束后删除，它相当于一个高级ACL的permit项。TACL主要用于匹配一个会话中的所有返回的报文，可以为某一应用返回的报文在防火墙的外部接口上建立了一个临时的返回通道。

下面以FTP检测为例说明多通道应用层协议检测的过程。

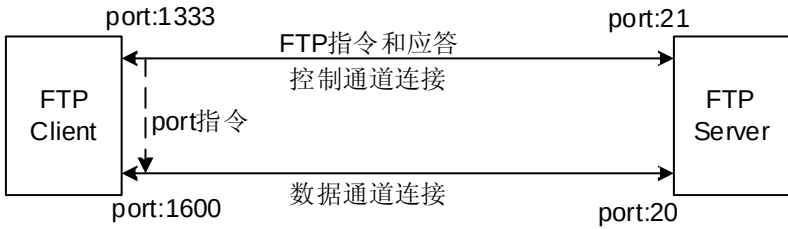


图5-2 FTP检测过程示意图

FTP连接的建立过程如下：

假设FTP Client以1333端口向FTP Server的21端口发起FTP控制通道的连接，通过协商决定由Server端的20端口向Client端的1600端口发起数据通道的连接，数据传输超时或结束后连接删除。

FTP检测在FTP连接建立到拆除过程中的处理如下：

- (1) 检查从出接口上向外发送的IP报文，确认为基于TCP的FTP报文。
- (2) 检查端口号确认连接为控制连接，建立返回报文的TACL和状态表。

- (3) 检查 FTP 控制连接报文，解析 FTP 指令，根据指令更新状态表，如果包含数据通道建立指令，则创建数据连接的 TACL；对于数据连接，不进行状态检测。
- (4) 对于返回报文，根据协议类型做相应匹配检查，检查将根据相应协议的状态表和 TACL 决定报文是否允许通过。
- (5) FTP 连接删除时，状态表及 TACL 随之删除。

单通道应用层协议（例如 SMTP，HTTP）的检测过程比较简单，当发起连接时建立 TACL，连接删除时随之删除 TACL 即可。

3. 传输层协议检测基本原理

这里的传输层协议检测是指通用 TCP/UDP 检测。通用 TCP 和 UDP 检测与应用层协议检测不同，是对报文的传输层信息进行的检测，如源、目的地址及端口号等。通用 TCP/UDP 检测要求返回到 ASPF 外部接口的报文要与前面从 ASPF 外部接口发出去的报文完全匹配，即源、目的地址及端口号恰好对应，否则返回的报文将被阻塞。因此对于 FTP，H.323 这样的多通道应用层协议，在不配置应用层检测而直接配置 TCP 检测的情况下会导致连接无法建立。

5.2 包过滤防火墙配置

包过滤防火墙的配置包括：

- 允许或禁止防火墙
- 设置防火墙缺省过滤方式
- 设置包过滤防火墙分片报文检测开关
- 配置分片报文检测的上、下门限值
- 在接口上应用访问控制列表

5.2.1 使能或禁止包过滤防火墙

请在系统视图下进行下列配置。

表5-1 允使能或禁止包过滤防火墙

操作	命令
使能包过滤防火墙	firewall packet-filter enable
禁止包过滤防火墙	undo firewall packet-filter enable

缺省情况下，SecPath 系列防火墙使能包过滤防火墙功能，SecPath 系列安全网关禁止包过滤防火墙功能。

5.2.2 设置防火墙缺省过滤方式

设置防火墙的缺省过滤方式，即在没有一个合适的规则去判定用户数据包是否可以通过的时候，防火墙采取的策略是允许还是禁止该数据包通过。

请在系统视图下进行下列配置。

表5-2 设置防火墙缺省过滤方式

操作	命令
设置缺省过滤方式为允许通过	firewall packet-filter default permit
设置缺省过滤方式为禁止通过	firewall packet-filter default deny

在防火墙开启时，系统缺省为拒绝任何报文通过。

当防火墙工作在透明模式下，若缺省过滤方式为 **deny**，除了绑定编号为 4000~4999 的以太网 ACL 外，还需要绑定编号为 1000~1999 的接口 ACL，才能正常转发报文。

5.2.3 设置包过滤防火墙分片报文检测开关

请在系统视图下进行下列配置。

表5-3 设置分片报文检测开关

操作	命令
打开分片报文检测开关	firewall packet-filter fragments-inspect
关闭分片报文检测开关	undo firewall packet-filter fragments-inspect



注意：

只有打开了分片报文检测开关，精确匹配模式才能真正有效。

5.2.4 配置分片报文检测的上、下门限值

请在系统视图下进行下列配置。

表5-4 配置分片报文检测的上、下门限值

操作	命令
指定上、下限分片状态记录数目	firewall packet-filter fragments-inspect { high low } { default number }
恢复上限分片状态记录数目为缺省值	undo firewall packet-filter fragments-inspect { high low }

缺省的上限（**high**）分片状态记录数目为 2000；下限（**low**）分片状态记录数目为 1500。

5.2.5 在接口上应用访问控制列表

将访问规则应用到接口时，同时会遵循时间段过滤原则，另外可以对接口的收发报文分别指定访问规则。

请在接口视图下进行下列配置。

表5-5 在接口上应用访问控制列表

操作	命令
指定接口上过滤接收报文的规则	firewall packet-filter <i>acl-number</i> { inbound outbound } [match-fragments { normally exactly }]
取消接口上过滤接收报文的规则	undo firewall packet-filter <i>acl-number</i> { inbound outbound }

基于接口的访问控制列表（即序号为 1000 到 1999 的 ACL）只能用参数 **outbound**。接口访问控制列表用来匹配从特定接口接收到的报文，然后允许或拒绝匹配的报文从某接口（包括接收报文的接口）发送出去。

高级访问控制列表提供标准匹配和精确匹配两种匹配方式。标准匹配即三层信息的匹配，匹配将忽略三层以外的信息；精确匹配则对所有的高级 ACL 的过滤规则进行匹配，这就要求防火墙必须记录首片分片报文的状态以获得完整的后续分片的匹配信息。

缺省的模式为标准匹配方式。

match-fragments 参数仅能应用于高级访问控制列表。

只有在启用包过滤防火墙功能后，在接口上应用的访问控制列表才能生效。

5.2.6 包过滤防火墙显示与调试

在完成上述配置后，在所有视图下执行如下 **display** 命令可以显示包过滤防火墙的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **debugging** 命令可以对包过滤防火墙进行调试。

表5-6 防火墙显示与调试

操作	命令
显示防火墙的统计信息	display firewall packet-filter statistics { all interface type number fragments-inspect }
显示分片表	display firewall fragment

操作	命令
打开防火墙包过滤调试信息开关	debugging firewall packet-filter { { all icmp tcp udp fragments-inspect others } [interface type number] denied permitted }
关闭防火墙包过滤调试信息开关	undo debugging packet-filter firewall { { all icmp tcp udp fragments-inspect others } [interface type number] denied permitted }
打开分片报文的检测事件信息的调试开关	debugging firewall packet-filter fragments-inspect events
关闭分片报文的检测事件信息的调试开关	undo debugging firewall packet-filter fragments-inspect events
清除包过滤防火墙的统计信息	reset firewall packet-filter statistics { all interface type number }

5.2.7 包过滤防火墙典型配置举例

1. 组网需求

以下通过一个公司配置防火墙的实例来说明防火墙的配置。

该公司通过一台 SecPath 防火墙的接口 Ethernet1/0/0 访问 Internet，防火墙与内部网通过以太网接口 Ethernet0/0/0 连接。公司内部对外提供 WWW、FTP 和 Telnet 服务，公司内部子网为 129.38.1.0，其中，内部 FTP 服务器地址为 129.38.1.1，内部 Telnet 服务器地址为 129.38.1.2，内部 WWW 服务器地址为 129.38.1.3，公司对外地址为 202.38.160.1。在防火墙上配置了地址转换，这样内部 PC 机可以访问 Internet，外部 PC 可以访问内部服务器。通过配置防火墙，希望实现以下要求：

- 外部网络只有特定用户可以访问内部服务器。
- 内部网络只有特定主机可以访问外部网络。

假定外部特定用户的 IP 地址为 202.39.2.3。

2. 组网图

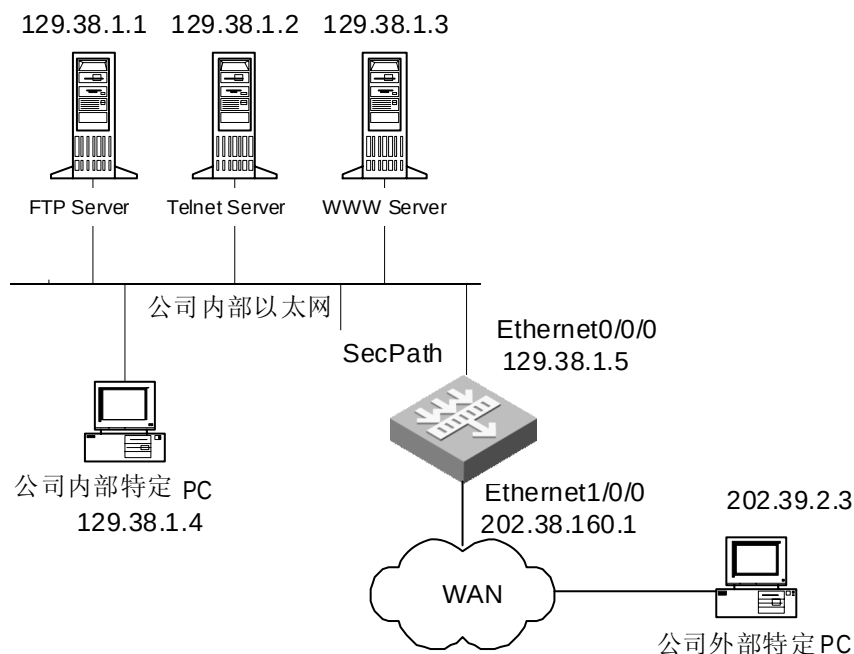


图5-3 包过滤防火墙配置案例组网图

3. 配置步骤

使能包过滤防火墙。

```
[H3C] firewall packet-filter enable
```

设置防火墙缺省过滤方式为允许包通过。

```
[H3C] firewall packet-filter default permit
```

创建访问控制列表 3001。

```
[H3C] acl number 3001
```

配置规则允许特定主机访问外部网，允许内部服务器访问外部网。

```
[H3C-acl-adv-3001] rule permit ip source 129.38.1.4 0
```

```
[H3C-acl-adv-3001] rule permit ip source 129.38.1.1 0
```

```
[H3C-acl-adv-3001] rule permit ip source 129.38.1.2 0
```

```
[H3C-acl-adv-3001] rule permit ip source 129.38.1.3 0
```

```
[H3C-acl-adv-3001] rule deny ip
```

创建访问控制列表 3002。

```
[H3C] acl number 3002
```

配置规则允许特定用户从外部网访问内部服务器。

```
[H3C-acl-adv-3002] rule permit tcp source 202.39.2.3 0 destination 129.38.1.0  
0.0.0.3
```

配置规则允许特定用户从外部网取得数据（只允许端口大于 1024 的包）。

```
[H3C-acl-adv-3002] rule permit tcp destination 129.38.1.4 0 destination-port  
gt 1024
```

```
[H3C-acl-adv-3002] rule deny ip
```

将规则 3001 作用于从接口 Ethernet0/0/0 进入的包。

```
[H3C-Ethernet0/0/0] firewall packet-filter 3001 inbound
```

将规则 3002 作用于从接口 Ethernet1/0/0 进入的包。

```
[H3C-Ethernet1/0/0] firewall packet-filter 3002 inbound
```

5.2.8 包过滤防火墙分片报文处理配置举例

1. 组网需求

该公司通过一台 SecPath 防火墙的接口 Ethernet1/0/0 访问 Internet，防火墙与内部网通过以太网接口 Ethernet0/0/0 连接。公司内部对外提供 WWW 和 Telnet 服务，公司内部子网为 200.1.1.0/24。内部 WWW 服务器地址为 200.1.1.1，内部 Telnet 服务器地址为 200.1.1.2，防火墙的外部接口 Ethernet1/0/0 的地址为 202.38.160.1。为了防止外部攻击者对内部 WWW 和 Telnet 服务器进行分片报文攻击，在防火墙外部接口的入方向上应用 ACL，以阻止到达内部服务器的分片报文。

2. 组网图

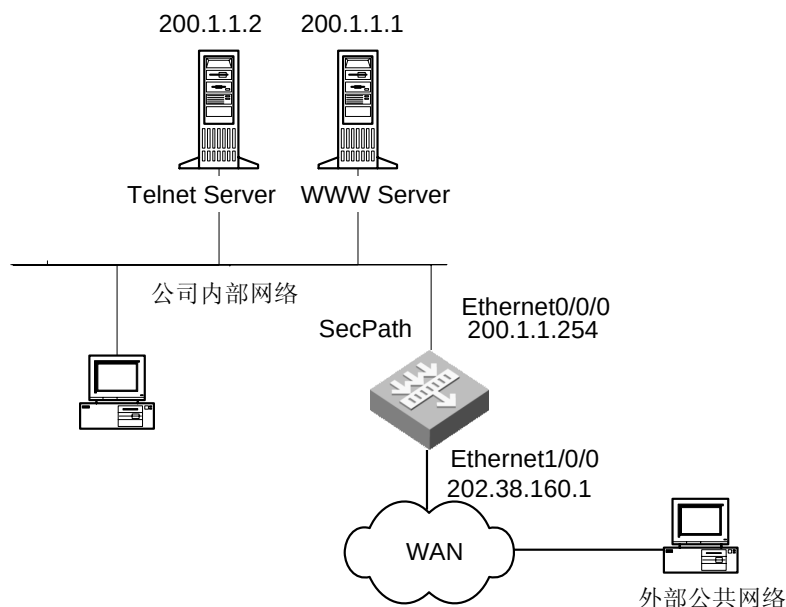


图5-4 包过滤防火墙分片报文处理组网图

3. 配置步骤

配置 ACL，使防火墙阻止来自外部网络到 WWW 和 Telnet 服务器的分片报文。

```
[H3C] acl number 3001
[H3C-acl-adv-3001] rule 1 deny ip source any destination 200.1.1.1 0 fragment
[H3C-acl-adv-3001] rule 2 deny ip source any destination 200.1.1.2 0 fragment
[H3C-acl-adv-3001] rule 3 permit tcp source any destination 200.1.1.1 0
destination-port eq 80
[H3C-acl-adv-3001] rule 4 permit tcp source any destination 200.1.1.2 0
destination-port eq 23
[H3C-acl-adv-3001] rule 5 deny ip
[H3C-acl-adv-3001] quit
```

配置包过滤防火墙，将 ACL 应用到外部接口的入方向。

```
[H3C] interface Ethernet 1/0/0
[H3C-Ethernet1/0/0] firewall packet-filter 3001 inbound
```

以上配置中的入站 ACL 只用于阻止到特定内部服务器的分片报文，并允许外部主机访问内部服务器。若要使由内部主机初始的会话的返回流量通过防火墙，还需添加其它的 ACL 规则，或者使用 ASPF 状态防火墙。

5.3 ASPF 配置

ASPF 主要配置包括：

- 允许防火墙
- 配置访问控制列表
- 定义一个 ASPF 策略
- 在选定的接口上应用 ASPF 策略

5.3.1 允许防火墙

此配置与包过滤防火墙配置相同，请参见上一节的内容。

5.3.2 配置访问控制列表

为了保护内部网络，需要在防火墙上配置访问控制列表，允许内部网的主机访问外部网络，同时拒绝外部网络的主机访问内部网络，并将访问控制列表应用到外部接口上。

表5-7 配置访问控制列表

操作	命令
配置访问控制列表（在 ACL 视图下）	rule deny
将 ACL 应用到出接口上（在接口视图下）	firewall packet-filter <i>acl-num</i> inbound

5.3.3 定义 ASPF 策略

请按以下步骤定义一个 ASPF 策略：

- 创建一个 ASPF 策略；
- 配置空闲超时值；
- 配置应用层协议检测；
- 配置通用 TCP 和 UDP 检测。

1. 创建一个 ASPF 策略

请在系统视图下进行下列配置

表5-8 创建一个 ASPF 策略

操作	命令
创建一个 ASPF 策略	aspf-policy <i>aspf-policy-number</i>
删除创建一个 ASPF 策略	undo aspf-policy <i>aspf-policy-numbe</i>

aspf-policy-number 为 ASPF 策略号，范围为 1～99。

2. 配置空闲超时值

请在 ASPF 策略视图下进行下列配置。

表5-9 配置空闲超时值

操作	命令
配置空闲超时值	aging-time { <i>syn</i> <i>fin</i> <i>tcp</i> <i>udp</i> } <i>seconds</i>
恢复默认的空闲超时值	undo aging-time { <i>syn</i> <i>fin</i> <i>tcp</i> <i>udp</i> }

该任务用来配置 TCP 的 SYN 状态等待超时值、FIN 状态等待超时值，TCP 和 UDP 会话表项空闲状态超时值的缺省值。缺省情况 SYN、FIN、TCP、UDP 的超时时间分别为 30s、30s、3600s 和 30s。

3. 配置应用层协议检测

请在 ASPF 策略视图下进行下列配置。

表5-10 配置应用层协议检测

操作	命令
为应用层协议配置 ASPF 检测	detect protocol [<i>acl number</i>] [<i>aging-time seconds</i>]
删除配置的应用协议检测	undo detect protocol [<i>acl number</i>]

应用层协议包括：FTP、HTTP、H.323、SMTP、SNMP、RTSP、SQLNET；传输层协议包括：TCP、UDP。应用层协议的超时时间缺省值为 3600 秒。基于 TCP 协议的超时时间缺省值为 3600 秒；基于 UDP 协议的 **timeout** 超时时间缺省值为 30 秒。当 *protocol* 为 FTP、SMTP 和 SNMP 时，支持 **acl** 选项。

在 *protocol* 选择 http 时，可以配置 Java 阻断和 ActiveX 阻断。

表5-11 配置 Java 阻断和 ActiveX 阻断检测

操作	命令
配置 Java 阻断检测	detect http [java-blocking [acl-number1] activex-blocking [acl-number2]]* [aging-time seconds]
取消对 HTTP 的检测规则	undo detect http [java-blocking activex-blocking]*

说明：

目前 Java 阻断功能只能过滤 HTTP 请求中以 “.class” 为后缀的 Java 请求。

4. 配置通用 TCP 和 UDP 协议检测

请在 ASPF 策略视图下进行下列配置。

表5-12 配置通用 TCP 和 UDP 协议检测

操作	命令
配置通用 TCP 协议检测	detect tcp [aging-time seconds]
配置通用 UDP 协议检测	detect udp [aging-time seconds]
删除通用 TCP 协议检测	undo detect tcp
删除通用 UDP 协议检测	undo detect udp

基于 TCP 协议的超时时间缺省值为 3600 秒；基于 UDP 协议的超时时间缺省值为 30 秒。

在不配置应用层检测，直接配置 TCP 或 UDP 检测的情况下，可能会产生部分报文无法返回的情况，故建议应用层检测和 TCP/UDP 检测配合使用。

说明：

对于 Telnet 应用，直接配置通用 TCP 检测即可实现 ASPF 功能。

5.3.4 在接口上应用 ASPF 策略

将定义好的 ASPF 策略应用到外部接口上，才能对通过接口的流量进行检测。

请在接口视图下进行下列配置。

表5-13 在接口上应用 ASPF 策略

操作	命令
在接口上应用 ASPF 策略	firewall aspf aspf-policy-number { inbound outbound }
删除该接口上应用的 ASPF 策略	undo firewall aspf aspf-policy-number { inbound outbound }

由于 ASPF 对于应用层协议状态的保存和维护都是基于接口的，因此，在实际应用中，必须保证报文入口的一致性，即必须保证连接发起报文和返回报文基于同一接口。

5.3.5 配置协议超时时间

该命令用于配置各种协议在会话表中的超时时间。

请在系统视图下进行下列配置。

表5-14 配置协议超时时间

操作	命令
配置所有协议超时时间为缺省值	firewall session aging-time default
配置各个协议的超时时间	firewall session aging-time { fin-rst fragment ftp h323 http icmp netbios ras rtsp smtp syn tcp telnet udp } { default seconds }

各种协议的缺省超时时间请参考命令手册。

说明：

请勿将 syn 的超时时间配置为与 fin-rst 或 tcp 的超时时间相同，否则表项的时间更新会失败。

5.3.6 配置 ASPF 的会话日志功能

ASPF 提供了增强的会话日志功能。可以对所有的连接进行记录，包括连接的时间、源地址、目的地址、使用的端口和传输的字节数。

请在 ASPF 策略视图下进行下列配置。

表5-15 配置 ASPF 的会话日志功能

操作	命令
使能 ASPF 的会话日志功能	log enable
关闭 ASPF 的会话日志功能	undo log enable

缺省情况下，关闭会话日志功能。

5.3.7 端口映射配置

请在系统视图下进行下列配置。

表5-16 配置端口映射

操作	命令
配置通用端口映射功能	port-mapping <i>application-name</i> port <i>port-number</i>
删除用户配置的通用端口映射	undo port-mapping <i>application-name</i> port <i>port-number</i>
配置主机端口映射功能	port-mapping <i>application-name</i> port <i>port-number</i> acl <i>acl-number</i>
删除用户配置的主机端口映射	undo port-mapping <i>application-name</i> port <i>port-number</i> acl <i>acl-number</i>

主机端口映射中特定主机的范围应由基本的 ACL 指定。

当配置监听非标准端口的应用层协议检测时（如 HTTP 监听的端口号为 8080，而非标准的端口号 80），需使用此命令配置相应的端口映射，以使 ASPF 状态检测正常工作。

5.3.8 ASPF 显示与调试

在完成上述配置后，在所有视图下执行如下 **display** 命令可以显示 ASPF 的运行情况，通过查看显示信息验证配置的效果。在用户视图下执行 **debugging** 命令查看 ASPF 调试信息。

表5-17 ASPF 显示与调试

操作	命令
显示所有 ASPF 配置情况	display aspf all
显示应用 ASPF 策略和访问列表的接口配置	display aspf interface
显示一个特定 ASPF 策略的配置	display aspf policy <i>aspf-policy-number</i>
显示 ASPF 当前会话状态	display aspf session [<i>verbose</i>]
显示 ASPF 统计信息	display aspf statistics

操作	命令
显示防火墙的会话表信息	display firewall session table [<i>verbose</i>] [<i>source ip-address</i>] [<i>destination ip-address</i>]
显示协议的会话超时时间	display firewall session aging-time
显示端口映射信息	display port-mapping [<i>application-name</i> <i>port port-number</i>]
打开 ASPF 调试开关	debugging aspf { <i>all</i> <i>verbose</i> <i>events</i> <i>ftp</i> <i>h323</i> <i>rtsp</i> <i>session</i> <i>smtp</i> <i>sqlnet</i> <i>tcp</i> <i>timers</i> <i>udp</i> }
关闭 ASPF 调试开关	undo debugging aspf { <i>all</i> <i>verbose</i> <i>events</i> <i>ftp</i> <i>h323</i> <i>rtsp</i> <i>session</i> <i>smtp</i> <i>sqlnet</i> <i>tcp</i> <i>timers</i> <i>udp</i> }
打开 HTTP 调试开关	debugging aspf http { <i>java-blocking</i> <i>activex-blocking</i> } { <i>all</i> <i>error</i> <i>event</i> <i>filter</i> <i>packet</i> }
关闭 HTTP 调试开关	undo debugging aspf http { <i>java-blocking</i> <i>activex-blocking</i> } { <i>all</i> <i>error</i> <i>event</i> <i>filter</i> <i>packet</i> }
清除 ASPF 的会话信息	reset aspf session
清除 ASPF HTTP 的统计信息	reset aspf statistic http [<i>java-blocking</i> <i>activex-blocking</i>]
清除防火墙的会话表信息	reset firewall session table

5.3.9 ASPF 使用注意事项

当使用 **detect**、**aging-time**、**port-mapping** 命令对现有的 ASPF 策略进行修改后，所做的修改只会对后续新建立的 session 有效，对于已经建立的 session 是不起作用的。如果不希望出现 session 与 ASPF 策略不一致的情况，可以手工清除 session，但这将导致当前已建立的 session 被中断。

5.3.10 ASPF 典型配置案例

1. 组网需求

在防火墙上配置一 ASPF 策略，检测通过防火墙的 FTP 和 HTTP 流量。要求：如果该报文是内部网络用户发起的 FTP 和 HTTP 连接的返回报文，则允许其通过防火墙进入内部网络，其他报文被禁止；并且，此 ASPF 策略能够过滤掉来自服务器 2.2.2.11 的 HTTP 报文中的 Java Applet。本例可以应用在本地用户需要访问远程网络服务的情况下。

2. 组网图

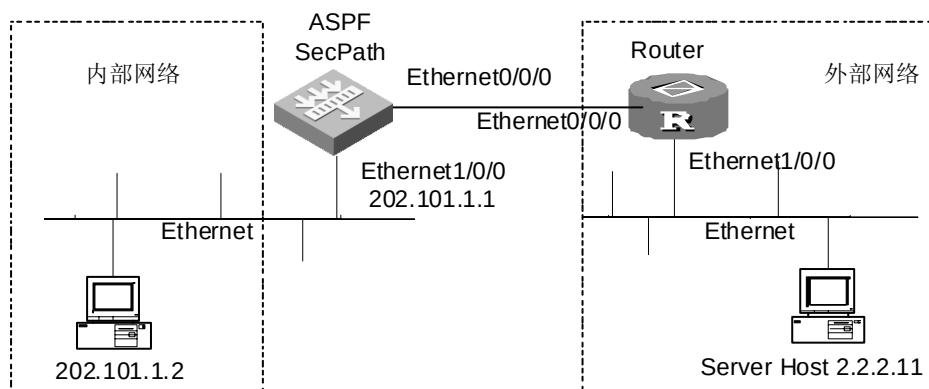


图5-5 ASPF 配置案例组网图

3. 配置步骤

使能包过滤防火墙功能。

```
[H3C] firewall packet-filter enable
```

配置访问控制列表 3111，以拒绝所有 TCP 和 UDP 流量进入内部网络，ASPF 会为允许通过的流量创建临时的访问控制列表。

```
[H3C] acl number 3111
[H3C-acl-adv-3111] rule deny tcp
[H3C-acl-adv-3111] rule deny udp
[H3C-acl-adv-3111] rule permit ip
[H3C-acl-adv-3111] quit
```

配置访问控制列表 2001，以过滤来自站点 2.2.2.11 的 Java Applet。

```
[H3C] acl number 2001
[H3C-acl-basic-2001] rule permit source 2.2.2.11 0
[H3C-acl-basic-2001] rule deny
[H3C-acl-basic-2001] quit
```

创建 ASPF 策略，策略号为 1，该策略检测应用层的两个协议：FTP 和 HTTP 协议，并定义没有任何行为的情况下，FTP 协议的超时时间为 3000 秒。

```
[H3C] aspf-policy 1
[H3C-aspf-policy-1] detect ftp aging-time 3000
[H3C-aspf-policy-1] detect http java-blocking 2001 aging-time 3000
[H3C-aspf-policy-1] quit
```

在接口上应用 ASPF 策略。

```
[H3C] interface Ethernet0/0/0
[H3C-Ethernet0/0/0] firewall aspf 1 outbound
```

在接口上应用访问控制列表 3111。

```
[H3C-Ethernet0/0/0] firewall packet-filter 3111 inbound
```

5.4 黑名单

5.4.1 黑名单简介

黑名单是根据报文的源 IP 地址进行过滤的一种方式。同基于 ACL 的包过滤功能相比，由于黑名单进行匹配的域非常简单，可以以很高的速度实现报文的过滤，从而有效地将特定 IP 地址发送来的报文屏蔽。黑名单最主要的一个特色是可以由 SecPath 防火墙动态地进行添加或删除，当防火墙中根据报文的行为特征察觉到特定 IP 地址的攻击企图之后，通过主动修改黑名单列表从而将该 IP 地址发送的报文过滤掉。因此，黑名单是防火墙一个重要的安全特性。

1. 黑名单的创建

黑名单表项有两种创建方式：通过命令行手工创建或由防火墙其他模块动态创建并插入黑名单列表。

(1) 通过命令行接口配置黑名单表项

可以使用如下的命令创建一条黑名单表项：

```
firewall blacklist sour-addr [ timeout minutes ]
```

在配置表项时，若使用 **timeout minutes** 参数，则意味着该黑名单表项会在指定的老化时间后被自动删除，从而对源自相应 IP 地址的报文过滤功能也随之消失；反之，若不使用该参数，则意味着该表项始终有效，不会被老化。

(2) 防火墙相关模块动态创建黑名单表项

防火墙相关模块可以动态的向黑名单中插入表项。比如，当攻击防范模块察觉到特定 IP 地址的攻击之后，如果进行了相关设定，则会将这个 IP 地址自动插入到黑名单表中。此后的一定时间内，来自这个 IP 地址的任何报文，都将被黑名单过滤掉。

当防火墙相关模块准备向黑名单插入的 IP 地址已经存在于黑名单之中，如果准备插入的老化时间比原有表项的老化时间要小，那么将会放弃插入操作。

目前，可以主动向黑名单中插入表项的防火墙模块是攻击防范模块，相应的配置请见第 12 章 攻击防范中的描述。

2. 黑名单表项的删除

可以通过如下命令删除黑名单表项：

```
undo firewall blacklist [ sour-addr ]
```

当使用 **sour-addr** 参数时，特定 IP 地址的表项会被删除。如果不使用 **sour-addr** 参数，那么当前黑名单表中所有的表项都会被删除。

黑名单表项的插入和删除独立于黑名单功能的运行状况，也就是说，无论黑名单是否被使能，都可以进行黑名单表项的插入和删除操作。

3. 黑名单的使能

黑名单功能在使能之后，才会对命中黑名单表项的报文进行过滤。否则，即使报文源地址在黑名单中，也不会被防火墙丢弃。

可以使用如下命令使能黑名单功能：

firewall blacklist enable

使用如下命令禁止黑名单功能：

undo firewall blacklist enable

防火墙缺省不使能黑名单功能。

5.4.2 黑名单配置

黑名单的配置包括：

- 配置黑名单表项
- 使能或禁止黑名单

1. 配置/删除黑名单表项

请在系统视图下进行下列配置。

表5-18 配置黑名单表项

操作	命令
配置黑名单表项	firewall blacklist sour-addr [timeout minutes]
删除黑名单表项	undo firewall blacklist [sour-addr]

插入表项时 *minutes* 的取值范围为 1~1000，单位为分钟。如果没有 **timeout minutes** 参数，表示此黑名单表项不进行老化。如果删除黑名单表项时没有 *sour-addr* 参数，表示删除当前黑名单中所有表项。

2. 使能/禁止黑名单

请在系统视图下进行下列配置。

表5-19 使能/禁止黑名单

操作	命令
使能黑名单功能	firewall blacklist enable
禁止黑名单功能	undo firewall blacklist enable

缺省情况下，未启动黑名单功能。

5.4.3 黑名单显示与调试

在所有视图下可以使用 **display** 命令，显示黑名单表项或黑名单功能的运行状态。
在用户视图下执行 **debugging** 命令，可以打开黑名单的调试开关。

表5-20 黑名单的显示和调试

操作	命令
显示当前黑名单表项信息或运行状态	display firewall blacklist { enable item [sour-addr] }
打开黑名单的调试开关	debugging firewall blacklist { all item packet }

5.4.4 黑名单典型配置案例

1. 组网需求

服务器和客户机分别位于防火墙 Trust 区域和 Untrust 区域中，现要在 100 分钟内过滤掉客户机发送的所有报文。

2. 组网图

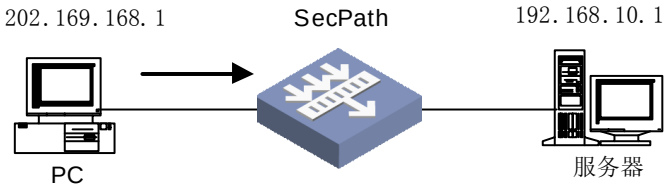


图5-6 黑名单过滤的组网图

3. 配置步骤

配置客户机地址到黑名单表项中。

```
[H3C] firewall blacklist 202.169.168.1 timeout 100
```

使能黑名单功能。

```
[H3C] firewall blacklist enable
```

经过以上配置，则在老化时间内（100 分钟），所有从客户机发出的报文都会被防火墙过滤掉。超过老化时间之后，该客户机的报文可以通过防火墙。

5.5 MAC 和 IP 地址绑定

5.5.1 MAC 和 IP 地址绑定简介

MAC 和 IP 地址绑定，指防火墙可以根据用户的配置，在特定的 IP 地址和 MAC 地址之间形成关联关系。对于声称从这个 IP 地址发送的的报文，如果其 MAC 地址不是指定关系对中的地址，防火墙将予以丢弃，是避免 IP 地址假冒攻击的一种方式。

1. MAC 和 IP 地址绑定的创建

可以使用如下的命令创建一条地址绑定关系：

firewall mac-binding ip-addr mac-addr

地址绑定关系以 IP 地址为插入的依据，如果使用命令行多次配置同一 IP 地址到地址绑定关系中，则后配置的表项会覆盖原有表项。同一个 MAC 地址可以同多个不同的 IP 地址绑定。

2. MAC 和 IP 地址绑定的删除

可以使用如下命令删除一个地址绑定关系：

undo firewall mac-binding [ip-addr]

当使用带 *ip-addr* 参数的命令时，特定 IP 地址的绑定关系会被删除。如果不指定 *ip-addr* 参数，那么当前地址绑定关系表中所有的表项都会被删除。

地址绑定关系的插入和删除独立于地址绑定功能的运行状况，也就是说，无论地址绑定是否被使能，都可以进行地址绑定关系的创建和删除操作。

3. MAC 和 IP 地址绑定的使能

地址绑定功能在使能之后，才会对命中地址绑定关系的报文进行 IP 地址和 MAC 地址绑定关系的比较，并对不符合绑定关系的报文进行过滤。否则，即使报文的 IP 地址和 MAC 地址不符合绑定关系，也不会被防火墙丢弃掉。

可以使用如下命令使能地址绑定功能：

firewall mac-binding enable

使用如下命令停止地址绑定功能：

undo firewall mac-binding enable

防火墙缺省不使能地址绑定功能。

5.5.2 MAC 和 IP 地址绑定配置

MAC 和 IP 地址绑定的配置包括：

- 配置 MAC 和 IP 地址绑定关系
- 使能或禁止 MAC 和 IP 地址绑定功能

1. 配置 MAC 和 IP 地址绑定关系

请在系统视图下进行下列配置。

表5-21 配置 MAC 和 IP 地址绑定

操作	命令
配置 MAC 和 IP 地址绑定关系	firewall mac-binding <i>ip-addr mac-addr</i>
删除 MAC 和 IP 地址绑定关系	undo firewall mac-binding [<i>ip-addr</i>]

删除地址绑定关系时，如果没有 *ip-addr* 参数，表示删除当前所有地址绑定关系。



注意：

- 地址绑定关系是静态 ARP 的另一种表现形式，配置地址绑定关系对报文的影响与配置静态 ARP 表项一致。在使能地址绑定功能的情况下，如果配置的地址绑定关系中的 IP 地址已经存在于静态 ARP 表中，则静态 ARP 表中的表项将被删除；如果配置静态 ARP 时已经存在相同 IP 地址的地址绑定关系表项，该静态 ARP 将配置失败，同时返回提示信息。在没有使能地址绑定功能的情况下，两者可以共存。
- MAC 和 IP 地址绑定对于 PPPoE 的地址是不起作用的，因为以太帧上面承载的是 PPP 报文，所以无法进行判断和处理。
- 不能将 A、B、C 类地址的广播地址进行绑定。
- 当被绑定的地址与防火墙的接口 IP 地址不在同一网段时，系统将会提示 “The IP address is not in the same subnet of the interfaces' IP address（绑定的 IP 地址与接口的 IP 地址不在同一子网）”，但绑定条目仍然会被创建。
- 在 MAC 和 IP 地址绑定功能使能的情况下，MAC 和 IP 地址绑定条目一旦被创建，就会被立即应用，防火墙将对所有通过的数据包进行检查，一旦不符合条件就被丢弃。由于报文经过路由转发会改变 MAC 地址，因此如果配置非直连网段的 IP 地址绑定，那么经过路由转发的该 IP 报文可能由于选择的路由不同而改变其 MAC 地址，如果 MAC 地址不匹配，这些报文将会被丢弃，造成不必要的通信中断。

2. 使能或禁止 MAC 和 IP 地址绑定功能

请在系统视图下进行下列配置。

表5-22 使能或禁止 MAC 和 IP 地址绑定功能

操作	命令
使能 MAC 和 IP 地址绑定功能	firewall mac-binding enable
禁止 MAC 和 IP 地址绑定功能	undo firewall mac-binding enable

缺省情况下，未启动 MAC 和 IP 地址绑定功能。

5.5.3 MAC 和 IP 地址绑定的显示与调试

在所有视图下可以使用 **display** 命令，显示地址绑定关系或地址绑定功能的运行状态。在用户视图下执行 **debugging** 命令，可以对地址绑定功能进行调试。在用户视图下执行 **reset** 命令可以清除 MAC 和 IP 地址绑定的统计信息。

表5-23 地址绑定的显示和调试

操作	命令
显示当前 MAC 和 IP 地址绑定关系信息	display firewall mac-binding item [ip-addr] [statistic]
显示当前 MAC 和 IP 地址绑定功能运行信息	display firewall mac-binding enable
打开 MAC 和 IP 地址绑定的调试开关	debugging firewall mac-binding { all item packet }
清除 MAC 和 IP 地址绑定的统计信息	reset firewall mac-binding item [ip-addr] statistic

5.5.4 MAC 和 IP 地址绑定典型配置案例

1. 组网需求

服务器和客户机分别位于防火墙 Trust 区域和 Untrust 区域中，客户机的 IP 地址为 202.169.168.1，对应的 MAC 地址为 00e0-fc00-0100，在防火墙上配置地址绑定关系，保证只有符合上述关系对的报文可以通过防火墙。

2. 组网图

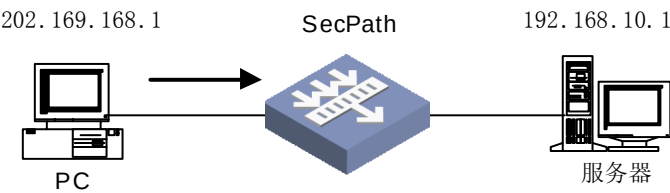


图5-7 地址绑定配置组网图

3. 配置步骤

配置客户机 IP 地址和 MAC 地址到地址绑定关系中。

```
[H3C] firewall mac-binding 202.169.168.1 00e0-fc00-0100
```

使能地址绑定功能。

```
[H3C] firewall mac-binding enable
```

5.6 安全区域配置

5.6.1 安全区域介绍

防火墙使用安全区域的概念来表示与其相连接的网络。防火墙预先定义了四个安全区域，这些安全区域也称为系统安全区域，分别为 **Local** 区域、**Trust** 区域、**Untrust** 区域和 **DMZ** 区域。这些区域分别代表了不同的安全级别，安全级别由高到低依次为 **Local**、**Trust**、**DMZ**、**Untrust**。

- **Local** 区域代表防火墙本地系统，所有发往防火墙自身 IP 地址的报文，都被看作发往防火墙的 **Local** 区域；
- **Trust** 代表用户网络中的私有网络；
- **Untrust** 代表公共网络或不安全的网络，如 **Internet**；
- **DMZ**（**Demilitarized Zone**，非军事区域）区域是一个既不属于内部网络，也不属于外部网络的一个相对独立的区域，它处于内部网络与外部网络之间。例如，在一个提供电子商务服务的网络中，某些主机需要对外提供服务，如 **Web** 服务器、**FTP** 服务器和邮件服务器等。为了更好地提供优质的服务，同时又要有效保护内部网络的安全，就需要将这些对外提供服务的主机与内部网络进行隔离，即放入 **DMZ** 区域中。这样可以有针对性地对内部网络中的设备和这些提供对外服务的主机应用不同的防火墙策略，可以在提供友好的对外服务的同时，最大限度地保护了内部网络。

5.6.2 安全区域配置

1. 进入安全区域视图

请在系统视图下进行下列配置。

表5-24 进入安全区域视图

操作	命令
进入安全区域视图	firewall zone zonenumber

2. 进入区域间视图

请在系统视图下进行下列配置。

表5-25 进入区域间视图

操作	命令
进入区域间视图	firewall interzone zone1 zone2

3. 创建安全区域

请在系统视图下进行下列配置。

表5-26 创建安全区域

操作	命令
创建安全区域	firewall zone name <i>zonename</i>
删除安全区域	undo firewall zone name <i>zonename</i>

缺省情况下，系统预先定义了四个安全区域：Local、Trust、Untrust 和 DMZ。这些系统定义的安全区域是不能被删除的。

4. 为安全区域添加接口

请在区域视图下进行下列配置。

表5-27 为安全区域添加接口

操作	命令
将接口添加到安全区域	add interface <i>interface-type interface-number</i>
将接口从安全区域中删除	undo add interface <i>interface-type interface-number</i>

缺省情况下，所有安全区域中未添加任何接口。

一个接口只能属于一个安全区域。将接口加入到一个安全区域中前，这个接口不能已经属于其它的区域，否则需要先将此接口从其它区域中删除。



注意：

若要实现防火墙和其它设备的互通，必须将相应的接口添加到某一安全区域中。

5. 设置安全区域的优先级

可以为安全区域设置一个优先级，优先级数值越高，表示此区域的安全性越高。

请在区域视图下进行下列配置。

表5-28 设置安全区域的优先级

操作	命令
设置安全区域的优先级	set priority <i>number</i>

缺省情况下，Local 区域的优先级为 100，Trust 区域的优先级为 85，Untrust 区域的优先级为 5，DMZ 区域的优先级为 50。系统定义的这些区域的优先级是不能被更改的。

 **说明：**
不同安全区域之间没有访问限制，且安全区域不支持策略配置，若需要访问控制，请在安全区域中的相应接口进行配置。

5.6.3 安全区域的显示

在任意视图下执行 **display** 命令可以查看安全区域的配置情况。

表5-29 安全区域的显示

操作	命令
显示安全区域所包含的接口	display zone [zone-name] interface
显示安全区域的优先级	display zone [zone-name] priority
显示安全区域所包含的接口和安全区域的优先级	display zone [zone-name]
显示安全区域间的配置信息	display interzone [zone1 zone2]

第6章 面向对象管理

6.1 对象管理简介

面向对象管理通过引入对象管理的概念，将 IP 地址和域名简化为地址对象和地址组对象，将源端口、目的端口以及协议号简化为服务对象和服务组对象，将通常的五元组简化为流对象。用户通过在流对象中简单的引用地址（组）对象和服务（组）对象，大大简化了配置管理的工作，提高了配置管理的易用性、可用性和用户友好性。

6.2 对象创建

系统当前支持以下六类对象的配置管理：

- 地址对象
- 地址组对象
- 服务对象
- 服务组对象
- 流对象
- 时间段对象

6.2.1 地址对象创建

在配置地址组对象和流对象之前，需要先创建地址对象。地址对象是面向对象管理中的基本管理单元，在后续流对象的配置管理中通过引用地址对象可以简化配置。系统支持创建 IP 地址和域名两种类型的地址对象。

请在系统视图下进行下列配置。

表6-1 创建/删除地址对象

操作	命令
创建地址对象	object address <i>object-name</i> { <i>address mask</i> <i>domain-name</i> }
删除地址对象	undo object address <i>object-name</i>

缺省情况下，未创建地址对象。

6.2.2 域名地址对象更新

当域名对应的地址更新后，可以使用此命令及时更新域名地址对象中引用的域名的信息。

请在系统视图下进行下列配置。

表6-2 域名地址对象更新

操作	命令
域名地址对象更新	object refresh dns

6.2.3 地址组对象创建

通过将多个地址对象添加到同一个地址组对象中，可以大大提高配置管理的速度，简化配置管理的操作。

1. 创建/删除地址组对象

请在系统视图下进行下列配置。

表6-3 创建/删除地址组对象

操作	命令
创建地址组对象	object address-group <i>object-group-name</i>
删除地址组对象	undo object address-group <i>object-group-name</i>

缺省情况下，未创建地址组对象。

2. 添加/删除地址组成员

在创建地址组对象后，用户可以将系统中已经存在的地址对象添加到地址组对象中，同一地址对象可以被添加到不同的地址组对象中。

请在地址组对象视图下进行下列配置。

表6-4 添加/删除地址组成员

操作	命令
添加地址组对象成员	add <i>object-name</i>
删除地址组对象成员	undo add <i>object-name</i>

缺省情况下，地址组对象中未添加地址对象。

6.2.4 服务对象创建

在配置服务组对象和流对象之前，需要先创建服务对象。服务对象是面向对象管理中的基本管理单元，在后续流对象的配置管理中通过引用服务对象可以简化配置。

系统支持 ICMP、TCP、UDP 和其它协议的对象配置和管理。通过将协议号、源端口、目的端口、ICMP 消息类型简化为服务对象，简化了配置管理的工作。

请在系统视图下进行下列配置。

表6-5 创建/删除服务对象

操作	命令
创建 TCP 和 UDP 服务对象	object service <i>object-name</i> protocol { <i>tcp</i> <i>udp</i> } [src-port <i>src-port1</i> to <i>src-port2</i>] [dst-port <i>dst-port1</i> to <i>dst-port2</i>]
创建 ICMP 服务对象	object service <i>object-name</i> protocol icmp type <i>icmp-type code icmp-code</i>
创建其它协议类型的服务对象	object service <i>object-name</i> protocol <i>protocol-number</i>
删除服务对象	undo object service <i>object-name</i>

缺省情况下，系统预先定义了多个服务对象，用户可以直接在服务组对象和流对象中引用这些服务对象。可以通过 **display object predefined service** 命令查看预定义的服务对象。

6.2.5 服务组对象创建

1. 创建/删除服务组对象功能

通过将多个服务对象添加到同一个服务组对象中，可以大大提高配置管理的速度，简化配置管理的操作。

请在系统视图下进行下列配置。

表6-6 创建/删除服务组对象功能

操作	命令
创建服务组对象	object service-group <i>object-group-name</i>
删除服务组对象	undo object service-group <i>object-group-name</i>

缺省情况下，未创建服务组对象。

2. 添加/删除服务组成员

在创建服务组对象后，用户可以将系统中已经存在的服务对象添加到服务组对象中，同一服务对象可以被添加到不同的服务组对象中。

请在服务组对象视图下进行下列配置。

表6-7 添加/删除服务组成员

操作	命令
添加服务组成员	add object-name
删除服务组成员	undo add object-name

缺省情况下，服务组对象中未添加服务对象。

6.2.6 流对象创建

1. 创建/删除流对象

系统将通常的五元组简化为流对象，一个流对象中可以包括地址（组）对象、服务（组）对象和时间段对象三类对象信息，方便用户记忆所配置的规则的用途，再通过在不同的应用中引用流对象，可以简化配置管理任务。

请在系统视图下进行下列配置。

表6-8 创建/删除流对象

操作	命令
创建流对象	acl name acl-name
删除流对象	undo acl name acl-name

缺省情况下，未创建流对象。

2. 添加/删除流规则

一个流对象中可以添加多条流规则，系统将根据配置的流规则对数据流进行过滤。

请在流对象视图下进行下列配置。

表6-9 添加/删除流规则

操作	命令
添加流规则	rule [rule-id] { permit deny } [source { src-name src-group-name }] [destination { dst-name dst-group-name }] [service { srv-name srv-group-name }] [time-range time-name] [logging]
删除流规则	undo rule rule-id [source] [destination] [service] [time-range] [logging]

缺省情况下，流对象中未添加流规则。

6.2.7 时间段对象创建

时间段用于描述一个特殊的时间范围。用户可能有这样的需求：一些规则需要在某个或某些特定时间段内生效，而在其他时间段则不利用它们进行过滤，即通常所说的按时间段过滤。这时，用户就可以先配置一个或多个时间段，然后在相应的规则下通过时间段名称引用该时间段，从而实现基于时间段的过滤。

同一个时间段对象中可以包括多个且不同类型的时间段。

请在系统视图下进行下列配置。

表6-10 配置时间段

操作	命令
创建一个时间段	time-range <i>time-name</i> { <i>start-time to end-time days-of-the-week</i> [from <i>start-time start-date</i>] [to <i>end-time end-date</i>] from <i>start-time start-date</i> [to <i>end-time end-date</i>] to <i>end-time end-date</i> }
删除一个时间段	undo time-range <i>time-name</i> [<i>start-time to end-time days-of-the-week</i> [from <i>start-time start-date</i>] [to <i>end-time end-date</i>] from <i>start-time start-date</i> [to <i>end-time end-date</i>] to <i>end-time end-date</i>]

6.3 流对象引用

6.3.1 包过滤中的流对象引用

在包过滤防火墙中，可以通过引用流对象对数据流进行过滤。

请在接口视图下进行下列配置。

表6-11 包过滤中的流对象引用

操作	命令
将流对象应用到包过滤防火墙中	firewall packet-filter <i>acl-name</i> { inbound outbound }
取消流对象在包过滤防火墙中的应用	undo firewall packet-filter <i>acl-name</i> { inbound outbound }

缺省情况下，流对象未应用到包过滤防火墙中。关于包过滤防火墙的内容请参见包过滤防火墙相关章节。

6.3.2 NAT 中的流对象引用

在 NAT 应用中，可以通过引用流对象对指定的数据流进行地址转换。

请在接口视图下进行下列配置。

表6-12 NAT 中的流对象引用

操作	命令
将流对象应用到 NAT 中	nat outbound <i>acl-name</i> [address-group <i>group-number</i> [no-pat]]
取消流对象在 NAT 中的应用	undo nat outbound <i>acl-name</i> [address-group <i>group-number</i> [no-pat]]

缺省情况下，未将流对象应用到 NAT 中。关于 NAT 的内容请参见 NAT 相关章节。

6.4 面向对象管理的显示和调试

在完成上述配置后，在任意视图下执行 **display** 命令可以查看面向对象管理的配置信息和运行情况。在用户视图下，执行 **reset** 命令可以清除统计信息。在用户视图下执行 **debugging** 命令可以打开调试信息开关。

表6-13 面向对象管理的显示和调试

操作	命令
显示地址对象	display object address [<i>object-name</i>]
显示地址组对象	display object address-group [<i>object-group-name</i>]
显示服务对象	display object service [<i>object-name</i>]
显示服务组对象	display object service-group [<i>object-group-name</i>]
显示系统预先定义的服务对象	display object predefined service
显示流对象	display acl { all name <i>acl-name</i> }
显示时间段对象	display time-range { all time-name }
打开地址对象的 DNS 解析调试开关	debugging object dns
关闭地址对象的 DNS 解析调试开关	undo debugging object dns
清除访问规则计数器	reset acl counter { all name <i>acl-name</i> }

第7章 透明防火墙

 说明：

仅 SecPath F100-C 防火墙和 SecPath F100-S 防火墙支持透明防火墙。

7.1 透明模式简介

缺省情况下，防火墙工作在路由模式下。当防火墙工作在透明模式（也可以称为桥接模式）下时，所有接口都不能配置 IP 地址，接口所在的安全区域是二层区域，和二层区域相关接口连接的外部用户同属一个子网。

当报文在二层区域的接口间进行转发时，需要根据报文的 MAC 地址来寻找出接口，此时防火墙表现为一个透明网桥。但是，防火墙与网桥存在不同，防火墙接收到的 IP 报文还需要送到上层进行相关过滤等处理，通过检查会话表或 ACL 规则以确定是否允许该报文通过。此外，还要完成其它防攻击检查。透明模式的防火墙支持 ACL 规则检查、ASPF 状态过滤、防攻击检查、流量监控等功能。

工作在透明模式下的防火墙在数据链路层连接局域网（LAN），网络终端用户无需为连接网络而对设备进行特别配置，就像使用以太网交换机一样进行网络连接。

7.1.1 获取地址表过程

采用透明模式，防火墙依据 MAC 地址表进行转发，地址表由 MAC 地址和接口两部分组成，透明模式防火墙必须获取 MAC 地址和接口的对应关系。

1. 广播消息包

透明模式防火墙与物理网段相连时，会监测该物理网段上的所有以太网帧，一旦监测到某个接口上节点发来的以太网帧，就提取出该帧的源 MAC 地址，并将该 MAC 地址与接收该帧的接口之间的对应关系加入到 MAC 地址表中，如下图所示：

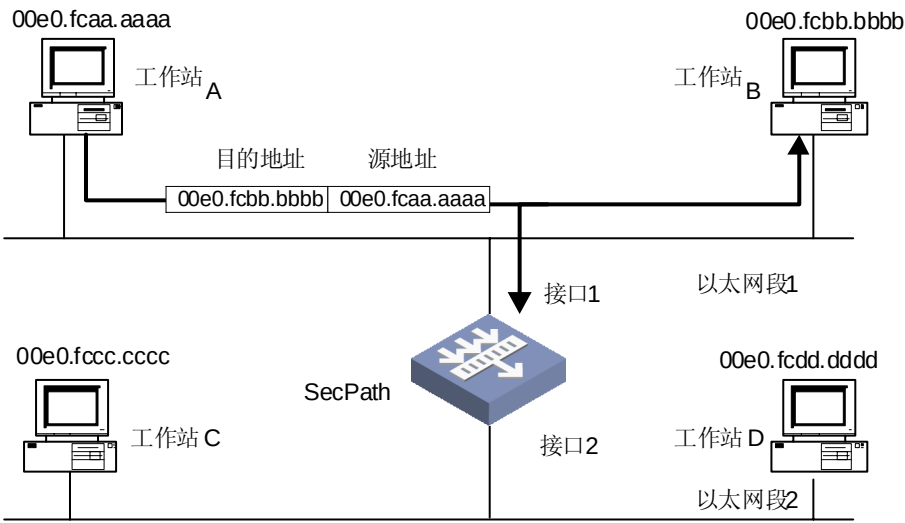


图7-1 广播消息包

A、B、C 和 D 四个工作站分布在两个局域网中，以太网段 1 与透明模式防火墙接口 1 相连，以太网段 2 与接口 2 相连。某一时刻，当工作站 A 向工作站 B 发送以太网帧时，透明模式防火墙和工作站 B 都将收到这个帧。

2. 反向学习工作站 A 的 MAC 地址和接口对应关系

透明模式防火墙收到这个以太网帧后，就知道工作站 A 与透明模式防火墙接口 1 相连（因为从接口 1 收到了该帧），于是工作站 A 的 MAC 地址与透明模式防火墙接口 1 之间的对应关系就被加入到 MAC 地址表中。如下图所示：

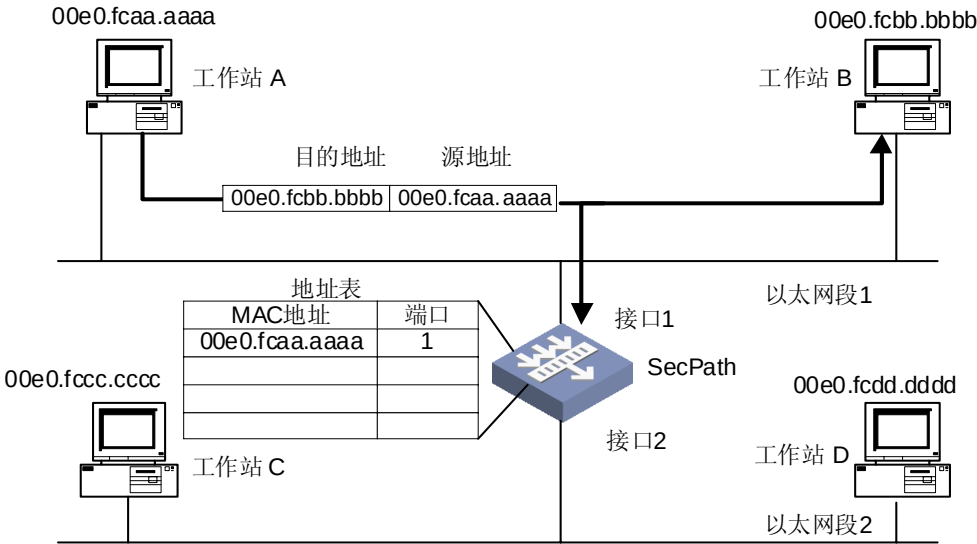


图7-2 反向学习工作站 A 的 MAC 地址和接口对应关系

3. 反向学习工作站 B 的 MAC 地址和接口对应关系

当工作站 B 对工作站 A 的以太网帧作出响应后，透明模式防火墙也能监测到工作站 B 回应的以太网帧，并知道工作站 B 也是与透明模式防火墙接口 1 相连的（因为从接口 1 收到了该帧），于是工作站 B 的 MAC 地址与透明模式防火墙接口 1 之间的对应关系也被加入到 MAC 地址表中。如下图所示：

