软件配置指导手册

Hammer10000 IP-DSLAM 接入交换机

发布版本：V2.00
发布日期：2003 年 7 月

港湾网络有限公司
北京市海淀区西三环北路 21 号久凌大厦
邮编：100089
电话：010-88512088　88512099
传真：010-68405011　68473171
E-mail：customer@harbournetworks.com
http:/ / www.harbournetworks.com

声明

本手册总体上较为全面地包含了该产品目前的功能特性和配置内容，如遇到产品的某些临时变化，或针对用户的某些特殊需求而采取的一些特殊变动，港湾网络有限公司保留继续使用该手册，并以其他方式通知用户的权利。

前言

前言部分说明了此手册的大致内容、组织方式、针对用户类型、图标含义以及与 Hammer10000 IP-DSLAM 接入交换机有关的相关文档。

文档内容

本手册主要是针对 HammerOS 操作系统编写的。HammerOS 系统由港湾网络有限公司自行独立开发，可以运行在 FlexHammer、μHammer、BigHammer 系列交换机、Hammer10000 IP-DSLAM 接入交换机以及 AeoHammer 无线访问设备上。本手册对 HammerOS 针对 Hammer10000 IP-DSLAM 接入交换机的特性和配置命令进行了详细说明，并对操作系统的一些缺省配置环境加以介绍，同时提供了一些典型的实用配置案例。

组织方式

文档主要由以下几个部分组成：

章	题目	内容描述
第 1 章	HammerOS 概述	简述 HammerOS 特性，并简述 VLAN，IGMP Snooping、STP、802.1x 等技术在 Hammer10000 IP-DSLAM 接入交换机上的应用。
第 2 章	访问交换机	主要讲述 HammerOS 系统的命令语法、用户权限的设置以及管理 Hammer10000 IP-DSLAM 接入交换机的途径等。
第 3 章	配置端口	讲述了 Hammer10000 IP-DSLAM 接入交换机端口的基本参数配置，并针对 VDSL 端口或者 VDSL 和 ADSL 端口的配置作了详尽的讲解。另外还介绍了端口镜像和多端口负载均衡（Load Sharing）。
第 4 章	虚拟局域网 VLAN	详细介绍了 VLAN 的作用、分类、聚合以及在 Hammer10000 IP-DSLAM 接入交换机中如何完成对 VLAN 各项的配置。
第 5 章	生成树协议 STP	讲解 STP 协议及其配置命令。
第 6 章	FDB 地址表	讲述了 FDB（Forwarding Database）地址表的内容和相关知识，以及如何在 Hammer10000 IP-DSLAM 接入交换机上配置静态 FDB 地址表。
第 7 章	IGMP Snooping	讲述了有关 IGMP Snooping 的相关配置操作及其应用。
第 8 章	动态主机控制协议中继（DHCP Relay）	主要讲述如何利用 DHCP Relay 进行配置来获取主机的动态 IP 地址。
第 9 章	配置 ARP 代理	主要讲述如何通过 ARP 代理实现 SubVLAN 之间的通信。

第 10 章	配置 DHCP 客户端代理（DHCP Client Proxy）	主要讲述 PPPoE 认证如何通过 DHCP Client Proxy 获取 IP 地址。
第 11 章	配置 PPP	主要讲述 PPP 相关的参数配置
第 12 章	NAS 接入服务	主要讲述网络访问服务器（Network Access Server，NAS）接入服务用户配置。
第 13 章	日志模块（Syslog）	介绍日志系统的功能以及如何使用。
第 14 章	Bootrom 启动和软件升级	介绍 Bootrom 启动选项的内容及其含义，并介绍通过 Xmodem 和 FTP 升级 HammerOS 的方法。

图标说明

图标	说明	
	注意	提示用户在操作过程中需要注意的地方。
	提示	表示给用户提示的附加说明信息。

针对用户类型

本手册主要是针对那些需要使用港湾网络有限公司 Hammer10000 IP-DSLAM 接入交换机实现网络配置和管理的用户或系统管理员，因此要求读者须熟悉以下知识：

- 局域网（Local Area Networks)(LANs)
- 以太网概念(Ethernet Concepts)
- 以太网交换和桥概念(Ethernet Switching and Bridging Concepts)
- 网络协议概念(Internet Protocol Concepts)
- 网络数据包交换概念（Internet Package Exchange Concepts）
- VDSL（Very high bit rate Digital Subscriber Line）技术
- ADSL（Asymmetric Digital Subscriber Line）技术
- IGMP（Internet Group Management Protocol） Snooping
- 用户认证协议IEEE 802.1x
- PPPoE相关协议
- DHCP相关协议
- Radius协议

相关文档

Hammer10000 IP-DSLAM 接入交换机涉及的文档部分主要包括：

- 软件配置指导手册——Hammer10000 IP-DSLAM接入交换机(本文档)
- 硬件安装指导手册——Hammer10000 IP-DSLAM接入交换机

目录

第 1 章 HammerOS 概述 1
1.1 特性概述 1
1.2 虚拟局域网 VLAN 2
1.3 生成树协议 STP 2
1.4 负载均衡 Load Sharing 3
1.5 网络组管理协议监听 IGMP Snooping 3
1.6 中继代理 DHCP Relay 4
1.7 Proxy ARP 4
1.8 802.1x 认证服务 4
1.9 PPPoE 终结 5
第 2 章 访问交换机 6
2.1 理解命令语法 6
2.1.1 命令输入规则 6
2.1.2 语法帮助 8
2.1.3 使用语法帮助补齐命令 9
2.1.4 命令简写 10
2.1.5 端口的表示方法 10
2.1.6 命令中的符号 11
2.1.7 命令参数类型 12
2.1.8 行编辑命令 13
2.1.9 历史命令（history）的使用 14
2.2 常用命令 14
2.2.1 show version 15
2.2.2 enable 15
2.2.3 terminal length 15
2.2.4 who 16
2.2.5 list 16
2.2.6 show services 16
2.2.7 save configuration 17
2.2.8 quit 17
2.2.9 logout 17
2.2.10 show idle-timeout 17
2.2.11 exit 18
2.2.12 常用命令列表 18
2.3 设置用户访问权限 20
2.3.1 系统缺省用户帐号 20
2.3.2 增加用户帐号 20
2.3.3 修改用户权限 21
2.3.4 查看系统用户信息 22
2.3.5 删除用户帐号 22
2.3.6 修改密码 22

2.4 管理 Hammer10000 IP-DSLAM 接入交换机的途径 23
2.4.1 通过配置口管理 Hammer10000 IP-DSLAM 接入交换机 23
2.4.2 通过 Telnet 远程管理 Hammer10000 IP-DSLAM 接入交换机 26
2.4.3 通过 SNMP 配置管理 Hammer10000 IP-DSLAM 接入交换机 29
2.5 配置静态路由 31
2.5.1 添加静态路由 31
2.5.2 显示静态路由 31
2.5.3 删除静态路由 32
2.6 存取配置文件 32
2.6.1 Flash 文件操作 33
2.6.2 通过 FTP 协议下载文件 33
2.6.3 通过使用 Xmodem 下载文件 34
2.6.4 通过 FTP 上传文件 34
2.6.5 通过使用 Xmodem 上传文件 35
2.7 配置 PVC 35
2.7.1 配置 PVC 的值 35
2.7.2 查看 PVC 的值 36
2.8 ping 命令 36
第 3 章 配置端口 38
3.1 xDSL 端口文件配置 38
3.1.1 创建端口配置文件 38
3.1.2 修改端口配置文件 38
3.1.3 利用端口配置文件对同类型端口进行配置 39
3.1.4 删除端口配置文件 39
3.1.5 更新端口配置文件 39
3.1.6 显示端口配置文件信息 39
3.2 以太网端口基本配置 39
3.2.1 使能或禁用端口 40
3.2.2 配置端口自适应模式 40
3.2.3 配置端口速率 40
3.2.4 配置端口双工模式 41
3.2.5 配置端口流控 41
3.2.6 显示端口信息 42
3.3 配置 VDSL 端口 43
3.3.1 配置 VDSL 端口上行速率等级 43
3.3.2 配置端口的下行速率等级 44
3.4 配置 ADSL 端口 44
3.4.1 配置端口的上行/下行速率 44
3.4.2 设置端口模式 45
3.4.3 配置上行/下行噪声容限 45
3.4.4 配置上行/下行的快速交织模式 46
3.4.5 配置上行/下行交织延时 46
3.4.6 设置端口门限 47
3.4.7 查看端口配置 47
3.5 端口镜像（Port Mirroring） 48

3.5.1 基于主控板的端口镜像配置 48
3.5.2 配置镜像组目的端口 49
3.5.3 取消端口镜像 49
3.5.4 向镜像组添加源端口 49
3.5.5 删除镜像组中的源端口 50
3.5.6 向镜像组添加插槽 50
3.5.7 删除镜像组中的插槽 50
3.5.8 删除镜像组 50
3.5.9 显示镜像组配置信息 51
3.6 多端口负载均衡(Load Sharing) 51
3.6.1 配置 Load Sharing 51
3.6.2 显示 Load Sharing 配置信息 52
3.7 端口配置命令列表 53
第 4 章 虚拟局域网 VLAN 55
4.1 VLAN 概述 55
4.2 VLAN 的分类 55
4.2.1 基于端口划分 VLAN（Port-Based VLAN） 56
4.2.2 基于标签划分 VLAN（Tagged VLAN） 56
4.2.3 混合使用 Tagged VLAN 和 Port-Based VLAN 57
4.3 VLAN 的命名 57
4.4 VLAN 聚合(Aggregation) 58
4.4.1 聚合综述 58
4.4.2 聚合的目的 58
4.4.3 聚合的特点 58
4.4.4 聚合的限制 58
4.4.5 配置 SubVLAN 59
4.5 Hammer10000 IP-DSLAM 接入交换机 VLAN 使用概述 59
4.5.1 使用目的 59
4.5.2 使用分类 60
4.5.3 资源分配 60
4.6 配置 VLAN 61
4.6.1 配置 VLAN 步骤 61
4.6.2 设置板内和板间隔离功能 63
4.6.3 配置 VLAN 举例 63
4.6.4 显示 VLAN 配置信息 64
4.6.5 删除 VLAN 64
第 5 章 生成树协议 STP 65
5.1 配置 STP 65
5.1.1 使能或关闭 STP 功能 65
5.1.2 指定 STP 的端口 65
5.1.3 配置 STP 参数 66
5.2 显示 STP 状态 67
5.2.1 显示 STP 状态 67
5.2.2 显示端口的 STP 状态 68
第 6 章 FDB 地址表 69

6.1 FDB 地址表概述 69
6.1.1 FDB 地址表的内容 69
6.1.2 FDB 地址表项类型 70
6.1.3 向 FDB 地址表添加地址表项 70
6.2 配置 FDB 地址表 71
6.2.1 创建静态地址表项 71
6.2.2 配置 FDB 地址表老化时间 71
6.2.3 删除静态地址表项 71
6.3 显示 FDB 地址表信息 72
6.3.1 显示 FDB 地址表中的所有地址表项 72
6.3.2 显示 FDB 地址表中的静态地址表项 73
6.3.3 显示 FDB 地址表项老化时间 74
6.4 FDB 地址表命令列表 74
第 7 章 IGMP Snooping 75
7.1 IGMP Snooping 概述 75
7.2 配置 IGMP Snooping 75
7.2.1 启动/关闭 IGMP Snooping 功能 75
7.2.2 配置系统多播路由器配置方式 75
7.2.3 手工删除多播路由器端口信息及所在的 VLAN 76
7.2.4 设置多播路由器老化时间 76
7.2.5 显示多播路由器设置状态和路由老化时间 76
7.2.6 显示多播路由器信息 76
7.2.7 添加/删除系统 IGMP Snooping 监听的 VLAN 77
7.2.8 显示 IGMP Snooping 的状态 77
7.2.9 显示所有被监听 VLAN 中的组信息 77
7.2.10 显示系统当前多播组信息 77
7.2.11 显示过滤和转发多播表项 78
7.2.12 设置系统离开报文处理模式 78
7.2.13 IGMP Snooping 的模块配置 78
第 8 章 动态主机配置协议中继（DHCP Relay） 80
8.1 DHCP Relay 的应用意义 80
8.2 DHCP Relay 原理 80
8.3 配置服务器参数文件 81
8.3.1 启动 DHCP Relay 服务之前的准备工作 81
8.3.2 启动 DHCP Relay 服务 82
8.4 应用配置实例 83
第 9 章 配置 ARP 代理 86
9.1 打开或关闭 SuperVLAN 的 ARP 代理功能 86
9.2 显示 SuperVLAN 的 ARP 代理功能状态 87
9.3 创建/删除 ARP 代理组 87
9.4 配置 ARP 代理组的 SubVLAN（端口）信息 87
9.5 显示 ARP 代理组信息 87
第 10 章 配置 DHCP 客户端代理（DHCP Client Proxy） 88
10.1 概述 88
10.2 DHCP 客户端代理配置命令 88

10.2.1 配置监听接口 88
10.2.2 配置 DHCP 服务器的 IP 地址 88
10.2.3 启用/禁用 DHCP 客户端代理功能 88
10.2.4 显示 DHCP 客户端代理的配置信息 89
10.3 应用配置实例 89
10.3.1 应用环境 89
10.3.2 配置步骤 89
第 11 章 配置 PPP 91
11.1 概述 91
11.1.1 PPP 工作流程 91
11.1.2 PPP 的验证方式：PAP 与 CHAP 92
11.2 PPP 配置命令 92
11.3 配置 LCP 协商参数 92
11.3.1 配置 PPP 立即响应对端的输入 92
11.3.2 取消 PPP 立即响应对端输入的配置 93
11.3.3 配置 PPP 发送第一个 LCP 包的延迟时间 93
11.3.4 取消 PPP 发送第一个 LCP 包的延迟时间的配置 93
11.3.5 配置 ECHO-REQUEST 重传时间间隔 93
11.3.6 配置 ECHO-REQUEST 重传的次数 93
11.4 配置 NCP 协商参数 93
11.4.1 配置接受对端非零 IP 地址 93
11.4.2 取消接受对端非零 IP 地址的配置 94
11.4.3 配置接受 DNS 服务器协商选项 94
11.4.4 接受/拒绝指定的 DNS 服务器 94
11.4.5 取消 DNS 服务器协商选项的配置 94
11.4.6 配置接受 WINS 服务器协商选项 94
11.4.7 接受/拒绝指定的 WINS 服务器 94
11.4.8 取消 WINS 服务器协商选项的配置 95
11.5 配置验证协商参数 95
11.5.1 配置 PPP 对对端的验证方式 95
11.5.2 取消 PPP 对对端的验证 95
11.5.3 配置等待验证应答包的超时时间 95
11.5.4 取消等待验证应答包的超时时间的配置 96
11.6 配置其他参数 96
11.6.1 配置等待 PPP 协商应答包的超时时间 96
11.6.2 取消等待 PPP 协商应答包的超时时间的配置 96
11.6.3 配置通过指定静态地址池为对端分配 IP 地址 96
11.6.4 配置通过 DHCP 代理方式为对端分配 IP 地址 96
11.6.5 取消为对端分配 IP 地址的方式 96
11.6.6 显示 PPP 配置信息 97
11.6.7 配置地址池的 IP 地址范围 97
11.6.8 删除静态地址池 98
11.6.9 显示所有静态地址池的信息 98
11.6.10 显示指定的静态地址池的信息 98
11.7 应用配置实例 99

第 12 章 NAS 接入服务 100
12.1 NAS 接入服务概述 100
12.2 802.1x 协议 103
12.2.1 802.1x 体系结构 103
12.2.2 802.1x 认证机制 105
12.2.3 协议实现内容 107
12.2.4 与不支持 802.1x 的设备的兼容 109
12.3 RADIUS 认证技术 109
12.4 802.1x 配置命令 111
12.4.1 使能/关闭 802.1x 认证服务 111
12.4.2 配置协议参数 111
12.4.3 配置对端口的 802.1x 控制 112
12.4.4 设置重新认证机制 114
12.4.5 设置异常下线检测机制（keepalive） 115
12.4.6 强制用户退出认证状态 116
12.4.7 配置客户端软件更新功能 117
12.4.8 清除 802.1x 统计信息 118
12.5 802.1x 显示命令 118
12.6 NAS 配置命令 119
12.6.1 设置用户绑定功能 119
12.6.2 设置计费高端记录功能 119
12.7 NAS 显示命令 120
12.8 RADIUS 配置命令 120
12.8.1 配置 RADIUS 认证服务 120
12.8.2 配置 RADIUS 计费服务 123
12.8.3 设置 RADIUS CUT 功能 125
12.8.4 配置 RADIUS 计费同步功能 127
12.8.5 配置 Session Timeout 处理机制 128
12.8.6 配置 RADIUS Server 主备切换功能 128
12.8.7 配置 RADIUS 属性 129
12.8.8 配置实例 130
12.8.9 RADIUS 显示命令 131
12.9 配置域 131
12.9.1 域的基本配置 132
12.9.2 域的认证配置 132
12.9.3 域的计费配置 133
12.9.4 配置实例 135
12.10 PPPoE 终结 136
12.10.1 概述 136
12.10.2 PPPoE 终结包括两个方面的配置任务 136
12.10.3 端口启用 PPPoE 功能 136
12.10.4 端口启用 PPPoE 网段内隔离 136
12.10.5 配置业务板网关地址 137
12.10.6 配置应用实例 137
12.11 DSL 端口绑定 140

12.11.1 MAC 地址绑定 140
12.11.2 MAC 地址数目限制 141
12.11.3 IP 地址绑定 142
12.12 单域认证 143
12.13 多域认证 144
12.14 服务器的主备切换 145
第 13 章 日志模块(Syslog) 152
13.1 日志模块概述 152
13.2 日志功能基本配置 152
13.2.1 打开或关闭日志服务 152
13.2.2 配置所要记录的日志信息的类型 152
13.2.3 配置所要记录的日志信息的最低级别 153
13.2.4 打开命令行操作日志记录功能 153
13.3 日志信息存储方式配置 154
13.3.1 打开或关闭日志信息保存到日志服务器的功能 154
13.3.2 增加或删除一个日志服务器 154
13.4 日志信息显示方式配置 155
13.4.1 打开或关闭终端显示日志信息的功能 155
13.4.2 打开或关闭在本终端显示日志信息的功能 156
13.4.3 配置是否显示时间信息 156
13.4.4 配置在终端可以显示的日志信息的最低级别 156
13.4.5 配置在终端可以显示的日志信息的类型 157
13.5 查看日志模块的配置情况 157
13.5.1 查看整个日志模块的配置信息 157
13.5.2 查看对本终端的日志显示属性的配置情况 158
13.6 日志模块命令列表 158
第 14 章 Bootrom 启动和软件升级 160
14.1 Bootrom 启动选项介绍 160
14.1.1 自启动 160
14.1.2 人工干预启动 161
14.2 升级 HammerOS 软件 161
14.2.1 通过 Xmodem 方式下载新版 HammerOS 162
14.2.2 通过 FTP 方式下载新版 HammerOS 163
14.2.3 通过 Xmodem 方式下载新版 HammerOS (for VDU) 163
14.2.4 通过 FTP 方式下载新版 HammerOS (for VDU) 164
14.3 重新启动交换机 164

第1章 HammerOS 概述

HammerOS 是港湾网络有限公司专为 Hammer 系列产品设计的操作系统，它可以运行在 FlexHammer、BigHammer、μHammer 系列交换机、Hammer10000 IP-DSLAM 接入交换机上。

1.1 特性概述

Hammer10000 IP-DSLAM 接入交换机的特性如下：

- Console 命令行配置
- Telnet 命令行配置
- FTP/Xmodem升级
- SNMP功能
- Syslog功能
- 支持IEEE802.1Q和802.1P标准的VLAN
- VLAN聚合
- 线速（Wire-Speed）二层交换，三层转发
- 端口镜像
- 支持上行端口捆绑（Load Sharing）
- 支持STP
- 支持VDSL接入
- 支持ADSL接入
- 支持IGMP Snooping
- 支持动态/静态FDB
- 静态路由
- 动态/静态ARP
- Proxy ARP
- 支持802.1x认证服务
- 支持802.1x 基于端口的网络访问控制
- 支持PPPoE
- 支持本地地址池IP Local Pool
- 支持DHCP Relay
- 支持Radius

- ACL限速
- MAC绑定/限制
- IP绑定
- 认证用户名绑定
- 业务板热插拔

1.2 虚拟局域网 VLAN

Hammer10000 IP-DSLAM 接入交换机的 VLAN 功能使您在构建自己的广播域时，不再受限于网络的物理连接。一个 VLAN 就是一群独立于具体网络拓扑的设备，它们在通讯时，不论如何连接，属于这一 VLAN 的所有设备都好像在一个真正的物理局域网上。

VLAN 的具体作用体现在以下几个方面：

- 可以控制广播数据，限制其广播的范围。某个VLAN内的广播报文只能被限制在这个VLAN内广播，其他VLAN将不会收到这个广播报文，从而避免了网络中的广播风暴。
- 提供了额外的安全特性。VLAN之间不能直接互相访问，必须通过三层转发，在不进行三层转发时，VLAN之间彼此是隔离的，在一定程度上提高了网络的安全性能。
- 简化了用户主机在网络中的移动和管理。当属于某个VLAN的主机的物理位置发生变化时，只要其仍然连接到属于这个VLAN的设备的端口上，无需进行任何额外设置，则仍能够实现与VLAN内的其他主机通信。

提示：

有关 VLAN 的详细配置信息见本文档第 4 章。

1.3 生成树协议 STP

Hammer10000 IP-DSLAM 接入交换机支持 IEEE802.1D 标准的 STP 协议，这一协议提供了网络的动态冗余切换机制。因此，使用 STP 可以为您在网络设计中实现部署备份线路，并且保证：

- 在主线路正常工作时，备份线路是关闭的。
- 当主线路出现故障时，自动激活备份线路，将数据流切换到备份线路，保证设备正常运行。

网络回路对网络是致命的打击，而冗余链路作为网络备份路径又极其重要。因此，使用 STP 可以保证当在网络结构上存在冗余路径情况下，阻止网络回路状态发生。STP 是运行在 Bridges 和 Switches 层上并与 802.1D 协议标准兼容的第二层协议。

为了实现上述功能，STP 要求对每个 VLAN 都含有一个“Root Switch”，保证 VLAN 中的所有

交换机并不处于同等地位的环上，而是处于具有不同优先级的树结构之上。

提示：

有关 STP 的详细配置信息见本文档第 5 章。

1.4 负载均衡 Load Sharing

Load Sharing 技术将网络流量聚集在一组端口上，用于在交换机之间形成大容量通道或容错通道，通道之间可以实现流量均衡。

Hammer10000 IP-DSLAM 接入交换机支持 Load Sharing 功能，通过创建 Load Sharing 来提升交换机之间的带宽。Load Sharing 把多个物理端口捆绑在一起当作一个逻辑端口来使用。

Load Sharing 的作用表现在以下几个方面：

- 如果Load Sharing中的一个端口发生堵塞或故障，那么数据包会被重新分配到该Load Sharing中的其他端口进行传输。
- 如果这个故障端口重新恢复正常，那么数据包将重新分配到该Load Sharing中的所有端口进行传输。

Hammer10000 IP-DSLAM 接入交换机的 Load Sharing 功能与 Intel 和 Cisco 同类产品的 Port Group 功能兼容。

提示：

有关端口 Load Sharing 的详细配置信息见本文档第 3 章内容。

1.5 网络组管理协议监听 IGMP Snooping

IGMP（Internet Group Management Protocol ）网络组管理协议是 IP 协议组中的一部分，用来支持和管理主机与组播路由器之间的 IP 组播。组播允许进行资源发现，使网络负载减到最小，在网上实现数据的有效传输。

IGMP Snooping 用于监听主机与路由器间的 IGMP 报文，并对监听到的 IGMP 报文进行处理。IGMP Snooping 使交换机能够跟踪与之物理相连的网络上每个组的成员。它在主机和直接邻接的组播路由器间运行，管理组成员关系。

提示：

有关端口 IGMP Snooping 的详细配置信息见本文档第 7 章内容。

1.6 中继代理 DHCP Relay

DHCP 通过中继代理（DHCP Relay）实现主机与非本地网络服务器的联系。当 DHCP Relay 接收到来自主机的 DHCP 申请时，它将申请转发到服务器。DHCP 中继修改 DHCP 请求报文，标识请求主机所在的子网，然后，DHCP Relay 将报文直接传送给 DHCP 服务器。DHCP 服务器为主机分配一个适当的 IP 地址，并将请求返回给 DHCP Relay，DHCP Relay 再将它传送给请求客户系统。

提示：

有关 DHCP Relay 的详细配置信息参见第 8 章内容。

1.7 Proxy ARP

Proxy ARP 的实现基于 RFC925、RFC1027 和 RFC3069，其目的是为属于同一网段却不属于同一广播域的终端提供 ARP 报文的代理中继，配置代理 ARP 的功能就是使用 ARP 代理来实现 Sub VLAN 之间的通信。对于 Hammer10000 IP-DSLAM 接入交换机产品，每个 Super VLAN 中可以配置多个 Sub VLAN，Sub VLAN 不是独立的网络接口，它的作用只是限制广播域。所以原则上讲，这些 Sub VLAN 之间不能互相通信，它们之间的信息相互隔离，这就保证了用户隐私数据的安全。如果出现需要通信的情况，就需要启动 Proxy ARP，使指定的 Super VLAN 下的 Sub VLAN 之间能够通信，同时，每个用户仍然处于自己的广播域，用户互通的同时并不会泄漏私有数据。

提示：

有关 Proxy ARP 的详细配置信息参见第 9 章内容。

1.8 802.1x 认证服务

港湾网络有限公司的 Hammer10000 IP-DSLAM 接入交换机支持 802.1x 认证服务。IEEE 802.1x 称为基于端口的访问控制协议（Port Based Network Access Control Protocol），该协议在利用 IEEE 802 LAN 的优势基础上提供了对连接到局域网的设备或用户进行认证和授权的一种手段。通过此方式的认证，能够在 LAN 这种多点访问环境中提供一种点对点识别用户的方式。

提示：

有关 802.1x 认证服务的详细讲解请见第 10 章内容。

1.9 PPPoE 终结

Hammer10000 IP-DSLAM 接入交换机内置 PPPoE 终结，由主控板（SMU）完成 PPPoE 用户接入认证过程，由业务板（ADU）完成 PPPoE 数据报文到以太网报文的转换。

内置 PPPoE 终结支持 PPPoE 端口间的网段内隔离，其隔离工作由业务板完成。每块业务板须配置一网关地址（IP/掩码），被隔离端口所获取 IP 地址须在同一网段。

提示：

有关 PPPoE 终结的详细讲解请见第 12 章内容。

第2章 访问交换机

本章内容主要涉及管理 Hammer10000 IP-DSLAM 接入交换机所需要的一些知识，包括：

- 理解命令语法
- 常用命令
- 设置用户访问权限
- 管理交换机的途径
- 配置静态路由
- 存取配置文件
- ping命令

 **注意：**

如果您想使对设备的配置内容在设备重新启动或关机再开启后仍能有效，请切记在进行配置后使用“ save configuration ”命令把配置保存到设备中。具体请参见本章稍后关于常用命令的介绍。

2.1 理解命令语法

这一节主要讲述通过命令行配置 Hammer10000 IP-DSLAM 接入交换机时对命令语法的理解和使用，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。

2.1.1 命令输入规则

使用命令行接口 Command Line Interface（CLI）输入命令，请按照以下步骤进行：

第一步：进入命令行接口，当出现命令提示符后，请确认您有登录 HammerOS 的相应权限。

Hammer10000 IP-DSLAM 接入交换机操作系统包含两种不同权限：一种是管理员权限，拥有对所有命令的配置权；另一种是普通用户权限，没有配置权，只有对部分内容的查看权。同时，Hammer10000 IP-DSLAM 接入交换机还设有两种管理模式：只读模式和配置模式。在只读模式下只有对接入交换机配置信息的查看权，而在配置模式下除了可以查看接入交换机的所有配置信息以外，还拥有对接入交换机的配置管理权。具有管理员权限的用户能够在这两种模式下操作，而具有普通用户权限的用户只能在只读模式下操作。

如果以普通用户身份登录，您只能在只读模式下操作，命令提示符为“ Harbour> ”。如果以系统管理员身份登录，您在两种模式下均可以操作，如果是在配置模式下，命令提示符为

“ Harbour(config)# ”。

提示：

首次登录请用系统缺省用户帐号，该帐号为管理员帐号，用户名：admin，密码：harbour。

第二步：输入完整的命令

如果键入的命令不含有任何需要用户输入的参数，请直接跳到第三步。如果键入命令中含有需要用户输入的参数，则继续以下步骤。

- 如果命令需要输入一个参数值，请输入这个值。在输入参数值时，可能需要输入关键字。命令的参数值部分一般指定了您应该输入什么样的参数，例如该参数可能是某个范围内的整数值，或者是一个字符串，或者是一个IP地址等等。关键字是指命令中要操作的对象。
- 如果命令需要输入多个参数值，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<cr> Just Press Enter to Execute command! 为止。

第三步：请按回车键执行命令。

【举例 1】 用户不需要输入参数的情况：

Harbour(config)# exit

“ exit ” 是一个不含参数和关键字的命令。命令名称为 exit。当键入此命令后，按回车则执行该命令。

【举例 2】 用户需要输入参数的情况：

Harbour(config)# config port 0:1 speed 10

其中，“ config port 0:1 speed 10 ” 是一个含有参数和关键字的命令。命令名称为 config，关键字为 port 和 speed，参数值为 0:1 和 10 。

提示：

当用户输入错误的命令或参数时，系统会给予提示信息，通知用户错误的原因。但有两种情况例外，那就是字符“ ！ ”和“ # ”。HammerOS 系统规定，字符“ ！ ”和“ # ”后面的所有内容均为注释信息，不作为配置命令的一部分。因此，当您输入配置命令时，如果在命令当中的某个空格后输入了“ ！ ”或者“ # ”，

那么该字符后的内容将不被处理，此时系统则认为您输入的命令不完全。如果是在命令的最开始处输入了“ ！ ”或者“ # ”，则相当于没有输入命令。

2.1.2 语法帮助

1．“ ？ ”的使用

命令行接口中内置有语法帮助。如果您对某个命令的语法不太确定，请输入该命令中您所知道的前面部分，然后键入“ ? ”，此时命令行会提示您该命令的含义或作用，如果您在命令的后面输入“ 空格 + ？ ”，此时命令行会提示您在已经输入的部分命令之后可能出现的命令清单。您可以根据其中的提示继续输入命令，直至出现

<cr> Just Press Enter to Execute command!

该提示信息表明命令输入完毕，按回车执行所键入的命令。

【举例】 获取 who 命令的帮助信息

第一步：键入命令：

Harbour>who

第二步：

- 如果接着键入“ ？ ”，系统显示如下信息：

who Display who is connected to the switch.

此信息说明 who 命令所要完成的功能；

- 如果接着输入“ 空格 + ？ ”，系统显示如下信息：

am Display me myself who is connected to the target machine.

<cr> Just Press Enter to Execute command!

此信息说明 who 后面可以继续键入 am 构成新的命令，或者直接按回车键执行 who 命令。

2．help 的使用

系统给用户设置了帮助信息，获取此信息，键入命令：

Harbour>help

HammerOS provides help feature as described blow.

1. Anytime you need help, just press "?" and don't

press Enter,you can see each possible command argument

and its description.

2. You can also input "list" and then press Enter

to execute this helpful command to view the list of

commands you can use.

根据提示信息得知可通过以下两种方法获得 HammerOS 提供的帮助信息：

1）在命令行中输入“ ？ ”号，不需按回车键，就可以看到每一个可能的命令参数以及相应的命令功能描述。

2）键入命令 list，按回车键，系统将显示当前命令模式下所有的命令清单，您可以从中选择需要的命令。

2.1.3 使用语法帮助补齐命令

用户输入“ Tab ”键后，HammerOS 提供对命令进行补齐的功能。当您输入了一部分命令后，然后输入“ 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。

【举例 1】 对 show 命令进行语法补齐

第一步：只键入命令 show 的前两个字母“ sh ”

```
Harbour>sh
```

第二步：接着按“ Tab ”键，系统会将这个命令补齐，如下所示：

```
Harbour>show
```

【举例 2】 对 show 命令进行语法补齐

第一步：键入命令 show

```
Harbour >show
```

第二步：再输入一空格键，然后按”Tab”键，系统会显示如下信息：

arp dot1x dsl-profile fdb history idle-timeout

igmp-snooping interface ip mirroring nas port

radius services snmp stpd sysattack syscontact

syslocation time version vlan

以上信息就是命令 show 之后可以继续输入的命令，然后按系统的提示信息继续键入您需要的命令。

2.1.4 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，交换机就能够识别该命令，用户可以直接回车执行该命令。但需要用户输入的参数如 VLAN 的名字（如例子中的 market）等则要求用户完整输入。

【举例 1】 将端口 0:1-0:5 以 untagged 的方式加入到 market 虚拟局域网中，键入命令：

```
Harbour(config)#config vlan market add port 0:1-0:5 untagged
```

上述命令也可简写为：

```
Harbour(config)#con vl market ad po 0:1-0:5 un
```

上述两条命令完成的功能相同。

注意：

当使用命令简写时，您必须输入足够多的字母，以确保在交换机的众多命令中不会造成歧义。

2.1.5 端口的表示方法

命令语法中使用参数<portlist>来表示 Hammer10000 IP-DSLAM 接入交换机的端口。Hammer10000 IP-DSLAM 接入交换机的端口表示需要两部分条件：插槽号（slot）和端口号（port），插槽号和端口号之间用“：”相隔。端口的表示类型包括以下四种：

1．表示一个端口，例如：

port 3:1

表示插槽 3 上的端口 1。

2．表示多个端口，中间用逗号分开，例如：

port 3:1，4:8，6:10

表示插槽 3 上的端口 1，插槽 4 上的端口 8 和插槽 6 上的端口 10。

3．表示某个插槽上多个连续的端口，用符号“－”连接，例如：

port 2:3－2:15

表示从插槽 2 的端口 3 到端口 15 的所有端口。

4．可以采用以上方式的组合来表示多个端口，例如：

port　2:1－2:4，4:20

表示端口 2:1、2:2、2:3、2:4 和 4:20。

5．主控板端口的表示方法

Hammer10000 IP-DSLAM 接入交换机具有两个主控板插槽，编号分别为 0 和 1。与业务板端口排序方法不同的是，主控板端口排序按从下到上的顺序。即 SMU 板最下方的以太网口为 0:1，若主控板上安装有上行扩展卡，则每个扩展卡上的端口是按照从上到下的顺序编号，参考图 2-1 以帮助用户理解：

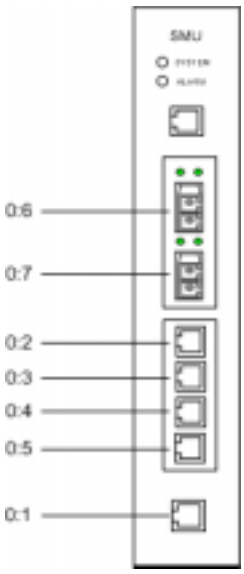


图 2-1 主控板端口排序

2.1.6 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，但不是命令本身的一个部分。表 2-1 对这些符号进行了概要说明。

表 2-1：命令行中的符号

符号	描述
尖括号 <>	尖括号表示此部分必须输入一个参数,该参数可以是字符串、数值范围、IP 地址、端口列表等。 例如命令 create vlan <name>，其中必须在<name>的位置中输入一个合法的字符串作为您所创建的 VLAN 的名字。 当输入的参数超过允许的范围时，系统将拒绝执行这条命令，并显示“ Unknown Command ”作为提示信息。
中括号 [ ]和竖直线 |	中括号一般和竖直线配合使用。中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： service telnet[enable|disable] 其中，中括号内包含由竖直线分隔的两个可选项，您必须输入 enable 或者 disable。如果中括号中只有一个可选项，那就直接输入那个可选项即可。
大括号 { }和星号 *	大括号一般和星号配合使用。大括号括起来的部分表示这部分命令可以不输入，也可以重复输入。重复输入的次数由大括号后紧跟的那个星号后的数字指定。 例如命令： show vlan {<name>}*1 表示您可以直接输入 show vlan ，也可以在 show vlan 后加上已经创建的某个 VLAN 的名字。 大括号中的命令可以输入 0-n 次。这个 n 的值由星号后的数字指定。此例中 n＝1，表示<name>参数可以出现 1 次。

2.1.7 命令参数类型

一般以尖括号“ < > ”括起来的部分是命令参数。HammerOS 的命令参数共有以下四种类型。

数值范围：

当尖括号中是两个数值由减号连接时，表示该参数是取值范围在那两个数值之间的某个数。

例如：<1-255>表示用户可以输入大于等于 1 并且小于等于 255 之间的任意一个整数，比如 2 就是一个合法的数字。

IP 地址：

当尖括号中是 A.B.C.D 时，表示该参数是一个 IP 地址，您必须输入一个合法的 IP 地址值。例如：192.168.0.1 就是一个合法的 IP 地址值。

端口列表：

当尖括号中是 portlist 时，表示该参数是输入端口列表。端口列表中的多个端口之间用逗号“ , ”分隔，如果是连续的多个端口号可以用该连续端口的最小端口再加上减号“ － ”，再加上该连续端口的最大端口号表示。

例如：端口 2:2，2:5-2:10，2:20 表示的端口列表为：插槽 2 上的端口 2、5、6、7、8、9、10、20。

字符串：

当尖括号中所列的不是以上三种情况时，可能表示该参数需要输入的是一个字符串或者是一个 16 进制的数，具体可以在输入命令到该参数部分时，输入“ 空格+？ ”键查看该部分参数的命令说明。

例如：<macaddr> 表示要输入的是一个 16 进制的 MAC 地址，输入 005023344325 为一个合法的 MAC 地址，<name>则表示要输入一个字符串作为某个对象的名字。

2.1.8 行编辑命令

表 2-2 列出了在命令行中可以使用的行编辑命令。

表 2-2：命令行中的行编辑命令

符号	描述
BackSpace 键或 Del 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	整行删除
Ctrl+w	将光标左边的字符全部删除

提示：

上述命令中的 Del 键、向上箭头键、向左箭头键、向右箭头键和向下箭头键命令只支持利用 Telnet 来配置交换机的方式，不支持串口配置。而命令 Ctrl+h、Ctrl+p、Ctrl+b、Ctrl+f 和 Ctrl+n 对上述两种登录方式均支持。

