FlexHammer5010 交换机
软件配置手册

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

P-(20)031103-130

版权声明

免责声明

本手册依据现有信息制作，其内容如有更改，恕不另行通知。港湾网络有限公司在编写该手册的时候已尽最大努力保证其内容准确可靠，但港湾网络有限公司不对本手册中的遗漏、不准确、或错误导致的损失和损害承担责任。

Users' Manual Copyright and Disclaimer

Copyright

Disclaimer

This document and the information contained herein is provided on an "AS IS" basis. Harbour Networks Limited may make improvements or changes in this documentation, at any time and without notice and as it sees fit. The information in this documentation was prepared by Harbour Networks Limited with reasonable care and is believed to be accurate. However, Harbour Networks Limited shall not assume responsibility for losses or damages resulting from any omissions, inaccuracies, or errors contained herein.

前言

前言介绍了本手册的大致内容、组织方式、针对用户类型、图标含义和相关文档。

文档内容

FlexHammer5010 上运行的操作系统 HammerOS(简称 HOS)，是由港湾网络有限公司自主研制开发。本手册介绍了 HammerOS 的功能、特性以及在 FlexHammer5010 上的配置方法，并且对所用到的命令给予了详尽的解释。

组织方式

章	题目	内容描述
第 1 章	HammerOS 概述	简述 HammerOS 的特性，包括 VLAN、Load Sharing、RSTP 等技术在交换机上的应用
第 2 章	访问交换机	讲述 HammerOS 系统的命令格式、用户权限的设置以及管理交换机的途径等
第 3 章	配置交换机的端口	讲述了交换机端口的基本参数配置，并针对如何解决 Load Sharing 作了详尽的介绍
第 4 章	ARP 管理	介绍 ARP 的相关知识及在交换机上的配置方法
第 5 章	FDB 表	讲述了 FDB 地址表的相关知识，以及如何在交换机上配置静态 FDB 地址表
第 6 章	虚拟局域网 VLAN	详细介绍了 VLAN 的作用、分类，以及如何在交换机上完成对 VLAN 各项的配置
第 7 章	生成树协议	讲述了 STP 和 RSTP 协议，以及如何在交换机上进行相关配置
第 8 章	DHCP Relay	讲述 DHCP Relay 原理及如何用 HammerOS 来配置 DHCP Relay
第 9 章	VRRP	介绍 VRRP 协议的原理及配置方法
第 10 章	IGMP Snooping	介绍网络组管理协议的配置和应用
第 11 章	QoS	讲述了 QoS 知识及相关配置，包括 Queue、Dot1p、ACL 等内容
第 12 章	日志管理	介绍日志管理功能及设置方法
第 13 章	网络管理服务 NMS	讲述了网络管理服务模块的意义及在交换机上的配置方法
第 14 章	ACL 配置	讲述了 ACL 的相关知识及在交换机上的配置方法
第 15 章	SNTP 协议	讲述了 SNTP 的特性及在交换机上的配置方法
第 16 章	虚拟堆叠	讲述了虚拟堆叠技术的特点及其在交换机上的配置方法
第 17 章	单播路由协议	介绍了单播路由协议的基本原理及 RIP 和 OSPF 的配置方法
第 18 章	组播路由协议	介绍了组播路由协议基本原理及 IGMP 和 PIM-SM 的配置方法

附　录	普通用户命令一览表 管理员命令一览表	普通用户和管理员的命令一览表

针对用户类型

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。这要求读者熟悉以下知识：

- 局域网（Local Area Networks）（LAN）
- 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）
- 服务质量（Quality Of Service）(QoS)
- 简单网络管理协议概念（Simple Network Management Protocol）（SNMP）

图标说明

图标	作用
	提示用户在配置交换机的过程中需要特别注意的地方
	表示给用户提示的附加说明信息

相关文档

1.《FlexHammer5010 软件配置手册》 (本手册)

2.《FlexHammer5010 硬件安装手册》

3.《H.link 配置使用手册》

4.《NAS 接入服务用户手册》

目录

第1章 HammerOS 概述

HammerOS 是港湾网络公司为 Hammer 系列交换机设计的操作系统，它运行在 FlexHammer、μHammer 及 BigHammer 系列交换机上。本章主要介绍了 HammerOS 的特性，以及相关技术的解释。

1.1 特性概述

在 FlexHammer5010 中 HammerOS 有如下特性：

- 支持IEEE 802.1Q和IEEE 802.1p标准的Virtual Local Area Networks (VLAN)
- 支持IEEE802.1d标准的Spanning Tree Protocol（STP）和IEEE802.1w标准的RSTP
- 线速（Wire-speed）二层交换
- 支持多端口到一个端口的镜像
- 支持端口捆绑 （Load sharing）
- 支持服务质量（QoS）
- 支持日志管理（Syslog）
- 支持IGMP Snooping
- 支持SNTP（Simple Network Time Protocol）协议
- 支持访问列表和数据包过滤
- 支持802.1x认证
- 支持H.Link
- 支持ACL访问控制
- 支持NMS网络管理服务
- 支持虚拟堆叠
- 支持Console 、Telnet命令行配置
- 支持DHCP Relay
- 支持VRRP虚拟路由器冗余协议
- 支持Simple Network Management Protocol (SNMP)
- 具有三层转发功能，支持RIP、OSPF等多种单播路由协议
- 支持IGMP、PIM-SM等组播路由协议

H.Link 是港湾网络有限公司的专有通讯协议。

1.2 虚拟局域网（VLAN）

HammerOS 的 VLAN 功能使您在构建自己的广播域时，不再受限于网络的物理连接。一个 VLAN 就是一群独立于具体网络拓扑的设备，它们在通讯时，不论如何连接，属于这一 VLAN 的所有设备都好像在一个真正的物理局域网上。VLAN 的具体作用体现在：

- 可以控制广播数据，限制其广播的范围。假设在VLAN“研发部”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。
- 提供了额外的安全特性。跨VLAN的访问只有通过三层转发，不能直接访问。例如，VLAN“市场部”的设备只能通过路由协议同VLAN“研发部”进行通信。
- 简化了设备在网络中的移动和管理。

具体来讲，VLAN 技术是为了创建第三层逻辑广播域，VLAN 可在一个 Switch 上划分，也可以跨越多个 Switch 划分。VLAN 实现了一个物理网段交换机群之间逻辑 LAN 划分，即分成多个逻辑广播域，避免广播风暴的发生。

有关 VLAN 的详细配置信息见本手册第 6 章。

1.3 生成树协议（STP 和 RSTP）

Hammer 交换机支持 IEEE802．1d 标准的 STP 协议，它提供了网络的动态冗余切换机制，STP 使您能在网络设计中部署备份线路。

RSTP 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。在网络设计中可以使用 RSTP 协议部署备份线路，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，自动快速启用备份线路，切换数据流。

有关生成树协议的详细配置信息见本手册第 7 章。

1.4 Load Sharing

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。其作用表现在以下两个方面：

1. 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。

2. 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。

HammerOS 的 Load Sharing 功能与 Intel 和 Cisco 同类产品的 Port Group 功能兼容。有关 Load Sharing 的详细配置信息见本手册第 3 章内容。

1.5 IGMP Snooping 网络组管理协议

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

IGMP snooping 用于监听主机与路由器之间的 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。

有关 IGMP Snooping 的详细内容请参阅本手册第 10 章。

1.6 服务质量 (QoS)

QoS 是指 IP 的服务质量，也就是 IP 数据流通过网络时的性能。其目的是向用户业务提供端到端的服务质量保证，QoS 还提供了更高效的带宽使用率。HammerOS 系列交换机目前已经实现了端口优先级调度，802.1p 的 VLAN tag 到优先级的映射，ToS 到优先级的映射等多项相关服务。

有关 QoS 的详细信息请参见本手册第 11 章。

1.7 日志管理（Syslog）

日志管理主要用来记录整个系统的运行情况以及用户操作行为。完整的日志管理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。

有关 syslog 方面的详细内容请参阅本手册第 12 章。

1.8 网络管理服务（NMS）

从安全的角度出发，我们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 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 NMS 的详细配置信息见本手册第 13 章。**

1.9 简单网络时间协议（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 的详细内容请参阅本手册第 15 章。**

1.10 802.1x 认证服务

FlexHammer5010 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 优势的基础上，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。

FlexHammer5010 采用了不同实现方式，即在开启 802.1x 功能时并不对 DHCP、IGMP、ARP、H.Link 和 vstack 报文的二层帧进行过滤，因此那些没有通过认证的用户尽管不能实现正常通信，但仍能够获取 IP 地址，并可进行 ARP 学习、建立 IGMP Snooping 组以及实现 H.Link 设备登录和虚拟堆叠管理等。

 **有关 NAS 协议的详细信息请参阅《NAS 接入服务用户手册》。另外由于 FlexHammer5010 不支持流量统计、基于 802.1x 的动态 ACL 修改，也不支持基于 802.1x 的带宽限制和多域认证，因此，FlexHammer5010 交换机的 NAS 命令和《NAS 接入服务用户手册》上的有一定的差异：**

NAS 接入服务用户手册	FlexHammer5010
以下命令参数或者参数的表达形式有变化	
config dot1x quiet-period <0-32767>	config dot1x quiet-period <0-65535>

config dot1x re-authentication period <1-32767>	config dot1x re-authentication period <1-65535>
config dot1x server-timeout <1-32767>	config dot1x server-timeout <1-65535>
config dot1x supp-timeout <1-32767>	config dot1x supp-timeout <1-65535>
config dot1x tx-period <1-32767>	config dot1x tx-period <1-65535>
config dot1x pae force-logoff mac <usermac> {port <portno>}*1	config dot1x pae force-logoff mac <address> {port <portno>}*1
config isp-domain <domain> accounting config-server id <id> type [primary|multi |backup]	config isp-domain <domain> accounting config-server id <0-4> type [primary|multi |backup]
config isp-domain <domain> authentication [add-server|delete-server] id <id>	config isp-domain <domain> authentication [add-server|delete-server] id <0-4>
config isp-domain <domain> authentication config-server id <id> type primary	config isp-domain <domain> authentication config-server id <0-4> type primary
以下命令在 FlexHammer5010 交换机上不支持	
config dot1x uplink-port <portno>	不支持
config dot1x access-limit route-engine [rate|acl|disable]	不支持
radius config-attribute access-bandwidth [uplink|downlink] Vendor-Specific <VendorType> {<VendorId>}*1	不支持
radius config-attribute access-bandwidth [uplink|downlink] default-value	不支持
radius config-attribute access-bandwidth [uplink|downlink] standard <1-255>	不支持
radius config-attribute access-bandwidth unit [bps|kbps]	不支持
radius config-attribute filter-id Vendor-Specific <VendorType> {<VendorId>}*1	不支持
radius config-attribute filter-id default-value	不支持
radius config-attribute filter-id standard <1-255>	不支持
show dot1x access-limit route-engine	不支持
show dot1x uplink-port	不支持
show dot1x vlan <vlanname> pae	不支持
show dot1x vlan <vlanname> user-count	不支持
show radius config-attribute bandwidth-unit	不支持
以下命令为 FlexHammer5010 特有的命令，没有写到《NAS 接入服务用户手册》中。	

show isp-domain	显示系统中配置的所有域
show isp-domain <domain>	显示域 domain 的详细配置信息
show radius config-attribute source-mac	显示使用哪个 RADIUS 属性携带用户的源 MAC 地址。

1.11 H.Link 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 FlexHammer5010 可以同时管理多达 36 个互连的 μHammer1008/μHammer1016/μHammer1024 交换机，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客户端设备，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、与平台无关等特点。

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

第2章 访问交换机

本章主要介绍管理 FlexHammer5010 所需要的一些基本知识，包括：

- Bootromr启动
- 理解命令格式
- 常用命令
- 设置访问权限
- 管理交换机的途径
- 配置SNMP
- 配置静态路由
- 存取配置文件及升级HammerOS
- 网络状态及系统的检测

2.1 Bootrom 启动

Bootrom 启动分成两种方式：

- 自动启动
- 人工干预启动

2.1.1 自动启动

在默认方式下，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，启动信息显示如下：

```
Hammer Boot Loader version 1.1, Harbour Networks, Inc.
Compiled Fri 02-NOV-2001 11:00

Memory selftest: ................OK

Base ethernet MAC address: 00:05:3b:00:04:90

Copyright(c) 2000-2001 by Harbour Networks, Inc.
System booting...

Uncompress start...
Uncompress success, enter device initialize, Please wait...

Init console ... done.
Console baudrate is 9600.

Entering HammerOS ......
```

```
Initializing environment ...... Done.
Loading startup config ...... Done.

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

然后按回车键，进行用户登录。

2.1.2 人工干预启动

按照以下步骤可以访问 Bootrom 菜单：

1 连接交换机的 Console 端口，注意终端的正确配置。

2 打开交换机电源，并且不停的按空格键。

3 当出现“Hammer: ”提示符，说明已经进入 Bootrom 菜单。

人工干预启动后显示 Bootrom 菜单信息：

```
Hammer Boot Loader version 1.1, Harbour Networks, Inc.
Compiled Fri 02-NOV-2001 11:00

Memory selftest: ................OK

Base ethernet MAC address: 00:05:3b:00:04:90

Copyright(c) 2000-2001 by Harbour Networks, Inc.
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
 r        - Reboot system

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

Bootrom 菜单选项及其含义如下：

?：显示帮助信息

h：显示帮助信息

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

r：重新启动交换机

2.2 理解命令格式

这一节主要讲述当您进入命令行执行配置时所要进行的步骤。请仔细阅读本节及后续内容中关于使用命令行接口的详细信息。使用命令行接口（CLI），请按照以下步骤：

第一步：当进入命令行接口出现命令提示符后，请确认您有相应的登录权限。

FlexHammer5010 交换机的命令行系统支持两个不同的管理模式：一为只读模式，二为配置模式。在只读模式下只能对交换机的一般信息进行查看，没有配置权限。在配置模式下则有对交换机的配置权和所有信息的查看权。只读模式下的命令提示符是“Harbour>”，配置模式下的命令提示符是“Harbour(config)#”。

FlexHammer5010 交换机的命令行系统对用户的划分也有两种：一为管理员用户，另一为普通用户。普通用户只能进入只读模式，管理员用户则可以进入任何模式，拥有所有的配置权限。

第二步：键入命令名称。

如果键入的命令不含需要用户输入的参数，那么请直接跳到第三步。如果键入命令中含有需要用户输入的参数，那么继续以下步骤：

1) 如果命令需要一个参数值，请输入一个参数值。在输入参数值时，可能要输入关键字。
2) 命令的参数值部分一般指定了您应该输入什么样的参数，是某范围内的数值，或者字符串或者 IP 地址。关键字是指命令中要操作的对象。
3) 如果命令需要多个参数值，请按命令的提示依次输入关键字和每个参数值。直到提示信息中出现<cr>按回车键信息为止。

第三步：输入完整的命令后，请按回车键。

例如：

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则执行。

用户需要输入参数的情况：Harbour(config)#config port 2,3 speed 10

这是一个含有参数和关键字的命令。关键字为 port 和 speed，参数值为 2，3 和 10。

2.2.1 语法帮助

命令行接口中内置有语法帮助。如果您对某个命令的语法不太确定，请输入该命令中您所知道的前面部分，接着键入“?”或“空格＋？”。如果输入“?”则解释该命令；如果输入“空格＋？”则列出可以输入的关键字。命令行会提示您剩余部分可能的命令的清单。您就可以根据提示的命令继续输入，直至出现以下提示命令为止：<cr>　Just Press Enter to Execute command!　这表明命令已输入完毕，按回车便可执行所键入的命令。

例如：

第一步：键入命令：who

第二步：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“空格+？”，系统显示如下信息：

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

<cr>　Just Press Enter to Execute command!

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

2.2.2 使用语法帮助补齐命令

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

例如：

第一步：键入命令：ping

第二步：再输入一空格键，然后按“Tab”键，显示如下信息：

-t　-count　-size　-waittime　–ttl　-pattern

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

如果一个命令比较长不好输入，您也可以使用“Tab”键。例如：

第一步：键入 show run

第二步：按“Tab”键，系统会自动补齐命令 show running-config

2.2.3 命令简写

命令简写是指您可以只输入命令单词或关键字的前边部分字母，只要那部分字母不会造成歧义，交换机就能够识别该命令，用户可以直接回车执行该命令。但需要用户输入的参数，如 VLAN 的名

字(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，键入命令：

harbour(config)#config vlan market add port 1-5 untagged

上述命令也可简写为：con vl market ad po 1-5 un

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

2.2.4 命令中的符号

您可能会在命令格式中看到各种符号，这些符号只是说明您该如何输入该命令，但不是命令本身的一个部分。表 2-1 对这些符号进行了概要说明。

表 2-1 命令行中的符号

符号	描述
尖括号 < >	尖括号表示该命令的该部分必须输入一个参数。 例如命令：create vlan <name> 您必须在<name>那个位置输入一个合法的字符串作为您所创建的 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，您必须选择输入其中一项。例如命令： config stpd default [enable|disable] 中括号内包含由竖直线分隔的两个可选项，您必须输入 enable 或者 disable。如果中括号中只有一个可选项，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。 例如命令：show vlan {<name>}*1 表示您可以直接输入 show vlan ，也可以在 show vlan 后加上已经创建的某个 vlan 的名字。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 交换机的端口表示

对于 FlexHammer5010 来说，端口参数<portlist>可以有以下几种表示方法：

- 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，中间用符号“-”连接：port 1-4　表示端口 1、2、3、4
- 表示多个端口，中间用逗号隔开：port　1-4，5，8　表示端口 1、2、3、4、5、8

2.2.6 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

  当尖括号中是两个由减号连接的数值时，表示该参数是取值范围在那两个数值之间的某个数。例如<1-255>表示用户可以输入大于等于 1 并且小于等于 255 之间的任意一个整数，比如 2 就是一个合法的数字。

- IP地址

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

- 端口列表

  当尖括号中是 portlist 时，表示该参数是输入端口列表。端口列表中的多个端口之间用逗号“,”分隔，如果是连续的多个端口号可以用该连续端口的最小端口加上减号“-”再加上该连续端口的最大端口号表示。例如：输入 1，3-6，8 表示的端口列表为：1，3，4，5，6，8。

- 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“？”键查看该部分参数的命令说明。例如：<macaddr> 表示要输入的是一个 16 进制的 MAC 地址，例如输入 005023344325 就是一个合法的 MAC 地址，而<name>则表示要输入一个字符串做为某个对象的名字。

2.2.7 行编辑命令

表 2-2 命令行中的行编辑命令

符号	描述
BackSpace 键或 Del 键或 Ctrl+h	向左删除一个字符
向上箭头键或 Ctrl+p	调用上一个历史命令
向左箭头键或 Ctrl+b	将光标向左移动一格
向右箭头键或 Ctrl+f	将光标向右移动一格
向下箭头键或 Ctrl+n	如果前边使用过向上箭头调用上一个历史命令，再单击向下箭头键可以显示下一个历史命

	令
Ctrl+a	将光标移动到行首
Ctrl+e	将光标移动到行尾
Ctrl+d	将光标所在位置的字符删除
Ctrl+k	将光标以后的字符全部删除
Ctrl+t	将光标所在的字符和光标左边的那个字符互相调换，并将光标向右移动一格
Ctrl+u	整行删除
Ctrl+w	将光标左边的字符全部删除

说明：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 配置交换机方式，不支持串口配置。而命令 Ctrl+h、Ctrl+p、Ctrl+b、Ctrl+f 和 Ctrl+n 对上述两种登录方式均支持。

2.2.8 命令模式

HammerOS 的命令行提供了两种模式，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。

- 只读模式的提示符以“>” 结尾，表示为“Harbour>”，进入配置模式后，提示符以“#”结尾，表示为“Harbour(config)#”。只有管理员才能进入配置模式，并且要输入进入配置模式的密码。
- 在配置模式下输入命令“interface <vlanname>”，就会进入相应的接口配置模式，提示符为“HammerOS(config-if)#”。

有关只读模式和配置模式的详细信息请参阅本章后续内容

2.3 常用命令

2.3.1 enable

【命令作用】用于由只读模式进入配置模式

【命令格式】enable

【命令模式】只读模式

【使用指导】只读模式的提示符以“>”结尾，表示为“Harbour>”，进入配置模式后，提示符以 “#”结尾，表示为“Harbour(config)#”。只有管理员才能进入配置模式，并且要输入进

入配置模式的密码。

【配置实例】由只读模式进入配置模式

```
Harbour>enable

Password：<enable-password>

Harbour(config)#
```

2.3.2 show history

【命令作用】HammerOS 能记住用户最近输入的 20 个历史命令。您可以使用以下命令 show history 来显示已经输入过的命令清单，同时您也可以用上下箭头键调用上一个或者下一个历史命令。详细内容可见上表：2-2。

【命令格式】show history

【命令模式】只读模式和配置模式

【配置实例】显示最近输入的历史命令

```
Harbour>show history

show history
list
show history
enable
show idle-timeout
exit
```

2.3.3 exit

【命令作用】退出当前模式，返回上一模式

【命令格式】exit

【命令模式】只读模式和配置模式

【使用指导】在只读模式下使用 exit 命令，将退出 HammerOS 系统，与 Quit，Logout 效果一样；
在配置模式下使用 exit 命令将退回到只读模式。

【配置实例】在只读模式下使用 exit 命令

```
Harbour>exit

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

在配置模式下使用 exit 命令

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

2.3.4 show version

【命令作用】显示交换机的版本信息

【命令格式】show version

【使用指导】显示内容包括产品的硬件版本号、软件版本号、生产日期、产品序列号以及设备的 MAC 地址

【命令模式】只读模式和配置模式

【配置实例】在交换机上显示版本信息

```
Harbour>show version

  Product    Name: FlexHammer5010
Hardware Version: Version 1.22
Bootrom  Version: Version 1.1
Software Version: Version 1.2(Release 1.21  Apr 22 2003 10:17:33)
Manufacture Date: 2002-12-26
Serial   Number: 01010033A122022000001
Base MAC Address: 00053b58013a

  Copyright(c) 2000-2001 by Harbour Networks, Ltd.
```

2.3.5 terminal length

【命令作用】设置终端每屏显示行数

【命令格式】terminal length <0-512>

【命令参数】length 指定的行数，范围从 0 至 512

【默认状态】每屏显示 20 行

【命令模式】只读模式和配置模式

【使用指导】如果参数 length 设为 0，则对每屏显示的行数不作限制

2.3.6 help

【命令作用】输出关于怎么使用“?”寻求帮助提示的文字

【命令格式】help

【命令模式】只读模式和配置模式

【配置实例】使用 help 命令

```
Harbour(config)#help

HammerOS provides help feature as described blow。
Anytime you need help, just press "?" and don't
press Enter you can see each possible command argument
and its description。

You can also input "list" and then press Enter
to execute this helpful command to view the list of
commands you can use。
```

该提示信息的大意是：通过以下两种方法，可以获得 HammerOS 提供的帮助信息：

一种方法是在命令行中输入“？”，不需按回车键，就可以看到每一个可能的命令参数以及相应的命令功能描述。

另一种方法是键入命令 list，按回车键，系统将显示当前命令模式下的所有命令清单，您可以从中选择需要的命令。

2.3.7 who

【命令作用】显示当前有哪些用户连接到目标机器

【命令格式】who

who am i

【命令模式】只读模式和配置模式

【使用指导】命令 who 显示所有连接到交换机的用户信息

命令 who am i 只显示自己（已与交换机连接）的信息

【配置实例】

```
Harbour(config)#who

SessionID - UserName ------- LOCATION ------- MODE ----
3            admin           console        CONFIG    (That's me。)
Total 1 sessions in current system

Harbour(config)#who am i

I am *Session [3] :  user admin connected from console。
```

2.3.8 list

【命令作用】显示当前模式下所有的命令

【命令格式】list

【命令模式】只读模式和配置模式

【配置实例】

```
Harbour>list

  clear
  enable
  exit
  help
  list
  logout
  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>
  quit
  show ACL [<name>|all]
  show arp {[<A.B.C.D>|permanent]}*1
```

```
show fdb  {[mac] <macaddr>}*1 {[vlan] <name>}*1
show fdb agingtime
show fdb permanent {[mac] <macaddr>}*1 {[vlan] <name>}*1
show history
show idle-timeout
show interface {<IFNAME>}*1
show ip route
show ip route <A.B.C.D/M>
show ip route <A.B.C.D>
show ip route [connected|static]
（.....省略了部分显示内容）
```

【相关命令】list<pattern>，该命令可根据关键字查找命令

2.3.9 show services

【命令作用】显示系统 services 状态

【命令格式】show services

【命令模式】只读模式和配置模式

【配置实例】

```
Harbour(config)#show services

Service telnet is up.
Service acl is down.
Service qos is down.
Service dhcprelay is down.
Service snmp agent is up.
Service snmp rmon is down.
Service snmp trap support is down.
```

2.3.10 quit/logout

【命令作用】关闭和目标机之间的连接，退出 HammerOS 系统

【命令格式】quit

logout

【命令模式】只读模式和配置模式

【使用指导】命令 quit 与命令 logout 作用相同

【配置实例】使用 quit 命令退出 HammerOS 系统

```
Harbour> quit

Quit.
Disconnected.
Thanks for using Harbour Networks's product.
Bye!
```

2.3.11 hostname

【命令作用】设置主机名称

【命令格式】hostname <hostname>

【命令模式】配置模式

【使用指导】在同一个网络中，最好统一规划主机名称

【配置实例】

```
Harbour(config)#hostname useA
useA(config)#
```

2.3.12 clear

【命令作用】清除屏幕显示

【命令格式】clear

【命令模式】任意模式

【使用指导】当屏幕显示内容太多，而且对您没有用处时，可以使用此命令

2.3.13 idle-timeout

【命令作用】设置系统的空闲超时时间。该时间是指对交换机进行的相邻两次操作之间所允许的最大空闲时间。当超过该时间时系统将自动执行 logout 操作。

【命令格式】idle-timeout <0-35791>

【命令模式】配置模式

【使用指导】<0-35791>表示空闲超时时间的范围，单位：分钟。当输入 0 时表示不对系统的空闲时间进行限制。

【配置实例】设置系统的空闲超时时间为 10 分钟

```
Harbour(config)#idle-timeout 10
```

【相关命令】show idle-timeout

该命令用于查看当前系统的空闲超时时间。

2.3.14 config timezone

【命令作用】配置交换机时区

【命令格式】config timezone <name> [positive|negative] <0-12> {<1-59>}*1

【参数说明】name 为本交换机时区名，输入 positive 表示在东区，输入 negative 表示在西区，<0-12>为小时数，<1-59>为分钟数。

【命令模式】配置模式

【配置实例】中国时区位于东 8 区

```
Harbour(config)#config timezone CST positive 8
```

2.3.15 show running-config

【命令作用】显示当前系统配置

【命令格式】show running-config

【命令模式】配置模式

【使用指导】这是一个很常用的命令，可以帮助系统管理员查看当前的系统配置情况

【配置实例】

```
Harbour(config)#show running-config

!HammerOS system config file ------------------------
!Syslog config
!Port config
!VLAN config
!FDB entry config
!Acl config
!Qos config
!Dscp config
!Tos config
!Bandwidth config
!Traceroute config
!Stpd config
!Route-policy rules config
!Interface config
!Static routes config
!Igmp snooping
!Arp config
!Sntp config
!Timezone config
!Dot1x config
!Port bind config
!RADIUS client config
!Usermanage config
!snmp config
!H.Link config
!Network access-control service config
!vstack cluster config
!end of config --------------------------------------
```

2.3.16 show startup-config

【命令作用】显示启动配置信息

【命令格式】show startup-config

【命令模式】配置模式

【使用指导】只有保存过系统配置文件才可以查看其内容

2.3.17 save configuration

【命令作用】保存当前的配置

【命令格式】save configuration

【命令模式】配置模式

【使用指导】如果您想让当前配置在交换机断电或重新启动后依然有效，切记一定要使用此命令保存您的配置

【配置实例】

```
Harbour(config)#save configuration

Trying save configuration to flash, please wait ......
Preparing configuration data to save...Done

Starting write configuration data to flash...Done。

Configuration save to flash successfully
```

2.3.18 erase startup-config

【命令作用】删除交换机中保存的系统启动配置信息

【命令格式】erase startup-config

【命令模式】配置模式

【使用指导】如果您想重新配置交换机的启动配置信息，请使用此命令删除以前的配置

【配置实例】