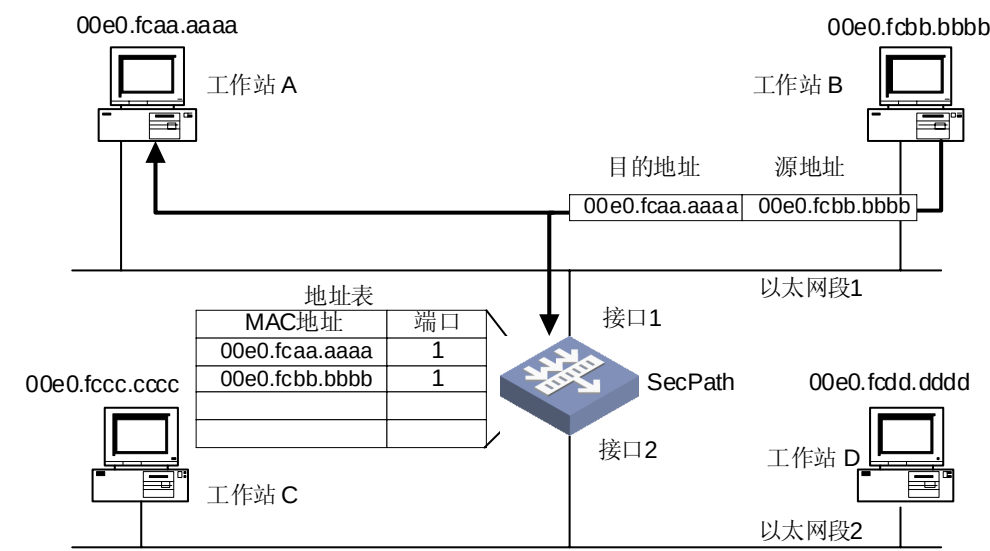


图7-3 反向学习工作站 B 的 MAC 地址和接口对应关系

反向学习过程一直进行，直到所有 MAC 地址与接口的对应关系（本例中为工作站 A、B、C 和 D）都被透明模式防火墙获取为止（假设所有的工作站都在使用中）。

7.1.2 转发和过滤

在链路层，透明模式防火墙根据下列三种情况对数据帧作出转发或不转发（即过滤）处理：

1. 查找地址表成功后的转发处理

若工作站 A 向工作站 C 发送以太网帧，透明模式防火墙通过查找地址表知道工作站 C 与接口 2 对应，则将该帧从接口 2 转发。如下图所示：

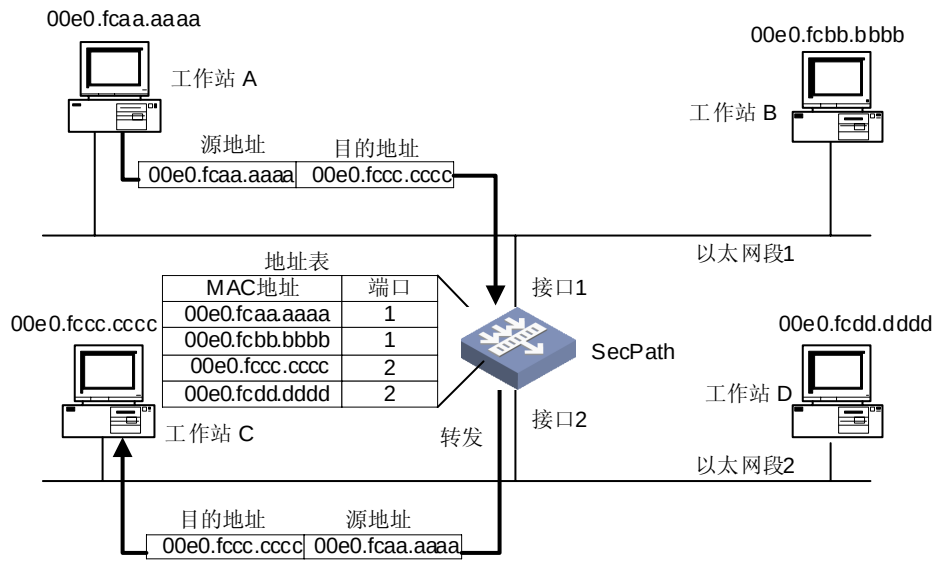


图7-4 查找地址表成功后的转发处理

需要注意的是：当透明模式防火墙在某接口接收到广播帧或多播帧时，将向其它接口进行转发或者将其丢弃。

2. 查找地址表成功后的不转发（过滤）处理

若工作站 A 向工作站 B 发送以太网帧，因工作站 B 与工作站 A 在同一个物理网段上，透明模式防火墙对此帧进行过滤，不转发该帧。

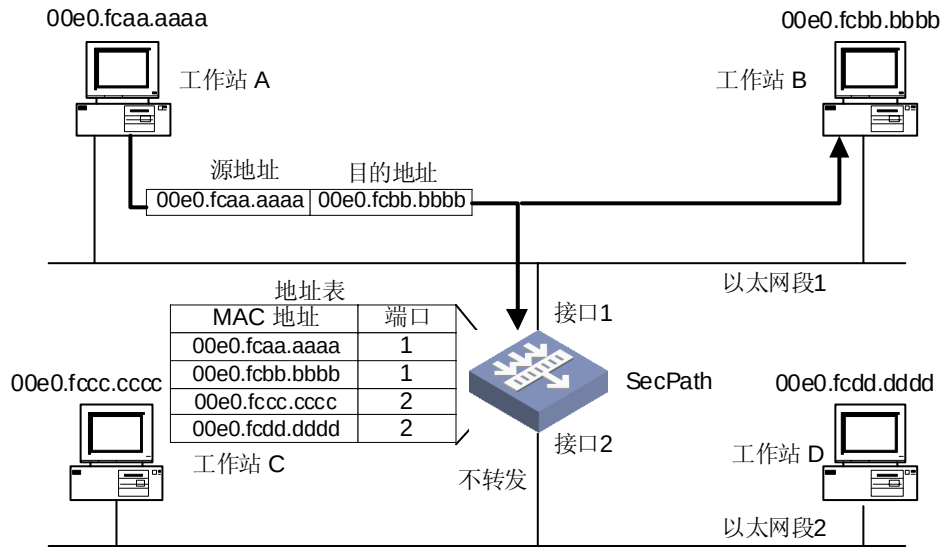


图7-5 查找地址表成功后的不转发（过滤）处理

3. 查找地址表失败后的转发处理

若工作站 A 向工作站 C 发送以太网帧，而在地址表中未找到关于工作站 C 的 MAC 地址与接口的对应关系，透明模式防火墙会如何处理呢？透明模式防火墙会把这个

发往未知目的 MAC 地址的帧向除发送该帧的源接口外的其它所有接口进行转发。在这种情况下，透明模式防火墙充当的实际上是集线器的角色，确保没有使信息停止传送。如下图所示：

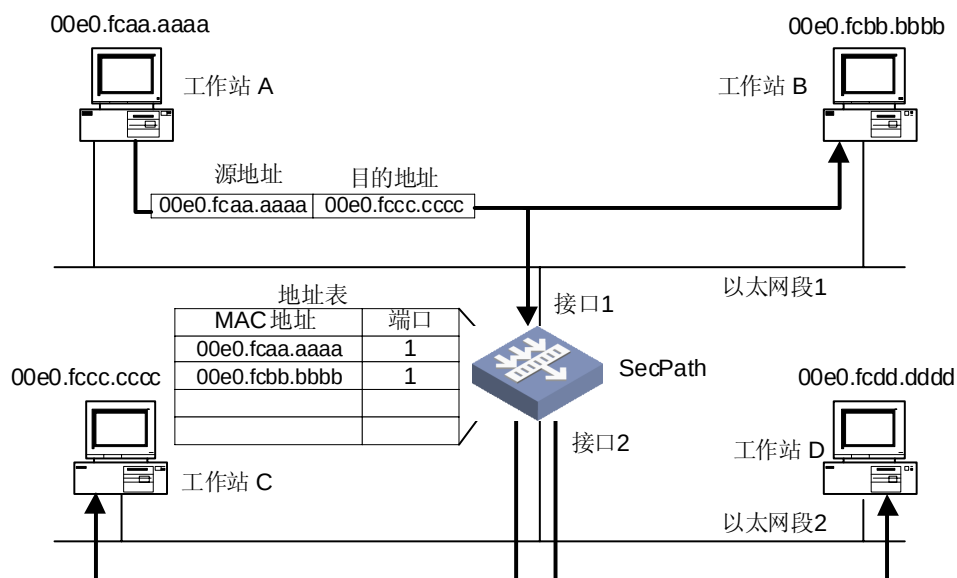


图7-6 查找地址表失败后的转发处理

7.2 防火墙透明模式配置

防火墙透明模式的配置包括：

- 配置防火墙的工作模式
- 配置防火墙的系统 IP 地址
- 启动/禁止 ARP 学习功能
- 配置对未知目的 MAC 地址的 IP 报文的处理方式
- 配置基于 MAC 地址的访问控制列表
- 配置在接口上应用访问控制列表
- 配置 MAC 地址转发表的老化时间
- 配置允许通过的报文类型
- 配置 VLAN ID 透传

7.2.1 配置防火墙的工作模式

请在系统视图下进行下列配置。

表7-1 配置防火墙的工作模式

操作	命令
配置防火墙工作在透明模式	firewall mode transparent
配置防火墙工作在路由模式	firewall mode route
恢复防火墙的工作模式为缺省模式	undo firewall mode

缺省情况下，防火墙工作在路由模式（**route**）下。

 说明：

- 当防火墙工作在透明模式时，系统自动启动桥接功能。仅 SecPath F 系列防火墙支持防火墙工作模式的配置。
- 当防火墙工作在透明模式时，部分攻击防范特性和命令将不可用。

7.2.2 配置防火墙系统 IP 地址

当防火墙工作在路由模式下时，其所有接口都工作在第三层，即可以为接口配置 IP 地址等第三层属性；当防火墙工作在透明模式下时，其所有接口都将工作在第二层，即转换为交换端口，且不能为接口配置 IP 地址等第三层属性。此时若要对防火墙进行管理或使其提供网络服务（例如 Telnet 或 SNMP），防火墙必须拥有 IP 地址，可以为防火墙配置系统 IP 地址用于代替接口 IP 地址以解决此问题。

请在系统视图下进行下列配置。

表7-2 配置防火墙系统 IP 地址

操作	命令
配置防火墙系统 IP 地址	firewall system-ip system-ip-address [address-mask]
恢复防火墙的缺省系统 IP 地址	undo firewall system-ip

当防火墙被配置为工作在透明模式下时，若此时系统中不存在 Loopback0 接口，则系统会为防火墙创建一个地址为 169.0.0.1/8 的 Loopback0 接口，此地址将为缺省的系统 IP 地址；若系统中已存在 Loopback0 接口，Loopback0 接口的地址将被设为系统 IP 地址。当修改 Loopback0 接口的地址或删除 Loopback0 接口时，系统 IP 地址也会被修改或删除。可以使用 **firewall system-ip** 命令修改系统 IP 地址。当防火墙工作在路由模式下时，不能配置系统 IP 地址。

7.2.3 启动/禁止 ARP 学习功能

当防火墙工作在透明模式时，内部和外部网络之间跨越防火墙进行通讯，某设备对自身进行访问或发起某对外连接，这都需要产生 ARP 请求和 ARP 响应，防火墙会自动学习 ARP 表项以备将来的地址解析需求。

由于系统维护的 ARP 表项总数目是有限的，当防火墙遭受 ARP Flood 攻击时，可能会因为过多的无用 ARP 表项而影响防火墙正常 ARP 解析功能。为了防止这种情况的发生，建议先禁止防火墙 ARP 表项学习功能，并通过命令人工添加实际使用的静态 ARP 表项。

请在系统视图下进行下列配置。

表7-3 启动/禁止 ARP 学习功能

操作	命令
启动 ARP 表项自动学习功能	firewall arp-learning enable
禁止 ARP 表项自动学习功能	undo firewall arp-learning enable

缺省情况下，当防火墙工作在透明模式下时，防火墙启动 ARP 表项自动学习功能。

7.2.4 配置对未知目的 MAC 地址的 IP 报文的处理方式

当工作在透明模式下的防火墙接收到未知目的 MAC 地址的 IP 报文时，即不能根据目的 MAC 地址找到出接口，则防火墙根据配置情况可以用三种方式进行处理：

- 直接丢弃该未知目的 MAC 地址的 IP 报文。
- 向除接收到该报文的接口外的其它所有接口（接口必须属于某一安全区域）广播 ARP 请求报文，并且丢弃原来的未知 MAC 地址的 IP 报文。收到 ARP 响应报文后，保存 MAC 地址和接口的对应关系。
- 将此未知目的 MAC 地址的 IP 报文从除接收接口外的其它所有接口（接口必须属于某一安全区域）发送出去，待收到响应报文后，将建立 MAC 地址与接口之间的对应关系。

请在系统视图下进行下列配置。

表7-4 配置对未知目的 MAC 地址报文的处理方式

操作	命令
配置对未知目的 MAC 地址的单播 IP 报文、组播报文和广播报文的处理方式	firewall unknown-mac { drop flood }
配置对未知目的 MAC 地址的单播 IP 报文的处理方式	firewall unknown-mac unicast { drop arp flood }
配置对组播和广播 IP 报文的处理方式	firewall unknown-mac { broadcast multicast } { drop flood }

操作	命令
恢复对未知目的 MAC 地址的 IP 报文的处理方式缺省值	undo firewall unknown-mac [unicast broadcast multicast]

缺省情况下，防火墙对未知目的 MAC 地址的单播、组播和广播报文的处理方式 **flood**。

7.2.5 配置基于 MAC 地址的访问控制列表

创建基于 MAC 地址的访问控制列表，ACL 的序号为 4000～4999。

请在系统视图下配置 **acl** 命令，在 ACL 视图下配置 **rule** 命令。

表7-5 配置基于 MAC 地址的访问控制列表

操作	命令
创建访问控制列表并进入 ACL 视图	acl number <i>acl-number</i>
删除访问控制列表	undo acl { number <i>acl-number</i> all }
创建基于 MAC 地址的访问控制规则	rule [<i>rule-id</i>] { permit deny } [type <i>type-code</i> <i>type-wildcard</i> isap <i>isap-code</i> <i>isap-wildcard</i>] [source-mac <i>sour-addr</i> <i>source-wildcard</i>] [dest-mac <i>dest-addr</i> <i>dest-wildcard</i>] [time-range <i>time-name</i>] [logging]
删除基于以太网 MAC 地址的访问控制规则	undo rule <i>rule-id</i> [time-range] [logging]

缺省情况下，未创建任何基于 MAC 地址的访问控制列表。

7.2.6 配置在接口上应用访问控制列表

请在接口视图下进行下列配置。

表7-6 配置在接口上应用访问控制列表

操作	命令
配置入/出接口方向上应用访问控制列表	firewall ethernet-frame-filter <i>acl-number</i> { inbound outbound }
删除入/出接口方向上的访问控制列表	undo firewall ethernet-frame-filter { inbound outbound }

缺省情况下，未在入/出接口方向上应用访问控制列表。

 说明：

- 要将基于 MAC 地址的访问控制列表应用到接口上，防火墙必须工作在透明模式下，否则系统会提示错误信息。
- 当防火墙工作在透明模式下时，对于报文进行二层的过滤之后还要进行三层的过滤。

7.2.7 配置 MAC 地址转发表的老化时间

MAC 地址转发表的老化时间是指在该表项在地址表中的生存时间，老化时间由老化定时器控制，若该定时器超时，就将该表项从地址表中删除。

请在系统视图下进行下列配置。

表7-7 配置 MAC 地址转发表的老化时间

操作	命令
配置 MAC 地址转发表的老化时间	firewall transparent-mode aging-time <i>seconds</i>
恢复 MAC 地址转发表的老化时间为缺省值	undo firewall transparent-mode aging-time

缺省情况下，MAC 地址转发表的老化时间为 300 秒。

7.2.8 配置允许通过的报文类型

可以配置透明防火墙是否允许 BPDU(Bridge Protocol Data Unit, 桥协议数据单元)、DLSw(Data Link Switching, 数据链路交换)和 IPX(Internetwork Packet Exchange, 网际报文交换)报文通过。

请在系统视图下进行下列配置。

表7-8 配置允许通过的报文类型

操作	命令
配置允许通过的报文类型	firewall transparent-mode transmit { bpdu dlsw ipx }
配置拒绝通过的报文类型	undo firewall transparent-mode transmit { bpdu dlsw ipx }

缺省情况下，防火墙不允许这些类型的报文通过。

7.2.9 配置 VLAN ID 透传

VLAN ID 透传是指接口直接转发报文，不对该报文中的 VLAN ID 做任何处理。即使出接口上有 VLAN ID 的情况下，也不会改变报文原有的 VLAN ID。

请在接口视图下进行下列配置。

表7-9 配置 VLAN ID 透传

操作	命令
使能接口的 VLAN ID 透传功能	bridge vlanid-transparent-transmit enable
禁止接口的 VLAN ID 透传功能	undo bridge vlanid-transparent-transmit enable

缺省情况下，禁止接口的 VLAN ID 透传功能。

当以太网子接口配置 VLAN ID 后，该子接口只会接收这个 VLAN 的数据，这就决定了该桥组负责传输哪些 VLAN 的数据。

在使能 VLAN ID 透传功能以后，系统不对报文的 VLAN ID 做任何处理，两端相连的交换机可以看成是直接相连的。为了正常通信，用户需要给两端交换机的 trunk 口配置相同的 VLAN ID。



注意：

如果某个接口启用 VLAN 透传，那么这个接口对应的物理接口和相应的子接口必须配置基于接口的访问控制列表以过滤从本接口收到的报文，防止报文又被转发回去。

7.3 透明防火墙的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示透明防火墙配置后的运行情况，通过查看显示信息验证配置的效果。在用户视图下，执行 **reset** 命令可以清除相关信息。在用户视图下，执行 **debugging** 命令可以对透明防火墙进行调试。

表7-10 透明防火墙的显示和调试

操作	命令
显示当前防火墙的工作模式	display firewall mode
显示以太帧过滤的统计信息	display firewall ethernet-frame-filter { all interface <i>interface-type</i> <i>interface-number</i> }
显示透明防火墙的配置信息	display firewall transparent-mode config
显示透明防火墙的 MAC 地址表信息	display firewall transparent-mode address-table [interface <i>interface-type</i> <i>interface-number</i> mac <i>mac-address</i>]
显示透明防火墙的流量信息	display firewall transparent-mode traffic [interface <i>interface-type</i> <i>interface-number</i>]
打开以太帧过滤的调试开关	debugging firewall eff [interface <i>interface-type</i> <i>interface-number</i>]

操作	命令
打开透明防火墙的以太网转发调试开关	debugging firewall transparent-mode eth-forwarding [interface <i>interface-type</i> <i>interface-number</i>]
打开透明防火墙的 IP 报文转发调试开关	debugging firewall transparent-mode ip-forwarding
清除以太帧的过滤信息	reset firewall ethernet-frame-filter { all interface <i>interface-type</i> <i>interface-number</i> }
清除 MAC 地址表中的信息	reset firewall transparent-mode address-table [interface <i>interface-type</i> <i>interface-number</i>]
清除透明防火墙的流量统计信息	reset firewall transparent-mode traffic [interface <i>interface-type</i> <i>interface-number</i>]

7.4 典型配置举例

7.4.1 VLAN ID 透传配置举例

1. 组网需求

PC1 和 PC2 分别连到交换机 SW1 和 SW2 上，然后通过防火墙进行桥接。在 PC1 上进行 ping PC2 的操作，如果两台防火墙的以太网子接口和 E0/1 接口都使能了 VLAN ID 透传功能，PC2 能成功地收到 PC1 的 ping 报文，且 PC1 能收到 PC2 的响应报文。

2. 组网图

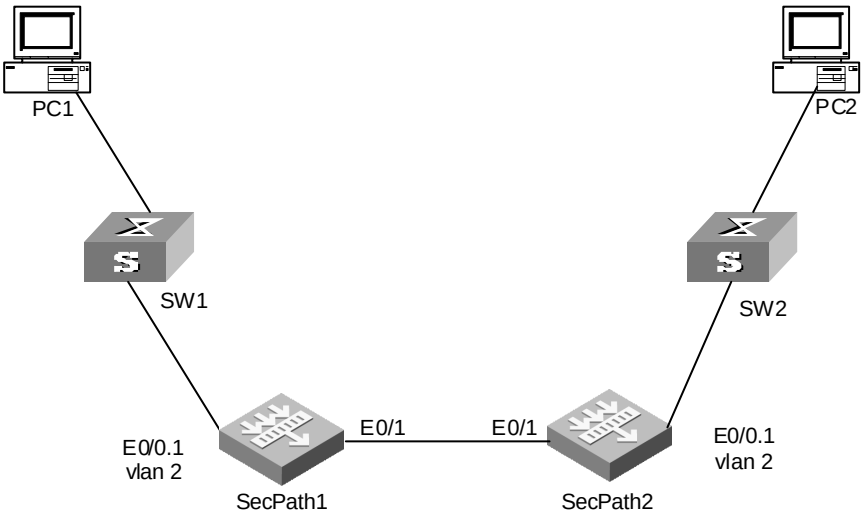


图7-7 以太网接口上实现 VLAN ID 透传组网图

3. 配置步骤

(1) 配置 SecPath1

在 SecPath1 上使能透明防火墙。

```
<H3C> system-view
```

```
[H3C] firewall mode transparent
```

使能 VLAN ID 透传功能。

```
[H3C] interface Ethernet 0/0.1
```

```
[H3C-Ethernet0/0.1] vlan-type dot1q vid 2
```

```
[H3C-Ethernet0/0.1] bridge vlanid-transparent-transmit enable
```

```
[H3C-Ethernet0/0.1] quit
```

```
[H3C] interface Ethernet 0/1
```

```
[H3C-Ethernet0/1] bridge vlanid-transparent-transmit enable
```

在 Ethernet0/0 接口配置访问控制列表以过滤从 Ethernet0/0.1 接口收到的报文，防止报文又被转发回去。

```
[H3C] acl number 1000
```

```
[H3C-acl-if-1000] rule deny interface Ethernet0/0.1
```

```
[H3C-acl-if-1000] rule permit interface any
```

```
[H3C-acl-if-1000] quit
```

```
[H3C] interface Ethernet 0/0
```

```
[H3C-Ethernet0/0] firewall packet-filter 1000 outbound
```

(2) 配置 SecPath2

在 SecPath2 上使能透明防火墙。

```
<H3C> system-view
```

```
[H3C] firewall mode transparent
```

使能 VLAN ID 透传功能。

```
[H3C] interface Ethernet 0/0.1
```

```
[H3C-Ethernet0/0.1] vlan-type dot1q vid 2
```

```
[H3C-Ethernet0/0.1] bridge vlanid-transparent-transmit enable
```

```
[H3C-Ethernet0/0.1] quit
```

```
[H3C] interface Ethernet 0/1
```

```
[H3C-Ethernet0/1] bridge vlanid-transparent-transmit enable
```

在 Ethernet0/0 接口配置访问控制列表以过滤从 Ethernet0/0.1 接口收到的报文，防止报文又被转发回去。

```
[H3C] acl number 1000
```

```
[H3C-acl-if-1000] rule deny interface Ethernet0/0.1
```

```
[H3C-acl-if-1000] rule permit interface any
```

```
[H3C-acl-if-1000] quit
```

```
[H3C] interface Ethernet 0/0
```

```
[H3C-Ethernet0/0] firewall packet-filter 1000 outbound
```


第8章 混合模式配置

说明：

仅 SecPath F1000-A 防火墙、SecPath F1000-S 防火墙、SecPath F1000-C 防火墙、SecPath F100-A 防火墙、SecPath F100-A-SI 防火墙、SecPath F100-M 防火墙和 SecPath F100-E 防火墙、SecPath F100-C-EI 防火墙、SecPath F100-C II 防火墙即新一代 F100-C 支持混合模式。

8.1 网桥简介

缺省情况下，防火墙工作在路由模式下。当防火墙工作在网桥模式（也称为桥接模式）下时，加入到桥组中的接口不能配置 IP 地址，接口所在的安全区域是二层区域，和二层区域相关接口连接的外部用户同属一个子网。

当报文在二层区域的接口间进行转发时，需要根据报文的 MAC 地址来寻找出接口，此时防火墙表现为一个透明网桥。但是，防火墙与网桥不同，防火墙接收到的 IP 报文还需要送到上层进行相关过滤等处理，通过检查会话表或 ACL 规则以确定是否允许该报文通过。此外，防火墙还要完成其它防攻击检查。网桥模式的防火墙支持 ACL 规则检查、ASPF 状态过滤、防攻击检查和流量监控等功能。

工作在网桥模式下的防火墙在数据链路层连接局域网（LAN），网络终端用户无需为连接网络而对设备进行特别配置，就像使用以太网交换机一样进行网络连接。

8.1.1 获取地址表过程

采用网桥模式，防火墙依据 MAC 地址表进行转发。地址表由 MAC 地址和接口两部分组成，网桥模式防火墙必须获取 MAC 地址和接口的对应关系。

1. 广播消息包

网桥模式防火墙与物理网段相连时，会监测该物理网段上的所有以太网帧，一旦监测到某个接口上节点发来的以太网帧，就提取出该帧的源MAC地址，并将该MAC地址与接收该帧的接口之间的对应关系加入到MAC地址表中，如图 8-1所示。

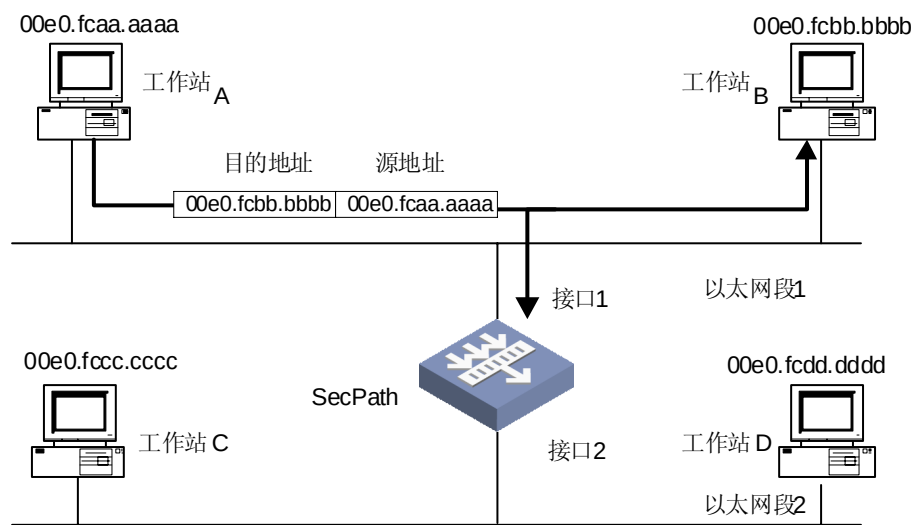


图8-1 广播消息包

A、B、C 和 D 四个工作站分布在两个局域网中，以太网段 1 与网桥模式防火墙接口 1 相连，以太网段 2 与接口 2 相连。某一时刻，当工作站 A 向工作站 B 发送以太网帧时，网桥模式防火墙和工作站 B 都将收到这个帧。

2. 反向学习工作站 A 的 MAC 地址和接口对应关系

网桥模式防火墙收到这个以太网帧后，就知道工作站A与网桥模式防火墙接口 1 相连（因为从接口 1 收到了该帧），于是工作站A的MAC地址与网桥模式防火墙接口 1 之间的对应关系就被加入到MAC地址表中，如 图 8-2所示。

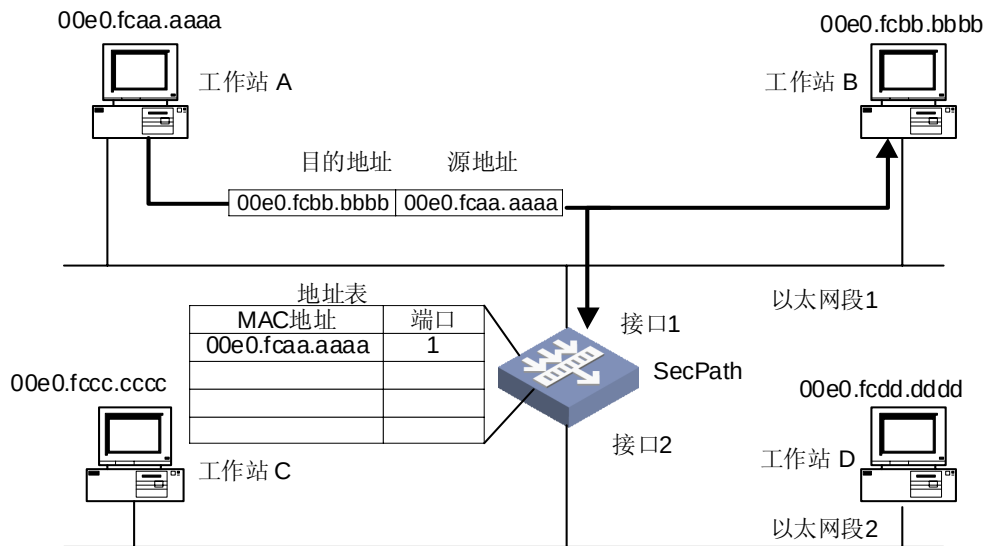


图8-2 反向学习工作站 A 的 MAC 地址和接口对应关系

3. 反向学习工作站 B 的 MAC 地址和接口对应关系

当工作站B对工作站A的以太网帧做出响应后，网桥模式防火墙也能监测到工作站B回应的以太网帧，并知道工作站B也是与网桥模式防火墙接口 1 相连的（因为从接口 1 收到了该帧），于是工作站B的MAC地址与网桥模式防火墙接口 1 之间的对应关系也被加入到MAC地址表中，如图 8-3所示。

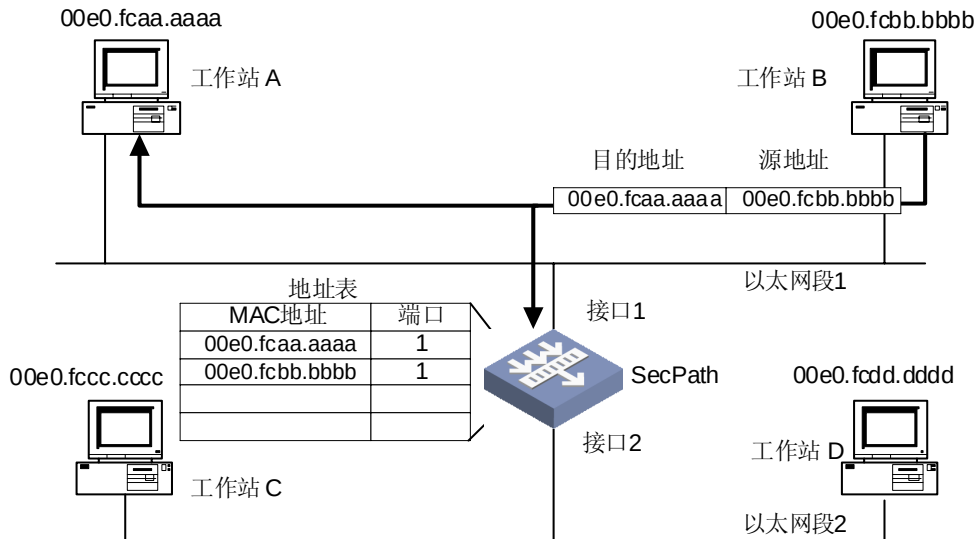


图8-3 反向学习工作站 B 的 MAC 地址和接口对应关系

反向学习过程一直进行，直到所有 MAC 地址与接口的对应关系（本例中为工作站 A、B、C 和 D）都被网桥模式防火墙获取为止（假设所有的工作站都在使用中）。

8.1.2 转发和过滤

在链路层，网桥模式防火墙根据下列三种情况对数据帧作出转发或不转发（即过滤）处理。

1. 查找地址表成功后的转发处理

若工作站A向工作站C发送以太网帧，网桥模式防火墙通过查找地址表知道工作站C与接口 2 对应，则将该帧从接口 2 转发，如图 8-4所示。

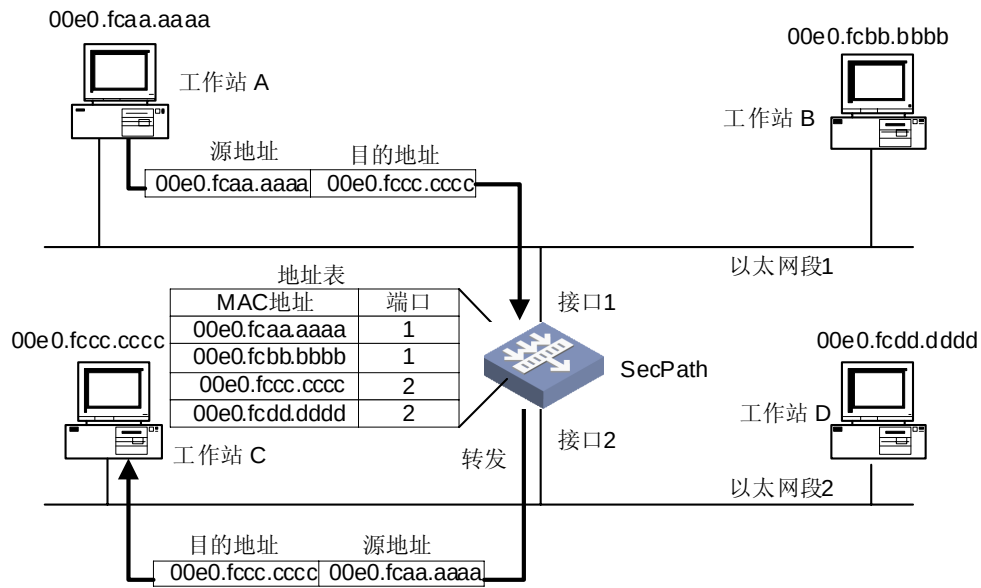


图8-4 查找地址表成功后的转发处理

需要注意的是：当网桥模式防火墙在某接口接收到广播帧或多播帧时，将向其它接口进行转发或者将其丢弃。

2. 查找地址表成功后的不转发（过滤）处理

若工作站A向工作站B发送以太网帧，因工作站B与工作站A在同一个物理网段上，网桥模式防火墙对此帧进行过滤，不转发该帧，如图 8-5所示。

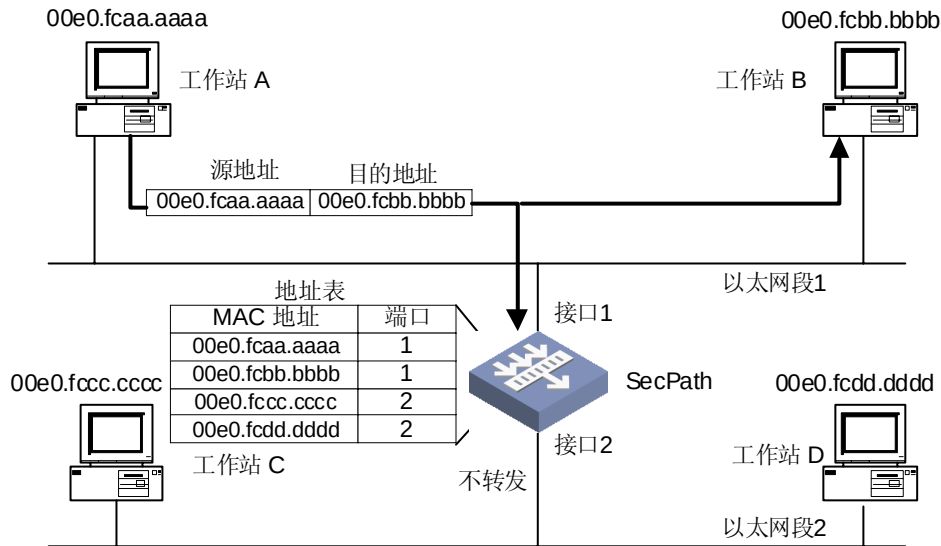


图8-5 查找地址表成功后的不转发（过滤）处理

3. 查找地址表失败后的转发处理

若工作站A向工作站C发送以太网帧，而在地址表中未找到关于工作站C的MAC地址与接口的对应关系，防火墙会把这个发往未知目的MAC地址的帧向除发送该帧的源接口外的其它所有接口进行转发。在这种情况下，网桥模式防火墙实际上充当的是集线器的角色，确保信息不停止传送，如图 8-6所示。

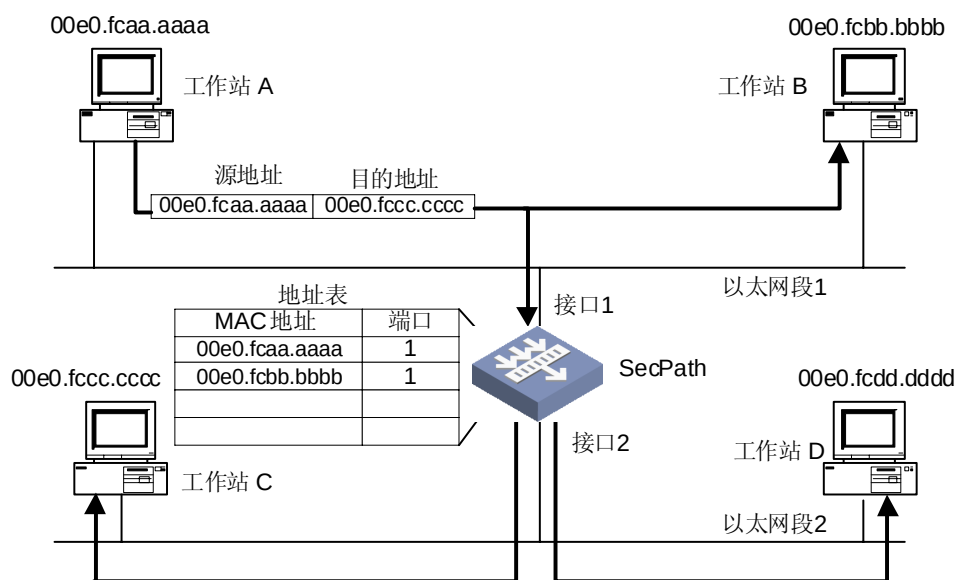


图8-6 查找地址表失败后的转发处理

8.2 网桥配置

网桥配置包括：

- (1) 网桥基本配置
 - 使能/禁用网桥功能
 - 使能/禁止桥组功能
 - 配置将接口加入到网桥组中
- (2) 配置网桥地址表
 - 配置静态地址表项
 - 允许/禁止动态学习地址
 - 配置动态地址表的老化时间
- (3) 配置以太网帧过滤
 - 配置基于 MAC 地址的访问控制列表
 - 在接口上应用访问控制列表
- (4) 配置网桥路由功能

- 配置 bridge-template 接口
 - 手工配置 bridge-template 接口的 MAC 地址
- (5) 配置网桥组对网络层协议的桥接功能
- (6) 配置网桥允许通过的报文类型
- (7) 配置对未知目的 MAC 地址的 IP 报文的处理方式
- (8) 配置 VLAN ID 透传

8.2.1 网桥基本配置

1. 使能/禁用网桥功能

请在系统视图下进行下列配置。

表8-1 使能/禁用网桥功能

操作	命令
使能网桥功能	bridge enable
禁用网桥功能	undo bridge enable

缺省情况下，禁用网桥功能。

2. 使能/禁止桥组

每一个桥组都是独立的，报文不能在分属不同桥组的端口之间传输。换句话说，从一个桥组端口接收到的报文，只能从相同桥组的其他端口发送出去。防火墙上有一个接口不能同时加入两个或两个以上的桥组。

请在系统视图下进行下列配置。

表8-2 使能/禁止桥组

操作	命令
使能网桥组	bridge bridge-set enable
删除网桥组	undo bridge bridge-set enable

缺省情况下，桥组未使能。

3. 配置将接口加入到网桥组中

可以将以太网接口、以太网子接口和 Tunnel 接口加入到网桥组中，但一个接口不能同时加入到两个或两个以上的桥组中。

请在接口视图下进行下列配置。

表8-3 配置将接口加入到网桥组中

操作	命令
将接口加入到网桥组中	bridge-set <i>bridge-set</i>
将接口从网桥组中删除	undo bridge-set <i>bridge-set</i>

缺省情况下，接口未加入到任何网桥组中。

接口加入桥组后，在接口上配置的三层属性将不生效。

 说明：

- 同一桥组中的接口若要互相通信，需将接口加入到安全区域中。
- 不同桥组中的接口若要互相通信，只需将 **bridge-template** 接口加入到安全区域中。

8.2.2 配置网桥地址表

网桥地址表记录了目的 MAC 地址和接口之间的对应关系，这是网桥转发的依据。

1. 配置静态地址表项

一般情况下，网桥地址表是根据该网桥获取的 MAC 地址和接口的对应关系动态生成的，但网桥地址表中也存在一些静态地址表项，它是由管理员手工配置和维护的，并且永远不会老化。

请在系统视图下进行下列配置。

表8-4 配置静态地址表项

操作	命令
配置静态地址表项	bridge bridge-set mac-address <i>mac-address</i> { permit interface <i>interface-type interface-number</i> deny }
删除静态地址表项	undo bridge bridge-set mac-address <i>mac-address</i> [interface <i>interface-type interface-number</i>]

缺省情况下，采用动态地址表进行转发帧。

2. 允许/禁止动态学习地址

请在系统视图下进行下列配置。

表8-5 允许/禁止动态学习地址

操作	命令
允许动态学习地址	bridge bridge-set learning
禁止动态学习地址	undo bridge bridge-set learning

缺省情况下，允许动态学习地址。

3. 配置动态地址表的老化时间

动态地址表的老化时间是由老化定时器控制的，若该定时器超时，就将该表项从网桥地址表中删除。

请在系统视图下进行下列配置。

表8-6 配置动态地址表的老化时间

操作	命令
配置动态地址表的老化时间	bridge aging-time seconds
恢复动态地址表老化时间的缺省值	undo bridge aging-time

缺省情况下，动态地址表的老化时间为 300 秒，取值范围为 10~1000000 秒。

说明：

当桥组学习到一个 MAC 地址时，如果 MAC 地址在地址表中不存在，则会创建一个新的地址表项，并初始老化定时器：

- 若在老化定时器超时前未收到来自此 MAC 地址的报文，等到老化定时器超时，将删除此地址表项。
- 若在老化定时器超时前收到了来自此 MAC 地址的报文，等到老化定时器超时，系统将重新初始老化定时器。

8.2.3 配置以太网过滤

1. 配置基于 MAC 地址的访问控制列表

创建基于 MAC 地址的访问控制列表，ACL 的序号为 4000~4999。

请在系统视图下配置 **acl** 命令，在 ACL 视图下配置 **rule** 命令。

表8-7 配置基于 MAC 地址的访问控制列表

操作	命令
创建访问控制列表并进入 ACL 视图	acl number acl-number
删除访问控制列表	undo acl { number acl-number all }

操作	命令
创建基于 MAC 地址的访问控制规则	rule [<i>rule-id</i>] { permit deny } [type <i>type-code</i> <i>type-wildcard</i> lsap <i>lsap-code</i> <i>lsap-wildcard</i>] [source-mac <i>sour-addr</i> <i>source-wildcard</i>] [dest-mac <i>dest-addr</i> <i>dest-wildcard</i>] [time-range <i>time-name</i>] [logging]
删除基于以太网 MAC 地址的访问控制规则	undo rule <i>rule-id</i> [time-range] [logging]

缺省情况下，未创建任何基于 MAC 地址的访问控制列表。

2. 在接口上应用访问控制列表

请在接口视图下进行下列配置。

表8-8 在接口上应用访问控制列表

操作	命令
在入/出接口方向上应用访问控制列表	firewall ethernet-frame-filter <i>acl-number</i> { inbound outbound }
删除入/出接口方向上的访问控制列表	undo firewall ethernet-frame-filter { inbound outbound }

缺省情况下，未在入/出接口方向上应用访问控制列表。

说明：

- 要将基于 MAC 地址的访问控制列表应用到接口上，接口必须被加入到桥组中，否则系统会提示错误信息。
- 对于桥组中的接口，报文进行二层的过滤之后还要进行三层的过滤。

8.2.4 配置网桥路由功能

网桥路由功能提供了一种结合路由和桥接的转发方法。对于指定的协议数据，如果是在网桥端口之间进行通讯，则进行桥接转发；如果是需要与非网桥组内的网络进行通讯，则可以进行网络协议的路由转发。

1. 配置 bridge-template 接口

bridge-template 接口存在于防火墙中，它不支持网桥，但是它在防火墙内代表整个和选路接口相对应的网桥组。**bridge-template** 接口的编号是它所代表的网桥组的编号。**bridge-template** 接口是一个虚拟的选路接口，在此接口上可以配置各种网络层的属性。对于每个网桥组来说，只能有一个 **bridge-template** 接口。

请在系统视图下进行下列配置。

表8-9 配置 bridge-template 接口

操作	命令
创建 bridge-template 接口，并将指定的网桥组连接到路由的网络中	interface bridge-template bridge-set
删除 bridge-template 接口	undo interface bridge-template bridge-set

2. 手工配置 bridge-template 接口的 MAC 地址

当链路两端的设备都为 SecPath 系列防火墙时，可能会因为系统在两端的 bridge-template 接口自动生成的 MAC 地址相同而产生冲突，所以建议手工指定 bridge-template 接口的 MAC 地址。

请在 bridge-template 视图下进行下列配置。

表8-10 手工配置 bridge-template 接口的 MAC 地址

操作	命令
配置 bridge-template 接口的 MAC 地址	mac-address H-H-H
删除手工配置的 MAC 地址	undo mac-address

缺省情况下，bridge-template 接口使用系统自动生成的 MAC 地址。

8.2.5 配置网桥组对网络层协议的桥接功能

请在系统视图下进行下列配置。

表8-11 配置网桥组对网络层协议的桥接功能

操作	命令
使能网桥组对网络层协议的桥接功能	bridge bridge-set bridging { ip ipx }
禁止网桥组对网络层协议的桥接功能	undo bridge bridge-set bridging { ip ipx }

缺省情况下，启用桥接功能。

8.2.6 配置网桥允许通过的报文类型

通过如下命令可以配置网桥是否允许 BPDU（Bridge Protocol Data Unit，桥协议数据单元）、DLSw（Data Link Switching，数据链路交换）和 IPX（Internetwork Packet Exchange，网际报文交换）报文通过。

请在系统视图下进行下列配置。

表8-12 配置允许通过的报文类型

操作	命令
配置允许通过的报文类型	bridge permit { bpdu dlsu ipx }
配置拒绝通过的报文类型	undo bridge permit { bpdu dlsu ipx }

缺省情况下，网桥允许 BPDU、DLSu 和 IPX 报文通过。

8.2.7 配置对未知目的 MAC 地址的 IP 报文的处理方式

当同一桥组下的接口接收到未知目的 MAC 地址的 IP 报文时，即不能根据目的 MAC 地址找到出接口，则桥组根据配置情况可以有如下三种处理方式：

- 直接丢弃该未知目的 MAC 地址的 IP 报文。
- 向除接收到该报文的接口外的属于同一桥组的其它所有接口（接口必须属于某一安全区域）广播 ARP 请求报文，并且丢弃原来的未知 MAC 地址的 IP 报文。收到 ARP 响应报文后，保存 MAC 地址和接口的对应关系。
- 将此未知目的 MAC 地址的 IP 报文从除接收接口外的属于同一桥组的其它所有接口（接口必须属于某一安全区域）发送出去，待收到响应报文后，将建立 MAC 地址与接口之间的对应关系。

请在系统视图下进行下列配置。

表8-13 配置对未知目的 MAC 地址的 IP 报文的处理方式

操作	命令
配置对未知目的 MAC 地址的单播 IP 报文、组播 IP 报文和广播 IP 报文的处理方式	bridge bridge-set firewall unknown-mac { drop flood }
配置对未知目的 MAC 地址的单播 IP 报文的处理方式	bridge bridge-set firewall unknown-mac unicast { drop arp flood }
配置对组播 IP 报文和广播 IP 报文的处理方式	bridge bridge-set firewall unknown-mac { broadcast multicast } { drop flood }
恢复对未知目的 MAC 地址的 IP 报文的处理方式为缺省值	undo bridge bridge-set firewall unknown-mac [unicast broadcast multicast]

缺省情况下，桥组对未知目的 MAC 地址的单播、组播和广播报文的处理方式为 **flood**。

8.2.8 配置 VLAN ID 透传

VLAN ID 透传是指通过配置对加入桥组设备的出接口支持 VLAN ID 透传，使接口直接转发报文，不对该报文中的 VLAN ID 做任何处理。

通过 VLAN ID 透传，可以使加入桥组的非以太网接口也能转发带有 VLAN ID 的报文，而不会因此丢失 VLAN ID，并且即使加入桥组设备的出接口上有 VLAN ID 的情况下，也不会改变报文原有的 VLAN ID，从而实现不同 VLAN 的隔离。

请在接口视图下进行下列配置

表8-14 使能 VLAN ID 透传

操作	命令
使能 VLAN ID 透传功能	bridge vlanid-transparent-transmit enable
禁用 VLAN ID 透传功能	undo bridge vlanid-transparent-transmit enable

缺省情况下，禁用 VLAN ID 透传功能。

8.3 网桥的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示网桥配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **debugging** 命令可以对网桥进行调试。

在用户视图下，执行 **reset** 命令可以清除相关信息。

表8-15 网桥显示和调试

操作	命令
打开网桥的以太网转发调试信息开关	debugging bridge eth-forwarding [interface interface-type interface-number]
关闭网桥的以太网转发调试信息开关	undo debugging bridge eth-forwarding [interface interface-type interface-number]
打开网桥的 IP 转发调试开关	debugging bridge ip-forwarding
关闭网桥的 IP 转发调试开关	undo debugging bridge ip-forwarding
显示网桥模块中所有或指定的桥组的信息	display bridge information [bridge-set bridge-set]
显示 MAC 地址转发表的信息	display bridge address-table [bridge-set bridge-set interface interface-type interface-number mac mac-address] [static dynamic]
显示桥组中接口的流量统计数据	display bridge traffic [bridge-set bridge-set interface interface-type interface-number]
显示接口上的以太网过滤统计信息	display firewall ethernet-frame-filter { all interface interface-type interface-number }
清除 MAC 地址转发表	reset bridge address-table [bridge-set bridge-set interface interface-type interface-number]

操作	命令
清除桥组中接口的流量统计数据	reset bridge traffic [bridge-set <i>bridge-set</i> interface <i>interface-type interface-number</i>]
清除 ACL 规则过滤情况的统计信息	reset firewall ethernet-frame-filter { all interface <i>interface-type interface-number</i> }

8.4 网桥典型配置举例

8.4.1 同时支持路由和桥接举例

1. 组网需求

将防火墙的 Ethernet1/0/0 接口和 Ethernet2/0/0 接口加入到桥组中，通过使用 bridge-template 接口，实现报文能够在桥组和 Ethernet0/0/0 接口间路由。

2. 组网图

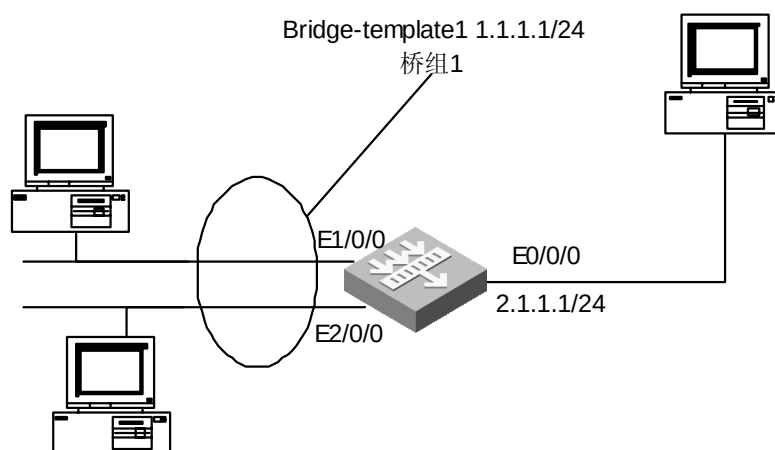


图8-7 同时支持路由和桥接组网图

3. 配置步骤

使能网桥功能。

```
[H3C] bridge enable
```

将接口加入到桥组。

```
[H3C] interface Ethernet1/0/0
```

```
[H3C-Ethernet1/0/0] bridge-set 1
```

```
[H3C-Ethernet1/0/0] quit
```

```
[H3C] interface Ethernet2/0/0
```

```
[H3C-Ethernet2/0/0] bridge-set 1
```

```
[H3C-Ethernet2/0/0] quit
```

创建并配置 bridge-template 接口。

```
[H3C] interface Bridge-template 1
[H3C-Bridge-Template1] ip address 1.1.1.1 255.255.255.0
[H3C-Bridge-Template1] quit
```

配置 Ethernet0/0/0 接口。

```
[H3C] interface Ethernet0/0/0
[H3C-Ethernet0/0/0] ip address 2.1.1.1 255.255.255.0
```

8.4.2 以太网子接口上使用网桥举例

1. 组网需求

SecPathA 与 SecPathB 之间仅存在一条物理链路，但通过在以太网子接口上使用网桥功能，使得 SecPathA 与 SecPathB 上的桥组能够互通。

2. 组网图

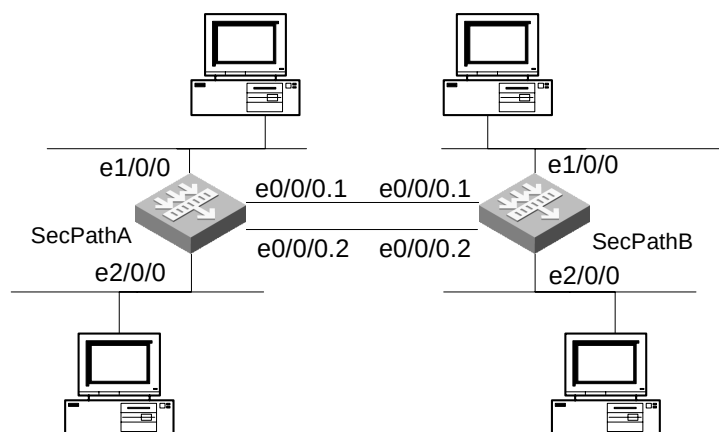


图8-8 以太网子接口上使用网桥网图

3. 配置步骤

(1) 配置 SecPathA

使能防火墙的网桥功能，并使能桥组 1 和桥组 2。

```
[H3C] bridge enable
[H3C] bridge 1 enable
[H3C] bridge 2 enable
```

将以太网接口和以太网子接口加入到相应的桥组。

```
[H3C] interface Ethernet 1/0/0
[H3C-Ethernet1/0/0] bridge-set 1
[H3C-Ethernet1/0/0] quit
[H3C] interface Ethernet 2/0/0
[H3C-Ethernet2/0/0] bridge-set 2
```

```
[H3C-Ethernet2/0/0] quit
[H3C] interface Ethernet 0/0/0.1
[H3C-Ethernet0/0/0.1] vlan-type dot1q vid 1
[H3C-Ethernet0/0/0.1] bridge-set 1
[H3C-Ethernet0/0/0.1] quit
[H3C] interface Ethernet 0/0/0.2
[H3C-Ethernet0/0/0.2] vlan-type dot1q vid 2
[H3C-Ethernet0/0/0.2] bridge-set 2
```

(2) 配置 SecPathB

使能防火墙的网桥功能，并使能桥组 1 和桥组 2。

```
[H3C] bridge enable
[H3C] bridge 1 enable
[H3C] bridge 2 enable
```

将以太网接口和以太网子接口加入到相应的桥组。

```
[H3C] interface Ethernet 1/0/0
[H3C-Ethernet1/0/0] bridge-set 1
[H3C-Ethernet1/0/0] quit
[H3C] interface Ethernet 2/0/0
[H3C-Ethernet2/0/0] bridge-set 2
[H3C-Ethernet2/0/0] quit
[H3C] interface Ethernet 0/0/0.1
[H3C-Ethernet0/0/0.1] vlan-type dot1q vid 1
[H3C-Ethernet0/0/0.1] bridge-set 1
[H3C-Ethernet0/0/0.1] quit
[H3C] interface Ethernet 0/0/0.2
[H3C-Ethernet0/0/0.2] vlan-type dot1q vid 2
[H3C-Ethernet0/0/0.2] bridge-set 2
```

8.4.3 VLAN ID 透传配置举例

1. 组网需求

PC1 和 PC2 分别连到交换机 SW1 和 SW2 上，然后通过防火墙进行桥接。在 PC1 上进行 ping PC2 的操作，如果两台防火墙的以太网子接口和 E0/0/1 接口都使能了 VLAN ID 透传功能，PC2 能成功地收到 PC1 的 ping 报文，且 PC1 能收到 PC2 的响应报文。

2. 组网图

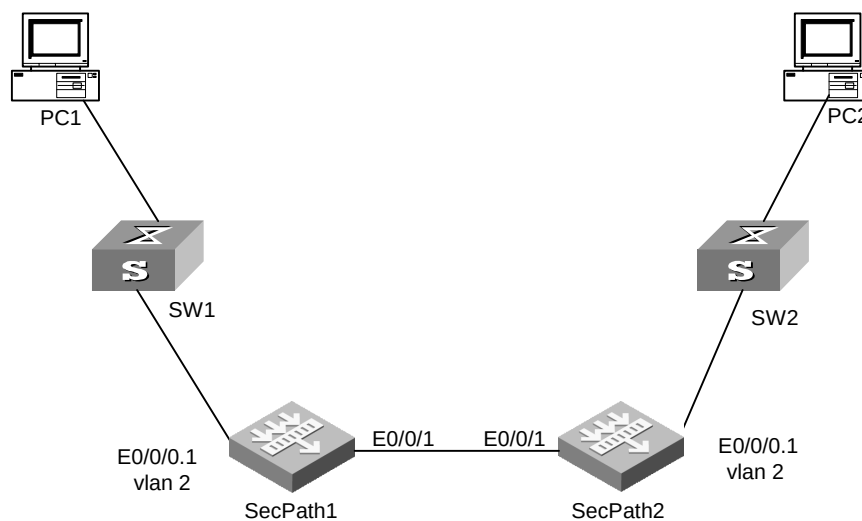


图8-9 以太网接口上实现 VLAN ID 透传组网图

3. 配置步骤

(1) 配置 SecPath1

在 SecPath1 上使能网桥功能，并使能桥组 2。

```
<H3C> system-view
[H3C] bridge enable
[H3C] bridge 2 enable
```

将接口加入到桥组，使能 VLAN ID 透传功能。

```
[H3C] interface Ethernet 0/0/0.1
[H3C-Ethernet0/0/0.1] bridge-set 2
[H3C-Ethernet0/0/0.1] vlan-type dot1q vid 2
[H3C-Ethernet0/0/0.1] bridge vlanid-transparent-transmit enable
[H3C-Ethernet0/0/0.1] quit
[H3C] interface Ethernet 0/0/1
[H3C-Ethernet0/0/1] bridge-set 2
[H3C-Ethernet0/0/1] bridge vlanid-transparent-transmit enable
```