2.1.9 历史命令（history）的使用

HammerOS 能记住用户最近输入的 20 个历史命令。您可以使用 show history 命令来显示已经输入过的命令清单，最多显示 19 条命令，这是因为 show history 命令本身也作为 20 个历史命令之一。您可以通过 Ctrl+b 或 Ctrl+n 键调用上一个或下一个历史命令，其操作方法请见上表 2-2。

【配置实例】显示最近使用过的历史命令

```
Harbour> show history
  list
  ex
  list
  show fdb mac
  show fdb mac 00:01:10:55:10:19
  show fdb vlan
  show vlan
  show fdb vlan
  show fdb vlan uplink
  show fdb agingtime
  show fdb
```

2.2 常用命令

这节主要讲述命令行中常用的一些命令，特定功能的命令将在以后的章节专门讲述。HammerOS 的命令行提供了两种操作模式，一种是只读模式，另一种是配置模式。在只读模式下用户可以查看大部分系统配置信息，在配置模式下用户能够查看所有系统配置信息，并能修改系统配置。此外，在配置模式下通过某些命令还可以进入某种协议的独立配置模式，如 CC 模式。

表 2-3：命令行操作模式

操作模式	描述	命令提示符
只读模式	查看部分系统配置信息	以“ > ”结尾，Harbour>
配置模式	查看、修改所有系统配置信息	以“ # ”结尾 Harbour(config)#

从只读模式进入配置模式的命令为“ enable ”，操作如下：

```
Harbour>enable
password：
```

输入进入配置模式密码后按回车便可进入配置模式，其显示为：

```
Harbour(config)#
```

退回上一级命令模式，使用命令：exit

2.2.1 show version

【命令作用】显示 Hammer10000 IP-DSLAM 接入交换机所插有的全部板卡或部分板卡的版本信息。

【命令语法】show version [all |<0-15>]

【使用指导】当选择 all 时，将显示交换机上所插有的全部板卡的版本信息；

当输入 0-15 时，将显示交换机上单一板卡的版本信息。

【命令模式】运行于只读模式和配置模式。

【配置实例】显示位于插槽 6 板卡的版本信息。

```
Harbour(config)# show version 6
--------- Board In Slot  6 Version Information ---------

   Board          Type : ADU_GS_32
   Hardware     Version : V .2
   FPGA         Version : A 1.3
   CPLD         Version : 1.0
   ADU Serial    Number : API-71
   ADU  Firmware Version : X3727
   ADU   Vendor     ID : GSPN

-------------------------------------------------------
```

2.2.2 enable

【命令作用】由只读模式进入配置模式。

【命令语法】enable

【命令模式】运行于只读模式。

【配置实例】由只读模式进入配置模式。

```
Harbour> enable
Password：
Harbour(config)#
```

2.2.3 terminal length

【命令作用】设置终端每屏显示的行数。

【命令语法】terminal length <value>

【使用指导】length <value>表示指定的行数，范围 0～512，缺省配置为 20 行。如果将参数 length 设为 0，则表示对每屏显示的行数不作限制。

【命令模式】运行于只读模式和配置模式。

2.2.4 who

【命令作用】显示当前有哪些用户连接到目标机器。

【命令语法】who

who am i

【命令模式】运行于只读模式和配置模式。

【使用指导】命令 who 显示所有连接到交换机的用户信息，而命令 who am i 只显示自己的信息。

【配置实例】

```
Harbour(config)# who
---SessionID---UserName---LOCATION----MODE----
5            admin      console    CONFIG(That's me.)
Total 1 sessions in current system.

Harbour(config)# who am i
I am Session [5] : user admin connected from console.
```

2.2.5 list

【命令作用】显示当前模式下的所有命令及其相应参数。

【命令语法】list

【命令模式】运行于只读模式和配置模式。

2.2.6 show services

【命令作用】显示系统服务如 Telnet、SNMP 等服务的状态是开启（up）还是关闭（down）。

【命令语法】show services

【命令模式】运行于只读模式和配置模式。

【配置实例】

```
Harbour(config)# show services
Service telnet is up.
Service snmp agent is down.
Trap support is down.
```

2.2.7 save configuration

【命令作用】把当前正在运行的配置写到设备的 Flash 中并保存。

【命令语法】save{configuration}*1

【命令模式】运行于配置模式。

【使用指导】如果您想让当前所作的配置在设备断电或重新启动后依然有效，切记一定要事先使用此命令保存您的配置。

2.2.8 quit

【命令作用】退出 Hammer10000 IP-DSLAM 接入交换机的 HammerOS 系统。

【命令语法】quit

【命令模式】运行于只读模式和配置模式。

【使用指导】命令 quit 与命令 logout 作用相同。

【配置实例】

```
Harbour(config)# quit
Quit.
Disconnected.
Thanks for using Harbour Networks's product.
Bye!
```

【相关命令】logout

2.2.9 logout

【命令作用】退出 Hammer10000 IP-DSLAM 接入交换机的 HammerOS 系统。

【命令语法】logout

【命令模式】运行于只读模式和配置模式。

【使用指导】命令 logout 与命令 quit 作用相同。

【配置实例】使用 logout 命令

```
Harbour(config)# logout
Quit.
Disconnected.
Thanks for using Harbour Networks's product.
Bye!
```

【相关命令】quit

2.2.10 show idle-timeout

【命令作用】显示 idle timeout（空闲超时）时间。该时间是指对 Hammer10000 IP-DSLAM 接

入交换机进行的相邻两次操作之间所允许的最大空闲时间。当超过该时间时系统将自动执行 logout 操作。

【命令语法】show idle-timeout

【命令模式】运行于只读模式和配置模式。

【使用指导】空闲时间是指在此时间段内未对系统作任何操作，使用 idle-timeout <value>命令可以指定空闲时间，超过这个时间后，退出系统并断开与交换机的连接。

【配置实例】

```
Harbour(config)# show idle-timeout
Idle time out is set to 10 minutes.
```

【相关命令】使用 idle-timeout <0-35791>命令可以设置这个超时时间，单位是分钟，设置为 0 表示总是处于连接状态。

2.2.11 exit

【命令作用】退出当前模式，返回上一模式。

【命令语法】exit

【命令模式】运行于只读模式和配置模式。

【使用指导】在普通用户模式下执行此命令，系统将退出 HammerOS 系统，与 quit 和 logout 效果一样。在配置模式下执行此命令将退回到只读模式。

【配置实例】

使用 exit 命令 (普通用户模式)

```
Harbour> exit
Exit
Disconnected.
Thanks for using Harbour Networks's product.
Bye!
```

使用 exit 命令 (管理员配置模式)

```
Harbour(config)# exit
Harbour>
```

【相关命令】quit,logout

2.2.12 常用命令列表

表 2-4 列出了只读模式下的常用命令。

表 2-4：只读模式下的常用命令

符号	描述
clear	清除屏幕信息
enable	进入配置模式，可以对交换机进行配置和写操作
exit	退出当前配置模式，返回到上一级配置模式
help	显示如何使用命令行中的语法帮助。
list	显示当前可用的命令列表。
logout	退出登录，断开连接
quit	退出命令行，断开连接（这个命令跟 logout 作用相同）
show history	显示已输入的历史命令
show services	显示当前系统提供的服务
show version [all |<0-15>]	显示板卡的版本信息
terminal length <value>	设置终端每屏输出的行数
who	显示当前连接到交换机的用户
who am i	显示当前用户信息
show idle-timeout	显示空闲超时时间
show time	显示系统当前时间

只读模式下除了 enable 以外的所有命令在配置模式下都有效，所以在表 2-5 列出配置模式下常用命令时就不再重复这些命令，配置模式下常用命令比较多，具体见附录。

表 2-5：配置模式下的常用命令

符号	描述
enable-password	修改自己进入配置模式的密码
config time <1970-2069> <1-12> <1-31> <HH:MM:SS>	配置系统时间
erase {startup-config}*1	删除交换机中保存的系统启动配置信息
hostname <hostname>	给交换机重新起个名字，例如本交换机缺省主机名为 Harbour
idle-timeout <value>	设置 Hammer10000 IP-DSLAM 接入交换机经过多长的空闲等待后系统自动进入登录前的状态
show running-config	显示系统当前正在运行的配置
show startup-config	显示系统的启动配置
save {configuration}*1	把当前正在运行的配置写到交换机中并保存。
config syscontact <.contact>	这个域用于存放负责管理交换机的人名及联系方式
config syslocation <.location>	这个域是留给用户设置的，表示该交换机所在的位置

注意：

HammerOS 的命令行的所有命令都是不区分大小写的。

2.3 设置用户访问权限

HammerOS 中提供了两种用户权限：

- ADMIN 管理员
- NORMAL普通用户

普通用户登录到 HammerOS 系统后，只能进入只读模式而不能进入配置模式。普通用户能查看大部分系统信息，只有以下信息对普通用户是不可见的：

- 系统中的用户信息
- 系统的配置信息（主要指系统中的配置文件内容以及系统全局配置信息）

管理员能进入配置模式并对系统的所有参数进行查看和设置。系统管理员还能增加、删除用户帐号，设置修改用户密码，修改用户权限，以及进行系统全局信息的配置。

2.3.1 系统缺省用户帐号

系统内置了一个缺省用户帐号，用户名是 admin，缺省密码是 harbour，该用户属于管理员。缺省用户 admin 的帐号不能被删除，用户名也不能被修改，只能修改它的密码。

2.3.2 增加用户帐号

可以按照以下步骤建立用户帐号：

1. 以用户名 admin 登录（或者用任何其他管理员的用户帐号登录）；
2. 输入 enable 命令进入配置模式；
3. 输入以下命令创建一个用户帐号：

【命令语法】user add <username> login-password <login_password>

【使用指导】其中<username>是所要添加用户的名称，用户名必须是以字母开头的、只包含大写或小写英文字母、数字、下划线且长度为 4-20 的字符串。<login_password>是该用户的登录密码，可以是由任意字符组成的长度为 6-20 的字符串。

注意：

系统对于用户名是不区分大小写的，对密码区分大小写。

通过上述方法创建的用户一般都是普通用户，如果想要创建一个管理员的用户帐号，可以在按照以上步骤创建完用户帐号后，对用户权限进行修改。具体见本章修改用户权限一节。

【配置实例】增加一个用户，用户名为 manager，登录密码为 harbour，在配置模式下操作。

```
Harbour(config)# user add manager login-password harbour
Successfully added user manager as a NORMAL_USER ,
To change user role use "user role" command .
```

表明用户已经成功添加。

2.3.3 修改用户权限

由于本系统中有两个不同级别的用户，所以具有管理员权限的用户通过以下两条命令可以将管理员用户转变为普通用户，也可以将普通用户转变为管理员用户。

1．将一个普通用户设为管理员，使用命令：

【命令语法】user role <username> ADMIN enable-password <enable_password>

【使用指导】其中<username>是该用户的用户名，<enable_password>是该用户进入配置模式的密码。在初次登录使用时，系统的缺省管理员的用户名是 admin，系统管理员的缺省密码是 harbour。在完成登录后，就可以进行与用户相关的操作。

2．将管理员设为普通用户，使用命令：

【命令语法】user role <username> NORMAL

【使用指导】其中<username>是该管理员的用户名。

【配置实例 1】将添加的普通用户 manager 的权限改为系统管理员，设其进入配置模式的密码为 harbour，在配置模式下进行操作：

```
Harbour(config)# user role manager admin enable-password harbour
Successfully change user manager to ADMIN mode.
```

【配置实例 2】将 manager 用户从系统管理员权限变为普通用户，在配置模式下，键入命令：

```
Harbour(config)# user role manager normal
```

按回车，显示如下信息：

```
Successfully change user manager to NORMAL mode.
```

表明用户权限已经成功修改。

2.3.4 查看系统用户信息

查看用户列表，在配置模式下，键入命令：

```
Harbour(config)# user list
```

按回车，显示如下信息：

```
UserName --------------- User_role ----------
admin                   ADMIN_USER
manager                 NORMAL_USER
Total 2 users in system.
```

2.3.5 删除用户帐号

可以用以下命令删除一个用户帐号：

【命令语法】user delete <username>

【使用指导】其中<username>是被删除用户的用户名。

【配置实例】删除用户 manager，键入命令：

```
Harbuor(config)# user delete manager
```

按回车即可。此时，再键入命令：

```
Harbour(config)# user list
```

按回车，显示如下信息：

```
UserName --------------- User_role ----------
admin           ADMIN_USER
Total 1 users in system.
```

说明用户 manager 已经被删除。

2.3.6 修改密码

1．管理员修改自己进入配置模式的密码

管理员除了能修改自己的登录密码外，还能修改自己的进入配置模式的密码，可以用以下命令修改自己的进入配置模式的密码：

```
enable-password
```

然后在提示符下输入并确认自己的新密码。

2．管理员修改其他用户的登录密码进入配置模式的密码

管理员还能够重新设置用户的密码，用以下命令：

【命令语法】user login-password <username>

user enable-password <username>

然后在提示符下输入并确认新密码。

2.4 管理 Hammer10000 IP-DSLAM 接入交换机的途径

Hammer10000 IP-DSLAM 接入交换机主要有以下几个管理途径：

- 使用一个终端（或者仿终端软件）连接到Hammer10000 IP-DSLAM接入交换机的串口（Console），从而通过终端来访问Hammer10000 IP-DSLAM接入交换机的命令行接口（CLI）。
- 使用Telnet管理Hammer10000 IP-DSLAM接入交换机。
- 使用SNMP管理软件管理Hammer10000 IP-DSLAM接入交换机。

Hammer10000 IP-DSLAM 接入交换机同时能支持多个连接：

- 一个Console口连接
- 最多同时能支持4个Telnet连接
- 最多同时能支持4个用户连接
- 一个用户最多同时开2个连接

2.4.1 通过配置口管理 Hammer10000 IP-DSLAM 接入交换机

可以通过将配置电缆连接到 Hammer10000 IP-DSLAM 接入交换机面板前端标有“ CONSOLE ”字样的接口进行管理。

连接 Console 口的超级终端配置如下：

- 波特率　　：9600
- 数据位　　：8
- 奇偶校验　：无

- 停止位　　：1
- 流量控制　　：无

更改串口波特率的命令如下：

【命令语法】config terminal Baudrate [115200|9600]。

【使用指导】波特率可设定为 9600bps 或者 115200bps。系统启动后 Console 口默认的波特率为 9600bps。

提示：

有关串口线针的情况和各个针的含义请参阅《硬件安装指导手册——Hammer10000 IP-DSLAM 接入交换机》。在使用 Console 口连接 Hammer10000 IP-DSLAM 接入交换机时，推荐用户使用 VT100 终端仿真。

设置 VT100 终端仿真的方法是：在超级终端界面中，打开文件菜单，选择属性工具条，出现一个窗口，点击设置标签，在终端仿真下拉列表中选择 VT100 即可，如下图所示：

图 2-2 选择终端仿真类型

一旦连接成功，在终端看到操作系统启动的界面后，您就可以通过命令行接口对设备进行配置了。

可以通过以下步骤利用 Console 连接登录到 Hammer10000 IP-DSLAM 接入交换机：

第一步：将 Hammer10000 IP-DSLAM 接入交换机的 Console 口和特定终端连接起来，正常给设备供电。

第二步：待 HammerOS 成功启动后，可以看到 Hammer10000 IP-DSLAM 接入交换机的登录提示信息：

```
############################################################
#                                                          #
#                   Welcome to HammerOS.                   #
#                                                          #
#      Press Return to connect and config this system.     #
#                                                          #
############################################################
```

按回车键进行登录。

第三步：此时，系统要求您输入用户名和密码。

- 如果您是首次登录，您应该使用缺省的用户名admin，此时输入登录密码harbour，按回车键进入只读模式，再输入enable，按回车，键入配置模式缺省密码harbour，回车后进入配置模式。此时您就可以以系统管理员的身份进行操作，并可使用Hammer10000 IP-DSLAM 接入交换机的所有功能。
- 如果您已经分配了一个自己的用户名和密码，而且您已有系统管理员的权限，那么，登录时就使用自己的用户名和密码。

第四步：当您成功登录交换机并进入配置模式时，系统显示如下信息：

```
Harbour(config)#
```

表明您可以对 Hammer10000 IP-DSLAM 接入交换机进行配置操作了。

第五步：给 Hammer10000 IP-DSLAM 接入交换机配置 IP 地址。

给 Hammer10000 IP-DSLAM 接入交换机配置 IP 地址可以使用以下命令：

```
Harbour(config)# config vlan default  ipaddress 192.168.1.232/24
```

其中，192.168.1.232/24 是要给此交换机设置的 IP 地址加子网掩码长度，成功执行该命令后，便可从 Hammer10000 IP-DSLAM 接入交换机的端口上以该 IP 地址 Telnet 登录到设备的命令行接口。

第六步：保存配置，键入命令：

```
Harbour(config)# save configuration
```

按回车，当出现如下提示信息时：

Are you sure to save the current configuration?[Y/N]y

Trying save configuration to flash, please wait .....

Preparing configuration data to save...Done.

Starting write configuration data to flash...Done.

Configuration save to flash successfully.

表明系统向 Flash 中写入配置信息成功，即保存成功。而且所做的配置立即生效。

第七步：当您完成对 Hammer10000 IP-DSLAM 接入交换机的操作后，键入命令：

```
Harbour(config)# logout  或
Harbour(config)# quit
```

此时可以断开与 Hammer10000 IP-DSLAM 接入交换机的连接，并退出命令行界面。

2.4.2 通过 Telnet 远程管理 Hammer10000 IP-DSLAM 接入交换机

1．使能或关闭 Telnet 服务

以下命令可以使能或关闭 Telnet 服务，但您必须是以系统管理员的身份登录。

1）使能 Telnet 服务，键入命令：

```
Harbour(config)# service telnet enable
```

按回车，显示信息：

```
Successfully changed telnet service to up.
```

表明 Telnet 服务打开成功。

2）关闭 Telnet 服务，键入命令：

```
Harbour(config)# service telnet disable
```

按回车，显示信息：

```
Successfully changed telnet service to down.
```

表明 Telnet 服务关闭成功。

3）可以用以下命令查看系统提供的 Telnet 服务是否被启用：

```
Harbour(config)# show services
```

如果显示 Service telnet is up. 则表明 Telnet 已经启用；如果显示 Service telnet is down. 则表明 Telnet 已经关闭。

2．使用 Telnet 连接到 Hammer10000 IP-DSLAM 接入交换机

任何一个有 Telnet 功能的工作站都能通过 TCP/IP 网络连接到 Hammer10000 IP-DSLAM 接入交换机，从而实现对设备的远程配置管理。如果使用 Telnet 登录，首先需要为 Hammer10000 IP-DSLAM 接入交换机配置 IP 地址。

在 Telnet 客户端，可通过以下命令连接 Hammer10000 IP-DSLAM 接入交换机进行配置：

【命令语法】telnet <A.B.C.D>

【使用指导】其中，<A.B.C.D>为 Hammer10000 IP-DSLAM 接入交换机的 IP 地址。

【配置实例】某一台 Hammer10000 IP-DSLAM 接入交换机的 IP 地址为 192.168.1.232，在 Telnet 客户端键入命令：

```
Harbour(config)# telnet 192.168.1.232
```

按回车，显示信息如下：

```
Trying 192.168.1.232...
Press Ctrl-Q to abort connect.
Connected to 192.168.1.232.
Press Ctrl-Q to force exit telnet.

HammerOS Release Version1.2 on Hammer10000 IP-DSLAM.

Login:
```

输入用户名和密码进行登录。

3．强制关闭一个非法 Telnet 连接

具有管理员权限的用户可以强制断开一个 Telnet 连接。用 who 命令查看当前连接的用户，如果发现有一个用户连接是非法的，那么可以根据用 who 命令所看到的该连接的 session ID，然后再用以下命令强制断开那个连接。

【命令语法】kill session <1-24>

【使用指导】其中<1-24>是 session ID 的取值范围。如果您输入的 session 是 Console 口连接的，将出现以下提示信息：

```
You can't kill a console session.
```

通过这种方法可以防止非法用户的登录，提高系统的安全特性。

4．Telnet 安全性

这里我们通过增加 Telnet 包过滤功能来加强 Telnet 的安全性。所谓 Telnet 包过滤是指在启用 Telnet 功能以后，管理员用户根据安全需要来指定哪些主机的 Telnet 数据包可以被交换机接受，而那些来自未被指定的主机的 Telnet 数据包将被丢弃。

启动/关闭 Telnet-Filter 功能

【命令语法】config telnet-filter [enable|disable]

【使用指导】enable 表示启动 Telnet-Filter 功能，此时所有的 Telnet 数据包都被丢弃；disable 表示关闭 Telnet-Filter 功能，此时 Telnet 恢复正常。

创建一条 Telnet 表项

【命令语法】create telnet-filter permit <A.B.C.D/M>

【使用指导】选择 permit 用于创建一条 Telnet 表项，表示允许来自网段<A.B.C.D/A.B.C.D>的 Telnet 数据包通过。地址参数中的第二个参数 M 为子网掩码长度。

【配置实例】创建一条 Telnet 表项以允许来自网段 10.10.10.1/24 的 Telnet 数据包通过

```
Harbour(config)# create telnet-filter permit 10.10.10.1/24
```

显示 Telnet-Filter 的配置信息

【命令语法】show telnet-filter

【配置实例】显示 telnet-filter 的配置信息

```
Harbour(config)# show telnet-filter

----------------------TELNET FILTER START----------------------
Telnet_filter is enabled.
Telnet_filter 10.4.1.1/24 permit.
----------------------TELNET FILTER END-----------------------
```

2.4.3 通过 SNMP 配置管理 Hammer10000 IP-DSLAM 接入交换机

简单网络管理协议 SNMP（Simple Network Management Protocol）提供了一种监控和管理计算机网络的系统方法。任何一个网络管理者都可以利用 SNMP 来管理 Hammer10000 IP-DSLAM 接入交换机，这样就要求在管理平台上建立 Management Information Base（MIB），因为网络中的所有变量都存放在 MIB 数据结构中。

1．使能/关闭 SNMP 服务

假定用户对 SNMP 网络知识已经熟悉，按下面方法可以使能和关闭 SNMP 服务：

1）使能 SNMP 服务，键入命令：

```
Harbour(config)# service snmp enable
```

按回车，显示信息：

```
Successfully changed snmp agent service to up.
```

表明 SNMP 服务使能成功。

2）关闭 SNMP 服务，键入命令：

```
Harbour(config)# service snmp disable
```

按回车，显示信息：

```
Successfully changed snmp agent service to down.
```

表明 SNMP 服务关闭成功。

可以用以下命令查看系统提供的 SNMP 服务的状态：

```
Harbour(config)# show services
```

如果显示 Service snmp agent is up，表明 SNMP 服务已经被打开；如果显示 Service snmp agent is down，表明 SNMP 服务已经关闭。

2．SNMP 配置

对 SNMP 的配置主要有以下参数：

Community 字符串：

这一字符串为远程网络管理员配置交换机提供了一种用户确认机制。在交换机上有两种 Community 字符串。读确认 Community 字符串允许对 Hammer10000 IP-DSLAM 接入交换机进行只读访问，缺省值为 public。读写确认 Community 字符串提供了对交换机读写操作的权限，缺省值为 private。

【命令语法】config snmp community [readonly|readwrite] <string>

3．配置 SNMP 的 Trap 功能

网管站（NMS）对网络设备发送各种查询报文，并接收来自被管设备的响应及陷阱（Trap）报文，将结果显示出来。代理（Agent）是驻留在被管设备上的一个任务，负责接收、处理来自网管站的请求报文，然后从设备上其他协议模块中取得管理变量的数值，形成响应报文，反送给 NMS。在一些紧急情况下，如接口状态发生改变，呼叫成功等时候，通过主动发送陷阱 Trap 报文来通知 NMS。

1）打开和关闭代理发送 Trap 报文功能

【命令语法】service snmp trap [enable|disable]

【使用指导】选择 enable，表示打开代理发送 Trap 报文功能；选择 disable，表示关闭代理发送 Trap 报文功能。

2）添加 Trap Receiver 的 IP 地址

【命令语法】config snmp trapreceiver add <A.B.C.D> version [v1|v2c] {community <string>}*1

【使用指导】<A.B.C.D>为增加的 Trap Receiver 的 IP 地址，选择 v1，表示 Trap 的版本是 v1，选择 v2c，表示 Trap 的版本是 v2c；

【配置实例】增加的 Trap Receiver 的 IP 地址为 10.1.30.100，Trap 的版本是 v1，键入命令：

```
Harbour(config)#config snmp trapreceiver add 10.1.30.100 version v1
Successfully added trapreceiver IP address is 10.1.30.100
The trap version is v1
The default trap community is public
```

3）删除 Trap Receiver 的 IP 地址

【命令语法】 config snmp trapreceiver delete <A.B.C.D>

【使用指导】 <A.B.C.D>为 Trap Receiver 的 IP 地址。

4）显示 SNMP 的 Trap Receiver 信息

【命令语法】 show snmp trapreceiver

【配置实例】

```
Harbour(config)# show snmp trapreceiver
IP address              Version         Community
12.12.12.1               v1                public
Total 1 trapreceiver IP address in system.
```

2.5 配置静态路由

静态路由是由用户定义的、一条可使数据包从源地址通过指定路径到达目的地址的路由。当动态路由协议未能创建一条到特定目的的路由时，静态路由就显得尤为重要。还可以通过配置某一静态路由为默认路由，把无路由的数据包发送到默认的网关。用户可以在配置模式下配置 Hammer10000 IP-DSLAM 接入交换机的静态路由信息。

2.5.1 添加静态路由

可以用以下命令增加一条静态路由：

【命令语法】ip route <A.B.C.D/M> <A.B.C.D> {<1-255>}*1

【使用指导】第一个<A.B.C.D> 为目的 IP 地址，M 为子网掩码长度，第二个<A.B.C.D>为下一跳的 IP 地址。

或者用以下命令增加一条静态路由信息：

【命令语法】 ip route <A.B.C.D> <A.B.C.D> <A.B.C.D> {<1-255>}*1

【使用指导】 该命令中将上一条命令的子网掩码长度改成了 IP 形式。

【配置实例】添加一条静态路由，假设其为 C 类地址，目的地址为 192.168.2.88，下一跳地址为 192.168.1.3，此处键入命令：

```
Harbour(config)# ip route 192.168.2.88/24 192.168.1.3
```

或者，键入命令：

```
Harbour(config)# ip route 192.168.2.88 255.255.255.0 192.168.1.3
```

按回车，执行该命令。

2.5.2 显示静态路由

用以下命令显示静态路由信息：

【命令语法】show ip route

【配置实例】在成功执行命令 ip route 192.168.2.88/24 192.168.1.3 之后，显示静态路由信息，键入命令：

```
Harbour(config)# show ip route
Codes: C - connected, S - static, R - RIP,
       >* - selected route

S>* 0.0.0.0/0 [1/0] via 10.16.0.254, harbour
C>* 2.2.2.0/24 is directly connected, pppoe1
```

```
C>* 10.0.0.0/16 is directly connected, uplink
C>* 10.10.1.0/24 is directly connected, server2
S   10.10.1.0/24 [1/0] via 10.11.1.254 inactive
C>* 10.16.0.0/16 is directly connected, harbour
C>* 12.1.0.0/16 is directly connected, server
C>* 192.168.0.0/16 is directly connected, adsl
S>* 192.168.2.0/24 [1/0] via 192.168.1.3, adsl
```

可见，已经成功加入一条静态路由信息：

```
192.168.2.0         255.255.255.0       192.168.1.3
```

2.5.3 删除静态路由

删除静态路由使用如下两条命令：

【命令语法】no ip route <A.B.C.D/M> <A.B.C.D> {<1-255>}*1

或者

no ip route <A.B.C.D> <A.B.C.D> <A.B.C.D> {<1-255>}*1

【使用指导】其中，第一条命令的第一个参数为目的网段的 IP 地址和子网掩码长度，第二个参数为下一跳的 IP 地址。第二条命令中将第一条命令的子网掩码长度改成了 IP 形式。

【配置实例】删除上述加入的那条静态路由，键入命令：

```
Harbour(config)# no ip route 192.168.2.88/24 192.168.1.3
```

或者，键入命令：

```
Harbour(config)# no ip route 192.168.2.88 255.255.255.0 192.168.1.3
```

按回车，执行该命令。

2.6 存取配置文件

在每次对交换机的配置进行修改后，都要对所做的修改进行保存。键入命令：

```
save {configuration}*1
```

此命令将修改后的配置保存到交换机的扩展 Flash 中。当显示如下信息时表明保存配置已经成功：

```
Configuration save to flash successfully。
```

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（例如不小心把交换机配置搞乱了，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交换机中。下载可以有多种方法，可以用 FTP 下载，也可用 Xmodem 下载。

2.6.1 Flash 文件操作

- 查看闪存中的文件

【命令语法】show flash

- 删除闪存中的文件

【命令语法】del file <filename>

【使用指导】闪存中的文件不可随意删除，在升级过程中下错文件后，可以用此命令删除相关文件。

- 重命名闪存中的文件

【命令语法】rename file <name> <newname>

【使用指导】闪存中的文件不可随意被改名，系统按照文件名识别文件的内容，在升级过程中如果下载的文件与系统要求的文件名不符，可以用此命令改过来。

2.6.2 通过 FTP 协议下载文件

第一步：用具有管理员权限的用户通过串口或者 Telnet 登录并进入配置模式。

第二步：正确配置交换机和被下载文件所在的主机，使之能正常通信，并打开主机上的 FTP server，配置登录用户名、密码和被下载文件路径。

第三步：输入命令

【命令语法】`download ftp [hammeros|config-file|cops3000|odiag3000|ooam3000|adufpga |vdubfpga|bootrom|gtiooct|file]<A.B.C.D><username><password><filename>`

【使用指导】其中，<A.B.C.D>为文件所在主机的 IP 地址，<username>是 FTP 的用户名，<password>为 FTP 用户名的密码, <filename>为被下载的文件名。

第四步：等待下载完毕后，输入 reboot 命令重新启动交换机，当显示下面信息时，表明通过 FTP 下载成功：

```
Trying download file from ftp server, please wait...
Successfully finished receiving file.

Trying write file to flash......

Finished.

You've successfully download new image file
Now you can type reboot command to reboot system.
```

2.6.3 通过使用 Xmodem 下载文件

第一步：用具有管理员权限的用户通过串口或者 Telnet 登录并进入配置模式；

第二步：输入命令

【命令语法】download xmodem [hammeros|config-file|cops3000|odiag3000|ooam3000|

adufpga|vdubfpga|bootrom|gtiooct]

第三步：打开串口超级终端的发送文件菜单，选择您所要下载的配置文件并选择 Xmodem 协议，选择发送，系统开始下载指定文件信息。

第四步：等待下载完毕后，当显示下面信息时，表明下载成功：

```
Writing configuration to flash, please wait ...... finished.
Configuration saved to flash successfully.
```

第五步：输入 reboot 命令重新启动交换机。

2.6.4 通过 FTP 上传文件

通过 FTP 协议上传文件，即将 Flash 中的文件上传到主机上，利用命令：

【命令语法】upload ftp [hammeros|config-file|cops3000|odiag3000|ooam3000|

fpga|bootrom|gtiooct|file] <A.B.C.D> <username> <password> <filename>

【使用指导】选择 hammeros 表示上传系统应用程序文件；

选择 config-file 表示上传系统配置文件；

<A.B.C.D>为 FTP 服务器的 IP 地址；

<username>为 FTP 服务的用户名；

<password>FTP 服务的密码；

<filename>为所生成的文件名。

使用该命令，可把文件名为 filename 的文件上载到 FTP 服务器上,并且保存到 FTP 服务器的文件名也为 filename。

【配置实例】 假设地址 10.1.30.92 处存在一 FTP 服务器，用户 user1 为此服务器的合法用户，并具有上传文件的写权限，其读写密码为 drv。在 HammerOS 配置模式下，输入命令：

```
Harbour(config)#  upload  ftp  config-file  10.1.30.92  user1  drv
sysconfig.txt
Trying upload file to ftp server, please wait...
Successfully finished Upload file.
Finished.
You've successfully upload config file.
```

此时交换机的配置信息将被上传到 FTP 服务器指定目录下，以文件 sysconfig.txt 保存。

2.6.5 通过使用 Xmodem 上传文件

通过 Xmodem 协议上传文件，即将 Flash 中的文件上传到主机上：

【命令语法】upload xmodem [hammeros|config-file|cops3000|odiag3000|ooam3000|fpga|bootrom|gtiooct]

【使用指导】选择 hammeros 表示上传系统应用程序文件；选择 config-file 表示上传系统配置文件。

【配置实例】将系统配置信息上传到本地磁盘文件中，按以下步骤进行：

第一步：在配置模式下，键入命令：

```
Harbour(config)#upload xmodem config-file
```

按回车，显示如下信息:

```
Trying upload file by console, please wait...
Trying upload file by console via xmodem protocol......
```

第二步：在超级终端中，选择传送菜单的接收文件，使用的接收协议是 Xmodem，点击接收按钮，出现如下提示信息：

```
Successfully finished upload file.
Finished.

You've successfully upload config file
Upload Complete.
```

到此为止，配置信息上传完毕。

提示：

通过文件的上传和下载，可以很方便的对多台相同配置的 Hammer10000 IP-DSLAM 接入交换机进行配置。

2.7 配置 PVC

2.7.1 配置 PVC 的值

【命令语法】config pvc operation [<VPI:VCI>]

【参数说明】

VPI	VPI 的范围在<0-127>
VCI	VCI 的范围在<17－127>

【使用指导】可以使用 show pvc 命令查看 PVC 的值，确定配置是否成功,这里要注意远端用户 Modem 的 PVC 值要与交换机的 PVC 值一致。

【命令模式】配置模式。

【配置实例】

```
Harbour(config)# config pvc operation 8：35
```

2.7.2 查看 PVC 的值

【命令语法】show pvc

【命令模式】配置模式。

【配置实例】

```
Harbour(config)# show pvc
```

2.8 ping 命令

Hammer10000 IP-DSLAM 接入交换机提供 ping 命令来检测网络基本连接情况：

ping 命令发送 Internet Control Message Protocol (ICMP) echo 消息到网络中的某个 IP 设备。普通用户和管理员用户都可以使用 ping 命令。

【命令语法】ping {[-t]}*1 {[-count] <1-65535>}*1 {[-size] <1-6400>}*1 {[-waittime] <1-255>}*1 {[-ttl] <1-255>}*1 {[-pattern] <user_pattern>}*1 <A.B.C.D>

ping 命令的众多选项可以都不输入，而使用最简单的格式。例如：

```
ping 192.168.0.1
```

以此来测试 Hammer10000 IP-DSLAM 接入交换机是否可以跟 IP 地址为 192.168.0.1 的设备连接通信。

如果设备连通，则出现以下信息：

```
PING 192.168.0.1 : 56 data bytes.
Press Ctrl-c to Stop.

Reply from 192.168.0.1 : bytes=56: icmp_seq=0 ttl=128 time=10 ms
Reply from 192.168.0.1 : bytes=56: icmp_seq=1 ttl=128 time=5 ms
Reply from 192.168.0.1 : bytes=56: icmp_seq=2 ttl=128 time=5 ms
Reply from 192.168.0.1 : bytes=56: icmp_seq=3 ttl=128 time=5 ms
Reply from 192.168.0.1 : bytes=56: icmp_seq=4 ttl=128 time=5 ms

----192.168.0.1 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss

round-trip(ms) min/avg/max = 0/36/100
```

如果设备没有连通，出现以下信息：

```
PING 192.168.0.1 : 56 data bytes.
Press Ctrl-c to Stop.

Request time out.
Request time out.
Request time out.
Request time out.
Request time out.

----192.168.0.1 PING Statistics----
5 packets transmitted, 0 packets received, 100% packet loss
```

表 2-6 描述了 ping 的各个选项。

表 2-6：ping 命令选项

符号	描述
-t	使用 t 选项后，ping 命令将一直向目标 IP 地址发送 ICMP echo 消息，直到用户用 Ctrl+c 中断。 缺省不用 t 选项时，ping 命令发送完 5 个 ICMP echo 消息就停止发送了。
-count <1-65535>	count 选项指定 ping 程序总共发送多少个 ICMP echo 消息后就退出 ping 程序。
-size <1-6400>	size 选项指定发送的 ICMP echo 消息的附加内容长度。
-waittime <1-255>	waittime 选项指定 ping 程序等待多少秒之后如果还未收到应答就认为目标不可通。
-ttl <1-255>	ttl 选项指定 ICMP 数据包的 ttl（time to live）值。
-pattern <user_patter>	pattern 选项指定 ICMP 数据包中用户自己定义的 1-16 个 16 进制数。

第3章 配置端口

这一章主要讲述如何使用 HammerOS 来配置 Hammer10000 IP-DSLAM 接入交换机的端口。Hammer10000 IP-DSLAM 接入交换机包括以太网端口和 xDSL 端口。利用 HammerOS 可以对 Hammer10000 IP-DSLAM 接入交换机的不同端口实现配置，主要包括：

- 以太网端口
- VDSL端口
- ADSL端口

此外，通过配置端口镜像和多端口负载均衡，可以更好地提高 Hammer10000 IP-DSLAM 接入交换机的性能。

3.1 xDSL 端口文件配置

为了方便用户对 Hammer10000 IP-DSLAM 接入交换机的 xDSL 端口进行各种配置，特创建相应类型的端口配置文件，从而使用户可以利用所创建的端口配置文件对同类型端口直接配置，以简化用户操作，节省时间，提高效率。