```
Harbour(config)#erase startup-config

Are you sure want to erase startup-config? [Y/N]y
Trying erase all configuration from flash, please wait ......
  finished
Successfully erase all configuration info from flash
```

2.3.19 reboot

【命令作用】重新启动交换机

【命令格式】reboot

【命令模式】配置模式

【使用指导】重新启动交换机前，如果需要保存配置数据，请键入 save configuration。

如果您想使改变的配置在重新启动交换机或者交换机关机再开后仍然能有效，请切记在进行配置后使用“save configuration”命令把配置保存到交换机中。

2.3.20 常用命令列表

表 2-3 命令行中只读模式下的常用命令

命令	描述
clear	清除屏幕显示
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 <pattrn>	显示在当前模式下含有关键字 pattern 的所有的命令
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
show services	显示当前系统提供的服务
show version	显示 HammerOS 的版本信息
who	显示当前连接到交换机的用户
show idle-timeout	显示 idle timeout（空闲超时）时间

只读模式下除了 enable 以外的所有命令在配置模式下都有效，所以在表 2-4 列出配置模式下常用命令时就不再重复这些命令。

表 2-4 命令行中配置模式下的一些常用命令

命令	描述
clear timezone	取消交换机的时区配置，恢复缺省时区配置
config timezone <name> [positive|negative] <0-12> {<1-59>}*1	配置交换机时区
enable-password	修改进入配置模式的密码，必须大于或者等于 6 个字符
erase {startup-config}*1	删除交换机启动配置
hostname <hostname>	设置系统的网络名称，例如，在本手册中，网络名称为 HammerOS
idle-timeout <0-35791>	设置经过多长的空闲等待系统自动进入登录前的状态
kill session <1-24>	强制断开特定 telnet 连接
login-password	设置登录密码
reboot	重新启动交换机
save configuration	保存系统配置信息
show interface {<IFNAME>}*1	显示接口状态
show running-config	显示系统的运行配置
show time	显示系统时间信息
show version	显示系统版本信息
terminal length <0-512>	设置终端屏幕所显示的行数
user add <username> login-password	添加登录密码为<login_password>的用户<username>到系统中

<login_password>	
user delete <username>	从系统中删除用户<username>
user enable-password <username>	设置用户<username>的配置密码
user list	显示所有系统用户
user login-password <username>	设置系统用户<username>的登录密码
user role <username> ADMIN enable-password <enable_password>	把用户<username>转变为系统管理员，且密码为<enable_password>
user role <username> NORMAL	把用户<username>转变为普通用户
who am i	仅仅显示用户自己的连接信息
reboot	重新启动交换机

HammerOS 命令行的所有命令都是不区分大小写的。

2.4 设置访问权限

HammerOS 中提供了两种用户权限：

- NORMAL普通用户

  普通用户能查看大部分系统信息，但不能查看系统中的用户信息和系统的配置信息（主要指系统中的配置文件内容以及系统全局配置信息）。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。

- ADMIN 管理员

  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用户帐号，删除用户帐号，设置修改用户密码，以及进行系统全局信息配置等。

2.4.1 系统缺省用户帐号

系统缺省内置了一个管理员用户帐号，用户名是 admin，缺省密码是 harbour。缺省用户 admin 的帐号不能被删除，用户也不能被修改，只能修改他的密码。

2.4.2 增加用户帐号

可以按照以下步骤建立用户帐号：

1. 以用户名 admin 登录（或者用任何其他管理员的用户帐号登录）；

2. 输入只读密码，进入只读模式；

3. 在只读模式下，输入 enable 命令，输入配置模式密码，进入配置模式；

4. 在配置模式下，利用以下命令创建一个用户帐号：

【命令格式】user add <username> login-password <login_password>

【参数说明】<username>是用户的名称，<login_password>代表用户登录密码。

【使用指导】其中<username>是所要添加用户的名称，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、下划线且长度为 4-20 的字符串。<login_password>是该用户的登录密码，可以是由任意字符组成的长度为 6-20 的字符串。

【命令模式】配置模式

【配置实例】增加一个用户，用户名为 manager，登录密码为 harbour，在配置模式下，键入命令：

```
Harbour(config)#user add manager login-password harbour

Successfully added user manager as a NORMAL_USER ,
To change user role use “user role” command
```

系统对于用户名是不区分大小写的，对密码区分大小写。

通过上述方法创建的用户一般都是普通用户，如果想要创建一个管理员的用户帐号，可以在按照以上步骤创建完用户帐号后，对用户权限进行修改。具体见本章下一节（修改用户权限）

2.4.3 修改用户权限

由于本系统中有两个不同级别的用户，所以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。

将一个用户设为管理员，使用如下命令：

【命令格式】user role <username> admin enable-password <enable_password>

【参数说明】<username>是该用户的用户名，<enable_password>是该用户的登录密码。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#user add manager login-password 111111
Harbour(config)#user role manager admin enable-password 111222

Successfully change user manager to ADMIN mode.
```

将管理员设为普通用户，使用如下命令：

【命令格式】user role <username> normal

【参数说明】<username>是该管理员的用户名

【配置实例】将管理员用户 manager 的权限改为普通用户

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

Successfully change user manager to NORMAL mode.
```

2.4.4 查看系统用户信息

查看用户列表，使用命令 user list

例如:在配置模式下，键入命令：user list。显示如下信息：

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

2.4.5 删除用户帐号

可以用以下命令删除一个用户帐号：

【命令格式】user delete <username>

【参数说明】username 是欲删除用户帐号的用户名。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#user delete manager

Successfully delete user manager .
```

2.4.6 修改密码

- 管理员修改自己的登录密码，在配置模式下输入 login-password。根据提示，输入新密码和确认新密码即可。
- 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，在配置模式下输入 enable-password。然后在提示符下输入新密码和确认新密码即可。
- 管理员还能够重新设置其他用户的密码，用以下命令：user login-password <username>、user enable-password <username>。并在提示符下输入新密码和确认新密码，就可以设置用户的登录密码和配置模式密码。

例如：修改用户 manager 的登录密码为 network，键入命令： user login-password manager

按回车，执行该命令。并输入新密码：network 和确认新密码：network。

修改用户 manager 进入配置模式的密码为 enter_config，键入命令：user enable-password manager

按回车，执行该命令。输入新密码： enter_config 和确认新密码： enter_config

注意：执行该命令必须确保 manager 是 admin 用户，否则系统会报错！

2.5 管理交换机的途径

本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。

本交换机同时能支持多个连接：

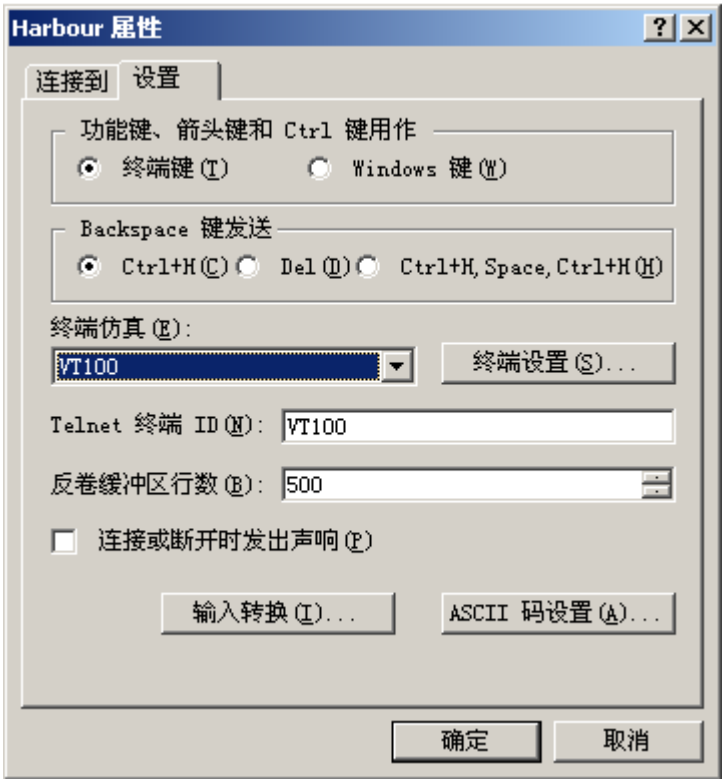
- 一个Console口连接
- 最多同时能支持3个telnet连接
- 最多同时能支持4个用户连接
- 一个用户最多同时开2个连接

2.5.1 使用 Console 口连接到交换机

可以通过在交换机前面板上标有“Console”字样的 RJ-45 串口与终端计算机的 COM 口相连。连接到 Console 端口的终端应按如下配置：

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

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。如下图所示：



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

例如：通过 Console 口连接登录到交换机后，我们给交换机配置一个 192.168.0.232 的 IP 地址，按以下步骤进行：

第一步：将交换机的 Console 口和特定终端连接起来，正常给交换机供电。

第二步：待 HammerOS 成功启动后，就可以看到交换机的提示登录信息：

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

第三步：此时，系统要求您输入用户名和密码。

- 如果您是首次登录交换机，您就应该使用缺省的用户名 admin 进行登录，此时输入登录密码 harbour，按回车键，进入只读模式，输入 enable，按回车，键入配置模式缺省密码 harbour。
- 如果您已经分配了一个自己的用户名和密码，而且您已有系统管理员的权限，那么，登录时就使用自己的用户名和密码。

第四步：当您成功登录交换机时，系统显示如下信息：Harbour(config)#，表明您可以对命令行进行操作了。

第五步：然后给交换机的某个 VLAN（可以是 default VLAN 或者新创建的 VLAN，此处以 default VLAN 为例）配置 IP 地址。输入命令：config vlan default ipaddress 192.168.0.232/24。成功执行该命令后，就可以从该 VLAN 的端口上以该 VLAN 的 IP 地址 telnet 到交换机的命令行接口。

第六步：保存配置，键入命令：save configuration

```
Trying save configuration to flash, please wait ......
Preparing configuration data to save...Done。
Starting write configuration data to flash...Done。
Configuration save to flash successfully。
```

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

第七步：当您完成对交换机的操作后，键入命令：logout 或 exit 就可以断开与交换机的连接，并退出命令行界面。

2.5.2 使用 telnet 管理交换机

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，首先应该给交换机配置一个 IP 地址。然后在配置模式下输入命令：telnet <A.B.C.D>

注意：这里的参数<A.B.C.D>必须与本交换机的 IP 地址在同一网段。

例如：远程登录一台 IP 地址为 192.168.0.232 的交换机

在配置模式下，键入命令：

```
harbour(config)#telnet 192.168.0.232

Connected to 192.168.0.232。
Press Ctrl-Q to force exit telnet。
HammerOS Version1.1 on FlexHammer。
Login：
```

输入用户名和密码进行登录。

2.5.3 打开和关闭 Telnet 服务

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

1．打开 Telnet 服务：

【命令格式】service telnet enable

【配置实例】

```
Harbour(config)#service telnet enable

Successfully changed telnet service to up.
```

2．关闭 Telnet 服务：

【命令格式】service telnet disable

【配置实例】

```
Harbour(config)#service telnet disable

Successfully changed telnet service to down.
```

可以用 show service 命令查看系统提供的 Telnet 服务是否被打开：如果显示 Service telnet is up. 则表明 Telnet 已经打开；如果显示 Service telnet is down. 则表明 Telnet 已经关闭。

2.5.4 强制关闭一个非法 Telnet 连接

具有管理员权限的用户可以强制断开一个 Telnet 连接，步骤如下：

第一步：用 who 命令查看当前连接的用户。

第二步：如果发现有一个用户连接是非法的，那么可以根据用 who 命令所看到的该连接的 sessionID，然后用以下命令强制断开那个连接：kill session <1-24>，其中<1-24>是 sessionID 的取值范围。

如果您输入的 sessionID 是通过 console 口连接的，您将不能删除这个用户，此时系统会出现以下提示信息：You can't kill a console session.

通过强制关闭非法的 telnet 连接可以防止非法用户登录，从而提高系统的安全特性。

2.6 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系统的方法。当网络管理者利用 SNMP 管理交换机时，要求在管理平台上建立 Management Information Base（MIB 管理信息库），使网络中的所有变量都存放在 MIB 数据结构中。

2.6.1 打开或关闭 SNMP 服务

1．打开 SNMP 服务：

【命令格式】service snmp enable

【配置实例】

```
Harbour(config)#service snmp enable

Successfully changed snmp agent service to up.
```

2．关闭 SNMP 服务：

【命令格式】service snmp disable

【配置实例】

```
Harbour(config)#service snmp disable

Successfully changed snmp agent service to down.
```

可以用 show service 命令查看系统提供的 snmp 服务的状态：

如果显示 Service snmp agent is up，表明 snmp 服务已经被打开；

如果显示 Service snmp agent is down，表明 snmp 服务已经关闭。

2.6.2 SNMP 参数配置

对 SNMP 的参数配置使用以下命令：

【命令格式】config snmp community [readonly|readwrite] <string>

【使用指导】community 字符串为远程网络管理员配置交换机提供了一种用户确认机制。在交换机上有两种 Community 字符串：读确认 Community 字符串（readonly）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（readwrite）提供了对交换机读写操作的权限，缺省值为 private。

【命令模式】配置模式

【相关命令】show snmp community-string

该命令可用于查看 SNMP 的 Community 字符串信息。

2.6.3 打开或关闭代理发送 trap 报文功能

【命令格式】service snmp trap [enable|disable]

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

【命令模式】配置模式

2.6.4 配置 SNMP 的 trapagent-address

【命令格式】config snmp trapagent-address [<A.B.C.D>|auto]

【使用指导】选择<A.B.C.D>是 trap 的目的 ip 地址；选择 auto,表示由系统填写本设备的 ip 地址

【命令模式】配置模式

service snmp rmon [enable|disable]	配置 snmp rmon 服务，打开或关闭 snmp rmon 服务，enable 为打开 snmp rmon 服务，disable 为关闭 snmp rmon 服务

2.6.5 配置 SNMP 的 RMON 服务

【命令格式】config snmp rmon [enable|disable]

【使用指导】enable 为打开 snmp rmon 服务；disable 为关闭 snmp rmon 服务

【命令模式】配置模式

2.6.6 添加 trapreceiver

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

【使用指导】trapreceiver 是接收 trap 信息的主机；<A.B.C.D>为 traprceiver 的 IP 地址；

v1/v2c 表示 trap 两个版本;如果这个 traprceiver 同时还承担对交换机的远程配置，那么可以为其设置 community 字符串。

【命令模式】配置模式

【配置实例】添加一个 trapreceiver，地址为 10.1.30.100，trap 的版本是 v1，键入命令：

```
Harbour(config)#config snmp trapreceiver add 10.1.30.100 version v1

Successfully added trapreceiver IP address is 10.1.30.100
The trap version is v1
The default trap community is public
```

2.6.7 删除 trapreceiver

【命令格式】config snmp trapreceiver delete <A.B.C.D>

【使用指导】<A.B.C.D>为 trapreceiver 的 IP 地址

【命令模式】配置模式

【配置实例】删除一个地址为 10.1.20.20 的 trapreceiver

```
Harbour(config)#config snmp trapreceiver delete 10.1.20.20
```

2.6.8 显示 trapreceiver 信息

【命令格式】show snmp trapreceiver

【命令模式】配置模式

【配置实例】显示 SNMP 的 trapreceiver 信息

```
Harbour(config)#show snmp trapreceiver

IP address            Version        Community
12.12.12.1             v1              public
Total 1 trapreceiver IP address in system.
```

2.7 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。

2.7.1 增加静态路由

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

ip route <A.B.C.D > <A.B.C.D> <A.B.C.D>{<1-255>}*1

【使用指导】第一个参数<A.B.C.D/M>为目的网段的 IP 地址和子网掩码长度，或者按照第二种命令格式将子网掩码由长度 M 的形式改为 IP 地址的形式。最后一个参数<A.B.C.D>为下一跳的 IP 地址。<1-255>表示路由的优先级，不设置时默认为 1，表示建立的这条静态路由具有最高优先级。

【命令模式】配置模式

【配置实例】添加一条去往 192.168.1.88 的静态路由，下一跳地址为 192.168.0.3。

```
Harbour(config)#ip route 192.168.1.88/24 192.168.0.3
```

或者可以用下一条命令增加一条静态路由信息：

```
Harbour(config)#ip route 192.168.1.88 255.255.255.0 192.168.0.3
```

2.7.2 删除静态路由

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

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

【使用指导】第一个参数<A.B.C.D/M>为目的网段的 IP 地址和子网掩码长度，或者按照第二种命令格式将子网掩码由长度 M 的形式改为 IP 地址的形式。最后一个参数<A.B.C.D>为下一跳的 IP 地址。

【命令模式】配置模式

【配置实例】删除一条去往 192.168.1.88 的静态路由，其下一跳地址为 192.168.0.3

```
Harbour(config)#no ip route 192.168.1.88/24 192.168.0.3
```

或者可以用下一条命令删除静态路由：

```
Harbour(config)#no ip route 192.168.1.88 255.255.255.0 192.168.0.3
```

2.7.3 显示静态路由信息：

【命令格式】show ip route

【使用指导】显示的内容包括目标 IP 地址、子网掩码和下一跳网关的 IP 地址。

【命令模式】只读模式和配置模式

【配置实例】

```
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 ***
```

2.7.4 配置静态路由命令列表

参数	描述
ip route <A.B.C.D/M> <A.B.C.D> {<1-255>}*1	添加一条静态路由，M 为子网掩码长度
ip route <A.B.C.D > <A.B.C.D> <A.B.C.D>{<1-255>}*1	添加一条静态路由，子网掩码采用 IP 地址的形式
no ip route <A.B.C.D/M> <A.B.C.D> {<1-255>}*1	删除一条静态路由，M 为子网掩码长度
no ip route <A.B.C.D> <A.B.C.D> <A.B.C.D> {<1-255>}*1	删除一条静态路由，子网掩码采用 IP 地址的形式
show ip route	显示静态路由信息
show ip route <A.B.C.D/M>	显示属于<A.B.C.D/M>网段的静态路由信息
show ip route <A.B.C.D>	显示目的地址为<A.B.C.D>的静态路由信息
show ip route [connected|static]	显示静态路由的 connected 信息或 static 信息
show ip route summary	显示静态路由的描述信息

2.8 存取配置文件及升级 HammerOS

在每次对交换机的配置进行修改后，都要对所做的修改进行保存。键入命令“save configuration”，将修改后的配置保存到交换机的扩展 FLASH 中。当显示如下字符串时：Configuration save to flash successfully。表明保存配置已经成功。

用户还可以把一份好的配置文件保存到文本文件中，在需要的时候（例如不小心把交换机配置搞乱了，不知道怎样把配置恢复到以前的状态时）再把配置文件下载到交换机中。下载可以有 2 种方法，可以用 FTP 下载，也可用 Xmodem 下载。

此外，用户可以将交换机中的配置文件内容上传到本地磁盘文件中，上传可以有 2 种方法，可以用 FTP 上传，也可用 Xmodem 上传。

2.8.1 通过 FTP 协议下载配置文件和 HammerOS

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

第二步：输入命令 download ftp [config-file|hammeros] <A.B.C.D> <username> <password>

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

第三步：等待下载完毕后，输入 reboot 命令重新启动交换机。

例如：假设地址 10.1.30.16 处存在一 FTP 服务器，并且此服务器上存在一个名为 sysconfig.txt 的配置文件，用户 useA 为此服务器的合法用户，密码是 harbour，在 HammerOS 配置模式下，输入命令：

```
Harbour(config)#download ftp config-file 10.1.30.16 useA harbour
  sysconfig.txt
```

系统显示如下信息

```
Trying download file from ftp server, please wait...

Successfully finished receiving file.

Trying write file to flash......
Finished.

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

2.8.2 通过使用 Xmodem 协议下载配置文件和 HammerOS

使用 Xmodem 协议下载文件，利用如下命令：

【命令格式】download xmodem [hammeros|config-file]{baudrate [9600|115200]}*1

【参数说明】选择 hammeros，下载文件为系统应用程序文件；选择 config-file， 下载文件为系统配置信息文件，如果选择 baudrate 则用户可以选择下载文件的带宽：9600 或 115200

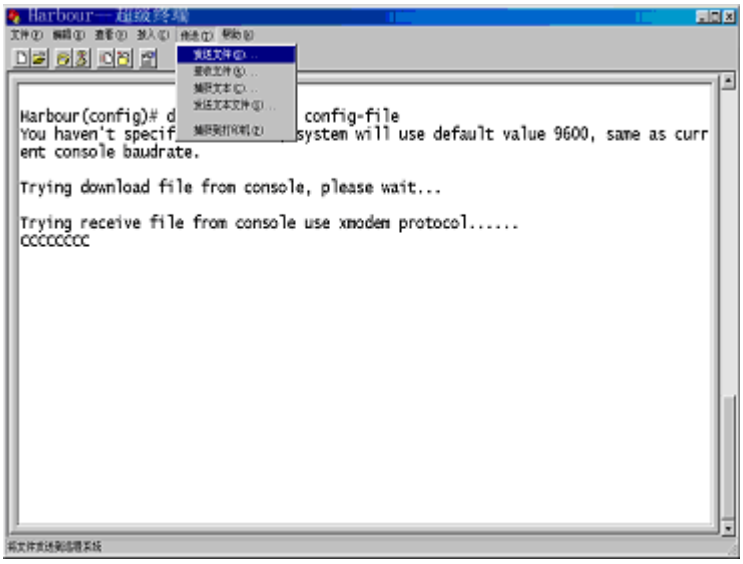
【配置实例】假设您机器上的 c:\windows\desktop 目录下存在一个系统配置文件：sysconfig.txt，把它下载到您的交换机上，可以如下操作：

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

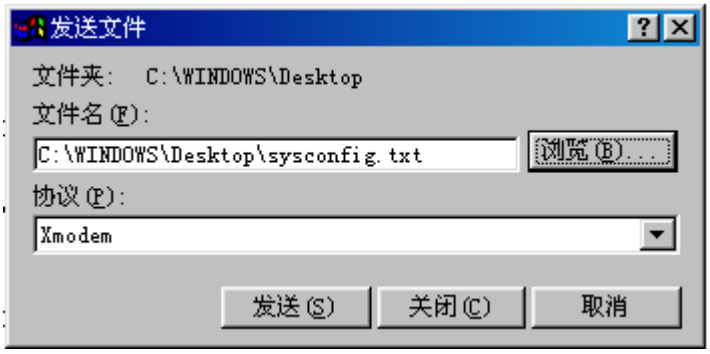
第二步：输入命令 download xmodem config-file。显示信息如下：

```
You haven't specified baudrate, system will use default value 9600, same as
   current console baudrate.

Trying download file from console, please wait...

Trying receive file from console use xmodem protocol......
CCC
```

第三步：打开串口超级终端的发送文件菜单



选择您所要下载的配置文件及协议（一定用 Xmodem）



选择“发送”，系统开始下载指定文件信息。

第四步：等待下载完毕后，显示下面信息，表明下载成功，


```
Successfully finished receiving file.

Trying write file to flash......Finished.

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

输入 reboot 命令重新启动交换机。

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

2.8.3 通过 FTP 协议上传配置文件和 HammerOS

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

【命令格式】upload ftp [hammeros|config-file] <A.B.C.D> <username> <password> <filename>

【参数说明】选择 hammeros，上传文件为系统应用程序文件；

选择 config-file，上传文件为系统配置信息文件。

<A.B.C.D>为 FTP 服务器的 IP 地址；

<username>为 FTP 服务器的用户名；

<password> FTP 服务器的密码；

<filename>为所生成的文件名。

【配置实例】假设地址 10.1.30.16 处存在一 FTP 服务器，并且此服务器上存在一个名为 sysconfig.txt 的空白文件，用户 useA 为此服务器的合法用户，密码是 harbour，并具有上传文件的写权限。在 HammerOS 配置模式下，输入命令：

```
Harbour(config)#upload ftp config-file 10.1.30.16 useA harbour
  sysconfig.txt
```

系统显示如下信息

```
Trying upload file to ftp server, please wait...
Successfully finished Upload file.
Finished.
You've successfully upload config file.
```

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

2.8.4 通过使用 Xmodem 协议上传配置文件和 HammerOS

通过 Xmodem 协议上传文件，即将 FLASH 中的文件上传到主机上，利用如下命令：

【命令格式】upload xmodem [hammeros|config-file]{baudrate [9600|115200]}*1

【参数说明】选择 hammeros，上传文件为系统应用程序文件；

选择 config-file，上传文件为系统配置信息文件。

如果选择 baudrate 则用户可以选择上传文件的带宽：9600 或 115200。不输入时，系统默认使用 9600。

【命令模式】配置模式

【配置实例】将系统应用程序文件上传到本地磁盘文件中，按以下步骤进行：

第一步：在配置模式下，键入命令：

```
Harbour(config)#upload xmodem hammeros baudrate 115200
```

按回车，显示如下信息：

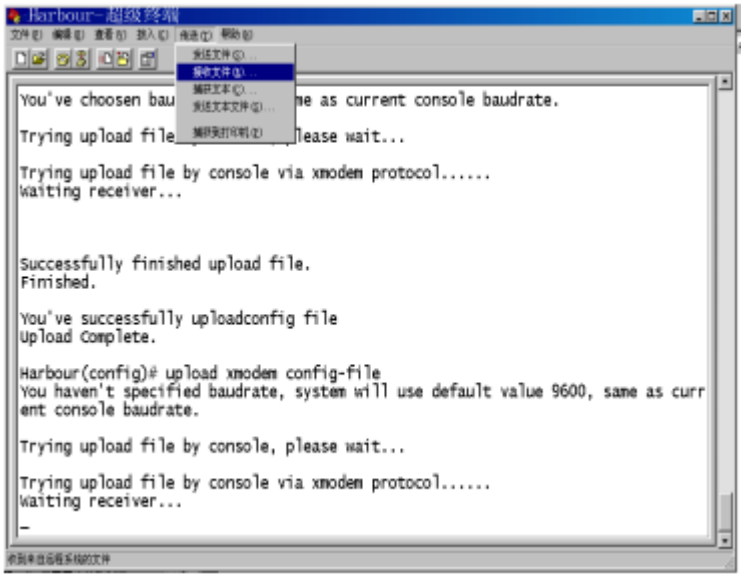
```
System's current console baudrate is 9600.
You've choosen change console baudrate to 115200 when upload file.
Please change your terminal's baudrate to 115200 in 10 seconds.
After that, you can start receive file.
```

第二步：迅速改变终端的带宽为 115200bps

此时一定要在 10 秒之内改变终端的连接带宽为 115200bps，待完成操作后要恢复终端连接带宽为 9600bps 时，要先挂断再连并在 10 秒之内改回 9600。

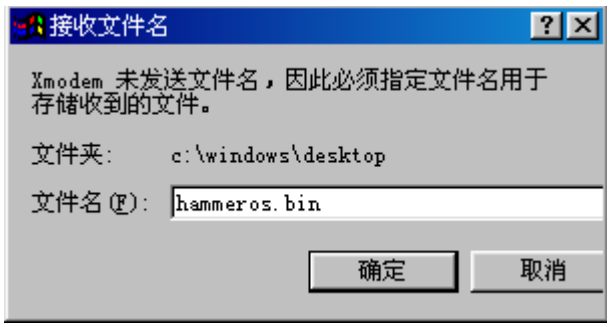
点击“配置”按钮后，在下图所示的端口设置中，将波特率设为 115200，然后点击“确定”即可。

第三步：在超级终端中，选择传送菜单的“接收文件”



选择存放系统应用程序文件所在的目录，使用的接收协议是 Xmodem。

点击“接收”按钮，并输入系统应用程序文件名称，例如：hammeros.bin



点击“确定”按钮出现界面如下：

文件上传完毕出现如下提示信息：

```
Successfully finished upload file.
Finished.

You've successfully uploadimage file
Upload Complete.
```

到此为止，配置信息上传完毕。

通过文件的上传和下载，可以很方便地对多台相同配置的交换机进行配置。

2.9 网络状态及系统的检测

2.9.1 用 ping 命令检测网络基本连接

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。ping 命令的语法是：

ping {[-t]}*1 {[-count] <1-65535>}*1 {[-size] <0-6400>}*1 {[-waittime] <1-255>}*1 {[-ttl] <1-255>}*1 {[-pattern] <user_pattern>}*1 <A.B.C.D>

ping 命令的众多选项可以都不输入，而使用最简单的格式。例如：ping 192.168.0.1，用来测试交换机是否可以跟 IP 地址为 192.168.0.1 的设备连接通信。如果设备连通，则出现以下信息：

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

Reply from 192.168.0.1 : bytes=56: icmp_seq=0 ttl=128 time=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
```

表 2-5 ping 命令选项

参数	描述
-t	使用 t 选项后，ping 命令将一直向目标 IP 地址发送 ICMP echo 消息，直到用户用 Ctrl+c 中断。

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

2.9.2 用 traceroute 命令检测设备间的报文行径

交换机提供了 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。traceroute 命令的语法是：

traceroute {[-a] <A.B.C.D>}*1 {[-f] <1-30>}*1 {[-m] <2-255>}*1 {[-p] <1-65535>}*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。例如：traceroute 202.96.13.137。通过该命令可以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。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。

如果设备连通，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   10.8.1.1         < 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，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   * * *
```

输入 CTRL+C 可以中断 traceroute 命令，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。

交换机提供了两种 traceroute 的发包方式，用户可以选择发送 UDP 数据报或者 ICMP 数据报，UNIX 操作系统中的 traceroute 程序发送 UDP 报文，而 Windows 98 则发送 ICMP 报文。选择 traceroute 发包模式的命令格式为：config tracert_mode [udp|icmp]

表 2-6 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

2.9.3 显示 CPU 利用率

使用以下命令显示 CPU 的利用率：show cpu usage。

例如：Harbour (config)#show cpu usage

```
cpu usage: 9%
```

2.9.4 显示内存状况

使用以下命令显示内存当前使用状况：show memory status

例如：Harbour (config)#show memory status

```
=============================================================
  =======
MODULE-NAME         32       64       128      256      512      1024
  2048
```



```
ROUTE           1104      6      1      5      0      0      2
VIRTUAL_END        0      0      0      0      1      0      0
MANAGE_CLI     24472   1375     73      2      6      0      0
RSTP               0      0      0      0    242      0      0
SLAB_SHOW          0      0      0      0      5      0      0
FDB                7      0      1     24      0      0      0
VLAN               0      0      1      0      0      0      0
ACL                0      0    240      0      0      0      0
RADIUS_CLIENT      3      1      1      0      0      0      0
ARP                0      1      0      0      0      0      0
TIMER              0      5      0      0      0      0      0
MANAGE_USER        3      2      0      0      0      0      0
20                 1      0      0      0      0      0      0
QoS                4      0      0      0      0      0      0
IGMP_SNOOPING      2      0      0      0      0      0      0
============================================================
  =======
MODULE-NAME       4096    8192    16K     32K     64K     128K
ROUTE              0      29      0       0       1       0
VIRTUAL_END        2       0      0       0       0       0
MANAGE_CLI         1       0      0       0       0       0
RSTP               0       0      0       0       0       0
SLAB_SHOW          0       0      0       0       0       0
FDB                0       0      0       0       0       0
VLAN               0       0      0       0       0       0
ACL                0       0      0       0       0       0
RADIUS_CLIENT      0       0      0       0       0       0
ARP                0       0      0       0       0       0
TIMER              0       0      0       0       0       0
MANAGE_USER        0       0      0       0       0       0
20                 0       0      0       0       0       0
QoS                0       0      0       0       0       0
IGMP_SNOOPING      0       0      0       0       0       0
===========Total             CacheSize:1720320             Total
  UsageMemSize:1498196==========
```

第3章 配置交换机的端口

这一章主要讲述如何使用 HammerOS 来配置 FlexHammer5010 的端口，主要包括：

- 打开或关闭指定端口
- 打开或关闭指定端口的自适应功能
- 配置端口速率
- 配置端口的半双工或全双工模式
- 配置端口的流控
- 配置多端口负载均衡组（Load Sharing）
- 端口镜像（Port mirroring）