(2) 配置 SecPath2

在 SecPath2 上使能网桥功能，并使能桥组 2。

```
<H3C> system-view
[H3C] bridge enable
[H3C] bridge 2 enable
```

将接口加入到桥组，使能 VLAN ID 透传功能。

```
[H3C] interface Ethernet 0/0/0.1
```



```
[H3C-Ethernet0/0/0.1] bridge-set 2
[H3C-Ethernet0/0/0.1] vlan-type dot1q vid 2
[H3C-Ethernet0/0/0.1] bridge vlanid-transparent-transmit enable
[H3C-Ethernet0/0/0.1] quit
[H3C] interface Ethernet 0/0/1
[H3C-Ethernet0/0/1] bridge-set 2
[H3C-Ethernet0/0/1] bridge vlanid-transparent-transmit enable
```

第9章 PKI 配置

9.1 PKI 简介

9.1.1 概述

PKI（Public Key Infrastructure，公钥基础设施）是通过使用公开密钥技术和数字证书来确保系统信息安全并负责验证数字证书持有者身份的一种体系，它是一套软硬件系统和安全策略的集合，提供了一整套安全机制。PKI 采用证书进行公钥管理，通过第三方的可信任机构，把用户的公钥和其他标识信息捆绑在一起，以在网上验证用户的身份。PKI 为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便的使用加密和数字签名技术，从而保证网上数据的机密性、完整性、有效性。数据的机密性是指数据在传输过程中不能被非授权者偷看；数据的完整性是指数据在传输过程中不能被非法篡改；数据的有效性是指数据不能被否认。

一个PKI系统由公开密钥密码技术、证书认证机构、注册机构、数字证书和相应的PKI存储库共同组成，如图9-1所示。

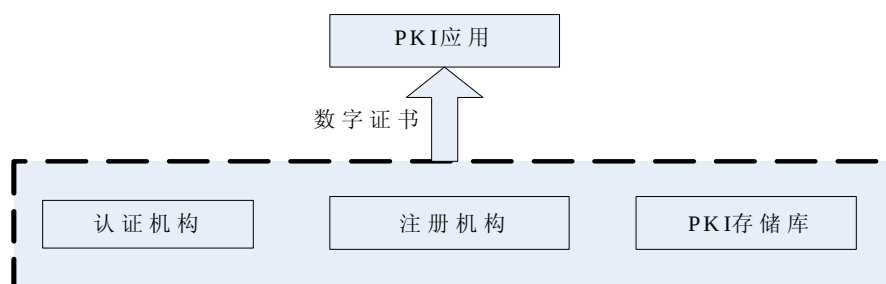


图9-1 PKI 组成框图

认证机构用于签发并管理证书；注册机构用于个人身份审核、证书废除列表管理等；PKI 存储库用于对证书和日志等信息进行存储和管理，并提供一定的查询功能；数字证书是PKI应用信任的基础，是PKI系统的安全凭据。数字证书又称为PKC（Public Key Certificate，公共密钥证书），是基于公共密钥技术发展起来的一种主要用于验证的技术。它是一个经证书认证中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件，可作为各类实体在网上进行信息交流及商务活动的身份证明。证书是有生命期的，在证书生成时指定，认证中心也可以在证书的有效期到来前吊销证书，结束证书的生命期。

9.1.2 相关术语

- **公钥密码算法**：是指加密密钥和解密密钥为两个不同密钥的密码算法，用户生成一对密钥：将其中的一个向外界公开，称为公钥；另一个则自己保留，称为私钥。密钥对中任一密钥加密的信息只能用另一密钥进行解密，因此它们常用于签名和加密。在通信过程中，发送方用自己的私钥对信息进行签名，接受方可以用发送方的公钥验证其签名；发送方也可以用接受方的公钥对信息进行加密，而也只有相应接受方的私钥能够对其解密。
- **认证机构（CA，Certificate Authority）**：CA 是一个向个人、计算机或任何其它实体颁发证书的可信实体。CA 受理证书申请，根据证书管理策略验证申请人的信息，然后用其私钥对证书进行签名，并颁发该证书。
- **注册机构（RA，Registration Authority）**：RA 是 CA 的延伸，一方面向 CA 转发实体传输过来的证书申请请求，另一方面向目录服务器转发 CA 颁发的数字证书和证书撤消列表，以提供目录浏览和查询服务。
- **轻量级目录访问协议（LDAP，Light-weight Directory Access Protocol）服务器**：LDAP 提供了一种访问 PKI 数据库（Repository）的方式，通过该协议来访问并管理 PKI 信息。LDAP 服务器提供目录浏览服务，负责将注册机构服务器传输过来的用户信息以及数字证书加入到 LDAP 服务器上。这样用户通过访问 LDAP 服务器就能够得到自己和其他用户的数字证书。
- **证书废除列表（CRL，Certificate Revocation List）**：证书具有一定的寿命，另外由于泄露密钥、业务终止等原因，CA 也可通过称为证书吊销的过程来缩短这一寿命。一个证书一旦被撤消，证书中心就要公布 CRL 来声明该证书是无效的，并列出被认为不能再使用的证书的序列号。CRL 为应用程序和其它系统提供了一种检验证书有效性的方式，它们存储在数据库（LDAP 服务器）中，提供了一种通知用户和其他应用的中心管理方式。

9.1.3 主要应用

PKI 作为一组在分布式计算系统中利用公钥技术和 X.509 证书所提供的安全服务，可以为各种目的颁发证书，如 Web 用户身份验证、Web 服务器身份验证、使用安全/多用途 Internet 邮件扩充协议（S/MIME，Secure/Multipurpose Internet Mail Extensions）的安全电子邮件、虚拟专用网络（VPN，Virtual Private Network）、IP 安全性(IP security)、Internet 密钥交换协议（IKE，Internet Key Exchange）、安全套接字协议层/传输层安全性（SSL/TLS，Secure Sockets Layer/Transport Layer Security）和数字签名。证书还可以由一个 CA 颁发给另一个 CA，以建立证书层次结构。

9.1.4 配置任务列表

针对一个使用 PKI 的网络，配置 PKI 的目的就是为指定的设备向 CA 申请一个本地证书并进行证书的有效性验证。配置任务包括：

- PKI 证书申请配置
- PKI 证书验证配置
- 显示和调试配置

9.2 证书申请配置

9.2.1 证书申请概述

证书申请就是实体向 CA 自我介绍的过程，实体向 CA 提供身份信息，该信息随后将成为所颁发证书的一部分。CA 根据一套标准受理申请，对证书申请者的信用度、申请证书的目的、身份的真实可靠性等问题进行审查，确保证书与身份绑定的正确性。该标准可能要求进行脱机的、非自动的带外方式（如电话、磁盘、电子邮件等）身份验证。如果申请被成功受理，CA 随后将向该用户颁发证书，同时将用户的一些公开信息和证书放到 LDAP 服务器上提供目录浏览服务。用户随后可以到指定位置下载自己的公钥数字证书，也可以通过 LDAP 服务器获得其他用户的公钥数字证书。根据 PKI 证书管理策略，实现本地证书申请的配置任务包括：

- 进入 PKI 域视图
- 指定信任的 CA
- 配置证书申请的服务器
- 配置实体命名空间
- 创建本地公、私密钥对
- 配置查询证书申请处理状态的重发间隔和次数
- 配置证书申请模式
- 手工申请证书
- 证书获取

9.2.2 进入 PKI 域视图

PKI 域是将信任同一第三方可信任机构的一组 PKI 用户进行统一管理，即组内的每个成员只需同 CA 建立单一的信任关系即可，无需每位成员之间互相建立成对的信任关系，这样大大减轻了系统负荷，极大加强了 PKI 证书体系的扩展能力。

在配置域参数之前，必须首先进入 PKI 域视图。

请在系统视图下进行下列配置。

表9-1 进入 PKI 域视图

操作	命令
指定 PKI 域名并进入域视图	pki domain name
删除指定的 PKI 域及域内的所有配置信息	undo pki domain name

缺省情况下，未指定 PKI 域名。

说明：

目前一个设备只支持两个 PKI 域，所以若要在已存在两个域的情况下添加新域，则需使用相应的 undo 命令删除一个旧域。

9.2.3 配置信任的 CA

在申请证书时，是通过为主体提供担保的另一个可信实体认证中心来完成注册颁发的。认证中心是公钥基础设施的核心，有了大家信任的认证中心，用户才能放心方便的使用公钥技术带来的安全服务。

请在 PKI 域视图下，进行下列配置。

表9-2 指定信任的 CA

操作	命令
指定本设备信任 CA 的名称	ca identifier name
删除本设备信任 CA 的名称	undo ca identifier

缺省情况下，未指定本设备信任的 CA。

说明：

CA 在受理证书请求（以及颁发证书、吊销证书和发布 CRL）时所采用的一套标准被称为 CA 策略。通常，CA 以一种叫做证书惯例声明（CPS, Certification Practice Statement）的文档发布其策略，CA 策略可以通过带外或其他方式获取。由于不同的 CA 使用不同的方法验证公钥与主体之间的绑定，所以在选择信任的 CA 进行证书申请之前，理解其策略是非常重要的。

9.2.4 配置申请证书的服务器

1. 配置证书申请所使用的实体

在向 CA 发送证书申请请求时，必须指定所使用的实体名，以向 CA 表明自己的身份。

请在 PKI 域视图下，进行下列配置。

表9-3 配置证书申请所使用的实体名

操作	命令
配置证书申请所使用的实体名	certificate request entity <i>entity-name</i>
取消证书申请所使用的实体名	undo certificate request entity

缺省情况下，未指定设备申请证书时所使用的实体名称。

说明：

关于实体entity-name的相关信息，请参阅 9.2.5 实体命名空间部分。

2. 配置证书申请的注册受理机构

注册管理一般由一个独立的注册机构（即 RA）来承担，它接受用户的注册申请，审查用户的申请资格，并决定是否同意 CA 给其签发数字证书。注册机构并不给用户签发证书，而只是对用户进行资格审查。有时 PKI 把注册管理的职能交给 CA 来完成，而不设立独立运行的 RA，但这并不是取消了 PKI 的注册功能，而只是将其作为 CA 的一项功能而已。

请在 PKI 域视图下，进行下列配置。

表9-4 选择证书申请注册机构

操作	命令
指定证书注册申请的受理机构	certificate request from { <i>ca</i> <i>ra</i> }
删除证书注册申请的受理机构	undo certificate request from

缺省情况下，未指定证书注册申请的受理机构。

PKI 安全策略推荐使用 RA 作为注册受理机构。

3. 配置申请证书的服务器位置

证书申请之前必须指定注册服务器位置 URL，随后实体可通过简单证书注册协议（SCEP，Simple Certification Enrollment Protocol）向该服务器提出证书申请，SCEP 是专门用于与认证权威机构进行通信的协议。

请在 PKI 域视图下进行下列配置。

表9-5 指定申请证书的服务器位置

操作	命令
设置证书申请注册机构的位置	certificate request url <i>string</i>
删除证书申请注册机构的位置	undo certificate request url

缺省情况下，未指定证书申请机构的服务器位置。

4. 配置 LDAP 服务器地址

在 PKI 系统中，用户的证书和 CRL 信息的存储是一个非常核心的问题。一般采用 LDAP 目录服务器，用来存储证书和 CRL。

请在 PKI 域视图下，进行下列配置。

表9-6 指定 LDAP 服务器地址

操作	命令
指定 LDAP 服务器 IP 地址	ldap-server ip <i>ip-address</i> [port <i>port-num</i>] [version <i>version-number</i>]
删除 LDAP 服务器 IP 地址	undo ldap-server

缺省情况下，未指定 LDAP 服务器。

5. 配置验证根证书时使用的指纹

当防火墙从 CA 获得身份证书时，需要使用 CA 的根证书来验证身份证书的真实性和合法性。当防火墙从 CA 获得其根证书时，需要验证 CA 根证书的指纹，即根证书内容的散列值，该值对于每一个证书都是唯一的。如果 CA 根证书的指纹与在此处配置的指纹不同，则防火墙将拒绝接收根证书。指纹可以为 MD5 指纹或者 SHA1 指纹。

请在 PKI 域视图下，进行下列配置。

表9-7 配置验证根证书时使用的指纹

操作	命令
配置验证根证书时使用的指纹	root-certificate fingerprint { md5 sha1 } <i>string</i>
取消配置的指纹	undo root-certificate fingerprint

缺省情况下，未配置验证证书时使用的指纹。

当选择 MD5 指纹时，*string* 必须为 32 个字符，并且以 16 进制的形式输入；当选择 SHA1 指纹时，*string* 必须为 40 个字符，并且以 16 进制的形式输入。

9.2.5 配置实体命名空间

1. 命名空间概述

在构建 PKI 时，要考虑的一个重要的问题便是实体的命名空间（Name Space）。在一份证书中，必须证明公钥及其所有者的姓名是一致的，每个 CA 都要用它认为重要的信息对一个实体进行细致的描述。这里可以通过唯一的标识符（或称 DN-distinguished name）来唯一确定单个主体，它由许多部分组成，如用户通用名、组织单位、国家或者证书持有人的姓名等信息。DN 在网络上应该是唯一的。

本章介绍了进入 PKI 实体视图后如何对实体的 DN 相关信息进行配置，内容包括：

- 定义 PKI 实体名称
- 配置实体 FQDN
- 配置实体所属国家
- 配置实体所属州省
- 配置实体所在地理区域
- 配置实体所属组织名称
- 配置实体所属组织部门
- 配置实体通用名
- 配置实体 IP 地址

说明：

实体的配置信息必须与 CA 证书颁发策略相匹配，以确认实体 DN 配置任务，如哪些实体参数必须配置，哪些可选配，否则证书申请可能会失败。

2. 定义 PKI 实体名称

PKI 实体视图提供了配置实体 DN 各项属性的平台。

请在系统视图下进行下列配置。

表9-8 配置实体名称

操作	命令
配置实体名称，并进入该实体视图	pki entity name-str
删除此实体名称及该实体参数	undo pki entity name-str

缺省情况下，未指定实体名称。

 说明：

- 实体名称必须与注册受理机构配置 **certificate request entity** *entity-name* 中指定的 *entity-name* 一致，否则该实体的证书申请会失败。*name-str* 只是用来方便引用，不用于证书的任何字段。
 - Windows 2000 CA 服务器对证书申请的数据长度有一定的要求，entity 配置项超过一定的数据长度后，申请证书将失败。
-

3. 配置实体的 FQDN 名称

FQDN（Fully Qualified Domain Name）是实体在网络中的唯一标识，如 Email 地址，一般形式为：user.domain，可被解析为 IP 地址。FQDN 与指定实体 IP 地址的功能相同，可选配。

请在 PKI 实体视图下进行下列配置。

表9-9 实体 FQDN 配置

操作	命令
配置实体 FQDN 名称	fqdn <i>name-str</i>
删除此实体 FQDN 名称	undo fqdn

缺省情况下，未指定实体 FQDN。

4. 配置实体所属国家

请在 PKI 实体视图下进行下列配置。

表9-10 实体所属国家配置

操作	命令
配置实体所属国家代码	country <i>country-code-str</i>
删除此实体所属国家代码	undo country

缺省情况下，未指定实体所属国家。

 说明：

代码用标准的 2 字符代码。例如：CN 是中国的合法国家代码，US 是美国的合法国家代码。

5. 配置实体所属州省

在 PKI 实体视图下进行下列配置。

表9-11 实体所属州省配置

操作	命令
配置实体所属州省	state <i>state-str</i>
删除此实体所属州省	undo state

缺省情况下，未指定实体所属州省。

6. 配置实体所在地理区域

在 PKI 实体视图下进行下列配置。

表9-12 实体所在地理区域配置

操作	命令
配置实体所在地理区域	locality <i>locality-str</i>
删除此实体所在地理区域	undo locality

缺省情况下，未指定实体所在的地理区域。

7. 配置实体所属组织名称

在 PKI 实体视图下进行下列配置。

表9-13 实体所属组织配置

操作	命令
配置实体所属组织名称	organization <i>org-str</i>
删除此实体所属组织名称	undo organization

缺省情况下，未指定实体所属的组织。

8. 配置实体所属组织部门

可以使用这个可选择的字段在同一个单位内区分不同的部门。

请在 PKI 实体视图下进行下列配置。

表9-14 实体所属部门配置

操作	命令
配置实体所属组织部门	organization-unit <i>org-unit-str</i>
删除此实体所属组织部门	undo organization-unit

缺省情况下，未指定实体所属的部门。

9. 配置实体的通用名

请在 PKI 实体视图下进行下列配置。

表9-15 实体通用名配置

操作	命令
配置实体通用名	common-name <i>name-str</i>
删除此实体通用名	undo common-name

缺省情况下，未指定实体的通用名。

10. 配置实体的 IP 地址

与指定实体 FQDN 的功能相同，可选配。

请在 PKI 实体视图下进行下列配置。

表9-16 实体 IP 地址配置

操作	命令
配置实体 IP 地址	ip <i>ip-address</i>
删除此实体 IP 地址	undo ip

缺省情况下，未指定实体 IP 地址。

9.2.6 创建公、私密钥对

密钥对的产生是证书申请过程中重要的一步，它使用了一对密钥：私钥和公钥。私钥由用户保留；公钥和其他信息则交于 CA 中心进行签名，从而产生证书。另外，每一个由 CA 颁发的证书都会有有效期，证书生命周期的长短由签发证书的 CA 中心来确定。当用户的私钥被泄漏或证书的有效期快到时，用户应该删除旧的密钥对，产生新的密钥对，重新申请新的证书。

该配置任务用来产生本地密钥对。如果此时已经有了 RSA 密钥，系统提示是否替换原有密钥。产生的密钥对的命名方式为：防火墙名称+host。主机密钥的最小长度为 512 位，最大长度为 2048 位。

请在系统视图下进行下列配置。

表9-17 创建和销毁本地 RSA 密钥对

操作	命令
创建本地 RSA 密钥对	rsa local-key-pair create
销毁本地 RSA 密钥对	rsa local-key-pair destroy

缺省情况下，本地没有 RSA 密钥对，需要用户创建。



注意：

- 当本地证书已存在时，为保证密钥对与现存证书的一致性，不应执行创建密钥对命令，必须删除本地证书后方可执行该命令生成新的密钥对。
- 若本地已有 RSA 密钥对，则创建的新密钥对将覆盖掉旧密钥对。
- 这两个密钥对本来是提供给 SSH 使用，其中本地服务器密钥对周期性由本地服务器改变；主机密钥对不变。申请证书时我们使用的是主机密钥对。

9.2.7 配置查询证书申请处理状态的重发间隔和次数

实体在发送证书申请后，如果 CA 采用手工验证申请，会需要很长时间才能发布证书。在此期间，客户端需要定期发送状态查询，以便在证书签发后能及时获取到证书。

请在 PKI 域视图下，进行下列配置。

表9-18 配置证书申请状态查询的重发间隔和次数

操作	命令
配置证书申请状态查询重发间隔和次数	certificate request polling {interval minutes count count }
恢复证书申请状态查询重发间隔和次数为缺省值	undo certificate request polling { interval count }

缺省情况下，证书申请状态查询重发次数为 5，间隔为 20 分钟。

9.2.8 配置证书申请模式

证书申请有手工发起和自动发起方式。如果是自动方式，则在本地没有自己的证书时自动通过 SCEP 协议进行申请，而且在证书快要过期时自动申请新的证书。如果为手工方式，则需要手工完成各项证书申请工作。

请在 PKI 域视图下，进行下列配置。

表9-19 证书申请模式

操作	命令
配置证书获取方式	certificate request mode { manual auto [key-length key-length password { simple cipher } password]* }
恢复证书获取方式为缺省值	undo certificate request mode

缺省情况下，证书申请为手工方式。

9.2.9 手工申请证书

完整的证书请求由用户公钥和相关登记信息构成，在完成以上配置后，即可向 PKI 注册认证机构发起申请本地证书请求。

请在系统视图下进行下列操作。

表9-20 证书申请操作

操作	命令
证书申请操作	pki request-certificate domain <i>domain-name</i> [<i>password</i>] [pkcs10 [<i>filename filename</i>]]



注意：

- 如果本地证书已存在，不允许再执行证书申请操作，避免因相关配置的修改使得证书与登记信息不匹配。若想重新申请，请先使用 **pki delete-certificate** 命令删除存储于本地的 CA 证书与本地证书，然后再执行此申请命令。
- 当出现无法通过 SCEP 协议向 CA 申请证书的异常情况时，可以使用可选参数 **pkcs10** 打印出本地的证书请求信息，用户保存该信息，并将该信息通过带外方式发送给 CA 进行证书请求。
- 证书申请之前必须保证实体的时钟必须与 CA 同步，否则申请的证书的有效期会出现异常。
- 如果使用 Windows CA 服务器进行证书获取，那么在安装 Windows CA 服务器时，RA 的标示符（或称 DN-distinguished name）不能与 CA 的标示符一致，否则会导致获取不到 CA 证书和本地证书。
- 该操作不被保存在配置中。

9.2.10 手工获取证书

这里证书获取的目的有两个：其一是将 CA 签发的证书中与本安全域有关的证书存放到本地，以提高证书的查询效率，减少向 PKI 证书存储库查询的次数；其二是为证书的验证做好准备。

下载数字证书时如果选择参数 **local**，则下载本地证书，如果参数为 **ca**，则下载 CA 的证书。

请在系统视图下进行下列操作。

表9-21 证书获取操作

操作	命令
获取证书并下载至本地	pki retrieval-certificate { local ca } domain <i>domain-name</i>



注意：

- 如果本地已有 CA 证书存在，则不允许执行获取 CA 证书操作，避免因相关配置的修改使得证书与登记信息不匹配。若想重新获取，请先使用 `pki delete-certificate` 命令删除 CA 证书与本地证书后，再执行此获取命令。
- 该操作不被保存在配置中。

9.2.11 导入证书

使用以下配置可以导入已有的本地证书或 CA 证书。

请在系统视图下进行下列操作。

表9-22 导入证书

操作	命令
导入证书	<code>pki import-certificate { local ca } domain domain-name { der p12 pem } [filename filename]</code>

9.2.12 删除证书

用户可以删除一个已经存在的本地证书或 CA 证书。

请在系统视图下进行下列操作。

表9-23 删除证书

操作	命令
删除证书	<code>pki delete-certificate { local ca } domain domain-name</code>

9.3 证书验证配置

9.3.1 证书验证配置任务列表

在数据通信的各个环节，通信双方都需验证相应证书的有效性。证书验证的目的也就是检查一个证书的有效性。验证证书需要作签发时间、签发者信息以及证书的有效性几方面的验证。证书验证的核心就是检查 CA 在证书上的签名，并确定证书仍在有效期内，而且未被废除。由于人们相信 CA 不会发行伪造证书，所以含有它的真实签名的任何证书都可得到验证。比如你收到的一封邮件，邮件中附有一个包含公共密钥的证书，而该邮件使用了私有密钥加密，为了确定该用户是否合法持有该证书并且证书没有过期（通过 CRL 判断），以及该证书是否值得信任，就必须验证证书是否有效。

要实现证书验证功能，一般需要完成以下配置及操作任务：

- 配置 CRL 发布点位置
- 配置 CRL 更新周期
- 配置是否必须检查 CRL
- 获取 CRL
- 证书验证

9.3.2 配置 CRL 发布点位置

请在 PKI 域视图下进行下列配置。

表9-24 CRL 发布点位置配置

操作	命令
指定 CRL 发布点位置	crl url { url-string scep }
删除 CRL 发布点位置	undo crl url

缺省情况下，未指定 CRL 发布点位置。

9.3.3 配置 CRL 更新周期

CRL 的更新周期是指本地从 CRL 存储服务器上下载 CRL 的时间间隔。

请在 PKI 域视图下进行下列配置。

表9-25 CRL 更新周期配置

操作	命令
设置更新 CRL 的周期	crl update-period hours
恢复更新 CRL 的周期为缺省值	undo crl update-period

缺省情况下，根据 CRL 的有效期进行更新。

 说明：

手工配置的 CRL 更新时间将优先于 CRL 中指明的更新时间。

9.3.4 配置是否必须检查 CRL

配置证书验证时可以设置是否必须进行 CRL 检查。可以直接在 CA 中心进行验证，也可以将 CRL 下载到本地进行验证。

请在 PKI 域视图下进行下列配置。

表9-26 配置 CRL 检查

操作	命令
禁止 CRL 检查	crl check disable
使能 CRL 检查	undo crl check disable

缺省情况下，必须进行 CRL 检查。

9.3.5 获取 CRL

在完成以上配置后，即可在系统视图下发起 CRL 获取操作。下载 CRL 目的是验证当前本地所获得证书的合法性。

请在系统视图下进行下列操作。

表9-27 CRL 获取操作

操作	命令
获取 CRL 并下载至本地	pki retrieval-crl domain <i>domain-name</i>

 说明：

该操作不被保存在配置中。

9.3.6 验证证书

用户可以检查一个证书的有效性。如果使用参数 **local**，则验证本地证书。如果参数为 **ca**，则验证 CA 的证书。

请在系统视图下进行下列操作。

表9-28 证书验证操作

操作	命令
检验本地证书的有效性	pki validate-certificate { local ca } domain <i>domain-name</i>

 说明：

该操作不被保存在配置中。

9.4 显示和调试

1. 证书显示

证书成功获取后，用户可以通过下面的操作，显示下载到本地的 CA 签名的证书内容。证书格式及内容遵循 X.509 标准，包含关于用户及 CA 自身的各种信息，如：能唯一标识用户的姓名及其他标识信息，如个人的 E-mail 地址、证书持有者的公钥、签发个人证书的认证机构的名称、个人证书的序列号和个人证书的有效期（证书有效起止日期）等。

请在任意视图下进行下列操作。

表9-29 PKI 显示和调试操作

操作	命令
显示证书内容	display pki certificate { { local ca } domain <i>domain-name</i> request-status }

2. CRL 显示

CRL 成功获取后，用户可以通过下面的操作，显示和查看下载到本地的 CRL 内容。CRL 内容遵循 X.509 标准，包含的内容有：CRL 的版本号、签名算法、证书签发机构名、此次签发时间、下次签发时间、用户公钥信息、签名算法、签名值、序列号、撤销日期等。

请在任意视图下进行下列操作。

表9-30 PKI 显示和调试操作

操作	命令
显示 CRL 内容	display pki crl domain <i>domain-name</i>

3. 配置显示及调试

在配置过程中，可执行 **display current-configuration** 命令显示当前的 PKI 配置情况。在证书操作过程中，可打开 PKI 调试开关对相应证书操作进行监控和诊断。

请在用户视图下进行下列操作。

表9-31 PKI 显示和调试操作

操作	命令
打开 PKI 调试开关	debugging pki { all verify request retrieval error }
关闭 PKI 调试开关	undo debugging pki { all verify request retrieval error }

缺省情况下，PKI 调试开关全部关闭。

9.5 典型配置举例

9.5.1 使用 PKI 证书方法进行 IKE 协商认证

1. 组网需求

在 SecPathA 和 SecPathB 之间建立一个 IPsec 安全隧道对 PC A 代表的子网（10.1.1.x）与 PC B 代表的子网（10.1.2.x）之间的数据流进行安全保护。SecPathA 和 SecPathB 之间使用 IKE 自动协商建立安全通信，IKE 认证策略采用 PKI 证书体系进行身份认证。

图 1-2 中假设 SecPathA 和 SecPathB 使用不同的 CA（可以相同，根据实际情况确定）。

2. 组网图

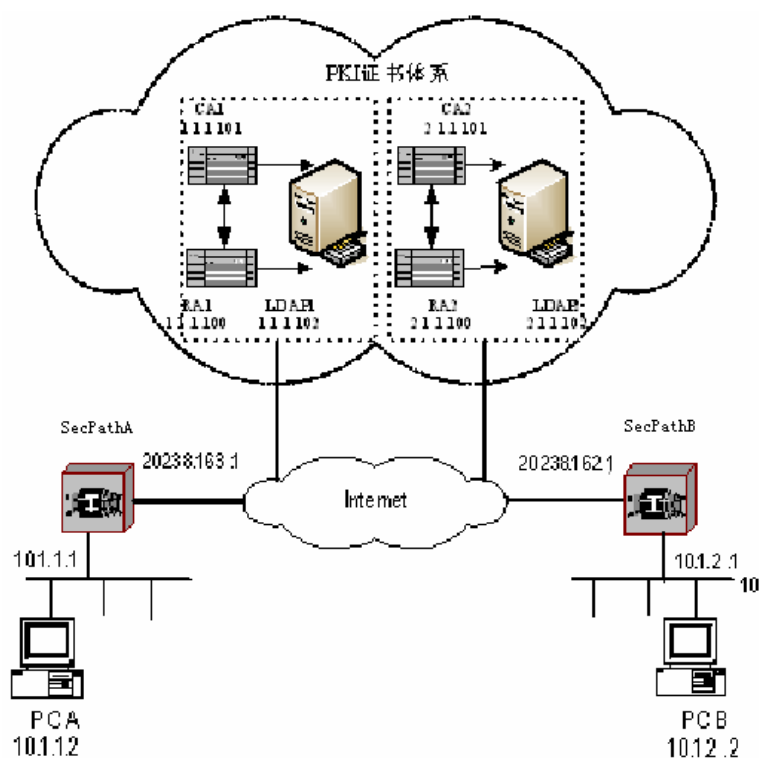


图9-2 PKI 进行 IKE 协商认证的组网图

3. 配置步骤

(1) SecPathA 配置：

在 SecPathA 上使用缺省的 IKE 策略，并配置使用 PKI (rsa-signature) 方法为身份认证策略。

```
[H3C] ike proposal 1
[H3C-ike-proposal-1] authentication-method rsa-signature
[H3C-ike-proposal-1] quit
# 实体 DN 配置。

[H3C] pki entity en
[H3C-pki-entity-en] ip 202.38.163.1
[H3C-pki-entity-en] common-name SecPathA
[H3C-pki-entity-en] quit
# PKI 域参数配置。

[H3C] pki domain 1
[H3C-pki-domain-1] ca identifier CA1
[H3C-pki-domain-1] certificate request url
http://1.1.1.100/certsrv/mscep/mscep.dll
[H3C-pki-domain-1] certificate request entity en
[H3C-pki-domain-1] certificate request from ra
[H3C-pki-domain-1] ldap-server ip 1.1.1.102
# CRL 发布点位置配置（若 CRL 必须检查为 disable，则无需配置）。

[H3C-pki-domain-1] crl url ldap://1.1.1.102
[H3C-pki-domain-1] quit
# 用 RSA 算法生成本地的密钥对。

[H3C] rsa local-key-pair create
# 证书申请

[H3C] pki retrieval-certificate ca domain 1
[H3C] pki request-certificate domain 1
(2) SecPathB 配置：
# 在 SecPathB 上使用缺省的 IKE 策略，并配置使用 PKI（rsa-signature）方法为身
份认证策略。

[H3C] ike proposal 1
[H3C-ike-proposal-1] authentication-method rsa-signature
[H3C-ike-proposal-1] quit
# 实体 DN 配置。

[H3C] pki entity en
[H3C-pki-entity-en] ip 202.38.162.1
[H3C-pki-entity-en] common-name SecPathB
[H3C-pki-entity-en] quit
# PKI 域参数配置。

[H3C] pki domain 1
[H3C-pki-domain-1] ca identifier CA2
```

```
[H3C-pki-domain-1] certificate request url
http://2.1.1.100/certsrv/mscep/mscep.dll
[H3C-pki-domain-1] certificate request entity en
[H3C-pki-domain-1] certificate request from ra
[H3C-pki-domain-1] ldap-server ip 2.1.1.102
# CRL 发布点配置（若 CRL 必须检查为 disable，则无需配置）。

[H3C-pki-domain-1] crl url ldap://2.1.1.102
[H3C-pki-domain-1] quit

# 用 RSA 算法生成本地的密钥对。

[H3C] rsa local-key-pair create

# 证书申请

[H3C] pki retrieval-certificate ca domain 1
[H3C] pki request-certificate domain 1
```

 说明：

以上是对 IKE 协商采用 PKI 身份认证方法的配置，若希望建立 IPsec 安全通道进行安全通信，还需要进行 IPsec 的相应配置，具体内容请参考“IPsec 配置”章和“IKE 配置”章中的配置。

9.6 证书故障诊断与排除

9.6.1 故障之一：获取 CA 的证书失败

故障排除：发出手工 CA 证书请求时失败，可能有以下原因：

(1) 软件原因

- 没有设置信任的 CA 名称。
- SCEP 证书请求的服务器 URL 位置不正确或未配置，可通过 ping 命令测试服务器是否连接正常。
- 没有设置证书注册机构。
- 设备的系统时钟与 CA 服务器的时钟不同步。

(2) 硬件原因

- 网络连接是否有故障，如网线折断，接口松动。

9.6.2 故障之二：本地证书申请失败

故障排除：防火墙配置完 PKI 域参数、实体 DN、创建了新 RSA 密钥对后，发出手工证书请求时失败，可能有以下原因：

(1) 软件原因

- 申请之前没有先获取 CA/RA 的证书。
- 未创建密钥对或目前的密钥对已有证书。
- 没有设置信任的 CA 名称。
- SCEP 证书请求的服务器 URL 位置不正确或未配置，可通过 ping 命令测试服务器是否连接正常。
- 没有设置证书注册机构。
- 没有配置实体 DN 中必配属性，可通过查看 CA/RA 注册策略选择相关的属性进行配置。

(2) 硬件原因

- 网络连接是否有故障，如网线折断，接口松动。

9.6.3 故障之三：CRL 获取失败

故障排除：获取 CRL 发生失败，可能有以下原因：

(1) 软件原因

- 获取 CRL 之前未先取得本地证书。
- 未设置 LDAP 服务器的 IP 地址。
- 未设置 CRL 分布点位置。
- LDAP 服务器版本配置错误。

(2) 硬件原因

- 网络连接是否有故障，如网线折断，接口松动。

第10章 SSL 配置

10.1 SSL 简介

SSL 协议是由 Netscape 公司开发的，是一种在两台设备之间提供安全通道的协议。它具有保护传输数据以及识别通信机器的功能。SSL 协议设计目标主要有两个：第一是为客户端与服务器之间的传输提供保密性；第二是身份认证（包括服务器认证和可选客户端认证）。协议本身可以分为两层：底层为 SSL 记录协议，上层为 SSL 握手协议、SSL 密码变化协议和 SSL 警告协议。这四个协议中最为复杂的是 SSL 握手协议。

SSL 记录协议：主要负责把上层的数据分块（Fragment），进行压缩（compress），在尾部加 MAC（保证数据的完整性），最后加密数据和 MAC，再把加密好的整块 record 传输给接受方。

SSL 握手协议：客户端和服务器通过握手协议建立一个会话（session），包含一组参数，主要有会话 ID、对方的证书、加密套件、压缩算法、以及 mastersecret，还必须标记该会话是否为可恢复的。同时该会话可以被多个连接共享，避免昂贵的开销。

SSL 密码变化协议：这个协议使用一条消息——ChangeCipherSpec，客户端和服务端双方均可以发送，目的是通知接受方，随后的 record 都使用新的加密套件和参数。

SSL 警告协议：用来允许一方向另一方报告例外条件。消息本身非常简单，包含严重程度（Warning Level 和 Fatal Level）和详细的描述（具体的情况）。

SSL 协议提供了全面的安全策略：协商加密套件后，使用套件中的非对称加密算法实现会话密钥的交换，利用证书的身份认证方式保证用户的合法性，在传输过程中用密钥对数据进行加密，保证应用数据传输时的安全性。如果发生数据的篡改、用户身份验证非法等错误时，自动断开连接，防止各种类型的恶意攻击。

在 SSL 的基础上，实现 HTTPS 服务器和 HTTPS 客户端，保证远端合法用户可以安全的登录到设备上。对设备进行管理时，设备和远程用户之间的数据传输都是经过加密的，保证了设备的安全性。基于证书属性的访问控制，通过制定访问策略，控制登录到设备的用户的访问权限，保证设备资源不被非法的人员读取或者修改，提高设备的安全性。

另外，可以通过实现 SSL Proxy 对客户端发送的请求进行解密，把解密后的明文数据发送给 HTTP 服务器；SSL Proxy 从服务器获得响应，把响应的数据进行加密，发送给客户端。SSL Proxy 通过处理数据的加密和解密，可以减轻服务器的负荷，提高服务器的性能。

数字证书通常用来验证通信双方的身份，以保证通信的安全。服务器利用客户提供的证书进行身份验证之后，若客户身份合法，则可进一步利用证书中包含的属性以及属性值进行访问控制，只有当客户证书的属性值都符合服务器预先设置的条件时，才允许该客户访问服务器资源。基于证书属性的访问控制，为 SSL 进一步增强了安全访问控制能力。

SSL 主要的应用包括两个方面：HTTPS 和 SSL Proxy。

- HTTPS 应用

HTTPS 的应用包括服务器端和客户端的应用。

在设备上建立 HTTPS 服务，客户端通过 SSL 协议远程连接到设备上对设备进行管理。客户端与远程设备之间交互的数据经过加密，保证了数据传输的安全性和完整性，从而实现了设备的安全管理。此外，可以在设备上的 HTTPS 服务中实施基于证书属性的访问控制，为设备制定基于证书属性的访问控制方案和策略，对客户端的访问权限进行控制，进一步避免了非法客户对设备进行攻击，提高设备的安全性。

设备可以通过 HTTPS 客户端访问服务器资源，能够保证资源请求被安全可靠的传输到服务器端，而且能够从服务器安全可靠的、完整的获取资源。

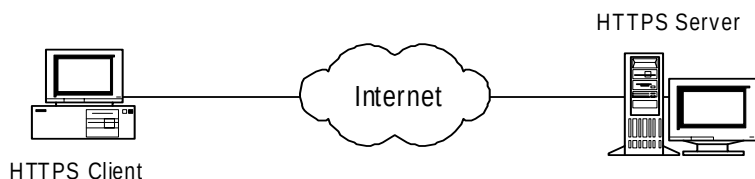


图10-1 HTTPS 应用图示

- SSL Proxy

客户端通过 SSL 协议与服务器连接，在握手阶段进行参数和密钥协商，这会占用 HTTPS 服务器大量的 CPU 资源；当传递应用数据时，需要进行数据的加密和解密，同样会占用大量的 CPU 资源。如果把 SSL 协议处理的过程从 HTTPS 服务器分离出来，而由 SSL Proxy 负责，将会减少 HTTP 服务器的 CPU 开销，从而提高 HTTP 服务器的性能。

SSL Proxy 处于 HTTPS 客户端与 HTTP 服务器两者之间，作为客户端与服务器通信的桥梁。当客户端发出 HTTPS 请求后，SSL Proxy 负责与客户端完成 SSL 连接，建立与客户端之间的 SSL 通道。之后，SSL Proxy 与目标 HTTP 服务器建立 TCP 连接，将客户端的资源请求以明文形式转发给 HTTP 服务器。当 SSL Proxy 收到 HTTP 服务器的响应之后，将该响应加密打包成 SSL 记录转发给 HTTPS 客户端，从而完成了 HTTPS 客户端与目标 HTTP 服务器的通信。SSL Proxy 在通信中分担了 HTTP 服务器的数据加密、解密操作，提高了服务器的性能。

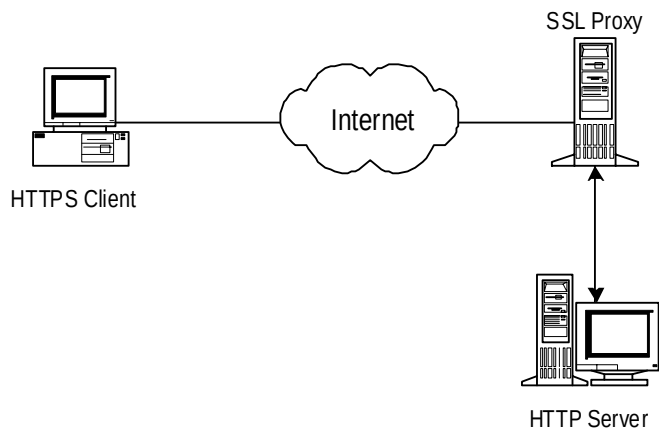
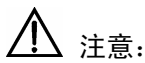


图10-2 SSL Proxy 应用图示

10.2 SSL 配置



注意：

若要使防火墙正常运行 SSL 代理功能，须确保防火墙的内存不能小于 512MB。

SSL 的配置包括：

- 配置服务器端 SSL 策略
- 配置 SSL 加密卡
- 配置基于证书属性的访问控制策略
- 配置 SSL Proxy 服务器策略

10.2.1 配置服务器端 SSL 策略

1. 创建服务器端 SSL 策略

服务器端策略是配置 SSL Proxy 启动时使用的 SSL 连接参数。需要使用 **ssl server-policy** 命令创建一个服务器端 SSL 策略，并进入服务器端 SSL 策略视图。

请在系统视图下进行下列配置，必需配置。

表10-1 创建服务器端 SSL 策略

操作	命令
创建一个服务器端 SSL 策略	ssl server-policy <i>policy-name</i>
删除一个或全部服务器端 SSL 策略	undo ssl server-policy { <i>policy-name</i> all }

 说明：

一个 HTTPS 服务器或 SSL Proxy 有可能根据不同需要使用不同的 SSL 策略，对于 SSL 策略应该能针对每一个策略有其单独的配置信息，所以采用 SSL 策略视图进行参数的配置。

2. 指定服务器端 SSL 策略使用的 PKI 域

服务器端在启动 HTTPS 服务器或 SSL Proxy 时，从配置的 PKI 域获取服务器端使用的证书和证书链以及用来验证客户端证书的 CA 证书。

请在服务器端 SSL 策略视图下进行下列配置，必需配置。

表10-2 配置 PKI 域

操作	命令
配置 PKI 域	<code>pki-domain pki-name</code>
删除此服务器端策略的 PKI 域	<code>undo pki-domain</code>

缺省情况下，未指定服务器端策略的 PKI 域。

 注意：

PKI域必须先系统在视图下配置好，且该PKI域必须先申请好证书和获取CA的证书。有关PKI的信息请参见 第 9 章 PKI配置。

3. 配置服务器端支持的加密套件列表

配置服务器端支持的加密套件列表。

请在服务器端策略视图下进行下列配置，可选配。

表10-3 配置服务器端支持的加密套件列表

操作	命令
增加服务器端使用的加密套件	<code>ciphersuite { rsa_rc4_128_md5 rsa_rc4_128_sha rsa_des_cbc_sha rsa_3des_ede_cbc_sha rsa_aes_128_cbc_sha rsa_aes_256_cbc_sha } *</code>
删减服务器端使用的加密套件	<code>undo ciphersuite [rsa_rc4_128_md5 rsa_rc4_128_sha rsa_des_cbc_sha rsa_3des_ede_cbc_sha rsa_aes_128_cbc_sha rsa_aes_256_cbc_sha] *</code>

缺省情况下，使用全部 6 种加密套件。

在使用 **undo ciphersuite** 命令时，如果不提供参数，表示撤销所有已配置的加密套件，恢复为上述 6 种都支持。

4. 配置 SSL 握手连接保持时间

请在服务器端策略视图下进行下列配置，可选配。

表10-4 配置服务器端 SSL 握手连接保持时间

操作	命令
配置服务器端 SSL 握手连接保持时间	handshake timeout time
恢复默认的服务器端 SSL 握手连接保持时间	undo handshake timeout

time 为握手连接的保持时间，单位为秒，范围为 180~7200。缺省情况下，保持时间为 3600 秒。

5. 配置 SSL 连接关闭模式

服务器的关闭模式有两种，一种为发送 **close-notify** 警告消息给客户端后，等待客户端的 **close-notify** 警告消息，即 **wait** 模式。另一种为非 **wait** 关闭模式，即服务器发送 **close-notify** 警告消息给客户端，在关闭会话前并不等待客户端的 **close-notify** 警告。

请在服务器端策略视图下进行下列配置，可选配。

表10-5 配置 SSL 连接关闭模式

操作	命令
配置 SSL 连接关闭模式为 wait 模式	close-mode wait
恢复默认的 SSL 连接关闭行为	undo close-mode wait

缺省情况下，服务器发送 **close-notify** 警告消息给客户端，在关闭会话前并不等待客户端的 **close-notify** 警告。

说明：

仅当使用硬件加密时，配置 **close-mode wait** 命令后，服务器的关闭模式才为 **wait** 模式；当使用软件加密时，此命令不生效。

6. 配置是否对客户端进行认证

服务器端在握手过程中可以选择是否进行基于证书的 SSL 客户端认证。

请在服务器端策略视图下进行下列配置，可选配。

表10-6 配置是否对客户端进行认证

操作	命令
配置服务器端需要认证客户端	client-verify enable
配置服务器端不对客户端进行认证	undo client-verify enable

缺省情况下，不进行客户端认证。

7. 配置会话缓存保存时间和大小

SSL 服务器可以配置会话缓存中单元的保存时间，它指定会话单元在缓存中保存时间值为 *time*，会话单元只有在超时后才会从缓存中清除。如果会话缓存中没有空间，新连接可以建立但会话将不会被缓存。同时可以指定会话缓存的空间大小。

请在服务器端策略视图下进行下列配置，可选配。

表10-7 配置会话缓存保存时间和大小

操作	命令
配置会话缓存保存时间和大小	session { timeout <i>time</i> cachesize <i>size</i> }*
恢复默认的会话缓存保存时间和大小	undo session { timeout cachesize }*

time 为会话缓存的保存时间，单位为秒，范围为 1800~72000，默认时间为 3600 秒。

size 为会话缓存空间的大小，单位为个，范围为 1000~10000，默认缓存大小为 2000 个单元。

8. 显示服务器端 SSL 策略

请在任意视图下执行以下命令。

表10-8 显示服务器端策略

操作	命令
显示一个或全部服务器端策略	display ssl server-policy { <i>policy-name</i> all }

9. 打开/关闭 SSL 服务器的调试开关

请在用户视图下执行以下命令。

表10-9 打开/关闭 SSL 服务器的调试开关

操作	命令
打开 SSL 服务器的调试开关	debugging ssl server { all event packet error process misc }
关闭 SSL 服务器的调试开关	undo debugging ssl server { all event packet error process misc }

缺省情况下，关闭 SSL 服务器的调试开关。

10.2.2 配置 SSL 加密卡

1. 配置服务器端使用的加密卡

当 SSL 服务器使用软件进行加密/解密时，将占用大量的 CPU 资源，从而影响了设备的整体处理效率。可以使用 SSL 加密卡对数据进行硬件加密/解密，以硬件方式完成数据的加密/解密运算。这样，消除了通过软件处理加密/解密对整体性能的影响，同时也提高了 SSL 的处理效率。

请在服务器端策略视图下进行下列配置。

表10-10 配置服务器端使用的加密卡

操作	命令
配置所使用的加密卡	use ssl-card slot-id
取消使用加密卡	undo use ssl-card

缺省情况下，未配置使用加密卡。

2. 使能/关闭加密卡

请在加密卡接口视图下进行下列配置。

表10-11 使能/关闭加密卡

操作	命令
关闭加密卡	shutdown
使能加密卡	undo shutdown

3. 显示 SSL 加密卡信息

请在任意视图下执行以下命令。

表10-12 SSL 的显示与调试

操作	命令
显示 SSL 加密卡的统计信息	display interface ssl-card [<i>slot-id</i>]

4. 打开/关闭 SSL 加密卡的调试开关

请在用户视图下执行以下命令。

表10-13 打开/关闭 SSL 加密卡的调试开关

操作	命令
打开 SSL 加密卡的调试开关	debugging ssl card { <i>all</i> <i>event</i> <i>packet</i> <i>error</i> <i>process</i> <i>misc</i> }
关闭 SSL 加密卡的调试开关	undo debugging ssl card { <i>all</i> <i>event</i> <i>packet</i> <i>error</i> <i>process</i> <i>misc</i> }

缺省情况下，关闭 SSL 加密卡的调试开关。

10.2.3 配置基于证书属性访问控制的策略

1. 配置证书属性过滤组

SSL Proxy 可以利用客户端证书进行访问控制。在配置基于证书属性访问控制方案前，需要配置方案涉及的属性过滤组。

请在系统视图下执行该命令，配置证书属性过滤组，并且进入属性组视图。

表10-14 配置证书属性过滤组

操作	命令
配置证书属性过滤组	pki certificate attribute-group <i>group-name</i>
删除一个证书属性过滤组	undo pki certificate attribute-group { <i>group-name</i> <i>all</i> }

说明：

- 执行 **undo** 命令后，该属性过滤组中的所有属性过滤条件均会被删除。
- 可以配置多个证书属性过滤组，但组名不能相同。

2. 配置证书属性过滤条件

在配置了一个属性过滤组之后，可以利用以下命令配置属性过滤条件。

请在属性过滤组视图下执行该命令。

表10-15 配置证书属性过滤条件

操作	命令
配置证书主题名或者颁发者名称的 dn 过滤条件	attribute id { subject-name issuer-name } dn { ctn nctn } attribute-value
配置证书主题名、颁发者名称、主题扩展名的 fqdn 过滤条件	attribute id alt-subject-name fqdn { equ nequ ctn nctn } attribute-value
配置证书主题名、颁发者名称、主题扩展名的 ip 过滤条件	attribute id alt-subject-name ip { equ nequ } attribute-value
删除一个属性过滤条件	undo attribute { id all }

 说明：

- 由于 alt-subject-name 属性的值不会以 dn 的方式出现，所以在 alt-subject-name 属性的过滤条件的配置中没有出现 dn。
- 同一个组内可以配置多条属性过滤条件，但 id 不能相同。
- 同一个组内的属性过滤条件之间是“与”的关系，即必须匹配这个组内的所有属性过滤条件。

3. 配置证书属性访问控制策略

在配置了证书属性过滤组之后，可以利用该命令配置属性访问控制策略。

请在系统视图下执行该命令，并且进入控制策略视图。

表10-16 配置证书属性访问控制策略

操作	命令
配置证书属性访问控制策略	pki certificate access-control-policy policy-name
删除一个证书属性访问控制策略	undo pki certificate access-control-policy { policy-name all }

 说明：

- 可以配置多个证书属性访问控制策略，但是策略名不能相同。
- 删除证书属性访问控制策略时，策略中的所有访问控制规则均会被删除。

4. 配置证书属性访问控制规则

在配置了证书属性访问控制策略之后，可以利用该命令配置控制规则。

请在证书属性访问控制策略视图下执行该命令。

表10-17 配置证书属性访问控制规则

操作	命令
配置证书属性访问控制规则	rule [<i>id</i>] { permit deny } <i>group-name</i>
删除证书属性访问控制规则	undo rule { <i>id</i> all }

 说明：

- 可以配置多个证书属性访问控制规则，但是 *id* 不能相同。
- 配置一个 *rule* 时，*group-name* 必须预先使用 **pki certificate attribute-group** 命令配置完成。

5. 显示证书属性过滤组的信息

在配置了证书属性过滤组之后，可以利用该命令来查看过滤组的信息。

请在任意视图下执行该命令。

表10-18 显示证书属性过滤组

操作	命令
显示证书属性过滤组信息	display pki certificate attribute-group { <i>group-name</i> all }

6. 显示证书属性访问控制策略的信息

在配置了证书属性访问控制策略之后，可以利用该命令来查看策略信息。

请在任意视图下执行该命令。

表10-19 显示证书属性访问控制策略

操作	命令
显示证书属性访问控制策略的信息	display pki certificate access-control-policy { <i>policy-name</i> all }

7. 打开/关闭证书属性访问控制调试开关

在进行基于证书属性访问控制时，利用该命令来打开/关闭证书属性访问控制调试开关。

请在用户视图下执行该命令。

表10-20 打开/关闭证书属性访问控制调试开关

操作	命令
打开证书属性访问控制调试开关	debugging pki acp
关闭证书属性访问控制调试开关	undo debugging pki acp

缺省情况下，关闭证书属性访问控制调试开关。

10.2.4 配置 SSL Proxy 服务器策略

1. 创建 SSL Proxy 服务器策略

SSL Proxy 服务器策略指定了运行 SSL Proxy 服务器时使用的配置参数。需要使用 **ssl proxy** 命令创建一个 SSL Proxy 服务器端策略，并进入 SSL Proxy 策略视图。请在系统视图下进行下列配置，必需配置。

表10-21 创建 SSL Proxy 服务器策略

操作	命令
创建一个 SSL Proxy 服务器策略	ssl proxy ssl-proxy-name
删除一个或全部 SSL Proxy 服务器策略	undo ssl proxy { ssl-proxy-name all }

说明：

一个 SSL Proxy 服务器有可能根据不同需要使用不同的 SSL Proxy 服务器策略。对于 SSL Proxy 服务器策略应该能针对每一个策略有其单独的配置信息，所以采用 SSL Proxy 服务器策略视图进行参数的配置。

2. 指定 SSL Proxy 服务器策略使用的端口

SSL Proxy 服务器策略可以指定 SSL Proxy 服务器使用的端口。

请在 SSL Proxy 服务器策略视图下进行下列配置，可选配置。

表10-22 配置 SSL Proxy 服务器的端口

操作	命令
配置 SSL Proxy 服务器端口	port port-number
恢复 SSL Proxy 服务器默认端口	undo port

缺省情况下，指定的 SSL Proxy 服务器端口为 443。

3. 指定 SSL Proxy 服务器使用的 SSL 服务器端策略

SSL Proxy 服务器策略配置中必须指定 SSL Proxy 服务器使用的 SSL 服务器端策略。

请在 SSL Proxy 服务器策略视图下进行下列配置，必需配置。

表10-23 配置 SSL Proxy 服务器策略的 SSL 服务器端策略

操作	命令
指定 SSL Proxy 服务器策略中使用的 SSL 服务器端策略	ssl-server-policy <i>policy-name</i>
取消指定的 SSL 服务器端策略	undo ssl-server-policy

缺省情况下，未指定任何 SSL 服务器端策略。

4. 指定 SSL Proxy 服务器策略使用的证书访问控制策略

请在 SSL Proxy 服务器策略视图下进行下列配置，可选配。

表10-24 配置 SSL Proxy 服务器策略的证书访问控制策略

操作	命令
指定 SSL Proxy 服务器策略中使用的证书访问控制策略	certificate access-control-policy <i>policy-name</i>
删除 SSL Proxy 服务器策略中使用的证书访问控制策略	undo certificate access-control-policy

缺省情况下，未指定任何证书访问控制策略。

5. 配置目标服务器的 IP 地址和端口号

请在 SSL Proxy 服务器策略视图下进行下列配置。

表10-25 配置目标服务器的 IP 地址和端口号

操作	命令
配置目标服务器的 IP 地址和端口号	server ip <i>ip-address</i> port <i>port-number</i>
删除已配置的目标服务器	undo server ip <i>ip-address</i>

缺省情况下，未配置目标服务器的 IP 地址和端口号。

6. 显示 SSL Proxy 服务器策略

请在任意视图下执行以下命令。

表10-26 显示服务器端 HTTPS 策略

操作	命令
显示一个或全部 SSL Proxy 服务器策略	display ssl proxy { <i>ssl-proxy-name</i> all }

7. 显示 SSL Proxy 的会话信息

请在任意视图下执行以下命令。

表10-27 显示 SSL Proxy 的会话信息

操作	命令
显示 SSL Proxy 的会话信息	display ssl-proxy session [statistics]

8. 清空 SSL Proxy 服务器连接的统计信息

该配置任务用来清空 SSL Proxy 服务器连接的统计信息。

请在用户视图下进行操作。

表10-28 清空 SSL Proxy 服务器连接的统计信息

操作	命令
清空 SSL Proxy 连接的统计信息	reset ssl proxy statistic

9. 清除 SSL Proxy 的连接

请在用户视图下执行以下命令。

表10-29 清除 SSL Proxy 的连接

操作	命令
清除 SSL Proxy 的连接	reset ssl-proxy session

10. 打开/关闭 SSL Proxy 的调试开关

请在用户视图下执行以下命令。

表10-30 打开/关闭 SSL Proxy 的调试开关

操作	命令
打开 SSL Proxy 的调试开关	debugging ssl proxy { all event packet error process misc }
关闭 SSL Proxy 的调试开关	undo debugging ssl proxy { all event packet error process misc }

缺省情况下，关闭 SSL Proxy 的调试开关。

11. 启动 SSL Proxy 服务器命令

在完成对 SSL Proxy 服务器的策略配置后，通过该命令，启动 SSL Proxy 服务器。
请在系统视图下执行。

表10-31 启动 SSL Proxy 服务器

操作	命令
启动 SSL Proxy 服务器	ssl proxy server <i>ssl-proxy-name</i> enable

 说明：

必须在执行该命令之前完成 SSL Proxy 服务器策略的定义。

12. 关闭 SSL Proxy 服务器命令

在启动 SSL Proxy 服务器之后，通过该命令，可关闭该 SSL Proxy 服务器。
请在系统视图下执行。

表10-32 关闭 SSL Proxy 服务器

操作	命令
关闭 SSL Proxy 服务器	undo ssl proxy server <i>ssl-proxy-name</i> enable

 说明：

命令中的 SSL Proxy 服务器策略名必须与正在运行的 SSL Proxy 服务器策略一致。

10.2.5 配置举例：建立 SSL Proxy 服务器

1. 组网需求

HTTPS 客户端通过 Internet 连接到防火墙上的 SSL Proxy 服务，然后防火墙再将请求发送给 HTTP 服务器。

2. 组网图

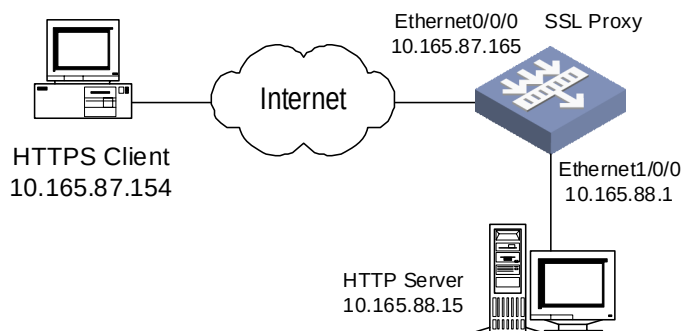


图10-3 SSL Proxy 服务器的组网图

3. 配置步骤

配置接口 IP 地址。

```
[H3C] interface Ethernet 0/0/0
[H3C-Ethernet0/0/0] ip address 10.165.87.165 255.255.255.0
[H3C-Ethernet0/0/0] quit
[H3C] interface Ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 10.165.88.1 255.255.255.0
[H3C-Ethernet1/0/0] quit
```

