SmartHammer 系列产品

软件配置手册

港湾网络

SmartHammer 系列产品软件配置手册

资料编号	P-1801XXXX-20040801-130
产品版本	V01R03B0122
资料状态	发行

手册使用说明

读者对象

本手册的读者对象为配置和管理 SmartHammer 系列产品的工程技术人员。本手册需要读者熟悉防火墙、交换、路由以及认证技术的基础知识。

内容介绍

本手册详细介绍了 SmartHammer 系列产品的配置方法，是工程技术人员了解该设备的软件特性，并顺利完成设备配置的指导文档。

具体包括以下内容：

第一部分：系统配置

章序号	题目	内容描述
第1章	系统管理	介绍了HSOS操作系统、实现系统配置的途径、系统文件管理以及常用系统管理命令
第2章	系统的引导	介绍了系统引导的基本概念，以及详细的系统引导过程及其配置方法。
第3章	配置SNMP	介绍了简单网络管理服务SNMP的基本概念以及配置方法。
第4章	系统监控与诊断	介绍了常用的系统信息查看方法以及系统诊断命令的使用。
第5章	配置系统日志	介绍了系统的日志的基本概念，以及详细的配置方法。
第6章	配置以太网接口	介绍了SmartHammer设备上的以太网接口类型以及详细的配置方法。并介绍了常见的故障分析。
第7章	配置GRE接口	介绍了GRE接口的基本概念及其配置方法。
第8章	配置VLAN接口	介绍了VLAN接口的基本特性及其配置方法。
第9章	配置LoopBack接口	介绍了LoopBack接口的基本特性及其配置方法。
第10章	配置透明桥	介绍了透明桥的基本概念及详细的转发原理及其配置方法。
第11章	配置ARP和代理ARP	介绍了地址解析协议ARP和代理ARP的的协议原理及其配置方法。
第12章	配置DHCP服务	介绍了动态主机配置协议DHCP的协议原理及其配置方法。
第13章	配置DHCP Relay服务	介绍了DHCP Relay的协议原理及其配置

		方法。
第14章	配置VRRP	介绍了虚拟冗余路由器协议VRRP的协议原理及其配置方法。
第15章	配置QoS	介绍了服务质量QoS的基本原理及其配置方法。

第二部分：AAA 配置

章序号	题目	内容描述
第16章	配置AAA授权功能	介绍了AAA授权功能在SmartHammer设备上的实现及其配置方法。
第17章	配置AAA认证和计费功能	介绍了AAA认证在SmartHammer 设备上的实现及其配置方法。

第三部分：防火墙配置

章序号	题目	内容描述
第18章	配置ACL	介绍了访问控制列表ACL的基本概念及其在SmartHammer设备上的配置方法
第19章	配置自适应安全过滤	介绍了自适应安全过滤的基本概念及其配置方法。
第20章	配置基于状态的资源控制	介绍了基于状态的资源控制的基本概念及其在SmartHammer设备上的配置方法。
第21章	配置NAT	介绍了NAT协议的原理及其在SmartHammer设备上的实现，以及配置方法等。
第22章	配置链路层过滤	介绍了链路层过滤的概念及其配置方法。

第四部分：VPN 配置

章序号	题目	内容描述
第23章	配置IPSec VPN	介绍了IPSec VPN的协议原理及其详细的配置方法，并配有丰富的配置案例。
第24章	配置L2TP VPDN	介绍了L2TP VPDN协议的原理及其详细的配置方法。

第五部分：接入认证配置

章序号	题目	内容描述
第25章	配置PPP Profile	介绍了PPP Profile的基本原理及其应用，并详细说明了其配置方法。
第26章	配置PPPoE认证	介绍了PPPoE认证协议的基本原理及其在配置方法。
第27章	配置WEB/Portal认证	介绍了WEB/Portal认证的基本原理及其应

		用情况，并详细介绍了配置方法。
第28章	配置IEEE802.1X接入认证	介绍了IEEE802.1X接入认证的基本原理及其应用情况，并详细介绍了配置方法。

第六部分：交换转发服务配置

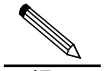
章序号	题目	内容描述
第29章	配置NetFlow	介绍了交换转发服务的协议原理及其配置方法。

第七部分：路由协议配置

章序号	题目	内容描述
第30章	配置静态路由	介绍了静态路由的基本概念及其配置方法。
第31章	配置策略路由	介绍了SmartHammer设备上支持的策略路由类型及其配置方法。

手册约定

手册中有关图标的约定如下：

图标	说明
 注意	这个图标表示提醒用户注意事项。
 提示	这个图标主要给出一些与正文相关的信息，同时给用户一些指引，协助用户更好的理解正文的内容。

获取技术支援

港湾网络有限公司建立了以总部技术支援中心、区域技术支援中心和本地技术支援中心为主体的完善的三级服务体系，并提供全天候 24 小时×365 天的电话热线服务。客户在产品使用及网络运行过程中遇到问题时请随时与港湾网络有限公司各地方的服务支持热线联系。请客户到www.harbournetworks.com获取各地服务支持热线电话。此外，客户还可通过港湾网络有限公司网站及时了解最新产品动态，以及下载需要的技术文档。

目录

第四部分 VPN 配置

第六部分 交换转发服务配置

第七部分 路由协议配置

第一部分

系统配置

1 系统管理

系统管理是对系统进行管理维护的一种重要手段，通过系统管理可以了解 SmartHammer 的基本用法，比如怎样进入 SmartHammer，如何上传下载配置文件，如何升级系统，以及如何获得帮助等。

1.1 HSOS概述

HSOS 是港湾网络有限公司为 SmartHammer 系列网络安全产品设计的操作系统，HSOS 提供丰富的软件特性，下面对其使用方法进行简单介绍。

1.1.1 命令行特性

这一节主要讲述当您进入命令行进行配置时所要进行的步骤。请仔细阅读本节以及后边几节中关于使用命令行接口的详细信息。

使用命令行接口（CLI），请按照以下步骤：

第 1 步：当进入命令行接口出现命令提示符后，请确认您有相应的权限。大多数配置命令都需要用户您有管理员权限。

第 2 步：键入命令名称。


注意

HSOS 命令行中的所有命令和关键字都是小写。

如果命令不含需要用户输入的参数，那么请直接跳到第 3 步。如果命令含需要用户输入的参数，那么继续以下步骤：

1）如果命令需要一个参数值，请输入一个参数值。在输入参数值时，可能要输入关键字。

2）命令的参数值部分一般指定了您应该输入什么样的参数，是某范围内的数值，或者字符串或者 IP 地址。关键字是指命令中要操作的对象。

3）如果命令需要多个参数值，请按命令的提示依次输入关键字和每个参数值。直到提示信息中出现让您按回车键信息为止。

第 3 步：输入完整的命令后，请按回车键。

例如：“exit” 是一个不含参数和关键字的命令。命令名称为 exit；“ip address A.B.C.D/M” 是一个含有参数和关键字的命令。其中命令名称为 ip，关键字为 address，参数值为 A.B.C.D/M。

1.1.2 语法帮助

命令行接口内置有语法帮助。如果您对某个命令的语法不是很确定，请输入该命令中您所知道的部分，然后输入“?”或“空格加 ？”。命令行会提示您已经输入的部分命令后剩余部分的可能的命令清单。

1.1.3 使用语法帮助补齐命令

HSOS 提供用户输入“Tab”键后，对命令进行补齐的功能。当您输入了一部分命令后，再输入“Tab”键，如果匹配的命令有多个，则列出可能的命令清单，如果匹配的命令只有一个，那么命令行会自动把用户输入的那部分命令补齐，并把光标移至最后。

1.1.4 命令中的符号

您可能会在命令语法中看到各种符号，这些符号只是说明您该如何输入该命令，但是不是命令本身的一个部分。下表对这些符号进行了概要说明。

表1-1 命令行中的符号

符号	描述
大写字母	大写字母表示该命令的该部分必须输入一个字符串参数。例如命令： subscriber-template pppoe NAME 中您必须在NAME那个位置输入一个合法的PPPoE模板

符号	描述
	的名字作为您所创建的PPPoE模板的名字。
A.B.C.D和A.B.C.D/M	A.B.C.D表示IP地址，M表示掩码。例如命令： address local A.B.C.D ip address A.B.C.D/M
圆括号 ( )和竖直线 |	圆括号一般和竖直线配合使用。圆括号括起来的部分表示这部分命令有几个用竖直线分隔开的可选项，您必须选择输入其中一项。 例如命令： authentication (chap|pap|both) (local|radius) 中，圆括号内包含由竖直线分隔的两个可选项，您必须输入或者chap 或者pap或者both其中的一个。
中括号 [ ]	中括号表示里面的参数可输入或可不输入。 例如命令： dns A.B.C.D [A.B.C.D] 中第二个参数如果输入表示有第二个DNS服务器，如果不输入表示只有一个DNS服务器
尖括号和数值范围	尖括号和数值范围表示输入的参数的取值范围在那两个数值之间的某个数。 例如命令：keep-alive <1-10000> 中SmartHammer设备向用户发送的keep-alive报文间隔可以取1到10000中的任一个数值。
B:E	B:E表示端口范围，B表示起始端口，E表示终止端口，B和E的范围都是0-65535
T.C	T.C表示ICMP协议type及code，T表示type，C表示code
H.H.H	H.H.H表示MAC地址，H为4位16进制的数，如0001.0203.0e0f，表示MAC地址00:01:02:03:0e:0f

1.1.5 快捷键命令

命令行中的快捷键

符号	描述
BackSpace键或Ctrl+h	向左删除一个字符
向上箭头键或Ctrl+p	调用上一个历史命令
向左箭头键或Ctrl+b	将光标向左移动一格
向右箭头键或Ctrl+f	将光标向右移动一格
向下箭头键或Ctrl+n	如果前边使用过向上箭头调用上一个历史命令的，再单击向下箭头键可以显示下一个历史命令。
Ctrl+a	将光标移动到行首
Ctrl+e	将光标移动到行尾
Ctrl+d	将光标所在位置的字符删除
Ctrl+k	将光标以后的字符全部删除
Ctrl+t	将光标所在的字符和光标左边的那个字符互相调换，并将光标向右移动一格

Ctrl+u	将光标左边的字符全部删除
Ctrl+w	将光标左边的单词删除
Ctrl+c	输入的字符不执行
Ctrl+z	使当前退到查看模式下


注意

在有些终端上按 ctrl+s 后，终端显示异常，可以按 ctrl+q 退出。

1.1.6 命令简写

命令简写是指您可以只输入命令单词或关键字的前边部分字母，只要那部分字母不会造成歧义，就可以直接回车执行该命令。但需要用户输入的参数如 PPPoE 模板的名字等，要完整输入。例如：

```
ip address 192.168.1.1/16
```

可以简写成：`ip add 192.168.1.1/16`


注意

当使用命令简写时，您必须输入足够多的字母，以确保在众多命令中不会造成歧义

1.1.7 命令模式

SmartHammer 设备支持丰富的命令模式，下表列出了所有的命令模式。

表1-2 SmartHammer 设备支持的所有命令模式

命令模式	提示符	进入方法
普通模式	SmartHammer>	系统引导起来后，输入密码
特权模式	SmartHammer#	在普通模式下输入密码
全局配置模式	SmartHammer(config)#	在特权模式下输入 configure terminal
TTY配置模式	SmartHammer (config-line)#	在全局配置模式下输入line tty
以太网接口配置模式	SmartHammer (config-if)#	在全局配置模式下输入interface IFNAME，例如：interface ge0
VLAN配置模式	SmartHammer (config-if)#	在配置模式下输入 interface IFNAME.VID
LoopBack接口配	SmartHammer	在全局配置模式下输入

命令模式	提示符	进入方法
置模式	(config-if)#	interface lo <0-1023>
BVI接口配置模式	SmartHammer (config-if)#	在全局配置模式下输入interface Name 其中Name必须以bvi开头，后面添加从0到255的数字。如bvi0
GRE接口配置模式	SmartHammer (config-if)#	在全局配置模式下输入interface gre <0-1023>
PPP模板配置模式	SmartHammer (config-ppp)#	在全局配置模式下输入ppp-profile NAME
DHCP配置模式	SmartHammer (config-dhcp)#	在全局配置模式下输入dhcp
SNMP配置模式	SmartHammer (config-snmp)#	在全局配置模式下输入snmp-server
QoS模板配置模式	SmartHammer (config-traffic-map)#	在全局配置模式下输入traffic-map MAPNAME
AAA认证模板配置模式	SmartHammer(config-aaa)#	在全局配置模式下输入 aaa Name
PPPoE认证模板配置模式	SmartHammer(config-sub)#	在全局配置模式下输入 subscriber-template pppoe NAME
8021x认证模板配置模式	SmartHammer(config-sub)#	在全局配置模式下输入 subscriber-template dot1x NAME
WEB认证模板配置模式	SmartHammer(config-sub)#	在全局配置模式下输入 subscriber-template webauth NAME
PORTAL配置模式	SmartHammer (config-portal-server)#	在全局配置模式下输入portal-server
VRRP模板配置模式	SmartHammer(config-vrrp)#	在全局配置模式下输入 vrrp-router <1-255>
L2TP模板配置模式	SmartHammer(config-l2tp)#	在全局配置模式下输入 subscriber-template L2TP NAME
IPSEC MAP配置模式	SmartHammer (config-crypto-map)#	在全局配置模式下输入 crypto map NAME <0-65535> isakmp
IPSEC 变换集配置模式	SmartHammer(cfg-crypto-trans)#	在全局配置模式下输入 crypto ipsec transform-set transform-set-name transform1 <transform2> <[transform3>
ISAKMP配置模式	SmartHammer (config-isakmp)#	在全局配置模式下输入crypto isakmp policy <1-1000>
策略路由配置模式	SmartHammer (config-policy-map)#	在全局配置模式下输入policy-map MAPNAME

1.1.8 常用命令介绍

表1-3 普通模式下的常用命令介绍

命令	描述
enable	进入特权模式，可以对SmartHammer设备进行配置和写操作
exit	退出当前模式，返回到上一级模式
ping WORD	网络连通性基本检测工具，WORD为对方主机地址
list	显示当前模式下可用的命令
show running-config	显示当前的配置信息（可以是没有保存的）
show startup-config	显示已经保存的启动配置信息
show table	显示静态路由表的表号
show version	显示版本信息

1.2 实现系统配置的途径

您可以通过以下途径对 SmartHammer 设备进行管理：

- 使用终端（或者仿终端软件）连接到 SmartHammer 设备的串口（Console）从而访问 SmartHammer 设备的命令行接口（CLI）
- 使用 Telnet 管理 SmartHammer 设备
- 使用 SSH 管理 SmartHammer 设备
- 图形化配置管理界面

1.2.1 通过配置口实现系统配置

- 波特率：9600
- 数据位：8
- 奇偶校验：无
- 停止位：1
- 流量控制：无

正确设置完 Console 的参数并将设备加电，可以看到 SmartHammer 设备的提示登录信息。

1.2.2 通过Telnet实现系统配置

任何一个有 Telnet 功能的工作站都能通过 TCP/IP 网络连接到 SmartHammer 设备。可以通过以下步骤 Telnet 登录到 SmartHammer 设备：

通过 Console 口用管理员用户的帐号登录到 SmartHammer 设备。进入接口配置模式。

然后给 SmartHammer 设备某个接口配置 IP 地址。给接口配置 IP 地址可以使用以下命令：

ip address A.B.C.D/M

此后可以从该接口上以该接口的 IP 地址 Telnet 登录到 SmartHammer 设备命令行接口。

默认情况下 Telnet 功能是打开的，如果你已经关闭了该功能，必须使用 service telnet 命令打开。

1.2.3 通过SSH方式实现系统配置

网络被攻击，很多情况是由于服务器提供了 Telnet 服务引起的。Telnet 服务有一个致命的弱点——它以明文的方式传输用户名及口令，所以，很容易被别有用心的人窃取口令。目前，一种有效代替 Telnet 服务的有用工具就是 SSH 服务。SSH 客户端与服务器端通讯时，用户名及口令均进行了加密，有效防止了对口令的窃听。SmartHammer 设备支持以 SSH 的方式对设备的管理。

任何一个有 SSH 功能的工作站都能通过 TCP/IP 网络连接到 SmartHammer 设备。可以通过以下步骤登录到 SmartHammer 设备：

通过 Console 口用管理员用户的帐号登录到 SmartHammer 设备。进入接口配置模式。

然后给 SmartHammer 设备某个接口配置 IP 地址。给接口配置 IP 地址可以使用以下命令：

```
ip address A.B.C.D/M
```

此后可以从该接口上以该接口的 IP 地址通过 SSH 命令登录到 SmartHammer 设备命令行接口。

默认情况下 SSH 功能是打开的，如果你已经关闭了该功能，必须使用 service ssh 命令打开。

1.3 系统文件管理

系统文件的管理是指对于配置文件、系统应用程序文件以及其他的一些文件比如计费信息、日志信息等的维护和管理。对于系统文件的管理，在没有特别指明的时候，都是在特权模式下操作。

1.3.1 copy命令使用

表1-4 copy 命令列表_TFTP

源	目的	说明	备注
tftp://A.B.C.D/config	disk0:config1	从TFTP服务器上下载配置文件config，放到CF卡上，并更名为config1	这里服务器的IP地址以A.B.C.D为例，实际情况中请根据需要修改，以下相同
tftp://A.B.C.D/config	flash0:config1	从TFTP服务器上下载配置文件config，放到Flash卡上，并更名为config1	
tftp://A.B.C.D/config	startup-config	从TFTP服务器上下载配置文件config，作为下次启动时的配置文件	可以用show system boot查看系统的启动配置文件设置
tftp://A.B.C.D/hsos	disk0:hsos1	从TFTP服务器上下载应用程序文件HSOS，放到CF卡上，并更名为hsos1	
tftp://A.B.C.D/hsos	flash0:hsos1	从TFTP服务器上下载应用程序文件HSOS，放到Flash卡上，并更名为hsos1	

表1-5 copy 命令列表_FTP

源	目的	说明	备注
ftp://USER:PASSWORD@A.B.C.D/config	disk0:config1	从FTP服务器上下载配置文件config，放到CF卡上，并更名为config1	USER是FTP服务器上的合法用户，其密码为PASSWORD，下同
ftp://USER:PASSWORD@A.B.C.D/config	flash0:config1	从FTP服务器上下载配置文件config，放到Flash卡上，并更名为config1	
ftp://USER:PASSWORD@A.B.C.D/config	startup-config	从FTP服务器上下载配置文件config，作为下次启动时的配置文件	可以用show system boot查看系统的启动配置文件设置
ftp://USER:PASSWORD@A.B.C.D/config	disk0:hsos1	从FTP服务器上下载应用程序文件hsos，放到CF卡上，并更名为hsos1	
ftp://USER:PASSWORD@A.B.C.D/hsos	flash0:hsos1	从FTP服务器上下载应用程序文件hsos，放到Flash卡上，并更名为hsos1	

表1-6 copy 命令列表_zmodem

源	目的	说明	备注
zmodem:config	disk0:config1	从串口相连的超级终端所在机器上下载配置文件，放到CF卡上，并更名为config1	
zmodem:config	flash0:config1	从串口相连的超级终端所在机器上下载配置文件，放到Flash卡上，并更名为config1	
zmodem:config	startup-config	从串口相连的超级终端所在机器上下载配置文件，作为下次启动时的配置文件	可以用show system boot查看系统的启动配置文件设置
zmodem:hsos	disk0:hsos1	从串口相连的超级终端所在机器上下载应用程序文件，放到CF卡上，并更名为hsos1	
zmodem:hsos	flash0:hsos1	从串口相连的超级终端所在机器上下载应用程序文件，放到Flash卡上，并更名为hsos1	

表1-7 copy 命令列表_ Flash0

源	目的	说明	备注
flash0:config1	TFTP://A.B.C.D/config	从Flash卡上上传配置文件config1，放到tftp服务器上，并更名为config。	
flash0:config1	ftp:USER:PASSWORD@//A.B.C.D/config	从Flash卡上上传配置文件config1，放到FTP服务器上，并更名为config	USER是FTP服务器上的合法用户，其密码为PASSWORD
flash0:config1	disk0:config	从Flash卡上拷贝配置文件config1，放到CF卡上，并更名为config	
flash0:config1	startup-config	从Flash卡上拷贝配置文件config1，放到NVRAM中	这里没有目的地，目的地实际为NVRAM。
flash0:hsos1	tftp://A.B.C.D/hsos	从Flash卡上上传应用程序文件hsos1，放到FTP服务器上，并更名为hsos	
flash0:hsos1	ftp:USER:PASSWORD@//A.B.C.D/hsos	从Flash卡上上传应用程序文件hsos1，放到FTP服务器上，并更名为hsos。	USER是FTP服务器上的合法用户，其密码为PASSWORD。
flash0:hsos1	disk0:hsos	从Flash卡上拷贝配置文件hsos1，放到CF卡上，并更名为hsos。	
flash0:hsos1	flash0:hsos	从Flash卡上拷贝配置文件hsos1，放到Flash卡上，并更名为hsos。	

表1-8 copy 命令列表_ FILE

startup-config running-config logmemory local_accounting 上面的四个文件之一。	tftp://A.B.C.D/file	拷贝相关信息，放到TFTP服务器上，并更名为FILE	
	ftp:USER:PASSWORD@//A.B.C.D/config	拷贝相关信息，放到FTP服务器上，并更名为FILE	USER是FTP服务器上的合法用户，其密码为PASSWORD
running-config	startup-config	保存当前的配置信息	作用与write memory、write FILE相同

注：
startup-config表示系统启动时的配置文件、running-config表示当前的配置信息、logmemory表示记录到系统内存中的日志信息、local_accounting表示计费信息、


注意

copy tftp://A.B.C.D/config1 tftp://A.B.C.D/config2 之类的命令，从语法上是正确的，但实际执行是无意义的，或者无效的，甚至是有害的，操作员应该为自己的操作负责。

1.3.2 保存配置文件


注意

每一次修改了 SmartHammer 设备的配置后，必须将配置保存到 SmartHammer 设备中，重新启动后，配置才能保持不变。

配置文件保存的步骤如下所述：

方法 1：

步骤**1**	write memory	将配置文件保存到系统中

方法 2：

步骤**1**	write file	将配置文件保存到系统中

方法 3：

步骤**1**	copy running-config startup-config	将配置文件保存到系统中


注意

1）以上三个命令作用相同，都实现保存配置文件的功能。

2）startup-config 表示系统启动时的配置项，而 running-config 表示系统启动后当前的配置项，操作员更改后的配置项反映在 running-config 中，系统刚启动时，running-config 就是 startup-config。

1.3.3 配置文件的上传与下载

用户还可以把一份好的配置文件保存到文本文件中，在需要的时候（例如不小心把 SmartHammer 设备配置搞乱了，不知道怎样把配置恢复到以前的状态时）再把配置文件下载到 SmartHammer 设备中，目前配置文件的上传和下载有三种方式：通

过 TFTP、通过 FTP 以及通过 zModem，下面一一介绍。

通过 TFTP 协议下载配置文件的步骤：

步骤1	copy tftp://A.B.C.D/config disk0:config1	将TFTP服务器/tftpboot目录下的文件config拷贝到CF卡上，取名为config1
步骤2	set boot config disk0:config1	指定系统启动时使用的配置文件
步骤3	reboot	重新启动系统

通过 FTP 协议下载配置文件的步骤：

步骤1	copy ftp://USER:PASSWORD@A.B.C.D/config flash0:config1	将FTP服务器上的文件config拷贝到Flash卡上，取名为config1，USER是FTP服务器上的合法用户，其密码为PASSWORD。
步骤2	set boot config flash0:config1	指定系统启动时使用的配置文件
步骤3	reboot	重新启动系统

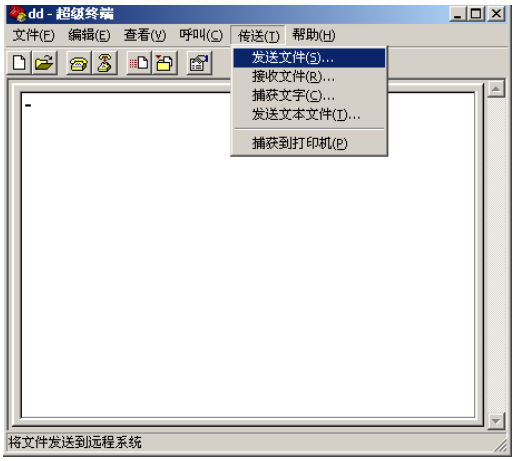
通过 zModem 协议下载配置文件的步骤：

步骤1	copy zmodem:config startup-config	从串口上下载配置文件config，作为下次启动时的配置文件。
步骤2	设置超级终端	设置超级终端，从超级终端发送文件。
步骤3	reboot	重新启动系统

超级终端的操作方法：

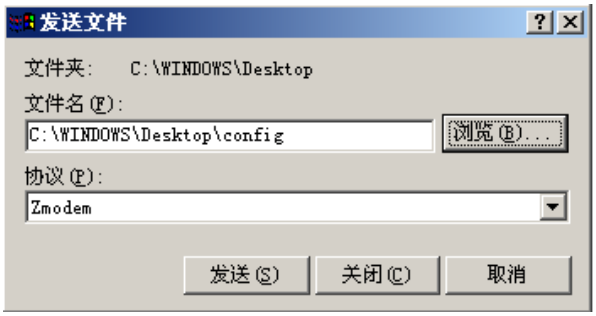
在超级终端中，选择传送菜单的“发送文件”：

图1-1 启动超级终端并点击“发送文件”操作界面



选择存放配置文件所在的目录，使用的发送协议是 zModem。

图1-2 选择存放配置文件所在的目录



点击“发送”，系统开始下载指定文件信息。

这样就会将配置文件下载到系统中，配置文件存放的位置根据操作员的输入而定，可以是 CF 卡，可以是 Flash 卡，也可以是 NVRAM。

通过 TFTP 协议上传配置文件的步骤如下所述：

通过 TFTP 协议上传配置文件的步骤：

步骤**1**	copy startup-config tftp://A.B.C.D/config	将系统的配置文件拷贝到TFTP服务器/tftpboot目录下，取名为config

通过 FTP 协议上传配置文件的步骤如下所述：

通过 FTP 协议上传配置文件的步骤：

步骤**1**	copy startup-config ftp://USER:PASSWORD@A.B.C.D/config	将将系统的配置文件拷贝到FTP服务器，取名为config，USER是FTP服务器上的合法用户，其密码为PASSWORD。

1.3.4 系统升级

随着港湾公司对系统的不断完善，升级系统是一件常见的事情，目前系统升级有三种方式：通过 TFTP、通过 FTP 以及通过 zModem，下面一一介绍。

通过 TFTP 协议升级系统的步骤如下所述：

通过 TFTP 协议升级系统的步骤：

步骤**1**	copy tftp://A.B.C.D/hsos	将TFTP服务器/tftpboot目录下的文件

	disk0:hsos1	hsos拷贝到CF卡上，取名为hsos1。注意hsos必须是有效的系统应用程序文件
步骤2	set boot system disk0:hsos1	指定系统启动时使用的系统应用程序文件
步骤3	reboot	重新启动系统

通过 FTP 协议升级系统的步骤如下所述：

通过 FTP 协议升级系统的步骤：

步骤1	copy ftp://USER:PASSWORD@A.B.C.D/hsos flash0:hsos1	将FTP服务器上的文件hsos拷贝到Flash卡上，取名为hsos1，USER是FTP服务器上的合法用户，其密码为PASSWORD。注意hsos必须是有效的系统应用程序文件
步骤2	set boot system flash0:hsos1	指定系统启动时使用的系统应用程序文件
步骤3	reboot	重新启动系统

通过 zModem 协议升级系统的步骤如下所述：

通过 zModem 协议升级系统的步骤：

步骤1	copy zmodem:hsos flash0:hsos1	从串口上下载系统应用程序文件hsos，放到Flash卡上，并取名为hsos1。注意超级终端传送的文件必须是有效的系统应用程序文件
步骤2	设置超级终端	设置超级终端，从超级终端发送文件
步骤3	set boot system nvram	指定系统启动时使用的配置文件
步骤4	reboot	重新启动系统

超级终端的操作方法参见1.3.3

配置文件的上传与下载一节：


注意

1. 要使系统应用程序文件生效，必须重启系统。
2. 由于系统程序文件一般较大，zModem 协议采用的速率和终端使用的速率相同，如果您采用终端默认速率（9600）下载系统程序文件，可能需要较长的时间，如果您不能忍受这样长的时间，您可以采用更改终端速率的办法加快下载系统程序文件。
3. 根据 zModem 协议的规定，如果要取消接收，需要连续五次按 CTRL+X。

4. 目前，我们只能通过 zModem 协议下载文件，不能通过 zModem 协议上传文件。也就是说，不能通过 zModem 协议将文件保存到与防火墙串口相连的机器上。

更改终端速率方法：

您必须更改 SmartHammer 设备的速率和通过串口连接 SmartHammer 设备的客户机的速率，保证两个的速率是相同的。

1．更改 SmartHammer 设备的速率为 115200

在特权模式下输入命令：

```
SmartHammer# terminal speed NUM
```

其中 NUM 为您要更改的速率，可以为 9600，19200，115200 等。

2．更改客户机的速率

客户端如果使用超级终端，您可以通过以下方法更改速率，首先您断开超级终端，点击文件-〉属性

图1-3 更改客户机的速率操作界面 1

将会弹出以下窗口：

图1-4 更改客户机的速率操作界面 2

点击“配置”，出现以下窗口：

图1-5 更改客户机的速率操作界面 3

将每秒位数由 9600 转为 112500。

图1-6 更改客户机的速率操作界面 4

这时您再重新连接 SmartHammer 设备，在特权模式下输入命令：

```
SmartHammer# copy zmodem:hsos disk0
```

就可以用较快的速度下载 HSOS，下载完毕后，您通过输入 **reboot** 命令重新启动 SmartHammer 设备，然后您再把您的客户机的超级终端的速率通过以上“更改客户机的速率”方法重新改回 9600（必须这样做，因为系统重启后又恢复到默认的速率 9600），这样您就升级了 HSOS，并且可以通过串口正常连接 SmartHammer 设备。

1.3.5 其他系统文件的管理

其他系统文件的维护一般都是通过 copy 命令来实现的，他们的用法与配置文件或者系统程序文件的管理是一样的，使用 copy 命令，可以实现从网络(TFTP、FTP、zModem)到 SmartHammer 设备，从 SmartHammer 设备到网络(TFTP、FTP)的拷贝，以及从 SmartHammer 设备到 SmartHammer 设备的拷贝，这些 copy 命令具有很强的相似性，不过是将源和目的更改而已。关于 copy 命令的详细用法，请参考1.3.1 copy 命令使用一节。

上传系统应用程序文件的步骤如下所述：

上传系统应用程序文件的步骤：

步骤**1**	copy disk0:hsos1 tftp://A.B.C.D/hsos	将CF卡上的应用程序文件hsos1拷贝到TFTP服务器/tftpboot目录下取名为hsos。注意hsos1必须是有效的系统应用程序文件

系统应用程序文件也可以保存到 FTP 服务器上。同时，系统应用程序文件也可能放在 Flash 卡上。相应的语法请参考0

配置文件的上传与下载以及1.3.1　copy 命令使用一节。

保存内存日志记录信息的步骤如下所述：

保存内存日志记录信息的步骤：

步骤**1**	copy logmemory tftp://A.B.C.D/log	将系统内存中保存的日志记录拷贝到TFTP服务器/tftpboot目录下取名为log

内存日志记录信息也可以保存到 FTP 服务器上。相应的语法请参考“0

配置文件的上传与下载”的内容。

保存计费信息的步骤如下所述：

保存计费信息的步骤：

步骤**1**	copy local_accounting tftp://A.B.C.D/acct	将计费信息拷贝到TFTP服务器/tftpboot目录下取名为acct

计费信息也可以保存到 FTP 服务器上。相应的语法请参考“配置文件的上传和下载”一节。

最后计费信息也可以保存到 FTP 服务器上。相应的语法请参考0

配置文件的上传与下载一节。

保存当前配置信息的步骤：

步骤**1**	copy running-config tftp://A.B.C.D/config	将当前配置信息拷贝到TFTP服务器/tftpboot目录下取名为config

当前配置信息也可以保存到 FTP 服务器上。相应的语法请参考“配置文件的上传和下载”一节。


注意

startup-config 表示系统启动时的配置项，而 running-config 表示系统启动后当前的配置项，操作员更改后的配置项反映在 running-config 中，系统刚启动时，running-config 就是 startup-config。

升级 WEB 认证时的强制认证页面的步骤：

步骤**1**	copy tftp://A.B.C.D/pp.jpg portal_pop	从TFTP服务器上下载图形文件pp.jpg，作为web认证时的强制认证页面

您也可以从 FTP 服务器上下载相关图形文件。相应的语法请参考“配置文件的上传和下载”一节。

1.4 常用系统管理命令

1.4.1 关闭Telnet服务

关闭 Telnet 服务的步骤：

步骤**1**	no service telnet	关闭Telnet服务，执行该命令后将禁止其他机器Telnet到SmartHammer设备

默认情况下，Telnet 开关是打开的，即允许其他机器的 Telnet 操作。，可以用 show system service 查看系统提供的服务。

1.4.2 关闭SSH服务

关闭 SSH 服务的步骤：

步骤**1**	no service ssh	关闭SSH服务，执行该命令后将禁止其他机器SSH到SmartHammer设备

默认情况下，SSH 开关是打开的，即允许其他机器的 SSH 操作。，可以用 show system service 查看系统提供的服务。

1.4.3 查看谁在系统上

who 命令显示当前有哪些操作员登录进系统，查看谁在线上：

查看谁在系统上的操作步骤：

步骤**1**	查看当前有哪些操作员登录进系统

```
SmartHammer# who
     User            From          Graphic
     admin           console
*    guest1          A.B.C.D
     guest2          A.B.C.D         yes
```

表1-9 显示信息说明

标识	说明
*	表示当前管理员用户
User	登录用户名，空表示使用no login方式登录
From	登录地点，console表示从控制口登录，IP地指表示从网络登录的IP
Graphic	是否是从图形化界面登录，yes表示从图形化界面登录，空表示不是

以上结果表示目前有三个操作员在线上，他们都是通过 login 方式进入系统的），其中一个由 console 口接入，一个（就是自己）是从 A.B.C.D 使用 telnet 或 SSH 连接到系统，另外一个用户使用图形化界面登录。

1.4.4 清除其他登录用户

如果有多个操作员登录进系统，而有些操作员出现了异常，某个操作员可以将其他操作员踢出系统，这需要利用命令 clear tty。

清除其他登录用户的操作步骤：

步骤**1**	clear tty [user NAME] [host A.B.C.D]	踢出其他满足条件的用户，使用Console、telnet、SSH登录的管理员用户，但让自己保存在系统中。


注意

本指令只能清除满足条件的使用 Console、telnet、SSH 登录的管理员，对于使用港湾安全管理平台登录的管理员用户，该指令无法清除。

1.4.5 设置系统启动参数

利用 set boot 命令设置系统启动参数，该命令可以设置系统启动时的引导 hsos、配置文件以及其他引导参数。

设置启动时的引导系统：

步骤**1**	set boot system PLACE：FILE	设置系统从PLACE以FILE启动系统

例如：

```
SmartHammer# set boot system disk0:hsos
```

设置系统的启动 hsos，系统重启后，将以第一块 CF 卡上的 hsos 启动。

系统的启动参数实际上设置到 CFE 里面，这里对应 CFE 的环境变量为：HSOS_CONFIGHSOS_IMAGE。

设置系统启动配置文件的步骤：

步骤**1**	set boot config PLACE：FILE	设置系统从PLACE以FILE作为配置文件启动系统，如果是nvram，则不指定PLACE和FILE

例如：

```
SmartHammer# set boot config disk0:config
```

又如：

SmartHammer# set boot config nvram

设置系统的启动配置文件，系统重启后，将以第一块 CF 卡上的 config 作为配置文件。

1)系统的启动参数实际上设置到 CFE 里面，这里对应 CFE 的环境变量为：HSOS_CONFIG

2)boot config 的当前值就是 startup-config 的值，比如，show startup-config 就是查看 boot config 指定地点的内容，如果 boot config 的值是 nvram，则查看 nvram 的内容

设置系统启动的其他选项的步骤：

步骤**1**	set boot options OPTIONS	设置系统启动时的其他启动选项

例如：

```
SmartHammer# set boot options nowatchdog noconfig
```

设置系统的启动选项，系统重启后，将以无看门狗，无配置的方式运行。


注意

1)系统的启动参数实际上设置到 CFE 里面，这里对应 CFE 的环境变量为：HSOS_OPTIONS

2)如果设置了 noconfig，则系统始终以无配置的方式启动，而不管是否设置了启动配置文件。

例如，如果同时设置了：

```
SmartHammer# set boot config disk0:config
SmartHammer# set boot options nowatchdog noconfig
```

则系统以无配置方式启动，即 noconfig 的级别更高。

系统的启动参数实际上设置到 CFE 里面，因此这里设置完毕并重启后，您可以在 CFE 里看到对应的设置已经改变。在这里设置系统的启动参数与在 CFE 里设置其作用是一样的。


提示

关于 CFE 的设置，请参见第 2 章 系统的引导

1.4.6 重新分发配置

利用 configure memory 可以重新分发配置文件。配置文件是当前 boot config 的值，用 show system boot 查看，HSOS_CONFIG 的值就是当前的配置文件。configure memory 主要用在管理员忘记了密码的情况。这时管理员以无配置启动，进入系统后执行 configure memory，然后更改密码即可。

重新分发配置的步骤：

步骤**1**	configure memory	重新分发配置

例如：

```
SmartHammer# configure memory
```

重新分发配置文件里的配置，配置文件是用 show system boot 查看出来的 HSOS_OPTIONS 项的值。

2 系统的引导

Common Firmware Envionment 通用固件环境以下简称 CFE，是一个包含初始化过程和系统引导的软件模块。在系统初始化的时候使用。

2.1 CFE概述

CFE(Common Firmware Envionment)通用固件环境是一个包含初始化过程和系统引导的软件模块。该模块主要是进行一些底层驱动设备的初始化。所以当需要进行配置文件和系统应用程序文件的加载时才建议进入 CFE 模块，否则在系统启动时，无需进入。

该模块属于高级功能，一般用户请谨慎使用该模块。

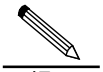
2.2 配置CFE

2.2.1 缺省配置

表2-1 SmartHammer 设备 CFE 的缺省设置信息

内容	缺省设置	备注
CFE下默认使用的串口（BOOT_CONSOLE）	Uart0	不能更改设置
ge0的MAC地址（ETH0_HWADDR）	00:08:0c:00:00:00	可更改设置，出厂时需更新
ge1的MAC地址（ETH1_HWADDR）	00:08:0c:00:00:01	可更改设置，出厂时需更新
ge2的MAC地址（ETH2_HWADDR）	00:08:0c:00:00:02	可更改设置，出厂时需更新
Eth3的MAC地址	00:08:0c:00:00:03	可更改设置，出厂时需更新

内容	缺省设置	备注
（ETH3_HWADDR）（当设备为SmartHamer M504时）		
CFE下加载代码使用的网络接口（NET_DEVICE）	Eth2（当设备为SmartHammer G503时） eth3（当设备为SmartHammer M504时）	可更改设置
CFE下加载代码使用的网络接口的IP地址（NET_IPADDR）	192.168.98.3	可更改设置
CFE下加载代码使用的网络接口的子网掩码（NET_NETMASK）	255.255.0.0	可更改设置
CFE下加载代码使用的网络接口的网关（NET_GATEWAY）	0.0.0.0	可更改设置
CFE下加载代码使用的网络接口的域名服务器（NET_NAMESERVER）	0.0.0.0	可更改设置
加载HSOS的引导参数（HSOS_OPTIONS）	无	可更改设置
加载HSOS的映像文件的配置（HSOS_CONFIG）	nvram	可更改设置
加载HSOS的映像文件名（HSOS_IMAGE）	disk0：hsos	可更改设置


提示

1) ETH 和 NET_等网络相关的变量使用 ifconfig 命令更新（使用 setenv 命令无效）。

2）HSOS_ 的变量使用 setenv 命令。

3 ）由于 SmartHammer G503 有 3 个网络接口，而 SmartHammer M504 有 4 个网络接口，所以在 SmartHammer M504 下多一个缺省配置为 eth3 的 MAC 地址（ETH3_HWADDR）。

2.2.2 配置SYSINFO文件的加载

SYSINFO 文件的加载由生产部门使用（其他人员禁用），通过加载 SYSINFO 文件可以设置本产品的生产序列号，硬件版本，出厂 MAC 地址等唯一标识信息。加载

可以根据加载文件所处的不同位置，而选择使用不同的渠道进行加载。使用网络 TFTP 加载、FLASH 加载或 CF 卡加载，加载后即可生效。

配置系统应用程序文件通过 CF 卡加载的步骤：

步骤**1**	load –raw host:filename|dev:filename	加载一个sysinfo文件


注意

选项-raw 加载 sysinfo 文件

2.2.3 配置直接引导

直接引导指通过设置环境变量，指定所加载的系统应用程序文件存储的地方，而使系统直接上电启动后，自动根据环境变量 HSOS_IMAGE 指定的位置，进行系统应用程序文件的加载，而不需要人为的干预。

配置直接引导的步骤：

步骤**1**	boot	执行加载的系统应用程序文件


注意

HSOS_IMAGE 环境变量一定要是有效值。

2.2.4 配置系统应用程序文件的加载

系统应用程序文件的加载可以根据加载文件所处的不同位置，而选择使用不同的渠道进行加载。使用网络 TFTP 加载、FLASH 加载或 CF 卡加载，但是加载后不执行，需要用 go 命令执行加载的软件，只有系统应用程序文件加载成功后，我们所提供的软件功能才能够正确地执行。

配置系统应用程序文件通过 CF 卡加载的步骤：

步骤**1**	load -z host:filename|dev:filename	加载一个文件
步骤**2**	go	执行加载的映象文件


注意

选项-z 加载压缩文件

2.2.5 配置网络参数

在 CFE 环境中可以进行一些网络配置，使其可以从网络引导。

配置网络参数的步骤：

步骤**1**	ifconfig device [options]	配置指定的网络接口，ifconfig命令激活网络接口，设置 IP地址和其它参量，device是网络接口的名字

配置时有如下选项：

-addr=a.b.c.d 指定接口的 IP 地址

-mask=a.b.c.d 指定接口的子网掩码

-gw=a.b.c.d 指定接口的网关

-dns=a.b.c.d 指定接口的 DNS 服务器

-domain=string 替 DNS 的请求指定一个域名(举例，“Harbournetworks.com”)

-hwaddr=xxx 指定接口的 MAC 地址


注意

在 SmartHammer M504 中，在 CFE 环境下，只有 eth2 和 eth3 可以使用全部功能。而 eth0 和 eth1 只能使用 ifconfig －hwaddr 命令配置其中的 MAC 地址。

2.2.6 配置实时时钟

在 CFE 环境下，可以进行实时时钟的设置和显示。

配置实时时钟的步骤：

步骤**1**	set time hh:mm:ss：MM:DD:YYYY	设置当前的年、月、日、时、分、秒

请使用各种时间段的有效值。年的范围为 2000-2030

2.2.7 配置AUX口

在 CFE 环境下，可以进行把 AUX 口作为 Console 口的设置以及在 HSOS 系统中作为调试用口。

配置 AUX 口为 Console 口的步骤：

步骤**1**	set console device-name	设置AUX口为Console口

该配置主要用途为辅助测试 AUX 口是否可用。完毕后使用 set console uart0 命令，把它改回系统默认使用的 uart0 口作为 console 口，因为 HSOS 我们的软件在 linux 下缺省固定使用 uart0 作为 console 口。如果用户 set console uart1 后，没有改回来就直接引导 HSOS 的话，超级终端联接的串口将不会有任何输出。这是由于 HSOS 缺省使用 uart0 作为 console 口。此时用户可以把串口线连接到 uart0 上，系统的信息将会输出到超级终端，系统可以正常使用。

2.2.8 配置环境变量

在 CFE 环境下，可以设置、显示和取消各种环境变量。环境变量主要用来在加载配置文件和系统应用程序文件的时候起作用，我们可以使用环境变量 HSOS_OPTIONS 来忽略配置文件（noconfig）、关闭看门狗；使用 HSOS_CONFIG 来选择是从哪个地方加载配置文件（支持的所有类型见下文）；使用 HSOS_IMAGE 来选择是从哪个地方加载 HSOS 文件（支持的所有类型见下文）。具体的使用情况请参考配置案例。

配置环境变量的步骤如下：

步骤**1**	setenv varname value	设置一个环境变量

使用 unsetenv varname value 可以取消一个环境变量设置。


注意

只有使用 HSOS_开头的环境变量才可以设置，其它的和网络有关的环境变量是通过 ifconfig 命令设置的，请注意区分。而且目前需要设置的环境变量只有 HSOS_CONFIG、HSOS_OPTIONS、HSOS_IMAGE。另 Setenv 的参数 value 必须使用 “” 括起来。

2.2.9 配置自检

在 CFE 环境下，可以对各种设备进行自检。

配置自检的步骤：

步骤**1**	test nvram	检测NVRAM设备是否完好
步骤**2**	test flash	检测FLASH设备是否完好
步骤**3**	test cpld	检测CPLD设备是否完好
步骤**4**	test sdram	检测SDRAM设备是否完好
步骤**5**	test pci	检测PCI从设备是否完好
步骤**6**	test disk disk0	检测CF卡设备是否完好
步骤**7**	test fatfs device-name	测试设备是否有文件系统，且查看里面的内容

建议第 1、2、3 项只在出厂进行装备测试时使用。如果此命令在非出厂时使用，切忌自检过程中掉电，否则会破坏设备内保存的有效数据。第 7 项的 device-name 可以为 disk0 或者 flash0。

2.3 配置信息显示命令

表2-2 CFE 配置信息显示命令列表

命令	解释
printenv	显示设置的环境变量
show time	显示当前的时钟
show device	显示一个在BIOS里边配置设备驱动列表
show device	显示CFE下命令行的帮助信息
ping	显示当前网络是否联通

2.4 配置案例

2.4.1 忽略配置文件

案例描述：

使 CFE 在引导系统软件时忽略配置文件。

配置步骤：

步骤**1**	设置HSOS_OPTIONS环境变量
	SmartHammer>setenv HSOS_OPTIONS “noconfig”

2.4.2 关闭看门狗

案例描述：

使 CFE 在系统应用程序文件执行时 watchdog 不起作用。

配置步骤：

步骤1	设置HSOS_OPTIONS环境变量
	SmartHammer>setenv HSOS_OPTIONS “nowatchdog”

2.4.3 设置多个配置选项

案例描述：

使用空格设置多个启动选项，本案例选项为无配置文件且关闭看门狗。

配置步骤：

步骤1	设置HSOS_OPTIONS环境变量
	SmartHammer>setenv HSOS_OPTIONS “noconfig nowatchdog”

2.4.4 设置使用CF卡加载配置文件

案例描述：

使用存储在 CF 卡里的配置文件进行加载


注意

由于 CF 卡上的文件系统是 FAT16，所以其上面的文件名必须符合 FAT16 的约定，即文件名不超过 8 个英文字符，点后面的扩展名不超过 3 个英文字符。

配置步骤：

步骤1	设置HSOS_CONFIG环境变量，使用CF卡加载。
	SmartHammer>setenv HSOS_CONFIG “disk0:config”

2.4.5 设置使用FLASH加载配置文件

案例描述：

使用存储在 FLASH 里的配置文件进行加载。

配置步骤：

步骤**1**	设置HSOS_CONFIG环境变量，使用FLASH加载。
	SmartHammer>setenv HSOS_CONFIG “flash0:config”


注意

由于 FLASH 上的文件系统是 FAT16，所以其上面的文件名必须符合 FAT16 的约定，即文件名不超过 8 个英文字符，点后面的扩展名不超过 3 个英文字符。

2.4.6 设置使用NVRAM加载配置文件

案例描述：

使用存储在 NVRAM 里的配置文件进行加载。

配置步骤：

步骤**1**	设置HSOS_CONFIG环境变量，使用NVRAM加载。
	SmartHammer>setenv HSOS_CONFIG “nvram”

2.4.7 设置使用CF卡加载系统应用程序文件

案例描述：

使用存储在 CF 卡里的系统应用程序文件进行加载，然后直接执行。


注意

由于 CF 卡上的文件系统是 FAT16，所以其上面的文件名必须符合 FAT16 的约定，即文件名不超过 8 个英文字符，点后面的扩展名不超过 3 个英文字符。

配置步骤：

步骤**1**	设置HSOS_IMAGE环境变量，使用CF卡加载系统应用程序文件。

	SmartHammer>setenv HSOS_IMAGE “disk0:HSOS.IMG”
步骤**2**	使步骤1加载的系统应用程序文件执行
	SmartHammer>boot

2.4.8 设置使用CF卡加载系统应用程序文件

案例描述：

使用存储在 CF 卡里的系统应用程序文件进行加载，然后重新启动系统以使刚加载的系统应用程序文件得以执行。

注意	由于 CF 卡上的文件系统是 FAT16，所以其上面的文件名必须符合 FAT16 的约定，即文件名不超过 8 个英文字符，点后面的扩展名不超过 3 个英文字符。

配置步骤：

步骤**1**	设置HSOS_IMAGE环境变量，使用CF卡加载系统应用程序文件。
	SmartHammer>setenv HSOS_IMAGE “disk0:HSOS”
步骤**2**	重新启动防火墙，然后3秒提示中不敲任意键，系统将会根据HSOS_IMAGE设置的内容去自动执行步骤1加载的系统应用程序文件。
	SmartHammer>reset

2.4.9 设置使用FLASH加载系统应用程序文件

案例描述：

使用存储在 FLASH 里的系统应用程序文件进行加载，然后直接执行。

注意	由于 FLASH 上的文件系统是 FAT16，所以其上面的文件名必须符合 FAT16 的约定，即文件名不超过 8 个英文字符，点后面的扩展名不超过 3 个英文字符。

配置步骤：

步骤**1**	设置HSOS_IMAGE环境变量，使用FLASH加载系统应用程序文件。

	SmartHammer>setenv HSOS_IMAGE “flash0:HSOS.IMG”
步骤2	使步骤1加载的系统应用程序文件执行。
	SmartHammer>boot

2.4.10 设置使用FLASH加载系统应用程序文件

使用存储在 FLASH 里的 HSOS 文件进行加载，然后重新启动系统以使刚加载的系统应用程序文件得以执行。


注意

由于 FLASH 上的文件系统是 FAT16，所以其上面的文件名必须符合 FAT16 的约定，即文件名不超过 8 个英文字符，点后面的扩展名不超过 3 个英文字符。

配置步骤：

步骤1	设置HSOS_IMAGE环境变量，使用FLASH加载系统应用程序文件。
	SmartHammer>setenv HSOS_IMAGE “flash0:HSOS.IMG”
步骤2	重新启动防火墙，然后3秒提示中不敲任意键，系统将会根据HSOS_IMAGE设置的内容去自动执行步骤1加载的系统应用程序文件。
	SmartHammer>reset

2.4.11 设置使用网络通过TFTP加载系统应用程序文件

案例描述：

设置 HSOS_IMAGE 环境变量，从网络通过 TFTP 协议加载，然后直接执行。

配置步骤：

步骤1	设置HSOS_IMAGE环境变量，从网络通过TFTP协议加载系统应用程序文件。
	SmartHammer>setenv HSOS_IMAGE “192.168.0.1:HSOS.IMG”
步骤2	使步骤1加载的系统应用程序文件执行
	SmartHammer>boot