交换机的端口可以连接 10Base-T、100Base-T 或者 1000Base-T 网络，可以工作在半双工或全双工模式，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，HammerOS 根据端口对端的性能自动调整端口的速率和双工模式。
- 用户也可以手工配置端口速率、双工模式和流控模式。流控功能与自协商是相对独立的，可以分别配置。

3.1 端口基本参数配置

3.1.1 使能或关闭指定的端口

对于启动后的交换机，在缺省情况下，端口都是使能的。当然，您可以根据实际需要对各个端口的状态进行配置。 利用以下命令使能或关闭一个或多个指定端口：

【命令格式】`config port [<portlist>|all] [enable|disable]`

【使用指导】参数`<portlist>`与 `all` 用于控制所要配置的端口，`portlist` 表示端口列表，允许一次配置多个端口；`all` 表明对所有端口进行操作。`enable` 与 `disable` 两个参数选择其一，如果键入 `enable`，则使能需要配置的端口；如果为 `disable`，则关闭这些端口。

【配置实例】关闭端口 1，3，5，7—12，配置如下：

```
Harbour(config)#config port 1,3,5,7-12 disable
```

3.1.2 配置端口的自适应模式

【命令格式】config port [<portlist>|all] auto [on|off]

【使用指导】参数<portlist>为端口列表，选择 all 表示对所有端口进行操作。选择 on 表示使能端口的自适应模式；选择 off 表示关闭端口的自适应模式。

【配置实例】关闭端口 24 的自适应模式

```
Harbour(config)#config port 24 auto off
```

3.1.3 配置端口的速率

【命令格式】config port [<portlist>|all] speed [10|100|1000]

【使用指导】参数<portlist>为端口列表，选择 all 表示对所有端口进行操作。选择 10 表示端口速度设置为 10M 模式，选择 100 表示端口速率设置为 100M 模式。选择 1000 表示端口速率设置为 1000M 模式。

【配置实例】将端口 25 的速率设置为 100Mbps

```
Harbour(config)#config port 25 speed 100
```

注意：

- **FlexHammer5010 以太网电口的速率只能是 10/100M，不可以配置为 1000M。扩展模块中如果插入的是千兆光模块，则其端口速度也不可以配置；如果是千兆电口模块，可以配置相应端口速率为 1000M 模式，但必须指明端口的主从关系，参见下一节内容。**
- **只有关闭端口的自适应模式才可以进行端口速率的配置。**

3.1.4 配置千兆电口的主从模式

【命令格式】config port [<portlist>|all] mode [master|slave]

【参数说明】参数<portlist>为端口列表，选择 all 表示对所有端口进行操作。

选择 master 把端口设置成主模式；选择 slave 表示把端口设置成从模式。

【使用指导】由于 FlexHammer5010 的上行端口可以是光口也可以是电口，如果是光口，其速率固定为 1000M，如果是电口，且您已手动指定了端口速率为 1000M，那么您还需要利用此命令将一端设置成主模式，另一端设置成从模式。

【命令模式】配置模式

3.1.5 配置端口的双工模式

【命令格式】config port [<portlist>|all] duplex [full|half]

【使用指导】参数<portlist>为端口列表，选择 all 表示对所有端口进行操作。选择 full 表示配置端口为全双工模式；选择 half 将端口设置为半双工模式。

【配置实例】将端口 24 设置为全双工模式

```
Harbour(config)#config port 24 duplex full
```

注意：只有关闭端口的自适应模式才可以进行端口双工模式的配置。

3.1.6 配置端口的流控

【命令格式】config port [<portlist>|all] flowcontrol [on|off]

【使用指导】参数<portlist>为端口列表，选择 all 表示对所有端口进行操作。选择 on 表示使能端口的流量控制功能；选择 off 表示关闭端口的流量控制功能。

【配置实例】使能所有端口的流量控制

```
Harbour(config)#config port all flowcontrol on
```

3.1.7 配置端口的地址学习功能

我们可以手工指定端口的地址学习功能：

【命令格式】config port [<portlist>|all] learn [on|off]

【参数说明】<portlist>表示端口的列表，all 表示所有的端口。选择 on 表示使能该端口的学习功能，选择 off 表示关闭该端口的学习功能。

【命令模式】配置模式

【配置实例】关闭端口 3 和 4 的自适应功能，并设置端口的速度为 10Mbps，双工模式为半双工，同时使能端口的地址学习功能，依次键入下面命令：

```
Harbour(config)#config port 3,4 auto off

Harbour(config)#config port 3,4 speed 10

Harbour(config)#config port 3,4 duplex half

Harbour(config)#config port 3,4 learn on

Harbour(config)#show port 3

------------------------------------------------------------------
  ------
              Port:3 's Configuration Information

Link State      : Up            Port State      : Enabled
Port Type       : 100BaseT       Speed          : 10
Autonegotiation  : Disabled       Duplex         : Half
Flowcontrol     : Disabled       Learn State     : Enabled

Port VLAN ID    : 2047
Port VLAN Name   : default
Port Summary    : normal
------------------------------------------------------------------
  ------
```

注意：千兆光口不支持半双工，不能工作在 10/100 兆模式。

3.1.8 端口配置命令列表

表 3-1 HammerOS 的端口配置命令表

命令	描述
config port [<portlist>|all] [enable|disable]	使能或关闭指定端口
config port [<portlist>|all] auto [on|off]	使能或关闭指定端口的自适应功能
config port [<portlist>|all] speed [10|100|1000]	配置端口的速度为 10 Mbps 或者 100Mbps 或者 1000Mbps
config port [<portlist>|all] duplex [full|half]	配置端口的双工模式为全双工或者半双工
config port [<portlist>|all] flowcontrol [on|off]	使能或关闭端口的流控制功能
config port [<portlist>|all] mode [master|slave]	配置千兆电口的主从模式
config port [<portlist>|all] learn [on|off]	使能或者关闭端口的地址学习功能
show port [<portlist>|all] {[configuration|stats]}*1	显示指定端口的信息 输入 configuration 选项时显示端口配置信息 输入 stats 选项时显示端口流量统计信息 缺省不输入任何选项时显示端口配置信息

3.2 多端口负载均衡组

HammerOS 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和增加冗余备份功能，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 就是一个逻辑端口。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 中的其他端口进行传输。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 中的所有端口进行传输，从而提升交换机之间的带宽。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度。同时，Load Sharing 对客户间的数据包的顺序提供了保障。

本公司的 Hammer 系列产品都支持 Load Sharing 功能，同时与 Intel 和 Cisco 同类产品的 Port Group 功能兼容。

注意：必须在相互连接的两台交换机上都设置 Load Sharing， 并且要对每对直接连接的两个做对应配置，否则会在网络中造成回路，导致交换机不能正常工作。

3.2.1 Load Sharing 规则

要设置 Load Sharing，必须创建 Load Sharing 的一组端口。Load Sharing 定义必须遵从以下规则：

- 用Load Sharing连接两个交换机时，要求Switch 1中Load Sharing的端口和Switch 2中Load Sharing的端口按端口号大小次序依次对应连接。例如，Switch 1的Load Sharing组中包括端口1、2、3、4，Switch 2的Load Sharing组中包括端口6、7、9、10，当两台交换机进行Load Sharing连接时，端口连接的对应关系为：1ー6，2ー7，3ー9，4ー10。
- 建议Load Sharing成员端口的速率保持一致，且必须处于全双工状态。
- FlexHammer5010最多可以设置6个Load Sharing组，每个Load Sharing组最多包含8个端口。
- 1个Load Sharing组相当于一个端口，因此在配置时，不得更改从端口的参数。
- 配置的load Sharing组中所有成员的自学习功能必须保证一致，推荐load Sharing组的成员端口都处于自学习功能打开状态。
- 定义一个Load Sharing组时要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。
- 一个Load Sharing组中的所有端口必须属于同一VLAN，且端口的tag模式也要相同。
- 当端口工作于secure模式时，不能创建Load sharing。
- 当从端口up，而主端口down的情况下，load sharing会创建失败。
- Config port [<portlist>|all] [normal|secure] 中portlist不能包含Load sharing从端口号。
- Config port [<portlist>|all] secure [permit|deny]中portlist不能包含Load sharing从端口号。
- Config port [<portlist>|all] secure [add|delete] macgroup [<macfiltername>|all] 中portlist不能包含Load sharing从端口号。

3.2.2 创建一个 Load Sharing 组

【命令格式】`create sharing <master_portno> grouping <portlist>`

【使用指导】`<master_portno>`表示所创建的 `Load Sharing` 组的主端口号，`<portlist>`表示与该 `Load Sharing` 相关的端口列表。

【命令模式】配置模式

3.2.3 删除一个 Load Sharing 组

【命令格式】`delete sharing <master_portno>`

【使用指导】`<master_portno>`表示要删除的 `Load Sharing` 组的主端口号。

【命令模式】配置模式

3.2.4 配置成员端口的转发模式

【命令格式】`config sharing <master_portno> select-mode <rtag>`

【参数说明】<master_portno>表示 Load Sharing 组的主端口号，<rtag>为端口的转发模式。包括以下几种模式：

- smac: 基于源 MAC 地址负载均衡模式
- dmac: 基于目的 MAC 地址负载均衡模式
- sdmac: 基于源和目的 MAC 地址负载均衡模式
- slip: 基于源 IP 地址负载均衡模式
- dip: 基于目的 IP 地址负载均衡模式
- sdip: 基于源和目的 IP 地址负载均衡模式

【命令模式】配置模式

3.2.5 配置 Load Sharing 例子

以下的例子定义一个 Load Sharing 组，包含端口 10-14，并以端口 12 为逻辑上的主端口。其中，端口 12 在逻辑上代表物理端口 10、11、12、13、14。指明 shaing 成员端口的转发模式基于源和目的 MAC 地址。

```
Harbour(config)#create sharing 12 grouping 10-14
Harbour(config)#config sharing 12 select-mode sdmac
```

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（如上例中的端口 12 代表整个 Load Sharing 组中的所有端口）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 Load Sharing 中的其他非主端口的端口进行操作。这样，通过对端口 12 的配置来完成对 Load Sharing 中所有端口的配置。例如关闭 Load Sharing 组中的端口 10，11，12，13，14：

```
Harbour(config)#create sharing 12 grouping 10-14
Harbour(config)#config port 12 disable
```

3.2.6 显示 Load Sharing 配置

【命令格式】show sharing

【使用指导】显示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。

【配置实例】

```
Harbour(config)#create sharing 1 grouping 1-3,5,7
Harbour(config)#config sharing 1 select-mode sdmac
Harbour(config)#show sharing

Sharing information:
Master Port: 1       Group Ports: 1   2   3   5   7
```

```
Forwarding Port Selecting Mode : Source mac and Destination mac address
```

3.3 端口镜像

端口镜像通过将一个或多个端口的数据复制到指定的端口上来实现网络流量分析和错误诊断。FlexHammer5010 交换机支持端口镜像功能，端口镜像功能基于如下规则：

- 每一个设备中，只能将一个端口作为镜像的目标端口。
- 可以将多个端口镜像到一个端口。
- 可以分别设置镜像端口的发包或者收包。

3.3.1 配置镜像目标端口

镜像目标端口，指数据复制到的目标端口。交换机的任何一个端口都可以作为一个目标端口。一台 FlexHammer5010 只能设置一个镜像目标端口，被设置为镜像目标端口的端口不能再被设置成镜像源端口。指定镜像的目标端口，利用如下命令：

【命令格式】`config mirroring <mirrornum> to <port>`

【使用指导】`<mirrornum>`为镜像配置索引号，`<port>`为镜像目标端口

【命令模式】配置模式

3.3.2 配置镜像源端口组的发包和收包

FlexHammer5010 支持多端口到一个端口的镜像，并可以分别设置镜像源端口的发包和收包，利用如下命令：

【命令格式】`config mirroring <mirrornum> [add|delete] port [<portlist>|all] [egress|ingress]`

【参数说明】

- mirrornum 表示镜像组的索引号
- add 表示向镜像组添加源端口
- delete 表示从镜像组中删除源端口
- portlist 表示指定的参与镜像的源端口
- all 表示所有源端口参与镜像
- egress 表示镜像所有源端口的发送包
- ingress 表示镜像所有源端口的接收包

【命令模式】配置模式

【配置实例】

镜像端口 1-10 的发送包

```
Harbour(config)#config mirroring 1 add port 1-10 egress
```

镜像端口 1-10 的接收包

```
Harbour(config)#config mirroring 1 add port 1-10 ingress
```

3.3.3 取消端口镜像

【命令格式】config mirroring <mirrornum> disable

【参数说明】<mirrornum>表示镜像组索引号

【命令模式】配置模式

3.3.4 显示镜像信息

【命令格式】show mirroring

【命令模式】配置模式

【配置实例】配置镜像目标端口为 5，镜像源端口为 6-12 的发送包，镜像源端口 25-30 的接收包，并显示镜像信息，命令如下：

```
Harbour(config)#config mirrror 1 to 5
Harbour(config)#config mirroring 1 add port 6-12 egress
Harbour(config)#config mirroring 1 add port 25-30 ingress
Harbour(config)#show mirroring

Mirroring information:
The port which mirror to    : 5
The ports which egress traffic mirror from : 6 7 8 9 10 11 12
The ports which ingress traffic mirror from : 25 26 27 28 29 30
```

3.4 端口安全配置

端口安全可以对端口的访问使能进行控制，使得端口可以按要求被配置在某个范围内允许使用，从而达到端口安全的目的。FlexHammer5010 支持端口安全功能，端口安全功能基于如下规则：

1. 每个端口既可以工作在安全模式又可以工作在非安全模式，可以在两种模式之间进行任意的切换。
2. 端口既可以允许所有的地址使用（此时工作在非安全模式，此模式也是端口的缺省模式），也可以允许部分或不允许部分地址进行使用。当然，如果需要的话也可配置为所有的地址都不能使用。
3. 对于用户配置的静态 FDB 地址，无论端口是在安全或非安全模式，这些静态的 FDB 地址在对应的端口上都可以进行访问。也就是说，只要用户配置了某个端口的静态 FDB，在该端口的地址就可以正常工作。

4. 端口安全不能使用在端口学习状态关闭的情况下。

3.4.1 实现机制

控制端口的访问是通过设置端口的学习位来实现的，即禁止端口的硬件地址学习能力，同时将需要进行源地址学习的包送往 CPU，由软件处理该地址学习与否，从而达到基于包的源 MAC 地址控制端口转发。如果该端口允许该 MAC 地址的包访问就由软件设置软/硬件二层转发表，反之则不设置。

3.4.2 创建地址组

【命令格式】create macgroup <name>

【命令作用】创建地址组，地址组用于将一些地址汇集到一起，然后可以将这些地址组与端口进行相连，从而可以进行端口的安全控制。地址组的名称只能由数字或字母组成，并且必须以字母开头，长度不能超过 30。系统共允许创建 256 个地址组。

【参数说明】<name>为地址组的名称

【命令模式】配置模式

【配置举例】

```
Harbour(config)#create macgroup mactest
```

3.4.3 删除地址组

【命令格式】delete macgroup [<name>|all]

【命令作用】删除已经配置的地址组

【参数说明】<name>为已经创建的地址组的名称。选择 all，表示对所有 macgroup 进行操作。

【命令模式】配置模式

【配置举例】删除已经创建的名称为 macgroup 地址组

```
Harbour(config)#delete macgroup mactest
```

3.4.4 向地址组中添加/删除地址

【命令格式】config macgroup <name> [add|delete] <mac>

【命令作用】向/从地址组中添加/删除地址。操作的地址不能是多播或广播地址，只能是单播地址。添加地址的数量没有限制，但一个地址组中不能有相同的地址存在。地址的输入格式为 12 个数字或字母的组合。

【参数说明】<name>为地址组的名称。选择 add 表示向地址组添加地址；选择 delete 表示从地址组中删除已添加的地址；<mac>是实际要添加的地址。

【命令模式】配置模式

【配置举例】

```
Harbour(config)#config macgroup mactest add 001122334455
```

```
Harbour(config)#config macgroup mactest delete 001122334455
```

3.4.5 配置端口工作在安全或者非安全模式

【命令格式】config port [<portlist>|all] [normal|secure]

【命令作用】配置端口工作在安全或非安全模式：端口工作在非安全模式时，我们已经进行与端口安全相关的配置将不起作用，只有端口工作在安全模式这些配置才起作用。可以通过下面的命令在端口的模式之间进行切换。创建端口安全后，默认的端口安全模式为 permit。

【参数说明】<portlist>为端口的列表，选择 all 表示对所有端口进行操作；选择 normal 表示将端口配置为非安全模式；选择 secure 表示将端口配置为安全模式。

【命令模式】配置模式

【配置举例】配置端口 1 工作在安全模式

```
Harbour(config)#config port 1 secure
```

3.4.6 配置端口在安全模式下的状态控制

【命令格式】config port [<portlist>|all] secure [permit|deny]

【使用指导】端口工作在安全模式时，可以有两种控制状态：permit/deny。

1、如果选择 permit，则所有与端口相连的地址组中的地址（后面会介绍如何将端口与地址组相连）在此端口上将可以进行访问。注意：如果此端口没有与任何的地址组相连，则此时此端口将禁止所有的地址进行访问（如果配置了静态的 FDB 除外）。

2、如果选择 deny，则所有与端口相连的地址组中的地址将被禁止在此端口上进行访问。注意：如果此端口没有与任何的地址组相连，则所有的地址在此端口上都可以进行访问。如果此端口当前为非安全模式，执行该命令会自动将端口设置为安全模式。

【参数说明】<portlist>为端口的列表，选择 all 表示对所有端口进行操作。选择 permit，将状态设置为允许状态；选择 deny，将状态设置为拒绝状态。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#config port 1 secure permit
```

3.4.7 将地址组与安全端口关联（或取消关联）

【命令格式】config port [<portlist>|all] secure [add|delete] macgroup [<macfiltername>|all]

【使用指导】将地址组与安全端口进行关联（或者取消关联）。

将地址组与安全端口进行关联就可以结合地址组中的地址和安全端口的状态进行安全的控制。注意：如果此端口当前为非安全模式，执行该命令会自动将端口设置为安全模式，如果端口已经是安全的则不会改变端口当前的 permit/deny 状态控制。端口

与地址组之间是多对多的关系。也就是说，一个端口可以关联多个地址组，一个地址组也可以关联多个端口。

【参数说明】<portlist>为端口的列表。选择 all 表示对所有端口进行操作；选择 add 表示将地址组与端口相连；选择 delete 表示将地址组与端口断开连接；macfiltername 为地址组的名称，规则同上；选择 all 表示将所有的地址组与端口关联（或者断开关联）。

【配置实例】

```
Harbour(config)#config port 1 secure add macgroup mactest
```

3.4.8 显示地址组信息

【命令格式】show macgroup {<name>}*1

【命令作用】显示地址组的信息：包括地址组的名称、所有的地址、与其进行连接的所有的端口。

【参数说明】<name>为地址组的名称，规则同上面提到的一样。如果不输入地址组的名称将显示所有地址组的信息。

3.4.9 显示每个端口的信息

【命令格式】show perport [<portist>|all]

【使用指导】显示端口的信息。显示每个端口是安全/非安全模式，如果是安全模式显示与其相关联的所有的地址组的名称，是 permit 还是 deny 控制状态；此端口所属的地址组是否是安全的；地址组的地址学习的使能控制。

【参数说明】<portlist>为端口的列表，选择 all 表示对所有端口进行操作。

3.5 广播包抑制（Boradcast Limit）

广播包抑制功能可以有效地控制端口每秒收到的广播包数量，有效地防止广播攻击。

3.5.1 使能/关闭广播包抑制功能

【命令格式】config Broadcast_Limit [enable|disable]

【参数说明】enable 使能广播包抑制功能；disable 关闭广播包抑制功能

【命令模式】配置模式

3.5.2 配置端口的广播包接收数量上限

【命令格式】config Broadcast_Limit <1-262143>

【使用指导】配置每个端口每秒最多可接收的广播包数量，超过此值的广播包将被丢弃，默认值为 4096。

【命令模式】配置模式

3.5.3 查看广播包抑制配置信息

【命令格式】show Broadcast_Limit

【使用指导】显示当前广播包抑制功能的配置状态信息

【命令模式】配置模式

【配置实例】目前广播包抑制功能打开，每个端口每秒最多接收 10000 个广播包

```
Harbour(config)#show broadcast_limit

State            Value
_ _ _ _ _ _ _ _ _ _ _ _ _ __ _ _ _ _ _ _

enable           10000
```

3.6 下行环路检测（Loop Detect）

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。针对这一问题的解决方法是：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 disable 这个端口。配置下行环路检测的命令如下：

config loopdetect enable　　使能端口环路检测

config loopdetect disable　　关闭端口环路检测

如果端口下游存在环路，则最多 10 秒之后，使用命令 show port <portlist>查看该端口信息时，会发现该端口被 disable，并有 self-looped 的说明。

例如：端口 22 的下游存在环路，在使能端口环路检测功能之前使用 show port 22 命令查看到该端口的 Port State 为 Enabled。使能端口环路检测功能之后在查看端口 22 的信息，可以看到该端口的 Port State 为 Disabled（self_looped）:

```
Harbour(config)#show port 22

-----------------------------------------------------------------
  -----------
              Port:22 's Configuration Information

Link State     : Up            Port State     : Enabled
Port Type      : 100BaseT       Speed          : 100
Autonegotiation : Enabled        Duplex          : Full
Flowcontrol    : Disabled       Learn State     : Enabled

Port VLAN ID    : 2047
Port VLAN Name  : default
Port Summary    : normal
-----------------------------------------------------------------
  -----------

Harbour(config)#config loopdetect enable
```

```
Harbour(config)#show port 22

------------------------------------------------------------------
  -----------
             Port:22 's Configuration Information

Link State       : Up               Port State       : Disabled
  (self_looped)
Port Type      : 100BaseT       Speed          : 100
Autonegotiation : Enabled        Duplex         : Full
Flowcontrol    : Disabled       Learn State    : Enabled

Port VLAN ID    : 2047
Port VLAN Name  : default
Port Summary    : normal
------------------------------------------------------------------
  -----------
```

在人工检查并排除端口下游的环路后，要使得 port 22 恢复正常，请先 disable 端口 22，再 enable 端口 22。按顺序执行命令：

```
config port 22 disable

config port 22 enable
```

第4章 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，您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，您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。

4.1 添加 ARP 表项

添加一条静态 ARP 表项，可以利用如下命令：

【命令格式】config arp add <A.B.C.D> <mac_address>

【参数说明】<A.B.C.D>代表创建静态 ARP 的 IP 地址，<mac_address>代表 IP 地址对应的 MAC 地址

【命令模式】配置模式

【配置实例】添加一个静态 ARP 表项：

```
Harbour(config)#config arp add 10.5.1.32 00E02B123456
```

4.2 删除某个 ARP 表项

【命令格式】config arp delete <A.B.C.D>

【参数说明】<mac_address>为所要删除的设备的 MAC 地址

【命令模式】配置模式

【配置实例】删除一个已经存在的 ARP 表项：

```
Harbour(config)#config arp delete 00E02B123456
```

4.3 查看 ARP 表

【命令格式】show arp {[<A.B.C.D>|permanent]}*1

【参数说明】<A.B.C.D>代表 IP 地址，permanent 代表手工创建的静态 ARP 表

【使用指导】当不输入任何参数时显示系统中所有 arp 表项信息，包括动态与静态。

输入 IP 地址<A.B.C.D>可以查看指定 IP 地址对应的 ARP 表。

输入参数 permanent 时查看系统中所有手工创建的静态 ARP 表。

【命令模式】只读模式或者配置模式

【配置实例】

```
Harbour(config)#show arp

ARP  TABLE  LIST:

IP  ADDRESS          MAC  ADDRESS             TYPE          REFERENCE
  USE
```

```
-------------------------------------------------------------------
  ----------
11.1.0.1            00:50:fc:3c:13:d0      DYNAMIC              0
  1
-------------------------------------------------------------------
  ----------
TOTAL :1
```

说明：ARP 表项的容量为 4000 条

4.4 显示所有创建的静态 APR 表项

【命令格式】show arp user

【使用指导】此命令用于显示所有创建的静态 ARP 表项。该命令与命令 show arp permanent 的不同之处在于：show arp permanent 只显示状态为 up 的端口的静态 ARP 表项；show arp user 显示所有端口（up 或 down）的静态 ARP 表项。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#show arp user

Begin to show arp config table information
Physics Address    IP Address           Interface
00:11:22:33:44:55   1.1.1.3              default
Total 1 information
End to show arp table information
```

4.5 显示 ARP 表项数

【命令格式】show arp summary

【使用指导】此命令用于显示 ARP 表中的所有 ARP 表项数

【命令模式】配置模式

【配置实例】

```
Harbour(config)#show arp summary

ARP table information
Total 2 information
```

4.6 清除 ARP 表

【命令格式】clear arp

【使用指导】此命令用于清除 ARP 表，执行此命令后，ARP 表中的所有动态表项被清除

【命令模式】配置模式

4.7 ARP 地址解析表的配置

命令	说明
clear arp	清除 ARP 表，执行此命令后，ARP 表中的所有动态表项均被清除
config arp add <A.B.C.D> <mac_address>	添加一条静态 ARP 表项，<A.B.C.D> 表示目标设备的 IP 地址，<mac_address> 表示与目标设备 IP 地址对应的 MAC 地址
config arp delete <A.B.C.D>	删除一条 ARP 地址解析表项，<A.B.C.D> 表示目标设备的 IP 地址
show arp {[<A.B.C.D>|permanent]}*1	查看 ARP 地址解析表项 当不输入任何参数时显示系统中所有 ARP 表项的信息，包括动态与静态 当只输入 IP 地址<A.B.C.D>可以查看指定 IP 地址对应的 ARP 表 当只输入 permanent 时查看系统中所有手工创建的静态 ARP 表
show arp user	显示所有创建的静态 ARP 表项。该命令与命令 show arp permanent 的不同之处在于： show arp permanent 只显示状态为 up 的端口的静态 ARP 表项； show arp user 所有端口（up 或 down）的静态 ARP 表项

第5章 FDB 表

本章讲述了 FDB（Forwarding Database）地址表的内容和相关知识，以及如何在 FlexHammer5010 上配置静态 FDB 地址表。

5.1 FDB 地址表概述

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

5.1.1 FDB 地址表的内容

HammerOS 的 FDB 地址表数目由产品决定，FlexHammer5010 可以存储最多 8k 条地址表项。每个 FDB 地址表项都包含以下内容：

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

FDB 地址表项的标志的含义：

System ：系统（交换机）自动产生的第三层静态 FDB 地址表项。

Permenant ：该 FDB 地址表项是一个静态地址表项。

Dynamic ：该 FDB 地址表项是一个动态地址表项。

L3 ：该 FDB 地址表项是一个用于三层转发的地址表项。

如果收到数据帧的目的 MAC 地址不在 FDB 地址表中，那么该数据将被发送给除源端口外该数据包所属 VLAN 的其他所有端口。FlexHammer5010 的每一个 FDB 地址表项由 MAC 地址和 VLANID 唯一标识。

5.1.2 FDB 地址表的地址表项类型

MAC 地址表共有三种地址表项：

动态地址表项——最开始的时候，交换机 FDB 地址表中的所有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。这样能防止地址表项变得过于庞大，当确信某个设备从网络中去除后，就把该设备的地址表项删除掉。当交换机关机重启动或者 reset 时，所有的动态地址表项都将被删除。

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，直到交换机关机或者重启。

永久地址表项——永久地址表项将一直保存在 MAC 地址表中，即使交换机关机或者重启。永久地址表项必须由系统管理员手工设定。一个永久地址表项可以是一个单播地址，也可以是一个组播地址（本系统暂时不支持组播地址）。所有由命令行输入的静态地址表项都将被存储为永久地址表项。FlexHammer5010 交换机最多能支持 1K 个静态地址表项。永久地址表项一经建立，不会老化，但会随交换机的配置变化而变化。

以下事件的发生都会引起永久地址表项被删除：

- 删除一个与FDB静态表项关联的VLAN
- 修改一个与FDB静态表项关联的VLAN的tag值
- 从VLAN中删除与FDB静态表项关联的一个端口

以下事件的发生都不会引起永久地址表项的变化：

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

5.1.3 一个地址表项怎样被加入到 FDB 地址表中去

FDB 地址表中的地址表项可以通过以下两个途径被加入：

- 交换机自学习。交换机可以根据收到的数据包的源MAC地址、端口、VLANID，来自动更新FDB地址表。
- 可以通过命令行接口手工增加地址表项到FDB地址表中。

5.2 配置 FDB 地址表

5.2.1 添加 FDB 地址表及配置老化时间

添加一个静态地址表项到 FDB 地址表中，可以利用如下命令：

【命令格式】`create fdbentry <mac_address> vlan <name> port <portlist> {priority <0-7>}*1`

【参数说明】`<mac_address>`是 MAC 地址，`<name>`是 vlan 的名称，`<portlist>`是端口号

【命令模式】配置模式

【配置实例】添加一个静态地址表项到 FDB 地址表中：

```
Harbour(config)#create fdbentry 00E02B123456 vlan market port 4
```

通过此命令，使这个静态永久地址表项具有以下属性：

- MAC 地址是 00:E0:2B:12:34:56
- VLAN 名字是 market
- 端口号是 4

配置 FDB 地址表的老化时间，利用如下命令：

【命令格式】config fdb agingtime [0|<10-1000000>]

【参数说明】[0|<10-1000000>]是老化时间，单位是秒。选择 0 表示地址表项永远不老化，缺省值是 80 秒。

【命令模式】配置模式

【配置实例】将 FDB 地址表的老化时间设为 40 秒：

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

5.2.2 删除 FDB 表中的地址表项

【命令格式】delete fdbentry {mac <mac_address> vlan <name>}*1

【参数说明】<mac_address>为所要删除的设备的 MAC 地址，<name>为所要删除的设备所属的 VLAN 名称。如果只是输入“delete fdbentry”，则删除所有的动态地址表项。

【命令模式】配置模式

【配置实例】删除 vlan market 中端口 4 的地址表项：

```
Harbour(config)#delete fdbentry mac 00E02B123456 vlan market
```