SSL 服务器端策略配置：

定制 SSL Proxy 服务器上使用的 SSL 服务器端策略。

```
[H3C] ssl server-policy myssl
```

PKI域配置，关于PKI的配置请参见 第 9 章 PKI配置。

```
[H3C-ssl-server-policy-myssl] pki-domain 1
```

证书属性过滤组的配置：

配置一个名为 mygroup1 和 mygroup2 的证书属性过滤组，并且在组下配置过滤条件。

```
[H3C] pki certificate attribute-group mygroup1
[H3C-cert-attribute-group-mygroup1] attribute 1 subject-name dn ctn cn=H3C
[H3C-cert-attribute-group-mygroup1] attribute 2 alt-subject-name ip equ
10.165.87.154
[H3C-cert-attribute-group-mygroup1] quit
[H3C] pki certificate attribute-group mygroup2
[H3C-cert-attribute-group-mygroup2] attribute 1 alt-subject-name fqdn nctn
H3C
[H3C-cert-attribute-group-mygroup2] attribute 2 issuer-name dn ctn H3C
```

证书 ACP 策略配置：

配置一个名为 myacp 的基于证书属性的访问控制策略，并且配置该策略的控制规则。

```
[H3C] pki certificate access-control-policy myacp
```

```
[H3C-cert-acp-myacp] rule 1 deny mygroup1
```

```
[H3C-cert-acp-myacp] rule 2 permit mygroup2
```

SSL Proxy 服务器策略配置：

定制 SSL Proxy 服务器策略。

```
[H3C] ssl proxy myproxy
```

配置 SSL 服务器端策略为 myssl。

```
[H3C-sslproxy-myproxy] ssl-server-policy myssl
```

配置证书 ACP 为 myacp。

```
[H3C-sslproxy-myproxy] certificate access-control-policy myacp
```

配置目标 HTTP 服务器。

```
[H3C-sslproxy-myproxy] server ip 10.165.88.15 port 80
```

运行 SSL Proxy 服务器：

选择 SSL Proxy 服务器配置 myproxy，启动 SSL Proxy 服务器。

```
[H3C] ssl proxy server myproxy enable
```

配置路由策略，使防火墙将进入的 HTTPS 请求交由 CPU 进行处理，否则防火墙将对进入的报文执行正常转发的操作，则不能起到 SSL Proxy 的作用：

配置 ACL，用来匹配将要进行 SSL 代理的数据流。

```
[H3C] acl number 3000
```

```
[H3C-acl-adv-3000] rule permit tcp source any destination 10.165.88.15 0  
destination-port eq 443
```

```
[H3C-acl-adv-3000] quit
```

配置路由策略，使防火墙将匹配 ACL 的报文转发到 loopback 接口上，即交由 CPU 处理。

```
[H3C] interface LoopBack 1
```

```
[H3C-LoopBack1] ip address 1.1.1.1 255.255.255.255
```

```
[H3C-LoopBack1] quit
```

```
[H3C] route-policy https permit node 1
```

```
[H3C-route-policy] if-match acl 3000
```

```
[H3C-route-policy] apply ip-address next-hop 1.1.1.1
```

```
[H3C-route-policy] quit
```

将路由策略应用到接口上。

```
[H3C] interface Ethernet 0/0/0
```

```
[H3C-Ethernet0/0/0] ip policy route-policy https
```

第11章 Web 和邮件过滤

11.1 Web 和邮件过滤简介

在传统的网络安全方案中，对网络攻击的防范主要针对来自外部的各种攻击。但是随着网络在各行各业的普及，来自一个局域网内部的攻击也越来越多，这就要求网络设备能够应对构建安全内网的需求，需要增加内网安全特性。

防火墙的 Web 和邮件过滤功能可以阻止内部用户访问非法的网址或访问含有非法内容的网页，防止内网用户向外网非法邮件地址发送邮件或向外发送与工作无关的邮件。当内部网络受到外部的攻击时，通过邮件告警功能，可以向网络管理员发送告警邮件，通知网络管理员采取相应措施。

SecPath 防火墙还提供了对来自外部的 SQL（Structure Query Language，结构化查询语言）注入攻击进行防范的功能。防火墙通过检查接收到的 HTTP 报文中的 HTTP 命令以判断其是否为对数据库的攻击，从而有效的保护网络中数据库的安全。

11.2 配置 Web 过滤

11.2.1 配置 Web 地址过滤

1. 使能/关闭 Web 地址过滤功能

在配置防火墙的 Web 地址过滤功能之前，首先要使能 Web 地址过滤功能，这样与其相关的配置才能生效。

请在系统视图下进行下列配置。

表11-1 使能 Web 地址过滤功能

操作	命令
使能 Web 地址过滤功能	firewall url-filter host enable
关闭 Web 地址过滤功能	undo firewall url-filter host enable

缺省情况下，关闭 Web 地址过滤功能。

**注意：**

- 开启Web地址过滤功能之前要先配置ASPF策略，**detect http**，**detect tcp**，才能使Web地址过滤功能生效。有关ASPF的内容请参见 5.3 ASPF配置。
- 对于监听非标准端口的 HTTP 协议，必须使用 **port-mapping** 命令正确的配置端口映射，这样 Web 地址过滤功能才能生效。

2. 配置默认过滤行为

可以对防火墙的默认过滤行为进行配置，使之允许或者拒绝未与管理员配置的网址发生匹配的数据报通过。

请在系统视图下进行下列配置。

表11-2 配置默认过滤行为

操作	命令
配置默认过滤行为	firewall url-filter host default { permit deny }

缺省情况下，允许未发生匹配的数据报通过。

3. 配置过滤地址

在过滤网址时，对哪些网址进行过滤是基于预先配置的网址文件中的地址条目。管理员可以对网址过滤文件进行管理，包括添加、删除和清除所有网址过滤地址。

请在系统视图下进行下列配置。

表11-3 配置过滤地址

操作	命令
添加过滤地址	firewall url-filter host add { permit deny } url-address
删除过滤地址	firewall url-filter host delete url-address
清除所有过滤地址	firewall url-filter host clear

**说明：**

若保存使用 **firewall url-filter host add** 命令添加的过滤地址，必须使用 **firewall url-filter host save-file** 命令将过滤地址保存到过滤文件中，否则当前添加的过滤地址在防火墙下次启动时将丢失。

4. 保存/加载 Web 地址过滤文件

在配置完过滤地址后，可以将其保存到网址过滤文件中。日后若要对其进行配置或修改，可以加载地址过滤文件。

请在系统视图下进行下列配置。

表11-4 保存/加载 Web 地址过滤文件

操作	命令
保存/加载 Web 地址过滤文件	firewall url-filter host { save-file load-file } file-name
取消对当前过滤文件的加载	undo firewall url-filter host load-file

如果要使 Web 地址过滤文件中的条目生效并对地址进行过滤，必须将其加载。

5. 配置 IP 地址过滤

当用户使用 IP 地址对 Web 进行访问时，可以配置防火墙是否允许此类请求通过。

请在系统视图下进行下列配置。

表11-5 配置 IP 地址过滤

操作	命令
配置 IP 地址过滤	firewall url-filter host ip-address { permit deny }

缺省情况下，防火墙将阻止目标 URL 为 IP 地址的 Web 请求通过。

6. 使用 ACL 对 IP 地址进行过滤

使用以下命令可以使用 ACL 对目标 URL 为 IP 地址的 Web 请求进行过滤。

请在系统视图下进行下列配置。

表11-6 使用 ACL 对 IP 地址进行过滤

操作	命令
使用 ACL 对 IP 地址进行过滤	firewall url-filter host acl-number number
取消配置的 ACL 规则	undo firewall url-filter host acl-number

缺省情况下，未配置任何 ACL 规则。

当防火墙接收到目标 URL 为 IP 地址的 Web 请求时，首先与 **firewall url-filter host acl-number** 命令中的 ACL 进行匹配。如果匹配结果为 **permit**，则允许该请求通过；如果匹配结果为 **deny**，则拒绝该请求；如果在 ACL 中未找到匹配条目或者没有配置 **firewall url-filter host acl-number** 命令，则防火墙根据 **firewall url-filter host ip-address { permit | deny }** 命令的配置结果来决定是否允许该请求通过。

使用此命令只能引用一个 ACL 规则，随后配置的规则将覆盖原先的配置。

7. Web 地址过滤功能的显示和调试

使用以下命令可以查看网址过滤信息和打开网址过滤的调试开关。

请在任意视图下执行 **display** 命令，在用户视图下执行 **debugging** 命令和 **reset** 命令。

表11-7 Web 地址过滤的显示与调试

操作	命令
显示网址过滤信息	display firewall url-filter host { enable all item url-address item-all }
打开网址过滤调试开关	debugging firewall url-filter host { all error event filter packet }
关闭网址过滤调试开关	undo debugging firewall url-filter host { all error event filter packet }
清除 Web 地址过滤的统计信息	reset firewall url-filter host counter

11.2.2 配置 Web 内容过滤

1. 使能/关闭 web 内容过滤功能

在配置防火墙的 Web 内容过滤功能之前，首先要使能 Web 内容过滤功能，这样与其相关的配置才能生效。

请在系统视图下进行下列配置。

表11-8 使能 Web 内容过滤功能

操作	命令
使能 Web 内容过滤功能	firewall webdata-filter enable
关闭 Web 内容过滤功能	undo firewall webdata-filter enable

缺省情况下，关闭 Web 内容过滤功能。



注意：

- 开启 Web 内容过滤功能之前要先配置 ASPF 策略，**detect http**，**detect tcp**，才能使 Web 内容过滤功能生效。有关 ASPF 的内容请参见 5.3 ASPF 配置。
- 对于监听非标准端口的 HTTP 协议，必须使用 **port-mapping** 命令正确的配置端口映射，这样 Web 内容过滤功能才能生效。
- 当网页中的某些内容被过滤后，可能会出现 Internet Explorer 浏览器频繁闪烁的现象。

2. 配置 Web 内容过滤关键字

在过滤网页时,对哪些网页进行过滤是基于预先配置的 Web 内容过滤文件中的关键字条目。管理员可以对内容过滤文件进行管理,包括添加、删除和清除所有内容过滤关键字。

请在系统视图下进行下列配置。

表11-9 配置内容过滤关键字

操作	命令
添加过滤关键字	firewall webdata-filter add keywords
删除过滤关键字	firewall webdata-filter delete keywords
清除所有过滤关键字	firewall webdata-filter clear

说明:

- 添加的 Web 内容过滤关键字不能为 HTML 语言的标记,例如<head>、<html>、<title>、<script>等等,否则合法的网页可能会被过滤掉。
- 若保存使用 **firewall webdata-filter add** 命令添加的关键字,必须使用 **firewall webdata-filter save-file** 命令将关键字保存到过滤文件中,否则当前添加的关键字在防火墙下次启动时将丢失。

3. 保存/加载 web 内容过滤文件

在配置完过滤关键字后,可以将其保存到 Web 内容过滤文件中。日后若要对其进行配置或修改,可以加载内容过滤文件。

请在系统视图下进行下列配置。

表11-10 保存/加载 Web 内容过滤文件

操作	命令
保存/加载 Web 内容过滤文件	firewall webdata-filter { save-file load-file } file-name
取消对当前过滤文件的加载	undo firewall webdata-filter load-file

如果要使 Web 内容过滤文件中的条目生效并对内容进行过滤,必须将其加载。

4. Web 内容过滤功能的显示和调试

使用以下命令可以查看 Web 内容过滤信息和打开内容过滤的调试开关。

请在所有视图下执行 **display** 命令,在用户视图下执行 **debugging** 命令和 **reset** 命令。

表11-11 Web 内容过滤的显示与调试

操作	命令
显示 Web 内容过滤信息	display firewall webdata-filter { enable all item keywords item-all }
打开 Web 内容过滤调试开关	debugging firewall webdata-filter { all error event filter packet }
关闭 Web 内容过滤调试开关	undo debugging firewall webdata-filter { all error event filter packet }
清除 Web 内容过滤的统计信息	reset firewall webdata-filter counter

11.2.3 配置 SQL 注入攻击防范

1. 使能/关闭 SQL 注入攻击防范功能

在配置防火墙的 SQL 注入攻击防范功能之前，首先要使能 SQL 注入攻击防范功能，这样与其相关的配置才能生效。

请在系统视图下进行下列配置。

表11-12 使能 SQL 注入攻击防范功能

操作	命令
使能 SQL 注入攻击防范功能	firewall url-filter parameter enable
关闭 SQL 注入攻击防范功能	undo firewall url-filter parameter enable

缺省情况下，关闭 SQL 注入攻击防范功能。



注意：

- 开启 SQL 注入攻击防范功能之前要先配置 ASPF 策略，detect http，detect tcp，才能使 SQL 注入攻击防范功能生效。有关 ASPF 的内容请参见 5.3 ASPF 配置。
- 对于监听非标准端口的 HTTP 协议，必须使用 port-mapping 命令正确的配置端口映射，这样 SQL 注入攻击防范功能才能生效。

2. 配置 SQL 注入攻击过滤关键字

在阻止 SQL 注入攻击时，对哪些 HTTP 命令进行过滤是基于预先配置的 SQL 注入攻击过滤文件中的关键字条目。若指定的关键字出现在 HTTP 命令中，防火墙将阻止此 HTTP 请求。管理员可以对过滤文件进行管理，包括添加、删除和清除所有过滤关键字。用户可以根据自己的需要，将一些表名、字段、以及一些系统的和自定义的存储过程名作为关键字。

请在系统视图下进行下列配置。

表11-13 配置过滤关键字

操作	命令
添加过滤关键字	firewall url-filter parameter add keywords
添加系统缺省的过滤关键字	firewall url-filter parameter add-default
删除过滤关键字	firewall url-filter parameter delete keywords
清除所有过滤关键字	firewall url-filter parameter clear

缺省情况下，系统预定义了以下关键字：**^select^**、**^insert^**、**^update^**、**^delete^**、**^drop^**、**--**、**'**、**^exec^**和**%27**。当执行 **firewall url-filter parameter add-default** 命令时，系统将自动添加以上这些缺省的关键字，方便了用户的输入，也防止用户无意中删除某些关键字，或者不恰当地使用 **firewall url-filter parameter clear** 命令时可以很快地恢复缺省配置。

说明：

若保存使用 **firewall url-filter parameter add** 和 **firewall url-filter parameter add-default** 命令添加的关键字，必须使用 **firewall url-filter parameter save-file** 命令将关键字保存到过滤文件中，否则当前添加的关键字在防火墙下次启动时将丢失。

3. 保存/加载 SQL 注入攻击过滤文件

配置完过滤关键字后，可以将其保存到 SQL 注入攻击过滤文件中。日后若要对其进行配置或修改，可以加载过滤文件。

请在系统视图下进行下列配置。

表11-14 保存/加载 SQL 注入攻击过滤文件

操作	命令
保存/加载 SQL 注入攻击过滤文件	firewall url-filter parameter { save-file load-file } file-name
取消对当前过滤文件的加载	undo firewall url-filter parameter load-file

如果要使 SQL 注入攻击过滤文件中的条目生效并对 HTTP 命令进行过滤，必须将其加载。

4. SQL 注入攻击防范功能的显示和调试

使用以下命令可以查看 SQL 注入攻击防范的过滤信息和打开 SQL 注入攻击防范的调试开关。

请在所有视图下执行 **display** 命令，在用户视图下执行 **debugging** 命令和 **reset** 命令。

表11-15 SQL 注入攻击防范的显示与调试

操作	命令
显示 SQL 注入攻击过滤信息	display firewall url-filter parameter { enable all item keywords item-all }
显示每个关键字匹配的次数	display firewall url-filter parameter counter detail
打开 SQL 注入攻击防范调试开关	debugging firewall url-filter parameter { all error event filter packet }
关闭 SQL 注入攻击防范调试开关	undo debugging firewall url-filter parameter { all error event filter packet }
清除 SQL 注入攻击防范的统计信息	reset firewall url-filter parameter counter

11.3 配置邮件过滤

11.3.1 配置邮件地址过滤

在企业内部向外发送邮件时，可能需要进行过滤，防止向外部非法地址发送公司资料或者与工作无关的信息。防火墙提供了对电子邮件地址进行过滤的功能。

1. 使能/关闭邮件地址过滤功能

在配置防火墙的邮件地址过滤功能之前，首先要使能邮件地址过滤功能，这样与其相关的配置才能生效。

请在系统视图下进行下列配置。

表11-16 使能邮件地址过滤功能

操作	命令
使能邮件地址过滤功能	firewall smtp-filter rcptto enable
关闭邮件地址过滤功能	undo firewall smtp-filter rcptto enable

缺省情况下，关闭邮件地址过滤功能。

**注意：**

- 开启邮件地址过滤功能之前要先配置ASPF策略，detect smtp，detect tcp，才能使邮件地址过滤功能生效。有关ASPF的内容请参见 5.3 ASPF配置。
- 对于监听非标准端口的 SMTP 协议，必须使用 port-mapping 命令正确的配置端口映射，这样邮件地址过滤功能才能生效。

2. 配置默认过滤行为

可以对防火墙的默认过滤行为进行配置，使之允许或者拒绝未与管理员配置的邮件地址发生匹配的数据报通过。

请在系统视图下进行下列配置。

表11-17 配置默认过滤行为

操作	命令
配置默认过滤行为	firewall smtp-filter rcptto default { permit deny }
恢复到缺省的过滤行为	undo firewall smtp-filter rcptto default

缺省情况下，允许未发生匹配的数据报通过。

3. 配置邮件过滤地址

在过滤邮件时，对哪些地址进行过滤是基于预先配置的邮件地址过滤文件中的地址条目。管理员可以对地址过滤文件进行管理，包括添加、删除和清除所有邮件过滤地址。

请在系统视图下进行下列配置。

表11-18 配置过滤地址

操作	命令
添加过滤地址	firewall smtp-filter rcptto add { permit deny } mail-address
删除过滤地址	firewall smtp-filter rcptto delete mail-address
清除所有过滤地址	firewall smtp-filter rcptto clear

**说明：**

若保存使用 **firewall smtp-filter rcptto add** 命令添加的过滤地址，必须使用 **firewall smtp-filter rcptto save-file** 命令将过滤地址保存到过滤文件中，否则当前添加的过滤地址在防火墙下次启动时将丢失。

4. 保存/加载邮件地址过滤文件

在配置完过滤地址后，可以将其保存到邮件地址过滤文件中。日后若要对其进行配置或修改，可以加载地址过滤文件。

请在系统视图下进行下列配置。

表11-19 保存/加载邮件地址过滤文件

操作	命令
保存/加载邮件地址过滤文件	firewall smtp-filter rcptto { save-file load-file } file-name
取消对当前过滤文件的加载	undo firewall smtp-filter rcptto load-file

如果要使邮件地址过滤文件中的条目生效并对地址进行过滤，必须将其加载。

11.3.2 配置邮件主题过滤

在企业内部向外发送邮件时，可以根据邮件主题对邮件进行过滤。

1. 使能/关闭邮件主题过滤功能

在配置防火墙的邮件主题过滤功能之前，首先要使能邮件主题过滤功能，这样与其相关的配置才能生效。

请在系统视图下进行下列配置。

表11-20 使能邮件主题过滤功能

操作	命令
使能邮件主题过滤功能	firewall smtp-filter subject enable
关闭邮件主题过滤功能	undo firewall smtp-filter subject enable

缺省情况下，关闭邮件主题过滤功能。



注意：

- 开启邮件主题过滤功能之前要先配置ASPF策略，**detect smtp**，**detect tcp**，才能使邮件主题过滤功能生效。有关ASPF的内容请参见 5.3 ASPF配置。
- 对于监听非标准端口的 SMTP 协议，必须使用 **port-mapping** 命令正确的配置端口映射，这样邮件主题过滤功能才能生效。

2. 配置主题过滤关键字

在过滤邮件时，对哪些主题进行过滤是基于预先配置的邮件主题过滤文件中的关键字条目。管理员可以对主题过滤文件进行管理，包括添加、删除和清除所有主题过滤关键字。

请在系统视图下进行下列配置。

表11-21 配置主题过滤关键字

操作	命令
添加过滤关键字	firewall smtp-filter subject add <i>mail-subject</i>
删除过滤关键字	firewall smtp-filter subject delete <i>mail-subject</i>
清除所有过滤关键字	firewall smtp-filter subject clear

说明：

若保存使用 **firewall smtp-filter subject add** 命令添加的关键字，必须使用 **firewall smtp-filter subject save-file** 命令将关键字保存到过滤文件中，否则当前添加的关键字在防火墙下次启动时将丢失。

3. 保存/加载邮件主题过滤文件

在配置完过滤关键字后，可以将其保存到邮件主题过滤文件中。日后若要对其进行配置或修改，可以加载主题过滤文件。

请在系统视图下进行下列配置。

表11-22 保存/加载邮件主题过滤文件

操作	命令
保存/加载邮件主题过滤文件	firewall smtp-filter subject { save-file load-file } <i>file-name</i>
取消对当前过滤文件的加载	undo firewall smtp-filter subject load-file

如果要使邮件主题过滤文件中的条目生效并对主题进行过滤，必须将其加载。

11.3.3 配置邮件内容过滤

在过滤邮件时，可以对邮件中的正文文本信息进行过滤。从而保证内部信息不会轻易的传输到外部网络。

1. 使能/关闭邮件内容过滤功能

在配置防火墙的邮件内容过滤功能之前，首先要使能邮件内容过滤功能，这样与其相关的配置才能生效。

请在系统视图下进行下列配置。

表11-23 使能邮件内容过滤功能

操作	命令
使能邮件内容过滤功能	firewall smtp-filter content enable
关闭邮件内容过滤功能	undo firewall smtp-filter content enable



注意：

- 开启邮件内容过滤功能之前要先配置ASPF策略，**detect smtp**，**detect tcp**，才能使邮件主题过滤功能生效。有关ASPF的内容请参见 5.3 ASPF配置。
- 对于监听非标准端口的 SMTP 协议，必须使用 **port-mapping** 命令正确的配置端口映射，这样邮件内容过滤功能才能生效。

缺省情况下，关闭邮件内容过滤功能。

2. 配置内容过滤关键字

在过滤邮件时，对哪些内容进行过滤是基于预先配置的邮件内容过滤文件中的关键字条目。管理员可以对内容过滤文件进行管理，包括添加、删除和清除所有内容过滤关键字。

请在系统视图下进行下列配置。

表11-24 配置内容过滤关键字

操作	命令
添加过滤关键字	firewall smtp-filter content add <i>content-keywords</i>
删除过滤关键字	firewall smtp-filter content delete <i>content-keywords</i>
清除所有过滤关键字	firewall smtp-filter content clear

说明：

若要保存使用 **firewall smtp-filter content add** 命令添加的关键字，必须使用 **firewall smtp-filter content save-file** 命令将关键字保存到过滤文件中，否则当前添加的关键字在防火墙下次启动时将丢失。

3. 保存/加载邮件内容过滤文件

在配置完过滤关键字后，可以将其保存到邮件内容过滤文件中。日后若要对其进行配置或修改，可以加载内容过滤文件。

请在系统视图下进行下列配置。

表11-25 保存/加载邮件内容过滤文件

操作	命令
保存/加载邮件内容过滤文件	firewall smtp-filter content { save-file load-file } file-name
取消对当前过滤文件的加载	undo firewall smtp-filter content load-file

如果要使邮件内容过滤文件中的条目生效并对内容进行过滤，必须将其加载。

11.3.4 配置邮件附件过滤

在企业内部向外发送邮件时，可以根据邮件附件名对邮件进行过滤。

1. 使能/关闭邮件附件过滤功能

在配置防火墙的邮件附件过滤功能之前，首先要使能邮件附件过滤功能，这样与其相关的配置才能生效。

请在系统视图下进行下列配置。

表11-26 使能邮件附件过滤功能

操作	命令
使能邮件附件过滤功能	firewall smtp-filter attach enable
关闭邮件附件过滤功能	undo firewall smtp-filter attach enable



注意：

- 开启邮件附件过滤功能之前要先配置ASPF策略，**detect smtp**，**detect tcp**，才能使邮件附件过滤功能生效。有关ASPF的内容请参见 5.3 ASPF配置。
- 对于监听非标准端口的 SMTP 协议，必须使用 **port-mapping** 命令正确的配置端口映射，这样邮件附件过滤功能才能生效。

缺省情况下，关闭邮件附件过滤功能。

2. 配置过滤附件名

在过滤附件时，对哪些附件进行过滤是基于预先配置的邮件附件过滤文件中的附件名条目。管理员可以对附件过滤文件进行管理，包括添加、删除和清除所有过滤附件名。

请在系统视图下进行下列配置。

表11-27 配置过滤附件名

操作	命令
添加过滤附件名	firewall smtp-filter attach add <i>file-name</i>
删除过滤附件名	firewall smtp -filter attach delete <i>file-name</i>
清除所有过滤附件名	firewall smtp -filter attach clear

说明：

若保存使用 **firewall smtp-filter attach add** 命令添加的过滤附件名，必须使用 **firewall smtp-filter attach save-file** 命令将过滤附件名保存到过滤文件中，否则当前添加的过滤附件名在防火墙下次启动时将丢失。

3. 保存/加载邮件附件过滤文件

在配置完过滤附件名后，可以将其保存到邮件附件过滤文件中。日后若要对其进行配置或修改，可以加载附件过滤文件。

请在系统视图下进行下列配置。

表11-28 保存/加载邮件附件过滤文件

操作	命令
保存/加载邮件附件过滤文件	firewall smtp-filter attach { save-file load-file } <i>file-name</i>
取消对当前过滤文件的加载	undo firewall smtp-filter attach load-file

如果要使邮件附件过滤文件中的条目生效并对附件进行过滤，必须将其加载。

11.3.5 邮件过滤功能的显示和调试

使用以下命令可以查看邮件过滤信息和打开邮件过滤的调试开关。

请在所有视图下执行 **display** 命令，在用户视图下执行 **debugging** 命令和 **reset** 命令。

表11-29 邮件过滤的显示与调试

操作	命令
显示邮件过滤信息	display firewall smtp-filter { all { rcptto subject content attach } { item <i>string</i> item-all } }
打开邮件过滤调试开关	debugging firewall smtp-filter
关闭邮件过滤调试开关	undo debugging firewall smtp-filter
清除邮件过滤的统计信息	reset firewall smtp-filter [rcptto subject content attach] counter

第12章 攻击防范与报文统计

12.1 攻击防范与报文统计简介

12.1.1 攻击防范简介

通常的网络攻击，一般是侵入或破坏网络上的服务器（主机），盗取服务器的敏感数据或干扰、破坏服务器对外提供的服务；也有直接破坏网络设备的网络攻击，这种破坏影响较大，会导致网络服务异常，甚至中断。防火墙的攻击防范功能能够检测出多种类型的网络攻击，并能采取相应的措施保护内部网络免受恶意攻击，保证内部网络及系统的正常运行。

12.1.2 网络攻击的种类

网络攻击可分为拒绝服务型攻击、扫描窥探攻击和畸形报文攻击三大类：

1. 拒绝服务型攻击

拒绝服务型（DoS, Denial of Service）攻击是使用大量的数据包攻击系统，使系统无法接受正常用户的请求，或者主机挂起不能提供正常的工作。主要的 DoS 攻击有 SYN Flood、Fraggle 等。拒绝服务攻击和其他类型的攻击不同之处在于：攻击者并不是去寻找进入内部网络的入口，而是阻止合法用户访问网络资源。

2. 扫描窥探攻击

扫描窥探攻击是利用 ping 扫描（包括 ICMP 和 TCP）来标识网络上存活着的系统，从而准确的指出潜在的目标。利用 TCP 和 UDP 端口扫描，就能检测出操作系统和监听着的潜在服务。攻击者通过扫描窥探就能大致了解目标系统提供的服务种类和潜在的安全漏洞，为进一步侵入系统做好准备。

3. 畸形报文攻击

畸形报文攻击是通过向目标系统发送有缺陷的 IP 报文，使得目标系统在处理这样的 IP 报文时会崩溃，给目标系统带来损失。主要的畸形报文攻击有 Ping of Death、Teardrop 等。

12.1.3 典型的网络攻击

1. IP 地址欺骗（IP Spoofing）攻击

为了获得访问权，入侵者生成一个带有伪造源地址的报文。对于使用基于 IP 地址验证的应用来说，此攻击方法可以导致未被授权的用户可以访问目的系统，甚至是以 root 权限来访问。

2. Land 攻击

所谓 Land 攻击，就是把 TCP SYN 包的源地址和目标地址都配置成受害者的 IP 地址。这将导致受害者向它自己的地址发送 SYN-ACK 消息，结果这个地址又返回 ACK 消息并创建一个空连接，每一个这样的连接都将保留直到超时掉。各种受害者对 Land 攻击反应不同，许多 UNIX 主机将崩溃，Windows NT 主机会变的极其缓慢。

3. Smurf 攻击

简单的 Smurf 攻击，用来攻击一个网络。方法是发 ICMP 应答请求，该请求包的目标地址配置为受害网络的广播地址，这样该网络的所有主机都对此 ICMP 应答请求作出答复，导致网络阻塞。

高级的 Smurf 攻击主要用来攻击目标主机。方法是将上述 ICMP 应答请求包的源地址改为受害主机的地址，最终导致受害主机接收到大量的 ICMP 应答消息而崩溃。攻击报文的发送需要一定的流量和持续时间，才能真正构成攻击。理论上讲，网络的主机越多，攻击的效果越明显。Smurf 攻击的另一个变体为 Fraggle 攻击。

4. WinNuke 攻击

WinNuke 攻击通常向装有 Windows 系统的特定目标的 NetBIOS 端口（139）发送 OOB（out-of-band）数据包，引起一个 NetBIOS 片断重叠，致使目标主机崩溃。还有一种是 IGMP 分片报文，一般情况下，IGMP 报文是不会分片的，所以，不少系统对 IGMP 分片报文的处理有问题。如果收到 IGMP 分片报文，则基本可判定受到了攻击。

5. SYN Flood 攻击

由于资源的限制，TCP/IP 栈只能允许有限个 TCP 连接。而 SYN Flood 攻击正是利用这一点，它伪造一个 SYN 报文，其源地址是伪造的或者是一个不存在的地址，向服务器发起连接，服务器在收到报文后用 SYN-ACK 应答，而此应答发出去后，不会收到 ACK 报文，造成一个半连接。如果攻击者发送大量这样的报文，会在被攻击主机上出现大量的半连接，消耗尽其资源，使正常的用户无法访问。直到半连接超时。在一些创建连接不受限制的实现里，SYN Flood 具有类似的影响，它会消耗掉系统的内存等资源。

6. ICMP 和 UDP Flood 攻击

这种攻击短时间内用大量的 ICMP 消息（如 ping）和 UDP 报文向特定目标不断请求回应，致使目标系统负担过重而不能处理合法的传输任务。

7. 地址扫描与端口扫描攻击

运用扫描工具探测目标地址和端口，对此作出响应的表示其存在，用来确定哪些目标系统确实存活并且连接在目标网络上，这些主机使用哪些端口提供服务，为后续的攻击做准备。

8. Ping of Death 攻击

所谓 Ping of Death，就是利用一些尺寸超大的 ICMP 报文对系统进行的一种攻击。IP 报文的长度字段为 16 位，这表明一个 IP 报文的最大长度为 65535。对于 ICMP 回应请求报文，如果数据长度大于 65507，就会使 ICMP 数据+IP 头长度(20)+ICMP 头长度(8) > 65535。对于有些路由器或系统，在接收到一个这样的报文后，由于处理不当，会造成系统崩溃、死机或重启。

12.1.4 报文统计分析功能简介

对于防火墙来说，不仅要监控数据流量，还要对内外部网络之间的连接发起情况进行检测，因此要进行大量的统计计算与分析。防火墙的统计分析一方面可以通过专门的分析软件对日志信息进行事后分析；另一方面，防火墙系统本身可以完成一部分分析功能，它表现在具有一定的实时性。比如，通过分析外部网络向内部网络发起的 TCP 或 UDP 连接总数是否超过设定的阈值，可以确定是否需要限制该方向的新连接发起，或者限制向内部网络某一 IP 地址发起新连接。

下图是防火墙的一个典型应用，当启动了外部网络到 DMZ 区域的基于 IP 地址的统计分析功能时，如果外部网络对服务器发起的 TCP 连接数超过了设定的阈值，防火墙将限制外部网络向该服务器发起新连接，直到连接数降到正常的范围。

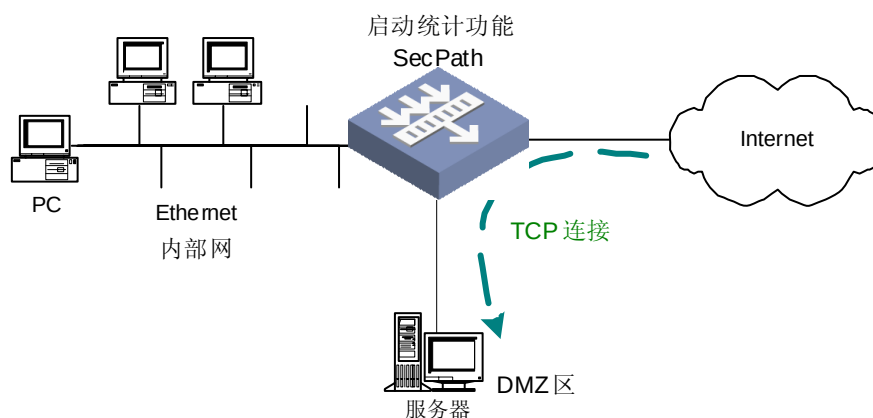


图12-1 防火墙拒绝外部网络向服务器发起过多的连接

12.2 攻击防范配置

攻击防范的配置包括：

- 使能 ARP Flood 攻击防范功能
- 使能 ARP 欺骗攻击防范功能
- 使能 IP 欺骗攻击防范功能
- 使能 Land 攻击防范功能
- 使能 Smurf 攻击防范功能
- 使能 WinNuke 攻击防范功能
- 使能 Fraggle 攻击防范功能
- 使能 Frag Flood 攻击防范功能
- 使能 SYN Flood 攻击防范功能
- 使能 ICMP Flood 攻击防范功能
- 使能 UDP Flood 攻击防范功能
- 使能 ICMP 重定向报文控制功能
- 使能 ICMP 不可达报文控制功能
- 使能地址扫描攻击防范功能
- 使能端口扫描攻击防范功能
- 使能带源路由选项 IP 报文控制功能
- 使能带路由记录选项 IP 报文控制功能
- 使能 Tracert 报文控制功能
- 使能 Ping of Death 攻击防范功能
- 使能 Teardrop 攻击防范功能
- 使能 TCP 报文合法性检测功能
- 使能 IP 分片报文检测功能
- 使能超大 ICMP 报文控制功能

12.2.1 使能/关闭 ARP Flood 攻击防范功能

请在系统视图下进行下列配置。

表12-1 使能/关闭 ARP Flood 攻击防范功能

操作	命令
使能 ARP Flood 攻击防范功能	firewall defend arp-flood [max-rate rate-number]
关闭 ARP Flood 攻击防范功能	undo firewall defend arp-flood [max-rate]

缺省为关闭 ARP Flood 攻击防范功能。ARP 报文的最大连接速率范围为 1～1,000,000，缺省为 100。

12.2.2 配置 ARP 欺骗攻击防范功能

请在系统视图下进行下列配置。

表12-2 配置 ARP 欺骗攻击防范功能

操作	命令
使能 ARP 欺骗攻击防范功能, 并使用非宽松检测	firewall defend arp-spoofing
关闭 ARP 欺骗攻击防范功能	undo firewall defend arp-spoofing
使能 ARP 欺骗攻击防范功能, 并使用宽松检测	firewall defend arp-spoofing loose
取消宽松检测, 使用非宽松检测模式	undo firewall defend arp-spoofing loose

缺省为关闭 ARP 欺骗攻击防范功能。

ARP 欺骗攻击防范有两种模式，一种为宽松检测模式，一种为非宽松检测模式。当使用非宽松检测（即不配置 **loose** 选项）时，防火墙会将目的 MAC 地址为单播地址的 ARP 请求视为攻击报文，并将其丢弃。若使用宽松检测（即配置 **loose** 选项），目的 MAC 地址为单播地址的 ARP 请求不被视为攻击报文，且不进行丢弃。

12.2.3 使能/关闭 IP 欺骗攻击防范功能

请在系统视图下进行下列配置。

表12-3 使能/关闭 IP 欺骗攻击防范功能

操作	命令
使能 IP 欺骗攻击防范功能	firewall defend ip-spoofing
关闭 IP 欺骗攻击防范功能	undo firewall defend ip-spoofing

缺省为关闭 IP 欺骗攻击防范功能。

 说明：

IP 欺骗攻击防范功能不能在透明模式下应用。

12.2.4 使能/关闭 Land 攻击防范功能

请在系统视图下进行下列配置。

表12-4 使能/关闭 Land 攻击防范功能

操作	命令
使能 Land 攻击防范功能	firewall defend land
关闭 Land 攻击防范功能	undo firewall defend land

缺省为关闭 Land 攻击防范功能。

12.2.5 使能/关闭 Smurf 攻击防范功能

请在系统视图下进行下列配置。

表12-5 使能/关闭 Smurf 攻击防范功能

操作	命令
使能 Smurf 攻击防范功能	firewall defend smurf
关闭 Smurf 攻击防范功能	undo firewall defend smurf

缺省为关闭 Smurf 攻击防范功能。

12.2.6 使能/关闭 WinNuke 攻击防范功能

请在系统视图下进行下列配置。

表12-6 使能/关闭 WinNuke 攻击防范功能

操作	命令
使能 WinNuke 攻击防范功能	firewall defend winnuke
关闭 WinNuke 攻击防范功能	undo firewall defend winnuke

缺省为关闭 WinNuke 攻击防范功能。

12.2.7 使能/关闭 Fraggle 攻击防范功能

请在系统视图下进行下列配置。

表12-7 使能/关闭 Fraggle 攻击防范功能

操作	命令
使能 Fraggle 攻击防范功能	firewall defend fraggle
关闭 Fraggle 攻击防范功能	undo firewall defend fraggle

缺省为关闭 Fraggle 攻击防范功能。

12.2.8 使能/关闭 Frag Flood 攻击防范功能

请在系统视图下进行下列配置。

表12-8 使能/关闭 Frag Flood 攻击防范功能

操作	命令
使能 Frag Flood 攻击防范功能	firewall defend frag-flood [max-identical-rate max-identical-rate] [max-total-rate max-total-rate]
关闭 Frag Flood 攻击防范功能	undo firewall defend frag-flood [max-identical-rate] [max-total-rate]

缺省为关闭 Frag Flood 攻击防范功能。最大相同分片报文速率 *max-identical-rate* 范围为 1~10,000, 缺省为 50。最大分片报文速率 *max-total-rate* 范围为 1~10,000, 缺省为 100。

说明：

对于目的地为防火墙自身的分片报文攻击，防火墙只告警，但不丢弃报文。否则，防火墙将告警，并丢弃报文。

12.2.9 使能/关闭 SYN Flood 攻击防范功能

SYN Flood 攻击防范功能可对安全域和 IP 地址分别进行配置，使能该功能需要首先打开 SYN Flood 攻击防范功能全局开关和使能受保护域（或受保护 IP 所在域）入方向的 IP 统计功能为前提。

1. 使能/关闭 SYN Flood 攻击防范功能

请在系统视图下进行下列配置。

表12-9 使能/关闭 SYN Flood 攻击防范功能

操作	命令
打开 SYN Flood 攻击防范功能全局开关	firewall defend syn-flood enable
关闭 SYN Flood 攻击防范功能全局开关	undo firewall defend syn-flood enable

缺省为关闭 SYN Flood 攻击防范功能全局开关。

2. 配置 SYN Flood 攻击防范功能

请在系统视图下进行下列配置。

表12-10 配置 SYN Flood 攻击防范功能

操作	命令
使能对 IP 的 SYN Flood 攻击防范功能	firewall defend syn-flood ip <i>ip-address</i> [max-rate <i>rate-number</i>] [tcp-proxy]
使能对域内所有 IP 的 SYN Flood 攻击防范功能	firewall defend syn-flood zone <i>zone-name</i> [max-rate <i>rate-number</i>] [tcp-proxy]
关闭对某 IP 的 SYN Flood 攻击防范功能	undo firewall defend syn-flood ip <i>ip-address</i> [max-rate] [tcp-proxy]
关闭对所有 IP 的 SYN Flood 攻击防范功能	undo firewall defend syn-flood ip
关闭对某域内所有 IP 的 SYN Flood 攻击防范功能	undo firewall defend syn-flood zone <i>zone-name</i> [max-rate] [tcp-proxy]
关闭对所有域内 IP 的 SYN Flood 攻击防范功能	undo firewall defend syn-flood zone
关闭所有的 SYN Flood 攻击防范功能	undo firewall defend syn-flood

缺省为关闭 SYN Flood 攻击防范功能。SYN 包最大连接速率（**max-rate**）取值范围为 1~1,000,000，缺省值为 1000；当启用 TCP 代理时，则当检测到受保护主机或安全区域受到 SYN Flood 攻击时，TCP 代理自动启动，当不再受到攻击时，TCP 代理自动关闭。

说明：

- SYN Flood 的 IP 配置的优先级比域配置的优先级高。如果对特定 IP 配置开启 SYN Flood 攻击防范功能，同时也对该 IP 所在的域内的所有 IP 配置开启了防范功能，则该 IP 的各检测参数以 IP 配置为准；若此时取消 IP 配置，则该 IP 的各检测参数以域配置为准。
- SecPath 防火墙的 Flood 攻击防范功能（即 SYN Flood、ICMP Flood 和 UDP Flood 的总和）最多支持同时配置对 1000 个 IP 进行保护。
- 若要对 SYN Flood 攻击进行防范，则必须配置 TCP 代理。



注意：

真正开启 SYN Flood 攻击防范功能必须满足三点：

- 使能受保护域（或受保护 IP 所在域）入方向的 IP 统计功能。
- 打开 SYN Flood 攻击防范功能全局开关。
- 配置具体的 SYN Flood 攻击防范功能。
- 对于目标为防火墙自身的攻击，需对 Local 域进行配置。

3. 配置 TCP 代理

TCP 代理(TCP-Proxy)对目的主机或目的区域的所有主机提供保护,用来防范 SYN Flood 的攻击。当外部主机与启用了 TCP 代理保护的某个主机或某个安全域中的主机建立 TCP 连接时,必须先与防火墙完成 TCP 三次握手后,才能与目的主机建立 TCP 连接。如果不能与防火墙完成三次握手,则不允许与目的主机建立 TCP 连接,有效的防止了内部主机受到恶意攻击。

表12-11 配置 TCP 代理

操作	命令
配置为特定 IP 或安全区域启用 TCP 代理	firewall tcp-proxy { ip ip-address zone zone-name }
配置为特定 IP 或安全区域关闭 TCP 代理	undo firewall tcp-proxy { ip ip-address zone zone-name }

缺省情况下,未对任何 IP 地址或安全区域启用 TCP 代理。

说明:

如果在配置 SYN Flood 攻击时也启用了 TCP 代理,则在此处的配置优先于 SYN Flood 攻击中的配置,即无论是否受到 SYN Flood 攻击,都启用 TCP 代理,对目的主机或目的安全区域进行保护。

12.2.10 使能/关闭 ICMP Flood 攻击防范功能

ICMP Flood 攻击防范功能可对安全域和 IP 分别进行配置,使能该功能须以打开 ICMP Flood 攻击防范功能全局开关和使能受保护域(或受保护 IP 所在域)入方向的 IP 统计功能为前提。

1. 使能/关闭 ICMP Flood 攻击防范功能

请在系统视图下进行下列配置。

表12-12 使能/关闭 ICMP Flood 攻击防范功能

操作	命令
打开 ICMP Flood 攻击防范功能全局开关	firewall defend icmp-flood enable
关闭 ICMP Flood 攻击防范功能全局开关	undo firewall defend icmp-flood enable

缺省为关闭 ICMP Flood 攻击防范功能全局开关。

2. 配置 ICMP Flood 攻击防范功能

请在系统视图下进行下列配置。

表12-13 配置 ICMP Flood 攻击防范功能

操作	命令
使能对 IP 的 ICMP Flood 攻击防范功能	firewall defend icmp-flood ip <i>ip-address</i> [max-rate <i>rate-number</i>]
使能对域内所有 IP 的 ICMP Flood 攻击防范功能	firewall defend icmp-flood zone <i>zone-name</i> [max-rate <i>rate-number</i>]
关闭对某 IP 的 ICMP Flood 攻击防范功能	undo firewall defend icmp-flood ip <i>ip-address</i> [max-rate]
关闭对所有 IP 的 ICMP Flood 攻击防范功能	undo firewall defend icmp-flood ip
关闭对某域内所有 IP 的 ICMP Flood 攻击防范功能	undo firewall defend icmp-flood zone <i>zone-name</i> [max-rate]
关闭对所有域内 IP 的 ICMP Flood 攻击防范功能	undo firewall defend icmp-flood zone
关闭所有的 ICMP Flood 攻击防范功能	undo firewall defend icmp-flood

缺省为关闭 ICMP Flood 攻击防范功能。ICMP 包最大连接速率（**max-rate**）取值范围为 1~1,000,000，缺省值为 1000。

说明：

- ICMP Flood 的 IP 配置的优先级比域配置的优先级高。如果对特定 IP 配置开启 ICMP Flood 攻击防范功能，同时也对该 IP 所在的域内的所有 IP 配置开启了防范功能，则该 IP 的各检测参数以 IP 配置为准；若此时取消 IP 配置，则该 IP 的各检测参数以域配置为准。
- SecPath 防火墙的 Flood 攻击防范功能（即 SYN Flood、ICMP Flood 和 UDP Flood 的总和）最多支持同时配置对 1000 个 IP 进行保护。



注意：

真正开启 ICMP Flood 攻击防范功能必须满足三点：

- 使能受保护域（或受保护 IP 所在域）入方向的 IP 统计功能。
- 打开 ICMP Flood 攻击防范功能全局开关。
- 配置具体的 ICMP Flood 攻击防范功能。
- 对于目标为防火墙自身的攻击，需对 Local 域进行配置。

12.2.11 使能/关闭 UDP Flood 攻击防范功能

UDP Flood 攻击防范功能可对安全域和 IP 分别进行配置，使能该功能须以打开 UDP Flood 攻击防范功能全局开关和使能受保护域（或受保护 IP 所在域）入方向的 IP 统计功能为前提。

1. 使能/关闭 UDP Flood 攻击防范功能

请在系统视图下进行下列配置。

表12-14 使能/关闭 UDP Flood 攻击防范功能

操作	命令
打开 UDP Flood 攻击防范功能全局开关	firewall defend udp-flood enable
关闭 UDP Flood 攻击防范功能全局开关	undo firewall defend udp-flood enable

缺省为关闭 UDP Flood 攻击防范功能全局开关。

2. 配置 UDP Flood 攻击防范功能

请在系统视图下进行下列配置。

表12-15 配置 UDP Flood 攻击防范功能

操作	命令
使能对 IP 的 UDP Flood 攻击防范功能	firewall defend udp-flood ip <i>ip-address</i> [max-rate <i>rate-number</i>]
使能对域内所有 IP 的 UDP Flood 攻击防范功能	firewall defend udp-flood zone <i>zone-name</i> [max-rate <i>rate-number</i>]
关闭对某 IP 的 UDP Flood 攻击防范功能	undo firewall defend udp-flood ip <i>ip-address</i> [max-rate]
关闭对所有 IP 的 UDP Flood 攻击防范功能	undo firewall defend udp-flood ip
关闭对某域内所有 IP 的 UDP Flood 攻击防范功能	undo firewall defend udp-flood zone <i>zone-name</i> [max-rate]
关闭对所有域内 IP 的 UDP Flood 攻击防范功能	undo firewall defend udp-flood zone
关闭所有的 UDP Flood 攻击防范功能	undo firewall defend udp-flood

缺省为关闭 UDP Flood 攻击防范功能。UDP 包最大连接速率（**max-rate**）取值范围为 1~1,000,000，缺省值为 1000。

说明：

- UDP Flood 的 IP 配置的优先级比域配置的优先级高。如果对特定 IP 配置开启 UDP Flood 攻击防范功能，同时也对该 IP 所在的域内的所有 IP 配置开启了防范功能，则该 IP 的各检测参数以 IP 配置为准；若此时取消 IP 配置，则该 IP 的各检测参数以域配置为准。
- SecPath 防火墙的 Flood 攻击防范功能（即 SYN Flood、ICMP Flood 和 UDP Flood 的总和）最多支持同时配置对 1000 个 IP 进行保护。

**注意：**

真正开启 UDP Flood 攻击防范功能必须满足三点：

- 使能受保护域（或受保护 IP 所在域）入方向的 IP 统计功能。
- 打开 UDP Flood 攻击防范功能全局开关。
- 配置具体的 UDP Flood 攻击防范功能。
- 对于目标为防火墙自身的攻击，需对 Local 域进行配置。

12.2.12 使能/关闭 ICMP 重定向报文控制功能

请在系统视图下进行下列配置。

表12-16 使能/关闭 ICMP 重定向报文控制功能

操作	命令
使能 ICMP 重定向报文控制功能	firewall defend icmp-redirect
关闭 ICMP 重定向报文控制功能	undo firewall defend icmp-redirect

缺省为关闭 ICMP 重定向报文控制功能。

12.2.13 使能/关闭 ICMP 不可达报文控制功能

请在系统视图下进行下列配置。

表12-17 使能/关闭 ICMP 不可达报文控制功能

操作	命令
使能 ICMP 不可达报文控制功能	firewall defend icmp-unreachable
关闭 ICMP 不可达报文控制功能	undo firewall defend icmp-unreachable

缺省为关闭 ICMP 重定向报文控制功能。

12.2.14 使能/关闭地址扫描攻击防范功能

请在系统视图下进行下列配置。

表12-18 使能/关闭地址扫描攻击防范功能

操作	命令
使能地址扫描攻击防范功能	firewall defend ip-sweep [max-rate rate-number] [blacklist-timeout minutes]
关闭地址扫描攻击防范功能	undo firewall defend ip-sweep

缺省为关闭地址扫描攻击防范功能。最大扫描速率（**max-rate**）取值范围为 1～10,000，缺省值为 4000；加入黑名单时间（**blacklist-timeout**）取值范围为 0～1,000 分钟，缺省值为 0，表示不加入黑名单。



注意：

- 开启地址扫描攻击防范功能必须满足两点：1. 使能连接发起域出方向的 IP 统计功能；2. 配置地址扫描攻击防范功能。
- 加入黑名单的老化时间应该大于防火墙会话的超时时间（使用命令 **firewall session aging-time** 设置），否则会导致攻击通过防火墙。建议将加入黑名单时间设置为大于 2 分钟。
- 必须使能防火墙的黑名单功能后，此命令设置的黑名单功能才能生效。关于黑名单的描述请参见 5.4 黑名单。

12.2.15 使能/关闭端口扫描攻击防范功能

请在系统视图下进行下列配置。

表12-19 使能/关闭端口扫描攻击防范功能

操作	命令
使能端口扫描攻击防范功能	firewall defend port-scan [max-rate <i>rate-number</i>] [blacklist-timeout <i>minutes</i>]
关闭端口扫描攻击防范功能	undo firewall defend port-scan

缺省为关闭端口扫描攻击防范功能。最大扫描速率（**max-rate**）取值范围为 1～10,000，缺省值为 4000；加入黑名单时间（**blacklist-timeout**）取值范围为 0～1,000 分钟，缺省值为 0，表示不加入黑名单。



注意：

- 开启端口扫描攻击防范功能必须满足两点：1. 使能连接发起域出方向的 IP 统计功能；2. 配置端口扫描攻击防范功能。3. 对于目标为防火墙自身的攻击，需对 Local 域进行配置。
- 加入黑名单的老化时间应该大于防火墙会话的超时时间（使用命令 **firewall session aging-time** 设置），否则会导致攻击通过防火墙。建议将加入黑名单时间设置为大于 2 分钟。
- 必须使能防火墙的黑名单功能后，此命令设置的黑名单功能才能生效。关于黑名单的描述请参见 5.4 黑名单。

12.2.16 使能/关闭源路由选项 IP 报文控制功能

请在系统视图下进行下列配置。

表12-20 使能/关闭带源路由选项 IP 报文控制功能

操作	命令
使能带源路由选项 IP 报文控制功能	firewall defend source-route
关闭带源路由选项 IP 报文控制功能	undo firewall defend source-route

缺省为关闭源路由选项 IP 报文控制功能。

12.2.17 使能/关闭路由记录选项攻击防范功能

请在系统视图下进行下列配置。

表12-21 使能/关闭路由记录选项攻击防范功能

操作	命令
使能路由记录选项攻击防范功能	firewall defend route-record
关闭路由记录选项攻击防范功能	undo firewall defend route-record

缺省为关闭路由记录选项攻击防范功能。

12.2.18 使能/关闭 Tracert 报文控制功能

请在系统视图下进行下列配置。

表12-22 使能/关闭 Tracert 报文控制功能

操作	命令
使能 tracert 报文控制功能	firewall defend tracert
关闭 tracert 报文控制功能	undo firewall defend tracert

缺省为关闭 Tracert 报文控制功能。

12.2.19 使能/关闭 Ping of Death 攻击防范功能

请在系统视图下进行下列配置。

表12-23 使能/关闭 Ping of Death 攻击防范功能

操作	命令
使能 Ping of Death 攻击防范功能	firewall defend ping-of-death
关闭 Ping of Death 攻击防范功能	undo firewall defend ping-of-death

缺省为关闭 Ping of Death 攻击防范功能。

12.2.20 使能/关闭 Teardrop 攻击防范功能

请在系统视图下进行下列配置。

表12-24 使能/关闭 TearDrop 攻击防范功能

操作	命令
使能 TearDrop 攻击防范功能，并使用非宽松检测	firewall defend teardrop
关闭 TearDrop 攻击防范功能	undo firewall defend teardrop
使能 TearDrop 攻击防范功能，并使用宽松检测	firewall defend teardrop teardrop-loose
取消宽松检测，使用非宽松检测模式	undo firewall defend teardrop teardrop-loose

缺省为关闭 TearDrop 攻击防范功能。

Teardrop 攻击防范有两种模式：一种为宽松检测模式，另一种为非宽松检测模式。

- 使用非宽松检测模式（即不配置 **teardrop-loose** 选项）时，防火墙将对所有接口收到的数据包进行检测。
- 使用宽松检测模式（即配置 **teardrop-loose** 选项）时，防火墙将对从 **bridge-template** 接口收到的数据包不进行 teardrop 攻击检测，但是对其他接口收到的数据包还会进行检测。

12.2.21 使能/关闭 TCP 报文标志合法性检测功能

请在系统视图下进行下列配置。

表12-25 使能/关闭 TCP 报文标志合法性检测功能

操作	命令
使能 TCP 报文标志合法性检测功能	firewall defend tcp-flag
关闭 TCP 报文标志合法性检测功能	undo firewall defend tcp-flag

缺省为关闭 TCP 报文标志合法性检测功能。

12.2.22 使能/关闭 IP 分片报文检测功能

请在系统视图下进行下列配置。

表12-26 使能/关闭 IP 分片报文检测功能

操作	命令
使能 IP 分片报文检测功能	firewall defend ip-fragment
关闭 IP 分片报文检测功能	undo firewall defend ip-fragment

缺省为关闭 IP 分片报文检测功能。

12.2.23 使能/关闭超大 ICMP 报文控制功能

请在系统视图下进行下列配置。

表12-27 使能/关闭超大 ICMP 报文控制功能

操作	命令
使能超大 ICMP 报文控制功能	firewall defend large-icmp [length]
关闭超大 ICMP 报文控制功能	undo firewall defend large-icmp

缺省为关闭超大 ICMP 报文攻击防范功能。报文最大长度取值范围为 28~65535 字节，缺省值为 4000。

12.3 设置防火墙连接数量和连接速率监控的告警级别

防火墙的系统统计功能可以对连接数量和连接速率进行监控。防火墙对于连接数量或连接速率超过所设定的限制时将会进行告警。告警级别分为两种，一种为“告警”，是指当连接数量和连接速率超过设置的上限阈值时，仅输出告警信息；另一种为“丢弃”，是指当连接数量或连接速率超过设置的上限阈值时，输出告警信息，并且丢弃后续报文。仅当连接数量或连接速率恢复到设置的下限阈值时，不再丢弃报文。

请在系统视图下进行下列配置。

表12-28 设置防火墙连接数量和连接速率监控的告警级别

操作	命令
设置告警级别为输出告警信息，并丢弃报文	firewall statistic warning-level drop
设置告警级别为仅输出告警信息	undo firewall statistic warning-level drop

缺省情况下，告警级别为仅输出告警信息。

 说明：

该命令仅对基于安全区域和 IP 的统计功能有效，对于系统统计功能无效。

12.4 系统统计功能的配置

在配置流量限制功能前，必须开启对应的统计功能。对应的统计功能关闭后，相关的限制告警功能也相应失效。

统计功能配置包括：

- 使能系统统计功能
- 使能系统连接数量监控
- 使能系统报文比率异常告警检测

12.4.1 使能/关闭系统统计功能

使能系统统计，可以对所有流经防火墙的数据进行统计。

请在系统视图下进行下列配置。

表12-29 使能/关闭系统统计功能

操作	命令
使能系统统计功能	firewall statistic system enable
关闭系统统计功能	undo firewall statistic system enable