2.4.12 设置使用网络加载系统应用程序文件

案例描述：

设置 HSOS_IMAGE 环境变量，从网络通过 TFTP 协议加载，然后重新启动系统以使刚加载的系统应用程序文件得以执行。

配置步骤：

步骤**1**	设置HSOS_IMAGE环境变量，从网络通过TFTP协议加载系统应用程序文件。
	SmartHammer>setenv HSOS_IMAGE “192.168.0.1:HSOS.IMG”
步骤**2**	重新启动防火墙，然后3秒提示中不敲任意键，系统将会根据HSOS_IMAGE设置的内容去自动执行步骤1加载的系统应用程序文件。
	SmartHammer>reset

2.4.13 设置使用多种方式加载系统应用程序文件

案例描述：

设置 HSOS_IMAGE 环境变量，使用多种方式加载系统应用程序文件，然后直接执行加载软件。例如：先从 CF 卡加载，如果不行再从 FLASH 加载，注意两种加载方式中间使用空格分割。


注意

由于 CF 卡和 FLASH 上的文件系统是 FAT16，所以其上面的文件名必须符合 FAT16 的约定，即文件名不超过 8 个英文字符，点后面的扩展名不超过 3 个英文字符。

配置步骤：

步骤**1**	设置HSOS_IMAGE环境变量，先从CF卡加载系统应用程序文件，如果不行再从FLASH加载，注意两种加载方式中间使用空格分割。
	SmartHammer>setenv HSOS_IMAGE “disk0:HSOS.IMG flash0:HSOS.IMG”
步骤**2**	使步骤1加载的系统应用程序文件执行
	SmartHammer>boot

2.4.14 设置使用多种方式加载系统应用程序文件

案例描述：

设置 HSOS_IMAGE 环境变量，使用多种方式加载，然后重新启动系统以使刚加载的系统应用程序文件得以执行，例如：先从 CF 卡加载，如果不行再从 FLASH 加载，注意两种加载方式中间使用空格分割。


注意

由于 CF 卡和 FLASH 上的文件系统是 FAT16，所以其上面的文件名必须符合 FAT16 的约定，即文件名不超过 8 个英文字符，点后面的扩展名不超过 3 个英文字符。

配置步骤：

步骤**1**	设置HSOS_IMAGE环境变量，先从CF卡加载系统应用程序文件，如果不行再从FLASH加载，注意两种加载方式中间使用空格分割。
	SmartHammer>setenv HSOS_IMAGE “disk0:HSOS.IMG flash0:HSOS.IMG”
步骤**2**	重新启动防火墙，然后3秒提示中不敲任意键，系统将会根据HSOS_IMAGE设置的内容去自动执行步骤1加载的系统应用程序文件。
	SmartHammer>reset

2.4.15 配置网络接口

案例描述：

配置网络的 MAC 地址和 IP 地址。


注意

顺序应该是先配置 MAC 地址然后配置 IP 地址

配置步骤：

步骤**1**	设置ge0的MAC地址
	SmartHammer>ifconfig ge0 –hwaddr=00:08:0c:00:00:00
步骤**2**	设置ge0的IP地址
	SmartHammer>ifconfig ge0 –addr=192.168.0.1

2.5 故障分析

2.5.1 加载HSOS.IMG文件出错

故障现象	无法加载HSOS文件
分析与解决	分析：HSOS文件的加载都是通过HSOS_IMAGE环境变量的设置内容进行的，如果HSOS_IMAGE文件设置的不对，将不会正确加载文件 解决方法：HSOS_IMAGE设置正确的内容，保证其所指定的设备内有系统的压缩文件。

2.5.2 使用LOAD命令引导HSOS.IMG文件出错

故障现象	使用Load加载完HSOS文件后，使用go命令无法启动HSOS文件
分析与解决	分析：由于LOAD命令，缺省加载的为非压缩文件，而为HSOS.IMG压缩文件，所以go命令无法正确执行 解决方法：使用LOAD命令时加上 –z 选项，表示加载的是压缩文件

2.5.3 重新启动后ge0网口无法引导HSOS.IMG文件

故障现象	使用ifconfig分别先后配置完ge0、ge1、ge2，然后重新启动，本来和ge0相连的网口通过TFTP无法引导HSOS文件
分析与解决	分析：由于在防火墙的CFE配置中存储在NET_DEVICE中的只能有一个网络接口，该变量的值为上一次启动时最后设置的网络接口，在我们的故障现象中即为ge2，而我们和TFTP Server连接的是ge0，又由于TFTP引导是本机的网络接口是从NET_DEVICE中得到的，所以无法引导。 解决方法：重新通过ifconfig命令设置一下ge0的接口，改变NET_DEVICE中的值为ge0

3 配置 SNMP

本章涉及 SmartHammer 设备 SNMP 的配置，内容主要包括：

- SNMP 概述
- 配置 community 访问权限
- 配置 SNMP trap 参数

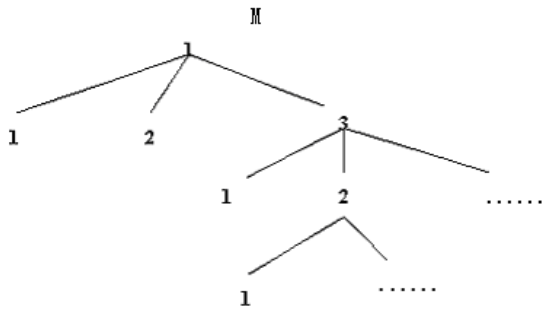
3.1 SNMP概述

SNMP(Simple Network Management Protocol 简单网络管理协议)是目前在数据通讯网中使用得最广泛的网络管理协议，也是被广泛接受并被实际使用的工业标准。它的设计目标是使管理信息能在网络任意两点间传送，使网络管理员可以在网络中的任何节点检索信息，修改配置，查找故障，诊断故障，规划流量及生成报告。它采用轮询机制，提供最基本的功能集。SNMP 是一个应用层协议，在传输层采用 UDP 协议，目前很多公司的网络产品都支持此协议。

SNMP 的体系设计也遵循客户端/服务器模式，分为 NMS(Network Managmetn Station，网管站)和 Agent(代理)两部分。NMS 作为客户端，被管设备上的 Agent 作为服务器。NMS 可以向 Agent 发出请求报文，Agent 收到请求报文后，根据报文内容对被管设备的管理对象进行所要求的操作，并根据操作结果生成响应报文，返回给管理站。同时在被管设备上产生了管理站所关心的事件时 Agent 也可以主动发送 Trap 报文来通知 NMS。

为了唯一标识被管设备中的管理对象，SNMP 采用树形层次结构来组织被管设备中的管理对象，每一个管理对象都是树的一个节点，并可用从树根开始的全路径来唯一加以识别。例如：管理对象 M，可以用从根开始的路径{1，3，2，1}来加以识别。

图3-1 MIB 树结构示意图



{1，3，2，1}就是 M 的对象标识符，而所有管理对象的集合就是 MIB(管理信息库)，它表述了被管设备中所有可管理的对象。

3.2 配置SNMP

3.2.1 缺省设置

表3-1 SNMP 团体访问权限的缺省设置

内容	缺省设置	备注
只读（ro）访问权限community	public	可更改设置
读写（rw）访问权限community	private	可更改设置
trap访问权限(trap-community)	public	可更改设置

3.2.2 配置community访问权限

SNMP v1 采用 community（共同体）的认证方案，每个 SNMP 报文中都有一个称为 community 的字符串，作为 NMS 和 Agent 通讯的口令。如果收到的 SNMP 报文的 community 同设备认可的 community 不符，该报文将会被丢弃。同时不同的 community 还具有不同的访问权限。只读的共同体只能对设备信息进行查询，而可读写的共同体除此之外还能对设备进行配置。

当使用 SNMP 网管系统(如港湾公司的 HammerView 等)需要管理 SmartHammer 设备时，您需要先配置 community 访问权限。

配置 community 访问权限的步骤：

步骤1	snmp-server	进入SNMP配置模式
步骤2	community public [ro]	设置community只读（ro）访问权限为public
步骤3	community private rw	设置community读写（rw）访问权限为private

3.2.3 配置SNMP trap参数

当 SmartHammer 设备上产生了管理站所关心的事件时（如接口的链路断开），SmartHammer 设备也可以主动发送 trap 报文来通知 SNMP 网管系统（如港湾公司的 HammerView 等）。

配置 SNMP trap 参数的步骤：

步骤1	snmp-server	进入SNMP配置模式
步骤2	trap-host A.B.C.D	设置trap目的主机IP地址
步骤3	write memory	保存配置

3.3 配置信息显示命令

表3-2 SNMP 配置信息显示命令

命令	解释
show running-config	显示配置信息

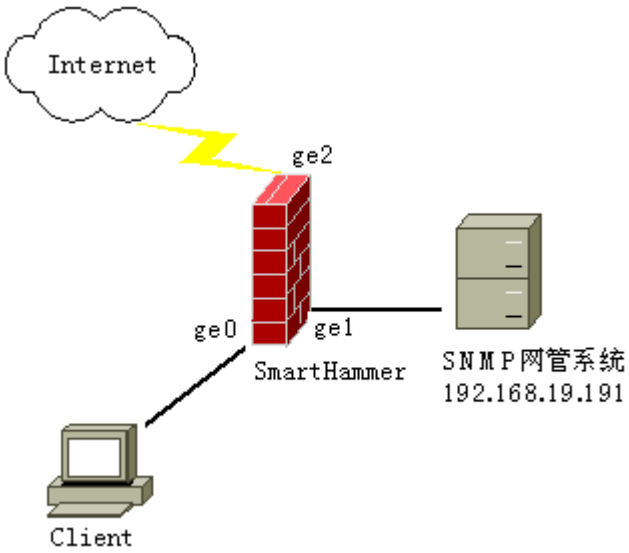
3.4 配置案例

3.4.1 配置SNMP

案例描述：

为 SmartHammer 设备配置 Community 只读访问权限为 public，Community 读写访问权限为 private，接收 trap 的服务器地址 192.168.19.191。SNMP 网管系统同时作为接收 trap 的服务器，IP 地址为 192.168.19.191，用户可以通过网管系统来读取配置和接收 trap 信息。

图3-2 SNMP 配置案例组网图



配置步骤：

步骤**1**	配置SNMP community访问权限
	SmartHammer# configure terminal SmartHammer(config)# snmp-server SmartHammer(config-snmp)# community public SmartHammer(config-snmp)# community private rw SmartHammer(config-snmp)# end
步骤**2**	配置SNMP trap参数
	SmartHammer# configure terminal SmartHammer(config)# snmp-server SmartHammer(config-snmp)# trap-host 192.168.19.191 SmartHammer(config-snmp)# end
步骤**3**	保存配置
	SmartHammer# write memory

3.5 常见故障

3.5.1 管理站无法收到SNMP trap报文

故障现象	管理站无法收到SNMP trap报文
分析与解决	发送SNMP trap目的IP地址是否配置正确 community访问权限是否正确 链路是否正常

4 系统监控与诊断

系统监控与诊断是对系统进行管理维护的一种重要手段，通过系统监控与诊断可以了解 SmartHammer 设备目前运行的基本情况，比如，当前的 CPU 运行状况、内存状况、系统运行时间等等信息。值得注意的是，系统的监控与诊断主要是通过查看系统的一些底层信息来获得的，而不是针对软件配置错误而言的。

4.1 查看系统信息

SmartHammer 设备提供了一组用于查看系统信息的 show 命令，以方便操作员对系统的运行情况进行监控与诊断。这些命令都是在特权模式下进行操作的。

4.1.1 查看系统启动参数

利用命令 show system boot 完成该操作，查看系统启动参数的步骤如下所述：

查看步骤：

步骤**1**	显示系统的启动参数
	show system boot SmartHammer# show system boot HSOS_SYSTEM disk0:hsos HSOS_CONFIG nvram HSOS_OPTIONS nowatchdog 表示系统启动时，是用第一块CF卡中的hsos启动的，配置文件为NVRAM里的配置信息，设置了启动选项为nowatchdog，即以无看门狗的方式启动。

4.1.2 查看CPU信息

利用命令 show system cpuinfo 查看 CPU 信息的

查看步骤：

步骤1	显示当前的CPU情况
	SmartHammer# show system cpuinfo system type : SiByte AC11NPU processor : 0 cpu model : SiByte SB1 V0.2 FPU V0.2 BogoMIPS : 465.30 wait instruction : no microsecond timers : yes tlb_entries : 64 extra interrupt vector : yes hardware watchpoint : no VCED exceptions : not available VCEI exceptions : not available processor : 1 cpu model : SiByte SB1 V0.2 FPU V0.2 BogoMIPS : 465.30 wait instruction : no microsecond timers : yes tlb_entries : 64 extra interrupt vector : yes hardware watchpoint : no VCED exceptions : not available VCEI exceptions : not available 可以看到，系统类型为SiByte AC11NPU，目前有两个CPU，它们的类型都为SiByte SB1 V0.2 FPU V0.2，还有一些跟CPU相关的其他信息。

4.1.3 查看系统CPU利用率

利用命令 show system cpu-usage 可以查看 CPU 利用率。

查看步骤：

步骤1	查看系统CPU利用率
	SmartHammer# show cpu-usage CPU usage statics: Recent 1 sec: average 0.00% Recent 5 sec: average 0.40% Recent 1 min: average 0.03% 表示CPU最近1秒钟、最近5秒钟以及最近1分钟的利用率为0%，0.40%和0.03%。

4.1.4 查看系统当前的日期和时间

查看步骤：

步骤**1**	查看系统当前的日期和时间
	SmartHammer#show system date 2005/01/17 16:52:11

4.1.5 查看内存使用情况

查看步骤：

步骤**1**	显示当前内存使用情况
	SmartHammer# show system meminfo total: used: free: shared: buffers: cached: Mem: 1053356032 139894784 913461248 0 401408 77529088 Swap: 0 0 0 MemTotal: 1028668 kB MemFree: 892052 kB MemShared: 0 kB Buffers: 392 kB Cached: 75712 kB SwapCached: 0 kB Active: 3260 kB Inactive: 119304 kB HighTotal: 131072 kB HighFree: 69500 kB LowTotal: 897596 kB LowFree: 822552 kB SwapTotal: 0 kB SwapFree: 0 kB 我们可以看到总的内存容量为1028668 kB，空闲的内存容量为892052 kB，没有共享内存，Buffers大小为392 kB，缓冲大小为75712 kB。

4.1.6 查看系统内存利用率

利用命令 show system memory-usage 可以查看系统内存利用率。

查看步骤：

步骤**1**	可以看到总的内存容量为388534272字节，空闲的内存容量为240570368字节，已经使用的内存为147963904字节，使用率为38.08%。

```
SmartHammer# show memory-usage
Memory usage statics:
Total memory:   388534272
Used memory:    147963904
Free memory:    240570368
Usage:          38.08%
```

4.1.7 查看系统提供的服务

查看步骤：

步骤**1** 显示系统提供的服务情况

```
SmartHammer# show system service
Service          On/Off
Telnet           on
SSH              on
```

目前，SmartHammer 设备提供了 Telnet 和 SSH 的服务记录。

4.1.8 查看系统连续运行的时间

查看步骤：

步骤**1** 查看系统连续运行的时间

```
SmartHammer# show system uptime
current time              : 15:45
system runtime            :  20 hours 16 minutes
```

表示当前时间是下午3:45，系统运行已经20小时16分钟了。

4.1.9 查看系统启动的Logo

查看步骤：

步骤**1** 显示系统启动logo

```
SmartHammer# show version
Harbour OS KIDA_1.3_98
Build 98 at Tue Jan 13 16:45:23 EST 2004.
Copyright (c) Harbour Networks Limited All rights reserved.
```

可以看到当前的系统版本是第3版，build号是98，编译时间是2004年1月13日下午4点。

4.2 系统诊断

4.2.1 ping命令的使用

SmartHammer 设备提供了 ping 命令用来检测网络的基本连接情况，ping 命令发送 Internet Control Message Protocol (ICMP) 请求报文到网络中的某个 IP 设备。普通用户和管理员用户都可以使用 ping 命令。

如果在设定时间内没有收到目的设备响应报文，则不输出任何信息，否则显示响应报文的字节数、报文序号、TTL 、响应时间。按 CTRL+C 可以结束 ping 状态。

检测步骤：

步骤**1** 测试SmartHammer设备到IP地址为192.168.0.1的设备的连通性。

```
SmartHammer(config)# ping 192.168.0.1
```

如果设备连通，则出现以下信息：

```
SmartHammer# ping 10.13.2.14
PING 10.13.2.14 (10.13.2.14): 56 data bytes
64 bytes from 10.13.2.14: icmp_seq=0 ttl=64 time=0.3 ms
64 bytes from 10.13.2.14: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 10.13.2.14: icmp_seq=2 ttl=64 time=0.0 ms
64 bytes from 10.13.2.14: icmp_seq=3 ttl=64 time=0.0 ms
```

如果没有连通则出现以下信息：

```
SmartHammer# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1): 56 data bytes
```

4.2.2 traceroute命令的使用

traceroute 是另一种检测网络连接情况的命令，只有管理员权限的用户才可以使用，它与 ping 命令不同的是它不但可以测试网络是否连通还可以获知数据包的传输路径中在哪一个地方出现问题。Traceroute 命令的输出信息包括到达目的地所有经过的网关的 IP 地址和到此网关所用时间，如果某网关超时则显示“*”。例如：

检测步骤：

步骤**1**	测试SmartHammer设备到IP地址为192.168.19.1的设备的连通性。
	SmartHammer# traceroute 192.168.19.1 traceroute to 192.168.19.1 (192.168.19.1), 30 hops max, 40 byte packets 1 192.168.19.1 (192.168.19.1) 0.666 ms 0.263 ms 0.241 ms

5 配置系统日志

系统日志是了解系统的运行情况和当前的网络情况的一种重要手段。同时完整的日志信息也是保证系统安全的重要措施。本部分内容详细介绍了系统日志的配置方法。

5.1 日志系统概述

SmartHammer 设备支持系统日志功能，Syslog 模块即系统日志模块，主要用来记录整个系统的运行情况。完整的日志模块能够帮助管理员及时了解和监控系统的工作情况，并实时记录系统的异常信息。日志信息来源于系统中所有的运行模块，日志系统完成信息的收集、管理、存储和显示。日志信息可以显示到终端，这种方式主要用于调试和查看系统状态。也可以存储到系统内存，还可以存储到日志服务器，这种方式用于长期跟踪系统的运行情况以及用户的命令行操作行为。以下给出 Syslog 模块在 SmartHammer 设备上的配置命令。

5.1.1 配置系统日志

SmartHammer 设备系统日志的配置格式如下：

log DAEMON LOCATION MASKPRI PRIORITY

表5-1 Syslog 配置语法

参数	有效值	解释
DAEMON	(all|aam|acl|arp|bridge|cli|crypto|dhcp|dot1x|gre|inspect|l2tp|nat|netflow|nsm|policy|portal ppp|pppoe|qos|vrrp|vlan|webauth|packet)	需要记录日志的模块名称，其中all表示所有模块，cli表示终端操作模块。

参数	有效值	解释
LOCATION	(console|memory|A.B.C.D)	记录日志的地方，可以记录到控制终端、内存或者其他日志服务器。
MASKPRI	(upto|only|except)	对于优先级的控制，upto表示系统将对等于或大于priority级别的日志类型做日志信息，only表示系统将对等于priority级别的日志类型做日志信息，except表示系统将对不等于priority级别的日志类型记录日志信息。
PRIORITY	(emergencies|alerts|critical|errors|warnings|notifications|informational)	日志级别划分如下： 0： 系统不可用； 1：实时操作； 2：严重； 3：错误； 4：告警； 5： 提示； 6： 一般信息，对应于emergencies到informational，数值越大，级别越低。

5.1.2 缺省配置

表5-2 Syslog 的缺省设置信息

内容	缺省设置	备注
记录日志的内存大小	1K	可更改设置

5.1.3 配置记录所有模块的日志信息

根据日志信息的配置语法：

log DAEMON LOCATION MASKPRI PRIORITY

当 DAEMON 为 all 时，表示记录所有模块的日志信息。

记录所有模块的日志信息的配置步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	log all memory upto informational	将所有模块大于等于优先级informational的日志信息记录到系统

		内存，informational的优先级最低，这其实表示了系统将记录最为广泛的日志信息
步骤3	end	退到enable模式下
步骤4	write terminal	显示配置

模块 all 代表了所有的模块，但是，执行 log all memory upto informational 后，仍然可以往系统里添加 log pppoe memory upto informational 的配置项，此时 PPPoE 的相关信息会记录两次；随后执行 no log all memory upto informational，只会将第一项删除，log pppoe memory upto informational 配置项仍然有效。

5.1.4 配置记录单个模块的日志信息

根据日志信息的配置语法：

log DAEMON LOCATION MASKPRI PRIORITY

当 DAEMON 为具体的某一模块时，表示记录该模块的日志信息。配置单个模块的日志信息的步骤如下所述（以 PPPoE 模块为例）：

记录单个模块的日志信息的配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	log pppoe memory upto informational	将PPPoE模块大于等于优先级informational的日志信息记录到系统内存，informational的优先级最低，这其实表示了系统将记录最为广泛的日志信息
步骤3	end	退到enable模式下
步骤4	write terminal	显示配置

表5-3 Syslog 目前支持的模块

模块名称	解释
all	Logging all daemons
aaam	Logging AAA mangement daemon
acl	Logging acl daemon
arp	Logging arp daemon
bridge	Logging bridge daemon
cli	Logging cmdline of operators
crypto	Logging crypto module
dhcp	Logging dhcp daemon
dot1x	Logging dot1x daemon
gre	Logging gre module
hproxy	Logging http proxy daemon
inspect	Logging inspect daemon
l2tp	Logging l2tp daemon
nat	Logging nat daemon
netflow	Logging netflow daemon
nsm	Logging nsm daemon
policy	Logging policy routing daemon
portal	Logging portal daemon
ppp	Logging ppp daemon
pppoe	Logging pppoe daemon
qos	Logging qos daemon
vrrp	Logging vrrp daemon
vlan	Logging vlan daemon
webauth	Logging web authentication daemon
packet	Logging packet daemon

5.1.5 配置日志的记录地方

根据日志信息的配置语法：

log DAEMON LOCATION MASKPRI PRIORITY

其中的 LOCATION，可以根据实际情况，配置为控制终端、系统内存或者其他日志服务器。

配置日志记录地方为控制终端的步骤如下所述（以 PPPoE 模块为例）：

配置日志记录地方为 console 的步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	log pppoe console upto informational	将PPPoE模块大于等于优先级informational的日志信息记录到控制终端，informational的优先级最低，这其实表示了系统将记录最为广泛的日志信息
步骤**3**	end	退到enable模式下

步骤4	write terminal	显示配置

Console 所表示的控制终端是用串口相连的终端，即配置日志记录地方为 Console 时，相应的日志信息只会通过串口输出到对应的终端上，如果您是通过 Telnet 或者 ssh 进入系统的，您不能在终端上看到日志输出信息，如果您要看到相应的信息，需要执行命令 terminal monitor。

配置日志记录地方为系统内存的步骤如下所述（以 PPPoE 模块为例）：

配置日志记录地方为系统内存的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	log pppoe memory upto informational	将PPPoE模块大于等于优先级informational的日志信息记录到系统内存，informational的优先级最低，这其实表示了系统将记录最为广泛的日志信息
步骤3	end	退到enable模式下
步骤4	write terminal	显示配置

配置日志记录地方为其他日志服务器的步骤如下所述：（以 PPPoE 模块为例，日志服务器的 IP 地址假设为 192.168.0.1）

配置日志记录地方为其他日志服务器的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	log pppoe 192.168.0.1 upto informational	将PPPoE模块大于等于优先级informational的日志信息记录到日志服务器192.168.0.1，informational的优先级最低，这其实表示了系统将记录最为广泛的日志信息
步骤3	end	退到enable模式下
步骤4	write terminal	显示配置

5.1.6 配置模块的优先级标志

根据日志信息的配置语法：

log DAEMON LOCATION MASKPRI PRIORITY

其中的 MASKPRI，可以根据实际情况，配置为大于等于、等于或者不等于对应的优先级。

配置模块优先级标志为大于等于的步骤如下所述（以 PPPoE 模块为例）：

配置模块优先级标志为大于等于的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	log pppoe memory upto informational	将PPPoE模块大于等于优先级informational的日志信息记录到系统内存，informational的优先级最低，这其实表示了系统将记录最为广泛的日志信息
步骤3	end	退到enable模式下
步骤4	write terminal	显示配置

配置模块优先级标志为等于的步骤如下所述（以 PPPoE 模块为例）：

配置模块优先级标志为等于的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	log pppoe memory only informational	将PPPoE模块等于优先级informational的日志信息记录到系统内存
步骤3	end	退到enable模式下
步骤4	write terminal	显示配置

配置模块优先级标志为不等于的步骤如下所述（以 pppoe 模块为例）：

配置模块优先级标志为不等于的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	log pppoe memory except informational	将PPPoE模块不等于优先级informational的日志信息记录到系统内存
步骤3	end	退到enable模式下
步骤4	write terminal	显示配置

upto 表示大于等于某个级别的日志信息。如 upto informational 表示大于等于 informational 级别的日志信息，由于 informational 的级别最低，这就相当于记录了所有级别的日志。

5.1.7 配置模块的优先级

根据日志信息的配置语法：

log DAEMON LOCATION MASKPRI PRIORITY

其中的 PRIORITY，可以根据实际情况，配置相应的 0-6 级优先级。配置模块优先级为大于等于 informational 的步骤如下所述（以 PPPoE 模块为例）：

配置模块优先级为大于等于 informational 的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	log pppoe memory upto informational	将PPPoE模块大于等于优先级informational的日志信息记录到系统内存
步骤3	end	退到enable模式下
步骤4	write terminal	显示配置

日志级别说明：

日志信息	日志级别	含义
emergencies	0	系统不可用
alerts	1	警告，需要采取行动
critical	2	严重
errors	3	错误
warnings	4	告警
notifications	5	提示
informational	6	一般信息

5.1.8 配置记录日志的内存大小

当往记录日志的地方为系统内存时，由于系统内存的有限性，不能无限使用，因此需要限制大小，默认情况下为 1K 字节。配置记录日志的内存大小的步骤如下所述：

配置记录日志的内存大小的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	log memsize 20	配置记录日志信息的系统内存的大小为20k
步骤3	end	退到enable模式下
步骤4	write terminal	显示配置

5.1.9 配置系统日志的速率限制

SmartHammer 设备系统日志的速率限制配置格式如下：

log DAEMON ratelimit <1-15>

DAEMON 表示具体的设施，比如 DOT1X，PPPoE 等设施，<1-15>表示每秒钟发

送多少条日志。为了让速率限制支持突发，只有在有持续大量的日志情况下，才会表现出多少秒钟记录一次日志，在少量或者突发情况下，ratelimit 不会限制速率。

配置日志速率限制的步骤如下所述（以 pppoe 模块为例）

配置日志速率限制的步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	log pppoe ratelimit 5	配置记录pppoe模块日志信息的速率限制位5秒一次
步骤**3**	end	退到enable模式下
步骤**4**	write terminal	显示配置

5.1.10 在Telnet或者ssh终端上查看日志

正如前面已经提到的，当记录日志信息的地方配置为 console 时，日志信息只输出到与系统相连的串口终端上，如果要在 Telnet 或者 ssh 终端上显示日志信息，必须执行命令 terminal monitor。

配置在 Telnet 或者 ssh 终端查看日志信息的步骤如下所述：

配置在 Telnet 或者 ssh 终端查看日志信息的步骤：

步骤**1**	terminal monitor	配置在Telnet或者ssh终端上显示日志信息

terminal monitor 只是将显示到串口终端的信息同时显示到 Telnet 或者 ssh 终端，如果没有配置日志信息记录的地方为 console 或者删除了对应的配置项，则 terminal monitor 配置后仍然不会有对应的日志信息显示。

该命令只在 Telnet 或者 ssh 终端上有效，在串口终端上执行该命令，没有实际意义。

5.1.11 保存系统内存中的日志信息

我们可以将保存在系统内存中的日志信息通过 copy 命令拷贝到其他机器上，配置保存系统内存中的日志信息到 TFTP 服务器上的步骤如下所述：

保存系统内存中的日志信息到 TFTP 服务器上的步骤：

步骤**1**	copy logmemory tftp://192.168.0.1/log	将系统内存中保存的日志记录拷贝到TFTP服务器/tftpboot目录下取名为log

内存日志记录信息也可以保存到 FTP 服务器上，还可以通过 zModem 协议保存到与系统相连的超级终端所在的机器上。相应的语法请参考“配置文件的上传和下载”一节。


提示

关于 copy 命令的详细用法，请参考“配置文件的上传和下载”一节。

5.2 配置信息显示命令

5.2.1 显示配置的日志信息

与查看其他配置信息的方式一样，执行命令 write terminal 或者 show running-config 显示配置的日志信息，显示当前配置的步骤如下所述：

显示当前配置的步骤：

步骤1	write terminal	显示当前的配置信息，包括日志信息

使用 show running-config 可以达到相同的效果，显示当前配置的日志信息。

5.2.2 显示内存中记录的信息

执行 show logmemory 命令查看系统内存中记录的日志信息，显示内存中记录的日志信息的步骤如下所述：

显示内存中记录的日志信息的步骤：

步骤1	显示当前系统内存中记录的日志信息
	Router# show logmemory May 30 01:52:48 Router vtysh[346]: command line(192.168.3.251): end May 30 01:52:49 Router vtysh[346]: command line(192.168.3.251): wr m May 30 01:52:52 Router vtysh[346]: command line(192.168.3.251): show debug May 30 01:52:55 Router vtysh[346]: command line(192.168.3.251): show logmemory

5.3 配置案例

5.3.1 将系统中所有模块的日志信息记录到日志服务器上

案例描述

将系统中所有模块的日志信息记录到日志服务器 192.168.19.1 上

配置步骤

步骤1	将系统中所有模块的日志信息记录到日志服务器192.168.19.1上
	SmartHammer(config)# log all console except alerts
步骤2	退出配置模式下，回到特权模式
	SmartHammer(config)# exit
步骤3	保存配置信息
	SmartHammer# write memory

5.3.2 将系统中PPPoE模块除了alert级别的日志信息记录到Console口上

案例描述

将系统中 PPPoE 模块除了 alert 级别的日志信息记录到 Console 口上。

配置步骤

步骤1	将系统中PPPoE模块除了alert级别的日志信息记录到console口上
	SmartHammer(config)# log all 192.168.0.1 upto informational
步骤2	退出配置模式下，回到特权模式
	SmartHammer(config)# exit
步骤3	保存配置信息
	SmartHammer# write memory

5.3.3 综合配置案例

案例描述

将系统中 PPPoE 模块的日志信息记录到 console 口上，并在某 Telnet 或者 ssh 终端上查看该信息；同时将 dot1x 模块的日志信息记录到系统内存中，系统内存限制大小为 20K，记录完毕后将日志信息拷贝到 FTP 服务器 192.168.0.1 上，取名为

log.txt：

配置步骤

步骤**1**	将PPPoE模块的日志信息记录到控制终端上
	SmartHammer(config)# log pppoe console upto informational
步骤**2**	退出配置模式下，回到特权模式
	SmartHammer(config)# exit
步骤**3**	保存配置信息
	SmartHammer# write memory
步骤**4**	在SmartHammer设备的Telnet或者ssh终端上配置，使得Telnet或者ssh终端上可以查看日志信息
	SmartHammer# terminal monitor
步骤**5**	进入配置模式
	SmartHammer# configure terminal
步骤**6**	将dot1x模块的日志信息记录到系统内存中，系统内存的大小限制为20K。
	SmartHammer(config)# log dot1x memory upto informational SmartHammer(config)# log memsize 20
步骤**7**	将系统内存中的日志信息拷贝到TFTP服务器上，并取名为log.txt
	SmartHammer# copy logmemory tftp://192.168.0.1/log.txt


注意

如果日志记录达到内存大小的设置限制，则日志信息会循环记录，始终保持规定大小的最新日志信息。

6 配置以太网端口

以太网端口的配置比较简单，主要用于让系统管理员根据实际情况配置以太网端口，以便在实际组网时满足需要。通过端口的配置管理，可以让通过网络连接介质（比如网线）连接的两个端口更好的协同工作。比如，让网线两端的端口速率保持一致。通常情况下，您并不需要更改端口设置。

6.1 以太网端口概述

以太网端口的配置是进行系统配置的一个组成部分，通过配置以太网端口可以实现更改端口的带宽设置、双工模式以及端口速率等设置等功能。对于端口的命名，如果是 100M 网卡，则名称前缀为 eth，比如 eth0，eth1 等等，如果是 1000M 网卡，则名称前缀为 ge，比如 ge0，ge1 等等，SmartHammer 设备的所有端口缺省状态下是打开的。

6.2 配置以太网端口

6.2.1 缺省配置

表6-1 端口缺省设置信息

内容	缺省设置	备注
端口自协商配置（auto on/off）	on	可以更改设置
端口双工模式(duplex)	无	可以更改设置
端口速率(speed)	无	可以更改设置
打开关闭端口(shutdown/no shutdown)	no shutdown	可以更改设置

6.2.2 启用自协商功能

默认情况下，端口参数是自协商的，在自协商模式下，端口的所有参数都是自动协商出来的，不能设置端口的参数。

启用端口自协商功能的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	auto on	启用端口的自协商功能
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

6.2.3 禁用自协商功能

默认情况下，端口参数是自协商的。禁用自协商功能后，可以对端口参数进行配置。

禁用端口自协商功能的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	auto off	禁用端口的自协商功能
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

缺省情况下端口的自协商功能是打开的，用户必须关闭端口的自协商功能后才能对端口的其他参数进行配置。

6.2.4 双工设置

双工就是在相对的方向上可以同时传输信息。半双工可以实现双向的通信，但不能在两个方向上同时进行，必须轮流交替地进行。与共享式 HUB 相连时，应置以太网口为半双工方式；与交换式 LANSWITCH 相连时，一般置以太网口为全双工方式。

配置端口双工模式的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	duplex (full|half)	配置端口的双工模式

步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

6.2.5 速率设置

端口速率表示了端口收发数据包的速率，通常为 10M 和 100M。要使网络互联设备可以正常工作，必须保证相互连接的两个端口配置有相同的速率。

端口速率设置的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	speed (10|100)	配置端口的速率
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置


注意

1000M 的配置为非标准配置，不支持手工配置，必须自协商。

6.2.6 关闭端口

端口关闭后将不再收发数据，主要用于系统故障的发现和诊断，但是通常情况下不需要这样做。

关闭端口的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	shutdown	关闭端口
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

6.3 配置信息显示命令

6.3.1 显示所有端口的信息

显示所有端口信息的步骤：

配置步骤：

步骤**1**	显示所有端口的信息

```
SmartHammer# show interface
Interface lo: Link status is down,Admin status is up
index 1 metric 1 mtu 16436 <UP,LOOPBACK,RUNNING>
Auto-Negotiation is disabled,  Duplex mode:  Full, Speed:  100Mbps
inet 127.0.0.1/8
input packets 0, bytes 0, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 0, bytes 0, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0
Interface ge0: Link status is up,Admin status is up
index 2 metric 1 mtu 1500
<UP,BROADCAST,RUNNING,MULTICAST,LINK>
HWaddr: 00:80:c2:00:10:00
Auto-Negotiation is disabled,  Duplex mode:  Full, Speed:  100Mbps
inet 192.168.0.55/16 broadcast 192.168.255.255
input packets 116, bytes 8646, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 86, bytes 5908, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0
Interface ge1: Link status is up,Admin status is up
index 3 metric 1 mtu 1500
<UP,BROADCAST,RUNNING,MULTICAST,LINK>
HWaddr: 00:80:c2:00:10:01
Auto-Negotiation is disabled,  Duplex mode:  Full, Speed:  100Mbps
inet 172.16.16.88/16 broadcast 172.16.255.255
input packets 18, bytes 1332, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 7, bytes 402, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0
Interface ge2: Link status is down,Admin status is up
  index 4 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:80:c2:00:10:02
  Auto-Negotiation is disabled,  Duplex mode:  Full, Speed:  100Mbps
  input packets 0, bytes 0, dropped 0, multicast packets 0
  input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
  output packets 0, bytes 0, dropped 0
  output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0
```

可以看到，当前有四个端口（lookback、ge0、ge1以及ge2），以及每个端口的一些具体信息（可以参考下一节显示某个端口的信息）。

6.3.2 显示某个端口的信息

显示某个端口信息的步骤：

步骤1	显示某个端口的信息
	SmartHammer# show interface ge0 Interface ge0: Link status is up,Admin status is up index 2 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST,LINK> HWaddr: 00:80:c2:00:10:00 Auto-Negotiation is disabled, Duplex mode: Full, Speed: 100Mbps inet 192.168.0.55/16 broadcast 192.168.255.255 input packets 5620, bytes 649403, dropped 0, multicast packets 0 input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0 output packets 746, bytes 61016, dropped 0 output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0 collisions 0 可以看到端口ge0的具体信息，连接状态是up的，即物理上和其他端口处于连接上状态，管理状态是up的，即没有在该接口上运行shutdown；端口索引为2，跳数为1，mtu为1500（可以携带的最大包长）；硬件地址：10:22:33:44:55:25；自协商已经被禁止，全双工，端口速率100Mbps；端口ip地址为192.168.0.55，子网掩码为16位长，广播地址为 192.168.255.255；目前收到了5620个包，共649403字节长，丢包个数为0，收到多播包0个，接收错误0次；输出了746个包，共61016字节长，丢包个数为0，输出错误0次。

6.4 配置案例

案例描述

将端口 ge0 的带宽设置为 100K，速率设置为 100Mbps，双工模式设置为全双工，关闭端口 ge0。

配置步骤：

步骤1	进入以太网端口配置模式
	SmartHammer(config)# interface ge0
步骤2	配置端口带宽为100K
	SmartHammer(config-if)# bandwidth 100
步骤3	配置端口ge0的带宽为100Mbps
	SmartHammer(config-if)# speed 100

步骤4	配置端口ge0为全双工工作模式
	SmartHammer(config-if)# duplex full
步骤5	关闭端口ge0
	SmartHammer(config-if)# shutdown

6.5 故障分析

用如下方法测试以太网端口是否正常工作：

- 在网络负载小时，从 PC 机（PC 机与 SmartHammer 设备位于同一局域网内）ping SmartHammer 设备的以太网口，观察是否能正确返回全部报文；
- 在网络负载大时，查看连接双方(如 SmartHammer 设备和交换机)的端口统计信息，观察接收到错帧的统计数量是否快速增加。
- 如果这两项测试中有任何一项不能通过，则可以断定 SmartHammer 设备的以太网口工作不正常。
- 在确认以太网有故障之后可按如下步骤进行排错：
- 查看物理设备连接是否正常
- 在物理设备连接正常的情况下，网线两端端口对应的 Link 指示灯应点亮。
- 查看连接双方速率设置是否一致
- 如果一方工作于 100Mbps 模式，而另一方工作于 10Mbps 模式时，端口也不会正常工作。故障表现为：配置为 100Mbps 模式的一方显示为端口 DOWN；配置为 10Mbps 模式的一方则显示为端口 UP。对于这种故障，只要使用 speed 命令把连接双方的速率配成一致即可。
- 查看连接双方是否处于同一网络
- 连接双方必须处于同一网络，即二者的网络地址一样而主机地址不同，如果二者网络地址不一样请用 ip address 命令正确设置 IP 地址。
- 查看连接双方的双工模式是否一致（其中一方为 SmartHammer 设备）
- 当双工模式不一致，即一方工作于全双工模式，而另一方工作于半双工模式，故障表现为：

网络流量增大时，配置为半双工模式的一方显示碰撞频繁（如连接共享式 Hub 则整个网络段上所以其它机器都显示碰撞严重），配置为全双工模式的一方则显示接收到大量错包，同时，双方丢包严重。

可用 show interface [IFNAME]命令查看以太网收发包的错误率，碰撞现象一般可以通过网口状态指示灯观察到；

在连接共享式 Hub 时，应该以半双工模式工作；在连接 Lanswitch 时，一般使用全双工模式工作。

7 配置 GRE 接口

GRE 协议的英文全称是 Generic Routing Encapsulation，即通用路由封装协议，它规定了如何将一种协议的报文封装在另一种协议的报文中进行传输。

7.1 GRE端口概述

本章讲述 SmartHammer 上 GRE 隧道功能的使用和 GRE 接口的配置。使用 GRE 协议与对端路由器或防火墙设备建立虚拟的、点对点通信。GRE 是第三层的隧道协议，它利用一种协议的传输能力为另一种协议建立了点到点的隧道，被封装的报文将在隧道的两端进行封装和解封。

SmartHammer 仅支持封装 IP 类型的网络数据包。

7.1.1 配置GRE接口

GRE 接口需要手工创建，配置 GRE 接口分为以下几步：

- 创建 GRE 接口。
- 指定 GRE 接口的 IP 地址。
- 配置 GRE 接口对应的物理接口。
- 配置 GRE 隧道的对端 IP 地址。

7.1.2 创建GRE接口

GRE 接口是用于 GRE 通信的虚拟接口，默认情况下该接口并不存在，因此需要手工创建。SmartHammer 通过 GRE 接口将 GRE 封包的网络数据包发送到对应的物理接口，再发送到对端设备。

创建 GRE 接口的配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface gre <0-1023>	创建一个gre接口，<0-1023>为要创建的GRE接口的编号


注意

对于已建立的 GRE 通信，删除 GRE 接口会断开相应的 GRE 隧道

7.1.3 绑定GRE接口到物理接口

GRE 接口是虚拟接口，因此必须要指定其对应的物理接口

绑定 GRE 接口到物理接口的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface gre <0-1023>	创建一个gre接口，<0-1023>为要创建的GRE接口的编号
步骤3	source (A.B.C.D|IFNAME)	其中A.B.C.D是要绑定的物理接口的IP地址，或者IFNAME是要绑定的物理接口的名字

7.1.4 配置GRE隧道对端IP地址

配置 GRE 隧道对端 IP 地址的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface gre <0-1023>	创建一个gre接口，<0-1023>为要创建的GRE接口的编号
步骤3	destination A.B.C.D	其中A.B.C.D为GRE隧道对端物理接口的IP地址

7.1.5 配置GRE接口的IP地址

配置 GRE 接口的 IP 地址的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface gre <0-1023>	创建一个gre接口，<0-1023>为要创建的GRE接口的编号
步骤3	ip address A.B.C.D/M	A.B.C.D/M为GRE接口的IP地址

7.2 配置信息显示命令

显示 GRE 接口信息：

步骤1	show interface gre <0-1023>	显示GRE接口的信息

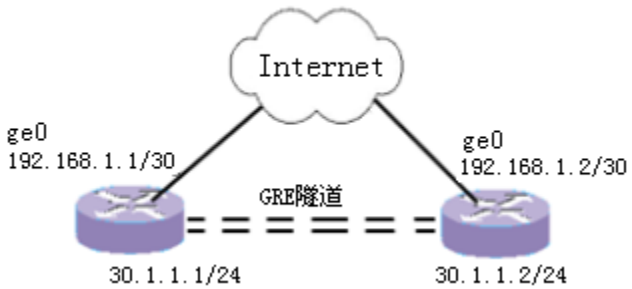
7.3 配置案例

7.3.1 将系统中所有模块的日志信息记录到日志服务器上

案例描述

通过 ge0 接口 IP 地址 192.168.1.1/30 与对端 SmartHammer(IP 为 192.168.1.2/30)建立 GRE 隧道，gre0 的 IP 地址 30.1.1.1/24，如下图所示：

配置 GRE 隧道组网图：



配置步骤：

步骤1	配置物理接口的IP地址
	SmartHammer(config)interface ge0 SmartHammer(config-if)ip address 192.168.1.1/30 SmartHammer(config)exit
步骤2	创建gre0
	SmartHammer(config)interface gre0
步骤3	绑定gre接口到物理接口
	SmartHammer(config-if)source ge0
步骤4	配置隧道对端IP地址
	SmartHammer(config-if)destination 192.168.1.2
步骤5	配置gre0接口IP地址

	SmartHammer(config-if)ip address 30.1.1.1/24 SmartHammer(config-if)exit

对端 SmartHammer 设备也要做类似的配置。其配置如下：

配置步骤：

步骤**1**	配置物理接口的IP地址
	SmartHammer(config)interface ge0 SmartHammer(config-if)ip address 192.168.1.2/30 SmartHammer(config)exit
步骤**2**	创建gre0
	SmartHammer(config)interface gre0
步骤**3**	绑定gre接口到物理接口
	SmartHammer(config-if)source ge0
步骤**4**	配置隧道对端IP地址
	SmartHammer(config-if)destination 192.168.1.1
步骤**5**	配置gre0接口IP地址
	SmartHammer(config-if)ip address 30.1.1.2/24 SmartHammer(config-if)exit

8 配置 VLAN 接口

本章涉及 SmartHammer 设备 VLAN 的配置，内容主要包括：

- VLAN 概述
- 配置接口封装的链路层协议为 VLAN

8.1 VLAN概述

在一个物理局域网内，通过对端口的划分，将局域网内的设备分割为几个各自独立的群组，群组内部的设备之间可以自由地通讯，而当分属不同群组的设备要进行通讯时，必须进行三层的路由转发；通过这种方式，一个物理局域网就如同被划分为几个相互隔离的局域网，这些不同的群组就称为虚拟局域网（VLAN）。对于以端口划分的 VLAN 而言，任何一个端口的集合都可以被看作是一个 VLAN。VLAN 的划分不受硬件设备物理连接的限制，用户可以通过命令灵活地划分端口，创建定义 VLAN。使用 VLAN 的优点如下：

1．VLAN 能帮助控制流量

在传统网络中，不管是否必要，大量广播数据被直接送往所有网络设备，从而导致网络堵塞。而 VLAN 的设置能够使每个 VLAN 只包含那些必须相互通信的设备，从而减少广播、提高网络效率。

2．VLAN 提供更高的安全性

每个 VLAN 中的设备只能与本 VLAN 中的设备通信。例如，如果 Market 部门 VLAN 内设备要和 Sales 部门 VLAN 内设备通信，则只有通过路由器才能进行，在没有三层路由设备的情况下两个部门不能直接通信，从而提高了网络安全性能。

3．VLAN 使网络设备的变更和移动更加方便

在传统网络中，网络管理员不得不在网络设备的变更和移动上花费大量的时间和精力。如果用户移动到另一个不同的子网，那么每个终端的地址都得重新设置。而使用 VLAN 则不需要这些复杂繁琐的设置。

8.1.1 SmartHammer设备对VLAN的支持

SmartHammer 设备起到连接不同的 VLAN 的作用，它各有一个端口连接到这些 VLAN 上，从 SmartHammer 设备的角度与从终端的角度来看，整个网络看起来像自然的局域网一样连接。

SmartHammer 设备只实现对 VLAN 的终结功能。

8.1.2 802.1Q协议简介

在两个设备之间的链路上，包可能属于 VLAN1，也可能属于 VLAN2。所以 IEEE 的 802.1Q 提出了一个方案，给包增加一个附加信息（称为 VLAN 标识，VLAN Tag），以便设备能够分清这个包应该发给哪个 VLAN。

VLAN 标识占两个字节，其中 3 位表示优先级，12 位用于表示 VLAN 的 ID，1 位用于表示地址是否属于规范格式。通过使用以太网类型 0x8100 来确定存在 VLAN 标识。例如，以太网中可能出现带 Tag 和不带 Tag 的数据包，如下图所示：

不带 VLAN 标识的以太网包

6	6	2	46--1500	4
目的	源	协议	数据	FCS

带 VLAN 标识的以太网包

6	6	2	2	2		4
目的	源	8100	VLAN tag	协议类型	数据	FCS

但是，如果终端收到一个带 VLAN 标识的包，它可能会混淆，所以设备必须区分哪些端口连的是交换机，哪些端口连接的是终端。

在交换机中，直接与主机相连的端口是无法识别 802.1Q 报文的，那么这种端口称为 Access 端口；对于与交换机相连的端口，可以识别和发送 802.1Q 报文，那么这种端口称为 Tag Aware 端口。

交换机在把带 VLAN 标识的包发送给 Access 端口时，需要先除去包中的 VLAN 标

识。

8.2 配置接口封装的链路层协议为 VLAN

如果要让 SmartHammer 设备识别带 VLAN 标识的包，需要创建一个以太网子接口，并且为其指定一个 VLAN ID，则可以通过该子接口接收/转发带 VLAN 标识的包。

VLAN ID 值的说明：

SmartHammer 设备的 VLAN ID 值的范围是 1-4094，这个值是通过使用 interface IFNAME.VID 指令创建以太网子接口时设定的，例如，如果创建了一个以太网子接口 ge1.10，则为这个子接口指定了 VLAN ID 为 10。

配置接口封装的链路层协议为 VLAN 的步骤:

步骤1	interface IFNAME.VID	用于创建创建以太网子接口，并在该接口上使用VLAN封装，VLAN ID为VID。
步骤2	ip address A.B.C.D/M	设置端口的IP地址


注意

当该以太网接口已加入网桥，则不能创建 VLAN 子接口

8.3 配置信息的显示

VLAN 配置信息显示命令:

步骤1	show interface	显示接口信息

8.4 配置案例

8.4.1 在两个VLAN之间做路由连接

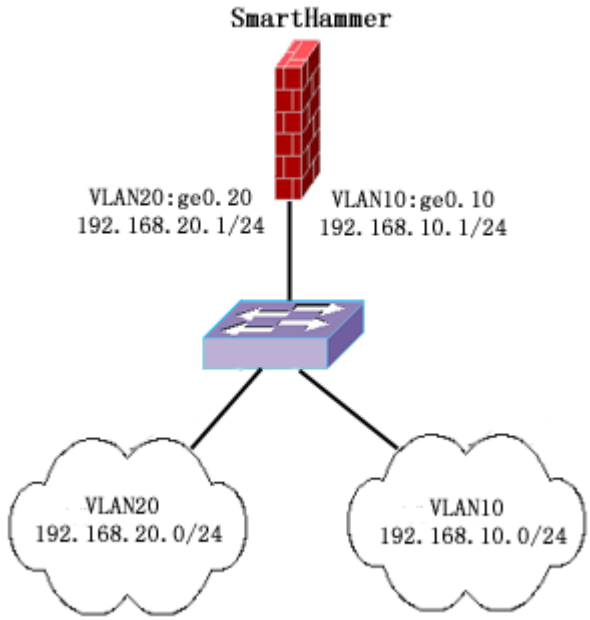
案例描述

交换机与 SmartHammer 设备相连。在该交换机上划分两个 VLAN：VLAN 10 和

VLAN 20，VLAN 10 的 VLAN ID 为 10，包含端口 1、2、3，端口 1 为 Taged 端口，连接 SmartHammer 的 ge0 接口，端口 2、3 为 Untaged 端口，下接 192.168.10.0/24 网段；VLAN 20 的 VLAN ID 为 20，包含端口 1、4、5，端口 1 为 Taged 端口，连接 SmartHammer 的 ge0 接口，端口 4、5 为 Untaged 端口，下接 192.168. 20.0/24 网段；

在 SmartHammer 设备的 ge0 接口上也划分两个 VLAN，ge0.10 和 ge0.20，VLAN ID 分别为 10 和 20。ge0.10 的 IP 地址为 192.168.10.1/24；ge0.20 的 IP 地址为 192.168. 20.1/24。