注意：对由系统创建的 FDB 表项不能删除。

5.3 显示 FDB 地址表中的地址表项

5.3.1 显示 FDB 地址表中的所有地址表项：

【命令格式】show fdb {[mac]<macaddr>}*1 {[vlan]<name>}*1

【参数说明】<macaddr>代表 MAC 地址，<name>代表 VLAN 名

【使用指导】当 MAC 地址和 VLAN 名字一个都不输入时，将显示本交换机 FDB 地址表中的所有地址表项信息。当只输入 MAC 地址时，将显示本交换机所有 VLAN 中含该 MAC 地址的 FDB 地址表项。当只输入 VLAN 名字时，将显示此 VLAN 中的所有 FDB 地址表项信息。当既输入 MAC 地址又输入 VLAN 名字时，将显示该 VLAN 中此 MAC 地址的 FDB 地址表项信息。

【命令模式】只读模式或者配置模式

【配置实例】

```
Harbour(config)#show fdb

------- Begin of MAC Address Table Information (all)-------

MAC address       Port  vlan name                  Flags
------------------      ----      ------------------------------
  --------------------
00:05:3b:02:30:00   0    default                        System L3
  Permanent
00:05:3b:02:30:00    0    System Cluster                   System
  Permanent
00:05:4b:00:04:90   10   System Cluster               Dynamic
------------------      ----      ------------------------------
  --------------------
```

5.3.2 显示 FDB 地址表中的静态地址表项：

【命令格式】show fdb permanent {[mac] <macaddr>}*1 {[vlan] <name>}*1

【参数说明】<macaddr>代表 MAC 地址，<name>代表 VLAN 名

【使用指导】当 MAC 地址和 VLAN 名字一个都不输入时，将显示本交换机 FDB 地址表中的所有的静态永久地址表项信息。当只输入 MAC 地址时，将显示本交换机所有 VLAN 中含该 MAC 地址的静态地址表项。当只输入 VLAN 名字时，将显示此 VLAN 中的所有静态地址表项信息。当既输入 MAC 地址又输入 VLAN 名字时，将显示该 VLAN 中此 MAC 地址的静态地址表项的信息。

【命令模式】只读模式或者配置模式

【配置实例】

```
Harbour(config)#show fdb permanent mac 004532659872

-------      Begin      of      Permanent      MAC      Information
  (macaddr:[004532659872])-------

MAC address       Port  VLAN name             Flags
------------------ ---- ------------------------------
00:45:32:65:98:72   0    default               System
00:45:32:65:98:72   0    sun                  Permanent

------------------ ---- ------------------------------

Total 2 permanent mac showed.

----------  End of Permanent MAC Information ----------
```

5.3.3 显示 FDB 地址表的使用信息

【命令格式】show fdb summary

【使用指导】显示当前系统中 FDB 表的总数量以及动态和静态 FDB 表的数量信息。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#sh fdb summary

---------------- FDB usage ----------------
Static                          3
Dynamic                         0
Total                           3
-------------------------------------------
```

5.4 MAC 地址绑定

出于网络安全考虑，需要对接入用户进行控制，通过对交换机建立静态 FDB 实现 MAC 地址绑定，用以防止地址假冒。实现 MAC 地址绑定前，需要首先关闭交换机端口的地址学习功能，然后通过为该端口绑定一个静态 MAC 地址。这样，凡是来自该 MAC 地址的报文将允许通过，而来自其他陌生 MAC 地址的报文均被丢弃，从而限制了在该端口上允许通过的 MAC 地址。设置 MAC 地址绑定的步骤如下：

第一步：关闭端口的地址学习功能

config port [<portlist>|all] learn off

第二步：建立一条 FDB 地址表项以实现基于端口的 MAC 地址绑定

create fdbentry <mac_address> vlan <name> <portlist>

5.5 FDB 地址表配置命令列表

表 5-1 FDB 地址表配置命令表

命令	描述
config fdb agingtime [0|<10-1000000>]	设置 FDB 地址表中的地址表项老化时间，缺省值为 80 秒，值 0 表示该地址表项永远不老化。
create fdbentry <mac_address> vlan <name> port <portlist> {priority <0-7>}*1	创建一个静态的永久地址表项。 <mac_address>：数据包的目的 MAC 地址； <name>： 数据包所属的 VLAN； <portlist>：数据包转发的目的端口号 {priority <0-7>}：优先级
delete fdbentry {mac<mac_address> vlan <name>}*1	删除静态 FDB 地址表项，如果不输入大括号中的可选参数，则删除所有的动态地址表项
show fdb {[mac] <macaddr>}*1 {[vlan] <name>}*1	当 MAC 地址和 VLAN 名字一个都不输入时，将显示本交换机 FDB 地址表中的所有的地址表项的信息

	地址表项的信息。 当只输入 MAC 地址时，将显示本交换机中所有的 VLAN 中含该 MAC 地址的 FDB 地址表项。 当只输入 VLAN 名字时，将显示本交换机中所有在该 VLAN 中的 FDB 地址表项的信息。 当既输入 MAC 地址又输入 VLAN 名字时，将显示该 VLAN 中此 MAC 地址的 FDB 地址表项的信息。
show fdb permanent {[mac] <macaddr>}*1 {[vlan] <name>}*1	当 MAC 地址和 VLAN 名字一个都不输入时，将显示本交换机 FDB 地址表中的所有的静态地址表项的信息。 当只输入 MAC 地址时，将显示本交换机中所有的 VLAN 中含该 MAC 地址的静态地址表项信息。 当只输入 VLAN 名字时，将显示本交换机中所有在该 VLAN 中的静态地址表项的信息。 当既输入 MAC 地址又输入 VLAN 名字时，将显示该 VLAN 中此 MAC 地址的静态地址表项的信息。
show fdb summary	显示当前系统中 FDB 表的总数量以及动态和静态 FDB 表的数量信息。

第6章 虚拟局域网 VLAN

6.1 VLAN 概述

简单地讲，VLAN 是指那些看起来好像在同一个物理局域网中能够相互通信的设备的集合。对于以端口划分的 VLAN 而言，任何一个端口的集合（甚至交换机上的所有端口）都可以被看作是一个 VLAN。VLAN 的划分不受硬件设备物理连接的限制，用户可以通过命令灵活地划分端口，创建定义 VLAN。使用 VLAN 的优点如下：

1．VLAN 能帮助控制流量

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

2．VLAN 提供更高的安全性

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

3．VLAN 使网络设备的变更和移动更加方便

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

6.2 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

6.2.1 以端口划分的 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。不同 VLAN 中的成员不能相互通信，即使它们在物理上属于同一个交换机的同一个 I/O 模块。如果要互相通信就必须通过三层交换机进行路由。这就意味着每一个 VLAN 的 IP 地址必须唯一，且不属于相同网段。

例如，在交换机上，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。

6.2.2 以标签划分的 VLAN

标签就是在以太网帧中插入的特定标记，称为 tag，它也是某个指定 VLAN 的标识号 VLANID。

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 稍微大一点，这可能导致其他设备中的数据包计数错误，使得在含有非 802.1Q 网桥或路由器的网络中有可能导致连接出现问题。

6.2.3 Tagged VLAN 的应用

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

使用 Tagged VLAN 的另一个好处就是一个端口可以属于多个 VLAN。这一点在某个设备（例如服务器）必须属于多个 VLAN 的时候特别有用，此设备必须有支持 802.1Q 的网络接口卡。

6.2.4 指定 VLAN 标签

每个 VLAN 都可被赋予一个 802.1Q VLAN tag。 当向一个由 802.1Q 标签定义的 VLAN 中添加端口时，您可以决定该端口是否使用这个 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，其 VLANID 为 2047。

并不是所有端口都必须使用标签。当数据流从交换机的一个端口输出时，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 端口的配置情况决定加上或者去掉数据包中的标签。

如果交换机收到带 tag 标记的数据包，当这个 tag 值与接收数据端口的 tag 值不同时，说明这个数据包来自其他 VLAN，因此交换机将丢弃该数据包。

图 6-1 说明了使用 Tag（tagged）和未使用 Tag（untagged）划分 VLAN 的网络物理结构图。

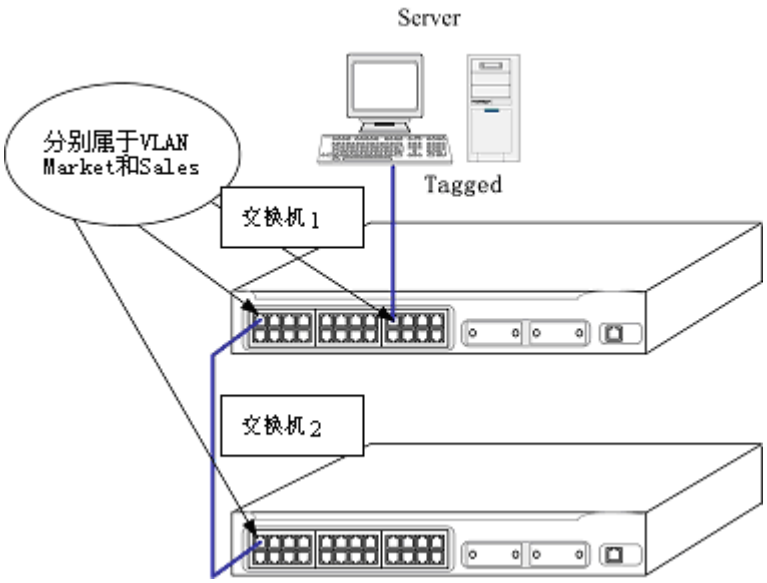


图 6-1 以 tagged 和 untagged 划分 VLAN

交换机 1 的端口 1 和交换机 2 的端口 1 同时属于 VLAN Market 和 VLAN Sales，且两个端口之间有中继线连接。跨交换机的 VLAN Market 和 VLAN Sales 通过这条中继线相连，从而实现跨交换机的 VLAN 通信。其中：

- 中继端口都为tagged。
- 连接到交换机1端口9上的Server须含有支持802.1Q Tagged的网络接口卡（NIC）。
- 连接Server的交换机1的端口9必须同时属于VLAN Market和VLAN Sales。
- 除了连接Server的交换机1的端口8和两台交换机的端口1是tagged以外，其他端口都是untagged。
- 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Server收发的数据都是加标签的（tagged）；从其余终端工作站收和发的数据都是untagged。

6.2.5 混合使用 Tagged VLAN 和 Port-Based VLAN

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

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

6.3 配置 VLAN 的有关规则

Hammer 交换机的 VLAN 配置要求遵循一定的规则，我们对 VLAN 的命名、端口的添加、IP Address 的配置、Tag 值的范围等有一定的要求。

6.3.1 缺省 VLAN

每一台 Hammer 交换机出厂时都有一个缺省的 VLAN，该 VLAN 有以下属性：

- VLAN 的名字是default
- 它包含所有端口
- default VLAN的所有端口都是untagged的
- default VLAN的VLANID是2047

6.3.2 VLAN 的名字

每个 VLAN 的名字可以是由以字母开头的 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、引号等字符都是不合法的。

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

您应该在整个网络中统一规划命名您的 VLAN。

6.3.3 VLAN 端口的添加

FlexHammer5010 的端口可以以两种形式属于某个 VLAN，分别是：IEEE 802.1Q tagged 模式 和 IEEE 802.1Q untagged 模式。一个端口在 IEEE 802.1Q untagged 模式下只能属于一个 VLAN，以 IEEE 802.1Q tagged 模式可以属于多个 VLAN。

添加 VLAN 端口，利用如下命令：

【命令格式】config vlan <name> add port <portlist> [tagged|untagged]

【参数说明】<name>是 vlan 的名称，<portlist>是端口列表，选择 tagged 表示向 VLAN 添加 tagged 端口，选择 untagged 表示向 VLAN 添加 untagged 端口。

【使用指导】当我们向一个指定 VLAN 中添加 IEEE 802.1Q untagged 端口时：

如果该端口属于 Default VLAN，则该端口可以添加到指定的 VLAN 中，同时交换机会自动从 Default VLAN 中将该端口删除。

如果该端口不属于 Default VLAN，那么该端口肯定以 IEEE 802.1Q untagged 模式属于某个其他 VLAN，则不能将该端口添加到指定的 VLAN 当中。

当我们往一个指定 VLAN 中添加 IEEE 802.1Q tagged 端口时，不再受该端口与其他 VLAN 关系的限制。如果该端口已经以 IEEE 802.1Q untagged 模式属于该 VLAN 时，

端口可以添加成功，但该端口将不再以 untagged 模式属于该 VLAN。

【配置实例】创建一个名称为 market 的 VLAN，且端口 2 已经以 IEEE 802.1Q untagged 模式属于该 VLAN。

```
Harbour(config)#show vlan market

VLAN ID          : 2045
Name            : market
MAC address      : 00:45:32:65:98:72
Tagged Ports     :
Untagged Ports   : 2  4  5  8  9  10
```

当我们向 market 添加一个以 IEEE 802.1Q tagged 模式属于该 VLAN 的端口 2 时，

键入命令：

```
Harbour(config)#config vlan market add port 2 tagged
Harbour(config)#show vlan market

VLAN ID         : 2045
Name           : market
MAC address     : 00:45:32:65:98:72
Tagged Ports    : 2
Untagged Ports  : 4  5  8  9  10
```

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

6.3.4 配置 IP 地址

对于交换机，要求在一台交换机中，不同 VLAN 必须配置成不同子网段的 IP Address。配置 IP 地址，利用如下命令：

【命令格式】config vlan <name> ipaddress <A.B.C.D/M>

config vlan <name> ipaddress <A.B.C.D> <A.B.C.D>

【参数说明】<name>为所要配置的 VLAN 的名称，<A.B.C.D>为给该 VLAN 配置的 IP 地址，M 为子网掩码数。或者利用第二个命令的格式，输入点分十进制形式的掩码。

【配置实例】给缺省 VLAN default 配置一个 IP 地址 192.168.0.232，子网掩码数为 24，键入命令：

```
Harbour(config)#config vlan default ipaddress 192.168.0.232/24
```

或者，键入命令：

```
Harbour(config)#config  vlan  default  ipaddress  192.168.0.232
  255.255.255.0
```

6.3.5 VLAN 的 Tag 值范围

FlexHammer5010 的 VLAN 的 Tag 值要求在 1-4094 范围之间。

6.4 配置 VLAN

这一小节主要讲述在交换机上配置 VLAN 相关的命令。配置 VLAN 包括以下几步：

1．创建 VLAN 并给该 VLAN 取名。

2．如果需要的话给该 VLAN 分配 IP 地址和子网掩码。

3．给 VLAN 指定一个 Tag（或者使用创建时系统分配的 Tag）。

4．在 VLAN 中加入端口。当您加入端口时可以指定是否使用 802.1Q tag。

表 6-1HammerOS 的 VLAN 配置命令表

命令	描述
create vlan <name>	创建一个 VLAN
config vlan <name> ipaddress <A.B.C.D/M>	配置名为<name>的 VLAN 的 IP 地址和网络掩码长度
config vlan <name> ipaddress <A.B.C.D> <A.B.C.D>	配置名为<name>的 VLAN 的 IP 地址和网络掩码
config vlan <name> tag <1-4094>	指定 VLAN 的 tag 即 VLANID
config vlan <name> [add|delete] port <portlist> [tagged|untagged]	在 VLAN 中增加或删除端口，并设置该端口是 tagged 还是 untagged

6.4.1 配置 VLAN 举例

以下的例子是在交换机上创建了一个名为 development 的 VLAN，给该 VLAN 分配 IP 地址 202.106.15.3 和子网掩码 255.255.255.0，然后加入端口 3，6，17-20，并指定端口为 untagged 模式。

```
Harbour(config)#create vlan development
Harbour(config)#config vlan development ipaddress 202.106.15.3
  255.255.255.0
Harbour(config)#config vlan development add port 3,6,17-20 untagged
```

又如，在交换机上，创建了一个名为 video 的 Tag-Based VLAN，分配给该 VLAN 的 VLANID 是 128。把端口 4 至端口 8 加入该 VLAN 并设为 tagged 模式。

```
Harbour(config)#create vlan video
Harbour(config)#config vlan video tag 128
Harbour(config)#config vlan video add port 4-8 tagged
```

6.4.2 删除 VLAN

【命令格式】delete vlan [<name>|all]

【使用指导】选择 name ，删除指定的 vlan，选择 all 删除所有的 vlan(default 除外)。删除一个 VLAN 后，该 VLAN 的 untagged 模式的端口将被以 untagged 模式放回缺省 VLAN default 中。

【命令模式】配置模式

6.4.3 删除 VLAN 的 IP 地址

【命令格式】no vlan <name> ip

【命令模式】配置模式

【配置实例】删除 vlan market 的 IP 地址

```
Harbour(config)#no ip-vlan market
```

6.4.4 显示 VLAN 配置信息

【命令格式】show vlan {<name>}*1

【使用指导】name 可以输入也可以不输入。当输入 name 的时候，就只显示这个 name 的 VLAN 的信息。当不输入 name 的时候，显示当前交换机中的所有 VLAN 的信息。show 命令所显示的 VLAN 信息包括以下内容：

- VLAN 名字（VLAN name）
- VLANID
- IP 地址
- 属于该 VLAN 的 tagged 模式的端口
- 属于该 VLAN 的 untagged 模式的端口

【配置实例】创建了一个 VLAN development，显示 VLAN 的配置信息，键入命令：

```
Harbour(config)#show vlan development

VLAN ID          : 2046
Name             : development
IP Address       : 202.106.15.3 /24
MAC address      : 10:82:c3:45:11:22
Tagged Ports     :
Untagged Ports   :  3  6  17  18  19  20
```

6.5 Super VLAN 和 Proxy ARP 的配置

6.5.1 Super VLAN 概述

VLAN Aggregation（VLAN 聚合）技术提供一种机制使处于同一个交换机中分属不同 VLAN 的主机分配在相同的 Ipv4 子网中，而且使用同一个默认网关。在当前一个大规模的交换局域网环境内这种机制相对于今天的传统 Ipv4 寻址体系具有许多优点。

VLAN 聚合的主要优点是节省 IP 地址。在交换网络环境中引进 Sub VLAN 和 Super VLAN，它们是一种可以实现 IP 地址划分的更加优化的途径。它通常将多个不同的 VLAN 划分至同一 IP 子网，而不是每个 VLAN 单独占用一个子网，然后将整个 IP 子网指定为一个 VLAN 聚合（super VLAN），它包含整个 IP 子网内的所有 VLAN（Sub VLAN）。

实质上不同的 Sub VLAN 仍保留各自独立的广播域而一个或多个 Sub VLAN 同属于一个 Super VLAN，并且都使用 Super VLAN 的接口地址为默认网关 IP 地址。Sub VLAN 中的主机的 IP 地址与 Super VLAN 所对应的 IP 子网没有直接的关系，这些主机的 IP 子网掩码只是反映了它们所属的 Super VLAN。当不同 Sub VLAN 中的主机需要相互之间通讯时需要在 Super VLAN 开启 ARP 代理。

VLAN 聚合产生了一个更加有效地地址分配体系并且这种模式也给网络工程师提供了一种规范的默认网关分配的机制。VLAN Aggregation 具有以下特点：

- 若干个小VLAN（Sub VLAN）同属于一个大VLAN（Super VLAN）。
- Super VLAN对应IPv4子网地址，所有该Super VLAN的Sub VLAN都属于该子网。
- Sub VLAN实现广播域隔离。
- 不同的Sub VLAN仍保留各自独立的广播域，实现同一子网中的广播的隔离，避免广播风暴的产生。
- 同一子网Super VLAN中的不同Sub VLAN互通需要Super VLAN开启arp-proxy。

6.5.2 Super VLAN 配置

向一个 Super VLAN 中添加或删除 Sub VLAN

【命令原型】config vlan <name> [add|delete] subvlan <name>

【参数说明】第一个<name>指 Super VLAN 的名称。第二个<name>指 subvlan 的名称。

【命令模式】配置模式

【配置实例】

```
Harbour(config)# config vlan super add subvlan sub
Harbour(config)# show  vlan

VLAN ID       : 2046
Name         : super
VLAN Type     : Super-VLAN
Mac address   : 00:05:3b:58:00:a0
Sub-vlan list  : sub
Tagged Ports   :
Untagged Ports :

VLAN ID       : 2045
Name         : sub
VLAN Type     : Sub-VLAN
Mac address   : 00:05:3b:58:00:a0
Parent VLAN   : super
Tagged Ports   :
Untagged Ports :
---------------------------------
```

```
Total vlans   : 3
```

6.5.3 Proxy ARP（ARP 代理）概述

为了同一 SuperVLAN 但不同 SubVLAN 的主机之间能通信，必须用到 Proxy ARP 协议实现地址解析。因为不同 SubVLAN 共用同一个网关，即 SuperVLAN 的路由地址，相当于一个代理 ARP 服务器。代理网关能处理不同 SubVLAN 的主机之间的 ARP 包并转发数据包。

例如 SubVLAN1 和 SubVLAN2 在同一个 Super VLAN，SubVLAN1 的主机 H1 要与 SubVLAN2 的主机 H2 通信，H1 广播 ARP 请求包（查找 SubVLAN2 的主机 H2 硬件地址）；代理网关查找并回答请求，提供代理网关自己的以太网地址；H1 将发往 H2 的数据报发送给代理网关；代理网关收到发往 H2 的数据报后，根据转发表中的信息将数据报转发给 H2。这样，通过代理 ARP 的实现，不同广播域的主机 H1 和主机 H2 之间的通信看上去就象在同一广播域内通信。

如果出于安全考虑，要禁止某 SubVLAN 同其他 SubVLAN 通信，就把该 SubVLAN 的 ProxyARP 功能关闭。

6.5.4 Proxy ARP 配置

1、打开或关闭 ARP 代理功能

打开或关闭某一 Super VLAN 或者 Sub VLAN 的 ARP 代理功能，对 Super VLAN 的配置将会应用于该 Super VLAN 下的所有 Sub VLAN 上。

【命令原型】config proxyarp [supervlan|subvlan] <vlanname> [enable|disable]

【参数说明】选择 supervlan 和 subvlan 表示操作的对象，enable 和 disable 表示使能或者禁止操作。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#config proxyarp subvlan sub enable
```

2、显示某一 Super VLAN/Sub VLAN 的 arp 代理设置

【命令原型】show proxyarp [supervlan|subvlan] <vlanname>

【参数说明】supervlan 、subvlan 表示显示内容的对象。

【命令模式】只读模式或者配置模式。

【配置实例】

```
Harbour(config)#show proxyarp subvlan sub
```

```
----Begin to show this subvlan proxyarp status----

Subvlan Name          : sub
Search List aging time  : 120(s)
Cache entry aging time  : 300(s)
Proxy ARP status       : Enable

-----End to show this subvlan proxyarp status-----

config proxyarp searchtime <0-300>
```

3、配置 ARP 代理的 search time

【命令原型】config proxyarp searchtime <0-300>

【参数说明】<0-300>表示 proxyarp 的搜索时间间隔，单位秒。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#config proxyarp searchtime 123
Now search List aging time is 123(s)
Harbour(config)#sh pro sub sub

----Begin to show this subvlan proxyarp status----

Subvlan Name          : sub
Search List aging time  : 123(s)
Cache entry aging time  : 300(s)
Proxy ARP status       : Enable

-----End to show this subvlan proxyarp status-----

config proxyarp agetime <0-196605>
```

4、配置 ARP 代理的 age time

【命令原型】config proxyarp agetime <0-196605>

【参数说明】<0-196605> 表示 proxyarp 老化的时间，单位为秒。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#con proxyarp agetime 321
Now Proxyarp entry aging time is 321(s)
Harbour(config)#sh pro sub sub

----Begin to show this subvlan proxyarp status----

Subvlan Name          : sub
Search List aging time  : 123(s)
```

```
Cache entry aging time  : 321(s)
Proxy ARP status       : Enable

-----End to show this subvlan proxyarp status-----
show proxyarp table {<A.B.C.D>}*1
```

5、显示系统当前的 ARP 代理表项

【命令原型】show proxyarp table {<A.B.C.D>}*1

【参数说明】{<A.B.C.D>}*1 表示显示某一指定 ip 地址的 arp 代理表项

【配置模式】只读模式或者配置模式

【配置实例】

```
Harbour(config)#show proxyarp table
Begin to show proxyarp table information
Ip Address        Mac Address        Subvlan       timeout (s)
------------------------------------------------------------------------
192.168.0.200      00:50:fc:3c:13:d0   sub          210
------------------------------------------------------------------------
Total proxyarp entries: 1
End to show proxyarp table information
```

6、根据 IP 删除相应 ARP 代理的表项

【命令原型】config proxyarp delete <A.B.C.D>

【参数说明】<A.B.C.D>表示指定的 ip 地址

【命令模式】配置模式

【配置实例】

```
Harbour(config)#config proxyarp delete 192.168.0.200
```

6.6 VLAN 子接口的配置

6.6.1 VLAN 子接口介绍

VLAN 子接口就是在一个 VLAN 的虚拟接口上配置几个子接口，每个子接口都可以配置 IP 地址，每个子接口独立工作。但它们都通过相同的 VLAN 来收发数据包。也就是说一个 VLAN 的所有子接口的二层都是一样的。它们只是在三层处理时有区别。

在一个接口创建多个子接口，然后在每个子接口上可以配置一个和其他的子接口在不同网段的 IP 地址，这样一个接口就可以和多个网段的子网进行连接，方便了对网络设备的管理。同时通过这种创建不同子接口的方式也可以实现网络的备份管理。

6.6.2 VLAN 子接口的配置规则

- 每个 VLAN 可以支持多个子接口，子接口也支持动态路由。在创建子接口时先创建主接口，同时每个子接口都创建在 VLAN 上，在删除 VLAN 的同时，VLAN 下的所有子接口也会被同时删除。（注意：Sub VLAN 上不支持子接口的创建）
- 每个子接口只支持 IP 地址的配置，除了在子接口上配置 IP 地址外，现在子接口不支持任何其他配置。

6.6.3 VLAN 子接口的创建

【命令原型】create sub-interface <subifname> vlan <vlanname>

【参数说明】<subifname>：要创建的子接口的名称，建议采用“vlan 名称”＋“_”开头，

<vlanname>：子接口所在 VLAN 的名称。

【命令模式】配置模式

【配置实例】在 vlan default 上创建一个名称为 default_1 的子接口

```
Harbour(config)# create sub-interface default_1 vlan default
```

6.6.4 VLAN 子接口的删除

【命令原型】delete sub-interface <subifname> vlan <vlanname>

【参数说明】<subifname>：要删除的子接口的名称，一般采用“vlan 名称”＋“_”开头，

<vlanname>：子接口所在 VLAN 的名称。

【命令模式】配置模式

【配置实例】在 vlan default 上删除一个名称为 default_1 的子接口

```
Harbour(config)#delete sub-interface default_1 vlan default
```

6.6.5 配置 VLAN 子接口的 IP 地址

【命令原型】config sub-interface <subifname> ipaddress <A.B.C.D/M>

【参数说明】<subifname>：要配置的子接口的名称。<A.B.C.D/M>：要在子接口上配置的 IP 地址，M 为子网掩码长度；也可以采用<A.B.C.D> <A.B.C.D>的形式。

【命令模式】配置模式

【配置实例】给子接口 default_1 配置 IP 地址 1.1.1.1/24

Harbour(config)# config sub-interface default_1 ipaddress 1.1.1.1/24

6.6.6 删除 VLAN 子接口上的 IP 地址

【命令原型】no sub-interface <subifname> ipaddress

【参数说明】<subifname>：要配置的子接口的名称。

【命令模式】配置模式

【配置实例】删除子接口 default_1 配置 IP 地址

```
Harbour(config)#no sub-interface default_1 ipaddress
```

6.6.7 显示 VLAN 上的子接口

【命令原型】show sub-interface {vlan<name>}*1

【参数说明】<name>：子接口所在的 VLAN 的名称。

【命令模式】配置模式

【配置实例】显示 vlan default 上配置的子接口

Harbour(config)#show sub-interface default

```
************sub-interface of vlan default ************
Interface default_1
index 8 metric 1 mtu 1500 <BROADCAST,LINK0,MULTICAST>
inet 1.1.1.1/24 broadcast 1.1.1.255

Total sub-interface entry: 1
```

6.6.8 VLAN 子接口的命令列表

下表列出了 vlan 中 sub-interface 的所有配置命令。

命令	解释
create sub-interface <subifname> vlan <vlanname>	在 vlan 上创建一个子接口， <subifname>：子接口名称 <vlanname>：vlan 名称
delete sub-interface <subifname> vlan <vlanname>	从 vlan 中删除子接口 <subifname>：子接口名称 <vlanname>：vlan 名称
config sub-interface <subifname> ipaddress <A.B.C.D/M>	配置子接口的 IP 地址
show sub-interface {vlan<name>}*1	显示系统中配置 vlan 的信息。

6.7 VLAN 端口隔离

6.7.1 VLAN 端口隔离概述

VLAN 端口隔离用以限制 VLAN 内各端口之间的访问操作，VLAN 内每个端口只能和上行端口通信，相互之间隔离，不能相互访问。上行口为普通工作模式，ingress 包按普通方式转发。VLAN 的端口隔离配置必须遵循以下规则：

1. Default VLAN 不可配置端口隔离
2. VLAN 上行端口不支持 Load sharing
3. VLAN 上行端口不支持 mirrored_to_port
4. VLAN 的上行端口不能从 VLAN 中删除
5. 端口隔离的 VLAN 不支持基于 VLAN 的 QoS

6.7.2 创建 VLAN 端口隔离

【命令格式】config vlan <name> uplink_port <portno>

【使用指导】为 VLAN 设置上行端口，该端口为 VLAN 成员端口。一个 VLAN 配置了上行端口后，该 VLAN 内每个端口只能和上行端口通信，相互之间隔离，不能相互访问。

【参数说明】参数<name>为 VLAN 名称；portno 为上行口端口号。

【配置实例】

```
Harbour(config)#create vlan iso_vlan
Harbour(config)#config vlan iso_vlan add port 1,2,3 untagged
Harbour(config)#config vlan iso_vlan uplink_port 1
```