缺省情况下，系统统计功能为打开。

 注意：

请慎重使用关闭系统统计功能的命令！关闭系统统计功能后，和系统统计相关的检测功能也失效。在有流量的情况下，关闭统计功能后，很可能导致以后的统计功能不准，并连带影响与统计相关的功能。

12.4.2 配置系统连接数监控

该命令用来配置系统的 TCP 连接和 UDP 连接总数的上限阈值和下限阈值。当防火墙系统的 TCP 或 UDP 连接个数超过设定的阈值上限后，防火墙将输出日志进行告警，而当 TCP、UDP 连接个数降到设定的阈值下限时，表示连接数恢复到正常。

请在系统视图下进行下列配置。

表12-30 配置系统连接数限制

操作	命令
配置系统连接数限制	firewall statistic system connect-number { tcp udp } high high-value low low-value
恢复系统连接数限制为缺省值	undo firewall statistic system connect-number { tcp udp }

缺省情况下，基于系统的 TCP 和 UDP 连接的上限阈值为 500000，下限阈值为 450000。

12.4.3 配置系统报文比率异常告警检测

该命令用来配置不同类型的报文在正常情况下一段时间内所占的百分比以及允许的变动范围，系统定时检测收到的各类报文百分比，并和配置进行比较，如果某类型（TCP、UDP、ICMP 或其他）报文百分比超过配置的上限阈值（加波动范围）或低于配置的下限阈值（减波动范围），则系统输出日志告警。

请在系统视图下进行下列配置。

表12-31 配置系统报文比率异常告警检测

操作	命令
配置系统报文比率异常告警检测	firewall statistic system flow-percent tcp tcp-percent udp udp-percent icmp icmp-percent alternation alternation-percent [time time-value]
恢复系统报文比率异常告警检测为缺省值	undo firewall statistic system flow-percent

在缺省情况下，TCP、UDP、ICMP 报文分别所占的百分比为 75、15、5；各种报文所允许的百分比的波动范围为 25；检测周期为 60 分钟。

此命令 TCP、UDP、ICMP 三种报文所占百分比需要同时被配置，并且三种报文所占百分比之和不能超过 100%；如果 TCP、UDP、ICMP 三种报文百分比之和超过 100%，则命令不会生效。

此告警信息是基于系统当前的统计值，如果当前系统统计信息没有被清除，此告警信息会按照配置的时间间隔定时进行输出。

12.5 域统计功能的配置

统计功能配置包括：

- 使能域统计功能
- 使能域连接数量监控

- 使能域连接速率监控

12.5.1 使能/关闭域统计功能

请在域视图下进行下列配置。

表12-32 使能/关闭域统计功能

操作	命令
使能域统计功能	statistic enable zone { inzone outzone }
关闭域统计功能	undo statistic enable zone { inzone outzone }

缺省情况下，防火墙的域统计功能关闭。



注意：

域统计功能关闭后，配置在域上的流量监控功能也失效。

12.5.2 配置域连接数量监控

该命令用来配置基于域的某一方向上发起的 TCP 连接和 UDP 连接总数的上限阈值和下限阈值。通过对域的连接数量的限制，用户可以限制当前域向外发起的连接数量，同时也可以限制外部向当前域发起连接的数量。当连接数超过设定的阈值上限或恢复到阈值下限时，系统将根据 **firewall statistic warning-level** 命令的设置采取相应操作。配置了域统计功能使能后，连接数监控功能缺省值自动生效。

请在域视图下进行配置。

表12-33 配置域连接数量监控

操作	命令
配置域连接数量监控	statistic connect-number zone { inzone outzone } { tcp udp } high high-limit low low-limit
恢复域连接数量监控为缺省值	undo statistic connect-number zone { inzone outzone } { tcp udp }

基于域的 TCP 和 UDP 连接的上限阈值的缺省值为 500000，下限阈值的缺省值为 450000。



注意：

域上的连接数量检测功能必须先配置使能对应域的统计功能，否则此命令没有效果。

12.5.3 配置域连接速率监控

该命令用来配置域发起的 TCP 连接和 UDP 连接速率（每秒）的上限阈值和下限阈值。通过对域的连接速率的限制，用户可以限制当前域向外发起的连接速率，同时也可以限制外部向当前域发起连接的速率。当连接速率超过设定的阈值上限或恢复到阈值下限时，系统将根据 **firewall statistic warning-level** 命令的设置采取相应操作。配置了域统计功能使能后，连接速率监控功能缺省值自动生效。

请在域视图下进行配置。

表12-34 配置域连接速率监控

操作	命令
配置域连接速率监控	statistic connect-speed zone { inzone outzone } { tcp udp } { high high-limit low low-limit }
恢复域连接速率监控为缺省值	undo statistic connect-speed zone { inzone outzone } { tcp udp }

基于域的 TCP 和 UDP 连接速率的上限阈值的缺省值为 10000，下限阈值的缺省值为 9000。



注意：

域上的连接速率检测功能必须先配置使能对应域的统计功能，否则此命令没有效果。

12.6 IP 统计功能的配置

统计功能配置包括：

- 使能 IP 统计功能
- 使能 IP 连接数量监控
- 使能 IP 连接速率监控

12.6.1 使能/关闭 IP 统计功能

使能（关闭）防火墙基于 IP 的统计功能。执行使能命令后，将对当前域的出或入方向数据包根据 IP 地址进行统计。对于当前域的出方向数据包，统计其源地址。对于当前域的入方向数据包，统计其目的地址。

域的入方向指数据包的目的地址为本域，而源地址不为本域。域的出方向指数据包的源地址为本域，而目的地址不为本域。

请在域视图下进行下列配置。

表12-35 使能/关闭 IP 统计功能

操作	命令
使能 IP 统计功能	statistic enable ip { inzone outzone }
禁止 IP 统计功能	undo statistic enable ip { inzone outzone }

缺省情况下，防火墙的 IP 统计功能关闭。



注意：

IP 统计功能关闭后，基于 IP 的流量监控功能也失效。

12.6.2 配置 IP 连接数量监控

基于本域 IP 地址的某一方向（本域出/入方向），可以配置发起的 TCP/UDP 连接总数的上限阈值和下限阈值。

该命令用来在本域配置 IP 地址的某一方向（本域出入方向）上，限制发起的 TCP 连接和 UDP 连接总数的上限阈值和下限阈值。通过对基于 IP 的连接数量的限制，用户可以限制当前域的 IP 向外发起的连接数量，同时也可以限制外部向当前域的 IP 发起连接的数量。当连接数量超过设定的阈值上限或恢复到阈值下限时，系统将根据 **firewall statistic warning-level** 命令的设置采取相应操作。配置了域统计功能使能后，连接数量监控功能缺省值自动生效。

请在域视图下进行配置。

表12-36 配置 IP 连接数量监控

操作	命令
配置基于安全区域出方向的 IP 连接数量监控	statistic connect-number ip outzone { tcp udp } high high-limit low low-limit statistic connect-number id id ip outzone { tcp udp } high high-limit low low-limit acl-number acl-number
恢复基于安全区域出方向的 IP 连接数量监控为缺省值	undo statistic connect-number [id id] ip outzone { tcp udp }
配置基于安全区域入方向的 IP 连接数量监控	statistic connect-number ip inzone { tcp udp } high high-limit low low-limit
恢复基于安全区域入方向的 IP 连接数量监控为缺省值	undo statistic connect-number ip inzone { tcp udp }

基于 IP 的 TCP 和 UDP 连接的上限阈值的缺省值为 500000，下限阈值的缺省值为 450000。

**注意：**

IP 上的连接数量监控功能必须先配置使能对应 IP 的统计功能，否则此命令没有效果。

12.6.3 配置 IP 连接速率监控

该命令用来在本域配置 IP 地址的某一方向（本域出/入方向）上，限制发起的 TCP 连接和 UDP 连接速率的上限阈值和下限阈值。通过对基于 IP 的连接速率的限制，用户可以限制当前域的 IP 向外发起的连接速率，同时也可以限制外部向当前域的 IP 发起连接的速率。当连接速率超过设定的阈值上限或恢复到阈值下限时，系统将根据 **firewall statistic warning-level** 命令的设置采取相应操作。配置了域统计功能使能后，连接数速率监控功能缺省值自动生效。

请在域视图下进行配置。

表12-37 配置 IP 的连接速率监控功能

操作	命令
配置基于安全区域出方向的 IP 连接速率监控	statistic connect-speed ip outzone { tcp udp } high high-limit low low-limit statistic connect-speed id id ip outzone { tcp udp } high high-limit low low-limit acl-number acl-number
恢复基于安全区域出方向的 IP 连接速率监控为缺省值	undo statistic connect-speed [id id] ip outzone { tcp udp }
配置基于安全区域入方向的 IP 连接速率监控	statistic connect-speed ip inzone { tcp udp } high high-limit low low-limit
恢复基于安全区域入方向的 IP 连接速率监控为缺省值	undo statistic connect-speed ip inzone { tcp udp }

基于 IP 的 TCP 和 UDP 连接速率的上限阈值的缺省值为 10000，下限阈值的缺省值为 9000。

12.7 攻击防范与报文统计显示与调试

12.7.1 攻击防范显示与调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示攻击防范的配置情况，通过查看显示信息验证配置的效果。在用户视图下执行 **debugging** 命令可对攻击防范进行调试。

表12-38 攻击防范显示与调试

操作	命令
显示当前已启用的攻击防范类型	display firewall defend flag
显示 TCP 代理的会话信息	display firewall tcp-proxy session [zone zone-name ip ip-address]
打开所有攻击防范调试开关	debugging firewall defend all
打开 ARP Flood 攻击防范调试开关	debugging firewall defend arp-flood
打开 ARP 欺骗攻击防范调试开关	debugging firewall defend arp-spoofing
打开 IP 欺骗攻击防范调试开关	debugging firewall defend ip-spoofing
打开 Land 攻击防范调试开关	debugging firewall defend land
打开 Smurf 攻击防范调试开关	debugging firewall defend smurf
打开 Fraggle 攻击防范调试开关	debugging firewall defend fraggle
打开 Frag Flood 攻击防范调试开关	debugging firewall defend frag-flood
打开 WinNuke 攻击防范调试开关	debugging firewall defend winnuke
打开 SYN Flood 攻击防范调试开关	debugging firewall defend syn-flood
打开 ICMP Flood 攻击防范调试开关	debugging firewall defend icmp-flood
打开 UDP Flood 攻击防范调试开关	debugging firewall defend udp-flood
打开 ICMP 重定向报文攻击防范调试开关	debugging firewall defend icmp-redirect
打开 ICMP 不可达报文攻击防范调试开关	debugging firewall defend icmp-unreachable
打开地址扫描攻击防范调试开关	debugging firewall defend ip-sweep
打开端口扫描攻击防范调试开关	debugging firewall defend port-scan
打开路由记录选项攻击防范调试开关	debugging firewall defend route-record
打开带源路由选项报文攻击防范调试开关	debugging firewall defend source-route
打开 tracert 攻击防范调试开关	debugging firewall defend tracert
打开 Ping of Death 攻击防范调试开关	debugging firewall defend ping-of-death
打开 TearDrop 攻击防范调试开关	debugging firewall defend teardrop
打开 TCP 标志合法性检测调试开关	debugging firewall defend tcp-flag
打开 IP 分片报文检测调试开关	debugging firewall defend ip-fragment
打开超大 ICMP 报文攻击防范调试开关	debugging firewall defend large-icmp

说明：

当防火墙工作在透明模式下时，在检测到攻击的告警信息中，会出现攻击报文的数目为实际报文的（n-1）倍的情况（n 为当前 UP 状态的接口的数目）。这是由于工作在透明模式下的防火墙对于未知目的 MAC 地址的报文的处理方式所致，即在除接收接口以外的所有状态为 UP 的接口广播。

12.7.2 报文统计显示与调试

可在所有视图下使用 **display** 命令，请在用户视图下使用 **reset** 命令。

表12-39 统计信息显示命令

操作	命令
显示防火墙统计信息	display firewall statistic { system zone zone-name { inzone outzone } ip { ip-address { source-ip destination-ip both } which } }
显示防火墙系统的统计信息	display firewall statistic system [defend flow-percent [default]]
清除防火墙统计信息	reset firewall statistic system [defend current]
清除防火墙域统计信息	reset firewall statistic zone zone-name { inzone outzone }
清除防火墙 IP 统计信息	reset firewall statistic ip ip-address { source-ip destination-ip both }

12.8 SMTP 客户端配置

SecPath 防火墙支持 SMTP 客户端功能，可以定时和实时的向指定的邮件地址发送邮件。邮件可以向管理员报告防火墙的系统统计信息、攻击防范信息、流量告警信息、网页过滤信息和邮件过滤信息。通过这种方式，管理员可以及时了解到防火墙的状态信息，极大的提高了管理的灵活性和可维护性。

说明：

SMTP客户端的正常运行依赖于DNS客户端（DNSC）去进行名称解析，有关DNSC的介绍请参见 12.9 DNS客户端配置。

12.8.1 配置触发邮件的时间

使用以下命令可以配置防火墙触发邮件的时间，在每日到达指定的时间点时，将触发邮件。

请在系统视图下进行下列配置。

表12-40 配置触发邮件的时间

操作	命令
配置触发邮件的时间	smtpc trigger time <i>hh:mm</i>
取消配置的触发时间	undo smtpc trigger { all time <i>hh:mm</i> }

缺省情况下，未配置触发邮件的时间。

hh:mm 的时间范围为 00:00~23:59。通过多次执行此命令，可以添加多个触发时间点，最多可配置 5 个。

12.8.2 配置邮件的收件人地址

使用以下命令可以配置邮件的收件人地址。

请在系统视图下进行下列配置。

表12-41 配置邮件的收件人地址

操作	命令
配置邮件的收件人地址	smtpc administrator mail <i>mail-address</i>
取消配置的邮件的收件人地址	undo smtpc administrator { all mail <i>mail-address</i> }

缺省情况下，未配置收件人地址。

添加的收件人地址必须符合 SMTP 邮件地址的格式。通过多次执行此命令，可以添加多个收件人地址，最多可配置 5 个。

12.8.3 SMTP 客户端的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示 SMTP 客户端的配置情况，通过查看显示信息验证配置的效果。在用户视图下执行 **debugging** 命令可以对 SMTP 客户端进行调试。

表12-42 SMTP 客户端的显示与调试

操作	命令
显示 SMTP 客户端的配置信息	display smtpc [administrator trigger]
打开 SMTP 客户端的调试开关	debugging smtpc
关闭 SMTP 客户端的调试开关	undo debugging smtpc

12.9 DNS 客户端配置

DNS 客户端（DNSC）是使 SMTP 客户端正常工作的重要组件。DNSC 将域名解析为 IP 地址，以使 SMTP 客户端将邮件正确的发往目标地址。

12.9.1 配置 DNS 服务器

要进行 DNS 域名解析，需要知道域名服务器的地址，这样才能把查询请求报文发送到正确的服务器进行解析，使用下面的命令可以配置/删除 DNS 服务器的 IP 地址。请在系统视图下进行下面配置。

表12-43 配置 DNS 服务器

操作	命令
配置 DNS 服务器的 IP 地址	dnsc server ip <i>ip-address</i>
删除配置的 DNS 服务器	undo dnsc server { all ip <i>ip-address</i> }

缺省情况下，未配置 DNS 服务器。

12.9.2 配置 DNS 缓存

当 DNS 客户端进行名称解析时，可以将名称服务器返回的结果进行缓存。这样，当再有相同名称的解析请求时，就可以直接从 DNS 缓存中进行查找，无需再向名称服务器发出查询请求，减少了网络流量。

请在系统视图下进行下面配置。

表12-44 配置 DNS 缓存

操作	命令
添加 DNS 缓存条目	dnsc cache add domain <i>domain-name</i> type { a mx } ip <i>ip-address</i> ttl <i>ttl</i>
删除 DNS 缓存条目	dnsc cache delete domain <i>domain-name</i> type { a mx } undo dnsc cache { all domain <i>domain-name</i> type { a mx } }

缺省情况下，未配置 DNS 缓存条目。

12.9.3 DNS 客户端的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示 DNS 客户端的配置情况，通过查看显示信息验证配置的效果。在用户视图下执行 **debugging** 命令可以对 DNS 客户端进行调试。

表12-45 DNS 客户端的显示与调试

操作	命令
显示 DNS 客户端的配置信息	display dnsc { server cache }
打开 DNS 客户端的调试开关	debugging dnsc
关闭 DNS 客户端的调试开关	undo debugging dnsc

12.10 攻击防范与报文统计典型配置举例

12.10.1 使能 Land 攻击防范功能

1. 组网需求

将防火墙的以太网口 Ethernet 0/0/0 配置为 Trust 域，以太网口 Ethernet 2/0/0 配置为 Untrust 域，以太网口 Ethernet 1/0/0 配置为 DMZ 区。

2. 组网图

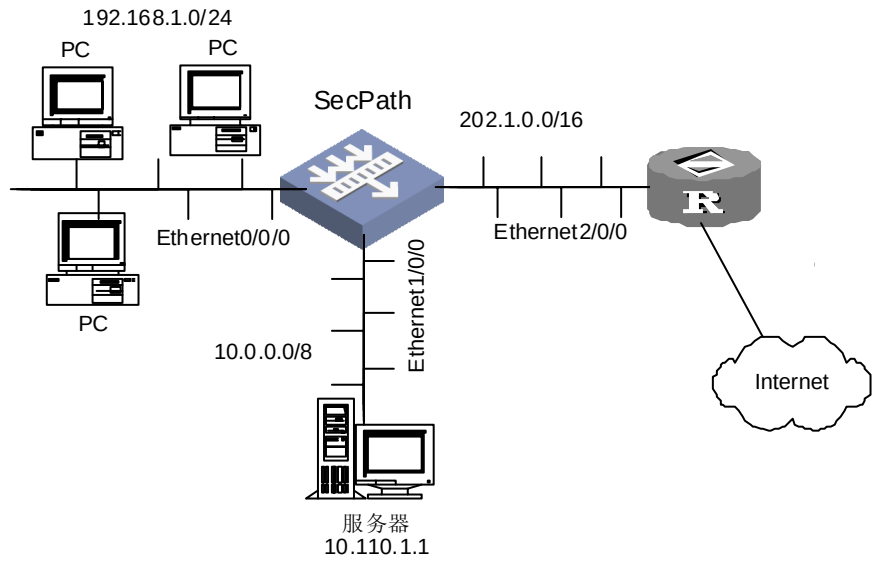


图12-2 防火墙攻击防范功能配置组网图

3. 配置步骤

配置防火墙：

配置防火墙接口 Ethernet 0/0/0。

```
[H3C] interface Ethernet 0/0/0
[H3C-Ethernet0/0/0] ip address 192.168.1.1 255.255.255.0
```

配置防火墙接口 Ethernet 2/0/0。


```
[H3C] interface Ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 202.1.0.1 255.255.0.0
# 配置防火墙接口 Ethernet 1/0/0。

[H3C] interface Ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 10.0.0.1 255.0.0.0
# 配置接口 Ethernet 0/0/0 加入防火墙 Trust 域。

[H3C] firewall zone trust
[H3C-zone-trust] add interface Ethernet 0/0/0
# 配置接口 Ethernet 2/0/0 加入防火墙 Untrust 域。

[H3C] firewall zone untrust
[H3C-zone-untrust] add interface Ethernet 2/0/0
# 配置接口 Ethernet 1/0/0 加入防火墙 DMZ 域。

[H3C] firewall zone DMZ
[H3C-zone-DMZ] add interface Ethernet 1/0/0
# 使能 Land 攻击防范功能。

[H3C-zone-DMZ] quit
[H3C] firewall defend land
```

12.10.2 使能 SYN Flood 攻击防范功能

1. 组网需求

将防火墙的以太网口 E0/0/0 配置为 Trust 域，以太网口 E2/0/0 配置为 Untrust 域，以太网口 E1/0/0 配置为 DMZ 区。需要对 DMZ 域内的服务器进行 SYN Flood 攻击防范。

2. 组网图

参见图 12-2。

3. 配置步骤

```
# 配置防火墙接口 Ethernet 0/0/0。

[H3C] interface Ethernet 0/0/0
[H3C-Ethernet0/0/0] ip address 192.168.1.1 255.255.255.0
# 配置防火墙接口 Ethernet 2/0/0。

[H3C] interface Ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 202.1.0.1 255.255.0.0
# 配置防火墙接口 Ethernet 1/0/0。

[H3C] interface Ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 10.0.0.1 255.0.0.0
```

```
# 配置接口 Ethernet 0/0/0 加入防火墙 Trust 域。

[H3C] firewall zone trust
[H3C-zone-trust] add interface Ethernet 0/0/0

# 配置接口 Ethernet 2/0/0 加入防火墙 Untrust 域。

[H3C] firewall zone untrust
[H3C-zone-untrust] add interface Ethernet 2/0/0

# 配置接口 Ethernet 1/0/0 加入防火墙 DMZ 域。

[H3C] firewall zone DMZ
[H3C-zone-DMZ] add interface Ethernet 1/0/0

# 使能 DMZ 域入方向的 IP 统计功能。

[H3C] firewall zone DMZ
[H3C-zone-DMZ] statistic enable ip inzone

# 打开 SYN Flood 攻击防范功能全局开关。

[H3C-zone-trust] quit
[H3C] firewall defend syn-flood enable

# 配置对服务器 10.110.1.1 进行 SYN Flood 攻击防范，配置 SYN 包的最大连接速
率为 500 包/秒，手工启动 TCP 代理。

[H3C] firewall defend syn-flood ip 10.110.1.1 max-rate 500 tcp-proxy
```

12.10.3 使能地址扫描攻击防范功能

1. 组网需求

将防火墙的以太网口 E0/0/0 配置为 Trust 域，以太网口 E2/0/0 配置为 Untrust 域，以太网口 E1/0/0 配置为 DMZ 区。需要对 Untrust 域进行地址扫描攻击检测。

2. 组网图

参见图 12-2。

3. 配置步骤

```
# 配置防火墙接口 Ethernet 0/0/0。

[H3C] interface Ethernet 0/0/0
[H3C-Ethernet0/0/0] ip address 192.168.1.1 255.255.255.0

# 配置防火墙接口 Ethernet 2/0/0。

[H3C] interface Ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 202.1.0.1 255.255.0.0

# 配置防火墙接口 Ethernet 1/0/0。

[H3C] interface Ethernet 1/0/0
```

```
[H3C-Ethernet1/0/0] ip address 10.0.0.1 255.0.0.0
# 配置接口 Ethernet 0/0/0 加入防火墙 Trust 域。

[H3C] firewall zone trust
[H3C-zone-trust] add interface Ethernet 0/0/0
# 配置接口 Ethernet 2/0/0 加入防火墙 Untrust 域。

[H3C] firewall zone untrust
[H3C-zone-untrust] add interface Ethernet 2/0/0
# 配置接口 Ethernet 1/0/0 加入防火墙 DMZ 域。

[H3C] firewall zone DMZ
[H3C-zone-DMZ] add interface Ethernet 1/0/0
# 使能 Untrust 域出方向的 IP 统计功能。

[H3C] firewall zone untrust
[H3C-zone-untrust] statistic enable ip outzone
[H3C-zone-untrust] quit
# 配置地址扫描攻击检测，配置最大扫描速率为 1000 包/秒，加入黑名单时间为 5
分钟，并使能黑名单功能。

[H3C] firewall defend ip-sweep max-rate 1000 blacklist-timeout 5
[H3C] firewall blacklist enable
```

12.10.4 监控基于域的连接数量

1. 组网需求

将防火墙的以太网口 Ethernet0/0/0 配置为 Trust 域，以太网口 Ethernet2/0/0 配置为 Untrust 域，以太网口 Ethernet1/0/0 配置为 DMZ 区。需要对 Trust 域向外发起的连接数目和其他域向 Trust 域发起的连接数目分别进行限制。

2. 组网图

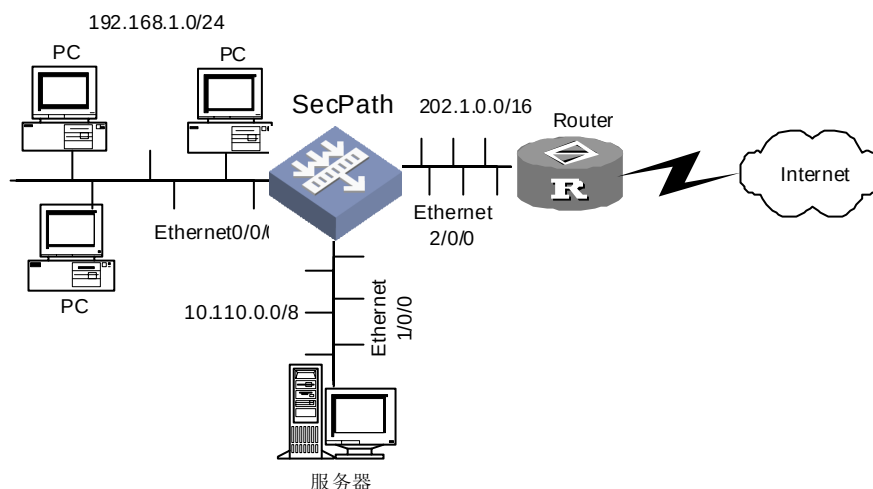


图12-3 防火墙统计功能配置组网图

3. 配置步骤

配置防火墙接口 Ethernet 0/0/0。

```
[H3C] interface ethernet 0/0/0
[H3C-Ethernet0/0/0] ip address 192.168.1.1 255.255.255.0
```

配置防火墙接口 Ethernet 2/0/0。

```
[H3C] interface ethernet 2/0/0
[H3C-Ethernet2/0/0] ip address 202.1.0.1 255.255.0.0
```

配置防火墙接口 Ethernet 1/0/0。

```
[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ip address 10.0.0.1 255.0.0.0
```

配置接口 Ethernet 0/0/0 加入防火墙 Trust 域。

```
[H3C] firewall zone trust
[H3C-zone-trust] add interface ethernet 0/0/0
```

配置接口 Ethernet 2/0/0 加入防火墙 Untrust 域。

```
[H3C] firewall zone untrust
[H3C-zone-untrust] add interface ethernet 2/0/0
```

配置接口 Ethernet 1/0/0 加入防火墙 DMZ 域。

```
[H3C] firewall zone dmz
[H3C-zone-dmz] add interface ethernet 1/0/0
```

使能 Trust 域的出方向报文统计。

```
[H3C] firewall zone trust
[H3C-zone-trust] statistic enable zone outzone
```

使能 Trust 域的入方向报文统计。

```
[H3C-zone-trust] statistic enable zone inzone
```

配置 Trust 域的入方向 TCP 连接数量限制上限为 120000。

```
[H3C-zone-trust] statistic connect-number zone inzone tcp high 120000 low 10000
```

配置 Trust 域的出方向 TCP 连接数量限制上限为 200000。

```
[H3C-zone-trust] statistic connect-number zone outzone tcp high 200000 low 10000
```

12.10.5 显示指定 IP 的统计信息

1. 组网需求

将防火墙的以太网口 Ethernet0/0/0 配置为 Trust 域，以太网口 Ethernet2/0/0 配置为 Untrust 域，以太网口 Ethernet1/0/0 配置为 DMZ 区。

2. 组网图

参见图 12-3。

3. 配置步骤

配置防火墙接口 Ethernet 0/0/0。

```
[H3C] interface ethernet 0/0/0
```

```
[H3C-Ethernet0/0/0] ip address 192.168.1.1 255.255.255.0
```

配置防火墙接口 Ethernet 2/0/0。

```
[H3C] interface ethernet 2/0/0
```

```
[H3C-Ethernet2/0/0] ip address 202.1.0.1 255.255.0.0
```

配置防火墙接口 Ethernet 1/0/0。

```
[H3C] interface ethernet 1/0/0
```

```
[H3C-Ethernet1/0/0] ip address 10.0.0.1 255.0.0.0
```

配置接口 Ethernet 0/0/0 加入防火墙 Trust 域。

```
[H3C] firewall zone trust
```

```
[H3C-zone-trust] add interface Ethernet 0/0/0
```

配置接口 Ethernet 2/0/0 加入防火墙 Untrust 域。

```
[H3C] firewall zone untrust
```

```
[H3C-zone-untrust] add interface ethernet 2/0/0
```

配置接口 Ethernet 1/0/0 加入防火墙 DMZ 域。

```
[H3C] firewall zone dmz
```

```
[H3C-zone-dmz] add interface ethernet 1/0/0
```

```
# 进入域视图。

[H3C] firewall zone trust

# 使能域的 IP 数据包出方向报文统计功能，统计源地址。

[H3C-zone-trust] statistic enable ip outzone

# 使能域的 IP 数据包入方向报文统计功能，统计目的地址。

[H3C-zone-trust] statistic enable ip inzone

# 显示 Trust 域的地址 192.168.1.3 向外部发起连接的统计数据。

<H3C> display firewall statistic ip 192.168.1.3 source-ip

# 显示外部向 Trust 域的地址 192.168.1.3 发起连接的统计数据。

<H3C> display firewall statistic ip 192.168.1.3 destination-ip
```

12.11 攻击防范故障诊断与排除

1. 故障之一：SYN Flood 攻击防范功能未起作用。

故障排除：可以按如下步骤进行。

- (1) 检查是否打开针对目的域（或目的 IP）的 SYN Flood 攻击防范功能。
- (2) 检查 SYN Flood 攻击防范功能全局开关是否打开。
- (3) 检查目的域（或目的 IP 所在的域）入方向的 IP 统计功能是否使能。

2. 故障之二：地址扫描攻击防范功能未起作用。

故障排除：可以按如下步骤进行。

- (1) 检查是否打开地址扫描攻击检测功能。
- (2) 检查扫描源所在域出方向的 IP 统计功能是否使能。

第13章 IDS 联动

13.1 IDS 联动功能简介

随着宽带网络的发展，用户对网络安全日益关注，需要使用 IDS 设备对报文进行深度检测。报文的深度检测是指对流经被保护网络的流量进行基于内容特征、协议异常分析以及流量异常分析等方式的检测，以防止黑客、网络病毒的入侵。但由于 IDS（Intrusion Detect System）是个旁路设备，只负责监听网络流量，无法真正阻断入侵行为，因此需要与防火墙联动，把入侵的报文流通知防火墙，让防火墙来阻断该入侵行为。

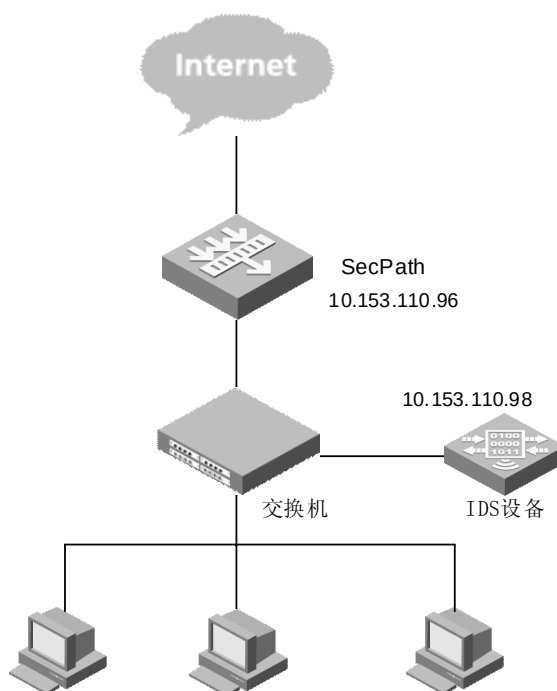


图13-1 IDS 典型组网图

IDS 设备发现可疑的数据流，通过 SNMP 协议向防火墙设备发送阻断可疑流的具体 IDS 联动消息，包括 MAC 地址，IP 地址，协议号，源、目的端口号，针对可疑流的动作，作用时间，生效/失效等。防火墙接收到 IDS 设备发来的联动消息，经过解析后生成并下发 ACL 规则，在防火墙转发数据包的适当时刻调用这些 ACL 规则并产生相应的动作，以达到阻断可疑数据流的目的。

13.2 IDS 联动配置

13.2.1 在接口下发 IDS 联动规则

当防火墙接收到来自 IDS 设备发送的联动消息后，经过解析会自动生成相应的 ACL 规则。若要使其对报文进行阻断，必须在防火墙的接口上下发该 IDS 联动的 ACL 规则，使其调用 ACL 规则并阻断报文。

请在接口视图下进行下列配置。

表13-1 在接口下发 IDS 联动规则

操作	命令
允许在接口下发 IDS 联动规则	ids-acl enable
取消在接口下发 IDS 联动规则	undo ids-acl enable

缺省情况下，不在任何接口下发 IDS 联动规则。



注意：

对于工作在透明模式下的防火墙，在接口下发的 IDS 联动规则的控制方向只能为 inbound 方向，若要保证对数据包进行严格的过滤，需在流量的出接口和入接口都配置下发 IDS 联动规则。

13.2.2 IDS 联动的显示与调试

使用以下命令可以查看 IDS 联动信息、IDS 联动生成的 ACL 规则记录和打开 IDS 联动功能的调试开关。

请在所有视图下执行 **display** 命令，在用户视图下执行 **debugging** 命令。

表13-2 IDS 联动的显示与调试

操作	命令
显示 IDS 联动信息	display ids { all controlled-interface name <i>name</i> source <i>ip-addr</i> destination <i>ip-addr</i> }
显示 IDS 联动生成的 ACL 规则	display ids-acl { all name <i>name</i> }
打开 IDS 联动功能的调试开关	debugging ids
关闭 IDS 联动功能的调试开关	undo debugging ids

13.3 IDS 典型配置举例

1. 组网需求

防火墙作为内部网络与外部网络的边界设备，所有流入流出的数据报均通过防火墙设备转发。IDS 设备监听内部网络中的数据报，并根据一定的检测规则对监听到的数据报进行处理。防火墙侦听 IDS 设备发送的联动消息，并在接口下发 ACL 规则以实现报文的阻断。

2. 组网图

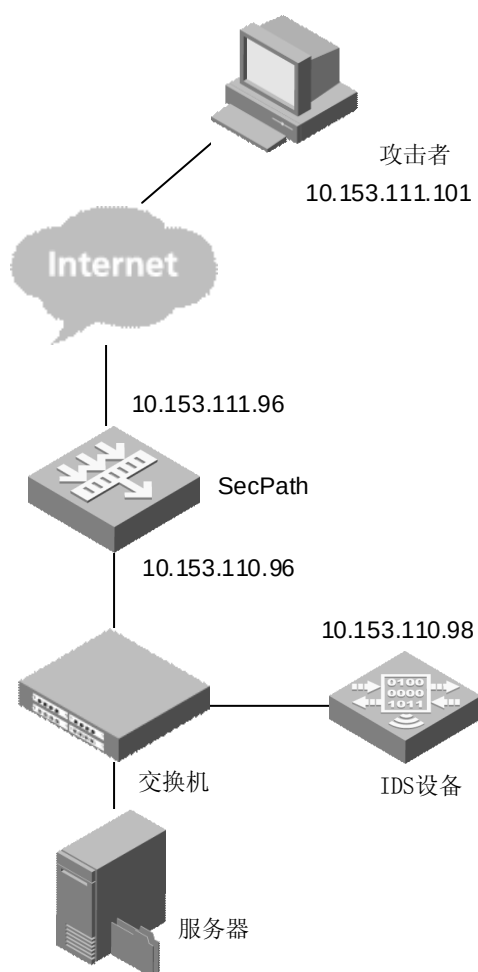


图13-2 IDS 联动组网图

3. 配置步骤

为防火墙的接口指定 IP 地址。

```
[H3C] interface GigabitEthernet 0/0
```

```
[H3C-GigabitEthernet0/0] ip address 10.153.110.96 24
```

SNMP 配置。

```
[H3C] snmp-agent
[H3C] snmp-agent community read public
[H3C] snmp-agent community write private
[H3C] snmp-agent sys-info version all
```

 说明：

要使 IDS 联动正常工作，必须保证 SNMP 协议数据报可以正常的在防火墙以及 IDS 设备间传送，并且防火墙的 SNMP 配置必须与 IDS 设备的 SNMP 配置相对应。关于更具体的 SNMP 配置请参阅本手册的“基础配置”部分中的“SNMP 配置”章节。

允许在接口下发 IDS 联动的 ACL 规则。

```
[H3C] interface GigabitEthernet 0/0
[H3C-GigabitEthernet0/0] ids-acl enable
```

 注意：

图中所示的内部网络中的交换机必须支持端口镜像功能，可以将希望监视的端口的流量镜像到与 IDS 设备监听口相连的端口上。

第14章 日志维护

14.1 日志简介

1. 日志种类划分

日志特性能够将系统消息或包过滤的动作等信息存入缓冲区或定向发送到日志主机上。通过对日志内容的分析和归档，管理员能够检查防火墙的安全漏洞、网络攻击的类型、何时何人试图违背安全策略。实时的日志记录还可以用来检测正在进行的入侵。

SecPath 防火墙统一考虑各种攻击和事件，将它们的各种日志输出格式、统计信息等内容进行规范，从而保证了日志风格的统一和日志功能的严谨性。

SecPath 防火墙包括以下几种日志信息：

- NAT/ASPF 日志
- 攻击防范日志
- 流量监控日志
- 黑名单日志
- 地址绑定日志

2. SecPath 上的日志输出原理

对于上述这些日志，根据日志输出方式的不同可以分为二进制流日志和 Syslog 日志两种。日志种类和日志输出方式之间的对应关系如下图所示。

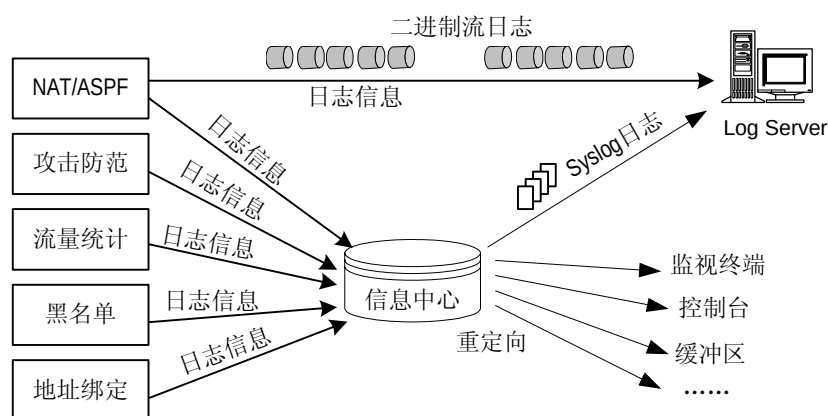


图14-1 SecPath 上的日志输出原理

在 SecPath 防火墙中，攻击防范、流量监控、黑名单和地址绑定产生的日志信息量小，因此采用 Syslog 方式以文本格式进行输出。这些日志信息必须通过 Comware

平台的信息中心进行日志管理和输出重定向，例如将其显示在终端屏幕上，或将 Syslog 日志发送给日志主机进行存储和分析。

相反，NAT/ASPF 产生的日志信息量很大，因此对于这种类型的流提供了一种“二进制”输出方式，直接输出到日志主机上以便对日志进行存储和分析，无需 SecPath 上的信息中心模块的参与。相比较而言，二进制流日志的传输效率高于 Syslog。

14.2 Syslog 日志配置

Syslog 日志的配置包括：

- 配置 Syslog 日志缓冲区的扫描时间
- 配置信息中心日志重定向

14.2.1 配置 Syslog 日志缓冲区的扫描时间

请在系统视图下进行下列配置。

表14-1 配置 Syslog 日志缓冲区的扫描时间

操作	命令
配置攻击防范的日志缓冲区的扫描频率	firewall defend log-time time
配置流量监控的日志缓冲区的扫描频率	firewall statistic log-time time
配置 HTTP 过滤日志缓冲区的扫描频率	firewall http log-time time
配置 FTP 过滤日志缓冲区的扫描频率	firewall ftp log-time time
配置 SNMP 过滤日志缓冲区的扫描频率	firewall snmp log-time time
配置 SMTP 过滤日志缓冲区的扫描频率	firewall smtp log-time time
恢复攻击防范的日志缓冲区的扫描频率为缺省值	undo firewall defend log-time
恢复流量监控的日志缓冲区的扫描频率为缺省值	undo firewall statistic log-time
恢复 HTTP 过滤的志缓冲区的扫描频率为缺省值	undo firewall http log-time
恢复 FTP 过滤的志缓冲区的扫描频率为缺省值	undo firewall ftp log-time
恢复 SNMP 过滤的志缓冲区的扫描频率为缺省值	undo firewall snmp log-time
恢复 SMTP 过滤的志缓冲区的扫描频率为缺省值	undo firewall smtp log-time

缺省情况下，日志缓冲区的扫描时间为 30 秒。

14.2.2 配置信息中心的日志重定向

通常情况下，输出到信息中心的日志信息会通过以下几种方式进行重定向：

- 通过 Console 口向本地控制台输出信息。

- 向远程 Telnet 终端输出信息，此功能有助于远程维护。
- 在 SecPath 防火墙内部分配适当大小的日志缓冲区，用于记录信息。
- 配置日志主机（Log Server），信息中心直接将信息发往日志主机，并在其上以文件的形式保存起来，供随时查看。
- 在 SecPath 防火墙内部分配适当大小的告警缓冲区，用于记录信息。
- 向 SNMP Agent 输出信息。

请在系统视图下进行下列配置。

表14-2 配置信息中心的日志重定向

操作	命令
向 Console 方向输出信息	info-center console channel { <i>channel-number</i> <i>channel-name</i> }
向 Telnet 终端或哑终端输出信息	info-center monitor channel { <i>channel-number</i> <i>channel-name</i> }
向 SNMP 输出信息	info-center snmp channel { <i>channel-number</i> <i>channel-name</i> }
设置日志缓冲区的大小以及向日志缓冲区输出信息的通道	info-center logbuffer [channel { <i>channel-number</i> <i>channel-name</i> }] size <i>buffersize</i>] *
设置向日志主机输出信息的信息通道以及其它参数	info-center loghost <i>X.X.X.X</i> [channel { <i>channel-number</i> <i>channel-name</i> }] facility <i>local-number</i> language { chinese english }] *
设置告警缓冲区的大小以及向告警缓冲区输出信息的通道	info-center trapbuffer [channel { <i>channel-number</i> <i>channel-name</i> }] size <i>buffersize</i>] *

详细配置请参见本手册的“基础配置”部分。

14.3 域间流日志配置

域间流日志是针对防火墙域间流的会话表实现的一种日志信息，支持二进制流日志格式（私有日志格式）。当防火墙的每个会话表项老化的时候，系统按照指定的格式将该会话表项对应的流的相关信息发送到日志主机，日志主机可为支持二进制流日志格式的 XLog 日志分析主机。

14.3.1 配置防火墙域间流日志

表14-3 配置防火墙域间流日志

操作	命令	说明
进入系统视图	system-view	-
进入域间视图	firewall interzone zone1 zone2	必选
使能域间流日志功能	session log enable [acl-number acl-number]	必选 缺省情况下，未使能域间流日志功能
退回系统视图	quit	-
配置流日志格式	firewall session log-type { syslog binary }	必选 防火墙流日志暂时只支持以二进制格式发送
配置二进制流日志主机	firewall binary-log host ip-address [port-number]	必选 缺省情况下，端口号为 9002

14.3.2 配置防火墙流日志统计阈值

表14-4 配置防火墙流日志统计阈值

操作	命令	说明
进入系统视图	system-view	-
配置流日志统计时间阈值	firewall session log-threshold time value	可选 缺省情况下，统计时间阈值为 600 分钟
配置流日志统计报文数阈值	firewall session log-threshold mega-packet value	可选 缺省情况下，统计报文数阈值为 4095 MPacket
配置流日志统计字节数阈值	firewall session log-threshold mega-byte value	可选 缺省情况下，统计字节数阈值为 4095 MByte

说明：

- 对于同一条数据流，在达到任意一种类型的阈值时，系统就会对此流进行日志统计。
 - 长时间持续流纪录的时间为正常结束流时间与防火墙会话表的老化时间之和。
-

14.4 配置 NAT 日志

表14-5 配置 NAT 日志

操作	命令	说明
进入系统视图	system-view	-
配置 NAT 日志格式	firewall nat log-type { syslog binary }	必选 缺省情况下，NAT 日志以 Syslog 的格式发送
配置二进制流日志主机	firewall binary-log host ip-address [port-number]	必选 当 NAT 日志格式为 binary 时，系统将把 NAT 日志发送到此处配置的日志主机 缺省情况下，端口号为 9002

14.5 日志的清除

在用户视图下，执行 **reset** 命令可清除防火墙的日志缓冲区。

表14-6 日志显示和调试

操作	命令
清除防火墙的日志缓冲区	reset firewall log-buf { defend session statistic http ftp snmp smtp }

14.6 日志典型配置举例

14.6.1 输出攻击防范日志到日志主机

1. 组网需求

将防火墙的以太网口 Ethernet0/0/0 配置为 Trust 域，以太网口 Ethernet1/0/0 配置为 Untrust 域，以太网口 Ethernet2/0/0 配置为 DMZ 区。

2. 组网图

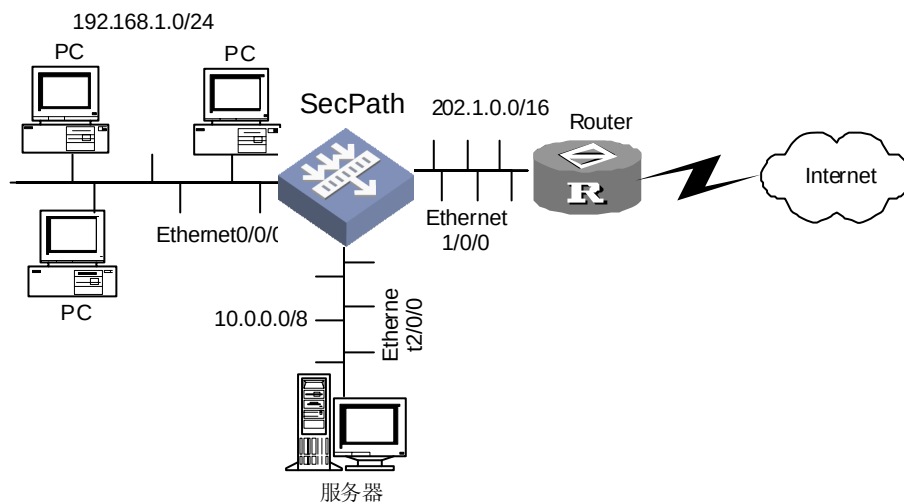


图14-2 防火墙日志功能配置组网图

3. 配置步骤

配置防火墙接口 Ethernet 0/0/0。

```
[H3C] interface Ethernet 0/0/0
```

```
[H3C-Ethernet0/0/0] ip address 192.168.1.1 255.255.255.0
```

配置防火墙接口 Ethernet 1/0/0。

```
[H3C] interface Ethernet 1/0/0
```

```
[H3C-Ethernet1/0/0] ip address 202.1.0.1 255.255.0.0
```

配置防火墙接口 Ethernet 2/0/0。

```
[H3C] interface Ethernet 2/0/0
```

```
[H3C-Ethernet2/0/0] ip address 10.0.0.1 255.0.0.0
```

将接口 Ethernet 0/0/0 加入防火墙 Trust 域。

```
[H3C] firewall zone trust
```

```
[H3C-zone-trust] add interface Ethernet 0/0/0
```

将接口 Ethernet 1/0/0 加入防火墙 Untrust 域。

```
[H3C] firewall zone untrust
```

```
[H3C-zone-untrust] add interface Ethernet 1/0/0
```

将接口 Ethernet 2/0/0 加入防火墙 DMZ 域。

```
[H3C] firewall zone dmz
```

```
[H3C-zone-dmz] add interface Ethernet 2/0/0
```

开启信息中心，配置将日志发送到 IP 地址为 192.168.1.10 的日志主机。

```
[H3C] info-center enable
```

```
[H3C] info-center loghost 192.168.1.10 language english
```


打开攻击防范的端口扫描攻击开关，将攻击的源地址加入黑名单，老化时间设为 10 分钟，并使能黑名单功能。

```
[H3C] firewall defend port-scan max-rate 100 blacklist-timeout 10
```

```
[H3C] firewall blacklist enable
```

使能 Untrust 域的 IP 出方向报文统计。

```
[H3C] firewall zone untrust
```

```
[H3C-zone-untrust] statistic enable ip outzone
```

从 Untrust 域的 PC 机上利用工具（如 nmap）对 Trust 域的服务器进行端口扫描。防火墙将 PC 机的地址加入黑名单，老化时间为 10 分钟，并立即输出加入黑名单的日志信息。在攻击防范的扫描时间到达后，输出 UDP 端口扫描攻击的日志信息。

14.6.2 域间流日志配置举例

1. 组网需求

Server 位于 untrust 区域，PC 位于 trust 区域。在防火墙上使能 trust 域和 untrust 域的域间流日志功能，日志将被发送到 DMZ 区域中的 XLog 日志主机。

2. 组网图

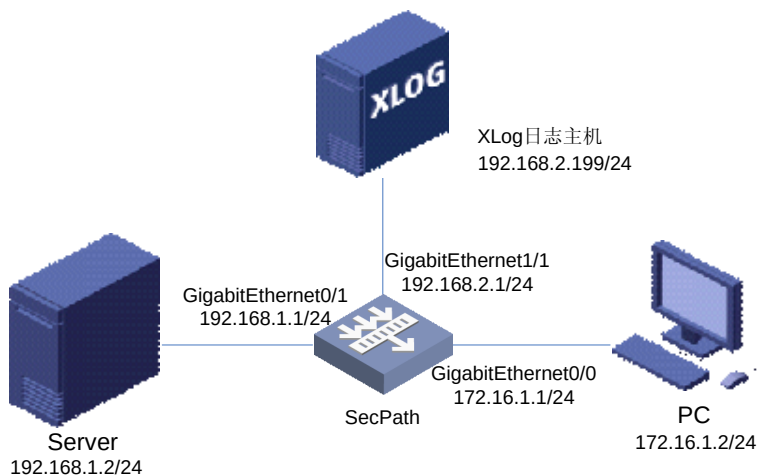


图14-3 防火墙域间流日志功能配置组网图

3. 配置步骤

为接口配置 IP 地址。

```
<H3C> system-view
```

```
[H3C] interface GigabitEthernet 0/0
```

```
[H3C-GigabitEthernet0/0] ip address 172.16.1.1 24
```

```
[H3C-GigabitEthernet0/0] quit
```

```
[H3C] interface GigabitEthernet 0/1
```

```
[H3C-GigabitEthernet0/1] ip address 192.168.1.1 24
```

```
[H3C-GigabitEthernet0/1] quit
[H3C] interface GigabitEthernet 1/1
[H3C-GigabitEthernet1/1] ip address 192.168.2.1 24
[H3C-GigabitEthernet1/1] quit
# 将接口加入域。

[H3C] firewall zone trust
[H3C-zone-trust] add interface GigabitEthernet 0/0
[H3C-zone-trust] quit
[H3C] firewall zone untrust
[H3C-zone-untrust] add interface GigabitEthernet 0/1
[H3C-zone-untrust] quit
[H3C] firewall zone DMZ
[H3C-zone-dmz] add interface GigabitEthernet 1/1
[H3C-zone-dmz] quit
# 进入域间视图并使能域间流日志功能。

[H3C] firewall interzone trust untrust
[H3C-interzone-trust-untrust] session log enable
[H3C-interzone-trust-untrust] quit
# 设置域间流日志格式为二进制格式。

[H3C] firewall session log-type binary
# 设置二进制流日志的日志主机地址。

[H3C] firewall binary-log host 192.168.2.199 9002
```

14.6.3 NAT 日志配置举例

1. 组网需求

Server 位于 untrust 区域，PC 位于 trust 区域。在防火墙上使能 NAT，并对 NAT 进行日志统计，NAT 日志将被发送到 DMZ 区域中的 XLog 日志主机。

2. 组网图

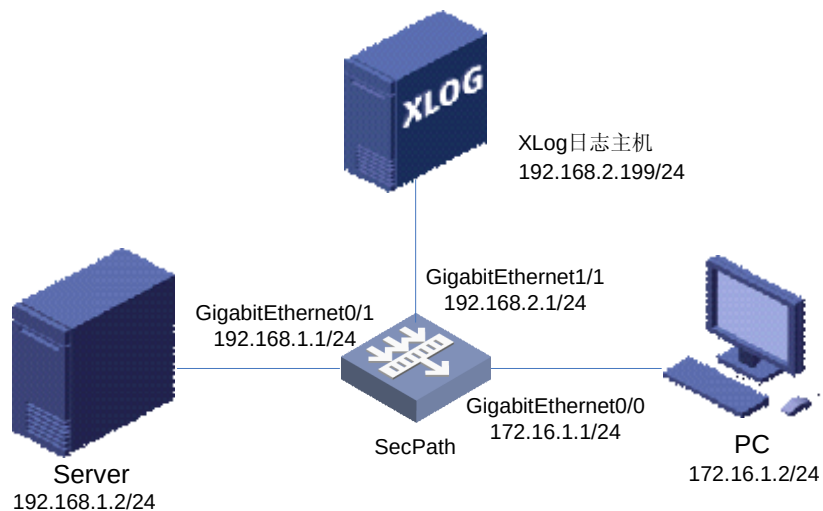


图14-4 防火墙 NAT 日志功能配置组网图

3. 配置步骤

将接口加入域。

```
<H3C> system-view
[H3C] firewall zone trust
[H3C-zone-trust] add interface GigabitEthernet 0/0
[H3C-zone-trust] quit
[H3C] firewall zone untrust
[H3C-zone-untrust] add interface GigabitEthernet 0/1
[H3C-zone-untrust] quit
[H3C] firewall zone DMZ
[H3C-zone-dmz] add interface GigabitEthernet 1/1
[H3C-zone-dmz] quit
```

在 ACL 规则中使能日志功能。

```
<H3C> system-view
[H3C] acl number 3001
[H3C-acl-adv-3001] rule permit ip source 172.16.1.0 0.0.0.255 destination
192.168.1.0 0.0.0.255 logging
[H3C-acl-adv-3001] quit
```

配置 NAT 地址池。

```
[H3C] nat address-group 0 192.168.1.10 192.168.1.20
```

为接口配置 IP 地址并在接口 GigabitEthernet0/1 配置 NAT 功能。

```
[H3C] interface GigabitEthernet 0/0
[H3C-GigabitEthernet0/0] ip address 172.16.1.1 24
```

```
[H3C-GigabitEthernet0/0] quit
[H3C] interface GigabitEthernet 1/1
[H3C-GigabitEthernet1/1] ip address 192.168.2.1 24
[H3C-GigabitEthernet1/1] quit
[H3C] interface GigabitEthernet 0/1
[H3C-GigabitEthernet0/1] ip address 192.168.1.1 24
[H3C-GigabitEthernet0/1] nat outbound 3001 address-group 0
[H3C-GigabitEthernet0/1] quit
# 设置 NAT 日志格式为二进制格式。
[H3C] firewall nat log-type binary
# 设置二进制流日志的日志主机地址。
[H3C] firewall binary-log host 192.168.2.199 9002
```

目 录

第 1 章 VRRP配置.....	1-1
1.1 VRRP简介	1-1
1.2 VRRP配置	1-2
1.2.1 添加或删除虚拟IP地址	1-3
1.2.2 设置备份组的优先级	1-3
1.2.3 设置备份组的抢占方式和延迟时间	1-4
1.2.4 设置认证方式及认证字	1-5
1.2.5 设置VRRP的定时器.....	1-5
1.2.6 设置监视指定接口.....	1-6
1.2.7 设置虚拟IP地址是否可以使用ping命令ping通	1-6
1.2.8 设置是否需要检查VRRP报文的TTL值.....	1-7
1.3 VRRP显示和调试	1-7
1.4 VRRP典型配置举例	1-8
1.4.1 VRRP单备份组举例.....	1-8
1.4.2 VRRP监视接口举例.....	1-9
1.4.3 多备份组举例.....	1-10
1.5 VRRP故障诊断与排错	1-11
第 2 章 双机热备配置	2-1
2.1 双机热备简介	2-1
2.2 双机热备的基本原理	2-1
2.2.1 RDMP	2-1
2.2.2 RDO	2-2
2.2.3 状态协商接口.....	2-3
2.2.4 RCP	2-3
2.2.5 SCP	2-4
2.3 双机热备的特点.....	2-4
2.3.1 支持配置命令和动态表项的备份	2-4
2.3.2 支持防火墙的各种部署方式	2-5
2.4 双机热备配置任务简介	2-5
2.5 创建RDO	2-6
2.5.1 配置准备	2-6
2.5.2 创建RDO	2-6
2.6 配置本端HA接口	2-6
2.6.1 配置准备	2-6
2.6.2 配置本端HA接口	2-6
2.7 配置VIF	2-7

2.7.1 配置准备	2-7
2.7.2 配置VIF.....	2-7
2.8 配置双机热备的调整和优化.....	2-8
2.8.1 配置准备	2-8
2.8.2 配置RDO静态优先级	2-9
2.8.3 配置通告间隔.....	2-9
2.9 双机热备的显示和维护	2-10
2.10 典型配置举例	2-10
2.10.1 网桥模式典型组网应用	2-10
2.10.2 路由模式—主备典型组网应用	2-12

第1章 VRRP 配置

1.1 VRRP 简介

在数据通信过程中，各种软件或硬件错误都可能导致网络连接异常中断，造成数据传输失败。为了避免网络设备或线路出现故障时引起数据通信中断，Comware 系统提供 VRRP（Virtual Router Redundancy Protocol，虚拟路由冗余协议）技术确保在通信线路或设备故障时提供备用方案，从而保障数据通信的畅通，有效增强了网络的强壮性和可靠性。