3.1.1 创建端口配置文件

【命令语法】`create [adsl-profile|adsl-thresh-profile|vdsl-profile] <name>`

【使用指导】选择 `adsl-profile`，表示创建的是 ADSL 端口的配置文件；

选择 `adsl-thresh-profile`，创建的是 ADSL 端口门限值的配置文件；

选择 `vdsl-profile`，创建的是 VDSL 端口的配置文件；

`<name>`为配置文件名。

3.1.2 修改端口配置文件

【命令语法】 `config dsl-profile <name>`

【使用指导】 `<name>`为所要操作的配置文件名。

注意：

当创建或修改配置文件时，系统会自动进入相应 Profile 配置模式，你可以对端口各种属性进行配置，完毕后输入 exit 退回到配置模式。

3.1.3 利用端口配置文件对同类型端口进行配置

【命令语法】config port [<portlist>|all] [attach|detach] dsl-profile <profilename>

【使用指导】选择 attach，表示将指定 profile 与端口关联，并重新刷新端口配置；

选择 detach，表示取消指定 profile 与端口的关联，并重新刷新端口配置；

选择<portlist>，表示将 profile 配置信息运用到指定端口列表；

选择 all，表示将 profile 配置信息运用到所有同类型端口；

<profilename>为所利用的配置文件名。

3.1.4 删除端口配置文件

【命令语法】 delete dsl-profile <profilename>

【使用指导】 <profilename>指所创建的端口配置文件名。

3.1.5 更新端口配置文件

【命令语法】 flush dsl-profile <name>

【使用指导】 <name>指内容发生变化的端口配置文件名。

3.1.6 显示端口配置文件信息

【命令语法】show dsl-profile {<name>}*1

【使用指导】<name>为所要显示的端口配置文件名。如果没有指定端口配置文件名，则显示所有的端口配置文件信息。

3.2 以太网端口基本配置

本节讲述如何对以太网端口属性进行基本配置，主要包括：

- 打开或关闭指定端口
- 打开或关闭指定端口的自适应功能
- 配置端口速度
- 配置端口的半双工或全双工模式
- 配置端口的流控

提示：

其中：自适应模式、双工模式、端口速率 10M/100M 这三个配置都是以太网口 10M/100M 电口的属性，以太网光口没有这三个属性。

3.2.1 使能或禁用端口

端口的状态有两种：enable 和 disable。在缺省情况下，所有 VDU 的端口都是 disable 状态。您也可以利用以下命令来使能或禁用一个或多个指定的端口：

【命令语法】config port [<portlist>|all] [enable|disable]

【使用指导】选择<portlist>，表示对指定端口进行操作。用户可以选择输入某个板卡的某个端口，如 6:1，也可输入某个板卡上的多个连续端口，如 6:1－6:6，还可输入某板卡上多个连续和不连续的端口，如 6:1,6:3-6:6；

选择 all，表示对交换机的所有端口进行操作；

选择 enable 表示使能指定的端口；

选择 disable 表示禁用指定的端口。

【命令模式】运行于配置模式。

3.2.2 配置端口自适应模式

缺省情况下，Hammer10000 IP-DSLAM 接入交换机的以太网电口设置为自适应模式，并根据端口所连接的对端端口的性能自动调整本端口的速度和双工模式。

【命令语法】config port [<portlist>|all] auto [on|off]

【使用指导】选择<portlist>，表示对指定端口进行操作。用户可以选择输入某个板卡的某个端口，如 6:1，也可输入某个板卡上的多个连续端口，如 6:1－6:6，还可输入某板卡上多个连续和不连续的端口，如 6:1,6:3-6:6；

选择 all，表示对交换机的所有端口进行操作；

选择 on 表示将端口设定为自适应（auto）模式；

选择 off 表示关闭端口的自适应模式。

【配置实例】配置端口 0:1 的工作模式为自协商模式：

```
Harbour(config)# config port 0:1 auto on
```

3.2.3 配置端口速率

Hammer10000 IP-DSLAM 接入交换机以太网的端口速率为 10/100Mbps，在自适应模式下将根据对端端口的速率自动进行调整。此外，您也可以通过手工配置将其设为某一种速率，具体如下：

【命令语法】config port [<portlist>|all] speed [10|100]

【使用指导】选择<portlist>，表示对指定端口进行操作。用户可以选择输入某个板卡的某个端口，如 6:1，也可输入某个板卡上的多个连续端口，如 6:1－6:6，还可输入某

板卡上多个连续和不连续的端口，如 6:1,6:3-6:6；

选择 all，表示对交换机的所有端口进行操作；

选择 10， 将端口速度设置为 10Mbps；

选择 100，将端口速度设置为 100Mbps。

【配置实例】 配置端口 0:1 速度为 10Mbps，键入命令：

```
Harbour(config)# config port  0：1  speed 10
```

3.2.4 配置端口双工模式

手工配置端口的双工模式如下：

【命令语法】config port [<portlist>|all] duplex [full|half]

【使用指导】选择<portlist>，表示对指定端口进行操作。用户可以选择输入某个板卡的某个端口，如 6:1，也可输入某个板卡上的多个连续端口，如 6:1－6:6，还可输入某板卡上多个连续和不连续的端口，如 6:1,6:3-6:6；

选择 all，表示对交换机的所有端口进行操作；

选择 full，将端口配置为全双工模式；

选择 half，将端口配置为半双工模式。

【配置实例】配置端口 0:1 为全双工工作模式，键入命令：

```
Harbour(config)# config port  0：1  duplex full
```

3.2.5 配置端口流控

可以用以下命令：

【命令语法】config port [<portlist>|all] flowcontrol [on|off]

【使用指导】选择<portlist>，表示对指定端口进行操作。用户可以选择输入某个板卡的某个端口，如 6:1，也可输入某个板卡上的多个连续端口，如 6:1－6:6，还可输入某板卡上多个连续和不连续的端口，如 6:1,6:3-6:6；

选择 all，表示对交换机的所有端口进行操作；

选择 on，打开端口流量控制；

选择 off，取消端口的流量控制。

【配置实例】配置端口 0:1 流量控制有效，键入命令：

```
Harbour(config)# config port  0：1  flowcontrol on
```

注意：

用户可以手工配置端口的速度、双工模式和流控模式。不过在对端口的速度、

双工模式进行手工配置前必须关闭端口的自适应模式。

3.2.6 显示端口信息

用户可以查看 Hammer10000 IP-DSLAM 接入交换机上所有端口或任意端口的信息，具体如下：

【命令语法】show port [<portlist>|all|active] {[switch-port|stats|stp|vlan-list]}*1

【使用指导】选择<portlist>，表示对指定端口进行操作。用户可以选择输入某个板卡的某个端口，如 6:1，也可输入某个板卡上的多个连续端口，如 6:1－6:6，还可输入某板卡上多个连续和不连续的端口，如 6:1,6:3-6:6；

选择 all，表示对交换机的所有端口进行操作；

选择 active，显示当前活动端口信息；

选择 switch-port，显示上行端口的配置信息；

选择 stats，显示端口的数据统计信息；

选择 stp，显示端口上运行 Spanning Tree Protocol 时的相关信息；

选择 vlan-list，显示端口被配置添加到的 VLAN 列表。

当大括号内的选项都不输入时，系统缺省显示端口的配置信息。

【命令模式】 在只读模式和配置模式下均可执行。

【配置实例】

```
Harbour(config)# show port 0:1
-------------------------------------------------------------------
-------
Port:<0:1> 's Current Value Information

Link state             : Up       Port state             : Enabled
AutoNegotiation         : On       Speed                  : 100BaseTX
Duplex                 : Full     FlowControl            : Off
LockState              : On       DropPacket             : On
Port Default VLAN ID     : 6        Port Default VLAN name    : harbour
-------------------------------------------------------------------
-------
```

注意：

端口类型分为以太网端口、ADSL、VDSL 等，由于多个类型的端口信息显示均使用 show port <portlist>形式，在命令行键入 show port 0：1，键入空格再按“？”，将显示出帮助信息，该帮助信息并非全部选项对指定端口有效，请按照各类型端口的指导说明操作选项。

配置端口属性操作出现的情况和上面类似。

3.3 配置 VDSL 端口

注意：

通常情况下，上述关于端口的基本配置命令同样对 VDSL 端口有效，但本节中关于 VDSL 端口的配置命令只对 VDSL 端口有效。

3.3.1 配置 VDSL 端口上行速率等级

配置 Hammer10000 IP-DSLAM 接入交换机 VDU 板上的 VDSL 端口上行速率等级的具体方法如下：

【命令语法】config port [<portlist>|all] vdsl uprate [r1.04|r2.08|r4.17|r8.33|r10.04|r12.5|r17|rom]

【使用指导】选择<portlist>，表示对指定端口进行操作。用户可以选择输入某个板卡的某个端口，如 6:1，也可输入某个板卡上的多个连续端口，如 6:1－6:6，还可输入某板卡上多个连续和不连续的端口，如 6:1,6:3-6:6；

选择 all，表示对交换机的所有端口进行操作；

速率等级与数据流速率的对应关系请见表 3-1：

表 3-1：速率等级与数据流速率对应关系

速率等级	指定端口指定方向的数据流速率
r1.04	1.04Mbps
r2.08	2.08Mbps
r4.17	4.17Mbps
r8.33	8.33Mbps
r10.04	10.04 Mbps
r12.5	12.5Mbps
r17	17Mbps
rom	当为上行数据流时，速率为 1.56 Mbps 当为下行数据流时，速率为 4.17 Mbps

【命令模式】运行于配置模式。

【配置实例】配置 Hammer10000 IP-DSLAM 接入交换机 VDU 板（假设为 6 槽）上 VDSL 端口 1 的上行速率等级为 r12.5。

```
Harbour(config)# config port 6:1 vdsl uprate r12.5
```

3.3.2 配置端口的下行速率等级

配置 Hammer10000 IP-DSLAM 接入交换机 VDU 板上的 VDSL 端口下行速率等级的具体方法如下：

【命令语法】config port [<portlist>|all] vdsl downrate [r1.04|r2.08|r4.17|r8.33|r10.04|r12.5|r17|rom]

【使用指导】选择<portlist>，表示对指定端口进行操作。用户可以选择输入某个板卡的某个端口，如 6:1，也可输入某个板卡上的多个连续端口，如 6:1－6:6，还可输入某板卡上多个连续和不连续的端口，如 6:1,6:3-6:6；

选择 all，表示对交换机的所有端口进行操作；

速率等级与数据流速率的对应关系请见表 3－1。

【命令模式】运行于配置模式。

【配置实例】配置 Hammer10000 IP-DSLAM 接入交换机 VDU 板（假设为 6 槽）上 VDSL 端口 1 的下行速率等级为 r2.08。

```
Harbour(config)# config port 6:1 vdsl downrate r2.08
```

3.4 配置 ADSL 端口

3.4.1 配置端口的上行/下行速率

在这里，用户可以根据网络的实际情况配置 ADSL 端口上行/下行的最大/最小速率，具体如下：

【命令语法】config port [<portlist>|all] adsl [downrate|uprate] [max|min] <value>

【使用指导】选择<portlist>，表示对指定端口进行操作。用户可以选择输入某个板卡的某个端口，如 6:1，也可输入某个板卡上的多个连续端口，如 6:1－6:6，还可输入某板卡上多个连续和不连续的端口，如 6:1,6:3-6:6；

选择 all，表示对交换机的所有端口进行操作；

选择“downrate”表示配置 ADSL 端口的下行速率，选择“uprate”表示配置 ADSL 端口的上行速率；

选择“max”表示配置端口速率的最大值，选择“min”表示配置端口速率的最小值。同时还要在其后的<value>处输入具体数值，数值范围是：下行速率范围：1～255；上行速率范围：1～32 个单位。

ADSL 承载信道速率是 32Kbps 的整数倍，其默认的最大速率是 8.160Mbit/s，所以下行速率的范围（即 32Kbps 的倍数范围）是 1～255。

注意：

如果无法建立连接或者连接不稳定，建议适当降低线路速率。

【命令模式】 运行于配置模式。

【配置实例】 配置 Hammer10000 IP-DSLAM 接入交换机 ADU 板(假设为 11 槽)上端口 1 的最小下行速率为 100（即 3.2Mbps）。

```
Harbour(config)# config port 11:1 adsl downrate min 100
```

3.4.2 设置端口模式

ADSL 端口有四种工作模式：multimode、g.lite 和 g.dmt、T1.413，具体如下：

【命令语法】 config port [<portlist>|all] adsl mode [multimode|g.lite|g.dmt| T1.413]

【使用指导】

选择<portlist>，表示对指定端口进行操作。用户可以选择输入某个板卡的某个端口，如 6:1，也可输入某个板卡上的多个连续端口，如 6:1－6:6，还可输入某板卡上多个连续和不连续的端口，如 6:1,6:3-6:6；

选择 all，表示对交换机的所有端口进行操作；

设置端口的工作模式，包括 multimode、g.lite、g.dmt、T1.413。

【命令模式】 运行于配置模式。

3.4.3 配置上行/下行噪声容限

通过设置上行/下行数据流的噪声容限可以保证数据的传输质量。

【命令语法】config port[<portlist>|all] adsl noisemargin [downstream] [maximum|target] <value>

config port [<portlist>|all] adsl noisemargin [upstream] [target] <value>

【使用指导】 选择<portlist>，表示对指定端口进行操作。用户可以选择输入某个板卡的某个端口，如 6:1，也可输入某个板卡上的多个连续端口，如 6:1－6:6，还可输入某板卡上多个连续和不连续的端口，如 6:1,6:3-6:6；

选择 all，表示对交换机的所有端口进行操作；

选择“ downstream ”表示配置 ADSL 端口下行数据流的噪声容限；

选择“ upstream ”表示配置 ADSL 端口上行数据流的噪声容限。

噪声容限取值范围见表 3-2：

表 3-2： 噪声容限取值范围

参数	描述	取值范围
maximum	最大噪声容限	0～31dB
target	目标噪声容限	0～31dB

注意：

最大噪声容限须不小于目标噪声容限。 建议采用系统默认值。

【命令模式】运行于配置模式。

【配置实例】配置 Hammer10000 IP-DSLAM 接入交换机 ADU 板(假设为 11 槽)上端口 1 下行速率的最大噪声容限为 20dB。

```
Harbour(config)# config port 11:1 adsl noisemargin downsteam maximum 20
```

3.4.4 配置上行/下行的快速交织模式

【命令语法】config port [<portlist>|all] adsl fimode [fast|interleaved]

【使用指导】选择<portlist>，表示对指定端口进行操作。用户可以选择输入某个板卡的某个端口，如 6:1，也可输入某个板卡上的多个连续端口，如 6:1－6:6，还可输入某板卡上多个连续和不连续的端口，如 6:1,6:3-6:6；

选择 all，表示对交换机的所有端口进行操作；

[fast|interleaved]分别为通道的快速模式和交织模式。快速通道延时低，抗干扰能力差；交织通道延时高，抗干扰能力强。

【命令模式】运行于配置模式。

【配置实例】配置 Hammer10000 IP-DSLAM 接入交换机 ADU 板(假设为 11 槽)上端口 1 的通道模式为快速模式

```
Harbour(config)# config port 11:1 adsl fimodel fast
```

3.4.5 配置上行/下行交织延时

配置端口上行/下行数据流交织延时的方法如下：

【命令语法】config port [<portlist>|all] adsl interdelay [downstream|upstream] <value>

【使用指导】选择<portlist>，表示对指定端口进行操作。用户可以选择输入某个板卡的某个端口，如 6:1，也可输入某个板卡上的多个连续端口，如 6:1－6:6，还可输入某板卡上多个连续和不连续的端口，如 6:1,6:3-6:6；

选择 all，表示对交换机的所有端口进行操作；

选择“ downstream ”表示配置 ADSL 端口下行数据流的交织延时，选择“ upstream ”表示配置 ADSL 端口上行数据流的交织延时。延时可选择的参数为：1, 2, 4, 8, 16, 32 和 64 ，单位为 ms。

【命令模式】运行于配置模式。

【配置实例】配置 Hammer10000 IP-DSLAM 接入交换机 ADU 板(假设为 11 槽)上端口 1 上行数据流的交织延时为 32ms。

```
Harbour(config)# config port 11:1 adsl interdelay upstream 32
```

3.4.6 设置端口门限

可配置的端口门限包括：

- lossframe：帧丢失
- losssignal：信号丢失
- losslink：连接丢失
- losspower：供电丢失
- ess：误码秒数

【命令语法】 config port [<portlist>|all] adsl threshold [lossframe|losssignal |losslink|losspower|ess] <value>

【使用指导】选择<portlist>，表示对指定端口进行操作。用户可以选择输入某个板卡的某个端口，如 6:1，也可输入某个板卡上的多个连续端口，如 6:1－6:6，还可输入某板卡上多个连续和不连续的端口，如 6:1,6:3-6:6；

选择 all，表示对交换机的所有端口进行操作；

配置门限：Hammer10000 IP-DSLAM 接入交换机将下述内容在 15 分钟内出现的次数作为它们的门限：

参数名	描述	取值范围
lossframe	帧丢失门限	范围 0～255，0 表示不对该参数设定门限
losssignal	信号丢失门限	范围 0～255，0 表示不对该参数设定门限
losslink	连接丢失门限	范围 0～255，0 表示不对该参数设定门限
losspower	掉电门限	范围 0～255，0 表示不对该参数设定门限
ess	误码秒数门限	范围 0～255，0 表示不对该参数设定门限

3.4.7 查看端口配置

用户查看 ADSL 端口的配置信息。

【命令语法】show port [<portlist> | all | active] adsl [line-config]

【使用指导】选择 all，表示查看所有端口的配置信息

选择<portlist>，表示查看指定端口的配置值信息

选择 active，显示当前活动端口信息

3.5 端口镜像（Port Mirroring）

端口镜像的概念简而言之就是让一个或多个端口工作在监视模式下，这些被监视的端口称为镜像源端口。在监视模式下，将镜像源端口接收和转发的数据镜像到交换机的某个指定端口上，这个指定的端口被称为镜像目的端口。这样便可以通过镜像目的端口监视镜像源端口数据包的收发统计信息，可以捕捉并查看分析通过源端口的数据包的内容。

Hammer10000 IP-DSLAM 接入交换机支持基于主控板的端口镜像功能，

3.5.1 基于主控板的端口镜像配置

基于主控板配置的端口镜像特性如下：

- Hammer10000 IP-DSLAM接入交换机的主控板上最多可含有四个用于端口和插槽管理的芯片：dev0、dev2、dev3、dev4。每个芯片只允许有一个镜像源端口（source port）。
- 镜像源端口和镜像目的端口必须是对应于不同芯片上的端口。
- 镜像目的端口可以监视到的包类型如下：

源端口转发的数据包

源端口的广播包和未知目的的单播包、IGMP 包

每个芯片分别对应的插槽号和端口号如下：

- Dev0： 端口port：0:1，插槽slot：9～15
- Dev2： 插槽slot：1～8
- Dev3： 端口port：0:2～0:5
- Dev4： 端口port：0:6～0:9

主控板上的端口编号参见 2.1.5 的图 2-1。

用户可以通过命令行配置端口镜像以实现对某端口或某插槽上的数据流量的监视。当配置某插槽作为端口镜像的源端口时，该槽上所有 ADSL/VDSL 端口的数据都被发送到镜像目的端口。

此外 Hammer10000 IP-DSLAM 接入交换机在端口镜像实现的管理上使用了端口镜像组概念。端口镜像组保存了用户配置的源端口和目的端口，每个组中的源端口可以有多个，目的端口只能有一个。Hammer10000 IP-DSLAM 接入交换机支持 32 个镜像组。

基于主控板的镜像配置命令如下表所示，有关配置命令的详细说明请参见本章稍后部分的详细说明。

表 3-3：基于主控板的镜像配置命令

配置命令	功能描述
config mirroring <1-32> to <port>	配置镜像组的目的端口
config mirroring <1-32> add port <portlist>	向镜像组添加源端口
config mirroring<1-32> delete port <portlist>	删除镜像组中的源端口
config mirroring <1-32> add slot <0-15>	向镜像组添加插槽
config mirroring <1-32> delete slot <0-15>	删除镜像组中的插槽
config mirroring <1-32> disable	删除镜像组
show mirroring{<1-32>}*1	根据组号显示镜像组的配置信息
show mirroring	显示所有镜像组的配置信息

提示：

建议只配置一组端口镜像组。由于端口镜像的实现机制，配置多个组可能会引起目的端口捕捉不到源端口上的所有数据包。

3.5.2 配置镜像组目的端口

【命令语法】config mirroring <1-32> to <port>

【使用指导】<1-32>为镜像组的组号，Hammer10000 IP-DSLAM 接入交换机支持 32 个镜像组；<port>为目的端口的端口号，每个镜像组只能有一个目的端口，其中：对基于主控板的镜像配置，目的端口必须和源端口位于不同的设备

【配置实例】配置镜像组 1 的目的端口为 0:1：

```
Harbour(config)# config mirroring 1 to 0:1
```

3.5.3 取消端口镜像

取消一个镜像组在目的端口的应用，可以用如下命令：

【命令语法】config mirroring <1-32> disable

【使用指导】<1-32>为镜像组的组号，使用此命令将取消某个镜像组到目的端口的应用，也就是删除镜像组中的目的端口。

3.5.4 向镜像组添加源端口

【命令语法】config mirroring <1-32> add port <portlist>

【使用指导】<1-32>为镜像组的组号，Hammer10000 IP-DSLAM 接入交换机支持 32 个镜像组；<portlist>为源端口的端口列表，其中：对基于主控板的镜像配置，每个镜像组中可以添加多个源端口，不过只限于主控板上的端口，并且各源端口必须位于不同的设备。

【配置实例】基于主控板的镜像配置，将端口 0:2 和 0:8 作为镜像源端口添加到镜像组 1 中：

```
Harbour(config)# config mirroring 1 add port 0:2, 0:8
```

3.5.5 删除镜像组中的源端口

【命令语法】config mirroring <1-32> delete port <portlist>

【使用指导】<1-32>为镜像组的组号，Hammer10000 IP-DSLAM 接入交换机支持 32 个镜像组；<portlist>为源端口的端口列表。

【配置实例】基于主控板的镜像配置，删除镜像组 1 中的源端口 0:2：

```
Harbour(config)# config mirroring 1 delete port 0:2
```

3.5.6 向镜像组添加插槽

表示某插槽上的所有端口都作为端口镜像的源端口。

【命令语法】config mirroring <1-32> add slot <0-15>

【使用指导】<1-32>为镜像组的组号，Hammer10000 IP-DSLAM 接入交换机支持 32 个镜像组；<0-15>为插槽号，可以添加 1～2 个插槽，当添加 2 个插槽时这 2 个插槽必须属于不同的设备。

【配置实例】将插槽 8 作为镜像源端口添加到镜像组 10 中：

```
Harbour(config)# config mirroring 10 add slot 8
```

3.5.7 删除镜像组中的插槽

【命令语法】config mirroring <1-32> delete slot <0-15>

【使用指导】<1-32>为镜像组的组号，Hammer10000 IP-DSLAM 接入交换机支持 32 个镜像组；<0-15>为插槽号。

【配置实例】从镜像组 10 中删除插槽 8：

```
Harbour(config)# config mirroring 10 delete slot 8
```

3.5.8 删除镜像组

要删除一个镜像组，需要删除镜像组内的源端口、插槽，并取消端口镜像以删除目的端口，如此才能完成删除镜像组的操作。

删除源端口使用命令 config mirroring <1-32> delete port <portlist>。

删除插槽使用命令 config mirroring <1-32> delete slot <0-15>。

删除目的端口使用命令 config mirroring <1-32> disable。

3.5.9 显示镜像组配置信息

【命令语法】show mirroring {<1-32>}*1

或

show mirroring

【使用指导】<1-32>为镜像组的组号，当输入这个参数时，系统将根据输入的组号显示镜像组的信息。当不输入这个参数时，系统将显示所有配置的镜像组信息。

【配置实例】显示镜像组 1 的配置信息

```
Harbour(config)# show mirroring 1
Port Mirror Configurations:

Mirroring Group 1:
         Source Port: 0:1
         Source Slot:
         Target Port: 0:4
```

3.6 多端口负载均衡(Load Sharing)

Hammer10000 IP-DSLAM 接入交换机支持多端口负载均衡（Load Sharing）功能，此功能可以将多个物理端口捆绑在一起作为一个逻辑端口，目的在于提升交换机之间的通信带宽。除此之外，Load Sharing 还可以加强交换机间连接的可靠性，当组内的一个成员端口发生故障时，数据包可以继续在其他端口转发，使连接不中断。

当两台交换机之间通过多个端口连接并传输数据时，创建 Load Sharing 将非常有助于提高设备间的传输速率。

注意：

必须在相互连接的两台交换机上都设置 Load Sharing,并且要对每对直接连接的两个端口进行对应配置，否则会导致交换机不能正常工作

3.6.1 配置 Load Sharing

要设置 Load Sharing，必须创建 Load Sharing 的一组端口，并且这些 Load Sharing 端口在同一个 VLAN 内必须具有相同的 Untagged/Tagged 属性。

Hammer10000 IP-DSLAM 接入交换机中的 Load Sharing 定义必须遵从以下规则：

- 只能对主控板的端口设置Load Sharing
- Hammer10000 IP-DSLAM接入交换机主控板最多可包含四个用于端口和插槽管理的芯片（dev0、dev2、dev3、dev4），每个芯片分别对应的槽插号和端口号如下：

  dev0： 端口 port：0:1，插槽 slot：9～15

  dev2： 插槽 slot： 1～8

  dev3： 端口 port ：0:2～0:5

  dev4： 端口 port ：0:6～0:9

只能在 dev3 或 dev4 上创建 Load Sharing 组，属于一个 Load Sharing 组的所有端口必须是对应同一个芯片上的端口。

定义一个 Load Sharing 组，可以选取其中一个端口作为主端口，这个主端口在逻辑上代表这个 Load Sharing 组。创建或删除一个 Load Sharing 组可以用以下命令：

1．创建一个 Load Sharing 组，键入命令：

【命令语法】create sharing <string> grouping <portlist>

【使用指导】其中，< string >为主端口号，<portlist>为该 Load Sharing 组的成员端口列表。

【配置实例】创建一个 Load Sharing 组，其中包括端口 0:3～0:5，设置 0:3 为主端口

```
Harbour(config)# create sharing 0:3 grouping 0:3-0:5
```

2．删除一个 Load Sharing 组，键入命令：

【命令语法】delete sharing <string>

【使用指导】其中< string > 表示所创建的 Load Sharing 的主端口号。

注意：配置 Load Sharing 之前，应该配置所有成员端口的各种属性参数相同，以保证成员端口状态一致达到负载均衡和故障冗余目的。这些参数包括：自适应模式、速率、双工模式、流控以及端口 STP 的各种属性配置，同时注意取消端口镜像配置以免额外带宽占用，影响线速转发。

3.6.2 显示 Load Sharing 配置信息

利用 show sharing 命令可以查看 Load Sharing 的配置信息，例如：

```
Harbour(config)# show sharing
Sharing port group  1 information:
    Master Port: 0:3  Group Ports: 0:3  0:4  0:5
```

3.7 端口配置命令列表

表 3-4 列出了 Hammer10000 IP-DSLAM 接入交换机的所有端口配置命令。

表 3-4：Hammer10000 IP-DSLAM 接入交换机的端口配置命令表

端口类型	命令	描述
端口基本命令	config port [<portlist>|all] [enable|disable]	打开或关闭指定端口
	config port [<portlist>|all] auto [on|off]	打开或关闭指定端口的自适应功能
	config port [<portlist>|all] speed [10|100]	切换指定端口的速度至 10 MBps 或者 100MBps
	config port [<portlist>|all] duplex [full|half]	设置端口的双工模式为全双工或者半双工
	config port [<portlist>|all] flowcontrol [on|off]	打开或关闭指定端口的自动流控制
VDSL 端口配置命令	config port [<portlist>|all] vdsl uprate [r1.04| r2.08|r4.17|r8.33|r10.04|r12.5|r17|rom]	配置端口上行速率等级
	config port [<portlist>|all] vdsl downrate [r1.04|r2.08|r4.17|r8.33|r10.04|r12.5|r17|rom]	配置端口下行速率等级
ADSL 端口配置命令	config port [<portlist>|all] adsl [downrate|uprate] [max|min] <value>	配置端口的上行/下行速率
	config port [<portlist>|all] adsl mode [multimode|g.lite|g.dmt| T1.413]	配置端口的工作模式
	config port [<portlist>|all] adsl noisemargin [downstream] [maximum|target] <value> config port [<portlist>|all] adsl noisemargin [upstream] [target] <value>	配置上行/下行噪声容限
	config port [<portlist>|all] adsl fimode [fast|interleaved]	配置上行/下行的快速交织模式
	config port [<portlist>|all] adsl interdelay [downstream|upstream] <value>	配置上行/下行的交织时延
	config port [<portlist>|all] adsl threshold [lossframe|losssignal|losslink|losspower|ess] <value>	配置端口门限值

	show port [<portlist> | all | active] adsl [line-config]	查看端口配置
多端口负载均衡组	create sharing <string> grouping <portlist>	创建一个 Load Sharing 组
	delete sharing <string>	删除一个 Load Sharing 组
	show sharing	显示 Load Sharing 的配置信息
端口镜像配置命令	config mirroring <1-32> to <port>	配置镜像组的目的端口
	config mirroring <1-32> add port <portlist>	向镜像组添加源端口
	config mirroring <1-32> delete port <portlist>	删除镜像组中的源端口
	config mirroring <1-32> add slot <0-15>	向镜像组添加插槽
	config mirroring <1-32> delete slot <0-15>	删除镜像组中的插槽
	config mirroring <1-32> disable	删除镜像组
	show mirroring {<1-32>}*1	根据组号显示镜像组的配置信息
	show mirroring	显示所有镜像组的配置信息

第4章 虚拟局域网 VLAN

在交换机上设置虚拟局域网 Virtual Local Area Networks （VLAN）能使网络管理员的配置管理工作变得轻松。这一章主要讲述 VLAN 的相关概念，并说明如何在 Hammer10000 IP-DSLAM 接入交换机上设置 VLAN 的各项属性。

4.1 VLAN 概述

同属一个 VLAN 的所有通信设备看起来好象在同一个物理局域网中。任何一个端口的集合（甚至交换机上的所有端口）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 的好处

- 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 能设置每个 VLAN 中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。

- VLAN提供更高的安全性

在每个 VLAN 中的设备只能与在同一 VLAN 中的设备通信。例如，如果在市场部的 VLAN *Market* 中的设备必须跟销售部的 VLAN *Sales* 中的设备通信时，就必须通过路由设备才能进行。否则，两个部门就不能直接通信，从而提高网络安全性能。

- 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。

例如，在 VLAN 网络中，如果市场部 VLAN Market 中的一台终端移动到了另一个网络中的某个端口，若要保留它的原有子网资格，您只需将那个端口设置到 VLAN Market 中就可以了。

4.2 VLAN 的分类

Hammer10000 IP-DSLAM 接入交换机最多支持 4K 个 VLAN。用户可以根据以下标准创建 VLAN：

- 物理端口
- 802.1Q tag
- 以上标准的组合

4.2.1 基于端口划分 VLAN（Port-Based VLAN）

在一个 Port-Based VLAN 中，用一个 VLAN 的名字来代表交换机中的一个或多个端口组成的一组端口。每一个端口最多只能属于一个 Port-Based VLAN。

4.2.2 基于标签划分 VLAN（Tagged VLAN）

标签（Tagging）就是在以太网帧中插入特定的记号（叫做 Tag）。标签通常包含某个指定 VLAN 的鉴定数字，叫做 VLANid。

 **注意：**

使用 802.1Q 标签的数据包可能导致数据包长度比现行的 IEEE 802.3/以太网帧的最大字节数 1，518 稍微大一点。而这可能导致其他设备中的数据包计数错误，这又可能在存在非 802.1Q 的网桥或者路由器的网络中导致连接出现问题。

1．Tagged VLAN 的应用

标签（Tagging）最常应用在跨交换机创建 VLAN。交换机之间的连接通常叫做中继。使用标签后，可以通过一个或多个中继创建跨多个交换机的 VLAN。一个 VLAN 可以很轻易地通过中继跨多个交换机。

使用 Tagged VLAN 的另一个好处就是一个端口可以属于多个 VLAN。这一点在当您有一个设备（例如服务器）必须属于多个 VLAN 的时候特别有用。这个设备必须有支持 802.1Q 的网络接口卡 Network Interface Card（NIC）。

2．指定 VLAN 标签

每一个 VLAN 都可以赋予一个 802.1Q VLAN Tag（标签）。当端口被加到一个 802.1Q 标签定义好的 VLAN 中去时，您可以决定该端口是否使用该 VLAN 的标签。Hammer10000 IP-DSLAM 接入交换机的缺省模式是所有主控板端口都属于一个名叫 default 的 VLAN 中，但是不使用该 VLAN 的标签（VLANid）-- 2047。

并不是所有端口都必须使用标签。当数据流从交换机的一个端口进入，交换机实时决定是否需将该 VLAN 的标签加入到数据包中。交换机根据每个 VLAN 的端口的配置情况决定加上或者去掉数据包中的标签。

 **注意：**

如果交换机收到带 Tag 标记的数据包，而接收数据的端口并不属于该

Tag(VLANid)所标识的 VLAN 时，那么交换机将丢弃该数据包。

4.2.3 混合使用 Tagged VLAN 和 Port-Based VLAN

您可以混合使用 Tagged VLAN 和 Port-Based VLAN。一个给定的端口可以属于多个 VLAN，前提是该端口只能在一个 VLAN 中是未加标签的（Untagged）。换句话说，一个端口同时能属于一个 Port-Based VLAN 和多个 Tagged VLAN。

注意：

出于 VLAN 分类的目的，如果交换机收到一个含 802.1Q 标签的数据包，但是该 802.1Q 标签所含的 VLANid 的值为 0，那么交换机会把该数据包当作是未标签的（untagged）。

4.3 VLAN 的命名

Hammer10000 IP-DSLAM 接入交换机支持 4K 个不同的 VLAN。每个 VLAN 的名字可以是以字母开头的 1 至 29 个字符组成，这些字符只能是字母、数字或者下划线“ _ ”。空格符、逗号、引号等字符都是不合法的。此外，VLAN 的名字是区分大小写的。

VLAN 的名字都只是本地标志。也就是说，在一台交换机上设置的 VLAN 的名字只对该交换机有意义。如果另一台交换机（Switch2）与该交换机(Switch1)相连，那么这个交换机(Switch1)的 VLAN 的名字对那台交换机（Switch2）来讲毫无意义。

注意：

应该在整个网络中统一规划命名您的 VLAN。

缺省 VLAN(Default VLAN)

每一台 Hammer10000 IP-DSLAM 接入交换机出厂时都有一个缺省 VLAN，该 VLAN 有以下属性：

- VLAN 的名字是 default
- 它包含所有主控板端口
- default VLAN的所有端口均为untagged
- default VLAN已分配了一个VLANid是2047

4.4 VLAN 聚合(Aggregation)

4.4.1 聚合综述

随着网络的发展，网络不断膨胀，网络地址资源日趋紧张。由于 B 类地址的匮乏，现在有许多网络不得不用更多的 C 类地址来代替单个的 B 类地址。这虽然解决了一定的问题，但每个子网不得不维护一个路由表，因此造成了资源的更大浪费。于是人们提出了超网的概念（Supernetting），可以使几个高位地址相同的子网共用同一个路由表。

4.4.2 聚合的目的

VLAN 聚合的目的是帮助供应商提高 IP 地址的利用率，通过聚合可以使所有在同一子网上的客户（终端用户）通过统一的路由去使用不同的广播域。

给超网（Super VLAN）分配一个子网地址，指定超网的路由地址，其他剩余的地址可以分配给各个主机使用，好像他们只是在同一个大的子网；然后把这个大的子网任意分成若干个“子网”，这些主机的子网掩码完全相同。超网下面只包含子网，不能指定主机。由于各个子网（Sub VLAN）不需要真正的子网网段，有效地提高了 IP 的利用率。这样的子网可以分配足够小，而且可以方便扩展，无需重新定义子网的大小。出于安全目的，可以阻止子网间的相互直接访问，要相互通信需通过路由（因为所有子网的路由都是超网的路由地址）。

如果不使用聚合的话，每个子网需要设置一个路由地址，而且要分配一个子网地址，结果必然有很多地址被空闲。比如某个网络的总容量只需要 3 个 C 类地址的子网，可能不得不申请使用一个 B 类的地址，而 B 类地址数量又很少，因此会造成地址空间的紧张，浪费资源。

4.4.3 聚合的特点

在子网内部的广播和相互通信不会被发送到子网以外，有效的提供了安全要求。而且子网之间是完全隔离的。

所有主机位于同一子网中，他们使用同超网一样的子网掩码。使用超网地址作为路由地址，可以分配超网所在子网的地址有效。

所有子网间通信都需要超网路由，不会使用 ARP 的重定向功能直接访问。

4.4.4 聚合的限制

根据聚合的以上特点，它也有如下的限制：

1. 超网的子网不得是一个超网，也就是不许嵌套。因为超网有自己的路由，也就是有地址，

而子网不许有地址，因此如果超网作为子网，就有矛盾。

2. 由上面所述，超网必须面对终端用户，也就是说超网是终端用户群形成的子网的集合。
3. 子网不得有 IP 地址。
4. 超网不得直接包含端口。

4.4.5 配置 SubVLAN

VLAN 聚合的目的是为了解决网络中 IP 地址浪费问题，配置 VLAN 聚合，利用命令：

【命令语法】 config vlan [<name>|<1-4095>] [add|delete] [subvlan|subvlanbyport] <string>

【使用指导】输入<name>，表示即将配置的 Super VLAN 的名字。

输入<1-4095>，表示即将配置的 VLAN 的 VID 值。

[add|delete]， 选择 add 表示添加子 VLAN，选择 delete 表示删除子 VLAN。

[subvlan|subvlanbyport]，选择 subvlan 表示我们将直接添加一个子 VLAN。选择 subvlanbyport 表示我们可以通过输入 xDSL 端口号或端口列表，将端口所在的 SubVLAN 添加到 SuperVLAN 中。

<string> 表示子 VLAN 的名字或者 xDSL 端口号或端口列表。

【配置实例 1】向名为 test 的 SuperVLAN 中添加子 VLAN “dsl2048”，命令如下：

```
Harbour(config)# config vlan test add subvlan dsl2048
```

【配置实例 2】将端口 2:1 所在的子 VLAN 添加到名为 test 的 SuperVLAN 中：

```
Harbour(config)# config vlan test add subvlanbyport 2:1
```

