μHammer2E / 2ED / 24E / 24ED / 2024E

软件配置手册

港湾网络

μHammer2E/2ED/24E/24ED/2024E 软件配置手册

资料编号	P-18080010-20041213-CN1041V
产品版本	V01R04B01D22
资料状态	发行

手册使用说明

读者对象

本手册主要是针对有一定网络知识的用户，以及负责组建网络设备并熟悉交换机配置的系统管理员。如果读者熟悉以下知识，对学习本手册将有很大帮助：

- 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）
- IP 多播概念（IP Multicast Concepts）
- 简单网络管理协议概念（Simple Network Management Protocol，SNMP）
- 因特网组播管理协议监听（Internet Group Management Protocol Snooping，IGMP Snooping）
- H.Link 协议
- 802.1x 认证服务

H.Link 协议是港湾网络有限公司的私有协议。

内容介绍

本手册主要针对 HammerOS 操作系统而设计，该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、IP-DSLAM 等系列交换机上。

本手册详细讲解μHammer2E/2ED/24E/24ED/2024E 交换机的功能特性和配置操作，并对所涉及的配置命令给予详尽的解释。此外，还就 HammerOS 操作系统的一些缺省配置环境加以说明。

《μHammer2E/2ED/24E/24ED/2024E 软件配置手册》共分为三个部分：

第一部分 HammerOS 概述

主要介绍 HammerOS 操作系统，具体包括以下内容：

章序号	题目	内容描述
第1章	HammerOS概述	介绍HammerOS的特性以及相关技术。

第二部分 软件配置

主要介绍如何进行 μHammer2E/2ED/24E/24ED/2024E 交换机的软件配置，具体包括以下内容：

章序号	题目	内容描述
第2章	访问交换机	介绍管理Hammer系列交换机的相关内容；
第3章	配置端口	介绍如何使用HammerOS配置交换机的端口；
第4章	配置VLAN	介绍VLAN的相关内容以及如何配置VLAN的各项属性；
第5章	配置H.Link	介绍如何配置H.Link协议；
第6章	配置FDB表	介绍FDB地址表的相关内容以及如何配置静态FDB地址表；
第7章	配置MacLimit	介绍MacLimit内容和相关知识，以及如何配置MacLimit的功能。
第8章	配置多域STP	介绍多域STP协议的相关内容以及如何配置多域STP协议；
第9章	配置RSTP	介绍RSTP协议的相关内容以及如何配置RSTP协议；
第10章	配置IGMP Snooping	介绍IGMP Snooping的相关内容以及如何配置IGMP Snooping；
第11章	配置日志模块	介绍日志模块的相关内容以及如何配置日志模块；
第12章	配置NMS	介绍NMS协议的相关内容以及如何配置NMS协议；
第13章	配置SNTP	介绍SNTP协议的相关内容以及如何配置SNTP协议；
第14章	配置LLDP	介绍LLDP协议的相关内容以及如何配置LLDP协议；
第15章	利用Web管理交换机	介绍利用Web管理交换机的相关配置，包括登录、配置端口、配置VLAN、配置FDB地址表、配置STP、配置多端口负载均衡组、设置用户访问权限以及如何查看相关的系统信息。

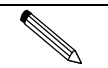
第三部分 启动选项和软件升级

主要介绍如何配置μHammer2E/2ED/24E/24ED/2024E交换机启动选项和进行软件升级，具体包括以下内容：

章序号	题目	内容描述
第16章	启动选项和软件升级	介绍启动选项和如何进行HammerOS软件升级。

手册约定

手册中有关图标的约定如下：

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

获取技术支援

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

目录

第一部分

HammerOS 概述

1 HammerOS 概述

本章主要介绍 HammerOS 的特性并解释相关的技术。

HammerOS 是港湾网络有限公司为 Hammer 系列交换机设计的操作系统，它运行在 μHammer、FlexHammer、BigHammer 系列交换机上。

1.1 特性概述

- 支持 IEEE 802.1Q 和 IEEE 802.1P 标准的 VLAN（Virtual Local Area Networks）；
- 支持 IEEE802.1D 标准的 STP（Spanning Tree Protocol）和 IEEE802.1w 标准的 RSTP（Rapid Spanning Tree Protocol）协议；
- 支持端口捆绑（Load Sharing）；
- 线速（Wire-speed）二层交换；
- 支持 IGMP Snooping（Internet Group Management Protocol Snooping）网络组管理协议监听；
- 支持 Console 命令行配置；
- 支持 Telnet 命令行配置；
- 支持 SNMP（Simple Network Management Protocol）；
- 支持 Web 方式配置；
- 支持 HammerView；
- 支持 H.Link 协议；
- 支持端口镜像；
- 支持 ARP 管理；
- 支持 VCN（端口隔离）；
- 支持安全端口、MAC 地址绑定；
- 支持内部和外部自环功能；
- 支持服务质量（QoS）；
- 提供日志功能（syslog）；
- 支持 NMS 访问控制；

- 支持 SNTP（Simple Network Time Protocol）；
- 支持 802.1x 认证服务。

1.2 VLAN

HammerOS 的 VLAN（Virtual LAN）功能使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：

- 可以控制广播数据，限制其广播的范围。假设在 VLAN 中，“研发部”VLAN（名为“研发部”的 VLAN）中的一个设备发出了一个广播报文，那么只有“研发部”这个 VLAN 中的设备才能收到该广播报文。其他部门将不会收到该广播报文。
- 提供了额外的安全特性。跨 VLAN 的访问不能直接进行，只能通过三层转发才能实现。例如，“市场部”VLAN 的设备只能通过路由协议同“研发部”VLAN 中的设备进行通讯。
- 简化了设备在网络中的移动和管理。


提示

有关 VLAN 的详细配置信息，请参见“第 4 章 配置 VLAN”。

1.3 STP

Hammer 交换机支持 IEEE802.1D 标准的 STP（Spanning Tree Protocol）协议，这一协议提供了网络的动态冗余切换机制。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。 使用 STP 可以让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。

由此可见，使用 STP 可以保证网络结构上存在冗余路径时，阻止网络回路发生。

网络回路对网络来说是致命的打击，但冗余链路作为网络备份路径又是非常重要的。

STP 实现上述功能时，要求对每个 VLAN 都设有一个“Root Switch”，保证每个 VLAN 中的各个交换机并不位于同等地位的环上，而是位于具有不同优先级的树结构之上。

RSTP（Rapid Spanning Tree Protocol）协议是依据 IEEE802.1w 标准，对 STP 802.1D 协议进行改进后的协议，它提供了网络的动态冗余切换机制，并在 P2P（非共享）链路上，能够进行端口状态的快速切换。

RSTP 协议使得网络设计中可以部署备份线路，并保证在主线路正常工作时，备份线路关闭；而在主线路出现故障时，能自动快速地使能备份线路，切换数据流。


提示

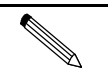
有关多域 STP、RSTP 的详细配置信息，请参见“第 8 章 配置多域 STP”、“第 9 章 配置 RSTP”。

1.4 Load Sharing

Trunk/Load Sharing 技术是一种将网络流量聚集在一组端口上的方法，它可以形成一个交换机之间的大容量通道或容错通道，通道之间可以实现流量均衡。

HammerOS 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。其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；
- 如果这个坏掉的端口重新恢复正常，那么数据包将重新分配到该 Load Sharing 中的所有端口进行传输。


提示

HammerOS 的 Load Sharing 功能与 Intel 和 Cisco 同类产品的 Port Group 功能兼容。

有关端口 Load Sharing 的详细配置信息，请参见“3.1.14 配置多端口负载均衡组”。

1.5 IGMP Snooping

IGMP Snooping（Internet Group Management Protocol Snooping）网络组管理协议监听是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之间的 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，请参见“第 10 章 配置 IGMP Snooping”。

1.6 QoS

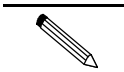
QoS（Quality of Service）是指 IP 的服务质量，是指 IP 数据流通过网络时的性能。它的目的就是向用户的业务提供端到端的服务质量保证，QoS 还带来了更高效的带宽使用率等。μHammer2E/2ED/24E/24ED/2024E 交换机目前已经实现了 802.1P 的端口优先级调度。


提示

有关 QoS 的详细信息，请参见“第 3 章 配置端口”。

1.7 日志模块

日志模块（Syslog）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。


提示

有关日志模块的详细内容，请参见“第 11 章 配置日志模块”。

1.8 NMS

从安全的角度出发，在原有的访问控制基础上增加了新的控制，通过检查来访者的 IP 来确定来访者是否有访问权限。只有通过合法的 IP 访问才可以建立连接，连接之后进一步检查用户名和密码，都通过以后才可以访问和配置交换机。

有关网络管理服务 NMS 的详细内容，请参见“第 12 章 配置 NMS”。

1.9 SNTP

简单网络时间协议 SNTP（Simple Network Time Protocol）是网络时间协议 NTP 的一个简化版本，用于同步因特网上的设备时钟。它与 NTP 的功能相同，只是比 NTP 更加简单。SNTP 可以在单播模式（点对点）和广播模式（点对多点）下操作，采用客户端/服务器的运行方式。在网络设备中运行 SNTP 协议有利于设备的管理和维护。

有关简单网络时间协议 SNTP 的详细内容，请参见“第 13 章 配置 SNTP”。

1.10 802.1x认证服务

港湾网络有限公司 Hammer 系列交换机支持 802.1x 认证服务器。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。

有关 802.1x 认证服务的详细讲解，请参阅港湾网络有限公司的《NAS 接入服务用户手册》。

1.11 远程集群管理

H.Link 协议是港湾网络有限公司的专有通讯协议，用以实现对远程设备的本地管理。用作 H.Link 服务器端的 μHammer2E/2ED/24E/24ED/2024E 交换机可以同时管理多达 36 个互连的 μHammer1008/μHammer1016/μHammer1024 以及支持 802.1Q VLAN 的 μHammer1008Q/1008QL/1008QR/1016Q/1024Q 系列交换机，互连级数最多为 4 级，其工作原理是服务器端使用 H.Link 协议将多个远程客户端设备映射为本地虚拟子设备，通过虚拟子设备配置远程子设备，由此实现远程设备的本地化、集中化管理。此外，该协议还具有简单、可扩展、平台无关等特点。


提示

有关 H.Link 协议的详细讲解，请参阅港湾网络有限公司的《H.Link 用户配置手册》。

第二部分

软件配置

2 访问交换机

本章主要介绍管理 μHammer2E/2ED/24E/24ED/2024E 交换机的相关内容。

2.1 理解命令语法

本节主要介绍进入命令行进行配置时所要进行的步骤。请按照以下步骤，使用命令行接口（CLI）。

配置步骤

步骤1	当进入命令行接口出现命令提示符后，登录HammerOS。
	在本交换机操作系统中，共有两个不同的权限，一为管理员权限，另一为普通用户权限。对于不同的配置命令有不同的用户权限，而且多数配置命令都要求有管理员权限。如果以系统管理员身份登录，在配置模式下出现以下命令提示符：Harbour(config)#
步骤2	键入命令。
	如果键入的命令不含需要用户输入的参数，那么请直接跳到步骤3。 如果键入的命令含有需要用户输入的参数，那么继续以下步骤：如果命令需要输入参数值，请输入参数值。在输入参数值时，可能要输入关键字，关键字是指命令中要操作的对象。命令的参数值部分一般指定了输入参数的类型，可以是某范围内的数值，也可以是字符串或者IP地址。 如果命令需要多个参数值，请按命令的提示依次输入关键字和每个参数值，直到提示信息中出现“<cr>”信息为止。
步骤3	输入完整的命令后，请按回车键。
	以下举例说明。 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，当键入此命令后，按回车键则执行该命令。 2）用户需要输入参数的情况： Harbour(config)# config port 2,3 speed 10 “config port 2,3 speed 10”是一个含有参数和关键字的命令。其中，命令名称为config，关键字为port 和 speed，参数值为2、3、10。


提示

首次登录请用系统缺省用户帐号。有关配置模式的说明，请参见“2.2.8 常用命令”中相应部分的内容。

2.2 语法帮助

命令行接口中内置有语法帮助。如果对某个命令的语法不太确定，请输入已知的该命令中前面的部分，然后键入“?”或“ ?”（空格加?）。命令行会提示该命令剩余部分的可能的命令清单。可以根据提示的内容继续输入命令，直至提示命令出现以下内容为止： <cr> Just Press Enter to Execute command!

此时表明命令输入完毕，按回车执行所输入的命令。

以下举例说明。

配置步骤

步骤1	输入命令。
	who
步骤2	如果接着输入“?”。
	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“ ?”，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。

2.2.1 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。

以下以 μHammer24E 交换机为例说明。

配置步骤

步骤1	输入命令。
	show
步骤2	再输入一空格键，然后按“Tab”键。

系统会显示如下信息：

access-control	age	arp	broadcast-limit
console	debug	degrade	dot1p
dot1x	fdb	history	idle-timeout
igmp-snooping	ip	isp-domain	lldp
maclimit	mirroring	monitor	nas
nms-access-profile	port	radius	running-config
services	sharing	snmp	sntp-client
sntp-server	spanning-tree	startup-config	stpd
syscontact	syslocation	syslog	sysname
tech-support	time	vcn	version
virtual	vlan	vlanmode	webbrowser

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

2.2.2 命令简写

命令简写是指可以只输入命令单词或关键字的前面部分字母，只要输入的字母不会造成歧义，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（例子中为 market）等，要求完整输入。

例如，将端口 1-5 以 untagged 的方式加入到 market 虚拟局域网中，命令如下：

```
config vlan market add port 1-5 untagged
```

上述命令也可简写为如下形式，这两条命令的功能相同：

```
con vl market ad po 1-5 un
```


注意

当使用命令简写时，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。

2.2.3 端口表示

对于 µHammer2E/2ED/24E/24ED/2024E 交换机，端口参数<portlist>可以有以下几种表示方法。

表2-1 端口参数表示方法及示例

表示方法	示例	示例说明
表示一个单独的端口	port 3	表示端口3
表示一个连续范围内的端口，用“-”连接	port 1-4	表示端口1、2、3、4

表示多个端口，中间用“,”隔开	port 1-4,5,8	表示端口1、2、3、4、5、8

2.2.4 命令中的符号

命令语法中的各种符号只是说明该如何输入该命令，但不是命令本身的一个部分。表 2-2 对这些符号进行了说明。

表2-2 命令行中的符号

符号	描述
尖括号 < >	尖括号表示命令的该部分必须输入一个参数。 例如：create vlan <name> tag <1-4094> 该命令中必须在<name>那个位置输入一个合法的字符串作为所创建的VLAN的名字。
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，必须选择输入其中一项。 例如：config stpd default [enable|disable] 该命令中，中括号内包含由竖直线分隔的两个可选项，必须输入enable 或者disable。如果中括号中只有一个可选项，则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：show vlan {<name>}*1 表示可以直接输入show vlan，也可以在show vlan后加上已经创建的某个VLAN的名字。也就是说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。

2.2.5 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，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。

n 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加上减号“-”，再加上该连续端口的最大端口号表示。

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

提示

有关端口表示方法的详细信息请参见“2.2.3 端口表示”。

n 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 16 进制数，具体可以在输入命令到该参数部分时，输入问号“？”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。

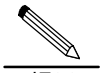
2.2.6 行编辑命令

在命令行中，可以使用的行编辑命令如表 2-3 所示。

表2-3 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

符号	描述
	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 来配置交换机方式，不支持串口配置；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。

2.2.7 历史命令使用

HammerOS 能记住用户最近输入的 20 个历史命令。可以使用 show history 命令来显示已经输入过的命令清单，同时也可以用上下箭头键调用上一个或者下一个历史命令，详细内容见表 2-3 。

例如，在登录之后，输入命令：

```
show history
```

信息显示如下：

```
enable
```

2.2.8 常用命令

本节主要讲述命令行中一些常用的命令，特定功能的命令将在以后的章节专门讲述。


注意

HammerOS 的命令行的所有命令都是不区分大小写的。

如果希望重新启动交换机或交换机关机再开后改变的配置仍然有效，请切记在进行配置后使用 “save configuration” 命令，将配置保存到交换机中。

HammerOS 的命令行提供两种模式，一种是只读模式，另一种是配置模式。在只读模式下用户只能查看一部分系统配置信息，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。

只读模式下的命令提示符是以“>”结尾的，提示符如下：

```
Harbour>
```

只读模式下，输入命令 enable，如下：

```
Harbour>enable
```

按回车，输入密码后进入配置模式。配置模式下的命令提示符是以“#”结尾的，提示符如下：

```
Harbour(config)#
```

退回上一级命令模式，使用命令：

```
exit
```

使用 show version 命令可以显示版本信息。例如，在 μHammer24E 交换机上执行该命令后，显示如下：

```
Harbour> show vers

HammerOS V01R04B01D00 on uHammer24E.

Hardware Version: Version 2.40
Software Version: V01R04B01D00(Compiled Nov 12 2003 10:09:08)
Manufacture Date: 2003-10-15
Serial   Number: 01010163A122022000005
Base Mac Address: 00053b445549

Copyright(c) 2000-2004 by Harbour Networks, Ltd.
```

表 2-4 列出了只读模式下的常用命令。

表2-4 命令行中只读模式下的常用命令

符号	描述
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
list <patten>	根据关键字查找命令
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

符号	描述
show services	显示当前系统提供的服务
show version	显示交换机的软件版本信息
terminal length <0-512>	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	显示本主机用户信息

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表 2-4 中的命令。

表2-5 命令行中配置模式下的常用命令

符号	描述
enable-password	修改进入配置模式的密码
erase startup-config	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 HammerOS
idle-timeout <0-35791>	设置用户可以不进行操作的空闲等待时间，单位是分钟
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	把当前正在运行的配置写到交换机中并保存

2.3 配置用户访问权限

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、删除用户账号，设置修改用户密码，以及进行系统的全局信息的配置。

2.3.1 系统缺省用户账号

系统缺省内置了一个用户账号，用户名是 admin，缺省密码是 harbour。用户是管理员。缺省用户 admin 的账号不能被删除，用户名也不能被修改，只能修改其密码。

2.3.2 增加用户账号

配置步骤

步骤1	以用户名admin登录（或者用其他管理员的用户账号登录）。	
步骤2	enable	进入配置模式。
步骤3	user add <username> login-password <login_password>	创建一个用户账号。 其中，<username>是所要添加用户的名称，用户名必须以字母开头，只包含大写或小写英文字母、数字、下划线及长度为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

系统对于用户名不区分大小写，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账号，可以在按照以上步骤创建完用户账号后，对用户权限进行修改。具体见“2.3.4 修改用户权限”。

2.3.3 删除用户账号

配置步骤

步骤1	user delete <username>	删除一个用户账号。 其中，<username>是用户名。

2.3.4 修改用户权限

由于本系统中有两个不同级别的用户，所以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。

设置管理员用户

配置步骤

步骤1	user role <username> admin enable-password <enable_password>	将一个用户设为管理员。 其中，<username>是用户名，<enable_password>是该用户的登录密码。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。

设置普通用户

配置步骤

步骤1	user role <username> normal	将管理员设为普通用户。 其中，<username>是该管理员的用户名。

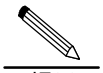
2.3.5 修改密码

管理员除了能够修改自己的登录密码外，还能修改自己进入配置模式的密码。

修改配置模式密码

配置步骤

步骤1	enable-password	修改自己进入配置模式的密码。


提示

在提示符下输入新密码和确认新密码。

修改其他用户密码

配置步骤

步骤1	user login-password <username>	设置其他用户的登录密码。
步骤2	user enable-password <username>	设置其他用户的配置模式的密码。

提示符下输入并确认新密码就可以设置用户的登录密码和配置模式密码。

2.3.6 查看系统用户信息

配置步骤

步骤1	user list	在配置模式下，查看用户列表。 显示如下所示结果： UserName ----------User_role ------ admin ADMIN_USER manager NORMAL_USER Total 2 users in system.