VRRP 提高网络与外界连接的可靠性，适用于支持组播或广播的局域网（如以太网等）。通过将多台路由器组成一个备份组（也可认为是虚拟路由器）作为本地网络统一的出口网关，而备份组内的路由器对本地网络是透明的。在备份组内有一台路由器处于活动状态，承担报文转发任务，一台路由器处于备份状态并随时接替任务，其余路由器处于监听状态。当处于活动状态的路由器出现故障时，将会由处于备份状态的路由器接替其工作，而其余处于监听状态的路由器将再决定出另一台路由器担任备份工作。这样本地主机就可以不作任何修改地继续工作，极大地提高了通信的可靠性。

通常，一个网络内的所有主机都设置一条缺省路由（如下图所示，10.100.10.1），这样，主机发出的目的地址不在本网段的报文将被通过缺省路由发往路由器 Router，从而实现了主机与外部网络的通信。当路由器出现故障时，本网段内所有以此路由器为缺省路由下一跳的主机将断掉与外部的通信。

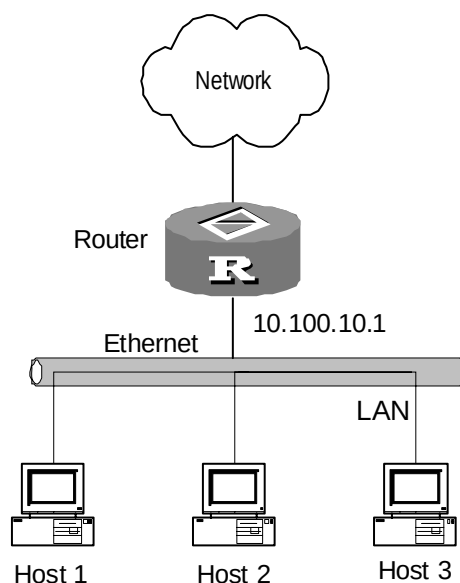


图1-1 局域网组网方案

VRRP 就是为解决上述问题而提出的，它为具有多播或广播能力的局域网（如：以太网）设计。我们结合下图来看一下 VRRP 的实现原理。VRRP 将局域网的一组路由器（包括一个 Master 即活动路由器和若干个 Backup 即备份路由器）组织成一个虚拟路由器，称之为一个备份组。

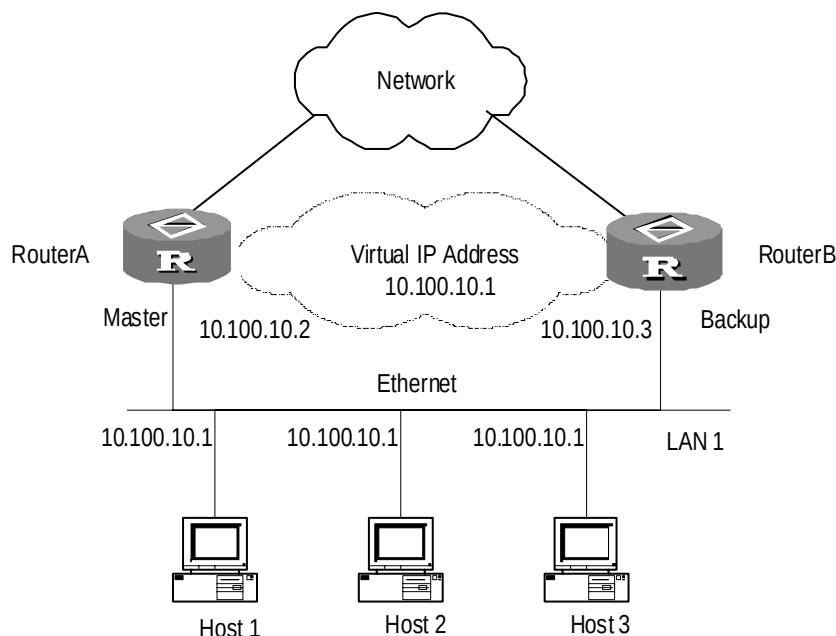


图1-2 VRRP 组网示意图

这个虚拟的路由器拥有自己的 IP 地址 10.100.10.1（这个 IP 地址可以和备份组内的某个路由器的接口地址相同），备份组内的路由器也有自己的 IP 地址（如 Master 的 IP 地址为 10.100.10.2，Backup 的 IP 地址为 10.100.10.3）。局域网内的主机仅仅知道这个虚拟路由器的 IP 地址 10.100.10.1，而并不知道具体的 Master 路由器的 IP 地址 10.100.10.2 以及 Backup 路由器的 IP 地址 10.100.10.3，它们将自己的缺省路由下一跳地址设置为该虚拟路由器的 IP 地址 10.100.10.1。于是，网络内的主机就通过这个虚拟的路由器来与其它网络进行通信。如果备份组内的 Master 路由器出现故障，Backup 路由器将会通过选举策略选出一个新的 Master 路由器，继续向网络内的主机提供路由服务。从而实现网络内的主机不间断地与外部网络进行通信。

关于 VRRP 协议的详细信息，可以参考 RFC 2338。

1.2 VRRP 配置

VRRP 的基本配置包括：

- 添加或删除虚拟 IP 地址
- 设置备份组的优先级
- 设置备份组的抢占方式和延迟时间

VRRP 的高级配置包括：

- 设置备份组的认证方式和认证字
- 设置备份组的定时器
- 设置监视指定接口
- 设置虚拟 IP 地址是否可以使用 ping 命令 ping 通
- 设置检查 VRRP 报文的 TTL 域

1.2.1 添加或删除虚拟 IP 地址

将一个本网段的 IP 地址指定给到一个虚拟路由器（也称为一个备份组），或将一个指定到一个备份组虚拟 IP 地址从虚拟地址列表中删除。

请在接口视图下进行下列配置。

表1-1 添加/删除虚拟 IP 地址

操作	命令
添加虚拟 IP 地址	vrrp vrid <i>virtual-router-ID</i> virtual-ip <i>virtual-address</i>
删除虚拟 IP 地址	undo vrrp vrid <i>virtual-router-ID</i> virtual-ip <i>virtual-address</i>

备份组号 *virtual-router-ID* 范围从 1 到 255，虚拟地址可以是备份组所在网段中未被分配的 IP 地址，也可以是属于备份组某接口的 IP 地址。对于后者，称拥有这个接口 IP 地址的防火墙为一个地址拥有者（IP Address Owner）。当指定第一个 IP 地址到一个备份组时，系统会创建这个备份组，以后再指定虚拟 IP 地址到这个备份组时，系统仅仅将这个地址添加到这个备份组的虚拟 IP 地址列表中。防火墙的一个接口可以同时加入到 14 个备份组中。而一个备份组最多可以配置 16 个虚拟 IP 地址。在对一个备份组进行其它配置之前，必须先通过指定一个虚拟 IP 地址的命令将这个备份组创建起来。

备份组中最后一个虚拟 IP 地址被删除后，这个备份组也将同时被删除掉。也就是这个接口上不再有这个备份组，这个备份组的所有配置都不再有效。

1.2.2 设置备份组的优先级

VRRP 中根据优先级来确定参与备份组的每台防火墙的地位，备份组中优先级最高的防火墙将成为 Master。

优先级的取值范围为 0 到 255（数值越大表明优先级越高），但是可配置的范围最小值是 1，最大值是 254。优先级 0 为系统保留给特殊用途来使用，255 则是系统保留给 IP 地址拥有者。

请在接口视图下进行下列配置。

表1-2 设置备份组的优先级

操作	命令
设置备份组的优先级	vrrp vrid <i>virtual-router-ID</i> priority <i>priority-value</i>
恢复为缺省值	undo vrrp vrid <i>virtual-router-ID</i> priority

缺省情况下，优先级为 100。

 说明：

对于所有 VRRP 组成员，存在配置优先级和运行优先级两种优先级，配置优先级即用 **vrrp vrid** 配置的优先级，非 IP 拥有者的运行优先级与配置优先级是相同的；IP 拥有者的运行优先级是不可配置的，始终为 255。

1.2.3 设置备份组的抢占方式和延迟时间

在非抢占方式下，一旦备份组中的某台防火墙成为 Master，只要它没有出现故障，其它路由器即使随后被配置更高的优先级，也不会成为 Master。如果防火墙设置为抢占方式，它一旦发现自己的优先级比当前的 Master 的优先级高，就会成为 Master，相应地，原来的 Master 将会变成 Backup。

在设置抢占的同时，还可以设置延迟时间。这样可以使得 Backup 延迟一段时间成为 Master。其目的在性能不够稳定的网络中，Backup 可能因为网络堵塞而无法正收到 Master 的报文，使用 **vrrp vrid** 命令配置了抢占延迟时间后，可以避免因网络的短暂故障而导致的备份组内防火墙的状态频繁转换。

延迟的时间以秒计，范围为 0~255。

请在接口视图下进行下列配置。

表1-3 设置和取消备份组的抢占方式和延迟时间

操作	命令
设置备份组的抢占方式和延迟时间	vrrp vrid <i>virtual-router-ID</i> preempt-mode [timer delay <i>delay-value</i>]
取消备份组的抢占方式	undo vrrp vrid <i>virtual-router-ID</i> preempt-mode

缺省方式是抢占方式，延迟时间为 0 秒。

 说明：

取消抢占方式，则延迟时间就会自动变为 0 秒。

1.2.4 设置认证方式及认证字

VRRP 提供了两种认证方式，分别是：

- Simple：简单字符认证。
- MD5：MD5 认证。

在一个安全的网络中，可以采用缺省值，则防火墙对要发送的 VRRP 报文不进行任何认证处理，而收到 VRRP 报文的防火墙也不进行任何认证。

在一个有可能受到安全威胁的网络中，可以将认证方式设置为 Simple，则发送 VRRP 报文的防火墙就会将认证字填入到 VRRP 报文中，而收到的 VRRP 报文的防火墙会将收到的 VRRP 报文中的认证字和本地配置的认证字进行比较，相同则认为是真实的、合法的 VRRP 报文，否则认为是一个非法的报文，将其丢弃。这种情况下，应当设置长度为不超过 8 个字符的认证字。

在一个非常不安全的网络中，可以将认证方式设置为 MD5，则防火墙就会利用 Authentication Header 提供的认证方式和 MD5 算法来对 VRRP 报文进行认证。如果以明文形式输入，长度为 1~8 个字符，如：1234567；如果以密文形式输入，长度必须为 24，并且必须是密文形式，如：_(TT8F]Y\5SQ=^Q`MAF4<1!!。

对于没有通过认证的报文将做丢弃处理，并向网管发送陷阱报文。

请在接口视图下进行下列配置。

表1-4 设置认证方式和认证字

操作	命令
设置认证方式和认证字	vrrp authentication-mode { md5 key simple key }
恢复为缺省值	undo vrrp authentication-mode

缺省认证方式为不进行认证。

 说明：

一个接口上的备份组要设置相同的认证方式和认证字。

1.2.5 设置 VRRP 的定时器

VRRP 备份组中的 Master 防火墙通过定时（*adver-interval*）发送 VRRP 报文来向组内的防火墙通知自己工作正常。如果 Backup 超过一定时间（*master-down-interval*）没有收到 Master 发送来的 VRRP 报文，则认为它已经无法正常工作。同时就会将自己的状态转变为 Master。

用户可以通过设置定时器的命令来调整 Master 发送 VRRP 报文的间隔时间（*adver-interval*）。而 Backup 的 *master-down-interval* 的间隔时间大约是

adver-interval 的 3 倍。如果网络流量过大或者不同的防火墙上的定时器差异等因素，会导致 *master-down-interval* 异常到时而导致状态转换。对于这种情况，可以通过将 *adver-interval* 的间隔时间延长和设置延迟时间的办法来解决。*adver-interval* 的时间单位是秒。

请在接口视图下进行下列配置。

表1-5 设置 VRRP 定时器

操作	命令
设置 VRRP 定时器	vrrp vrid virtual-router-ID timer advertise <i>adver-interval</i>
恢复为缺省值	undo vrrp vrid virtual-router-ID timer advertise

缺省情况下，*adver-interval* 的值是 1 秒，取值范围为 1~255。

1.2.6 设置监视指定接口

VRRP 监视接口功能，更好地扩充了备份功能，即不仅在备份组所在的接口出现故障时提供备份功能，而且在防火墙的其它接口不可用时，也可以使用备份功能。具体做法是通过设置监视某个接口的命令来实现。当被监视的接口 DOWN 时，这个接口的防火墙的运行优先级会自动降低一个数额（*priority-reduced*），于是就会导致备份组内其它防火墙的运行优先级高于这个防火墙的运行优先级，从而使得其它运行优先级高的防火墙转变为 Master，达到对这个接口监视的目的。

请在接口视图下进行下列配置。

表1-6 设置和取消监视接口

操作	命令
设置监视指定接口	vrrp vrid virtual-router-ID track interface-type interface-number [reduced <i>priority-reduced</i>]
取消监视指定接口	undo vrrp vrid virtual-router-ID track [interface-type interface-number]

缺省情况下，*priority-reduced* 的值为 10。

说明：

当防火墙为 IP 地址所有者时，不允许对其进行监视接口的配置。

1.2.7 设置虚拟 IP 地址是否可以使用 ping 命令 ping 通

本配置任务可以使用户能够使用 ping 命令来 ping 通备份组的虚拟 IP 地址。根据 VRRP 的标准协议，备份组的虚拟 IP 地址是无法使用 ping 命令来 ping 通的。这时

防火墙连接的用户无法通过 **ping** 命令来判断一个 IP 地址是否被备份组使用。如果用户将自己的主机 IP 配置与备份组的虚拟 IP 地址相同的 IP 地址，将会使本网段的报文都发送到用户的主机，导致本网段的数据不能被正确转发。

使用下面的命令进行配置后，用户将可以使用 **ping** 命令 ping 通备份组的虚拟 IP 地址。

请在系统视图下进行下列配置。

表1-7 设定虚拟 IP 地址是否可以使用 ping 命令 ping 通

操作	命令
设定虚拟 IP 地址可以使用 ping 命令 ping 通	vrrp ping-enable
设定虚拟 IP 地址不可以使用 ping 命令 ping 通	undo vrrp ping-enable

缺省情况下，用户不能使用 **ping** 命令 ping 通备份组的虚拟 IP 地址。

需要注意的是，此配置需要在备份组建立之前就进行设定。如果防火墙上已经建立了备份组，系统将不允许再进行此配置。

1.2.8 设置是否需要检查 VRRP 报文的 TTL 值

VRRP 协议规定 VRRP 报文的 TTL 值只能为 255。如果 Backup 检查到 VRRP 报文的 TTL 值不是 255，就会将此报文丢弃。

可以使用下面的命令来设置取消检查 VRRP 报文的 TTL 值。

请在接口视图下进行下列配置。

表1-8 设置是否取消检查 VRRP 报文的 TTL 值

操作	命令
设置取消检查 VRRP 报文的 TTL 值	vrrp un-check ttl
设置恢复检查 VRRP 报文的 TTL 值	undo vrrp un-check ttl

缺省情况下，需要检查 VRRP 报文的 TTL 值。

1.3 VRRP 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示 VRRP 配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **debugging vrrp** 命令可以对 VRRP 进行调试。

表1-9 VRRP 显示和调试

操作	命令
显示 VRRP 的状态信息	display vrrp [interface type number [virtual-router-ID]]
使能对 VRRP 报文的调试	debugging vrrp packet
禁止对 VRRP 报文的调试	undo debugging vrrp packet
使能对 VRRP 状态的调试	debugging vrrp state
禁止对 VRRP 状态的调试	undo debugging vrrp state

缺省情况下，VRRP 调试开关关闭。

1.4 VRRP 典型配置举例

1.4.1 VRRP 单备份组举例

1. 组网需求

主机 A 把 SecPathA 和 SecPathB 组成的 VRRP 备份组作为自己的缺省网关，访问 Internet 上的主机 B。

VRRP 备份组构成：备份组号为 1，虚拟 IP 地址为 202.38.160.111，SecPathA 做 Master，SecPathB 做 Backup，允许抢占。

2. 组网图

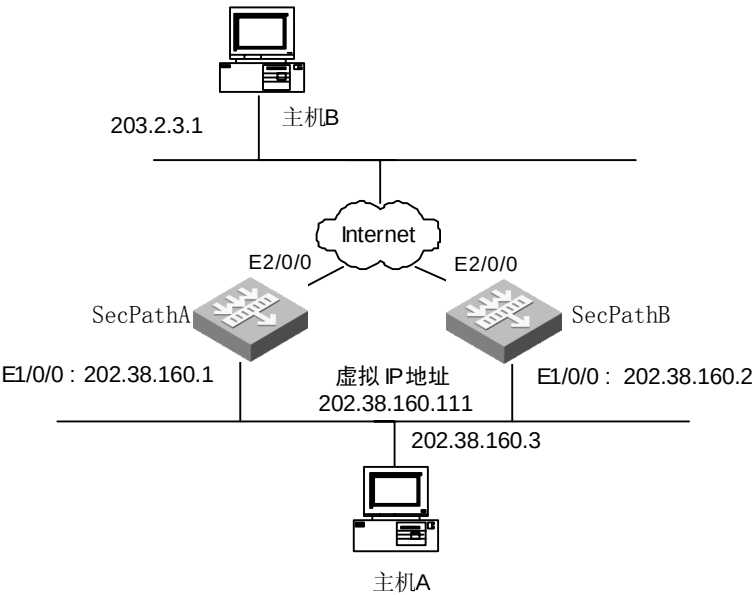


图1-3 VRRP 配置组网图

3. 配置步骤

配置 SecPathA:

```
[H3C-Ethernet1/0/0] ip address 202.38.160.1 24
[H3C-Ethernet1/0/0] vrrp vrid 1 virtual-ip 202.38.160.111
[H3C-Ethernet1/0/0] vrrp vrid 1 priority 120
```

配置 SecPathB:

```
[H3C-Ethernet1/0/0] ip address 202.38.160.2 24
[H3C-Ethernet1/0/0] vrrp vrid 1 virtual-ip 202.38.160.111
```

备份组配置后不久就可以使用。主机 A 可将缺省网关设为 202.38.160.111。

正常情况下，SecPathA 执行网关工作，当 SecPathA 关机或出现故障，SecPathB 将接替执行网关工作。

设置抢占方式，目的是当 SecPathA 恢复工作后，能够继续成为 Master 执行网关工作。

1.4.2 VRRP 监视接口举例

1. 组网需求

即使 SecPathA 仍然工作，但当其连接 Internet 的接口不可用时，可能希望由 SecPathB 来执行网关工作。可通过配置监视接口来实现上述需求。

为了便于说明，设备备份组号为 1，并增加授权字和计时器的配置（在该应用中不是必须的）。

2. 组网图

如图 1-3。

3. 配置步骤

配置 SecPathA:

创建一个备份组。

```
[H3C-Ethernet1/0/0] vrrp vrid 1 virtual-ip 202.38.160.111
```

设置备份组的优先级。

```
[H3C-Ethernet1/0/0] vrrp vrid 1 priority 120
```

设置备份组的认证字。

```
[H3C-Ethernet1/0/0] vrrp authentication-mode md5 vrrppwd
```

设置 Master 发送 VRRP 报文的间隔时间为 5 秒。

```
[H3C-Ethernet1/0/0] vrrp vrid 1 timer advertise 5
```

设置监视接口。

```
[H3C-Ethernet1/0/0] vrrp vrid 1 track Ethernet2/0/0 reduced 30
```

配置 SecPathB:

创建一个备份组。

```
[H3C-Ethernet1/0/0] vrrp vrid 1 virtual-ip 202.38.160.111
```

设置备份组的认证字。

```
[H3C-Ethernet1/0/0] vrrp authentication-mode md5 vrrppwd
```

设置 Master 发送 VRRP 报文的间隔时间为 5 秒。

```
[H3C-Ethernet1/0/0] vrrp vrid 1 timer advertise 5
```

正常情况下，SecPathA 执行网关工作，当 SecPathA 的接口 Ethernet2/0/0 不可用时，SecPathA 的优先级降低 30，低于 SecPathB 优先级，SecPathB 将抢占成为 Master 执行网关工作。

当 SecPathA 的接口 Ethernet2/0/0 恢复工作后，SecPathA 能够继续成为 Master 执行网关工作。

1.4.3 多备份组举例

1. 组网需求

在 Comware 中，允许一台防火墙为多个备份组作备份。

通过多备份组设置可以实现负荷分担。如 SecPathA 作为备份组 1 的 Master，同时又兼职备份组 2 的 Backup，而 SecPathB 正相反，作为备份组 2 的 Master，并兼职备份组 1 的 Backup。一部分主机使用备份组 1 作网关，另一部分主机使用备份组 2 作为网关。这样，以达到分担数据流，而又相互备份的目的。

2. 组网图

如图 1-3。

3. 配置步骤

配置 SecPathA:

创建一个备份组 1。

```
[H3C-Ethernet1/0/0] vrrp vrid 1 virtual-ip 202.38.160.111
```

设置备份组的优先级。

```
[H3C-Ethernet1/0/0] vrrp vrid 1 priority 120
```

创建一个备份组 2。

```
[H3C-Ethernet1/0/0] vrrp vrid 2 virtual-ip 202.38.160.112
```

配置 SecPathB:

创建一个备份组 1。


```
[H3C-Ethernet1/0/0] vrrp vrid 1 virtual-ip 202.38.160.111
```

创建一个备份组 2。

```
[H3C-Ethernet1/0/0] vrrp vrid 2 virtual-ip 202.38.160.112
```

设置备份组的优先级。

```
[H3C-Ethernet1/0/0] vrrp vrid 2 priority 120
```

1.5 VRRP 故障诊断与排错

VRRP 配置不是很复杂，如果功能不正常，基本可以通过查看配置以及调试信息来定位。以下，就如何排除常见的故障加以说明。

故障之一：控制台上频频给出配置错误的提示

这表明收到一个错误的 VRRP 报文，一种可能是备份组内的另一台防火墙由于配置不一致造成的，另一种可能是有的机器试图发送非法的 VRRP 报文。对于第一种可能，可以通过修改配置来解决。对于第二种可能，则是有些设备有不良企图，应当通过非技术手段来解决。

故障之二：同一个备份组内出现多个 Master 防火墙

这分为两种情况，一种是多个 Master 并存时间较短，这种情况是正常的。无需进行人工干预。另一种是多个 Master 长时间共存，这很有可能是由于 Master 收不到 VRRP 报文，或者收到的报文不合法造成的。

解决的方法是，先在多个 Master 之间互相 ping，如果 ping 不通，则是其它问题。如果能 ping 通，则一定是配置不同造成的，对于同一个 VRRP 备份组的配置，必须要保证虚拟 IP 地址个数、每个虚拟 IP 地址、定时器间隔时间和认证方式完全一样。

故障之三：VRRP 的状态频繁转换

这种情况一般是由于备份组的定时器间隔时间（*adver-interval*）设置太短造成的，加大这个时间间隔或者设置抢占延迟都可以解决这种故障。

第2章 双机热备配置

2.1 双机热备简介

双机热备就是双机状态备份，即部署两台防火墙，通过冗余设备管理协议（RDMP，Redundancy Device Management Protocol）完成防火墙的主备状态的协商。在确定主备防火墙后，由主防火墙进行业务的转发，而备防火墙处于监控状态，同时主防火墙会定时向备防火墙发送状态信息和需要备份的信息。当主防火墙出现故障后，备防火墙会及时接替主防火墙上的业务。

在流量传输过程中，根据两个防火墙的主备状态选择采用哪一条虚拟通路进行业务传输。当主用通路出现故障后，防火墙的主备状态会自动进行切换，并且会将业务引导到另一个防火墙上进行正常传输，从而保障了业务的不间断性。

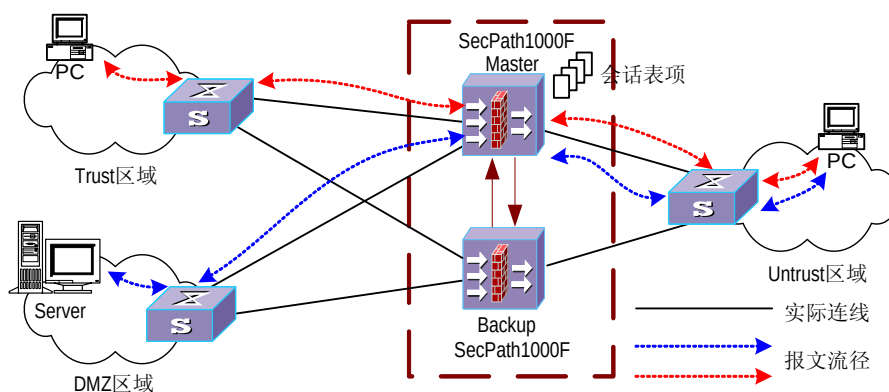


图2-1 双机热备方案

状态备份最主要的优点是可以保护当前业务不会中断，例如语音电话等业务。如果防火墙不具备状态备份功能，状态切换后，当前活动的业务就会中断，只有重新进行连接。采用双机热备组网方案可以很好地解决传统组网方案（例如 VRRP 等）的缺陷。

2.2 双机热备的基本原理

2.2.1 RDMP

防火墙采用 RDMP（Redundancy Device Management Protocol，冗余设备管理协议）协议实现防火墙的双机热备。通过在两个防火墙之间运行 RDMP 协议，可以保证在主设备发生故障的情况下，业务被自动引导到备份设备上继续处理。同时，RDMP 协议还支持主备设备之间的连接状态、地址转换信息、配置信息等数据的同

步。通过对状态信息进行备份，可以避免流量在切换到备份设备后，先前已经建立的业务中断。

RDMP 由两个协议组成：

- RCP（Redundancy link Control Protocol，冗余链路控制协议）：用于两台物理设备之间的主备状态协商、底层链路状态管理；
- SCP（Synchronization Control Protocol，数据同步控制协议）：用于完成两台设备之间的状态信息备份和恢复。

2.2.2 RDO

RDMP 引入了 RDO（Redundancy Device Object，冗余设备对象）和 VIF（Virtual Interface，虚拟接口）的概念。

RDO 是抽象的虚拟设备，区别于真实的物理设备。两个相同 ID 的 RDO 对外呈现为一个具有完整业务功能的设备实体。只有 RDO 状态为 Master 的防火墙处理业务流量，完成防火墙的过滤、地址转换、转发等业务功能。

VIF 是虚拟设备中处理业务数据的实体（具有实际的 IP 地址），同时它绑定的接口的状态也会直接影响到设备 RDO 的状态。每个 RDO 和真实设备一样拥有多个虚拟接口（VIF）用来处理业务，必须为每个虚拟接口指定其对应的真实的接口。

物理设备和冗余设备之间的逻辑关系如图 2-2 所示。

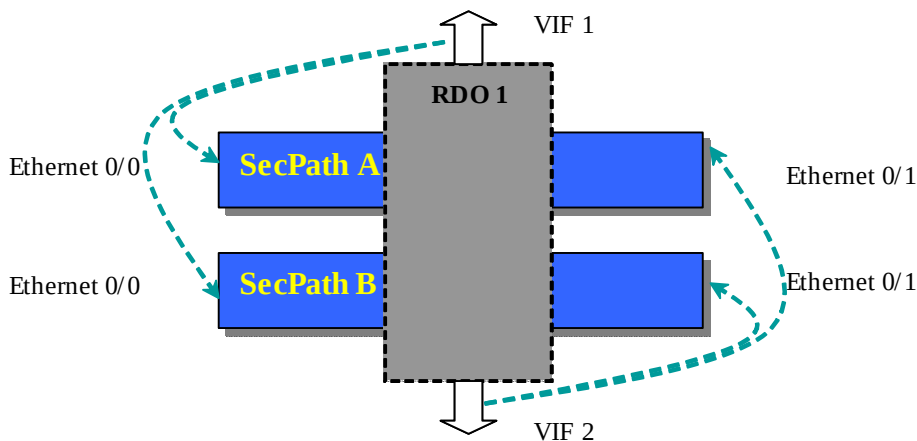


图2-2 物理设备和冗余设备对象的逻辑关系图

在图 2-2 中，SecPath A 和 SecPath B 分别运行 RDMP，通过各自配置的 RDO 1，并且将 RDO 1 中的 VIF 1 和两台设备的 Ethernet 0/0 绑定，VIF 2 和两台设备的 Ethernet 0/1 绑定，这样就形成了一个具有两个接口的虚拟设备（RDO 1）。

2.2.3 状态协商接口

RDMP 采用标准的以太网接口作为状态协商的接口（HA Interface），用来在互为主备的两台防火墙之间传输协商报文以及其它数据。

2.2.4 RCP

在 RDMP 中，RCP 主要用于两台物理设备之间的主备状态协商、底层链路状态管理。

通过比较两台设备之间 RDO 的实时优先级决定 RDO 的主备状态，优先级高的为主设备。如果优先级相同，再比较双方 HA 接口的 MAC 地址，MAC 地址大的为主设备。

实时优先级是由设备上配置的 RDO 静态优先级、该 RDO 中每个 VIF 的权值以及该 RDO 中每个 VIF 对应的接口状态决定的。具体计算方法为：

$\text{RDO 的实时优先级} = \text{RDO 静态优先级} - \text{所有 DOWN 状态的 VIF 的权值}$ 。

例如，在防火墙A上，RDO 1 配置的静态优先级为 100，VIF状态如表 2-1所示。

表2-1 防火墙 A 状态表

VIF	对应的接口	权值	接口状态
VIF1	Ethernet 0/0/0	20	UP
VIF2	Ethernet 0/0/1	10	UP
VIF3	Ethernet 1/0/0	10	DOWN

根据上面的计算公式，防火墙 A 上的 RDO 1 实时优先级应该是 90。

在防火墙B上，RDO 1 配置的静态优先级为 100，VIF状态如表 2-2所示。

表2-2 防火墙 B 状态表

VIF	对应的接口	权值	接口状态
VIF1	Ethernet 0/0/0	20	UP
VIF2	Ethernet 0/0/1	10	UP
VIF3	Ethernet 1/0/0	10	UP

根据上面的计算公式，防火墙 B 上的 RDO 1 实时优先级应该是 100。

两台设备之间通过周期发送协商报文实现主备协商。协商报文中携带了本端的实时优先级信息，在对端收到协商报文后，把报文中的优先级和本端优先级进行比较，确定本设备的状态。在上面的例子中，防火墙 B 上的 RDO 1 的状态为 Master，而防火墙 A 上的 RDO 1 为 Backup。

2.2.5 SCP

在 RDMP 中，SCP 主要用于完成两台设备之间的状态信息备份和恢复，同时也保证了同步过程中的数据传输错误处理。

数据同步包括了数据的批量同步和实时同步两个过程：

- 批量同步通常发生在一台备份设备刚刚加入到网络中的时候，主设备会向备份设备同步自己保存的各种状态数据和相关配置。
- 实时同步通常发生在完成了批量同步之后，此时 SCP 进入稳定同步状态。在这个阶段，SCP 会将主设备上新创建、更新、删除的状态数据实时的备份到备份设备上。

2.3 双机热备的特点

2.3.1 支持配置命令和动态表项的备份

由于 SecPath 系列防火墙是状态防火墙，当首包通过检测后，会在安全区域之间形成动态的会话表项，只有命中该会话表项的后续报文（包括返回报文）才能够通过 SecPath 防火墙。这样就要求会话的进路径和出路径必须一致。因此只有保障了主备防火墙的状态一致性，才能在状态发生切换后业务不会中断。

双机热备的备份方式：

- 自动实时备份：当形成动态备份信息时，主设备自动将该动态数据备份到备份设备。
- 自动批量备份：当备份设备接入到网络中或重新启动时，主设备将所有配置命令和动态备份信息批量备份到备份设备，备份设备将执行需要进行双机备份的配置命令，以实现主备设备的配置同步。
- 手动批量同步：在主设备上输入配置同步命令，将主设备上的需要双机备份的配置命令和动态备份信息发送到备份设备。

 说明：

- 双机热备不支持 NAT Easy IP 特性和将防火墙接口地址作为 NAT 全局地址的情况。
- 批量备份过程中，在主备未达到稳态（即主备批量备份未完成）时，不允许执行任何操作。
- 采用手动批量同步方式时，如果在主设备上连续不断的输入配置同步命令，将会导致备份设备的表项异常。
- 主备切换的情况下，主备切换时间间隔为主备切换过程中原有连接中断时间。该时间仅与 `ad-interval` 时间，以及接口状态轮询时间（5 秒）有关。
- 主备切换的情况下，主备切换达到稳态的时间应该等于通告时间的超时时间加上切换后配置及状态信息同步完成的时间之和。该时间和需要恢复的配置文件的大小、表项的多少，以及当时 CPU 的占用率有关。恢复的时长随着需要恢复的资源多少而递增。
- 双机热备不支持 TCP-Proxy 和流日志，即开启双机热备功能后，TCP-Proxy 和流日志功能将不生效。
- 通过命令行手工配置的黑名单表项，只能通过自动批量备份和手动批量备份进行同步，这些表项不能自动实时备份到备份设备。
- 为了保证主备业务的正常进行，主备状态信息需要保证一致。因此，在有业务流量的情况下，不要在备机上执行 `reset nat session` 命令。
- 此外，在有数据业务的情况下，执行 `scp batch-sync config` 命令会清除备机的状态信息，如果此时需要同步配置，应该执行 `scp batch-sync all` 命令。

2.3.2 支持防火墙的各种部署方式

SecPath 系列防火墙支持路由模式和网桥模式两种方式的组网。针对这两种防火墙的部署方式，RDMP 协议都能够很好的支持防火墙的备份，从而在保证系统可靠性的同时，继续保持了现有防火墙组网灵活的特点。

2.4 双机热备配置任务简介

表2-3 双机热备配置任务简介

配置任务		说明	详细配置
创建 RDO		必选	2.5
配置本端 HA 接口		必选	2.6
配置 VIF		必选	2.7
配置双机热备的调整和优化	配置 RDO 静态优先级	可选	2.8.2
	配置通告间隔	可选	2.8.3

2.5 创建 RDO

在配置双机热备之前，必须先在每台设备上创建 RDO，这样才能够配置其它功能并使其生效。

2.5.1 配置准备

完成本配置无需任何配置准备。

2.5.2 创建 RDO

表2-4 创建 RDO

操作	命令	说明
进入系统视图	system-view	-
创建 RDO，并进入 RDO 视图	rdo rdo-id	必选



注意：

互为主备状态的两个设备之间的 RDO ID 号必须一致。

2.6 配置本端 HA 接口

2.6.1 配置准备

在配置本端 HA 接口之前，需完成以下任务：

- 本端设备已创建 RDO

2.6.2 配置本端 HA 接口

本端和对端防火墙需要使用 HA 接口协商双方的主备状态并同步配置命令和状态信息。

表2-5 配置本端 HA 接口

操作	命令	说明
进入系统视图	system-view	-
进入 RDO 视图	rdo rdo-id	必选

操作	命令	说明
配置本端 HA 接口	ha-interface interface <i>interface-name</i> [peer-mac <i>mac-address</i>]	必选 可以通过 peer-mac 参数指定对端 HA 接口的 MAC 地址。若不指定，则使用广播 MAC 地址 FFFF-FFFF-FFFF

**注意：**

- 双机热备的协商报文和业务同步数据都使用 HA 接口进行传输，这些报文不同于普通报文，因此防火墙的防火墙模块（如黑名单、包过滤等）对这些报文不起作用。
- HA 接口必须为物理接口。
- 如果 HA 接口的物理状态为 DOWN 时，RDO 状态在设备重新启动后会停止在 Init 状态。因此，请在双机热备环境中，始终保持 HA 接口的物理状态为 UP。
- 如果 HA 接口的物理状态为 DOWN 时，会导致主备设备的状态都为 Master，这时两台设备都将响应 ARP 报文，进行数据转发，导致业务不能正常运行。因此，请在双机热备环境中，始终保持 HA 接口的物理状态为 UP。
- HA 接口不能与实际的业务接口复用。
- 主备设备间的 HA 接口需使用线缆直接相连。

2.7 配置 VIF

本节主要介绍配置防火墙的虚拟接口及其所绑定的接口等。完成以下配置任务后，两台互为主备的防火墙就能够对外提供服务，保证业务的正常运转。

2.7.1 配置准备

在配置 VIF 之前，需完成以下任务：

- 对于路由模式，需配置主备防火墙上被绑定的业务接口的 IP 地址，使主备防火墙两端的两台设备之间路由可达
- 本端和对端设备均已创建 RDO

2.7.2 配置 VIF

配置虚拟接口包括配置接口的虚拟 IP 地址、接口权值和虚拟 MAC 地址。

当防火墙工作在路由模式下时，主备设备上互为备份的业务接口必须配置相同的虚拟接口 ID、虚拟 IP 地址和虚拟 MAC 地址。虚拟 IP 地址必须与接口的真实 IP 地址

在同一网段，但是不能与接口的真实 IP 地址相同。虚拟 MAC 地址不能与接口的真实 MAC 地址相同。

当防火墙工作在网桥模式下时，不能配置虚拟 IP 地址和虚拟 MAC 地址。

接口权值用于动态更新优先级，当接口 DOWN/UP 的时候，系统根据权值对 RDO 实时优先级进行调整。

表2-6 配置 VIF

操作	命令	说明
进入系统视图	system-view	-
进入 RDO 视图	rdo rdo-id	必选
路由模式下配置 VIF	vif vif-id interface type number virtual-ip ip-address [virtual-mac H-H-H] [reduce value-reduced]	必选 缺省情况下， <i>value-reduced</i> 的值为 10
网桥模式下配置 VIF	vif vif-id interface type number [reduce value-reduced]	必选 缺省情况下， <i>value-reduced</i> 的值为 10



注意：

- 虚拟接口不能重复配置，必须首先用 **undo** 命令取消掉原来的配置，才能重新配置。
- 虚拟接口的地址不能与被绑定接口的地址相同。
- 接口绑定 VIF 后，修改 VIF 所对应的接口 IP 地址，设备不进行 VIF 接口的 IP 地址合法性检测。
- 批量备份过程中不能用 **undo** 命令取消虚拟接口。
- 为了保证 RDO 的实时优先级为正值，在一个 RDO 下每个绑定接口的权值（*value-reduced*）总和不能大于或等于对应 RDO 的静态优先级。
- 当使能了双机热备功能后，请不要配置并使用 VRRP，否则会导致双机热备功能异常。

2.8 配置双机热备的调整和优化

本节主要介绍怎样调整和优化双机热备，使其能够适应不同的网络需求。包括配置 RDO 的静态优先级和通告间隔等。

2.8.1 配置准备

在调整和优化双机热备之前，需完成以下任务：

- 对于路由模式，需配置主备防火墙上被绑定的业务接口的 IP 地址，使主备防火墙两端的两台设备之间路由可达
- 本端和对端设备均已创建 RDO

2.8.2 配置 RDO 静态优先级

RDO 静态优先级是指设备的接口全部为 UP 状态时的 RDO 的优先级。根据静态优先级与各接口的实际状态、权值可以计算出 RDO 的实时优先级。通过比较 RDO 的实时优先级可以确定设备之间的主备关系，优先级数值高的为 Master。

表2-7 配置 RDO 静态优先级

操作	命令	说明
进入系统视图	system-view	-
进入 RDO 视图	rdo rdo-id	必选
配置 RDO 静态优先级	priority value	必选 缺省情况下，静态优先级为 100

说明：

若本端和对端的实时优先级相等，则根据双方 HA 接口的 MAC 地址确定主备关系，MAC 地址大的为 Master。

2.8.3 配置通告间隔

一个 RDO 中的主设备会定期发送抑制报文，通知备份设备自己处于正常工作的状态，并且通告自己的优先级。备份设备根据通告时间间隔确定收到抑制报文的超时时间，如果连续三次未收到抑制报文则认为主设备已经出现故障，并进行状态切换。

表2-8 配置通告间隔

操作	命令	说明
进入系统视图	system-view	-
进入 RDO 视图	rdo rdo-id	必选
配置通告间隔	ad-interval time-value	必选 缺省情况下，通告间隔为 3 秒

**注意：**

- 由于不同型号产品的硬件性能差异，以及设备在实际应用中的业务量大小等因素，双机热备中的备机在批量备份与恢复过程中可能会不能及时处理主机发来的通告报文，从而导致主备设备无法达到稳定同步状态，发生主备频繁切换的异常现象，可以通过配置更大的通告时间间隔来避免此现象。建议用户配置的通告时间间隔大于或等于 3 秒，以防止上述问题发生。
- 当实际应用中存在较大流量或较多会话，或配置文件较大时，建议用户增加通告时间间隔，以保证双机热备功能正常运行。
- 本端和对端需设置相同的通告间隔。

2.9 双机热备的显示和维护

完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后双机热备的运行情况，通过查看显示信息验证配置的效果。

表2-9 双机热备的显示和维护

操作	命令
显示所有 RDO 的全局信息	display rdo
显示指定 RDO 的详细信息	display rdo rdo-id
显示双机热备同步模块的信息	display rdo sync-modules

说明：

在主备设备切换的过程中，如果打开了信息中心的日志开关，可能会导致主/备设备在黑名单配置或其它配置恢复时，用户终端上打印信息过多而影响正常操作。可以通过命令 **undo info-center enable** 关闭信息中心的日志开关来避免此类问题。

2.10 典型配置举例

2.10.1 网桥模式典型组网应用

1. 组网需求

- 防火墙 SecPathA 和 SecPathB 工作在网桥模式下。
- SecPathA 和 SecPathB 启用双机热备，保证业务的不间断运行。
- 两台防火墙的 HA 接口都为各自的 E0/0/1 接口。

- 在正常情况下，业务流量都通过 SecPathA 转发，SecPathB 监控 SecPathA 的状态。
- 假设 SecPathA 的 Ethernet0/0/1 接口的 MAC 地址为 0001-0001-0001，SecPathB 的 Ethernet0/0/1 接口的 MAC 地址为 0002-0002-0002。

2. 组网图

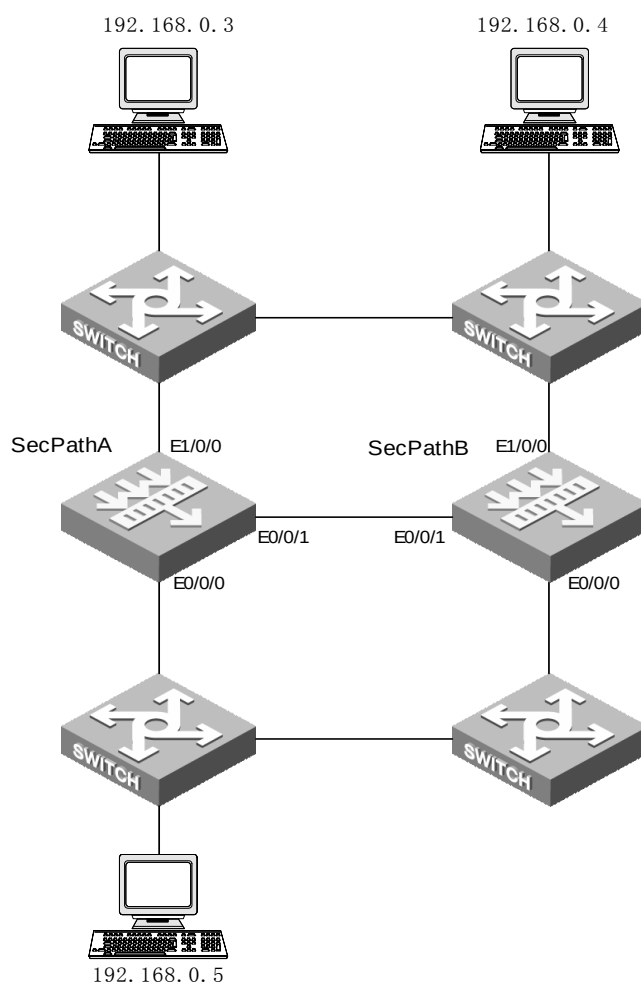


图2-3 网桥模式下双机热备组网图

3. 配置步骤

(1) 配置 SecPathA

配置防火墙使能网桥功能，并使能桥组 1。

```
<SecPathA> system-view
[SecPathA] bridge enable
[SecPathA] bridge 1 enable
```

将接口加入到桥组。

```
[SecPathA] interface Ethernet 0/0/0
```

```
[SecPathA-Ethernet0/0/0] bridge-set 1
[SecPathA-Ethernet0/0/0] quit
[SecPathA] interface Ethernet 1/0/0
[SecPathA-Ethernet1/0/0] bridge-set 1
[SecPathA-Ethernet1/0/0] quit
# 创建冗余设备对象 RDO 1。

[SecPathA] rdo 1
[SecPathA-rdo1] priority 105
[SecPathA-rdo1] ha-interface interface Ethernet 0/0/1 peer-mac 0002-0002-0002
[SecPathA-rdo1] vif 1 interface Ethernet0/0/0
[SecPathA-rdo1] vif 2 interface Ethernet1/0/0
```

(2) 配置 SecPathB

配置防火墙使能网桥功能，并使能桥组 1。

```
<SecPathB> system-view
[SecPathB] bridge enable
[SecPathB] bridge 1 enable
```

将接口加入到桥组。

```
[SecPathB] interface Ethernet 0/0/0
[SecPathB-Ethernet0/0/0] bridge-set 1
[SecPathB-Ethernet0/0/0] quit
[SecPathB] interface Ethernet 1/0/0
[SecPathB-Ethernet1/0/0] bridge-set 1
[SecPathB-Ethernet1/0/0] quit
# 创建冗余设备对象 RDO 1。

[SecPathB] rdo 1
[SecPathB-rdo1] ha-interface interface Ethernet 0/0/1 peer-mac 0001-0001-0001
[SecPathB-rdo1] vif 1 interface Ethernet0/0/0
[SecPathB-rdo1] vif 2 interface Ethernet1/0/0
```

2.10.2 路由模式一主备典型组网应用

1. 组网需求

- 防火墙 SecPathA 和 SecPathB 工作在路由模式下。
- PC1 和 PC2 之间路由可达。
- SecPathA 和 SecPathB 启用双机热备，两台防火墙上均配置一个 RDO。
- 两台防火墙的 HA 接口都为各自的 E1/0/0 接口。
- 在正常情况下，PC1 和 PC2 访问的业务流量都通过 SecPathA 转发，SecPathB 监控 SecPathA 的状态。

- 当 SecPathA 或者链路出现故障，比如 SecPathA 脱机或者相连的上下行链路故障等，业务流量都会自动切换到 SecPathB，通过 SecPathB 转发。
- 假设 SecPathA 的 Ethernet1/0/0 接口的 MAC 地址为 0001-0001-0001，SecPathB 的 Ethernet1/0/0 接口的 MAC 地址为 0002-0002-0002。

2. 组网图

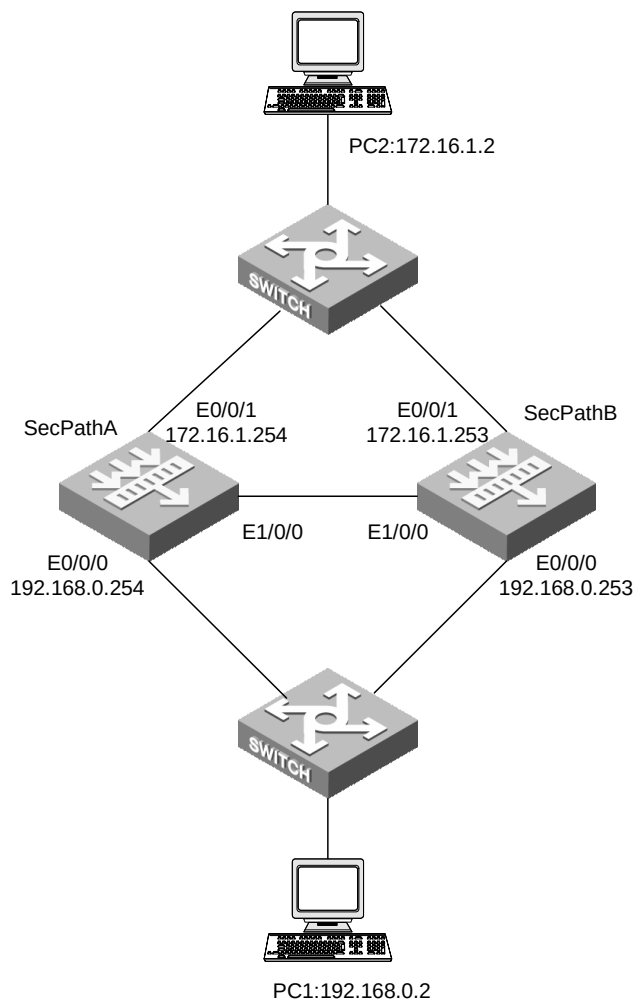


图2-4 配置双机热备路由模式-主备方式组网图

3. 配置步骤

(1) 配置 SecPathA

配置 SecPathA 的接口地址。

```
[SecPathA] interface Ethernet 0/0/0
[SecPathA-Ethernet0/0/0] ip address 192.168.0.254 24
[SecPathA-Ethernet0/0/0] quit
[SecPathA] interface Ethernet 0/0/1
[SecPathA-Ethernet0/0/1] ip address 172.16.1.254 24
```

```
[SecPathA-Ethernet0/0/1] quit
[SecPathA]
```

创建冗余设备对象 RDO 1。

```
[SecPathA] rdo 1
[SecPathA-rdo1] priority 105
[SecPathA-rdo1] ha-interface interface Ethernet 1/0/0 peer-mac 0002-0002-0002
[SecPathA-rdo1] vif 1 interface Ethernet 0/0/0 virtual-ip 192.168.0.1
[SecPathA-rdo1] vif 2 interface Ethernet 0/0/1 virtual-ip 172.16.1.1
```

(2) 配置 SecPathB

配置 SecPathB 的接口地址。

```
[SecPathB] interface Ethernet 0/0/0
[SecPathB-Ethernet0/0/0] ip address 192.168.0.253 24
[SecPathB-Ethernet0/0/0] quit
[SecPathB] interface Ethernet 0/0/1
[SecPathB-Ethernet0/0/1] ip address 172.16.1.253 24
[SecPathB-Ethernet0/0/1] quit
[SecPathB]
```

创建冗余设备对象 RDO 1。

```
[SecPathB] rdo 1
[SecPathB-rdo1] ha-interface interface Ethernet 1/0/0 peer-mac 0001-0001-0001
[SecPathB-rdo1] vif 1 interface Ethernet 0/0/0 virtual-ip 192.168.0.1
[SecPathB-rdo1] vif 2 interface Ethernet 0/0/1 virtual-ip 172.16.1.1
```

(3) PC1 配置

IP 地址：192.168.0.2

网关：192.168.0.1

(4) PC2 配置

IP 地址：172.16.1.2

网关：172.16.1.1

目 录

第 1 章 QoS简介	1-1
1.1 概述	1-1
1.2 传统的分组投递业务	1-1
1.3 新业务引发的新需求	1-1
1.4 拥塞的产生、影响和对策	1-2
1.4.1 拥塞的产生	1-2
1.4.2 拥塞的影响	1-2
1.4.3 对策	1-3
1.5 几种主要的流量管理技术	1-3
第 2 章 流分类、流量监管和流量整形	2-1
2.1 流分类简介	2-1
2.2 流量监管和流量整形简介	2-1
2.2.1 流量评估与令牌桶	2-2
2.2.2 流量监管	2-3
2.2.3 流量整形	2-3
2.2.4 物理接口限速	2-4
2.3 流量监管和流量整形配置	2-5
2.3.1 流量监管配置	2-5
2.3.2 流量整形配置	2-7
2.3.3 接口限速配置	2-7
2.4 流量监管与流量整形显示和调试	2-7
2.4.1 显示TP规则	2-7
2.4.2 显示接口的TP配置情况和统计信息	2-8
2.4.3 显示接口的TS配置情况和统计信息	2-8
2.4.4 显示接口的LR配置情况和统计信息	2-8
2.5 流量监管与流量整形典型配置举例	2-9
第 3 章 拥塞管理	3-1
3.1 拥塞管理简介	3-1
3.1.1 拥塞管理策略	3-1
3.1.2 拥塞管理技术的对比	3-5
3.2 先进先出队列的配置	3-6
3.2.1 配置FIFO队列的长度	3-7
3.3 优先队列的配置	3-7
3.3.1 配置优先列表	3-7
3.3.2 在接口上应用优先列表组	3-9

3.3.3 优先队列的显示和调试	3-9
3.4 定制队列的配置	3-9
3.4.1 配置定制列表	3-10
3.4.2 在接口上应用定制列表	3-12
3.4.3 定制队列的显示和调试	3-12
3.5 加权公平队列的配置	3-12
3.5.1 在接口上应用加权公平队列	3-12
3.5.2 加权公平队列的显示和调试	3-13
3.6 基于类的队列的配置	3-13
3.6.1 配置接口最大可用带宽	3-14
3.6.2 定义类并配置其匹配规则	3-15
3.6.3 定义流行为并配置其特性	3-18
3.6.4 配置策略	3-23
3.6.5 应用策略	3-24
3.6.6 基于类的队列的显示和调试	3-24
3.7 RTP优先队列的配置	3-25
3.7.1 在接口上应用RTP队列	3-25
3.7.2 配置最大预留带宽	3-26
3.7.3 RTP报文队列的显示和调试	3-26
3.8 典型配置举例	3-26
3.8.1 优先队列配置举例	3-26
3.8.2 基于类的队列配置举例	3-27
3.8.3 定制队列配置举例	3-29
第4章 DAR配置	4-1
4.1 DAR简介	4-1
4.2 配置DAR	4-1
4.2.1 配置协议的匹配规则	4-1
4.2.2 配置HTTP协议的匹配规则	4-1
4.2.3 配置RTP协议的匹配规则	4-2
4.2.4 配置DAR应用协议的端口号	4-2
4.2.5 重命名用户预定义协议	4-3
4.2.6 使能/关闭DAR的报文统计功能	4-3
4.2.7 配置DAR可识别的最大连接数	4-3
4.3 DAR的显示和调试	4-4
4.4 DAR典型配置举例	4-4
4.4.1 DAR配置举例	4-4
第5章 拥塞避免	5-1
5.1 拥塞避免简介	5-1
5.2 WRED的配置	5-2

5.2.1 使用WRED	5-3
5.2.2 设置WRED计算平均队列长度的指数	5-3
5.2.3 设置WRED各优先级参数	5-3
5.2.4 设置WRED各DSCP参数	5-4
5.3 WRED的显示和调试	5-4
第 6 章 MPLS QoS	6-1
6.1 MPLS QoS概述	6-1
6.2 MPLS QoS配置	6-1
6.2.1 配置MPLS PQ	6-1
6.2.2 配置MPLS CQ	6-2
6.2.3 配置MPLS CBQ	6-3
6.2.4 配置MPLS CAR	6-5
6.3 MPLS QoS典型配置举例	6-6
6.3.1 对同一VPN内的流进行QoS配置	6-6

第1章 QoS 简介

1.1 概述

服务质量 (Quality of Service, 简称 QoS) 是各种存在服务供需关系的场合中普遍存在的概念, 它评估服务方满足客户服务需求的能力。评估通常不是精确的评分, 而是注重分析在什么条件下服务是好的, 在什么情况下还存在着不足, 以便有针对性地作出改进。

在因特网中, QoS 所评估的就是网络投递分组的服务能力。由于网络提供的服务是多样的, 因此对 QoS 的评估可以基于不同方面。通常所说的 QoS, 是对分组投递过程中可为延迟、延迟抖动、丢包率等核心需求提供支持的服务能力的评估。

1.2 传统的分组投递业务

传统的 IP 网络无区别地对待所有的报文, 防火墙处理报文采用的策略是先进先出 FIFO (First In First Out), 它依照报文到达时间的先后顺序分配转发所需要的资源。所有报文共享网络和防火墙的资源, 至于得到资源的多少完全取决于报文到达的时机。这种服务策略称作 Best-Effort (尽力而为), 它尽最大的努力将报文送到目的地, 但对分组投递的延迟、延迟抖动、丢包率和可靠性等需求不提供任何承诺和保证。

传统的 Best-Effort 服务策略只适用于对带宽、延迟性能不敏感的 WWW、文件传输、e-mail 等业务。

1.3 新业务引发的新需求

随着计算机网络的高速发展, 越来越多的网络接入因特网。Internet 无论从规模、覆盖范围和用户数量上都拓展得非常快。越来越多的用户使用 Internet 作为数据传输的平台, 开展各种应用。同样地, 服务提供商也希望通过新业务的开展来增加收益。

除了传统的 WWW、e-mail、FTP 应用外, 用户还尝试在 Internet 上拓展新业务, 比如远程教学、远程医疗、可视电话、电视会议、视频点播等。企业用户也希望通过 VPN 技术, 将分布在各地的分支机构连接起来, 开展一些事务性应用: 比如访问公司的数据库或通过 Telnet 管理远程设备。

这些新业务有一个共同特点, 即对带宽、延迟、延迟抖动等传输性能有着特殊的需求。比如电视会议、视频点播需要高带宽、低延迟和低延迟抖动的保证。事务处理、

Telnet 等关键任务虽然不一定要求高带宽，但非常注重低延迟，在拥塞发生时要求优先获得处理。

新业务的不断涌现对 IP 网络的服务能力提出了更高的要求，用户已不再满足于能够简单地将报文送达目的地，而是还希望在投递过程中得到更好的服务，诸如支持为用户提供专用带宽、减少报文的丢失率、管理和避免网络拥塞、调控网络的流量、设置报文的优先级。所有这些，都要求网络应当具备更为完善的服务能力。