此时端口 1 为 vlan iso_vlan 的上行端口， vlan iso_vlan 的其他成员端口 2、3 之间不能访问，只能各自与上行口通信。

注意：当 VLAN 配置了上行端口时，show vlan 命令中会有所反映，例如：

```
Harbour(config)#show vlan iso_vlan
```

```
VLAN ID       : 2046
Name          : iso_vlan
VLAN Type     : Normal
MAC address   : 00:05:3b:80:00:01
Uplink Port   : 1
Tagged Ports  :
Untagged Ports : 1  2  3
```

6.7.3 删除 VLAN 端口隔离

【命令格式】no vlan <name> uplink_port

【命令作用】取消 VLAN 端口隔离配置。

【参数说明】参数 name 为 VLAN 的名称。

【配置实例】

```
Harbour(config)#no vlan iso_vlan uplink_port
```

第7章 生成树协议

本章包括以下内容

- STP 协议介绍、相关配置及显示 STP 状态
- RSTP 协议介绍、相关配置及显示 RSTP 状态

7.1 STP

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

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

7.1.1 STP 相关配置

使能或关闭 STP

Hammer 交换机中 STP 缺省状态是关闭的。使能或关闭指定的 STP，利用命令：

config stpd default [enable | disable]

如果键入 enable，表示 STP 有效，如果键入 disable，则表示 STP 无效。

例如：使能 STP，在配置模式下，键入命令：

config stpd default enable

使能或关闭指定 STP 的端口

Hammer 交换机中所有端口默认都是参与 STP 计算的。使能或关闭指定的 STP 端口，在配置模式下，键入命令：

config stpd default port [<portlist>|all] [enable|disable]

其中<portlist>|all 表示所要操作的端口列表，all 表示对所有端口进行操作；如果键入 enable，表示使该端口的 stp 有效，如果为 disable，则无效。

例如：使能指定端口 10 的 STP 功能，在配置模式下，键入命令：

config stpd default port 10 enable

配置指定 STP 的参数

一旦运行某个指定 STP 的 STP 协议后，您可能需要根据具体的网络结构调整该 STP 的一些参数。以下的 STP 协议参数可以在 Hammer 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

配置运行 STP 协议时本交换机的优先级

设置运行 STP 协议时本交换机的优先级。利用命令：

config stpd default priority <0-65535>

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。

例如：设置运行 STP 协议时本交换机的优先级为 2000，键入命令：

config stpd default priority 2000

配置根桥交换机发送 BPDU 的时间间隔

设置当本交换机被选为根桥时发送 BPDU 的时间间隔，利用命令：

config stpd default hellotime <1-10>

HelloTime 的取值范围是 1-10，单位为秒，缺省值是 2 秒。

例如：设置当本交换机被选为根桥时发送 BPDU 的时间间隔为 5 秒，键入命令：

config stpd default hellotime 5

注意：HelloTime 必须小于等于 ForwardDelay-2

配置根桥交换机端口状态切换的时间间隔

设置当本交换机被选为根桥时端口状态切换的时间间隔，利用命令：

config stpd default forwarddelay <4-30>

ForwardDelay 的取值范围是 4-30，单位秒，缺省值为 15 秒。

例如：设置当本交换机被选为根桥时端口状态切换的时间间隔为 20 秒，键入命令：

config stpd default forwarddelay 20

注意：ForwardDelay 的时间必须大于等于 HelloTime+2

配置 BPDU 报文老化的最长时间间隔

设置 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。利用命令：

config stpd default maxage <6-40>

MaxAge 的取值范围是 6-40，单位为秒，缺省值为 20 秒。

例如：设置 BPDU 报文老化的最长时间间隔为 30 秒，键入命令：

config stpd default maxage 30

注意：Maxage 的时间必须大于等于 2*(HelloTime + 1)，小于等于 2*(ForwardDelay – 1)

配置参与 STP 计算的端口的优先级

配置参与 STP 计算的端口的优先级，利用命令：

config stpd default port [<portlist> | all] priority <0-255>

其中，<portlist>表示对指定端口进行操作，all 表示对所有端口进行操作。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。

例如：设置参与 STP 计算的端口 10 的优先级为 120，键入命令：

config stpd default port 10 priority 120

配置参与 STP 计算端口的路径开销

配置参与 STP 计算端口的路径开销，利用命令：

config stpd default port [<portlist> | all] cost <1-65535>

其中，<portlist>表示对指定端口进行操作，all 表示对所有端口进行操作。取值范围是 1-65535，HammerOS 根据端口的当前速度设置不同的缺省值：

- 10Mbps 端口缺省值为 100
- 100Mbps 端口缺省值为 19
- 1000Mbps 端口缺省值为 4

例如：设置参与 STP 计算端口的路径开销为 200，键入命令：

config stpd default port 10 cost 200

7.1.2 显示 STP 状态

显示 STP 的状态

STP 的显示内容包括：

- BridgeID
- Root BridgeID
- STP 的各种配置的参数

利用命令：show stpd default

例如：显示 STP 状态信息，键入命令：show stpd default。信息显示如下：

```
 STP Domain default information

---------------------------------------------------------
-- Designated Root Info --
Priority            :  32768
Mac address         :  00：05：3b：00：04：90
Max Age             :  30
Hello Time          :  5
Forward Delay       :  20
-- STP Domain Config Info --
Priority            :  32768
Mac address         :  00：05：3b：00：04：90
Root Path Cost      :  200
Root Port           :  10
Bridge Max Age      :  30
```



```
Bridge Hello Time   :  5

Bridge Forward Delay:  20

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

显示端口的 STP 状态

端口的 STP 显示内容包括：

- 端口状态
- Designated port
- 端口的各种配置参数

利用下面的命令：

show stpd default port [<portlist> | all]

其中，<portlist>表示对指定端口进行操作，all 表示对所有端口进行操作。

例如：显示端口 10 的 STP 状态，键入命令：

show stpd default port 10

信息显示如下：

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

Port 10 's Spanning Tree Protocol Information

Port Join STP Domain default 's Calculate

-- Port Info --

Port id              :  18

Priority             :  120

State                :  Disable

Path Cost            :  100

Designated Cost      :  0

-- Designated Port --

Port id              :  18

Priority             :  128

-- Designated Root --
```

```
    Priority             :  32768
    Mac address          :  00：05：3b：00：04：90
    -- Designated Bridge --
    Priority             :  32768
    Mac address          :  00：05：3b：00：04：90
    ---------------------------------------------------------------------
```

7.1.3 STP 的配置命令列表

表 7-1 STP 配置命令列表

命令	解释
config stpd default [enable | disable]	使能或关闭 STP
config stpd default priority <0-65535>	设置运行 STP 协议时本交换机的优先级。 优先级的取值范围是 0-65535，缺省值为 32768。 优先级数值越低，越有可能成为网络中的根桥（Root Bridge）。优先级值为 0 代表了最高的优先级。
config stpd default hellotime <1-10>	设置当本交换机被选为根桥时发送 BPDU 的时间间隔。 HelloTime 的取值范围是 1-10，单位为秒，缺省值是 2 秒。
config stpd default forwarddelay <4-30>	设置当本交换机被选为根桥时端口状态切换的时间间隔。 ForwardDelay 的取值范围是 4-30，单位秒，缺省值为 15 秒。
config stpd default maxage <6-40>	设置 BPDU 报文老化的最长时间间隔，收到超过这个时间的 BPDU 报文，就直接丢弃。 MaxAge 的取值范围是 6-40，单位为秒，缺省值为 20 秒。
config stpd default port [<portlist>|all] [enable|disable]	指定参与 STP 协议计算的端口。
config stpd default port [<portlist> | all] priority <0-255>	配置参与 STP 计算的端口的优先级。 端口优先级的取值范围是 0-255，缺省值

	是 128。 优先级数值越低，端口越容易成为根端口（Root Port），优先级值为 0 代表了最高的优先级。
config stpd default port [<portlist> | all] cost <1-65535>	配置参与 STP 计算端口的路径开销。 取值范围是 1-65535，HammerOS 根据端口的当前速度设置不同的缺省值： 10Mbps 端口缺省值为 100 100Mbps 端口缺省值为 19 1000Mbps 端口缺省值为 4
show stpd default	显示 STP 状态信息
show stpd default port [<portlist> | all]	显示端口 STP 状态信息

7.2 RSTP

RSTP 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。

7.2.1 配置 RSTP

在交换机上配置 RSTP 包含以下内容：

- 使能或者关闭交换机 RSTP 功能
- 使能或者关闭端口的 RSTP 功能
- 配置指定的 RSTP 参数

使能或者关闭交换机的 RSTP 功能

Hammer 交换机中 RSTP 功能是默认关闭的。使能或者关闭 RSTP 功能，在配置模式下，键入命令：

config spanning-tree [enable | disable]

如果键入 enable， 表示使能 RSTP；如果键入 disable， 表示关闭 RSTP 功能。

例如：使能 RSTP，在配置模式下，键入命令：

config spanning-tree enable

使能或者关闭端口的 RSTP 功能

Hammer 交换机中所有端口都是默认参与 RSTP 计算的。使能或者关闭端口的 RSTP 功能，在配置模式下，键入命令：

Config spanning-tree port <portlist> [none-stp] [yes | no]

其中<port>表示所要操作的端口的端口号；如果参数为 yes，则表示关闭该端口的 RSTP 功能，如果参数为 no，表示使能该端口的 RSTP 功能。

例如：关闭指定端口 10 的 RSTP 功能，在配置模式下，键入命令：

config spanning-tree port 10 none-stp yes

配置指定的 RSTP 参数

一旦运行了 RSTP 协议，您可能需要根据具体的网络结构调整 RSTP 的一些参数：

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

另外，每个端口还有以下参数可以调整：

- Path Cost
- Port Priority
- P2P 属性
- Edge 属性

配置运行 RSTP 协议时本交换机的优先级

设置运行 RSTP 协议时本交换机的优先级，利用命令：

Config spanning-tree priority <0-61440>

交换机优先级的范围为 0-61440，缺省值为 32768。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 代表了最高的优先级。交换机的优先级数值应该是 4096 的倍数。例如：设置运行 RSTP 协议时本交换机的优先级为 8192，键入命令：

config spanning-tree priority 8192

配置本交换机发送 BPDU 的时间间隔

设置本交换机发送 BPDU 的时间间隔，利用命令：

Config spanning-tree hello-time <1-10>

HelloTime 的取值范围是 1－10，单位为秒，缺省值为 2 秒。例如：设置本交换发送 BPDU 的时间间隔为 4 秒，键入命令：

config spanning-tree hello-time 4

配置本交换机端口状态切换的时间间隔

设置本交换机端口状态切换的时间间隔，利用命令：

Config spanning-tree forward-delay <4-30>

ForwardDelay 的取值范围是 4－30，单位为秒，缺省值为 15 秒。例如，设置本交换机端口状态切换的时间间隔为 10 秒，键入命令：

config spanning-tree forward-delay 10

注意：Hello-time， Max-Age 和 Forward-Delay 的配置值必须满足以下关系：

2*(Hello-time + 1) <= Max-Age <= 2*(Forward-Delay -1)

配置 BPDU 报文老化的最长时间间隔

设置 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。利用命令：

Config spanning-tree maximum-age <6-40>

Maximum-age 的取值范围是 6－40，单位为秒，缺省值为 20 秒。例如，设置 RSTP BPDU 报文老化的最长时间间隔为 30 秒，键入命令：

config spanning-tree maximum-age 30

注意：Hello-time， Max-Age 和 Forward-Delay 的配置值必须满足以下关系：

2*(Hello-time + 1) <= Max-Age <= 2*(Forward-Delay -1)

配置参与 RSTP 计算的端口的优先级

配置参与 RSTP 计算的端口的优先级，利用命令：

Config spanning-tree port <port> [priority] <0-240>

端口优先级的取值范围是 0－240，端口优先级的值应该是 16 的倍数，其缺省值是 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。例如，设置参与 RSTP 计算的端口 10 的优先级为 96，键入命令：

config spanning-tree port 10 priority 96

配置参与 RSTP 计算的端口的路径开销

配置参与 RSTP 计算的端口的路径开销，利用命令：

Config spanning-tree port <port> [path-cost] [auto | <1-200000000]

端口的路径开销的取值范围是 1-200000000。 用户可以自己设定端口开销，也可以使用系统的默认设置，即 auto。 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 计算的端口的端口路径开销。

- 10Mbps 端口缺省值为 2000000
- 100Mbps 端口缺省值为 200000
- 1000Mbps 端口缺省值为 20000

例如，设置参与 RSTP 计算的端口 10 的路径开销为 300000，键入命令：

config spanning-tree port 10 path-cost 300000

配置交换机的 STP 协议的版本

为了兼容 IEEE 802.1d 标准规定的 STP 协议，在 RSTP 运算中，用户可以设置交换机运行 802.1d 的 STP 协议，利用命令：

config spanning-tree [force-version] [0 | 2]

当取 force-version 的值为 2 时，交换机运行 RSTP 协议；当取 force-version 的值为 0 时，交换机运行老的 STP 协议。其缺省值为 2，即交换机默认执行 RSTP 协议。例如，设置交换机运行 IEEE 802.1d STP 协议，键入命令：

config spanning-tree force-version 0

选择 STP 协议的工作模式

用户可以选择运行 802.1d STP 协议或者 802.1w RSTP 协议，利用命令：

config spanning-tree mode [stp|rstp]

stp 表示 802.1d STP 协议，rstp 表示 802.1w RSTP 协议。如用户希望运行 RSTP 时，键入命令：

config spanning-tree mode rstp

配置端口的 P2P 属性：

配置端口的 P2P 属性，利用命令：

Config spanning-tree port <port> p2p [yes | no | auto]

可以取值 yes， no， auto。其缺省值为 auto， 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。例如，设置端口 10 的 P2P 属性为真，键入命令：

config spanning-tree port 10 p2p yes

配置端口的 edge 属性：

配置端口的 Edge 属性，利用命令：

config spanning-tree port <port> [edge] [yes | no]

edge 属性可以取值 yes， no，其缺省值为 no。当交换机的这个端口直接与主机相连，或者这个端口再不与其他交换机连接的情况下，可以设置端口的 edge 属性为 yes，这样可以使得端口可以进行快速的状态转换。例如，设置端口 10 的 edge 属性为真，键入命令：

config spanning-tree port 10 edge yes

7.2.2 显示 RSTP 状态

显示交换机 RSTP 的状态

RSTP 的显示内容：

- BridgeID
- Root BridgeID
- RSTP 的各种配置的参数

显示 RSTP 状态的内容，利用命令：show spanning-tree。例如，在交换机上，显示 RSTP 状态信息，键入命令：

show spanning-tree

信息显示如下：

----------SPANNING TREE infomation in STP domain 2047 ----------

-- Designated Root Info --

Priority : 133726292

MAC address : 00:05:3b:04:00:50

Designated Port ID : 0/13

Max Age : 20

Hello Time : 2

Forward Delay : 15

-- STP Domain Config Info --

Priority : 133726272

MAC address : 22:22:22:22:22:22

Root Port : 0/18

Root Path Cost : 200000

Bridge Max Age : 20

Bridge Hello Time : 2

Bridge Forward Delay : 15

Bridge ForceVersion : 2

----------All ports infomation in STP domain 2047 ----------

Num	pri	path--cost	role	span-state	lnk	p2p	edg	pen	dcost	designated root id
0/24	128	2000000	Dis	Discarding	N	N	N	N	200000	32768:00053b040050
0/23	128	2000000	Dis	Discarding	N	N	N	N	200000	32768:00053b040050
0/22	128	2000000	Dis	Discarding	N	N	N	N	200000	32768:00053b040050
0/21	128	2000000	Dis	Discarding	N	N	N	N	200000	32768:00053b040050
0/20	128	2000000	Dis	Discarding	N	N	N	N	200000	32768:00053b040050
0/19	128	2000000	Dis	Discarding	N	N	N	N	200000	32768:00053b040050
0/18	128	200000	Root	Forwarding	Y	Y	N	N	200000	32768:00053b040050
0/17	128	2000000	Dis	Discarding	N	N	N	N	200000	32768:00053b040050
0/16	128	2000000	Dis	Discarding	N	N	N	N	200000	32768:00053b040050
0/15	128	2000000	Dis	Discarding	N	N	N	N	200000	32768:00053b040050
0/14	128	2000000	Dis	Discarding	N	N	N	N	200000	32768:00053b040050

0/13	128	2000000	Dis	Discarding	N	N	N	N	200000 32768:00053b040050
0/12	128	2000000	Dis	Discarding	N	N	N	N	200000 32768:00053b040050
0/11	128	2000000	Dis	Discarding	N	N	N	N	200000 32768:00053b040050
0/10	128	2000000	Dis	Discarding	N	N	N	N	200000 32768:00053b040050
0/9	128	2000000	Dis	Discarding	N	N	N	N	200000 32768:00053b040050
0/8	128	2000000	Dis	Discarding	N	N	N	N	200000 32768:00053b040050
0/7	128	2000000	Dis	Discarding	N	N	N	N	200000 32768:00053b040050
0/6	128	2000000	Dis	Discarding	N	N	N	N	200000 32768:00053b040050
0/5	128	2000000	Dis	Discarding	N	N	N	N	200000 32768:00053b040050
0/4	128	2000000	Dis	Discarding	N	N	N	N	200000 32768:00053b040050
0/3	128	2000000	Dis	Discarding	N	N	N	N	200000 32768:00053b040050
0/2	128	2000000	Dis	Discarding	N	N	N	N	200000 32768:00053b040050
0/1	128	2000000	Dis	Discarding	N	N	N	N	200000 32768:00053b040050

显示端口的 RSTP 状态

端口的 RSTP 状态的显示内容：

- 端口状态
- 端口配置参数

显示端口 RSTP 状态，利用下面的命令：show spanning-tree port <port>。其中，<port>表示指定端口的端口号。例如，在交换机上，显示端口 10 的 STP 状态，键入命令：

show spanning-tree port 10

信息显示如下：

----- port 0/0 infomation in STP domain 2047 -----

Num	pri	path--cost	role	span-state	lnk	p2p	edg	pen	dcost	designated root id
0/10	128	2000000	Dis	Discarding	N	N	N	N	200000	32768:00053b040050

7.2.3 RSTP 的配置命令列表

表 7-2RSTP 配置命令列表

命令	解释
config spanning-tree [enable | disable]	使能或关闭 RSTP 功能
config spanning-tree priority <0-61440>	配置桥的优先级（4096 的倍数）
config spanning-tree maximum-age <6-40>	配置 BPDU 的老化时间
config spanning-tree hello-time <1-10>	配置桥的 hello-time
config spanning-tree forward-delay <4-30>	配置桥的 forward-delay
config spanning-tree [force-version] [0 | 2]	配置 RSTP 协议的版本
config spanning-tree mcheck yes	检测是否有运行 802.1d STP 的桥相连
config spanning-tree port <port> [path-cost] [auto | <1-200000000]	配置端口的路径开销
config spanning-tree port <port> [priority] <0-240>	配置端口的优先级(16 的倍数)
config spanning-tree port <port> [none-stp] [yes | no]	配置端口使能或关闭 RSTP 功能
config spanning-tree port <port> p2p [yes | no | auto]	配置端口的 P2P 属性
config spanning-tree port <port> [edge] [yes | no]	配置端口的 edge 属性
show spanning-tree	查看桥的 RSTP 的配置状态
show spanning-tree port <port>	查看端口的 RSTP 的配置状态

第8章 DHCP Relay

这一章主要讲述如何用 HammerOS 来配置 DHCP Relay。包括：

- DHCP概述
- DHCP Relay概述
- DHCP Relay在交换机上的配置
- DHCP Relay命令参考
- 配置示例

8.1 DHCP 概述

动态主机配置协议(Dynamic Host Configuration Protocol,简称 DHCP)是基于 TCP/IP 协议簇的一种动态地址分配方案。与手工配置相比，DHCP 具有以下优势：

- DHCP是一种基于公开标准的协议：最早出现于RFC1531和1541,最新的规范由IETF的RFC2131和2132所定义。
- 对IP地址的动态分配：可规定地址的租借期限，超过租借期限的IP地址将被回收以重新使用。
- 自动配置：客户端的配置是自动进行的，所有TCP/IP参数的分配和改变对用户来说都是透明的。
- DHCP是基于BOOTP的：它提供了更多的特性，更大的分配灵活性，加入了自动分配可以重用的网络地址和额外的配置选项功能。

当一台连接到 TCP/IP 网络上的计算机启动时，DHCP 能够自动地为这台计算机配置有关的 TCP/IP 参数，包括 IP 地址、子网掩码、缺省网关、DNS 等等。这样，可把所有 TCP/IP 协议的配置信息集中地存储到 DHCP 服务器上。集中的存储和管理能够避免 IP 地址的冲突，同时把管理员从繁重的手工配置劳动中解放出来。网络的规模越大，DHCP 的优势就越明显。

8.2 DHCP Relay 概述

如果 DHCP 客户机与 DHCP 服务器在同一个物理网段，则客户机可以正确地获得动态分配的 ip 地址。如果不在同一个物理网段，则需要 DCHP Relay Agent(中继代理)。

用 DHCP Relay 代理可以去掉在每个物理的网段都要有 DHCP 服务器的必要,它可以传递消息到不在同一个物理子网的 DHCP 服务器，也可以将服务器的消息传回给不在同一个物理子网的 DHCP 客户机。

8.3 DHCP Relay 在交换机上的配置

DHCP Relay 在交换机上的配置包括：

1. VLAN 的监听
2. DHCP 服务器的设置
3. DHCP Relay 服务的启动和停止
4. 显示 DHCP Relay 监听状态
5. 显示 DHCP 服务器地址
6. 显示 DHCP Relay 服务的状态

8.3.1 VLAN 的监听

指定 DHCP Relay 服务所监听的 vlan 接口。可以利用如下命令：

【命令原型】config dhcpr listen [add|delete] <vlanname>

【使用指导】参数 add 表示 DHCP Relay 服务所监听的 vlan 接口，delete 表示删除 DHCP Relay 服务所监听的 vlan 接口；vlanname 表示 vlan 接口的名称。

【命令模式】配置模式

【配置实例】指定 DHCP Relay 服务所监听的 vlan 接口 e2。

```
Harbour(config)#config dhcpr listen add e2
```

注意：此处必须先给接口 e2 分配 ip 地址。

注意：如果当 dhcpr 服务已经启动的情况下，如果增加或删除了一个 vlan 接口时，只有重新启动 dhcpr 服务，才会有效。

8.3.2 DHCP 服务器的设置

【命令原型】config dhcpr targetip [add|delete] <A.B.C.D> {id <1-32>}*1

【使用指导】参数 add 表示增加一个 dhcp 服务器的 IP 地址，delete 表示删除一个 dhcp 服务器的 IP 地址；<A.B.C.D>表示 DHCP 服务器的 IP 地址；id 是 DHCP 服务器序号。

注意：在 dhcpr 服务已经启动的情况下，如果增加或删除了一个 DHCP 服务器时，只有重新启动 dhcpr 服务，才会有效。

【配置实例】增加一个 DHCP 服务器地址 10.7.100.9

```
config dhcpr targetip add 10.7.100.9
```

删除一个 DHCP 服务器地址 10.7.100.9 时，可使用如下命令：

```
config dhcpr targetip delete 10.7.100.9
```

注意：如果 DHCP 服务器与交换机处于不同网段时，需要配置本交换机到 DHCP 服务器的路由。可以使用 ip route 命令指定。

8.3.3 使能或者禁止 DHCP Relay 服务

【命令原型】service dhcpr [enable|disable]

【命令指导】选择参数 enable 表示使能 DHCP Relay 服务,选择 disable 表示禁用 DHCP Relay 服务

【命令模式】配置模式

【配置实例】启动 DHCP Relay 服务

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

注意：如果没有接口被监听或没有配置 DHCP 服务器，将不能启动 DHCP Relay 服务。并将提示如下错误：

No interface is listened by dhcp relay , Failed to start dhcp relay

/There is no configured target server.

8.3.4 显示 DHCP Relay 监听状态

显示 DHCP Relay 服务当前监听的 vlan 接口，可以利用如下命令：

【命令原型】show dhcpr listen

【命令模式】只读模式或者配置模式

【命令模式】只读或者配置模式

【配置实例】

```
Harbour(config)# show dhcpr listen

Dhcp relay listen vlan: e2
Dhcp relay listen vlan: e3
Dhcp relay listen vlan: e4
```

可以看出，当前 DHCP Relay 服务监听的 vlan 接口有：e2,e3,e4

8.3.5 显示 DHCP 服务器地址

显示当前 DHCP 服务器地址，可以利用如下命令：

【命令原型】show dhcpr targetip

【命令模式】只读模式或者配置模式

【配置实例】

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

```
dhcpr target ip 10.7.100.9  id  1
```

可以看出，当前配置的 DHCP 服务器地址有：10.7.100.9

8.3.6 显示 DHCP Relay 服务状态

显示 DHCP Relay 服务状态，可以利用如下命令：

【命令原型】show dhcpr status

【命令模式】只读模式或者配置模式

【配置实例】

```
Harbour(config)# show dhcpr status

Dhcp relay is down
```

表明当前 DHCP Relay 服务没有启动。

8.4 配置实例

```
Harbour(config)# config dhcpr listen add e2
Harbour(config)# config dhcpr listen add e3
Harbour(config)# config dhcpr listen add e4
Harbour(config)# config dhcpr targetip add 10.7.100.9
Harbour(config)# service dhcpr enable

Successfully start dhcp relay
```

8.5 DHCP Relay 命令参考

命令	解释
config dhcpr listen [add|delete] <vlanname>	配置 VLAN 的监听
config dhcpr targetip [add|delete] <A.B.C.D> {id <1-32>}*1	配置 DHCP 服务器的地址
service dhcpr [enable|disable]	启动或停止 DHCP Relay 服务
show dhcpr listen	显示 DHCP Relay 监听接口
show dhcpr targetip	显示配置的 DHCP 服务器地址
show dhcpr status	显示 DHCP Relay 服务状态

第9章 VRRP 协议

本章包括如下内容：

- VRRP协议介绍
- VRRP的相关配置
- 显示VRRP配置信息
- 使用举例

9.1 VRRP 概述

9.1.1 VRRP（Virtual Router Redundancy Protocol）协议介绍

目前指定缺省网关一般有两种方法，一种是使用如最短路径优先(OSPF)协议或路由信息协议(RIP)等动态路由协议来确定正确的缺省网关。 OSPF 和 RIP 能够绕过任意故障点来选择最佳网关，但动态路由协议对终端系统的处理开销较大，且收敛过程慢。另一种方法是使用静态配置的缺省网关来减少处理开销。但这种方法的风险是使作为缺省网关的路由器成为单一故障点。对于一个主机来说，经常使用第二种方法来实现默认网关配置。

VRRP 可避免静态指定网关的缺陷。通过 VRRP，一组路由器可以一起协同工作，共同组成一台虚拟路由器。该虚拟路由器对外配有一个虚拟 IP 地址和 MAC 地址，VRRP 从路由器组中选出一台作为 master，负责转发数据包。当主路由器发生故障时，备份路由器会迅速接管主路由器，主机不必改变缺省网关地址，且此过程对于终端系统是透明的。这样就提供了在故障发生时更快、更有效地解决方法。

此外，该协议还可以在负载分担应用中发挥作用。例如，VRRP 可以使一台路由器作为一个 IP 子网的主路由器，同时作为另一个子网的备份路由器。用这种方式配置的两台路由器可以实现负载分担：每一台路由器都相互作为另一台路由器的冗余备份路由器。

VRRP 协议实现了局域网的冗余性和恢复性，提高了网络的高可靠性。

9.1.2 VRRP 协议状态

参与 VRRP 协议的路由器有三种状态，当路由器以这些状态中的其中一种存在时，它将执行该状态所需要进行的工作。这些 VRRP 状态如下：

- 初始状态：

所有的路由器都是从初始状态开始，这只是个过渡状态。路由器处于此状态时表明 VRRP 还没有运

行，当一个接口第一次启用时就进入该状态。

- 备份状态：

处于该状态的路由器通过收发主路由器发来的数据包来监听主路由器的状态，并时刻准备接管主路由器。

- 活跃状态：

处于活跃状态的路由器称为主路由器，主路由器负责转发被发送到此 VRRP 组的虚拟 MAC 地址的数据包。并且主路由器还向备份路由器发送周期性广播报文。在一个 VRRP 组中必须有且只能有一台主路由器。

9.2 VRRP 配置规则

在配置交换机的 VRRP 时，需要遵循一定的标准规范。配置规则如下：

9.2.1 虚拟路由器 ID

一个虚拟路由器由唯一的虚拟路由器标识号(VRID)确定，FlexHammer5000 系列共支持 255 个虚拟路由器，VRID 的范围为 1-255。 VRID 缺省值为 1。

9.2.2 工作接口

虚拟路由器的工作接口和系统中的 interface 是对应的。

9.2.3 IP 地址

一个虚拟路由器可指定一个 IP 地址，虚拟路由器的 IP 地址和工作接口的 IP 地址应该属于同一个 IP 网络。

9.3 配置 VRRP

在交换机上配置 VRRP 包含以下内容：

- 配置虚拟路由器的各种参数
- 使能或关闭虚拟路由器
- 恢复虚拟路由器的各种参数的缺省值

配置虚拟路由器的各种参数

运行 VRRP 协议，可以根据需要配置虚拟路由器的各种参数。其中必须配置的参数有：

- VRID，取值为1－255，缺省是1
- IP地址，和所在接口在同一网段

可调整的参数有：

- 优先级，缺省为100
- 广播间隔，缺省为1秒
- 抢占模式，缺省为抢占模式
- 认证密码。
- 名字，缺省为HOS—VRRP

9.3.1 配置虚拟路由器 IP 地址并启动

配置虚拟路由器的接口、IP 地址并启动。利用命令：

【命令原型】vrrp {<1-255>}*1 ipaddress <A.B.C.D>

【参数说明】vrid 取值为 1－255，缺省是 1；<A.B.C.D>为虚拟路由器的 ip 地址。

【命令模式】接口模式

【配置实例】创建一个 VRID 号是 10，在网段 11.1.20.30 的虚拟路由器，并启动，则键入命令：

```
Harbour(config-if)# vrrp 10 ipaddress 11.1.20.30
```