4.5 Hammer10000 IP-DSLAM 接入交换机 VLAN 使用概述

4.5.1 使用目的

在 Hammer10000 IP-DSLAM 接入交换机中使用 VLAN，主要有以下三个目的：

- 进行端口隔离
- 限制广播，进行流量控制
- 实现VLAN 聚合
- 实现静态组播

4.5.2 使用分类

在我们的系统当中，为了使 VLAN 功能操作更加清晰、简化，进一步对 VLAN 进行了划分，按照使用特点分为以下四类：

1） Normal VLAN

传统的 VLAN 概念。特征：

a）可以具有 IP 地址

b）能且只能包含有 Tag、Untag 的端口

2） Sub VLAN

用于为实现 VLAN 聚合。特征：

a）不能配置 IP 地址

b）能且只能包含有一个端口

c）只能属于 Super VLAN

3） Super VLAN

用于实现 VLAN 聚合。特征：

a)在使用时必须分配一个 IP 地址

b)不能包含端口

c)只能包含 Sub VLAN

4） Multicast VLAN

用于组播的实现。特征：

a）拥有一个组地址

b）包含有该组对应的组用户端口

4.5.3 资源分配

在 Hammer10000 IP-DSLAM 接入交换机出厂时，为了简化用户操作，系统会自动创建以下三种类型 VLAN：

1、缺省 VLAN(Default VLAN)

该 VLAN 有以下属性：

- VLAN 的名字是default
- VLAN的属性为Normal
- 它包含所有主控板端口
- default VLAN的所有端口均为untagged

- default VLAN已分配了一个VLANid是2047

2、系统保留 VLAN(Reserved VLAN)

该 VLAN 有以下属性：

- VLAN 的名字是reserved
- VLAN 的属性为Normal
- Reserved VLAN已分配了一个VLANid是2046
- 该VLAN需占用一个IP地址
- 该VLAN 用于系统内部通信，不允许用户对其进行操作

3、DSL VLAN

对应每一个业务板端口，系统都会自动创建一个 DSL VLAN，即每一个业务板端口都唯一地属于自己的 DSL VLAN，从而实现了业务板端口间的隔离。DSL VLAN 是不可见的，我们可以通过查看业务板端口来获得对应 DSL VLAN 的信息。DSL VLAN 属于 Sub VLAN 类。但当一个 DSL VLAN 属于一个 Super VLAN 后，该 DSL VLAN 便会出现在 Super VLAN 的 SubVLAN 列表中。

以上三种类型的 VLAN 都需占用系统的 VLAN 资源，即他们包括于系统支持的 4K 个 VLAN 当中。当在配置 VLAN 时，若遇与以上 VLAN 相冲突的情况，请重新使用别的 VLAN 资源。针对 Hammer10000 IP-DSLAM 接入交换机的使用特点，不需对业务板端口进行 VLAN 关系操作，只要采用默认配置即可。

4.6 配置 VLAN

本节主要讲述 Hammer10000 IP-DSLAM 接入交换机中有关 VLAN 配置的命令。为了方便用户操作，可通过 VID 进行 VLAN 的相关操作。

4.6.1 配置 VLAN 步骤

1、创建一个 VLAN

【命令语法】create vlan [<name>|<1-4095>] {[super|sub]}*1

【使用指导】若输入<name>表示根据名称来创建 VLAN，系统自动为该 VLAN 分配可用 VID 资源；若输入<1-4095>表示根据 VID 来创建 VLAN，系统按照一定规则自动为该 VLAN 命名；选择 super 表示创建 Super VLAN；选择 sub 表示创建 Sub VLAN；缺省参数表示创建 Normal VLAN。

VLAN 命名规则：若为 Normal VLAN：<vlan+VID>；若为 Sub VLAN：

<subvlan+VID>；若为 Super VLAN：<supervlan+VID>；若为 Multicast VLAN：<multicastvlan+VID>

2、配置 VLAN 标签（Tag）（或者使用创建时系统分配的 Tag）

【命令语法】config vlan <name> tag <value>

【使用指导】<name>为该 VLAN 的名称；

<value>为该 VLAN 的标签值，取值范围：1-4095。

3、向 VLAN 中添加/删除端口

【命令语法】config vlan [<name>|<1-4095>] [add|delete] port <portlist> [tagged|untagged]

【使用指导】选择 add 表示向 VLAN 中添加端口；

选择 delete 表示从 VLAN 中删除端口；

选择 tagged 表示所添加或删除的端口使用 802.1Qtag；

选择 untagged 表示所添加或删除的端口不使用 802.1Qtag。

注意：

SuperVLAN 不能包含端口。

4、配置 VLAN 的 IP 地址

【命令语法】config vlan [<name>|<1-4095>] ipaddress <A.B.C.D> <A.B.C.D>

或者

config vlan [<name>|<1-4095>] ipaddress <A.B.C.D/M>

【使用指导】在 ipaddress 后面输入 VLAN 的 IP 地址及子网掩码或掩码长度。

注意：

Sub VLAN、Multicast VLAN 不能配置 IP 地址。

表 4-1 列出了配置 VLAN 的相关命令。

表 4-1：Hammer10000 IP-DSLAM 接入交换机的 VLAN 配置命令表

命令	描述
create vlan [<name>|<1-4095>] {[super|sub]}*1	创建一个 VLAN
config vlan [<name>|<1-4095>] ipaddress <A.B.C.D/M>	配置 VLAN 的 IP 地址和网络掩码长度
config vlan <[<name>|<1-4095>] ipaddress <A.B.C.D> <A.B.C.D>	配置 VLAN 的 IP 地址和网络掩码
config vlan <name> tag <value>	指定 VLAN 的 Tag 即 VLANid
config vlan [<name>|<1-4095>] [add|delete] port <portlist> [tagged|untagged]	在 VLAN 中增加或删除主控板端口，并设置该端口是 tagged 还是 untagged

4.6.2 设置板内和板间隔离功能

所谓板内隔离是指某一个业务板上的端口之间的隔离，业务板上的每个端口各属于一个 VLAN，彼此之间不能进行通信，从而实现了板内的端口隔离。如果要取消这种隔离状态，需要启用 Proxy ARP 功能。

板间隔离是指分属于不同业务板上的端口之间的隔离。例如端口 2:1 和 3:1，尽管这两个端口各属于不同的 VLAN，但 Hammer10000 IP-DSLAM 接入交换机的三层功能可以使这两个端口实现通信，若要使它们不能通信，需要启用板间隔离功能。

ADU 业务板支持板内、板间隔离。

使用以下命令可以启动或关闭业务板的板内板间隔离功能：

【命令语法】config vlan [<name>|<1-4095>] separation [on|off]

【使用指导】其中，<name>是某个 Normal VLAN 的名称；选择 on 表示启动板内板间隔离功能，此时，该 Normal VLAN 内的所有 DSL 端口将不能互相通信，实现了二层 VLAN 间的广播包的隔离，使端口之间不能收到彼此的广播包。

4.6.3 配置 VLAN 举例

【配置实例 1】在该实例中创建一个名为 development 的 VLAN，然后加入主控板上的端口 2，并指定端口为 untagged 模式。

```
Harbour(config)# create vlan development
Harbour(config)# config vlan development add port 0:2 untagged
```

【配置实例 2】在该实例中创建一个名为 video 的 Tag-Based VLAN，分配给该 VLAN 的 VLANid 是 128。把主控板上的端口 2 至端口 5 加入该 VLAN 并设为 tagged 模式。

```
Harbour(config)# create vlan video
Harbour(config)# config vlan video tag 128
Harbour(config)# config vlan video add port 0:2-0:5 tagged
```

4.6.4 显示 VLAN 配置信息

显示 VLAN 配置信息，利用命令：

【命令语法】show vlan {<name>}*1

【使用指导】<name>为所要显示的 VLAN 的名称。如果没有指定 VLAN 的名称，则显示所有的 VLAN 的配置信息。 该命令显示的 VLAN 信息包括以下内容：

VLANid

VLAN 名字（VLAN name）

VLAN 属性

MAC 地址

属于该 VLAN 的 tagged 模式的端口

属于该 VLAN 的 untagged 模式的端口

Parent VLAN，当该 VLAN 是一个子 VLAN 时，此项目显示

SubVLAN，当该 VLAN 是一个 SuperVLAN 时，此项目显示

【配置举例】 显示缺省 VLAN default 的配置信息：

```
Harbour(config)# show vlan default

VLAN ID        : 2047
Vlan Name      : default
Vlan Type      : Normal
Mac address    : 00:05:3b:48:08:a6
Tagged Ports   :
Untagged Ports : 0:1   0:2   0:4
```

4.6.5 删除 VLAN

【命令语法】delete vlan [<name>|<1-4095>]

【使用指导】若输入<name>表示按照 VLAN 名称删除 VLAN，若输入 VID，表示按照 VLAN VID 删除 VLAN。

第5章 生成树协议 STP

Hammer10000 IP-DSLAM 接入交换机支持 IEEE802.1D 标准的 STP 协议，它提供了网络的动态冗余切换机制。STP 使您能在网络设计中部署备份线路，并且保证：

- 在主线路正常工作时，备份线路是关闭的。
- 当主线路出现故障时自动使能备份线路，切换数据流。

注意：

Hammer10000 IP-DSLAM 接入交换机中只在上行端口支持生成树协议。

5.1 配置 STP

Hammer10000 IP-DSLAM 接入交换机的 STP 配置包含以下内容：

- 使能或关闭STP
- 使能或关闭STP的端口
- 配置指定的STP的参数

5.1.1 使能或关闭 STP 功能

在缺省状态下，HammerOS 中的 STP 功能是关闭的，若要使用此功能，需要先执行使能 STP 的命令。同样，在 STP 使能状态下若要关闭它，则执行关闭命令，具体命令如下：

【命令语法】config stpd default [enable|disable]

【使用指导】键入 enable 使 STP 有效；键入 disable 关闭 STP。

注意：

目前 Hammer10000 IP-DSLAM 接入交换机不支持 STP 的端口多域配置，只支持单域操作，缺省域名为 default。

5.1.2 指定 STP 的端口

Hammer10000 IP-DSLAM 接入交换机中所有端口在默认情况下都是参与 STP 计算的。使能或关闭指定的 STP 端口的命令如下：

【命令语法】config stpd default port [<portlist>|all] [enable|disable]

【使用指导】<portlist>表示所要操作的端口列表；

all 表示对所有端口进行操作；

如果键入 enable，表示使指定端口的 STP 有效；

如果键入 disable，表示使指定端口的 STP 无效。

5.1.3 配置 STP 参数

运行 STP 协议后，您可能会根据具体的网络结构需要调整 STP 的一些参数。Hammer10000 IP-DSLAM 接入交换机提供的 STP 参数包括：

- Bridge Priority
- Hello Time
- Forward Delay
- Max Age
- Path Cost
- Port Priority

表 5-1 列出了 STP 参数配置命令的格式及相关参数值的解释。

表 5-1：STP 参数配置命令格式及参数解释

config stpd default priority <0-65535>
设置运行 STP 协议时本交换机的优先级。 优先级的取值范围是 0-65535，缺省值为 32768。 优先级数值越低，越有可能成为网络中的根桥（Root Bridge）。优先级值为 0 代表了最高的优先级。
config stpd default hellotime <1-10>
设置当本交换机作为根桥时发送 BPDU 的时间间隔。 HelloTime 的取值范围是 1-10，单位为秒，缺省值是 2 秒。 HelloTime 必须小于等于 ForwardDelay - 2
config stpd default forwarddelay <4-30>
设置当本交换机作为根桥时端口状态切换的时间间隔。 ForwardDelay 的取值范围是 4-30，单位秒，缺省值为 15 秒。 ForwardDelay 的时间必须大于等于 HelloTime+2
config stpd default maxage <6-40>
设置 BPDU 报文老化的最长时间间隔，收到超过这个时间的 BPDU 报文，就直接丢弃。

MaxAge 的取值范围是 6-40，单位为秒，缺省值为 20 秒。 MaxAge 的时间必须大于等于 2*(HelloTime + 1)，小于等于 2*(ForwardDelay – 1)
config stpd default port [<portlist>|all] priority <0-255>
配置参与 STP 计算的端口的优先级。 端口优先级的取值范围是 0-255，缺省值是 128。 优先级数值越低，端口越容易成为根端口（Root Port），优先级值为 0 代表了最高的优先级。
config stpd default port [<portlist>|all] cost <1-65535>
配置参与 STP 计算的端口的路径开销。 取值范围是 1-65535，HammerOS 根据端口的当前速率设置不同的缺省值： 10Mbps 端口缺省值为 100 100Mbps 端口缺省值为 19 1000Mbps 端口缺省值为 4

注意：请配置 Load sharing 所有成员端口的 STP 属性保持一致。

5.2 显示 STP 状态

5.2.1 显示 STP 状态

STP 的显示内容包括：

- BridgeID
- Root BridgeID
- STP的各种配置参数

【命令语法】 show stpd default

【配置举例】

```
Harbour(config)# show stpd default
           STP Domain default information
-------------------------------------------------
-- Designated Root Info --
Priority             : 32768
Mac address          : 00:05:3b:00:00:00
Max Age              : 20
Hello Time           : 2
Forward Delay        : 15

-- Bridge Info --
Priority             : 32768
```

```
Mac address          : 00:05:3b:00:00:00
Root Path Cost       : 0
Root Port             : 0
Bridge Max Age       : 20
Bridge Hello Time    : 2
Bridge Forward Delay : 15
-------------------------------------------------
```

5.2.2 显示端口的 STP 状态

端口的 STP 显示内容包括：

- 端口状态
- Designated port
- 端口的各种配置参数

【命令语法】 show stpd default port [<portlist>|all]

【配置举例】

```
Harbour(config)#show  stpd default port  0：1

-----------------------------------------------------------------
Port 0:1 's Spanning Tree Protocol Information
Port Join STP Domain default 's Calculate
-- Port Info --
Port id              : 1
Priority             : 128
State                : Forwarding
Path Cost            : 19

Designated Cost      : 0

-- Designated Port --
Port id              : 1
Priority             : 128

-- Designated Root --
Priority             : 32768
Mac address          : 00:05:3b:00:22:22

-- Designated Bridge --
Priority             : 32768
Mac address          : 00:05:3b:00:22:22
```

第6章 FDB 地址表

讲述了 FDB（Forwarding Database）地址表的内容和相关知识，以及如何在 Hammer10000 IP-DSLAM 接入交换机上配置静态 FDB 地址表。

6.1 FDB 地址表概述

交换机从它的所有端口接收 Media Access Control (MAC)地址信息，形成 MAC 地址表并维护它。当交换机收到一帧数据时，它将根据自己的 MAC 地址表来决定是将这帧数据进行过滤还是转发。此时，维护的这张 MAC 表就是 FDB 地址表。

6.1.1 FDB 地址表的内容

HammerOS 的 FDB 地址表数目由产品决定，Hammer10000 IP-DSLAM 接入交换机的 FDB 地址表项包含以下内容：

- MAC地址
- 与MAC地址关联的端口号（Port）
- 与MAC地址关联的VLAN的名称(VLAN Name)
- 该FDB地址表项的标志(Flags)

FDB 地址表项的标志(Flags)的含义：

- Age ：该FDB地址表项可以被老化掉
- CPU ：发送到该MAC的数据将被送到交换机的CPU
- RouteEngine ：发送到该MAC的数据将被送到交换机的路由引擎
- System ：系统（交换机）自动产生的FDB地址表项
- Permenant ：该FDB地址表项是一个静态地址表项
- Sharing ：该FDB地址表项是从Load Sharing一个成员端口上学到的
- Multicast ：该FDB地址表项是一个多播地址表项
- Broadcast ：该FDB地址表项是一个广播地址表项

如果收到的数据帧的目的 MAC 地址不在 MAC 地址表中，那么该数据将被发送给数据源设备所属于的那个 VLAN 的所有端口。

6.1.2 FDB 地址表项类型

FDB 地址表共有三种地址表项：

- **动态地址表项** —— 最开始的时候，交换机中的所有FDB地址表中的地址表项都是动态的。如果一段时间（老化时间Agingtime）之后设备没有数据传输，那么该地址表项就会被删除。这样能防止地址表项变得过于庞大，当确信某个设备从网络中去除后，就把该设备的地址表项删除掉。当交换机关机重启动后，所有的动态地址表项都将被删除。关于动态地址表项的生存时间的设置，请参考本章稍后有关FDB地址表项配置的内容。
- **固定地址表项** —— 如果老化时间（Agingtime）被设为０，那么该地址表项将存储在FDB地址表中而不会被动态删除，直到交换机关机或者重启。
- **永久地址表项** —— 永久地址表项将一直保存在FDB地址表中，即使交换机关机或者重启。永久地址表项必须由系统管理员手工设定。一个永久地址表项可以是一个单播地址，也可以是一个组播地址（本系统暂时不支持组播地址）。所有由命令行输入的静态地址表项都将被存储为永久地址表项。

永久地址表项一经建立，不会更改。但会随交换机的配置变化而变化。

例如，以下事件的发生都会引起永久地址表项被删除：

- 一个与FDB静态表项关联的VLAN被删除
- 一个端口的模式从untagged变成tagged
- 一个端口从VLAN中被删除

以下事件的发生都不会引起永久地址表项的变化：

- 一个端口被关闭（disable）
- 一个端口被堵塞（block）
- 一个端口down掉（link down）

注意：

DSL 端口不支持静态 MAC 表项功能。

6.1.3 向 FDB 地址表添加地址表项

FDB 地址表中的地址表项可以通过以下两个途径加入：

1. 交换机自学习。交换机可以根据收到的数据包的源 MAC 地址、接收数据包的端口及该端口所在的 VLAN 来自动更新 FDB 地址表。

2. 您可以通过命令行接口手工增加地址表项到 FDB 地址表中。

6.2 配置 FDB 地址表

6.2.1 创建静态地址表项

【命令语法】create fdbentry <mac_address> vlan [<name>|<1-4095>] <portlist>

【使用指导】<mac_address>表示所连接的设备或主机的 MAC 地址，<portlist>表示连接设备或主机的端口号。当通过多个上行端口连接一台设备时，如果这些端口属于多个 VLAN，可以设置一个 MAC 地址关联多个端口。例如，Hammer10000 IP-DSLAM 接入交换机通过端口 0:1 和端口 0:2 连接一台 MAC 地址为 00:E0:2B:12:34:56 的设备，端口 0:1 属于 VLAN group1，端口 0:2 属于 VLAN group2，通过以下配置实现 MAC 地址与这两个端口关联：

```
Harbour(config)# create fdbentry 00E02B123456 vlan group1 0:1
Harbour(config)# create fdbentry 00E02B123456 vlan group2 0:2
```

需要注意的是，要实现关联多个端口，必须确保这些端口不属于相同 VLAN。在一个 VLAN 内，一个 MAC 地址只能关联一个端口，也就是说在参数<portlist>处只能输入一个端口号。

【配置实例】向 FDB 表添加一条静态地址表项，目的 MAC 地址是 00:E0:2B:39:35:56，连接端口是 3:4，VLAN 名为 market

```
Harbour(config)# create fdbentry 00E02B393556 vlan market 3:4
```

6.2.2 配置 FDB 地址表老化时间

【命令语法】 config fdb agingtime <0-630>

【使用指导】 缺省值为 400 秒，当配置为 0 时，表示地址表项永远不老化。

【配置实例】设置 FDB 地址表的老化时间为 40 秒：

```
Harbour(config)# config fdb agingtime  40
```

6.2.3 删除静态地址表项

用以下的命令可以删除 FDB 地址表中的静态地址表项：

【命令语法】 delete fdbentry <mac_address> vlan [<name>|<1-4095>]

【使用指导】 < mac_address >表示要删除的设备的 MAC 地址，<name>表示要删除的设备所属的 VLAN 名称,<1-4095>表示 VLAN 的 VID。

【配置实例】 删除一条 MAC 地址为 00:11:22:33:44:55 的静态地址表项信息，键入命令：

```
Harbour(config)# delete fdbentry 001122334455 vlan market
```

注意：

由系统创建的 FDB 表项不能被删除。

6.3 显示 FDB 地址表信息

6.3.1 显示 FDB 地址表中的所有地址表项

显示 FDB 地址表中的所有地址表项的命令如下：

【命令语法】 show fdb {[mac] <macaddr>}*1 {[vlan] [<name>|<1-4095>]}*1

或

show fdb port <portlist>

show fdb slot <0-15>

【使用指导】

当 MAC 地址和 VLAN 名字一个都不输入时，将显示本交换机 FDB 地址表中除了到 CPU 的 FDB 表项之外的所有的地址表项的信息。

注意：

到 CPU 的 FDB 表项均不显示。

当只输入 MAC 地址时，将显示本交换机中所有的 VLAN 中含该 MAC 地址的 FDB 地址表项。

当只输入 VLAN 名字时，将显示本交换机中所有在该 VLAN 中的 FDB 地址表项的信息。

当既输入 MAC 地址又输入 VLAN 名字或 VID 时，将显示该 VLAN 中此 MAC 地址的 FDB 地址表项的信息。

当只输入端口时，将显示本交换机中该端口中的 FDB 地址表项。

当只输入槽号时，将显示本交换机中该槽对应所有端口包含的 FDB 地址表项。

如果没有确定后面的可选输入值，将显示所有的 FDB 地址表信息。

Flags 参数包括：Permanent、CPU、System、Age、IGMP。

在启用 802.1x 功能时，如果有用户认证并且通过时，系统将自动创建一个 802.1x Permanent 表项。当用户退出时，该表项同时自动删除。

【配置实例】 在 Hammer10000 IP-DSLAM 接入交换机上，显示 FDB 地址表项内容，键入命令：

```
Harbour(config)# show fdb
----- Begin of Mac Address Table Information (all)-----

Total 1 mac address entry showed.

Mac address       Port  Vlan name        Flags
-----------------------------------------------------
00:04:93:40:47:06  <3:23>  default        Age
------------------— ---- ----------------------------

--------  End of Mac Address Table Information -------
```

6.3.2 显示 FDB 地址表中的静态地址表项

【命令语法】show fdb permanent {[mac] <macaddr>}*1 {[vlan] [<name>|<1-4095>]}*1

【使用指导】

当 MAC 地址和 VLAN 名字一个都不输入时，将显示本交换机 FDB 地址表中的所有的静态永久地址表项的信息。

当只输入 MAC 地址时，将显示本交换机中所有的 VLAN 中含该 MAC 地址的静态地址表项。

当只输入 VLAN 名字或 VID 时，将显示本交换机中所有在该 VLAN 中的静态地址表项的信息。

当既输入 MAC 地址又输入 VLAN 名字或 VID 时，将显示该 VLAN 中此 MAC 地址的静态地址表项的信息。

如果没有确定后面的可选输入值，将显示所有的静态地址表信息。

【配置实例】在 Hammer10000 IP-DSLAM 接入交换机上，显示 FDB 静态地址表项内容：

```
Harbour(config)# show fdb permanent
------- Begin of Permanent Mac Information (all)-------

Total 1 permanent MAC showed.

Mac address       Port    Vlan name                   Flags
------------------ ------ ------------------------------
00:01:02:28:73:16  < 7:20> dsl2387                     802_1x Permanent
------------------ ------ ------------------------------

----------  End of Mac Address Table Information ----------
```

注意：

在启用 802.1x 功能时，如果有用户认证并且通过时，系统将自动创建一个 Permanent 表项；当用户退出时，该表项同时自动删除。

6.3.3 显示 FDB 地址表项老化时间

显示 FDB 地址表项老化时间，利用以下命令：

【命令语法】show fdb agingtime

6.4 FDB 地址表命令列表

配置 MAC 地址表可以使用如表 6-1 所列的命令。

表 6-1：Hammer10000 IP-DSLAM 接入交换机的 FDB 地址表命令列表

config fdb agingtime <0-630>
设置 FDB 地址表中的地址表项老化时间，缺省值为 400 秒，值 0 表示地址表项永远不老化。
create fdbentry <mac_address> vlan [<name>|<1-4095>] <portlist>
创建一个静态的永久地址表项。<mac_address>为设备的 MAC 地址，如果在这一个 MAC 地址相关有多个端口，那么数据包将被转发到所有目的端口。
delete fdbentry <mac_address> vlan [<name>|<1-4095>]
删除指定 MAC 地址的地址表项。
show fdb {[mac] <macaddr>}*1 {[vlan] [<name>|<1-4095>]}*1 或 show fdb port <portlist> show fdb slot <0-15>
显示 FDB 地址表项的信息。如果不输入后面的可选项，则显示除了到 CPU 的 FDB 表项之外的所有的 FDB 表信息。
show fdb agingtime
显示 FDB 表项的老化时间。
show fdb permanent {[mac] <macaddr>}*1 {[vlan] [<name>|<1-4095>]}*1
显示 FDB 永久地址表项的信息。如果不输入后面的可选项，则显示所有的 FDB 表信息。

第7章 IGMP Snooping

7.1 IGMP Snooping 概述

IGMP Snooping 用于监听主机与路由器之间的 IGMP 报文。因此其所完成的主要功能是接收 IGMP 报文，并对于不同的报文进行处理。

IGMP（Internet Group Management Protocol ）网络组管理协议是 IP 协议组中的一部分，用来支持和管理主机与组播路由器之间的 IP 组播。IGMP 使组播路由器能够跟踪与之物理相连的网络上每个组的成员。它在主机和直接邻接的组播路由器间运行，这个协议的机制允许主机通知本地路由器，它希望接收到发往某个特定组播组的信息。因此，组播允许进行资源发现，使网络负载减到最小，在网上实现数据的有效传输。

HammerOS 支持 IGMP Snooping 功能。

7.2 配置 IGMP Snooping

注意：

如果不启用组播服务，不可以配置静态组播路由，否则容易造成攻击，使组播不可用。

7.2.1 启动/关闭 IGMP Snooping 功能

【命令语法】`config igmp-snooping [enable|disable]`

【使用指导】选择“`enable`”表示启用 `IGMP Snooping`；选择“`disable`”则关闭 `IGMP Snooping`，同时清除所有监听的 `VLAN` 信息。

【命令模式】运行于配置模式。

【配置实例】关闭 `IGMP Snooping` 功能

```
Harbour(config)# config igmp-snooping disable
```

7.2.2 配置系统多播路由器配置方式

设置系统自动学习或者手动配置多播路由器端口信息的命令如下：

【命令语法】`config igmp-snooping router [automatism|manual]`

【命令模式】运行于配置模式。

【使用指导】系统默认为 `automatism` 模式。

【配置实例】

```
Harbour(config)# config igmp-snooping router automatism
```

7.2.3 手工删除多播路由器端口信息及所在的 VLAN

手工删除连接多播路由器端口信息及所在的 VLAN，利用命令：

【命令语法】config igmp-snooping router del port [<portlist>] vlan_id [<1-4095>]

【使用指导】参数<portlist>表示与多播路由器相连的端口；

参数[<1-4095>] ，表示与多播路由器相连的端口所属 VLAN 的 Tag 值；

该命令在多播路由器为手动配置模式时执行有效。

7.2.4 设置多播路由器老化时间

设置多播路由器接口老化的时间，如果在指定的时间内没有收到查询报文，则对系统的多播组进行删除处理，具体如下

【命令语法】config igmp-snooping router agingtime [default|<180-600>]

【使用指导】 参数<default> = 240 秒；

参数<180-600>，表示老化时间的配置范围为 180 秒到 600 秒。

7.2.5 显示多播路由器设置状态和路由老化时间

多播路由器端口设置状态有两种：auto 或 manual。用户可通过以下命令查看当前的设置状态。

【命令语法】show igmp-snooping router status

【使用指导】该命令用于显示 IGMP Snooping 路由器的状态模式和路由老化时间。

【命令模式】在只读模式和配置模式下执行。

【配置实例】

```
Harbour(config)# show igmp-snooping route status
Router mode is automatism.Router AgingTime is 240s.
```

7.2.6 显示多播路由器信息

显示多播路由器信息，具体如下：

【命令语法】 show igmp-snooping router

【配置实例】

```
Harbour(config)# show igmp-snooping route
current route have :
port: 0:2 vlan: 2045 IP: 9.9.9.253 mac: 00:01:40:55:e0:bb  Igmp version: 2
Aging
```

```
Flag: 0
```

7.2.7 添加/删除系统 IGMP Snooping 监听的 VLAN

添加/删除系统 IGMP Snooping 监听的某个 VLAN 或所有 VLAN，利用命令：

【命令语法】config igmp-snooping vlan [add|delete] byvid [all|<1-4095>]

config igmp-snooping vlan [add|delete] byport <portlist>

【使用指导】选择 add，表示将指定的 VLAN 添加到系统 igmp-snooping 进行监听；

选择 delete，删除系统 igmp-snooping 监听的某个指定 VLAN；

byvid 操作： 选择 all，表示对所有 VLAN 进行操作；选择参数<1-4095>（ VLAN 的 Tag 号），表示对指定的 VLAN 进行操作；

byport 操作：表示对用户端口所在的 VLAN 进行操作。

7.2.8 显示 IGMP Snooping 的状态

查看 IGMP Snooping 状态是否激活可以使用如下命令：

【命令语法】 show igmp-snooping status

【使用指导】 该命令用于显示 igmp-snooping 是处于开启还是关闭状态。

【命令模式】 在只读模式和配置模式下执行。

【配置实例】

```
Harbour(config)# show igmp-snooping status
IGMP_SNOOPING is enable.
```

7.2.9 显示所有被监听 VLAN 中的组信息

【命令语法】 show igmp-snooping vlan [all|<1-4095>]

【命令模式】 在只读模式和配置模式下执行。

【配置实例】

```
Harbour(config)# show igmp-snooping vlan all
VLAN: dsl2240 in the Group: 2043
VLAN: dsl2496 in the Group: 2041
VLAN: dsl2497 in the Group:
VLAN: dsl2498 in the Group: 2040
```

7.2.10 显示系统当前多播组信息

显示系统中建立的多播组中加入端口的信息，利用命令：

【命令语法】 show igmp-snooping group [all|<1-4095>]

【使用指导】 <1-4095>为多播组对应的 ID 号。

【配置实例】

```
Harbour(config)# show igmp-snooping group all
Group Vid: 2041 IP: 224.2.228.14  Port List: 9:1
Group Vid: 2040 IP: 224.2.248.4  Port List: 9:3
Group Vid: 2043 IP: 239.255.255.250  Port List: 5:1
Total multicast group number: 3
```

7.2.11 显示过滤和转发多播表项

显示系统目前建立的过滤和转发的多播表项，具体如下：

【命令语法】 show igmp-snooping multicastmac

【使用指导】配置实例中的 Filtermac 表示系统中过滤的未知多播表项；

Groupmac 表示当前系统中用户正在点播的多播转发表项。

【配置实例】

```
Harbour(config)# show igmp-snooping multicastmac
Filtermac:1:0:5e:2:f3:24 agenumber: 1    vid: 2045
Filtermac:1:0:5e:7f:2:2 agenumber: 1     vid: 2045
Filtermac:1:0:5e:7f:2:2 agenumber: 2     vid: 20
Filtermac:1:0:5e:2:e7:b4 agenumber: 4    vid: 20
Filtermac:1:0:5e:2:fd:ed agenumber: 4    vid: 20
Filtermac:1:0:5e:2:dd:78 agenumber: 4    vid: 2045
Filtermac:1:0:5e:2:b5:fb agenumber: 4    vid: 20
Filtermac:1:0:5e:2:b0:cf agenumber: 4    vid: 20
Filtermac:1:0:5e:2:91:32 agenumber: 4    vid: 20
Filtermac:1:0:5e:0:1:18 agenumber: 3     vid: 2498
Filtermac:1:0:5e:0:0:2 agenumber: 3      vid: 20
Groupmac:1:0:5e:2:e4:e Group VID: 2041  Member number: 1
Groupmac:1:0:5e:2:f8:4 Group VID: 2040  Member number: 1
Groupmac:1:0:5e:7f:ff:fa Group VID: 2043  Member number: 1
Total filter multi mac: 11
Total group multi mac: 3
```

7.2.12 设置系统离开报文处理模式

配置系统离开报文的处理模式，取值为[silent |fast]，silent 表示接收到用户的离开报文后，还需要一个查询间隔才能将用户从加入的多播组中删除；fast 表示接收到用户的离开报文后，立即从多播组中进行删除，系统默认为 fast。具体如下：

【命令语法】 config igmp-snooping leave [silent|fast]

【使用指导】 其中 silent 表示默默离开；fast 表示快速离开。

7.2.13 IGMP Snooping 的模块配置

显示 IGMP Snooping 模块部分的配置信息，具体如下：

【命令语法】 show igmp-snooping config

【配置实例】

```
Harbour(config)# show igmp-snooping config
!igmp snooping ------------------------------------------------
config igmp-snooping enable
config igmp-snooping vlan add byvid 2047
config igmp-snooping vlan add byvid 2898
config igmp-snooping vlan add byvid 2899
config igmp-snooping vlan add byvid 2900
config igmp-snooping vlan add byvid 2901
config igmp-snooping vlan add byvid 2902
config igmp-snooping vlan add byvid 2903
config igmp-snooping vlan add byvid 2045
config igmp-snooping router automatism
config igmp-snooping router agingtime 240
config igmp-snooping leave fast
```

第8章 动态主机配置协议中继（DHCP Relay）

8.1 DHCP Relay 的应用意义

这里先需要介绍一下 DHCP（动态主机配置协议，Dynamic Host Configuration Protocol）。DHCP 是从原有的 BootP 协议发展而来，原来的目的是为无盘工作站分配 IP 地址，当前更多的用于对多个客户计算机集中分配 IP 地址以及 IP 地址相关信息，从而能够将 IP 地址和 TCP/IP 的设置统一管理起来，避免不必要的地址冲突。DHCP 通常用在网络中对众多的 DOS/Windows 计算机进行地址管理，避免网络管理员手工设置和分配地址的麻烦。

动态分配 IP 地址具有以下优点：

- DHCP服务器可为客户机自动分配地址。
- 动态地址分配尤其适合那些暂时与网络相连并且和一大批主机共用某个有限的地址池同时又不要求永久地址的主机。
- 当地址分配给一个永久与网络相连的主机并且地址池中可用地址很少时，也建议使用动态分配，当某个客户租用过期或主动释放其IP地址时，DHCP服务器会及时回收该地址以备重新分配。

除了能够方便管理之外，DHCP 还可节省 IP 地址。假设网络中有 50 台计算机，可提供的 IP 地址为 40 个，由于 50 台计算机不会同时启动，所以 40 个 IP 地址应该能够满足要求。而使用静态 IP 地址的设置方式则必须为每台交换机都分配一个地址。DHCP 也可用于其他 IP 地址的设置，如缺省网关、DNS 服务器等，从而减少一个大型网络的管理任务。

当客户机与 DHCP 服务器在同一个物理网段，客户机可以正确地获得动态分配的 IP 地址。但是，如果客户机与 DHCP 服务器不在同一个物理网段，就需要应用 DCHP Relay （DHCP 中继代理）了。用 DHCP Relay 可以去掉在每个物理的网段都要有 DHCP 服务器的必要，它可以传递消息到不在同一个物理子网的 DHCP 服务器，也可以将服务器的消息传回给不在同一个物理子网的客户机。

8.2 DHCP Relay 原理

DHCP Relay 用于实现主机与非本地网络服务器的联系。当 DHCP Relay 接收到来自主机的 DHCP 申请时，它将申请转发到服务器。DHCP 中继修改 DHCP 请求的报文，标识请求主机所在的子网，然后，DHCP Relay 将报文直接传送给 DHCP 服务器。DHCP 服务器为主机分配一个适当的 IP 地址，并将请求返回给 DHCP Relay，DHCP Relay 再将它传送给请求客户系统。下图描述了 DHCP Relay 的工作过程：

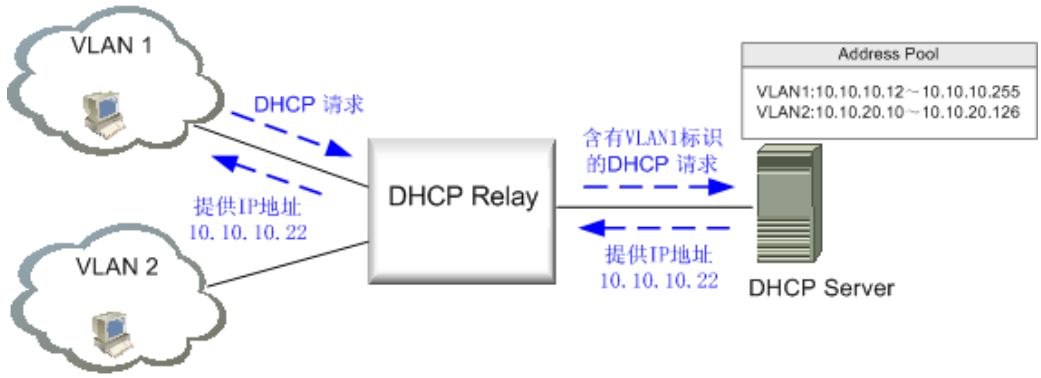


图 8-1 DHCP Relay 工作原理

属于 VLAN1 的一个主机通过 DHCP Relay 发出一个 DHCP 请求，DHCP Relay 将这个请求打上 VLAN1 的标识，然后转发给 DHCP Server。DHCP Server 维护着一个地址池（Address Pool），其中保存着对各网段可分配的 IP 地址。DHCP Server 根据请求中的 VLAN 标识为其分配一个适当的 IP 地址，然后发送给 DHCP Relay，由 DHCP Relay 返回给 VLAN1 中请求 IP 地址的那个主机。

8.3 配置服务器参数文件

8.3.1 启动 DHCP Relay 服务之前的准备工作

创建 Super VLAN，并配置 IP 地址

如果用户希望客户机能够通过 DHCP Relay 从 DHCP Server 申请到地址池中各个网段的地址，就必须要为运行 DHCP Relay 服务的 Hammer10000 IP-DSLAM 接入交换机创建一个或多个 Super VLAN，并为每个 Super VLAN 分别配置对应网段的 IP 地址。如果某个 Super VLAN 没有配置 IP 地址，则该 Super VLAN 不能作为监听接口，即客户机不能从该 Super VLAN 申请到地址。

配置监听接口

配置监听接口，也就是配置监听的 VLAN，在配置模式下使用如下命令：

【命令语法】config dhcpr listen [add|delete] <vlanname>

【使用指导】参数<vlanname>为所要添加的监听接口所在 VLAN 的名称。

查看当前监听接口，可以在配置模式下使用如下命令：

【命令语法】show dhcpr listen

注意：

1. **在没有配置任何监听接口时，DHCP Relay 服务无效。**
2. **只有当某个 VLAN 被配置了 IP 地址以后，才可以被配置成监听接口。**
3. **在 DHCP Relay 服务启动之前配置的监听接口，将在 DHCP Relay 服务启动后发生作用。**
4. **在 DHCP Relay 服务启动以后对原有监听接口的删除或是添加新的监听接口都不能在本次服务中起作用，需要停止该项服务后重新启动。**