2.4 管理交换机的途径

μHammer 2E/2ED/24E/24ED/2024E 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）连接到交换机的串口（Console），从而通过终端来访问交换机的命令行接口（CLI）；
- 使用 Telnet 管理交换机；
- 使用 SNMP 管理软件管理交换机；
- 使用 Web 浏览器如 Internet Explorer 来管理交换机。

μHammer 2E/2ED/24E/24ED/2024E 交换机能同时支持多个连接：

- 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。

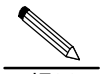
通过 Telnet、Web、SNMP 管理交换机，必须先把这些服务打开。默认情况下，Telnet 服务是打开的。

2.4.1 使用Console口连接到交换机

可以通过在交换机面板前端的标有 Console 字样的 RJ45 串口连接交换机内置的命令行接口。

Console 端口的配置如下：

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



提示

有关串口线针的情况和各个针的含义，请参阅相关的《μHammer2E/2ED 硬件安装手册》、《μHammer24E/24ED 硬件安装手册》或《μHammer2024E 硬件安装手册》。

在使用 Console 口连接交换机时，推荐用户使用 VT100 终端仿真。设置方法：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。

一旦连接成功，在终端中看到操作系统启动的界面后，就可以通过命令行接口对交换机进行配置。

可以通过以下步骤通过 Console 连接登录到交换机，并给交换机配置一个 IP 地址（在本例中 IP 地址为 192.168.0.232）。

配置步骤

步骤1	将交换机的Console口和特定终端连接起来，正常给交换机供电。
步骤2	待HammerOS成功启动后，就可以看到交换机的提示登录信息，按回车键进行登录。
步骤3	此时，系统要求输入用户名和密码。 如果是首次登录交换机，请使用缺省的用户名admin登录，登录密码为harbour。登录后，可以以系统管理员的身份进行操作，并可使用本交换机的所有功能函数。 如果不是首次登录，使用拥有系统管理员权限的帐号登录。
步骤4	成功登录交换机时，系统显示如下信息：Harbour(config)# 表明可以对命令行进行配置操作。
步骤5	给交换机配置IP地址。

	Harbour(config)#config ipaddress 192.168.0.232/24 其中，192.168.0.232/24 是要设置的IP地址和子网掩码。 成功执行该命令后，就可以从交换机的端口上以该IP地址telnet登录到交换机的命令行接口。
步骤6	保存配置。
	Harbour(config)#save configuration 按回车，当出现如下提示信息时： 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，并且所做的配置立即生效。
步骤7	当完成对交换机的操作后，断开与交换机的连接，并退出命令行界面。
	logout exit

2.4.2 使用Telnet连接到交换机

任何一个有 Telnet 功能的工作站都能通过 TCP/IP 网络连接到交换机，从而实现对交换机的配置管理。如果使用 Telnet 登录交换机，首先这个交换机应该有一个 IP 地址。

配置步骤

步骤1	telnet <A.B.C.D>	使用Telnet连接到IP地址为A.B.C.D的交换机。 例如，某台μHammer24E交换机的IP地址为192.168.0.232。 telnet 192.168.0.232 按回车，连接成功后，输入用户名和密码进行登录。

2.4.3 Console与Telnet远程（RADIUS）认证

Console 与 Telnet 远程（RADIUS）认证的目的是将设备管理的帐号、密码进行统一、集中管理，从而降低管理难度。

Console 与 Telnet 远程（RADIUS）认证具有以下功能：

- 超级用户帐号（admin）只能在本地认证，无论是否配置了需要远程认证；
- 远程认证只支持 PAP 认证；

- 在 RADIUS 服务器上创建帐号时，需指定用户是管理员还是普通用户。管理员可进入设备的 config 模式，而普通用户只能进入 view 模式。并且 RADIUS 服务器应能够将用户的级别信息通过 RADIUS 标准属性 6（service-type）返回。service-type 等于 6（Administrative）表示管理员帐号，service-type 等于 7（NAS Prompt）表示普通帐号，如果该 RADIUS 服务器不返回此信息，交换机默认为管理员账号；
- 管理员帐号（非 admin）通过远程 RADIUS 认证后，输入 enable，不需要输入密码就可以直接进入 config 模式；非管理员帐号通过远程 RADIUS 认证后，输入 enable，会被提示无权进入 config 模式，而只能访问 view 模式；
- 配合港湾 RADIUS 服务器，可以对访问交换机的用户实现更完善的管理，包括记录、查询、管理交换机的历史操作以及查询、切断在线的访问用户。

表2-6 Console 与 Telnet 远程（RADIUS）认证缺省配置信息

内容	缺省设置	备注
配置使用本地还是远程RADIUS认证	local	可更改设置
配置使用远程RADIUS认证及计费时的超时时间	16秒	可更改设置

配置步骤

步骤1	config login-auth [local|radius]	配置模式下，配置使用本地还是远程RADIUS认证。
步骤2	config login-radius time <1-600>	配置模式下，配置使用远程RADIUS认证及计费时的超时时间。
步骤3	config login-radius domain <domain>	配置模式下，配置使用哪个域的RADIUS服务器完成远程RADIUS认证。 其中，domain为已创建的某个域。


提示

由于该认证只支持 PAP 认证方式，而默认的域 default 使用的是 EAP-MD5 认证方式，且通常的 802.1x 接入服务会使用默认的域 default。因此，建议为 Console 与 Telnet 远程认证单独创建一个域，并指定 Console 与 Telnet 远程认证通过该域的服务器进行，当然这个域也可以使用与 default 域相同的服务器。详细的域设置及 RADIUS 服务器的添加，请参考《NAS 接入服务用户手册》。服务端的管理请参考相关的 RADIUS 手册。

2.4.4 使能/关闭Telnet服务

配置步骤

步骤1	service telnet [enable|disable]	配置模式下，启用或关闭Telnet服务。
步骤2	show services	查看系统提供的Telnet服务是否被打开。 如果显示“Service telnet is up.”，表明Telnet已经打开； 如果显示“Service telnet is down.”，表明Telnet已经关闭。 例如，下例表示已经打开Telnet服务： Harbour> show services Service telnet is up. Service snmp agent is down. Service snmp rmon is down. Service snmp trap support is down. Service Web manage is up.


提示

以上命令可以启用或关闭 Telnet 服务，但必须是以系统管理员的身份登录。

2.4.5 强制关闭非法Telnet连接

具有管理员权限的用户可以强制断开一个 Telnet 连接。

配置步骤

步骤1	who	查看当前连接的用户。
步骤2	kill session <1-24>	强制断开非法连接。 其中，<1-24>是用who命令所看到的该连接的sessionid的取值范围。 如果输入的session是console口连接的，将出现以下提示信息： You can't kill a console session.


提示

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。

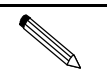
2.4.6 配置SNMP

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利用 SNMP 来管理交换机，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。

SNMP 服务配置

配置步骤

步骤1	service snmp [enable| disable]	启用/关闭SNMP服务。
步骤2	service snmp trap [hlink|spanning-tree] [on|off]	配置模式下，允许/禁止部分模块的SNMP trap功能。 其中，选择hlink，表示对H.Link模块的代理发送trap功能进行控制；选择spanning-tree，表示对STP和RSTP模块的代理发送trap功能进行控制；选择on，表示允许代理发送trap报文功能，但如果没有命令service snmp trap enable，该模块的代理发送trap报文功能仍然属于关闭状态；选择off，表示禁止代理发送trap报文功能。
步骤3	show services	显示系统提供的SNMP服务的状态。 如果显示“Service snmp agent is up.”，表明SNMP服务已经打开；如果显示“Service snmp agent is down.”，表明SNMP服务已经关闭。
步骤4	show snmp trap status	配置模式下，显示HLINK模块和生成树模块的代理发送trap报文功能的状态。


提示

H.Link 模块的 trap 内容包括：端口的使能、禁止、link-up、link-down、设备的登录、退出、冷启动、热启动、同步成功、同步失败;

spanning-tree 模块的 trap 内容包括：根桥的改变、拓扑的改变。

SNMP 参数配置

配置 SNMP 时，主要有以下参数：

- Community 字符串：交换机提供了一个远程网络管理员配置交换机的用户确认机制。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。

- System contact：用于存放负责管理交换机的人名及联系方式。
- System name：交换机指定的名称，例如，uHammer24E 就可以作为 System name 的名称。
- System location：交换机所在的位置，该参数由用户设置。

2.4.7 使用Web浏览器管理交换机

HammerOS 是一个运行在交换机上的、可对设备进行管理的操作系统。任何一个有 Web 浏览功能的工作站都能通过 TCP/IP 网络连接到交换机，并通过 Web 来实现对交换机的管理。

配置步骤

步骤1	给交换机配置一个IP地址（与Telnet一样）；
步骤2	将交换机的Web功能打开；
步骤3	通过网线将工作站与交换机的一个端口连接起来；
步骤4	打开Web浏览器（如Internet Explorer），在地址栏中输入所配置的IP地址值；
步骤5	在出现的登录界面中，输入用户名和密码，进入配置页面。


提示

有关 Web 浏览器管理交换机的详细内容见“第 15 章 利用 Web 管理交换机”。

2.4.8 使能/关闭Web服务

配置步骤

步骤1	service webserver [enable|disable]	启用/关闭Web服务。
步骤2	show services	查看系统提供的Web服务的状态。 如果显示“Service Web manage is up.”，表明Web服务已经打开；如果显示“Service Web manage is down.”，表明Web服务已经关闭。

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交换机的静态路由信息。

配置步骤

步骤1	ip route <A.B.C.D/M> <A.B.C.D> {<host_mac_addr>}*1	增加一条静态路由。 其中，<A.B.C.D/M>为目的网段的IP地址和子网掩码长度；<A.B.C.D>为下一跳的IP地址，即网关的IP地址；<host_mac_addr>是可选参数，指在配置主机路由时同时添加主机的arp静态表项。
	ip route <A.B.C.D> <A.B.C.D> <A.B.C.D>	增加一条静态路由。 该命令中将上一条命令的子网掩码长度改成了IP形式。
步骤2	show ip route	显示静态路由信息。

使用 no ip route <A.B.C.D/M> <A.B.C.D>和 no ip route <A.B.C.D> <A.B.C.D> <A.B.C.D>可以删除一条静态路由。

2.6 配置交换机IP地址

配置步骤

步骤1	config ipaddress <A.B.C.D/M>	配置IP地址。 其中，<A.B.C.D>为交换机的IP地址，M为使用长度表示的子网掩码。
	config ipaddress <A.B.C.D> <A.B.C.D>	配置IP地址。 其中，第一个<A.B.C.D>为交换机的IP地址，第二个<A.B.C.D>为使用16进制表示的子网掩码。

2.7 ARP管理

地址转换协议 ARP（Address Resolution Protocol）提供了主机的 MAC 地址与 IP 地址的映射。交换机会自动学习这种映射并维护映射表。如果对某些特定的主机，不希望交换机通过自学习的方式获得它们的地址映射，因为在一个庞大的网络中这种学习可能需要占用一定的时间，同时也有学习不到的危险，也可以通过手工的方式为这些主机建立静态的地址映射表项。

2.7.1 创建永久地址映射表项

配置步骤

步骤1	config arp add <A.B.C.D> <mac_address>	配置模式下，创建永久地址映射表项。 其中，<A.B.C.D>为所连接的某个指定主机的IP地址；<mac_address>为所连接主机的物理MAC地址。当创建了永久地址映射表项后，如果要使其在交换机重启后仍然有效，需要执行save configuration命令进行保存。

2.7.2 删除地址映射表项

配置步骤

步骤1	config arp delete [<A.B.C.D>|all]	配置模式下，删除地址映射表项。 其中，<A.B.C.D>为所连接的某个指定主机的IP地址，选择这个参数表示要删除该主机的地址映射表项，选择all表示删除所有连接的主机的地址映射表项。如果要删除永久地址映射表项，需要在完成操作后执行save configuration命令进行保存，否则当重新启动交换机时该永久地址映射表项仍会出现。

2.7.3 显示地址映射表项

配置步骤

步骤1	show arp {[<A.B.C.D>|permanent]}*1	只读模式和配置模式下，显示地址映射表项。 其中，选择<A.B.C.D>表示显示该IP地址所对应主机的地址映射表项；选择permanent表示显示所有的永久地址映射表项；不输入任何参数，表示显示所有映射地址表项（包括动态和永久映射地址表项）。

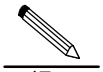
2.8 存取配置文件

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。

配置步骤

步骤1	save configuration	将修改后的配置保存到交换机的扩展FLASH中。

用户还可以把配置文件通过上传保存到主机文件中，在需要的时候（例如不小心把交换机配置搞乱，需要把配置恢复到以前的状态）再把配置文件下载到交换机中。上传/下载的方法有三种：通过 FTP、通过 TFTP、通过 xmodem。


提示

在使用 FTP 时，请在对应的主机上启动 FTP 服务器，设置好目录、用户名称、密码。关于 FTP 服务器的设置，请参考 windows/unix 的有关帮助，或利用其它共享软件。

2.8.1 通过FTP上传/下载配置文件

通过 FTP 上传配置文件

配置步骤

步骤1	进入配置模式。
步骤2	通过FTP上传配置文件。
	upload ftp config-file <A.B.C.D> <username> <password> <filename> 其中，<A.B.C.D>表示文件上传至IP地址为<A.B.C.D>的主机；<username>表示ftp用户名；<password>表示FTP用户名的密码；<filename>表示文件被保存时使用的名称。

通过 FTP 下载配置文件

配置步骤

步骤1	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。
步骤2	通过FTP下载配置文件。
	download ftp config-file <A.B.C.D> <username> <password> <filename> 其中，<A.B.C.D>表示文件所在主机的IP地址；<username>表示FTP用户名；<password>表示FTP用户名的密码；<filename>表示被下载的文件名。

2.8.2 通过TFTP协议上传/下载配置文件

小文件传输协议 TFTP（Trivial File Transfer Protocol）是网络应用程序，比 FTP 简单，且比 FTP 功能少。它使用 UDP 协议而不是 TCP 协议，在不需要用户权限或目录可见的情况下使用。在 RFC 1350 内有对 TFTP 的详细说明。

通过 TFTP 上传配置文件

配置步骤

步骤1	进入配置模式。
步骤2	将配置文件上传至地址为<A.B.C.D>的主机，并保存成名为<filename>的文件。
	upload tftp config-file <A.B.C.D> <filename>
步骤3	按回车执行命令，并等待直至上传完毕。 Trying upload file to tftp server. Please wait....Done Successfully finished Upload file. Finished. You've successfully upload config file 这就完成了上传配置文件的操作。

通过 TFTP 下载配置文件

配置步骤

步骤1	进入配置模式。
步骤2	通过TFTP下载配置文件。
	download tftp config-file <A.B.C.D> <filename> 其中，<A.B.C.D>为文件所在主机的IP地址；<filename>为被下载的文件名。
步骤3	等待下载完毕后，输入reboot命令重新启动交换机。

2.8.3 通过xmodem协议上传/下载配置文件

配置步骤

步骤1	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。
步骤2	输入命令上传或下载配置文件。
	download xmodem config-file，通过使用xmodem协议下载配置文件 upload xmodem config-file，通过使用xmodem协议上传配置文件
步骤3	打开串口超级终端的传送菜单，选择要下载或上传的配置文件，选择“发送”或“接收”，系统开始下载或上传指定文件信息。

步骤4	以下载配置文件为例，等待下载完毕后，当显示下面信息时，表明下载成功。 输入reboot 命令重新启动交换机。 Trying to download file from console, please wait... Trying to receive file from console using xmodem protocol..... Successfully finished receiving file. Trying to write file to flash..... Finished. You've successfully downloaded new config file Now you can type reboot command to reboot system.

2.9 检测网络基本连接情况

交换机提供了 ping 命令用来检测网络的基本连接情况。ping 命令发送 Internet Control Message Protocol（ICMP）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。

配置步骤

步骤1	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。

表 2-7 给出了 ping 的各个选项的说明。

表2-7 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_pattern>	pattern选项指定ICMP数据包中用户自定义的1-16个16进制数。

2.10 检测数据报行进路径

交换机提供 traceroute 命令用来检测交换机到目的地之间数据报行进的路径。traceroute 命令发送 Internet Control Message Protocol（ICMP）echo 消息或者 UDP 报文到网络中的某个 IP 设备。只有管理员用户可以使用 traceroute 命令。

配置步骤

步骤1	traceroute {[-a] <A.B.C.D>}*1 {[-f] <1-30>}*1 {[-m] <2-255>}*1 {[-q] <1-10>}*1 {[-w] <1-65535>}*1 <A.B.C.D>	traceroute命令的众多选项可以都不输入，而使用最简单的格式。

如果交换机不能与目的 IP 设备连接通信，通过 traceroute 命令可以获知数据报的传输在路径中哪一个地方出现问题。

输入 Ctrl+C 可以中断 traceroute 命令。

表 2-8 给出了 traceroute 的各个选项的说明。

表2-8 traceroute 命令选项

符号	描述
-a <A.B.C.D>	设定UDP数据报源IP地址，该参数只对udp模式有效。
-f <1-30>	指定数据报的初始ttl（time to live）值，缺省值为1。
-m <2-255>	指定数据报的最大ttl（time to live）值，即指定搜寻目的IP设备的最大跳数，缺省值为30。
-q <1-10>	指定每一跳中的搜索次数，缺省值为3。
-w <1-65535>	指定traceroute程序每一次搜索所等待的时间，单位为秒，缺省值为2。
<A.B.C.D>	目的IP地址。

2.11 配置案例

2.11.1 配置用户访问权限

案例描述

增加一个用户，用户名为 manager，登录密码为 harbour，并将其权限改为系统管理员，其进入配置模式的密码改为 harbour，之后由于需要将其改回为普通用户，后又将其删除。

配置步骤

步骤1	增加一个用户，用户名为manager，登录密码为harbour。
	Harbour(config)#user add manager login-password harbour

	Successfully added user manager as a NORMAL_USER. To change user role use "user role" command.
步骤2	将添加的用户manager的权限改为系统管理员，其进入配置模式的密码为harbour。
	Harbour(config)#user role manager admin enable-password harbour Successfully change user manager to ADMIN mode.
步骤3	将用户manager从系统管理员权限变为普通用户。
	Harbour(config)#user role manager normal Successfully change user manager to NORMAL mode.
步骤4	删除用户manager。
	Harbour(config)#user delete manager

2.11.2 配置SNMP

案例描述

显示 SNMP 的 trap 控制状态。

配置步骤

步骤1	显示SNMP的trap控制状态。
	Harbour(config)# sh snmp trap status Snmp hlink trap: on. Snmp spanning-tree trap: on. Service snmp trap is disabled.

2.11.3 配置静态路由

案例描述

添加一条静态路由，目的地址所在网段为 192.168.1.0，目的地址是 192.168.1.88，下一跳地址为 192.168.0.3，并显示配置的静态路由信息。

配置步骤

步骤1	添加一条静态路由，目的地址所在网段为192.168.1.0，目的地址是192.168.1.88，下一跳地址为192.168.0.3。
	Harbour(config)# ip route 192.168.1.88/24 192.168.0.3
步骤2	查看配置的静态路由信息。

```
Harbour(config)# show ip route

***    begin route table info ***
Destination net-----NetMask-------------Gateway-------------
127.0.0.1              255.255.255.255       127.0.0.1
192.168.1.0            255.255.255.0         192.168.0.3
***    end route table info ***
可见，已经成功加入一条静态路由信息：
192.168.1.0            255.255.255.0         192.168.0.3
```

2.11.4 配置交换机IP地址

案例描述

将 μHammer24E 交换机的 IP 地址配置为 192.168.0.232，子网掩码配置为 255.255.255.0，并查看交换机的 IP 地址。

配置步骤

步骤1	将μHammer24E交换机的IP地址配置为192.168.0.232，子网掩码配置为255.255.255.0。
	Harbour(config)#config ipaddress 192.168.0.232 255.255.255.0 也可以采用以下命令： Harbour(config)#config ipaddress 192.168.0.232/24
步骤2	查看交换机的IP地址。
	Harbour(config)#show ip Switch ip address information: ---------- Switch ip address : 192.168.0.232 Switch netmask : 255.255.255.0 ----------

2.11.5 ARP管理

案例描述

为某个主机创建一条永久地址映射表项，该主机的 IP 地址为 10.1.31.41，物理 MAC 地址为 00:50:ba:f2:4b:0a，并显示所有的地址映射表项，然后删除 IP 地址为 10.1.31.41 的主机的地址映射表项。

配置步骤

步骤1	为某个主机创建一条永久地址映射表项，该主机的IP地址为10.1.31.41，物理MAC地址为00:50:ba:f2:4b:0a。
	Harbour(config)# config arp add 10.1.31.41 0050baf24b0a
步骤2	显示所有的地址映射表项。

	Harbour(config)# show arp Arp table information Physics Address Ip Address Type ---------- ---------- ---------- 00:10:5c:b4:49:6f 10.1.30.80 dynamic 00:50:ba:f2:4b:0a 10.1.31.41 permanent ---------- ---------- ---------- Total 2 information
步骤3	删除IP地址为10.1.31.41的主机的地址映射表项。
	Harbour(config)# config arp delete 10.1.31.41

2.11.6 存取配置文件

案例描述

首先保存配置文件，然后通过 FTP 上传配置文件，后又通过 FTP 下载配置文件。

配置步骤

步骤1	保存配置文件。
	Harbour(config)# save configuration Preparing configuration data to save...Done. Starting write configuration data to flash...Done. Configuration save to flash successfully.
步骤2	通过FTP上传配置文件。
	Harbour(config)# upload ftp config-file 10.1.30.48 anonymous guest u24e.cfg Trying to upload file to ftp server, please wait... Successfully finished uploading file. Finished. You've successfully uploaded config file.
步骤3	通过FTP下载配置文件。
	Harbour(config)# download ftp config-file 10.1.30.48 anonymous guest u24e.cfg 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.