图8-1 VLAN 案例组网图



配置步骤

步骤**1**	创建子接口ge0.10，并指定IP地址
	SmartHammer# configure terminal SmartHammer(config)# interface ge0.10 SmartHammer(config-if)# ip address 192.168.10.1/24 SmartHammer(config-if)# exit
步骤**2**	创建子接口ge0.20，并指定IP地址
	SmartHammer(config)# interface ge0.20 SmartHammer(config-if)# ip address 192.168.20.1/24 SmartHammer(config-if)# exit

步骤3	保存配置
	SmartHammer(config)# write memory

8.5 故障分析

8.5.1 VLAN无法正常工作

故障现象	VLAN无法正常工作
分析与解决	1.请检查配置，是否是您需要配置的VLAN ID，您的配置是否正确 2.网络拓扑是否正确 3.线路是否正常 4.VLAN状态是否正确

8.6 常用调试功能

8.6.1 debug vlan recv

应用环境：当 VLAN 转发不正常时。

调试实例：

```
SmartHammer(config)# terminal monitor
SmartHammer(config)# debug vlan recv
Recv from device ge1.20 VLAN ID: 20
```

结果分析：

显示从 ge1.20 接口成功收到报文。


注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug vlan recv 命令禁用此功能。

8.6.2 debug vlan send

应用环境：当 VLAN 转发不正常时。

调试实例：

```
SmartHammer(config)# debug vlan send
Send from device ge1.10, dst 05:10:3C:42:DE:5F, src 00:11:5D:B3:4C:25
SmartHammer(config)# terminal monitor
```

结果分析：

显示从 ge1.10 接口成功发送报文


注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug vlan send 命令禁用此功能。

9 配置 LoopBack 接口

9.1 LoopBack接口概述

LoopBack 接口是 SmartHammer 中由软件实现的环回接口，它是 SmartHammer 中应用广泛的一种虚拟接口，通常用于测试及管理的作用，由于 LoopBack 的 IP 地址不占用实际 IP 地址，因此对于一些服务和路由协议的运行来说，在 LoopBack 接口上配置比在物理接口上配置要方便。

9.2 配置LoopBack接口

LoopBack 接口默认只有一个，其在系统中的接口名为 lo，要产生更多的 LoopBack 接口需要手工创建。

9.2.1 缺省情况

缺省情况只有 IP 地址为 127.0.0.1/8 的一个 Loopback 设备，即端口 lo。

9.3 配置信息的显示

LoopBack 接口配置信息显示命令：

步骤**1**	show interface lo <NUM>	显示Loopback接口的信息

9.4 配置案例

案例描述：

创建 Loopback 接口 lo1，配置该接口 IP 地址 192.168.0.2/32。

配置步骤：

步骤**1**	创建接口lo1
	SmartHammer(config)interface lo1
步骤**2**	配置lo1的IP地址为192.168.0.2/32
	SmartHammer (config-if)ip address 192.168.0.2/32 SmartHammer (config)exit

这样，管理员可以运行 Telnet 或者 SSH 软件远程登录 192.168.0.2。

10 配置透明网桥

本章涉及 SmartHammer 设备产品对透明网桥的配置，内容主要包括：

- 透明网桥概述
- 配置透明网桥
- 配置网桥组端口

10.1 透明网桥概述

透明网桥功能：最初是由 DEC 公司提出，并被 802.1 委员会采纳并标准化。透明网桥具有以下特征：

- 杂侦听和存储转发能力
- 点学习能力
- 生成树算法

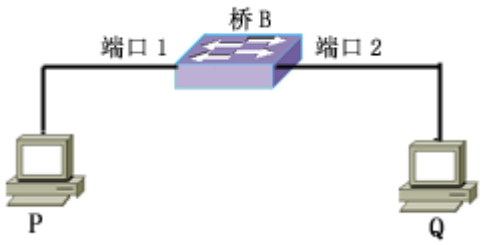
透明网桥使用最方便，易于安装。当桥接入互连的局域网内，就能运行。它不会影响现存的局域网，原有的软硬件无须改变，也不要设置地址开关和加载路径选择表参数，对于用户来说，该网桥是透明的，即该网桥进入或离开整个网络，用户感觉不到。透明网桥接收来自各局域网发送的帧，并将它送到目的局域网。它的缺点是不能最优地利用系统的带宽，只能用于分支拓扑结构的互连网络中。

10.1.1 透明网桥的特征

- 混杂侦听和存储转发

最基本的透明网桥形式，是连接到两个或更多 LAN 上(与 LAN 之间的接口称为端口)的网桥。这种网桥混杂侦听传输经过的每个包，存储接收到的每一个包直到它可以被发送到除源 LAN 之外的 LAN 上去，如下图所示：

图10-1 最简单的网桥连接



网桥拓展了 LAN 的功能。在用网桥连接几个 LAN 时，网桥在接收包时，并不马上发送它，而是先把整个包接收下来并存储，然后等待另外一边的 LAN 变为空闲。这样可以避免网桥两边的两个站点在同时发送时所导致的冲突。

■ 站点学习功能

网桥想知道哪些站点在哪些 LAN 上，则它使用如下的策略：

1）网桥混杂侦听，接收所经过的每一个包。

2）对于每一个接收到的包，网桥都会在缓冲区（称为站点缓冲区）中记录下源地址信息和该包所来自的端口的信息。

3）对于收到的每一个包，网桥在站点缓冲区内查找包的目的地址：

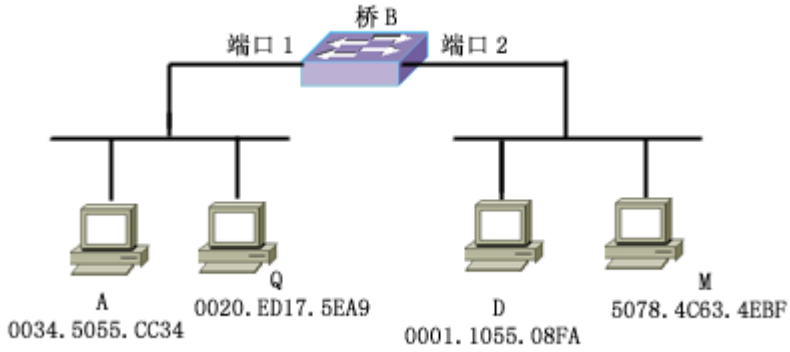
如果站点缓冲区内没找到这个地址，网桥把这个包转发给除接收此包的接口之外的所有接口。

如果在站点缓冲区内找到这个地址，则网桥只向列表中指定的接口转发该包。如果该指定的接口就是接收该包的接口，则抛弃这个包（即过滤）。

4） 网桥对站点缓冲区中的每一条目进行计时，然后删除那些在一定时间(用参数 aging time 表示)内一直没有包发送来的地址项。

假定拓扑结构如下图所示，桥 B 开始的时候对拓扑结构一无所知。

图10-2 开始时，网桥 B 不知道任何站点的地址



现在假定站点 A 要发送一个包给 D。这个包如下图所示：

图10-3 A 向 D 发送的数据包

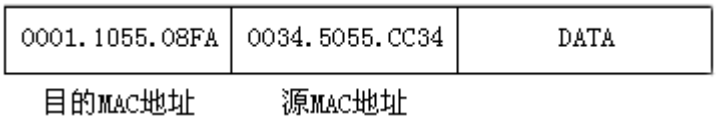
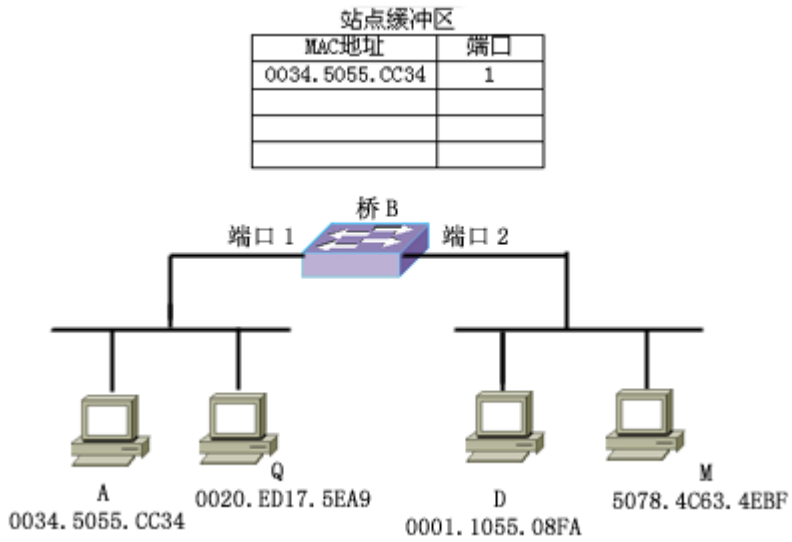


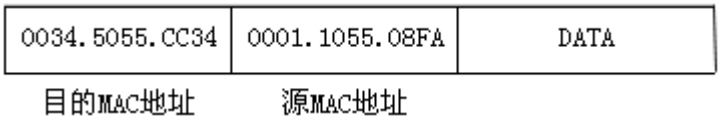
图10-4 网桥知道了 A 的位置



网桥通过查看包的源地址并注意到包是从端口 1 收到的，则它判断出 A 在端口 1 的那端。但网桥还不知道站点 D 位于何处，所以它把这个包往所有端口(端口 1 除外)转发。在这个例子里，只往端口 2 转发这个包。如上图所示。

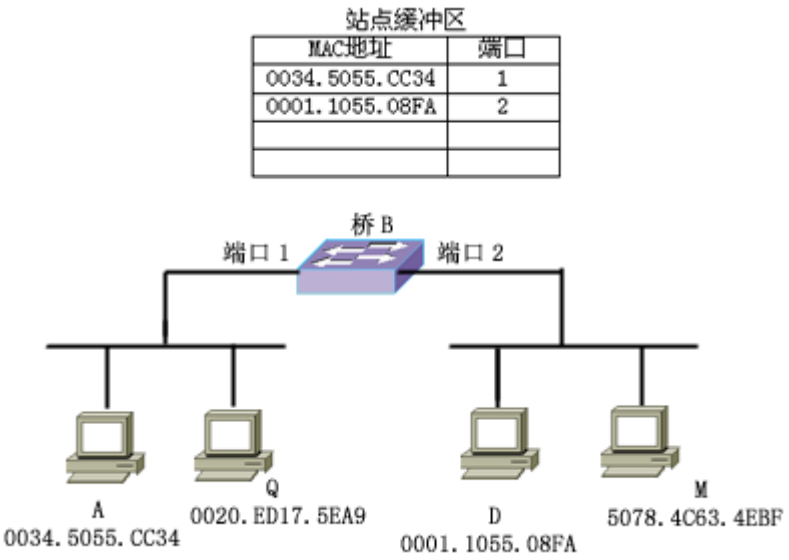
现在假定站点 D 要发送一个包给站点 A

图10-5 站点 D 向站点 A 发送数据包



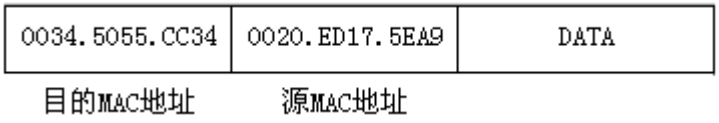
网桥发现这个包是通过端口 2 发送过来的，因而可以判断出 D 位于端口 2 的位置。而且，网桥已经知道 A 位于端口 1 的位置，因而直接把这个包转发到端口 1，如下图所示：

图10-6 网桥知道了 D 的位置



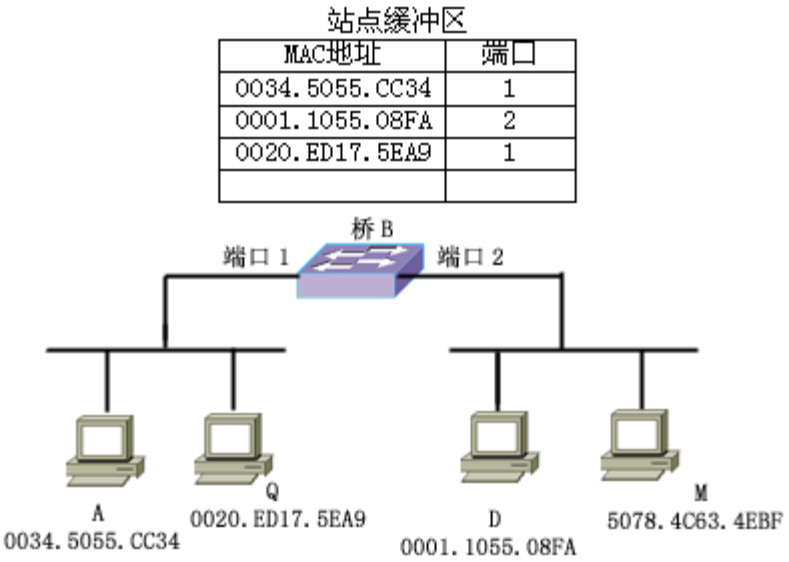
现在假定站点 Q 发送了一个包给 A，如下图所示：

图10-7 Q 向 A 发送一个数据包



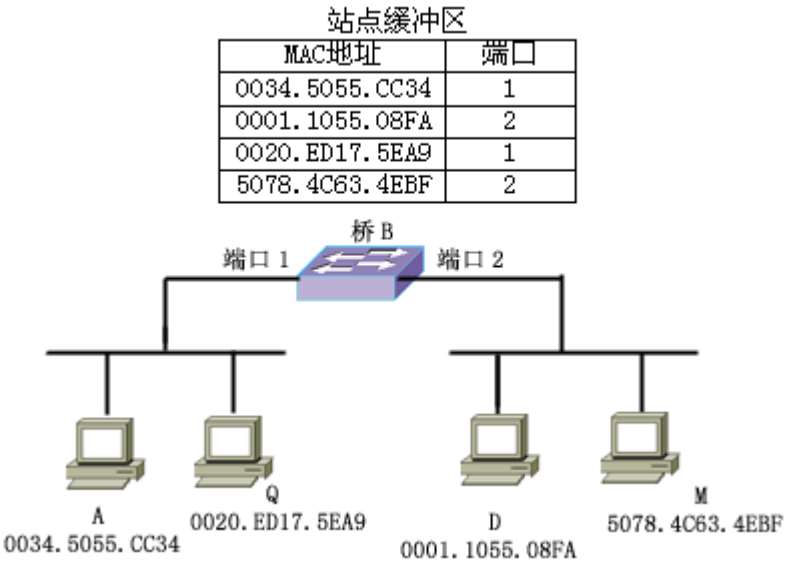
网桥发现这个包是 Q 通过端口 1 发送过来的，因而判断出 Q 位于端口 1 的位置。而网桥已经知道 A 也位于端口 1 的位置，因而知道它没有必要对这个包进行转发，如下图所示：

图10-8 网桥知道了 Q 的位置



按照这个规则，最终，网桥将建立如下图所示的站点缓冲区：

图10-9 网桥现在知道了整个拓扑结构



10.1.2 SmartHammer 设备上透明网桥的实现

在 SmartHammer 设备上是通过配置 BVI（Bridge-group Virtual Interface）接口实现透明网桥功能。

一个 BVI 接口代表一个网桥，将不同的端口（物理或虚拟端口）加入同一个网桥中，从而可以实现在不同端口之间的桥接交换，配置为同一个网桥组中的所有端口属于同一个二层的广播域。

SmartHammer 防火墙可以实现在混合模式下工作，即在不同的 BVI 之间或 BVI 与其它的端口之间可以实现路由的能力。

SmartHammer 防火墙目前不启用 STP（生成树）协议。

10.2 配置透明网桥

10.2.1 缺省设置

SmartHammer 设备产品关于透明网桥的缺省设置信息如以下表格所示：

表10-1 透明网桥的缺省设置信息：

内容	缺省设置	备注
STP	disable	不可更改设置
网桥优先级（priority）	32768	建议不更改
网桥组端口（port）优先级（priority）	32768	建议不更改

10.2.2 创建透明网桥

创建透明网桥的步骤：

步骤**1**	interface NAME	创建一个网桥（BVI端口），NAME以bvi开头，后面添加从0到255的数字，代表从0到255的网桥
步骤**2**	write memory	保存配置

10.2.3 配置网桥组端口

配置透明网桥后，需要将实际物理接口和虚拟接口加入网桥中，这些接口被称为网桥组端口。

网桥组端口的 ID 由两部分组成：1 字节的优先级和 1 字节的端口号。当网桥有两个端口都连接在 LAN 上从而形成回路时，可以通过网桥端口 ID 来影响端口的选择，ID 越小的端口越有可能成为指定端口。因此，如果网桥端口的优先级越小，则网桥端口的 ID 越小，越有可能成为指定端口。

同一个接口只能加入到一个网桥组。以太网主接口和子接口（VLAN 接口）不能同时加入网桥组。

配置网桥组端口的步骤：

步骤**1**	interface NAME	进入一个端口
步骤**2**	bridge-group <0-255>	将本端口加入一个网桥组，同时该端口的所有IP地址将被删除
步骤**3**	write memory	保存配置


注意

1)将一个端口加入一个网桥组时该端口的所有 IP 地址将被删除。

2）以太网主接口和子接口（VLAN 接口）不能同时属于同一个网桥组。

3）以太网主接口和子接口（VLAN 接口）不能同时属于不同的网桥组。

4）一个网桥组中最多只能加入 254 个端口。

10.3 配置信息显示命令

表10-2 透明网桥配置信息显示命令

命令	解释
show bridge [NUM]	显示网桥（组）信息
show bridge-group [NUM]	显示网桥组下各端口的信息
show bridge-fdb NUM	显示网桥的FDB信息
show bridge fdb IFNAME	显示网桥组下各端口的FDB信息

10.3.2 显示信息实例

show bridge 显示实例：

步骤**1**	show bridge命令显示举例
	SmartHammer# show bridge ---------- Bridge : bvi1 bridge id : fa00.00034708d824 designated root : fa00.00034708d824

表10-3 show bridge 命令显示信息各个主要字段的解释

字段	含义
Bridge id	本网桥组的ID。包括两个部分：priority和address。如本例中，是2个字节的优先级fa00，和6个字节的MAC地址0003.4708.d824
Designated root	指明网桥的优先级和MAC地址。

show bridge-group 显示实例：

步骤**1**	show bridge-group命令显示举例

```
SmartHammer # show bridge-group
================================================
Bridge   : bvi1
------------------------------------------------
 bridge port : interface ge0 (1)
 port id                    : 8001
 state                      : forwarding
 designated root        : fa00.00034708d824
 designated bridge      : fa00.00034708d824
 ------------------------------------------------
```

表10-4 show bridge 命令显示信息各个主要字段的解释：

字段	含义
Port id	指明端口的ID
state	指明端口的状态
designated root	指明根网桥的优先级和MAC地址。
designated bridge	指明该端口所连LAN上的指定网桥的优先级和MAC地址

show bridge-fdb 显示举例：

步骤**1** show bridge-fdb命令显示举例

```
SmartHammer # show bridge-fdb 20
-----------------------------------------------------------------
Bridge   : bvi20

Address                 Action          Interface
00:0d:56:4f:a9:c8       forwarding      ge0
00:08:0c:00:00:01       forwarding      ge0
00:0d:56:4f:a6:ee       forwarding      ge0
00:10:dc:4a:eb:37       forwarding      ge0
50:78:4c:65:2a:c9       forwarding      ge0
00:10:dc:4e:a8:41       forwarding      ge0
00:10:5c:b3:9c:25       forwarding      ge0
50:78:4c:68:3c:33       forwarding      ge0
00:c0:9f:21:25:d2       forwarding      ge0
00:01:40:55:84:df       forwarding      ge0
00:08:0c:19:01:01       forwarding      ge0
00:08:74:d9:9b:47       forwarding      ge0
00:0b:db:55:4a:3a       forwarding      ge0
00:0b:db:62:e3:ef       forwarding      ge0
00:05:3b:10:78:96       forwarding      ge0
00:10:dc:0e:63:84       forwarding      ge1
00:20:ed:a7:06:cc       forwarding      ge1
```

show bridge fdb 命令显示举例：

步骤**1** show bridge fdb命令显示举例

```
SmartHammer # show bridge fdb ge0
-------------------------------------------------------------
Bridge    : bvi20

Address                  Action            Interface
00:0d:56:4f:a9:c8        forwarding        ge0
00:08:0c:00:00:01        forwarding        ge0
00:0d:56:4f:a6:ee        forwarding        ge0
00:10:dc:4a:eb:37        forwarding        ge0
50:78:4c:65:2a:c9        forwarding        ge0
00:10:dc:4e:a8:41        forwarding        ge0
00:10:5c:b3:9c:25        forwarding        ge0
50:78:4c:68:3c:33        forwarding        ge0
00:c0:9f:21:25:d2        forwarding        ge0
00:01:40:55:84:df        forwarding        ge0
00:08:0c:19:01:01        forwarding        ge0
00:08:74:d9:9b:47        forwarding        ge0
00:0b:db:55:4a:3a        forwarding        ge0
00:0b:db:62:e3:ef        forwarding        ge0
00:05:3b:10:78:96        forwarding        ge0
```

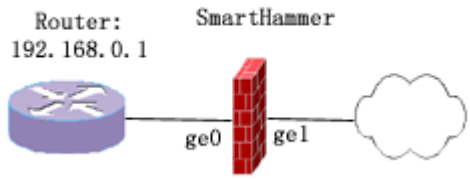
10.4 配置案例

10.4.1 配置透明网桥

案例描述

将 SmartHammer 设备插入一个原有的网络结构中，不改变原有拓扑和配置，将 SmartHammer 设备的 ge0 和 ge1 两个端口加入网桥组 0（BVI0）中。ge0 口连接 Router（192.168.0.1），ge1 口连接 192.168.0.0/16 网段其余机器。

案例组网图



配置步骤：

步骤1	创建透明网桥组0（BVI0）
	SmartHammer# configure terminal SmartHammer(config)# interface bvi0 SmartHammer(config-if)# exit

步骤2	将端口ge0加入透明网桥组0
	SmartHammer(config)# interface ge0 SmartHammer(config-if)# bridge-group 0 SmartHammer(config-if)# exit
步骤3	将端口ge1加入透明网桥组0
	SmartHammer(config)# interface ge1 SmartHammer(config-if)# bridge-group 0 SmartHammer(config-if)# exit
步骤4	保存配置
	SmartHammer (config)#write memory

10.5 常见故障

10.5.1 透明网桥无法正常工作

故障现象	在网桥的两个端口之间数据无法转发
分析与解决	是否将正确的端口加入网桥 链路是否正常 端口状态是否正常（该端口Admin状态是否是up）

10.6 常用调试功能

10.6.1 debug bridge recv

应用环境：当网桥转发不正常时。

调试实例：

```
SmartHammer(config)# terminal monitor
SmartHammer(config)# debug bridge recv
Recv from bridge bvi100, device ge1.10, dst 05:10:3C:42:DE:5F
```

结果分析：

显示从网桥 bvi100 的 ge1.10 端口成功收到报文。


注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug bridge recv 命令禁用此功能。

10.6.2 debug bridge send

应用环境：当网桥转发不正常时。

调试实例：

```
SmartHammer(config)# terminal monitor
SmartHammer(config)# debug bridge send
Send from device ge1.10
```

结果分析：

显示从网桥的 ge1.10 端口已发送报文


注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug bridge send 命令禁用此功能。

11 配置 ARP 和代理 ARP

本章涉及 SmartHammer 防火墙产品 ARP 的配置，内容主要包括：

- 配置静态 ARP
- 配置代理 ARP

11.1 ARP概述

11.1.1 ARP协议简介

Address Resolution Protocol (ARP)是一种将 IP 转化成以 IP 对应的物理地址的一种协议，或者说 ARP 协议是一种将 IP 地址转化成 MAC 地址的一种协议，它靠维持在内存中保存的一张表来使 IP 得以在网络上被目标机器应答。

11.1.2 ARP协议的作用

为什么要将 IP 转化成 MAC 呢？我们知道，在以太网中，对于处于同一子网的两个通信实体来说，他们的一次 IP 通信过程大致如下：

当源端发送一个 IP 包之前，它必须知道目的端的以太网地址才可以完成封装，可是此时源端只能知道目的端的 IP 地址（通过用户的事先配置或者查路由表），这样就必须依靠 ARP 协议来完成目的端以太网地址的解析。因此源端发送一个包含目的 IP 地址的 ARP 请求，目的端收到后向源端返回 ARP 应答，通告自己的 MAC 地址，源端获得目的端 MAC 地址后才可以将 IP 包封装在以太网头中发送出去。

11.1.3 代理ARP简介

代理 ARP （proxy ARP），它是一种 IP 网络地址复用技术。代理 ARP 要求在主网络采用 ARP 协议进行 IP 地址→物理地址映射，当主网络上各台主机调用 ARP 解

析隐藏网络上主机的物理地址时，SmartHammer 防火墙代替主机响应，给出的物理地址是 SmartHammer 防火墙本身的物理地址，由 SmartHammer 防火墙来应答。而 SmartHammer 防火墙要求对隐藏网络的各主机了如指掌，这样所有进入隐藏网络的数据报文都先送到 SmartHammer 防火墙，SmartHammer 防火墙再将报文送往应该到达的主机，同样 SmartHammer 防火墙也掌握主网络上的主机，以便对外出的数据进行合适的操作。

11.2 ARP的配置

11.2.1 配置静态ARP

静态 ARP 主要针对特殊的主机或服务器而设立的，这种主机或服务器设备的 IP 和 MAC 通常不会改变，使用静态 ARP 可以提高系统性能和减轻网络负担(因为它避免了相关 ARP 报文的发送和处理)

在某些特定情况下（如局域网网关有一些固定的 IP 地址），就可利用静态 ARP 功能将这些 IP 地址绑定到某个指定网卡，使得到这些 IP 地址的报文只能通过该网关进行转发；或当用户需要过滤掉一些非法 IP 地址时，也可通过手工配置静态 ARP 表中的映射项来实现。

在接口下实现用户 IP 地址和 MAC 地址的绑定功能，可以通过以下步骤实现：

配置静态 ARP 的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	ip arp A.B.C.D xx:xx:xx:xx:xx:xx	添加静态ARP
步骤3	write memory	保存配置

添加的静态 ARP 表项的 IP 地址必须与 SmartHammer 某个接口的 IP 地址同属一个网段。

11.2.2 配置代理ARP

对于快速发展着的网络，接入网络的主机越来越多，物理分布也越来越广，在这种情况下，以太网中信息报文的冲突几率越来越大，严重影响网络传输的速率和效率，且物理距离的增大也大大增加了通讯的难度。于是不得不在物理上对网络进行重新

划分，以提高网络效率，但是同时为了满足属于同一逻辑网段但不属于同一物理网段的主机间进行通讯的要求，又不得不将不同的物理网段连接起来，为解决这一问题，提出了代理 ARP 的解决方案。

配置代理 ARP 的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface NAME	进入一个端口
步骤3	ip proxy-arp	启动接口下代理ARP功能
步骤4	write memory	保存配置

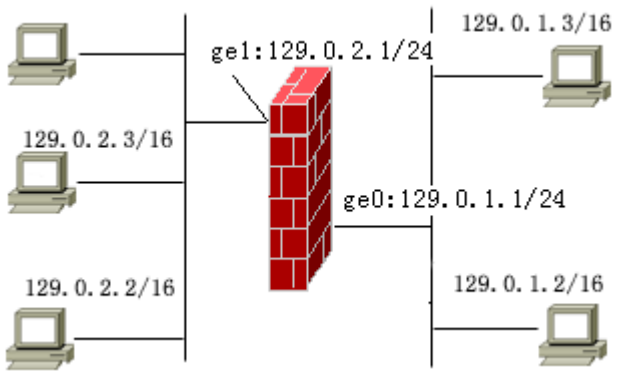
11.3 配置案例

11.3.1 代理ARP配置

案例描述

有两个属于同一逻辑网段 129.0.0.0/16 的子网段 129.0.1.0 和 129.0.2.0 处于不同的物理网络，它们通过 SmartHammer 连接在一起，SmartHammer 的 ge0 接口与子网段 129.0.1.0/24 相连，ge0 的 IP 地址为 129.0.1.1/24；SmartHammer 的 ge1 接口与子网段 129.0.2.0/24 相连，ge1 的 IP 地址为 129.0.2.1/24。(注意图中所有的主机的掩码都为 16)。

图11-1 代理 ARP 配置案例组网图



配置步骤：

步骤**1**	在接口ge0下启动Proxy ARP
	SmartHammer# configure terminal SmartHammer(config)# interface ge0 SmartHammer(config-if)# ip proxy-arp SmartHammer(config-if)# exit
步骤**2**	在接口ge1下启动Proxy ARP
	SmartHammer(config)# interface ge1 SmartHammer(config-if)# ip proxy-arp SmartHammer(config-if)# exit
步骤**3**	保存配置
	SmartHammer(config)# write memory

11.4 故障分析

11.4.1 代理ARP无法正常工作

故障现象	在两个接口下配置代理ARP，但两个接口之间互相不通。
分析与解决	1）请检查配置，您的配置是否正确 2）两个接口所接的子网段必须与该接口所配置的IP地址在同一网段。 3）线路是否正常

11.5 常用调试功能

11.5.1 debug arp recv

应用环境：当 ARP 工作不正常时。

调试实例：

```
SmartHammer(config)# terminal monitor
SmartHammer(config)# debug arp recv
rcvd req 172.16.6.10 0000.0c00.6fa2, dst 172.16.6.62 ge0
```

结果分析：

显示收到 172.16.6.10 到 172.16.6.62 的 ARP Request。


注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug arp recv 命令禁用此功能。

11.5.2 debug arp send

应用环境：当网桥转发不正常时。

调试实例：

```
SmartHammer(config)# terminal monitor
SmartHammer(config)# debug arp send
sent req 172.16.22.7 0000.0c01.e117, dst 172.16.22.96 0000.0000.0000 ge0
```

结果分析：

显示发送 172.16. 22.7 到 172.16. 22.96 的 ARP Request。

注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug arp send 命令禁用此功能。

12 配置 DHCP 服务

12.1 DHCP服务概述

DHCP 的全称是动态主机配置协议（Dynamic Host Configuration Protocol）。SmartHammer 设备可以作为 DHCP Server，用于实现对网络中 IP 地址的动态分配和集中管理。动态分配是指当 DHCP 客户端第一次从 DHCP Server 租用到 IP 地址后，并非永久的使用该地址，只要租约到期，客户端就要释放(Release)这个 IP 地址以给其它工作站使用。为了实现 IP 地址的动态分配，必须设置 DHCP Server 拥有一个 IP 地址范围，用来分配给用户，这个用来分配给客户端的地址范围也叫 IP 地址池（IP Pool）。

12.2 配置DHCP Server

下图反映了 DHCP 客户端从 DHCP 服务器申请 IP 地址的过程。主机 A（客户端）先广播 DHCPDISCOVER 包寻找网络上的 DHCP 服务器，DHCP 服务器向客户端单播包含配置参数的 DHCPOFFER 消息。

DHCP 客户端从 DHCP 服务器申请 IP 地址

- 当客户端第一次登录到网络时，它会向网络广播一个 DHCPDISCOVER 消息，此时由于客户端还不知道自己属于哪一个网路，所以封包的来源地址为 0.0.0.0，目的地址则为 255.255.255.255。
- 由于网络上可能不止一个 DHCP 服务器，凡是具有有效 IP 地址信息的 DHCP

服务器均从各自还没有租出的地址中选择一个空闲 IP，然后将该提议回应给客户端。

- 客户端从接收到的第一个提议中选定 IP 地址信息，并广播一条租用地址的消息请求。由发出该提议的 DHCP 服务器响应该消息，确认已接受请求并开始租用。
- 客户端收到确认后开始使用此地址


注意

DHCP 客户端可以接收多个 DHCP 服务器的消息，自己从中选一个 DHCP 服务器，同时也暗示它拒绝了其它 DHCP 服务器应答的配置参数。

12.2.1 缺省设置

DHCP 服务缺省为不启用

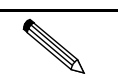
12.2.2 配置DHCP 子网范围

供 DHCP 分配的地址的集合称为 DHCP 地址池，地址池可以不是连续的，但它们总是属于一个或者多个不同的网段，这种网段称为 DHCP 分配地址的 subnet 即子网范围。必须要配置 DHCP 子网后 DHCP 服务器才知道在哪个接口启用 DHCP 服务，因此，合法的 DHCP 子网范围隶属于某个接口所在的子网，如接口 ge0 的 IP 地址为 172.1.1.1/24，则相应的 DHCP 子网配置为 **share-net** NAME subnet 172.1.1.0/24。

该命令用于配置 DHCP 的子网范围，同时启用子网范围所在接口的 DHCP 服务。

配置 DHCP 子网范围的步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	dhcp	进入DHCP配置模式
步骤**3**	share-net NAME subnet A.B.C.D/M	配置名为NAME的一个子网，范围A.B.C.D/M
步骤**4**	end	返回特权模式


提示

可以配置比接口地址所在子网更小的 DHCP Subnet，超过接口地址所在子网范围的 DHCP subnet 和不存在接口地址子网的 DHCP Subnet 是无效的。你必须退出到配置模式才会启用相应接口上的 DHCP 服务。

12.2.3 配置DHCP地址池

在一个 subnet 中供 DHCP 分配的地址的集合称为 DHCP 地址池。必须配置 DHCP 地址池 DHCP 服务器才知道要分配哪些 IP 地址。

配置 DHCP 地址池的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	dhcp	进入DHCP配置模式
步骤3	share-net NAME A.B.C.D E.F.G.H <LEASE>	命令share-net NAME A.B.C.D E.F.G.H <LEASE>用于向DHCP子网中增加地址池。A.B.C.D和E.F.G.H分别是该地址池的开始地址和结束地址。可选项<LEASE>为该地址池的租期。地址池的租期意味客户端不是无限时长占用该IP地址，在租期将到前客户端必须对已占用的IP地址续租。租期的设置视情况而定，一般在地址紧张的情况下可设定较短的租期如两小时。如果地址池充分，可以考虑分配客户端长达数星期的地址租期
步骤4	end	返回特权模式

12.2.4 配置DHCP 网关地址

DHCP 网关地址是 DHCP 服务器分配给客户端的默认网关，如果不配置 DHCP 网关地址，客户端的默认网关将是 0.0.0.0

配置 DHCP 网关地址的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	dhcp	进入DHCP配置模式
步骤3	share-net NAME router A.B.C.D	命令share-net NAME router A.B.C.D 用于配置DHCP服务器分配给客户端的默认网关地址，A.B.C.D是将要分配的默认网关
步骤4	end	返回特权模式


注意

客户端可能不接受 DHCP 服务器分配的网关地址

12.2.5 配置DHCP DNS服务器地址

DHCP DNS 服务器地址是分配给客户端的 DNS 地址。客户端在分配到有效的 DNS 地址后才能通过 DNS 服务器正确解析 IP 地址。

配置 DHCP DNS 服务器地址的步骤:

步骤1	configure terminal	进入全局配置模式
步骤2	dhcp	进入DHCP配置模式
步骤3	share-net NAME dns A.B.C.D <A.B.C.D>	命令share-net NAME dns A.B.C.D <A.B.C.D>用于配置DHCP服务器分配给客户端的DNS域名服务器地址，A.B.C.D是将要分配的主DNS地址，第二个可选项<A.B.C.D>是将要分配的辅DNS地址
步骤4	end	返回特权模式


注意

客户端可能不接受 DHCP 服务器分配的 DNS 地址

12.2.6 配置DHCP WINS 服务器地址

DHCP WINS 服务器地址是分配给客户端的 WINS 地址。客户端在分配到有效的 WINS 地址后才能通过 WINS 服务器正确解析 IP 地址。

配置 DHCP WINS 服务器地址的步骤:

步骤1	configure terminal	进入全局配置模式
步骤2	dhcp	进入DHCP配置模式
步骤3	share-net NAME wins A.B.C.D	命令share-net NAME wins A.B.C.D 用于配置DHCP服务器分配给客户端的Windows域名解析服务器地址，Windows域名解析仅用于联网的windows机器解析windows域名
步骤4	end	返回特权模式


注意

客户端可能不接受 DHCP 服务器分配的 Windows 域名解析服务器地址

12.3 地址分配信息显示命令

表12-1 显示 DHCP 分配 IP 的信息:

执行命令	说明
show dhcp-ip	显示已分配IP信息
show dhcp-ip active	显示活动IP详细信息
show dhcp-ip sumary	显示分配IP统计信息

12.3.2 show dhcp-ip

显示 DHCP 服务器分配的 IP 地址信息，步骤如下：

查看步骤：

步骤1	显示DHCP服务器分配的IP地址信息
	SmartHammer# show dhcp-ip 192.168.0.10 00:20:ed:a7:06:cc 192.168.0.25 00:10:dc:0e:63:84 192.168.1.253 00:0d:56:4f:a9:c8 192.168.3.253 00:01:02:28:af:32 192.168.4.251 00:10:dc:df:e0:9b 192.168.4.253 50:78:4c:66:be:b0 192.168.4.254 00:10:5c:b3:9c:25 192.168.5.252 00:0b:db:65:3f:51 192.168.5.253 00:20:ed:a8:a8:25 192.168.5.254 00:0b:db:53:91:61 Total: 10

12.3.3 show dhcp-ip active

显示 DHCP 服务器分配的 IP 地址信息，并且包含客户端主机名及地址的租期信息等。例如：

查看步骤：

步骤1	显示DHCP服务器分配的IP地址信息，并且包含客户端主机名及地址的租期信息等
	SmartHammer# show dhcp-ip active host name : "ac-server" ip address : 192.168.0.10 MAC : 00:20:ed:a7:06:cc lease starts : Friday, April 23, 2004 10:10:45 lease ends : Friday, April 23, 2004 11:10:45

12.3.4 show dhcp-ip summary

显示 DHCP 服务器分配 IP 的统计信息，例如：

查看步骤：

步骤1	显示DHCP服务器分配IP的统计信息

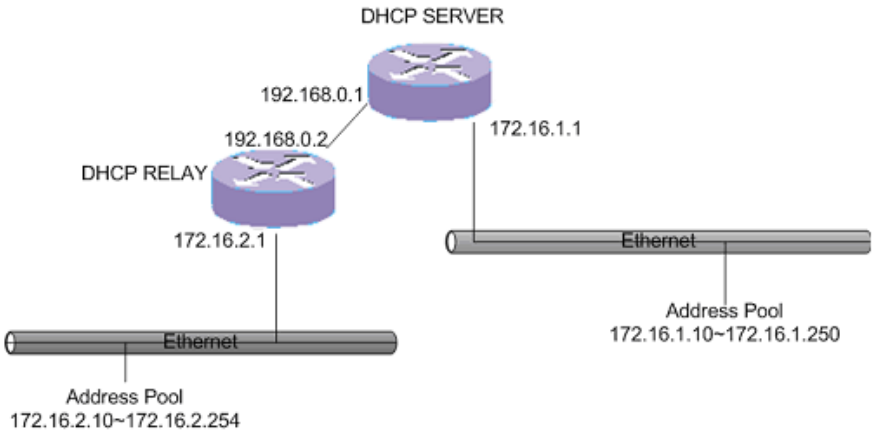
```
SmartHammer# show dhcp-ip  summary
General Statistics
    Active IP          :  10
    Abandoned IP       :  0
    Expired Leases     :  0
Usage by Network :
    Network          Netmask          Active  Abandoned  Expired
  11.1.1.0     255.255.255.128          0          0          0
  12.1.0.0     255.255.252.0            0          0          0
  127.0.0.0        255.0.0.0            0          0          0
  13.1.1.0     255.255.255.248          0          0          0
  149.1.0.0        255.255.0.0          0          0          0
  172.16.0.0       255.255.0.0          0          0          0
  192.168.0.0      255.255.0.0          10         0          0
```

12.4 配置案例

案例描述：

配置设备（DHCP Server）给两个子网分配 IP 地址，如下图所示，172.16.1.0/16 为直接相连的子网，172.16.2.0/16 为通过另一台 SmartHammer 防火墙（DHCP Relay）后的子网。

图12-1 DHCP 服务配置案例组网图



配置步骤：

步骤**1**	配置图中DHCP SERVER所在的设备上接口IP地址
	Router(config) interface ge0 Router(config-if) ip address 192.168.0.1/24 Router(config-if) exit Router(config) interface ge1 Router(config-if) ip address 172.16.1.1/24 Router(config) exit Router(config) ip route 172.16.2.0/24 192.168.0.2 Router(config) exit
步骤**2**	配DHCP相关参数
	Router(config)dhcp Router(config-dhcp)share-net ge1 subnet 172.16.1.0/24 Router(config-dhcp)share-net ge1 router 172.16.1.1 Router(config-dhcp)share-net ge1 dns 202.99.16.1 Router(config-dhcp)share-net ge1 172.16.1.10 172.16.1.250 7200 Router(config-dhcp)share-net ge0 subnet 192.168.0.1/24 Router(config-dhcp)share-net ForRelay subnet 172.16.2.0/24 Router(config-dhcp)share-net ForRelay 172.16.2.10 172.16.2.254 86400 Router(config-dhcp)exit

:

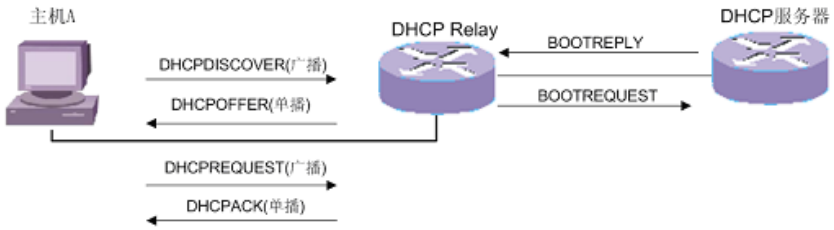
注意	对于给 DHCP RELAY 分配 IP 地址的情况，share-net ge0 subnet 192.168.0.1/24 是必不可少的指令，它指定了在 192.168.0.1/24 的相应接口上启动 DHCP 服务。

13 配置 DHCP Relay

13.1 DHCP Relay概述

DHCP Relay 是用来将一个网段的 DHCP 请求转发给其它网段的 DHCP Server，由其它网段的 DHCP Server 分配 IP 地址。DHCP Relay 存在的原因是因为 DHCP 客户端还没有 IP 环境设定，这时由 DHCP Relay 来接管客户的 DHCP 请求然后将 DHCP 消息传递给 DHCP Server，再将 DHCP 服务器的应答消息传给客户端，客户端获得 IP 地址。当然也可以在每一个网段之中安装 DHCP Server 但这样的话设备成本会增加而且管理上面也比较分散。DHCP Relay 的工作原理如下图所示：

图13-1 DHCP 客户端通过 Relay 从 DHCP 服务器申请 IP 地址



13.2 配置DHCP Relay

配置 DHCP Relay 只需要指定 DHCP 服务器的地址。

13.2.1 配置DHCP 服务器的IP地址

配置 DHCP 服务器的 IP 地址的步骤：

步骤**1**	configure terminal	进入全局配置模式

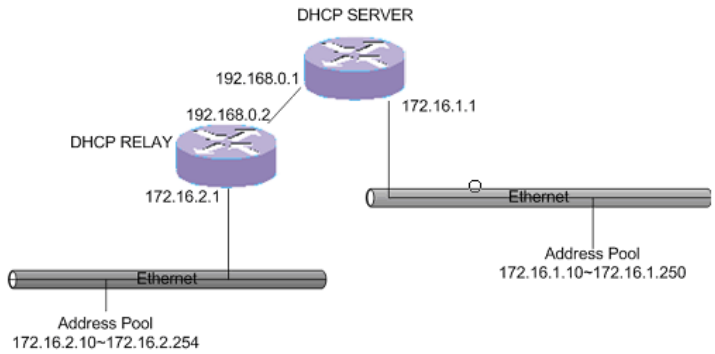
步骤2	dhcp	进入dhcp模式配置模式
步骤3	relay A.B.C.D <A.B.C.D>	配置DHCP Relay服务器IP地址使用命令relay A.B.C.D <A.B.C.D> <A.B.C.D>为可选的第二个DHCP服务器IP地址
步骤4	end	返回特权模式

13.3 配置案例

案例描述

配置 SmartHammer 防火墙（DHCP RELAY）从 DHCP SERVER（192.168.0.1）给客户端分配 IP 地址，如下图所示：

图13-2 DHCP Relay 配置案例组网图



配置步骤：

步骤1	Router(config) interface ge0 Router(config-if) ip address 192.168.0.2/24 Router(config-if) exit Router(config) interface ge1 Router(config-if) 172.16.2.1/24 Router(config) exit	配接口IP地址
步骤2	Router(config) ip route 0.0.0.0/0 192.168.0.1 Router(config) exit	配置静态路由
步骤3	Router(config)#dhcp Router(config-dhcp)#relay 192.168.0.1 Router(config-dhcp)#exit	配DHCP相关参数

13.4 常见故障

13.4.1 客户端无法获得IP地址

故障现象	DHCP Relay转发了DHCP客户端的BOOTREQUEST消息，客户端仍然无法获得IP地址。
分析与解决	查看DHCP服务器是不是配置相应的IP地址池，如果DHCP服务器没配置地址池或配置了错误的地址池，客户端将得不到IP地址。 查看DHCP服务器有没到到达DHCP Relay的路由，如果没有，DHCP Relay将收不到DHCP服务器的应答的消息

14 配置 VRRP

14.1 VRRP协议概述

Virtual Router Redundancy Protocol(VRRP)，虚拟路由器冗余协议，被设计运行于具有多播能力的局域网中，给局域网中的主机提供网关备份功能。

使用 VRRP 可以将局域网中的多个路由设备配置为互相之间作路由备份的虚拟路由器组，该组中的所有路由器采用 VRRP 协议来实现路由器之间以及路由器与所在局域网之间的镜像。如果一台路由器出现故障，其它的路由器会自动代替失效的路由器绕过故障点重新路由，路由的恢复时间仅在数秒之内，且此过程对于终端系统是透明的。

VRRP 路由器有两种状态：主路由器和备份路由器。VRRP 在路由器组中根据一定规则选出一台作为主路由器，负责转发数据包。其他路由器则作为备份路由器。主路由器通过定时发送 VRRP 通告包来与其他备份路由器通信，以保证备份路由器及时了解主路由器的状态。正常情况下，备份路由器不处理发往虚拟路由器的数据包。当主路由器发生故障时，备份路由器在一定的时间内没有收到主路由器发送的 VRRP 通告包，就会迅速转换成主路由器，接管主路由器的工作，从而将对路由转发功能的影响减到最小。这样就提供了在故障发生时快速、有效的解决方法。

VRRP 协议只有一种报文：通告报文。它封装在 IP 分组中，使用 IP 协议号 112。该报文为多播报文，使用多播地址 224.0.0.18 在局域网内广播。

14.2 配置VRRP虚拟路由器

SmartHammer 支持 VRRP 协议，在 SmartHammer 设备中，VRRP 虚拟路由器的参数包括：虚拟 IP 地址、优先级、通告时间、认证方式，以及是否使用抢占模式等。用户可以配置多个 VRRP 虚拟路由器，每个接口上也可以启用多个 VRRP 虚拟路由器。

SmartHammer 设备中的 VRRP 不支持虚拟 MAC，虚拟路由器使用工作接口的真实 MAC。这样并不影响 VRRP 的功能，而且可以避免所连接的交换设备中的 FDB

表频繁更新。

14.2.1 缺省配置

表14-1 VRRP 虚拟路由器的缺省设置

内容	缺省设置	备注
通告时间间隔（advertise-time）	1秒	可更改设置
优先级 （priority）	100	可更改设置
抢占模式 （preempt-mode）	不启用	可更改设置
认证方式 （authentication）	不认证	可更改设置

14.2.2 创建VRRP虚拟路由器

在配置 VRRP 虚拟路由器之前，首先需要在配置模式下创建一个 VRRP 虚拟路由器。

创建虚拟路由器的步骤:

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	vrrp-router NUM	创建一个ID为NUM的VRRP虚拟路由器，虚拟路由器的ID可以配置为1到255之间。
步骤**3**	write terminal	显示配置

14.2.3 配置IP地址

虚拟路由器的 IP 地址没有默认值，必须由用户配置，而且虚拟路由器的 IP 地址和工作接口必须在同一子网段内。例如：虚拟路由器要在地址为 10.1.0.1/24 的接口上启用，则虚拟路由器 IP 地址必须为 10.1.0.x。每个虚拟路由器可以配置多个 IP 地址。如果配置的虚拟路由器 IP 地址与工作接口的 IP 地址相同，则该虚拟路由器成为 IP 地址所有者。

配置虚拟路由器 IP 地址的步骤:

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	vrrp-router NUM	配置ID为NUM的VRRP虚拟路由器，如果不存在该虚拟路由器，则创建该虚拟路由器。
步骤**3**	ip address A.B.C.D	配置虚拟路由器的IP地址
步骤**4**	write terminal	显示配置


注意

必须配置至少一个 IP 地址，否则虚拟路由器无法启动。如果该虚拟路由器已经启用，则不能修改它的虚拟 IP。不同路由设备上配置的同一组的 VRRP 虚拟路由器虚拟 IP 必须相同。不同组的 VRRP 虚拟路由器虚拟 IP 不能相同，而且除了 IP 地址所有者与接口地址相同以外，虚拟 IP 不能与该网段内的其它地址重复。

14.2.4 配置优先级

虚拟路由器的优先级用于选举主路由器。在虚拟路由器组中，优先级最高的被选举为主路由器，其它的为备份路由器。备份路由器的优先级可以配置为 1-254。优先级 255 为虚拟 IP 地址所有者保留，不能配置。默认的优先级为 100。

配置虚拟路由器优先级的步骤

步骤1	configure terminal	进入全局配置模式
步骤2	vrrp-router NUM	配置ID为NUM的VRRP虚拟路由器，如果不存在该虚拟路由器，则创建该虚拟路由器。
步骤3	priority <1-254>	配置VRRP路由器的优先级
步骤4	write terminal	显示配置

14.2.5 配置通告时间间隔

虚拟路由器中的主路由器每隔一段时间要发送通告报文，通知备份路由器自己的状态。如果备份路由器在三个间隔时间收不到通告报文，将重新进行路由器选举，选出新的主路由器。默认的通告时间间隔为 1 秒。

配置虚拟路由器通告时间间隔的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	vrrp-router NUM	配置ID为NUM的VRRP虚拟路由器，如果不存在该虚拟路由器，则创建该虚拟路由器。
步骤3	advertise-time <1-10>	配置虚拟路由器的通告时间间隔
步骤4	write terminal	显示配置


注意

不同路由设备上配置的同一组的 VRRP 虚拟路由器通告时间必须相同。

14.2.6 配置抢占模式

如果设置了抢占模式，则优先级高的备份路由器可以抢占主路由器。但是如果主路由器是 IP 地址所有者，则不能被抢占。默认不使用抢占模式。

配置虚拟路由器抢占模式的步骤:

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	vrrp-router NUM	配置ID为NUM的VRRP虚拟路由器，如果不存在该虚拟路由器，则创建该虚拟路由器。
步骤**3**	preempt-mode	配置虚拟路由器使用强制模式
步骤**4**	write terminal	显示配置

14.2.7 配置认证方式

为了保证安全性，VRRP 路由器可以对收到的每个 VRRP 报文进行认证，检测报文的合法性。可以使用的认证方法有两种：一种是明文密码认证，相当于 pap 认证；另一种是 IP 头认证，相当于 IPSEC 使用的 AH 认证。默认不使用认证。

认证方式是基于接口的，所以该命令在接口上配置。

配置虚拟路由器认证方式的步骤:

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	interface IFNAME	进入相应接口配置模式
步骤**3**	ip vrrp authentication (pap|ah) password WORD	配置该接口上VRRP虚拟路由器的认证方式和认证密码。
步骤**4**	write terminal	显示配置


注意

如果该接口上已经启用了虚拟路由器，则不能修改认证方式。

14.3 在接口启动VRRP虚拟路由器

配置完 VRRP 虚拟路由器之后，可以在接口启动它。使用 no ip vrrp router NUM 命令可以在接口上禁用 VRRP 虚拟路由器。

在接口上启动虚拟路由器的步骤:

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入相应接口配置模式
步骤3	ip vrrp router NUM	在接口上启用ID为NUM的VRRP虚拟路由器
步骤4	write terminal	显示配置

14.4 VRRP管理命令

表14-2 VRRP 配置管理命令列表

命令	解释
show vrrp router [NUM]	显示配置的VRRP虚拟路由器信息，NUM用于指定要显示的虚拟路由器的ID
show vrrp state	显示启用的VRRP虚拟路由器的运行状态
show vrrp interface	显示启用虚拟路由器的接口信息
show memory vrrp	显示VRRP模块使用的内存信息

14.5 配置案例

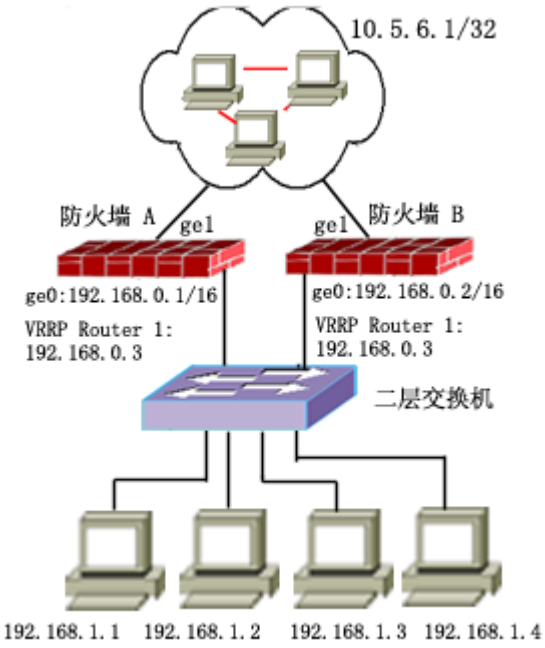
14.5.1 虚拟网关备份

案例描述

防火墙 A 和防火墙 B 的接口 ge0 上启用一个 VRRP 虚拟路由器，ID 为 1。这样防火墙 A 和防火墙 B 的接口 ge0 可以相互备份。

防火墙 A 接口 ge0 的 IP 地址是 192.168.0.1/16，防火墙 B 接口 ge0 的 IP 地址是 192.168.0.2/16。VRRP 虚拟路由器 1 的虚拟 IP 为 192.168.0.3。局域网中的主机都将默认网关设为 VRRP 虚拟路由器 1 的虚拟 IP 地址 192.168.0.3。

图14-1 虚拟网关备份案例组网图



配置防火墙 A:

步骤**1**	在防火墙A中配置VRRP虚拟路由器1。
	SmartHammer# configure terminal SmartHammer(config)# vrrp-router 1 SmartHammer(config-vrrp)# ip address 192.168.0.3 SmartHammer(config-vrrp)# advertise-time 1 SmartHammer(config-vrrp)# preempt-mode SmartHammer(config-vrrp)# priority 200
步骤**2**	在接口ge0上配置该接口上的所有VRRP虚拟路由器使用PAP认证方式，认证密码为123。然后启用VRRP虚拟路由器1。
	SmartHammer# configure terminal SmartHammer(config)# interface ge0 SmartHammer(config-if)# ip vrrp authentication pap password 123 SmartHammer(config-if)# ip vrrp router 1

配置防火墙 B:

步骤**1**	在防火墙B中配置VRRP虚拟路由器1。
	SmartHammer# configure terminal SmartHammer(config)# vrrp-router 1 SmartHammer(config-vrrp)# ip address 192.168.0.3 SmartHammer(config-vrrp)# advertise-time 1 SmartHammer(config-vrrp)# preempt-mode

	SmartHammer(config-vrrp)# priority 100
步骤2	在接口ge0上配置该接口上的所有VRRP虚拟路由器使用PAP认证方式，认证密码为123。然后启用VRRP虚拟路由器1。
	SmartHammer# configure terminal SmartHammer(config)# interface ge0 SmartHammer(config-if)# ip vrrp authentication pap password 123 SmartHammer(config-if)# ip vrrp router 1

在上述两个防火墙上启用 VRRP 虚拟路由器 1 之后，由于防火墙 A 的优先级 200 比防火墙 B 的优先级 100 高，所以防火墙 A 成为主路由器，对目标地址为虚拟 IP 的分组执行路由转发功能。而防火墙 B 成为备份路由器，不转发目标地址为虚拟 IP 的分组。如果防火墙 A 的接口 ge0 down 掉，那么防火墙 B 将转换为主路由器，它的接口 ge0 接替防火墙 A 的接口 ge0，对目标地址为虚拟 IP 的分组执行路由转发功能。

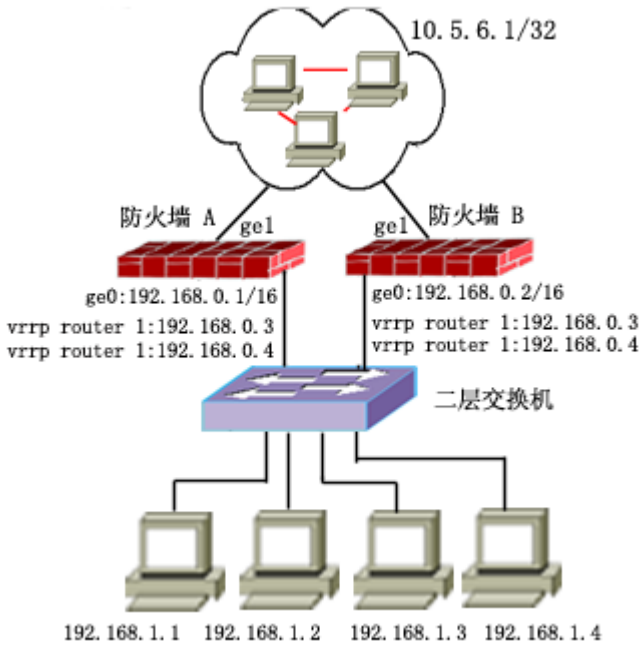
14.5.2 负载均衡

案例描述

防火墙 A 和防火墙 B 的接口 ge0 上同时启用 VRRP 虚拟路由器 1 和 VRRP 虚拟路由器 2。这样防火墙 A 和防火墙 B 的接口 ge0 可以相互备份，而且可以实现负载均衡。

防火墙 A 接口 ge0 的 IP 地址是 192.168.0.1/16，防火墙 B 接口 ge0 的 IP 地址是 192.168.0.2/16。VRRP 虚拟路由器 1 的虚拟 IP 为 192.168.0.3。VRRP 虚拟路由器 2 的虚拟 IP 为 192.168.0.4。局域网中的一部分主机将默认网关设为 VRRP 虚拟路由器 1 的虚拟 IP 地址 192.168.0.3，另一部分主机将默认网关设为 VRRP 虚拟路由器 2 的虚拟 IP 地址 192.168.0.4。

图14-2 通过 VRRP 实现负载均衡案例组网图



配置防火墙 A：

步骤**1**	在防火墙A中，配置VRRP虚拟路由器1
	SmartHammer# configure terminal SmartHammer(config)# vrrp-router 1 SmartHammer(config-vrrp)# ip address 192.168.0.3 SmartHammer(config-vrrp)# advertise-time 1 SmartHammer(config-vrrp)# preempt-mode SmartHammer(config-vrrp)# priority 200
步骤**2**	在防火墙A中配置VRRP虚拟路由器2
	SmartHammer# configure terminal SmartHammer(config)# vrrp-router 2 SmartHammer(config-vrrp)# ip address 192.168.0.4 SmartHammer(config-vrrp)# advertise-time 1 SmartHammer(config-vrrp)# preempt-mode SmartHammer(config-vrrp)# priority 100
步骤**3**	在接口ge0上启用VRRP虚拟路由器1和2
	SmartHammer# configure terminal SmartHammer(config)# interface ge0 SmartHammer(config-if)# ip vrrp router 1 SmartHammer(config-if)# ip vrrp router 2

配置防火墙 B:

步骤1	在防火墙B中配置VRRP虚拟路由器1
	SmartHammer# configure terminal SmartHammer(config)# vrrp-router 1 SmartHammer(config-vrrp)# ip address 192.168.0.3 SmartHammer(config-vrrp)# advertise-time 1 SmartHammer(config-vrrp)# preempt-mode SmartHammer(config-vrrp)# priority 100
步骤2	在防火墙A中配置VRRP虚拟路由器2
	SmartHammer# configure terminal SmartHammer(config)# vrrp-router 2 SmartHammer(config-vrrp)# ip address 192.168.0.4 SmartHammer(config-vrrp)# advertise-time 1 SmartHammer(config-vrrp)# preempt-mode SmartHammer(config-vrrp)# priority 200
步骤3	在接口ge0上启用VRRP虚拟路由器1和2
	SmartHammer# configure terminal SmartHammer(config)# interface ge0 SmartHammer(config-if)# ip vrrp router 1 SmartHammer(config-if)# ip vrrp router 2

在上述两个防火墙上启用 VRRP 虚拟路由器 1 和 2 之后，由于防火墙 A 上虚拟路由器 1 的优先级 200 比防火墙 B 上虚拟路由器 1 的优先级 100 高，所以防火墙 A 成为虚拟路由器 1 的主路由器，对目标地址为虚拟路由器 1 的虚拟 IP 192.168.0.3 的分组执行路由转发功能。而防火墙 B 上虚拟路由器 2 的优先级 200 比防火墙 A 上虚拟路由器 2 的优先级 100 高，所以防火墙 B 成为虚拟路由器 2 的主路由器，对目标地址为虚拟路由器 2 的虚拟 IP 192.168.0.4 的分组执行路由转发功能。

如果防火墙 A 的接口 ge0 down 掉，那么防火墙 B 将转换为虚拟路由器 1 的主路由器，它的接口 ge0 接替防火墙 A 的接口 ge0，对目标地址为虚拟路由器 1 的虚拟IP 192.168.0.3的分组执行路由转发功能。同时它还是虚拟路由器2的主路由器，对目标地址为虚拟路由器 2 的虚拟 IP 192.168.0.4 的分组执行路由转发功能。

这样防火墙 A 的接口 ge0 和防火墙 B 的接口 ge0 可以互相备份，同时两个接口都可以执行路由转发功能，实现负载均衡。

14.6 故障分析

防火墙 A 和防火墙 B 上都启用了虚拟路由器 1，但是两个都成为了主路由器，没有备份路由器。

故障现象	防火墙 A 和防火墙 B 上都启用了虚拟路由器 1，但是两个都成了主路由器，没有备份路由器。
分析与解决	有可能是以下几种情况导致（可以使用 debug vrrp 查看调试信息） 1．防火墙 A 或者 B 没有收到对方发送的通告包，debug vrrp packet 可以看到是否收到了 vrrp 包，并会显示收到的包是否正确。 2．如果收到了错误的包，请检查防火墙 A 和 B 上配置的认证方式是否相同，通告时间是否相同，虚拟 IP 是否相同。两边的配置除了优先级以外都应该相同。 3．如果没有收到包，请检查接口是否可以 ping 通。

14.7 常用调试功能

14.7.1 debug vrrp state

应用环境：

在启用 vrrp router 时，查看它的状态转换是否正确

调试实例：

```
SmartHammer# debug vrrp state
SmartHammer(config-if)# ip vrrp router 1
<VRRP><DEBUG><Enable vrrp router 1 succeed>
  Vrrp-router 1 enabled succeed!
<VRRP><DEBUG><Vrrp router 1 state : INIT to BACKUP>
SmartHammer (config-if)# <VRRP><DEBUG><Vrrp router 1 state : BACKUP to
MASTER>
```

结果分析：

vrrp router 1 启动成功，而且状态转换正确。

14.7.2 debug vrrp packet

应用环境：

当启用 vrrp router 后，发现它的状态错误时

调试实例：

```
SmartHammer(config-if)# ip vrrp router 1
SmartHammer(config-if)# end
SmartHammer# debug vrrp state
<VRRP><DEBUG><Vrrp router 1 state : BACKUP to MASTER>
SmartHammer# debug vrrp packet
<VRRP><DEBUG><Recv vrrp packet: passwd mismatch!>
<VRRP><DEBUG><Vrrp router 1 send : ADVERTISEMENT>
<VRRP><DEBUG><Vrrp send ARP for 192.168.10.100, mac=00:08:9b:08:6e:a1>
```

结果分析：

由于两边配置的认证密码不一致，vrrp 包认证错误，导致状态转换错误。

15 配置 QoS

本章涉及基于 QoS 功能的配置，内容主要包括：

- QoS 概述
- QoS 在 SmartHammer 上的实现
- QoS 配置

15.1 QoS概述

QoS 为英文 Quality of Service 缩写，即服务质量。简单地说，QoS 能够对穿过设备的数据包进行合理的排队，对其中特定的数据包赋以较高的优先级，从而加速传输的过程，以实现实时交互。

由于每种应用系统对网络的要求有所不同，这使得带宽本身并不能解决网络拥塞的问题。QoS 所追求的传输质量在于：数据包不仅要到达其欲传输的目的地址，而且要保证数据包的顺序性、完整性和实时性。通过 QoS，网络可以按照业务的类型或级别加以区分，并能够依次对各级别进行处理。

15.1.1 QoS的提出

随着 Internet 规模的不断增大，各种各样的网络服务争相涌现，先进的多媒体系统层出不穷。由于实时业务对网络传输时延、延时抖动等特性较为敏感，当网络上有突发性高的 FTP 或者含有图像文件的 HTTP 等业务时，实时业务就会受到很大影响；另一方面，多媒体业务占去了大量的带宽，这样，现有网络要保证的关键业务就难以得到可靠的传输。

解决这些问题的最简单的办法当然是增大带宽，但是这种方法代价高昂，而且带宽也不可能无限增大，所以并不十分可行。这就要求网络管理者对不同的服务区别管理，而不能对所有的数据包一视同仁。于是，各种 QoS 技术应运而生。

15.1.2 QoS的解决方案

IETF 已经建议了很多服务模型和机制，以满足 QoS 的需求。其中比较有名的有：综合业务模型(Int-Serv)，区分业务模型(Diff-serv)，多协议标记交换（MPLS），流量工程和约束路由。

在 SmartHammer 设备上实现了区分业务模型，所以下面介绍一下区分业务模型。

15.1.3 区分业务模型

基本概念

Diff-Serv IETF 组织制订了 IP 网络的 QoS 标准——区分服务(Diff-Serv)，为在 IP 网络上提供服务质量保证奠定了基础。

区分服务区域的主要成员有：核心路由器、边缘路由器。在区分服务中，网络的边缘设备对每个分组进行分类、标记 DS 域，用 DS 域来携带 IP 分组对服务的需求信息。在网络的核心节点上，路由器根据分组头上的 DS 码点（Code Point）选择码点所对应的转发处理。

IP QoS 的业务区分结构使用 IPV4 报头中的业务类型（TOS）字段，并将 8 位 TOS 字段重新命名，作为 DS 字段，其中 6 位可供目前使用，其余 2 位以备将来使用。该字段可以按照预先确定好的规则加以定义，使下行节点通过识别这个字段，获取足够的信息来处理到达输入端口的数据包并将他们正确地转发给下一跳的路由器。这里需要注意的是在 IPV4 网中所定义的 TOS 字段与在 Diff-Serv 中的 DS 字段不同。IPV4 报头中 TOS 字段定义 Diff-Serv 充分考虑了 IP 网络本身灵活，可扩展性强的特点，将复杂的服务质量保证通过 DS 字段转换为先进的单跳行为，从而大大减少了信令的工作。

优先级排列

差分服务提供一种简单粗略的方法对各种服务加以分类。不过用其它方法也可以，目前有两个每跳(PHBs)的标准，其中对两个最有代表性的服务等级(业务类别)作了规定：

快速转发(EF)：有一个单独的码点(DiffServ 值)。EF 可以把延迟和抖动减到最小，因而能提供综合服务质量的最高等级。任何超过服务范围(由本地服务策略决定)的业务都会被删除。

保证转发(AF)：有四个等级，每个等级有三个下降过程(总共有 12 个码点)。超过

AF 范围的业务不会象“业务范围内”的业务那样以尽可能高的概率传送出去。这意味着业务量有可能下降，但不是绝对的。

根据预定策略的标准，PHBs 适用于网络入口的业务。业务在这点加以标记，然后根据这个标记进行路由指向，没有作标记的业务就放到了网络的出口。

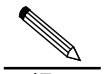
队列调度算法

由于实现 QoS 的基本方法是按照不同优先级入队列，所以为了实现公平性，必然要有先进的队列调度算法来实现公平调度。比较有名的算法有 WRR、DRR、WFQ、RED、WRED 等。

15.1.4 SmartHammer设备对QoS的支持

SmartHammer 设备支持 3 层 QoS，也支持按认证用户保证服务质量。

默认情况下支持根据 Ipv4 头中的 TOS 域进行服务质量保证，也可以设定指定的流进行服务质量保证，算法则采用多级 DRR 算法，在高低优先级间进行 PQ 调度，在同一优先级中进行 DRR 调度。


提示

对于认证用户服务质量保证请参考相关认证章节。并且只支持数据包在出接口时，进行 QoS 处理，在入接口时不支持 QoS 处理，即只支持下行 QoS，不支持上行 QoS。

15.2 配置QoS

15.2.1 配置traffic-map

流量映射和 Acl 进行了有机的结合，在配置 Traffic-map 之前需要先配置 Access-list，用 Access-list 来指定流，然后在 Traffic-map 中对指定的流进行服务质量保证。

在配置 QoS 时，可以指定优先级和速率。

- 优先级值域范围为 0-7，其中 0 代表最高优先级，7 为最低优先级。
- 速率值域范围为 64-102400，单位为 kbit。

配置 Traffic-map 步骤:

步骤1	configure terminal	进入全局配置模式
步骤2	access-list ID permit host A.B.C.D	添加一条access-list，指定流
步骤3	traffic-map MAPNAME	建立Traffic-map模板
步骤4	filter ID priority <0-7> rate <64-102400>	将流的Access-list ID和Traffic-map联系起来，并指明优先级和速率要求
步骤5	end	返回特权模式
步骤6	show run	显示配置


注意

相关的 Access-list 需要先定义，然后才可以用 filter 命令保证服务质量。

15.3 配置案例

15.3.1 对特定流进行速率限制

案例描述

对源 IP 为 192.168.0.20，目的 IP 为 10.1.0.1 的流进行流量限制，并且从高优先级队列输出，速率限制在 1024kbps。

配置步骤:

步骤1	进行流定义
	SmartHammer(config)#access-list 2001 permit ip host 192.168.0.20 host 10.1.0.1
步骤2	定义traffic-map 模板，建立过滤器
	SmartHammer(config)#traffic-map limit SmartHammer(config-traffic-map)#filter 2001 priority 0 rate 1024 SmartHammer(config-traffic-map)#end SmartHammer#write memory

第二部分

AAA 配置

16 配置 AAA 授权功能

本章涉及 SmartHammer 设备 AAA 授权的配置，内容主要包括：

- AAA 授权功能概述
- 配置管理员用户信息
- 配置指令优先级
- 配置登录方式

16.1 AAA授权功能概述

AAA 是 Authentication，Authorization and Accounting（认证、授权和计费）的简称，它把认证、授权和计费这三种安全功能集中起来，作为一个可剪裁的模块，并提供了一个统一的配置框架来进行管理。

我们将 AAA 的授权与认证、计费分开来进行，AAA 的授权主要是指对 SmartHammer 的管理员用户的访问控制，包括：

- 哪些管理员用户可以登录 SmartHammer
- 具有不同访问权限的管理员用户可以得到哪些不同的服务

AAA 授权主要是通过本地验证来确定哪些管理员用户可以被授权使用哪些服务，对用户进行访问控制，使不同的管理员用户具有不同的使用级别。

AAA 授权功能可以对管理员用户授予 16 个级别（0-15），数字越大优先级别越高。

AAA 授权功能可以对指令授予 16 个级别（0-15），数字越大优先级别越高。

当管理员用户的优先级别大于或等于指令的优先级别时，管理员用户可以使用该指令；

当管理员用户的优先级别小于指令的优先级别时，该指令对用户不可见（管理员用户对于这些指令既不能使用，也不能通过 list、?等命令查看到改指令）

AAA 授权功能实现的前提

对于使用 Console 口、SSH 以及 Telnet 登录到 SmartHammer 设备的管理员用户，可以通过配置 line tty 指令选择不同的登录方式（使用用户名和密码登录（login 方式）和只使用密码登录（no login 方式）），**AAA 的授权功能只作用于 login 方式**。

以 login 方式登录的管理员用户，其用户名和密码是通过 SmartHammer 设备的“添加管理员用户”指令添加的，默认的管理员用户的优先级别为最高（15），通过 SmartHammer 设备的“添加管理员用户优先级别”指令可以指定管理员用户的优先级别。

默认的指令的优先级别为最低（0），除少数指令以外（将在本章中详细列出），都可以通过“设置指令优先级别”指令设置指令的优先级。

16.2 配置管理员用户信息

16.2.1 缺省配置

表16-1 SmartHammer 设备管理员用户信息的缺省设置：

内容	缺省设置	备注
用户优先级别	15	可更改设置
指令优先级别	0	
登录方式	no login	

16.2.2 配置管理员用户名和密码

本配置用于在 SmartHammer 设备中添加管理员用户名和密码，添加的管理员用户只能用于用户使用 Console 口、SSH、 Telnet 以及图形化管理界面登录到 SmartHammer 设备，而不能用于 WEB、802.1x 和 PPPoE 等认证方式的本地认证。


注意

在进行用户登录操作前，必须要先设置管理员用户名和密码。

配置管理员用户名和密码的步骤：

步骤**1**	user NAME password PASSWORD admin	添加管理员用户名和密码（Password为明文密码）
步骤**2**	write memory	保存配置

注意

1）请不要使用 user NAME secret SECRET admin 添加管理员用户名和密码。

2）user NAME secret SECRET admin 指令也可以添加管理员用户名和密码，但是我们不推荐您使用本指令添加管理员用户名和密码，原因如下：

本指令主要使用于设备在启动时从配置文件中读取配置；您输入的 SECRET 表示是已加密后的密码，如果您不知道 SECRET 加密前的形式，那么这个用户的密码对于您来说将是未知，您将无法在登录时使用这个用户名和密码。

3）本指令与 AAA 认证与计费功能的添加本地认证用户名指令不同。

4）管理员用户密码永远以加密形式显示，不受 no service password-encryption 命令限制。

5）用户的明文密码必须至少为 4 位。

6）最多只能创建 1024 个管理员用户。

16.2.3 配置管理员用户的优先级别

本配置用于在 SmartHammer 设备中为已添加的管理员用户配置优先级别。

管理员用户的优先级别只作用于 Login 登录方式，并且需要和指令优先级别结合使用。

通过管理员用户优先级别和配置指令优先级别，可以确保不同的管理员用户可以具有不同的配置、管理级别。级别低的管理员用户不可以进行高级别的配置管理工作。

管理员用户优先级从 0 到 15，数字越大，优先级越高。

当登录的管理员用户的优先级大于或等于指令的优先级时，管理员用户可以看见该条指令，并使用该条指令。

当登录的管理员用户的优先级别小于指令的优先级别时，该指令对管理员用户不可见（管理员用户对于这些指令既不能使用，也不能通过 list、?等命令查看到改指令）

配置管理员用户优先级的步骤:

步骤1	user NAME privilege <0-15>	设置管理员用户的优先级，如果不使用本指令，用户默认的优先级为15
步骤2	write memory	保存配置

16.2.4 配置管理员用户登录的地址范围

本配置通过将用户名和 ACL 绑定，用于对 SmartHammer 设备中添加的管理员用户名设置登录的地址范围。

只有在绑定的 ACL 允许 IP 地址范围内的用户可以登录。

配置管理员用户登录地址范围的步骤:

步骤1	user NAME access-class <1-99>	设置管理员用户使用的IP地址范围
步骤2	write memory	保存配置

注意

在您进行用户登录操作前，必须要先设置管理员用户名和密码。

16.2.5 配置管理员密码最大重试次数

当管理员使用正确的用户名和错误的密码登录，输入密码的次数超过我们的限制时，为了防止有人恶意破译密码，可以在一段时间内封禁改用户名，即在这一段时间内，使用该用户名登录，无论密码正确还是错误，用户都无法登录。当超过这段时间后，使用正确的用户名、密码，可以登录。

配置管理员密码最大重试次数的步骤：

步骤1	user try-limit <3-60> block <10-10000000>	当管理员使用同一用户名，输入错误密码N次后，对使用该用户名登录的管理员封禁的时间（秒）。
步骤2	write memory	保存配置

注意

1）管理员用户的优先级别指令只作用于 login 登录方式

2）该指令只对从网络登录的管理员做限制，对从 console 登录的管理员不做限制

16.2.6 配置指令优先级

本配置用于在 SmartHammer 设备中为指令配置优先级别，指令的优先级别只作用于 login 登录方式，指令优先级需要和管理员用户优先级结合使用。

通过配置指令优先级别和管理员用户优先级别，可以确保不同的管理员用户可以具有不同的配置、管理级别。级别低的管理员用户不可以进行高级别的配置管理工作。

指令优先级从 0 到 15，数字越大，优先级越高。

表16-2 SmartHammer 设备中各种指令模式：

模式	提示符	模式
普通模式	>	exec
特权模式	#	privilege
全局配置模式	(config)#	config
以太网接口配置模式	(config-if)#	interface
VLAN配置模式	(config-if)#	vlan
BVI接口配置模式	(config-if)#	bridge
GRE接口配置模式	(config-if)#	gre
PPP模板配置模式	(config-ppp)#	ppp
PPPoE认证模板配置模式	(config-sub)#	pppoe
802.1x认证模板配置模式	(config-sub)#	dot1x
WEB认证模板配置模式	(config-sub)#	web
PORTAL配置模式	(config-portal-server)#	portal
DHCP配置模式	(config-dhcp)#	dhcp
SNMP配置模式	(config-snmp)#	snmp
QoS模板配置模式	(config-traffic-map)#	qos
AAA模板配置模式	(config-aaa)#	aaa
L2TP模板配置模式	(config-l2tp)#	l2tp
IPSEC MAP配置模式	(config-crypto-map)#	ipsec-map
IPSEC 变换集配置模式	(cfg-crypto-trans)#	ipsec-crypto
ISAKMP配置模式	(config-isakmp)#	isakmp
策略路由配置模式	(config-policy-map)#	route-policy
HTTP代理配置模式	(config-http-proxy)#	http-proxy
VRRP模板配置模式	(config-vrrp)#	vrrp

在 SmartHammer 设备中，您可以对大多数指令使用配置指令优先级别，除了以下几条指令以外。

为了保证指令优先级的真正可靠性，以下几条指令优先级别永远为 15，不能改动。

SmartHammer 设备中指令优先级别永远为 15 的指令:

- privilege MODE level LEVEL [COMMAND-STRING]
- privilege MODE reset [COMMAND-STRING]
- line tty
- user NAME privilege LEVEL
- user NAME password PASSWORD [admin]
- user NAME secret SECRET [admin]
- user NAME access-class <1-99>
- user try-limit <3-60> block <30-10000000>
- no user NAME
- no user NAME block
- no user NAME access-class
- no user try-limit
- service password-encryption
- service telnet
- no service password-encryption
- no service telnet
- clear local acct

配置指令优先级的步骤：

步骤**1**	privilege MODE level LEVEL [COMMAND-STRING]	设置指令的优先级为LEVEL
步骤**2**	write memory	保存配置


注意

指令的优先级别指令只作用于 Login 登录方式

16.2.7 配置复原指令优先级

本配置用于在 SmartHammer 设备中复原指令的优先级别为 0，指令的优先级别只作用于 Login 登录方式。

配置复原指令优先级的步骤：

步骤**1**	privilege MODE reset [COMMAND-STRING]	复原指令的优先级为0

步骤2	write memory	保存配置


注意

1）指令的优先级别指令只作用于 login 登录方式

2）优先级小于 15 的用户无法使用表 1-16 中的指令，为了便于您管理，请必须添加一个优先级等于 15 的最高权限用户。

16.2.8 配置登录方式

本配置用于在 SmartHammer 设备中配置登录方式，SmartHammer 设备共有两种登录方式，分别为：

login 登录方式 ：使用用户名和密码登录

no login 登录方式 ：只使用密码登录

用户优先级和指令优先级只作用于 login 登录方式。

配置登录方式的步骤：

步骤1	line tty	进入TTY配置模式
步骤2	login	使用login登录方式
	no login	使用no login登录方式
步骤3	write memory	保存配置


注意

请在配置 login 登录方式后注意使用前面章节介绍的命令添加管理员用户，否则，在您退出后，由于没有管理员用户名和密码，将无法再次登录本设备。

16.3 配置信息显示命令

表16-3 AAA 授权功能配置信息显示命令列表：

命令	解释
show local user	显示当前已添加的本地用户和管理员用户信息
show running-config	显示当前配置，如果存在service password-encryption命令，本地用户名和密码将以user NAME secret SECRET形式显示，否则将以user NAME password PASSWORD形式显示，管理员用户名、密码永远以密文形式显示。

show local user 命令显示举例:

步骤1	show local user命令显示举例:
	SmartHammer # show local user ---------- Name : guest; Password: ******** ---------- Name : admin; Password: ******** admin ---------- Total Users: 2 管理员用户的后面会显示"admin" 可以看到当前的管理员用户为“admin”，有一个本地用户，名称为guest。

16.4 配置案例

16.4.1 配置AAA授权功能

案例描述：

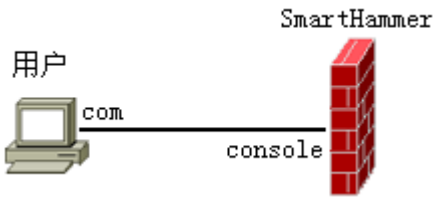
配置 SmartHammer 设备使用 login 登录方式，添加两个管理员用户 guest 和 admin，其中 guest 的优先级为 3，admin 的优先级为 4，设置 exec 模式下 enable 指令的优先级为 4，限制用户 guest 不能进入特权模式。

结果：

用户 guset 无法看见和使用 enable 命令，因此无法进入特权模式；

用户 admin 可以看见和使用 enable 命令，可以进入特权模式

图16-1 配置 AAA 授权功能案例组网图



配置步骤：

步骤1	配置使用login登录方式
	SmartHammer# configure terminal SmartHammer(config)# line tty SmartHammer(config-line)# login SmartHammer(config-line)# exit

	SmartHammer(config)#
步骤2	添加管理员用户
	SmartHammer(config)# user guest password guest admin SmartHammer(config)# user admin password admin admin
步骤3	设置用户优先级
	SmartHammer(config)# user guest privilege 3 SmartHammer(config)# user admin privilege 4
步骤4	设置指令enable的优先级为4
	SmartHammer(config)# privilege exec level 4 enable SmartHammer(config)# exit SmartHammer# exit
步骤5	保存配置
	SmartHammer (config)# write memory

案例达到的效果如下：

图16-2 以 guest 用户登录

```
Login: guest
Password:

        Harbour Networks Limited.
        version G503_1.3_0064
        Build  2004-06-16 at 三 6 月 16 11:21:33 CST 2004.
SmartHammer> enable
% Unknown command.
SmartHammer> list
  exit
  list
  ping WORD
  telnet WORD
  telnet WORD PORT
  traceroute WORD
SmartHammer>
  exit          Exit current mode and down to previous mode
  list          Print command list
  ping          send echo messages
  show          Show running system information
  telnet        Open a telnet connection
  traceroute    Trace route to destination
SmartHammer>
```

以上可以看出，当我们以 guest 用户登录时，指令“enable”对用户不可用，也不能通过 list 命令显示。

图16-3 以 admin 用户登录

```
Login: admin
Password:

        Harbour Networks Limited.
        version G503_1.3_0064
        Build   2004-06-16 at 三 6 月 16 11:21:33 CST 2004.
SmartHammer>
  enable      Turn on privileged mode command
  exit        Exit current mode and down to previous mode
  list        Print command list
  ping        send echo messages
  show        Show running system information
  telnet      Open a telnet connection
  traceroute  Trace route to destination
SmartHammer> list
  enable
  exit
  list
  ping WORD
  telnet WORD
  telnet WORD PORT
  traceroute WORD
SmartHammer> enable
Password:
SmartHammer#
```

以上可以看出，当我们以 admin 用户登录时，指令“enable”对用户可用，这就是配置了指令优先级的明显效果。

16.4.2 限制登录用户IP地址范围功能

案例描述：

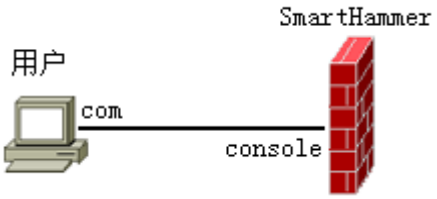
配置 SmartHammer 设备使用 login 登录方式，防火墙 ge0 接口的地址为：192.168.0.1/16，添加管理员用户 admin，限制 admin 用户登录的 IP 只能是 192.168.19.182。

预期目的：

用户 admin 从 192.168.19.182 机器登录，登录成功；

用户 admin 从 192.168.19.182 以外的机器登录，登录失败。

图16-4 案例组网图



配置步骤：

步骤**1**	配置使用login登录方式
	SmartHammer# configure terminal SmartHammer(config)# line tty SmartHammer(config-line)# login SmartHammer(config-line)# exit SmartHammer(config)#
步骤**2**	添加管理员用户
	SmartHammer(config)# user admin password admin admin
步骤**3**	设置用户登录IP地址范围
	SmartHammer(config)# access-list 1 permit 192.168.19.182 SmartHammer(config)# user admin access-class 1
步骤**4**	保存配置
	SmartHammer (config)# write memory

16.5 故障分析

16.5.1 用户无法登录

故障现象	存在该用户，但使用这个用户名无法登录
分析与解决	1）该用户是否是管理员用户 2）是否对该用户名限制登录的IP地址范围 3）是否该用户处于封禁状态，使用no user NAME block给用户解禁 4）用户密码存在问题，请使用user NAME password PASSWORD admin指令重设一遍用户密码。

16.5.2 指令优先级设错

故障现象	本来只想对router ospf指令设置优先级，结果对router rip指令也设置了优先级

分析与解决	您开始使用的指令是privilege config level 5 router，它将对该模式下所有以router开头的多级指令设置优先级；您可以只使用privilege config level 5 router ospf，对router ospf指令设置优先级

16.6 常用调试功能

16.6.1 Debug aaam login

应用环境：用户无法登录设备，在如 7.1 中重新设置完用户名和密码后，用户仍然无法登录。为了在终端显示该调试信息，需要执行命令 terminal monitor。

调试实例：

```
SmartHammer# terminal monitor
SmartHammer# debug aaam login
This admin user [test] does not exist
Admin user [test] from 192.168.1.2 Login Failed
```

结果分析：

由于不存在 test 这个用户，所以用户无法登录 SmartHammer，请在 SmartHammer 上添加该用户，则用户可以登录。


注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug aaam login 命令禁用此功能。

17 配置 AAA 认证和计费功能

本章涉及 SmartHammer 设备 AAA 认证和计费功能的配置，内容主要包括：

- AAA 认证和计费功能概述
- 配置本地认证用户信息
- 配置 AAA 认证功能
- 配置 AAA 计费功能

17.1 AAA认证和计费功能概述

17.1.1 AAA认证和计费功能概述

AAA 是 Authentication，Authorization and Accounting（认证、授权和计费）的简称，它把认证、授权和计费这三种安全功能集中起来，作为一个可剪裁的模块，并提供了一个统一的配置框架来进行管理。AAA 功能可采用 RADIUS 协议来实现。

我们将 AAA 的授权与认证、计费分开来进行，AAA 的认证、计费功能主要包括：

- 哪些用户可以通过我们的接入设备访问网络
- 如何对正在使用网络资源的用户进行计费

AAA 通过下列服务来实现上面提到的安全功能：

- 认证：验证用户是否具有访问权，AAA 提供了多种验证方式，包括本地验证、RADIUS 验证等，可根据需要灵活选用。
- 授权：授权用户可以使用哪些服务，对用户进行访问控制。
- 计费：记录用户使用网络资源的情况，提供结算数据。

AAA 的优点：

- 灵活易控
- 可伸缩
- 标准化的认证方法，如 RADIUS
- 多重备用系统

17.1.2 RADIUS概述

RADIUS 是远程认证拨号用户服务（Remote Authentication Dial-In User Service）的简称，它是一种分布式的客户机/服务器系统，能保护网络不受未授权访问的干扰，可用在既要求高安全性、又要求维持远程用户访问的各种网络环境中（如用来管理使用串口和调制解调器的大量分散拨号用户）。RADIUS 服务器上包含了所有的用户认证和网络服务访问信息。

RADIUS 服务器对用户的认证过程通常需要利用接入服务器等设备的代理认证功能，即在接入设备上运行 RADIUS 客户端，每次用户接入时将用户信息提交给服务器进行认证。通常整个操作步骤如下：

第 1 步：客户端（SmartHammer 设备）将用户名和加密口令发送至 RADIUS 服务器。

第 2 步：从 RADIUS 服务器返回下述响应报文之一：

- ACCEPT：表明用户通过认证。
- REJECT：表明用户没有通过认证，提示用户重新输入用户名和口令，否则访问被拒绝。

17.1.3 SmartHammer设备的AAA认证和计费功能实现

SmartHammer 设备的 AAA 认证和计费功能只涉及配置关于 AAA 认证和计费的参数（地点、认证服务器参数），您必须将其和 Web、PPPoE、802.1x 等接入认证模板结合使用，通过在接入认证模板中设置使用的 AAA 认证和计费模板，才可以正常实现 SmartHammer 设备的认证和计费功能。

在 Web、PPPoE、802.1x 等接入认证模板中配置的与认证、计费有关的信息包括：

- 使用的 AAA 认证和计费模板
- 认证方式
- 间歇计帐间隔

这时您应注意：

- 在同一个 Web、PPPoE、802.1x 等接入认证模板中可以配置使用多个 AAA 认证和计费模板。
- 在同一个 Web、PPPoE、802.1x 等接入认证模板中，您可以对所有用户设定一个 AAA 认证和计费模板，或是针对不同的用户群体（GROUP）设定不同的

AAA 认证和计费模板（将在第 6 部分详细介绍）。

- 在 Web、PPPoE、802.1x 等接入认证模板中以 by GROUP 为后缀使用的 AAA 认证和计费模板表示该 AAA 认证和计费模板只对这个 GROUP 中包括的用户有效。
- 在 Web、PPPoE、802.1x 等接入认证模板中不以 by GROUP 为后缀使用的 AAA 认证和计费模板表示该 AAA 认证和计费模板对所有用户有效。

17.2 配置AAA认证和计费功能

17.2.1 缺省配置

图17-1 SmartHammer 设备关于 AAA 认证和计费参数的缺省设置信息：

内容	缺省设置	备注
认证地点	local	可更改设置
计费地点	none	可更改设置

17.2.2 配置本地认证用户名和密码

本配置用于在 SmartHammer 设备中添加本地认证用户名和密码，添加的本地认证用户也只能用于 WEB、802.1x 和 PPPoE 等认证方式的本地认证，而不能用于用户使用 Console 口、SSH、 Telnet 以及图形化管理界面登录到 SmartHammer 设备。


注意

在您进行本地认证操作前，必须要先设置本地认证用户名和密码。

配置本地认证用户名和密码的步骤：

步骤**1**	user NAME password PASSWORD	添加本地认证用户名和密码（PASSWORD 为明文密码）
步骤**2**	write memory	保存配置

注意事项：

- 请不要使用 user NAME secret SECRET 添加本地认证用户名和密码。

- user NAME secret SECRET 指令也可以添加本地认证用户名和密码，但是我们不推荐您使用本指令添加本地认证用户名和密码，原因如下：
- 本指令主要使用于设备在启动时从配置文件中读取配置；您输入的 SECRET 表示是已加密后的密码，如果您不知道 SECRET 加密前的形式，那么这个用户的密码对于您来说将是未知，您将无法在本地认证时使用这个用户名和密码。
- 本指令与 AAA 授权功能的添加管理员用户名指令不同。
- 本地认证用户名不能用于使用 Console 口、SSH、Telnet 以及图形化管理界面登录到 SmartHammer 设备的登录用户。
- 最多只能创建 8192 个本地认证用户。

17.2.3 配置使用本地认证

SmartHammer 设备的 AAA 认证功能可以使用两种认证地点：

- 本地认证：

在无法使用 Radius 服务器时可以使用本地认证，本地认证的用户名和密码是通过上节的的“配置本地用户名和密码”添加到 SmartHammer 设备设备上。

- Radius 认证服务器认证

配置使用本地认证的步骤:

步骤**1**	aaa NAME	进入名为NAME的AAA模板，如果不存在该模板，则创建模板
步骤**2**	authentication local	配置接入用户使用本地认证

在取消某个 AAA 模板前，请先在接入认证模板中取消对这个 AAA 模板的使用，否则您无法取消该模板。

17.2.4 配置使用RADIUS服务器认证

SmartHammer 设备的 AAA 认证功能可以使用两种认证地点：

- 本地认证
- Radius 认证服务器认证：

配置接入用户使用 Radius 认证服务器认证时，请确保在您的网络中有 SmartHammer 设备可达的 Radius 认证服务器。

SmartHammer 设备可以实现多认证服务器功能，可以避免在只使用一台 Radius 认证服务器时，出现的由于该服务器故障导致用户无法认证通过的问题。在 SmartHammer 设备上配置多个 Radius 认证服务器参数，这几台 Radius 认证服务器应具有完全相同的用户名、密码信息，当其中某台 Radius 认证服务器出现故障时，SmartHammer 设备还可以向其他 Radius 认证服务器进行认证。接入用户的用户名、密码信息是保存在 Radius 认证服务器上。

配置使用 Radius 服务器认证的步骤:

步骤1	aaa NAME	进入名为NAME的AAA模板，如果不存在该模板，则创建模板
步骤2	authentication server A.B.C.D <1-10000> SECRETS	配置使用的Radius认证服务器的地址、端口、共享密钥
步骤3	source-ip A.B.C.D	配置使用Radius认证时NAS地址

注意事项:

- 在取消某个 AAA 模板前，请先在接入认证模板中取消对这个 AAA 模板的使用。否则您无法取消该模板。
- 您在配置使用 Radius 认证时必须要配置 NAS 地址，否则 SmartHammer 设备无法向 Radius 认证服务器发送认证信息。
- 您配置的 NAS 地址必须是 SmartHammer 设备上与 Radius 服务器相连的那个接口的 IP 地址，否则 SmartHammer 设备无法向 Radius 认证服务器发送认证信息。
- 在同一个接入认证模板下，如果一个用户名可以匹配到的一个使用本地认证的 AAA 模板，则对该接入用户采用本地认证，不考虑该接入用户可以匹配的其他 AAA 模板。
- 在同一个接入认证模板下，如果一个用户名可以匹配到多个使用 Radius 服务器认证的 AAA 模板（没有匹配到任何使用本地认证的 AAA 模板），则对该接入用户采用 Radius 服务器认证，向匹配到的所有的 AAA 模板中的 Radius 认证服务器发送认证请求。

17.2.5 配置不计费

SmartHammer 设备的 AAA 计费功能可以使用三种计费方式：

- 不计费：

使用不计费方式，用户认证通过后（不论采用本地认证还是 Radius 服务器认证），

将无法查到用户的计费信息。

- 本地计费
- Radius 计费服务器计费

配置使用不计费的步骤：

步骤1	aaa NAME	进入名为NAME的AAA模板，如果不存在该模板，则创建模板。
步骤2	accounting none	配置对接入用户不计费


注意

在取消某个 AAA 模板前，请先在接入认证模板中取消对这个 AAA 模板的使用。否则您无法取消该模板。

17.2.6 配置使用本地计费

SmartHammer 设备的 AAA 计费功能可以使用三种计费方式：

- 不计费
- 本地计费：

使用本地计费，接入用户的计费信息将保存在 SmartHammer 设备上，SmartHammer 设备只保存最新的 1000 条计费信息，在 SmartHammer 设备重启后将不保存重启前所有的本地计费信息。

- Radius 计费服务器计费

配置对接入用户使用本地计费方式，您可以在 SmartHammer 设备上使用以下命令查看本地计费信息或者把本地计费信息备份到其他机器上。

查看本地记费信息

您可以在该接入用户下线后使用：

show local acct

查看用户的本地计费信息。

保存本地记费信息

由于 SmartHammer 设备只保存最新的 1000 条本地计费信息，您可以通过

copy local_accounting ftp://A.B.C.D/FILENAME

或

copy local_accounting tftp://A.B.C.D/FILENAME

将本地计费信息备份到别的机器上。

配置使用本地计费的步骤：

步骤1	aaa NAME	进入名为NAME的AAA模板，如果不存在该模板，则创建模板
步骤2	accounting local	配置接入用户使用本地计费


注意

1)在取消某个 AAA 模板前，请现在接入认证模板中取消对这个 AAA 模板的使用。否则您无法取消该模板。

2)在 SmartHammer 设备重启后，您将不能够通过 *show local acct* 查看到重启前的本地计费信息。

17.2.7 配置使用RADIUS服务器计费

SmartHammer 设备的 AAA 计费功能可以使用三种计费方式：

- 不计费
- 本地计费
- Radius 计费服务器计费：

SmartHammer 设备可以实现计费服务器备份功能，可以避免在只使用一台 Radius 计费服务器时，出现的由于该服务器故障导致用户计费信息无法保存的问题。在 SmartHammer 设备上配置多个 Radius 计费服务器参数，SmartHammer 设备会向所有的 Radius 计费服务器发送计费信息。

接入用户的计费信息将被保存在 Radius 计费服务器上。

配置使用 Radius 服务器计费的步骤：

步骤1	aaa NAME	进入名为NAME的AAA模板，如果不存在该模板，则创建模板
步骤2	accounting server A.B.C.D <1-10000> SECRETS	配置使用的Radius计费服务器的地址、端口、共享密钥
步骤3	source-ip A.B.C.D	配置使用Radius计费时NAS地址

注意事项：

- 取消某个 AAA 模板前，请先在接入认证模板中取消对这个 AAA 模板的使用。否则您无法取消该模板。
- 您在配置使用 Radius 计费时必须要配置 NAS 地址，否则 SmartHammer 设备

无法向 Radius 计费服务器发送计费信息。

- 您配置的 NAS 地址必须是 SmartHammer 设备上与 Radius 服务器相连的那个接口的 IP 地址，否则 SmartHammer 设备无法向 Radius 认证服务器发送认证信息。
- 在同一个接入认证模板下，如果一个用户名可以匹配到多个使用 Radius 服务器计费的 AAA 模板，则对该接入用户采用 Radius 服务器计费，向匹配到的所有的 AAA 模板中的 Radius 计费服务器发送计费请求信息。
- 在同一个接入认证模板下，如果一个用户名可以匹配到多种计费方式（不计费、本地计费、Radius 服务器计费）的 AAA 模板，则对该接入用户采用所有它可以匹配到的计费方式。

17.3 配置信息显示命令

表17-1 AAA 认证和计费功能配置信息显示命令列表：

命令	解释
show local acct	显示本地计费信息
show running-config	显示当前配置

配置步骤：

步骤**1** show local acct命令显示举例

```
SmartHammer# show local acct
=============================================================
===
Name            IPAddress          MAC                      On-Time
Bytes-in   Bytes-out
-------------------------------------------------------------------
SmartHammer1    192.168.0.191   00:05:3a:ef:5d:ec   65784
67804526    23670432
-------------------------------------------------------------------
SmartHammer2    192.168.19.182 00:10:4c:5a:bc:ed   4678
1354423         651492
```

17.4 配置案例

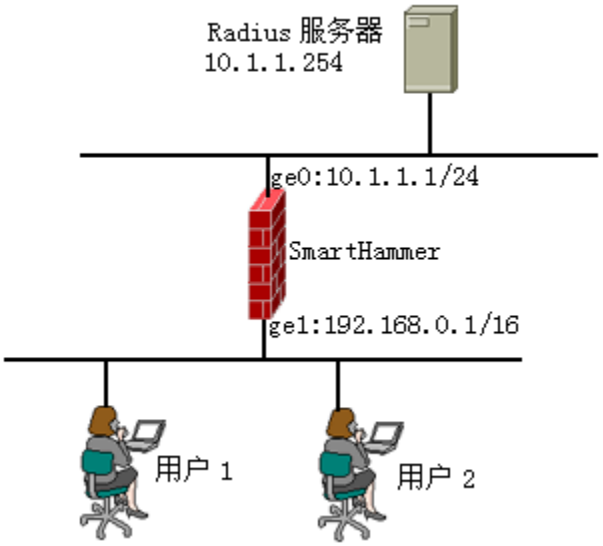
17.4.1 所有用户属于同一个ISP

案例描述：

在 SmartHammer 设备的 ge1 接口（192.168.0.1）上启动 Web 认证，使用 Radius 服务器认证和计费。

使用 SmartHammer 设备进行认证的用户同属于一个 ISP，他们都使用相同的 Radius 认证和计费服务器，Radius 服务器（10.1.1.254）与 SmartHammer 设备的 ge0 接口相连。

图17-2 所有用户属于同一个 ISP 案例组网图



配置步骤：

步骤**1**	配置AAA认证和计费模板
	SmartHammer# configure terminal SmartHammer (config)# aaa web SmartHammer (config-aaa)# authentication server 10.1.1.254 1812 88--99 SmartHammer (config-aaa)# accounting server 10.1.1.254 1813 88--99 SmartHammer (config-aaa)# source-ip 10.1.1.1 SmartHammer (config-aaa)# exit
步骤**2**	配置Web认证模板和Portal模板

	SmartHammer (config)# subscriber-template webauth hammer SmartHammer (config-sub)# aaa-group web SmartHammer (config-sub)# dns-server 10.1.1.2 SmartHammer (config-sub)# accounting-interval 120 SmartHammer (config-sub)# authentication-url http://192.168.0.1/ SmartHammer (config-sub)# exit SmartHammer (config)# portal-server SmartHammer (config-portal-server)# keep-alive 120 SmartHammer (config-portal-server)# authentification chap SmartHammer (config-sub)# exit
步骤3	在接口上启用Web认证
	SmartHammer (config)# interface ge0 SmartHammer (config-if)# ip address 10.1.1.1/24 SmartHammer (config-if)# exit SmartHammer (config)# interface ge1 SmartHammer (config-if)# ip address 192.168.0.1/16 SmartHammer (config-if)# webauth subscriber-template hammer SmartHammer (config-if)# exit