配置 DHCP Server 的 IP 地址

在运行 DHCP Relay 的交换机上需要配置所有用到的 DHCP Server 的 IP 地址，于是需要在配置模式下使用如下命令：

【命令语法】config dhcpr targetip [add|delete] <A.B.C.D>

【使用指导】选择 add，表示向 DHCP Relay 添加一个目标 IP；

选择 delete，表示从 DHCP Relay 删除一个目标 IP；

<A.B.C.D>，表示要添加/删除目标的 IP 地址。

【命令作用】将网络上可用的 DHCP Server 的 IP 地址，添加到运行 DHCP Relay 的交换机上来作为一个 target ip ，于是客户机申请 IP 地址时，将向所有的 target ip 广播。

利用 show dhcpr targetip 命令可以显示 DHCP Server 的 IP 地址(此命令运行于 cc 命令节点下)，例如：

```
Harbour(config)# show dhcpr targetip
dhcpr  target IP 192.168.1.100
```

8.3.2 启动 DHCP Relay 服务

保证先配置监听接口和 DHCP Server 的 IP 地址之后，再启动 DHCP Relay 服务。

- 启动DHCP Relay服务

在配置模式下可以启动 DHCP Relay 服务：

service dhcpr enable

在配置模式下可以查看当前 DHCP Relay 服务的状态，键入命令：

show dhcpr status

例如：

```
Harbour(config)# show dhcpr status
```

DHCP Relay is up

- 关闭DHCP Relay服务

service dhcpr disable

8.4 应用配置实例

在 Hammer10000 IP-DSLAM 接入交换机中配置 DHCP Relay 时，应首先创建一个或多个 SuperVLAN，并为这些 SuperVLAN 分别配置 IP 地址和子网掩码，以标明其所属的网段。然后将这些 SuperVLAN 配置为 DHCP Relay 的监听接口，并启动 DHCP Relay 服务。如果某个 SuperVLAN 没有配置 IP 地址，则该 SuperVLAN 不能作为监听接口，即客户机不能从这个 SuperVLAN 申请到地址。

注意：

所配置的监听接口只有在 DHCP Relay 启动后才发生作用。另外，如果是在 DHCP Relay 启动后配置监听接口，那么在本次 DHCP Relay 服务中，监听接口并不起作用，需要停止本次服务并重新启动才可生效。此外，别忘记为 DHCP Relay 设置 DHCP Server 的 IP 地址（在配置命令中表现为 targetip，即目标服务器地址）。

例如下图所示的网络结构，其中 SuperVLAN market 的 IP 地址为 30.30.30.30/24，它包括两个 SubVLAN：dsl2048 和 dsl2050。SuperVLAN finance 的 IP 地址为 20.20.20.20/24，它也包括两个 SubVLAN：dsl2110 和 dsl2112。属于各子 VLAN 的主机都要通过 DHCP Server 获取相应的 IP 地址。Hammer10000 IP-DSLAM 接入交换机为其提供 DHCP Relay 服务。

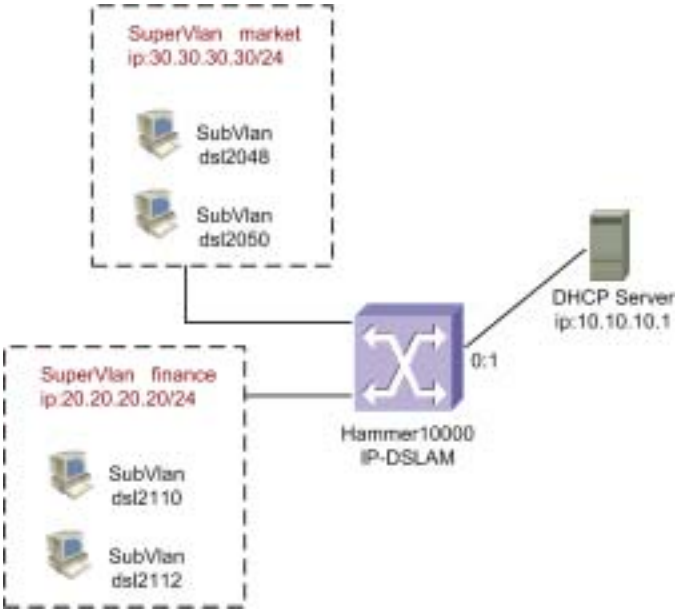


图 8-1 DHCP Relay 应用组网图

配置步骤：

！创建 SuperVLAN market，IP 地址为 30.30.30.30/24；创建 SuperVLAN finance，IP 地址为 20.20.20.20/24

Harbour(config)# create vlan market

Harbour(config)# config vlan market ipaddress 30.30.30.30/24

Harbour(config)# create vlan finance

Harbour(config)# config vlan finance ipaddress 20.20.20.20/24

！向 SuperVLAN market 添加 SubVLAN dsl2048 和 dsl2050；向 SuperVLAN finance 添加 SubVLAN dsl2110 和 dsl2112；

Harbour(config)# config vlan market add subvlan dsl2048

Harbour(config)# config vlan market add subvlan dsl2050

Harbour(config)# config vlan finance add subvlan dsl2110

Harbour(config)# config vlan finance add subvlan dsl2112

！创建上行 VLAN，取名为 uplink，将端口 0:1 以 untagged 方式添加到此 VLAN 中，设 VLAN 的 IP 地址为 10.10.10.3/24。

Harbour(config)#config port 0:1 enable

Harbour(config)#create vlan uplink

Harbour(config)#config vlan uplink ip 10.10.10.3/24

Harbour(config)#config vlan uplink add port 0:1 untagged

！在配置模式下将 SuperVLAN market 和 finance 以及上行 VLAN－uplink 配置为 DHCP Relay 的监听接口

Harbour(config)# config dhcpr listen add market

Harbour(config)# config dhcpr listen add finance

Harbour(config)# config dhcpr listen add uplink

!配置所有用到的 DHCP Server 的 IP 地址，本例中只有一个 DHCP Server，IP 地址为 10.10.10.1

Harbour(config)# config dhcpr targetip add 10.10.10.1

！启动 DHCP Relay 服务

Harbour(config)# service dhcpr enable

第9章 配置 ARP 代理

Proxy ARP 的实现基于 RFC925、RFC1027 和 RFC3069，其目的是为属于同一网段却不属于同一广播域的终端提供 ARP 报文的代理中继，配置代理 ARP 的功能就是使用 ARP 代理来实现 SubVLAN 之间的通信。对于 Hammer10000 IP-DSLAM 接入交换机产品，我们使用 VLAN 聚合技术来实现用户数据的隔离和 IP 地址的节约。配置 SuperVLAN 作为父 VLAN，每个 SuperVLAN 对应一个网络接口，在 SuperVLAN 的下面又可以配置一些 SubVLAN，子 VLAN 不是独立的网络接口，它的作用只是限制广播域。所以原则上讲，这些 SubVLAN 之间不能互相通信，它们之间的信息相互隔离，这就保证了用户隐私数据的安全。如果出现需要通信的情况，就需要启动 Proxy ARP，使指定的 SuperVLAN 下的 SubVLAN 之间能够通信，同时，每个用户仍然处于自己的广播域，用户互通的同时并不会泄漏私有数据。

Proxy ARP 原理

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。源端不知道目的端的 MAC 地址，因此发送一个目的 IP 地址的 ARP REQUEST，目的端收到后向源端发送 ARP REPLY 通告自己的 MAC 地址（目的端同时学习到源端的 MAC 地址或者和源端相同的过程通过 ARP REQUEST 得到源端 MAC 地址，这取决于通信实体协议栈的实现），两端获得 MAC 地址后就将 IP 包封装在以太网头中发送出去。由于我们 Hammer10000 IP-DSLAM 接入交换机的每个用户被隔离在不同的广播域中，所以 ARP REQUEST 并不会被发送到目的端，Proxy ARP 的作用就是架起源端和目的端两个广播域的桥梁，在两端转发 ARP 报文以实现互通。

考虑到实际的使用需求，我们提出了 proxyarp group 的概念，对于配置为同一个 group 的所有的同一 SuperVLAN 中的 SubVLAN 实现其互通，这样能够较好的满足集团用户需要互通的需求。系统缺省的是每个 SubVLAN 分别属于一个 group，所以是相互隔离的。

ARP 代理的使用很简单，大概分为三部分：

1．启动/禁用 SuperVLAN Proxy ARP 功能；

2．创建 proxyarp group；

3．将 DSL 端口对应的 VLAN 添加到 proxyarp group 中。

9.1 打开或关闭 SuperVLAN 的 ARP 代理功能

打开或关闭 SuperVLAN ARP 代理功能，在配置模式下利用命令：

【命令语法】`config vlan <name> proxyarp [enable|disable]`

【使用指导】`name` 为 `SuperVLAN` 的名字。

选择 enable，表示代理 ARP 功能打开；

选择 disable，表示代理 ARP 功能关闭。

9.2 显示 SuperVLAN 的 ARP 代理功能状态

显示 SuperVLAN ARP 代理功能状态，在配置模式下利用命令：

【命令语法】show vlan <name> proxyarp

9.3 创建/删除 ARP 代理组

创建/删除一个可以互通的 ARP 代理组，其语法格式如下：

【命令语法】create proxyarpgroup <name> supervlan <name>

delete proxyarpgroup {<name>}*1

【使用指导】其中输入 group 的名字和 SuperVLAN 的名字，为 proxyarp group 的名字。系统中最大的 group 数目为 64。

9.4 配置 ARP 代理组的 SubVLAN（端口）信息

可以对 proxyarp group 中的可以互相通信的 SubVLAN（端口）进行配置和管理：

【命令语法】config proxyarpgroup <name> [add|del] port <portlist>

【使用指导】name：配置的 proxyarp group 的名字；

add|del：增加或者删除端口信息；

portlist：端口列表。

9.5 显示 ARP 代理组信息

对 proxyarp group 当前存在的 SubVLAN（端口）信息进行查看

【命令语法】show proxyarpgroup {<name>}*1

【使用指导】name：proxyarp group 的名字。

如果不输入任何组的名字将显示所有的 group 信息。

第10章 配置 DHCP 客户端代理（DHCP Client Proxy）

10.1 概述

Hammer10000 IP-DSLAM 接入交换机在 PPPoE 接入的 IP 地址协商阶段，通过 DHCP 客户端代理服务向 DHCP 服务器申请地址池中定义的 IP 地址，然后将新申请的 IP 地址返回给客户机，完成 PPPoE 接入的动态分配 IP 地址。当 PPPoE 用户下线时，Hammer10000 IP-DSLAM 接入交换机发送 DHCP Release 报文通知 DHCP Server 释放 IP 地址。为了保证 DHCP 客户端代理与 DHCP 服务器的正常通信，必须配置一个监听接口。此监听接口必须是与 DHCP 服务器连接通信的上行端口，并且需要为此接口配置一个 VLAN，并设置 VLAN 的 IP 地址。

10.2 DHCP 客户端代理配置命令

10.2.1 配置监听接口

【命令语法】 config dhcpc-proxy listen [add|delete] <vlanname>

【使用指导】 [add|delete]：选择 add 表示增加一个 VLAN 到 DHCP 客户端代理的监听接口中，选择 delete 表示从 DHCP 客户端代理的监听接口中删除一个 VLAN；

<vlanname>：指定的待加入监听接口的 VLAN 名字(该 VLAN 必须配置了 IP 地址)。

【命令模式】 运行于配置模式。

【配置实例】 向 DHCP 客户端代理的监听接口中添加名为 uplink 的 VLAN

```
Harbour(config)# config dhcpc-proxy listen add uplink
```

提示：

被侦听 VLAN 为与 DHCP 服务器相通的上行 VLAN。

10.2.2 配置 DHCP 服务器的 IP 地址

【命令语法】 config dhcpc-proxy targetip <A.B.C.D>

【使用指导】 <A.B.C.D>：DHCP 服务器的 IP 地址。

【命令模式】 运行于配置模式。

【配置实例】 配置 DHCP 服务器的 IP 地址为 50.1.1.2

```
Harbour(config)# config dhcpc-proxy targetip 50.1.1.2
```

10.2.3 启用/禁用 DHCP 客户端代理功能

【命令语法】 service dhcpc-proxy [enable|disable]

【使用指导】 [enable|disable]：选择 enable 表示启用 DHCP 客户端代理功能，选择 disable 表示禁用 DHCP 客户端代理功能。

【命令模式】 运行于配置模式。

【配置实例】 启用 DHCP 客户端代理服务

```
Harbour(config)# service dhcpc-proxy enable
```

提示：

1、启用 DHCPC-PROXY 前必须先配置侦听的 VLAN 和 targetip 地址；

2、PPP 的 IP 分配方式采用 DHCPC-RPOXY 后，不可禁用 DHCP 客户端代理服务。

10.2.4 显示 DHCP 客户端代理的配置信息

【命令语法】 show dhcpc-proxy config

【命令模式】 运行于配置模式。

【配置实例】

```
Harbour(config)# show dhcpc-proxy config
target ip     : 50.1.1.2
listened vlan : uplink
dhcpc-proxy service enabled
```

10.3 应用配置实例

10.3.1 应用环境

- Hammer10000 IP-DSLAM接入交换机通过0:1端口与DHCP服务器相连；
- DHCP服务器的IP地址是：50.1.1.2；

10.3.2 配置步骤

1）创建一个 VLAN 作为 DHCP 客户端代理的监听接口。

```
Harbour(config)# create vlan uplink

Harbour(config)# config vlan uplink ipaddress 50.1.1.1/24

Harbour(config)# config vlan uplink add port 0:1 untagged
```

2）配置 DHCP 客户端代理并启动该功能

```
Harbour(config)# config dhcpc-proxy listen add uplink
```

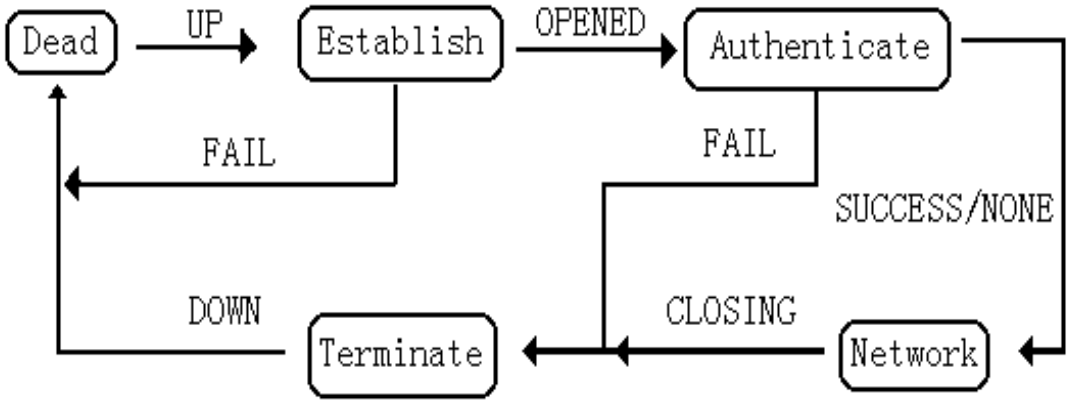
```
Harbour(config)# config dhcpc-proxy targetip 50.1.1.2

Harbour(config)# service dhcpc-proxy enable
```

第11章 配置 PPP

11.1 概述

PPP 协议是提供在点到点链路上承载网络层数据包的一种链路层协议。PPP 定义了一整套协议，包括链路控制协议（LCP）、网络层控制协议（NCP）和验证协议（PAP 和 CHAP）。PPP 由于能够提供用户验证、易于扩充和支持同异步而获得较广泛的应用。PPP 文档见于 RFC 1661、RFC 1994、RFC 1334、RFC 1990、RFC 1974。



11.1.1 PPP 工作流程

（1）PPP 在建立链路之前首先进行 LCP 协商，协商内容包括工作方式是 SP 还是 MP、Magic Number、验证方式和最大传输单元等。

（2）LCP 协商过后进入 Establish 阶段，此时 LCP 状态为 Opened，表示链路已经建立。

（3）如果配置了验证(远端验证本地或者本地验证远端)就进入 Authenticate 阶段,开始 CHAP 或 PAP 验证。

（4）如果验证失败进入 Terminate 阶段，拆除链路，LCP 状态转为 Down；如果验证成功就进行 NCP 协商，此时 LCP 状态仍为 Opened，而 IPCP 或 IPXCP 的状态机进入初始状态。

（5）NCP 协商支持 IPCP 和 IPXCP 协商，IPCP 协商主要包括双方的 IP 地址，IPXCP 协商主要包括双方的网络号和节点号。通过 NCP 协商来选择和配置一个或多个网络层协议。每个选中的网络层协议配置成功后，该网络层协议就可通过这条链路发送报文了。

（6）此链路将一直保持通信，直至有明确的 LCP 或 NCP 帧关闭这条链路，或发生了某些外部事件（例如，用户的干预）。

11.1.2 PPP 的验证方式：PAP 与 CHAP

- PAP 认证是两次握手验证，口令以明文的方式传输，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，然后返回不同的响应。

- CHAP 认证是三次握手验证，口令是密文方式的，其验证过程如下：

  1）验证方向被验证方发送一些随机产生的报文(Challenge)；

  2）被验证方用自己的口令字和 MD5 算法对该随机报文进行加密，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）。

11.2 PPP 配置命令

配置 PPP 参数必须在指定的节点（Super VLAN）下进行，其分类如下：

- LCP协商参数配置
- IPCP协商参数配置
- 验证协商参数配置
- 其他参数配置

进入一个 VLAN 接口进行 PPP 配置，命令如下：

【命令语法】 `interface <IFNAME>`

【使用指导】 `<IFNAME>`：待配置 PPP 参数的 VLAN 名称。

【命令模式】 运行于配置模式。

【配置实例】 进入 VLAN 名为 user 的接口进行 PPP 配置

```
Harbour(config)# interface user
```

11.3 配置 LCP 协商参数

11.3.1 配置 PPP 立即响应对端的输入

【命令语法】 `ppp lcp fast-start`

【命令模式】 运行于 config-if 模式。

11.3.2 取消 PPP 立即响应对端输入的配置

【命令语法】 no ppp lcp fast-start

【命令模式】 运行于 config-if 模式。

11.3.3 配置 PPP 发送第一个 LCP 包的延迟时间

【命令语法】 ppp lcp delay <0-255>

【使用指导】 <0-255>：配置的延迟时间，单位是秒，缺省配置为 2。

【命令模式】 运行于 config-if 模式。

【配置实例】 配置 PPP 发送第一个 LCP 包的延迟时间是 10 秒

```
Harbour(config-if)# ppp lcp delay 10
```

11.3.4 取消 PPP 发送第一个 LCP 包的延迟时间的配置

【命令语法】 no ppp lcp delay

【命令模式】 运行于 config-if 模式。

11.3.5 配置 ECHO-REQUEST 重传时间间隔

【命令语法】 ppp lcp interval <10-120>

【使用指导】 <10-120>：配置重传的时间间隔，单位是秒，系统默认值为 10 秒。

【命令模式】 运行于 config-if 模式。

【配置实例】 配置 ECHO-REQUEST 重传的时间间隔为 20 秒

```
Harbour(config-if)# ppp lcp interval 20
```

11.3.6 配置 ECHO-REQUEST 重传的次数

【命令语法】 ppp lcp retransmit <1-30>

【使用指导】 <1-30>：配置重传的次数，系统默认值为 10 次。

【命令模式】 运行于 config-if 模式。

【配置实例】 设置 ECHO-REQUEST 重传的次数为 10 次

```
Harbour(config-if)# ppp lcp retransmit 10
```

11.4 配置 NCP 协商参数

11.4.1 配置接受对端非零 IP 地址

【命令语法】 ppp ipcp accept-address

【命令模式】 运行于 config-if 模式。

11.4.2 取消接受对端非零 IP 地址的配置

【命令语法】 no ppp ipcp accept-address

【命令模式】 运行于 config-if 模式。

11.4.3 配置接受 DNS 服务器协商选项

【命令语法】 ppp ipcp dns [accept]

【命令模式】 运行于 config-if 模式。

11.4.4 接受/拒绝指定的 DNS 服务器

【命令语法】 ppp ipcp dns [<A.B.C.D>] {<A.B.C.D>}*1 [accept | reject]

【使用指导】 第一个[<A.B.C.D>]：主 DNS 服务器的 IP 地址；

第二个[<A.B.C.D>]：从 DNS 服务器的 IP 地址；

选择 accept：接受对端指定非零的 IP 地址作为 DNS 服务器；

选择 reject：拒绝对端指定非零的 IP 地址作为 DNS 服务器。

【命令模式】 运行于 config-if 模式。

【配置实例】 配置接受 IP 地址 100.1.1.1 作为 DNS 服务器

```
Harbour(config-if)# ppp ipcp dns 100.1.1.1 accept
```

提示：

必须先使用“ppp ipcp dns [accept]”配置才能使用该命令。

11.4.5 取消 DNS 服务器协商选项的配置

【命令语法】 no ppp ipcp dns

【命令模式】 运行于 config-if 模式。

11.4.6 配置接受 WINS 服务器协商选项

【命令语法】 ppp ipcp wins [accept]

【命令模式】 运行于 config-if 模式。

11.4.7 接受/拒绝指定的 WINS 服务器

【命令语法】 ppp ipcp wins [<A.B.C.D>] {<A.B.C.D>}*1 [accept | reject]

【使用指导】 第一个[<A.B.C.D>]：主 WINS 服务器的 IP 地址；

第二个[<A.B.C.D>]：从 WINS 服务器的 IP 地址；

选择 accept：接受指定非零的 IP 地址作为 WINS 服务器；

选择 reject：拒绝指定非零的 IP 地址作为 WINS 服务器。

【命令模式】 运行于 config-if 模式。

【配置实例】 配置接受 IP 地址 100.1.1.1 作为 WINS 服务器

```
Harbour(config-if)# ppp ipcp wins 100.1.1.1 accept
```

提示：

必须先使用“ppp ipcp wins [accept]”配置才能使用该命令。

11.4.8 取消 WINS 服务器协商选项的配置

【命令语法】 no ppp ipcp wins

【命令模式】 运行于 config-if 模式。

11.5 配置验证协商参数

11.5.1 配置 PPP 对对端的验证方式

【命令语法】 ppp authentication [chap|pap]

【使用指导】 选择 chap：对对端进行 CHAP 验证；

选择 pap：对对端进行 PAP 验证。

【命令模式】 运行于 config-if 模式。

【配置实例】 配置 PPP 对对端进行 CHAP 验证

```
Harbour(config-if)# ppp authentication chap
```

11.5.2 取消 PPP 对对端的验证

【命令语法】 no ppp authentication

【命令模式】 运行于 config-if 模式。

【配置实例】 取消 PPP 对对端的验证

```
Harbour(config-if)# no ppp authentication
```

11.5.3 配置等待验证应答包的超时时间

【命令语法】 ppp timeout authentication <0-255>

【使用指导】 <0-255>：配置等待验证应答包的超时时间数，单位为秒。

【命令模式】 运行于 config-if 模式。

【配置实例】 配置等待验证应答包的超时时间为 20 秒

```
Harbour(config-if)# ppp timeout authentication 20
```

11.5.4 取消等待验证应答包的超时时间的配置

【命令语法】 no ppp timeout authentication

【命令模式】 运行于 config-if 模式。

11.6 配置其他参数

11.6.1 配置等待 PPP 协商应答包的超时时间

【命令语法】 ppp timeout retry <1-255>

【使用指导】 <1-255>：配置等待 PPP 协商应答包的超时时间数，单位为秒。

【命令模式】 运行于 config-if 模式。

【配置实例】 配置等待 PPP 协商应答包的超时时间为 20 秒

```
Harbour(config-if)# ppp timeout retry 20
```

11.6.2 取消等待 PPP 协商应答包的超时时间的配置

【命令语法】 no ppp timeout retry

【命令模式】 运行于 config-if 模式。

11.6.3 配置通过指定静态地址池为对端分配 IP 地址

【命令语法】 peer ip address pool [default|<poolname>]

【使用指导】 default：使用默认的地址池为对端分配 IP 地址；

<poolname>：使用指定名字 poolname 的地址池为对端分配 IP 地址。

【命令模式】 运行于 config-if 模式。

【配置实例】 配置通过 test 静态地址池为对端分配 IP 地址

```
Harbour(config-if)# peer ip address pool test
```

11.6.4 配置通过 DHCP 代理方式为对端分配 IP 地址

【命令语法】 peer ip address dhcpc-proxy

【命令模式】 运行于 config-if 模式。

11.6.5 取消为对端分配 IP 地址的方式

【命令语法】 no peer ip address

【命令模式】 运行于 config-if 模式。

11.6.6 显示 PPP 配置信息

【命令语法】show ppp configuration

【命令模式】运行于 config-if 模式。

【配置实例】显示 PPP 配置信息。

```
Harbour(config-if)# show ppp configuration

interface user ppp configuration
------------------------------------------------------------
lcp delay time: 2(seconds)
lcp fast start: yes
lcp echo retries: 10
lcp echo intervals: 10(seconds)
ipcp accept address: yes
primary dns ip address: (null)
secondary dns ip address: (null)
accept peer dns settings: (null)
primary wins ip address: (null)
secondary wins ip address: (null)
accept peer wins settings: (null)
peer ip address: 50.1.1.2 [dhcpc-proxy]
ppp authentication mode: chap
ppp timeout retry: 3(times)
ppp timeout authentication: 10(seconds)
```

11.6.7 配置地址池的 IP 地址范围

【命令语法】ip local pool [default|<poolname>] <A.B.C.D> {<A.B.C.D>}*1

【使用指导】default：给默认的静态地址池配置 IP 地址范围；

<poolname>：给名为<poolname>的静态地址池配置 IP 地址范围；

第一个<A.B.C.D>：起始静态 IP 地址。此处应输入可用的合法 IP 地址，不要输入用作特殊用途的 D 类和 E 类地址；

第二个<A.B.C.D>：终止静态 IP 地址。此处应输入可用的合法 IP 地址，不要输入用作特殊用途的 D 类和 E 类地址。该参数为可选项，如果不输入则表示地址池内只包含一个地址，即指定的第一个<A.B.C.D>地址。

【命令模式】 运行于配置模式。

【配置实例】 配置静态地址池 test 的 IP 地址范围是 100.1.1.2-100.1.1.254

```
Harbour(config)# ip local pool test 100.1.1.2 100.1.1.254
```

提示：

一个静态地址池相当于 DHCP Server 上分配的一个作用域。每个 Super VLAN 对应一个地址池，地址池中的 IP 只能连续分配，地址范围和相关 Super VLAN 必

须属于同一网段。

11.6.8 删除静态地址池

【命令语法】 no ip local pool [default|<poolname>]

【使用指导】 default：删除默认的静态地址池；

<poolname>：删除名为<poolname>的静态地址池。

【命令模式】 运行于配置模式。

【配置实例】 删除静态地址池 test

```
Harbour(config)# no ip local pool test
```

提示：

如果地址池中已分配出 IP 地址，则无法删除这个地址池，只有收回全部 IP 地址后，此地址池才可以删除。

11.6.9 显示所有静态地址池的信息

【命令语法】 show ip local pool

【命令模式】运行于只读模式和配置模式。

【配置实例】

```
Harbour(config)# show ip local pool
 pool            first           last         total    free
 test            100.1.1.2     100.1.1.254      253      252
 new             100.1.2.2     100.1.2.254      253      253
```

11.6.10 显示指定的静态地址池的信息

【命令语法】 show ip local pool [default|<poolname>]{[detail|assigned]}*1

【使用指导】 default：显示默认的静态地址池信息；

<poolname>：显示名为 poolname 的静态地址池信息；

detail：显示静态地址池的所有 IP 地址信息；

assigned：仅显示已经分配出去的静态 IP 地址信息。

【命令模式】 运行于只读模式和配置模式。

【配置实例】 显示名为 test 的静态地址池已经分配出去的地址信息

```
Harbour(config)# show ip local pool test assigned
IP Address      Host-name       Assigned-time        Client-ID
100.1.1.2       ppp01          2003-5-12 05:56:46    00:01:30:55:98:e2
```

```
%Assigned IP number : 1
```

11.7 应用配置实例

应用环境

- 存在一个名为user的Super VLAN，用于接入用户；
- 通过静态地址池为接入用户分配IP地址，其IP地址范围是100.1.1.2～100.1.1.254，网关为100.1.1.1。

配置步骤

1、配置 user 的 IP 地址作为接入的网关

```
Harbour(config)# config vlan user ipaddress 100.1.1.1/24
```

2、配置一个静态地址池 test，其 IP 地址范围是 100.1.1.2～100.1.1.254

```
Harbour(config)# ip local pool test 100.1.1.2 100.1.1.254
```

3、进入接口 user 中进行 PPP 配置（只需要配置一小部分参数，其余参数都使用默认值）

```
Harbour(config)# interface user
Harbour(config-if)# ppp authentication chap
Harbour(config-if)# peer ip address pool test
```

第12章 NAS 接入服务

本章主要由以下三个部分组成：

- NAS接入服务概述
- 接入服务配置命令详解
- 接入服务应用配置实例

12.1 NAS 接入服务概述

随着宽带以太网建设规模的迅速扩大，为了适应用户数量急剧增加和宽带业务多样性的要求，港湾网络有限公司通过在 Hammer 系列交换机上嵌入接入服务完成用户的认证和管理功能，以便更好地支持宽带网络的计费、安全、运营和管理的要求。嵌入了接入服务的 Hammer 交换机称为网络访问服务器（Network Access Server，NAS）。

接入服务在运用 802.1x 协议和 RADIUS 协议的基础上，实现对用户接入的认证和管理功能。使用接入服务主要有以下优点：

- **简洁高效**：纯以太网技术内核，保持IP网络无连接特性，去除冗余昂贵的多业务网关设备，消除网络认证计费瓶颈和单点故障，易于支持多业务；
- **容易实现**：可在普通L3、L2、IP DSLAM上实现，网络综合造价成本低；
- **安全可靠**：在二层网络上实现用户认证，并可以通过设备实现MAC、端口、账户和密码等绑定技术，具有很高的安全性；
- **易于运营**：控制流和业务流完全分离，易于实现多业务运营。

接入服务在运用 802.1x 基于端口的访问控制协议的基础上扩展了该协议，实现了基于用户 MAC 地址的访问控制，可以对设备一个端口上的多个接入用户分别进行认证和管理，提供对用户接入的灵活控制，同时能够与动态主机配置协议中继代理（DHCP Relay）相结合，为计费服务器提供用户的 IP 地址。

接入服务提供 3 种身份验证方式：PAP，CHAP 和 EAP-MD5 方式，根据业务运营的不同需求，可以使用其中任何一种身份验证方式实现接入服务：

1．使用 PAP 方式进行身份验证

如图 12-1 所示，首先用户终端向 Hammer 交换机发送 EAPOL-START 报文请求接入服务，交换机返回 EAP-REQUEST/IDENTITY 报文到用户终端，要求用户提供身份标识，用户终端返回 EAP-RESPONSE/IDENTITY 响应报文表示连接建立。然后交换机发送 EAP-REQUEST/PAP 报文通知用户使用 PAP 方式验证身份，用户终端发送 EAP-RESPONSE/PAP 报文到交换机，

该报文中含有用户名和用户密码。交换机根据来自用户终端的 EAP-RESPONSE/PAP 报文组装并发送 ACCESS REQUEST 报文到 RADIUS 服务器。RADIUS 服务器对用户进行认证，如果认证通过，返回 ACCESS ACCEPT 报文给交换机，由交换机完成相应操作以允许用户接入，同时发送 EAP-SUCCESS 报文到用户终端通知用户接入成功。

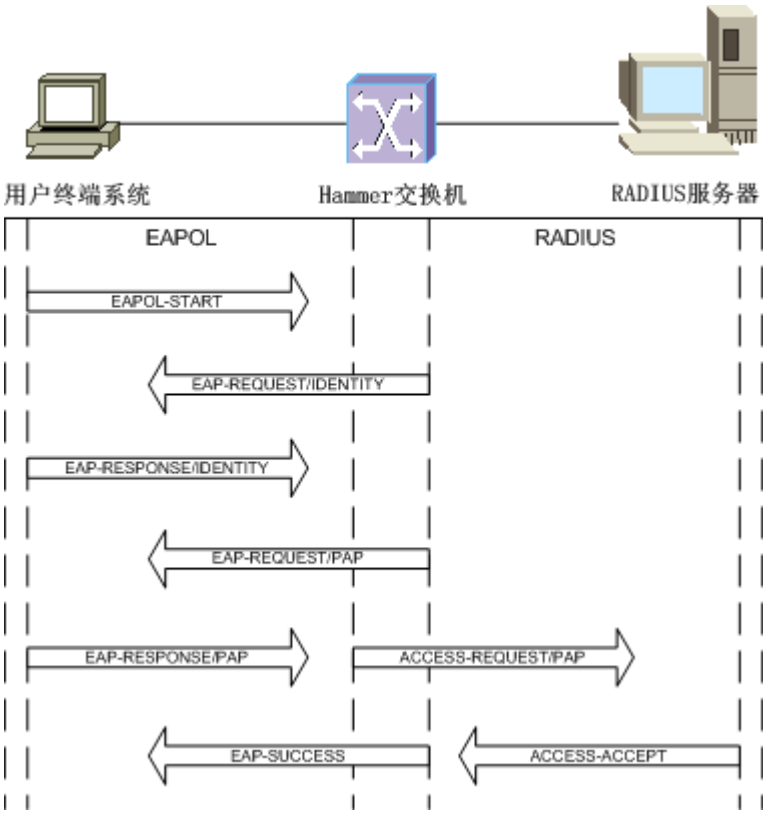


图 12-1 使用 PAP 方式进行身份验证的过程

2．使用 CHAP 方式进行身份验证

如图 12-2 所示，首先用户终端向 Hammer 交换机发送 EAPOL-START 报文请求接入服务，交换机返回 EAP-REQUEST/IDENTITY 报文到用户终端，要求用户提供身份标识，用户终端回复 EAP-RESPONSE/IDENTITY 表示连接建立。然后交换机生成 Challenge 信息，并发送 EAP-REQUEST/CHALLENGE 报文通知用户使用 CHAP 方式验证身份，用户终端返回 EAP-RESPONSE/MD5-CHALLENGE 响应报文给交换机。交换机根据来自用户终端的 EAP-RESPONSE/MD5-CHALLENGE 报文组装并发送 ACCESS REQUEST 报文送到 RADIUS 服务器。RADIUS 服务器对用户进行认证，如果认证通过，返回 ACCESS ACCEPT 报文给交换机，由交换机完成相应操作以允许用户接入，同时发送 EAP-SUCCESS 报文到用户终端通知用户接入成功。

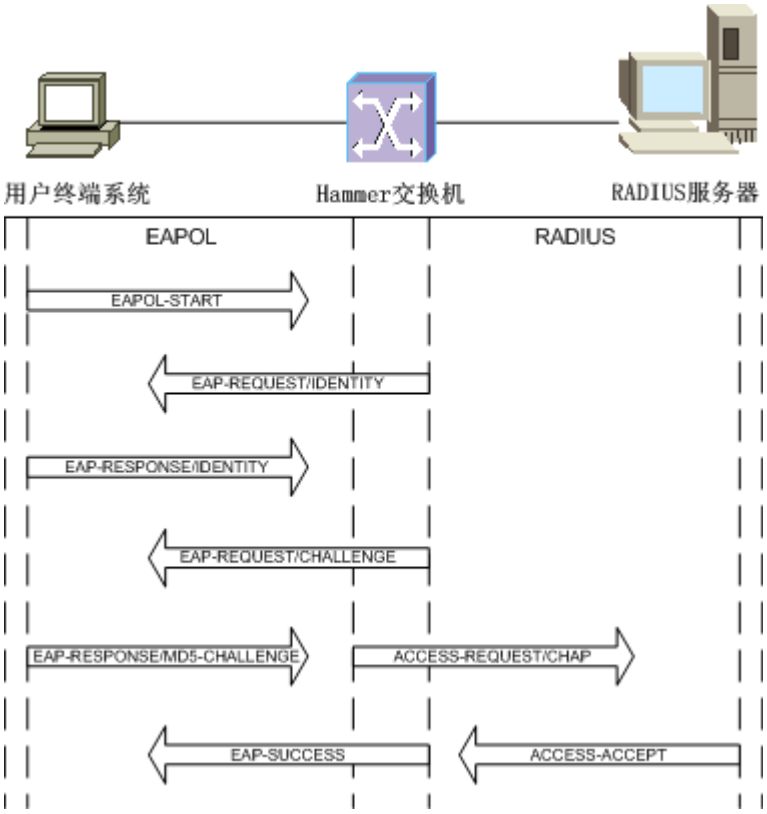


图 12-2 使用 CHAP 方式进行身份验证的过程

3．使用 EAP-MD5 方式进行身份验证

如图 12-3 所示，首先用户终端向 Hammer 交换机发送 EAPOL-START 报文请求接入服务，交换机返回 EAP-REQUEST/IDENTITY 报文到用户终端，要求用户提供身份标识，用户终端回复 EAP-RESPONSE/IDENTITY 表示连接建立。然后由交换机发送 ACCESS-REQUEST 到 RADIUS 服务器，RADIUS 服务器生成 Challenge 信息，并将 ACCESS-CHALLENGE 报文发送给交换机。接下来，交换机向用户终端发送 EAP-REQUEST/CHALLENGE 报文通知用户使用 EAP-MD5 方式验证身份，终端返回 EAP-RESPONSE/MD5-CHALLENGE 报文作为响应。交换机将来自用户终端的 EAP-RESPONSE/MD5-CHALLENGE 报文封装到 ACCESS REQUEST 报文中，并发送到 RADIUS 服务器。RADIUS 服务器对用户进行认证，如果认证通过，则返回 ACCESS ACCEPT 报文给交换机，由交换机完成相应操作以允许用户接入，同时发送 EAP-SUCCESS 报文到用户终端通知用户接入成功。