2.11.7 检测网络基本连接情况

案例描述

检测与 IP 地址为 192.168.0.1 的设备的连接情况。

配置步骤

步骤1	检测与IP地址为192.168.0.1的设备的连接情况。
	Harbour(config)# ping 192.168.0.1 如果设备连通，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=100 ms Reply from 192.168.0.1 : bytes=56: icmp_seq=1 ttl=128 time=33 ms Reply from 192.168.0.1 : bytes=56: icmp_seq=2 ttl=128 time=16 ms Reply from 192.168.0.1 : bytes=56: icmp_seq=3 ttl=128 time=0 ms Reply from 192.168.0.1 : bytes=56: icmp_seq=4 ttl=128 time=33 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

2.11.8 检测数据报行进路径

案例描述

测试交换机发出的数据报到达 IP 地址为 202.96.13.137 的设备所经过的路径。

配置步骤

步骤1	测试交换机发出的数据报到达IP地址为202.96.13.137的设备所经过的路径。
	harbour(config)# traceroute 202.96.13.137 如果设备连通，出现以下信息： traceroute 202.96.13.137

```
Type Control-C to abort.
Tracing the route to 202.96.13.137

 1    10.7.4.1      < 10 ms   < 10 ms   < 10 ms
 2    10.8.1.1              < 10 ms     16 ms     16 ms
 3    10.4.1.254              16 ms     16 ms   < 10 ms
 4    10.1.0.144              16 ms   < 10 ms     16 ms
 5    218.244.39.98           16 ms     16 ms     16 ms
 6    218.244.36.157          66 ms     50 ms     50 ms
 7    202.96.6.181           266 ms     66 ms     66 ms
 8    202.96.6.81             50 ms     66 ms     66 ms
 9    202.96.13.137           50 ms     66 ms     50 ms
```

如果设备没有连通，则出现以下信息：

```
traceroute 202.96.13.137

Type Control-C to abort.
Tracing the route to 202.96.13.137

 1    10.7.4.1              < 10 ms   < 10 ms   < 10 ms
 2    10.6.1.1              < 10 ms     16 ms     16 ms
 3    10.4.1.254              16 ms     16 ms   < 10 ms
 4    10.1.0.144              16 ms   < 10 ms     16 ms
 5    218.244.39.98           16 ms     16 ms     16 ms
 6    218.244.36.157          66 ms     50 ms     50 ms
 7    * * *
 8    * * *
 9    * * *
10    * * *
```

上述信息表明，交换机发出的数据报在218.244.36.157之前的路径上都能正常传输，但在218.244.36.157的下一跳出了问题。

3 配置端口

本章主要介绍如何配置交换机的端口。

3.1 配置端口

3.1.1 缺省配置信息

μHammer2E/2ED/24E/24ED/2024E 交换机关于端口的缺省设置信息如以下表格所示：

表3-1 端口缺省配置信息

内容	缺省设置	备注
使能/禁用端口	enable	可更改设置
端口自适应模式（auto）	自适应	可更改设置
端口自协商能力（capable）	100M	可更改设置
端口流控（flowcontrol）	off	可更改设置
端口地址学习功能（learning）	enable	可更改设置
端口广播抑制（broadcast-limit）	on	可更改设置
端口广播抑制模式（broadcast-limit mode）	3	可更改设置
端口带宽模式（bandwidth mode）	Normal	可更改设置


注意

μHammer2E/2ED/2024E 交换机不支持千兆模块板，也就是不支持 HC－1SFP、HC－1GTX、HC－1ST 这三种可选配模块。
μHammer24ED 交换机不支持 HC－1ST 这种可选配模块。

3.1.2 使能/禁用端口

配置步骤

步骤1	config port [<portlist>|all] [enable|disable]	使能/禁用一个或多个指定端口。 其中，选择<portlist>，表示所要配置的端口；选择all，表示对所有端口进行操作；

		选择enable，表示启用端口；选择disable，表示禁用端口。

快速以太网端口可以连接 10Base-T 或者 100Base-TX 网络，可以工作在半双工或全双工模式，这就要求用户根据实际情况对其进行配置。

缺省情况下，HammerOS 将交换机的所有端口设置为自适应模式，并根据端口对端的性能自动调整端口的速率和双工模式。用户可以手工配置端口的速率、双工模式和流控模式。

3.1.3 配置端口自适应模式

配置步骤

步骤1	config port [<portlist>|all] auto [on|off]	配置端口自适应模式。 其中，选择all，表示对所有端口进行操作；选择<portlist>，表示对指定的端口进行操作；选择on，将端口配置为自适应模式；选择off，关闭端口的自适应模式。


注意

当关闭自协商后，端口将自动设置为 100M full 模式。

百兆光口和千兆光口默认状态都是自协商关闭、全双工。它们的自协商、双工和速率是不能配置的。

3.1.4 配置端口自协商能力

当开启了端口的自协商功能后，端口可以协商两种速率：10M 和 100M。

配置步骤

步骤1	config port [<portlist>|all] capable [10|100]	将端口协商的速率指定为某一个值。 例如，将某一个端口的自协商速率指定为10M时，那么即使与该端口连接的另一端口的自适应速率能达到100M，也只能以10M的速率运行。


注意

只支持端口 1-24，不支持模块板端口的协商能力修改。

3.1.5 配置端口速率

在自协商关闭以后可以配置端口速率。

配置步骤

步骤1	config port [<portlist>|all] speed {[10|100]}*1 {[1000] [master|slave]}*1	配置端口速率。 其中，选择all，表示对所有端口进行操作；选择<portlist>，表示对指定的端口进行操作；选择10，将端口速率设置为10Mbps；选择100，将端口速率设置为100Mbps；选择1000，将端口速率设置为1000Mbps；master为1000M GTX模块板端口的主模式，slave为其从模式。

3.1.6 配置端口双工模式

在自协商关闭以后可以配置端口双工模式。

配置步骤

步骤1	config port [<portlist>|all] duplex [full|half]	配置端口双工模式。 其中，选择all，表示对所有端口进行操作；选择<portlist>，表示对指定的端口进行操作；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。

3.1.7 配置端口流控

配置步骤

步骤1	config port [<portlist>|all] flowcontrol [on|off]	配置端口流控。 其中，选择all，表示对所有端口进行操作；选择<portlist>，表示对指定的端口进行操作；选择on，设置端口流量控制；选择off，取消端口的流量控制。

3.1.8 配置端口地址学习功能

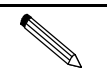
配置步骤

步骤1	config port [<portlist>|all] learning [enable|disable]	配置端口地址学习功能。 其中，选择all，表示对所有端口进行操作；选择<portlist>，表示对指定的端口进行操作；选择enable，启用指定端口的地址自学习功能；选择disable，关闭指定端口的地址自学习功能。

3.1.9 配置端口内部自环和外部自环

配置步骤

步骤1	config port [<portlist>|all] interloopback	配置端口内部自环功能。 其中，选择<portlist>，表示对指定端口进行操作；选择all，表示对所有端口进行操作。
步骤2	config port [<portlist>|all] exterloopback	配置端口外部自环功能。 其中，选择<portlist>，表示对指定端口进行操作；选择all，表示对所有端口进行操作。


提示

端口的自环功能便于对端口的连通性进行检测。

端口的外部自环功能需要使用自环头。

自环操作只能在端口 1-24 使用。

3.1.10 配置端口描述信息

配置步骤

步骤1	config port [<portlist>|all] description <description>	配置端口的描述信息。 其中，选择<portlist>，表示对指定端口进行操作；选择all，表示对所有端口进行操作；<description>表示端口的描述说明文字。

3.1.11 查看端口信息

配置步骤

步骤1	show port [<portlist>|all] {[configuration|stats]}*1	查看端口信息。 其中，选择configuration 或直接回车，表示查看端口的配置信息；选择stats，表示查看端口的统计信息。

3.1.12 清除端口统计信息

配置步骤

步骤1	clear port [<portlist>|all] stats	清除端口的统计信息，使其重新开始计数。 其中，选择<portlist>，表示对指定端口进行操作；选择all，表示对所有端口进行操作。

提示

清除端口统计信息后，端口收发报文的统计数据都被置零。

3.1.13 配置端口镜像

HammerOS 支持端口镜像（Mirror），把指定端口的所有数据报文重定向到镜像端口，以方便诊断错误。

μHammer2E/2ED/24E/24ED/2024E 只支持一个镜像端口。

配置镜像端口

配置步骤

步骤1	config mirroring to <portno>	配置镜像端口。 其中，<portno>表示指定的镜像端口。
步骤2	config mirroring [add|delete] port [<portlist>|all]	配置参与镜像的端口。 其中，选择add，表示向镜像端口添加数据源端口；选择delete，表示从镜像端口删除数据源端口；选择all，表示所有的端口都参与镜像；选择<portlist>，表示指定的端口参与镜像。

取消镜像端口功能

配置步骤

步骤1	config mirroring disable	取消端口镜像功能。


注意

Load Sharing 端口内部不支持互相镜像。
被镜像端口的输入/输出数据都会被镜像到指定端口。

3.1.14 配置多端口负载均衡组

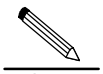
μHammer2E/2ED/24E/24ED/2024E 交换机能够通过创建多端口负载均衡组（Load Sharing）来提升交换机之间的带宽。Load Sharing 把多个物理端口捆绑在一起当作一个逻辑端口来使用。例如，在 VLAN 中所看到的 Load Sharing 是一个逻辑端口。Load Sharing 同时对客户间的数据包顺序提供保障。

如果 Load Sharing 中的一个端口发生堵塞或故障，那么数据包会被分配到该 Load Sharing 中的别的端口中进行传输。如果这个坏掉的端口恢复正常，那么数据包将分配到该 Load Sharing 中的所有端口来进行传输，从而增加交换机之间的带宽。


注意

必须在相互连接的两台交换机上都设置 Load Sharing，否则会在网络中造成回路，导致交换机不能正常工作。

当一台交换机的两个以上端口要同时向相邻的交换机发送数据时，创建 Load Sharing 非常有助于提高传输速率。


提示

港湾网络有限公司的 μHammer2E/2ED/24E/24ED/2024E 系列交换机支持 Load Sharing 功能，同时与 Intel 和 Cisco 的同类产品的 Port Group 功能兼容。

要配置 Load Sharing，必须创建 Load Sharing 的一组端口。

在 μHammer2E/2ED/24E/24ED/2024E 交换机中，创建 Load Sharing 必须遵从以下规则：

- 交换机只支持一个 Load Sharing；

- 1-26 端口支持 Load Sharing；
- 一个 Load Sharing 组中最大端口数目为 4。

定义一个 Load Sharing 组，可以选取其中的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。如果 Load Sharing 组中有 UP 的端口，应该选取 UP 的端口中端口号最小的作为主端口。

创建 Load Sharing 组

配置步骤

步骤1	create sharing <portno> grouping <portlist>	创建一个Load Sharing组。 其中，<portno>代表允许输入的所创建的Load Sharing的主端口号。Load Sharing中的端口根据报文的源MAC和目的MAC地址来进行地址学习。

删除 Load Sharing 组

配置步骤

步骤1	delete sharing <portno>	删除一个Load Sharing组。

在实际组网中，主端口会随实际物理网络连接状态的变化而改变。创建了 Load Sharing 后，在配置 VLAN 或 STP 时，将该 Load Sharing 作为一个逻辑端口使用，使用当前状态下该Load Sharing逻辑上的主端口指定该Load Sharing。进行 VLAN 配置时，对该主端口的操作等同于对该 Load Sharing 组中的所有端口操作，并且将不能再对该 Load Sharing 中的其它非主端口的端口进行操作。对主端口的操作将会同时修改其它从端口。


注意

主端口为 1000M 端口，配置端口的速率为 1000M。如果从端口为 1000M 端口，则配置跟着修改，如果从端口为 100M 端口，则不修改。

3.1.15 配置端口优先级

μHammer2E/2ED/24E/24ED/2024E 交换机端口支持 802.1p 优先级队列，通过优

先级来实现对重要任务的保护。用户可以配置优先级的优先程度，即配置高低优先级数据通过的比例，这个比例称作 weight，表示在有多少个高优先级数据包通过后允许一个低优先级的数据包通过。该功能只有在网络发生拥塞时才有意义，当网络不拥塞时，所有包都可以顺利通过。

配置步骤

步骤1	config dot1p [enable|disable]	启动/停止优先级处理功能。
步骤2	config dot1p weight <0-7>	设置高低优先级数据包通过比例。
步骤3	show dot1p weight	显示高低优先级数据包通过比例。

3.1.16 配置端口带宽

μHammer2E/2ED/24E/24ED/2024E 交换机支持端口带宽的配置。用户可以限制端口的实际带宽，以便达到管理、区分权限等目的。用户还可以具体的配置带宽限制所针对的流量方向，包括限制入流量、限制出流量或者同时限制两个方向的流量。

在配置带宽的同时，还允许用户设置端口带宽的精度模式，更灵活有效的进行配置管理。用户可以配置“Normal”（普通模式）或者“Precision”（精确模式）。在“Normal”模式下，配置的粒度为 100K；在“Precision”模式下，配置的粒度为 10K。

用户可以选择自己习惯的带宽粒度进行端口带宽的配置，更方便快捷的进行管理。

配置步骤

步骤1	config port [<portlist>|all] [input-bandwidth|output-bandwidth] speed <speednumber>	配置端口的带宽值。
步骤2	config bandwidth mode <Normal|Precision>	配置端口的带宽粒度模式。
步骤3	show port [<portlist>|all] bandwidth	查看端口的带宽配置。 其中，用户配置的端口的实际带宽 = 端口的带宽值 × 带宽粒度。

提示

可设置的端口带宽值为 0－100M。端口带宽值为 0，表示该端口没有进行带宽限制。

由于在不同的粒度模式下可以配置的带宽值是不同的，因此如果更改了端口带宽的粒度模式，系统需要重新配置所有端口的带宽值。

只有端口 1－24 可以配置端口带宽。


注意

端口入流量带宽是建立在流控的前提下的，因此要使入流量带宽起作用，需要网络双方的流控都打开，也就是打开该端口和该端口连接设备的流控功能。端口出流量带宽不以流控为前提。

3.2 配置案例

3.2.1 配置端口速率、双工模式、流控和描述信息

案例描述

关闭所有端口的自适应模式后，将所有端口设置为速率 10Mbps、全双工模式，打开流控，并设置描述信息为“the_port_is_linked”。

配置步骤

步骤1	关闭所有端口的自适应模式。
	Harbour(config)#config port all auto off
步骤2	将所有端口的速率设置为10Mbps。
	Harbour(config)#config port all speed 10
步骤3	将所有端口设置为全双工模式。
	Harbour(config)#config port all duplex full
步骤4	打开所有端口的流量控制。
	Harbour(config)#config port all flowcontrol on
步骤5	将所有端口的描述内容都配置为“the_port_is_linked”。
	Harbour(config)#config port all description the_port_is_linked

3.2.2 清除端口统计信息

案例描述

首先查看当前端口 24 的统计信息，然后清除端口 24 统计信息，之后再显示端口 24 执行清除操作后的端口统计信息。

配置步骤

步骤1	查看当前端口24的统计信息。
	Harbour> show port 24 stats

	Port:24 's Statistics Information

	Tx Octets :1152045 Tx good frames : 6154 Tx total frames : 6154 Tx unicast frames : 6100 Tx Ununicast frames : 54 Rx Octets :87543345 Rx good frames : 241312 Rx total frames : 241312 Rx multicast frames : 645 Rx broadcast frames: 232091 CRC error frames : 0 Oversize frames : 0 Fragments : 0 Jabber : 0 Dropped frames : 2 Undersize frames : 0 Collision : 0 Late collision : 0 ----------
步骤2	清除端口24统计信息。
	Harbour(config)# clear port 24 stats
步骤3	此时再显示端口24的统计信息。如果该端口处于空闲状态，即未被使用，则端口的所有状态将显示为零；如果该端口正被使用，那么在清空以后，会立刻有数据流过，因此它的一些数值不是零。
	Harbour> show port 24 stats ---------- Port:24 's Statistics Information Tx good frames : 0 Tx total frames : 0 Tx unicast frames : 0 Tx Ununicast frames : 0 Rx good frames : 0 Rx total frames : 0 Rx multicast frames : 0 Rx broadcast frames: 0 CRC error frames : 0 Oversize frames : 0 Fragments : 0 Jabber : 0 Dropped frames : 0 Undersize frames : 0 Collision : 0 Late collision : 0 ----------

3.2.3 配置镜像端口

案例描述

将镜像端口设置为 1，向该镜像端口添加数据源端口 2-5，接着，从该镜像端口删除数据源 2。

配置步骤

步骤1	将镜像端口设置为1。
	Harbour(config)#config mirroring to 1
步骤2	向该镜像端口添加数据源端口2-5。此时，通过端口2-5的数据包全部从1端口通过，这样可以通过截取端口1的数据包达到诊断错误的目的。
	Harbour(config)#config mirroring add port 2-5

步骤3	从该镜像端口删除数据源2。
	Harbour(config)#config mirroring delete port 2

3.2.4 配置多端口负载均衡组

案例描述

定义一个 Load Sharing 组，包含端口 10-13，并以端口 12 为逻辑上的主端口，显示出当前系统中正在运行的 Load Sharing 组信息，然后关闭 Load Sharing 组中的端口 10、11、12、13。

配置步骤

步骤1	定义一个Load Sharing组，包含端口10-13，并以端口12为逻辑上的主端口。端口12在逻辑上代表物理端口10、11、12、13。通过对端口12的配置来完成对该Load Sharing组中所有端口的配置。
	Harbour(config)#create sharing 12 grouping 10-13
步骤2	显示出当前系统中正在运行的Load Sharing组信息，包括主端口以及组中所含的端口列表。
	Harbour(config)#show sharing Sharing port group 12 information: Master Port: 12 Group Ports: 10 11 12 13 Load sharing according as Destination Mac.
步骤3	关闭Load Sharing组中的端口10、11、12、13。
	Harbour(config)#config port 12 disable

3.2.5 配置端口带宽

案例描述

配置端口 1-4 的带宽，并进行查看。

配置步骤

步骤1	配置端口带宽。执行后，用户配置的带宽粒度模式为精确模式，即端口粒度为10Kbps；端口1-4的入流量限制为320，实际的带宽即为320*10Kbps=3200Kbps，即3.2Mbps；端口1-4的出流量的实际带宽是640*10Kbps=6400Kbps，即6.4Mbps。
	Harbour(config)#config bandwidth mode precision Harbour(config)#config port 1-4 input-bandwidth speed 320 Harbour(config)#config port 1-4 output-bandwidth speed 640
步骤2	查看执行以上配置命令后端口1-4当前的带宽配置。

```
Harbour(config)#show port 1-4 bandwidth
-------------------------------------------------------------------------------------------
                    Port Bandwidth Configuration Information

Bandwidth interval-mode is 1     Bandwidth interval-value is 10(Kbps)

Port 1 :
    input config is          320 ,    output config is          640
    input value   is   3200(Kbps) ,    output value   is 6400(Kbps)

Port 2 :
    input config is          320 ,    output config is          640
    input value   is   3200(Kbps) ,    output value   is 6400(Kbps)

Port 3 :
    input config is          320 ,    output config is          640
    input value   is   3200(Kbps) ,    output value   is 6400(Kbps)

Port 4 :
    input config is          320 ,    output config is          640
    input value   is   3200(Kbps) ,    output value   is 6400(Kbps)

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

4 配置 VLAN

本章主要介绍 VLAN 的相关概念，以及如何配置 VLAN 的各项属性。

4.1 VLAN概述

虚拟局域网络 VLAN（Virtual Local Area Networks）主要指看起来好象在同一个物理局域网中通信的设备集合。在交换机上设置 VLAN 能使网络管理员的配置管理工作变得轻松。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。

4.1.1 VLAN的优点

- 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 能设置在每个 VLAN 中只包含必须相互通信的设备，从而减少广播、提高网络效率。

- 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，市场部的 VLAN Market 中的设备和销售部的 VLAN sales 中的设备通信，就必须通过路由设备才能进行。两个部门不能直接通信，从而提高系统安全性能。

- 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，用户的终端地址必须重新设置。而使用 VLAN 则不需要这些复杂的设置。

例如，在 VLAN 网络中，市场部的 VLAN Market 中的一台终端移动到了另一个网络中的某个端口，但需要保留它的原有子网资格，则只需将那个端口设置在 VLAN Market 中即可。

4.1.2 VLAN的分类

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

以端口划分 VLAN

在一个 Port-Based VLAN（基于端口的 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。

例如，可以设置端口 1、9 和 15 属于 VLAN Market，端口 3 和 14 属于 VLAN Finance，端口 6、18-21 属于 VLAN Sales。

以标签划分 VLAN

标签就是在以太网帧中插入的特定的记号，称为 tag。标签是某个指定 VLAN 的标识号 VLAN id。


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 1518 稍大，这样可能导致其它设备中的数据包计数错误，或者可能导致在非 802.1Q 的网桥或者路由器的网络中的连接出现问题。

标签（Tagging）最常应用在跨交换机创建 VLAN 中。此时，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 的另一个优点是一个端口可以属于多个 VLAN，并且使用这些 VLAN 的标签。当有一个设备（例如服务器）必须属于多个 VLAN 时，这一点特别有用。当然这个设备必须有支持 802.1Q 的网络接口卡。

每一个 VLAN 都可以赋予一个 802.1Q VLAN Tag。当端口被加到一个 802.1Q 标签定义好的 VLAN 中去时，用户可以决定该端口是否使用该 VLAN 的标签。HammerOS 交换机的缺省模式是所有端口都属于一个名叫 default 的 VLAN，但不使用该 VLAN 的标签，该 VLAN 的标签 VLAN id 是 2047。

并非所有端口都必须使用标签。当数据流从交换机的一个端口输出时，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，而接收数据的端口又并不属于配置了带该 Tag（VLAN id）的 VLAN 时，那么交换机将丢弃该数据包。

图4-1 VLAN 标签

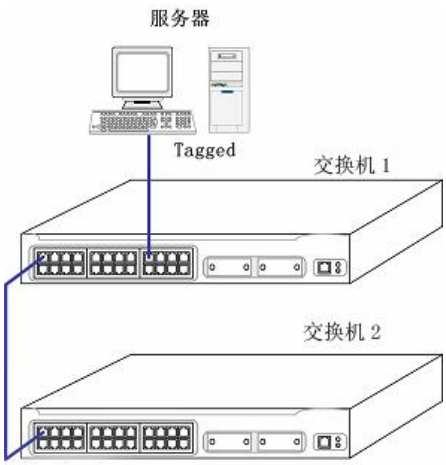


图 4-1 中，交换机 1 的端口 1 和交换机 2 的端口 1 是两台交换机的中继端口，都同时属于 VLAN Market 和 VLAN Sales。这两个端口之间的连接使两台交换机上的 VLAN Market 和 VLAN Sales 连接起来，使这两个 VLAN 都能跨交换机通信。

中继端口都是加标签(tagged)的。连接到交换机 1 的端口 8 的服务器有支持 802.1Q Tagged 的网络接口卡（NIC）。服务器所连的交换机 1 的端口 8 同时属于 VLAN Market 和 VLAN Sales。除了服务器所连的交换机 1 的端口 8 和两台交换机的端口 1 是加标签（tagged）的以外，别的端口都是未加标签（untagged）的。

当数据转发到交换机的端口时，交换机决定数据送达到目的端口是否需要加标签（tagged）。所有服务器收发的数据都是加标签（tagged）的。从其余终端工作站收和发的数据都是未加标签（untagged）的。

混合使用 Tagged VLAN 和 Port-Based VLAN

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。


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 VLAN id 的值为 0，那么交换机会把该数据包当作是未标签（untagged）的。

4.2 配置VLAN

μHammer2E/2ED/24E/24ED/2024E 交换机支持 256 个不同的 VLAN。每个 VLAN 的名字可以由以字母开头的 1 至 30 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、引号等字符都是不允许的。

VLAN 的名字只是本地标志，即在一台交换机上设置的 VLAN 的名字只对该交换机有意义。


提示

为了方便维护，应该在整个网络中统一规划命名 VLAN。

4.2.1 缺省配置信息

μHammer2E/2ED/24E/24ED/2024E 交换机关于 VLAN 的缺省配置信息如以下表格所示：

表4-1 缺省配置信息

内容	缺省设置	备注
缺省VLAN 的名字	default	不可更改设置
包含的端口	所有端口	可更改设置
端口标签	untagged（未标签）	可更改设置

4.2.2 创建VLAN

配置步骤

步骤1	create vlan <name> tag <1-4094>	配置模式下，创建VLAN。 其中，<name>为要创建的VLAN名；Tag取值范围是1－4094。

4.2.3 更改VLAN名称

配置步骤

步骤1	config vlan <name> rename <name>	对VLAN的配置不作更改，只更改VLAN的名称。 其中，第一个<name>表示原来的VLAN名；第二个<name>表示新的VLAN名。

4.2.4 删除VLAN

配置步骤

步骤1	delete vlan {<name>}*1	删除VLAN。 其中，选择<name>，表示删除指定的VLAN；不选择<name>，表示删除所有VLAN。

4.2.5 添加VLAN端口

交换机的端口可以以两种形式属于某个 VLAN，分别是：

- IEEE 802.1Q tagged 模式
- IEEE 802.1Q untagged 模式

默认情况下，所有端口都以 untagged 模式加入 default VLAN。

在 single 模式下一个端口只能在 IEEE 802.1Q untagged 模式下属于一个 VLAN，同时可以以 IEEE 802.1Q tagged 模式属于多个 VLAN；在 multiple 模式下一个端口可以在 IEEE 802.1Q untagged 模式下属于多个 VLAN，同时可以以 IEEE

802.1Q tagged 模式属于多个 VLAN。

VLAN 中每个端口只能有唯一的一个 default VID。端口的 default VID 为该端口所属的多个 VLAN 中的其中一个 VLAN 的 VID。这样在该端口上收到的没有加 802.1Q Tag 值的正常数据，会在该端口的 default VID 所属的 VLAN 中转发。

当端口第一次以 untagged 方式加入到 VLAN 中时，它的 default VID 由系统自动分配为这个 VLAN 的 VID，在 multiple 方式下这个端口还可以 untagged 方式加入到其他 VLAN 中，此时端口的 default VID 将不会发生改变，除非使用 config port [<portlist>|all] inputvlan <name>命令指定端口的 default VID。

配置步骤

步骤1	config vlan <name> add port <portlist> [tagged|untagged]	添加VLAN端口。 其中，选择tagged，表示向VLAN添加tagged端口；选择untagged，表示向VLAN添加untagged端口。

命令格式 `config port [<portlist>|all] inputvlan <name>`

命令功能 指定某个端口的默认 VLAN。

命令模式 配置模式

参数说明

参数	说明
portlist	端口列表
name	VLAN 名。 必须为系统中已创建的VLAN。

使用指导 当一个端口以 untag 属于多个 vlan 的时候，使用本命令可以设置端口的默认 vlan。

配置实例