17.4.2 多ISP支持

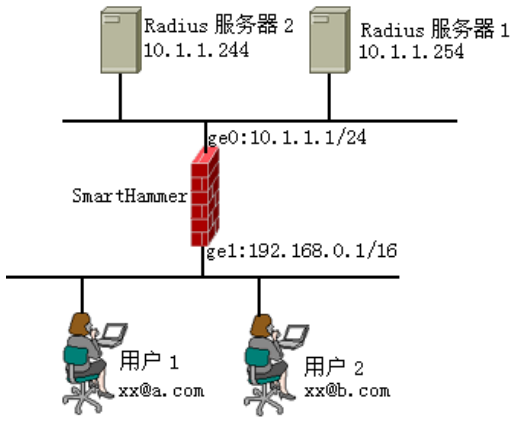
案例描述：

在 SmartHammer 设备的 ge1 接口（192.168.0.1）上启动 Web 认证，使用 Radius 服务器认证和计费。

使用 SmartHammer 设备进行认证的用户分属于两个不同的 ISP，属于 ISP1 的用户的用户名以“@a.com”为结尾，他们使用 Radius 服务器 1（10.1.1.254）；属于 ISP2 的用户的用户名以“@b.com”为结尾，，他们使用 Radius 服务器 2（10.1.1.244）。

这两个 Radius 服务器与 SmartHammer 设备的 ge0 接口相连。

图17-3 多 ISP 支持案例组网图



配置步骤：

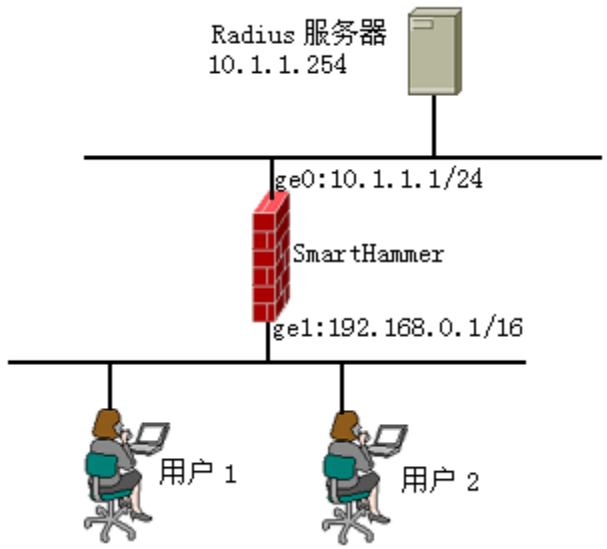
步骤**1**	配置两个AAA认证和计费模板
	SmartHammer# configure terminal SmartHammer (config)# aaa web1 SmartHammer (config-aaa)# authentication server 10.1.1.254 1812 88--99 SmartHammer (config-aaa)# accounting server 10.1.1.254 1813 88--99 SmartHammer (config-aaa)# source-ip 10.1.1.1 SmartHammer (config-aaa)# exit SmartHammer (config)# aaa web2 SmartHammer (config-aaa)# authentication server 10.1.1.244 1812 88--99 SmartHammer (config-aaa)# accounting server 10.1.1.244 1813 88--99 SmartHammer (config-aaa)# source-ip 10.1.1.1 SmartHammer (config-aaa)# exit
步骤**2**	配置Web认证模板和Portal模板
	SmartHammer (config)# subscriber-template webauth hammer SmartHammer (config-sub)# aaa-group web1 by @a.com$ SmartHammer (config-sub)# aaa-group web2 by @b.com$ SmartHammer (config-sub)# dns-server 10.1.1.2 SmartHammer (config-sub)# accounting-interval 120 SmartHammer (config-sub)# authentication-url http://192.168.0.1/ SmartHammer (config-sub)# exit SmartHammer (config)# portal-server SmartHammer (config-portal-server)# keep-alive 120 SmartHammer (config-portal-server)# authentification chap SmartHammer (config-sub)# exit
步骤**3**	在接口上启用Web认证

```
SmartHammer (config)# interface ge0
SmartHammer (config-if)# ip address 10.1.1.1/24
SmartHammer (config-if)# exit
SmartHammer (config)# interface ge1
SmartHammer (config-if)# ip address 192.168.0.1/16
SmartHammer (config-if)# webauth subscriber-template hammer
SmartHammer (config-if)# exit
```

17.4.3 本地认证 + Radius服务器计费

在 SmartHammer 设备的 ge1 接口（192.168.0.1）上启动 Web 认证，使用本地认证和 Radius 服务器计费。Radius 服务器（10.1.1.254）与 SmartHammer 设备的 ge0 接口相连。

图17-4 本地认证 + Radius 服务器计费案例组网图



配置步骤：

步骤**1**	配置AAA认证和计费模板
	SmartHammer# configure terminal SmartHammer (config)# aaa web SmartHammer (config-aaa)# authentication local SmartHammer (config-aaa)# accounting server 10.1.1.254 1813 88--99 SmartHammer (config-aaa)# source-ip 10.1.1.1 SmartHammer (config-aaa)# exit
步骤**2**	配置Web认证模板和Portal模板

	SmartHammer (config)# subscriber-template webauth hammer SmartHammer (config-sub)# aaa-group web SmartHammer (config-sub)# dns-server 10.1.1.2 SmartHammer (config-sub)# accounting-interval 120 SmartHammer (config-sub)# authentication-url http://192.168.0.1 SmartHammer (config-sub)# exit SmartHammer (config)# portal-server SmartHammer (config-portal-server)# keep-alive 120 SmartHammer (config-portal-server)# authentification chap SmartHammer (config-sub)# exit
步骤3	添加本地用户
	SmartHammer (config)# user hammer password hammer
步骤4	在接口上启用Web认证
	SmartHammer (config)# interface ge0 SmartHammer (config-if)# ip address 10.1.1.1/24 SmartHammer (config-if)# exit SmartHammer (config)# interface ge1 SmartHammer (config-if)# ip address 192.168.0.1/16 SmartHammer (config-if)# webauth subscriber-template hammer SmartHammer (config-if)# exit

17.5 故障分析

17.5.1 用户无法认证成功

故障现象	使用本地认证，用户无法认证成功
分析与解决	确认已添加该本地用户，并且密码正确

故障现象	使用Radius服务器认证，用户无法认证成功，Radius服务器没有收到认证请求报文
分析与解决	请确认 1）用户是否能匹配到使用本地认证的 AAA 模板 2）SmartHammer 设备是否可达 Radius 认证服务器 3)是否在 SmartHammer 设备的 AAA 模板上配置了正确的 Radius 认证服务器参数（服务器地址、端口、共享密钥） 4）是否在SmartHammer设备的AAA模板上配置了正确的NAS地址

故障现象	使用Radius服务器认证，用户无法认证成功，Radius服务器没有返回任何认证应答报文
分析与解决	请确认 1）在 Radius 认证服务器上 Radius 认证服务是否已启动 2）是否在 Radius 认证服务器上配置了正确的 NAS 地址 3)是否在 SmartHammer 设备的 AAA 模板上配置了正确的 Radius 认证服务器参数（服务器地址、端口、共享密钥） 4）是否在SmartHammer设备的AAA模板上配置了正确的NAS地址

故障现象	使用Radius服务器认证，用户无法认证成功，Radius服务器返回REJECT（认证失败）报文
分析与解决	请确认 1）在 Radius 认证服务器上配置了正确的 NAS 地址 2）SmartHammer 设备的 AAA 模板上配置了共享密钥匙否与 Radius 认证服务器上配置的相同 3）是否在SmartHammer设备的AAA模板上配置了正确的NAS地址

故障现象	使用Radius服务器认证，用户无法认证成功，Radius服务器返回REJECT（认证失败）报文
分析与解决	请确认 1）SmartHammer设备的AAA模板上配置了共享密钥匙否与Radius认证服务器上配置的相同 2）用户是否可以匹配到多个AAA模板，请确保这多个AAA模板所对应的Radius认证服务器上的用户和密码完全一致，否则可能导致这些Radius认证服务器返回不同的认证结果，从而导致接入用户无法正常上线

17.5.2 用户使用Radius服务器计费不成功

故障现象	使用Radius服务器认证，用户无法计费成功，Radius服务器没有收到计费请求报文
分析与解决	请确认 1）SmartHammer 设备是否可达 Radius 计费服务器 2)是否在 SmartHammer 设备的 AAA 模板上配置了正确的 Radius 计费服务器参数（服务器地址、端口、共享密钥） 3）是否在SmartHammer设备的AAA模板上配置了正确的NAS地址

故障现象	使用Radius服务器认证，用户无法计费成功，Radius服务器没有返回计费应答报文
分析与解决	请确认 1）在 Radius 计费服务器上，Radius 计费服务是否已启动 2）是否在 Radius 计费服务器上配置了正确的 NAS 地址 3)是否在 SmartHammer 设备的 AAA 模板上配置了正确的 Radius 计费服务器参数（服务器地址、端口、共享密钥） 4）是否在SmartHammer设备的AAA模板上配置了正确的NAS地址

17.6 常用调试功能

17.6.1 debug (dot1x |pppoe| webauth) auth

应用环境：

当用户无法认证成功时。 为了在终端显示该调试信息，需要执行命令 terminal monitor

调试实例：

```
SmartHammer# terminal monitor
SmartHammer# debug dot1x auth
No response to retry sending auth RADIUS packet
```

结果分析：

显示从 Radius 计费服务器没有返回应答信息。

这时您需要确认：

- SmartHammer 设备是否可达 Radius 认证服务器
- 在 Radius 认证服务器上 Radius 认证服务是否已启动
- 是否在 Radius 认证服务器上配置了正确的 NAS 地址
- 是否在 SmartHammer 设备的 AAA 模板上配置了正确的 Radius 认证服务器参数（服务器地址、端口、共享密钥）

是否在 SmartHammer 设备的 AAA 模板上配置了正确的 NAS 地址


注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug (dot1x |pppoe| webauth) auth 命令禁用此功能。

17.6.2 debug (dot1x |pppoe| webauth) acct

应用环境：

当用户无法计费成功时，或者您配置了使用间歇计费后用户能够认证通过，但上线后不久异常下线。为了在终端显示该调试信息，需要执行命令 terminal monitor。

调试实例：

```
SmartHammer# terminal monitor
SmartHammer# debug dot1x acct
No response to retry sending acct start or intrim RADIUS packet
```

结果分析：

显示从 Radius 认证服务器没有返回应答信息。

这时您需要确认：

- SmartHammer 设备是否可达 Radius 计费服务器
- 在 Radius 计费服务器上 Radius 计费服务是否已启动
- 是否在 Radius 计费服务器上配置了正确的 NAS 地址
- 是否在 SmartHammer 设备的 AAA 模板上配置了正确的 Radius 计费服务器参数（服务器地址、端口、共享密钥）
- 是否在 SmartHammer 设备的 AAA 模板上配置了正确的 NAS 地址


注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug (dot1x |pppoe| webauth) acct 命令禁用此功能。

第三部分

防火墙配置

18 配置 ACL

ACL 即 Access-list，主要为访问控制提供包过滤条件，另外也为带宽管理、入侵检测、应用代理等提供过滤规则，找出满足条件的数据包。ACL 本身并不直接起作用，必须与其它指令结合使用。

18.1 ACL概述

ACL 相当于过滤规则，找出满足条件的数据包，ACL 根据 listid 主要分为以下几类：

<1-99>：标准 ACL，只能使用源 IP 进行过滤；

<100-199>：扩展 ACL，提供基于源 IP 和目标 IP 的过滤；

<200-299>：链路层 ACL，提供基于链路层协议和 MAC 地址的过滤；

<700-799>：链路层 ACL，提供基于 MAC 地址的过滤；

<1300-1999>：标准 ACL，提供基于源 IP 以及源端口的过滤；

<2000-2699>：扩展 ACL，提供基于源地址、目标地址、源端口和目标端口的过滤；

<2700-2999>：扩展 ACL，提供基于源地址、目标地址、tcp、udp 端口的过滤。

18.2 配置ACL功能

18.2.1 缺省配置

表18-1 ACL 的缺省设置信息：

内容	缺省设置	备注
ACL预编译（access-list Num compiled）	off	可更改设置

18.2.2 配置ACL并进行预编译

ACL 本身并不直接起作用，可与其它指令结合使用。ACL 是有顺序的，在已有的 ACL 中增加新的规则时只能在最后进行追加，不能插入，可以一次性删除整个链表，也可删除其中的一条规则。

配置 ACL 的步骤:

步骤**1**	configure terminate	进入配置模式
步骤**2**	access-list NUM (drop|permit) ……	配置一条ACL规则，可使用类似的命令在同一个ACL中添加多条规则
步骤**3**	access-list Num compiled	对ACL进行预编译（规则少的时候没有必要进行预编译）
步骤**4**	Show ip access-list [Num]	显示指定的ACL或显示所有ACL


注意

1)Access-list 指令中的 permit/drop 参数在包过滤功能中表示对匹配成功的数据包的具体处理动作，而在其它功能（traffic-map 等）中被忽略，不执行相关动作，规则只是用来对数据包进行匹配。

2)规则中的掩码与网络掩码正好相反，0 表示对应的位要严格匹配，1 表示对应的位不进行匹配，例如匹配 172.168.1.0/24 网段的所有 IP 地址，则表示为：172.168.1.0 0.0.0.255，即前面 24 位要匹配，后面 8 位不匹配，什么都行。

18.3 配置信息显示命令

表18-2 ACL 配置信息显示命令列表：

命令	解释
show ip access-list	显示所有ACL的配置内容
show ip access-list Num	显示指定ACL的配置内容
show ip access-list compiled	显示所有ACL的预编译信息
show ip access-list LISTNUM compiled	显示指定ACL的预编译信息

18.4 配置案例

18.4.1 配置标准ACL

案例描述：

配置标准 ACL，仅对源地址进行匹配。先添加一条规则，匹配源地址为 172.168.0.1/24 网段的数据包，再添加一条规则，匹配源地址为 172.16.1.1 的主机。

配置步骤：

步骤1	进入配置模式
	SmartHammer#configure terminal
步骤2	配置ACL规则，ACL名称为1
	SmartHammer(config)#access-list 1 permit 172.168.0.0 0.0.0.255 SmartHammer(config)#access-list 1 permit 172.16.1.1
步骤3	退出配置模式，显示配置的ACL
	SmartHammer(config)#exit SmartHammer#show ip access-list 1

18.4.2 配置扩展ACL，加入大量规则，并进行预编译

案例描述：

- 配置扩展 ACL，对源地址、目标地址、协议端口等进行匹配。
- 添加一条规则，匹配协议为 TCP、源地址为 172.168.0.0/24 网段、目标地址为 200.1.0.0/16、目标端口为 80 的数据包；
- 添加另一条规则，匹配协议为 UDP、源地址为任意地址、目标地址为 200.1.0.0/16、目标端口为 53 的数据包；
- 添加另外 1000 条规则。
- 对 ACL 进行预编译。

配置步骤：

步骤1	进入配置模式
	SmartHammer#configure terminal
步骤2	配置ACL规则，ACL名称为1

	SmartHammer(config)#access-list 2700 permit tcp 172.168.0.0 0.0.0.255 200.1.0.0 0.0.255.255 eq 80 SmartHammer(config)#access-list 2700 permit udp any 200.1.0.0 0.0.255.255 eq 53
步骤3	对ACL进行预编译
	SmartHammer(config)#access-list 2700 compiled
步骤4	退出配置模式，显示配置的ACL
	SmartHammer(config)#exit SmartHammer#show ip access-list 2700

18.4.3 配置链路层ACL

案例描述：

配置一条 Access-list 的规则，禁止 MAC 为 00:01:02:03:04:05 的 ARP 请求数据包，配置另一条 Access-list 的规则，禁止 MAC 为 00:01:02:03:04:06 的所有类型数据包。

配置步骤：

步骤1	进入配置模式
	SmartHammer#configure terminal
步骤2	配置ACL规则，ACL名称为200
	SmartHammer (config)# access-list 200 deny 0x0806 0x0000 0001.0203.0405 0.0.0
步骤3	配置ACL规则，ACL名称为700
	SmartHammer (config)# access-list 700 deny 0001.0203.0406 0.0.0
步骤4	退出配置模式，显示配置的ACL
	SmartHammer(config)#exit SmartHammer#show ip access-list 200 SmartHammer#show ip access-list 700

18.5 故障分析

18.5.1 输入的ACL指令与显示的不一致

故障现象	输入的ACL指令与显示的不一致，如输入： access-list 1 permit 172.168.1.1 0.0.255.255， 显示却为： access-list 1 permit 172.168.0.0 0.0.255.255, 源IP地址的后16位发生了变化
分析与解决	正常现象，由于后16位不进行匹配，所以自动将其置0。

	对于如下两条规则，系统认为是相同的两条规则，只添加一条： access-list 1 permit 172.168.1.1 0.0.255.255， access-list 1 permit 172.168.2.1 0.0.255.255， 这是正常现象。

19 配置自适应安全过滤

自适应安全过滤是基于状态的包过滤功能，它根据数据包进出接口的安全域和安全级别自动确定数据包的缺省处理策略。自适应安全过滤不仅能控制途经设备的数据，而且对设备本身也起保护作用。

19.1 自适应安全过滤概述

自适应安全过滤基于安全域，在缺省情况下，每个接口所连接的网络都有一个特定的安全域设定，设备本身也有一个安全域设定。每个安全域可以设置一个安全级别，当自适应安全过滤功能启用后，系统会自动根据数据包进出接口的安全域和安全级别数据访问特性来确定数据包的缺省处理策略。有了自适应安全过滤，通过最简单的配置就可以使各个安全域受到有效的安全保护，也可以方便的对应用同一安全域的接口进行统一管理。

19.2 配置自适应安全过滤

19.2.1 缺省配置

表19-1 自适应安全过滤的出厂设置信息：

内容	缺省设置	备注
ge接口设置接口安全域（ip security－policy）	general	可更改设置
设置本地安全域（local ip sercurity－policy）	general	可更改设置
启用自适应安全过滤（ip service adaptive）	on	可更改设置

19.2.2 配置自适应安全过滤

使用安全域过滤包含三方面的内容：

- 接口安全域，在接口上应用特定的安全域设定，根据安全域的安全级别和

access-list 设定执行数据包过滤。

各安全域对应保护功能如下表表示：

表19-2 安全域对应防护功能

安全域	防护功能
普通级安全域	具有ip inspect功能
限制级安全域	具有ip inspect功能和包过滤功能，相当于外网
控制级安全域	具有ip inspect功能和包过滤功能，相对于DMZ
保护级安全域	具有ip inspect功能和包过滤功能，相对于内网
隔离级安全域	完全隔离

在未有匹配的 access-list 时其访问策略如下表所示：

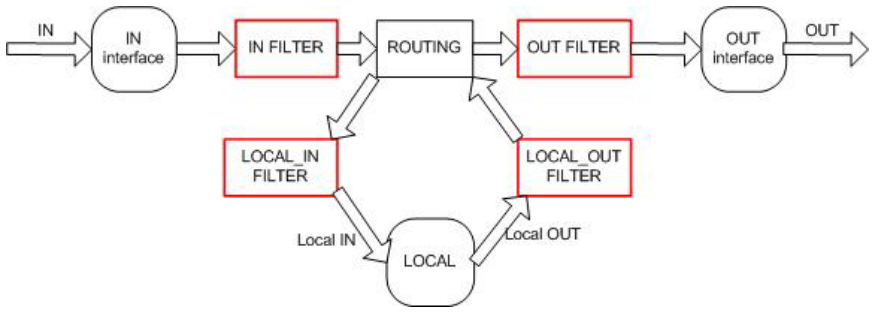
表19-3 安全域访问策略

离开 / 进入	普通级	限制级	控制级	保护级	隔离级
普通级安全域	√	×	×	×	×
限制级安全域 (10-39)	√	★	×	×	×
控制级安全域 (40-69)	√	√	★	×	×
保护级安全域 (70-99)	√	√	√	★	×
隔离级安全域	×	×	×	×	×

√表示可访问，×表示不可访问，★表示根据安全级别确定。

- ip access-list 过滤。在安全域设定了 access-list 之后应用此安全域的接口首先根据此 access-list 决定数据访问策略。access-list 的控制点如下：

图19-1 Access-list 的控制点



- 状态检测，对于已建和相关连接的数据包允许通过，这个判断是在所有

Access-list 过滤之前进行。

数据报文先经过状态检测，然后通过 ACL。若 ACL 中没有匹配的设置则再通过安全域及安全级别的过滤。

数据报文先经过状态检测，然后通过 ACL。若 ACL 中没有匹配的设置则再通过安全域及安全级别的过滤。

自适应安全过滤功能出厂时缺省设置为启用，所有 ge 接口设置接口安全域**普通级**，通过 Ip security-policy 指令调整接口的安全域，可以改变缺省策略。在取消接口上的安全级别设置后，接口启用默认安全域为普通级安全域。

设备本身也具有安全域，可以把设备本身也看作一个接口设备。访问设备的数据包与进入接口和设备本身的安全级别有关，设备对外访问的数据包与设备本身和离开接口的安全级别有关。设备本身的安全级别可以通过指令 local ip security-policy 进行设置，出厂设置为**普通级**。

配置自适应安全过滤。首先应根据具体需求生成用户自定义的安全域，当然也可以使用系统设定的安全域，但系统设定的安全域没有加载 ACL 且不能被修改。内网的安全域应在保护级范围内，DMZ 的安全域应在控制级范围内，外网应在限制级范围内。之后应该设置一些合适的 ACL 并将其加载到特定的用户自定义安全域中，这样所有应用此安全域的接口都将共享此设置。当修改安全域设置时，所有应用此安全域的接口都将相应改变安全策略。

配置自适应安全过滤的步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	security-policy (restricted| controlled| protected) NAME	新建用户自定义的安全域，若使用内置安全域则可以不设置
步骤**3**	Ip security_level ……	修改安全级别，不同安全域取值范围不同
步骤**4**	ip access-group num (in|out)	配置ACL过滤，辅助过滤
步骤**5**	exit	退出security-policy模式
步骤**6**	……	设定不同应用范围的安全域，重复步骤2－5
步骤**7**	interface NAME	进入inetface模式
步骤**8**	ip security-policy (general| restricted| controlled| protected| isolated| NAME)	配置接口的安全域
步骤**9**	exit	退出interface模式
步骤**10**	……	针对不同interface，重复步骤7－9
步骤**11**	local ip security-policy (general| restricted| controlled| protected| isolated| NAME)	配置本地安全域
步骤**12**	access-list Num (permit|drop) ……	添加ACL过滤规则
步骤**13**	access-list Num compiled	如规则太多，进行预编译
步骤**14**	exit	退出configure模式
步骤**15**	show ip access-list (Num)	显示配置的access-list信息
步骤**16**	show security-policy	显示安全域所有设置
步骤**17**	show running-config	显示当前配置


注意

在没有配置的情况下，设备所有接口都根据其默认的安全域进行数据过滤。启用的 Access-list 本身没有缺省策略。

19.3 配置信息显示命令

表19-4 自适应安全过滤配置信息显示命令列表：

命令	解释
show ip security-policy [Name]	显示安全域相关配置。
Show running-config	显示当前配置
show ip access-list [Num]	显示access-list的信息

show acl interface [IFNAME]	显示接口安全级别以及接口上ACL和NAT启用情况

19.4 配置案例

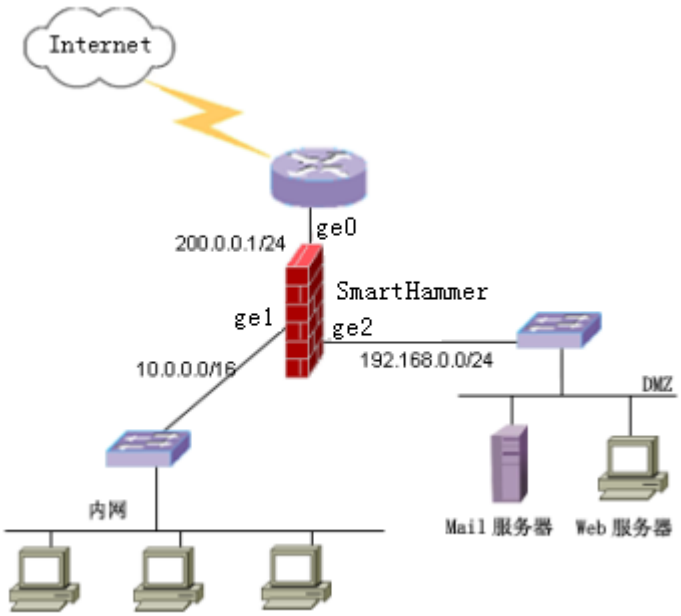
19.4.1 典型的防火墙实施方案

使用系统内置安全域案例描述：

设备按照接口划分为三个安全域，ge0 连接的为外网，ge1 连接的为内网，ge2 连接的为 DMZ 区。

按照实施需求，大的原则是：内网可以访问外网和 DMZ；DMZ 可以访问外网，但不可以访问内网；外网既不可以访问内网，也不可以访问 DMZ。设备本身只允许通过 console 进行配置。

图19-2 典型防火墙实施方案组网图



配置步骤：

步骤**1**	配置各接口安全级别以及设备本身的安全级别，按照实施要求，各安全域安全级别由高到低如下：内网、设备本身、DMZ、外网，因此，将其安全域分别确定为：protected、protected、controlled、restricted
	SmartHammer#configure terminal SmartHammer(config)#interface ge0 SmartHammer(config-if)#ip security-policy restricted SmartHammer(config-if)#exit SmartHammer(config)#interface ge1 SmartHammer(config-if)#ip security-policy protected SmartHammer(config-if)#exit SmartHammer(config)#interface ge2 SmartHammer(config-if)#ip security-policy controlled SmartHammer(config-if)#exit SmartHammer(config)#local ip security-security protected

到目前为止，已经满足的大的实施原则，即内网可以访问外网、DMZ、外网，还有设备本身；DMZ 可以访问外网但不可以访问内网；外网既不可以访问内网也不可以访问 DMZ，现有配置下，内网不可以可以访问设备，如希望访问，则将设备的安全级别调得低于内网即可。需要注意的是，如使用 telnet 在内网对设备进行配置，在设备安全级别调高于内网时，则配置后 telnet 访问会被断开。

使用用户自定义安全域案例描述：

基于以上的基本原则，根据实际应用做以下修改：

DMZ 的部分服务器还需要对外提供服务，因此 DMZ 的部分服务器还需让外网访问。另外还限制内网部分 IP 地址对 DMZ 部分服务器的访问。组网图如上图所示。

配置步骤：

步骤**1**	新建用户自定义安全域，配置各接口安全级别以及设备本身的安全域，按照实施要求，各安全域安全级别由高到低如下：内网、设备本身、DMZ、外网。
	SmartHammer#configure terminal SmartHammer(config)#security-policy restricted net_out SmartHammer(config-security-policy)#exit SmartHammer#configure terminal SmartHammer(config)#security-policy controlled net_DMZ SmartHammer(config-security-policy)#exit SmartHammer#configure terminal SmartHammer(config)#security-policy protected net_local SmartHammer(config-security-policy)#ip security-level 75 SmartHammer(config-security-policy)#exit

SmartHammer#configure terminal
SmartHammer(config)#security-policy protected net_in
SmartHammer(config-security-policy)#exit

SmartHammer#configure terminal
SmartHammer(config)#interface ge0
SmartHammer(config-if)#ip security-policy net_out
SmartHammer(config-if)#exit

SmartHammer(config)#interface ge1
SmartHammer(config-if)#ip security-policy net_in
SmartHammer(config-if)#exit

SmartHammer(config)#interface ge2
SmartHammer(config-if)#ip security-policy net_DMZ
SmartHammer(config-if)#exit

SmartHammer(config)#local ip security-security net_local

到目前为止，已经满足的大的实施原则，即内网可以访问外网、DMZ、外网，还有设备本身；DMZ可以访问外网但不可以访问内网；外网既不可以访问内网也不可以访问DMZ，
现有配置下，内网可以访问设备，如不希望访问，则将设备的安全级别调得高于内网即可。需要注意的是，如使用telnet在内网对设备进行配置，则配置后telnet访问会被断开。

步骤2 允许外网访问DMZ部分服务器

在外网接口ge0引用的安全域net_out上添加ACL过滤规则，允许这些服务器被访问。另外，还需给这些服务器分配公有地址，并做地址映射，这样才能够通过访问一个公有地址，访问到具有私有地址的服务器上，具体地址映射的配置参见NAT部分。

允许web服务器192.168.0.1的80端口被访问
SmartHammer(config)#access-list 2700 permit tcp any 192.168.0.1 eq 80

允许邮件服务器192.168.0.2的25端口被访问
SmartHammer(config)#access-list 2700 permit tcp any 192.168.0.2 eq 25

类似加入其它允许访问的服务器端口

在外网接口ge0引用的安全域net_out上启用access-list 2700
SmartHammer(config)#security-policy restricted net_out
SmartHammer(config-security-policy)#ip access-group 2700 in
SmartHammer(config-security-policy)#exit

步骤3 限制内网部分主机对特定DMZ服务器的访问

SmartHammer(config)#access-list 2701 drop ip 10.0.1.0 0.0.0.255 192.168.0.3
SmartHammer(config)#security-policy restricted net_in
SmartHammer(config-security-policy)#ip access-group 2701 in
SmartHammer(config-security-policy)#exit

19.5 故障分析

19.5.1 配置好自适应安全过滤后 web/portal认证失败

故障现象	停止自适应安全过滤功能，web/portal认证功能正常，但启用了自适应安全过滤后，认证失败
分析与解决	有以下几个可能的原因： 1)设备的8082端口没有被允许访问； 2)portal server的http认证端口没有被允许访问； 3)设备没有被允许访问radius认证服务器的认证端口; 4）用户没有被允许访问dns server的dns服务端口。 解决办法： 设置access-list，允许访问必要的端口。

19.5.2 不能通过telnet继续管理设备

故障现象	调整了安全级别之后，，telnet连接断开，重新连接仍然失败
分析与解决	可能的原因： 调整了安全级别之后，设备本身的安全级别高于访问接口的安全级别，没有显式的添加access-list允许控制主机访问设备，控制主机对telnet服务的访问被禁止，所以连接中断。这属于正常现象。 解决办法： 通过console口进行配置，允许原控制机对设备的telnet访问

19.5.3 入口Ip access-list对PPPOE认证 不能进行有效控制

故障现象	在接口上启用了PPPOE认证，并在此接口上添加access-list，规则不起作用
分析与解决	原因如下： 每个PPPOE连接都建立一个虚拟的设备，通过这个虚拟的设备接入，所以在物理接口上的access-list不起作用。 解决办法： 对于PPPOE认证用户，通过在其出口上设置access-list进行限制

19.5.4 ip access-list对802.1X认证不能进行有效控制

故障现象	ip access-list不能对802.1X认证阶段的报文进行控制
分析与解决	原因如下： 802.1X认证报文属于2层报文，IP层的access-list对其不起作用 解决办法： 在接口上添加ethernet access-group 进行限制； 或者通过取消接口上的802.1X禁止所有用户认证； 或者认证后限制用户对外访问达到控制用户效果。

19.6 常用调试功能

19.6.1 debug acl

应用环境：

启用 ip service adaptive 功能时，数据包的转发结果与预期结果不符，但关闭 ip sevice adaptive 功能时数据包转发结果与预期结果相符，这时可调试安全自适应过滤功能的正确性。为了在终端显示该调试信息，需要执行命令 terminal monitor。

调试实例：

启用ip service adaptive，启用debug acl功能，得到如下debug信息：

```
<FIREWALL><1963-10-25 17:38:06><fw><ACL><DEBUG><action=permit
pos=default in=ge0 src=192.168.19.196 dst=192.168.19.99 len=84 tos=0x00
prec=0x00 ttl=64 id=0 DF proto=ICMP type=8 code=0 id=5380 seq=5159 >
```

结果分析：

从结果可以看出，从 192.168.19.196 访问设备地址 192.168.19.99 的数据包被允许通过，数据包类型为 ICMP，从 ge0 口进来，没有匹配 access-list 规则，缺省策略为允许。

20 配置基于状态的资源控制

本章涉及基于状态的资源和连接控制功能的配置，内容主要包括：

- 基于状态的资源和连接控制功能概述
- 基于状态的资源和连接控制配置

20.1 基于状态的资源控制概述

做为一款防火墙产品，同时需要具备防止攻击和保证正常数据通过的功能。当防火墙遇到大量攻击时，如果所有的连接资源都被攻击所占用，则正常数据就无法通过设备。

基于状态的资源和连接控制基于这样的观点：监视所有连接的状态，如果连接长时间没有应答，一直处于半连接状态，浪费了连接资源；连接已经建立，但长时间没有数据穿过，浪费了连接资源；如果有超出正常范围的大量半连接充斥设备，很可能是受到了半连接攻击；网络上流行某种协议的病毒，它也会占用宝贵的网络资源和连接资源，使正常数据无法通过设备。

基于状态的资源和连接控制可以通过几种方法解决上述问题：监视所有连接的状态，网络管理员可以设置特定协议的半连接老化时间，加速半连接的老化；设定特定协议的连接超时时间，防止资源浪费；监视特定协议的连接状态，当连接正常或不正常断开时，删除连接资源；设定半连接的高低警戒线，当半连接达到高警戒线水平时，删除老的半连接直到低警戒线水平；通过限制特定协议的连接数目，有效防止各种网络病毒。

20.2 配置基于状态的资源控制

20.2.1 缺省配置

表20-1 基于状态的资源和连接控制的缺省设置信息：

内容	缺省设置	备注
ip inspect 服务	disable	可更改设置
系统、TCP、UDP、ICMP和其它协议最大连接数目	655360	可更改设置
系统、TCP、UDP、ICMP和其它协议半连接数目高警戒线(maxincomplete highwatermark)	500	可更改设置
系统、TCP、UDP、ICMP和其它半连接数目低警戒线(maxincomplete lowwatermark)	400	可更改设置
系统、TCP、UDP、ICMP和其它分钟半连接数目高警戒线(one-minute halfopen highwatermark)	500	可更改设置
系统、TCP、UDP、ICMP和其它分钟半连接数目低警戒线(one-minute halfopen lowwatermark)	400	可更改设置
TCP协议建连超时时间(established idletime)	3600秒	可更改设置
UDP协议建连超时时间(established idletime)	30秒	可更改设置
ICMP协议超时时间	10秒	可更改设置
其它协议超时时间	30秒	可更改设置
TCP协议同步发送超时时间(synsent waittime)	20秒	可更改设置
TCP协议同步接收超时时间(synrecv waittime)	10秒	可更改设置
TCP协议finwait超时时间	5秒	可更改设置
TCP协议closewait超时时间	5秒	可更改设置
TCP协议timewait超时时间	5秒	可更改设置
TCP协议closetime超时时间	5秒	可更改设置
UDP协议半连接超时时间	10秒	可更改设置

20.2.2 配置ip inspect服务

根据实际网络情况，可以打开或者关闭 ip inspect 服务。

配置打开 ip inspect 服务的步骤：

步骤**1**	configure terminal	进入全局配置模式

步骤2	ip service inspect	配置系统打开inspect服务
步骤3	end	返回特权模式
步骤4	show ip inspect information	显示inspect配置信息

20.2.3 配置连接数目限制

根据实际网络情况，可以适当增加或减小设备总的连接数目，限制连接资源的使用。适当分配 TCP、UDP、ICMP 和其它协议的连接数目。

配置连接数目限制的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	ip inspect max NUMBER	配置系统允许的最大连接数目
步骤3	ip inspect max NUMBER tcp	配置TCP允许的最大连接数目
步骤4	ip inspect max NUMBER udp	配置UDP允许的最大连接数目
步骤5	ip inspect max NUMBER icmp	配置ICMP允许的最大连接数目
步骤6	ip inspect max NUMBER generic	配置其它允许的最大连接数目
步骤7	end	返回特权模式
步骤8	show ip inspect information	显示inspect配置信息

20.2.4 配置半连接数目限制

根据实际网络情况，可以适当增加或减小设备总的半连接数目，限制连接资源的使用。适当分配 TCP、UDP、ICMP 和其它协议的半连接数目，这种限制比较适用于网络上出现半连接攻击的情况，防止设备资源耗尽。

配置半连接数目限制的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	ip inspect maxincomplete high NUMBER	配置系统半连接数目高警戒线，如果半连接数目达到高警戒线，系统则会删除半连接，直到达到低警戒线，如果NUMBER为-1，则不限制半连接数目
步骤3	ip inspect maxincomplete low NUMBER	配置系统半连接数目低警戒线，如果半连接数目达到高警戒线，系统则会删除半连接，直到达到低警戒线，如果高低警戒线相等，系统则不会再创建连接，直到有连接老化

步骤4	ip inspect maxincomplete high NUMBER tcp	配置TCP半连接数目高警戒线，如果半连接数目达到高警戒线，系统则会删除TCP半连接，直到达到低警戒线，如果NUMBER为-1，则不限制半连接数目
步骤5	ip inspect maxincomplete low NUMBER tcp	配置TCP半连接数目低警戒线，如果半连接数目达到高警戒线，系统则会删除TCP半连接，直到达到低警戒线，如果高低警戒线相等，则不会再创建连接，直到有连接老化
步骤6	ip inspect maxincomplete high NUMBER udp	配置UDP半连接数目高警戒线，如果半连接数目达到高警戒线，系统则会删除UDP半连接，直到达到低警戒线，如果NUMBER为-1，则不限制半连接数目
步骤7	ip inspect maxincomplete low NUMBER udp	配置UDP半连接数目低警戒线，如果半连接数目达到高警戒线，系统则会删除UDP半连接，直到达到低警戒线，如果高低警戒线相等，则不会再创建连接，直到有连接老化
步骤8	ip inspect maxincomplete high NUMBER icmp	配置ICMP半连接数目高警戒线，如果半连接数目达到高警戒线，系统则会删除ICMP半连接，直到达到低警戒线，如果NUMBER为-1，则不限制半连接数目
步骤9	ip inspect maxincomplete low NUMBER icmp	配置ICMP半连接数目低警戒线，如果半连接数目达到高警戒线，系统则会删除ICMP半连接，直到达到低警戒线，如果高低警戒线相等，则不会再创建连接，直到有连接老化
步骤10	ip inspect maxincomplete high NUMBER generic	配置其它协议半连接数目高警戒线，如果半连接数目达到高警戒线，则会删除其它协议半连接，直到达到低警戒线，如果NUMBER为-1，则不限制半连接数目
步骤11	ip inspect maxincomplete low NUMBER generic	配置其它协议半连接数目低警戒线，如果半连接数目达到高警戒线，则会删除其它协议半连接，直到达到低警戒线，如果高低警戒线相等，则不会再创建连接，直到有连接老化
步骤12	end	返回特权模式
步骤13	show ip inspect information	显示inspect配置信息


注意

当系统半连接数目达到高警戒线后，如果高低警戒线相等，则设备则不会创建新连接，直到有连接老化；如果高警戒线大于低警戒线，则会删除半连接，直到达到低警戒线；如果高警戒线为-1，则对半连接不做限制，当然会受连接总数限制。

20.2.5 配置基于ACL的主机连接数限制

根据实际网络情况，可以适当限制一些主机的连接数目，比如：有些主机滥用网络资源，攻击服务器，则可以限制它的连接数目。

配置基于 ACL 的主机连接数限制的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	ip inspect max flow <0-655360> (src|dst|dst-dport) list Access-List	配置主机的最大连接数目，主机或主机的特定端口号由ACL进行匹配

20.3 配置信息显示命令

表20-2 基于状态的资源和连接控制配置信息显示命令列表：

命令	解释
show ip inspect information	显示inspect配置信息
show ip inspect information (tcp|udp|icmp|generic)	显示inspect协议配置信息
show ip inspect information flow	显示inspect基于ACL的流数限制的配置信息
show ip inspect idletime (tcp|udp|icmp|generic)	显示inspect协议超时时间配置
show ip inspect statistics	显示inspect所有统计
show ip inspect statistics (tcp|udp|icmp|generic)	显示inspect协议统计
show ip inspect statistics flow	显示inspect的基于ACL的流数限制的统计信息

20.4 配置案例

20.4.1 限制ICMP协议半连接数目

案例描述：

当网络上出现半连接攻击时，通过 show 命令我们可以看到当前设备上的半连接数目，已经超出平常正常范围，这时我们可以看一下是什么类型的协议，然后通过命令设置对应协议的半连接数目高警戒线和低警戒线，高警戒线最好和低有一些差距，以便使正常数据可以在低和高警戒线间建立连接。

配置步骤：

步骤1	查看半连接统计
	SmartHammer#show ip inspect statistics icmp Protocol icmp summary: Max Count Hwatermark Halftotal Halflist Lwatermark 65536 1038 -1 1038 1038 400
步骤2	限制ICMP半连接数目
	SmartHammer#configure terminal SmartHammer(config)#ip inspect maxicomplete high 500 icmp SmartHammer(config)#exit SmartHammer#show ip inspect statistics icmp Protocol icmp summary: Max Count Hwatermark Halftotal Halflist Lwatermark 65536 426 500 426 426 400
步骤3	保存配置
	SmartHammer#write memory

20.4.2 配置老化时间

如果网络上大量充斥半连接，可以是 UDP 或者 TCP Syn flood 攻击，也可以通过加快老化来减少资源占用。默认 UDP 半连接老化为 10 秒，而 TCP 的 Syn 阶段分为 SynSent 和 SynRecv 分别为 20 秒和 10 秒，SynSent 为设备等待 Server 应答时间，SynRecv 为等待客户端第三次握手时间，则我们可以适当减小老化时间，加快假半连接老化。对于 SynSent 可以不用更改，或者适当加大，因为 Server 可能响应较慢。

配置步骤：

步骤1	查看超时时间设置
	SmartHammer#show ip inspect idletime TCP idletime:3600 UDP idletime:30 ICMP idletime:10 Generic idletime:30
步骤2	设置超时时间
	SmartHammer#configure terminal SmartHammer(config)#ip inspect udp halfopen idletime 5 SmartHammer(config)#ip inspect tcp synrecv-time 5
步骤3	保存配置
	SmartHammer(config)#exit SmartHammer#write memroy

20.4.3 配置基于ACL的主机连接数限制

如果某主机中病毒或者某网段中病毒，疯狂向外发包，可以使用基于 ACL 的主机连接数限制，来限制此主机或此网段的连接数目，有效利用网络资源。

配置步骤：

步骤1	查看网络数据分析结果，确定限制范围
	可以用NetFlow，或者通过主机抓包，得到限制范围
步骤2	设置ACL
	SmartHammer#configure terminal SmartHammer(config)#access-list 88 permit 192.168.1.0 0.0.0.255
步骤3	设置inspect
	SmartHammer(config)#ip inspect max flow 5 src list 88
步骤4	保存配置
	SmartHammer(config)#exit

以上限制 192.168.1.0/24 网段每台主机最多只能有 5 个流穿过设备。

20.4.4 配置基于ACL的主机连接数限制

如果网络上存在大量 syn-flood 攻击报文，为了有效保护防火墙后的 Server，或者 Server 上的特殊服务，可以使用基于 ACL 的目的主机保护或者特定端口保护。

配置实例：

步骤1	查看网络数据分析结果，确定受保护范围
	可以用NetFlow，或者通过主机抓包，得到受保护范围。
步骤2	设置ACL
	SmartHammer#configure terminal SmartHammer(config)#access-list 2100 permit tcp 192.168.1.0 0.0.0.255 192.168.2.1 0.0.0.0 eq http
步骤3	设置inspect
	SmartHammer(config)#ip inspect max flow 3000 dst-dport list 2100
步骤4	保存配置
	SmartHammer(config)#exit SmartHammer#write memory

以上限制 192.168.2.1 服务器最多只能有 3000 个连接。

20.5 故障分析

20.5.1 设备不允许用户远程登录

故障现象	网络管理员无法远程登录设备
分析与解决	分析： 无法远程登录原因有很多，如设备接口 IP 地址没有配置，或者网络管理员使用机器没有路由等。但由于本模块也可能是导致不通原因之一，就是网络管理员错误的设置了半连接或者连接数为 0，这样设备不会建立任何连接。 解决： 通过串口连接到设备上，查看关于连接的设置，如果tcp设置连接或者半连接高警戒线数目为0，则修改成非0数值即可。然后再查看设备总的连接或者半连接高警戒线数目是否为0，如果是则修改成非0即可。

21 配置 NAT

NAT 即网络地址转换，NAT 最初的引入是为了解决公有地址短缺，但后来被证明是一项非常有用的技术，可用于多种用途。NAT 主要用于私用地址向公有地址的转换，解决地址短缺问题，并提供了单向隔离，具有很好的安全特性。NAT 还可用于目标地址的映射，使公有地址可访问配置私有地址的服务器，另外还可用于服务器的负载均衡和地址复用等。正确理解了 NAT 的概念后，NAT 可以具有很多更灵活的应用。

21.1 NAT概述

传统意义上的 NAT 基本上是基于源地址的 NAT，我们称作 source NAT，可细分为 dynamic NAT、PAT 和 static NAT。dynamic NAT 和 PAT 是一种单向的针对源地址的映射，主要用于内网访问外网，减少公有地址的数目，隐藏内部地址。dynamicNAT 指动态的将源地址转换映射到一个相对较小的地址池中，对于同一个源 IP，不同的连接可能映射到地址池中不同的地址；PAT 是指将所有源地址都映射到同一个地址上，通过端口的映射实现不同连接的区分。Static NAT 是一种一对一的双向地址映射，主要用于内部服务器向外提供服务的情况。在这种情况下，内部服务器可以主动访问外部，外部也可以主动访问这台服务器，相当于在内、外网之间建立了一条双向通道。

广义上的 NAT 还包括基于目标地址的 NAT，我们称作 destination NAT，可分为目标地址映射、目标端口映射、服务器负载均衡等。基于目标地址的 NAT 也称为反向 NAT 或地址映射。Destination NAT 是一种单向的针对目标地址的映射，主要用于内部服务器向外部提供服务的情况，它与 static NAT 的区别在于它是单向的。外部可以主动访问内部，内部却不可以主动访问外部。另外，可使用 Destination NAT 实现负载均衡的功能，即可以将一个目标地址转换为多个内部服务器地址。也可以通过端口的映射将不同的端口映射到不同的机器上。

NAT 不仅仅可用于公有地址和私有地址之间的转换，还可用于公有地址与公有地址之间、私有地址与私有地址之间的转换。


注意

NAT 的负载均衡功能只是将一个目标地址均衡转换到不同的内部主机地址上，它并不检测内部主机是否运行正常。它仅仅是一种特殊的地址转换功能，并不是真正意义上的负载均衡。

21.2 配置NAT

配置 NAT 规则，并在特定 interface 上启用。在设置 NAT 规则链之前，首先要明确如下概念：

Source NAT 是在离开接口时进行转换的，Destination NAT 是在进入接口时进行转换的。同一规则链上可同时设置 Static、Source、Destination 三种类型的 NAT，但要保证转换都是在同一个接口上进行的。

每个 interface 上只能启用一条 NAT 规则链。

配置 NAT 的步骤:

步骤**1**	configure terminal	进入配置模式
步骤**2**	ip nat pool POOLNAME A.B.C.D A.B.C.D netmask A.B.C.D	配置一个地址池（可选，配置Dynamic NAT时需要）
步骤**3**	ip nat NAME ……	配置一条NAT规则，可为source NAT，也可为destination NAT
步骤**4**	……	如上配置需要的多条NAT规则
步骤**5**	interface NAME	进入interface模式
步骤**6**	ip nat NAME	在接口上启用NAT
步骤**7**	show running-configure	显示配置

21.3 配置信息显示命令

表21-1 NAT 配置信息显示命令列表：

命令	解释
show ip nat pool	显示地址池的配置信息
show ip nat	显示NAT配置信息
show ip nat translations	显示NAT转换信息
show running-config	显示当前配置

21.4 配置案例

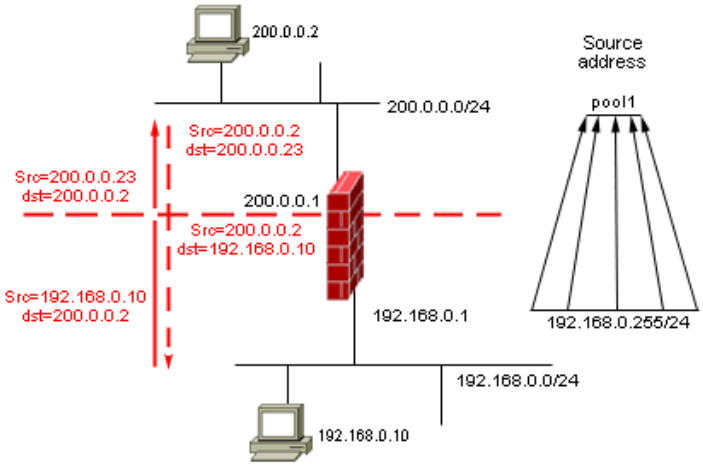
21.4.1 配置动态 NAT和PAT

案例描述：

配置动态 NAT，将源地址 192.168.0.0/24 网段的地址转换为 200.0.0.20 到 200.0.0.40 之间的公有地址池中。

配置 PAT，将源地址为 192.168.1.0/24 网段的地址全部转换为 200.0.0.30。

动态 NAT 和 PAT 配置案例组网图



配置步骤：

步骤1	建立一个ACL，配置动态地址转换前的源地址范围为192.168.0.0/24
	SmartHammer(config)#access-list 1 permit 192.168.0.0 0.0.0.255
步骤2	配置一个地址池，限定动态转换后的源地址范围为200.0.0.20-200.0.0.40
	SmartHammer(config)#ip nat pool pool1 200.0.0.20 200.0.0.40 netmask 255.255.255.0
步骤3	配置一条动态NAT转换规则
	SmartHammer(config)#ip nat test source list 1 pool pool1
步骤4	建立一个ACL，配置转换前的源地址范围为192.168.1.0/24
	SmartHammer(config)#access-list 1 permit 192.168.1.0 0.0.0.255
步骤5	配置一条PAT转换规则
	SmartHammer(config)#ip nat test source list 1 200.0.0.30
步骤6	如需要，在test规则链中配置其它的NAT规则，既可以是动态NAT，也可以是静态NAT，还可以是destnation NAT。
	SmartHammer(config)#ip nat test ……

步骤7	进入interface模式ge0（ge0为直连200.0.0.0/24网段的接口地址），启用NAT规则链，注意：Source NAT在设备出口进行转换，所以要在ge0上启用NAT规则链。
	SmartHammer(config)#interface ge0 SmartHammer(config-if)#ip nat test

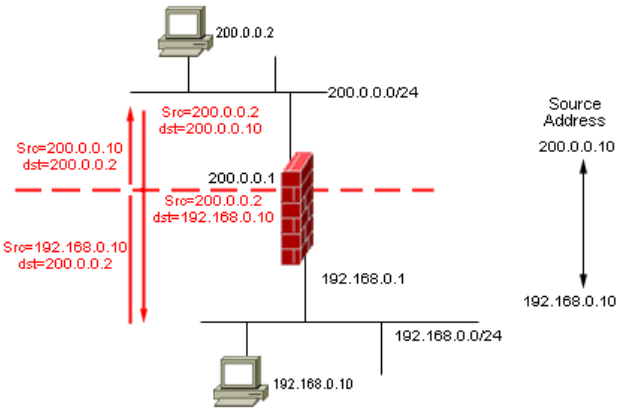
21.4.2 配置静态NAT

案例描述：

配置静态 NAT，将源地址 192.168.0.10 的主机地址转换为 200.0.0.10 的公有地址池中。

案例组网图：

图21-1 配置静态 NAT 案例组网图



配置步骤：

步骤1	配置一条NAT转换规则
	SmartHammer(config)#iip nat test source static 192.168.0.10 200.0.0.10
步骤2	进入interface模式ge0（ge0为直连200.0.0.0/24网段的接口地址），启用NAT规则链，注意：Source NAT在设备出口进行转换，所以要在ge0上启用NAT规则链。
	SmartHammer(config)#interface ge0 SmartHammer(config-if)#ip nat test