1.4 拥塞的产生、影响和对策

传统网络所面临的服务质量问题，主要是由网络拥塞引起的。所谓拥塞，是指由于供给资源的相对不足而造成服务速率下降（引入了额外的延迟）的一种现象。

1.4.1 拥塞的产生

在因特网分组交换的复杂环境下，拥塞极为常见。以下图中的两种情况为例：

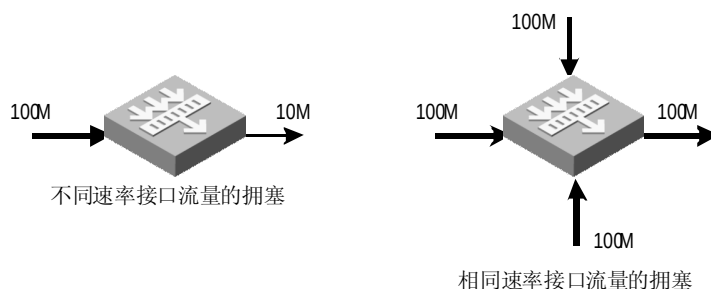


图1-1 流量拥塞示意图

- (1) 分组流从高速链路进入防火墙，由低速链路转发出去。
- (2) 分组流从相同速率的多个接口同时进入防火墙，由一个相同速率的接口转发出去。

如果流量以线速到达，那么就会遭遇资源的瓶颈而导致拥塞。

不仅仅是链路带宽的瓶颈会导致拥塞，任何用以正常转发处理的资源的不足，如可分配的处理器时间、缓冲区、内存资源的不足，都会造成拥塞。此外，在某个时间内对所到达的流量控制不力，使之超出了可分配的网络资源，也是引发网络拥塞的一个因素。

1.4.2 拥塞的影响

拥塞有可能会引发一系列的负面影响：

- 拥塞增加了报文传输的延迟和延迟抖动。
- 过高的延迟会引起报文重传。

- 拥塞使网络的有效吞吐率降低，造成网络资源的损害。
- 拥塞加剧会耗费大量的网络资源（特别是存储资源），不合理的资源分配甚至可能导致系统陷入资源死锁而崩溃。

可见，拥塞使流量不能及时获得资源，是造成服务性能下降的源头。然而在分组交换以及多用户业务并存的复杂环境下，拥塞又是常见的，因此必须慎重加以对待。

 说明：

当发生拥塞后，设备的处理性能会有所下降。当网络的吞吐率降低到 QoS 能够处理的范围内后，设备的处理性能会逐渐恢复正常。

1.4.3 对策

增加网络带宽是解决资源不足的一个直接途径，然而它并不能解决所有导致网络拥塞的问题。

解决网络拥塞问题的一个更有效的办法是增加网络层在流量控制和资源分配上的功能，为有不同服务需求的业务提供有区别的服务，正确地分配和使用资源。在进行资源分配和流量控制的过程中，尽可能地控制好那些可能引发网络拥塞的直接或间接因素，减少拥塞发生的概率；并在拥塞发生时，依据业务的性质及其需求特性权衡资源的分配，将拥塞对 QoS 的影响减到最小。

1.5 几种主要的流量管理技术

流分类、流量监管、流量整形、拥塞管理、拥塞避免和物理接口限速是构造有区别地实施服务的基石，它们主要完成如下功能：

- **流分类：**依据一定的匹配规则识别出对象。流分类是有区别地实施服务的前提。
- **流量监管：**对进入防火墙的特定流量的规格进行监管。当流量超出规格时，可以采取限制或惩罚措施，以保护运营商的商业利益和网络资源不受损害。流量监管是在 IP 层上实现的。
- **拥塞管理：**网络拥塞是必须采取的解决资源竞争的措施。通常是将报文放入队列中缓存，并采取某种调度算法安排报文的转发次序。
- **拥塞避免：**过度的拥塞会对网络资源造成损害。拥塞避免监督网络资源的使用情况，当发现拥塞有加剧的趋势时采取主动丢弃报文的策略，通过调整流量来解除网络的过载。
- **流量整形：**一种主动调整流的输出速率的流控措施，通常是为了使流量适配下游路由器可供的网络资源，避免不必要的报文丢弃和拥塞。流量整形也是在 IP 层上实现的。

- 物理接口限速：与 TP 相比，LR 能够限制在物理接口上通过的所有报文。TP 在 IP 层实现，对于不经过 IP 层处理的报文不起作用。当用户只要求对所有报文限速时，使用 LR 比较简单。

在这些流量管理技术中，流分类是基础，它依据一定的匹配规则识别出报文，是有区别地实施服务的前提；而流量监管、流量整形、拥塞管理和拥塞避免从不同方面对网络流量及其分配的资源实施控制，是有区别地提供服务思想的具体体现。

一般情况下，QoS 执行以下功能：

- 流分类
- 流量监管和流量整形
- 拥塞管理
- 拥塞避免

第2章 流分类、流量监管和流量整形

2.1 流分类简介

流分类采用一定的规则识别符合某类特征的报文，它是有区别地进行服务的前提和基础。

流分类规则可以使用 IP 报文头的 ToS 字段的优先级位，识别出有不同优先级特征的流量；也可以由网络管理者设置流分类的策略，例如综合源地址、目的地址、MAC 地址、IP 协议或应用程序的端口号等信息对流进行分类。一般的分类依据都局限在封装报文的头部信息，使用报文的内容作为分类的标准是比较少见的。分类的结果是没有范围限制的，它可以是一个由五元组（源地址、源端口号、协议号码、目的地址、目的端口号）确定的狭小范围，也可以是到某网段的所有报文。

一般在网络边界对报文分类时，同时设置报文 IP 头的 ToS 字段中的优先级位，这样，在网络的内部就可以直接使用 IP 优先级作为分类标准。而队列技术如 WFQ 也可以使用这个优先级来对报文进行不同的处理。下游（downstream）网络可以选择接收上游（upstream）网络的分类结果，也可以按照自己的标准重新进行分类。

进行流分类是为了有区别地提供服务，它必须与某种流控或资源分配动作关联起来才有意义。具体采取何种流控动作，与所处的阶段以及网络当前的负载状况有关。例如，当报文进入网络时依据承诺速率对它进行监管；流出结点之前进行整形；拥塞时的队列调度管理；拥塞加剧时要采取拥塞避免措施等。

2.2 流量监管和流量整形简介

如果不限制用户发送的流量，那么大量用户不断突发的数据只会使网络更拥挤。为了使有限的网络资源能够更好地发挥效用，更好地为更多的用户服务，必须对用户的流量加以限制。比如限制每个时间间隔某个流只能得到承诺分配给它的那部分资源，防止由于过分突发所引发的网络拥塞。

流量监管和流量整形就是一种通过对流量规格的监督，来限制流量及其资源使用的流控策略。进行流量监管或整形有一个前提条件，就是要知道流量是否超出了规格，然后才能根据评估结果实施调控策略。一般采用令牌桶（Token Bucket）对流量的规格进行评估。

2.2.1 流量评估与令牌桶

1. 令牌桶的特点

令牌桶可以看作是一个存放令牌的容器，它有一定的容量。系统按设定的速度向桶中放置令牌，当桶中令牌满时，多出的令牌溢出，桶中令牌不再增加。

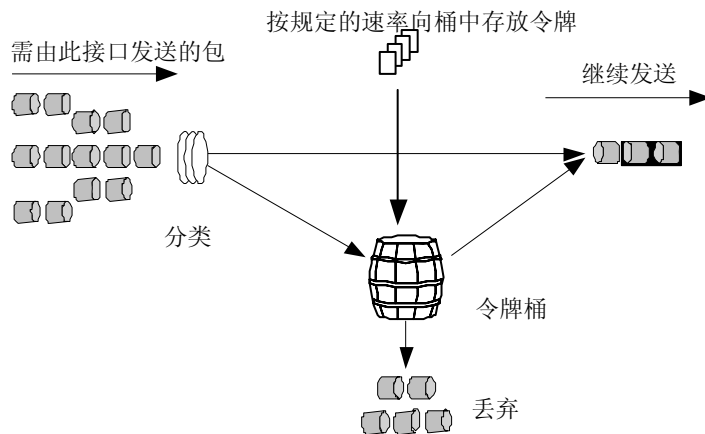


图2-1 用令牌桶评测流量

2. 用令牌桶评估流量

在用令牌桶评估流量规格时，是以令牌桶中的令牌数量是否足够满足报文的转发为依据的。如果桶中存在足够的令牌可以用来转发报文（通常用一个令牌关联一个比特的转发权限），称流量遵守或符合（conform）这个规格，否则称为不符合或超标（excess）。

评估流量时令牌桶的参数设置包括：

- 平均速率：向桶中放置令牌的速率，即允许的流的平均速度。通常设置为承诺信息速率（Committed Information Rate, CIR）。
- 突发尺寸：令牌桶的容量，即每次突发所允许的最大的流量尺寸。通常设置为承诺突发尺寸（Committed Burst Size, CBS），设置的突发尺寸必须大于最大报文长度。

每到达一个报文就进行一次评估。每次评估，如果桶中有足够的令牌可供使用，则说明流量控制在允许的范围内，此时要从桶中取走与报文转发权限相当的令牌数量；否则说明已经耗费太多令牌，流量超标了。

3. 复杂评估

为了评估更复杂的情况，实施更灵活的调控策略，可以设置两个令牌桶。例如流量监管（Traffic Policing，简称 TP）中有三个参数：

- 承诺信息速率 CIR（Committed Information Rate）
- 承诺突发尺寸 CBS（Committed Burst Size）

- 超出突发尺寸 EBS (Excess Burst Size)

它使用了两个令牌桶，每个桶投放令牌的速率一样，均为 CIR，只是尺寸不同——分别为 CBS 和 CBS+EBS（这两个桶简称 C 桶和 E 桶），代表所允许的不同突发级别。每次评估时，依据“C 桶有足够的令牌”、“C 桶令牌不足，但 E 桶足够”以及“C 桶和 E 桶都没有足够的令牌”的情况，可以分别实施不同的流控策略。

2.2.2 流量监管

流量监管 (Traffic Policing) 的典型应用是监督进入网络的某一流量的规格，把它限制在一个合理的范围之内，或对超出的部分流量进行“惩罚”，以保护网络资源和运营商的利益，例如可以限制 HTTP 报文不能占用超过 50% 的网络带宽。如果发现某个连接的流量超标，流量监管可以选择丢弃报文，或重新设置报文的优先级。

流量监管广泛地用于监管进入因特网服务提供商 ISP 的网络流量。TP 还包括对所监管流量的流分类服务，并依据不同的评估结果，实施预先设定好的监管动作。这些动作可以是：

- 转发：比如对评估结果为“符合”的报文继续正常转发的处理。
- 丢弃：比如对评估结果为“不符合”的报文进行丢弃。
- 改变优先级并转发：比如对评估结果为“部分符合”的报文，将之标记为其它的优先级后再进行转发。
- 进入下一级的监管：流量监管可以逐级堆叠，每级关注和监管更具体的目标。

2.2.3 流量整形

流量整形 (Traffic Shaping) 是一种主动调整流量输出速率的措施。一个典型应用是基于下游网络结点的 TP 指标来控制本地流量的输出。

流量整形与流量监管的主要区别在于，流量整形对流量监管中需要丢弃的报文进行缓存——通常是将它们放入缓冲区或队列内，也称流量整形 (Traffic Shaping，简称 TS)，如图 2-2 所示。当令牌桶有足够的令牌时，再均匀的向外发送这些被缓存的报文。流量整形与流量监管的另一区别是，整形可能会增加延迟，而监管几乎不引入额外的延迟。

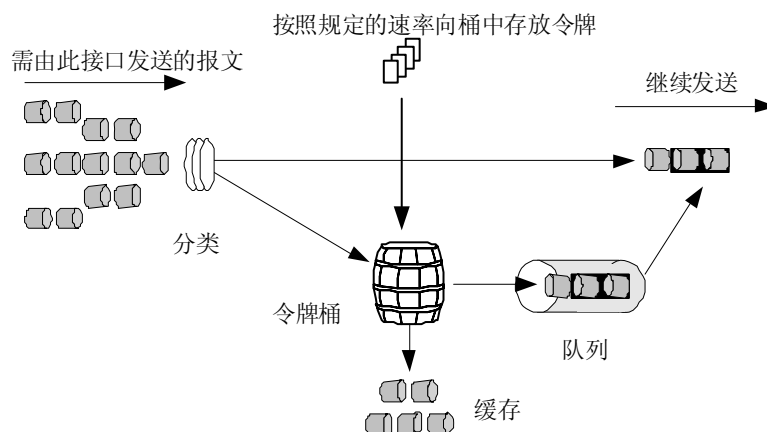


图2-2 TS 示意图

例如，在下图所示的应用中，SecPathA 向 SecPathB 发送报文。SecPathB 要对 SecPathA 发送来的报文进行 TP 监管，对超出规格的流量直接丢弃。

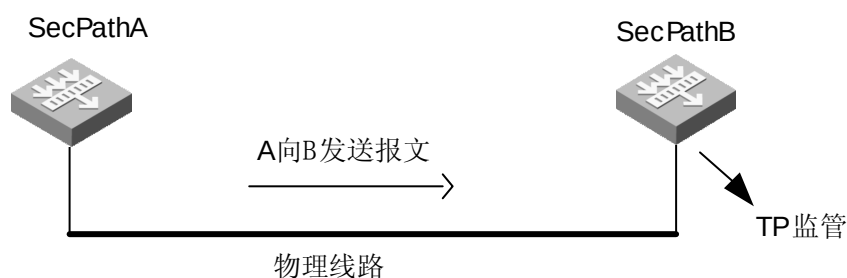


图2-3 流量整形的应用

为了减少报文的无谓丢失，可以在 SecPathA 的出口对报文进行 TS 处理。将超出 TS 流量特性的报文缓存在防火墙中。当可以继续发送下一批报文时，TS 再从缓冲队列中取出报文进行发送。这样，发向 SecPathB 的报文将都符合 SecPathB 的流量规定。

2.2.4 物理接口限速

利用物理接口限速（Line Rate, LR）可以在一个物理接口上限制发送报文（包括紧急报文）的总速率。

LR 也是采用令牌桶进行流量控制。如果在防火墙的某个接口上配置了 LR，所有经由该接口发送的报文首先要经过 LR 的令牌桶进行处理。如果令牌桶中有足够的令牌，则报文可以发送；否则，报文将入 QoS 队列进行拥塞管理。这样，就可以对通过该物理接口的报文流量进行控制。

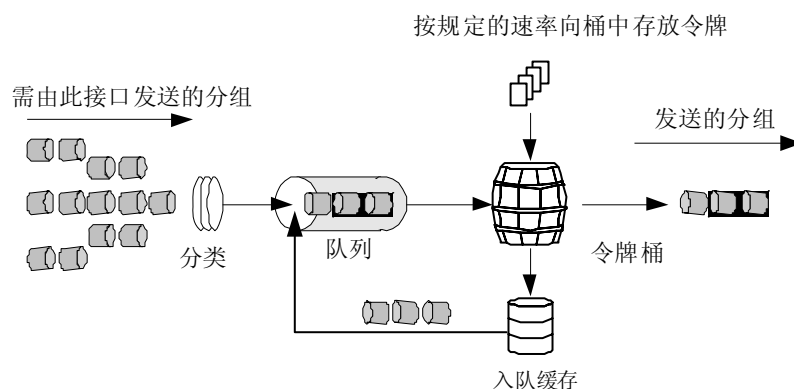


图2-4 LR 处理过程示意图

由于采用了令牌桶控制流量，当令牌桶中存有令牌时，可以允许报文的突发性传输；当令牌桶中没有令牌时，报文必须等到桶中生成了新的令牌后才可以继续发送。这就限制了报文的流量不能大于令牌生成的速度，达到了限制流量，同时允许突发流量通过的目的。

与 TP 相比，LR 能够限制在物理接口上通过的所有报文。TP 在 IP 层实现，对于不经过 IP 层处理的报文不起作用。当用户只要求对所有报文限速时，使用 LR 比较简单。

2.3 流量监管和流量整形配置

流量监管配置主要包括：

- 配置 CAR 列表
- 应用 CAR 策略

流量整形配置主要包括：

- 为某一类别的流设置整形参数
- 为所有的流设置整形参数

物理接口限速配置主要包括：

- 设置物理接口限速 LR

2.3.1 流量监管配置

流量监管的配置包括两方面的任务，一是定义那些需要实施监管的报文的特征，二是定义对这些报文的监管策略。

1. 配置 CAR 列表

在应用 CAR 策略之前，可以通过创建 CAR 列表对报文进行分类。对于不同的 *carl-index*，本命令的重复执行将创建多个 CAR 列表；对于同一个 *carl-index*，本命令的重复执行将修改 CAR 列表的参数。

请在系统视图下进行下列配置。

表2-1 配置 CAR 列表

操作	命令
创建/修改 CAR 列表	qos carl <i>carl-index</i> { precedence <i>precedence-value</i> dscp <i>dscp-value</i> mac <i>mac-address</i> }
删除 CAR 列表	undo qos carl <i>carl-index</i>

当需要在一条 CAR 列表中同时匹配多个优先级或 DSCP 值时，可指定多个不同的 *precedence-value* 或 *dscp-value*。

2. 应用 CAR 策略

本命令的重复执行将在接口上配置多个 CAR 策略。本命令只对 IP 数据包进行处理，对其他的数据包不进行处理。

请在接口视图下进行下列配置。

表2-2 应用 CAR 策略

操作	命令
应用 CAR 策略	qos car { inbound outbound } { any acl <i>acl-number</i> carl <i>carl-index</i> } cir <i>committed-information-rate</i> cbs <i>committed-burst-size</i> ebs <i>excess-burst-size</i> green <i>action</i> red <i>action</i>
删除 CAR 策略	undo qos car { inbound outbound } { any acl <i>acl-number</i> carl <i>carl-index</i> } cir <i>committed-information-rate</i> cbs <i>committed-burst-size</i> ebs <i>excess-burst-size</i>

其中，CIR 不能超过 CBS×20。

命令中对数据包采取的动作 (*action*) 有以下几种：

- **continue**: 继续由下一个 CAR 策略处理。
- **discard**: 丢弃数据包。
- **pass**: 发送数据包。
- **remark-prec-continue** *new-precedence* : 设置新的 IP 优先级 *new-precedence*，并继续由下一个 CAR 策略处理，取值范围 0~7。
- **remark-prec-pass** *new-precedence*: 设置新的 IP 优先级 *new-precedence*，并发送数据包到目的地址，取值范围 0~7。

CAR 策略可以应用于报文到达的接口，也可应用于报文离开的接口。

2.3.2 流量整形配置

为某一类流或所有的流设置整形参数就可以使系统开始进行整形。

qos gts acl 用来为符合某一 ACL 的流设置整形参数，使用不同的 ACL 可以为不同的流设置整形参数。

qos gts any 用来为所有的流设置整形参数，重复使用将替代原来的设置。

qos gts acl 不能和 **qos gts any** 同时使用。

请在接口视图下进行下列设置。

表2-3 为某一类别的流或所有流设置整形参数

操作	命令
为某一类别的流设置整形参数	qos gts { any acl acl-number } cir committed-information-rate [cbs committed-burst-size [ebs excess-burst-size [queue-length]]]
取消对某一类别的流整形	undo qos gts { any acl acl-number }

2.3.3 接口限速配置

配置接口限速就是限制物理接口向外发送数据的速率。

请在接口视图下进行下列配置。

表2-4 设置接口限速

操作	命令
设置接口限速	qos lr cir committed-information-rate [cbs committed-burst-size [ebs excess-burst-size]]
取消接口限速	undo qos lr

2.4 流量监管与流量整形显示和调试

2.4.1 显示 TP 规则

在完成上述配置后，在所有视图下执行 **display** 命令可以显示 TP 的某条规则或所有访问规则，通过查看显示信息验证配置的效果。

表2-5 显示 TP 规则

操作	命令
显示 TP 规则	display qos carl [<i>carl-index</i>]

2.4.2 显示接口的 TP 配置情况和统计信息

在完成上述配置后，在所有视图下执行 **display** 命令可以显示 TP 在各接口上的参数设置情况和运行统计信息，通过查看显示信息验证配置的效果。

表2-6 显示接口的 TP 配置情况和统计信息

操作	命令
显示接口的 TP 配置情况和统计信息	display qos car interface [<i>interface-type</i> <i>interface-number</i>]

2.4.3 显示接口的 TS 配置情况和统计信息

在完成上述配置后，在所有视图下执行 **display** 命令可以显示某个接口或所有接口的 TS 配置情况和统计信息，通过查看显示信息验证配置的效果。

表2-7 显示接口的 TS 配置情况和统计信息

操作	命令
显示接口的 TS 配置情况和统计信息	display qos gts interface [<i>interface-type</i> <i>interface-number</i>]

2.4.4 显示接口的 LR 配置情况和统计信息

在完成上述配置后，在所有视图下执行 **display** 命令可以显示某个接口或所有接口的 LR 配置情况和统计信息，通过查看显示信息验证配置的效果。

表2-8 显示接口的 LR 配置情况和统计信息

操作	命令
显示接口的 LR 配置情况和统计信息	display qos lr interface [<i>interface-type</i> <i>interface-number</i>]

2.5 流量监管与流量整形典型配置举例

1. 配置需求

如图 2-5 所示, SecPath1 通过接口 ethernet0/0/0 和 SecPath2 的接口 ethernet1/0/0 互连, Server、PC1、PC2 可经由 SecPath1 和 SecPath2 访问 Internet。Server、PC1 与 SecPath1 的 ethernet1/0/0 接口在同一网段, PC2 与 SecPath1 的 ethernet2/0/0 接口在同一网段。要求在 SecPath2 上对接口 ethernet1/0/0 接收到的源自 Server 和 PC1 的报文流分别实施流量控制如下:

来自 server 的报文流量约束为 54000bps, 流量小于 54000bps 时可以正常发送, 流量超过 54000bps 时则将违规报文的优先级设置为 0 后进行发送;

来自 PC 的报文流量约束为 8000bps, 流量小于 8000bps 时可以正常发送, 流量超过 8000bps 时则丢弃违规报文;

同时, 对 SecPath2 的 ethernet 1/0/0 和 ethernet 0/0/0 接口收发报文有如下要求:

- SecPath2 的 ethernet 1/0/0 接口接收报文的总流量限制为 0.5Mbps, 如果超过流量限制则将违规报文丢弃;
- 经由 SecPath2 的 ethernet 0/0/0 接口进入 Internet 的报文流量限制为 1Mbps, 如果超过流量限制则将违规报文丢弃。

2. 组网图

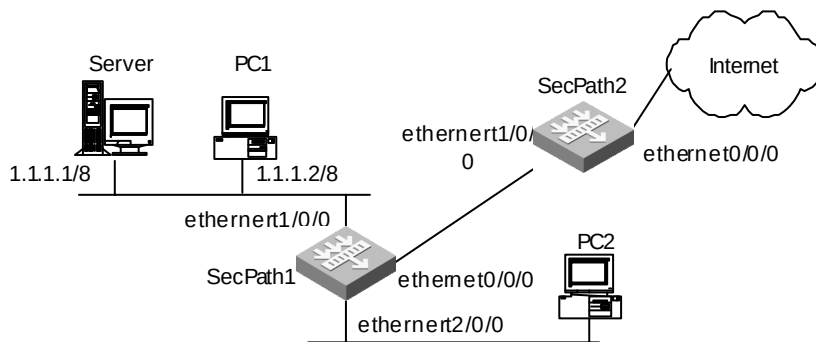


图2-5 流量监管、流量整形配置组网图

3. 配置步骤

(1) 配置 SecPath1:

在 SecPath1 的 ethernet0/0/0 接口上配置 TS, 对该接口发送的报文进行流量整形 (对超过 0.5Mbps 的报文流进行整形), 以降低在 SecPath2 接口 ethernet1/0/0 处的丢包率。

```
[H3C] interface ethernet0/0/0
```

```
[H3C-Ethernet0/0/0] qos gts any cir 500000
```

(2) 配置 SecPath2:

配置 ACL 规则列表，分别匹配来源于 Server 和 PC1 的报文流。

```
[H3C] acl number 2001
```

```
[H3C-acl-basic-2001] rule permit source 1.1.1.1 0.0.0.0
```

```
[H3C] acl number 2002
```

```
[H3C-acl-basic-2002] rule permit source 1.1.1.2 0.0.0.0
```

在 ethernet1/0/0 接口上进行 TP 配置，对 ethernet1/0/0 接收到的不同报文流进行相应流量控制。

```
[H3C] interface ethernet1/0/0
```

```
[H3C-Ethernet1/0/0] qos car inbound acl 2001 cir 54000 cbs 54000 ebs 0 green  
pass red remark-prec-pass 0
```

```
[H3C-Ethernet1/0/0] qos car inbound acl 2002 cir 80000 cbs 80000 ebs 0 green  
pass red discard
```

```
[H3C-Ethernet1/0/0] qos car inbound any cir 500000 cbs 500000 ebs 0 green pass  
red discard
```

在 ethernet0/0/0 接口上进行 TP 配置，对由 Ethernet 0/0/0 接口发送的报文进行流量控制，报文流量不能超过 1Mbps，如果超过流量限制则将违规报文丢弃。

```
[H3C] interface ethernet0/0/0
```

```
[H3C-Ethernet0/0/0] qos car outbound any cir 1000000 cbs 1000000 ebs 0 green  
pass red discard
```


第3章 拥塞管理

3.1 拥塞管理简介

对于网络单元，当分组到达的速度大于该接口发送分组的速度时，在该接口处就会产生拥塞。如果没有足够的存储空间来保存这些分组，其中的一部分就会丢失。分组的丢失又可能会导致发送该分组的主机或路由器因超时而重传此分组，这将导致恶性循环。

拥塞管理的中心内容就是当拥塞发生时如何制定一个资源的调度策略，决定报文转发的处理次序。

3.1.1 拥塞管理策略

对于拥塞管理，一般采用排队技术，使用一个队列算法对流量进行分类，之后用某种优先级别算法将这些流量发送出去。每种队列算法都是用以解决特定的网络流量问题，并对带宽资源的分配、延迟、延迟抖动等有着十分重要的影响。

这里介绍几种常用的队列调度机制。

1. FIFO（先进先出队列，First-In First-Out Queuing）

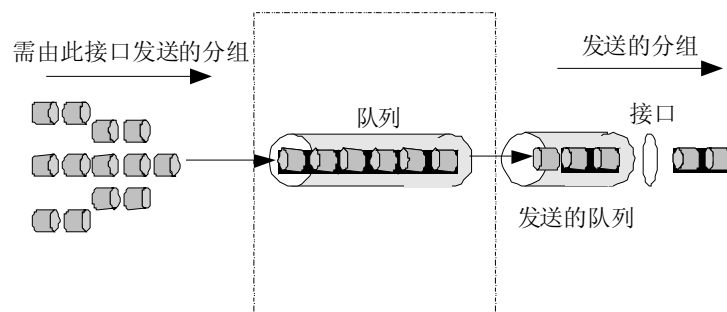


图3-1 先进先出队列示意图

如上图所示，FIFO 按照时间到达的先后决定分组的转发次序。用户的业务流在防火墙能够获得的资源取决于分组的到达时机及当时的负载情况。Best-Effort 报文投递方式采用的就是 FIFO 的排队策略。

如果防火墙的每个端口只有一个基于 FIFO 的输入或输出队列，那么恶性的应用可能会占用所有的网络资源，严重影响关键业务数据的传送。

每个队列内部报文的发送（次序）关系默认是 FIFO。

2. PQ (优先队列, Priority Queuing)

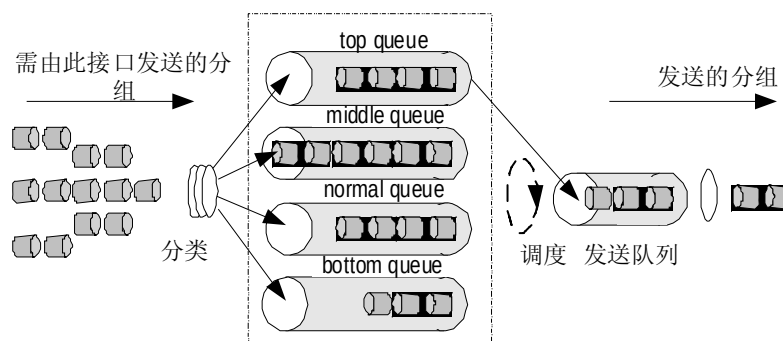


图3-2 优先队列示意图

PQ 队列是针对关键业务应用设计的。关键业务有一个重要的特点，即在拥塞发生时要求优先获得服务以减小响应的延迟。PQ 可以根据网络协议（比如 IP, IPX）、数据流入接口、报文长短、源地址/目的地址等灵活地指定优先次序。优先队列将报文分成 4 类，分别为高优先队列（top）、中优先队列（middle）、正常优先队列（normal）和低优先队列（bottom），它们的优先级依次降低。缺省情况下，缺省数据流进入 normal 队列。

在队列调度时，PQ 严格按照优先级从高到低的次序，优先发送较高优先级队列中的分组，当较高优先级队列为空时，再发送较低优先级队列中的分组。这样，将关键业务的分组放入较高优先级的队列，将非关键业务的分组放入较低优先级的队列，可以保证关键业务的分组被优先传送，非关键业务的分组在处理关键业务数据的空闲间隙被传送。

PQ 的缺点是如果较高优先级队列中长时间有分组存在，那么低优先级队列中的报文将可能一直得不到服务。

3. CQ (定制队列, Custom Queuing)

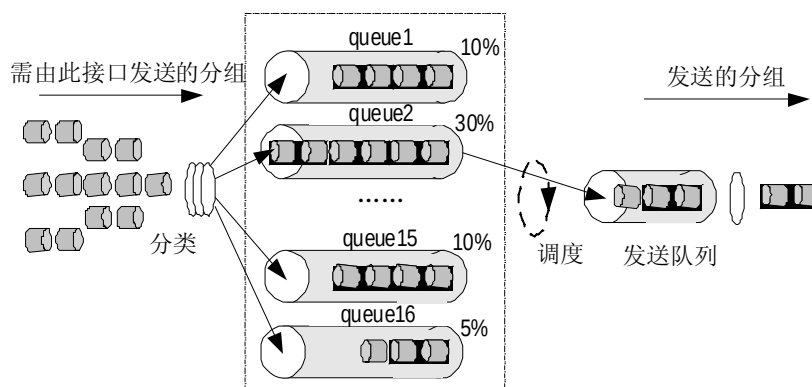


图3-3 定制队列示意图

CQ 按照一定的规则将分组分成 17 类（对应于 17 个队列），分组根据自己的类别按照先进先出的策略进入相应的 CQ 队列。

在 CQ 的 17 个队列中，0 号队列是系统队列（图中未画出），不允许用户配置；1 到 16 号队列是用户队列，如图 3-3 所示。用户可以配置流分类的规则，指定 16 个用户队列占用接口带宽的比例关系。在队列调度时，系统队列中的分组被优先发送。直到系统队列为空，再采用轮询的方式按照预先配置的带宽比例依次从 1 到 16 号用户队列中取出一定数量的分组发送出去。这样，就可以使不同业务的分组获得不同的带宽，既可以保证关键业务能获得较多的带宽，又不至于使非关键业务得不到带宽。缺省情况下，缺省数据流进入 1 号队列。

定制队列的另一个优点是：可根据业务的繁忙程度分配带宽，适用于对带宽有特殊需求的应用。虽然 16 个用户队列的调度是轮询进行的，但对每个队列不是固定地分配服务时间片——如果某个队列为空，那么马上换到下一个队列调度。因此，当没有某些类别的报文时，CQ 调度机制能自动增加现存类别的报文可占的带宽。

4. WFQ（加权公平队列，Weighted Fair Queuing）

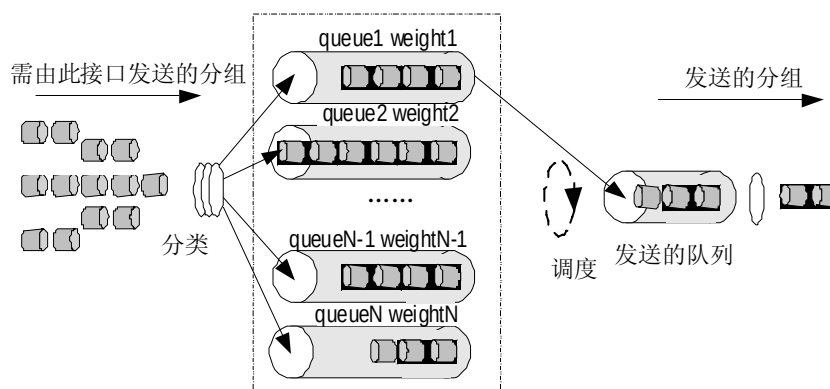


图3-4 加权公平队列示意图

在介绍加权公平队列前，先要理解公平队列 FQ（Fair Queue）。FQ 是为了公平地分享网络资源，尽可能使所有流的延迟和延迟抖动达到最优而推出的。它照顾了各方面的利益，主要表现在：

- 不同的队列获得公平的调度机会，从总体上均衡各个流的延迟。
- 短报文和长报文获得公平的调度：如果不同队列间同时存在多个长报文和短报文等待发送，应当顾及短报文的利益，让短报文优先获得调度，从而在总体上减少各个流的报文间的延迟抖动。

与 FQ 相比，WFQ 在计算报文调度次序时增加了优先权方面的考虑。从统计上，WFQ 使高优先权的报文获得优先调度的机会多于低优先权的报文。WFQ 能够按流的“会话”信息（协议类型、源和目的 TCP 或 UDP 端口号、源和目的 IP 地址、ToS 域中的优先级位等）自动进行流分类，并且尽可能多地提供队列，以将每个流均匀地放入不同队列中，从而在总体上均衡各个流的延迟。在出队的时候，WFQ 按流的

优先级 (precedence) 来分配每个流应占有出口的带宽。优先级的数值越大, 所得的带宽越多。

例如: 接口中当前共有 5 个流, 它们的优先级分别为 0、1、2、3、4, 则带宽总配额为所有 (流的优先级+1) 的和。即

$$1 + 2 + 3 + 4 + 5 = 15$$

每个流所占带宽比例为: (自己的优先级数 + 1) / (所有 (流的优先级 + 1) 的和)。即每个流可得的带宽分别为: 1/15, 2/15, 3/15, 4/15, 5/15。

由于 WFQ 在拥塞发生时能均衡各个流的延迟和延迟抖动, 所以 WFQ 在一些特殊场合得到了有效的应用。比如在使用资源预留协议 RSVP (Resource Reservation Protocol) 的保证型业务中, 通常就是采用 WFQ 作为调度策略; 在流量整形 TS 中, 也采用 WFQ 调度缓存的报文。

5. CBQ (基于类的队列, Class Based Queue)

CBQ 是对 WFQ 功能的扩展, 为用户提供了定义类的支持。CBQ 为每个用户定义的分类分配一个单独的 FIFO 预留队列, 用来缓冲同一类的数据。在网络拥塞时, CBQ 对输出报文根据用户定义类规则进行匹配, 并使其进入相应的队列, 在入队列之前必须进行拥塞避免机制 (尾部丢弃或 WRED, Weighted Random Early Detection, 加权随机早期检测) 和带宽限制的检查。在报文出队列时, 加权公平调度每个类对应的队列中的报文。

CBQ 提供一个紧急队列, 紧急报文入紧急队列, 该紧急队列采用 FIFO 调度, 没有带宽限制。这样, 如果 CBQ 加权公平对待所有类的队列, 语音报文这类对延迟敏感的数据流就可能不能及时发送。为此将 PQ 特性引入 CBQ, 称其为 LLQ (Low Latency Queueing, 低延迟队列), 为语音报文这样的对延迟敏感的数据流提供严格优先发送服务。

LLQ 将严格优先队列机制与 CBQ 结合起来使用, 用户在定义类时可以指定其享受严格优先服务, 这样的类称作优先类。所有优先类的报文将进入同一个优先队列, 在入队列之前需对各类报文进行带宽限制的检查。报文出队列时, 将首先发送优先队列中的报文, 直到发送完后才发送其他类对应的队列的报文。在发送其他队列报文时将仍然按照加权公平的方式调度。

为了不让其他队列中的报文延迟时间过长, 在使用 LLQ 时将会为每个优先类指定可用最大带宽, 该带宽值用于拥塞发生时监管流量。如果拥塞未发生, 优先类允许使用超过分配的带宽。如果拥塞发生, 优先类超过分配带宽的数据包将被丢弃。LLQ 还可以指定 Burst-size。

系统在为报文匹配规则时, 总是先匹配优先类, 然后再匹配其他类。对多个优先类, 按照配置顺序逐一匹配; 对其他类, 也是按照配置顺序逐一匹配。对类中多个规则, 按照配置顺序逐一匹配。

6. RTP（Real-time Transport Protocol）优先队列

RTP 优先队列是一种解决实时业务（包括语音与视频业务）服务质量的简单的队列技术。其原理就是将承载语音或视频的 RTP 报文送入高优先级队列，使其得到优先发送，保证时延和抖动降低为最低限度，从而保证了语音或视频这种对时延敏感业务的服务质量。

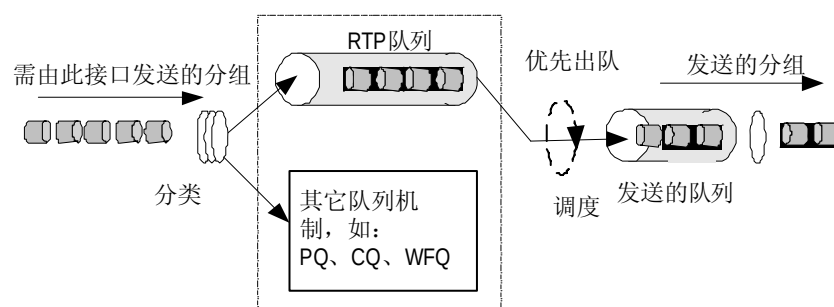


图3-5 RTP 队列示意图

如上图所示，RTP 优先队列将 RTP 报文送入一个具有较高优先级的队列。RTP 报文是端口号在一定范围内为偶数的 UDP 报文，端口号的范围可以配置。RTP 优先队列可以同任何一种队列（包括 FIFO、PQ、CQ、WFQ 与 CBQ）结合使用，而它的优先级是最高的。但由于 CBQ 中的 LLQ 也可以解决实时业务，所以一般不推荐将 RTP 优先队列与 CBQ 结合应用。

3.1.2 拥塞管理技术的对比

SecPath 防火墙提供了以上拥塞管理技术。突破了传统 IP 设备的单一 FIFO 拥塞管理策略，提供了强大的 QoS 能力，使得 IP 设备可以满足不同业务所要求的不同服务质量的要求。为了更好的利用拥塞管理技术，现对各种队列技术做一比较。

表3-1 拥塞管理技术对比

类型	队列数	优点	缺点
FIFO	1	1、不需要配置，易于使用。 2、处理简单，延迟小。	1、所有的报文，无论紧急与否，语音还是数据，均进入一个“先进先出”的队列，发送报文所占用的带宽、延迟时间、丢失的概率均由报文到达队列的先后顺序决定。 2、对不配合的数据源（即没有流控机制的流，如 UDP 报文发送）无约束力，不配合的数据源会造成配合的数据源（如 TCP 报文发送）带宽受损失。 3、对时间敏感的实时应用（如 VoIP）的延迟得不到保证。

类型	队列数	优点	缺点
PQ	4	可对不同业务的数据提供绝对的优先，对时间敏感的实时应用（如 VoIP）的延迟可以得到保证。对优先业务的报文的带宽占用可以绝对优先。	1、需配置，系统开销大。 2、如果不对高优先级的报文的带宽加限制，会造成低优先级的报文得不到带宽。
CQ	16	1、可对不同业务的报文按带宽比例分配带宽。 2、当没有某些类别的报文时，能自动增加现存类别的报文可占的带宽。	需配置，系统开销大。
WFQ	可配置	1、配置容易。 2、可以保护配合（交互）的数据源（如 TCP 报文发送）的带宽。 3、可以减小延迟抖动。 4、可以减小数据量小的交互式应用的延迟。 5、可以为不同优先级的流分配不同的带宽。 6、当流的数目减少时，能自动增加现存流可占的带宽。	系统开销比 FIFO 要大，但比 PQ、CQ 要小。
CBQ	可配置 (0~64)	1、可以对数据根据灵活、多样的分类规则进行划分，分别为 EF（加速转发）、AF（确保转发）、BE（尽力转发）业务提供不同的队列调度机制。 2、可以为 AF 业务提供严格、精确的带宽保证，并且保证各类 AF 业务之间根据权值按一定的比例关系进行队列调度。 3、可以为 EF 业务提供绝对优先的队列调度，确保实时数据的时延；同时通过对高优先级数据流量的限制，克服了 PQ 的低优先级队列可能“饿死”的弊病。 4、对于尽力转发的缺省类数据，提供 WFQ 队列调度。	系统开销大

3.2 先进先出队列的配置

先进先出队列 FIFO 的配置包括：

- 配置 FIFO 队列的长度

3.2.1 配置 FIFO 队列的长度

FIFO 是接口缺省使用的队列调度机制，可以通过配置命令改变其队列长度。

请在接口视图下进行下列配置。

表3-2 配置 FIFO 队列的长度

操作	命令
配置 FIFO 队列的长度	qos fifo queue-length <i>queue-length</i>
恢复 FIFO 队列的缺省长度	undo fifo queue-length

FIFO 队列的缺省长度为 75。

3.3 优先队列的配置

优先队列 PQ 的配置包括：

- 配置优先列表
- 在接口上应用优先列表组

3.3.1 配置优先列表

1. 根据网络层协议配置优先列表

根据协议类型对分组进行分类，使之进入不同的队列。对于同一个 *pql-index*，本命令的重复使用可以为 *pql-index* 建立多个规则。

系统以规则被配置的顺序来匹配分组，如果发现分组与某个规则匹配，便结束整个查找过程。

请在系统视图下进行下列配置。

表3-3 根据网络层协议配置优先列表

操作	命令
根据网络层协议配置优先列表	qos pql pql-index protocol ip [<i>queue-key key-value</i>] queue { <i>top</i> <i>middle</i> <i>normal</i> <i>bottom</i> }
删除 <i>pql-index</i> 中相应的分类规则	undo qos pql pql-index protocol ip [<i>queue-key key-value</i>]

2. 根据分组来自的接口配置优先列表

根据分组来自的防火墙接口进行分类，使之进入不同的队列。

请在系统视图下进行下列配置。

表3-4 根据接口配置优先列表

操作	命令
根据分组来自的接口配置优先列表	qos pql pql-index inbound-interface interface-type interface-number queue { top middle normal bottom }
删除 <i>pql-index</i> 中相应的分类规则	undo qos pql pql-index inbound-interface interface-type interface-number

3. 配置缺省队列

为不与任何规则匹配的包指定一个缺省队列。

请在系统视图下进行下列配置。

表3-5 配置缺省队列

操作	命令
配置缺省队列	qos pql pql-index default-queue { top middle normal bottom }
恢复缺省队列的缺省值	undo qos pql pql-index default-queue

可以给一个优先列表的组定义多条规则，然后把该组规则应用在某接口上。当一个分组到达该接口时（需要由此接口传送出去），系统沿规则链匹配该分组，如果匹配上某规则，则进入相应的队列，匹配结束；如果分组不与任何规则匹配，则进入缺省队列。

缺省队列的缺省值为 **normal**。

4. 配置队列长度

设置各队列的长度（即队列所能容纳的分组的个数）。

请在系统视图下进行下列配置。

表3-6 配置队列长度

操作	命令
配置队列长度	qos pql pql-index queue { top middle normal bottom } queue-length queue-length
形式恢复各队列长度的缺省值	undo qos pql pql-index queue { top middle normal bottom } queue-length

各队列的缺省长度如下表所示。

表3-7 队列缺省长度

队列	长度
top	20
middle	40
normal	60
bottom	80

3.3.2 在接口上应用优先列表组

将一组优先列表应用到接口上。对于同一个接口，本命令的重复使用将为接口设定新的优先列表组。

请在接口视图下进行下列配置。

表3-8 在接口上应用优先列表组

操作	命令
在接口上应用优先列表组	qos pq pql pql-index
取消使用 PQ	undo qos pq

缺省情况下，接口不使用 PQ，而使用 FIFO。

3.3.3 优先队列的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示优先列表及在接口上的应用情况，通过查看显示信息验证配置的效果。

表3-9 显示优先列表及在接口上的应用情况

操作	命令
显示优先列表的状态	display qos pql [pql-index]
显示接口上优先列表的配置情况	display qos pq interface [interface-type interface-number]

3.4 定制队列的配置

定制队列 CQ 的配置包括：

- 配置定制列表
- 在接口上应用定制列表组

3.4.1 配置定制列表

定制列表共可分为 16 个组（1~16），每个组指明了什么样的分组进入什么样的队列、各队列的长度和每次轮询各队列所能连续发送的字节数等信息。在一个接口上只能应用一个定制列表组。

1. 根据网络层协议配置定制列表

根据协议类型对分组进行分类，使之进入不同的队列。目前，Comware 只支持对 IP 报文进行分类。

请在系统视图下进行下列配置。

表3-10 根据网络层协议配置定制列表

操作	命令
根据网络层协议配置定制列表	qos cql cql-index protocol ip [queue-key key-value] queue queue-number
删除 <i>cql-index</i> 中相应的分类规则	undo qos cql cql-index protocol ip [queue-key key-value]

2. 根据分组来自的接口配置定制列表组

建立基于接口的分类规则。对于同一个 *cql-index*，本命令的重复使用可以为 *cql-index* 增加新的规则。

请在系统视图下进行下列配置。

表3-11 根据接口配置定制列表组

操作	命令
根据分组来自的接口配置定制列表组	qos cql cql-index inbound-interface interface-type interface-number queue queue-number
删除 <i>cql-index</i> 中相应的分类规则	undo qos cql cql-index inbound-interface interface-type interface-number

3. 配置缺省队列

为那些不与任何规则匹配的分组指定一个缺省队列。

请在系统视图下进行下列配置。

表3-12 配置缺省队列

操作	命令
配置缺省队列	qos cql cql-index default-queue queue-number
恢复缺省队列的缺省值	undo qos cql cql-index default-queue

我们可以给一个定制列表的组定义多条规则，然后把该组应用在某接口上。当一个分组到达该接口时（由此接口传送出去），系统沿规则链匹配该分组，如果匹配上某规则，则进入相应的队列，匹配结束；如果分组不与任何规则匹配，则进入缺省队列。

缺省队列的缺省值为 1。

4. 配置队列长度

设置各定制队列的长度（即队列所能容纳的分组的个数）。

请在系统视图下进行下列配置。

表3-13 配置队列长度

操作	命令
配置队列长度	qos cql cql-index queue queue-number queue-length queue-length
恢复各队列长度的缺省值	undo qos cql cql-index queue queue-number queue-length

其中：*queue-length* 为队列的最大长度，缺省值为 20。

5. 配置队列连续发送字节数

设置各队列每次轮询所发送分组的字节数。

请在系统视图下进行下列配置。

表3-14 配置队列连续发送字节数

操作	命令
配置连续发送字节数	qos cql cql-index queue queue-number serving byte-count
恢复发送字节数的缺省值	undo qos cql cql-index queue queue-number serving

其中：

byte-count：当防火墙调度 CQ 的用户队列时，它连续从这个队列中取出分组进行发送，直到发送的字节数不少于为该队列配置的 *byte-count* 的值或者队列为空，再转而调度 CQ 的下一个用户队列。因此，*byte-count* 的值会影响 CQ 各用户队列之间占用接口带宽的比例关系，并且决定了多长时间防火墙才会调度 CQ 的下一个队列。*byte-count* 的缺省字节数为 1500。

如果 *byte-count* 的值过小，由于防火墙每次至少发送一个分组才会转向下一个队列，各个队列实际获得的带宽很可能与预想的效果相差甚远；如果 *byte-count* 值过大，则可能会造成队列间切换延迟太大。

3.4.2 在接口上应用定制列表

请在接口视图下进行下列配置。

表3-15 在接口上应用定制列表

操作	命令
在接口上应用定制列表	qos cq cql <i>cql-index</i>
取消使用 CQ	undo qos cq

缺省情况下，接口不使用 CQ，而使用 FIFO。

3.4.3 定制队列的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示定制列表状态及在接口上的应用情况，通过查看显示信息验证配置的效果。

表3-16 显示定制列表状态及在接口上的应用情况

操作	命令
显示定制列表状态	display qos cql [<i>cql-index</i>]
显示定制列表在接口上应用情况	display qos cq interface [<i>interface-type interface-number</i>]

3.5 加权公平队列的配置

加权公平队列 WFQ 的配置包括：

- 在接口上应用加权公平队列

3.5.1 在接口上应用加权公平队列

WFQ 对报文按流进行分类，对于 IP 网络，五元组（源 IP 地址、目的 IP 地址、源端口号、目的端口号、协议号）和 IP 优先级或者 DSCP 相同的报文属于同一个流。在接入层的网络中，通常使用 IP 优先级和五元组配合进行流分类；在汇聚层网络中通常使用 DSCP 值和五元组配合进行流分类。WFQ 默认是使用 IP 优先级和五元组配合进行流分类，用户可以通过下面命令来做出选择。

当接口没有使用 WFQ 策略时，使用本命令可以使接口使用 WFQ 策略，同时可指定 WFQ 的参数。如果接口已经使用了 WFQ 策略，使用本命令可以修改 WFQ 的参数。

请在接口视图下进行如下配置。

表3-17 使用加权公平队列或修改 WFQ 的参数

操作	命令
使用加权公平队列或修改 WFQ 的参数	qos wfq [precedence dscp] [queue-length max-queue-length [queue-number total-queue-number]]
取消使用 WFQ	undo qos wfq

缺省情况下，接口不使用 WFQ，而使用 FIFO。

total-queue-number：队列的总数目，可取的值为：16、32、64、128、256、512、1024、2048、4096，缺省值为 256。



注意：

- Dialer 口上可以应用 WFQ 队列，但是只有当物理接口上配置为缺省队列，WFQ 队列才能成功应用到 Dialer 口上。
- 在 Dialer 口上应用队列配置时，如果和 Dialer 口绑定的物理接口已经和相连的设备建立了连接，则 Dialer 口上的配置无法马上更新到该物理接口上。只有当物理接口再次建立连接时，Dialer 口上的配置才能更新到该物理接口上。

3.5.2 加权公平队列的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示接口加权公平队列的配置情况和统计信息，通过查看显示信息验证配置的效果。

表3-18 显示接口加权公平队列的配置情况和统计信息

操作	命令
显示接口加权公平队列的配置情况和统计信息	display qos wfq interface [interface-type interface-number]

3.6 基于类的队列的配置

基于类的队列 CBQ 的配置包括：

- 配置接口最大可用带宽
- 定义类，并在类视图中定义一组流分类规则
- 定义流行为，并在流行为视图中定义一组 QoS 特性
- 定义策略，在策略视图下为使用的类中指定对应的流行为
- 在接口视图下应用 QoS 策略

为方便用户使用，系统预定义了一些类、流行为以及策略，具体如下。

1. 系统预定义的类

系统预定义了一些类，并为这些类定义了通用的规则，用户定义策略时可直接使用这些类，这些类包括：

(1) 缺省类

default-class: 匹配的是缺省数据流。

(2) 基于 DSCP 的预定义类

ef、af1、af2、af3、af4: 分别匹配 IP DSCP 值 ef、af1、af2、af3、af4

(3) 基于 IP 优先级的预定义类

ip-prec0, ip-prec1, ...ip-prec7: 分别匹配 IP 优先级 0, 1, ...7

(4) 基于 MPLS EXP 的预定义类

mpls-exp0, mpls-exp1, ...mpls-exp7: 分别匹配 MPLS EXP 值 0, 1, ...7

2. 系统预定义的流行为

系统预定义了一些流行为，并为这些流行为定义了 QoS 特性：

(1) **ef:** 定义了一个特性为入 EF 队列，占用带宽为接口可用带宽的 20%

(2) **af:** 定义了一个特性为入 AF 队列，占用带宽为接口可用带宽的 20%

(3) **be:** 不定义任何特性

3. 系统预定义的策略

系统预定义了一个策略，为该策略指定了使用的预定义类，并为这些类指定预定义的动作。该策略名为 **default**，具有缺省的 CBQ 动作。

default 策略的具体规则如下：

(1) 预定义类 **ef**，采用预定义流行为 **ef**

(2) 预定义类 **af1~af4**，采用预定义流行为 **af**

(3) **default-class** 类，采用预定义流行为 **be**

3.6.1 配置接口最大可用带宽

该带宽指 CBQ 中报文入队列带宽检查时使用的最大接口带宽，并非指物理接口的实际带宽。

请在接口视图下进行下列配置。

表3-19 配置 MP 绑定带宽

操作	命令
配置本接口的带宽	qos max-bandwidth <i>bandwidth</i>
恢复本接口的带宽缺省值	undo qos max-bandwidth

bandwidth 是接口的可用带宽，单位 Kbps，范围为 1 到 1000000。缺省情况下，对于物理接口，其取值为物理接口实际的波特率或速率；对于虚拟接口模板（Virtual Template）、VE 等逻辑接口，取值为 64Kbps。

建议该值小于物理接口或逻辑链路的实际可用带宽。



注意：

如果接口上同时配置了 LR 和百分比类型的 CBQ，请将此命令中设置的带宽与 LR 的限制速率保持一致。

3.6.2 定义类并配置其匹配规则

定义类首先要创建一个类名称，然后在此类视图下配置其匹配规则。

1. 定义类并进入类视图

请在系统视图下进行下列配置。

表3-20 定义一个类并进入类视图

操作	命令
定义类并进入类映射视图	traffic classifier <i>tcl-name</i> [operator { and or }]
删除类并进入类映射视图	undo traffic classifier <i>tcl-name</i>

用户定义类名 *tcl-name* 不允许为系统预定义类。

缺省为 **and**，即类视图下各匹配规则之间的关系为逻辑与。

2. 定义或删除匹配所有数据包的规则

请在类视图下进行下列配置。

表3-21 定义或删除匹配所有数据包的规则

操作	命令
定义匹配所有数据包的规则	if-match [not] any
删除匹配所有数据包的规则	undo if-match [not] any

3. 定义或删除 classifier 匹配规则

请在类视图下进行下列配置。

表3-22 定义或删除 classifier 匹配规则

操作	命令
定义 classifier 匹配规则	if-match [not] classifier <i>tcl-name</i>
删除 classifier 匹配规则	undo if-match [not] classifier <i>tcl-name</i>

该命令不能递归使用，例如，traffic classifier A 定义了匹配 traffic classifier B 的规则，traffic classifier B 不能再直接或者间接的引用 traffic classifier A。

4. 定义或删除 ACL 匹配规则

定义 ACL 匹配规则。

请在类视图下进行下列配置。

表3-23 定义或删除 ACL 匹配规则

操作	命令
定义 ACL 匹配规则	if-match [not] acl <i>access-list-number</i>
删除 ACL 匹配规则	undo if-match [not] acl <i>access-list-number</i>

5. 定义或删除 MAC 地址匹配规则

请在类视图下进行下列配置。

表3-24 定义或删除 MAC 地址匹配规则

操作	命令
定义 MAC 地址匹配规则	if-match [not] { destination-mac source-mac } <i>mac-address</i>
删除 MAC 地址匹配规则	undo if-match [not] { destination-mac source-mac } <i>mac-address</i>

目的 MAC 地址匹配规则只对出方向的策略有意义，并且只对以太类型的接口有意义。

源 MAC 地址匹配规则只对入方向的策略有意义，并且只对以太类型的接口有意义。

6. 定义或删除类的入接口匹配规则

请在类视图下进行下列配置。

表3-25 定义或删除类的入接口匹配规则

操作	命令
定义类的入接口匹配规则	if-match [not] inbound-interface <i>type number</i>
删除类的入接口匹配规则	undo if-match [not] inbound-interface <i>type number</i>

匹配的接口删除时，该规则自动删除。

7. 定义或删除 DSCP 匹配规则

DSCP (Differentiated Services CodePoint, 差分服务编码点) 是 IETF DiffServ 工作组将 IP 报文头 ToS 字节的高 6 位重新定义的域, ToS 字节因而也改名为 DS 字节。在 DiffServ 方案中, 在网络入口处根据服务要求对业务进行分类、流量控制, 同时设置 DSCP, 在网络中将依据分组的 DSCP 值来区分每一类通信并为之服务 (包括资源分配、分组丢弃策略等)。

用户可以根据 DSCP 值来设置分类的匹配规则。

请在类视图下进行下列配置。

表3-26 定义或删除 DSCP 匹配规则

操作	命令
定义 DSCP 匹配规则	if-match [not] dscp { <i>dscp-value</i> }
删除 DSCP 匹配规则	undo if-match [not] dscp { <i>dscp-value</i> }

8. 定义或删除 IP 优先值匹配规则

请在类视图下进行下列配置。

表3-27 定义或删除 IP 优先值匹配规则

操作	命令
定义 IP 优先值匹配规则	if-match [not] ip-precedence { <i>ip-precedence-value</i> }
删除 IP 优先值匹配规则	undo if-match [not] ip-precedence

配置时将需要配置的 IP 优先值用一条命令进行配置, 否则最后配置的 **if-match ip-precedence** 命令会覆盖前面的配置。

9. 定义或删除 RTP 协议端口匹配规则

请在类视图下进行下列配置。

表3-28 定义或删除 RTP 协议端口匹配规则

操作	命令
定义 RTP 协议端口匹配规则	if-match [not] rtp start-port <i>starting-port-number</i> end-port <i>end-port-number</i>
删除 RTP 协议端口匹配规则	undo if-match [not] rtp start-port <i>starting-port-number</i> end-port <i>end-port-number</i>

由于 RTP 队列优先于 CBQ，所以如果同时配置了 RTP 队列与基于匹配 RTP 协议的类的调度队列，只有 RTP 队列生效。

10. 定义或删除协议匹配规则

请在类视图下进行下列配置。

表3-29 定义或删除协议匹配规则

操作	命令
定义协议匹配规则	if-match [not] protocol <i>protocol-name</i>
删除协议匹配规则	undo if-match [not] protocol <i>protocol-name</i>