```
Create vlan test1 tag 2000
Config vlan test1 add port 3 untag
Create vlan test2 tag 2001
Config vlan test2 add port 3 untag
Config port 3 inputvlan test2
```

4.2.6 删除VLAN端口

交换机的端口可以两种形式从一个 VLAN 中删除，分别是

- IEEE 802.1Q tagged 模式
- IEEE 802.1Q untagged 模式

tagged 模式端口的删除在 multiple、single 方式下的处理方式一致，也比较简单，就不再介绍。

下面着重介绍在 single 和 multiple 模式下删除 untagged 端口的方式。

配置步骤

步骤1	config vlan <name> delete port <portlist> untagged	single模式、multiple模式下，从VLAN中删除端口。

在 single 模式下，从一个 VLAN 中以 IEEE 802.1Q untagged 方式删除一个端口，这个端口将会被添加到 default VLAN 中去，同时它的 default VID 也会改变为 2047。

在 multiple 模式下，从一个 VLAN 中以 IEEE 802.1Q untagged 方式删除一个端口分为两种情况：如果只有这一个 VLAN 以 IEEE 802.1Q untagged 方式包含该端口，操作与 single 模式相同；如果除了这个 VLAN，还存在其他的 VLAN 以 IEEE 802.1Q untagged 方式包含该端口，并且端口的 default VID 为这个 VLAN 的 VID，则端口的 default VID 将改变为其它 VLAN 中 VID 较大的值。

4.2.7 配置VLAN描述信息

配置步骤

步骤1	config vlan [<name>|all] description <description>	在创建一个VLAN后，对这个VLAN加以文字描述。 其中，选择<name>，表示对指定的VLAN进行操作；选择all，表示对所有VLAN进行操作；选择<description>，输入描述内容。当输入描述文字时，不能使用空格，在需要用空格的地方改用下划线将描述内容连起来。

使用命令 clear vlan [<name>|all] description 可以清空 VLAN 的描述信息。

4.2.8 配置VLAN模式

在平台上存在两种 VLAN 模式，multiple 和 single。multiple 模式允许配置端口以 untagged 方式属于几个 VLAN，single 模式则限制一个端口只能以 untagged 方式属于一个 VLAN。

允许用户在这两个模式间进行切换。切换之前系统将会删除 default VLAN 外的所有已存在的 VLAN，所有端口的 default VID 还原为 default VLAN 的 VID。

配置步骤

步骤1	config vlanmode [multiple|single]	切换VLAN模式。
步骤2	show vlanmode	显示当前的VLAN模式。

4.2.9 修改VLAN的Tag

配置步骤

步骤1	config vlan <name> tag <1-4094>	修改 VLAN 的 tag 值。其中，<name>表示要修改的VLAN名，可以是default vlan；Tag的取值范围是<1-4094>。

4.2.10 配置PVID区段

配置步骤

步骤1	config baselevel <0-15>	配置PVID区段。
步骤2	show baselevel	显示PVID的区段和范围。

提示

此命令用来改变交换机的 PVID 的区段以及范围。在改变交换机的 PVID 的区段之前，用户必须删除以前配置的所有 VLAN，才能成功调用此命令。改变区段后，用户需重新配置所需的 VLAN。请慎用此命令。

表4-2 PVID 的区段划分（1）

区段 / 范围	0	1	2	3	4	5	6	7
BaseLevel	0	1	2	3	4	5	6	7

BaseVid	0	256	512	768	1024	1280	1536	1792
PVID range (User can set)	1-254	256-510	512-766	768-1022	1024-1278	1280-1534	1536-1790	1792-2046
PVID of Default VLAN	255	511	767	1023	1279	1535	1791	2047

表4-3 PVID 的区段划分（2）

区段 / 范围	8	9	10	11	12	13	14	15
BaseLevel	8	9	10	11	12	13	14	15
BaseVid	2048	2304	2560	2816	3072	3328	3584	3840
PVID range (User can set)	2048-2302	2304-2558	2560-2814	2816-3070	3072-3326	3328-3582	3584-3838	3840-4093
PVID of Default VLAN	2303	2559	2815	3071	3327	3583	3839	4094

4.2.11 显示VLAN配置信息

配置步骤

步骤1	show vlan {<name>}*1	显示VLAN信息。 其中，<name>可以输入也可以不输入；输入name，只显示这个name的VLAN的信息；不输入name，显示当前交换机中的所有VLAN的信息。 该命令显示的VLAN信息包括以下内容：VLAN id、VLAN名字、MAC address、属于该VLAN的tagged模式的端口、属于该VLAN的untagged模式的端口、该VLAN的描述。

4.2.12 配置Console管理功能

交换机提供了 VLAN 的 console 功能来限制用户对交换机的管理，只有成为 console VLAN 的 VLAN 才能访问交换机，并 ping 通交换机的 ip 地址。其他 VLAN 的成员不能通过 telnet、Web 等手段管理交换机，增加了交换机的安全性。

配置步骤

步骤1	config vlan <name> console	配置模式下，配置某个VLAN作为console VLAN。


提示

只有一个 VLAN 可以设置为 console vlan。

4.2.13 配置VCN

启动 VCN 将为交换机的所有端口（除上行端口外）分别创建一个 VLAN，使端口之间隔离开来，不能相互通信，只能和上行端口通信。

配置步骤

步骤1	config vcn up <portlist> [notagout|tagout] baseVID <1-4094>	启动VCN。 其中，<portlist>表示指定哪个端口作为上行通信端口，可以指定一个或两个上行端口；选择notagout，表示上连端口以untagged方式属于VCN所创建的所有VLAN；选择tagout，表示上连端口以tagged方式属于VCN所创建的所有VLAN；<1-4094>表示baseVID的值，其中baseVID为上行端口所属VLAN的 tag 值，其它VLAN的tag值根据端口号依次递增。当边界值超过了规定的范围后，将返回起始值进行循环。在multiple模式下如果某个VID被已存在的VLAN占用，那么将会跳过这个VID继续寻找下一个未被占用的VID。

每个 VLAN 包含对应的端口（untagged） 和所有上行端口（tagged 或 untagged），同时所有上行端口属于一个 VLAN。每个下行 VLAN 的名称表示为 vcndvlan 加上端口号，上行 VLAN 的名称表示为 vcnuvlan。例如 vcndvlan1 为一个合法的 VLAN 名称。


提示

VCN 命令就是创建 VLAN 的一条批处理命令;
使用 VCN 命令将会删除以前配置的所有 VLAN;
在 single 和 multiple 模式下配置 VCN 有不同之处。

single 模式下配置 VCN

配置步骤

步骤1	config vcn disable	关闭VCN，即删除所有由VCN创建的上、下行VLAN。
步骤2	show vcn	显示当前VCN状态信息。

single 模式下，配置 VCN 以后不能再进行增加、删除、修改 VLAN 等操作；配置 VCN 以后，如果需要改变 VLAN mode 或者 baselevel，必须先使用 config vcn disable 命令关闭 VCN 之后才能配置；配置 VCN 以后，如果又使用了配置 VCN 的命令，必须先使用 config vcn disable 命令关闭以前的 VCN 之后才能配置。

multiple 模式下配置 VCN

multiple 模式下不允许使用 config vcn disable 和 show vcn 这两个命令，但是可以使用 delete vlan 命令删除所有 VLAN。

multiple 模式下，配置 VCN 以后，允许用户使用普通 VLAN 的操作命令来增加、删除、修改 VLAN 以及修改端口的 default VID 等；配置 VCN 以后，如果需要改变 VLAN mode 或者 baselevel，系统会自动删除所有 VLAN；配置了 VCN 以后，如果又使用了配置 VCN 的命令，系统会自动删除以前所有 VLAN。


注意

对于有模块板的交换机配置 VCN 要注意以下事项：

1、如果槽位没有插模块板，show port 这个端口是显示不出来的，当然在配置 VCN 的时候也不会为这个端口创建 VLAN。

2、配置好 VCN 之后，请尽量不要修改交换机的硬件配置（比如重启前某槽位插有模块板，重启后没有；或者重启前没有，重启后有），尤其是重启前这个槽位作为上行端口，重启后模块板拔掉，将会出现异常。如果必须修改配置，请重新配置 VCN。

3、对于支持 SFP 的交换机也要注意，如果光收发器不在位，配置 VCN 的时候将不会为其创建 VLAN。同样，配置好 VCN 后也尽量不要修改交换机硬件配置（光收发器的在位与否），如果必须修改，请重新配置 VCN。

4.3 配置案例

4.3.1 添加VLAN端口

案例描述

创建一个名称为 market 的 VLAN，将端口 2 和 4 以 IEEE 802.1Q untagged 模式加入该 VLAN，显示 VLAN market 的信息，再向 market 添加一个 IEEE 802.1Q tagged 模式的属于该 VLAN 的端口 2，显示 VLAN market 的信息。

配置步骤

步骤1	创建一个名称为market的VLAN，将端口2和4以IEEE 802.1Q untagged模式加入该VLAN。
	Harbour(config)#create vlan market tag 2000 Harbour(config)#config vlan market add port 2 untagged Harbour(config)#config vlan market add port 4 untagged
步骤2	查看VLAN market 的信息。
	Harbour(config)# show vlan market VLAN ID : 2000 Name : market Mac address : 00:25:33:44:55:11 Tagged Ports : Untagged Ports : 2 4 Description : normal
步骤3	向market添加一个IEEE 802.1Q tagged模式的属于该VLAN的端口2。
	Harbour(config)#config vlan market add port 2 tagged
步骤4	再查看VLANmarket 的信息。
	Harbour(config)# show vlan market VLAN ID : 2000 Name : market Mac address : 00:25:33:44:55:11 Tagged Ports : 2 Untagged Ports : 4 Description : normal

端口 2 以 IEEE 802.1Q tagged 模式属于 VLAN market，而 untagged ports 中就没有端口 2 了。

4.3.2 删除VLAN端口

案例描述

在 multiple 模式下，从一个 VLAN 中以 IEEE 802.1Q untagged 方式删除一个端口分为两种情况：如果只有这一个 VLAN 以 IEEE 802.1Q untagged 方式包含该端口，操作与 single 模式相同；如果除了这个 VLAN，还存在其他的 VLAN 以 IEEE 802.1Q untagged 方式包含该端口，并且端口的 default VID 为这个 VLAN 的 VID，则端口的 default VID 将改变为其它 VLAN 中 VID 较大的值。

配置步骤

步骤1	创建VLAN v1、v2和v3。
	Harbour(config)#create vlan v1 tag 2001 Harbour(config)#create vlan v2 tag 2002 Harbour(config)#create vlan v3 tag 2003
步骤2	向VLAN v1、v2和v3中以untagged模式添加端口1。
	Harbour(config)#config vlan v1 add port 1 untagged Harbour(config)#config vlan v2 add port 1 untagged Harbour(config)#config vlan v3 add port 1 untagged
步骤3	从VLAN v2中删除端口1。此时端口1的default VID将会变为2003，即2001与2003中的较大的那个值。
	Harbour(config)#config port 1 inputvlan v2 Harbour(config)#config vlan v2 delete port 1 untagged

4.3.3 配置VLAN模式

案例描述

切换 VLAN 模式为 single 模式，并显示当前的 VLAN 模式。

配置步骤

步骤1	切换VLAN模式为single模式。
	Harbour(config)# config vlanmode single Warning : all vlans will be deleted Are you sure want to change vlan mode yet? [Y/N] 输入Y确认后，有如下提示： Trying delete all system vlan exclude default vlan, please wait .....finished. Successfully delete all system vlan exclude default vlan.
步骤2	显示当前的VLAN模式。
	Harbour(config)# show vlanmode % vlan mode is single

4.3.4 显示PVID区段

案例描述

显示 PVID 区段。

配置步骤

步骤1	显示PVID区段。
	Harbour(config)# show baselevel BaseLevel : 15 Base Vid : 3840 VID Range : 3840 – 4094

4.3.5 配置VCN

案例描述

显示利用配置 VCN 命令所创建的 VLAN 信息。

配置步骤

步骤1	显示利用配置VCN命令所创建的VLAN信息。
	Harbour(config)# show vlan VLAN ID : 2047 Name : default Mac address : 00:05:3b:00:00:00 Tagged Ports : Untagged Ports : Description : normal VLAN ID : 2000 Name : vcnuvlan Mac address : 00:05:3b:00:00:00 Tagged Ports : Untagged Ports : 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 Description : normal VLAN ID : 2001 Name : vcndvlan1 Mac address : 00:05:3b:00:00:00 Tagged Ports : 1 Untagged Ports : 2

```
Description          : normal

VLAN ID              : 2002
Name                 : vcndvlan2
Mac address          : 00:05:3b:00:00:00
Tagged Ports         : 1
Untagged Ports       : 3
Description          : normal

VLAN ID              : 2003
Name                 : vcndvlan3
Mac address          : 00:05:3b:00:00:00
Tagged Ports         : 1
Untagged Ports       : 4
Description          : normal

VLAN ID              : 2004
Name                 : vcndvlan4
Mac address          : 00:05:3b:00:00:00
Tagged Ports         : 1
Untagged Ports       : 5
Description          : normal
```

5 配置 H.Link

本章主要介绍 H.LINK 协议的相关概念，以及如何配置 H.LINK 协议。

5.1 H.LINK概述

H.Link 协议是港湾网络有限公司的专有通讯协议，实现对远程设备的本地管理。服务器将多个远程子设备映射为本地虚拟子设备，通过虚拟子设备配置远程子设备，由此实现远程设备的本地化管理。

H.Link 协议分为客户端和服务器端，客户端运行于 μHammer1000 和 μHammer1000Q 系列交换机上。μHammer1000 和 μHammer1000Q 系列交换机一旦启动，H.Link 客户端即开始运行，寻找并注册到服务器端。

μHammer2E/2ED/24E/24ED/2024E 交换机上运行 H.Link 服务器端。服务器端需要手工配置以完成服务器端和客户端的通信连接。

在 μHammer2E/2ED/24E/24ED/2024E 交换机上，H.Link 的配置文件需要单独保存，并且支持通过 FTP 方式上传、下载。必要时，可以共享配置文件，也可以在无法手工恢复当前配置时，通过下载原先保存的配置文件完成。

5.2 配置H.LINK

5.2.1 启动H.LINK服务

配置步骤

步骤1	hlink start	启动H.Link服务

5.2.2 停止H.LINK服务

配置步骤

步骤1	hlink end	停止H.Link服务

5.2.3 查看H.LINK状态

配置步骤

步骤1	hlink status	查看H.Link的状态

5.2.4 进入H.LINK配置模式

配置步骤

步骤1	hlink config	进入H.Link配置模式

5.2.5 上传/下载H.LINK

H.Link 的上传、下载与交换机配置文件的上传、下载过程一样，只是参数由 config-file 变为 hlink-config-file 而已。

在保存/下载 H.Link 配置文件的交换机上启动 FTP 服务，设置好工作目录、用户名、密码，然后关闭 H.Link 服务，否则会提示关闭。


注意

上传时需要有写的权限，而下载时只需要有读的权限。

5.3 配置案例

案例描述

关闭 H.Link 后，查看 H.Link 的状态，再启动 H.Link，再次查看状态，然后进入 H.Link 的配置模式。

配置步骤

步骤1	关闭H.Link服务。
	Harbour(config)# hlink end Closing H.Link protocol. Please wait...
步骤2	查看H.Link的状态。显示现在是关闭的。
	Harbour(config)# hlink status H.Link is stopped.
步骤3	再启动H.Link服务。
	Harbour(config)# hlink start Initiazing H.Link protocol. Please wait... Initiaze successfully.
步骤4	再次查看状态。此时H.Link已经运行。
	Harbour(config)# hlink status H.Link is running.
步骤5	进入H.Link 的配置模式。进入H.Link配置模式后就可以进行有关H.Link的所有配置操作了。
	Harbour(config)# hlink config Harbour(HLINK-ROOT)#

具体内容请参阅《H.Link 用户配置手册》。

6 配置 FDB 表

本章主要介绍 FDB（Forwarding Database）地址表的内容和相关知识，以及如何配置静态 FDB 地址表。

6.1 FDB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 地址表就是 FDB 地址表。

6.1.1 FDB表的内容

FDB 地址表包含多条表项，不同产品的 FDB 地址表包含的表项数量不同。每条 FDB 地址表项由以下几项组成：

- 收到的数据源设备 MAC 地址；
- 连接该数据源设备的端口标志；
- flag 标志；
- 对于多播地址，还包含所属 VLAN 的名字。

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的那个 VLAN 的所有端口。

6.1.2 FDB表的地址表项类型

MAC 地址表共有三种地址表项：

- 动态地址表项

最初，交换机中的所有 MAC 地址表中的地址表项都是动态的；如果经过一段时间（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，这样能够防止地址表项变得过于庞大；当确信某设备从网络中去除后，就把该设备的地址表项删除掉；当交换机关机之后重新启动或者 reset 时，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，请参阅“6.2 配置 FDB 表”。

- 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 MAC 地址表中而不会被动态删除，直至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 MAC 地址表中，即便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。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。μHammer2E/2ED/24E/24ED/2024E 交换机最多能支持 1000 个静态地址表项。

6.1.3 添加地址表项途径

FDB 地址表中的地址表项可以通过以下两种途径被加入：

- 交换机自学习。交换机可以根据收到的数据包的源 MAC 地址、收到数据包的端口、收到数据包的端口所在的 VLAN 来自动更新 FDB 地址表。
- 手工配置。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表

6.2.1 缺省配置信息

μHammer2E/2ED/24E/24ED/2024E 交换机关于端口的缺省设置信息如以下表格所示：

表6-1 FDB 表缺省配置信息

内容	缺省设置	备注
FDB地址表项老化时间（agingtime）	80秒	可更改设置

6.2.2 配置FDB地址表项老化时间

配置步骤

步骤1	config fdb agingtime <0-800>	配置FDB地址表中的地址表项老化时间。


提示

值为 0 表示该地址表项永远不老化。

6.2.3 创建单播FDB永久地址表项

配置步骤

步骤1	create fdbentry <mac_address> port <portno>	创建一个静态的永久地址表项。 其中，<mac_address>表示设备的MAC地址；<portno>表示指定的端口号。


提示

一个单播 MAC 地址只能相关一个端口。

最多只能创建1000条单播地址(包括废弃非法地址项即discard 地址项)。

当动态 FDB 表项学习达到极限时，创建单播 FDB 永久地址表项可能会出现失败的情况。

创建或删除 trunk，系统会自动删除 trunk 组端口上的 FDB 静态表项。

6.2.4 删除单播FDB地址表项

配置步骤

步骤1	delete fdbentry {<mac_address>}*1	删除指定MAC地址的FDB地址表项。 当<mac_address>不输入时，表示删除所有动态FDB表项。

6.2.5 丢弃非法FDB地址表项

配置步骤

步骤1	disgard fdbentry <mac_address>	丢弃非法FDB表项。


提示

1）非法的地址项与创建的单播地址项之和最多为 1000 项；

2）对于已经存在 FDB 表中的地址项，不能直接将其废弃，而必须先删除后再用该命令将其废弃；

3）不能直接将已经废弃的地址项转化为正常的地址项，而必须先将其删除后再用 create 命令重新创建；

4）不能将多播或广播地址项废弃；

5）当动态 FDB 表项学习达到极限时，创建丢弃 FDB 表项可能会出现失败的情况。

6.2.6 显示FDB地址表项

配置步骤

步骤1	show fdb {[dynamic|permanent]}*1 {[mac] <macaddr>}*1	显示FDB地址表中的静态地址表项。 其中，当参数都不输入时，表示显示所有的FDB地址表信息；当mac地址不输入时，显示当前交换机FDB地址表中所有静态永久地址表项的信息；当输入dynamic时，显示动态地址表项；当输入permanent时，显示静态地址表项；用户可以指定MAC地址，来确定某个VLAN是否包含一个特定的MAC地址。

6.2.7 显示FDB表的摘要信息

配置步骤

步骤1	show fdb summary	显示FDB地址表摘要信息，包含了静态的、动态的、多播的和总的FDB个数。

6.2.8 静态FDB与Maclimit、dot1x动态单播优先级关系

1）802.1x 和 maclimit 的动态单播优先级更高。

（这里指的动态单播都是指 802.1x 和 maclimit 创建的静态 mac，对于用户来说是自动创建的，因此称为动态单播）。

2）如果已经存在 dot1x 的动态单播，用户再创建相同 MAC 的静态单播（包括 discard 这个 MAC）将会创建失败，并给出错误提示。

3）如果已经在某端口上配置的 Maclimit，如果又在这个端口上配置静态单播（包括 discard 这个 MAC），将会创建失败，并给出错误提示。

4）如果系统已经存在用户配置的静态单播（包括 discard 这个 MAC），并且有创建 dot1x 和 maclimit 动态单播的要求，那么将会覆盖用户的配置，不需要给出提示。

6.2.9 配置静态组播FDB

配置组播 FDB 是将组播 MAC 绑定到端口。对于目的 MAC 是组播 MAC 的报文，首先会查询是否有与该 MAC 对应的表项；若有，则报文从表项中所绑定的端口发出；若没有，则在整个 VLAN 中广播。组播地址分为 IP 组播和非 IP 组播。

创建 IP 组播 FDB 地址表

配置步骤

步骤1	create mfdb mac <mac_address> vlan <name> port <portlist>	配置模式下，创建IP组播FDB地址表。其中，<mac_address>表示MAC地址；<name>表示VLAN名；<portlist>表示端口列表。
步骤2	show mfdb	显示组播FDB地址表。

创建非 IP 多播 FDB 地址表

配置步骤

步骤1	create mfdb mac <mac_address> port <portlist>	配置模式下，创建非IP组播FDB地址表。其中，<mac_address>表示MAC地址；<portlist>表示端口列表。
步骤2	show fdb	显示组播FDB地址表。

删除组播 FDB 表

配置步骤

步骤1	delete mfdb <mac_address> {vlan <name>}*1	删除组播FDB表。
步骤2	show mfdb	显示组播FDB地址表。


提示

（1）最多只能创建 256 项组播地址项；其中可以包括最多 224 项的非 IP 组播及最多 256 项的 IP 组播。

（2）一个组播地址项对应的端口号可以不只一个；对于 IP 多播，这些端口号只能位于同一个 vlan 内；

（3）可以创建相同地址，但 vlan 不同 IP 多播地址项；

（4）IP组播即范围在 0x01005e000000 到 0x01005e7fffff 内的组播地址；非 IP 组播地址就是 IP 组播地址范围以外的组播地址。

6.3 配置案例

案例描述

显示 FDB 地址表中的所有地址表项。

配置步骤

步骤1 显示FDB地址表中的所有地址表项。

```
Harbour(config)# show fdb

---------- Begin of MAC address table information ----------

MAC address               Port                 Flags
------------------------- -------------------- ------------------------------
00:05:3b:00:00:47         4                    Age
00:05:33:22:55:13         4                    Age
00:05:3b:00:00:11         4                    Age
00:0b:db:53:3b:9f         4                    Age
00:05:3b:58:01:67         4                    Age
00:05:3b:8c:e9:11         4                    Age
00:05:3b:6a:00:57         4                    Age
00:10:5c:b3:d5:59         4                    Age
00:25:33:44:55:11         0                    System CPU Permanent
00:20:ed:aa:be:19         1                    Age
00:20:ed:aa:c8:ff         4                    Age
```

```
00:10:dc:41:85:10          4                    Age
00:10:dc:47:7e:af          4                    Age
00:0b:db:53:3b:85          4                    Age
00:05:3b:40:00:b2          4                    Age
00:05:3b:11:25:db          4                    Age
-------------------------- -------------------------- ------------------------------

Total 16 MAC address entry showed.