21.4.3 配置destination NAT

案例描述：

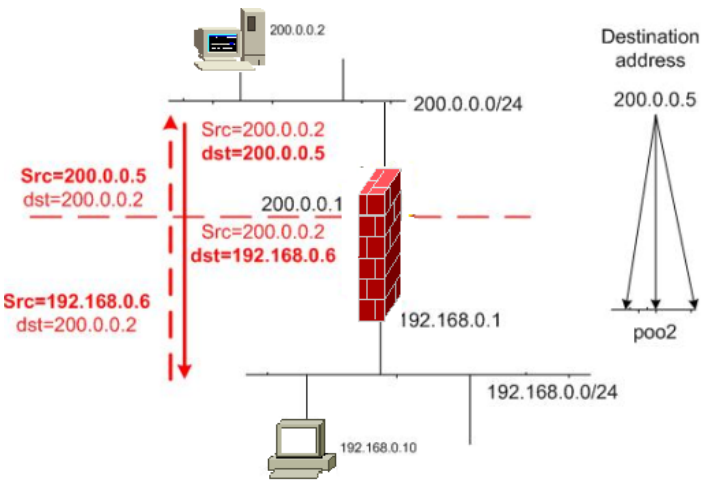
配置 destination NAT，其中包含多种方式的目标地址转换：

- 将地址为 200.0.0.5 的公有目标地址转换到范围为 192.168.0.5 到 192.168.0.8 的私有地址池中；将地址为 200.0.0.6 的公有地址转换为 192.168.0.9 的私有地址；
- 将目标地址为 200.0.0.7，目标端口为 80 的数据包的目标地址转换为私有地址 192.168.0.10；将目标地址为 200.0.0.7，目标端口为 21 的数据包的目标地址转换为私有地址 192.168.0.11；
- 将目标端口为 23 的数据包全部重定向到私有地址 192.168.0.12 的主机上，目标端口不变；将目标端口为 8080 的数据包全部重定向到设备本身，目标端口转换为 3128；

案例组网图：

配置 destination NAT，将目标地址 200.0.0.5 转换到一个地址池中，如下图：

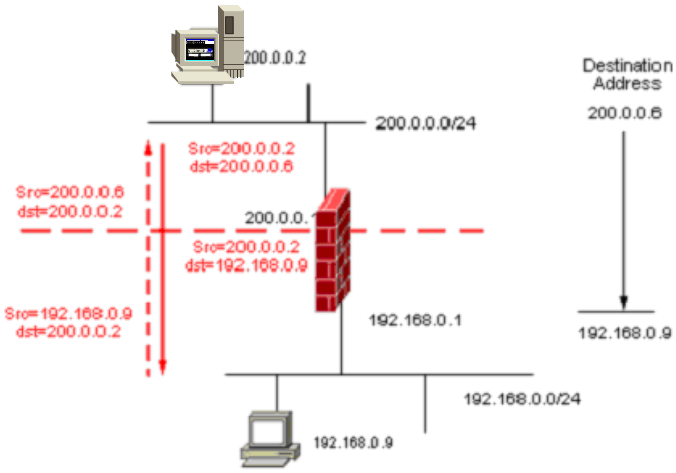
图21-2 配置 destination NAT 案例组网图 a




```
Ip nat pool pool2 192.168.0.5 192.168.0.8 netmask 255.255.255.0
ip nat test destination 200.0.0.5  pool2
```

配置 destination NAT，将目标地址 200.0.0.6 转换为固定的地址 192.168.0.9，如下图：

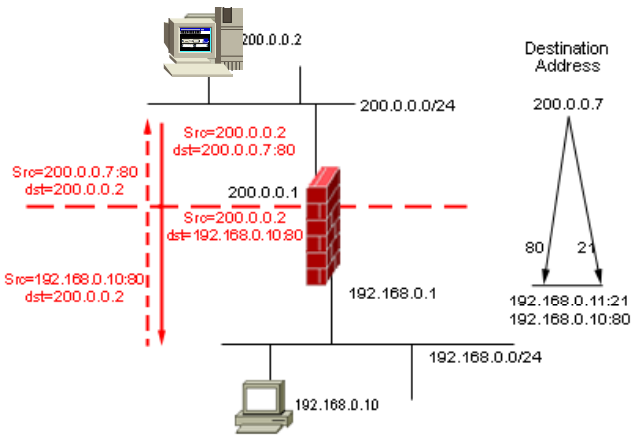
图21-3 配置 destination NAT 案例组网图 b



lp nat test destination 200.0.0.6 192.168.0.9

配置 destination NAT，将目标地址 200.0.0.7 的不同服务转换到不同的主机上，如下图：

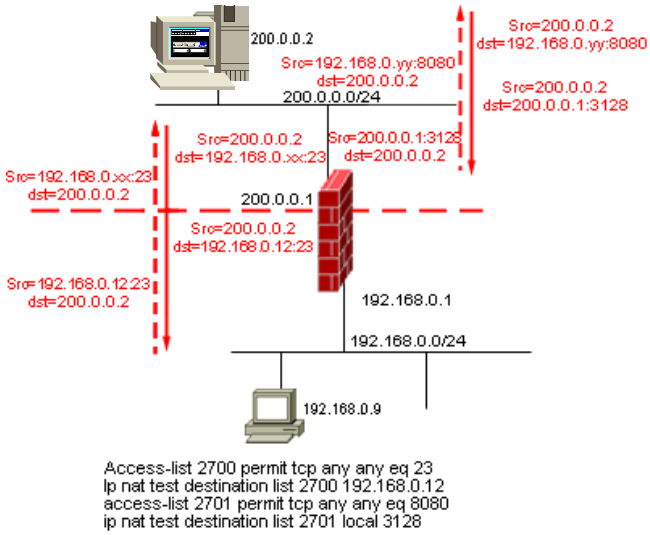
图21-4 配置 destination NAT 案例组网图 c



lp nat test destination tcp 200.0.0.7 21 192.168.0.11
ip nat test destination tcp 200.0.0.7 80 192.168.0.10

配置 destination NAT，将满足条件的数据包重定向到指定 IP 或设备本身，如下图：

图21-5 配置 destination NAT 案例组网图 d



配置步骤：

步骤**1**	建立一个地址池，配置转换后的目标地址范围为192.168.0.5-192.168.0.8
	SmartHammer(config)# ip nat pool pool2 192.168.0.5 192.168.0.8
步骤**2**	配置一条NAT转换规则，将目标地址200.0.0.5转换到地址池pool2上。
	SmartHammer(config)#ip nat test destination 200.0.0.5 pool2
步骤**3**	配置一条NAT转换规则，将目标地址200.0.0.6转换为地址192.168.0.9。
	SmartHammer(config)# ip nat test destination 200.0.0.5 192.168.0.9
步骤**4**	配置一条NAT转换规则，将目标地址200.0.0.7，tcp端口为80数据包的目标地址转换为192.168.0.10。
	SmartHammer(config)# ip nat test destination tcp 200.0.0.7 80 192.168.0.10
步骤**5**	配置一条NAT转换规则，将目标地址200.0.0.7，tcp端口为21数据包的目标地址转换为192.168.0.11。
	SmartHammer(config)# ip nat test destination tcp 200.0.0.7 21 192.168.0.11
步骤**6**	配置一条范围为2700-2999的ACL，配置目标端口为23的数据包
	SmartHammer(config)# access-list 2700 permit any any eq 23
步骤**7**	配置一条NAT转换规则，将满足access-list 2700的数据包重定向到92.168.0.12上。
	SmartHammer(config)# ip nat test destination list 2700 192.168.0.12
步骤**8**	配置一条范围为2700-2999的ACL，配置目标端口为8080的数据包
	SmartHammer(config)# access-list 2701 permit any any eq 8080
步骤**9**	配置一条NAT转换规则，将满足access-list 2701的数据包重定向到设备3128端口上。
	SmartHammer(config)# ip nat test destination list 2701 192.168.0.12 local 3128

步骤10	进入interface模式ge0（ge0为直连200.0.0.0/24网段的接口地址），启用NAT规则链，注意：Destination NAT在设备入口进行转换，所以要在ge0上启用NAT规则链。
	SmartHammer(config)#interface ge0 SmartHammer(config-if)#ip nat test

21.5 故障分析

21.5.1 连接时通时断

故障现象	做了NAT之后，经过NAT ping另外网络的机器，时通时断；或刚开始是通的，一会儿又断了；或一直不通
分析与解决	1)转换后的地址有冲突，别人已经使用。有些地址可能ping不通，但不能排除地址已被使用的可能，因为对方可以禁止了ping包。 2)可以查看被ping的机器中的ARP表项，NAT转换后的地址对应的MAC是否为设备的MAC地址，如不是，证明有其它机器使用了此IP。使用无人使用的地址作为NAT转换后的地址。

21.6 常用调试功能

21.6.1 debug nat

应用环境：

启用 NAT 的情况下，调试 NAT 的正确性。为了在终端显示该调试信息，需要执行命令 terminal monitor。

调试实例：

步骤1	配置NAT
	ip nat test source list 1 172.16.16.1
步骤2	配置access-list
	access-list 1 permit 192.168.0.0 0.0.255.255
步骤3	在出口上启用NAT
	ip nat test
步骤4	启用debug nat命令后得到如下结果：
	<FIREWALL><1963-10-25 18:07:57><NAT><DEBUG>< SRC=192.168.19.1 DST=172.16.16.2 PROTO=icmp, Mangling SRC to 172.16.16.1> <FIREWALL><1963-10-25 18:07:57><NAT><DEBUG>< SRC=172.16.16.2 DST=172.16.16.1 PROTO=icmp, Mangling DST to 192.168.19.1>

结果分析：

从结果可以看出，192.168.19.1 被转换为地址 172.16.16.1，对应的,172.16.16.1 被转换为 192.168.19.1，说明 NAT 规则起作用了。

22 配置链路层过滤

22.1 链路层过滤概述

链路层过滤针对 Ethernet 协议和 MAC 地址进行过滤。链路层过滤没有状态，与自适应安全过滤没有直接关系，属于不同的过滤机制，在不同的层次进行过滤。

22.2 配置链路层过滤

22.2.1 缺省配置

表22-1 链路层过滤的缺省设置信息

内容	缺省设置	备注
链路层过滤缺省策略（无相关命令）	permit	不可更改设置

22.2.2 配置链路层过滤

配置链路层过滤需要 Access-list 配合，利用 Access-list 配置过滤规则，然后在接口启用过滤功能。

表22-2 配置链路层过滤的步骤

步骤**1**	configure terminal	进入配置模式
步骤**2**	Interface NAME	进入interface节点
步骤**3**	ethernet access-group Num (in|out)	配置链路层过滤
步骤**4**	exit	退出interface节点
步骤**5**		针对不同interface，重复步骤2-4
步骤**6**	show ip access-list (Num)	显示配置的access-list信息

注意

如果数据包没有匹配链路层 Access-list 规则，则缺省允许通过。

22.3 配置信息显示命令

表22-3 链路层过滤的配置信息显示命令列表

命令	解释
show ip access-list [Num]	显示Access-list的信息
show running-config	显示当前配置
show acl interface [IFNAME]	显示接口安全级别以及接口上ACL和NAT启用情况

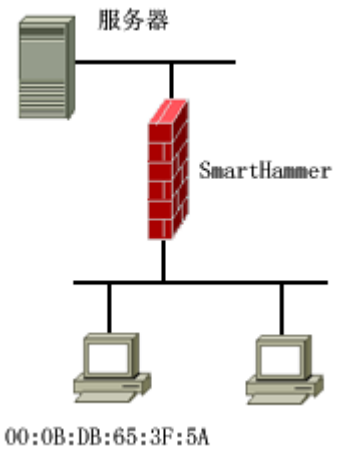
22.4 配置案例

22.4.1 典型的防火墙实施方案

案例描述：

配置链路层过滤，禁止来自 MAC 地址为 00:0B:DB:65:3F:5A 的 ARP 请求。

图22-1 链路层过滤配置案例组网图



配置步骤：

步骤**1**	配置用于过滤的access-list，禁止来自MAC地址为00:0B:DB:65:3F:5A的ARP请求。
	SmartHammer#configure terminal SmartHammer(config)#access-list 200 deny 0x0806 0x0000 000b.db65.3f5a 0.0.0
步骤**2**	在接口ge0上启用access-list
	SmartHammer(config)#interface ge0 SmartHammer(config-if)#ethernet access-group 200 in SmartHammer(config-if)#exit

22.5 常用调试功能

22.5.1 debug acl

应用环境：

启用了链路层过滤规则后调试规则的正确性。为了在终端显示该调试信息，需要执行命令 terminal monitor。

调试实例：

启用链路层过滤规则且打开acl debug之后，得到如下debug信息：

```
<FIREWALL><1963-10-25 17:38:06><ACL><DEBUG><ACTION=deny POS=if_in
IN=ge0 SRCMAC=00:0B:DB:65:3F:5A DSTMAC=00:08:0c:30:00:01
ETHPROTO=2054>
```

结果分析：

从结果可以看出，从 ge0 进来，来自 MAC 地址 00:0B:DB:65:3F:5A 的 ARP 包被禁止通过。

第四部分

VPN 配置

23 配置 IPSec VPN

23.1 IPSec VPN概述

IPSec 用于保护敏感信息在 Internet 上安全的传输。它在网络层对 IP 数据包进行加密和认证。 IPSec 提供了以下网络安全服务，这些安全服务是可选的，通常情况下，本地安全策略决定了采用以下安全服务的一种或多种。

- 数据的机密性—IPSec 的发送方对发给对端的数据进行加密
- 数据的完整性—IPSec 的接收方对接收到的数据进行验证以保证数据在传送的过程中没有被修改
- 数据来源的认证—IPSec 接收方验证数据的起源
- 抗重播—IPSec 的接收方可以检测到重播的 IP 包丢弃

使用 IPSec 可以避免数据包的监听、修改和欺骗，数据可以在不安全的公共网络环境下安全的传输，IPSec 的典型运用是构建 VPN。IPSec 使用 “封装安全载荷（ESP）”或者“鉴别头（AH）”证明数据的起源地、保障数据的完整性以及防止相同数据包的不断重播;使用 ESP 保障数据的机密性。密钥管理协议称为 ISAKMP 根据安全策略数据库（SPDB）随 IPSec 使用用来协商安全联盟（SA）并动态的管理安全联盟数据库。

相关术语解释：

- 鉴别头（AH）：用于验证数据包的安全协议
- 封装安全有效载荷（ESP）： 用于加密和验证数据包的安全协议；可与 AH 配合工作可也以单独工作
- 加密算法：ESP 所使用的加密算法
- 验证算法：AH 或 ESP 用来验证对方的验证算法
- 密钥管理：密钥管理的一组方案，其中 IKE（Internet 密钥交换协议）是默认的密钥自动交换协议

23.2 配置IPSec VPN

23.2.1 缺省配置

表23-1 SmartHammer 设备关于 IPSec VPN 的缺省设置信息：

内容	缺省设置	备注
使能/禁止isakmp密钥监听和协商	enable	可更改设置
密钥协商时协商双方的身份标识	ip address	可更改设置
密钥协商验证对方的方式	预共享密钥(pre-shared)	不能更改设置
isakmp 安全联盟的生存期	3600秒	可更改设置
IPsec 安全联盟的生存期	86400秒	可更改设置
安全协议的工作方式	通道模式	可更改传输模式
加密算法	3DES	可更改设置
验证HASH算法	md5	可更改设置
密钥协商模式	主模式	可更改野蛮模式

23.2.2 配置ISAKMP SA协商策略

在全局配置模式下配置 IKE（Internet Key Exchange）的协商策略。IKE 策略定义了 IKE 协商的一组参数。两端 VPN 设备通过 IKE 协议协商相同的策略，IKE 策略用来定义 IKE 协商过程中的参数，这些参数用于建立 isakmp SA。

配置 ISAKMP SA 协商策略的步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	crypto isakmp policy <1-1000>	进入IKE策略配置
步骤**3**	encryption *(IKE policy)*	配置密钥交换所采用的加密算法，默认3DES加密
步骤**4**	hash *(IKE policy)*	配置密钥交换所采用的加密算法，默认md5加密
步骤**5**	group *(IKE policy)*	配置密钥交换所采用的Diff-Hellmen数组，默认group2
步骤**6**	lifetime *(IKE policy)*	配置isakmp sa的生存期，默认86400秒


注意

用户可以配置多条 IKE 策略，当 SmartHammer 设备进行 IKE 协商时试图协商到两端设备相同的 IKE 策略

23.2.3 配置转换集

转换集是可接受的安全协议和算法组合。两端 SmartHammer 设备通过协商达成共识使用某个相同的转换集进行 IPSec 通信。

配置转换集的步骤:

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	crypto ipsec transform-set transform-set-name <transform1> <transform2> <transform3>	配置转换集
步骤**3**	mode (tunnel | transport)	配置转换集协商IPSec SA的模式

转换集为 AH 认证、ESP 认证、ESP 加密和 IP 压缩算法的任意组合。转换集定义了 IPSec 安全协议和算法。可接受的转换集见下表。

表23-2 可接受的转换集组合：

类型	名称	解释
AH验证	ah-md5-hmac	AH验证md5哈希算法
	ah-sha-hmac	AH验证sha哈希算法
ESP验证	esp-md5-hmac	ESP验证md5哈希算法
	esp-sha-hmac	ESP验证sha哈希算法
ESP加密	esp-aes128	ESP加密128位AES加密算法
	esp-aes256	ESP加密256位AES加密算法
	esp-3des	ESP加密3DES加密算法
	esp-des	ESP加密DES加密算法
	esp-null	ESP不加密
IP-IP压缩	comp-deflate	IP-IP压缩


注意

采用 esp-null 和 esp-des 的转换集建立的 IPSec 通信是非常不安全的，建议 esp-null 仅适用于 IP 载荷已加密的情况，如 SSL 数据包。

23.2.4 配置IPSec SA自动协商策略

配置 IPSec SA 自动协商策略的步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	crypto map *NAME* <0-65535> isakmp	配置IPSec SA自动协商策略,NAME为map名，<0-65536>为序列号，isakmp指定为自动协商
步骤**3**	match address ACLNAME	配置进行Ipsec通信的加密访问列表
步骤**4**	set peer A.B.C.D	IPSec通信的对端路由器地址
步骤**5**	set local-address A.B.C.D	IPSec通信的本地路由器地址
步骤**6**	set pfs group	配置pfs所使用的Diffle-Hellmen数组
步骤**7**	set transform-set TAG	配置ipsec sa协商的转换集，每组策略可以指定一组转换集
步骤**8**	set security-association lifetime <3600-86400>	配置IPSec SA的生存期
步骤**9**	exit	退出IPSec策略配置模式

注意

必须在 interface 模式下使用命令 **crypto map** *NAME* 启用当前的 crypto map 配置

23.2.5 手工配置IPsec安全策略

手工配置 IPsec 安全策略的步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	crypto map *NAME* <0-65535> manual	手工配置IPsec安全策略，NAME为map名，<0-65536>为序列号，manual指定为手工配置SA
步骤**3**	match address *ACLNAME*	配置选择进行IPSec通信的Access list 地址范围
步骤**4**	set peer A.B.C.D	IPSec通信的对端路由器地址
步骤**5**	set local-address A.B.C.D	IPSec通信的本地路由器地址
步骤**6**	set session-key (inbound|outbound) ah <256-4294967295> *WORD*	手工为AH协议设置IPsec会话密钥，inbound为入方向，outbound为出方向，〈256-4294967295〉为该SA的SPI(安全策略索引)号，WORD为AH协议的验证密钥
步骤**7**	set session-key (inbound|outbound) esp <256-4294967295> cipher *WORD* authenticator	手工为ESP协议设置IPsec会话密钥，inbound为入方向，outbound为出方向，〈256-4294967295〉为该SA的SPI(安全策

	WORD authenticator *WORD*	略索引) 号，WORD为WORD为ESP协议的加密密钥和验证密钥
步骤**8**	set transform-set TAG	配置ipsec sa所采用的转换集
步骤**9**	exit	退出IPSec策略配置模式

使用手工方式的安全策略时，为了对数据流实施安全处理，除了设置安全策略中的安全转换集，还需要设置这些安全转换所需的参数，参数包括安全联盟的安全参数索引和各安全转换算法的密钥。安全参数索引的设置必须保证可以用目的地址、协议和安全参数索引唯一的确定一个安全联盟。密钥的长度因算法而异，以下为具体的要求，所说长度指的是输入十六进制串的长度。

表23-3 算法与密钥长度要求

算法名	密钥长度
ah-md5-hmac	32
ah-sha-hmac	40
esp-null	不需要
esp-des	16
esp-3des	48
esp-aes128	32
esp-aes56	64
esp-md5-hmac	32
esp-sha-hmac	40


注意

必须在 interface 模式下使用命令 **crypto map** *NAME* 启用当前的 crypto map 配置；加密和验证用的密钥字符串长度必须与相应的加密或验证算法匹配

23.2.6 配置共享密钥

配置共享密钥的步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	crypto isakmp key key-string address A.B.C.D	配置一条密钥，key-string是密钥字符，A.B.C.D是该密钥对应的对端VPN设备的IP地址


注意

必须在要建立 IPSec VPN 的两台 SmartHammer 设备上配置相同的共享密钥才能验证通过，如果配置 *A.B.C.D* 为 0.0.0.0，则对所有地址的 IKE 协商都将使用相同的密钥，这将非常不安全。

23.2.7 配置SmartHammer设备所属的域名

可以配置未向域名机构注册的域名，不影响 IKE 的协商。

配置 SmartHammer 设备所属的域名的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	ip domain-name *WORD*	配置域名,WORD为要配置的域名

23.2.8 配置允许IKE协商

IKE 协商默认为允许，IKE 不需要在不同的接口上分别启用，而是在 SmartHammer 设备的所有接口上启用。一旦禁止了 IKE 协商，也就禁止了所有接口上 SA 的建立。

配置允许 IKE 协商的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	crypto isakmp enable	配置允许IKE协商

23.3 IPSec VPN显示和清除命令

IPSec VPN 显示命令列表：

步骤1	show crypto isakmp policy <1-1000>	显示ISAKMP策略
步骤2	show crypto map {NAME}	显示Crypto Map策略
步骤3	show crypto ipsec sa	显示已建立IPSec SA
步骤4	show crypto isakmp sa	显示已建立ISAKMP SA

清除 SA 命令：

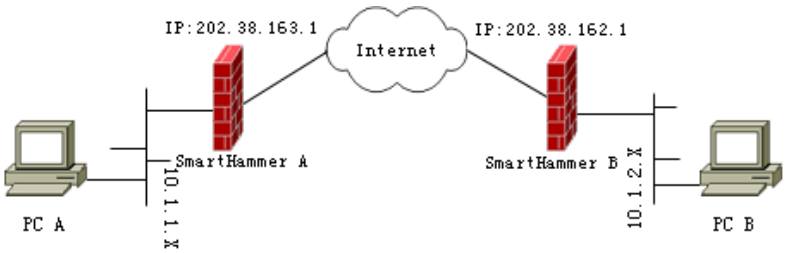
步骤1	clear crypto isakmp [CONNECTION-NAME]	清除isakmp sa，CONNECTION-NAME为已经启用的crypto map名，其格式为map名称#map序号，例如：crypto map harbour 10 isakmp对应的连接名称为”harbour#10”
步骤2	clear crypto sa [CONNECTION-NMAE]	清除ipsec sa，A.B.C.D为对端IP地址，CONNECTION-NAME为已经启用的crypto map名

23.4 配置案例

案例描述：

假定网络环境如下图所示，PC 机 A 到 PC 机 B 的流量需要经过各自的 SmartHammer 设备 后在 Internet 上传输，为了保证流量在 Internet 传输过程中的安全性，有必要在 SmartHammer A 和 SmartHammer B 之间建立 IPSec 的 VPN 隧道以保障通信安全。

图23-1 IPSec VPN 配置案例组网图：



配置任务：

- 配置前准备
- 配置 IKE 协商策略
- 创建转换集
- 创建进入隧道的 access-list
- 创建安全策略
- 配置隧道的起点与终点
- 选择进入隧道的数据流
- 配置安全联盟的生存时间
- 配置安全联盟使用的密钥
- 配置安全联盟使用的变换集
- 配置两端验证共享密钥
- 在接口上应用安全策略

配置步骤：

SmartHammer A 上的配置：

步骤**1**	配置前准备
	SmartHammer(config)# interface ge0 SmartHammer(config-if)# ip address 202.38.163.1/30 SmartHammer(config-if)# exit

步骤2	配置IKE协商策略
	SmartHammer(config)# crypto isakmp policy 1 SmartHammer(config-isakmp)# encryption des SmartHammer(config-isakmp)# hash md5 SmartHammer(config-isakmp)# authentication pre-share SmartHammer(config-isakmp)# exit
步骤3	配置转换集
	SmartHammer(config)# crypto ipsec transform-set ts esp-des esp-md5-hmac SmartHammer(cfg-crypto-trans)# mode tunnel SmartHammer(cfg-crypto-trans)# exit
步骤4	创建进入隧道的access-list
	SmartHammer (config)#access-list 101 permit ip 10.1.2.0 0.0.0.255 10.1.1.0 0.0.0.255
步骤5	创建安全策略
	SmartHammer(config)# crypto map map-name 0 isakmp SmartHammer(config-crypto-map)#
步骤6	配置隧道的起点与终点
	SmartHammer(config-crypto-map)# set peer 202.38.162.1
步骤7	选择进入隧道的数据流
	SmartHammer(config-crypto-map)# match address 101
步骤8	配置安全联盟的生存时间
	SmartHammer(config-crypto-map)# set security-association lifetime 3600
步骤9	配置安全联盟使用的变换集
	SmartHammer(config-crypto-map)# set transform-set ts
步骤10	配置两端验证共享密钥
	SmartHammer(config-crypto-map)# exit SmartHammer(config)# crypto isakmp key 1234567890 address 202.38.162.1
步骤11	在接口上应用安全策略
	SmartHammer(config)# interface ge0 SmartHammer(config-if)# crypto map map-name SmartHammer(config-if)# exit

SmartHammer B 上的配置:

步骤1	配置前准备
	SmartHammer(config)# interface ge0 SmartHammer(config-if)# ip address 202.38.162.1/30 SmartHammer(config-if)# exit
步骤2	配置IKE协商策略
	SmartHammer(config)# crypto isakmp policy 1 SmartHammer(config-isakmp)# encryption des SmartHammer(config-isakmp)# hash md5 SmartHammer(config-isakmp)# authentication pre-share SmartHammer(config-isakmp)# exit
步骤3	配置转换集
	SmartHammer(config)# crypto ipsec transform-set ts esp-des esp-md5-hmac SmartHammer(cfg-crypto-trans)# mode tunnel SmartHammer(cfg-crypto-trans)# exit

步骤4	创建进入隧道的access-list
	SmartHammer (config)#access-list 101 permit ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255
步骤5	创建安全策略
	SmartHammer(config)# crypto map map-name 0 isakmp SmartHammer(config-crypto-map)#
步骤6	配置隧道的起点与终点
	SmartHammer(config-crypto-map)# set peer 202.38.163.1
步骤7	选择进入隧道的数据流
	SmartHammer(config-crypto-map)# match address 101
步骤8	配置安全联盟的生存时间
	SmartHammer(config-crypto-map)# set security-association lifetime 3600
步骤9	配置安全联盟使用的变换集
	SmartHammer(config-crypto-map)# set transform-set ts
步骤10	配置两端验证共享密钥
	SmartHammer(config-crypto-map)# exit SmartHammer(config)# crypto isakmp key 1234567890 address 202.38.163.1
步骤11	在接口上应用安全策略
	SmartHammer(config)# interface ge0 SmartHammer(config-if)# crypto map map-name SmartHammer(config-if)# exit

23.5 故障分析

23.5.1 不能建立隧道

故障现象	安全联盟协商不成功，不能建立SA，在命令show crypto ipsec sa中看不到相关信息
分析与解决	1）查看是否已禁止IKE自协商 2）查看两端设备的相应的要保护的access-list是否对称 3）IKE协商策略是否一致 4）转换集是否一致 5）验证密钥是否已配置

24 配置 L2TP VPDN

本章涉及对 SmartHammer 防火墙产品 L2TP VPDN 功能的配置，内容主要包括：

- L2TP 协议概述
- 配置和启用 L2TP 模板


注意

在配置 L2TP 模板之前，必须先配置好 PPP profile!

24.1 L2TP协议概述

PPP 定义了一种通过二层（L2）点对点连接传输多协议报文的封装机制。典型情况下，一个用户通过某种接入技术（如 ISDN，ADSL 拨号等）获得一个到网络接入服务器（NAS）的二层连接，并在该连接上进行 PPP 会话。在这样的配置中，二层终节点和 PPP 会话的终节点位于同样的物理设备上（也就是说，NAS）。

L2TP（Layer Two Tunneling Protocol）是一种二层隧道协议，它扩展了 PPP 的模型，通过二层隧道将 PPP 会话的终点延伸到另一个通过分组交换网互连的不同设备上，而不是二层接入的终节点。从而将 PPP 会话从二层终结的限制中解脱出来，扩大了 PPP 的应用范围。

L2TP 包括 LAC 和 LNS 两种功能：

- LAC（L2TP Access Concentrator）：L2TP 访问集中器。是 L2TP 隧道的一个端点，是 L2TP 网络服务器（LNS）的对等体（peer）。LAC 负责在一个 LNS 和一个远地系统之间转发 PPP 报文，并维护 LAC 和 LNS 之间的隧道（TUNNEL）和会话（SESSION）连接。
- LNS（L2TP Network Server）：L2TP 网络服务器。是 L2TP 隧道的一个端点，是 LAC 的对等体。负责维护与远地系统之间的 PPP 连接，为远地系统提供对内部网的访问服务。

L2TP 隧道给远程拨号用户提供了连接到 VPN 网关的解决方案，拨号 VPN 又称为 VPDN(virtual private dial network)。在这种应用中，由 VPN 网关提供 LNS 功能，如果拨号用户本身支持 L2TP，则可以采用自愿隧道模式直接连接到 LNS；如果拨号用户本身不支持 L2TP，则可以通过当地 ISP 提供的 LAC 功能采用强制隧道模式连接到 LNS。

这两种连接方式的拓扑结构如下所示：

图24-1 L2TP 客户端直接接入 LNS

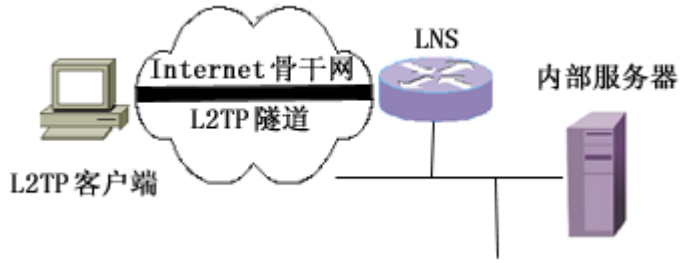
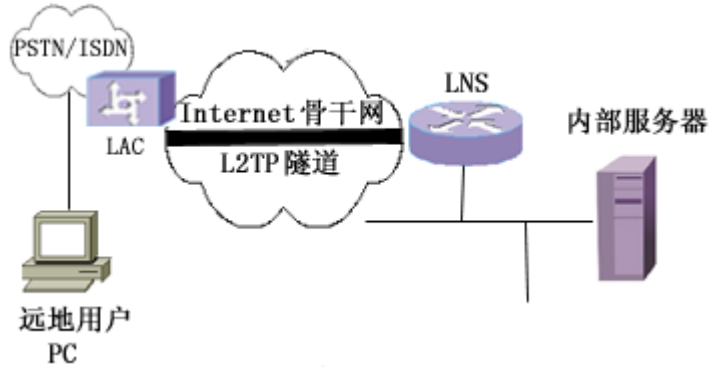
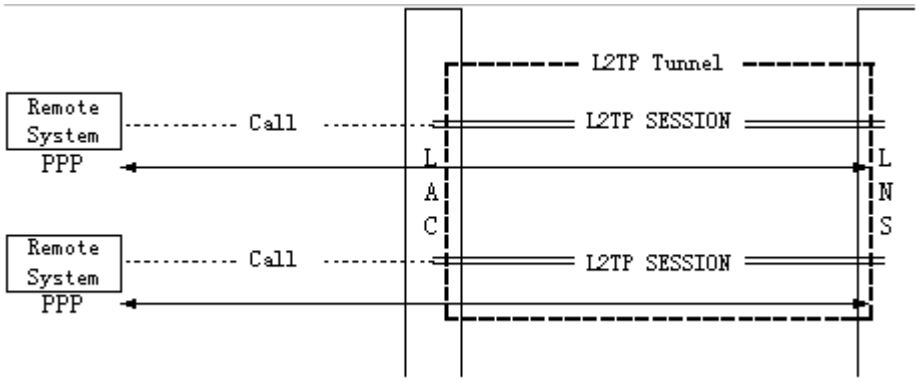


图24-2 拨号用户通过 LAC 远程接入 LNS



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。

图24-3 隧道透传 PPP 帧



L2TP 连接的维护以及 PPP 数据的传送都是通过 L2TP 报文的交换来完成的，这些报文封装在 UDP 报文里从而在承载在 TCP/IP 上。

L2TP 报文可以分为两种类型，一种是控制报文，另一种是数据报文。控制报文用于隧道连接和会话连接的建立与维护。控制报文的传输是可靠的，使用了报文编号确认，滑动窗口，超时重传，隧道保活检测等机制保证控制报文的传输。数据报文则用于承载用户的 PPP 会话数据包。数据报文本身不保证可靠传输，应该根据上层应用由上层协议保证数据报文的可靠投递。

24.2 配置L2TP模板

SmartHammer 设备目前只支持 L2TP 的 LNS 功能，不支持 LAC 功能，而且 LNS 只是监听接口的 L2TP 连接请求，不会主动发起 L2TP 连接请求。

在 SmartHammer 设备中，L2TP 协议的参数都是在 L2TP 模板中配置的，包括：所使用的 PPP Profile，L2TP 监听的接口地址，L2TP 隧道认证，隧道维护参数等。用户可以配置和启用多个 L2TP 模板。但是必须保证每个 L2TP 模板中配置的监听地址不能相同。

24.2.1 缺省配置

SmartHammer 设备关于 L2TP 模板的缺省设置信息如以下表格所示：

表24-1 模板的缺省设置信息

内容	缺省设置	备注
隧道活动探测时间（hello-time）	不启用	可更改设置
隧道接收窗口大小(receive-window)	4	可更改设置
隧道认证(tunnel authentication)	不启用	可更改设置
隧道IP地址唯一性检测(unique-ip)	不启用	可更改设置
隧道本地名称(localname)	主机名	可更改设置
最大隧道数限制(max tunnel)	500	可更改设置
最大会话数限制(max session)	500	可更改设置

24.2.2 配置使用的PPP profile

L2TP 协议是基于 PPP 的应用，L2TP 会话中传输的就是 PPP 会话，因此必须要有 PPP 的支持。L2TP 模板中所使用的 PPP 相关的参数在 PPP profile 中配置。PPP profile 的详细配置参见“PPP profie 配置”部分。

配置 PPP pfrole 的步骤:

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	subscriber-template l2tp NAME	配置名为NAME的L2TP 模板，如果不存在该模板，则创建模板
步骤**3**	ppp profle NAME	配置使用的PPP profle
步骤**4**	write terminal	显示配置


注意

1）在 L2TP 模板下必须要配置 PPP profile，否则 L2TP 模板不能启用。

2）在一个 L2TP 模板下只可以配置一个 PPP profile。

3）请参考“PPP profile 配置”部分。

24.2.3 配置L2TP监听的地址

L2TP 客户端或者 LAC 在发送隧道连接请求时，会指定要连接的 LNS 地址。LNS 则在指定的地址上监听 L2TP 连接请求。这个地址必须是一个活动接口的地址。

LNS 只监听该地址上的隧道连接请求。每个 L2TP 模板只能配置一个监听地址，而且不能与其它模板中的配置相同。否则 L2TP 模板无法启用。

配置监听地址命令:

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	subscriber-template l2tp NAME	配置名为NAME的L2TP 模板，如果不存在该模板，则创建模板
步骤**3**	listen address A.B.C.D	指定L2TP监听的地址
步骤**4**	write terminal	显示配置


注意

1）每个 L2TP 模板只能配置一个而且必须配置一个监听地址，该地址必须是一个活动接口的地址，而且不能与其它已经启用的 L2TP 模板配置相同的地址，否则 L2TP 模板不能启用。

24.2.4 配置隧道活动探测时间

在 L2TP 模板中可配置 L2TP 隧道的保活探测时间。在 L2TP 隧道建立之后，如果在指定的时间内隧道没有报文的交互，则 LAC 或 LNS 将发送 Hello 控制报文，探测隧道的活动性，对该控制报文，对方是必须应答的。如果三次重发后得不到应答，则认为该隧道已经不可用，将强制关闭该隧道。LAC 和 LNS 的 Hello 报文发送是独立的，其时间可以不同。默认的隧道活动探测时间是 0 秒，也就是说不发送 hello 探测报文。

配置隧道活动探测时间的步骤:

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	subscriber-template l2tp NAME	配置名为NAME的L2TP 模板，如果不存在该模板，则创建模板
步骤**3**	hello-time <1-3600>	配置隧道活动探测时间
步骤**4**	write terminal	显示配置


注意

隧道活动探测时间应该比 PPP Profile 中的 echo-time 时间要长，建议设置为 echo-time 时间的 2-3 倍。

24.2.5 配置隧道接收窗口的大小

L2TP 隧道的控制报文是可靠传输的，对所发送的每个控制报文都需要对方进行确认。为了提高吞吐量，允许 LAC 或 LNS 在得到确认之前连续发送一窗口的控制报文，然后对端可以予以一次性确认。这个窗口大小由对端的接收窗口大小来规定，也就是说，对方的接收窗口大小就是本方的发送窗口大小。默认情况下，这个值是 4。可以通过命令改变这个默认窗口大小。接收窗口的值对 LAC 和 LNS 而言是独立的，可以设置为不同的值。

配置隧道接收窗口大小的步骤:

步骤1	configure terminal	进入全局配置模式
步骤2	subscriber-template l2tp NAME	配置名为NAME的L2TP 模板，如果不存在该模板，则创建模板
步骤3	receive-window <1-300>	配置隧道接收窗口大小
步骤4	write terminal	显示配置

24.2.6 配置L2TP会话数上限

在一个 L2TP 隧道内可以有多个 L2TP 会话，而每个 L2TP 会话对应于一个 PPP 会话，用户可以根据需要限制 L2TP 会话的个数，从而限制承载的 PPP 会话的个数。如果 L2TP 会话数达到该限制，将不再接受 L2TP 会话连接请求。

配置 L2TP 会话数上限的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	subscriber-template l2tp NAME	配置名为NAME的L2TP 模板，如果不存在该模板，则创建模板
步骤3	max session <1-8192>	配置L2TP会话数上限
步骤4	write terminal	显示配置

24.2.7 配置L2TP隧道数上限

系统中每个 L2TP 隧道都会占用一定的处理资源，用户可以根据需要限制 L2TP 隧道的个数。如果 L2TP 隧道数达到该限制，将不再接受隧道连接请求。

配置 L2TP 隧道数上限的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	subscriber-template l2tp NAME	配置名为NAME的L2TP 模板，如果不存在该模板，则创建模板
步骤3	max tunnel <1-8192>	配置L2TP隧道数上限
步骤4	write terminal	显示配置

24.2.8 配置隧道的本地名称

一条 L2TP 隧道建立后，会有一个本端分配的数字标识，有一个对端分配的数字标识，有一个本地名，有一个对端所赋予的远端名。由这四项唯一标志一条隧道。L2TP 隧道本地名的缺省值为防火墙的主机名。

配置 L2TP 隧道的本地名的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	subscriber-template l2tp NAME	配置名为NAME的L2TP 模板，如果不存在该模板，则创建模板
步骤3	localname NAME	配置L2TP隧道的本地名
步骤4	write terminal	显示配置

24.2.9 配置隧道IP地址唯一性检测

如果配置对 L2TP 隧道的 IP 地址唯一性进行检测，那么每个 IP 地址只允许建立一条隧道。缺省配置为不检测隧道 IP 地址的唯一性，也就是说每个 IP 地址可以允许建立多条隧道。

配置隧道 IP 地址唯一性检测的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	subscriber-template l2tp NAME	进入模板配置模式，如果不存在该模板，则会创建该模板
步骤3	unique-ip	配置隧道的IP地址唯一性检测
步骤4	write terminal	显示配置

24.2.10 配置隧道认证

在建立 L2TP 隧道的过程中，LNS 和 LAC 中的任何一方都可以要求对方认证。比如说，从 LNS 的角度来看，如果不信任 LAC 的话，可以要求对 LAC 进行认证；信任的话，则可以不要对 LAC 进行认证。反之，在 LAC 看来也是一样的。LAC 和 LNS 之间的隧道认证过程类似于 PPP 使用的 CHAP 认证方式。

如果配置了隧道认证，则会向隧道对端发送 challenge，要求对方认证。因此在隧道两端都要配置隧道认证的密码。如果模板中没有配置隧道对端的密码，或者对端认证不通过，将无法建立隧道连接。由于有些 L2TP 客户端软件不支持隧道认证，因此默认配置为不要求对方认证。

配置隧道认证的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	subscriber-template l2tp NAME	进入模板配置模式，如果不存在该模板，则会创建该模板
步骤3	tunnel authentication	配置隧道认证
步骤4	write terminal	显示配置

24.2.11 配置隧道对端的IP地址和密码

L2TP 隧道的密码用于对隧道进行认证，隧道双方认证的密码是相同的。因此只要有一方配置了隧道认证，那么双方都必须配置认证密码。L2TP 控制报文中的 AVP 加密也使用的是同样的密码。隧道对端的认证密码在全局配置模式下配置。

配置隧道对端的名称和密码的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	l2tp peer ip A.B.C.C password WORD	配置L2TP隧道对端的IP地址和密码
步骤3	write terminal	显示配置

24.3 启动L2TP VPDN功能

在 L2TP 模板配置完后，如果允许防火墙使用 L2TP VPDN 功能，则需要在全局配置模式启动它。对应的 no 命令可以禁用它。可以同时启用多个 L2TP 模板，只要每个模板中配置的监听地址不同。这种情况下，每个 L2TP 模板监听一个接口地址

上的 L2TP 连接请求。

启动 L2TP VPDN 的配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	vpdn enable l2tp subscriber-template NAME	配置启用L2TP VPDN，启用的L2TP模板名为NAME
步骤3	write terminal	显示配置

24.4 L2TP管理命令

表24-2 L2TP 配置管理命令列表

命令	解释
show l2tp subscribe-template [NAME]	显示L2TP 模板信息，NAME用于指定显示的模板
show l2tp tunnel [A.B.C.D]	显示L2TP隧道信息，A.B.C.D指定隧道对端的IP地址
show l2tp session	显示所有L2TP会话信息
clear l2tp sesssion	强制关闭所有L2TP会话
clear l2tp tunnel [A.B.C.D]	强制关闭指定的L2TP隧道，A.B.C.D指定隧道对端的IP地址

24.4.2 显示信息举例

显示已经配置的 L2TP 模板：

步骤1	显示配置的名为test的L2TP模板
	SmartHammer#show l2tp subscriber-template test subscriber-template l2tp test ppp profile test listen address 192.168.19.10 tunnel authentication hello-time 60 receive-window 10 max-tunnel 8000 max-session 8000 unique-ip localname harbour

显示 L2TP 隧道认证密码：

步骤**1** 显示配置的L2TP隧道认证密码

```
SmartHammer#show l2tp peerl2tp peer ip 10.1.1.1 password haha
l2tp peer ip 10.4.1.2 password 123456
!
```

显示已经建立和正在建立的 L2TP 隧道：

步骤**1** 显示已经建立和正在建立的L2TP隧道

```
SmartHammer#show l2tp tunnel
============================================================
LocID    RemID    Name          IPAdress          Port     SessNum
State
------------------------------------------------------------
74       7        lac0          10.88.1.226       52958    1
established
============================================================
Total Tunnels:     1
```

表24-3 show l2tp tunnel 各字段含义

字段	意义
LocID	由本端分配给该TUNNEL的数字标识
RemID	由对端分配给该TUNNEL的数字标识
Name	对端为该TUNNEL指定的名字
IPAddress	TUNNEL对端的IP地址
Port	TUNNEL对端的UDP端口号
SessNum	属于该TUNNEL的SESSION数目
State	TUNNEL当前所处的状态，可以有： "IDLE"，"WAIT-REPLY"，"WAIT-CONN"，"ESTABLISHTED"，"RECV-STOPCCN"，"SENT-STOPCCN"

显示已经建立和正在建立的 L2TP 会话：

步骤**1** 显示已经建立和正在建立的L2TP会话

```
SmartHammer#show l2tp session
============================================================
      LocID    RemID    TunID      State
------------------------------------------------------------
        19        5       74     WAIT-REPLY
      2368        6       74     ESTABLISHTED
       175        7       74     ESTABLISHTED
============================================================
 Total Sessions:     3
```

表24-4 各字段的含义

字段	意义
LocID	由本端分配给该SESSION的一个数字标识
RemID	由对端分配给该SESSION的一个数字标识
TunID	该SESSION所属的TUNNEL的本地标识
State	该SESSION现在所处的状态，可能有： "IDLE"，"WAIT-TUNNEL"，"WAIT-REPLY"，"WAIT-CONN"， "ESTABLISHED"，"RECV-CDN"，"SENT-CDN"

24.4.3 强制清除命令举例

举例 1：

步骤**1**	清除所有L2TP会话，将同时清除对应的PPP用户
	SmartHammer#clear l2tp session ========== Total clear sessions: 5

举例 2：

步骤**1**	清除对端IP地址为10.1.1.1的L2TP隧道
	SmartHammer#clear l2tp tunnel 10.1.1.1 ========== Total clear tunnels: 1

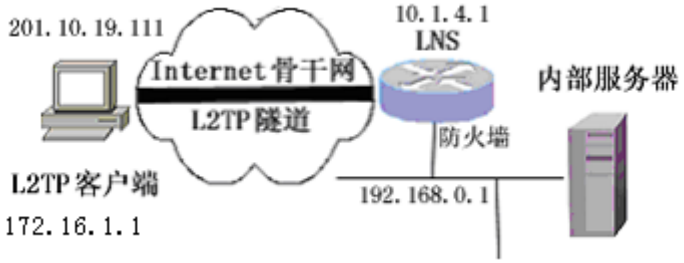
24.5 配置案例

24.5.1 L2TP客户端直接连接到LNS

案例描述

远程用户希望访问本地局域网，由于本地局域网使用的是私有地址，从 INTERNET 上不能直接访问。如果用户有 L2TP 客户端，则可以使用 L2TP 客户端远程拨入本地 VPN 网关上的 LNS，建立 L2TP 隧道，然后通过 PPP 协商由本地 VPN 网关对远程用户进行认证，并给他分配一个本地的私网地址，从而在远程用户和 LNS 之间建立一条基于 L2TP 的 VPDN 连接，使远程用户可以象本地用户一样访问本地局域网。

图24-4 L2TP 客户端直接连接到 LNS 组网图



VPN 网关的配置步骤：

步骤**1**	首先配置一个PPP认证用的AAA模板
	SmartHammer# configure terminal SmartHammer(config)# aaa-group local SmartHammer(config-aaa)# authentication local SmartHammer(config-aaa)# accounting none 具体细节参见“AAA模板配置”部分。
步骤**2**	添加远程拨号PPP用户的用户名和密码，由于使用本地认证，需要在本地添加远程用户
	SmartHammer# configure terminal SmartHammer(config)# user vpdn14 password 12345
步骤**3**	配置PPP Profile使用的本地IP地址池0的地址范围为从172.16.1.2开始的200个地址
	SmartHammer# configure terminal SmartHammer(config)# ip pool 0 172.16.1.2 200
步骤**4**	然后配置使用的PPP profile
	SmartHammer# configure terminal SmartHammer(config)# ppp profile l2tp SmartHammer(config-ppp)# address local 172.16.1.1/16 SmartHammer(config-ppp)# address pool local 0 SmartHammer(config-ppp)# max-user 200 SmartHammer(config-ppp)# authentication chap SmartHammer(config-ppp)# aaa-group local SmartHammer(config-ppp)# dns 10.1.1.1 SmartHammer(config-ppp)# wins 10.1.1.1 SmartHammer(config-ppp)# echo-time 60 具体细节参见“PPP profile配置”部分。 **注意本地地址不要与任意接口地址在同一网段。**
步骤**5**	再配置LNS使用的L2TP模板
	SmartHammer# configure terminal SmartHammer(config)# subscriber-template l2tp lns SmartHammer(config-l2tp)# ppp profile l2tp SmartHammer(config-l2tp)# listen address 10.1.4.1 SmartHammer(config-l2tp)# localname lns0 SmartHammer(config-l2tp)# hello-time 150
步骤**6**	启用L2TP模板7

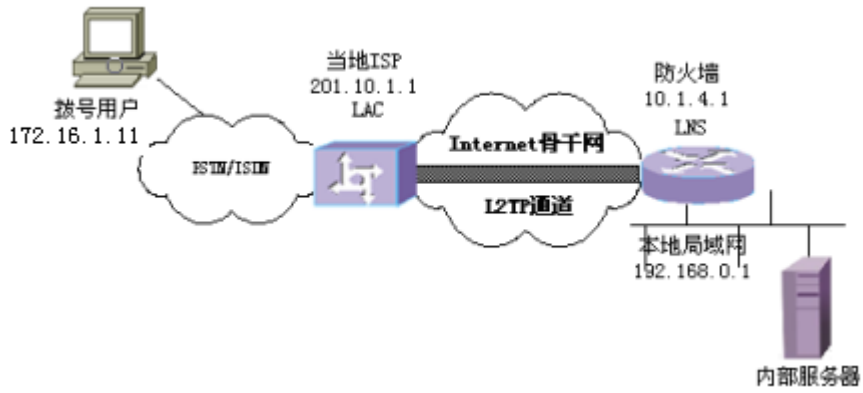
	SmartHammer# configure terminal SmartHammer(config-l2tp)# vpdn enable l2tp subscriber-template lns
步骤7	L2TP客户端的配置
	远程用户如果不能访问互联网，则需要先拨号到当地的ISP，获得访问公网的权限，假定通过当地的ISP获得一个公网地址为201.10.19.111。然后L2TP客户端设置VPN连接的地址为lns的监听地址10.1.4.1，用户名为vpdn14 密码为12345，拨号即可。

24.5.2 拨号客户端通过LAC连接到LNS

组网需求

远程用户希望访问本地局域网，由于本地局域网使用的是私有地址，从 INTERNET 上不能直接访问。如果远程用户没有 L2TP 客户端，但是有其它拨号客户端（例如 PPPoE），则可以使用当地 ISP 支持的拨号方式拨入当地的 ISP，通过 ISP 提供的 LAC 建立到本地 VPN 网关上的 LNS 之间的 L2TP 隧道，然后通过 PPP 协商由本地 VPN 网关对远程用户进行认证，并给他分配一个本地的私网地址，从而在远程用户和 LNS 之间建立一条 VPDN 连接，使远程用户可以象本地用户一样访问本地局域网。

图24-5 拨号客户端通过 LAC 连接到 LNS 组网图



VPN 网关的配置步骤:

步骤1	先配置一个PPP认证用的AAA模板，参照上例。
步骤2	添加远程用户的用户名和密码，参照上例。
步骤3	配置PPP Profile使用的本地IP地址池范围，参照上例。