9.3.2 删除虚拟路由器

【命令原型】no vrrp {<1-255>}*1 ipaddres

【参数说明】vrid 取值为 1－255，缺省是 1；

【命令模式】接口模式

【配置实例】删除 VRID 是 10 的虚拟路由器，则键入如下命令：

```
Harbour(config-if)# no vrrp 10 ipaddress
```

9.3.3 配置虚拟路由器的优先级

【命令原型】vrrp {<1-255>}*1 priority <1-254>

【参数说明】vrid 取值为 1－255，缺省是 1；优先级的取值范围是 1-254，缺省值为 100。

0、255 为保留优先级值，不可配置。优先级数值越高，表示优先级越高。255 为保留优先级值，工作接口所在地址与 IP 地址一致的主路由器其优先级自动设置为 255。当优先级为 0 时，表示主路由器将要释放其主动权给备份路由器。

【命令模式】接口模式

【配置实例】设置虚拟路由器 10 的优先级为 120，键入命令：

```
Harbour(config-if)# vrrp10 priority 120
```

9.3.4 恢复虚拟路由器优先级的缺省值

虚拟路由器优先级的缺省值是 100，恢复缺省值的命令为：

【命令原型】no vrrp {<1-255>}*1 priority

【参数说明】vrid 取值为 1－255，缺省是 1；

【命令模式】接口模式

【配置实例】恢复虚拟路由器 10 的优先级为缺省值，键入命令：

```
Harbour(config-if)# no vrrp10 priority
```

9.3.5 配置虚拟路由器的报文发送间隔

设置虚拟路由器的广播间隔。利用命令：

【命令原型】vrrp {<1-255>}*1 advertise-timer <1-5>

【参数说明】vrid 取值为 1－255，缺省是 1；广播间隔的取值范围是 1-5，单位为秒，缺省值为 1 秒。

【命令模式】接口模式

【配置实例】设置虚拟路由器 10 的广播间隔为 2 秒，键入命令：

```
Harbour(config-if)# vrrp 10 advertise-timer 2
```

9.3.6 恢复虚拟路由器的报文发送间隔为缺省值

【命令原型】no vrrp {<1-255>}*1 advertise-timer

【参数说明】vrid 取值为 1－255，缺省是 1；

【命令模式】接口模式

9.3.7 配置虚拟路由器的抢占模式

【命令原型】vrrp {<1-255>}*1 preempt [on|off]

【参数说明】vrid 取值为 1－255，缺省是 1；

【命令模式】接口模式

【使用指导】抢占模式是指是否允许优先级高的备份路由器取代低优先级的主路由器的模式，on 为允许抢占，off 为禁止抢占，缺省值为 on。

【配置实例】设置虚拟路由器 10 的抢占模式为禁止抢占，键入命令：

```
Harbour(config-if)# vrrp 10 preempt off
```

9.3.8 配置虚拟路由器的认证密码

设置虚拟路由器的认证密码。利用命令：

【命令原型】vrrp {<1-255>}*1 authentication <password>

【参数说明】vrid 取值为 1－255，缺省是 1；

【使用指导】虚拟路由器的认证方法为简单的明文认证。

【命令模式】接口模式

【配置实例】配置虚拟路由器 10 的认证密码是 ABC，键入命令：

```
Harbour(config-if)# vrrp 10 authentication ABC
```

9.3.9 恢复虚拟路由器的缺省认证密码

恢复虚拟路由器的缺省认证密码，利用命令：

【命令原型】no vrrp {<1-255>}*1 authentication

【参数说明】vrid 取值为 1－255，缺省是 1；

【命令模式】接口模式

9.3.10 配置虚拟路由器的名字

配置虚拟路由器的名字，利用命令

【命令原型】vrrp {<1-255>}*1 name <name>

【参数说明】vrid 取值为 1－255，缺省是 1；name 的缺省值是 HOS-VRRP

【命令模式】接口模式

9.3.11 恢复虚拟路由器的缺省名字

恢复虚拟路由器的缺省名字，利用命令

【命令原型】no vrrp {<1-255>}*1 name

【参数说明】vrid 取值为 1－255，缺省是 1；

【命令模式】接口模式

9.3.12 配置备份组接口跟踪

配置备份组接口跟踪后，VRRP 备份组的优先级可以根据交换机上其他接口的状态进行变化。用户可以在接口模式下使用 TRACK 命令指定 VRRP 备份组优先级根据哪些接口的状态进行变化，当指定的接口 DOWN 时，VRRP 备份组优先级减少一个数值，该数值用户可以指定。

【命令原型】vrrp {<1-255>}*1 track <IFNAME> {<1-255>}*1

【参数说明】第一个{<1-255>}表示 VRRP 组号，第二个{<1-255>}表示变化的优先级数值。

<IFNAME>表示跟踪的端口名。

【命令模式】接口模式

9.4 显示虚拟路由器状态信息

用以下命令可以显示虚拟路由器的状态：

【命令原型】show vrrp {<1-255>}*1

【使用指导】VRID 可键入也可不键入。当不输入 VRID 域时，显示当前所有虚拟路由器的状态信息。如键入某个 VRID，则仅显示此虚拟路由器的状态信息。show 命令所显示的虚拟路由器信息包括以下内容：

【命令模式】接口模式或者配置模式

虚拟路由器名字

- 接口名称
- 路由器标示符（VRID）
- 路由器当前状态
- IP地址及掩码
- 优先级
- 广播间隔
- 抢占模式
- 虚拟MAC地址
- 认证方法
- 响应arp模式

示例：显示虚拟路由器 1 的配置信息：

```
Harbour(config-if)# show vrrp 1
------------------------Virtual Router Information------------------

Interface Name             :a
Router Name                :HOS_VRRP
Virtual ID                 :1
State                      :initiation
Priority                   :100
Preempt                    :on
Advertisement interval       :1
Answer arp                 :off
Authentication              :text
Password                   :HOS
Ip address                 :10.5.4.1/24
Virtual Mac address          :00:00:5e:00:01:01

-------------------------Virtual           Router           Information
End--------------------
```

9.5 VRRP 协议配置举例

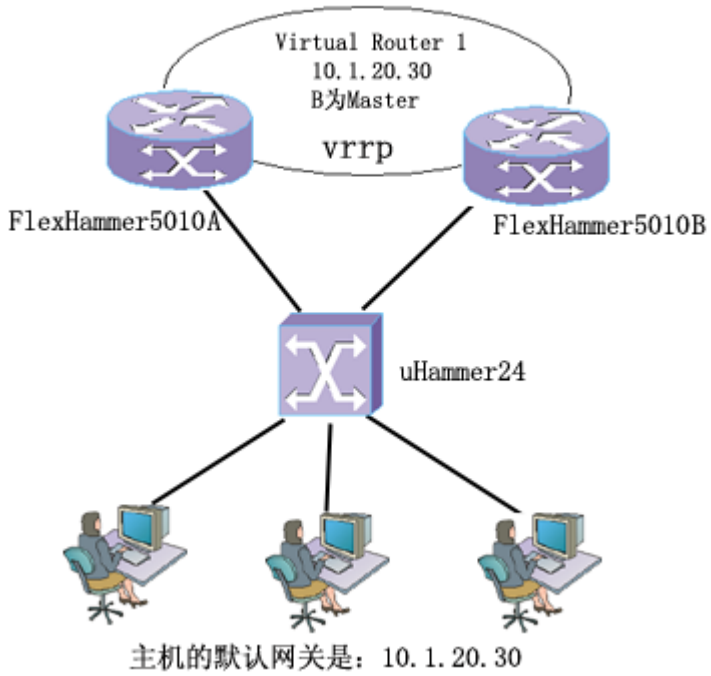
下例是在 FlexHammer5010 交换机 A 中，创建一个虚拟路由器 1，分配一个 IP 地址 10.1.20.30，工作接口是 default，键入命令：

```
Harbour(config)# interface default
Harbour(config-if)# vrrp ipaddress 10.1.20.30
Harbour(config-if)# exit
```

下例是在 FlexHammer5010 交换机 B 中，也创建一个虚拟路由器 1，分配一个 IP 地址 10.1.20.30，工作接口是 default，键入命令：

```
Harbour(config)# interface default
Harbour(config-if)# vrrp ipaddress 10.1.20.30
Harbour(config-if)# exit
```

其关系如下图所示：



说明：在 FlexHammer5010 交换机 A 和交换机 B 中，都存在名为 *default* 的 VLAN，在交换机 A 中，分配给 VLAN *default* 的 IP 地址是 10.1.20.10/24；在交换机 B 中，分配给 VLAN *default* 的 IP 地址是 10.1.20.30/24。主机的默认网关设为 10.1.20.30。

对于在虚拟路由器 1，由于交换机 B 中工作接口地址与虚拟路由器 IP 地址一致，其优先级自动设置为 255，交换机 B 成为主路由器，交换机 A 则成为备份路由器。

正常情况下，即当 VRRP 运行时。在虚拟路由器中，由主路由器负责转发发送到其虚拟 MAC 地址上的数据包，并且定时向备份路由器发送 VRRP 包，这个广播间隔可由用户来设置。

如果这个通告突然停止，备份路由器就会设置一个间隔定时器，如果还没有通告出现，备份路由器就认为主路由器发生了故障，并且开启故障处理过程，接管主路由器。因为主机的默认网关不变，所以这个接管过程对终端主机来说是透明的，这样就为终端主机提供了不间断的服务。

9.6 VRRP 协议的命令列表

FlexHammer5010 中 VRRP 模块的配置命令表：

命令	解释	命令模式

vrrp {<1-255>}*1 ipaddress <A.B.C.D>	配置虚拟路由器的 IP 地址并启动	接口模式
no vrrp {<1-255>}*1 ipaddress	删除虚拟路由器	接口模式
vrrp {<1-255>}*1 priority <1-254>	配置具有 VRID 号的虚拟路由器的优先级，取值范围为 1-254，数值越高表示优先级越高，缺省值为 100。	接口模式
no vrrp {<1-255>}*1 priority	恢复虚拟路由器的缺省优先级	接口模式
vrrp {<1-255>}*1 preempt [on|off]	配置虚拟路由器的抢占模式，缺省为允许抢占。	接口模式
vrrp {<1-255>}*1 authentication [data]	配置具有 VRID 号的虚拟路由器的认证密码	接口模式
no vrrp {<1-255>}*1 authentication	恢复虚拟路由器的缺省认证数据	接口模式
vrrp {<1-255>}*1 advertise-timer <1-5>	配置虚拟路由器的报文发送间隔，缺省为 1 秒	接口模式
no vrrp {<1-255>}*1 advertise-timer	恢复虚拟路由器的报文发送间隔	接口模式
vrrp {<1-255>}*1 name <name>	配置虚拟路由器的名字，缺省为 HOS一VRRP	接口模式
no vrrp {<1-255>}*1 name	恢复虚拟路由器的缺省名字 HOS—VRRP	接口模式
show vrrp {<1-255>}*1	显示虚拟路由器的状态信息	接口模式 配置模式

第10章 IGMP Snooping

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

IGMP Snooping 用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。

10.1 启动 IGMP Snooping

启动 IGMP，在配置模式下，键入命令：

```
service igmp snooping enable
```

10.2 配置 IGMP Snooping 超时时间间隔

1．配置路由器端口的超时时间间隔，利用命令：

```
config igmp snooping router_timeout <10～2147483647>
```

router_timeout ：表示要调整的是路由器端口的时间间隔，默认值为 260 秒。

10~2147483647 ：表示调整路由器端口的超时范围。

2．配置主机端口的超时时间间隔，利用命令：

```
config igmp snooping host_timeout <10～2147483647>
```

host_timeout ：表示要调整的是主机端口的时间间隔，默认值为 260 秒。

10~2147483647 ：表示超时时间范围。

例如，配置接口，router_timeout = 500 秒，host_timeout = 600 秒，键入命令：

```
Harbour(config)#config igmp snooping router_timeout 500
Harbour(config)#config igmp snooping host_timeout 600
```

使用以下命令可以查看主机和路由器端口的超时时间间隔：

```
show igmp snooping summary
```

例如：

```
Harbour(config)#show igmp snooping summary

---------- igmp snooping summary ----------
Router timeout                  260s(D)
Host   timeout                  260s(D)
Total    group                  0
Max     group                  255
-------------------------------------------
D: default.
```

10.3 清除 IGMP Snooping 信息

清除某个 VLAN 或所有 VLAN 中的组成员，在配置模式下，利用命令：

```
clear igmp snooping vlan [name|all]
```

其中，参数<name>为指定 VLAN 的名称，all 代表所有的 VLAN。

例如，清除 default 中的所有组成员关系，在配置模式下，键入命令：

```
Harbour(config)#clear igmp snooping vlan default
```

10.4 关闭 IGMP Snooping 功能

关闭 IGMP，在配置模式下，键入命令：

```
service igmp snooping disable
```

10.5 显示 IGMP Snooping 信息

显示指定 VLAN 中或所有 VLAN 中的组成员信息，在配置模式下，利用命令：

```
show igmp snooping vlan <name>
```

其中，参数<name>为指定 VLAN 的名称，当<name>为 all 时，表示所有的 VLAN。

例如，显示 default 中的所有组成员关系，键入命令：

```
show igmp snooping vlan default
```

10.6 IGMP Snooping 命令表

表 10-1 IGMP Snooping 配置命令表

命令	描述
Service igmp-snooping [enable|disable]	启用/禁止 IGMP Snooping 功能
config igmp snooping router_timeout <10～2147483647>	指定路由器超时的时间间隔（默认值 260 秒）
config igmp snooping host_timeout <10～2147483647>	指定主机超时的时间间隔（默认值 260 秒）
clear igmp snooping vlan [name|all]	清除某个 VLAN 中或所有 VLAN 中的组成员信息列表，当 name 为 all 时表示全部的 VLAN
show igmp snooping timer	显示主机和路由器端口的超时时间间隔
show igmp snooping vlan <name>	显示某个 VLAN 中或所有 VLAN 中的组成员

第11章 QoS

11.1 QoS 概述

11.1.1 概述

QoS（Quality of Service）指 IP 的服务质量，也就是 IP 数据流通过网络时的性能，它的目的是向用户业务提供端到端的服务质量保证。它有一套度量指标，包括业务可用性、延迟、可变延迟、吞吐量和丢包率。QoS 在可预测、可测量性方面比传统 IP 有了很大提高，基本解决了商业用户的需求，因而可以吸引更多的商业用户，形成一个新的利润增长点，带来可增值的业务种类。另外， QoS 还带来了更高效的带宽使用率等。因此可以说 QoS 将是今后一段时间促进 IP 网络增长的关键技术。

不同的应用有不同的 QoS 需求，如语音、图像对抖动和时延敏感，则要求保证带宽和高的优先级；数据和文件传输则对时延不敏感，则可在保证带宽的前提下采用较低的优先级。FlexHammer5010 最多支持 4 个优先级队列。支持严格优先级 SP（Strict Priority）和加权轮循优先级 WRR（Weighted Round Robin）两种调度策略。

- 严格优先级调度机制SP：严格按优先级的高低从队列中提取转发数据，高优先级队列的数据没有清空之前，不转发低优先级队列中的数据。
- 加权轮询调度机制WRR：可以设置以包为单位的Low，Normal，Medium，High的权重比例，按比例轮循4个队列。

目前版本的 QoS 功能只支持 CoS 队列优先级调度和 802.1p 及基于 MAC、PORT、VLAN、ACL 的优先级之间的映射。CoS 队列优先级调度可以分为三个过程：对数据包进行分类；指定不同的优先级队列；得到不同的服务质量（按优先级转发）。

11.1.2 QoS 优先级顺序

配置 QoS 命令优先级的顺序从低到高为：基于 MAC < PORT 重映射< 基于 VLAN < 基于 ACL。

所以如果先配有优先级高的 QoS 策略，再配置低的策略，低的策略将不会发生作用，所以建议在配置 QoS 之前需要全局考虑，避免实际功能与设计中的不一样。

11.1.3 区别服务（DiffServ）

FlexHammer5010 的 QoS 功能提供针对 IPv4 包的区别服务（DiffServ），该服务主要应用 IPv4 报头字段中的 DSCP 域，可以向用户提供以下服务：

- 重写IPv4数据流中的DSCP值
- 根据IPv4数据包中的DSCP值，映射到本地的转发优先级队列中，实现转发优先排序

目前版本支持的 DiffServ 方式有以下三种：

- 基于PORT的DiffServ

- 基于VLAN的DiffServ
- 基于ACL的DiffServ

11.1.4 服务类型（ToS）

FlexHammer5010 的 QoS 可以根据以下规则重写 IPv4 数据流的 ToS 域：

- 基于VLAN重写ToS域
- 基于ACL重写ToS域

FlexHammer5010 支持基于端口（入口和出口）的带宽限制，百兆口粒度为 1M，千兆口粒度为 8 兆。

11.2 QoS 相关配置

11.2.1 使能或者禁止 QoS 服务

使能/禁止 QoS 功能。通过设置 CoS 优先级到相应队列的映射关系来实现。

【命令格式】service qos [enable|disable]

【使用指导】初始化状态下 8 个 802.1p 优先级映射到唯一的 0 号 CoS 队列。如果选择 enable 则启动 4 个 CoS 队列，8 个 802.1p 分别映射到相应的 CoS 队列；如果选择 disable 则禁止 QoS 功能，与 QoS 相关的命令不可用。

【命令模式】配置模式

11.2.2 CoS 优先级调度策略配置

CoS 优先级调度策略的配置，利用如下命令：

【命令格式】config WRR-queue bandwidth <low,normal,medium,high>

【使用指导】4 个 CoS 优先级队列 0、1、2、3 分别表示 low、normal、medium、high。

如果采用严格轮循方式（SP）则执行命令：config WRR-queue bandwidth 0,0,0,0。这样只有在高优先级的队列清空以后，低优先级队列中的包才转发。

如果采用加权轮循方式（WRR）执行命令：config WRR-queue bandwidth 1,2,3,4。Low：Norma：Medium：High 的权重比例关系为 1：2：3：4，即每一次轮循从 High 队列中取 4 个包；从 Medium 队列中取 3 个包；从 Norma 队列中取 2 个包；从 Low 队列中取 1 个包。这四个参数的取值范围都是 1-255。

【命令模式】配置模式

查看 CoS 优先级配置，利用以下命令：

【命令格式】show wrr-queue

【使用指导】显示 4 个优先级队列与权重的对应关系

【配置模式】只读或者配置模式

【配置实例】配置加权轮循权重为 1,2,3,4，则有如下显示：

```
Harbour(config)#config WRR-queue bandwidth 1,2,3,4
Harbour(config)#show wrr-queue

-------- QoSQueue -------- WRR value --------
--------  Low    --------   1   -----------
--------  Normal --------   2   -----------
--------  Medium --------   3   -----------
--------  High   --------   4   -----------
```

11.2.3 802.1p 优先级到 CoS 队列的映射关系配置

配置 802.1p 的优先级到 CoS 的映射关系，利用命令：

【命令格式】config priority <0-7> qosqueue [Low|Normal|Medium|High]

【使用指导】通过设置 CoS_SEL 寄存器的相应位来指定 802.1p 优先级到 CoS 队列的映射关系。

【命令模式】配置模式

11.2.4 查看 802.1p 优先级到 CoS 队列的映射关系配置

可以用如下命令查看 802.1p 优先级到 CoS 队列的映射关系配置。

【命令格式】show dot1p-QosQueue-mapping

【配置实例】

没有配置 802.1p 优先级到 CoS 队列的映射关系时，我们查看一下它们的映射关系。

```
Harbour(config)#show dot1p-qosqueue-mapping

--------Dot1p Priority--------------QoS Queue ---------
---------     0     --------  Low     --------
---------     1     --------  Low     --------
---------     2     --------  Normal  --------
---------     3     --------  Normal  --------
---------     4     --------  Medium  --------
---------     5     --------  Medium  --------
---------     6     --------  High    --------
---------     7     --------  High    --------
```

下面我们把 802.1p 优先级 7 映射到表示为 Low 的 0 号 CoS 队列。我们再查看一下他们的映射关系。

```
Harbour(config)#config priority 7 qosqueue low
Harbour(config)#show dot
Harbour(config)#show dot1p-qosqueue-mapping

--------Dot1p Priority-----------QoS Queue ---------
---------     0     --------    Low      --------
---------     1     --------    Low      --------
---------     2     --------    Normal    --------
---------     3     --------    Normal    --------
---------     4     --------    Medium    --------
---------     5     --------    Medium    --------
---------     6     --------    High     --------
---------     7     --------    Low      --------
```

11.2.5 基于 MAC 的优先级配置

【命令格式】create fdbentry <mac_address> vlan <name> port <portlist> {priority <0-7>}*1

【使用指导】为创建静态 FDB 表项的命令添加优先级参数，则以此 MAC 地址为源 MAC 的数据包会根据配置的 802.1p 优先级来选择 CoS 队列。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#create fdb 001122334455 vlan default port 5 priority
  7
Harbour(config)#show qos mac

****************************MAC
  Qos*******************************
MAC address         Port  VLAN name                Priority
00:11:22:33:44:55     5    default                    7
```

11.2.6 基于 PORT 的优先级配置

使能或者禁止端口到 802.1p 优先级的重新映射功能，利用如下命令：

【命令格式】config port [<portlist>|all] remap-priority [on|off]

【使用指导】使能/禁止端口对 802.1p 优先级的重新映射功能

【命令模式】配置模式

11.2.7 配置端口到 802.1p 优先级的重新映射

【命令格式】config port [<portlist>|all] remap-priority <0-7>

【使用指导】通过设置相应端口重新映射 priority 的值改变端口对 802.1p 优先级的重新映射。则从此端口接收的数据包根据配置的 802.1p 优先级来选择 CoS 队列。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#config port 1 remap-priority on
Harbour(config)#config port 1 remap-priority 6
```

```
Harbour(config)#show qos port

**************************Port
  Qos*****************************
Port: 1's 802.1p priority is 6.
```

11.2.8 基于 VLAN 的优先级配置

【命令格式】config vlan <name> priority <0-7>

【使用指导】通过改变 VLAN 的优先级属性来实现属于某一个 VLAN 的数据流的优先级的重新映射。属于该 VLAN 的数据流的 802.1p 优先级被配置的优先级取代，转发到相应的 CoS 队列。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#config vlan test priority 7
Harbour(config)#show qos vlan

**************************VLAN
  Qos*****************************
VLAN: test's 802.1p priority is 7.
```

11.2.9 基于 ACL 的优先级配置

【命令格式】config acl <name> priority <0-7>

【使用指导】通过修改 ACL 策略的优先级属性来实现基于 ACL 的数据流优先级的重新映射。则匹配上该 ACL 策略的数据流的 802.1p 优先级被配置的优先级取代，转发到相应的 CoS 队列。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#config acl test priority 6
Harbour(config)#show qos acl

**************************Acl
  Qos*****************************
ACL : test's 802.1p priority is 6.
```

11.3 DiffServ 相关配置

IP 包头中的 ToS（Type Of Service）域代表了相应的服务类型。DiffServ 将 8 位 ToS 字段重新命名，作为 DS (DifferServer)字段，利用前 6 位做为 DSCP（ DifferServer CodePoint）域，这个域的值我们称为 codepoint，交换机可以使用这个域进行包服务类型的区分。在交换机中可以实现根据服务的级别对于包重写 DSCP 域，或者根据 DSCP 域来进行 QoS 的区分，实现区别服务。DiffServ 的配置用于处理 IPv4 首部的 DSCP 域，内容包括：

1．重写 IPv4 报文首部中的 DSCP 域

- 基于进入特定端口IPv4报文DSCP域的重写

- 基于特定VLAN的IPv4报文DSCP域的重写
- 基于特定ACL的IPv4报文DSCP域的重写

2．映射不同的 DSCP 值到 802.1p 定义的优先级，使得带有不同的 DSCP 值的 IPv4 报文得到不同的发送优先级别。是否进行优先级映射可由用户选择配置。

DiffServ 功能模块的命令集有一定的配置顺序，建议按以下顺序配置：

1）service qos enable

2）config dscp to-802.1p map codepoint [0-7|8-15|16-23|24-31|32-39|40-47|48-55|56-63] priority <0-7>

3）config dscp enable

4）config dscp to-802.1p [on|off] ，默认打开

11.3.1 使能或者禁止 Differv 服务

【命令格式】config dscp [enable|disable]

【使用指导】启动或关闭 DiffServ 服务，默认启动时同时打开 differv 优先级映射功能。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#config dscp enable
```

11.3.2 使能或者禁止 Differv 优先级映射功能

【命令格式】config dscp to-802.1p [on|off]

【使用指导】打开或关闭 DiffServ 优先级映射功能。

on 表示交换机将根据 IPV4 数据流的 DSCP 值，将其映射到不同的本地优先级转发队列中去，从而得到不同级别的发送优先服务。

off 表示交换机不进行优先级映射，具有不同 DSCP 值的 IPV4 数据流在本地的转发优先级没有高低之分。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#config dscp to-802.1p on
Harbour(config)#config dscp to-802.1p off
```

11.3.3 配置 Differv 到 802.1p 的映射关系

【命令格式】config dscp to-802.1p map codepoint [0-7|8-15|16-23|24-31|32-39|40-47|48-55|56-63] priority <0-7>

【使用指导】配置 differv 每一段 dscp codepoint 值到 802.1p 优先级的映射关系。默认配置为：

```
dscp codepoint     802.1pri
0-7                0
8-15               1
16-23              2
23-31              3
32-39              4
40-47              5
48-55              6
56-63              7
```

【命令模式】配置模式

【配置实例】

```
Harbour(config)#dscp to-802.1p map codepoint 16—23 priority 2
```

11.3.4 基于 VLAN 的 DSCP 配置

【命令格式】config vlan <vlanname> dscp <0-63>

【使用指导】配置基于 vlan 的 dscp

【命令模式】配置模式

【配置实例】Harbour(config)#config vlan default dscp 6

【命令格式】no vlan <name> dscp

【使用指导】去除 vlan 的 dscp 属性

【命令模式】配置模式

【配置实例】Harbour(config)#no vlan default dscp

11.3.5 基于 ACL 的 DSCP 配置

【命令格式】config acl <name> dscp <0-63>

【使用指导】配置基于 acl 的 dscp

【命令模式】配置模式

【配置实例】Harbour(config)#config acl acl_1 dscp 24

【命令格式】no acl <name> dscp

【使用指导】去除 acl 的 dscp 属性

【命令模式】配置模式

【配置实例】Harbour(config)#no acl acl_1 dscp

11.3.6 基于 PORT 的 DSCP 配置

【命令格式】config port [<portlist>|all] dscp <0-63>

【使用指导】portlist 端口列表，例如 8-12 表示 8，9，10，11，12 端口。dscp 后面的参数就是给端口配置的 codepoint 的值

【命令模式】配置模式

【配置实例】Harbour(config)#config port 1，3一12，5 dscp 63

【命令格式】no port [<portlist>|all] dscp

【使用指导】去除 port 的 dscp 属性

【命令模式】配置模式

【配置实例】Harbour(config)#no port 4 dscp

11.3.7 查看 DiffServ 的配置信息

【命令格式】show dscp [vlan|acl|port|all]

【使用指导】显示 DiffServ 的配置信息

【命令模式】配置模式

【配置实例】

```
Harbour(config)#show dscp all

-------------VLAN DSCP-------------
VLANName                         DSCP
--------                        ----
v1                               10
-------------------------------------

-------------ACL  DSCP-------------
AclName                          DSCP
-------                         ----
test                             10
-------------------------------------
```

11.3.8 查看 DiffServ 到 8021.p 的映射信息

【命令格式】show dscp map

【使用指导】显示 DiffServ 到 802.1p 的映射信息

【命令模式】配置模式

【配置实例】

```
Harbour(config)#show dscp map

dscp codepoint    802.1pri
0-7              0
8-15             1
16-23            2
```

```
23-31           3
32-39           4
40-47           5
48-55           6
56-63           7
```

11.4 ToS 相关配置

IP 包头中的 ToS（Type Of Service）域代表了相应的服务类型。在交换机中可以使用这个域进行包服务类型的区分，可以根据以下规则来重写该域的值：

- 基于特定VLAN的IPv4报文ToS域的重写
- 基于特定ACL的IPv4报文ToS域的重写

11.4.1 使能或者禁止 ToS 服务

【命令格式】config tos [enable|disable]

【使用指导】启动或关闭 tos 服务。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#config tos enable
```

11.4.2 基于 VLAN 的 ToS 配置

【命令格式】config vlan <name> tos_p <1-7>

【使用指导】配置基于 vlan 的 ToS，重写在该 vlan 中转发的 IP 数据的 ToS 域

【命令模式】配置模式

【配置实例】Harbour(config)#config vlan test tos_p 6

【命令格式】no vlan <name> tos_p

【使用指导】去除 vlan 的 tos 属性

【命令模式】配置模式

【配置实例】Harbour(config)#no vlan test tos_p

11.4.3 基于 ACL 的 ToS 配置

【命令格式】config acl <name> tos_p <0-7>

【使用指导】配置基于 ACL 的 tos，重写匹配该 ACL 项的 IP 数据的 tos 域

【命令模式】配置模式

【配置实例】Harbour(config)#config acl acl_1 tos_p 5

【命令格式】no acl <name> top_p

【使用指导】去除 ACL 的 tos 属性

【命令模式】配置模式

【配置实例】Harbour(config)#no acl acl_1 tos_p

11.4.4 查看 ToS 配置信息

【命令格式】show tos_p [vlan|acl|all]

【使用指导】显示 ToS 的配置信息

【命令模式】配置模式

【配置实例】