------------------ End of MAC address table information ----------------------
```

7 配置 MACLIMIT

本章主要介绍 MacLimit 内容和相关知识，以及如何配置 MacLimit 的功能。

7.1 概述

MacLimit 即 MAC 址址限制，是指在设备可以配置每个端口下允许的 MAC 数量，以达到部分防代理的作用。

7.1.1 MacLimit实现的功能

MacLimit 只对动态学习到的 MAC 起作用。如果设置某个端口指定数量的主机服务，当使用该端口通信的主机数量超过预设定值，就采取特定的惩罚措施。Maclimit 功能的配置和管理粒度是端口，而且能对 trunk 端口作为一个逻辑端口进行管理。同时还可以配合 802.1x 来完成特定的策略。

7.1.2 MacLimit工作方式

用户使用此功能的时候对某端口设定的是合法用户的名额数和非法用户的名额数，以及惩罚方式和惩罚时间。

功能启动后，先被发现连接在此端口的动态 MAC，称为合法用户。合法用户名额满了以后，接着被发现的动态 MAC 称为非法用户。交换机将转发合法用户的帧，而不转发非法用户的帧。在非法用户的名额也满了以后，如果继续出现新的陌生动态 MAC，交换机开始根据设定方式和时间惩罚该端口。惩罚措施是以下三种中的一种：

- 不惩罚，交换机会尽量保证合法用户的通信，但是由于非法用户数的增加，此时交换机会出现丢帧的现象。
- 关闭端口，并持续一段时间；

n 关闭端口的学习功能，并持续一段时间；

非法用户的概念其实就是增加了一个缓冲：当发现有超过期望数量的 MAC 出现的时候，并没有马上惩罚，而是不转发那些多出的 MAC 地址；当 MAC 数在超过了缓冲仍然增加的时候将会启动开始惩罚端口。

7.2 配置MacLimit

7.2.1 打开MacLimit功能

命令格式 `maclimit port [<portlist>|all] on enable <0-128> disable <0-128> pType <0-2> pTime <0-300>`

命令功能 配置 MacLimit 功能

命令模式 配置模式

参数说明

参数	说明
[<portlist>|all]	表示要配置**MACLimit**功能的端口，如果该端口属于某个**trunk**，那么只用主端口才能配置成**MACLimit**模式。
enable <0-128>	设置可以利用此端口进行通信的合法用户的个数，先连到此端口的用户为合法用户。合法用户的计数不计入设置在此端口的静态**MAC** 地址。
disable <0-128>	设置非法用户的个数；合法用户的名额是有限的，在合法用户数占满以后，连接到此端口的用户就称为非法用户；在非法用户的数量超过了设定值的时候，就会开始惩罚。
pType <0-2>	表示惩罚类型，**0**：不惩罚；**1**：关端口；**2**：关闭端口学习功能；**0**不惩罚，在这种状态下交换机会尽量保证合法用户的通信，但是由于非法用户数的增加，此时交换机会出现丢包的情况。在关端口的情况下，连在此端口的所有用户都不能通信。在关端口学习功能打开时，此时端口对合法用户和非法用户都不转发，但是运营商可以通过在此端口增加静态**MAC**的方法放行一些特殊用途的用户。
pTime<0-300>	表示惩罚时间，单位为分钟。“**0**” 表示惩罚时间为无穷大，惩罚措施永远生效。在惩罚时间结束以后，合法用户的名额仍然还由原来的合法用户占据，防止出现通信震荡。

使用指导 只在配置模式下使用该命令。

配置实例

```
Harbour(config)# maclimit port 1-3 on enable 2 disable 1 pType 2 pTime
10
```

打开端口 1，2，3 的 MacLimit 功能，合法用户数为 2 个，非法用户数为 1 个，惩罚措施为关端口学功能，惩罚时间为 10 分钟。即当某端口下有大于 3 个 MAC 时，该端口的学习功能将自动关闭，除静态加入的 MAC 之外其它均不能进行数据的转发，直至 10 分钟后惩罚结束。

7.2.2 关闭MacLimit功能

命令格式

```
maclimit port [<portlist>|all] off
```

命令功能 关闭 MacLimit 功能

命令参数

参数	说明
[<portlist>|all]	为端口列表

使用指导 只在配置模式下使用该命令。

配置实例

```
Harbour(config)# maclimit port 1-3 off
```

关闭端口 1，2，3 的 MacLimit 功能

7.2.3 显示MacLimit状态

命令格式

```
show maclimit port [<portlist>|all]
```

命令功能 显示 MacLimit 状态

命令参数

参数	说明
[<portlist>|all]	为端口列表

命令模式 配置模式

使用指导 只在配置模式下使用该命令。

配置实例

```
Harbour(config)# show maclimit port 1-3
```

显示端口 1，2，3 的 MacLimit 状态

7.3 配置nohub

nohub 功能限制端口下连接的 MAC 数不能多于一个，如果多于一个将永远关闭该端口。 MacLimit 是原来 nohub 功能的扩展，而为了向前兼容，所以仍然保留了 nohub 的相关命令行。该组命令只是 MacLimit 设置的一个特例。

7.3.1 打开nohub功能

命令格式 `config port [<portlist>|all] nohub enable {punishTime <0-300>}*1`

命令功能 打开 nohub 功能

命令参数

参数	说明
[<portlist>|all]	为端口列表
punishTime <0-300>	为惩罚时间
0	为永久惩罚，默认为**0**

命令模式 配置模式

使用指导 只在配置模式下使用该命令。

配置实例

```
Harbour(config)# config port 1-3 nohub enable
```

打开端口 1，2，3 的 nohub 功能，惩罚时间为 0。该项配置等效于

```
maclimit port 1-3 on enable 1 disable 0 pType 1 pTime 0
```

7.3.2 关闭nohub功能

命令格式 `config port [<portlist>|all] nohub disable`

命令功能 关闭 nohub 功能

命令参数

参数	说明
[<portlist>|all]	为端口列表

命令模式 配置模式

使用指导 只在配置模式下使用该命令。

配置实例

```
Harbour(config)# config port 1-3 nohub disable
```

关闭端口 1，2，3 的 nohub 功能。该项配置等效于

```
maclimit port 1-3 off
```

7.3.3 显示nohub功能

命令格式

```
show port [<portlist>|all] nohub
```

命令功能 显示 nohub 功能

命令参数

参数	说明
[<portlist>|all]	为端口列表

命令模式 配置模式

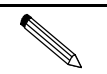
使用指导 只在配置模式下使用该命令。

配置实例

```
Harbour(config)# show port 1-3 nohub
```

显示端口 1，2，3 的 nohub 功能。该项配置等效于

```
show maclimit port 1-3
```



提示

Maclimit/nohub 支持 TRUNK，但必须在 TRUNK 之后进行配置。Maclimit 还可与 802.1x 认证同时使用，但需特定的 radius 配合，具体配置可参考相关手册。

8 配置多域 STP

本章主要介绍多域 STP 协议的相关概念，以及如何配置多域 STP 协议。

8.1 多域STP概述

多域 STP 是扩展的 802.1d，它允许在同一台交换设备上同时存在多个 STP 域，各个 STP 域都按照 802.1d 运行，各域之间互不影响。它提供了一种能够更为灵活和稳定的网络环境，可以基本实现在 VLAN 中计算生成树。

8.2 配置多域STP

8.2.1 缺省配置信息

μHammer2E/2ED/24E/24ED/2024E 交换机关于多域 STP 的缺省设置信息如以下表格所示：

表8-1 多域 STP 表缺省配置信息

内容	缺省设置	备注
使能/关闭STP域	disable	可更改设置
运行STP域的优先级（priority）	32768	可更改设置
根桥发送BPDU的时间间隔（hellotime）	2秒	可更改设置
根桥端口状态切换的时间间隔（forwarddelay）	15秒	可更改设置
BPDU报文老化的最长时间间隔（maxage）	20秒	可更改设置
参与STP计算的端口的优先级（port priority）	128	可更改设置
参与STP计算端口的路径开销（port cost）	10Mbps端口 100 100Mbps端口 19 1000Mbps端口 4	可更改设置

8.2.2 创建/删除STP域

创建 STP 域

配置步骤

步骤1	create stpd <name>	创建STP域。

删除 STP 域

配置步骤

步骤1	delete stpd <name>	删除STP域。

提示

每台交换机可创建的 STP 域的最大值为 255 个；实际数目受限于系统可用资源和交换机的端口数。

域名字长度不超过 30 个字符。

8.2.3 增加/删除端口

配置步骤

步骤1	config stpd <name> [add|delete] [<portlist>|all]	向STP域中增加或删除端口。
步骤2	config stpd <name> port [<portlist>|all] [enable|disable]	根据需要可以使能或关闭某个端口的STP功能。

注意

将某个端口加入到 STP 域时，如果该端口已经存在于另一个域，命令将主动把该端口从原 STP 域移除，这意味着针对该端口的配置信息也会丢失。

可在 STP 配置之前或之后对交换机进行 Load Sharing 配置（请参照 “3.1.14 配置多端口负载均衡组”）。如果 Load Sharing 一组端口，STP 将以组内端口号最小的端口为计算单元，组内其它端口的不同配置信息将丢失，并以最小端口配置为标准进行合并。合并后 STP 以最小端口号操作 Load Sharing 组。特别地，如果原最小端口不属于任何 STP 域，合并后组内其它端口将不属于任何 STP 域。该规则通用于 STP 与端口相关的操作。

8.2.4 使能/关闭STP域

配置步骤

步骤1	config stpd <name> [enable|disable]	使能或关闭指定的STP。

注意

如果系统尚未存在任何 STP 域时，config stpd default enable 命令将自动创建名为 default 的域，并加入所有端口的相关命令，目的是兼容以前的非多域 STP 的配置。

8.2.5 配置STP域参数

一旦运行某指定 STP 的 STP 协议后，用户可能需要根据具体的网络结构调整该 STP 的参数。以下的 STP 协议参数可以在 μHammer2E/2ED/24E/24ED/2024E 交换机中调整：

- Bridge Priority
- Hello Time
- Forward Delay
- Max Age

另外每个端口上有以下参数可以调整：

- Path Cost
- Port Priority

配置步骤

步骤1	config stpd <name> priority <0-65535>	配置运行STP域的优先级。 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。
步骤2	config stpd <name> hellotime <1-10>	配置当前交换机被选为根桥时发送BPDU的时间间隔，单位为秒。
步骤3	config stpd <name> forwarddelay <4-30>	配置当前交换机被选为根桥时端口状态切换的时间间隔，单位为秒。
步骤4	config stpd <name> maxage <6-40>	配置BPDU报文老化的最长时间间隔，如果收到超过这个时间的BPDU报文，就直接丢

		弃，单位为秒。
步骤5	config stpd <name> port [<portlist>|all] priority <0-255>	配置参与STP计算的端口的优先级。 其中，<portlist>表示对指定端口进行操作；all表示对指定STP域的所有端口进行操作。 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。
步骤6	config stpd <name> port [<portlist>|all] cost <1-65535>	配置参与STP计算端口的路径开销。 其中，<portlist>表示对指定端口进行操作；all表示对指定STP域的所有端口进行操作。


注意

HelloTime 和 ForwardDelay 必须满足以下条件:

HelloTime ≤ ForwardDelay – 2

Maxage 必须满足以下条件:

2 ×（HelloTime + 1） ≤ Maxage ≤ 2 ×（ForwardDelay – 1）

8.2.6 显示STP域状态

配置步骤

步骤1	show stpd [<name>|all]	显示STP域的内容。 其中，<portlist>表示对指定端口进行操作；all表示对指定STP域的所有端口进行操作。 此命令显示的内容包括STP状态、BridgeID、Root BridgeID、STP的各种配置参数。
步骤2	show stpd <name> port [<portlist>|all]	显示端口的STP状态。 其中，<portlist>表示对指定端口进行操作，all表示对指定STP域的所有端口进行操作。 此命令显示的内容包括端口状态、Designated port、端口的各种配置参数。

8.2.7 配置调试模式

在调试模式下，可打印出 STP 域和端口的关键状态信息，以便技术人员调试和诊断网络。

配置步骤

步骤1	debug stpd	进入STP调试模式。

使用 no debug stpd 可以退出 STP 调试模式。

8.2.8 下行环路检测

如果交换机端口的下游存在不支持 STP 协议的设备，且这些不支持 STP 协议的设备的链路存在环路，则会形成广播风暴，从而影响整个网络的正常运行。针对这一问题，解决方法是对端口下游链路环路进行检测，如果检测到交换机端口的下游存在环路，则自动关闭这个端口。

配置步骤

步骤1	config loopdetect [enable| disable]	启用或关闭端口环路检测。 其中，选择enable，表示启用端口环路检测；选择disable，表示关闭端口环路检测。

如果端口下游存在环路，则最多 10s 之后，使用命令 show port <portlist> 查看该端口信息时，会发现该端口被关闭。

8.3 配置案例

8.3.1 下行环路检测

案例描述

端口 4 的下游存在环路，在启用端口环路检测功能之前使用 show port 4 命令查看到该端口的 Port State 为 Enabled。启用端口环路检测功能之后，再查看端口 4 的信息，可以看到该端口的 Port State 为 Disabled。

配置步骤

步骤1	在启用端口环路检测功能之前使用show port 4命令查看端口。
	Harbour(config)# show port 4 ----------

	Port:4 's Configuration Information Link state : Up Port state : Enabled AutoNegotiation : Enabled Speed : 100BaseTX Duplex : Full FlowControl : Disabled Port VLAN ID : 2047 Port VLAN name : default Port Description : 1234 Port Learning : Enable ----------
步骤2	启用端口环路检测功能。
	Harbour(config)# config loopdetect enable
步骤3	再查看端口4的信息。
	Harbour(config)# show port 4 ---------- Port:4 's Configuration Information Link state : Up Port state : Disabled AutoNegotiation : Enabled Speed : 100BaseTX Duplex : Full FlowControl : Disabled Port VLAN ID : 2047 Port VLAN name : default Port Description : 1234 Port Learning : Enable ----------

9 配置 RSTP

9.1 RSTP概述

RSTP（Rapid Spanning Tree Protocol）协议是依据 IEEE802.1w 标准，对 STP 802.1D 协议进行改进后的协议，它提供了网络的动态冗余切换机制，并能够在 P2P（非共享）链路上进行端口状态的快速切换。

RSTP 协议使网络设计中可以部署备份线路，并保证在主线路正常工作时，备份线路关闭；在主线路出现故障时，能自动快速地开启备份线路、切换数据流。

9.2 配置RSTP

9.2.1 缺省配置信息

μHammer2E/2ED/24E/24ED/2024E 交换机关于 RSTP 的缺省设置信息如以下表格所示：

表9-1 RSTP 表缺省配置信息

内容	缺省设置	备注
STP协议模式（spanning-tree mode）	STP	可更改设置
使能/关闭RSTP	disable	可更改设置
启用/关闭端口RSTP	启用	可更改设置
运行RSTP优先级（priority）	32768	可更改设置
发送BPDU的时间间隔（hello-time）	2秒	可更改设置
端口状态切换时间间隔（forward-delay）	15秒	可更改设置
BPDU报文老化的最长时间间隔（maximum-age）	20秒	可更改设置
参与RSTP计算的端口优先级（port priority）	128	可更改设置
STP版本（force-version）	2	可更改设置
端口P2P属性（p2p）	auto	可更改设置
端口Edge属性（edge）	no	可更改设置

9.2.2 STP模式切换

配置步骤

步骤1	config spanning-tree mode [stp|rstp]	配置模式下，切换STP协议模式。 其中，选择stp，表示进入STP协议模式；选择rstp，表示进入RSTP协议模式。
步骤2	show spanning-tree mode	配置模式下，显示当前STP协议模式。

9.2.3 使能/关闭RSTP

配置步骤

步骤1	config spanning-tree [enable|disable]	配置模式下，使能或者关闭RSTP功能。 其中，选择enable，表示启用RSTP；选择disable，表示关闭RSTP功能。

9.2.4 启用/关闭端口RSTP

配置步骤

步骤1	config spanning-tree port <port> [none-stp] [yes|no]	配置模式下，启用或者关闭端口的RSTP功能。 其中，<port>表示所要操作的端口的端口号；选择yes，表示关闭该端口的RSTP功能；选择no，表示启用该端口的RSTP功能。

9.2.5 配置RSTP参数

配置步骤

步骤1	config spanning-tree priority <0-61440>	设置交换机运行RSTP协议时的优先级。交换机优先级数值越低，越有可能成为网络中的根桥（Root Bridge）；优先级值为0代表最高的优先级；交换机的优先级数值应该是4096的倍数。
步骤2	config spanning-tree hello-time <1-10>	配置交换机发送BPDU的时间间隔，单位为秒。
步骤3	config spanning-tree forward-delay <4-30>	配置交换机端口状态切换的时间间隔，单位为秒。
步骤4	config spanning-tree maximum-age <6-40>	配置RSTP BPDU报文老化的最长时间间隔，如果收到超过这个时间的BPDU报文，

		就直接丢弃，单位为秒。
步骤5	config spanning-tree port **[<portlist>|all] priority** <0-240>	配置参与RSTP计算的端口的优先级。 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代表了最高优先级。
步骤6	config spanning-tree port **[<portlist>|all] path-cost** [auto | <1-200000000>]	配置参与RSTP计算的端口的路径开销。 用户可以自己设定端口开销，也可以选择auto，使用系统的默认设置。端口路径开销设置为auto时，由RSTP自动检测端口类型，从而决定参加RSTP计算的端口的路径开销。10Mbps端口缺省值为2000000；100Mbps端口缺省值为200000；1000Mbps端口缺省值为20000。
步骤7	config spanning-tree [force-version] [0|2]	在RSTP运算中，配置交换机运行802.1D的STP协议，向后兼容IEEE 802.1D标准规定的STP协议。 当force-version的值为2时，交换机运行RSTP协议；当force-version的值为0时，交换机运行老的STP协议。
步骤8	config spanning-tree port **[<portlist>|all]** p2p [yes | no | auto]	配置端口的P2P属性。 RSTP会自动检测端口的P2P类型。只有在P2P为真的情况下，才可能利用RSTP运算，进行端口状态的快速转移。
步骤9	config spanning-tree port **[<portlist>|all] edge** [yes|no]	配置端口的Edge属性。 当交换机的这个端口直接与主机相连，或者这个端口在不与其它交换机连接的情况下，可以设置端口的Edge属性为yes，这样可以使端口进行快速的状态转换。
步骤10	**config spanning-tree port [<portlist>|all] mcheck**	配置 RSTP 计算端口的 mcheck。 该命令强迫指定端口立即进入**RSTP**通讯状态，可以检查该端口所**LAN**网是否已经发生拓扑变化，或者对端桥已经迁移。


注意

HelloTime、MaxAge、ForwardDelay 必须满足以下关系：

2 ×（HelloTime + 1） ≤ MaxAge ≤ 2 ×（ForwardDelay – 1）

9.2.6 显示RSTP状态

配置步骤

步骤1	show spanning-tree	显示RSTP状态的内容。

		RSTP的显示内容包括BridgeID、Root BridgeID、RSTP的各种配置参数。
步骤2	show spanning-tree port <port>	显示端口RSTP状态。 其中，<port>表示指定端口的端口号。 端口的RSTP状态的显示内容包括端口状态、端口配置参数。

9.2.7 使能/关闭RSTP调试功能

配置步骤

步骤1	debug spanning-tree [bridge|rolesel] no debug spanning-tree [bridge|rolesel]	对RSTP协议和桥状态机进行调试。
步骤2	debug spanning-tree port [<portlist>|all] [info|roletrns|sttrans|topoch|migrate|transmit|p2p|edge|pcost|all] no debug spanning-tree port [<portlist>|all] [info|roletrns|sttrans|topoch|migrate|transmit|p2p|edge|pcost|all]	对RSTP协议指定端口状态机进行调试。
步骤3	debug spanning-tree port [<portlist>|all] bpdu [rx|tx|all] no debug spanning-tree port [<portlist>|all] bpdu [rx|tx|all]	打开指定端口bpdu收发调试过程。
步骤4	debug spanning-tree port [<portlist>|all] skip [rx|tx|all] <1-10000>	让指定端口跳过指定数目的bpdu报文的收发。

9.3 配置案例

案例描述

配置运行 RSTP 的优先级、发送 BPDU 时间间隔、端口状态切换时间间隔等参数。

配置步骤

步骤1	配置交换机运行RSTP协议时的优先级为8192。
	Harbour(config)#config spanning-tree priority 8192
步骤2	配置交换机发送BPDU的时间间隔为4秒。
	Harbour(config)#config spanning-tree hello-time 4
步骤3	配置交换机端口状态切换的时间间隔为10秒。
	Harbour(config)#config spanning-tree forward-delay 10
步骤4	配置RSTP BPDU报文老化的最长时间间隔为30秒。
	Harbour(config)#config spanning-tree maximum-age 30
步骤5	配置参与RSTP计算的端口10的优先级为96。
	Harbour(config)#config spanning-tree port 10 priority 96

步骤6	配置参与RSTP计算的端口10的路径开销为300000。
	Harbour(config)#config spanning-tree port 10 path-cost 300000
步骤7	配置交换机运行IEEE 802.1D STP协议。
	Harbour(config)#config spanning-tree force-version 0
步骤8	配置端口10的P2P属性为真。
	Harbour(config)#config spanning-tree port 10 p2p yes
步骤9	配置端口10的Edge属性为真。
	Harbour(config)#config spanning-tree port 10 edge yes

10 配置 IGMP Snooping

本章主要介绍 IGMP Snooping 的相关概念，以及如何配置 IGMP Snooping。

10.1 概述

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 用来监听主机与路由器之间的 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。

10.2 配置IGMP Snooping

10.2.1 缺省配置信息

μHammer2E/2ED/24E/24ED/2024E 交换机关于 IGMP Snooping 的缺省设置信息如以下表格所示：

表10-1 IGMP Snooping 缺省配置信息

内容	缺省设置	备注
路由器端口的超时时间间隔（router_timeout）	260秒	可更改设置
主机端口的超时时间间隔（host_timeout）	260秒	可更改设置
收到离开报文的端口被删除的延迟时间（immediate-leave enable time）	10秒	可更改设置

10.2.2 使能/关闭IGMP Snooping

配置步骤

步骤1	config igmp-snooping [enable|disable]	配置模式下，使能或关闭IGMP Snooping。 其中，选择enable，表示启动IGMP Snooping；选择disable，表示关闭IGMP Snooping。


注意

当系统中已存在相应的静态 IP 多播地址时，IGMP-SNOOPING 的动态多播地址将创建失败。

10.2.3 配置IGMP Snooping时钟

配置步骤

步骤1	config igmp-snooping router_timeout <10-2147483>	配置路由器端口的超时时间间隔。 其中，router_timeout表示要调整的是路由器端口的时间间隔；<10-2147483>表示调整后路由器端口的时间间隔范围，默认值为260秒。
步骤2	config igmp-snooping host_timeout <10-2147483>	配置主机端口的超时时间间隔。 其中，host_timeout表示要调整的是主机端口的时间间隔；<10-2147483>表示调整后的主机端口的时间间隔范围，默认值为260秒。

10.2.4 清除IGMP Snooping 信息

配置步骤

步骤1	clear igmp-snooping vlan [<name>|all]	配置模式下，清除某个VLAN中的组成员。 其中，选择<name>，表示清除指定名称的VLAN；选择all，表示清除所有VLAN中的组成员。


注意

使用创建静态组播 FDB 命令会自动替换已存在的动态多播组。

10.2.5 使能/关闭IGMP Snooping立即离开功能

当组中的一个成员离开时立即将消息发送给 IGMP Snooping 路由器，使其立即离开，该功能适用于对快速离开要求严格的地方。

使能 IGMP Snooping 立即离开功能

配置步骤

步骤1	config igmp-snooping immediate-leave enable {time <0-600>}*1	启用IGMP Snooping立即离开功能。 其中，time设定收到离开报文的端口被删除的延迟时间，默认是10秒。

关闭 IGMP Snooping 立即离开功能

配置步骤

步骤1	config igmp-snooping immediate-leave disable	关闭IGMP Snooping立即离开功能。

10.2.6 配置静态路由器端口

静态路由器端口不会动态超时被删除，一直存在，直至停止 IGMP Snooping 功能或被手工删除。

添加静态路由器端口

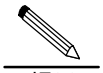
配置步骤

步骤1	config igmp-snooping router_port add <portlist> vlan <name>	添加静态路由器端口。 其中，<portlist>表示端口列表；<name>表示VLAN的名字。

删除静态路由器端口

配置步骤

步骤1	config igmp-snooping router_port delete <portlist> {vlan <name>}*1	删除静态路由器端口。 其中，<portlist>表示端口列表；<name>表示VLAN的名字。


提示

最多只能设置 32 个路由端口。

10.2.7 配置路由端口

配置是否添加路由端口到组播组。

命令格式 **config igmp-snooping add-router-port [enable|disable]**

命令模式 配置模式

语法描述

关键字和参数	说明
enable|disable	使能或关闭

默认状态 该命令的默认设置为 enable。

使用指导 如果一台交换机设备上有多个路由端口，则可以禁止将路由端口加入各个组播组，避免一个路由端口的组播组流量传递到另外的路由端口中。

最好在开启 igmp snooping 之前配置该命令。

配置实例 禁止将路由端口加入各个组播组：