步骤4	配置使用的PPP profile，参照上例。
步骤5	配置L2TP隧道认证的密码。
	SmartHammer# configure terminal SmartHammer(config)# l2tp peer ip 10.1.1.1 password lac0
步骤6	配置LNS使用的L2TP模板。
	SmartHammer# configure terminal SmartHammer(config)# subscriber-template l2tp lns SmartHammer(config-l2tp)# ppp profile l2tp SmartHammer(config-l2tp)# listen address 10.1.5.1 SmartHammer(config-l2tp)# hello-time 150 SmartHammer(config-l2tp)# tunnel authentication SmartHammer(config-l2tp)# localname lns0
步骤7	启用L2TP模板
	SmartHammer# configure terminal SmartHammer(config-l2tp)# vpdn enable l2tp subscriber-template lns
步骤8	LAC的配置
	远程用户通过LAC接入LNS。 LAC的配置必须与LNS一致，它的IP地址配置为10.1.1.1，认证密码配置为lac0，VPN域对应的lns地址为10.1.5.1。
步骤9	L2TP客户端的配置
	远程用户可以使用LAC支持的任意拨号方式接入LAC。 客户端指定用户名为vpdn14@VPN，密码为12345。

24.6 常见故障

24.6.1 L2TP客户端直接拨号到LNS，无法建立连接

故障现象	L2TP客户端直接拨号到LNS，无法建立连接
分析与解决	有可能是以下几种情况导致客户端无法建立连接（可以使用debug l2tp查看调试信息） 1）客户端的用户名密码错误，确认一下用户名和密码。 2）客户端指定的连接地址不是模板中配置的地址，或者该地址不是活动接口的地址。 3）PPP用户数已达到最大值，使用show ppp summary命令查看总的PPP用户数。 4）L2TP隧道或会话数已达到最大值，使用show l2tp tunnel命令查看总的隧道数，使用show l2tp sessionl命令查看总的会话数。 5）配置的AAA认证模板和PPP profile是否正确。

	6）如果采用Radius服务器对用户进行认证，查看SmartHammer设备是否可达Radius认证服务器，以及Radius认证服务是否已启动。 7）L2TP客户端一般不支持隧道认证，查看L2TP模板中是否配置了隧道认证 。

24.6.2 客户端直接连接到LNS，出现异常断开连接

故障现象	L2TP客户端直接连接到LNS，出现异常断开连接
分析与解决	1）有可能是以下几种情况导致L2TP客户端异常断开连接： 由于网络故障导致L2TP隧道的hello报文没有应答，SmartHammer设备断开隧道连接。请确认网络线路没有故障，而且L2TP模板中配置的监听地址所在的接口正常工作。 2）如果在PPP profile中设置了Idle Time，将导致用户在一段时间内没有流量时，SmartHammer设备强制关闭PPP会话。 3）如果PPP profile中配置使用DHCP地址池，可能是DHCP 地址续租失败，导致关闭PPP会话。请确认到DHCP server之间可达，而且DHCP server的地址池没有用完。

24.6.3 用户通过LAC连接到LNS，无法建立连接

故障现象	用户通过LAC连接到LNS，无法建立连接
分析与解决	有可能是以下几种情况导致用户无法建立连接： 1）用户指定的用户名密码错误，确认一下用户名和密码，而且LAC能够解析用户指定的VPN域名。 2）LAC指定的连接地址不是LNS模板中配置的地址，或者该地址不是活动接口的地址。 3）LNS中配置了隧道认证，但是LAC不支持隧道认证，或者认证的隧道密码配置错误 。确认LAC与LNS的配置一致。 4）PPP用户数已达到最大值，使用show ppp summary命令查看总的PPP用户数。 5）L2TP隧道或会话数已达到最大值，使用show l2tp tunnel命令查看总的隧道数，使用show l2tp sessionl命令查看总的会话数。

24.7 常用调试功能

24.7.1 debug l2tp tunnel

应用环境：当 LAC 无法与 LNS 建立隧道时

调试实例：

```
Mar  3 14:00:31 mjh l2tpd[391]: Recv: SCCRQ
Mar  3 14:00:31 mjh l2tpd[391]: Tunnel(28294) start
Mar  3 14:00:31 mjh l2tpd[391]: Peer is not authorized to create a tunnel
Mar  3 14:00:31 mjh l2tpd[391]: Send: StopCCN
Mar  3 14:00:31 mjh l2tpd[391]: Recv: ZLB
```

结果分析：

LNS 收到了 LAC 的 SCCRQ 隧道连接请求，但是 LNS 配置了对隧道进行认证，由于没有配置该 LAC 的名称和密码，因此认为该 LAC 没有建立隧道的权限，拒绝它的连接请求。


注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug l2tp tunnel 命令禁用此功能。

24.7.2 debug l2tp session

应用环境：当 LAC 无法与 LNS 建立会话时

调试实例：

```
Mar  3 13:55:38 mjh l2tpd[395]: Recv: ICRQ
Mar  3 13:55:38 mjh l2tpd[395]: Send: ICRP
Mar  3 13:55:38 mjh l2tpd[395]: Recv: ICCN
Mar  3 13:55:38 mjh l2tpd[395]: Send: ZLB
Mar  3 13:55:38 mjh l2tpd[395]: Start PPP
Mar  3 13:55:38 mjh l2tpd[395]: Send: CDN
Mar  3 13:55:38 mjh l2tpd[395]: Free session(64792/20912): ppp terminated
```

结果分析：

LNS 与 LAC 之间的 L2TP 会话已经建立起来了，而且启动了 PPP 会话，但是由于 PPP 会话终止，导致 L2TP 会话关闭。至于 PPP 会话终止的原因，可以进一步调

试 PPP 部分，参见“PPP profile 配置”部分。

第五部分

接入认证配置

25 配置 PPP Profile

本章涉及对 SmartHammer设备中 PPP 协议功能的配置，内容主要包括：

- PPP 协议概述
- 配置本地 IP 地址池
- 配置 PPP Profile

在配置 PPP Profile 之前，必须先配置好 AAA 模板。而且 PPP Profile 必须与 L2TP 或 PPPoE 一起使用，不能单独使用。

25.1 PPP协议概述

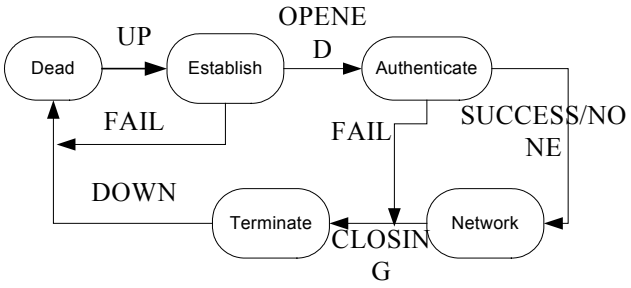
PPP（Point-to-Point Protocol 点到点协议）是为在对等单元之间传输数据包这样的简单链路设计的链路层协议。最初的设计目的主要是用来通过拨号或专线方式建立点对点连接传输数据。由于它具备用户认验能力和 IP 地址分配功能，可以很好地对用户进行接入控制和管理，因此成为广域网上应用最广泛的协议之一。例如，家庭拨号上网就是通过 PPP 在用户端和运营商的接入服务器之间建立通信链路。随着宽带接入取代拨号上网的趋势，PPP 也衍生出新的应用：如 PPP 与其它的协议结合派生出了符合宽带接入要求的新协议 PPPoE（PPP over Ethernet）、PPPoA（PPP over ATM），以及适应 VPN 发展要求而产生的 PPTP、L2TP 协议等。

PPP 协议中提供了一整套方案来解决链路建立、维护、拆除、上层协议协商、认证等问题。它主要包含这样几个部分：

- 链路控制协议 LCP（Link Control Protocol）：LCP 负责创建，维护或终止一次物理连接；
- 网络控制协议 NCP（Network Control Protocol）：NCP 是一族协议，负责解决物理连接上运行什么网络协议，以及解决上层网络协议发生的问题；
- 认证协议：用于对用户进行身份验证，最常用的包括口令验证协议 PAP（Password Authentication Protocol）和挑战握手验证协议 CHAP（Challenge-Handshake Authentication Protocol）。

PPP 链路状态机如下图所示。一个典型的链路建立过程分为三个阶段：链路创建阶段、认证阶段和网络层协商阶段。

图25-1 PPP 状态迁移图



25.2 配置本地IP地址池范围

PPP 是点对点连接方式，连接的两端都必须有地址。本地的地址由我们指定，对端的地址通过地址池分配。每个 PPP 用户在上线之后都会给他分配一个地址。这个地址可以通过 DHCP 服务器，RADIUS 服务器，或者本地地址池分配。如果使用本地地址池给 PPP 用户分配 IP 地址，就必须先配置本地的 IP 地址池。本地 IP 地址池是在全局配置模式下配置，然后在 PPP Profile 中引用的。

配置本地 IP 地址池的步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	ip pool <0-255> A.B.C.D (NUM|E.F.G.H)	指定IP地址池的ID和地址范围
步骤**3**	write terminal	显示配置

提示

本地 IP 地址池最多可以配置 256 个，通过 ID 标志，ID 可以配置为 0－255 之间。地址池相互之间不能有重叠。如果该地址池已经被 PPP Profile 使用，则必须先从 PPP Profile 中取消对它的使用，然后才能删除该地址池。

25.3 配置PPP Profile

在 SmartHammer 设备中，PPP 协议的参数都是在 PPP Profile 中配置的，包括：认证方式、认证和计费模板、计费间隔、异常下线探测时间、地址分配方式、DNS 服务器和 WINS 服务器地址等。

SmartHammer 设备提供的 L2TP VPDN 功能和 PPPoE 接入认证功能，都是基于 PPP 协议的应用，必须先配置好 PPP Profile，然后才能在 L2TP 或 PPPoE 中使用。用户可以配置多个 PPP Profile，由其它协议选用。

如果某个 PPP Profile 已经被其它模板使用，则不能删除该 PPP Profile。必须先取消对它的使用才能删除。如果使用该 PPP Profile 的 PPP 用户已经上线，则不能删除和更改该 PPP Profile 中的本地地址、地址池和 AAA 模板。必须先让用户下线，才能删除或更改这些参数。

25.3.1 缺省配置

PPP Profile 的缺省设置信息:

内容	缺省设置	备注
认证方式	pap	可更改设置
用户名唯一性检测	不启用	可更改设置
链路活动探测时间	60秒	可更改设置
链路空闲时间限制	不限制	可更改设置
实时计费	不启用	可更改设置


注意

使用 no ppp-profile NAME 可以删除一个名为 NAME 的 PPP Profile。如果该 PPP Profile 被 L2TP 或 PPPoE 模板引用，则必须先从 L2TP 或 PPPoE 模板中取消引用，然后才能删除该 PPP Profile。

25.3.2 配置AAA模板

PPP 模板中必须配置使用的 AAA 模板。AAA 模板中配置了 PPP 用户的本地认证和 radius 认证服务器的参数。

配置 AAA 模板的步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	ppp-profile NAME	配置名为NAME的PPP Profile，如果不存在该模板，则创建模板
步骤**3**	aaa-group NAME [by GROUP]	配置使用的AAA认证和计费模板（详见第十一部分）。by GROUP用于设定使用该AAA模板的用户组，GROUP为一个模式匹配，即以一个正则表达式来表示一个或一组用户，例如^h代表以h开头，e$代表以e结尾等。即：aaa-group 1 by @a.com$表示所有用户名以@a.com结束的用户使用AAA模板1中的配置。
步骤**4**	write terminal	显示配置


注意

1）在 PPP Profile 下必须要配置 AAA 模板，否则无法对 PPP 用户进行接入认证。

2)在一个 PPP Profile 下可以配置多个 AAA 模板,可以同时对 PPP 用户进行多种计费。

3）不以 by GROUP 为后缀使用的 AAA 认证和计费模板，表示所有用户可以匹配该模板。

4）以 by GROUP 为后缀使用的 AAA 认证和计费模板，表示只有用户名和 GROUP 可以匹配的用户,可以使用该模板,用于对多 ISP 的支持。用户名请详细参考对“AAA 认证和计费模板”的配置和注意事项。

25.3.3 配置认证方式

PPP 模板中可以配置 PPP 用户的认证方式。本地认证支持 pap 和 chap 两种方式。Radius 认证支持 pap、chap、ms-chap、ms-chapv2 四种方式。

- PAP（口令验证协议）
- PAP 是一种明文验证协议，其验证过程如下：

1）被验证方发送用户名和口令到验证方；

2）验证方根据用户配置查看是否有此用户以及口令是否正确，然后返回验证成功或失败的响应。

- CHAP（挑战-握手验证协议）

CHAP 是一种加密验证协议，其验证过程：

1）验证方向被验证方发送一串随机产生的数据(Challenge)；

2）被验证方用自己的口令字和 MD5 算法对该随机数据进行加密，将生成的密文发回验证方(Response)；

3）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）。

- MS-CHAP（微软挑战-握手验证协议）

MS-CHAP 与 CHAP 基本类似，也是一种加密验证协议。不同的是 MS-CHAP 使用基于 MPPE 的加密算法，而不是 MD5 加密算法。

- MS-CHAPv2 是 MS-CHAP 的增强版本。

配置认证方式的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	ppp-profile NAME	配置名为NAME的PPP Profile，如果不存在该模板，则创建模板
步骤3	authentication (mschap-v2|mschap|chap|pap)	配置认证方式，默认值为pap。本地认证支持pap和chap两种方式。Radius认证支持pap、chap、ms-chap、ms-chapv2四种方式。
步骤4	write terminal	显示配置

使用 no authentication 可以取消对认证方式的设置，使其恢复到缺省配置。如果 AAA 模板中配置为本地认证，则只可以选择 pap 和 chap 两种认证方式；如果 AAA 模板中配置为 radius 认证，则可以选择以上四种认证方式。

25.3.4 配置实时计费

PPP Profile 中可以设置给 Radius 计费服务器发送计费信息的时间间隔。使用 Radius 计费服务器进行计费时，一般在计费开始时发送计费开始报文，在计费结束时发送计费结束报文（携带用户上线时长和流量），供 Radius 计费服务器计算用户计费信息。为了保证用户计费信息的准确性和实时性，可以设置用户上线后，每隔一段时间发送一次 Radius 间隔计费报文，也携带用户上线时长和流量。默认值为 0，即不使用实时计费，只在用户下线时发送计费信息。

配置实时计费的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	ppp-profile NAME	配置名为NAME的PPP Profile，如果不存在该模板，则创建模板
步骤3	accounting-interval <60-3600>	配置实时计费间隔，默认值为0（不使用实时计费）
步骤4	write terminal	显示配置

25.3.5 配置链路活动探测时间

PPP 连接建立过程中，在 LCP 协商完成后，将定期发送 lcp echo request 报文，探测链路是否存在。如果收到 lcp echo request 报文，必须回答 lcp echo reply 报文。如果三次重发后，没有收到 lcp echo reply 报文，则认为链路已经断开。发送 lcp echo request 的时间可以在 ppp profile 中设置。默认为 60 秒。

配置链路活动探测时间：

步骤1	configure terminal	进入全局配置模式
步骤2	subscriber-template ppp NAME	配置名为NAME的PPP Profile，如果不存在该模板，则创建模板
步骤3	echo-time <60-3600>	配置链路活动探测时间，每隔这个时间间隔设备会发送echo request报文检测客户端是否在线，如果超过3个时间间隔客户端没有回应报文，设备强制用户下线
步骤4	write terminal	显示配置

使用 no echo-time 可以取消对链路活动探测时间的设置，使其恢复到缺省配置。echo-time 的缺省值为 60 秒，如果设置的时间太长，则用户异常下线很长时间才能检测到；如果设置的时间太短，则对系统性能有一定影响，因此需要权衡设置。

25.3.6 配置链路空闲时间限制

PPP Profile 中可以设置用户的最大空闲时间限制，如果在设定的时间内没有流量发生，就强制用户下线。默认值为 0，即不限制空闲时间。

配置链路空闲时间限制的步骤:

步骤1	configure terminal	进入全局配置模式
步骤2	subscriber-template ppp NAME	配置名为NAME的PPP Profile，如果不存在该模板，则创建模板
步骤3	idle-time <60-3600>	配置链路空闲时间限制，如果用户超过这

		个时间没有流量发生，设备强制用户下线
步骤4	write terminal	显示配置

25.3.7 配置PPP本地地址

PPP 是点对点连接方式，连接的两端都必须有地址。本地的地址由我们指定，对端的地址通过地址池分配。本地地址和掩码同时确定了对端地址的网段范围，所以配置的地址池都必须在该网段范围内，但是不能包括该地址。

配置 PPP 本地地址的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	ppp-profile NAME	配置名为NAME的PPP Profile，如果不存在该模板，则创建模板
步骤3	address local A.B.C.D/M	指定PPP本地的地址和掩码
步骤4	write terminal	显示配置
步骤5	write memory	保存配置


注意

任意接口地址都不能配置在该网段范围内。

25.3.8 配置动态地址池

如果 PPP 用户端设置为动态获取 IP 地址，则在用户认证通过后，PPP 服务器端将给用户分配一个动态 IP 地址。该地址可以由 PPP 从本地地址池中分配，也可以由 PPP 从指定的 dhcp 服务器或 radius 服务器获取，然后分配给 PPP 用户。

配置动态地址池的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	ppp-profile NAME	配置名为NAME的PPP Profile，如果不存在该模板，则创建模板
步骤3	address pool local <0-255>	指定使用本地IP地址池给客户端分配地址，<0-255>为IP地址池的ID。
步骤4	address pool dhcp	指定使用DHCP 服务器给PPP用户分配地址
步骤5	address pool radius	指定使用radius 服务器给PPP用户分配地址
步骤6	write terminal	显示配置

说明：

- 这三种地址池分配方式是互斥的，只能使用其中一种，而且必须配置其中一种。推荐使用本地地址池分配方式，可以提高系统性能。
- 如果已经配置了一种地址池分配方式，想要改变为另外一种，则必须先删除原有的地址分配方式，才可以配置新的地址分配方式。
- 在配置使用的本地地址池之前必须先配置了 PPP 本地地址，本地地址池必须配置在该本地地址的网段范围内。本地地址池可以配置多个，但是相互之间不能有重叠。删除本地地址池，将导致已经使用该地址的用户下线。
- 配置使用 DHCP 服务器分配地址时，可以使用内置的 DHCP 服务器或者通过 DHCP relay 使用其它网段的 DHCP 服务器，因此必须保证启用了 DHCP 服务器或者 DHCP relay。删除该地址分配方式将导致已经使用该地址池的所有用户下线。
- 配置使用 radius 服务器分配地址时，必须保证使用的 radius 服务器具有地址分配功能。删除该地址分配方式将导致已经使用该地址池的所有用户下线。

25.3.9 配置静态地址池

如果 PPP 用户端设置为使用静态配置的 IP 地址，而且 PPP Profile 配置了静态地址池，则在用户认证通过后，PPP 服务器端将检测用户配置的静态 IP 地址是否在 PPP Profile 配置的静态地址池范围内。如果用户端配置的静态 IP 地址不在静态地址池范围内，或者该地址已经被其他用户使用，则该用户不能上线。

配置静态地址池的步骤:

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	ppp profile NAME	配置名为NAME的PPP Profile，如果不存在该模板，则创建模板
步骤**3**	address pool static <0-255>	指定PPP用户使用静态配置IP地址时，可以使用的地址池
步骤**4**	write terminal	显示配置


注意

1）静态地址池只能配置一个，而且可以与以上的三种动态地址分配方式一起使用，但是不能配置与动态地址池重叠的地址。

2）删除静态地址池，将导致已经使用该地址池的所有用户下线。

25.3.10 配置用户QoS参数

PPP Profile 中可以配置用户的 QoS，对能够与这些设置相匹配的用户作 QoS，对不能与这些设置相匹配的用户不作 QoS。

配置用户 QoS 参数的步骤:

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	ppp-profile NAME	配置名为NAME的PPP Profile，如果不存在该模板，则创建模板
步骤**3**	traffic to id NAME priority <0-7> rate <64-100000>	配置用户的QoS。如果该用户认证成功后，从Radius返回的FilterID属性值和设定的NAME相同，则按照定义的带宽和优先级提供给用户。本命令与下面的traffic to name命令可以同时使用，但本命令具有较高的优先级，即PPP首先按返回的FilterID属性值匹配，如果没有匹配成功的话再按用户名匹配，如果二者都没有匹配成功，则不对用户作QoS。
步骤**4**	traffic to name PATTERN priority <0-7> rate <64-100000>	配置用户的QoS。如果用户名和设定的某个PATTERN模式匹配，则按照定义的带宽和优先级提供给用户。PATTERN为一个模式匹配，即以一个正则表达式来表示一个或一组用户，例如^h代表以h开头，e$代表以e结尾等。本命令与上面的traffic to id命令可以同时使用，但本命令具有较低的优先级，即PPP首先按返回的FilterID属性值匹配，如果没有匹配成功的话再按用户名匹配，如果二者都没有匹配成功，则不对用户作QoS。
步骤**5**	write terminal	显示配置


注意

如果一个用户的用户名以及从Radius服务器返回的FilterID属性都无法匹配您所配置的这些与 QoS 相关命令，那么对该用户不作QoS，该用户可以使用的带宽为该端口下最大带宽。

25.3.11 配置用户名唯一性检测

PPP Profile 中可以限制每个用户名只能建立一个 PPP 连接。默认不限制每个用户名的连接数。

配置用户名唯一性检查的步骤:

步骤1	configure terminal	进入全局配置模式
步骤2	ppp-profile NAME	进入模板配置模式，如果不存在该模板，则会创建该模板
步骤3	unique-user-name	配置用户名唯一性检测
步骤4	write terminal	显示配置


注意

这个命令对系统性能有一定影响，因此缺省配置为不使用这个命令。

25.3.12 配置最大用户数限制

PPP Profile 中可以限制 PPP 用户的最大数目。如果 PPP 用户数达到该限制，将不再接受 PPP 连接请求。默认值为 500。

配置最大回话数限制的步骤:

步骤1	configure terminal	进入全局配置模式
步骤2	ppp-profile NAME	配置名为NAME的PPP Profile，如果不存在该模板，则创建模板
步骤3	max-user <1-8192>	配置最大用户数限制
步骤4	write terminal	显示配置

25.3.13 配置DNS和WINS服务器

PPP Profile 可以配置 PPP 用户使用的 DNS 和 WINS 服务器地址。如果不使用 DHCP 服务器给 PPP 用户分配地址，或者 DHCP 服务器没有配置 DNS 和 WINS 服务器，则 PPP 用户使用 PPP Profile 配置的 DNS 和 WINS 服务器。如果模板配置使用 DHCP 服务器分配地址，而且 DHCP 服务器配置了 DNS 和 WINS 服务器，则 PPP 用户使用 DHCP 服务器指定的 DNS 和 WINS 服务器。

配置 DNS 和 WINS 服务器的步骤:

步骤1	configure terminal	进入全局配置模式
步骤2	subscriber-template ppp NAME	配置名为NAME的PPP Profile，如果不存在该模板，则创建模板
步骤3	dns A.B.C.D [E.F.G.H]	配置PPP用户使用的DNS服务器地址，最多可以配置两个
步骤4	wins A.B.C.D [E.F.G.H]	配置PPP用户使用的WINS服务器地址，最多可以配置两个

步骤5	write terminal	显示配置


注意

如果没有设置 DNS 或 WINS 服务器地址，PPP 用户可能无法解析域名导致无法上网。

25.4 PPP Profile配置管理命令

图25-2 PPP Profile 配置管理命令列表

命令	解释
show ppp-profile [NAME]	显示配置的PPP Profile
show ppp user [NAME]	显示PPP用户的详细信息，NAME为用户名
show ppp interface <0-8191>	显示PPP虚拟接口下用户的详细信息
show ppp summary	显示所有PPP用户的概要信息
show ppp total	显示总的PPP用户数
clear ppp user [NAME]	强制清除指定的PPP用户，NAME为用户名。清除PPP用户，将导致对应的PPPoE或L2TP会话关闭。
clear ppp interface <0-8191>	强制清除指定PPP虚拟设备对应的PPP用户，<0-8191>为PPP虚拟设备号。清除PPP用户，将导致对应的PPPoE或L2TP会话关闭。

25.4.2 显示信息举例

举例 1：

步骤1	show ppp-profile命令显示举例
	SmartHammer # show ppp-profile test ppp-profile test aaa-group local authentication pap address local 172.16.16.2/16 address pool local 172.16.16.10 500 echo-time 60 account-interval 60 max-session 8000 dns 10.1.1.1 wins 10.1.1.1 !

举例 2：

步骤1	show ppp user命令显示举例

```
SmartHammer # show ppp user z13
=========================================================
  UserName :      z13
  Interface   :   ppp0
  StartTime :     Sun Apr 24 14:31:19 2005
  StandTime :     11323
  IPAddress :     172.16.0.8
  BytesOut :      309013                    BytesIn :     13588
  PPP profile   :     test
  Protocol Type :     pppoe
=========================================================
```

举例 3：

步骤**1** show ppp summary命令显示举例

```
SmartHammer # show ppp summary
Username      Interface      IPAddress      StandTime     ProtoType
=========================================================
z11           ppp10          172.16.0.8     11497         pppoe
z12           ppp11          172.16.0.9     11497         pppoe
z13           ppp12          172.16.0.10    11497         l2tp
=========================================================
Total Users:   3
```

25.4.3 强制清除举例

举例 1：

步骤**1** clear ppp user命令举例

```
Router# clear ppp user z4
=========================================================
Total clear users:      1
```

举例 2：

步骤**1** clear ppp interface命令举例

```
Router# clear ppp interface 0
=========================================================
Total clear users:      1
```

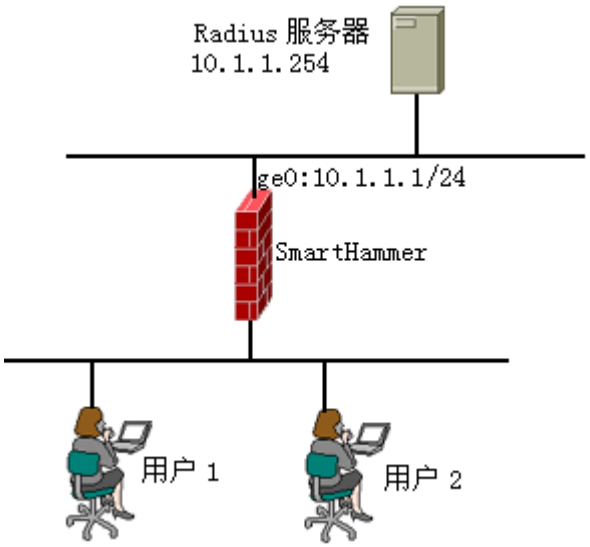
25.5 配置案例

案例描述:

在 SmartHammer 设备的 ge1 接口（不要配置 IP 地址）上启动 PPPoE 接入认证，使用 Radius 服务器认证和计费。

使用 SmartHammer 设备进行认证的用户同属于一个 ISP，他们都使用相同的 Radius 认证和计费服务器，Radius 服务器（10.1.1.254）与 SmartHammer 设备的 ge0 接口相连。

图25-3 PPP Profile 配置案例组网图



配置步骤：

步骤**1**	配置AAA认证和计费模板，采用RADIUS认证和计费方式
	SmartHammer# configure terminal SmartHammer (config)# aaa pppoe SmartHammer (config-aaa)# authentication server 10.1.1.254 1812 88--99 SmartHammer (config-aaa)# accounting server 10.1.1.254 1813 88--99 SmartHammer (config-aaa)# source-ip 10.1.1.1 SmartHammer (config-aaa)# exit
步骤**2**	配置本地地址池范围
	SmartHammer# configure terminal SmartHammer (config)# ip pool 0 192.168.0.2 1000
步骤**3**	配置PPP profile

	SmartHammer (config)# ppp-profile hammer SmartHammer (config-ppp)# aaa-group pppoe SmartHammer (config-ppp)# address local 192.168.0.1/16 SmartHammer (config-ppp)# address pool local 0 SmartHammer (config-ppp)# echo-time 60 SmartHammer (config-ppp)# accounting-interval 120 SmartHammer (config-ppp)# authentication chap SmartHammer (config-ppp)# max-user 1000 SmartHammer (config-ppp)# dns 10.1.0.1 10.1.0.4 SmartHammer (config-ppp)# wins 10.1.0.1 10.1.0.4 SmartHammer (config-ppp)# exit
步骤**4**	配置PPPoE接入认证模板
	参见PPPoE配置部分。
步骤**5**	在接口上启用PPPoE接入认证
	参见PPPoE配置部分。

25.6 常见故障

在 SmartHammer 设备中，PPP Profile 是被 L2TP 和 PPPoE 使用，因此故障分析要先确定不是 L2TP 或 PPPoE 模块的问题，然后再确定是不是 PPP 的故障。

25.6.1 PPP用户无法上线

故障现象	PPP用户无法上线
分析与解决	有可能是以下几种情况导致用户无法上线（可以使用debug ppp命令查看出错信息） 1）用户名密码错误：您可以确认一下用户名和密码。 2）PPP用户数是否已达到最大值：使用show ppp total命令查看总的PPP用户数。 3）配置的地址池是否已经用完。 4）如果采用Radius服务器认证，检查SmartHammer设备是否可达Radius认证服务器，Radius认证服务是否已启动。 5）是否在Radius认证服务器上配置了正确的NAS地址 6）配置的AAA认证和计费模板是否正确

25.6.2 PPP用户异常下线

故障现象	PPP用户异常下线
分析与解决	有可能是以下几种情况导致PPP用户异常下线（可以使用debug ppp命令查看出错信息） 1）使用Radius服务器计费，计费错误。用户上线后发送的开始计费请求报文，或者是用户的间歇计费请求报文，没有得到Radius计费服务器的回应，都会导致用户下线。您需要确认：

	SmartHammer设备是否可达Radius认证服务器 Radius认证服务是否已启动 是否在Radius认证服务器上配置了正确的NAS地址 您配置的AAA认证和计费模板是否正确 2）是否设置了idle-time导致由于用户在一段时间内没有流量，SmartHammer设备强制用户下线 3）由于网络故障导致lcp echo request报文没有应答，SmartHammer设备强制用户下线，请确认SmartHammer设备与用户之间网络可达 4）如果PPP profile中配置使用DHCP地址池，可能是DHCP 地址续租失败，导致关闭PPP会话。请确认到DHCP server之间可达，而且DHCP server的地址池没有用完。

25.6.3 用户端显示已上线但是上不了网

故障现象	用户端显示已上线但是上不了网
分析与解决	有可能是以下几种情况引起（可以使用debug ppp命令查看出错信息） 1）没有设置DNS和WINS服务器，导致无法解析域名，而不能上网。 2）客户端软件故障，地址没有获取到或者默认路由没有添加上。如果使用的是L2TP拨号软件，可以查看L2TP客户端的L2TP虚拟网卡是否获取到了地址，默认路由是否指向L2TP虚拟网卡。可以重新认证一次，如果还是不行，则需要重新安装客户端。

25.7 常用调试功能

PPP 的调试命令包括：

- debug ppp lcp 显示 LCP 阶段的关键事件和错误信息
- debug ppp auth 显示认证阶段的关键事件和错误信息
- debug ppp ipcp 显示 IPCP 阶段的关键事件和错误信息
- debug ppp acct 显示计费阶段的关键事件和错误信息
- debug ppp dhcp 显示 DHCP 分配地址阶段的关键事件和错误信息
- debug ppp packet 显示接收和发送的所有 PPP 报文内容
- debug ppp 显示以上所有阶段的调试信息

25.7.1 debug ppp

应用环境：

当 PPPoE 或 L2TP 客户端无法正常上线时，已经用 debug pppoe 或 debug l2tp 排除 PPPoE 或 L2TP 阶段的问题，需要查看 PPP 阶段的信息。(为了在终端显示该调试信息，需要执行命令 terminal monitor)

调试实例：

```
SmartHammer# debug ppp
SmartHammer# terminal moniter
<HARBOUR><2005-03-24 18:04:47><Harbour><PPP><DEBUG><PPP started for
PPPOE session: 31504>
<HARBOUR><2005-03-24 18:04:47><Harbour><PPP><DEBUG><Create interface
ppp0>
<HARBOUR><2005-03-24 18:04:47><Harbour><PPP><DEBUG><sent [LCP
ConfReq id=0x1 <auth pap> <magic 0xc13ac301>]>
<HARBOUR><2005-03-24 18:04:47><Harbour><PPP><DEBUG><Recv [LCP
ConfReq id=0x0 <magic 0x3838733a>] >
<HARBOUR><2005-03-24 18:04:47><Harbour><PPP><DEBUG><sent [LCP ConfAck
id=0x0 <magic 0x3838733a>]>
<HARBOUR><2005-03-24 18:04:47><Harbour><PPP><DEBUG><Recv [LCP
ConfAck id=0x1 <auth pap> <magic 0xc13ac301>] >
<HARBOUR><2005-03-24 18:04:47><Harbour><PPP><DEBUG><sent [LCP
EchoReq id=0x0 magic=0xc13ac301]>
<HARBOUR><2005-03-24 18:04:47><Harbour><PPP><DEBUG><Recv [PAP
AuthReq id=0x3 user="z123" password=<hidden>] >
<HARBOUR><2005-03-24 18:04:47><Harbour><PPP><DEBUG><sent [PAP AuthNak
id=0x3 "Login incorrect"]>
<HARBOUR><2005-03-24 18:04:47><Harbour><PPP><DEBUG><AUTH failed>
<HARBOUR><2005-03-24 18:04:47><Harbour><PPP><DEBUG><sent [LCP
TermReq id=0x2 "Authentication failed"]>
<HARBOUR><2005-03-24 18:04:47><Harbour><PPP><DEBUG><Recv [LCP
EchoRep id=0x0 magic=0x3838733a] >
<HARBOUR><2005-03-24 18:04:47><Harbour><PPP><DEBUG><Recv [LCP
TermAck id=0x2 "Authentication failed"] >
```

结果分析：

从以上结果可以看出，由于用户认证失败，所以不能上线。

注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug ppp 命令禁用此功能。

26 配置 PPPoE 认证

本章涉及 PPPoE 接入认证模板的配置，内容主要包括：

- PPPoE 接入认证功能概述
- 配置 PPPoE 接入认证模板
- 在端口启用 PPPoE 接入认证模板

26.1 PPPoE概述

PPPoE（PPP over Ethernet）是一种在以太网络中传输 PPP 帧信息的技术。它通过把最经济的局域网技术以太网和点对点协议的可扩展性及管理控制功能结合在一起，使网络服务提供商和电信运营商能够利用可靠和熟悉的技术来加速部署高速互联网业务。

PPPoE 协议提供了将广播式网络中的多台主机连接到访问集中器（AC）的一种标准，它利用 PPP 协议栈本身所具有的特点，实现在广播式网络上对用户进行计费和管理。在这种网络模型中，每一个主机使用自己的 PPP 协议栈，呈现给用户的还是熟悉的用户接口，而且访问控制、支付以及服务类型都能基于每一个用户。SmartHammer 设备支持 PPPoE 宽带拨号协议，可以实现接入带宽限制，并可以根据时间、流量进行实时计费。

PPPoE 协议共包括两个阶段：PPPoE 的发现阶段（PPPoE Discovery Stage）和 PPPoE 的会话阶段（PPPoE Session Stage）。PPPoE 发现阶段用于进行 PPPoE 协商，建立 PPPoE 会话；PPPoE 会话阶段，则只是在 PPPoE 帧中封装了 PPP 帧，用来在以太网上传输 PPP 会话。

26.2 配置PPPoE模板

26.2.1 缺省配置

表26-1 PPPoE 接入认证模板的缺省设置信息：

内容	缺省设置	备注
MAC地址唯一性检测 (unique-mac)	不启用	可更改设置
PPPoE接入服务器名 (acname)	主机名	可更改设置
PPPoE强制推送网页 (hurl)	不启用	可更改设置
端口下的最大连接数 (max-session)	500	可更改设置

26.2.2 配置使用的PPP Profile

PPPoE 协议的目的就是在以太网上传输 PPP 会话，因此必须要有 PPP 的支持。PPPoE 模板中所使用的 PPP 相关的参数在 PPP profile 中配置。PPP profile 的详细配置参见“PPP Profie 配置”部分。

配置 PPPoE 模板使用的 PPP profile 的步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	subscriber-template pppoe NAME	配置名为NAME的PPPoE模板，如果不存在该模板，则创建模板
步骤**3**	ppp profle NAME	配置使用的PPP profle
步骤**4**	write terminal	显示配置


注意

1)在 PPPoE 模板下必须要配置 PPP profile，否则 PPPoE 模板不能启用。如果 PPPoE 模板已经启用，则不能修改和删除它的 PPP prfile。

2)在一个 PPPoE 模板下只可以配置一个 PPP profile。

请详细参考“PPP profile 配置”部分。

26.2.3 配置PPPoE接入服务器名

PPPoE 接入服务器名唯一地标志某个特定的接入服务器。PADO 报文中必须包含 PPPoE 接入服务器名，以供 PPPoE 客户端选择。

配置 PPPoE 接入服务器名的步骤:

步骤1	configure terminal	进入全局配置模式
步骤2	subscriber-template pppoe NAME	配置名为NAME的PPPoE接入认证模板，如果不存在该模板，则创建该模板
步骤3	acname NAME	配置PPPoE接入服务器名
步骤4	write terminal	显示配置

使用 no acname NAME 可以取消对 PPPoE 接入服务器名的设置，使其恢复到缺省配置。PPPoE 接入服务器名的缺省值为防火墙的主机名。

26.2.4 配置PPPoE服务

PPPoE 服务用来表示 PPPoE 服务器提供的服务类型。在 PADO 和 PADR 报文中都必须包含 PPPoE 服务。

配置 PPPoE 服务的步骤:

步骤1	configure terminal	进入全局配置模式
步骤2	subscriber-template pppoe NAME	配置名为NAME的PPPoE接入认证模板，如果不存在该模板，则创建该模板
步骤3	service WORD	配置PPPoE服务
步骤4	write terminal	显示配置

使用 no service WORD 可以删除配置的 PPPoE 服务。PPPoE 服务没有默认配置，因此必须在 PPPoE 模板下配置 PPPoE 服务。

26.2.5 配置PPPoE强制推送网页

PPPoE 服务器端可以通过 PADM 报文，在用户上线时给他推送一个指定的网页。该特性是 PPPoE 扩展特性，如果客户端不支持该特性，则不会显示该网页。

配置 PPPoE 强制推送网页的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	subscriber-template pppoe NAME	配置名为NAME的PPPoE接入认证模板，如果不存在该模板，则创建该模板
步骤3	hurl WORD	配置PPPoE强制推送网页，WORD为以 http:// 开头的网页地址
步骤4	write terminal	显示配置

26.2.6 配置MAC地址唯一性检测

PPPoE 认证方式下可以配置对 MAC 地址唯一性进行检测。如果配置了对 MAC 地址唯一性进行检测，则同一个 MAC 地址只允许一个 PPPoE 连接。

配置 MAC 地址唯一性检测的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	subscriber-template pppoe NAME	进入模板配置模式，如果不存在该模板，则会创建该模板
步骤3	unique-mac	配置MAC地址唯一性检测
步骤4	write terminal	显示配置

注意

执行 no unique-mac 可以取消对 mac 地址唯一性的设置，使其恢复到缺省配置。

该配置对系统性能有一定影响，因此缺省配置为不使用该配置。

26.3 在接口启用PPPoE接入认证

配置完一个 PPPoE 接入认证模板后，必须要在 SmartHammer 设备的某一个接口上启用它，才可以开启 PPPoE 接入认证功能。

用户可以配置多个 PPPoE 接入认证模板，但在一个接口下一次只可以启用一个 PPPoE 接入认证模板。

在端口上启用 PPPoE 接入认证服务的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入接口配置模式
步骤3	pppoe subscriber-template NAME	在接口上启用PPPoE接入认证
步骤4	pppoe max-session <1-8191>	限制该接口下的最大连接数
步骤5	write terminal	显示配置


注意

1）用户可以配置多个 PPPoE 接入认证模板，但在一个接口下一次只可以启用一个 PPPoE 接入认证模板。

2）用户必须通过可以透传 PPPoE 报文的二层交换机接入 SmartHammer 设备，而不能通过三层交换机接入，因为 PADI 报文是二层广播包。

3）在启用 PPPoE 的接口上，不要配置 IP 地址，否则用户可能不用认证就可以直接访问。

26.4 配置信息显示命令

表26-2 PPPoE 接入认证配置信息显示命令列表：

命令	解释
show pppoe interface [IFNAME]	显示启用PPPoE接入认证的接口信息，IFNAME用于指定显示的接口名
show pppoe subscribe-template [NAME]	显示PPPoE接入认证模板信息，NAME用于指定显示的模板
show pppoe session	显示所有PPPoE连接的信息
show memory pppoe	显示PPPoE接入认证内存使用情况（供高级用户分析故障使用）

show pppoe interface 命令显示举例：

```
SmartHammer # show pppoe interface
============================================================
interface   ge2
<up>
<enable pppoe>
Subscriber Template Name   :   test
Max Session                :   500
Session Num                :   100
============================================================
```

show pppoe subscribe-template 命令显示举例：

```
SmartHammer # show pppoe subscribe-template test
subscriber-template pppoe test
ppp profile test
hurl http://www.harbournetworks.com
acname harbour
service pppoe
!
```

show pppoe session 命令显示举例：

```
SmartHammer# show pppoe session
SessID          MAC Address          Interface        State
============================================================
  9485      00:08:74:d9:9b:0f            ge0       ESTABLISHTED
============================================================
Total Sessions:      1
```

26.5 配置案例

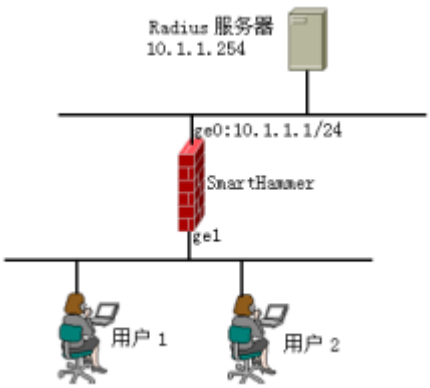
26.5.1 所有用户属于同一个ISP

案例描述：

在 SmartHammer 设备的 ge1 接口（不要配置 IP 地址）上启动 PPPoE 接入认证，使用 Radius 服务器认证和计费。

使用 SmartHammer 设备上进行认证的用户同属于一个 ISP，他们都使用相同的 Radius 认证和计费服务器，Radius 服务器（10.1.1.254）与 SmartHammer 设备的 ge0 接口相连。

图26-1 所有用户属于同一个 ISP 配置案例组网图



配置步骤：

步骤**1**	配置AAA认证和计费模板
	SmartHammer# configure terminal SmartHammer (config)# aaa pppoe

	SmartHammer (config-aaa)# authentication server 10.1.1.254 1812 88--99 SmartHammer (config-aaa)# accounting server 10.1.1.254 1813 88--99 SmartHammer (config-aaa)# source-ip 10.1.1.1 SmartHammer (config-aaa)# exit
步骤**2**	配置本地IP地址池范围
	SmartHammer (config)# ip pool 0 192.168.0.2 1000
步骤**3**	配置PPP profile
	SmartHammer (config)# ppp-profile hammer SmartHammer (config-ppp)# aaa-group pppoe SmartHammer (config-ppp)# address local 192.168.0.1/16 SmartHammer (config-ppp)# address pool local 0 SmartHammer (config-ppp)# echo-time 60 SmartHammer (config-ppp)# accounting-interval 120 SmartHammer (config-ppp)# authentication chap SmartHammer (config-ppp)# max-user 1000 SmartHammer (config-ppp)# dns 10.1.0.4 10.1.0.4 SmartHammer (config-ppp)# wins 10.1.0.4 10.1.0.4 SmartHammer (config-ppp)# exit
步骤**4**	配置PPPoE接入认证模板
	SmartHammer (config)# subscriber-template pppoe hammer SmartHammer (config-sub)# ppp profile pppoe SmartHammer (config-sub)# acname firewall SmartHammer (config-sub)# service pppoe SmartHammer (config-sub)# hurl http://www.harbournetworks.com
步骤**5**	在接口上启用PPPoE接入认证，并限制该端口下最大连接数为2000
	SmartHammer (config)# interface ge0 SmartHammer (config-if)# pppoe subscriber-template hammer SmartHammer (config-if)# pppoe max-session 2000 SmartHammer (config-if)# exit
步骤**6**	保存配置
	SmartHammer (config)# write memory

26.6 故障分析

26.6.1 PPPoE用户无法上线

故障现象：用户无法上线

分析与解决：

有可能是以下几种情况导致用户无法上线（您可以使用 debug pppoe session 和 debug pppoe packet 命令查看出错原因）

- 用户接入的交换机是否是可以透传 PPPoE 报文的二层交换机，否则认证报文无法通过交换机到达 SmartHammer 设备，可以使用 debug pppoe packet 命令查看是否收到了客户端的 PPPoE 报文。

- 启用 PPPoE 认证服务的接口状态是否 up，该接口是否能 ping 通。可以使用 show pppoe interface 查看启用 PPPoE 服务的接口状态。
- 该接口下的 PPPoE 连接数是否已达到最大值。可以使用 show pppoe interface 命令查看该接口的连接数和最大限制连接数。还可以使用 debug pppoe session 查看连接过程中的关键事件和错误信息。
- 如果 pppoe 连接过程正常，但是用户还是上不了线，则可能是 ppp 连接过程中出错。可以使用 debug ppp 查看 ppp 连接过程的关键事件和出错信息。（请参考“配置 ppp profile”部分的故障分析）
- 检查用户名和密码输入是否正确。
- 如果采用 Radius 服务器认证，检查 SmartHammer 设备是否可达 Radius 认证服务器，以及 Radius 认证服务器上是否启动了 Radius 认证服务。
- 是否在 Radius 认证服务器上配置了正确的接入服务器地址。
- 配置的 AAA 认证和计费模板是否正确（请参考 AAA 系统配置的故障分析）

26.6.2 用户异常下线

故障现象：用户异常下线

分析与解决：

有可能是以下几种情况导致用户异常下线（您可以使用 debug pppoe 命令查看出错原因）

- 使用 Radius 服务器计费，计费错误。用户上线后发送的开始计费请求报文，或者是用户的间歇计费请求报文，没有得到 Radius 计费服务器的回应，都会导致用户下线。您需要确认：
- SmartHammer 设备是否可达 Radius 认证服务器
- Radius 认证服务是否已启动
- 是否在 Radius 认证服务器上配置了正确的 NAS 地址
- 您配置的 AAA 认证和计费模板是否正确（请参考第十一部分的故障分析）。
- 是否由于您在 ppp profile 中设置了 idle-time 导致由于用户在一段时间内没有流量，SmartHammer 设备强制用户下线。
- 由于网络故障导致 lcp echo request 报文没有应答，SmartHammer 设备强制用户下线，请确认 SmartHammer 设备与用户之间网络可达。

26.7 常用调试功能

PPPoE 的调试命令包括：

- debug pppoe discovery 显示 PPPoE discovery 阶段的关键事件和错误信息
- debug pppoe packet 显示接收和发送的所有报文
- debug pppoe 显示以上所有的调试信息

26.7.1 debug pppoe

应用环境：

当接入用户无法正常上线时，查看用户上线阶段的信息。(为了在终端显示该调试信息，需要执行命令 terminal monitor)

调试实例：

```
SmartHammer# debug pppoe
SmartHammer# terminal moniter
<HARBOUR><2005-03-24 15:10:22><Harbour><PPPOE><DEBUG> Recv PADI
<HARBOUR><2005-03-24 15:10:22><Harbour><PPPOE><DEBUG> Recv  PADI:
exceed max session
```

结果分析：

显示收到了接入用户的 PADI 报文

但是会话数已经达到了接口设置的最大会话数限制，所以用户不能上线。

注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug pppoe 命令禁用此功能。

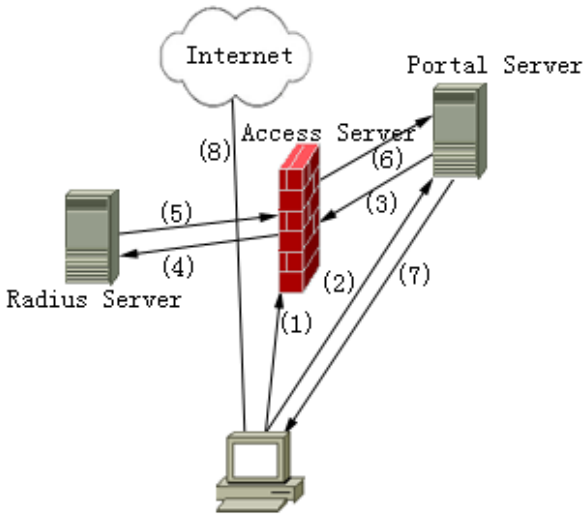
27 配置 WEB/Portal 认证

Web/Portal 认证是基于 HTTP 协议的认证方式，客户端不需安装任何软件，使用 Web 浏览器就可以进行认证，极大地方便了设备的安装实施。采用 Web/Portal 认证，可以为用户提供基于时间和流量的计费方式，提供基于用户的带宽管理和有效性检测。

27.1 WEB/Portal认证概述

Web/Portal 认证是通过 HTTP 协议进行认证，参与认证的功能部件主要有三个：Access Server、Portal Server 和认证服务器，三个部分可作为独立的设备，也可集成到同一个设备上。SmartHammer 设备集成了 Access Server 和 Portal Server，并提供内置的帐号认证方式。

图27-1 认证流程图



（1）用户对外访问

（2）用户访问重定向至 Portal Server

（3）Portal Server 向 Access Server 请求认证

（4）Access Server 向认证服务器请求认证

（5）认证服务器向 Access Server 返回认证结果

（6）Access Server 向 Portal Server 返回认证结果

（7）Portal Server 向用户返回认证结果

27.2 配置Web/Portal认证

27.2.1 缺省配置

表27-1 SmartHammer 设备 Web/Portal 认证的缺省设置信息

内容	缺省设置	备注
空闲检测（idle-time）	off	可更改设置
用户唯一性限制（unique-verify）	off	可更改设置
认证方式（authentification）	chap	可更改设置
用户在线检测间隔（keep-alive）	off	建议设置
访问控制服务器（access-server A.B.C.D default)	127.0.0.1	可更改设置
认证后弹出的第一个Web页面（portal-url URL）	off	可更改设置
Web认证接入用户数（webauth max-session <1-8000>）	4000	可更改设置

27.2.2 配置Portal Server

Portal Server 提供用户接入认证的 Web 接口。Portal Server 维护用户在线信息，并与提供访问控制功能的 Access Server 交互，进行认证。Portal Server 的具体功能和作用参见概述中的认证流程图。

配置 Portal Server 的步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	portal-server	配置Portal Server
步骤**3**	access-server A.B.C.D default	配置Access-server的地址，当Loopback地址没有配置时，此命令不用配置，缺省为127.0.0.1
步骤**4**	authentification (pap|chap)	配置Web认证方式，缺省为CHAP

步骤5	keep-alive <30-600>	配置异常下线检测间隔
步骤6	portal-url URL	配置认证后弹出的第一个Web页面的URL，可以不配置
步骤7	(background-page|popup-page) FILE	配置portal页面的背景图片（可不配）
步骤8	exit	退出配置模式
步骤9	show portal server	查看Portal Server配置


注意

1）如果 Loopback 地址改变了，必须配置 Access-server 的地址为这个 Loopback 的地址或设备上任何一个有效地址;