其中 *protocol-name* 为 IP 协议。

3.6.3 定义流行为并配置其特性

定义流行为首先需要创建一个流行为名称，然后在此流行为视图下配置其特性。

1. 定义流行为并进入流行为视图

请在系统视图下进行下列配置。

表3-30 定义一个流行为并进入流行为视图

操作	命令
定义一个流行为并进入流行为视图	traffic behavior <i>behavior-name</i>
删除流行为	undo traffic behavior <i>behavior-name</i>

behavior-name: 流行为名，不允许为系统预定义流行为。

2. 配置确保转发 (AF)，并配置最小可保证带宽

请在流行为视图下进行下列配置。

表3-31 配置确保转发 (AF)，并配置最小可保证带宽

操作	命令
配置确保转发 (AF)，并配置最小可保证带宽	queue af bandwidth { <i>bandwidth</i> pct percentage }
删除确保转发配置	undo queue af

该行为只能应用在接口的出方向。

在同一策略下需要用同一单位配置 **queue ef** 和 **queue af**，或者用 *bandwidth*，或者用百分比进行配置。

3. 配置加速转发 (EF)，并配置至少保证的最大带宽

请在流行为视图下进行下列配置。

表3-32 配置加速转发 (EF)，并配置至少保证的最大带宽

操作	命令
配置加速转发 (EF)，并配置至少保证的最大带宽	queue ef bandwidth { <i>bandwidth</i> [cbs committed-burst-size] pct percentage [cbs_ratio ratio] }
取消该配置	undo queue ef

该命令在流行为视图下不能与 **queue af**，**queue-length**，**wred** 同时使用。

缺省类不能与包含该命令的行为关联。

在同一策略下各个类需用同一单位配置 **queue ef** 和 **queue af**，或者用 *bandwidth*，或者用百分比进行配置。

4. 配置采用公平队列

请在流行为视图下进行下列配置。

表3-33 配置采用公平队列

操作	命令
配置采用公平队列	queue wfq [queue-number total-queue-number]
取消采用公平队列的配置	undo queue wfq

配置了该特性的流行为仅可以与缺省类关联使用。

5. 配置最大队列长度

配置最大队列长度，丢弃方式为尾丢弃。

请在流行为视图下进行下列配置。

表3-34 配置最大队列长度

操作	命令
配置最大队列长度	queue-length <i>queue-length</i>
取消最大队列长度的配置	undo queue-length

该命令必须在配置了 **queue af** 和 **queue wfq** 后使用; 执行 **undo queue af** 或 **undo queue wfq** 命令, 则 **queue-length** 也同时被取消。

如果是缺省类, 必须在配置了 **queue af** 或 **queue wfq** 后使用。

6. 配置丢弃方式为随机丢弃方式

请在流行为视图下进行下列配置。

表3-35 配置丢弃方式为随机丢弃方式

操作	命令
配置丢弃方式为随机丢弃方式	wred [dscp ip-precedence]
恢复缺省配置	undo wred

dscp: 表明在为一个包计算丢弃概率时使用的是 DSCP 值。

ip-precedence: 表明在为一个包计算丢弃概率时使用的是 IP 优先级值, 作为缺省配置。

该命令必须在配置了 **queue af** 或 **queue wfq** 后使用。**wred** 和 **queue-length** 是互斥的。删除时将删除在该随机丢弃下的其他配置。当接口上应用了包含 WRED 特性的 QoS 策略后, 原有的接口级的 WRED 配置失效。

缺省类 **default-class** 只能与配置基于 IP 优先级的随机丢弃方式的行为关联。

7. 设置 WRED 计算平均队列长度的指数

请在流行为视图下进行下列配置。

表3-36 设置 WRED 计算平均队列长度的指数

操作	命令
配置 WRED 计算平均队列长度的指数	wred weighting-constant <i>exponent</i>
取消 WRED 计算平均队列长度的指数的配置	undo wred weighting-constant

需配置了 **queue af** 或 **queue wfq**, 并已用 **wred** 使能了 WRED 丢弃方式后才可以配置该命令。

8. 配置 WRED 各 DSCP 的下限、上限和丢弃概率分母

请在流行为视图下进行下列配置。

表3-37 设置 WRED 各 DSCP 的下限、上限和丢弃概率分母

操作	命令
配置 WRED 各 DSCP 的下限、上限和丢弃概率分母	wred dscp dscp-value low-limit low-limit high-limit high-limit [discard-probability discard-prob]
取消 WRED 各 DSCP 的下限、上限和丢弃概率分母的配置	undo wred dscp dscp-value

dscp-value: DSCP 值, 取值范围为 0~63, 或可以是如下关键字: **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7** 或 **default**。

需已用 **wred dscp** 使能了基于 DSCP 的 WRED 丢弃方式。

取消 **wred** 配置, **wred dscp dscp-value** 配置同时被取消。

取消 **queue af** 或 **queue wfq** 配置, 丢弃参数的配置同时被取消。

9. 配置 WRED 各优先级的下限、上限和丢弃概率分母

请在流行为视图下进行下列配置。

表3-38 配置 WRED 各优先级的下限、上限和丢弃概率分母

操作	命令
设置 WRED 各优先级的下限、上限和丢弃概率分母	wred ip-precedence precedence low-limit low-limit high-limit high-limit [discard-probability discard-prob]
取消 WRED 各优先级的下限、上限和丢弃概率分母的配置	undo wred ip-precedence precedence

需已用 **wred ip-precedence** 使能了基于优先级的 WRED 丢弃方式。

缺省情况下, 已使能基于 IP 优先级的 WRED 丢弃方式。

取消 **wred** 配置, **wred ip-precedence** 配置同时被取消。

取消 **queue af** 或 **queue wfq** 配置, 丢弃参数的配置同时被取消。

10. 配置使用或取消流量监管

请在流行为视图下进行下列配置。

表3-39 配置使用或取消流量监管

操作	命令
配置使用流量监管	car cir committed-information-rate [cbs committed-burst-size ebs excess-burst-size] [green action [red action]]
配置取消流量监管	undo car

其中，CIR 不能超过 CBS×20。*action* 是对数据包采取的动作，有以下几种：

- **discard**: 丢弃数据包
- **pass**: 发送数据包。
- **remark-dscp-pass new-dscp**: 设置新的 DSCP 值 new-dscp，并发送。取值范围为 0~63。
- **remark-prec-pass new-precedence**: 设置新的 IP 优先级 new-precedence，并发送。取值范围为 0~7。

策略中的类关联了包含 TP 特性的行为时，可以应用到接口的入或出方向。

策略中的类关联了包含 TP 特性的行为时，将导致接口上原有的 **qos car** 命令失效。

如果多次使用本命令在同一个流行为上配置，最后一次的配置将覆盖前面的配置。

使用流量监管但未使用 AF 或 EF 配置的类，如果通过了监管的检测可以发送，但遇到接口拥塞，则将进入缺省队列。

11. 配置使用或取消流量整形

请在流行为视图下进行下列配置。

表3-40 配置使用或取消流量整形

操作	命令
配置使用流量整形	gts cir committed-information-rate [cbs committed-burst-size [ebs excess-burst-size [queue-length queue-length]]]
配置取消流量整形	undo gts

接口上应用的类策略中使用具有 **gts** 的流行为时，只能应用到接口的出方向。

接口上应用包含 TS 的类策略，将导致接口上原有的 **qos gts** 命令失效。

如果多次使用本命令在同一个流行为上配置，最后一次的配置将覆盖前面的配置。

使用流量整形但未使用 AF 或 EF 配置的类，如果通过了整形的检测可以发送，但遇到接口拥塞，则将进入缺省队列。

12. 配置标记报文的 DSCP 值

请在流行为视图下进行下列配置。

表3-41 配置标记报文的 DSCP 值

操作	命令
配置标记报文的 DSCP 值	remark dscp <i>dscp-value</i>
取消标记报文的 DSCP 值的配置	undo remark dscp

13. 配置标记报文的 IP 优先级值

请在流行为视图下进行下列配置。

表3-42 配置标记报文的 IP 优先级值

操作	命令
配置标记报文的 IP 优先级值	remark ip-precedence <i>ip-precedence-value</i>
取消标记报文的 IP 优先级值的配置	undo remark ip-precedence

3.6.4 配置策略

1. 定义策略并进入策略视图

策略映射定义该策略中每个类的流行为，而每个流行为由一组特性要求组成，例如 EF，AF，WFQ，流量监管（TP），流量整形（TS），WRED、标记等。

请在系统视图下进行下列配置。

表3-43 定义策略并进入策略视图

操作	命令
定义策略并进入策略视图	qos policy <i>policy-name</i>
删除指定策略	undo qos policy <i>policy-name</i>

策略名不允许是系统预定义策略。

策略创建时，缺省具有缺省类 **default-class**，该类关联 **be** 行为。

如果某接口应用了该策略，则不允许删除该策略，需要在应用的接口上取消对该策略的应用，然后再使用 **undo qos policy** 删除该策略。

2. 在策略中为类指定流行为

请在策略视图下进行下列配置。

表3-44 在策略中为类指定流行为

操作	命令
在策略中为类指定采用的流行为	classifier <i>tcl-name</i> behavior <i>behavior-name</i>
取消指定类在策略中的使用	undo classifier <i>tcl-name</i>

tcl-name: 类名，必须是已经定义的类，可以是系统定义或用户定义类。

behavior-name: 必须是已定义的流行为名，可以是系统定义或用户定义流行为。

3.6.5 应用策略

qos apply policy 命令是将一个策略映射到具体的接口上。一个策略映射可以在多个接口上得到应用。

请在接口视图下进行下列配置。

表3-45 将接口与所设置的策略相关联

操作	命令
在接口上应用关联的策略	qos apply policy <i>policy-name</i> { inbound outbound }
在接口上删除关联的策略	undo qos apply policy { inbound outbound }

QoS 策略在接口视图下应用的规则如下：

- 普通物理接口和 MP 引用的 VT，可以应用配置了各种特性（包括 **remark**、**car**、**gts**、**queue af**、**queue ef**、**queue wfq**、**wred** 等）的策略。
- 配置了流量整形（**gts**）和队列（**queue ef**、**queue af**、**queue wfq**）特性的策略，不能作为入方向策略应用在入接口上。
- 子接口不支持队列（**queue ef**、**queue af**、**queue wfq**）特性，但是支持流量整形（**gts**）与流量监管（**car**）。所以只配置了流量整形与流量监管的策略可以应用到子接口。

3.6.6 基于类的队列的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示基于类的队列的运行情况，通过查看显示信息验证配置的效果。

表3-46 基于类的队列的显示和调试

操作	命令
显示防火墙配置的类信息	display traffic classifier { system-defined user-defined } [<i>tcl-name</i>]

操作	命令
显示防火墙配置的流行为信息	display traffic behavior { system-defined user-defined } [<i>behavior-name</i>]
显示指定策略中指定类及与类关联的流行为的配置信息	display qos policy { system-defined user-defined } [<i>policy-name</i> [classifier <i>tcl-name</i>]]
显示指定接口或所有接口上策略的配置信息和运行情况	display qos policy interface [<i>interface-type</i> <i>interface-number</i> [inbound outbound]]
显示指定接口或所有接口的基于类的队列配置信息和运行情况。	display qos cbq interface [<i>interface-type</i> <i>interface-number</i>]
显示队列调试信息	debugging qos cbq { ef af be }

3.7 RTP 优先队列的配置

RTP 报文队列的配置包括：

- 在接口上应用 RTP 队列
- 配置带宽限制
- RTP 队列的显示和调试

3.7.1 在接口上应用 RTP 队列

设置接口上应用 RTP 队列。此命令没有缺省配置。

请在接口视图下进行如下配置。

表3-47 在接口上应用 RTP 队列

操作	命令
在接口上应用 RTP 队列	qos rtpq start-port <i>start-port-number</i> end-port <i>end-port-number</i> bandwidth <i>bandwidth</i> [cbs <i>committed-burst-size</i>]
关闭 RTP 队列在接口上的应用	undo qos rtpq



注意：

Dialer 口上可以应用 RTP 队列，但是只有当物理接口上配置为缺省队列，同时物理接口带宽足够的情况下，RTP 队列才能成功应用到 Dialer 口上。

3.7.2 配置最大预留带宽

配置最大预留带宽占接口实际可用带宽的百分比。

请在接口视图下进行下列配置。

表3-48 配置带宽限制

操作	命令
配置带宽限制	qos reserved-bandwidth pct <i>percentage</i>
恢复缺省的带宽限制	undo qos reserved-bandwidth

参数 *percentage* 是预留带宽占可用带宽的百分比，取值范围为 1~100，缺省值为 80。

3.7.3 RTP 报文队列的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示当前 RTP 队列机制的队列信息，包括当前的 RTP 队列长度和 RTP 报文的丢包数，显示所有接口的 RTP 队列配置情况和统计信息，通过查看显示信息验证配置的效果。

表3-49 显示接口 RTP 队列的配置情况和统计信息

操作	命令
显示接口 RTP 队列的配置情况和统计信息	display qos rtpq interface [<i>interface-type</i> <i>interface-number</i>]

3.8 典型配置举例

3.8.1 优先队列配置举例

1. 配置需求

如图 3-6所示，Server1 和 PC1 通过 SecPath1 向 PC2 发送数据（其中 Server1 发送关键业务数据，PC1 发送非关键业务数据）时，由于 SecPath1 入接口 ethernet0/0/0 的速率大于出接口 ethernet2/0/0 的速率，在 ethernet2/0/0 接口处可能发生拥塞，导致丢包。要求在网络拥塞时保证 server1 发送的关键业务数据得到优先处理。

2. 组网图

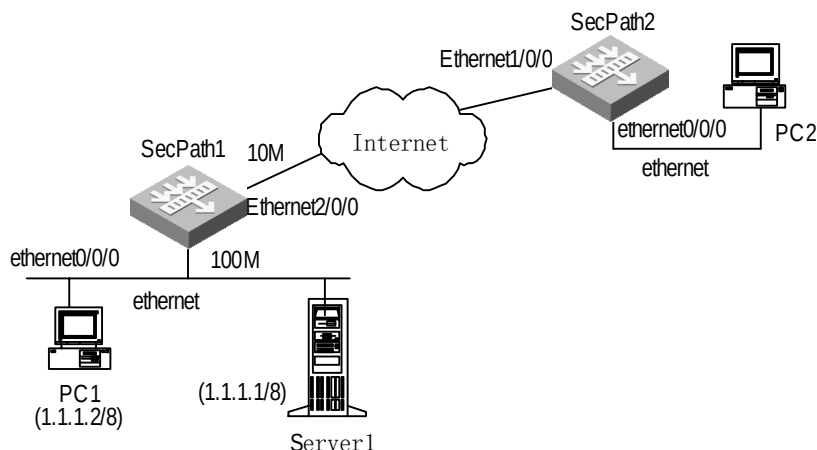


图3-6 优先队列配置组网图

3. 配置步骤

配置 SecPath1:

配置 ACL 规则列表，分别匹配来源于 Server1 和 PC1 的报文。

```
[H3C] acl number 2001
[H3C-acl-basic-2001] rule permit source 1.1.1.1 0
[H3C] acl number 2002
[H3C-acl-basic-2002] rule permit source 1.1.1.2 0
```

配置优先队列规则组，使得网络拥塞发生时，源自 Server1 的报文能够进入 PQ 的 top 队列缓存，源自 PC1 的报文能够进入 bottom 队列缓存，并且设定 top 队列的最大队列长度为 50、bottom 队列的最大队列长度为 100。

```
[H3C] qos pql 1 protocol ip acl 2001 queue top
[H3C] qos pql 1 protocol ip acl 2002 queue bottom
[H3C] qos pql 1 queue top queue-length 50
[H3C] qos pql 1 queue bottom queue-length 100
```

在接口 ethernet2/0/0 上启用优先队列规则组 1

```
[H3C] interface ethernet2/0/0
[H3C-Ethernet2/0/0] qos pq pql 1
```

3.8.2 基于类的队列配置举例

1. 组网需求

在下面的组网图中，从 SecPathC 发出的数据流经过 SecPathA 和 SecPathB 到达 SecPathD。SecPathC 发出的数据流根据 IP 报文的 DSCP 域分为 3 类，要求配置 QoS 策略，对于 DSCP 域为 AF11 和 AF21 的流进行确保转发（AF），最小带宽为 5%；对于 DSCP 域为 EF 的流进行加速转发（EF），最大带宽为 30%。

EF 流可以保证一定带宽,并保证时延和时延抖动,对于 EF 流的优先保证是通过 LLQ 技术实现的。AF 流只保证带宽, default 流(即不匹配任何定义的类的流)则没有带宽和时延保证。

在开始下面的配置之前,应保证:

- SecPathC 发出的流能够通过 SecPathA 和 SecPathB 可达 SecPathD。
- 报文的 DSCP 域在进入 SecPathA 之前已经设置完毕。

2. 组网图

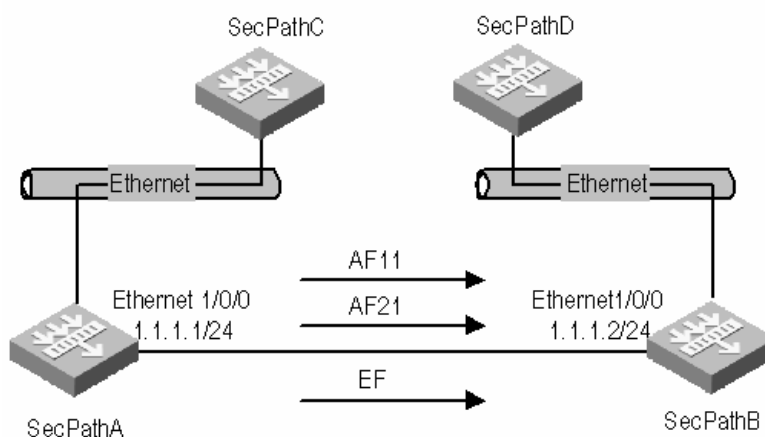


图3-7 基于类的队列配置组网图

3. 配置步骤

在 SecPathA 上进行配置。

定义三个类, 分别匹配 DSCP 域为 AF11、AF21 和 EF 的 IP 报文。

```
[H3C] traffic classifier af11_class
[H3C-classifier-af11_class] if-match dscp af11
[H3C-classifier-af11_class] traffic classifier af21_class
[H3C-classifier-af21_class] if-match dscp af21
[H3C-classifier-af21_class] traffic classifier ef_class
[H3C-classifier-ef_class] if-match dscp ef
[H3C-classifier-ef_class] quit
```

定义流行为, 配置 AF, 并分配最小可用带宽。

```
[H3C] traffic behavior af11_behav
[H3C-behavior-af11_behav] queue af bandwidth pct 5
[H3C-behavior-af11_behav] traffic behavior af21_behav
[H3C-behavior-af21_behav] queue af bandwidth pct 5
[H3C-behavior-af21_behav] quit
```

定义流行为, 配置 EF, 并分配最小可用带宽(对于 EF 流, 将同时保证带宽和时延)。

```
[H3C] traffic behavior ef_behav
[H3C-behavior-ef_behav] queue ef bandwidth pct 30
[H3C-behavior-ef_behav] quit

# 定义 QoS 策略，将已配置的流行为指定给不同的类。

[H3C] qos policy dscp
[H3C-qospolicy-dscp] classifier af11_class behavior af11_behav
[H3C-qospolicy-dscp] classifier af21_class behavior af21_behav
[H3C-qospolicy-dscp] classifier ef_class behavior ef_behav
[H3C-qospolicy-dscp] quit

# 将已定义的 QoS 策略应用在 SecPathA 的 ethernet1/0/0 出方向。

[H3C] interface ethernet1/0/0
[H3C-Ethernet1/0/0] ip address 1.1.1.1 255.255.255.0
[H3C-Ethernet1/0/0] qos apply policy dscp outbound
```

配置完成后，当发生拥塞时，可以观察到 EF 流被以较高的优先级转发。

3.8.3 定制队列配置举例

1. 组网需求

在下面的组网图中，两台防火墙 SecPathA 和 SecPathB 通过 Internet 连接，连接 SecPathA 的 PC 机作为 FTP 以及 HTTP 的服务器端，连接 SecPathB 的 PC 机作为 FTP 以及 HTTP 的客户端。配置路由使得数据流均经过 SecPathA 的接口转发至 SecPathB。

在开始下列配置前应保证：

- SecPathA 与 SecPathB 建立起连接，并且两台 PC 机建立起 FTP 连接。
- 连接 SecPathB 的 PC 机作为客户端从连接 SecPathA 的 server 端下载一个较大的文件，同时用 SecPathB 端的 PC 机用 http 协议从 SecPathA 端的 http server 上下载大文件。

定制 FTP 数据流与 HTTP 数据流以 1:2 的比例分享链路带宽。

2. 组网图

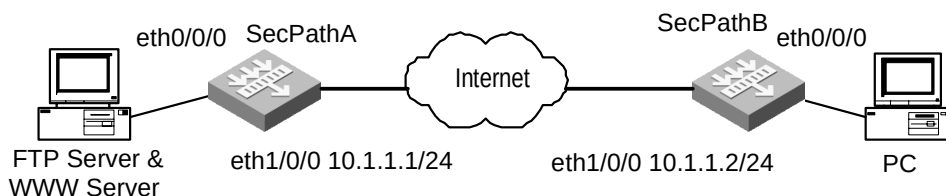


图3-8 定制队列配置组网图

3. 配置步骤

在 SecPathA 上进行配置。

配置 acl 规则分别匹配 FTP 报文与 HTTP 报文：

```
[H3C] acl number 3001
[H3C-acl-adv-3001] rule 0 permit tcp source-port eq ftp
[H3C-acl-adv-3001] rule 1 permit tcp source-port eq ftp-data
[H3C-acl-adv-3001] rule 2 deny ip
[H3C] quit
[H3C] acl number 3002
[H3C-acl-adv-3001] rule 0 permit tcp source-port eq www
[H3C-acl-adv-3001] rule 1 deny ip
[H3C-acl-adv-3001] quit
```

配置 CQ 规则，定制 FTP 流与 HTTP 流按 1: 2 的比例分享链路带宽。

```
[H3C] qos cql 1 queue 11 serving 1000
[H3C] qos cql 1 queue 12 serving 2000
[H3C] qos cql 1 protocol ip acl 3001 queue 11
[H3C] qos cql 1 protocol ip acl 3002 queue 12
```

将该规则应用在接口的出方向上。

```
[H3C] interface Ethernet1/0/0
[H3C-Ethernet1/0/0] ip address 10.1.1.1 255.255.255.0
[H3C-Ethernet1/0/0] qos cq cql 1
[H3C-Ethernet1/0/0] quit
```

第4章 DAR 配置

4.1 DAR 简介

Internet 已成为企业实现各种业务的主要媒介，各种基于业务的应用也不断地涌现。在这种形势下，仅仅依靠目前对报文中的 IP 报头进行检查的简单机制，已不能适应需求，所以提出了基于业务的深度应用识别的概念。

DAR（Deeper Application Recognition，深度应用识别）是一个智能的识别分类工具，它可以对报文中第 4 层到第 7 层的内容和一些动态协议（如 BT、HTTP、FTP、RTP）进行检查和识别，以区分出各种基于应用的协议，弥补了原先只能对报文进行简单分类的不足。

通过对报文进行深度的识别和分类，大大加强了用户对数据流的控制力度。将 DAR 与 QoS 模块结合起来，可以更有效地为关键业务的数据实施高优先级的策略，进一步保护了用户的投资。

4.2 配置 DAR

4.2.1 配置协议的匹配规则

当对数据流应用各种策略（如设置报文的优先级，为数据流分配带宽等）时，首先需要使用 DAR 的深度识别功能对数据流进行分类。

请在类视图下进行下列配置。

表4-1 定义或删除协议匹配规则

操作	命令
定义协议匹配规则	if-match [not] protocol <i>protocol-name</i>
删除协议匹配规则	undo if-match [not] protocol <i>protocol-name</i>

缺省情况下，未配置协议匹配规则。

4.2.2 配置 HTTP 协议的匹配规则

DAR 可以通过检查 HTTP 报文中的内容（如 HTTP 报文中的 URL 地址、hostname 主机名和 MIME 类型）对报文进行分类。

请在类视图下进行下列配置。

表4-2 定义或删除 HTTP 协议匹配规则

操作	命令
定义 HTTP 协议的匹配规则	if-match [not] protocol http [url <i>url-string</i> host <i>hostname-string</i> mime <i>mime-type</i>]
删除 HTTP 协议的匹配规则	undo if-match [not] protocol http [url <i>url-string</i> host <i>hostname-string</i> mime <i>mime-type</i>]

缺省情况下，未配置 HTTP 协议的匹配规则。

4.2.3 配置 RTP 协议的匹配规则

DAR 可以通过检查 RTP（Real-Time Transfer Protocol，实时传输协议）报文的负载类型对数据流进行分类。

请在类视图下进行下列配置。

表4-3 定义或删除 RTP 协议匹配规则

操作	命令
定义 RTP 协议的匹配规则	if-match [not] protocol rtp [payload-type { audio video <i>payload-string</i> }*]
删除 RTP 协议的匹配规则	undo if-match [not] protocol rtp [payload-type { audio video <i>payload-string</i> }*]

缺省情况下，未配置 RTP 协议的匹配规则。

4.2.4 配置 DAR 应用协议的端口号

系统预先定义了大量的协议及其使用的端口号，这些协议包括一些知名的协议和 10 个用户预定义协议 **user-defined01**、**user-defined02**、……、**user-defined10**。用户可以使用以下命令为这些协议赋予自定义的端口号，增强了应用的扩展性。

请在系统视图下进行下列配置。

表4-4 配置 DAR 应用协议的端口号

操作	命令
配置 DAR 应用协议的端口号	dar protocol <i>protocol-name</i> { tcp udp } port { <i>portvalue</i> range <i>port-min</i> <i>port-max</i> }*
恢复 DAR 应用协议的端口号为缺省值	undo dar protocol <i>protocol-name</i> { tcp udp } port

缺省情况下，十个用户预定义协议无端口号，其余各协议均有其缺省的端口号。

4.2.5 重命名用户预定义协议

缺省情况下，系统创建了十个用户预定义协议，名称为 **user-defined01**、**user-defined02**、……、**user-defined10**。用户可以使用以下配置对其进行重命名，以便于用户记忆和管理。

请在系统视图下进行下列配置。

表4-5 重命名用户预定义协议

操作	命令
重命名用户预定义协议	dar protocol-rename <i>old-name</i> <i>user-defined-name</i>
恢复用户预定义协议的缺省名称	undo dar protocol-rename <i>user-defined-name</i>

4.2.6 使能/关闭 DAR 的报文统计功能

通过使能 DAR 的报文统计功能，用户可以及时对各个接口上的应用协议的报文个数、数据流量以及流量的历史平均速率和历史最大速率进行监控，便于对数据流实施相应的策略。

请在以太网接口视图下进行下列配置。

表4-6 使能/关闭 DAR 的报文统计功能

操作	命令
使能 DAR 的报文统计功能	dar protocol-statistic [<i>flow-interval time</i>]
关闭 DAR 的报文统计功能	undo dar protocol-statistic

缺省情况下，关闭 DAR 的报文统计功能。

4.2.7 配置 DAR 可识别的最大连接数

当有大量的数据流经设备时，若 DAR 对其进行一一识别，将会消耗大量的系统资源，从而影响其它功能模块的正常工作。为了避免这种现象，用户可以对 DAR 能够识别的最大连接数目进行限制，以节省宝贵的系统资源。当连接数目超过设定的最大阈值时，DAR 将不再对其进行识别，直接将其标记为无法识别的报文。

请在系统视图下进行下列配置。

表4-7 配置 DAR 可识别的最大连接数

操作	命令
配置 DAR 可识别的最大连接数	dar max-session-count <i>count</i>
恢复 DAR 可识别的最大连接数的缺省值	undo dar max-session-count

DAR 可识别的最大连接数的缺省值与产品型号有关，请以实际产品为准。

4.3 DAR 的显示和调试

在任意视图下使用 **display** 命令可以对 DAR 的配置情况和运行状态进行查看；在用户视图下使用 **debugging** 命令可以对 DAR 进行调试；在用户视图下使用 **reset** 命令可以清除 DAR 的统计和会话信息。

表4-8 DAR 的显示和调试

操作	命令
查看 DAR 的模块信息	display dar information
查看 DAR 的协议信息	display dar protocol { all protocol-name }
查看用户预定义协议的重命名信息	display dar protocol-rename
查看 DAR 的报文统计信息	display dar protocol-statistic [protocol protocol-name top top-number all] [interface type number] [direction { in out }]
打开 DAR 的调试信息开关	debugging dar { packet event error all }
关闭 DAR 的调试信息开关	undo debugging dar { packet event error all }
清除会话连接缓存	reset dar session
清除 DAR 的协议统计信息	reset dar protocol-statistic { { protocol protocol-name interface type number }* all }

4.4 DAR 典型配置举例

4.4.1 DAR 配置举例

1. 组网需求

局域网 192.168.1.0/24 内的用户通过防火墙访问 Internet。为了确保关键业务数据的正常传输，要求为此数据流保证 1Mbps 带宽。此数据流基于 TCP 协议，使用的端口号为 10000。

2. 组网图

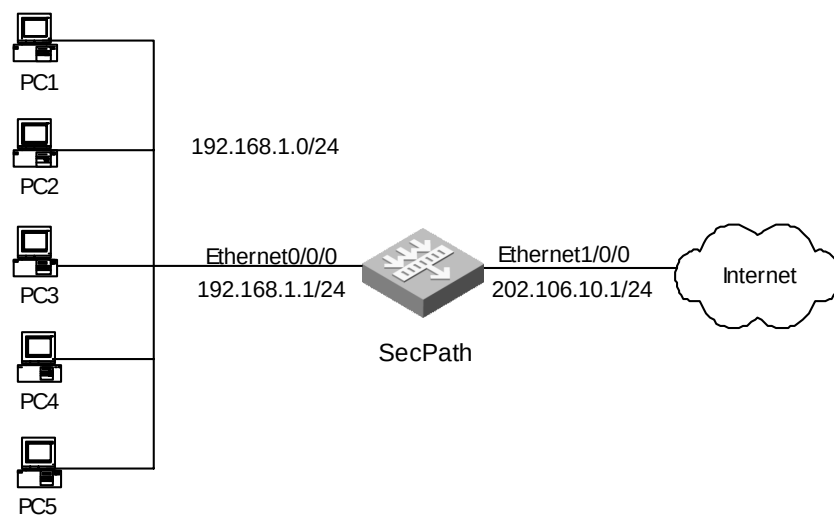


图4-1 DAR 典型应用组网图

3. 配置步骤

配置协议 user-defined01 使用 TCP 端口号 10000。

```
<H3C> system-view
```

```
[H3C] dar protocol user-defined01 tcp port 10000
```

创建类并设置匹配规则。

```
[H3C] traffic classifier test
```

```
[H3C-classifier-test] if-match protocol user-defined01
```

```
[H3C-classifier-test] quit
```

配置流行为。

```
[H3C] traffic behavior 1
```

```
[H3C-behavior-1] queue af bandwidth 1000
```

```
[H3C-behavior-1] quit
```

配置 QoS 策略。

```
[H3C] qos policy 1
```

```
[H3C-qospolicy-1] classifier test behavior 1
```

```
[H3C-qospolicy-1] quit
```

在接口上应用 QoS 策略。

```
[H3C] interface Ethernet 1/0/0
```

```
[H3C-Ethernet1/0/0] qos apply policy 1 outbound
```

第5章 拥塞避免

5.1 拥塞避免简介

过度的拥塞会对网络资源造成极大危害，必须采取某种措施加以解除。这里所说的拥塞避免（Congestion Avoidance），是指通过监视网络资源（如队列或内存缓冲区）的使用情况，在拥塞有加剧的趋势时，主动丢弃报文，通过调整网络的流量来解除网络过载的一种流控机制。

与端到端的流控相比，这里的流控有更广泛的意义，它影响到防火墙中更多的业务流的负载。当然，防火墙在丢弃报文时，并不排斥与源端的流控动作比如 TCP 流控的配合，更好地调整网络的流量到一个合理的负载状态。好的丢包策略和源端流控机制的组合，总是追求网络的吞吐量和利用效率最大化，并且使报文丢弃和延迟最小化。

1. 传统的丢包策略

传统的丢包策略采用尾部丢弃（Tail-Drop）的方法。当队列的长度达到某一最大值后，所有新到来的报文都将被丢弃。

这种丢弃策略会引发 TCP 全局同步现象——当队列同时丢弃多个 TCP 连接的报文时，将造成多个 TCP 连接同时进入拥塞避免和慢启动状态以降低并调整流量，而后又会在某个时间同时出现流量高峰，如此反复，使网络流量忽大忽小，造成网络带宽利用率降低，使带宽利用率总在高峰和低谷间振荡。

2. RED 与 WRED

为避免 TCP 全局同步现象，可使用 RED（Random Early Detection，随机早期检测）或 WRED（Weighted Random Early Detection，加权随机早期检测）。

在 RED 类算法中，为每个队列都设定一对低限和高限值，并规定：

- 当队列的长度小于低限时，不丢弃报文。
- 当队列的长度超过高限时，丢弃所有到来的报文。
- 当队列的长度在低限和高限之间时，开始随机丢弃到来的报文。方法是为每个到来的报文赋予一随机数，并用该随机数与当前队列的丢弃概率比较，如果大于丢弃概率则被丢弃。队列越长，丢弃概率越高——但有一个最大丢弃概率。

与 RED 不同，WRED 生成的随机数是基于优先权的，它引入 IP 优先权区别丢弃策略，考虑了高优先权报文的利益并使其被丢弃的概率相对较小。

RED 和 WRED 通过随机丢弃报文避免了 TCP 的全局同步现象——当某个 TCP 连接的报文被丢弃，开始减速发送的时候，其他的 TCP 连接仍然有较高的发送速度。这样，无论什么时候，总有 TCP 连接在进行较快的发送，提高了线路带宽的利用率。

直接采用队列的长度和低限、高限比较并进行丢弃（这是设置队列门限的绝对长度），将会对突发性的数据流造成不公正的待遇，不利于数据流的传输。所以，在和低限、高限比较并进行丢弃时，采用队列的平均长度（这是设置队列门限与平均长度比较的相对值）。计算 WRED 平均队列长度的公式：

平均队列长度 = (以前的平均队列长度 * (1 - 1 / (2 的 n 次方))) + (当前队列长度 * (1 / (2 的 n 次方)))

其中 n 是权重因子，是一个可配的参数。队列的平均长度既反映了队列的变化趋势，又对队列长度的突发变化不敏感，避免了对突发性数据流的不公正待遇。

当队列机制采用 WFQ 时，可以为不同优先级（precedence）的报文设定不同的权重因子、上限、下限、丢弃概率，从而对不同优先级的报文提供不同的丢弃特性。

WRED 和队列机制的关系如下图所示。

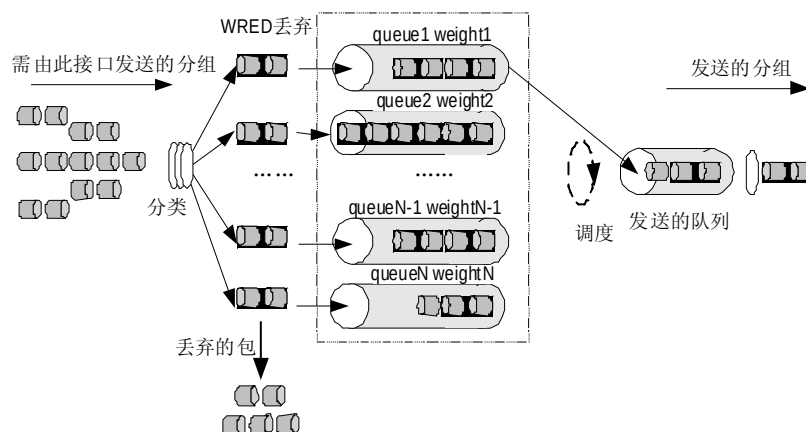


图5-1 WRED 和队列机制关系示意图

当 WRED 和 WFQ 配合使用时，可以实现基于流的 WRED。这是因为，在进行分类的时候，不同的流有自己的队列，对于流量小的流，由于其队列长度总是比较小，所以丢弃的概率将比较小。而流量大的流将会有较大的队列长度，从而丢弃较多的报文，保护了流量较小的流的利益。

5.2 WRED 的配置

WRED 的配置包括：

- 使用 WRED
- 设置 WRED 计算平均队列长度的指数
- 设置 WRED 各优先级参数

5.2.1 使用 WRED

请在接口视图下进行下列配置。

表5-1 使用 WRED

操作	命令
使用 WRED	qos wred [ip-precedence dscp]
恢复缺省形式	undo qos wred

WRED 只能和 WFQ 共同使用，不能单独使用或和其它的队列共同使用。

缺省情况为不使用 WRED，队列的丢弃方法为尾部丢弃。

 说明：

使用 WRED 之前接口上必须已经应用了 WFQ。

5.2.2 设置 WRED 计算平均队列长度的指数

设置 WRED 计算平均队列长度的滤波系数。

请在接口视图下进行下列配置。

表5-2 设置 WRED 计算平均队列长度的指数

操作	命令
设置 WRED 计算平均队列长度的指数	qos wred weighting-constant <i>exponent</i>
恢复指数的缺省值	undo qos wred weighting-constant

其中 *exponent* 为计算平均队列长度的滤波系数，取值范围为 1~16，缺省值为 9。

必须先使用 **qos wred** 在接口上应用 WRED，才可以配置 WRED 的参数。

5.2.3 设置 WRED 各优先级参数

当接口配置加权公平队列时，可以设置 WRED 各优先级的下限、上限以及丢弃概率分母。

请在接口视图下进行下列配置。

表5-3 设置 WRED 各优先级参数

操作	命令
设置 WRED 优先级参数	qos wred ip-precedence <i>ip-precedence</i> low-limit <i>low-limit</i> high-limit <i>high-limit</i> discard-probability <i>discard-prob</i>
恢复各优先级参数的缺省值	undo qos wred ip-precedence <i>ip-precedence</i>

必须先使用 **qos wred** 在接口上应用 WRED，才可以配置 WRED 的参数。

5.2.4 设置 WRED 各 DSCP 参数

当接口配置加权公平队列时，可以设置 WRED 各 DSCP 的下限、上限以及丢弃概率分母。

请在接口视图下进行下列配置。

表5-4 设置 WRED 各 DSCP 参数

操作	命令
设置 WRED 各 DSCP 参数	qos wred dscp <i>dscp-value</i> low-limit <i>low-limit</i> high-limit <i>high-limit</i> discard-probability <i>discard-prob</i>
恢复各 DSCP 参数的缺省值	undo qos wred dscp <i>dscp-value</i>

必须先使用 **qos wred** 在接口上应用 WRED，才可以配置 WRED 的参数。

5.3 WRED 的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示接口的 WRED 配置情况和统计信息，通过查看显示信息验证配置的效果。

表5-5 显示接口的 WRED 配置情况和统计信息

操作	命令
显示接口的 WRED 配置情况和统计信息	display qos wred interface [<i>interface-type</i> <i>interface-number</i>]

该命令可以显示某个接口或所有接口的 WRED 配置情况和统计信息

- *interface-type* 为接口类型。
- *interface-number* 为接口号。

第6章 MPLS QoS

6.1 MPLS QoS 概述

MPLS 的 QoS 主要完成以下功能：

根据需要在 CE 上或 PE 上对业务流进行分类，例如：把业务流分为三类：语音、视频和数据。

PE 在给报文加 Label 时，把 IP 报文携带的 IP 优先级标记影射到标签的 CoS 域，这样原来由 IP 携带的类型信息，现在由标签携带。

在 PE 路由器之间，根据标签的 CoS 域，进行有差别的调度（如 PQ、WFQ、CBQ 等），即把携带标签的业务流在一条 LSP 上进行有差别的 QoS 的传送。

 说明：

本章用户需要有 MPLS 相关知识背景。如需了解 MPLS 基本概念以及相关配置，请参考本书 MPLS 配置部分，本章仅涉及 MPLS QoS 的配置。

6.2 MPLS QoS 配置

配置 MPLS QoS 首先要进行 MPLS 的相关配置并指定为显示路由转发方式。MPLS 的详细配置请参见本手册的“MPLS”部分。本章仅介绍 MPLS QoS 的配置。

MPLS QoS 的可以分为四种：

- MPLS PQ
- MPLS CQ
- MPLS CBQ
- MPLS CAR

下面对这四种 MPLS QoS 的配置分别进行说明。

6.2.1 配置 MPLS PQ

配置 MPLS PQ 有两个步骤。首先要根据 MPLS EXP 配置优先列表，然后在接口上应用此优先列表。相关说明可参考“拥塞管理”中的“PQ 配置”。

1. 根据 MPLS EXP 配置优先列表

根据 MPLS EXP 值配置优先列表，并使匹配的分组进入不同的优先队列。

请在系统视图进行下列配置。

表6-1 根据网络协议配置优先列表

操作	命令
根据网络协议配置优先列表	qos pql pql-index protocol mpls exp mpls-experimental-value queue { top middle normal bottom }
删除 pql-index 中相应的分类规则	undo qos pql pql-index protocol mpls exp mpls-experimental-value

优先队列的相关配置请参见 3.1.1 拥塞管理策略。

2. 在接口上应用优先列表组

将一组优先列表应用到接口上。对于同一个接口，本命令的重复使用将为接口设定新的优先列表组。

请在接口视图下进行下列配置。

表6-2 在接口上应用优先列表组

操作	命令
在接口上应用优先列表组	qos pq pql pql-index
将接口的拥塞管理策略恢复为 FIFO	undo qos pq

6.2.2 配置 MPLS CQ

配置 MPLS CQ 有两个步骤。首先要根据 MPLS EXP 配置定制列表，然后在接口上应用此定制列表。相关说明可参考“拥塞管理”中的“CQ 配置”。

1. 根据 MPLS EXP 配置定制列表

根据 MPLS EXP 配置定制列表，并使匹配的分组进入不同的定制队列。

请在系统视图下进行下列配置。

表6-3 根据网络协议配置定制列表

操作	命令
根据 MPLS EXP 配置定制列表	qos cql cql-index protocol mpls exp experimental-number queue queue-number
删除相应的分类规则	undo qos cql cql-index protocol mpls exp experimental-number

*queue-number*取值为 0~16。关于定制队列的配置请参见 3.1.1 拥塞管理策略。

2. 在接口上应用定制列表

请在接口视图下进行下列配置。

表6-4 在接口上应用定制列表

操作	命令
在接口上应用定制列表	qos cq cql cql-index
将接口的拥塞管理策略恢复到 FIFO	undo qos cq

6.2.3 配置 MPLS CBQ

配置 MPLS CBQ 有四个步骤。第一，要定义类，根据 MPLS EXP 配置类的匹配规则；第二，要定义流行为，配置处理 MPLS EXP 域的方案；第三，定义一个 QoS 策略，为每个类指定具体的流行为；第四，在接口上应用此 QoS 策略。相关说明可参考“拥塞管理”中的“CBQ 配置”。

1. 配置匹配 mpls 报文的 exp 域的分类规则

MPLS QoS 允许用户在 PE 上通过 MPLS EXP 域来对 MPLS 报文进行分类并进入不同的队列，实现 QoS，IP 报文则不加改变地透明穿过 MPLS 网络。

首先要定义一个类并进入类视图，然后在类视图中配置匹配 mpls 报文的 exp 域的分类规则。

请在系统视图下进行下列配置。

表6-5 定义一个类并进入类视图

操作	命令
定义类并进入类映射视图	traffic classifier tcl-name [operator { and or }]
删除类并进入类映射视图	undo traffic classifier tcl-name [operator { and or }]

请在类视图下进行下列配置。

表6-6 匹配 mpls 的 exp 域的规则

操作	命令
定义匹配 MPLS 的 exp 域的规则	if-match [not] mpls-exp { mpls-experimental-value }
删除匹配 MPLS 的 exp 域的规则	undo if-match [not] mpls-exp

2. 设置 MPLS CBQ 流行为

首先在流行为视图下配置设置 MPLS EXP 域的值，然后在策略视图下将类与流行为关联，这样就可以对匹配类的报文进行 MPLS EXP 域的标记。

请在系统视图下进行下列配置。

表6-7 定义一个流行为并进入流行为视图

操作	命令
定义一个流行为并进入流行为视图	traffic behavior <i>behavior-name</i>
删除流行为	undo traffic behavior <i>behavior-name</i>

请在流行为视图下进行下列配置。

表6-8 设置 MPLS EXP 域的值来标记匹配的报文

操作	命令
设置 MPLS EXP 域的值来标记匹配的报文	remark mpls-exp <i>mpls-experimental-value</i>
取消 MPLS EXP 域的值	undo remark mpls-exp

3. 配置 MPLS CBQ 策略

首先要定义一个 QoS 策略名称，然后在 QoS 策略中为类指定流行为，即对不同类的报文标记不同的 EXP 值。

请在系统视图下进行下列配置。

表6-9 定义策略并进入策略视图

操作	命令
定义策略并进入策略视图	qos policy <i>policy-name</i>
删除指定策略	undo qos policy <i>policy-name</i>

请在策略视图下进行下列配置。

表6-10 在策略中为类指定流行为

操作	命令
在策略中为类指定采用的流行为	classifier <i>tcl-name</i> behavior <i>behavior-name</i>
取消指定类在策略中的使用	undo classifier <i>tcl-name</i>

tcl-name：类名，必须是已经定义的类，可以是系统定义或用户定义类。

behavior-name：必须是已定义的流行为名，可以是系统定义或用户定义流行为。

4. 应用 QoS 策略

请在接口视图下进行下列配置。

表6-11 将接口与所设置的策略相关联

操作	命令
在接口应用关联的策略	qos apply policy <i>policy-name</i> { inbound outbound }
在接口删除关联的策略	undo qos apply policy { inbound outbound }

6.2.4 配置 MPLS CAR

配置 MPLS CAR 有两个步骤。一是确定哪些报文需要实施监管，二是定义对这些报文的监管策略。确定哪些报文需要实施监管的方法可以使用访问控制列表 (ACL)，也可以使用 TP 列表 (*carl-index*)。如果要对所有报文都进行监管，可以使用关键字 “**any**”。相关说明可参考“流量监管配置”。

1. 接口应用 TP 策略，对 MPLS 报文进行标记

在接口应用 TP 策略 (CAR)，对 MPLS 报文进行标记。

请在接口视图下进行下列配置。

表6-12 在接口应用 TP 策略，对 MPLS 报文进行标记

操作	命令
在接口应用 TP 策略，对 MPLS 报文进行标记	qos car inbound { any acl <i>acl-number</i> carl <i>carl-index</i> } cir <i>committed-information-rate</i> cbs <i>committed-burst-size</i> ebs <i>excess-burst-size</i> green action red action
取消在接口应用的 TP 策略	undo qos car inbound { any acl <i>acl-number</i> carl <i>carl-index</i> } cir <i>committed-information-rate</i> cbs <i>committed-burst-size</i> ebs <i>excess-burst-size</i>

action 的取值为：

- **remark-mpls-exp-continue** *new-mpls-exp*：设置新的 MPLS EXP 值 *new-mpls-exp*，并继续由下一个 CAR 策略处理，取值范围 0~7。
- **remark-mpls-exp-pass** *new-mpls-exp*：设置新的 MPLS EXP 值 *new-mpls-exp*，并发送数据包到目的地址，取值范围 0~7。

只能在 PE 的入接口上才可以设置 MPLS 报文的 EXP 域。如果入方向为 IP 报文，出方向封装为 MPLS 报文，则配置的 TP 策略（设置 MPLS 报文的 EXP 域）生效。设置 MPLS 报文的 EXP 域时，两层标签都要设置，但不修改 IP 头部中的 TOS 域。

6.3 MPLS QoS 典型配置举例

6.3.1 对同一 VPN 内的流进行 QoS 配置

1. 组网需求

在下面的组网图中，CE1 和 CE2 都属于 VPN1，PE1 与 P 之间的链路带宽为 10M，P 与 PE2 之间的链路带宽为 10M，要求对 VPN1 中优先级不同的流给予不同的 QoS 保证。

此举例的配置可分为两个主要部分：

首先在 CE1、PE1、P、PE2 和 CE2 进行 MPLS VPN 的配置：

- PE1、P、PE2 之间运行 OSPF；
- PE 与 CE 之间建立 MP-EBGP 邻居；
- PE 与 PE 之间建立 MP-IBGP 邻居。

然后是在 PE1 和 P 上进行 MPLS QoS 的配置：

- 在 PE1 的入接口 Ethernet1/0/1 上配置 QoS 策略，根据 MPLS 报文的 DSCP 属性，设置报文 EXP 域的值。
- 在 P 上，根据 MPLS 报文的 EXP 域值区分流，并配置基于流的队列 CBQ：对于 EXP 为 1 的流保证 10%的带宽；对于 EXP 为 2 的流保证 20%的带宽；对于 EXP 为 3 的流保证 30%的带宽；而对于 EXP 为 4 的流，保证 40%的带宽并保证时延。

说明：

MPLS VPN 的配置请参考本手册“MPLS 操作”部分，本节只描述 MPLS QoS 部分的配置。

2. 组网图

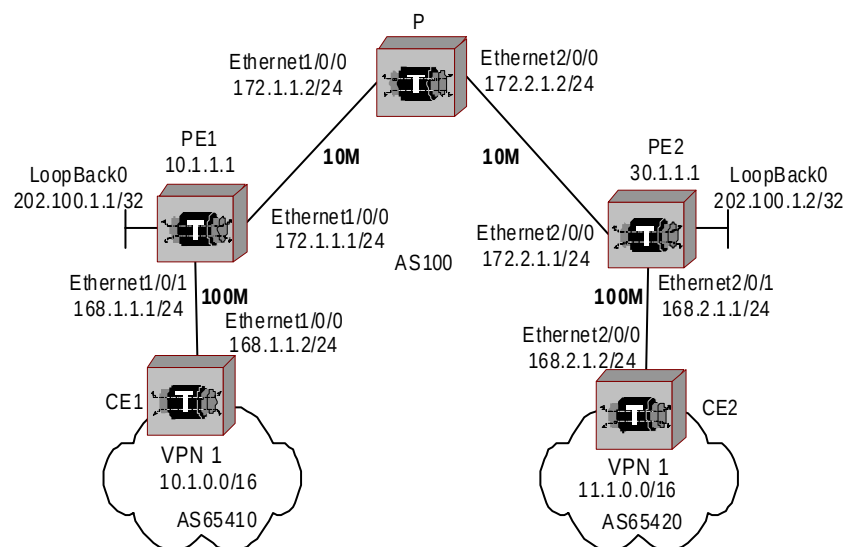


图6-1 MPLS QoS 组网图

3. 配置步骤

(1) PE1 的配置

定义四个类，分别匹配同一 VPN 内 DSCP 分别为 AF11、AF21、AF31 和 EF 的 MPLS 报文。

```
[PE1] traffic classifier af11
[PE1-classifier-af11] if-match dscp af11
[PE1-classifier-af11] traffic classifier af21
[PE1-classifier-af21] if-match dscp af21
[PE1-classifier-af21] traffic classifier af31
[PE1-classifier-af31] if-match dscp af31
[PE1-classifier-af31] traffic classifier efclass
[PE1-classifier-efclass] if-match dscp ef
[PE1-classifier-efclass] quit
```

定义四个流行为，设置 MPLS 报文 EXP 域的值。

```
[PE1] traffic behavior exp1
[PE1-behavior-exp1] remark mpls-exp 1
[PE1-behavior-exp1] traffic behavior exp2
[PE1-behavior-exp2] remark mpls-exp 2
[PE1-behavior-exp2] traffic behavior exp3
[PE1-behavior-exp3] remark mpls-exp 3
[PE1-behavior-exp3] traffic behavior exp4
[PE1-behavior-exp4] remark mpls-exp 4
[PE1-behavior-exp4] quit
```

定义 QoS 策略，为不同类的报文指定流行为，即对不同类的报文标记不同的 EXP 值。

```
[PE1] qos policy REMARK
[PE1-qospolicy-REMARK] classifier af11 behavior exp1
[PE1-qospolicy-REMARK] classifier af21 behavior exp2
[PE1-qospolicy-REMARK] classifier af31 behavior exp3
[PE1-qospolicy-REMARK] classifier efclass behavior exp4
[PE1-qospolicy-REMARK] quit
```

在 MPLS 网络的 PE 入接口上应用已定义的 QoS 策略。

```
[PE1] interface ethernet 1/0/1
[PE1-Ethernet1/0/1] qos apply policy REMARK inbound
[PE1-Ethernet1/0/1] quit
```

(2) P 的配置

定义四个类，分别匹配 EXP 域为 1、2、3 和 4 的 MPLS 报文。

```
[P] traffic classifier EXP1
[P-classifier-EXP1] if-match mpls-exp 1
[P-classifier-EXP1] traffic classifier EXP2
[P-classifier-EXP2] if-match mpls-exp 2
[P-classifier-EXP2] traffic classifier EXP3
[P-classifier-EXP3] if-match mpls-exp 3
[P-classifier-EXP3] traffic classifier EXP4
[P-classifier-EXP4] if-match mpls-exp 4
[P-classifier-EXP4] quit
```

定义流行为，为不同的流设置不同的带宽和时延保证。

```
[P] traffic behavior AF11
[P-behavior-AF11] queue af bandwidth pct 10
[P-behavior-AF11] traffic behavior AF21
[P-behavior-AF21] queue af bandwidth pct 20
[P-behavior-AF21] traffic behavior AF31
[P-behavior-AF31] queue af bandwidth pct 30
[P-behavior-AF31] traffic behavior EF
[P-behavior-EF] queue ef bandwidth pct 40
[P-behavior-EF] quit
```

定义 QoS 策略，使符合流分类策略的 4 条数据流满足：EXP1 流保证 10%带宽；EXP2 流保证 20%带宽；EXP3 流保证 30%带宽；EXP4 流保证 40%带宽并保证时延。

```
[P] qos policy QUEUE
[P-qospolicy-QUEUE] classifier EXP1 behavior AF11
[P-qospolicy-QUEUE] classifier EXP2 behavior AF21
```

```
[P-qospolicy-QUEUE] classifier EXP3 behavior AF31
[P-qospolicy-QUEUE] classifier EXP4 behavior EF
[P-qospolicy-QUEUE] quit
```

将 QoS 策略应用在 P 的 Ethernet2/0/0 接口的出方向上。

```
[P] interface ethernet 2/0/0
[P-Ethernet2/0/0] qos apply policy QUEUE outbond
```

配置完成后，VPN1 中的流量在发生拥塞时，DSCP 域为 af11、af21、af31、ef 的流量接收比例为 1:2:3:4，其中，ef 流比其他 3 条流的延时都小。

目 录

附录 A 缩略语表.....	A-1

附录 A 缩略语表

本命令索引包括手册中所出现的全部命令，按字母序排列，左边为命令行，右边为该命令所在的功能模块和页码。

A B C D E F G H I J K L M N O P Q R S T U V

ACK	Acknowledgement, Acknowledgment	通信协议中的肯定应答
ADSL	Asymmetric Digital Subscriber Line	非/不对称数字用户线（环）路
AFI	Address-Family Identifier	地址族标识
AS	Access Server;	接入服务器。
ASCII	American Standard Code for Information Interchange	美国信息交换标准码
ASE	Application Service Element	应用业务单元/应用业务要素
ASIC	Application Specific Integrated Circuit	专用集成电路
ASN	Autonomous System Number	自治系统号
BSP	Board Support Package	板级支持软件包
CoS	Class of Service	服务等级
CPU	Center Processing Unit	中央处理单元
C-RP	Candidate RP	候选汇聚点（路由器）
CSMA	Carrier Sense Multiple Access	载波检测多址
DF	Don't fragment	勿分片
DNIS	Dialed Number Identification Service	拨入号码识别服务
DoD	Direct Outward Dialing	直接拨出
DOS	Denial of Service	拒绝服务
DS	Differentiated Services	有差别服务
DSLAM	Digital Subscriber Line Access Multiplexer	数字用户线接入复接器
DU	DUration	工期
DVMRP	Distance Vector Multicast Routing Protocol	距离矢量组播路由协议
DVPN	Dynamic VPN	动态 VPN
EBGP	External BGP	外部 BGP
FIB	Forward Information Base	转发信息库
FQ	Fair Queue	公平队列

FR-LSR	Frame Relay LSR	帧中继自举路由器
HoVPN	Hierarchy of VPN	分层式 VPN
IBGP	Internal BGP	内部 BGP
ILS	Internet Locator Service	Internet 定位服务
L2VPN	Layer Two VPN	二层 VPN
L3VPN	Layer Three VPN	三层 VPN
LD	Label Distribution	标记分发
LFI	Link Fragmentation and Interleaving	链路分片和交叉
LIB	Indicator Light Immobility Board	指示灯固定板
LLQ	Low Latency Queueing	低延迟队列
LR	Location Registration	位置注册
MED	Multi-Exit Discriminators	多出口区分
NAPT	Network Address and Port Translation	网络地址端口转换、网络地址端口翻译、端口映射
NLRI	Network Layer Reachable Information	网络层可达信息
PAM	Port to Application Mapping	端口到应用的映射
PDU	Packet Data Unit	分组数据单元
PE	Provider Edge	运营商边缘
PFS	Perfect Forward Secrecy	完善的前向安全性
PHY	Physical Sublayer & Physical Layer	物理子层,物理层
RED	Random Early Detection	随机早期检测
RM	Remote Manager	远程管理台
RPT	Rendezvous Point Tree	共享树/汇集树
RPU	Path Process Unit	路由协议处理模块
RSVP-TE	RSVP-Traffic Engineering	RSVP-流量工程
RTPQ	Real-time Transport Protocol Queue	实时传输协议队列, RTP 队列
RTSP	Real Time Streaming Protocol	实时流协议
SBM	Successful Backward setup information Message	后向建立成功信息消息
SNPA	Subnetwork Points of Attachment	子网接入点
SP	Service Provider	业务提供商
SPE	Synchronous Payload Envelope	同步净负荷包络
ST	Segment Type	分段类型
TP	Traffic Policing	流量策略

UCT	Universal Coordinated Time	世界协调时间、通用协调时间
VOS	Virtual Operating System	虚拟操作系统