```
Harbour(config)#config igmp-snooping add-router-port disable
```

10.2.8 显示IGMP Snooping多播组成员信息

配置步骤

步骤1	show igmp-snooping vlan <name>	配置模式下，显示指定VLAN中或所有VLAN中的组成员信息。 其中，<name>为指定VLAN的名称，当<name>为all时，表示所有的VLAN。

10.2.9 显示IGMP Snooping摘要信息

配置步骤

步骤1	show igmp-snooping summary	显示路由器端口的统计信息和所有的组成员个数。立即离开功能是否打开及其延迟时间等。

10.2.10 使能/关闭IGMP Snooping调试功能

使能 IGMP Snooping 调试功能

配置步骤

步骤1	debug igmp-snooping	进入IGMP Snooping的调试模式。

关闭 IGMP Snooping 调试功能

配置步骤

步骤1	no debug igmp-snooping	退出IGMP Snooping的调试模式。

显示 IGMP Snooping 调试功能是否打开

配置步骤

步骤1	show debug igmp-snooping	显示IGMP Snooping的调试功能是否打开；

10.3 配置案例

10.3.1 配置IGMP Snooping时钟

案例描述

配置接口的 router_timeout 为 500 秒，host_timeout 为 600 秒。

配置步骤

步骤1	配置接口的router_timeout为500秒。

	Harbour(config)#config igmp-snooping router_timeout 500
步骤2	配置接口的host_timeout为600秒。
	Harbour(config)#config igmp-snooping host_timeout 600

10.3.2 显示IGMP Snooping摘要信息

案例描述

显示 IGMP Snooping 摘要信息。

配置步骤

步骤1 显示IGMP Snooping摘要信息。

```
Harbour(config)# show igmp-snooping summary
                ----------IGMP-SNOOPING Summary----------

                router time-out(s)                    260
                host time-out(s)                      260
                igmp_snooping group                     0
                igmp_snooping router                    1
                immediate leave                       enable
                immediate leave time-out(s)           20