2）如果不配置 keep-alive，则不对用户的异常下线情况进行检测，当用户与设备连接的线路出现问题，用户不能正常下线，则用户仍然会保持在线状况。在按时长计费的情况下会导致异常费用问题，因此建议用户设置 keep-alive。

3）如果配置了自适应安全过滤，应允许用户访问 Portal Server 的 http 认证端口。

27.2.3 配置AAA模板

配置认证服务模板，具体参见 AAA 系统配置部分

27.2.4 配置web认证模板

配置 Web 认证模板，指定 Web 认证方式和参数。启用了 Web 认证功能的设备作为一个 Access Server，与 Portal Server 结合，提供 Web/Portal 认证功能。

配置 web 认证模板的步骤：

步骤1	configure terminal	进入配置模式
步骤2	subscriber-template webauth NAME	配置名为NAME的Web认证模板，如果不存在该模板，则创建模板
步骤3	aaa-group NAME [by GROUP]	配置使用的AAA认证和计费模板（详见第十一部分）。by GROUP用于设定使用该AAA模板的用户组.
步骤4	accounting-interval <1-10000>	配置间歇计费间隔，可以不配，默认情况下不发送间歇计费
步骤5	authentication-url URL	配置Web认证页面的URL，用户可在此页面输入用户名和密码进行认证，内置Portal Server的Web认证页面URL为http://xx.xx.xx.xx/index.html（类似的具体内容放到表格外面介

		绍）
步骤**6**	dns-server A.B.C.D	配置dns-server，在用户未认证情况下，发往这个地址的数据包允许通过
步骤**7**	idle-time <60-3600>	配置用户最大闲置时间，这个时间内没有流量，则强制用户下线
步骤**8**	unique-verify	如果要求用户唯一性，则配置则命令
步骤**9**	exit	退出配置模式
步骤**10**	show webauth subscriber-template [template-name]	显示配置的模板信息
步骤**11**	Show webauth summary	查看Web模板配置
步骤**12**	write memory	保存配置


注意

DNS Server 必须配置，否则对于使用域名的 URL 请求，未认证前不会进行 URL 重定向。

设置了模板，并没有启用 Web/Portal 认证

27.2.5 在接口上启用Web认证

配置了 Web 认证模块后，Web 认证功能并没有启用，Web 认证功能的启用基于接口，需要在接口上配置

在接口上启用 Web 认证的步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	interface NAME	进入interface配置模式
步骤**3**	webauth subscriber-template WORD	启用Web模板，WORD是模板名，必须先配置好Web模板，然后再启用。
步骤**4**	show webauth interface [IFNAME]	显示Web认证的配置情况


注意

如启用了安全自适应过滤，则必须允许用户访问设备的 8082 端口，8082 端口是 Web/Portal 认证的 URL 重定向服务端口，用户在未认证前对于任何 IP 地址或域名的访问都由设备的 8082 端口提供 URL 重定向服务。另外，必须允许设备访问认证服务器的认证端口，必须允许用户访问 DNS Server 的 DNS 服务端口。

27.2.6 配置在线用户数限制

在接口上配置最大在线用户数。

在接口上配置最大在线用户数的步骤：

步骤1	configure terminal	进入配置模式
步骤2	Interface NAME	进入interface配置模式
步骤3	webauth max-session <1-8000>	配置最大在线用户数，只有Web模板启用，此命令才有意义。缺省为4000用户。
步骤4	show webauth interface [IFNAME]	显示Web认证的配置情况

27.2.7 配置免认证IP

在接口上配置免认证 IP，这些 IP 可以不通过认证就可以通过这个接口对外访问。

配置免认证 IP 有两种方式，第一种使用 IP/MAC 绑定，对匹配 IP 且 IP/MAC 校验无误的用户免认证。第二种使用 access-list，对匹配 access-list 的用户免认证，这种方式比较灵活，但不能对 MAC 进行校验。

采用 IP/MAC 绑定方式配置免认证 IP 的步骤：

步骤1	configure terminal	进入配置模式
步骤2	Interface NAME	进入interface配置模式
步骤3	webauth authorize A.B.C.D MAC	配置免认证IP，与MAC进行绑定，在访问时进行IP、MAC校验 此命令必须在启用Web认证后才生效
步骤4	show webauth interface [IFNAME]	显示Web认证的配置情况

采用 access-list 方式配置免认证 IP 的步骤：

步骤1	configure terminal	进入配置模式
步骤2	Interface NAME	进入interface配置模式
步骤3	webauth authorize filter (<1-99>|<100-199> |<1300-1999>|<2000-2699>)	配置免认证IP，匹配access-list的用户免认证 此命令必须在启用Web认证后才生效
步骤4	show webauth interface [IFNAME]	显示Web认证的配置情况

注意

必须配置 Web 认证后此命令才生效。

对于免认证用户，如果自行认证后使用网络，仍然会按照认证用户进行计费。

27.3 配置信息显示命令

表27-2 Web/Portal 认证配置信息显示命令

命令	解释
show webauth summary	显示Web认证的概要信息
show webauth subscriber-template [template-name]	显示Web/protal认证模板信息，template-name用于指定显示的模板
show webauth interface [IFNAME]	显示启用Web/Portal接入认证的端口信息，IFNAME用于指定显示的端口名
show webauth user [USER]	显示Web/Portal认证上线用户信息，USER用于指定显示用户的用户名
show webauth regex_user [USER]	显示Web/Portal认证上线用户信息，USER用于指定显示用户的用户名，是一个正则表达式，例如^h代表以h开头，e$代表以e结尾等。
show portal-server	显示Portal Server的配置信息

27.4 配置案例

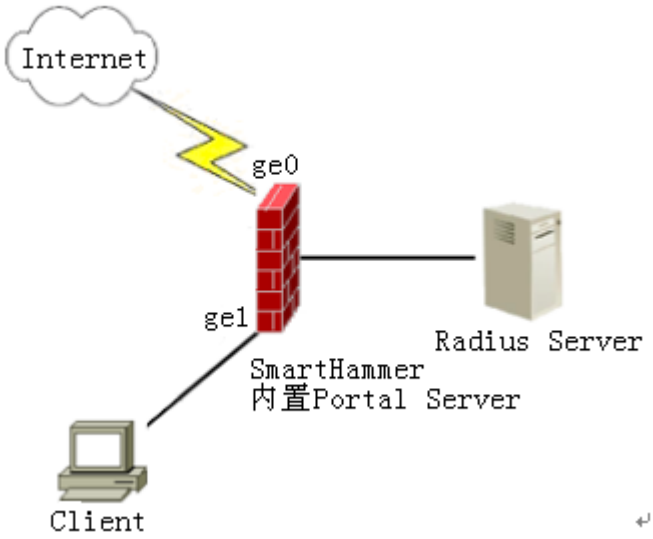
27.4.1 配置Web/Portal认证，使用内置Portal Server

案例描述：

配置 Web/Portal 认证，使 ge1 接入的用户必须经过 Web 认证才能够访问 Internet，Internet 从 ge0 接口接入。配置 Web/Portal 认证，需要配置 Portal server、Web 认证模板、AAA 模板，并在接口上进行启用。案例描述不清楚，想实现什么功能？需要配置哪些参数等。

配置 Web/Portal 认证，用户从 ge1 接入，ge0 上行接入 Internet。

图27-2 Web/Portal 认证配置案例组网图



配置步骤：

步骤**1**	配置Portal Server，并配置keep-alive和portal-url
	SmartHammer#configure terminal SmartHammer(config)#portal-server SmartHammer(config-portal-server)#keep-alive 60 SmartHammer(config-portal-server)#portal-url http://www.google.com/ SmartHammer(config-portal-server)#exit
步骤**2**	配置AAA模板，名字为radius-a，具体配置详见AAA系统配置
	SmartHammer(config)#aaa radius-a SmartHammer(config-aaa)#authentication server 1.1.1.8 1812 harbour SmartHammer(config-aaa)#accounting server 1.1.1.8 1813 harbour SmartHammer(config-aaa)#source-ip 1.1.1.1 SmartHammer(config-aaa)#exit
步骤**3**	配置Web认证模板，名字为web-a
	SmartHammer(config)#subscriber-template webauth web-a SmartHammer(config-sub)#aaa-group radius-a SmartHammer(config-sub)#accounting-interval 60 SmartHammer(config-sub)#dns-server 1.1.1.4 SmartHammer(config-sub)#idle-time 100 SmartHammer(config-sub)#authentication-url http://2.2.2.2/index.html SmartHammer(config-sub)#exit
步骤**4**	在接口上启用Web认证

```
SmartHammer(config)#interface ge1
SmartHammer(config-if)#webauth subscriber-template web-a
SmartHammer(config-if)#webauth max-session 2000
SmartHammer(config-if)#webauth authorize 2.2.2.10 00:0C:04:0A:3E:E4
SmartHammer(config-if)#exit
```

27.5 故障分析

27.5.1 输入域名无法弹出认证页面

故障现象	在浏览器输入域名形式的URL无法弹出认证页面，但输入IP形式的URL却可以弹出认证页面。
分析与解决	不能正确解析域名服务，原因有几个： 1）Web模板中的DNS Server没有配置或配置错误； 2）取消Web认证，确认是否能正常访问域名服务器，如不能，则必须先配置好域名服务器并能成功访问； 3）查看客户端的地址方配方式，是静态还是动态。如使用静态地址分配，则用户端设置的DNS Server有可能不正确；如使用动态地址分配，则DHCP Server配置中的DNS Server设置可能不正确；

27.5.2 只有输入设备本身地址的URL才能弹出认证页面

故障现象	输入设备地址上的URL可以弹出认证页面，但输入公有地址URL和域名URL却无法弹出URL
分析与解决	有两种可能的原因： 没有配置缺省路由或者域名服务器配置不正确

27.5.3 认证失败

故障现象	认证方式为radius，认证失败
分析与解决	将认证方式改为本地认证，看是否成功，如成功，则表明 radius 配置有问题，否则，查看是否配置了安全自适应过滤，必要的端口（设备的 8082 端口，Portal Server 的 http 认证端口，DNS Server 的 DNS 服务端口，认证服务器的认证端口）是否允许访问。 或抓包，检查认证数据包是否正确返回。 如Loopback接口上配置了127.0.0.1之外的地址，则在Portal Server模式下使用Access-server指令，配置Access-server的地址，配置为Loopback地址即可。

27.6 常用调试功能

27.6.1 debug webauth

应用环境：

当用户使用 Web/Portal 认证，输入了正确的用户名和密码仍然不能认证成功时，使用此命令定位出错的地方。**此命令与 debug Portal 结合使用**。为了在终端显示该调试信息，需要执行命令 terminal monitor。

调试实例：

实例**1**	用户认证上线
	Feb 9 11:23:22 (none) webauth[234]: portalsv, receive req_auth msg from portal Feb 9 11:23:22 (none) webauth[234]: portalsv, get ackrequest msg from portal Feb 9 11:23:22 (none) webauth[234]: IP TO DEV into ip address = b400a8c0 Feb 9 11:23:22 (none) webauth[234]: inerface name ge0 Feb 9 11:23:22 (none) webauth[234]: IP TO DEV ret=0, ifname=ge0, ifindex=2 Feb 9 11:23:22 (none) webauth[234]: portalsv, get interface by ip, ge0 Feb 9 11:23:22 (none) webauth[234]: get mac:00:01:40:55:84:DF Feb 9 11:23:22 (none) webauth[234]: usr_table, user login, user=lsh,ip=3019942080,snid=IREoWkMBVAI0MSdKLQJh Feb 9 11:23:22 (none) webauth[234]: SET USER FLAG IN Feb 9 11:23:22 (none) webauth[234]: usr_table, traffic limit may not be set, ret = -1 Feb 9 11:23:22 (none) webauth[234]: usr_table, user login success, user = lsh Feb 9 11:23:22 (none) webauth[234]: portalsv, send authmsg to portal: result len = 16

	Feb 9 11:23:22 (none) webauth[234]: portalsv, receive req_ackauth msg from portal Feb 9 11:23:22 (none) webauth[234]: portalsv, send ack_ackauth msg to portal
实例**2**	用户下线流程
	Feb 9 11:27:26 (none) webauth[234]: portalsv, receive req_logoff msg from portal Feb 9 11:27:26 (none) webauth[234]: usr_table, user logout, user=,ip=3019942080,snid= Feb 9 11:27:26 (none) webauth[234]: usr_table, user logout success, user = lsh Feb 9 11:27:26 (none) webauth[234]: portalsv, send ack_logoff msg to portal

结果分析：

首先需要了解 Web/Portal 认证的流程，详见前面的 Web/Portal 认证概述。这是一个通过本地认证上线的例子。因此对于 Webauth 模块来讲，首先要接受到来自 Portal Server 的 req_auth 消息，然后根据接口名称获得模板参数，进行上线操作，设置相关属性。如果其中哪一点中断，则表明相关操作没有完成。用户下线时，Webauth 模块也会收到来自 Portal Server 的下线消息，并注销用户，然后返回确认信息。


注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug webauth 命令禁用此功能。

27.6.2 debug portal

应用环境：

当用户使用 Web/Portal 认证，输入了正确的用户名和密码仍然不能认证成功时，使用此命令定位出错的地方。为了在终端显示该调试信息，需要执行命令 terminal monitor。

调试实例：

实例**1**	用户认证上线
	Feb 9 12:17:10 (none) userportal.cgi: to login: user=lsh, ip=192.168.0.180, snid=FVdeFUVTTC09TAQRHlwp Feb 9 12:17:10 (none) portal[242]: sub, addnode: name=lsh, ip=3019942080 Feb 9 12:17:10 (none) portal[242]: portalcl, make auth msg, user=lsh,

	ip=3019942080 Feb 9 12:17:10 (none) portal[242]: portalcl, send reqauth msg to webauth, user=lsh, ip=3019942080 Feb 9 12:17:10 (none) portal[242]: portalcl,get message from webauth: msgtype=4, ret=0 Feb 9 12:17:10 (none) portal[242]: portalcl, make finishack msg, ip=3019942080 Feb 9 12:17:10 (none) portal[242]: portalcl, send reqack msg to webauth, user=lsh, ip=3019942080 Feb 9 12:17:10 (none) userportal.cgi: response message len = 128 Feb 9 12:17:10 (none) userportal.cgi: login success Feb 9 12:17:10 (none) userportal.cgi: login pass: user=lsh ip=192.168.0.180, snid=FVdeFUVTTC09TAQRHlwp, result=36 Feb 9 12:17:15 (none) userportal.cgi: to keepalive: user=lsh, ip=192.168.0.180, snid=FVdeFUVTTC09TAQRHlwp Feb 9 12:17:15 (none) userportal.cgi: response message len = 128 Feb 9 12:17:15 (none) userportal.cgi: keepalive finish: user=lsh, ip=192.168.0.180, snid=FVdeFUVTTC09TAQRHlwp, result=32
实例**2**	用户下线流程
	Feb 9 12:17:56 (none) userportal.cgi: to logout: user=lsh, ip=192.168.0.180, snid=FVdeFUVTTC09TAQRHlwp Feb 9 12:17:56 (none) portal[242]: portalcl, make logoff msg, ip=3019942080 Feb 9 12:17:56 (none) portal[242]: portalcl, send reqlogoff msg to webauth, user=lsh, ip=3019942080 Feb 9 12:17:56 (none) webauth[234]: usr_table, user logout success, user = lsh Feb 9 12:17:56 (none) portal[242]: portalcl,get message from webauth: msgtype=6, ret=0 Feb 9 12:17:56 (none) userportal.cgi: response message len = 128 Feb 9 12:17:56 (none) userportal.cgi: logoff: user=lsh, ip=192.168.0.180, snid=FVdeFUVTTC09TAQRHlwp, result=35

结果分析：

用户上线首先要通过调用 cgi，cgi 将用户信息发送给 Portal Server 模块，Portal Server 保存用户信息，并向 Webauth 模块发送认证消息，当成功接受到认证消息后，会给 Webauth 发送确认信息，并通过 cgi 给用户返回认证结果。如果某一点日志中断，则相关点出现问题。


注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug portal 命令禁用此功能。

28 配置IEEE802.1X接入认证

本章涉及 IEEE 802.1x 接入认证功能的配置，内容主要包括：

- IEEE 802.1x 接入认证功能概述
- 配置 IEEE 802.1x 接入认证模板
- 在端口启用 IEEE 802.1x 接入认证模板

28.1 IEEE 802.1x接入认证概述

IEEE 802.1x 称为基于接口的访问控制协议（Port Based Network Access Control Protocol）。IEEE 802.1x 协议的体系结构包括三个重要的部分：Supplicant System 客户端、Authenticator System 认证系统、Authentication Server System 认证服务器系统。

客户端系统：一般为一个用户终端系统，该终端系统通常要安装一个客户端软件(用户可以使用港湾网络有限公司自己研发的 802.1x 客户端软件)，用户通过启动这个客户端软件发起 802.1x 协议的认证过程。客户端系统是支持基于端口的接入控制，客户端系统需支持 EAPOL（Extensible Authentication Protocol Over LAN）协议。

认证系统：通常为支持 802.1x 协议的网络设备。（SmartHammer 网络安全产品可以作为认证系统设备）该设备对应于不同用户的端口（可以是物理端口，也可以是用户设备的 MAC 地址、VLAN、IP 等）有两个逻辑端口：受控（Controlled Port）端口和不受控端口（Uncontrolled Port）。不受控端口始终处于双向连通状态，主要用来传递 EAPOL 协议帧，可保证客户端始终可以发出或接受认证。受控端口只有在认证通过的状态下才打开，用于传递网络资源和服务。受控端口可配置为双向受控和仅输入受控两种方式，以适应不同的应用环境。如果用户未通过认证，则受控端口处于未认证状态，则用户无法访问认证系统提供的服务。

认证服务器：通常为 RADIUS 服务器，该服务器可以存储有关用户的信息，比如用户所属的 VLAN、CAR 参数、优先级、用户的访问控制列表等等。认证服务器

和 RADIUS 服务器之间通过携带 EAP 报文的 RADIUS 报文进行通信。

28.2 配置IEEE 802.1x接入认证模板

IEEE802.1x 接入认证服务是通过 IEEE802.1x 模板来实现的，通过 IEEE802.1x 模板配置接入认证所需要的选项，然后在某个端口下使用该模板，从而使从该端口接入的用户都使用模板上的配置，达到更好的管理用户的目的。

用户可以配置多个模板，但在一个以太网端口下一次只可以使用一个模板。

用户通过使用 IEEE802.1x 客户端，输入用户名和密码，向接入服务器发送 EAP 报文进行接入认证。

28.2.1 缺省配置

表28-1 IEEE 802.1x 接入认证模板的缺省设置信息

内容	缺省设置	备注
认证方式（authentication-style）	eap	可更改设置
用户名唯一性（unique-verify）	disable	可更改设置
用户异常下线监测间隔（keep-alive）	unlimited	可更改设置
用户最大闲置时间（idle-timeout）	unlimited	可更改设置
间歇计费间隔（accounting-interval）	unlimited	可更改设置
端口下可以同时接入的最大用户数（max-session）	500个	可更改设置

28.2.2 配置IEEE802.1x接入认证模板与认证和计费相关参数

使用 IEEE802.1x 接入认证服务必须要在 IEEE802.1x 模板中配置与计费和认证相关的参数才可以实现。与认证和计费相关的参数包括：

使用的 AAA 认证和计费服务器信息

AAA 认证和计费服务器信息的设置在 AAA 认证和计费模板中，在 IEEE802.1x 模板中使用 AAA 认证和计费模板（详见 AAA 认证和计费功能）。

必须要在 IEEE802.1x 模板中配置 AAA 认证和计费服务器信息。

使用的认证方式（CHAP/EAP）

IEEE802.1x 接入认证用户可以使用以下两种认证方式：

EAP 认证方式：

SmartHammer 设备向 Radius 认证服务器发送的认证 Radius 报文中携带从客户端发送到 SmartHammer 设备的 EAP 报文，SmartHammer 设备不对从客户端发送到自己的携带用户密码的 EAP 报文进行解释，直接发给 Radius 认证服务器。

计算密码散列值的 Challenge 由 Radius 认证服务器产生。

SmartHammer 设备和 Radius 认证服务器需要两次交互才可以完成认证功能。

CHAP 认证方式：

SmartHammer 设备向 Radius 认证服务器发送的认证 Radius 报文中不携带 EAP 报文。

计算密码散列值的 Challenge 由 SmartHammer 设备产生。

SmartHammer 设备和 Radius 认证服务器只需要一次交互就可以完成认证功能。

间歇计费的间隔

使用 Radius 计费服务器进行计费时，一般在计费开始时发送计费开始报文，在计费结束时发送计费结束报文（携带用户上线时长和流量），供 Radius 计费服务器计算用户计费信息。为了保证用户计费信息的准确性和实时性，可以设置用户上线后，每隔一段时间发送一次 Radius 间隔计费报文，也携带用户上线时长和流量。

配置 IEEE802.1x 接入认证模板与认证和计费相关参数的步骤：

步骤1	subscriber-template dot1x NAME	配置名为NAME的IEEE802.1x接入认证模板，如果不存在该模板，则创建模板
步骤2	aaa-group NAME [by GROUP]	配置使用的AAA认证和计费模板。by GROUP用于设定使用该AAA模板的用户组。
步骤3	authentication-style (chap|eap)	配置认证方式，默认值为eap
步骤4	accounting-interval <1-10000>	配置间歇计费间隔，默认值为unlimited（不发送间歇计费）

注意事项：

- 在 IEEE802.1x 接入认证模板下必须要配置使用 AAA 认证和计费模板，否则无法进行接入认证。
- 在同一个 IEEE802.1x 接入认证模板下可以配置使用多个 AAA 模板。

- 不以 by GROUP 为后缀使用的 AAA 认证和计费模板，表示所有接入用户可以匹配该模板。
- 以 by GROUP 为后缀使用的 AAA 认证和计费模板，表示只有用户名和 GROUP 可以匹配的用户，可以使用该模板，用于对多 ISP 的支持。
- 请详细参考对“AAA 认证和计费模板”的配置和注意事项。

28.2.3 配置IEEE802.1x接入认证模板与用户QoS相关参数

配置一个 IEEE802.1x 接入认证模板（如果不存在该模板，则首先创建模板）与 QoS 相关参数，对能够与这些设置相匹配的接入用户作 QoS，对不能与这些设置相匹配的用户不作 QoS。

配置认证方式的步骤：

步骤1	subscriber-template dot1x NAME	配置名为NAME的IEEE802.1x接入认证模板，如果不存在该模板，则创建模板
步骤2	traffic to id NAME priority <0-7> rate <64-100000>	配置接入用户的QoS。如果该用户认证成功后，从Radius返回的FilterID属性值和设定的NAME相同，则按照定义的带宽和优先级提供给用户。
步骤3	traffic to name PATTERN priority <0-7> rate <64-100000>	配置接入用户的QoS。如果用户名和设定的某个PATTERN模式匹配，则按照定义的带宽和优先级提供给用户。

注意事项：

- 在 IEEE802.1x 接入认证模板下必须要配置使用 AAA 认证和计费模板，否则无法进行接入认证。
- 如果一个接入认证用户的用户名以及从 Radius 服务器返回的 FilterID 属性都无法匹配您所配置的这些与 QoS 相关命令，那么，对该接入用户不作 QoS，该用户可以使用的带宽为该端口下最大带宽。
- 配置接入用户的 QoS 时，traffic to id 命令与 traffic to name 命令可以同时使用，但 traffic to id 命令具有较高的优先级，即 IEEE802.1x 接入认证服务首先按返回的 FilterID 属性值匹配，如果没有匹配成功的话再按用户名匹配，如果二者都没有匹配成功，则不对用户作 QoS。
- traffic to name 命令中 PATTERN 为一个模式匹配，即以一个正则表达式来表示一个或一组用户，例如^h 代表以 h 开头，e$代表以 e 结尾等。

28.2.4 配置IEEE802.1x接入认证模板与异常下线相关参数

SmartHammer 设备可以配置以下参数保证不会由于用户 PC 机出现故障，或用户忘记下线而出现超常账单，造成多计费的情况。

异常下线相关参数包括：

- 用户异常下线监测间隔（Keep Alive）：SmartHammer 设备每隔 KeepAlive 时间间隔向接入用户的 PC 机发送 KeepAlive 报文，如果接入用户 PC 机返回应答报文，表示接入用户仍在线上；如果接入用户 PC 机没有返回应答报文，表示接入用户 PC 机出现死机情况或其他情况导致用户与 SmartHammer 设备之间网络不通，这时用户也无法正常使用网络，为了不增加用户的费用，当用户 3 个 Keep Alive 时间不给回应，则 SmartHammer 设备认为用户出现异常，强制用户下线，并向计费服务器发送计费信息。
- 用户最大闲置时间（Idle Timeout）：当接入用户在设定的 Idle Timeout 时间内没有流量发生，为了在按时长计费的情况下，确保不会因为接入用户忘记下线而对用户多计费的情况，SmartHammer 设备会强制用户下线，并向计费服务器发送计费信息。

配置 IEEE802.1x 接入认证模板与异常下线相关参数的步骤：

步骤1	subscriber-template dot1x NAME	配置名为NAME的IEEE802.1x接入认证模板，如果不存在该模板，则创建模板
步骤2	idle-timeout <60-3600>	配置用户最大闲置时间
步骤3	keep-alive <1-10000>	配置用户异常下线检测间隔


注意

1)在 IEEE802.1x 接入认证模板下必须要配置使用 AAA 认证和计费模板，否则无法进行接入认证。

2)这两条指令的默认值都是 Unlimited（即不设置），为了避免出现由于网络故障或用户忘记下线而造成的对用户多计费的现象，请您至少设置 Keep Alive 时间间隔。

28.2.5 配置IEEE802.1x接入认证模板与用户名唯一性相关参数

为了防止用户帐号被占用的情况，可以设置用户名唯一性参数，保证同时相同的用户名只允许一个用户在线。

该参数的默认值为不对用户名作限制，即相同的用户名同时允许多个用户在线。

配置 IEEE802.1x 接入认证模板与认用户名唯一性相关参数的步骤：

步骤**1**	subscriber-template dot1x NAME	配置名为NAME的IEEE802.1x接入认证模板，如果不存在该模板，则创建模板
步骤**2**	unique-verify	设置用户名唯一性


注意

在 IEEE802.1x 接入认证模板下必须要配置使用 AAA 认证和计费模板，否则无法进行接入认证。

28.2.6 配置在端口启用IEEE802.1x接入认证模板

配置完一个 IEEE802.1x 接入认证模板后必须要在 SmartHammer 设备的某一个端口上启用它，才可以对该端口下所有接入认证用户使用该模板。

用户可以配置多个 IEEE802.1x 接入认证模板，但在一个以太网端口下一次只可以使用一个 IEEE802.1x 接入认证模板。

配置在端口启用 IEEE802.1x 接入认证模板的步骤：

步骤**1**	interface IFNAME	进入IFNAME这个端口
步骤**2**	ip address A.B.C.D/M	设置端口的IP地址
步骤**3**	dot1x subscriber-template NAME	在端口上启用IEEE802.1x接入认证
步骤**4**	dot1x max-session <1-8000>	限制该端口下可以同时接入的最大用户数

注意事项：

- 用户可以配置多个 IEEE802.1x 接入认证模板，但在一个以太网端口下一次只可以启用一个 IEEE802.1x 接入认证模板。
- 请首先设置端口的 IP 地址，然后再启用 IEEE802.1x 接入认证模板。
- 用户必须通过可以透传 EAP 报文的二层交换机接入 SmartHammer 设备，而不能通过三层交换机接入。
- 在该端口有用户接入的情况下删除该端口下所有的 IP 地址，将会导致用户计费信息不准确，请避免该操作，或是您先使用 no dot1x subscriber-template NAME 在端口下停用 IEEE802.1x 认证，然后再删除 IP 地址。
- 在启用 IEEE802.1x 认证的端口下仍然可以有用户可以不使用 IEEE802.1x 认

证上网，这需要您使用 dot1x authorize A.B.C.D XX:XX:XX:XX:XX:XX 指令配置免认证用户。

28.3 显示信息举例

表28-2 IEEE 802.1x 接入认证配置信息显示命令列表

命令	解释
show dot1x interface [IFNAME]	显示启用IEEE802.1x接入认证的端口信息，IFNAME用于指定显示的端口名
show dot1x subscribe-template [NAME]	显示IEEE802.1x接入认证模板信息，NAME用于指定显示的模板
show dot1x summary	显示IEEE802.1x接入认证概要信息（包括模板在哪几个端口下被启用，各有多少上线用户）
show dot1x user [WORD]	显示IEEE802.1x接入认证上线用户信息，WORD用于指定显示用户的用户名

show dot1x interface 命令显示举例:

```
SmartHammer # show dot1x interface
============================================================
Interface    ge1
<enable IEEE802.1x>
Subscriber Template Name:    hammer
Max Session:    2000
============================================================
```

show dot1x subscribe-template 命令显示举例:

```
SmartHammer#show dot1x subscribe-template
============================================================
Subscriber Template Name: hammer
Keep alive Time                    : 120
Radius Accounting Interval    : 120
AAA GROUP                              : dot1x
Authentication-style              : eap
============================================================
```

show dot1x summary 命令显示举例

```
SmartHammer#show dot1x summary
============================================================
Subscriber Template Name: hammer
Keep alive Time                    : 120
Radius Accounting Interval   : 120
AAA GROUP                                : dot1x
Authentication-style             : eap
------------------------------------------------------------
interface        :     ge1
maxsession       :     2000
total users      :     1
------------------------------------------------------------
Total Interface : 1
Total Users        : 1
============================================================
```

show dot1x user 命令显示举例：

```
SmartHammer # show dot1x user
============================================================
User Name: (hammer)
Start Time: Tue Jan 13 14:19:57 2004
Standing Time: 637
Bytes Out : 8646                    Bytes In: 9786
IP Address: 192.168.1.200           MAC Address: 00:0b:db:64:4a:a3
Subscribe Template Used: hammer
AAA GROUP : dot1x
============================================================
total user :1
```

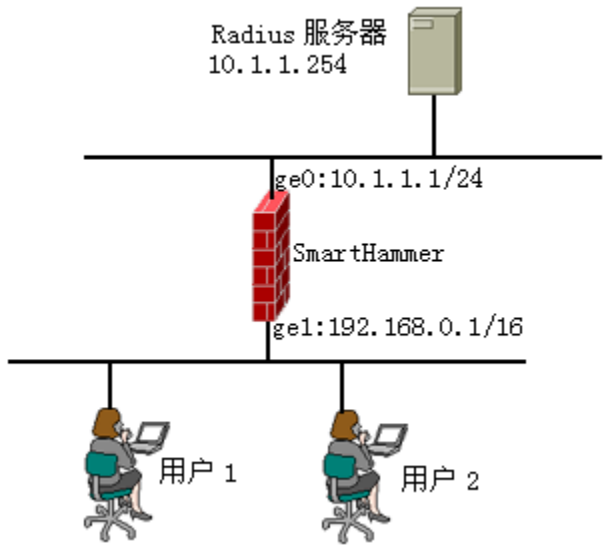
28.4 配置案例

案例描述:

在 SmartHammer 防火墙的 ge1 接口（192.168.0.1）上启动 IEEE802.1x 接入认证，使用 Radius 服务器认证和计费。

使用 SmartHammer 防火墙进行认证的用户同属于一个 ISP，他们都使用相同的 Radius 认证和计费服务器，Radius 服务器（10.1.1.254）与 SmartHammer 防火墙的 ge0 接口相连。

图28-1 IEEE802.1X 接入认证配置案例组网图



配置步骤：

步骤**1**	配置AAA认证和计费模板
	SmartHammer#configure terminal SmartHammer(config)#aaa dot1x SmartHammer(config-aaa)#authentication server 10.1.1.254 1812 88--99 SmartHammer(config-aaa)#accounting server 10.1.1.254 1813 88--99 SmartHammer(config-aaa)#source-ip 10.1.1.1 SmartHammer(config-aaa)#exit
步骤**2**	配置IEEE802.1x接入认证模板
	SmartHammer(config)#subscriber-template dot1x hammer SmartHammer(config-sub)#aaa-group dot1x SmartHammer(config-sub)#keep-alive 120 SmartHammer(config-sub)#accounting-interval 120 SmartHammer(config-sub)#authentication-style eap SmartHammer(config-sub)#exit
步骤**3**	在接口上启用IEEE802.1x接入认证，并限制该端口下最大接入用户数为2000
	SmartHammer(config)#interface ge0 SmartHammer(config-if)#ip address 10.1.1.1/24 SmartHammer(config-if)#exit SmartHammer(config)#interface ge1 SmartHammer(config-if)#ip address 192.168.0.1/16 SmartHammer(config-if)#dot1x subscriber-template hammer SmartHammer(config-if)#dot1x max-session 2000 SmartHammer(config-if)#exit
步骤**4**	配置DHCP

	SmartHammer(config)#dhcp 请见配置DHCP章中的具体配置
步骤5	保存配置
	SmartHammer(config)#write memory

28.5 常见故障

28.5.1 用户无法上线

故障现象：用户无法上线

分析与解决：有可能是以下几种情况导致用户无法上线（您可以使用 debug dot1x 命令查看出错原因）

- 用户名密码错误：您可以确认一下用户名和密码
- 该端口下接入用户数已达到最大值：使用 show dot1x summary 命令查看该端口接入用户以及最大限制用户数
- 用户接入的交换机是否是可以透传 EAP 报文的二层交换机，否则认证报文无法通过交换机到达 SmartHammer 网络安全产品
- 如果采用 Radius 服务器认证，SmartHammer 网络安全产品是否可达 Radius 认证服务器
- Radius 认证服务是否已启动
- 是否在 Radius 认证服务器上配置了正确的 NAS 地址
- 您配置的 AAA 认证和计费模板是否正确

28.5.2 用户异常下线

故障现象：用户异常下线

分析与解决：有可能是以下几种情况导致用户异常下线（您可以使用 debug dot1x 命令查看出错原因）

- 使用 Radius 服务器计费，计费错误。用户上线后发送的开始计费请求报文，或者是用户的间歇计费请求报文，没有得到 Radius 计费服务器的回应，都会导致用户下线。您需要确认：
- SmartHammer 网络安全产品是否可达 Radius 计费服务器
- Radius 计费服务器上 Radius 计费服务是否已启动
- 是否在 Radius 计费服务器上配置了正确的 NAS 地址

- 您配置的 AAA 认证和计费模板是否正确
- 是否由于您设置了 Idle Timeout 导致由于用户在一段时间内没有流量，SmartHammer 网络安全产品强制用户下线
- 由于网络故障导致 Keep Alive 报文没有应答，SmartHammer 网络安全产品强制用户下线，请确认 SmartHammer 网络安全产品与用户之间网络可达
- 由于另一个具有相同 MAC 地址的用户接入，导致用户下线

28.6 常用调试功能

28.6.1 debug dot1x login

应用环境：

当接入用户无法正常上线时，查看用户上线信息 (为了在终端显示该调试信息，需要执行命令 terminal monitor) 。

调试实例：

```
SmartHammer(config)# terminal monitor
SmartHammer(config)# debug dot1x login
Recv EAPOL-Start packet
Station hammer logout for auth failed
```

结果分析：

显示收到接入用户的上线请求报文（EAPOL-Start 报文）

但是用户认证失败，原因可能有很多种，您需要配合下面的 debug dot1x auth 查看更详细的信息，或您直接使用 debug dot1x 查看所有阶段的 IEEE802.1x 接入用户信息。


注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug dot1x login 命令禁用此功能。

28.6.2 debug dot1x auth

应用环境：

当接入用户无法正常上线时，查看用户上线时的认证信息。(为了在终端显示该调试信息，需要执行命令 terminal monitor)

调试实例：

```
SmartHammer(config)# terminal monitor
SmartHammer(config)# debug dot1x auth
No response to retry sending auth RADIUS packet
```

结果分析：

显示从 Radius 认证服务器没有返回应答信息。

这时您需要确认：

- SmartHammer 设备是否可达 Radius 认证服务器
- Radius 认证服务器上 Radius 认证服务是否已启动
- 是否在 Radius 认证服务器上配置了正确的 NAS 地址
- 是否在 SmartHammer 设备的 AAA 模板上配置了正确的 Radius 认证服务器参数（服务器地址、端口、共享密钥）
- 是否在 SmartHammer 设备的 AAA 模板上配置了正确的 NAS 地址

注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug dot1x auth 命令禁用此功能。。

28.6.3 debug dot1x acct

应用环境：

当接入用户无法正常计费时。(为了在终端显示该调试信息，需要执行命令 terminal monitor)

调试实例：

```
SmartHammer(config)# terminal monitor
SmartHammer(config)# debug dot1x acct
No response to retry sending acct start or intrim RADIUS packet
```

结果分析：

显示从 Radius 计费服务器没有返回应答信息。这时您需要确认：

- SmartHammer 设备是否可达 Radius 计费服务器
- Radius 计费服务器上 Radius 计费服务是否已启动
- 是否在 Radius 计费服务器上配置了正确的 NAS 地址
- 是否在 SmartHammer 设备的 AAA 模板上配置了正确的 Radius 计费服务器参数（服务器地址、端口、共享密钥）
- 是否在 SmartHammer 设备的 AAA 模板上配置了正确的 NAS 地址


注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug dot1x acct 命令禁用此功能。

28.6.4 debug dot1x session

应用环境：

当接入用户异常下线时。(为了在终端显示该调试信息，需要执行命令 terminal monitor)

调试实例：

```
SmartHammer(config)# terminal monitor
SmartHammer(config)# debug dot1x session
Station hammer logout for wait packet timeout
```

结果分析：

用户由于报文超时异常下线，原因有很多种，您需要结合 debug dot1x keep_alive 和 debug dot1x force_off 命令来查看更详细的信息，或您直接使用 debug dot1x 查看所有阶段的 IEEE802.1x 接入用户信息


注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug dot1x session 命令禁用此功能。

28.6.5 debug dot1x keep_alive

应用环境：

当接入用户异常下线时。(为了在终端显示该调试信息，需要执行命令 terminal monitor)

调试实例：

```
SmartHammer(config)# terminal monitor
SmartHammer(config)# debug dot1x keep_alive
Station logout for Keep-Alive
```

结果分析：

用户是由于连续发送三次 Keep-alive 报文没有回应，超时异常下线的，请查看用户和 SmartHammer 设备之间的链路是否畅通。


注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug dot1x keep_alive 命令禁用此功能。

28.6.6 debug dot1x force_off

应用环境：

当接入用户异常下线时。(为了在终端显示该调试信息，需要执行命令 terminal monitor)

调试实例：

```
SmartHammer(config)# terminal monitor
SmartHammer(config)# debug dot1x force_off
Station hammer exceed idle timeout
```

结果分析：

用户是由于您设置了 idle-timeout 指令，而且用户在这段时间内没有流量发生，为

了在按时长计费的情况下，确保不会因为用户忘记下线而对用户多计费，SmartHammer 设备强制用户下线。


注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug dot1x force_off 命令禁用此功能。

28.6.7 debug dot1x

应用环境：

当接入用户无法认证通过或出现异常时。(为了在终端显示该调试信息，需要执行命令 terminal monitor)

调试实例：

```
Recv EAPOL-Start packet
Recv RADIUS auth packet, MAC: 00:0b:db:64:4a:a3
User 00:0b:db:64:4a:a3 auth success
Recv RADIUS acct packet, MAC: 00:0b:db:64:4a
Station logout for Keep-Alive
Station hammer logout for wait packet timeout
Recv RADIUS acct packet, MAC: 00:0b:db:64:4a:a3
```

结果分析：

用户是由于连续发送三次 Keep-alive 报文没有回应，超时异常下线的，用户的认证和计费信息都正常，请查看用户和 SmartHammer 设备之间的链路是否畅通。


注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debugdot1x 命令禁用此功能。

第六部分

交换转发服务配置

29 配置 NetFlow

本章涉及 NetFlow 的配置，内容主要包括：

- NetFlow 功能概述
- NetFlow 配置

29.1 NetFlow概述

NetFlow 技术能够有效地提供网络流量测量，包括流量计帐和分析，基于应用的计帐和分析，也可以根据网络流量分布来查看网络带宽，是否足够以便升级网络，或者监视网络分析是否受到 DOS 攻击。

NetFlow 能够提供非常有价值的信息：当前什么用户在使用网络，什么应用，什么时间段利用，以及网络流量的流向.

NetFlow 可以把设备通过的流量以 UDP 包形式发送给收集器，由收集器收集并分析，整理，提供给网络管理员整个网络利用情况，可以做到实时收集实时分析，随时掌握整个网络。

29.2 SmartHammer设备对NetFlow的支持

NetFlow 技术为 Cisco 发明的技术，共有版本 1、版本 5、版本 7、版本 8、版本 9 五种版本，由于 Cisco 在路由器领域的地位，所以 NetFlow 成为事实上的标准。SmartHammer 设备支持版本 5，与 Cisco 兼容，所以对于支持 Cisco 版本 5 的收集器，SmartHammer 设备都支持。

29.3 配置NetFlow

29.3.1 缺省配置

表29-1 NetFlow 的缺省设置信息

内容	缺省设置	备注
网络流量收集	Disable	默认情况下不收集接口网络流量
网络流量输出	Disable	默认情况下不输出

29.3.2 配置网络流量数据输出

收集网络流量数据，需要指明收集网络流量数据的收集器的 IP 地址和端口号，以便把数据收集到数据库，进行实时分析或事后分析。

配置网络流量数据输出的步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	ip flow-export IP PORT	配置收集器的IP地址和端口号
步骤**3**	end	返回特权模式


注意

1）如果网络流量数据输出功能没有打开，但已经在接口上启动了数据收集功能，还是会收集的，只不过不会输出。

2）只允许配置一个收集器

29.3.3 配置接口网络流量数据收集

在接口下启用网络流量数据收集，允许在多个接口下进行数据收集，但是由于收集网络流量数据会占用一些资源，所以建议只在一些关键或敏感的接口上启用数据收集功能采集数据。

配置接口网络流量数据收集的步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	interface IFNAME	进入接口配置模式
步骤**3**	ip flow-collect	打开网络流量数据收集功能
步骤**4**	end	返回特权模式
步骤**5**	show running	显示配置信息

29.3.4 清除网络流量统计

当网络流量统计数据比较大时，可以使用命令清除当前的统计数据；当然，系统亦会每隔 12 小时自动清除一次统计数据。

清除网络流量统计的步骤：

步骤1	clear ip flow stat	清除网络流量统计

29.4 网络流量信息显示命令

表29-2 网络流量信息显示命令

命令	解释
show ip flows info	显示收集的流信息
show ip flows stat	显示流输出信息

29.5 配置案例

29.5.1 收集网络流量并发送给收集器

案例描述：

配置 NetFlow 监控防火墙外网接口的流量，并输出到收集器进一步分析流量大小，流量的应用，以及是否有攻击，从而可以监控防火墙外网的流量信息，防止攻击和非法入侵。

配置步骤：

步骤1	在外网接口上启动流量数据收集
	SmartHammer#configure terminal SmartHammer(config)#interface ge2 SmartHammer(config-if)#ip flow-collect SmartHammer(config-if)#exit SmartHammer(config)#
步骤2	启动流量数据输出
	SmartHammer(config)#ip flow-export 10.5.6.1 125 SmartHammer(config)#end
步骤3	显示流量数据输出统计

	SmartHammer#show ip flows stat flow export is enabled exporting flows to 10.5.6.1 (125) version 5 flow records 32 flows exported in 1 udp datagrams 0 flows failed due to lack of export packet 1 export packets were sent up to process level 0 export packets were dropped due to no route to dst last clearing of statistics Wed Apr 11 23:11:30 2001
步骤**4**	保存配置
	SmartHammer#write memory

第七部分

路由协议配置

30 配置静态路由

本章涉及静态路由功能的配置，内容主要包括：

- 静态路由概述
- 配置静态路由
- 配置缺省路由

30.1 静态路由概述

在 IP 设备中，单播路由的获得通常有两种途径：静态配置和动态路由获取。静态配置就是由网络管理员通过终端命令行等手段明确定义，被称为静态路由。

30.2 配置静态路由

静态路由是由用户配置的路由。当用户确信到达某个网段应该先转发到某个地址时，可以通过 ip route 命令配置这个静态路由。

配置静态路由的步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	ip route A.B.C.D/M (A.B.C.D|INTERFACE) [1-255]	配置静态路由
步骤**3**	ip route A.B.C.D E.F.G.H (A.B.C.D|INTERFACE) [1-255]	或通过本命令配置静态路由
步骤**4**	exit	退出配置模式
步骤**5**	show ip route	显示静态路由信息


注意

ip route A.B.C.D/M (A.B.C.D|INTERFACE) [1-255]指令和 ip route A.B.C.D E.F.G.H (A.B.C.D|INTERFACE) [1-255]指令都可以配置静态路由

30.3 配置缺省路由

有一类特殊的路由称为默认路由（或缺省路由），即目的地址和掩码为 0.0.0.0/0 的路由。它可以匹配任何目的地址，所以每个找不到对应路由的报文都将按默认路由转发。通常默认路由都是在用户认为有必要时通过静态路由配置的。在网络有一个唯一出口连接到其他网络时，配置默认路由是很有用的，它可以使 SmartHammer 所需要的路由数量大大降低。

配置缺省路由的步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	ip route 0.0.0.0/0 (A.B.C.D|INTERFACE)	配置缺省路由
步骤**3**	end	退出配置模式
步骤**4**	show running-config	显示静态路由信息

30.4 配置信息显示命令

表30-1 显示静态路由信息

命令	解释
show ip route	显示静态路由信息

30.5 配置案例

30.5.1 配置缺省路由

案例描述：

配置缺省路由，把每个没有对应路由的报文转发到 10.0.0.1。

配置案例：

步骤**1**	配置缺省路由
	SmartHammer(config)# ip route 0.0.0.0/0 10.0.0.1

30.6 常见故障

30.6.1 数据包转发不正常

故障现象：数据包转发不正常

分析与解决：有可能是以下几种情况导致数据包转发不正常

- 没有配置正确的静态路由
- 对于没有对应静态路由项的数据包没有配置缺省路由
- 静态路由指定的下一跳地址不可达

31 配置策略路由

本章涉及策略路由的配置，内容主要包括：

- 策略路由概述
- 配置策略路由
- 策略路由信息的显示
- 配置案例
- 常用调试功能

31.1 策略路由概述

所谓策略路由，顾名思义，即是根据一定的策略进行报文转发，因此策略路由是一种比目的路由更灵活的路由机制。在 SmartHammer 设备转发一个数据报文时，首先根据配置的规则对报文进行过滤，匹配成功则按照一定的转发策略进行报文转发。这种规则可以是基于标准和扩展访问控制列表；而转发策略则是控制报文按照指定的策略路由表进行转发。因此，策略路由是对传统 IP 路由机制的有效增强。

SmartHammer 设备支持按照 Access-list 提供的策略进行路由。数据包首先由 Access-list 进行匹配，匹配成功后路由至设定的主机或 Interface。

31.2 配置策略路由

31.2.1 策略路由配置

通常情况下，策略路由的目标为下一跳的主机地址，对于路由出口为直连链路或下一跳主机启用 ARP 代理等特殊应用，可使用出口 Interface 为路由目标。

配置策略路由，需要和 Access-list 相结合，Access-list 的配置参见配置 ACL 部分的内容。

配置策略路由的步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	policy-map MAPNAME	进入policy-map配置模式
步骤**3**	list (<1-99>|<100-199>|<1300-1999>|<2000-2699>|<2700-2999>) nexthop (A.B.C.D | INTERFACE)	配置路由策略，将满足access-list的数据包路由至下一跳，此命令可配置多条
步骤**4**	exit	返回特权模式
步骤**5**	show ip policy-map [NAME]	显示policy-map的配置信息

31.2.2 启用策略路由

启用策略路由的步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	Interface NAME	进入interface模式
步骤**3**	ip route-policy MAPNAME	启用指定的policy-map
步骤**4**	end	返回特权模式
步骤**5**	show running-config	显示配置信息

31.3 策略路由信息的显示

表31-1 策略路由信息显示命令

命令	解释
show ip policy-map [NAME]	显示策略路由的配置信息
show ip policy-map [NAME] memory	显示策略路由的资源使用情况

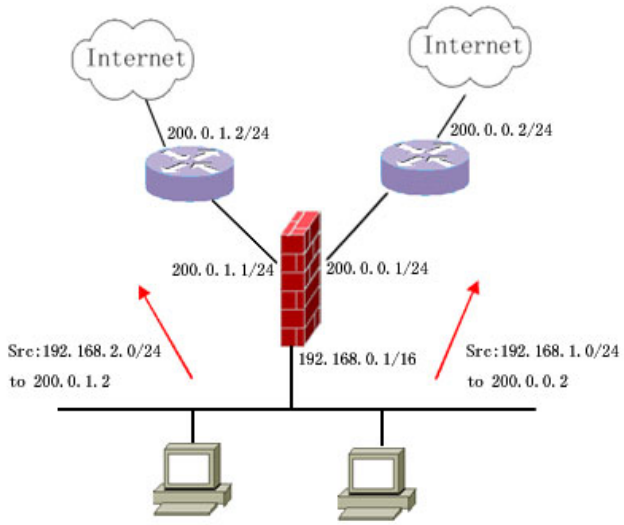
31.4 配置案例

31.4.1 配置策略路由

案例描述：

配置策略路由，将来自 192.168.1.0/24 网段的数据包路由至 SmartHammer 设备 200.0.0.2 上，将来自 192.168.2.0/24 网段的数据包路由至 SmartHammer 设备 200.0.0.1 上。通过这样的配置可有选择的限制不同的 IP 用户访问不同的网络或使用不同的网络出口。

图31-1 配置策略路由案例组网图



配置案例：

步骤**1**	配置Access-list，确定进行策略路由的主机范围，192.168.1.0/24与192.168.2.0/24使用不同的Access-list。
	SmartHammer(config)#access-list 1 permit 192.168.1.0 0.0.0.255 SmartHammer(config)#access-list 2 permit 192.168.2.0 0.0.0.255
步骤**2**	配置policy-map，将源地址为192.168.1.0/24网段的数据包（由Access-list 1过滤出来）路由至200.0.0.2，将源地址为192.168.2.0/24的数据包（由Access-list 2过滤出来）路由至200.0.1.2
	SmartHammer#configure terminal SmartHammer(config)#policy-map test SmartHammer(config-policy-map)# list 1 nexhop 200.0.0.2 SmartHammer(config-policy-map)# list 2 nexhop 200.0.1.2 SmartHammer(config-policy-map)#exit
步骤**3**	在接口上启用策略路由
	SmartHammer(config)#interface eth0 SmartHammer(config-if)ip route-policy test SmartHammer(config-if)exit

31.5 常用调试功能

应用环境：

在启用策略路由的情况下，调试策略路由的正确性。为了在终端显示该调试信息，

需要执行命令 terminal monitor。

调试实例：

步骤**1**	配置策略路由：
	policy-map test list 2000 nexthop 172.16.16.77
步骤**2**	配置Access-list
	access-list 2000 permit ip any 172.16.17.0 0.0.0.255
步骤**3**	在入口上启用
	ip route-policy test
步骤**4**	启用debug policy命令后得到如下结果：
	<FIREWALL><1963-10-26 05:32:25><fw><POLICY><DEBUG><NEXTHOP=172.16.16.77 IN=ge0 OUT=ge1 SRC=192.168.19.1 DST=172.16.17.5 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=ICMP TYPE=8 CODE=0 ID=30049 SEQ=256 >

结果分析：

从结果可以看出，从 192.168.19.1 发往 172.16.17.5 的 ICMP 数据包被路由至下一跳 172.16.16.77。