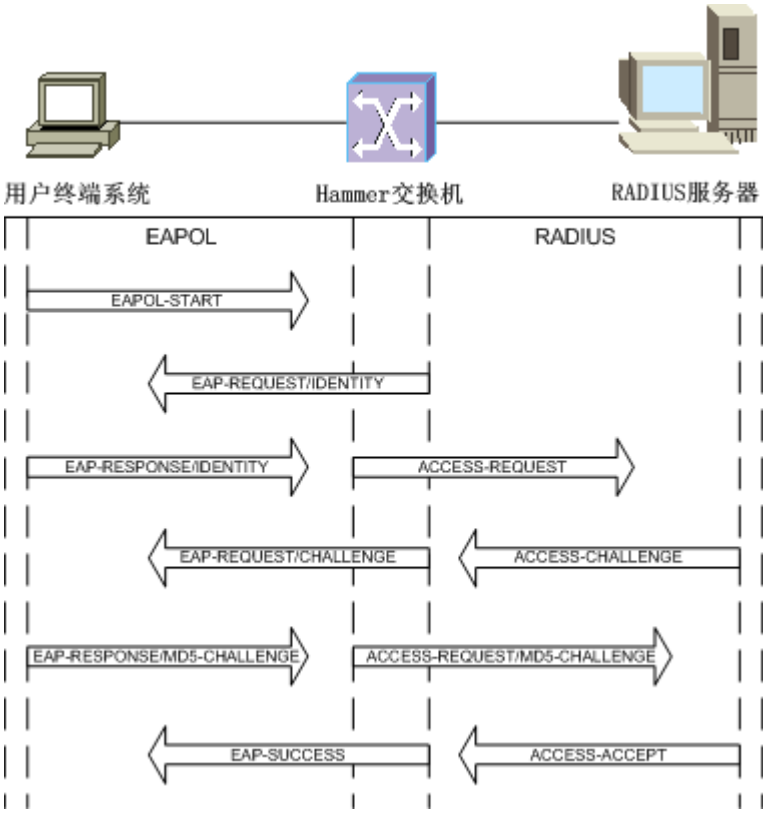


图 12-3 使用 EAP-MD5 方式进行身份验证的过程

12.2 802.1x 协议

在 IEEE 802 所定义的局域网环境中，只要存在物理的连接口，未经授权的网络设备就可以直接或通过连接到局域网的设备进入局域网络。随着局域网技术的广泛应用，在很多网络环境中，往往不希望未经授权的设备或用户连接到网络，使用网络提供的资源和服务。特别是在运营网络中的应用，对其安全认证的要求已经提到了议事日程上。如何既能够利用局域网技术简单、廉价的组网特点，同时又能够对用户或设备访问网络的合法性提供认证，是目前业界讨论的焦点。IEEE 802.1x 协议正是在这样的背景下提出的。

IEEE 802.1x 称为基于端口的访问控制协议（Port Based Network Access Control Protocol），该协议在利用 IEEE 802 LAN 的优势基础上提供了对连接到局域网的设备或用户进行认证和授权的一种手段。通过此方式的认证，能够在 LAN 这种多点访问环境中提供一种点对点识别用户的方式。这里的端口是指连接到 LAN 的一个单点结构，可以是被认证系统的 MAC 地址，也可以是服务器或网络设备上连接 LAN 的物理端口，或者是在 IEEE 802.11 无线 LAN 环境中定义的工作站和访问点。

12.2.1 802.1x 体系结构

IEEE 802.1x 协议的体系结构包括三个重要的组成部分：Supplicant 客户端、Authenticator System 认证系统、Authentication Server 认证服务器。下图描述了三者之间的关系以及相互之间的通信。

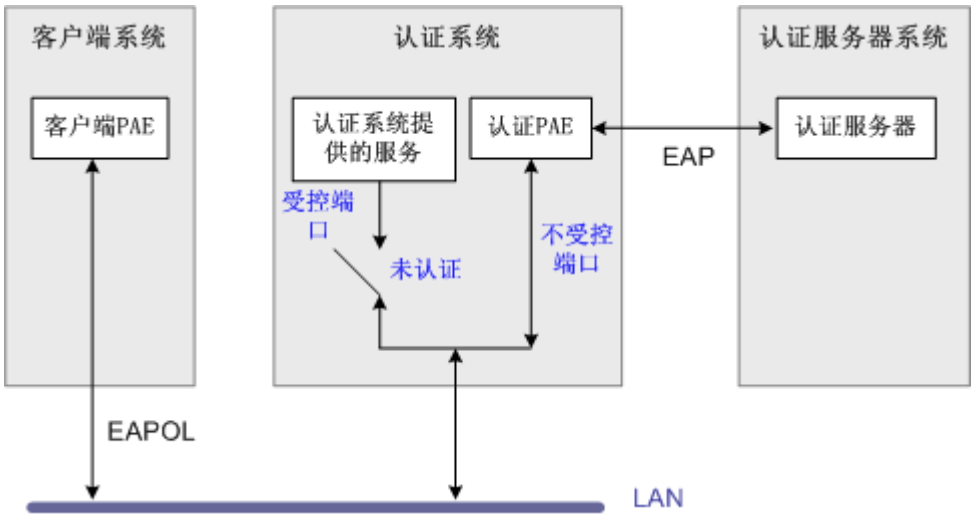


图 12-4 IEEE 802.1x 认证体系结构

客户端系统一般指用户终端系统，该终端系统通常需要安装一个客户端软件，用户通过启动这个客户端软件发起 802.1x 协议的认证过程。为了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。

认证系统通常指那些支持 802.1x 协议的网络设备，如港湾网络有限公司的 Hammer 系列交换机和无线访问点设备。支持 802.1x 协议的网络设备对应不同的用户端口（可以是物理端口，也可以是用户设备的 MAC 地址）有两个逻辑端口：受控端口（Controlled Port）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，可保证客户端始终能够发出或接受认证。受控端口只有在认证通过的状态下才可打开，用于传递网络资源和服务。受控端口可配置为双向受控、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，用户无法访问认证系统提供的服务。图 12-4 中认证系统的受控端口处于未认证状态，因此客户端无法访问认证系统提供的服务。

PAE 是端口访问实体（Port Access Entity），分为客户端 PAE 和认证系统 PAE：

- 客户端PAE：位于客户端，主要负责响应来自认证系统建立信任关系的请求。
- 认证系统PAE：位于认证系统，负责与客户端的通信，把从客户端收到的信息传送给认证服务器以完成认证。

认证系统的 PAE 通过不受控端口与客户端 PAE 进行通信，二者之间运行 EAPOL 协议。认证系统的 PAE 与认证服务器之间运行 RADIUS（Remote Authentication Dial In User Service）协议。

认证系统和认证服务器之间的通信可以通过网络进行，也可以使用其他的通信通道。例如当认证系统和认证服务器集成在一起时，两个实体之间的通信就可以不采用 RADIUS 协议。

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。当用户通过认证后，认证服务器会把用户的相关信息传递给认证系统，由认证系统构建动态的访问控制列表，用户的后续流量将接受上述参数的监管。

图 12-4 描述了终端用户的认证机制，对于网络设备之间的认证也是一样。例如：当一个网络设备 A 要求访问网络设备 B 所提供的服务时，系统 A 的 PAE 就成为客户端（Suppliant），系统 B 的 PAE 为认证系统（Authenticator）；如果 B 要求访问 A 所提供的服务时，B 的 PAE 就成为客户端，A 的 PAE 就成为认证系统。

12.2.2 802.1x 认证机制

802.1x 作为一种认证协议，在实现的过程中有很多重要的工作机制，这里我们主要介绍其中四种机制：

- 认证发起机制
- 退出认证机制
- 重新认证机制
- 认证报文丢失重传机制

1．认证发起机制

认证过程可以由用户主动发起，也可以由认证系统发起。一方面当认证系统探测到有未经过认证的用户使用网络时，就会主动发起认证,另一方面客户端可以通过客户端软件向认证系统发送 EAPOL-Start 报文发起认证。

◎ 由认证系统发起的认证

当认证系统检测到有未经认证的用户使用网络时，就会发起认证。在认证开始之前，端口的状态被强制“ 未认证 ”。

如果客户端的身份标识不可知，则认证系统会发送 EAP-Request/Identity 报文，请求客户端发送身份标识。这样，就开始了典型的认证过程。

客户端在收到来自认证系统的 EAP-Request/Identity 报文后，将发送 EAP-Response/Identity 报文响应认证系统的请求。

认证系统支持定期的重新认证，可以随时对一个端口发起重新认证的过程。如果端口状态为已认证状态，则当认证系统发起重新认证时，该端口通过认证，状态保持不变；如果未通过认证，则端口的状态改变为未认证状态。

◎ 由客户端发起认证

如果用户要上网，则可以通过客户端软件向认证系统发送 EAPOL-Start 报文主动发起认证。认证系统在收到客户端发送的 EAPOL-Start 报文后，会发送 EAP-Request/Identity 报文响应用户请求，要求用户发送身份标识，这样就启动了一个认证过程。

2．退出认证机制

有以下几种方式可以造成认证系统把端口状态从已认证状态改变成未认证状态：

a) 客户端未通过认证服务器的认证；

b) 管理性的控制端口始终处于未认证状态；

c) 与端口对应的 MAC 地址出现故障（管理性禁止或硬件故障）；

d) 客户端与认证系统之间的连接失败，造成认证超时；

e) 重新认证超时；

f) 客户端未响应认证系统发起的认证请求；

g) 客户端发送 EAPOL-Logoff 报文，主动下线。

退出已认证状态的直接结果就是导致用户下线，如果用户要继续使用网络则要重新发起一个认证过程。为什么要专门提供一个 EAPOL-Logoff 机制呢？主要是出于如下的安全考虑：当一个用户从一台终端退出后，很可能其他用户不通过发起一个新的认证过程，就可以利用该设备访问网络。提供专门的退出机制，以确保用户与认证系统专有的会话进程被中止，可以防止用户的访问权限被他人盗用。通过发送 EAPOL-Logoff 报文，可以使认证系统将对应的端口状态改变为未认证状态。

3．重新认证机制

为了保证用户和认证系统之间的链路处于激活状态，而不因为用户端设备发生故障造成异常死机，从而影响对用户计费的准确性，认证系统可以定期发起重新认证过程，该过程对于用户是透明的，即用户无需再次输入用户名和密码。

重新认证由认证系统发起，时间是从最近一次成功认证后算起。交换机上的重新认证功能可以激活或关闭，默认情况下是关闭的。重新认证的时间间隔默认值为 3600 秒（一个小时）。

注意：

重新认证的时间设定需要认真的规划，认证系统对端口进入的 MAC 地址的检测能力会影响到该时间的设定。如果对 MAC 地址的检测比较可靠，则重新认证时间可以设长一些。

4．认证报文丢失重传机制

对于认证系统和客户端之间通信的 EAP 报文，如果发生丢失，由认证系统负责进行报文的重传。在设定重传的时间时，考虑网络的实际环境，通常会认为认证系统和客户端之间报文丢失的几率比较低以及传送延迟低，因此一般通过一个超时计数器来设定，默认重传时间为 30 秒钟。

由于对用户身份合法性的认证最终由认证服务器执行，认证系统和认证服务器之间的报文丢失重传也很重要。

另外注意，对于用户的认证，在执行 802.1x 认证时，只有认证通过后，才能由 DHCP 发起（如

果配置为 DHCP 的自动获取）和 IP 地址分配的过程。当客户终端配置了 DHCP 自动获取 IP 地址时，则可能在未启动 802.1x 客户端之前，就发起了 DHCP 的请求，而此时认证系统处于禁止通行状态，这样认证系统会丢掉 DHCP 请求帧。

12.2.3 协议实现内容

802.1x 协议在实现整个安全认证的过程中，其三个关键部分（客户端、认证系统、认证服务器）之间是通过不同的通信协议进行交互的，因此有必要对其相关的通信协议做一介绍。

EAP 协议

802.1x 协议采用 EAP 协议在客户端、认证系统和认证服务器之间进行通信。EAP（Extensible Authentication Protocol 扩展的认证协议，RFC 2284）是 PPP 认证的一个通用协议，支持多种认证机制。EAP 在链路控制（LCP）阶段并不选择好一种认证机制，而是把这一步推迟到认证阶段，这就允许认证系统在确定某种特定认证机制之前请求更多的信息。

通过支持 EAP 协议，认证系统只需控制其受控端口的状态，而并不干涉通过非受控端口在客户端和认证服务器之间传递的认证信息，这样可实现认证流和业务流的完全分离。可以使用认证服务器来实现各种认证机制，认证系统仅仅需要传送认证信息，并根据认证返回的结果控制受控端口的状态。

EAP 帧结构如图 12-5 所示：

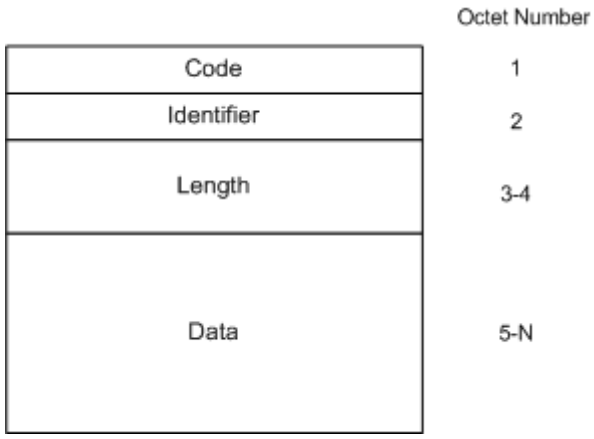


图 12-5 EAP 帧结构

EAP 帧格式中各字段含义如下：

字段	占用字节数	描述
Code	1 个字节	表示 EAP 帧的四种类型： 1. Request 2. Response 3. Success 4. Failure
Identifier	1 个字节	用于匹配 Request 和 Response。

		Identifier 的值和系统端口一起单独标识一个认证过程
Length	2 个字节	表示 EAP 帧的总长度
Data	0 或更多字节	表示 EAP 数据

EAPOL 协议

802.1x 协议定义了一种报文封装格式，这种报文称为 EAPOL（EAP over LANs 局域网上的扩展认证协议）报文，主要用于在客户端和认证系统之间传送 EAP 协议报文，以允许 EAP 协议报文在 LAN 上传送。

EAPOL 帧结构如图 12-6 所示：

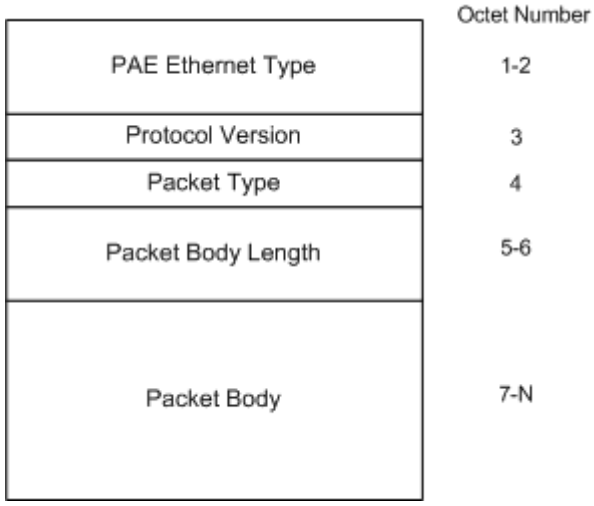


图 12-6 EAPOL 帧结构

EAPOL 帧格式中各字段含义如下：

字段	占用字节数	描述
PAE Ethernet Type	2 个字节	表示协议类型，802.1x 分配的协议类型为 888E
Protocol Version	1 个字节	表示 EAPOL 帧的发送方所支持的协议版本号。本规范使用值为 0000 0001
Packet Type	1 个字节	表示传送的帧类型，如下几种帧类型： a) EAP-Packet. 值为 0000 0000 ，表示为 EAP 帧 b) EAPOL-Start.值为 0000 0001 ，表示为 EAPOL-Start 帧 c) EAPOL-Logoff. 值为 0000 0010，表示为 EAPOL-Logoff 请求帧 d) EAPOL-Key.值为 0000 0011 ，表示为

		EAPOL-Key 帧. e) EAPOL-Encapsulated-ASF-Alert. 值为 0000 0100
Packet Body Length	2 个字节	表示 Packet Body 的长度
Packet Body	0 或更多字节	如果 Packet Type 为 EAP-Packet、EAPOL-Key 或 EAPOL-Encapsulated-ASF-Alert 的值，则 Packet Body 取相应的值；对于其他帧类型，该值为空。

EAPOL 帧可以携带 802.1q 的 VLAN 标记。

EAPOL 帧在二层传送时，必须要有目标 MAC 地址，当客户端和认证系统彼此之间不知道发送的目标时，其目标 MAC 地址使用由 802.1x 协议分配的组播地址 01-80-c2-00-00-03。

12.2.4 与不支持 802.1x 的设备的兼容

对于从一个没有认证的系统过渡到认证系统，最理想的状态是希望能够平滑的进行过渡。由于 802.1x 协议是一个比较新的协议，如果应用在原有的旧网络中，则可能存在与不支持 802.1x 协议的设备的兼容性问题。

如果客户端支持 802.1x 协议，而网络设备不支持（也就是没有认证系统），则客户端是不会收到认证系统响应的 EAP-Request/Identity 报文。在 802.1x 认证发起阶段，客户端首先发送 EAPOL-Start 报文到 802.1x 协议组申请的组播 MAC 地址，以查询网络上可以处理 802.1x 的设备（即认证系统），由于网络中没有设备充当认证系统，所以客户端是得不到响应的。因此客户端在发起多次连接请求无响应后，自动认为已经通过认证。

如果客户端不支持 802.1x 协议，而网络中存在 802.1x 协议的认证系统，则客户端是不会响应认证系统发送的 EAP-Request/Identity 报文，因此端口会始终处于未认证状态。在这种情况下，客户端只能根据协议参数 OperControlledDirections 设定的值通过受控端口访问认证系统，通过未受控端口访问某些通过设置可以访问的服务。

12.3 RADIUS 认证技术

RADIUS 的全称为（Remote Access Dail-In User Service），它是对远程拨号用户访问进行认证的一种协议，是在 RADIUS Server 和 RADIUS Client 之间进行认证、授权、计费的协议标准。认证即辨别用户是谁的过程，通常该过程通过输入有效的用户名和密码实现；授权是指对完成认证过程的用户授予相应权限，解决他能做什么的问题，在一些身份认证的实现中，认证和授权是统一在一起的；计费（Accounting）则是统计用户做过什么的过程，包括用户使用的时间和费用，可通过用户占用系统的时间、接收和发送的信息量来衡量。

RADIUS 采用 Client/Server 模型，在 NAS 上运行的是 Client 端，负责将用户信息传送到指定的 RADIUS 服务器上，并根据服务器返回的结果进行相应的处理。RADIUS 服务器包括两种类型：授权认证服务器和计费服务器。授权认证服务器（RADIUS Authentication Server）负责接收用户的连接请求、验证用户身份，并返回给客户需要的相关配置信息。一个授权认证服务

器也可以作为 RADIUS 客户的代理，将其连接到另一个授权认证服务器。计费服务器（RADIUS Accounting Server）负责接受用户计费开始请求和计费结束请求，并实现计费功能。

RADIUS 具有以下属性：

- RADIUS以Client/Server模式工作，实现了对远程用户的身份认证、授权和计费功能。
- RADIUS Client主要用来将用户信息传递给RADIUS Server；Server则对用户进行认证，并返回用户的配置信息。
- 为保证传输的安全性，RADIUS报文携带由MD5算法求得的128位验证字。
- 认证具有灵活性。采取多种认证机制，包括PAP和CHAP。

接入服务配置命令详解

12.4 802.1x 配置命令

12.4.1 使能/关闭 802.1x 认证服务

使能/关闭系统的 802.1x 认证服务，使用以下配置命令：

【命令语法】config dot1x [enable|disable]

【使用指导】选择 enable 表示使能 802.1x 认证服务，选择 disable 表示关闭 802.1x 认证服务。

【配置实例】使能 802.1x 认证服务

```
Harbour(config)# config dot1x enable
```

12.4.2 配置协议参数

802.1x 端口访问控制协议通过在客户端系统和认证系统之间传递 EAPOL 数据包、在认证系统和认证服务器之间传递 RADIUS 数据包实现访问控制，在传递数据包的过程中有如下的计时属性：

quietPeriod：是指在一次认证失败后多长时间内认证系统不接收来自客户端系统的认证请求，这项功能可以防止一些不良用户试图不停的进行认证。

txPeriod：认证系统在某个指定的时间内如果没有收到客户端系统的回复，便会重发 EAP-Request/Identity 数据帧到客户端，txPeriod 便是这个指定的重传 EAP-Request/Identity 数据帧的时间间隔。

reAuthMax：该参数用于设置当认证系统在某个指定的时间内没有收到客户端系统的回复时，向客户端重发 EAP-Request/Identity 数据帧的最大次数。

suppTimeout：认证系统在某个指定的时间内如果没有收到客户端系统的回复，便会重发 EAP-Request/Challenge 数据帧到客户端，suppTimeout 便是这个指定的重传 EAP-Request/ Challenge 数据帧的时间间隔。

max-req：该参数用于设置当认证系统在某个指定的时间内没有收到客户端系统的回复时，向客户端重发 EAP-Request/ Challenge 数据帧的最大次数。

serverTimeout：表示在认证过程中认证系统接收来自客户端数据包的超时时间和来自认证服务器数据包的超时时间。

1．配置 quietPeriod

配置 quiet 时间后，当用户终端收到从 Authentication Server 传来的拒绝该用户的接入请求报文后，在此时间间隔内，不论用户采取任何手段与服务器联系，系统将保持沉默不予理睬，默认值为 60 秒，使用以下配置命令：

【命令语法】config dot1x quiet-period <0-65535>

2．配置 txPeriod

配置认证系统向客户端系统重传 EAP-Request/Identity 数据帧的时间间隔，默认值为 30 秒，使用以下配置命令：

【命令语法】config dot1x tx-period <1-65535>

3．配置 reAuthMax

配置认证系统向客户端重传 EAP-Request/Identity 的最大次数，默认值是 2，用以下配置命令：

【命令语法】config dot1x reauth-max <1-10>

4．配置 suppTimeout

配置认证系统向客户端系统重传 EAP-Request/Challenge 数据帧的时间间隔，默认值是 30 秒，使用以下配置命令：

【命令语法】config dot1x supp-timeout <1-65535>

5．配置 max-req

配置认证系统向客户端重传 EAP-Request/Challenge 的最大次数，默认值是 2，用以下配置命令：

【命令语法】config dot1x max-req <1-10>

6．配置 serverTimeout

配置认证系统接收来自认证服务器的数据包的超时时间，默认值是 30 秒，使用以下配置命令：

【命令语法】config dot1x server-timeout <1-65535>

12.4.3 配置对端口的 802.1x 控制

1．配置端口的认证状态

端口有三种认证状态，分别是 auto、forceauth 和 forceunauth：

auto：此时端口处于接受认证状态，用户能否访问网络完全取决于用户能否认证成功。缺省配置下，端口的认证状态为 auto。

forceauth：此时端口无条件的处于已授权状态，用户可以不受限制的访问网络。

forceunauth：此时端口无条件的处于未经授权状态，用户不能访问网络。

【命令语法】config port [<portlist>|all] dot1x authcontrolledportcontrol [auto|forceauth|forceunauth]

【配置实例】将交换机的端口 11:1 设置为 auto 状态

```
Harbour(config)# config port 11:1 dot1x authcontrolledportcontrol auto
```

注意：

目前对端口认证状态只能（也是默认）设置为 auto 状态。

2．配置端口的控制模式

端口的控制模式有两种：一种是基于端口的控制，另一种是基于 MAC 的控制。在基于端口控制模式下，一个端口上只要有一个合法用户认证通过，则接在该端口下的其他用户不需认证即可获得访问权限；而在基于 MAC 控制模式下，一个端口上的每个用户都要进行独立的认证和计费，只有认证通过的合法用户才能获得访问权限，未通过认证的用户则无法访问网络。在同一系统的不同端口上可同时配置两种不同的控制模式。

【命令语法】config port [<portlist>|all] dot1x port-control-mode [MAC-based|port-based]

【使用指导】参数<portlist>表示端口号的列表，一次可以对多个端口进行相同的配置；

参数 all 表示对所有的端口进行配置；

参数 MAC-based 表示端口的控制模式是基于 MAC 的控制；

参数 port-based 表示端口的控制模式是基于端口的控制。

注意：

IP DSLAM 目前对端口控制模式只采用基于 MAC 的控制模式

【配置实例】配置交换机的端口 11：5 采用基于 MAC 的控制模式

```
Harbour(config)# config port 11:5 dot1x port-control-mode MAC-based
```

3．设置一个端口最多允许接入客户端的数目

一个端口在基于 MAC 的控制模式下可支持多个认证用户，使用以下命令设置允许端口接入的最大用户数：

【命令语法】config port [<portlist>|all] dot1x max-hosts <1-128>

【使用指导】参数<portlist>表示端口号的列表，允许一个端口接入的最大用户数目的范围，最大数目为 128，默认值为 1 个。该命令只对基于 MAC 控制模式的端口有效。

【配置实例】设置 11:5 端口允许接入的最大用户数是 10

```
Harbour(config)# config port 11:5 dot1x max-hosts 10
```

4．设置用户的身份验证方式

【命令语法】config dot1x authenticate-protocol [chap|eap-md5|pap]

【使用指导】选择 PAP、CHAP、EAP-MD5 身份验证方式。缺省配置下，802.1x 的身份验证方式为 EAP-MD5。

【配置实例】设置 CHAP 身份验证方式

```
Harbour(config)# config dot1x authenticate-protocol chap
```

12.4.4 设置重新认证机制

为了保证用户和认证系统（Hammer 系列交换机）之间的链路处于激活状态，而不因为用户端设备发生故障造成异常死机，从而影响对用户计费的准确性，认证系统可以定期发起重新认证过程。

1．使能/关闭重新认证机制

【命令语法】config dot1x re-authentication [enable|disable]

【使用指导】选择 enable 表示使能重新认证机制，选择 disable 表示关闭重新认证机制。系统缺省设置为关闭重新认证机制。

【配置实例】使能重新认证机制

```
Harbour(config)# config dot1x re-authentication enable
```

2．设置重新认证的时间间隔

【命令语法】config dot1x re-authentication period <1-65535>

【使用指导】该命令用于配置重新认证的时间间隔。重新认证由认证系统发起，时间是从最近一次成功认证后算起，范围是 1～65535 秒，默认值为 3600 秒，即 1 小时。

【配置实例】设置交换机重新认证的时间间隔为 4000 秒

```
Harbour(config)# config dot1x re-authentication period 4000
```

注意：

重新认证的时间设定需要认真规划，与认证服务器连接的网络状况会影响到该时间的设定。如果网络状况不佳，则推荐设置较长的重认证时间间隔。

12.4.5 设置异常下线检测机制（keepalive）

除了重新认证机制，为判断接入用户是否保持连接状态，接入模块还提供了另一种检测机制——异常下线检测机制。重新认证机制需要为每个在线用户启动一次完整的认证过程，在用户量较大的情况下，启动重新认证功能将导致频繁产生认证报文，对交换机造成一定的负担，而异常下线检测机制只需要少量的报文交互便可以确定用户是否在线。有关异常下线检测的命令如下：

1．使能/禁止异常下线检测功能

【命令语法】config dot1x keepalive [enable|disable]

【使用指导】选择 enable 表示启用异常下线检测功能，选择 disable 表示关闭异常下线检测功能。系统缺省为关闭该功能。

【配置实例】使能异常下线检测功能

```
Harbour(config)# config dot1x keepalive enable
```

2．设置异常下线检测的方法

异常下线检测机制提供两种检测方式：一种方式是由交换机主动向客户端定期发送检测请求（state-machine），请求报文利用了 802.1x 协议定义的 EAP Request/Identity 报文，如果收到客户端的 EAP Response/Identity 响应，说明该用户在线，反之，如果未收到响应则说明用户已经下线。另一种方式是由客户端主动向交换机定期发送检测请求报文（ping-pong），发送的时间间隔 KeepaliveRequestPeriod 和允许的最多无响应次数 KeepaliveMaxNoResponseCount 均由交换机决定，并通知给客户端。检测报文没有利用协议中规定的报文格式，而是定义了专门的格式。交换机收到来自客户端的检测报文后确认客户端在线并响应客户端的检测请求。如果在规定的时间内（该时间由命令行配置换算得出，它的值=客户端允许最多不响应次数 KeepaliveMaxNoResponseCount × 客户端定期发送 keepalive 请求的时间间隔 KeepaliveRequestPeriod + 30）没有收到客户端的检测请求，说明客户端已经异常下线。缺省时，系统使用 ping-pong 机制。

注意：

考虑到与其他厂家的兼容性，若客户端版本号为 0，则 Keepalive 的检测方法强制为 state-machine（因为版本号为 0 的客户端不支持 ping－pong 机制）。

配置命令如下：

【命令语法】config dot1x keepalive mechanism [ping-pong|state-machine]

3．设置交换机发送检测报文的时间间隔

【命令语法】config dot1x keepalive state-machine-period <10-3600>

【使用指导】该命令用于设置交换机每隔多长时间检测一次 802.1x 客户端是否仍为 active 状态。时间范围是 10～3600 秒，默认间隔为 120 秒。

【配置实例】设置交换机每隔 180 秒钟检测一次 802.1x 客户端的在线情况

```
Harbour(config)# config dot1x keepalive state-machine-period 180
```

4．设置客户端发送检测请求报文的时间间隔

【命令语法】config dot1x keepalive ping-pong-period <30-600>

【使用指导】该命令用于设置客户端发送检测请求报文（ping-pong）的时间间隔。设置范围是 30～600 秒，默认时间 30 秒。

【配置实例】设置检测请求报文的时间间隔为 180 秒

```
Harbour(config)# config dot1x keepalive ping-pong-period 180
```

5．设置允许客户端未响应的最大次数

【命令语法】config dot1x keepalive max-no-response-count <2-30>

【使用指导】设置了这条命令参数后，如果在规定的时间内（ping-pong-period × max-no-response-count + 30）没有收到客户端的检测请求报文，说明客户端已经异常下线，交换机将断开连接或进行重新认证。该命令使那些偶然短时掉线的客户端在迅速恢复连接时不必进行重新认证。该参数的范围是 2～30 次，缺省值是 3。

【配置实例】设置允许客户端未响应的最大次数为 3

```
Harbour(config)# config dot1x keepalive max-no-response-count 3
```

12.4.6 强制用户退出认证状态

出于对管理和安全的考虑，交换机允许管理者强令某个或某些用户退出 802.1x 认证状态，可根据以下条件强制用户退出：

1．根据客户端的 IP 地址强制用户退出认证状态

【命令语法】config dot1x pae force-logoff ip <address>

【使用指导】设置了这条命令后，对符合该 IP 地址的客户端，交换机将强制其退出认证状态。

【配置实例】令 IP 地址为 10.10.2.6 的客户端退出认证状态

```
Harbour(config)# config dot1x pae force-logoff ip 10.10.2.6
```

2．根据端口访问实体（PAE）的 ID 号强制用户退出认证状态

【命令语法】config dot1x pae force-logoff id <paeid>

【使用指导】该命令表示对 PAE 的 ID 号为<paeid>的客户端，交换机将强制其退出认证状态。

【配置实例】令 paeid 为 10 的客户端退出认证状态

```
Harbour(config)# config dot1x pae force-logoff id 10
```

3．根据客户端的 MAC 地址强制用户退出认证状态

【命令语法】config dot1x pae force-logoff mac <address> {port <portno>}*1

【使用指导】此命令强制 MAC 地址为< address >的客户端退出认证状态。当使用{port<portno>}参数时，表示该命令只对交换机某个指定端口（<portno>）上的 MAC 地址为< address >的客户端有效，如果不使用这个参数，则对任何端口上连接的 MAC 地址为< address >的客户端有效。

【配置实例】令交换机端口 3 上所连接的 MAC 地址为 12-00-1c-36-02-11 的客户端退出认证状态

```
Harbour(config)# config dot1x pae force-logoff mac 12001c360211 port 3
```

4．根据端口号强制用户退出认证状态

【命令语法】config dot1x pae force-logoff port <portno>

【使用指导】该命令强制交换机某个端口下的所有用户都退出认证状态。

【配置实例】令交换机端口 10 上的所有客户端退出认证状态

```
Harbour(config)# config dot1x pae force-logoff port 10
```

5．强制所有用户退出认证状态

【命令语法】config dot1x pae force-logoff all

【使用指导】该命令强制交换机上的所有 802.1x 用户退出认证状态。

【配置实例】令所有用户退出认证状态

```
Harbour(config)# config dot1x pae force-logoff all
```

12.4.7 配置客户端软件更新功能

1．配置客户端软件更新功能

【命令语法】config dot1x supp-upgrade-force [enable|disable]

【使用指导】选择 enable 表示启用客户端软件更新功能，选择 disable 表示关闭客户端软件更新功能。系统缺省为关闭该功能。

【配置实例】启用客户端软件更新功能

```
Harbour(config)# config dot1x supp-upgrade-force enable
```

2．配置客户端软件更新 URL 地址

【命令语法】config dot1x supp-upgrade-url <url>

【使用指导】参数<url>表示客户端软件更新 URL 地址。

12.4.8 清除 802.1x 统计信息

使用以下命令可以清除所有 802.1x 的统计信息：

【命令语法】config dot1x clear-statistic

12.5 802.1x 显示命令

有关 802.1x 的显示命令如表 12-1 所示。

表 12-1： 802.1x 显示命令列表

显示命令	描述
show dot1x	显示 802.1x 功能开启或关闭的状态以及相关的参数配置信息
show dot1x pae all	显示所有的 PAE 信息
show dot1x pae id <id>	根据 PAE id 索引值显示与之对应的 PAE 信息
show dot1x pae port <portlist>	根据端口号显示与之相关联的所有创建的 PAE 信息，以及 PAE 总数
show dot1x pae mac <address> {port<portlist>}*1	根据 MAC 地址显示对应的端口访问实体 PAE 绑定的用户 MAC 地址、Authenticator 状态、后台认证状态、重认证状态等信息
show port [<portlist>|all] dot1x	显示一组端口对应的 802.1x 相关信息，包括端口号、当前创建的 PAE 实体的个数以及在某一时刻曾经创建过最多的 PAE 实体的个数
show dot1x statistic	显示 802.1x 统计信息
show dot1x authenticate-protocol	查看用户身份验证方式

12.6 NAS 配置命令

12.6.1 设置用户绑定功能

如果希望端口只对特定的用户进行认证，可以设置用户绑定功能。每个端口最多可以绑定 16 个用户名。启用该功能后，只有端口上绑定的用户可以进行认证。如果一个用户希望绑定到多个端口，可以打开单用户多端口功能，该功能缺省为禁止状态。具体配置命令如下：

◎ 使能或禁止端口的用户绑定功能

【命令语法】config nas binduser port [<portlist>|all] [enable|disable]

◎ 使能或关闭一个用户绑定到多个端口的功能

【命令语法】config nas binduser multi-port-per-user [enable|disable]

◎ 在端口处添加或删除绑定的用户

【命令语法】config nas binduser [add|delete] port [<portlist>|all] user <username>

◎ 清除所有用户绑定信息

【命令语法】config nas binduser clear-all

12.6.2 设置计费高端记录功能

如果希望 NAS 对在线用户提供高端计费记录，可以设置计费高端记录功能。启用该功能后，上线用户的信息将记录在 NVRAM 中，系统掉电后不会丢失。该功能缺省为使能状态。具体配置命令如下：

◎ 使能或禁止计费高端记录功能

【命令语法】config nas high-memory [enable|disable]

◎ 设置高端记录用户在线时间更新间隔

【命令语法】config nas high-memory interval <30-60>

◎ 设置高端记录超时发送停止计费报文时长，当超过该设定值而高端记录无更新时，将认为该用户已下线，发送停止计费报文

【命令语法】config nas high-memory resend-interval <90-180>

◎ 显示高端设置

【命令语法】show nas high-memory {configuration}*1

提示：

该功能与计费同步互斥使用。

12.7 NAS 显示命令

有关 NAS 的显示命令如表 12-2 所示。

表 12-2：NAS 显示命令列表

show nas user username <name>	根据用户名显示用户信息
show nas user mac <address>	根据 MAC 地址显示用户信息
show nas user ip <address>	根据 IP 地址显示用户信息
show nas user port <portno>	根据端口号显示用户信息
show nas user vlan <vlanname>	根据 VLAN 显示用户信息
show nas user isp-domain <domain>	根据所在的域显示用户信息
show nas binduser port [<portlist>|all]	根据端口显示绑定用户信息
show nas binduser user <username>	根据用户名显示绑定用户信息
show nas user statistic	显示用户统计信息
show nas accounting-statistic	显示计费统计信息
show nas high-memory {configuration}*1	显示高端设置
show nas version	显示 NAS 版本信息

12.8 RADIUS 配置命令

当交换机从用户连接请求报文中提取出与用户相关的属性之后，重新组装成 RADIUS 格式报文，并与 RADIUS Server 通信以完成后续的认证、计费功能。

12.8.1 配置 RADIUS 认证服务

认证服务器（Authentication Server）具有如下属性：

- 认证服务器通过ID号进行标识。NAS包含一个认证服务器列表，当NAS发送认证请求时，它从列表中选择最靠前（ID最小）的且处于可用状态的认证服务器。因此在配置某个认证服务器时，必须将该服务器加入到列表中，如果不再使用某个认证服务器了，可以将它从列表中删除。
- 如果要使用某个认证服务器，必须将它的ID配置为处于可用状态的认证服务器中的最小ID值。如果此ID已经使用，则要先删除使用该ID的认证服务器，再加入新的认证服务器。

- server-ip是认证服务器的IP地址。
- client-ip是RADIUS Client的IP地址，即交换机上连接认证服务器的端口所属VLAN的IP地址。
- udp-port端口号，RADIUS Server 和RADIUS Client之间的Radius报文封装在UDP包内，UDP端口号可以使用默认端口号,也可以通过配置命令设置其它的端口号，该版本的RADIUS协议默认的认证端口号为1812。

1．启动/关闭 RADIUS 认证功能

启动 RADIUS 认证功能，使用以下配置命令：

```
Harbour(config)# radius authentication enable
```

关闭 RADIUS 认证功能，使用以下配置命令：

```
Harbour(config)# radius authentication disable
```

2．增加 RADIUS 认证服务器

【命令语法】radius authentication add-server id <0-4> server-ip <A.B.C.D> client-ip <A.B.C.D>

{udp-port <1-6500>}*1

【使用指导】增加一个 RADIUS 认证服务器，设置其 ID 号为 0～4 之一，也就是说系统最多可以设置五个认证服务器，并且要指明认证服务器的 IP 地址和 UDP 端口（默认值为 1812）。另外还要说明使用该认证服务器的客户端（Client）的 IP 地址。

【配置实例】增加一个 RADIUS 认证服务器，设其 ID 号为 1，IP 地址为 110.12.21.1，RADIUS Client 的 IP 地址为 110.12.21.2

```
Harbour(config)# radius authentication add-server id 1 server-ip 110.12.21.1
client-ip 110.12.21.2
```