                router port     vlan          vid       time-out
                ------------------------------------------------
          2     default         2047          Fixed
```

11 配置日志模块

本章主要介绍日志模块（Syslog）的相关内容，以及如何配置日志模块。

11.1 日志模块概述

日志模块（Syslog）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。日志信息可以在终端 monitor 显示，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 server，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。

11.2 配置日志模块

11.2.1 缺省配置信息

μHammer2E/2ED/24E/24ED/2024E 交换机关于日志模块的缺省设置信息如以下表格所示：

表11-1 日志模块缺省配置信息

内容	缺省设置	备注
使能/关闭保存syslog信息功能（memory-record）	enable	可更改设置

11.2.2 使能/关闭日志服务

配置步骤

步骤1	config syslog [enable|disable]	配置模式下，打开或关闭日志服务功能。其中，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。

11.2.3 配置日志信息类型

配置步骤

步骤1	config syslog type [<name>|all] [enable|disable]	配置模式下，配置日志模块是否对某一类型的日志信息进行记录。 其中，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；<name>为系统中支持的日志类型；all代表以上支持的所有日志类型。

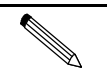

提示

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，PORT，RADIUS，ROUTE，SNMP，STP，SYSTEM，VLAN，WEB，IGMPSNP，HLINK，MACLIMI 等。

11.2.4 配置日志信息最低级别

配置步骤

步骤1	config syslog lowest-level <0-7>	配置模式下，配置日志模块对某一级别和该级别以上的日志信息进行记录。


提示

目前支持的日志信息级别从 0 到 7，依次为 EMERG、ALERT、CRIT、ERR、WARNING、NOTICE、INFO、DEBUG。

11.2.5 使能/关闭记录命令行操作日志功能

配置步骤

步骤1	record command-line [enable|disable]	配置模式下，配置日志模块是否对命令行操作行为进行日志记录。 其中，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。命令行操作的日志信息级别

	为6，即INFO类型。

11.2.6 使能/关闭保存日志到日志服务器功能

配置步骤

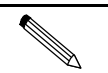
步骤1	config syslog server [enable|disable]	配置模式下，配置日志模块是否保存日志信息到日志服务器。 其中，选择enable，表示保存日志信息到服务器；选择disable，表示不保存日志信息到服务器。

在配置之前，保证日志服务器服务程序已启动。

11.2.7 增加/删除日志服务器

配置步骤

步骤1	config syslog [add|delete] server <A.B.C.D> {[port] <1-65535>}*1 {[facility] <0-7>}*1	配置模式下，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。 其中，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>表示是日志服务器server的IP地址；port表示是日志服务器上接收日志进程的服务端口号；facility表示是日志信息保存到日志服务器的文件索引号。

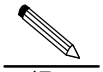


可以使用一条命令配置日志服务器信息，也可以使用多条子命令进行配置。关于日志服务器服务程序的配置详见相关手册。

11.2.8 使能/关闭终端显示日志功能

配置步骤

步骤1	config syslog monitor-terminal [enable|disable]	配置模式下，配置日志信息是否输出到用户终端。 其中，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。

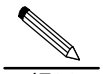


该命令是服务命令，将对所有终端起作用。

11.2.9 使能/关闭当前终端显示日志功能

配置步骤

步骤1	monitor [on|off]	配置模式下，决定是否在当前终端输出日志信息。 其中，选择on，表示允许在当前终端输出日志信息；选择disable，表示不允许在当前终端输出日志信息。



该命令只对当前终端起作用。

11.2.10 配置是否显示时间信息

配置步骤

步骤1	monitor timestamp [none|time|datetime]	配置模式下，配置是否在当前终端输出时间信息。

11.2.11 配置终端显示日志最低级别

配置步骤

步骤1	monitor lowest-level <0-7>	配置模式下，配置在当前终端输出某级别和该级别以上的日志信息。


提示

该命令只对当前终端起作用，目前支持的日志信息级别从 0 至 7，依次为 EMERG 、ALERT 、CRIT、ERR、WARNING、NOTICE、INFO、DEBUG。

11.2.12 配置终端显示日志类型

配置步骤

步骤1	monitor type [<typename>|all] [on|off]	配置模式下，配置当前终端输出某一类型的日志信息。 其中，<typename>表示系统中支持的日志类型；all代表以上支持的所有日志类型。


提示

该命令只对当前终端起作用。

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，PORT，RADIUS，ROUTE，SNMP，STP，SYSTEM，VLAN，WEB，IGMPSNP，HLINK，MACLIMI 等。

11.2.13 使能/关闭保存syslog信息功能

配置步骤

步骤1	config syslog memory-record [enable|disable]	配置模式下，配置是否启用保存syslog信息的功能。 其中，选择enable表示启用；选择disable表示停用。缺省状态下，为enable状态。

11.2.14 显示日志模块配置信息

配置步骤

步骤1	show syslog configuration	配置模式下，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。


提示

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。

11.2.15 显示终端日志显示属性配置信息

配置步骤

步骤1	show monitor configuration	配置模式下，配置在当前终端显示的日志类型、日志级别以及时间信息等。


提示

该命令只对当前终端起作用。

11.2.16 显示系统当前syslog信息

配置步骤

步骤1	show syslog	只读模式下，显示系统当前的syslog信息

11.2.17 显示系统重启前syslog信息

配置步骤

步骤1	show syslog history	只读模式下，显示系统重启之前的syslog信息。

11.3 配置案例

11.3.1 配置日志服务

案例描述

打开日志服务功能，注册 AUTH 类型的日志信息，配置所要记录日志信息的最低级别为 3。

配置步骤

步骤1	打开日志服务功能。
	Harbour(config)# config syslog enable Successfully changed syslog service to enable
步骤2	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。
	Harbour(config)# config syslog type auth enable Successfully changed syslog type auth to enable.
步骤3	配置所要记录日志信息的最低级别为3。级别3和级别3以上（即级别0－3）的日志信息将被记录。
	Harbour(config)# config syslog lowest-level 3 Successfully changed syslog service lowest-lever level 3 [ERR].

11.3.2 增加/删除日志服务器

案例描述

配置 IP 地址为 10.12.3.4 的日志服务器，服务端口为 8808，facility 为 5，删除 IP 地址为 10.1.4.1 的日志服务器，服务端口为 6500，facility 为 1。

配置步骤

步骤1	配置IP地址为10.12.3.4的日志服务器，服务端口为8808，facility 为5。
	Harbour(config)# config syslog add server 10.12.3.4 port 8808 facility 5 Successfully added syslog server 10.12.3.4.
步骤2	删除IP地址为10.1.4.1的日志服务器，服务端口为6500，facility为1。
	Harbour(config)# config syslog delete server 10.1.4.1 port 6500 facility 1 Successfully deleted syslog server 10.1.4.1

12 配置 NMS

本章主要介绍网络管理服务 NMS（Net Manage Service）的内容和相关知识，以及如何配置 NMS。

12.1 NMS概述

NMS（Net Manage Service）是从安全角度出发，在原有访问控制基础上增加的新的控制，即不仅需要合法的用户名和密码，还需要通过检查来访者的 IP 来确定来访者是否有访问权限。只有通过合法的 IP 访问才可以建立连接，连接之后进一步检查用户名和密码，只有全部通过以后才可以访问和配置交换机。

例如，管理员 A 管理交换机 B。A 有合法的用户名和密码，工作地点在某机房，IP 网段为 10.1.0.* ；B 的访问控制配置有 A 的用户名、密码和 IP 网段。如果 A 以合法的 IP 访问，使用合法的用户名和密码，则 B 接受 A 访问；如果 A 在其它地方，以非法的 IP 访问，则 B 拒绝 A 访问。

12.2 配置NMS

访问 μHammer2E/2ED/24E/24ED/2024E 交换机有多种方式：Console、Telnet、SNMP、Web 等。对于采用 Telnet、SNMP、Web 的访问，可以通过相应的访问控制命令进行配置，以加强对交换机访问控制的管理。

配置交换机的访问控制，必须先创建一个 NMS 访问控制组（nms-access-profile），然后配置这个组具有上述某种访问方式，再配置每个组包含的 IP 和 IP 网段。

12.2.1 缺省配置信息

μHammer2E/2ED/24E/24ED/2024E 交换机关于 NMS 的缺省设置信息如以下表格所示：

表12-1 NMS 缺省配置信息

内容	缺省设置	备注
访问控制组Web访问方式	disable	可更改设置
访问控制组telnet访问方式	enable	可更改设置
访问控制组SNMP访问方式	disable	可更改设置

12.2.2 启用/禁止访问控制服务

配置步骤

步骤1	config access-control {[telnet|web|snmp]}*1 [on|off]	启用或禁止访问控制服务。 其中，选择[telnet|web|snmp]，表示对其中的一种服务进行操作，不选择这个参数，表示将对三种服务同时进行操作；选择on，表示允许进行访问控制，只有在这种情况下，才能激活NMS的配置文件；选择off，表示禁止访问控制，此时被禁止进行访问控制的服务将始终处于enable状态，这种情况下，以上的NMS配置不生效。

12.2.3 创建访问控制组

配置步骤

步骤1	create nms-access-profile <access_profile_name>	配置模式下，创建一个访问控制组。 其中，<access_profile_name>表示要创建的访问控制组的组名。

12.2.4 删除访问控制组

配置步骤

步骤1	delete nms-access-profile <access_profile_name>	配置模式下，删除一个访问控制组。 其中，<access_profile_name>表示要创建的访问控制组的组名。

12.2.5 配置访问控制组访问方式

每个访问控制组都可以选择三种访问方式：Web，telnet，SNMP。用户可分别对这

三种访问方式加以启用或禁止。

启用/禁止访问控制组的 telnet 访问方式

配置步骤

步骤1	config nms-access-profile <access_profile_name> telnet [enable|disable]	启用/禁止访问控制组的telnet访问方式。 其中，<access_profile_name>表示已经创建的访问控制组的组名；选择enable，表示允许该组中的用户使用telnet服务；选择disable，表示禁止profile中的用户使用telnet服务。

启用/禁止访问控制组的 Web 访问方式

配置步骤

步骤1	config nms-access-profile <access_profile_name> web [enable|disable]	启用/禁止访问控制组的Web访问方式。 其中，<access_profile_name>，表示已经创建的访问控制组的组名；选择enable，表示允许该组中的用户使用Web服务；选择disable，表示禁止profile中的用户使用Web服务。

启用/禁止访问控制组的 SNMP 访问方式

配置步骤

步骤1	config nms-access-profile <access_profile_name> snmp [enable|disable]	启用/禁止访问控制组的SNMP访问方式。 其中，<access_profile_name>，表示已经创建的访问控制组的组名；选择enable，表示允许该组中的用户使用SNMP服务；选择disable，表示禁止profile中的用户使用SNMP服务。

12.2.6 配置访问控制组包含的IP地址

添加访问控制组包含的 IP 地址

配置步骤

步骤1	config nms-access-profile <access_profile_name> add ipaddress <A.B.C.D/M> 或者 config nms-access-profile <access_profile_name> add	配置模式下，向某个访问控制组中添加IP地址。 其中，<access_profile_name>表示某个访问控制组的组名；第一个<A.B.C.D>表示主机的IP地址；/M和<A.B.C.D>是子网掩码的两种表示方法， <A.B.C.D>是用IP地址形

	ipaddress <A.B.C.D> <A.B.C.D>	式表示的子网掩码，/M是用数字方式表示的子网掩码，这两种形式的掩码可以任选其一。

删除访问控制组包含的 IP 地址

配置步骤

步骤1	config nms-access-profile <access_profile_name> delete ipaddress <A.B.C.D> <A.B.C.D> 或者 config nms-access-profile <access_profile_name> delete ipaddress [all |<A.B.C.D/M>]	配置模式下，向某个访问控制组中删除IP地址。 其中，<access_profile_name>表示某个访问控制组的组名；第一个<A.B.C.D>表示主机的IP地址；/M和<A.B.C.D>是子网掩码的两种表示方法， <A.B.C.D>是用IP地址形式表示的子网掩码，/M是用数字方式表示的子网掩码，这两种形式的掩码可以任选其一。

12.2.7 查看访问控制组状态

配置步骤

步骤1	show nms-access-profile {<access_profile_name>}*1	配置模式下，查看某个访问控制组的状态。 其中，<access_profile_name>表示显示指定访问控制组的状态，如果不选择此参数，表示显示所有访问控制组的状态。

12.3 配置案例

案例描述

配置两个访问控制组，分别名为 group1 和 group2，其中禁止 group1 的 telnet 访问方式，允许 group2 的 telnet 访问方式，向 group1 添加属于 10.10.10.1/24 网段的 IP 地址，向 group2 添加属于 10.10.10.1/16 网段的 IP 地址。

配置步骤

步骤1	配置两个访问控制组，分别名为group1和group2，其中禁止group1的telnet访问方式，允许group2的telnet访问方式。

	Harbour(config)# create nms-access-profile group1 Harbour(config)# create nms-access-profile group2 Harbour(config)# config nms-access-profile group1 telnet disable Harbour(config)# config nms-access-profile group2 telnet enable
步骤2	向group1添加属于10.10.10.1/24网段的IP地址，向group2添加属于10.10.10.1/16网段的IP地址。由于group2中的网段包括group1中的网段，则属于group1中的IP不能够telnet到交换机，属于group2但不属于group1的IP可以telnet到交换机。
	Harbour(config)#config nms-access-profile group1 add ipaddress 10.10.10.1/24 Harbour(config)#config nms-access-profile group2 add ipaddress 10.10.10.1/16

注意

本章讨论的前提都是以在交换机中已经打开相应的服务为前提的。

打开或者关闭指定的服务，使用以下命令:

service [snmp|webserver|telnet] [enable|disable]。

当访问控制服务打开时，一个 IP 能否 telnet 到交换机，首先查看配置组中是否有该 IP 地址。如果有，则取该配置组的 telnet 许可权限；如果没有，则查看 IP 是否在某个子网中，并取其相应的权限，优先取最小子网的权限。如果配置组中没有该 IP 地址，则该 IP 无法 Telnet 到交换机上。

13 配置 SNTP

本章主要介绍 SNTP（Simple Network Time Protocol）协议的相关概念，以及如何配置 SNTP 协议。

13.1 概述

简单网络时间协议 SNTP（Simple Network Time Protocol）是网络时间协议（NTP）的一个简化版本。NTP 协议适用于同步因特网上的设备时钟。在不需要实现 NTP 完全功能的情况下，可以使用 SNTP，它与 NTP 的功能相同，只是比 NTP 更加简单。SNTP 采用客户端/服务器的运行方式，既可以在单播模式（点对点）下操作，也可以在广播模式（点对多点）下操作。在网络设备中运行 SNTP 协议有利于设备的管理和维护。

13.1.1 SNTP工作模式

SNTP 协议在维护网络设备的时间时有三种不同的工作模式：

- 单播模式（Unicast）

客户端向指定的服务器发出包含本地时间的请求报文，服务器返回响应报文，响应报文中含有服务器接收到的客户端请求报文的时间和服务器发出响应报文的时间。客户端收到服务器的响应报文后，通过报文中包含的各种时间值，可以计算出报文的循环周期以及本地设备时间值与服务器时间值的偏差。

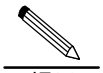
- 多播模式（Multicast）

服务器周期性的广播自己的时间值。客户端在接收到广播报文后，修改自己的时间值，以和服务器广播报文中的时间值一致。

- 单播/多播模式（Anycast）

当客户端不知道时间服务器的地址时采用这种方式，即客户端向指定的网络发出多播或广播请求报文，网络中的服务器在收到广播请求报文后，都以单播的方式响应客户端，但客户端只接收最先收到的响应报文，并记录下此服务器的地址，之后，

客户端和此服务器便工作在单播模式下。


提示

单播模式（Unicast）适用于作为 SNTP 客户端的交换机与因特网中 SNTP 服务器之间的通信;
多播模式（Multicast）和单播/多播模式（Anycast）适用于两台交换机（如两台 μHammer24E 交换机）之间的 SNTP 通信，其中一台作为 SNTP 客户端，另一台作为 SNTP 服务器。

13.1.2 SNTP配置规则

配置 SNTP 时，需要遵循一定的标准规范。配置规则如下：

- 工作模式：SNTP 协议支持三种工作模式，即单播模式（Unicast）、多播模式（Multicast）、单播/多播模式（Anycast）；缺省值为单播模式（Unicast）；
- 客户端的时间刷新频率：客户端每隔多长时间向服务器发送一次时间请求报文；
- 时间服务器的 IP 地址：当 SNTP 工作在单播模式（Unicast）下时，需要配置时间服务器的 IP 地址，以便客户端能和指定的服务器进行通信；
- 时间服务器的广播周期：当 SNTP 工作在多播模式（Multicast）下时，服务器周期性的广播自己的时间值，因此需要配置时间服务器的广播周期；
- 地方时区的调整：系统时钟内的时间值为国际标准时间，可以通过设置系统时区，使得显示的时间为当地时间。

13.2 配置SNTP客户端

13.2.1 缺省配置信息

μHammer2E/2ED/24E/24ED/2024E 交换机关于 SNTP 客户端的缺省设置信息如以下表格所示：

表13-1 SNTP 客户端缺省配置信息

内容	缺省设置	备注
SNTP客户端的缺省状态	关闭	可更改设置
SNTP客户端刷新周期（update-interval）	64秒	可更改设置

13.2.2 配置SNTP客户端工作模式

SNTP 的工作模式包括客户端工作模式和服务器工作模式。在运行 SNTP 客户端之前必须完成 SNTP 客户端工作模式的配置，SNTP 客户端启动后，不能修改工作模式。

配置步骤

步骤1	config sntp-client mode <1-3>	配置模式下，配置SNTP客户端工作模式。 其中，<1-3>表示相应的客户端工作模式，1表示单播模式（Unicast），2表示多播模式（Multicast），3表示单播/多播模式（Anycast）。

13.2.3 使能/关闭SNTP客户端

配置步骤

步骤1	config sntp-client [enable|disable]	配置模式下，启用或关闭SNTP客户端。 其中，选择enable，表示启用SNTP客户端；选择disable，表示关闭SNTP客户端。


注意

启动 SNTP 客户端以前，必须先配置 SNTP 客户端的工作模式和 SNTP 服务器的 IP 地址。

由于一台交换机不能同时担任 SNTP 客户端和 SNTP 服务器，所以在交换机上启用 SNTP 客户端时，必须令其 SNTP 服务器的状态为 disable。

13.2.4 配置客户端SNTP服务器IP地址

当 SNTP 客户端工作在单播模式（Unicast）下时，启动 SNTP 客户端之前，一定要先配置 SNTP 服务器的 IP 地址。

配置步骤

步骤1	config sntp-client server ipaddress <A.B.C.D>	配置模式下，指定SNTP客户端对应的SNTP服务器的IP地址。 其中，<A.B.C.D>表示SNTP服务器的IP地址。

13.2.5 配置SNTP客户端刷新周期

当客户端工作在单播/多播模式（Anycast）或单播模式（Unicast）下时，需要配置客户端的时间刷新周期，即配置客户端每隔多长时间向服务器端发送一次时间请求报文。

配置步骤

步骤1	config sntp-client update-interval <64-1024>	配置模式下，配置SNTP客户端刷新周期。其中，<64-1024>表示SNTP客户端的刷新周期范围，单位为秒。

13.2.6 显示SNTP客户端状态信息

配置步骤

步骤1	show sntp-client	配置模式下，显示SNTP客户端的状态信息。 此命令显示的SNTP客户端的信息包括以下内容：客户端的工作模式、时间服务器的IP地址、时间请求的发送间隔、SNTP是否启动。

13.3 配置SNTP服务器

13.3.1 缺省配置信息

μHammer2E/2ED/24E/24ED/2024E 交换机关于 SNTP 服务器的缺省设置信息如以下表格所示：

表13-2 SNTP 服务器缺省配置信息

内容	缺省设置	备注
SNTP服务器的缺省状态	关闭	可更改设置
SNTP服务器广播周期（broadcast-interval）	64秒	可更改设置

13.3.2 配置SNTP服务器工作模式

SNTP 的工作模式包括客户端工作模式和服务器工作模式。在运行 SNTP 服务器之

前必须完成 SNTP 服务器工作模式的配置，SNTP 服务器启动后，不能修改工作模式。

配置步骤

步骤1	config sntp-server mode <1-3>	配置模式下，配置SNTP服务器工作模式。 其中，<1-3>表示相应的客户端工作模式，1表示单播模式（Unicast），2表示多播模式（Multicast），3表示单播/多播模式（Anycast）。

13.3.3 使能/关闭SNTP服务器

配置步骤

步骤1	config sntp-server [enable|disable]	配置模式下，启用或关闭SNTP服务器。 其中，选择enable，表示启用SNTP服务器；选择disable，表示关闭SNTP服务器。


注意

启动 SNTP 服务器以前，必须先配置 SNTP 的工作模式。

13.3.4 配置SNTP服务器广播周期

当 SNTP 服务器工作在多播模式（Multicast）下时，服务器以一定的周期在指定的网络中广播自己的时间值。

配置步骤

步骤1	config sntp-server broadcast-interval <64-1024>	配置模式下，配置SNTP服务器的广播周期。 其中，<64-1024>表示SNTP服务器的广播周期范围，单位为秒。

13.3.5 显示SNTP服务器状态信息

配置步骤

步骤1	show sntp-server	配置模式下，显示SNTP服务器的状态信息。

	此命令显示的SNTP服务器的信息包括以下内容：服务器端的工作模式、服务器的时间广播周期。

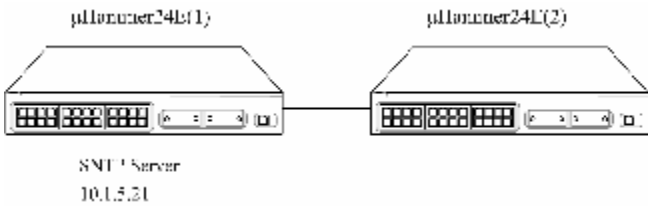
13.4 配置案例

案例描述

单播模式（Unicast）适用于交换机与因特网中的 SNTP 客户端或服务器进行 SNTP 通信；如果在两台交换机之间进行 SNTP 通信，其中一台是客户端，另一台是服务器，则选择多播模式（Multicast）或者单播/多播模式（Anycast）。如果在两台交换机之间进行 SNTP 通信，其中一台交换机的 SNTP 工作模式为多播模式（Multicast）时，另一台交换机也必须配置为多播模式（Multicast）；当作为 SNTP 客户端的交换机的工作模式为单播/多播模式（Anycast）t 时，作为 SNTP 服务器的交换机的工作模式可以是单播模式（Unicast），也可以是单播/多播模式（Anycast）。

下面以两台 μHammer24E 交换机为例，介绍 SNTP 协议的配置应用方法。

图13-1 SNTP 协议配置应用示例



配置步骤

步骤1	在μHammer24E（1）交换机上创建一个时间服务器，使其工作在Anycast模式下。
	Harbour(config)# config sntp-server mode 3 Harbour(config)# config sntp-server enable
步骤2	然后在需要同步时间的μHammer24E（2）交换机上进行配置。
	Harbour(config)# config sntp-client mode 3 Harbour(config)# config sntp-client server ipaddress 10.1.5.21 Harbour(config)# config sntp-client enable
步骤3	为了适应不同的精确性要求，用户也可以修改交换机的时间刷新频率。例如把时间刷新周期调整到100秒。
	Harbour(config)# config sntp-client update-interval 100

14 配置 LLDP

本章主要介绍 LLDP（Link Layer Discovery Protocol）的相关概念，以及如何配置 LLDP 协议。

14.1 LLDP概述

链路层邻居发现协议 LLDP（Link Layer Discovery Protocol）是链路层协议，解决了连接在同一设备上的所有节点之间的存活关系问题。具体来说，LLDP 协议定义了解决如下问题的机制：

- 设备发现：交换机如何发现与自身连接的是何种设备；
- 参数发现：交换机如何发现与自身连接的设备的有关参数，如邻接设备的设备类型、硬件版本、软件版本、邻接端口、邻接端口状态、IP 地址、MAC 地址、转发功能。


提示

通过 LLDP 协议得到的各种地址信息都有一定的生存时限，这些生存时限是由这些信息的发送者规定的，在某些动态的、经常变化的环境中是非常重要的。例如，在移动设备存在的情况下，就需要由移动设备决定与其相关的一些信息的生存时限。

14.2 配置LLDP

14.2.1 缺省配置信息

μHammer2E/2ED/24E/24ED/2024E 交换机关于 LLDP 的缺省设置信息如以下表格所示：

表14-1 LLDP 缺省配置信息

内容	缺省设置	备注
LLDP的缺省状态	启用	可更改设置
LLDP报文发送周期（lldp hello－time）	30秒	可更改设置
LLDP报文生存时间（lldp hold－time）	150秒	可更改设置

14.2.2 启用/关闭LLDP

配置步骤

步骤1	lldp run	启用LLDP功能。

使用 no lldp run 可以关闭 LLDP 功能。

14.2.3 配置LLDP报文发送周期

配置步骤

步骤1	config lldp hello－time <1-149>	配置模式下，配置LLDP报文的发送周期HelloTime。 其中，<1-149>表示HelloTime，单位为秒。

14.2.4 配置LLDP报文生存时间

配置步骤

步骤1	config lldp hold－time <31-65535>	配置模式下，配置LLDP报文的生存时间HoldTime。 其中，<31-65535>表示HoldTime，单位为秒。


注意

HoldTime 必须大于 HelloTime，并且最好满足以下条件：

HoldTime = n × HelloTime+1

14.2.5 显示LLDP配置参数

配置步骤

步骤1	show lldp	显示LLDP配置参数。 此命令显示LLDP配置参数，包括LLDP的版本信息、LLDP报文的发送周期HelloTime、LLDP报文的生存时限HoldTime。

14.2.6 显示LLDP报文流量

配置步骤

步骤1	show lldp traffic	显示LLDP报文流量。 此命令显示LLDP报文流量，包括发送报文个数、接收报文个数、错误报文个数。

14.2.7 显示LLDP邻居信息

配置步骤

步骤1	show lldp neighbors	显示LLDP收集到的邻居信息。 此命令显示LLDP收集到的邻居信息，包括邻接设备的设备类型、MAC地址。

14.2.8 显示LLDP详细邻居信息

配置步骤

步骤1	show lldp neighbors <index> detail	显示LLDP收集到的详细邻居信息。 其中，<index>表示邻居设备的编号。 此命令显示LLDP收集到的详细邻居信息，包括邻接设备的设备类型、硬件版本、软件版本、邻接端口、邻接端口状态、IP地址、MAC地址、转发功能。

14.2.9 显示LLDP邻居细节

配置步骤

步骤1	show lldp entry all	显示LLDP所有的邻居细节。

14.3 配置案例

案例描述

配置 LLDP 的 HelloTime 为 60 秒，配置 LLDP 的 HoldTime 为 100 秒。

配置步骤

步骤1	配置LLDP的HelloTime为60秒。
	Harbour(config)# config lldp hello－time 60
步骤2	配置LLDP的HoldTime为100秒。
	Harbour(config)# config lldp hold－time 100

15 利用 Web 管理交换机

本章主要介绍如何利用 Web 管理并配置交换机。

15.1 概述

HammerOS 提供了使用 Web 方式来管理交换机的功能，主要功能包括身份验证、设备配置管理、配置系统信息、保存配置信息、升级 OS 及配置文件跟以及退出登录。通过 Web 可非常直观地对交换机进行管理。

Web 功能管理包含以下模块：

- 设备管理
- 用户管理
- 系统信息
- 保存配置
- 升级 OS 及配置文件
- 退出登录

15.2 登录

15.2.1 登录Web界面

要使用 Web 页面进行交换机管理或进行交换机配置浏览，需要确认以下条件：

- IP 地址配置已完成；
- Web 服务已打开。

在 Web 浏览器中输入交换机缺省配置的 IP 地址后，链接到交换机，将看到欢迎界面。可选择中文或者英文进入系统配置。选择中文时，将看到如下图所示界面：

图15-1 登录 Web 界面

HammerOS 中提供了两种用户权限，即普通用户权限和管理员权限。与此对应，对 HammerOS 来说就有两种模式，即只读模式和配置模式。在只读模式下，用户只能对系统信息进行读操作，而不能进行配置信息的修改操作；在配置模式下，用户可以对交换机信息进行各种系统配置。以普通用户身份登录的用户只能进入只读模式，而不能进入配置模式；只有以系统管理员身份登录的用户才能进入配置模式。

15.2.2 登录身份

系统缺省内置了一个用户账号，此用户账号是管理员账号，用户名是 admin，缺省密码是 harbour。缺省用户 admin 的账号不能被删除，用户名也不能被修改，只能修改密码。如果用户选择的登录身份是系统管理员，还需要在管理密码栏中输入密码。输入完毕之后点击“登录”，即可登录，如果输入错误可点击“清除”，清除并重新输入。

以系统管理员身份登录：

- 用户名：admin
- 登录密码：harbour
- 登录身份：系统管理员
- 管理密码：harbour

单击“登录”后，出现如下图所示界面：

图15-2 设备管理

此时能够以系统管理员的身份对交换机进行管理配置。

15.3 IP地址管理

图15-3 IP 地址管理

在以系统管理员身份登录交换机后，点击“设备管理”栏中的 IP 地址，出现如上图所示界面。如果需要更改 IP 地址，点击“YES”后，输入要配置的 IP 地址和子网掩码，点击“确定”，就可以完成交换机 IP 地址的配置。

15.4 配置端口

HammerOS 可以对端口进行以下几种配置：

- 启用/禁用指定端口；
- 打开/关闭指定端口的自适应功能；
- 配置端口速率；
- 配置端口的半双工/全双工模式；
- 配置端口的流控；
- 配置端口的缺省 VLAN（VLAN 多模模式下）。

成功登录后，选择屏幕上“设备管理”菜单栏，再单击左侧“设备管理”窗口下的端口，可以看到如下图所示界面。该交换机面板显示了当前的端口状态：

- 绿色，表示该端口当前是启用状态并且链路已连接；
- 灰色，表示该端口当前是启用状态但无链路连接；
- 黄色，表示该端口当前管理状态已关闭。

图15-4 端口状态显示

对端口进行配置，单击面板上的相应端口就会有相应的表格显示，如图 15-5 为端口 1 的配置信息，并且可以对该端口进行配置，包括管理状态、自适应、双工、MAC 地址学习、速率、流控、缺省 VLAN（VLAN 多模模式下）。其中，只有当关闭自适应功能时，才可以配置端口的双工、速率和流控。

在下图所示界面中选择所需要的配置后，单击“应用修改”即可。

图15-5 端口配置信息

此外，还能够显示端口其它属性，比如所属虚拟子网、所属负载均衡组、所属生成树协议域、统计的信息等。

通过单击其它端口可以获取特定端口的相关信息。

注意

在配置端口的双工及速率时要关闭自适应功能。

15.5 配置VLAN

15.5.1 VLAN配置标准

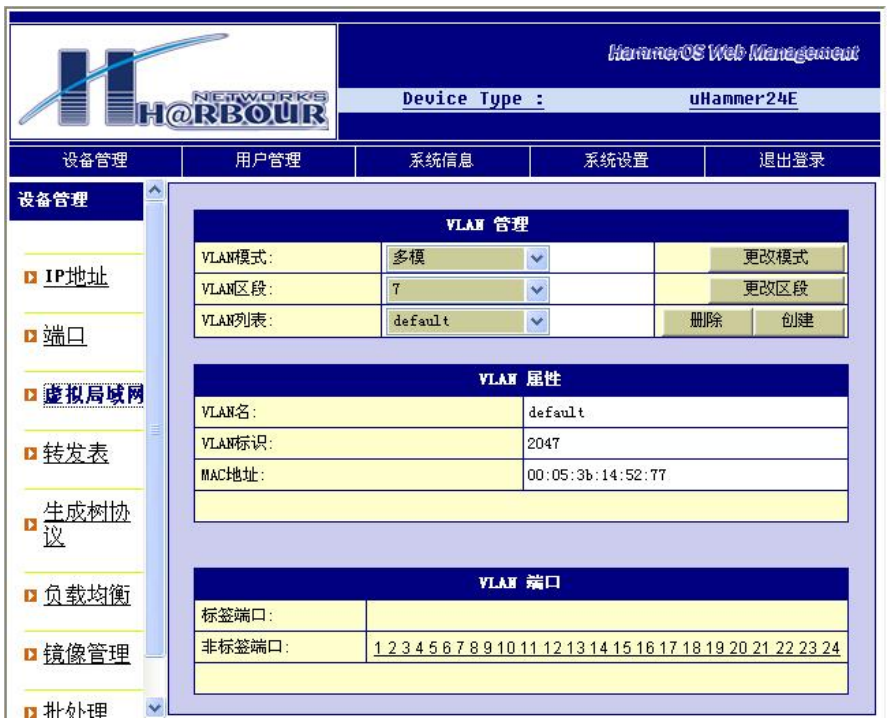
交换机最多支持 256 个 VLAN。用户可以根据以下标准创建 VLAN：

- 物理端口
- 802.1Q tag
- 以上标准的组合

15.5.2 Web中VLAN的配置

在主控制界面左侧“设备管理”链接栏中，单击“虚拟局域网”，进入虚拟局域网 VLAN 界面。如下图所示。图中，VLAN 端口列表中显示属于该 VLAN 的端口。点击相应端口，将显示该端口的信息。另外，在该 Web 界面中还提供了创建 VLAN、删除 VLAN、更改特定 VLAN 属性的功能。

图15-6 配置 VLAN



查看 VLAN 配置

在 VLAN 列表的下拉菜单中选择所要进行操作的 VLAN 名，下面的表格将显示相应 VLAN 的配置情况。如上图显示的是 VLAN default 的信息。

配置 VLAN 模式

设备的缺省 VLAN 模式为多模模式，在该模式下，同一个端口能够以 untagged 方式属于多个 VLAN；设备也可以工作在单模模式下，在该模式下，用户只能把同一个端口以 untagged 方式配置到一个 VLAN 中。如果要更改 VLAN 的模式，选择上图中“VLAN 管理”中的“VLAN 模式”下拉列表，再单击右边的“更改”即可。另外需要注意的是，如果用户更改了 VLAN 的模式，在前一模式下配置的所有 VLAN 信息将被自动删除。

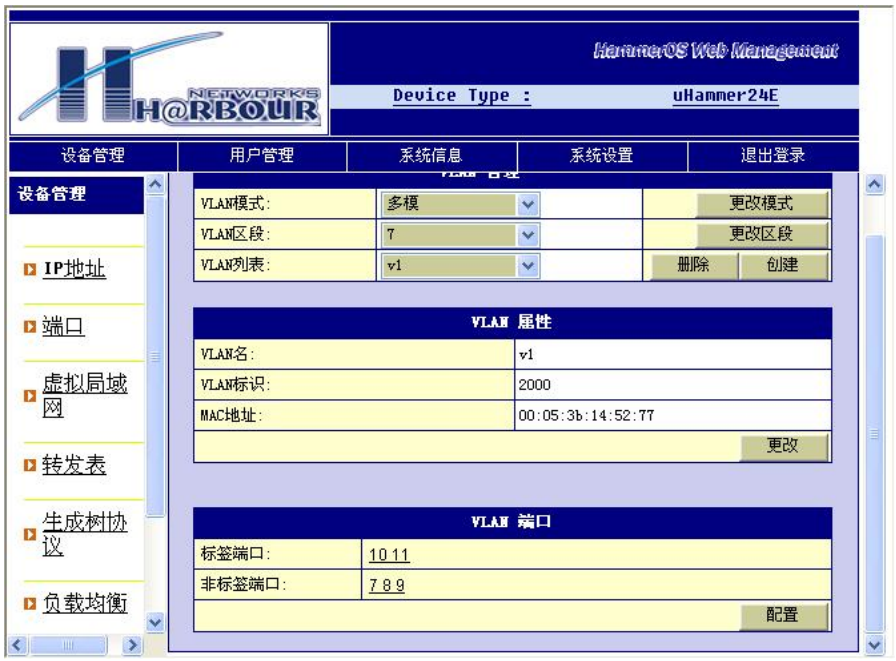
创建 VLAN

点击 VLAN 管理表格中的“创建”，出现如下图所示界面。

图15-7 创建 VLAN

在对话框中输入所要创建的 VLAN 名：vlan1，然后点击“确定”，出现如下图所示界面。

图15-8 设置 VLAN 信息



修改 VLAN 信息

在上图中点击“更改”，出现如下图所示界面。

图15-9 修改 VLAN 信息

在输入框中输入需要配置的数据。例如，设 VLAN 名称为 v1，然后单击“确定”即可。

删除 VLAN

在图 15-6 中，在 VLAN 列表中选择要进行删除操作的 VLAN 名，然后单击“删除”即可进行删除操作。

配置 VLAN 端口

单击 VLAN 端口表格中的“配置”，进入 VLAN 端口配置界面，出现如下图所示界面。

图15-10 配置 VLAN 端口

在左边的可用端口框中显示可以选择的端口（包括 tagged 端口和 untagged 端口）。选择需要加入的端口，单击“增加”。如果需要删除 VLAN 中的端口，则在成员框中选择要操作的端口，然后单击“删除”即可。配置完毕后，单击“返回”，返回 VLAN 的控制界面。

15.6 配置FDB地址表

15.6.1 FDB地址表概述

通过 Web Management 可以增加地址表项到 FDB 地址表中，从而实现对各种数据包的处理，即根据数据包的源地址和目的地址来决定该数据是过滤还是转发。有关 FDB 的内容详见“第 6 章 配置 FDB 表”。

15.6.2 Web中FDB地址表的配置

首先点击设备管理下的转发表出现如下图所示的页面。在多模模式下，FDB 的静态表项不再属于某个单独的 VLAN。

图15-11 配置 FDB 地址表

设置 FDB 地址表项老化时间

例如，需要设置地址表老化时间（agingtime）为 80，则在“老化时间”栏中填入 80 后，选择“提交”即可；如需修改，选择“重置”，重新输入即可。

如果老化时间（Ageingtime）被设置为 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，直至交换机关机或者重启。

创建永久地址表项

当创建的 FDB 地址是单播地址时，只能对应一个端口号，选择相应的端口号并输入 MAC 地址。

显示 FDB 地址表项

在“FDB 地址表”功能框中可以根据浏览类型来查询 FDB 地址表中的地址表项，包括四种类型：all（所有 FDB 地址表项），Permanent（静态地址表项），Age（动态地址表项），CPU（系统地址表项）。

15.7 Spanning-tree的配置

15.7.1 STP概述

本节主要讲述如何通过 Web 界面来实现对 Spanning-tree 进行配置。目前用两种方式实现了 Spanning-tree，一种为多域的 STP，一种为 RSTP。为了向前兼容，我们没有在 web 实现多域 STP 的配置，只是用多域的 STP 预创建一个 default 域来替代以前的单域的 STP，以下我们通称为 STP；在 RSTP 配置中，提供了主要参数的配置，其功能与单域的 STP 相仿。Web 中，不提供两种 spanning－tree 切换的功能，请在命令行中用 config spanning－tree mode stp/rstp 命令切换，切换后，web 界面会自动的跟着切换为相应的模式。

15.7.2 配置STP

配置 STP 需要做如下操作：

- 使能生成树协议域
- 使能参与 STP 协议计算的端口

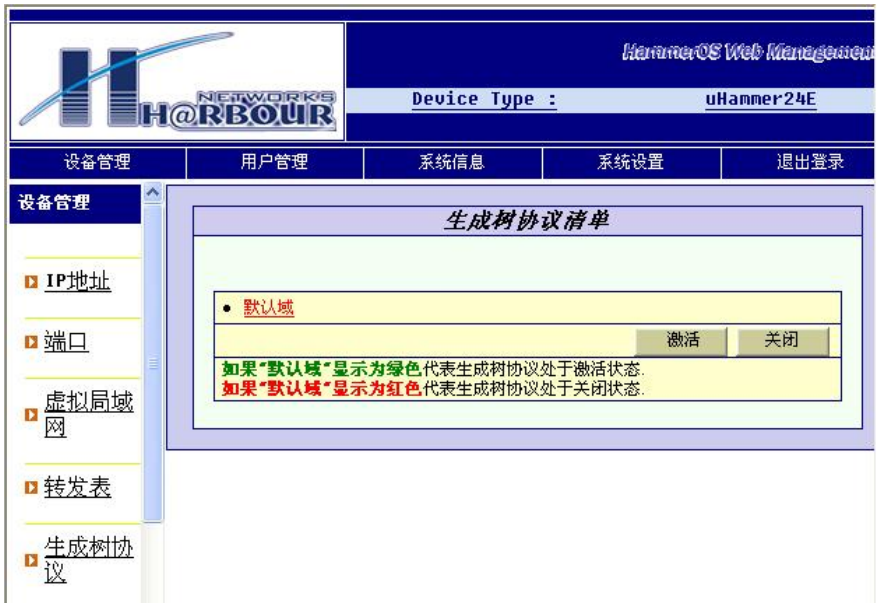
一旦运行 STP 协议后，您可能需要根据具体的网络结构调整 STP 协议的一些参数。以下的 STP 协议参数可以在 HammerOS 中调整：

- 优先级
- 桥发送 BPDU 时间间隔
- 桥切换时间间隔
- 根报文老化最大时间间隔

另外每个端口上有以下参数可以调整：根路径开销、优先级。

15.7.3 Web中STP的配置

图15-12 配置 STP



配置 STP 协议时，在上图所示的界面中，点击激活按钮，如果默认域字样变成了绿色，表示生成树协议已经激活，如果变成红色表示生成树协议还没有被激活。

关闭生成树协议方法与上述操作类似，选择后点击关闭按钮。

15.7.4 配置生成树协议的有关参数

单击要配置的生成树协议域项，结果如下图所示：

图15-13 配置生成树协议的有关参数

根据上图中相应的提示填入相应的值。

设置运行 STP 协议时本交换机的优先级

优先级 Priority 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。

设置当本交换机被选为根桥时发送 BPDU 的时间间隔

桥发送 BPDU 时间间隔的取值范围是 0-10，单位为秒，缺省值是 2 秒。

桥发送 BPDU 时间间隔必须小于等于桥切换时间间隔－2。

设置当本交换机被选为根桥时端口状态切换的时间间隔

桥切换时间间隔的取值范围是 4-30，单位为秒，缺省值为 15 秒。

桥切换时间间隔的时间必须大于等于桥发送 BPDU 时间间隔+2。

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。报文老化最大时间间隔的取值范围是 6-40，单位秒，缺省值为 20 秒。

报文老化最大时间间隔的时间必须大于等于 2*(桥发送 BPDU 时间间隔+1）小于等于 2*（桥切换时间间隔–1）。

修改完毕后单击使能即可。

15.7.5 使能STP Port

单击图 15-13 所示的相应端口，如单击端口 12，结果如下图所示：

图15-14 使能 STP Port

在上图中，单击端口退出 STP 计算按钮，则端口不参加计算，反之再重复以上步骤可以使端口使能。

15.7.6 配置STPD Port的有关参数

配置参与 STP 计算的端口的优先级 Priority

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。

配置参与 STP 计算端口的路径开销 Path Cost

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

15.7.7 配置RSTP

配置 RSTP 需要做如下操作：

- 使能生成树
- 使能参与 RSTP 协议计算的端口

一旦运行 RSTP 协议后，您可能需要根据具体的网络结构调整 RSTP 协议的一些参数。以下的 RSTP 协议参数可以在 HammerOS 中调整：

- 优先级
- 桥发送 BPDU 时间间隔
- 桥切换时间间隔
- 根报文老化最大时间间隔

另外每个端口上有以下参数可以调整：根路径开销、优先级。

15.7.8 Web中RSTP的配置

图15-15 配置 RSTP

配置 RSTP 协议时，在上图所示的界面中，点击激活按钮，如果 RSTP 字样变成了绿色，表示生成树协议已经激活，如果变成红色表示生成树协议还没有被激活。

关闭生成树协议方法与上述操作类似，选择后点击关闭按钮。

15.7.9 配置RSTP的有关参数

单击要配置的生成树协议域项，结果如下图所示：

图15-16 配置 RSTP 的有关参数

根据图中相应的提示填入相应的值。

设置运行 RSTP 协议时本交换机的优先级

优先级 Priority 的取值范围是 0-61440，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。

设置当本交换机被选为根桥时发送 BPDU 的时间间隔

桥发送 BPDU 时间间隔的取值范围是 0-10，单位为秒，缺省值是 2 秒。

桥发送 BPDU 时间间隔必须小于等于桥切换时间间隔－2。

设置当本交换机被选为根桥时端口状态切换的时间间隔

桥切换时间间隔的取值范围是 4-30，单位为秒，缺省值为 15 秒。

桥切换时间间隔的时间必须大于等于桥发送 BPDU 时间间隔+2。

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。报文老化最大时间间隔的取值范围是 6-40，单位秒，缺省值为 20 秒。

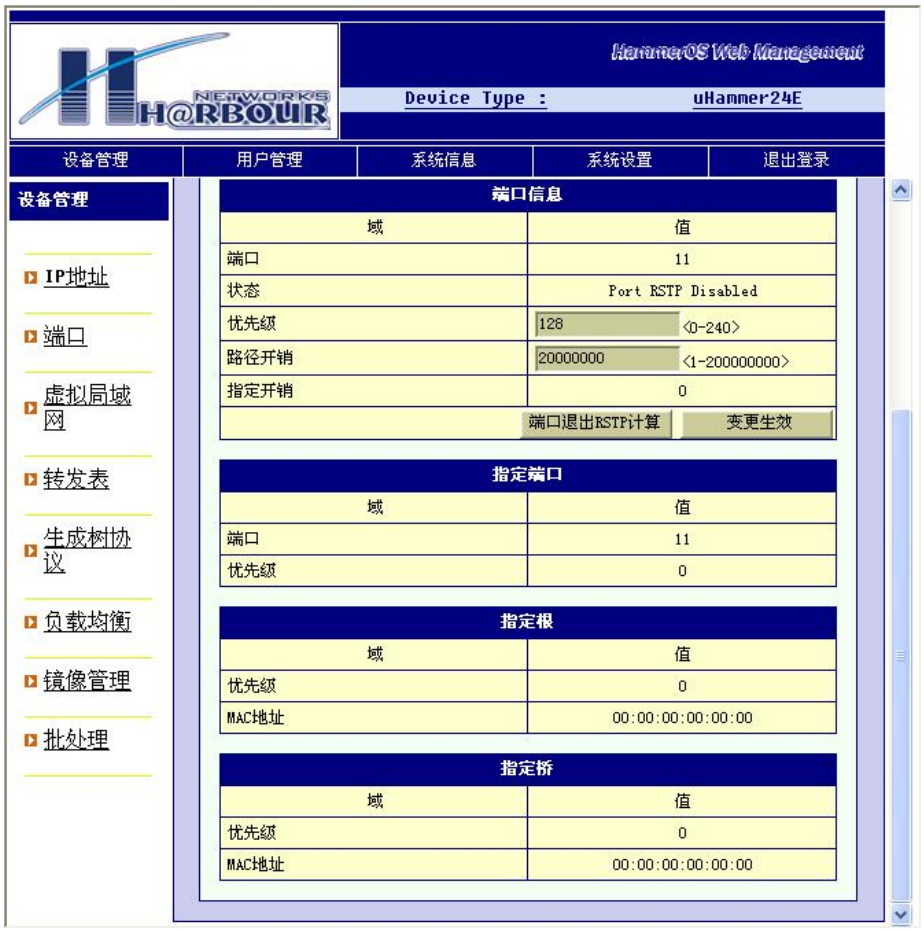
报文老化最大时间间隔的时间必须大于等于 2*（ 桥发送 BPDU 时间间隔+1）小于等于 2*（桥切换时间间隔–1）。

修改完毕后单击使能即可。

15.7.10 使能RSTP Port

单击图 15-16 所示的相应端口。如单击端口 11，结果如下图所示：

图15-17 使能 RSTP Port



在上图中，单击端口退出 RSTP 计算按钮，则端口 11 不参加计算，反之再重复以上步骤可以使端口使能。

15.7.11 配置RSTP Port的有关参数

配置参与 STP 计算的端口的优先级 Priority

端口优先级的取值范围是 0-240，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。

配置参与 STP 计算端口的路径开销 Path Cost

取值范围是 1-200000000，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 2000000
- 100Mbps 端口缺省值为 200000
- 1000Mbps 端口缺省值为 20000

15.8 配置多端口负载均衡组

15.8.1 在Web Server中配置Load Sharing

设置 Load Sharing，必须创建 Load Sharing 的一组端口。

在 μHammer2E/2ED/24E/24ED/2024E 交换机中，创建 Load Sharing 时必须遵从以下规则：

- 交换机只支持一个 Load Sharing；
- 1-24 端口支持 Load Sharing；
- 一个 Load Sharing 中最多有 4 个端口。

在主控制页面中右侧的“快速链接”栏中单击“负载均衡”，进入其控制界面，出现如下图所示界面。

图15-18 配置 Load Sharing

此时如果已经建立 Load Sharing，在主端口和组内端口中将会显示相应的端口。

15.8.2 创建Load Sharing

在上图中，单击“创建”，开始创建 Load Sharing，出现如下图所示界面。

图15-19 创建 Load Sharing

在选择主端口号下拉列表中选择要创建 Load Sharing 的主端口，然后选择端口组成员。

例如，创建的这个 Load Sharing 组的主端口为 1，成员端口为 1、2、3。然后单击“OK”，出现如下图所示界面。此时表明该 Load Sharing 组已经创建成功。

图15-20 Load Sharing 组创建成功

注意

不同 VLAN 组成员的端口不能捆绑。

15.8.3 删除Load Sharing

在图 15-19 Load Sharing 管理表格中，从主端口下拉菜单中选择要删除的 Load Sharing 主端口，点击“删除”，即可将所选定的 Load Sharing 删除。

注意

必须在相互连接的两台交换机上都设置 Load Sharing，否则会在网络中造成回路。

15.9 管理镜像信息

HammerOS 支持端口镜像，把指定端口或 VLAN 的所有数据包文重定向到镜像端口，以方便错误诊断。同时，HammerOS 支持通过 Web 来对端口镜像进行管理。点击【镜像管理】，出现如下图所示界面。

图15-21 镜像信息管理

选择要配置的镜像端口，然后点击“设置”，完成操作。

15.10 批处理

用户可以通过批处理来设置多个端口的端口参数或生成树参数。点击左下方窗口的“批处理”，进入如下图所示界面。

图15-22 批处理界面

在上图界面中，可以选择进行端口设置，或进行端口生成树协议参数的设置。

设置普通端口

在图 15-22 中，点击“普通端口设置”，进入如下图所示界面。

图15-23 选择批处理端口

在上图中，选择端口 13、14、15 进行设置，点击“下一步”，出现如下图所示界面。

图15-24 普通端口参数设置界面

完成设置后点击“提交”，进入下一步；如果当前不想设置，点击“重置”，放弃操

作。点击“提交”后，系统更新端口配置。

设置端口生成树协议

在图 15-22 中，点击“端口生成树协议设置”，出现如下图所示界面。

图15-25 选择批处理端口

选取端口 13、14、15 进行设置后，单击“下一步”，出现如下图所示界面。

图15-26 设置端口参数

点击“提交”后，系统进行相应配置更新。

15.11 设置用户访问权限

15.11.1 用户访问权限

HammerOS 中提供了两种用户：ADMIN 管理员、NORMAL 普通用户。用户权限可以通过 Web 页面来设置。

管理员能够进入配置模式，并对系统的所有参数进行查看和设置。管理员还能增加、删除用户账号和设置修改用户密码；在本 Web 的页面管理模块中，包括显示用户列表、增加用户、编辑特定用户。

点击“用户管理”，出现如下图所示界面。

图15-27 用户管理

15.11.2 增加用户

增加用户，可以按照以下步骤进行：

第一步：以用户名 admin 登录（或者用任何其他管理员的用户账号登录）。

第二步：单击页面上方的“用户管理”，进入用户管理界面，如图 15-27 所示；

当前系统中的用户列表将显示当前所有的用户名和用户身份；以后在其它界面中，只需点击超级链接“用户列表”，即可进入此界面。

第三步：单击界面左方窗口中的“增加”，即可进入增加用户界面，如下图所示。

图15-28 增加用户

用户名和密码有如下命名规则：

- 用户名必须为以字母开头的，只包含大写或小写的英文字母、数字、下划线的长度为 4-20 的字符串；
- 密码可以是由任意字符组成的长度为 6-20 的字符串。输入并且确认密码之后，点击“下一步”。

注意

用户名不区分大小写，密码区分大小写。

第四步：例如，输入用户名 manager，密码 harbour 后，单击“下一步”，出现如下图所示界面，显示添加用户成功的信息提示。

图15-29 添加用户成功

第五步：如果需要添加成为管理员用户，可单击“下一步”，否则按“完成”结束操作。

假设需要添加成为管理员。单击“下一步”后，进入如图 15-30 所示界面。在此界面中输入管理员密码，例如为 harbour，并确认输入一次，单击“完成”结束操作。可以由图 15-31 看出，用户 manager 已经变为管理员用户。

图15-30 添加管理员

图15-31 添加管理员成功

15.11.3 编辑用户信息

可以使用以下方法把一个用户设为管理员或者是设为普通用户。

在“快速链接”栏中点击“编辑”，进入修改用户界面，如下图所示。选择用户名，例如：选择 admin，然后单击“下一步”。

图15-32 选择用户

单击“下一步”，出现如下图所示界面。

图15-33 编辑用户信息

在上图界面中有三个选项：修改用户登陆密码、修改用户身份、修改管理员密码（如果用户是普通用户，将不显示该项）。如果选择修改密码，系统将提示重新输入密码；如果选择修改用户身份，则直接改变当前用户的身份（从普通用户成为管理员，需输入管理员密码）。

15.11.4 删除用户

在“快速连接”栏中点击“删除”，进入删除用户界面，如下图所示。

图15-34 删除用户

在用户列表中选择要删除的用户，单击“删除”即可。如果选择删除的用户姓名为admin，则出现错误提示，如下图所示。

图15-35 不能删除内置用户 admin

15.12 查看系统信息

点击菜单栏上的“系统信息”，将出现如下图所示界面，显示系统相关信息，如产品

名称、产品序列号、MAC 地址、系统名称、硬件版本号、Bootrom 版本号、软件版本号、生产日期。

图15-36 系统信息

15.13 系统设置

点击菜单栏上的“系统设置”，出现如下图所示界面，选择“确定”，即可将配置保存到扩展 FLASH 中。保存成功后，出现如图 15-38 所示界面。

图15-37 保存配置

图15-38 保存配置成功

注意

完成所有配置工作后，切记保存配置信息，否则重启后将丢失。

可以通过 Web 系统向交换机载入 HammerOS 系统或配置文件（Config File）。点击页面左方窗口的“上载”，进入如下图所示界面。选择上载文件类型，即 HammerOS 或 Config File，通过“浏览”选择上载的文件，然后点击“开始上载”即可。

图15-39 上载文件

15.14 退出登录

完成所有的配置后，可以退出登陆。单击菜单栏最右方的“退出登录”后，将出现初始登录界面。

第三部分

启动选项和软件升级

16 启动选项和软件升级

本章主要介绍 Bootrom 启动选项、升级 HammerOS 软件以及重新启动交换机。

16.1 Bootrom启动选项

Bootrom 启动分为两种方式：

- 自动启动
- 人工干预启动

16.1.1 自动启动

默认方式下，交换机在上电之后，用户不需要干预，交换机将进入直接启动模式，进入 HammerOS 操作系统中。例如，启动成功后，μHammer24E 交换机显示信息如下：