```
Harbour(config)#show tos all

-------------VLAN ToS-------------
VLANName                     ToS_P
--------                      -----
v1                              3
-----------------------------------
-------------ACL  ToS-------------
AclName                       ToS_P
-------                       -----
test                            2
-----------------------------------
```

11.5 带宽限制（bandwidth）

11.5.1 配置入口端口的带宽限制

【命令格式】config port [<portlist>|all] bandwidth input <0-127>

【使用指导】配置端口的入口带宽限制。参数<0-127> 指允许的带宽，单位 M（百兆口），8M（千兆口）。

【命令模式】配置模式

【配置实例】Harbour(config)#config port 3 bandwidth input 20

11.5.2 配置出口端口的带宽限制

【命令格式】config port [<portlist>|all] bandwidth output <0-127>

【使用指导】配置端口的出口带宽限制。参数<0-127> 指允许的带宽，单位 M（百兆口），8M（千兆口）。

【命令模式】配置模式

【配置实例】Harbour(config)#config port 3 bandwidth output 20

11.5.3 查看端口的带宽限制信息

【命令格式】show bandwidth port [<portlist>|all]

【使用指导】查看端口的带宽限制信息。参数[all]表示查看所有端口的带宽限制信息；
参数[portlist]表示查看特定端口的带宽限制信息

【命令模式】配置模式

【配置实例】Harbour(config)#show bandwidth port 3

11.6 QoS 命令列表

命令	描述
service qos [enable|disable]	使能/禁止 QoS 功能
config WRR-queue bandwidth <low,normal,medium,high>	配置队列加权轮循的权重
show WRR-queue	显示 4 个优先级队列与权重的对应关系
config priority <0-7> qosqueue [Low|Normal|Medium|High]	配置 802.1p 优先级到 COS 队列的映射关系
show dot1p-QosQueue-mapping	显示 802.1p 优先级到 COS 队列的映射关系
create fdbentry <mac_address> vlan <name> port <portlist> {priority <0-7>}	配置 FDB 对 802.1p 优先级的重新映射
config port [<portlist>|all] remap-priority <0-7>	配置相应端口对 802.1p 优先级的重新映射
config vlan <name> priority <0-7>	配置 VLAN 的数据流的优先级的重新映射
no vlan <name> priority	取消已经配置的 vlan 优先级配置信息
config acl <aclname> priority <0-7>	配置 ACL 策略的数据流的优先级的重新映射
no acl <name> priority	取消已经配置的 ACL 优先级配置信息
show qos [port|mac|vlan|acl|all]	显示不同类型的 QoS 优先级配置信息
config tos [enable|disable]	打开或关闭 tos 功能
config vlan <name> tos_p <1-7>	配置基于 vlan 的 Tos
no vlan <name> tos_p	去除基于 vlan 的 Tos 属性
config acl <aclname> tos_p <0-7>	配置基于 acl 的 Tos
no acl <name> top_p	去除基于 acl 的 Tos 属性
show tos_p [vlan|acl|all]	显示 tos 信息

第12章 日志管理

本章主要包括以下内容：

- 日志管理概述
- 日志功能基本配置
- 日志信息存储方式配置
- 日志信息显示方式配置
- 查看日志管理的配置情况
- 日志管理命令列表

12.1 日志管理概述

日志管理主要用来记录整个系统的运行情况以及用户操作行为。完整的日志管理能够帮助管理员及时了解和监控系统的工作情况，并实时记录系统的异常信息。日志信息来源于系统中所有的运行模块，日志系统完成信息的收集、管理、存储和显示。日志信息可以显示到终端 monitor，这种方式主要用于调试和查看系统状态。也可以存储到日志服务器 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。

12.2 日志功能基本配置

12.2.1 打开或关闭日志服务

【命令作用】打开或关闭日志服务功能

【命令格式】`config syslog [enable|disable]`

【参数说明】选择 `enable` 表示打开日志服务功能；选择 `disable` 表示关闭日志服务功能

【命令模式】配置模式

【配置实例】打开日志服务功能

```
Harbour(config)#config syslog enable

Successfully changed syslog service to enable
```

12.2.2 配置所要记录的日志信息的类型

【命令作用】配置日志管理是否对某一类型的日志信息进行记录

【命令格式】`config syslog type [<name>|all] [enable|disable]`

【参数说明】选择 `enable` 表示对指定类型的信息进行记录；选择 `disable` 表示不记录。

【命令模式】配置模式

【使用指导】`name` 为系统中支持的日志类型，可用 `show syslog configuration` 来查看日志类型，目前支持的类型有：`AUTH`，`BGP`，`CLI`，`SYSLOG`，`DEVCTRL`，`ARP`，`DOT1X`，`NAS`，`OSPF`，

PORT，FDB，RADIUS，RIP，ROUTE，SNMP，STP，SYSTEM，VLAN，WEB，SERVICE，DHCPR 等。all 代表以上支持的所有日志类型。

【配置实例】注册 AUTH 类型的日志信息，日志管理将对 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.
```

12.2.3 配置所要记录日志信息的最低级别

【命令作用】配置日志管理对某一级别和该级别以上的日志信息进行记录

【命令格式】config syslog lowest-level <0-7>

【命令模式】配置模式

【使用指导】目前支持的日志信息级别从 0 到 7，依次为 EMERG ，ALERT ，CRITERR，CRIT， ERR，WARNING，NOTICE，INFO，DEBUG。

【配置实例】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].
```

12.2.4 打开命令行操作日志记录功能

【命令作用】配置日志管理是否对命令行操作行为进行日志记录

【命令格式】record command-line [enable|disable]

【参数说明】enable 表示对命令行操作进行记录；disable 表示对命令行操作不进行记录。

【命令模式】配置模式

【使用指导】命令行操作的日志信息级别为 6，即 INFO 类型。

【配置实例】允许对命令行操作行为记录日志信息：

```
Harbour(config)#record command-line enable

Successfully changed syslog record CLI to enable.
```

12.2.5 打开或关闭有效用户通过 telnet 登录成功的日志记录功能

【命令作用】配置日志模块是否对有效用户通过 telnet 登录成功进行日志记录

【命令格式】record valid-access [enable|disable]

【参数说明】选择 enable 表示进行日志记录；选择 disable 表示不进行日志记录。

【命令模式】配置模式

【使用指导】命令行操作的日志信息级别为 5，即 NOTICE 类型。

【配置实例】允许对有效用户通过 telnet 登录成功进行日志记录：

```
Harbour(config)#record valid-access enable
```

12.3 日志信息存储方式配置

12.3.1 打开或关闭日志信息保存到日志服务器的功能

【命令作用】配置日志管理是否保存日志信息到日志服务器

【命令格式】config syslog server [enable|disable]

【参数说明】enable 表示保存日志信息到服务器；disable 表示不保存日志信息到服务器。

【命令模式】配置模式

【使用指导】在配置之前，保证日志服务器服务程序已启动。

【配置实例】允许日志保存到日志服务器：

```
Harbour(config)#config syslog server enable

Successfully changed syslog service logto server enable.
Warning: Syslog server config is empty.Please add syslog server.
```

12.3.2 增加或删除一个日志服务器

【命令作用】增加或删除一个日志服务器，包括日志服务器的 IP 地址，服务端口，日志信息的级别等信息

【命令格式】config syslog [add|delete] server <A.B.C.D>{[port] <1-65535>}*1 {[facility] <0-7>}*1

【参数说明】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 是日志服务器上接收日志进程的服务端口号，facility 对应于日志信息的级别,就是说这个日志服务器将保存某个级别和某个级别以上的日志信息。

【命令模式】配置模式

【使用指导】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。

【配置实例】配置了一个 IP 地址为 10.12.3.4 的日志服务器，服务端口为 8808，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
```

删除了一个日志服务器，其 IP 地址为 10.1.4.1，服务端口为 6500，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
```

12.4 配置日志信息的显示方式

12.4.1 打开或关闭终端显示日志信息的功能

【命令作用】配置日志信息是否输出到用户终端

【命令格式】config syslog monitor-terminal [enable|disable]

【参数说明】选择 enable 表示允许日志信息输出到客户端，选择 disable 表示不允许日志信息输出到客户端

【命令模式】配置模式

【使用指导】该命令是服务命令，将对所有终端起作用。

【配置实例】允许日志信息输出到所有用户终端：

```
Harbour(config)#config syslog monitor-terminal enable

Successfully changed syslog service logto monitor-terminal to
  enable.
```

12.4.2 打开或关闭在本终端显示日志信息的功能

【命令作用】决定是否在本终端输出日志信息

【命令格式】monitor [on|off]

【参数说明】选择 on 表示允许在本终端输出日志信息，选择 disable 表示不允许在本终端输出日志信息。

【命令模式】配置模式

【使用指导】该命令只对本终端起作用。

【配置实例】允许日志信息输出到自己的终端：

```
Harbour(config)#monitor on

Successfully changed your terminal display syslog messages.
```

12.4.3 配置是否显示时间信息

【命令作用】决定是否在本终端输出时间信息

【命令格式】monitor timestamp [none|time|datetime]

【命令模式】配置模式

【使用指导】该命令主要用来决定是否在本终端输出时间信息。

【配置实例】将在本终端输出时间信息：

```
Harbour(config)#monitor timestamp datetime
```

12.4.4 配置在终端可以显示的日志信息的最低级别

【命令作用】决定在本终端输出某一级别和某一级别以上的日志信息

【命令格式】monitor lowest-level <0-7>

【命令模式】配置模式

【使用指导】该命令只对本终端起作用，目前支持的日志信息级别从 0 到 7，依次为 EMERG，ALERT，CRITERR，CRIT，ERR，WARNING，NOTICE，INFO，DEBUG。

【配置实例】将在本终端输出级别 3 和级别 3 以上类型的日志信息：

```
Harbour(config)#monitor lowest-level 3

Successfully changed monitor lowest-lever level 3 [ERR]。
```

12.4.5 配置在终端可以显示的日志信息类型

【命令作用】决定在本终端输出某一类型的日志信息

【命令格式】monitor type [<typename>|all] [on|off]

【命令模式】配置模式

【使用指导】该命令只对本终端起作用，typename 为系统中支持的日志类型，可用 show syslog configuration 来查看日志类型，目前支持的类型有：AUTH，BGP，CLI，SYSLOG，DEVCTRL，ARP，DOT1X，NAS，OSPF，PORT，FDB，RADIUS，RIP，ROUTE，SNMP，STP，SYSTEM，VLAN，WEB，SERVICE，DHCPR 等。all 代表以上支持的所有日志类型。

【配置实例】将在本终端输出所有类型的日志信息：

```
Harbour(config)#monitor type all on

Successfully changed to display all messages.
```

12.5 查看日志管理的配置情况

12.5.1 查看整个日志管理的配置信息

【命令作用】显示日志管理的所有配置信息，包括各种服务的打开和关闭情况等。

【命令格式】show syslog configuration

【命令模式】配置模式

【使用指导】可以列出日志管理的所有配置信息，对使用日志管理命令具有一定指导作用。

【配置实例】

```
Harbour(config)#show syslog configuration

-----------------------------------------------------

Syslog Service is up.

--Service Syslog logto flashfile is up.

--Service Syslog logto server is down.

Have no syslog server.
```

--Service Syslog logto monitor-terminal is up.

--Log messages that not lower than level 4 [WARNING].

--Log these types messages:

--Not log these types messages:

:AUTH:BGP:CLI:SYSLOG:DEVCTRL:ARP:DOT1X:NAS:OSPF:PORT:FDB

:RADIUS:RIP:ROUTE:SNMP:STP:SYSTEM:VLAN:WEB:SERVICE:DHCPR

Record command-line is disabled

12.5.2 查看对本终端的日志显示属性的配置情况

【命令作用】包括所配置的可以在本终端显示的日志类型，日志级别以及时间信息等

【命令格式】`show monitor configuration`

【命令模式】配置模式

【使用指导】该命令只对本终端起作用。

【配置实例】

```
Harbour(config)#show monitor configuration
```

Monitor has been on.

Monitor show messages with none timestamp.

Monitor only display log messages that not lower than level 7 [DEBUG].

Monitor display messages of these types:

Monitor donot display messages of these types:

AUTH:BGP:CLI:SYSLOG:DEVCTRL:ARP:DOT1X:NAS:OSPF:PORT:FDB:RADIUS

:RIP:ROUTE:SNMP:STP:SYSTEM:VLAN:WEB:SERVICE:DHCPR:

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

12.6 日志模块命令列表

表 12-1 日志模块命令列表

命令	描述
config syslog [enable|disable]	起用或关闭日志服务功能。enable 表示起用，disable 表示关闭。
config syslog monitor-terminal [enable|disable]	允许或禁止把日志信息输出到终端。enable 表示允许，disable 表示禁止。
config syslog lowest-level <0-7>	配置所要记录的日志信息的最低级别。表示系统将对等于或大于 lowest-level 的日志类型做日志信息。0：系统不可用，1：实时操作，2：严重，3:错误， 4:告警，5：提示，6：一般信息， 7：调试
config syslog type [<name>|all] [enable|disable]	起用或关闭某一个日志类型或所有日志类型的日志功能。name 为该日志类型名字，all 表示代表所有日志类型。enable 表示起用，disable 表示关闭。
record command-line [enable|disable]	是否对命令行操作做日志记录。enable 表示允许，disable 表示禁止。
config syslog server [enable|disable]	允许或禁止把日志信息输出到日志服务器。enable 表示允许，disable 表示禁止。
config syslog [add|delete] server <A.B.C.D> {[port] <1-65535>}*1 {[facility] <0-7>}*1	配置或删除一个日志服务器。<A.B.C.D>为 IP 地址，port 为端口，facility 为日志信息的级别。
show syslog configuration	显示日志模块所有配置信息。
monitor [on|off]	开始显示或结束日志信息输出到本终端。
monitor timestamp [none|time|datetime]	允许在本终端输出时间信息。
monitor lowest-level <0-7>	设置本终端所要输出的日志信息的级别。该命令执行后，在本终端只显示等于或大于该级别的日志信息。
monitor type [<typename>|all] [on|off]	设置哪些日志类型的的日志信息可以输出到本终端。
show monitor configuration	显示对日志信息输出到本终端的配置信息。
record valid-access [enable|disable]	打开或关闭有效用户通过 telnet 登录成功的日志记录功能。

第13章 网络管理服务 NMS

本章主要包括以下内容：

- NMS 概述
- NMS 功能基本配置
- 在配置表里添加/删除 IP 地址
- 查看 NMS 的配置
- NMS 命令列表

13.1 NMS 概述

NMS(Net Management service)网络管理服务是用来实现访问控制、提高系统的安全性。通常情况下，只要用户拥有登录名和密码就可以登录到交换机，但有时我们出于安全性的考虑，希望用户的 IP 地址是某个特定的或是一个范围，这时就可以打开控制访问服务，将 IP 地址加入到访问配置表。当用户登录时，交换机首先验证该用户 IP 地址的合法性，如果 IP 合法，才会验证用户名和密码的合法性。系统最多允许创建 10 个访问控制配置表。

13.2 NMS 访问控制基本配置

13.2.1 打开或关闭访问控制服务

【命令作用】打开或关闭访问控制

【命令格式】config access-control {[telnet|snmp]}*1 [on|off]

【参数说明】选择 on 表示打开访问控制服务；选择 off 表示关闭访问控制服务

【命令模式】配置模式

【配置实例 1】打开访问控制功能，包括 telnet 和 snmp

```
Harbour(config)#config access-control on
Successfully changed access-control on.
```

【配置实例 2】打开 telnet 访问控制功能

```
Harbour(config)#config access-control telnet on
Successfully changed telnet access-control on
```

13.2.2 创建一个 NMS 访问控制配置

【命令作用】创建一个 NMS 访问控制配置

【命令格式】create nms-access-profile <access_profile_name>

【参数说明】<access_profile_name> 用户创建的访问控制配置的名称，不能超过 20 个字符。

【命令模式】配置模式

【配置实例】创建了一个名称为 admin 的访问控制

```
Harbour(config)#create nms-access-profile admin
Profile admin added success.
```

13.2.3 删除特定的 NMS 访问控制配置

【命令作用】删除特定的 NMS 访问控制配置

【命令格式】delete nms-access-profile <access_profile_name>

【参数说明】<access_profile_name>访问控制配置名称，不能超过 20 个字符。

【命令模式】配置模式

【配置实例】删除名称为 admin 的访问控制配置

```
Harbour(config)#delete nms-access-profile admin
Profile admin delete success.
```

13.2.4 允许或禁止 Telnet 访问控制

【命令作用】允许或禁止 Telnet 访问控制

【命令格式】config nms-access-profile <access_profile_name> telnet [enable|disable]

【参数说明】<access_profile_name>访问控制配置名称，不能超过 20 个字符。

选择 enable 表示打开 telnet 访问控制；选择 disable 表示关闭访问控制。

【命令模式】配置模式

【配置实例】允许 admin 进行 telnet 访问控制

```
Harbour(config)#config nms-access-profile admin telnet enable
Config profile admin's telnet-access enable success.
```

13.2.5 允许或禁止 SNMP 访问控制

【命令作用】允许或禁止 SNMP 访问控制

【命令格式】config nms-access-profile <access_profile_name> snmp [enable|disable]

【参数说明】<access_profile_name>访问控制配置名称，不能超过 20 个字符。

选择 enable 表示打开 telnet 访问控制；选择 disable 表示关闭访问控制。

【命令模式】配置模式

【配置实例】允许 admin 进行 SNMP 访问控制

```
Harbour(config)#config nms-access-profile admin snmp enable
Config profile admin's snmp-access enable success.
```

13.3 在配置表里添加/删除 IP 地址

13.3.1 在指定的配置表里添加 IP 地址

【命令作用】在指定的配置表里添加 IP 地址

【命令格式】config nms-access-profile <access_profile_name> add ipaddress <A.B.C.D/M>
或 config nms-access-profile <access_profile_name> add ipaddress <A.B.C.D>
<A.B.C.D>

【参数说明】<A.B.C.D/M> 和<A.B.C.D> <A.B.C.D>分别是两种 IP 地址和子网掩码的表示方式

【命令模式】配置模式

【配置实例】在 admin 配置表里成功地添加 IP 地址 10.5.3.1,子网为 255.255.255.0

```
Harbour(config)#config nms-access-profile admin add ipaddress 10.5.3.1/24
```

或

```
Harbour(config)#config nms-access-profile admin add ipaddress 10.5.3.1
                255.255.255.0
```

13.3.2 在指定的配置表里删除 IP 地址

【命令作用】在指定的配置表里删除 IP 地址

【命令格式】config nms-access-profile <access_profile_name> delete ipaddress
[all |<A.B.C.D/M>]
或 config nms-access-profile <access_profile_name> delete ipaddress
<A.B.C.D> <A.B.C.D>

【参数说明】选择 all 表示删除该配置表的所有 IP；<A.B.C.D/M> 和<A.B.C.D> <A.B.C.D>分别是两种 IP 地址和子网掩码的表示方式

【命令模式】配置模式

【配置实例】在 admin 配置表里成功地删除 IP 地址 10.5.3.1,其子网为 255.255.255.0

```
Harbour(config)#config nms-access-profile admin delete ipaddress
               10.5.3.1/24
```

或

```
Harbour(config)#config nms-access-profile admin delete ipaddress
                10.5.3.1 255.255.255.0
```

13.4 查看访问控制的配置

13.4.1 查看访问控制功能是否打开

【命令作用】查看访问控制功能是否打开

【命令格式】show access-control {[telnet|snmp]}*1

【命令模式】配置模式

【配置实例 1】查看所有的访问控制

```
Harbour(config)#show access-control

Telnet access-control is : on
SNMP  access-control is : on
```

【配置实例 2】只查看 telnet 的访问控制是否打开

```
Harbour(config)#show access-control telnet

Telnet access-control is:on
```

13.4.2 查看特定配置表的配置情况

【命令作用】查看特定配置表的配置情况

【命令格式】show nms-access-profile {<access_profile_name>}*1

【参数说明】<access_profile_name>表示查看指定的访问控制配置表，不加参数表示查看所有配置。

【命令模式】配置模式

【配置实例】查看 admin 的配置情况

```
Harbour(config)#show nms-access-profile admin

============================================================
Access profile name  : admin
Telnet access status : disable
SNMP   access status : disable
------------------------------------------------------------
Address List:
------------------------------------------------------------
No   ID   Network-IP          NetMask
------------------------------------------------------------
1    0    10.5.5.1           255.255.255.0
2    1    10.5.3.0           255.255.255.0
------------------------------------------------------------
Total 2 Addresses.
============================================================
```

13.5 访问控制命令列表

表 13-1 访问控制命令列表

命令	描述
config access-control { [telnet|snmp] }*1 [on|off]	打开或关闭访问控制。选择 on 表示打开；选择 off 表示关闭。
create nms-access-profile <access_profile_name>	创建一个访问控制配置。
delete nms-access-profile <access_profile_name>	删除特定的访问控制配置。
config nms-access-profile <access_profile_name> telnet [enable|disable]	允许或禁止 telnet 访问控制。
config nms-access-profile <access_profile_name> snmp [enable|disable]	允许或禁止 SNMP 访问控制。
config nms-access-profile <access_profile_name> add ipaddress <A.B.C.D/M>	在指定的配置表里添加 IP 地址。
config nms-access-profile <access_profile_name> add ipaddress <A.B.C.D> <A.B.C.D>	在指定的配置表里添加 IP 地址。
config nms-access-profile <access_profile_name> delete ipaddress [all |<A.B.C.D/M>]	在指定的配置表里删除 IP 地址。
config nms-access-profile <access_profile_name> delete ipaddress <A.B.C.D> <A.B.C.D>	在指定的配置表里删除 IP 地址。
show access-control {[telnet|snmp]}*1	查看访问控制功能是否打开。
show nms-access-profile {<access_profile_name>}*1	查看特定配置表的配置情况。

第14章 ACL 配置

14.1 ACL 概述

访问控制列表 ACL（Access Control List）是十分重要的条件列表，可以实现基于 MAC 地址、IP 地址、TCP/UDP 端口等包头字段的接入控制。它在网段之间实现强大的控制访问功能，过滤不需要的数据包和实现安全策略。

FlexHammer5010 的 ACL 配置规则如下：

- ACL的缺省方式是permit any，也就是说当使能ACL功能但是没有配置任何ACL规则的时候，所有的数据包都可以不受ACL的约束正常转发。
- 在没有配置优先级的条件下，执行ACL规则时采用自下向上匹配方式，即后配置的ACL规则先匹配。
- 具有优先级的概念，优先级高的ACL规则先匹配。

14.2 ACL 相关配置

14.2.1 启动/关闭 ACL 服务

【命令格式】service acl [enable|disable]

【使用指导】使能或者关闭 ACL 功能，如果选择 enable 表示使能 ACL 功能，如果选择 disable 表示关闭 ACL 功能

【命令模式】配置模式

14.2.2 添加基于 IP 的 ACL 配置

【命令格式】create acl <name> ip DIP [<A.B.C.D/M>|any] SIP [<A.B.C.D/M>|any] [permit|deny] ports [<portlist>|any]{precedence <0-255>}*1

【使用指导】生成并添加一条针对 IP 数据包的 ACL 策略。可匹配的内容为目的 IP 和源 IP 或任意值，并指定相应的物理端口号；precedence 为可选参数，指定策略的优先级(0-255)，默认为最低 0。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#create acl test_ip ip DIP 10.1.30.1/16 SIP
  10.1.40.8/16 deny ports any precedence 30
Harbour(config)#show acl all

ACL test_ip ip DIP 10.1.30.1/16 SIP 10.1.40.8/16 deny ports any
  precedence 30
```

14.2.3 添加基于 UDP 的 ACL 配置

【命令格式】create acl <name> udp DIP[<A.B.C.D/M>|any]ip-port [<dst_port>|any] SIP[<A.B.C.D/M>|any] ip-port [<src_port>|any][permit|deny] ports [<portlist>|any] {precedence <0-255>}*1

【使用指导】生成并添加一条针对 UDP 的 ACL 策略。可匹配的内容为目的 IP、源 IP、目的端口号和源端口号或它们任意值，并指定相应的物理端口号，precedence 为可选参数，指定策略的优先级（0-255），默认为最低 0。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#create acl test_udp udp DIP any ip-port 800 SIP any
  ip-port 400 deny ports any precedence 10
Harbour(config)#sh acl all

ACL test_udp udp DIP any ip-port 800 SIP any ip-port 400 deny ports
  any
precedence 10
```

14.2.4 添加基于 TCP 的 ACL 策略

【命令格式】create acl <name> tcp DIP [<A.B.C.D/M>|any] ip-port[<dst_port>|any] SIP [<A.B.C.D/M>|any]ip-port[<src_port>|any][permit|deny]ports [<portlist> |any]{precedence <0-255>}*1

【使用指导】生成并添加一条针对 TCP 的 ACL 策略。可匹配的内容为目的 IP、源 IP、目的端口号和源端口号或它们任意值，并指定相应的物理端口号， precedence 为可选参数，指定策略的优先级（0-255），默认为最低 0。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#create acl test_tcp tcp DIP 11.1.30.1/24 ip-port 800
  SIP 11.1.0.1/24 ip-port 400 deny ports any precedence 7
Harbour(config)#sh acl all

ACL test_tcp tcp DIP 11.1.30.1/24 ip-port 800 SIP 11.1.0.1/24 ip-port
  400 deny
ports any precedence 7
```

14.2.5 添加基于 ICMP 的 ACL 策略

【命令格式】create acl <name> icmp DIP [<A.B.C.D/M>|any]SIP [<A.B.C.D/M>|any] type [<icmp_type>|any] code [<icmp_code>|any] [permit|deny] ports [<portlist>|any] {precedence <0-255>}

【使用指导】生成并添加一条针对 ICMP 数据包的 ACL 策略。可匹配的内容为目的 IP 和源 IP 或任意值，ICMP 类型字段和 ICMP 代码字段，并指定相应的物理端口号， precedence 为可选参数，指定策略的优先级（0-255），默认为最低 0。

【命令模式】配置模式

14.2.6 添加基于 MAC+IP 的 ACL 策略

【命令格式】create acl <name> mac-ip destination [<dst_mac> |any]
[<A.B.C.D/M> |any] source [<src_mac> |any] [<A.B.C.D/M>|any]
[permit|deny] ports [<portlist>|any] {precedence <0-255>}*1

【使用指导】生成并添加一条针对 MAC+IP 数据包的 ACL 策略。可匹配的内容为目的 IP 和源 IP，目的 MAC 和源 MAC 或任意值，并指定相应的物理端口号， precedence 为可选参数，指定策略的优先级（0-255），默认为最低 0。

【命令模式】配置模式

【配置实例】

```
Harbour(config)#create ACL test_macip mac-ip destination
  001122334455
11.40.1.1/16 source 001234565566 11.1.30.1/16 deny ports
any precedence 100
Harbour(config)#sh acl all

ACL test_macip mac-ip destination 001122334455 11.40.1.1/16 source
  001234565566
11.1.30.1/16 deny ports any precedence 100
```

14.2.7 删除 ACL 策略

【命令格式】delete acl [<name>|all]

【使用指导】删除相应（name）的 ACL 策略，参数为 all 时删除所有 ACL 策略。

【命令模式】配置模式

14.2.8 查看 ACL 策略

【命令格式】show acl [<name>|all]

【使用指导】显示相应（name）的 ACL 策略，参数为 all 时显示已配置的所有 ACL 策略。

【命令模式】配置模式

14.2.9 设置计数器（counter）

可以为创建的某条ACL策略设置一个计数器counter，用以记录符合这条ACL策略的报文数。counter相关的命令如表 14-1 所示：

表 14-1counter 相关的命令

create counter <name>	创建一个计数器

config acl <name> counter <name>	将创建的计数器与某个已创建的 ACL 策略相关联
clear counter [<name>|all]	对某个计数器或所有计数器清零
no acl <name> counter	取消计数器与 ACL 策略的关联
delete counter [<name>|all]	删除某个计数器或所有计数器
show counter [<name>|all]	显示某个计数器或所有计数器

第15章 SNTP 协议

本章包括如下内容：

- SNTP 协议介绍
- SNTP 的相关配置
- 显示 SNTP 配置信息
- 使用举例

15.1 SNTP 概述

15.1.1 SNTP 协议介绍

SNTP（Simple Network Time Protocol）简单网络时间协议，它是用来使网络中的设备能维持相同的时间的一种通信协议，通过在网络设备中运行 SNTP 协议，有利于网络中设备的管理和维护。SNTP 协议采用客户端、服务器的方式。

15.1.2 SNTP 的三种工作模式

SNTP 协议在维护网络设备的时间时有三种不同的工作模式：

Unicast：客户端通过向指定的服务器发出包含本地时间请求的报文，服务器在响应报文中包含服务器接收到客户端请求报文的时间和服务器发出响应报文的时间。客户端在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的时间值和服务器的偏差。

Multicast：服务器端周期性的广播自己的时间值，客户端在接收到广播报文后，把自己的时间值改为和服务器广播报文中的时间值一致。

Anycast：当客户端不知道时间服务器的地址时采用此种方式，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。以后客户端和此服务器便工作在 unicast 模式下了。

15.2 配置 SNTP

在交换机上配置 SNTP 包含以下内容：

- 配置 SNTP 客户端或 SNTP 服务器的工作模式
- 使能（使 SNTP 客户端有效）或关闭 SNTP 的客户端
- 使能（使 SNTP 服务器有效）或关闭 SNTP 的服务器

- 配置 SNTP 客户端的各种参数

15.2.1 使能或关闭 SNTP 客户端

在一台 Hammer 交换机中 SNTP 客户端的缺省状态是关闭的。

【命令格式】config sntp-client [enable | disable]

【参数说明】如果键入 enable，表示使能运行 SNTP 客户端，如果键入 disable，则表示关闭运行 SNTP 的客户端。

【使用指导】在启动 SNTP 客户端以前必须先配置 SNTP 的工作模式。

【命令模式】配置模式

15.2.2 使能或关闭 SNTP 服务器

在一台 Hammer 交换机中 SNTP 服务器的缺省状态是关闭的。

【命令格式】config sntp-server [enable | disable]

【参数说明】如果键入 enable，表示开始运行 SNTP 服务器，如果键入 disable，则表示取消运行 SNTP 服务器。

【使用指导】在启动 SNTP 服务器以前必须先配置 SNTP 的工作模式。

【命令模式】配置模式

15.2.3 配置 SNTP 的工作模式

SNTP 的工作模式表明了网络中的时间协议以哪种方式来工作，SNTP 协议支持三种工作模式：unicast，multicast，anycast，缺省值为 unicast 模式。在运行 SNTP 之前一定要配置好 SNTP 的工作模式，一旦 SNTP 启动后，就不能再对它的工作模式进行修改了。