3．删除 RADIUS 认证服务器

删除某个认证服务器时只要说明其索引号即可，配置命令如下：

【命令语法】radius authentication delete-server id <0-4>

4．设置共享密钥

考虑到网络传输的安全性，RADIUS Client 和认证服务器 RADIUS Server 之间的报文要根据共享密钥进行加密封装。加密封装方法是将密钥字符串和 Radius 报文头部一起通过 HMAC_MD5 算法生成校验域。共享密钥的配置使用如下命令：

【命令语法】radius authentication config-server id <0-4> shared-secret <secret>

【使用指导】其中，<0-4>为 RADIUS Server 的索引值，<secret>为共享密钥。

5．设置重传时间间隔

当设备 RADIUS Client 向 RADIUS Server 发出请求的一段时间之后没有得到 RADIUS Server 的应答，RADIUS Client 可以向 RADIUS Server 重传数据包，重传数据包的时间间隔默认值为 10 秒，可以使用以下配置命令设置这个间隔：

【命令语法】radius authentication config-server id <0-4> retransmit-interval <5-300>

【使用指导】其中，<0-4>为 RADIUS Server 的索引值，<5-300>为重传时间间隔的取值范围，单位为秒。

6．设置重传的最大次数

当 RADIUS Client 需要向 RADIUS Server 重传数据包时，应配置 RADIUS Client 重传该数据包的最大次数，默认值为 3 次，可以使用以下配置命令：

【命令语法】radius authentication config-server id <0-4> max-retransmit-count <2-10>

【使用指导】其中，<0-4>为 RADIUS Server 的索引值，<2-10>为最大重传次数。

7．设置最大重传丢弃数

该参数用于判断 RADIUS Server 是否断掉。当 RADIUS Client 按上述规定的重传次数完成重传后，若仍未收到 RADIUS Server 的回复，则丢弃数据包，系统记录一次重传丢弃。当丢弃数超过所设置的最大重传丢弃数时，则认为 RADIUS Server 连接已断。利用以下命令设置最大重传丢弃数：

【命令语法】radius authentication config-server id <0-4> max-retransmit-drop-count <2-30>

【使用指导】其中，<0-4>为 RADIUS Server 的索引值，<2-30>为最大重传丢弃数。

8．设置最大发送失败数

该参数用于判断 RADIUS Server 是否断掉。如果 RADIUS Client 有超过最大发送失败数的包没有发送成功，则表明该 RADIUS Server 的连接已断。利用以下命令设置最大发送失败数：

【命令语法】radius authentication config-server id <0-4> max-send-fail-count <2-30>

【使用指导】其中，<0-4>为 RADIUS Server 的索引值，<2-30>为最大发送失败数。

9．设置认证服务器的当前状态

交换机可以将当前认证服务器的状态设置为 active、inactive、dead 三种状态，这三种状态各自表示的意义说明如下：

状态	描述
active	处于此状态的认证服务器能够与交换机一起完成正常的授权认证功能。
inactive	处于此状态的认证服务器不执行认证功能，但交换机仍会定期向该服务器发送检测报文，以便等待随时在需要的时候将服务器的状态改成 active。
dead	处于此状态的认证服务器不执行认证功能，交换机也不向该服务器发送检测报文。

如果有两台认证服务器，一台的状态为 inactive，另一台的状态为 dead。当状态为 inactive 的认证服务器改成 active 时，系统会自动将状态为 dead 的认证服务器设置为 inactive，并向其发送检测报文。

设置认证服务器当前状态的配置命令如下：

【命令语法】radius authentication config-server id <0-4> status [active|inactive|dead]

12.8.2 配置 RADIUS 计费服务

1．启动/关闭 RADIUS 计费功能

启动 RADIUS 计费功能，使用以下配置命令：

```
Harbour(config)#radius accounting enabled
```

关闭 RADIUS 计费功能，使用以下配置命令：

```
Harbour(config)#radius accounting disable
```

2．增加 RADIUS 计费服务器

增加一个 RADIUS 计费服务器，设置其 ID 索引号为 0~4 之一，也就是说系统最多可设置五个计费服务器，其中以 ID 号最小的计费服务器作为主计费服务器。此外，还要指明增加的计费服务器 的 IP 地址和 UDP 端口（默认值为 1813），以及使用该计费服务器的 RADIUS Client 的 IP 地址。使用以下配置命令：

【命令语法】radius accounting add-server id <0-4> server-ip <A.B.C.D> client-ip <A.B.C.D>

{udp-port <1-6500>}*1

【配置实例】增加一个 RADIUS 计费服务器，设其 ID 号为 1，IP 地址为 110.12.21.1，RADIUS Client 的 IP 地址为 110.12.21.2

```
            Harbour(config)# radius accounting add-server id 1 server-ip 110.12.21.1
client-ip 110.12.21.2
```

3．删除 RADIUS 计费服务器

删除某个计费服务器时只要说明其索引号即可，配置命令如下：

【命令语法】radius accounting delete-server id <0-4>

4．设置共享密钥

考虑到网络传输的安全性，传递的报文都是经过加密算法封装过的，配置某个计费服务器 RADIUS Server 和其 RADIUS Client 之间的共享密钥<secret>，将该字符串放到 md5 算法中和其它数据一同参与计算，可以使用以下配置命令：

【命令语法】radius accounting config-server id <0-4> shared-secret <secret>

【使用指导】其中，<0-4>为 RADIUS Server 的索引值，<secret>为共享密钥。

5．设置重传时间间隔

当 RADIUS Client 向 RADIUS Server 发出请求的一段时间之后没有得到 RADIUS Server 的应答，RADIUS Client 可以向 RADIUS Server 重传数据包，重传数据包的时间间隔默认值为 10 秒，可以使用以下配置命令设置这个间隔：

【命令语法】radius accounting config-server id <0-4> retransmit-interval <5-300>

【使用指导】其中，<0-4>为 RADIUS Server 的索引值，<5-300>为重传时间间隔的取值范围，单位为秒。

6．设置重传的最大次数

当 RADIUS Client 需要向 RADIUS Server 重传数据包时，应配置 RADIUS Client 重传该数据包的最大次数，默认值为 3 次，可以使用以下配置命令：

【命令语法】radius accounting config-server id <0-4> max-retransmit-count <2-10>

【使用指导】其中，<0-4>为 RADIUS Server 的索引值，<2-10>为最大重传次数。

7．设置最大重传丢弃数

该参数用于判断 RADIUS Server 是否断掉。当 RADIUS Client 按上述规定的重传次数完成重传后，若仍未收到 RADIUS Server 的回复，则丢弃数据包，系统记录一次重传丢弃。当该丢弃数超过所设置的最大重传丢弃数时，则认为 RADIUS Server 连接已断。利用以下命令设置最大重传丢弃数：

【命令语法】radius accounting config-server id <0-4> max-retransmit-drop-count <2-30>

【使用指导】其中，<0-4>为 RADIUS Server 的索引值，<2-30>为最大重传丢弃数。

8．设置最大发送失败数

该参数用于判断 RADIUS Server 是否断掉。如果 RADIUS Client 有超过最大发送失败数的包没有发送成功，则表明该 RADIUS Server 的连接已断。利用以下命令设置最大发送失败数：

【命令语法】radius accounting config-server id <0-4> max-send-fail-count <2-30>

【使用指导】其中，<0-4>为 RADIUS Server 的索引值，<2-30>为最大发送失败数。

9．设置计费服务器的当前状态

交换机可以将当前计费服务器的状态设置为 active、inactive、dead 三种状态，这三种状态各自表示的意义说明如下：

状态	描述
active	处于此状态的计费服务器能够与交换机一起完成正常的计费功能。
inactive	处于此状态的计费服务器不执行计费功能，但交换机仍会定期向该服务器发送检测报文，以便等待随时在需要的时候将服务器的状态改成 active。
dead	处于此状态的计费服务器不执行计费功能，交换机也不向该服务器发送检测报文。

如果有两台计费服务器，一台的状态为 inactive，另一台的状态为 dead。当状态为 inactive 的计费服务器改成 active 时，系统会自动将状态为 dead 的计费服务器设置为 inactive，并向其发送检测报文。

目前 Hammer10000 IP-DSLAM 接入交换机能自动识别计费服务器的状态，命令配置方式只能将计费服务器状态手动改为 active。

【命令语法】radius accounting config-server id <0-4> status active

12.8.3 设置 RADIUS CUT 功能

RADIUS CUT 是指由 RADIUS Server 主动发起断开与用户连接的信息。当 RADIUS Server 由于某种原因要求用户下线时，向认证系统（交换机）发送一种 RADIUS 格式的请求报文（CUT）。交换机在指定的 UDP 端口处监听该请求，一旦收到 CUT 请求，便按照以下步骤执行处理过程：

第一步：根据配置命令进行合法性检查。

通过命令行的配置，选择使用 CUT 报文中的 AUTHENTICATOR 字段进行报文的合法性检查，或者使用 MESSAGE AUTHENTICATOR 属性字段进行报文的合法性检查。Hammer 交换机采用和 RADIUS Server 相同的标准协议算法重新计算 AUTHENTICATOR 字段或 MESSAGE

AUTHENTICATOR 属性字段，当计算结果与 CUT 报文相一致时，认为其合法，否则丢弃该 CUT 报文。使用这种机制时，可由交换机直接切断与用户的连接。当然这要求配置人员必须首先了解 RADIUS Server 发出的 CUT 报文格式才能进行相应的配置。

第二步：按照相关属性定位用户。

如果没有找到对应用户，则说明该用户不在线，将不予处理；如果找到对应的用户，则根据配置命令使用以下其中一种方法切断交换机与用户的连接：

- 启动重认证机制，由RADIUS Server发送RADIUS_ACCESS_REJECT报文拒绝用户的认证请求。
- 由交换机自动设置直接切断该用户。

注意：

默认配置下，为了保证网络的安全，交换机不检测报文的合法性便直接断开与用户的连接，从而避免受到非法 CUT 报文的攻击。

网络中可能存在多个 RADIUS Server，包括认证服务器和计费服务器，可以设置交换机只处理某些服务器发出的 CUT 请求。因此在交换机中设置一个 CUT Server 列表，在此列表中存放着这些 Server 的信息。

有关 RADIUS CUT 功能的配置命令具体如下：

1．启动/关闭接收 CUT 报文功能

启动接收 CUT 报文功能，使用以下命令：

Harbour(config)# radius cut enable

关闭接收 CUT 报文功能，使用以下命令：

Harbour(config)# radius cut disable

2．列表中增加/删除认证服务器作为 CUT 服务器

向列表中增加一个认证服务器，使用以下命令：

【命令语法】radius cut add-server authentication id <0-4>{udp-port <1-6500>}*1

从列表中删除一个认证服务器，使用以下命令：

【命令语法】radius cut delete-server authentication id <0-4>

【使用指导】Hammer 系列交换机可为每个域最多设置 5 个认证服务器，id <0-4>代表认证服务器的索引号。

3．列表中增加/删除计费服务器作为 CUT 服务器

向列表中增加一个计费服务器，使用以下命令：

【命令语法】radius cut add-server accounting id <0-4> {udp-port <1-6500>}*1

从列表中删除一个计费服务器，使用以下命令：

【命令语法】radius cut delete-server accounting id <0-4>

【使用指导】Hammer 系列交换机可为每个域最多设置 5 个计费服务器，id <0-4>代表计费服务器的索引号。

4．设置校验 CUT 报文的方式

CUT 报文的合法性校验默认是关闭的，可以通过以下命令行配置以何种方式校验 CUT 报文的合法性：

【命令语法】radius cut verify-by [authenticator|message-authenticator|none]

【使用指导】参数 authenticator 表示校验 CUT 报文的 authenticator 字段；

参数 message-authenticator 表示校验 CUT 报文的 message-authenticator 属性；

参数 none 表示不校验 CUT 报文。

5．设置处理 CUT 请求机制

Hammer10000 IP-DSLAM 接入交换机具有两种处理 CUT 报文的机制：启动重认证机制和直接切断与用户连接机制：

【命令语法】radius cut process-by [reauthentication|logoff]

【使用指导】参数 reauthentication 表示启动重认证机制处理 CUT 请求；参数 logoff 表示直接断开与用户的连接。默认为直接断开连接。

提示：

本接入交换机暂无 reauthentication 启动重认证机制处理 CUT 请求。

12.8.4 配置 RADIUS 计费同步功能

如果 RADIUS 服务器支持计费同步报文，则当 NAS 因发生断电等意外情况而重新启动时，会向域中所有 RADIUS 计费服务器发一个计费类型为 Accounting-On 的计费同步报文，RADIUS 服务器收到该报文后对该 NAS 下的所有用户停止计费。

如果希望 NAS 在系统启动时向计费服务器发送 RADIUS 计费同步报文，可以设置 RADIUS

计费同步功能。启用该功能后，系统将在重启后向计费服务器发送计费同步报文，使部分或全部用户停止计费。

◎ 使能或禁止 RADIUS 计费同步功能

【命令语法】radius accounting sync [enable|disable]

◎ 显示 RADIUS 计费同步功能设置

【命令语法】show radius accounting sync

12.8.5 配置 Session Timeout 处理机制

Session Timeout 是 RADIUS Server 通过 Access Accept 报文传递的一个属性，在 RFC2866 中它的含义是授权用户本次接入服务的时间，如果该时间到达，就停止用户的接入服务，强制用户下线。港湾网络有限公司 Hammer 系列交换机的接入模块对这一属性进行了扩展，使得该属性既可以按照 RFC2866 中的标准使用，也可以将该属性解释为服务器希望对用户进行重认证，Session Timeout 的值为重认证的时间间隔。

【命令语法】radius accounting session-timeout-type [logoff|reauthenticate]

【使用指导】选择 logoff 表示按照 RFC2866 标准对 Session Timeout 进行处理；选择 reauthenticate 表示当设置的 session-timeout 时间到时后由服务器对用户进行重认证。

12.8.6 配置 RADIUS Server 主备切换功能

Hammer 系列交换机可为每个域最多设置 5 个 RADIUS 服务器（在主备服务器环境下一般为两个可用的服务器，一个为主用，一个为备用），如果正在使用的 RADIUS 主用服务器断掉，可以切换到备用的 RADIUS 服务器。其中的切换功能包括以下内容：

- 提供对正在认证的用户的处理。认证服务器发生切换时，可以让正在认证的用户不等待原来的认证请求，立即重新在备用服务器进行重认证；计费服务器发生切换时，可以让正在发送的计费请求不等待回复而重新发送计费请求到备用的计费服务器。
- 提供对已经认证通过的用户的处理。可以让已经认证通过的用户在认证服务器发生主备切换时在备用的服务器上重认证；也可以使主备切换对已经认证的用户透明，即不用重认证便可让用户继续使用接入服务。
- 提供对切换的RADIUS服务器的可用状态的检测功能。可以定期检测断掉的原服务器的可用状态，如果原服务器恢复为可用状态，可以自动将原服务器设回原服务类型（主/备），或通过命令切换到主服务器。
- 提供通过命令行切换主备RADIUS服务器的功能，使得在主用和备用服务器之间实现人工切换。

◎ 使能/禁止 RADIUS Server 主备切换功能

【命令语法】radius [accounting|authentication] server-switch [enable|disable]

【使用指导】选择 accounting 参数表示可以使能/禁止计费服务器的主备切换功能，选择 authentication 参数表示可以使能/禁止认证服务器的主备切换功能。缺省配置为 disable。

◎ 设置是否将主备切换信息通知给 802.1x 模块

在发生 RADIUS 服务器主备切换时，可以设置是否将此信息通知给 802.1x 模块。如果通知 802.1x 模块，就会让已经认证的用户通过备用服务器进行重认证；如果不通知 802.1x 模块，RADIUS 服务器主备切换对已经认证的用户是透明的，不会进行重认证。使用以下命令来配置发生 RADIUS 服务器主备切换时是否通知 802.1x：

【命令语法】radius serverswitch-notify [enable|disable]

12.8.7 配置 RADIUS 属性

由于在不同的网络环境下，不同的 RADIUS 服务器对某些 RADIUS 属性的具体值要求不同，如一些窄带的 RADIUS 服务器要求 Frame-Protocol 的值必须为 PPP，这使我们和它对接时，必须把该属性值设为 PPP。为了适应不同 RADIUS 服务器的要求，港湾网络有限公司的 Hammer 系列交换机提供了对这类属性值的配置功能。

◎ 配置 RADIUS 属性的值：

配置 Frame-Protocol 的值，配置命令如下：

【命令语法】radius config-attribute frame-protocol <0-255>

【使用指导】<0-255>为 Frame-Protocol 的值，该值与协议的对应关系如下：

属性值<0-255>	对应协议
1	PPP
2	SLIP
3	AppleTalk Remote Access Protocol (ARAP)
4	Gandalf proprietary SingleLink/MultiLink protocol
5	Xylogics proprietary IPX/SLIP
6	X.75 Synchronous

配置 nas-port-type 属性的值（nas-port-type 也是 RADIUS 属性之一），配置命令如下：

【命令语法】radius config-attribute nas-port-type <0-255>

【使用指导】<0-255>为 nas-port-type 的值，该值与 NAS 端口类型的对应关系如下：

属性值<0-255>	NAS 端口类型
0	Async
1	Sync
2	ISDN Sync
3	ISDN Async V.120
4	ISDN Async V.110
5	Virtual
6	PIAFS
7	HDLC Clear Channel
8	X.25
9	X.75
10	G.3 Fax
11	SDSL - Symmetric DSL
12	ADSL-CAP - Asymmetric DSL, Carrierless Amplitude Phase Modulation
13	ADSL-DMT - Asymmetric DSL, Discrete Multi-Tone
14	IDSL - ISDN Digital Subscriber Line
15	Ethernet
16	xDSL - Digital Subscriber Line of unknown type
17	Cable
18	Wireless - Other
19	Wireless - IEEE 802.11

◎ 显示 RADIUS 属性值的配置：

```
show radius config-attribute frame-protocol
show radius config-attribute nas-port-type
```

12.8.8 配置实例

实例 1：

打开 RADIUS 的认证功能，同时增加一个 RADIUS 认证服务器，该服务器的 IP 地址为 10.7.1.9，客户端的 IP 地址是 10.7.1.253，端口号 1812。设服务器与客户端的共享密钥为”xyzzy5461”。设置允许客户端向认证服务器重传报文的时间间隔为 5 秒，最大重传次数为 2 次，最大发送失败次数为 2 次，最大重传丢弃次数为 2 次。具体配置步骤如下：

```
Harbour(config)# radius authentication enable

Harbour(config)# radius authentication add-server id 0 server-ip 10.7.1.9
client-ip 10.7.1.253 udp-port 1812
```

Harbour(config)# radius authentication config-server id 0 shared-secret xyzzy5461

Harbour(config)# radius authentication config-server id 0 retransmit-

```
interval 5

Harbour(config)# radius authentication config-server id 0 max-retransmit-
count 2

Harbour(config)# radius authentication config-server id 0 max-send-fail-
count 2

Harbour(config)# radius authentication config-server id 0 max-retransmit-
drop-count 2
```

实例 2：

删除 ID 为 0 的 RADIUS 认证服务器，并关闭 RADIUS 的认证功能。配置步骤如下：

```
Harbour(config)# radius authentication delete-server id 0

Harbour(config)# radius authentication disable
```

12.8.9 RADIUS 显示命令

有关 RADIUS 信息的显示命令见表 12-3。

表 12-3： RADIUS 显示命令列表

显示命令	功能描述
show radius [accounting|authentication] server-switch	显示 RADIUS 认证或计费服务器的主备倒换功能是否启用
show radius accounting session-timeout-type	显示计费服务器的 Session Timeout 类型
show radius cut process-way	显示 CUT 请求处理机制
show radius cut verify-way	显示 CUT 报文校验方式
show radius idpool	显示 RADIUS 服务器 ID 号的使用情况，用于调试
show radius {configuration}*1	显示 RADIUS 配置信息
show radius config-attribute frame-protocol	显示 Frame-Protocol 属性的值
show radius config-attribute nas-port-type	显示 Nas-Port-Type 属性的值
show radius custom-attributes	显示 RADIUS 属性类型

12.9 配置域

在 Hammer10000 IP-DSLAM 接入交换机的接入模块中，我们引入了域（isp-domain）的概念。

不同的域可能由不同的 ISP 经营。接入设备根据用户输入的用户名中的域名部分（用户名@域名）来区分用户所属的域，并将其认证和计费请求发送到相应域的认证和计费服务器。

建立了域的概念以后，当我们在系统中增加 RADIUS 服务器时，必须将其分配给相应的域才能使用。系统中缺省包含一个名为 default 的域，如果不创建新的域，系统将所有的用户认证请求都发送到 default 域中的 RADIUS 认证服务器。

如果要删除一个域，应首先将属于该域的 RADIUS 服务器从域中删除。

注意：

默认域 default 不能删除。

12.9.1 域的基本配置

有关域的基本配置命令具体如下：

◎ 创建域

【命令语法】create isp-domain <domain>

【使用指导】其中<domain>为所创建的域的域名。

◎ 删除域

【命令语法】delete isp-domain <domain>

【使用指导】其中<domain>为所要删除的域的域名。

◎ 配置是否将完整的用户名发送给 RADIUS 服务器

完整的用户名表现为“ 用户名@域名 ”，当选择发送不完整的用户名时表示去掉用户名后面的域名部分。配置命令如下：

【命令语法】config isp-domain <domain> username [complete|incomplete]

【使用指导】选择 complete 表示将完整的用户名发送给 RADIUS 服务器；选择 incomplete 表示发送不带域名的用户名。例如用户输入的用户名和域名为 abc@domain，若配置为发送完整的用户名和域名，则将 abc@domain 作为用户名发送给 RADIUS 服务器；若使用不完整的用户名，则只将 abc 作为用户名发送给 RADIUS 服务器。

12.9.2 域的认证配置

◎ 向域中添加/删除认证服务器

【命令语法】config isp-domain <domain> authentication [add-server|delete-server] id <id>

【使用指导】add-server 表示向名为<domain>的域添加认证服务器；

delete-server 表示从名为<domain>的域删除认证服务器；

由于一个域可以包含多个认证服务器，因此需要指定每个认证服务器的 ID 标识<id>。

◎ 启动/禁止域内的 RADIUS 认证功能

【命令语法】config isp-domain <domain> authentication [enable|disable]

【使用指导】启动或停止某个域的认证功能并不影响其他域的认证或计费功能。

◎ 配置域的认证模式

每个域有两种认证模式：独立认证模式（independent）和主备认证模式（primary_backup）。如果使用独立认证模式，当域中的主认证服务器发生故障时，不把认证转移到域内的备用认证服务器上。如果使用主备认证模式，当域中的主认证服务器发生故障时，设备自动将认证切换到备用认证服务器上。

配置域的认证模式使用以下配置命令：

【命令语法】config isp-domain <domain> authentication mode [independent|primary-backup]

【使用指导】在<domain>处输入要配置的域的域名。选择 independent 表示使用独立认证模式，选择 primary-backup 表示使用主备认证模式。

应当注意的是，若要配置域的认证模式为 primary-backup，需要首先使能 RADIUS 认证服务器的主备切换功能，也就是先做如下配置：

```
Harbour(config)# radius authentication server-switch enable
```

◎ 指定主认证服务器

【命令语法】config isp-domain <domain> authentication config-server id <id> type primary

【使用指导】默认情况下，<id>值最小的认证服务器为主认证服务器。

12.9.3 域的计费配置

◎ 向域中添加/删除计费服务器

【命令语法】config isp-domain <domain> accounting [add-server|delete-server] id <id>

【使用指导】add-server 表示向名为<domain>的域添加计费服务器，delete-server 表示从名为<domain>的域删除计费服务器。由于一个域可以包含多个计费服务器，因此需要指定每个计费服务器的 ID 标识<id>。

◎ 启动/禁止域内的 RADIUS 计费功能

【命令语法】config isp-domain <domain> accounting [enable|disable]

【使用指导】默认为 enable。

◎ 配置计费服务器在域中的类型

【命令语法】config isp-domain <domain> accounting config-server id <id> type [primary|backup]

【使用指导】primary 表示把某个 RADIUS 计费服务器置为主计费服务器；backup 表示把域中的某个 RADIUS 计费服务器设置成备份计费服务器，若该计费服务器是主计费服务器，则从备份服务器中选择第一个备份计费服务器作为主计费服务器。

注意：

认证和计费服务器的主备切换是分开进行的，认证和计费服务器的主备切换互不影响。

◎ 配置域中 RADIUS 计费服务器的计费模式

【命令语法】config isp-domain <domain> accounting mode [independent|primary-backup|multi]

【使用指导】默认为 independent。

独立计费模式(independent)是指当 RADIUS 主计费服务器出现故障的时候，交换机不主动把计费信息发送到备用 RADIUS 计费服务器上；主备计费模式(primary-backup)是指当 RADIUS 主计费服务器出现故障的时候，交换机自动把计费切换到备用 RADIUS 计费服务器上；多服务器计费模式(multi)是指在交换机计费的时候，把一份计费信息同时向多个 RADIUS 计费服务器发送。

应当注意的是，若要配置域的计费模式为 primary-backup，需要首先使能 RADIUS 计费服务器的主备切换功能，也就是先做如下配置：

```
Harbour(config)# radius accounting server-switch enable
```

◎ 配置即时计费时间间隔

即时计费功能(Interim Update Accouting)是指在发送计费开始请求和计费结束请求之间定期发送即时计费请求，以便将在线用户的计费信息定期发送到 RADIUS 计费服务器。

配置即时计费请求的时间间隔，并打开发送功能，输入以下命令：

【命令语法】config isp-domain <domain> accounting interim-update-accounting interval <10-65535>

关闭即时计费请求发送功能，输入以下命令：

【命令语法】config isp-domain <domain> accounting interim-update-accounting disable

【使用指导】默认为 disable（即间隔时间为 0）。

◎ 配置开始计费时是否等待用户获取 IP

接入服务支持与 DHCP Relay、DHCP Proxy、IP Local Pool 功能相结合。即当用户获得了 IP 之后，会通知设备的 NAS 模块，从而可以通过相关命令察看到某用户动态获得的 IP 地址；当用户主动 Release 了自己的 IP 地址之后，我们也可以通过相关命令察看到该用户的 IP 为未知。如果用户是自动获取 IP 的方式，那么可以配置在发送计费请求报文之前是否获得用户的 IP 地址。

配置发送计费开始请求之前是否必须先得到用户 IP 地址，输入命令：

【命令语法】config isp-domain <domain> accounting start-need-ip [enable|disable]

【使用指导】参数 enable 表示认证通过之后一定要在得到 IP 地址以后再发计费请求，参数 disable 表示认证通过之后不必得到 IP 地址就可以发计费请求。默认为 enable。

◎ 配置交换机等待用户获取 IP 地址的最长时间：

如果设置为在认证通过之后一定要等到用户获得了 IP 地址再发送计费请求，那么需要设置经过多长时间之后如果用户还没有得到 IP 地址，则根据超时机制切断该用户的连接，配置命令如下：

【命令语法】config isp-domain <domain> accounting wait-ip <100-600>

【使用指导】参数<100-600>表示等待的时间，单位是秒，系统默认为等待 100 秒。

◎启动/禁止域的计费超时功能

用户认证通过后，会发送计费开始报文通知计费服务器，并在收到该报文的应答后确认对用户的计费开始。当配置了域的计费超时功能后，如果计费开始报文重传一定次数均未收到应答，则根据超时机制切断该用户的连接。输入命令如下：

【命令语法】config isp-domain <domain> accounting timeout [enable|disable]

【使用指导】参数 enable 表示认证通过之后一定要在得到计费开始报文的应答后才设置用户为上线状态；参数 disable 表示认证通过之后不必得到计费开始报文的应答就设置用户为上线状态。默认为 enable。

12.9.4 配置实例

在名为 harbour 的域中，设置在发送计费报文时需要用户的 IP 地址，等待用户端获取 IP 地址的超时时间设为 180 秒，并且使用即时计费功能，计费间隔设为 180 秒。配置步骤具体如下：

Harbour(config)# config isp-domain harbour accounting start-need-ip enable

Harbour(config)# config isp-domain harbour accounting wait-ip 180

Harbour(config)# config isp-domain harbour accounting interim-update-accounting interval 180

12.10 PPPoE 终结

12.10.1 概述

Hammer10000 IP-DSLAM 接入交换机内置 PPPoE 终结，由主控板（SMU）完成 PPPoE 用户接入认证过程，由业务板（ADU）完成 PPPoE 数据报文到以太网报文的转换。Hammer10000 IP-DSLAM 接入交换机接受客户机的 PPPoE 连接请求后，根据认证协商选项，通过与 Radius 认证服务器的交互完成对客户机接入的认证，同时发送 Radius 计费数据报文启动计费，最后分配给客户机一个合适的 IP 地址以完成 PPPoE 的接入。为客户机分配 IP 地址的方式有两种：一种是直接从本地 IP 地址池中分配 IP 地址，另外一种是通过 DHCP 客户端代理向 DHCP 服务器动态申请 IP 地址。

内置 PPPoE 终结支持 PPPoE 端口间的网段内隔离，其隔离工作由业务板完成。每块业务板须配置一网关地址（IP/掩码），被隔离端口所获取 IP 地址须在同一网段。原理为当业务板从启用 PPPoE 隔离的端口接收到上行数据报文后，如果发现其目的 IP 和网关地址在同一网段，则将报文丢弃。因此 PPPoE 用户无法访问同网段的其他 PPPoE 用户，起到 PPPoE 端口间网段内隔离的目的。

12.10.2 PPPoE 终结包括两个方面的配置任务

- PPPoE 参数配置
- PPP 参数设置（**请参考配置 PPP**）

12.10.3 端口启用 PPPoE 功能

【命令语法】 `config port [<portlist>|all] pppoe-terminate [enable|disable]`

【使用指导】 `[enable|disable]`：选择 `enable` 表示启用端口 `PPPoE` 接入功能，选择 `disable` 表示禁用端口 `PPPoE` 接入功能。

【命令模式】 运行于配置模式。

【配置实例】 配置端口 `14:15` 启用 `PPPoE` 功能

```
Harbour(config)# config port 14:15 pppoe-terminate enable
```

12.10.4 端口启用 PPPoE 网段内隔离

【命令语法】 `config port <portlist> pppoe-separation [enable|disable]`

【使用指导】 `[enable|disable]`：选择 `enable` 表示使能 `PPPoE` 网段内隔离功能，选择 `disable` 表示禁用 `PPPoE` 网段内隔离功能。

【命令模式】 运行于配置模式。

【配置实例】 配置端口 `14:15` 使能 `PPPoE` 网段内隔离功能

Harbour(config)# config port 14:15 pppoe-separation enable

注意：

端口配置 PPPoE 端口隔离后，必须配置业务板的网关地址，否则端口无法通过任何报文。

12.10.5 配置业务板网关地址

【命令语法】 config slot [<slotnumber>|all] gateway <A.B.C.D> <A.B.C.D>

【使用指导】 [<slotnumber>|all]：输入 slotnumber 表示业务板槽号，选择 all 表示配置所有业务板网关地址；

<A.B.C.D>： 网关 IP 地址；

<A.B.C.D>： 网关地址掩码。

【命令模式】 运行于配置模式。

【配置实例】 配置端口 14 槽业务板网关地址

Harbour(config)# config slot 14 gateway 100.1.1.1 255.255.255.0

12.10.6 配置应用实例

配置一个 PPPoE 接入环境需要涉及到几个相关部分的配置：

- VLAN 接口配置
- DHCP 客户端代理配置
- Radius 认证/计费配置
- 静态地址池配置
- PPP 配置
- 端口 PPPoE 配置

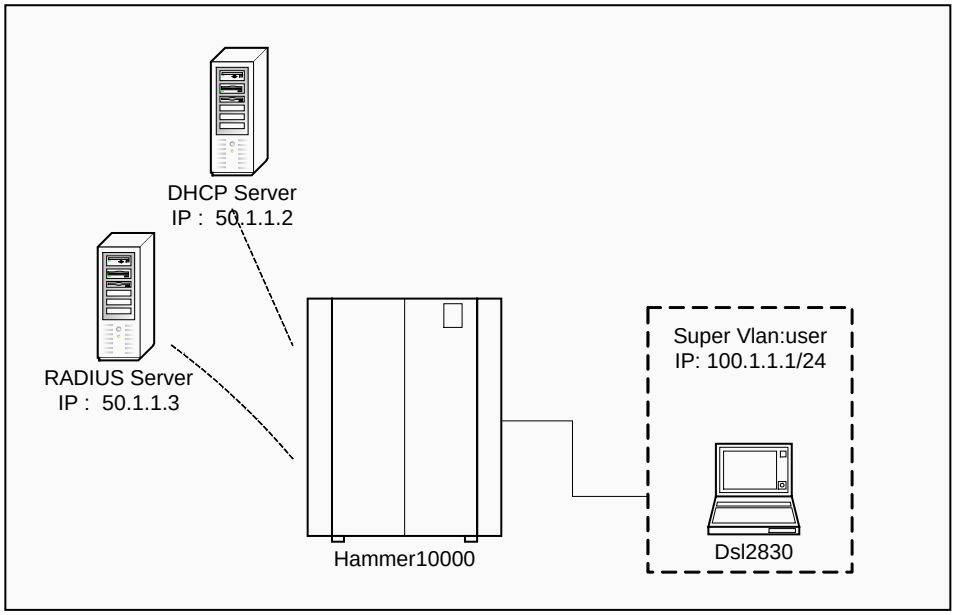


图 12-7　PPPoE 终结应用组网图

以端口 14:15 配置 PPPoE 接入为例，通过 DHCP 动态分配 IP 地址；DHCP 服务器和 Radius 认证/计费服务器的配置如图 12-7 所示。

配置步骤：

（1）创建一个接口 VLAN(uplink)，将端口 0:1 和 0:2 加入 uplink 中，Hammer10000 IP-DSLAM 接入交换机通过 0:1 端口 与 DHCP 服务器进行通信，通过 0:2 端口与 Radius 认证/计费服务器通信。

Harbour(config)# create vlan uplink

Harbour(config)# config vlan uplink ipaddress 50.1.1.1/24

Harbour(config)# config vlan uplink add port 0:1,0:2 untagged

（2）创建一个 SUPER VLAN(user)，包含主机接入端口所在的 SUB VLAN；dsl2830 是端口 14:15 所在的 SUB VLAN；DHCP 服务器配置了一个作用域，其 IP 地址范围为：100.1.1.2~100.1.1.254，网关：100.1.1.1。

Harbour(config)# create vlan user super

Harbour(config)# config vlan user ipaddress 100.1.1.1/24

Harbour(config)# config vlan user add subvlanbyport 14:15

（3）在配置模式下配置 Radius 参数

Harbour(config)# radius authentication add-server id 0 server-ip 50.1.1.3 client-ip 50.1.1.1

Harbour(config)# radius accounting add-server id 0 server-ip 50.1.1.3 client-ip 50.1.1.1

Harbour(config)# radius authentication enable

Harbour(config)# radius accounting enable

（4）配置 DHCP 客户端代理

Harbour(config)# config dhcpc-proxy listen add uplink

Harbour(config)# config dhcpc-proxy targetip add 50.1.1.2

Harbour(config)# service dhcpc-proxy enable

（5）创建静态地址池 pool1，IP 地址范围 100.1.1.2～100.1.1.254

Harbour(config)# ip local pool pool1 100.1.1.2 100.1.1.254

（6）进入 user 接口中进行 PPP 参数配置

Harbour(config)# interface user

Harbour(config-if)# ppp authentication chap

对端 IP 地址获取方式为 dhcp client-proxy 方式

Harbour(config-if)# peer ip address dhcpc-proxy

对端 IP 地址获取方式为静态地址池方式

Harbour(config-if)# peer ip address pool pool1

（7）启用端口 14:15 的 PPPoE 认证功能

Harbour(config-if)# config port 14:15 pppoe-terminate enable

12.11 DSL 端口绑定

12.11.1 MAC 地址绑定

此命令用来限定一个 DSL 端口上只能使用限定的 MAC 地址。若使该命令有效，需执行以下二个步骤：

第一步：使能 DSL 端口的 MAC 地址绑定

【命令语法】config port [<portlist>|all] bind mac enable

第二步：在 DSL 端口上绑定 MAC 地址

【命令语法】create bindmacentry <mac_address> <portlist>

【使用指导】每个端口上最多绑定 10 个 MAC 地址

相关命令：

1．禁止/使能 DSL 端口的 MAC 地址绑定

【命令语法】config port [<portlist>|all] bind mac [enable|disable]

2．创建/删除 DSL 端口绑定的 MAC 地址

【命令语法】create bindmacentry <mac_address> <portlist>

delete bindmacentry <mac_address> <portlist>

3．显示 DSL 端口绑定的 MAC 地址信息

【命令语法】show port [<portlist>|all] bind mac

注意：

所有源 MAC 未配置的包将丢弃。

12.11.2 MAC 地址数目限制

此命令用来限制每个端口上能够访问的 MAC 地址的个数。相关的命令如下：

【命令语法】config port [<portlist>|all] maclimit <0-128>

config port [<portlist>|all] maclimit [enable|disable]

【使用指导】其中，端口 MAC 数目限制相关命令如下（在 CONFIG_MODE 模式）。

1.配置 DSL 端口 MAC 数目限制 enable 或 disable。

【命令语法】config port [<portlist>|all] maclimit [enable|disable]

【使用指导】选择<portlist>表示对指定端口进行操作。用户可以选择输入某个板卡的某个端口，如 6:1，也可以输入某个板卡上的多个连续端口，如 6:1－6:6，还可以输入某板卡上多个连续和不连续的端口，如 6:1,6:3-6:6；

选择 all，表示对交换机的所有的 DSL 端口进行操作；

选择 enable，将端口 MAC 限制设为 enable；

选择 disable，将端口 MAC 限制设为 disable。

【配置实例】配置端口 4:1MAC 限制使能

Harbour(config)# config port 4：1 maclimit enable

2.配置 DSL 端口 MAC 限制数目。

【命令语法】config port [<portlist>|all] maclimit <0-128>

【使用指导】选择<portlist>表示对指定端口进行操作。用户可以选择输入某个板卡的某个端口，如 6:1，也可以输入某个板卡上的多个连续端口，如 6:1－6:6，还可以输入某板卡上多个连续和不连续的端口，如 6:1,6:3-6:6；