```
Bootrom ...... booting

Copyright Harbour Networks Co., Ltd. All Rights Reserved.
Bootrom Version V1R50
Compiled Mon 22-Sep-2003 10:00

Product name: uHammer24E
Serial number: 01010163A122022000005
Base ethernet MAC address: 00:05:3b:44:55:11
Manufacture date: 2004-02-12
Hardware revision: Version 2.30

System booting ......

Open console ...... Done.
Loading startup config ...... Done.
```

```
############################################################
#                                                          #
#                Welcome to HammerOS.                      #
#                                                          #
#    Press <ENTER> to connect and config this system.      #
#                                                          #
############################################################
```

然后按回车键，进行用户登录。

16.1.2 人工干预启动

配置步骤

步骤1	连接交换机的Console端口，终端应配置成：连接的波特率为9600bps，数据位为8位，无奇偶校验，停止位为1，无数据流控制。
步骤2	串口显示“system booting”后，快速按下空格键。
步骤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：

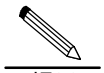
```
Copyright Harbour Networks Co., Ltd. All Rights Reserved.
Bootrom Version V1R50
Compiled Mon 22-Sep-2003 10:00

Product name: uHammer24E
Serial number: 01010163A122022000005
Base ethernet MAC address: 00:25:33:44:55:11
Manufacture date: 2003-10-15
Hardware revision: Version 2.00

System booting ......
 ?             - List all available commands
 h             - List all available commands
 b             - Boot an executable image
 g             - Boot an executable image with default configurations
 u             - Load and boot an executable image
 l             - Load configuration file and boot an executable image
 m             - Test system memory
 r             - Reboot system
```

```
Press 'h' or '?' To get helping information.
Hammer:
```

Bootrom 菜单选项及其含义如表 16-1 所示。

表16-1 Bootrom 菜单选项及其含义

选项	选项含义
?	显示所有命令信息；
h	显示所有命令信息；
b	直接执行HammerOS；
g	使用缺省配置执行HammerOS；
u	使用Xmodem协议下载HammerOS，并执行；
l	使用Xmodem协议下载配置文件，并执行HammerOS；
m	内存自检功能
r	重新启动交换机。


提示

下载的 HammerOS 存储到 FLASH 中。

16.2 升级HammerOS软件

HammerOS 提供了三种升级软件的方式：

- 通过串口用 Xmodem 协议下载 HammerOS；
- 通过 TCP/IP 网络用 ftp 协议下载 HammerOS；
- 通过网络用 tftp 协议下载 HammerOS。


注意

在下载 HammerOS 过程中掉电或重启会导致系统异常。

16.2.1 通过串口用Xmodem协议升级 HammerOS

配置步骤

步骤1	用具有管理员权限的用户名通过串口登录并进入配置模式。
步骤2	输入命令。
	download xmodem hammeros
步骤3	打开串口超级终端的“发送文件”菜单，选择HammerOS可执行文件，单击“发送”。
步骤4	下载完毕后，输入命令reboot，重新启动交换机。

16.2.2 通过TCP/IP网络用FTP协议升级 HammerOS

配置步骤

步骤1	用具有管理员权限的用户名通过串口或者TCP/IP网络登录并进入配置模式。
步骤2	输入命令。其中，<A.B.C.D>表示HammerOS文件所在机器的IP地址；<username>表示FTP的用户名；<password>表示该用户的密码；<filename>表示所要下载的文件名。
	download ftp hammeros <A.B.C.D> <username> <password> <filename>
步骤3	等待系统完成FTP下载并写入FLASH。
步骤4	完毕后，输入命令reboot，重新启动交换机


注意

下载之前，请确认 FTP 服务器可用，并且服务器上的参数和升级文件正确。

16.2.3 通过网络用TFTP协议升级 HammerOS

小文件传输协议 TFTP（Trivial File Transfer Protocol）是网络应用程序，比 FTP 简单，也比 FTP 功能少，在不需要用户权限或目录可见的情况下使用。TFTP 协议使用 UDP 协议而不使用 TCP 协议。在 RFC 1350 内有对 TFTP 的详细说明。

配置步骤

步骤1	用管理员权限登录并进入配置模式。

步骤2	输入命令。其中，<A.B.C.D>表示HammerOS文件所在机器的IP地址；<filename>表示所要下载的文件名。
	download tftp hammeros <A.B.C.D> <filename>
步骤3	等待系统完成下载并写入FLASH。
步骤4	完毕后，输入命令reboot，重新启动交换机。


注意

下载之前，请确认 TFTP 服务器可用，并且服务器上的参数和升级文件正确。

16.3 重新启动交换机

当需要重新启动交换机时，可以使用命令 reboot。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。

配置步骤

步骤1	save configuration	保存配置数据。