选择 all，表示对交换机的所有的 DSL 端口进行操作；

参数<0-128>，表示端口允许的 MAC 数目。为 0 时，表示此端口不接受任何 MAC 地址。

【配置实例】配置端口 4:1mac 限制使能

Harbour(config)# config port 4：1 maclimit 1

3.显示 DSL 端口 MAC 限制。

【命令语法】show port [<portlist>|all] maclimit

【使用指导】选择<portlist>表示对指定端口进行操作。用户可以选择输入某个板卡的某个端口，如 6:1，也可以输入某个板卡上的多个连续端口，如 6:1－6:6，还可以输入某板卡上多个连续和不连续的端口，如 6:1,6:3-6:6；

选择 all，表示对交换机的所有的 DSL 端口进行操作。

【配置实例】显示端口 4:1MAC 限制

```
Harbour(config)# show port  4：1  maclimit
```

12.11.3 IP 地址绑定

此命令用来限定一个 DSL 端口上只能使用绑定的 IP 地址。如果端口上已经绑定了 MAC 地址，则带此 IP 的 MAC 地址必须是此端口上绑定的 MAC。若使该命令有效，需执行以下两个步骤：

第一步：使能 DSL 端口的 IP 地址绑定

【命令语法】config port [<portlist>|all] bind ip enable

第二步：在 DSL 端口上绑定 IP 地址

【命令语法】create bindipentry <A.B.C.D> <portlist>

相关命令：

1．禁止 DSL 端口的 IP 地址绑定

【命令语法】config port [<portlist>|all] bind ip disable

2．删除 DSL 端口上绑定的 IP 地址

【命令语法】delete bindipentry <A.B.C.D> <portlist>

3．显示 DSL 端口上绑定的 IP 地址信息

【命令语法】show port [<portlist>|all|active] bind ip

【使用指导】每个端口上最多绑定 10 个 IP 地址。

注意：

启用绑定 IP 后将不允许启用 802.1x 认证。

接入服务应用配置实例

12.12 单域认证

在交换机的接入服务系统中有一个默认的域 default，如果不使用多域功能，则不必创建新的域，直接利用 default 域即可。以下我们将介绍实现单域认证的最小配置。

如图 12-8 所示，Hammer10000 IP-DSLAM 接入交换机的上行端口连接两个 RADIUS 服务器，每个服务器均具有认证和计费功能。IP 地址为 10.10.11.1 的服务器，其 ID 为 0，是系统默认的主认证计费服务器。

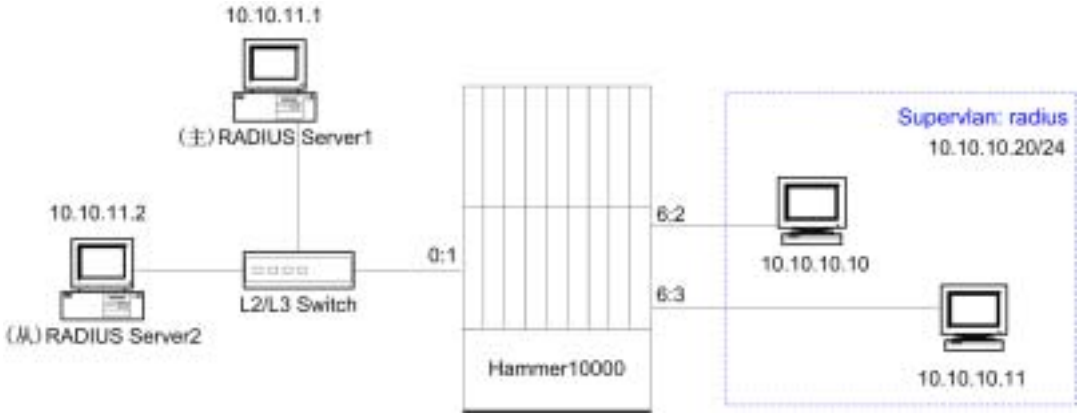


图 12-8 单域认证网络图

配置步骤具体如下：

1．配置 802.1x

！使能 802.1x 认证服务

Harbour(config)# config dot1x enable

！使能 802.1x 认证服务端口

Harbour(config)# config port 6:1-6:32 dot1x enable

！将连接客户的端口 6:1-6:32 的认证状态设为 auto

Harbour(config)# config port 6:1-6:32 dot1x authcontrolledportcontrol auto

2．配置 RADIUS

！增加两台认证计费服务器，每台服务器均具有认证计费功能。设 IP 地址为 10.10.11.1 的 RADIUS 服务器的 ID 为 0，IP 地址为 10.10.11.2 的 RADIUS 服务器的 ID 为 1（在没有指定主认证计费服务器的情况下，系统以 ID 号最小的服务器作为主服务器）。

Harbour(config)# radius authentication add-server id 0 server-ip 10.10.11.1 client-ip 10.10.11.254

Harbour(config)# radius accounting add-server id 0 server-ip 10.10.11.1 client-ip 10.10.11.254

Harbour(config)# radius authentication add-server id 1 server-ip 10.10.11.2 client-ip 10.10.11.254

Harbour(config)# radius accounting add-server id 1 server-ip 10.10.11.2 client-ip 10.10.11.254

！设置主认证服务器的共享密钥是“ harbour ”

Harbour(config)# radius authentication config-server id 0 shared-secret harbour

！使能 RADIUS 认证计费功能

Harbour(config)# radius authentication enable

Harbour(config)# radius accounting enable

12.13 多域认证

多域认证的 802.1x 及 RADIUS 配置与单域认证相同，不同的只是创建一些新的域，并把 RADIUS 服务器分配到相应的域中。以下我们将介绍实现多域认证的最小配置。

组网形式与图 12-8 相同，只是将两个服务器分别设在两个域（domain1、domain2）中。

配置步骤具体如下：

1．配置 802.1x

同单域认证配置。

2．配置 RADIUS

同单域认证配置。

3．配置域

！创建两个域，domain1 和 domain2

```
Harbour(config)# create isp-domain domain1

Harbour(config)# create isp-domain domain2
```

！将两个 RADIUS 服务器分别添加到 domain1 和 domain2 中

```
Harbour(config)# config isp-domain domain1 authentication add-server id 0

Harbour(config)# config isp-domain domain1 accounting add-server id 0
Harbour(config)# config isp-domain domain2 authentication add-server id 1

Harbour(config)# config isp-domain domain2 accounting add-server id 1
```

根据上述配置，如果用户 user01 要在 domain2 上通过认证，则需在客户端软件的用户名处输入用户名 user01@domain2。

12.14 服务器的主备切换

下面以认证服务器的主备切换为例，介绍一下 RADIUS 服务器主备切换的配置方法。组网形式与图 12-8 相同。两台 RADIUS 服务器在 domain1 域中均为认证服务器，其中 ID 为 0 的服务器为主认证服务器，要实现在 domain1 域中两台服务器能够主备切换。

配置步骤具体如下：

1．配置 802.1x

同单域认证配置。

2．配置 RADIUS

增加两台认证服务器，设 IP 地址为 10.10.11.1 的 RADIUS 服务器的 ID 为 0，IP 地址为 10.10.11.2 的 RADIUS 服务器的 ID 为 1（在没有指定主认证服务器的情况下，系统以 ID 号最小的服务器作为主认证服务器）。

```
            Harbour(config)# radius authentication add-server id 0 server-ip 10.10.11.1
client-ip 10.10.11.254

            Harbour(config)# radius authentication add-server id 1 server-ip 10.10.11.2
client-ip 10.10.11.254
```

！设置认证服务器的共享密钥是“ harbour ”

```
            Harbour(config)# radius authentication config-server id 0 shared-secret
harbour
            Harbour(config)# radius authentication config-server id 1 shared-secret
harbour
```

！使能 RADIUS 认证计费功能

```
Harbour(config)# radius authentication enable

Harbour(config)# radius accounting enable
```

！启动 RADIUS 认证服务器主备切换功能

```
            Harbour(config)# radius authentication server-switch enable
```

3．配置域

！创建域 domain1

```
            Harbour(config)# create isp-domain domain1
```

！将两个 RADIUS 服务器添加到 domain1 域中

```
Harbour(config)# config isp-domain domain1 authentication add-server id 0
Harbour(config)# config isp-domain domain1 authentication add-server id 1
```

！配置域的认证模式为 primary-backup

```
Harbour(config)# config isp-domain domain1 authentication mode
primary-backup
```

附录： 接入服务命令集

命令	功能描述
config nas binduser [add|delete] port [<portlist>|all] user <username>	在端口处添加或删除绑定的用户
config nas binduser port [<portlist>|all] [enable|disable]	使能或禁止用户绑定功能
config nas binduser clear_all	清除所有用户绑定信息
config nas binduser multi_port_per_user [enable|disable]	使能或关闭一个用户绑定到多个端口的功能
config dot1x authenticate-protocol [chap|eap-md5|pap]	配置用户的身份验证方式
config dot1x clear-statistic	清除 802.1x 统计信息
config dot1x keepalive [enable|disable]	启动或关闭异常下线检测功能
config dot1x keepalive max-no-response-count <2-30>	设置允许客户端未响应的最大次数
config dot1x keepalive mechanism [ping-pong|state-machine]	设置异常下线检测的方法
config dot1x keepalive state-machine-period <10-3600>	设置发送异常下线检测报文的时间间隔
config dot1x keepalive ping-pong-period <30-600>	设置交换机从发送异常下线检测报文开始到获得客户端响应之间的时间间隔
config dot1x max-req <1-10>	设置交换机向客户端重传数据帧的最大次数
config dot1x reauth-max <1-10>	配置交换机向客户端重传 EAP-Request/Identity 的最大次数
config port [<portlist>|all] dot1x max-hosts <2-512>	设置指定端口最多允许接入客户端的数目
config dot1x pae force-logoff ip < address >	根据客户端的 IP 地址强制用户退出认证状态
config dot1x pae force-logoff all	强制所有用户退出认证状态
config dot1x pae force-logoff id <paeid>	根据端口访问实体（PAE）的 ID 号强制用户退出认证状态
config dot1x pae force-logoff mac <usermac> {port <portno>}*1	根据客户端的 MAC 地址强制用户退出认证状态
config dot1x pae force-logoff port <portno>	根据端口号强制用户退出认证状态
config dot1x quiet-period <0-32767>	设置在一次认证失败后的多

	长时间内认证系统不接收来自客户端系统的认证请求
config dot1x re-authentication [enable|disable]	使能/关闭重新认证机制
config dot1x re-authentication period <1-32767>	设置重新认证的时间间隔
config dot1x server-timeout <1-32767>	设置认证系统接收来自认证服务器数据包的超时时间
config dot1x supp-timeout <1-32767>	设置认证系统接收来自客户端系统数据包的超时时间
config dot1x supp-upgrade-force [enable|disable]	配置客户端软件更新功能
config dot1x supp-upgrade-url <url>	配置客户端软件更新 URL 地址
config dot1x tx-period <1-32767>	设置认证系统向客户端系统重传 EAP-Request/Identity 数据帧的时间间隔
config isp-domain <domain> accounting [add-server|delete-server] id <id>	向域中添加/删除计费服务器
config isp-domain <domain> accounting [enable|disable]	启动/禁止域内的 RADIUS 计费功能
config isp-domain <domain> accounting config-server id <id> type [primary|multi |backup]	配置计费服务器在域中的类型
config isp-domain <domain> accounting interim-update-accounting disable	关闭即时计费请求发送功能
config isp-domain <domain> accounting interim-update-accounting interval <10-65535>	配置即时计费请求的时间间隔，并打开发送功能
config isp-domain <domain> accounting mode [independent|primary-backup|multi]	配置域中 RADIUS 计费服务器的计费模式
config isp-domain <domain> accounting start-need-ip [enable|disable]	配置发送计费开始请求之前是否必须先得到用户 IP 地址
config isp-domain <domain> accounting sync [enable|disable]	配置交换机重新启动后是否向 RADIUS 服务器发送计费同步报文
config isp-domain <domain> accounting wait-ip <100-600>	配置交换机等待客户端获取 IP 地址的最长时间
config isp-domain <domain> authentication [add-server|delete-server] id <id>	向域中添加/删除认证服务器
config isp-domain <domain> authentication [enable|disable]	启动/禁止域内的 RADIUS 认证功能
config isp-domain <domain> authentication config-server id <id> type primary	指定主认证服务器
config isp-domain <domain> authentication mode [independent |primary-backup]	设置域的认证模式

config isp-domain <domain> username [complete |incomplete]	设置是否将完整的用户名发送给 RADIUS 服务器
config port [<portlist>|all] dot1x authcontrolledportcontrol [auto|forceauth|forceunauth]	配置端口的认证状态
config port [<portlist>|all] dot1x [enable|disable]	使能/关闭 802.1x 认证服务
config port [<portlist>|all] dot1x port-control-mode [MAC-based|port-based]	配置端口的控制模式
create isp-domain <domain>	创建一个名为<domain>的域
delete isp-domain <domain>	删除一个名为<domain>的域
radius [accounting|authentication] server-switch [enable|disable]	使能/禁止 RADIUS Server 主备切换功能
radius accounting add-server id <0-4> server-ip <A.B.C.D> client-ip <A.B.C.D> {udp-port <1-6500>}*1	增加 RADIUS 计费服务器
radius accounting config-server id <0-4> max-retransmit-count <2-10>	设置向计费服务器重传数据包的最大次数
radius accounting config-server id <0-4> max-retransmit-drop-count <2-30>	设置最大重传丢弃数，用于检验计费服务器是否断线
radius accounting config-server id <0-4> max-send-fail-count <2-30>	设置最大重传失败数，用于检验计费服务器是否断线
radius accounting config-server id <0-4> retransmit-interval <5-300>	设置向计费服务器重传数据包的时间间隔
radius accounting config-server id <0-4> shared-secret <secret>	设置计费服务器与客户端之间的共享密钥
radius accounting delete-server id <0-4>	删除 RADIUS 计费服务器
radius accounting disable	关闭 RADIUS 计费功能
radius accounting enabled	启动 RADIUS 计费功能
radius accounting session-timeout-type [logoff|reauthenticate]	设置 Session Timeout 的处理机制
radius authentication add-server id <0-4> server-ip <A.B.C.D> client-ip <A.B.C.D> {udp-port <1-6500>}*1	增加 RADIUS 认证服务器
radius authentication config-server id <0-4> max-retransmit-count <2-10>	设置向认证服务器重传数据包的最大次数
radius authentication config-server id <0-4> max-retransmit-drop-count <2-30>	设置最大重传丢弃数，用于检验认证服务器是否断线
radius authentication config-server id <0-4> max-send-fail-count <2-30>	设置最大重传失败数，用于检验认证服务器是否断线
radius authentication config-server id <0-4> retransmit-interval <5-300>	设置向认证服务器重传数据包的时间间隔
radius authentication config-server id <0-4> shared-secret <secret>	设置认证服务器与客户端之

	间的共享密钥
radius authentication delete-server id <0-4>	删除 RADIUS 认证服务器
radius authentication disable	关闭 RADIUS 认证功能
radius authentication enable	启动 RADIUS 认证功能
radius config-attribute frame-protocol <0-255>	配置 Frame-Protocol 的属性值
radius config-attribute nas-port-type <0-255>	配置 nas-port-type 的属性值
radius config-attribute source-mac standard <100-255>	设置用标准属性类型<100-255>中的哪个属性携带源 MAC 地址信息
radius cut add-server [authentication|accounting] id <0-4> {udp-port <1-6500>}*1	向列表中增加一个认证或计费服务器
radius cut delelte-server [authentication|accounting] id <0-4>	从列表中删除一个认证或计费服务器
radius cut disable	关闭接收 CUT 报文功能
radius cut enable	启动接收 CUT 报文功能
radius cut process-by [reauthentication|logoff]	设置处理 CUT 请求机制
radius cut verify-by [authenticator|message-authenticator|none]	设置校验 CUT 报文的方式
radius serverswitch-notify [enable|disable]	设置是否将主备切换信息通知给 802.1x 模块
show dot1x	显示 802.1x 功能开启或关闭的状态以及相关的参数配置信息
show dot1x authenticate-protocol	显示用户的身份验证方式
show dot1x pae all	显示所有 PAE
show dot1x pae id <id>	根据 PAE id 索引值显示与之对应的 PAE 信息
show dot1x pae mac <address> {port <portlist>}*1	根据 MAC 地址显示对应的端口访问实体 PAE 绑定的用户 MAC 地址、Authenticator 状态、后台认证状态、重认证状态等信息
show dot1x pae port <portlist>	根据端口号显示与之相关联的所有创建的 PAE 信息，以及 PAE 总数
show dot1x statistic	显示 802.1x 统计信息
show nas binduser multi-port-per-user status	显示绑定多个端口的用户信息
show nas binduser port [<portlist>|all]	显示某一端口上的用户绑定

	信息
show nas binduser user <username>	根据用户名显示端口绑定信息
show nas accounting-statistic	显示计费统计信息
show nas user username <name>	根据用户名显示用户信息
show nas user mac <address>	根据 MAC 地址显示用户信息
show nas user ip <address>	根据 IP 地址显示用户信息
show nas user port <portno>	根据端口号显示用户信息
show nas user vlan <vlanname>	根据 VLAN 显示用户信息
show nas user isp-domain <domain>	根据所在的域显示用户信息
show nas user statistic	显示用户统计信息
show nas version	显示 NAS 版本信息
show port [<portlist>|all] dot1x	显示一组端口对应的 802.1x 相关信息，包括端口号、当前创建的 PAE 实体的个数以及在某一时刻曾经创建过最多的 PAE 实体的个数
show radius [accounting|authentication] server-switch	显示 RADIUS 认证或计费服务器的主备倒换功能是否启用
show radius accounting session-timeout-type	显示计费服务器的 Session Timeout 类型
show radius config-attribute frame-protocol	显示 Frame-Protocol 属性的值
show radius config-attribute nas-port-type	显示 Nas-Port-Type 属性的值
show radius custom-attributes	显示 RADIUS 属性类型
show radius cut process-way	显示 CUT 请求处理机制
show radius cut verify-way	显示 CUT 报文校验方式
show radius idpool	显示 RADIUS 服务器 ID 号的使用情况，用于调试
show radius {configuration}*1	显示 RADIUS 配置信息

第13章 日志模块(Syslog)

本章主要包括以下内容：

- 日志模块概述
- 日志功能基本配置
- 日志信息存储方式配置
- 日志信息显示方式配置
- 查看日志模块的配置情况
- 日志模块命令列表

13.1 日志模块概述

日志模块主要用来记录整个系统的运行情况以及用户操作行为。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 Monitor ，这种方式主要用于调试和查看系统状态。也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。

13.2 日志功能基本配置

13.2.1 打开或关闭日志服务

打开或关闭日志服务功能

【命令语法】`config syslog [enable|disable]`

【使用指导】选择 `enable` 表示打开日志服务功能；

选择 `disable` 表示关闭日志服务功能。

【命令模式】运行于配置模式。

【配置实例】

Harbour(config)# config syslog enable

Successfully changed syslog service to enable

打开日志服务功能。

13.2.2 配置所要记录的日志信息的类型

配置日志模块是否对某一类型的日志信息进行记录：

【命令语法】`config syslog type [<name>|all] [enable|disable]`

【使用指导】name 为系统中支持的日志类型，可用 show syslog configuration 来查看日志类型，目前支持的类型有 AUTH,CLI,SYSLOG,DEVCTRL,DOT1X,NAS,RADIUS,WEBAUTH,DHCPR,DHCPS,PORT,RIP,ROUTE,SNMP,STP,SYSTEM,VLAN,PORTB,GTDRV,FDB,TIMER,TELNETF,PACKETDEBUG,FFS,PPPOE,PPP,DHCPC,ADSL,IGMPS,L3SWITCH,BOARD,FPGA,LOCALBUS 等；

all 代表以上支持的所有日志类型；

选择 enable 表示对指定类型的信息进行记录；

选择 disable 表示不记录。

【命令模式】运行于配置模式。

【配置实例】

Harbour(config)# config syslog type auth enable

Successfully changed syslog type auth to enable.

注册 AUTH 类型的日志信息，日志模块将对 AUTH 类型的日志信息进行记录。

13.2.3 配置所要记录的日志信息的最低级别

配置日志模块对某一级别和高于该级别的日志信息进行记录

【命令语法】config syslog lowest-level <0-7>

【使用指导】目前支持的日志信息级别从 0 到 7 ，依次为 EMERG ， ALERT ， CRITERR ，WARNING ， NOTICE ， INFO ， DEBUG 。

【命令模式】运行于配置模式。

【配置实例】

Harbour(config)# config syslog lowest-level 3

Successfully changed syslog service lowest-lever level 3 [ERR].

级别 3 和高于级别 3 的日志信息将被记录，即级别 0、1、2、3 的日志信息将被记录。

注意：

数字越小，级别越高，如：级别 1 比级别 2 的级别高。

13.2.4 打开命令行操作日志记录功能

配置日志模块是否对命令行操作行为进行日志记录

【命令语法】record command-line [enable|disable]

【使用指导】选择 enable 表示对命令行操作进行记录；

选择 disable 表示对命令行操作不进行记录。

【命令模式】运行于配置模式。

【配置实例】

Harbour(config)# record command-line enable

Successfully changed syslog record CLI to enable.

允许对命令行操作行为记录日志信息。

注意：

命令行操作的日志信息级别为 6 ，即 INFO 类型。

13.3 日志信息存储方式配置

13.3.1 打开或关闭日志信息保存到日志服务器的功能

配置日志模块是否保存日志信息到日志服务器

【命令语法】`config syslog server [enable|disable]`

【使用指导】选择 `enable` 表示保存日志信息到服务器；

选择 `disable` 表示不保存日志信息到服务器。

【命令模式】运行于配置模式。

【配置实例】

Harbour(config)# config syslog server enable

Successfully changed syslog service logto server enable.

Warning: Syslog server config is empty.Please add syslog server.

允许日志保存到日志服务器。

注意：

在配置之前，保证日志服务器服务程序已启动。

13.3.2 增加或删除一个日志服务器

增加或删除一个日志服务器，包括配置日志服务器的 IP 地址，服务端口，日志信息的级别等信息

【命令语法】`config syslog [add|delete] server <A.B.C.D> {[port] <1-65535>}*1 {[facility] <0-7>}*1`

【使用指导】选择 add 表示增加一个日志服务器；

选择 delete 表示删除一个日志服务器；

A.B.C.D 表示日志服务器的 IP 地址；

port 是日志服务器上接收日志进程的服务端口号；

facility 对应于日志信息的级别，就是说这个日志服务器将保存某个级别和某个级别以上的日志信息。

可以使用一条命令配置日志服务器信息，也可以使用多条子命令进行配置。

关于日志服务器服务程序的配置详见相关手册。

【命令模式】运行于配置模式。

【配置实例 1】

Harbour(config)# config syslog add server 10.12.3.4 port 8808 facility 5

Successfully added syslog server 10.12.3.4.

配置了一个 IP 地址为 10.12.3.4 的日志服务器，服务端口为 8808 ，日志信息的级别 5 。

【配置实例 2】

Harbour(config)# config syslog delete server 10.1.4.1 port 6500 facility 1

Successfully deleted syslog server 10.1.4.1

删除了一个日志服务器，其 IP 地址为 10.1.4.1 ，服务端口为 6500 ，优先级为 1 。

13.4 日志信息显示方式配置

13.4.1 打开或关闭终端显示日志信息的功能

配置日志信息是否输出到用户终端。该命令是服务命令，将对所有终端起作用。

【命令语法】config syslog monitor-terminal [enable|disable]

【使用指导】选择 enable 表示允许日志信息输出到客户端；

选择 disable 表示不允许日志信息输出到客户端。

【命令模式】运行于配置模式。

【配置实例】

Harbour(config)# config syslog monitor-terminal enable

Successfully changed syslog service logto monitor-terminal to enable.

允许日志信息输出到所有用户终端。

13.4.2 打开或关闭在本终端显示日志信息的功能

决定是否在本终端输出日志信息，只对本终端起作用。

【命令语法】monitor [on|off]

【使用指导】选择 on 表示允许在本终端输出日志信息；
选择 off 表示不允许在本终端输出日志信息。

【命令模式】运行于配置模式。

【配置实例】

Harbour(config)# monitor on

Successfully changed your terminal display syslog messages.

允许日志信息输出到自己的终端。

13.4.3 配置是否显示时间信息

决定是否在本终端输出时间信息。

【命令语法】monitor timestamp [none|time| datetime]

【使用指导】该命令主要用来决定是否在本终端输出时间信息。

【命令模式】运行于配置模式。

【配置实例】

Harbour(config)# monitor timestamp datetime

将在本终端输出时间信息。

13.4.4 配置在终端可以显示的日志信息的最低级别

决定在本终端输出某一级别和高于该级别的日志信息。

【命令语法】monitor lowest-level <0-7>

【使用指导】该命令只对本终端起作用，目前支持的日志信息级别从 0 到 7 ，依次为 EMERG ，ALERT ， CRITERR ， WARNING ， NOTICE ， INFO ， DEBUG 。

【命令模式】运行于配置模式。

【配置实例】

Harbour(config)# monitor lowest-level 3

Successfully changed monitor lowest-lever level 3 [ERR]。

将在本终端输出级别 3 和高于级别 3 类型的日志信息。

13.4.5 配置在终端可以显示的日志信息的类型

决定在本终端输出某一类型的日志信息。

【命令语法】monitor type [<typename>|all] [on|off]

【使用指导】该命令只对本终端起作用，typename 为系统中支持的日志类型，可用 show syslog configuration 来查看日志类型，目前支持的类型有：AUTH ， BGP ， CLI ， SYSLOG ， DEVCTRL ， ARP ， DOT1X ， NAS ， OSPF ，PORT ， FDB ， RADIUS ， RIP ， ROUTE ， SNMP ， STP ， SYSTEM ， VLAN ，WEB ， SERVICE ， DHCPR 等。all 代表以上支持的所有日志类型；

on 代表允许该类型日志信息的输出；

off 代表禁止该类型日志信息的输出。

【命令模式】运行于配置模式。

【配置实例】

Harbour(config)# monitor type all on

Successfully changed to display all messages.

将在本终端输出所有类型的日志信息。

13.5 查看日志模块的配置情况

13.5.1 查看整个日志模块的配置信息

显示日志模块的所有配置信息，包括各种服务的打开和关闭情况等。

【命令语法】show syslog {configuration}*1

【使用指导】可以列出日志模块的所有配置信息，对使用日志模块命令具有一定指导作用。

【命令模式】运行于配置模式。

【配置实例】

Harbour(config)# show syslog configuration

Syslog Service is up.

--Service Syslog logto server is up.

Syslog-server-ip server-port facility

--- --- ---

1.1.1.1 8808 5

--Service Syslog logto monitor-terminal is up.

--Log messages whose level are not lower than level 3 [ERR].

--Log these types messages:

:AUTH

--Not log these types messages:

:CLI:SYSLOG:DEVCTRL:DOT1X:NAS:RADIUS:WEBAUTH:DHCPR:DHCPS:PORT:RIP:ROUTE:SNMP:STP:SYSTEM:VLAN:PORTB:GTDRV:FDB:TIMER:TELNETF:PACKETDEBUG:FFS:PPPOE:PPP:DHCPC:ADSL:IGMPS:L3SWITCH:BOARD:FPGA:LOCALBUS

Record command-line is enabled

13.5.2 查看对本终端的日志显示属性的配置情况

包括所配置的可以在本终端显示的日志类型，日志级别以及时间信息等。

【命令语法】show monitor {configuration}*1

【使用指导】该命令只对本终端起作用。

【命令模式】运行于配置模式。

【配置实例】

```
Harbour(config)# show monitor configuration
-----------------------------------------------------
Monitor has been on.
-----------------------------------------------------
Monitor show messages with datetime timestamp.
Monitor only displays log messages whose level are not lower than level 3
[ERR].
Monitor display messages of these types:
AUTH:
Monitor do NOT display messages of these types:
CLI:SYSLOG:DEVCTRL:DOT1X:NAS:RADIUS:WEBAUTH:DHCPR:DHCPS:PORT:RIP:ROUTE:SN
MP:STP:SYSTEM:VLAN:PORTB:GTDRV:FDB:TIMER:TELNETF:PACKETDEBUG:FFS:PPPOE:PPP:DHCPC:ADSL
:IGMPS:L3SWITCH:BOARD:FPGA:LOCALBUS:
-----------------------------------------------------
```

13.6 日志模块命令列表

日志模块命令列表

命令名称	命令功能描述
config syslog [enable|disable]	起用或禁用日志服务功能。enable 表示起用，disable 表示禁用。
config syslog monitor-terminal[enable|disable]	允许或禁止把日志信息输出到终端。enable 表示允许，disable 表示禁止。
config syslog lowest-level <0-7>	配置所要记录的日志信息的最低级别。表示系统将对等于或高于 lowest-level 的日志类型做日志信息。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，7 ：调试
config syslog type [<name>|all] [enable|disable]	启用或禁用某一个日志类型或所有日志类型的日志功能。name 为该日志类型名字，all 表示代表所有日志类型。enable 表示起用，disable 表示禁用。
record command-line [enable|disable]	是否对命令行操作做日志记录。enable 表示允许，disable 表示禁止。
config syslog server [enable|disable]	允许或禁止把日志信息输出到日志服务器。enable 表示允许，disable 表示禁止。
config syslog [add|delete] server <A.B.C.D> {[port] <1-65535>}*1 {[facility] <0-7>}*1	配置或删除一个日志服务器。<A.B.C.D>为 IP 地址，port 为端口，facility 为优先级别。
show syslog {configuration}*1	显示日志模块所有配置信息
monitor [on|off]	开始显示或结束日志信息输出到本终端。
monitor timestamp [none|time|datetime]	允许在本终端输出时间信息。
monitor lowest-level <0-7>	设置本终端所要输出的日志信息的级别。该命令执行后，在本终端只显示等于或高于该级别的日志信息。
monitor type [<typename>|all][on|off]	设置哪些日志类型的的日志信息可以输出到本终端。
show monitor {configuration}*1	显示对日志信息输出到本终端的配置信息。

第14章 Bootrom 启动和软件升级

本章包括如下内容：

- Bootrom启动选项介绍
- 升级HammerOS软件
- 重新启动交换机

14.1 Bootrom 启动选项介绍

Bootrom 启动分成两种方式：

- 自动启动
- 人工干预启动

14.1.1 自启动

在默认方式下，Hammer10000 IP-DSLAM 接入交换机在上电之后，用户不需要干预，交换机直接启动并进入 HammerOS 操作系统。以下是设备启动时显示的启动信息：

Hammer10000V2 Boot Loader Version 2.02

Compiled: Mar 26 2003 20:07:01

Copyright(c) 2000-2003 by Harbour Networks, Inc.

Uncompress start...

Uncompress success, enter device initialize, Please wait...

Load FPGA program ... ... Done.

Entering HammerOS .....izing environment .....

Loading startup config ..... done.

```
################################################################
#                                                              #
#                    Welcome to HammerOS.                      #
#                                                              #
#            Press Return to connect and config this system.   #
#                                                              #
```

```
################################################################
```

然后按回车键进行用户登录，系统提示用户输入登录名和密码。

14.1.2 人工干预启动

按照以下步骤可以访问 Bootrom 菜单：

1. 连接 Hammer10000 IP-DSLAM 接入交换机的 Console 端口，注意终端的正确配置。
2. 给设备加电，并且不停的按空格键。
3. 当出现“ Hammer: ”提示符，说明已经进入 Bootrom 菜单。人工干预启动后显示 Bootrom 菜单信息：

```
Hammer10000V2 Boot Loader Version 2.02
Compiled: Mar 26 2003 20:07:01
Base ethernet MAC address: 00:05:3b:00:04:99
Copyright(c) 2000-2003 by Harbour Networks, Inc.
 ?               - List all available commands
 h               - List all available commands
 g               - Boot an executable image
 dl              - Enter download mode to load new image or config file
 r               - Reboot system
Press 'h' or '?' To get helping information.
Hammer:
```

Bootrom 菜单选项及其含义如下：

- ?：显示所有的命令信息
- h：显示所有的命令信息
- g：直接执行HammerOS
- r：重新启动交换机

 **注意：**

HammerOS 的软件升级既可以通过 Xmodem 方式，也可以通过 FTP 的方式下载新的主机程序，并保存到 Flash 中。

14.2 升级 HammerOS 软件

HammerOS 提供了两种升级软件的方式：

- 通过Xmodem方式下载HammerOS
- 通过FTP方式下载HammerOS

14.2.1 通过 Xmodem 方式下载新版 HammerOS

可以按以下步骤通过 Xmodem 下载 HammerOS：

1. 用有管理员权限的用户名登录并进入配置模式。
2. 更改 Hammer10000 IP-DSLAM 接入交换机串口（Console 口）的波特率为 115200bps。

   系统启动后 Console 口默认的波特率为 9600bps，通过 Xmodem 方式下载新版 HammerOS 须先配置串口的波特率为 115200，运行命令：

【命令语法】`config terminal Baudrate [115200|9600]`

把系统 Console 口的波特率设定为 115200bps。

3. 输入命令

【命令语法】`download xmodem [hammeros|config-file|cops3000|odiag3000|ooam3000|adufpga|vdubfpga|bootrom|gtiooct]`

【使用指导】参数`[hammeros|config-file|cops3000|odiag3000|ooam3000|adufpga|vdubfpga|bootrom|gtiooct]`用以指明需要下载的内容，具体描述如表 14-1 所示：

表 14-1： 参数说明

参数	说明
hammeros	下载 HammerOS 操作系统
config-file	下载配置文件
cops3000	下载 cops3000 套片驱动
odiag300	下载 odiag3000 套片驱动
ooam3000	下载 ooam3000 套片驱动
adufpga|vdubfpga	下载 ADU、VDU 的 FPGA 代码
bootrom	下载 Bootrom 第二部分的代码。Hammer10000 IP-DSLAM 接入交换机的 Bootrom 包含两个部分，其中第二部分可通过下载方式获得。不下载这部分代码并不影响系统的启动，因此在用户不了解 Hammer10000 Bootrom 结构的情况下，建议不要下载此部分，以免导致灾难性后果。
gtiooct	下载 Globespan ADSL 套片代码

4. 打开超级终端菜单栏中的[传送]—[发送文件]，在其中的[文件名]框中选择要下载的文件，在[协议]框中选择 Xmodem，，然后选择[发送]，系统便开始下载文件。

5. 下载完毕，输入 reboot 命令重新启动交换机。

14.2.2 通过 FTP 方式下载新版 HammerOS

可以按以下步骤通过 FTP 下载新版的 HammerOS：

1．用有管理员权限的用户名登录并进入配置模式。

2．创建 VLAN，并配置 IP 地址。

3．输入命令：

【命令语法】download ftp [hammeros |config-file |cops3000 |odiag3000 |ooam3000 |fpga |bootrom |gtiooct|file] <A.B.C.D> <username> <password> <filename>

【使用指导】其中有关参数[hammeros|config-file|cops3000|odiag3000|ooam3000|fpga|bootrom|gtiooct]的说明请参见表 14-1。参数 file 表示下载一个文件到 Flash. <A.B.C.D>为存放 HammerOS 文件的计算机的 IP 地址,<username>是 FTP 的用户名，<password>为该用户的密码，<filename>为所要下载的文件名。

4．执行上述命令，等待系统完成 FTP 下载并将下载的文件写入 Flash 中。

5．完成后，输入 reboot 命令重新启动交换机，系统将显示：

```
Ip_Dslam is going to reboot
Disconnected.
Thanks for using Harbour Networks's product.
Bye!
```

14.2.3 通过 Xmodem 方式下载新版 HammerOS (for VDU)

可以按以下步骤通过 Xmodem 方式下载 HammerOS：

1．用有管理员权限的用户名登录并进入配置模式。

2．输入命令：

【命令语法】download xmodem vduos [all|<2-15>]

【使用指导】其中 all 表示把 HammerOS (for VDU)下载到所有 VDU 板上，<2-15>表示下载 HammerOS (for VDU)到特定槽位上的 VDU 板。

3．打开超级终端菜单栏中的[传送]—[发送文件]，在其中的[文件名]框中选择要下载的文件，在[协议]框中选择 Xmodem，，然后选择[发送]，系统便开始下载文件。

4．下载完毕后，输入 reboot 命令重新启动交换机。

14.2.4 通过 FTP 方式下载新版 HammerOS (for VDU)

可以按以下步骤通过 FTP 方式下载新版的 HammerOS：

1．用有管理员权限的用户名登录并进入配置模式；

2．创建 VLAN，并配置 IP 地址；

3．输入命令：

【命令语法】download ftp vduos [all|<2-15>] <A.B.C.D> <username> <password> <filename>

【使用指导】其中，all 表示把 HammerOS (for VDU)下载到所有 VDU 板上，<2-15>表示下载 HammerOS (for VDU)到特定槽位上的 VDU 板，<A.B.C.D>为存放 HammerOS 文件的计算机的 IP 地址，<username>是 FTP 的用户名，<password>为该用户的密码，<filename>为所要下载的文件名。

4．等待系统完成下载和写入 Flash；

5．完毕后，输入 reboot 命令重新启动交换机，系统将显示：

```
Ip_Dslam is going to reboot
Disconnected..............
Thanks for using Harbour Networks's product.
Bye!
```

14.3 重新启动交换机

当您需要重新启动交换机时，可以使用 reboot 命令。

使用此命令重新启动交换机之前，请考虑是否需要保存配置数据。如果需要保存配置数据，请键入：

```
Harbour(config)# save configuration
```

该命令完成保存配置数据的操作。

Reboot 命令格式如下：

```
Reboot {<2-15>|smu}*1
```

1．如果 reboot 后面不带参数，则表示对整个系统重新启动，系统显示：

```
Ip_Dslam is going to reboot
Disconnected..............
Thanks for using Harbour Networks's product.
Bye!
```

2．参数 smu 表示只对主控板复位，系统显示：

```
System is going to reboot
Disconnected..............
Thanks for using Harbour Networks's product.
Bye!
```

提示：

对主控板的复位等同于复位整个 Hammer10000 IP-DSLAM 接入交换机。

3．槽位号则表示只对某个业务板复位。

提示：

业务板不在位时执行该操作失败，提示 No board。

最后，感谢您对港湾网络产品的支持和信赖，如果您有好的意见和建议，请给我们发邮件 customer@harbournetworks.com，或登录我们的网站 www.harbournetworks.com 与我们联系，我们将认真对待您们的意见和建议。