【命令格式】cofig [sntp-client | sntp-server] mode <1-3>

【参数说明】如果键入 sntp-client 表示配置客户端的工作模式，如果键入 sntp-server 表示配置服务器端的工作模式。参数<1-3>分别代表 unicast，multicast，anycast。

【命令模式】配置模式

【配置实例】配置 sntp 的客户端的工作模式是 unicast

```
Harbour(config)#config sntp-client mode 1
```

15.2.4 配置客户端的 SNTP 服务器的 IP 地址

当 SNTP 客户端工作在 unicast 模式下时，在启动 SNTP 之前一定要先配置 SNTP 服务器的 IP 地址，以便客户端能和指定的服务器之间进行通信。

【命令格式】config sntp-client server ipaddr <A.B.C.D >

【参数说明】<A.B.C.D >为 SNTP 服务器的 IP 地址。

【命令模式】配置模式

【配置实例】配置客户端的服务器的 IP 地址为 10.5.4.66

```
Harbour(config)#config sntp-client server ipaddr 10.5.4.66
```

15.2.5 配置客户端的刷新周期

客户端的刷新周期是指客户端每隔多长时间向服务器端发起一次时间请求报文。当客户端工作在 anycast 和 unicast 模式下时，需要配置客户端的时间刷新周期。

【命令格式】config sntp-client update-interval <64-1024>

【参数说明】参数<64-1024>表示客户端刷新周期时间值，单位是秒，缺省值为 64（s）

【命令模式】配置模式

【配置实例】将客户端的刷新周期设置为 100 秒

```
Harbour(config)#config sntp-client update-interval 100
```

15.2.6 配置服务器端的广播周期

在 SNTP 的服务器工作在 multicast 模式下时，服务器以一定的周期向指定的网络中广播自己的时间值。

【命令格式】config sntp-server broadcast-interval <64-1024>

【参数说明】参数<64-1024>表示服务器端的广播周期，缺省值为 64（s）。

【命令模式】配置模式

【配置实例】配置时间服务器的广播周期为 66（s）

```
Harbour(config)#config sntp-server broadcast-interval 66
```

15.2.7 恢复 SNTP 客户端的工作模式为 unicast 模式

【命令格式】no sntp-client mode

【命令模式】接口模式

【配置实例】在 sntp 客户端关闭的状态下，想要恢复 sntp 客户端的工作模式为 unicast 模式

```
Harbour(config-if)#no sntp-client mode
```

15.2.8 恢复 SNTP 服务器的工作模式为 unicast 模式

【命令格式】no sntp-server mode

【命令模式】接口模式

【配置实例】在 sntp 服务器关闭的状态下，想要恢复 sntp 服务器的工作模式为 unicast 模式

```
Harbour(config-if)#no sntp-server mode
```

15.2.9 恢复 SNTP 客户端的缺省刷新周期

【命令格式】no sntp-client update-interval

【命令模式】接口模式

【配置实例】想要恢复 sntp 客户端的缺省刷新周期时间值（64s）：

```
Harbour(config-if)#no sntp-client update-interval
```

15.2.10 恢复 SNTP 服务器的缺省广播周期

【命令格式】no sntp-server broadcast-interval

【命令模式】接口模式

【配置实例】想要恢复 sntp 服务器端的缺省广播周期时间值（64s）：

```
Harbour(config-if)#no sntp-server broadcast-interval
```

15.3 显示 SNTP 的状态信息

15.3.1 显示客户端的状态

【命令格式】show sntp-client

【使用指导】show 命令所显示的 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

【配置实例】显示 SNTP 客户端的配置信息：

```
Harbour(config)#show sntp-client

------------sntp client's current state--------------
sntp-client are running.
sntp-client's mode is unicast.
sntp-server's IPAddress is 10.5.4.66.
sntp-client's update-interval is 64 seconds.
```

15.3.2 显示服务器端的状态

【命令格式】show sntp-server

【使用指导】show 命令所显示的 SNTP 服务器端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
- SNTP是否启动

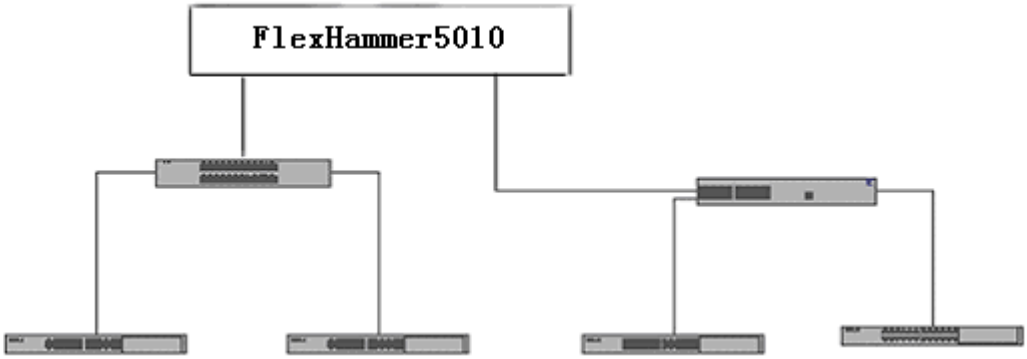
【配置实例】显示 SNTP 服务器端的配置信息：

```
Harbour(config)#show sntp-server

------------sntp server's current state--------------
```

```
sntp-server is running.
sntp-server's mode is unicast.
```

15.4 SNTP 协议配置举例

按下图的例子对一个二层网络实现 SNTP 的配置：



1、在交换机上创建一个时间服务器，使其工作在 anycast 模式下（当然也可以采用 unicast 或者 multicast 模式）：

Harbour(config)#config sntp-server mode 3

Harbour(config)#config sntp-server enable

2、然后在需要同步时间的交换机上键入如下命令：

Harbour(config)#config sntp-client mode 3

Harbour(config)#config sntp-client enable

3、为了适应不同的精确性要求，用户也可以对交换机的时间更新频率进行修改。例如把时间校正周期调整到 100（s）：

Harbour(config)#config sntp-client update-interval 100

第16章 虚拟堆叠

16.1 堆叠概述

堆叠技术是目前在以太网交换机上扩展端口使用较多的一种技术，是一种非标准技术。各厂商不支持混合堆叠，堆叠模式为各厂商自行制定。它将一组相互连接在一起的交换机当作一个整体来看待，实现系统的简易本地化集中管理，简化和方便整体操作。目前流行的堆叠有两种主要形式：菊花链模式和星型模式：

- 菊花链模式是一种基于堆叠的技术，对交换机的硬件没有特殊的要求，通过相对高速的端口串连和软件支持，最终构建一个多交换机的环状结构。
- 星型堆叠是一种高级堆叠技术，对交换机而言，需要提供一独立的高速交换中心，所有主机通过高速堆叠端口连接到同一的堆叠中心。

FlexHammer5010 是港湾公司最近开发的具有堆叠功能的新一代交换机，它具备目前流行的堆叠功能，并且支持菊花链和星型两种模式。使用堆叠功能可以为用户带来以下好处：

- 管理交换机不受空间的限制，它们可以都在本地也可以在远端，只要是在堆叠管理VLAN二层网络能够到达的地方，就可以管理到
- 节省资源，简化重复性的耗时工作
- 节省IP

由于实现的是三层堆叠，存在虚 IP 的概念。默认情况下堆叠服务是打开的，并且系统为每个交换机分配了一虚拟的 IP，系统默认的虚拟 IP 为 172.30.0.1/24 网段，如果该网段同用户的所有网段不冲突的话，用户不必关心该网段；如果同用户的所用网段冲突，用户可以通过手工的方式指定不冲突网段。目前的版本有些应用是基于三层的，所以用户在操作时应先设置好路由，以确保交换机能同网管站连通。

16.2 虚拟堆叠配置

16.2.1 启动或者关闭堆叠功能

【命令格式】`[start|stop] cluster`

【参数说明】启动或禁止堆叠功能，默认为启动状态，可以手工关闭

【命令模式】配置模式

16.2.2 配置 commander switch

【命令格式】`config cluster commander`

【参数说明】配置一台交换机作为堆叠系统的 `commander`，一个堆叠系统中只允许设置一台

Command switch

【命令模式】配置模式

16.2.3 查看堆叠成员信息

【命令格式】show cluster

【参数说明】查看堆叠系统中的交换机信息，其中 ID 为 0 的为 Command switch 其余为 Member switch

【命令模式】配置模式

【配置实例】

```
Harbour(config)#show cluster

The system is commander,stack cluster information.....
-------------------------------------------------------------------
  ------------
|ID      |duty       |deviceType           |stackPort  |macAddress
  |
-------------------------------------------------------------------
  ------------
|  0        |  commander|  FlexHammer5010         |  0            |
  00-05-3b-00-04-91     |
-------------------------------------------------------------------
  ------------
|  1        |  member     |  FlexHammer5010         |  6            |
  00-05-3b-00-38-99     |
-------------------------------------------------------------------
  ------------
|  2        |  member     |  FlexHammer5010         |  6            |
  00-05-3b-58-00-52     |
-------------------------------------------------------------------
  ------------
|  3        |  member     |  FlexHammer5010         |  11           |
  00-05-3b-58-00-32     |
-------------------------------------------------------------------
  ------------
|  4        |  member     |  FlexHammer5010         |  6            |
  00-05-3b-00-04-90     |
-------------------------------------------------------------------
  ------------
```

16.2.4 配置某一台交换机

【命令格式】config cluster member <1-7>

【参数说明】对一个堆叠系统中的一台交换机进行配置

【命令模式】配置模式

16.2.5 选择一组交换机升级

【命令格式】cluster download ftp [hammeros|config-file] <A.B.C.D> <username> <password>

<filename> [<clusterlist>|all]

【参数说明】对一个堆叠系统中的一组交换机进行升级

【命令模式】配置模式

16.2.6 选择一组交换机保存配置

【命令格式】cluster save [<clusterlist>|all]

【参数说明】对一个堆叠系统中的一组交换机进行保存配置

【命令模式】配置模式

16.2.7 选择一组交换机擦除配置

【命令格式】cluster erase [<clusterlist>|all]

【参数说明】对一个堆叠系统中的一组交换机的配置进行擦除

【命令模式】配置模式

16.2.8 选择一组交换机重新起动

【命令格式】cluster reboot [<clusterlist>|all]

【参数说明】对一个堆叠系统中的一台交换机进行重新启动

【命令模式】配置模式

16.2.9 配置堆叠系统的 trap receiver

【命令格式】config cluster trap version [v1|v2c] {community <string>}*1

【参数说明】对一个堆叠系统中的所有交换机配置统一的 trap receiver

【命令模式】配置模式

16.2.10 取消堆叠系统的 trap receiver

【命令格式】config cluster trap version [v1|v2c] {community <string>}*1

【参数说明】取消堆叠系统中 trap receiver，使其不再发送堆叠的 trap。

【命令模式】配置模式

16.2.11 查看堆叠系统的 trap 配置

【命令格式】show cluster snmp trap

【参数说明】查看堆叠系统中 trap 配置

【命令模式】配置模式

第17章 单播路由协议

本章包括如下内容：

- 单播路由概述及配置指导和命令说明
- RIP V1/V2 协议配置指导及命令说明
- OSPF V2 协议配置指导及命令说明

本章内容假定您对 IP 单播路由内容已经熟悉，如果不熟悉，请参阅下面的资料：

- RFC 1058 ——Routing Information Protocol（RIP）
- RFC 1723 ——RIP Version 2
- RFC 2328 ——OSPF Version 2

17.1 单播路由

17.1.1 单播路由概述

路由是三层交换机区别于二层交换机的重要概念。三层交换机实现了 IP 协议及相关的整个 TCP/IP 协议栈，可以提供三层路由转发功能，即跨越不同 IP 网段的 IP 报文转发。在这个意义上说，三层交换机的功能与 IP 路由器是类似的。

IP 路由是 IP 协议三层转发的控制信息，它说明最终达到某个网段的“下一步”应转发到哪里。一条 IP 路由的主要内容是目的地址及掩码、下一跳地址、出接口。其中目的地址及掩码描述目的地信息，下一跳地址和出接口描述在本交换机应该如何转发这类报文。

IPv4 通讯可以分为单播、组播、广播三大类。通常的 IP 数据通讯都使用单播方式，即每个报文的接收者有一个明确的唯一的 IP 地址。IP 组播可以支持用户将一个数据流发送给多个接收者，支持组播的网络会自动在适当的位置复制 IP 组播报文，而不需要数据源重复发出多份数据，可以显著节省网络带宽占用。而广播方式是无条件地发送给所有 IP 设备，所以它只少量应用在本地网段内部。

本章介绍单播路由及路由协议。在 IP 设备中，单播路由的获得通常有两种途径，一种是静态配置，由网络管理员通过命令行等手段明确定义，称为静态路由。在较复杂的网络上，静态配置负担太大，而且难以及时反映网络拓扑的动态变化，这时可以使用动态路由协议。动态路由协议通过网络设备之间的报文交互，动态地学习网络拓扑信息，自动生成路由信息。并且能够在网络拓扑变化时比较迅速地传播变动信息，更新每个设备上的路由表。

目前主流的单播路由协议有 RIP V1/V2、OSPF V2 等，在 FlexHammer5010 交换机上都能提供完善的支持。

17.1.2 基本命令配置向导

路由的相关配置工作主要是路由协议的配置，本节介绍静态路由，以及路由信息的查看。

1 .查看路由表

不熟悉三层交换机或路由器的用户首先要了解的是如何查看路由表。路由表的内容对于正确的报文转发起到关键性作用。查看路由表的命令是 show ip route。比如这个例子：

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


O   1.1.0.0/16 [110/10] is directly connected, v2, 00：03：26
C>* 1.1.0.0/16 is directly connected, v2
C>* 2.1.0.0/16 is directly connected, v3
S>* 100.0.0.0/16 [1/0] via 1.1.1.1, v2
S>* 101.0.0.0/24 [1/0] via 2.1.1.1, v3
O>* 120.0.0.0/16 [110/20] via 1.1.1.200, v2, 00：00：36
```

其中可以看到，C 开头的路由表示是本交换机的接口路由，它只是说明了本地所直接连接的网段。S 开头的是静态路由，它是用户配置的。O 开头的是 OSPF 协议自动得到的路由。

协议类型后面是“*”标志，它说明这个路由当前是生效的。例如第一个路由没有生效，因为路由表中有了一个相同的接口路由，它的优先级比 OSPF 协议高。

在目的地址后面，[m/n]中的 m 代表路由的优先级。n 代表协议内部的度量值(metric)。再后面是下一跳地址，和出接口名称（例子中的“v2”、“v3”）。最后是路由的生存时间。

路由的优先级用来管理不同来源的路由。当不同的协议都得到相同目的地的路由时，系统根据协议的优先级做取舍。协议的优先级是可以由用户修改的。

本系统采用的缺省路由优先级为：

路由类型	缺省优先级
接口路由	0

静态路由	1
RIP	120
OSPF	110

较小的优先级数值代表较高的优先级。

当出接口的状态为 DOWN 时，相关路由会失效或被删除。因为这时交换机不能从这个接口向外转发报文了。当接口状态变为 UP 时，接口路由和静态路由会立刻生效，而动态路由也应在较短时间内恢复。

2. 静态路由

如前所述，静态路由是由用户配置的路由。当用户确信到达某个网段应该先转发到某个地址时，可以通过 ip route 命令配置这个静态路由。

例如：ip route 100.0.0.0/16 1.1.1.1

或 ip route 100.0.0.0 255.255.0.0 1.1.1.1

这两个命令的作用是一样的。配置之后就可以看到上一节中显示路由例子中的 100.0.0.0/16 路由。

其中，100.0.0.0 是目的网段地址，/16 说明掩码长度为 16，即这个网段的地址实际上是 16 位长。或者用 255.255.0.0 代替/16，它同样说明掩码为两个全 1 的字节，即 16 个连续的 1（二进制）。1.1.1.1 是下一跳地址。

整个路由说明，到网段 100.0.0.0/16 的报文，例如目的地址为 100.0.1.1 或 100.0.10.3 的报文，都应该转发到 1.1.1.1 这个设备。1.1.1.1 应该是可以通向 100.0.0.0/16 网段的路由器或交换机。

用 no ip route 命令可以删除静态路由。

例如：no ip route 100.0.0.0/16 1.1.1.1

3. 默认路由

有一类特殊的路由称为默认路由（或缺省路由），即目的地址和掩码为 0.0.0.0/0 的路由。它可以匹配任何目的地址，所以每个找不到对应路由的报文都将按默认路由转发。通常默认路由都是在用户认为有必要时通过静态路由配置的。

例如：ip route 0.0.0.0/0 10.0.0.1

这时，本交换机将把每个没有对应路由的报文转发到 10.0.0.1。在网络有一个唯一出口连接到其他网络时，配置默认路由是很有用的，它可以使交换机所需要的路由数量大大降低。在计算机上，这个默认路由的下一跳地址称为缺省网关。

17.1.3 命令参考

ip route

【命令作用】建立一条静态路由。删除静态路由请使用对应的 no 命令。

【命令格式】{no} ip route [<A.B.C.D/M> | <A.B.C.D> <mask>] <nexthop> {<distance>}

【参数说明】<A.B.C.D/M> 目的 IP 地址及掩码长度

<A.B.C.D> 目的网段地址

<mask> 点分形式的子网掩码

<nexthop> 点分形式的下一跳 IP 地址。

<distance> 优先级，范围从 1 到 255，缺省为 1。255 为最低优先级。

【默认状态】未建立任何静态路由。

【命令模式】配置模式

【使用指导】在较简单的网络环境中不需要运行路由协议时，或由于某种原因需要人为指定路由时，使用静态路由是很合适的。

使用点分形式的子网掩码时，要求掩码从高位开始是连续的二进制“1”，如 255.255.0.0 或 255.255.128.0，不能是 255.0.255.0 或 255.1.0.0。

如果在命令中指定了路由优先级，那么当路由优先级大于静态路由默认的路由优先级时，这条静态路由就会被动态信息替代。
静态路由的优先级默认为 1，比任何动态路由都优先。

【配置实例】ip route 10.0.0.0 255.0.0.0 131.108.3.4 110

show ip route

【命令作用】显示路由表内容。可显示全部路由信息或指定的部分路由信息。

【命令格式】show ip route {<A.B.C.D/M> | <A.B.C.D> | connected | rip | ospf | static |

summary }

【参数说明】<A.B.C.D/M>显示路由表中目的 IP 地址为<A.B.C.D>、子网掩码长度

为 M(0-32)的所有路由表项。

<A.B.C.D>	显示路由表中目的 IP 地址为<A.B.C.D>的所有路由表项。
connected	显示路由表中所有直连路由。
rip	显示路由表中所有 RIP 路由。
ospf	显示路由表中所有 OSPF 路由。
static	显示路由表中所有静态路由。
summary	只显示路由的分类统计值和路由总量信息。

【命令模式】配置模式

【使用指导】命令输出信息从左至右输出信息为：

- 路由类型，如 C（接口路由）、S（静态路由）、R（RIP）、O（OSPF）；
- 生效标志，*表示路由生效；
- 目的地址和掩码；
- 路由优先级和协议内部 metric，如[110/10]；
- 下一跳地址，或说明为直接连接；
- 出接口名称；
- 路由生存时间。

【配置实例】

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

O   1.1.0.0/16 [110/10] is directly connected, v2, 00：03：26
C>* 1.1.0.0/16 is directly connected, v2
C>* 2.1.0.0/16 is directly connected, v3
S>* 100.0.0.0/16 [1/0] via 1.1.1.1, v2
S>* 101.0.0.0/24 [1/0] via 2.1.1.1, v3
O>* 120.0.0.0/16 [110/20] via 1.1.1.200, v2, 00：00：36
```

17.2 RIP 协议

17.2.1 RIP 协议概述

RIP 是 Routing Information Protocol （路由信息协议）的简称。它是所有路由协议中最简单的协议，在实际使用中有着广泛的应用。RIP 是基于 Distance-Vector（距离矢量，简称 D-V）算法的协议，它的协议信息封装在 UDP（User Datagram Protocol）数据报文中。

当路由器启动以后，首先通过运行 RIP 协议的端口分别向外发送一个 RIP request 报文。在此以后，

每隔 30 秒向外发送一次更新报文。对于某一条从其他路由器学习到的路由信息，如果在 180 秒内没有收到这条路由信息的更新报文，就将这条路由信息标志为不可达；若在其后 180 秒内仍未收到更新报文，就将该条路由从路由表中删除。

RIP 使用跳数（Hop Count）来衡量到达信宿机的距离，称为路由权值（Routing Metric）。在 RIP 中，路由器到与它直接相连网络的跳数为 0，通过一个路由器可达的网络的跳数为 1，其余依此类推。为限制收敛时间，RIP 规定 metric 取值 0~15 之间的整数，大于或等于 16 的跳数被定义为无穷大，即目的网络或主机不可达。

在 IETF 组织制订的 RFC 标准中，RIP 包括 RIPv1 和 RIPv2 两个版本。RIP-2 支持明文认证和 MD5 密文认证，并支持可变长子网掩码；而 RIP-1 就不支持上述内容。

RIP 协议的缺陷和解决方法：

首先，由于 D-V 算法本身存在缺陷，导致 RIP 协议在防止生成环路、收敛时间等方面的性能比较差。RIP 采取了一些措施来提高这些方面的性能：RIP 支持水平分割（Split Horizon）与毒性逆转法（Poison Reverse），并可采用触发更新（Triggered Update）。

其次，RIP 协议 30 秒钟发送一次更新报文，在带宽占用方面存在一些缺陷。在实际应用当中可以通过设置 RIP 协议中的报文发送间隔来减小带宽的浪费。

RIP 协议的优点：

一 、 尽管 RIP 协议存在一些缺陷，但在规模较小的网络中表现很好。在简单的网络当中，RIP 协议可以很快收敛，其性能是非常可以接受的。

二、 RIP 协议配置简单。协议越简单，实现越简单，配置方法越简单。当然，能够支撑的网络规模就不会很大。

三、 RIP 协议的应用非常广泛。RIP 协议是各个设备供应商的必须支持的协议之一。在新一代路由协议（如 OSPF，IS-IS）诞生以前，RIP 协议是为数不多的 IGP（内部网关协议）中最重要、应用最广泛的协议之一，至今仍然有很多网络依然在使用 RIP 协议。

RIP 协议路由存取机制：

运行 RIP 协议的路由器需要管理一个路由信息数据库，网络中所有可达信宿（包括主机地址和网络地址）在该路由数据库中都存在记录，这些记录称为路由项。路由信息数据库中包含下列信息：

- 目的地址：指主机或网络的地址。
- 下一跳地址：指为到达目的地，本路由器要经过的下一个路由器地址。
- 接口：指转发报文的接口。
- metric值：指本路由器到达目的地的开销，是一个0~16之间的整数。
- 定时器：路由项最后一次被修改的时间。
- 路由标记：区分路由为内部路由协议的路由还是外部路由协议的路由的标记。

RIP 协议将所有自己的路由信息和从其它路由器学习到的路由信息都存放于这个路由信息数据库中。当 RIP 协议发送 response 报文的时候，就会将所有存放于这个数据库中的路由信息发送出去。

下面以 RIP v1 为例，描述 RIP 的启动和运行过程(RIP v2 的过程相似，不同的是它以组播方式进行)：

某路由器刚启动 RIP 时，以广播的形式向相邻路由器发送请求报文，相邻路由器的 RIP 收到请求报文后，响应该请求，回送包含本地路由表信息的响应报文。

路由器收到响应报文后，修改本地路由表，同时向相邻路由器发送触发更新报文，广播路由修改信息。相邻路由器收到触发更新报文后，又向其各自的相邻路由器发送触发更新报文。在一连串的触发更新广播后，各路由器都能得到并保持最新的路由信息。

同时，RIP 每隔 30 秒向相邻路由器广播本地路由表，相邻路由器在收到报文后，对本地路由进行维护，选择一条最佳路由，再向其各自相邻网络广播修改信息，使更新的路由最终能达到全局有效。同时，RIP 采用超时机制对过时的路由进行超时处理，以保证路由的实时性和有效性。正是通过这些机制，使路由器能够了解到整个网络路由信息。

HAMMER OS 的 RIP 特性：

- 水平分割
- 触发更新
- 路由保持
- 支持RIPv1和RIPv2
- 支持简单明文认证和MD5认证
- 可配置RIP协议计时器

17.2.2 RIP 协议配置介绍

在下面的一些例子中说明如何配置协议及 RIP 的一些可选特性。在 RIP 协议的配置过程中，涉及到三个命令模式，分别是：

- 路由器配置模式：在HammerOS中，这种模式就是配置模式，即输入enable密码以后的模式。

- RIP协议配置模式：即输入router rip命令以后的模式。
- 端口配置模式：即输入interface <name>以后的模式。

下面是配置 RIP 协议时需要掌握的方面：

- 基本RIP配置
- 配置RIP协议版本
- 设置端口的认证类型和密码
- 在端口上启动（或抑制）水平分割
- 生成默认路由
- 配置协议Administrative Distance
- 配置协议时钟
- 重分布路由
- 配置缺省metric
- 监控和维护RIP
- 故障排除：

RIP 协议基本配置：

启动运行 RIP 协议是非常简单的，按照如下步骤就可以完成：

使用 router rip 命令启动 RIP 进程；

使用 network 命令指定端口运行 RIP 协议。

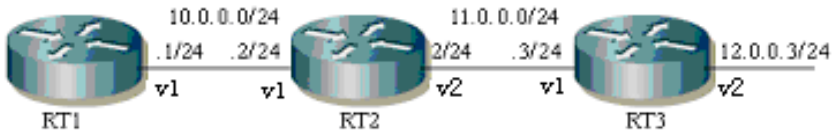


图 17-1 简单的 RIP 网络结构

图 17-1 例举了一个简单的 RIP 网络结构。具体配置如下：

RT1 基本配置命令：

```
RT1（config）#router rip
RT1（config-router）#network 10.0.0.0/24
```

RT2 基本配置命令：

```
RT2（config）#router rip
RT2（config-router）#network 10.0.0.0/24
RT2（config-router）#network 11.0.0.0/24
```

RT3 基本配置命令：

```
RT3（config）#router rip
RT3（config-router）#network 11.0.0.0/24
RT3（config-router）#network 12.0.0.0/24
```

在配置 RIP 协议的时候需要注意的地方：

首先，管理员应当非常清楚路由器的哪个端口要运行 RIP 协议，并为之配置好 IP 地址。

其次，参考命令手册中 network 命令的格式，把需要运行 RIP 协议的端口的 IP 地址和子网掩码作为命令的参数。

配置 RIP 协议版本

RIP 协议有两个版本，即 RIPv1 版本和 RIPv2 版本。可以通过命令来控制 HammerOS 使用哪个版本。配置版本有两种方式：在 RIP 协议配置模式下或端口模式下。

在图 17-1 中以 RT2 为例：

1） 协议配置模式下：

配置 RT2 接收和发送版本 1，在协议配置模式下输入命令：

```
RT2（config）#router rip
RT2（config-router）#version 1
```

配置 RT2 接收和发送版本 2，则在协议配置模式下输入命令：

```
RT2（config）#router rip
RT2（config-router）#version 2
```

2） 端口模式下：

配置 RT2 的 v1 端口接收版本 1，则配置方法如下：

```
RT2（config）#create vlan v1
```

```
RT2（config）#interface v1
RT2（config-if）#ip rip receive version 1
```

配置 RT2 的 v1 端口发送版本 1，则配置方法如下：

```
RT2（config）#create vlan v1
RT2（config）#interface v1
RT2（config-if）#ip rip send version 1
```

若配置版本 2（接收或发送），则只须将 ip rip receive|send version 命令的参数指定为 2 就可以实现了。

设置端口的认证类型和密码

RIP 协议中端口的认证类型有两种：明文认证和 MD5 认证。

指定认证类型的命令是端口配置模式下的 ip rip authentication mode 命令；指定认证密码的命令是端口配置模式下的 ip rip authentication string 命令。

【配置案例】

如图 17-1 中所示，在 RT2 的 v1 端口上配置明文认证：

```
RT2（config）#create vlan v1
RT2（config）#interface v1
RT2（config-if）#ip rip authentication mode text
```

在这个端口上指定明文认证的密码为“test”：

```
RT2（config-if）#ip rip authentication string test
```

在 RT2 的 v1 端口上配置 MD5 认证和密码“test”：

```
RT2（config）#create vlan v1
RT2（config）#interface v1
RT2（config-if）#ip rip authentication mode md5
RT2（config-if）#ip rip authentication string test
```

在端口上启动（或抑制）水平分割

通常，对于连接广播类型 IP 网络并使用距离矢量（D-V）算法路由协议的路由器，可以使用 split horizon（水平分割）机制来减小路由环路产生的可能性。水平分割将阻止路由信息返回起初发送的方向。这种机制可以优化多路由器环境的通信，尤其当某个连接崩溃时。但是，在一些非广播网（如

SMDS），水平分割不利于通信，则需要取消水平分割机制。

【配置案例】

如图 17-1 中所示，在 RT2 的 v1 端口启动水平分割：

```
RT2（config）#create vlan v1
RT2（config）#interface v1
RT2（config-if）#ip rip split-horizon
```

在 RT2 的 v1 端口抑制水平分割：

```
RT2（config）#create vlan v1
RT2（config）#interface v1
RT2（config-if）#no ip rip split-horizon
```

生成默认路由

在图 17-1 中，假定在 RT1 上配置了一些静态路由，但是不希望这些静态路由被 RIP 协议传播到其它路由器上，而同时又要使其它的路由器可以访问这些路由指向的网络，就可以采用让 RT1 在 RIP 协议中生成默认路由的方法来完成。

【配置案例】

在 RT1 上配置 RIP 协议，生成默认路由，在协议配置模式下：

```
RT1（config）#router rip
RT1（config-router）#default-information originate
```

配置了这样的命令以后，RT1 就会向其它路由器发送包含 0.0.0.0/0 默认路由的 RIP 报文了。

配置协议的 Administrative Distance

一个协议的 Administrative Distance 指的是一个路由信息源的可信度等级。Administrative Distance 是一个 0 到 255 的整数，通常情况下，值越高可信度越低。Distance 的值为 255 意味着路由信息源根本不可信，应该被忽略。可以在协议配置模式下配置 RIP 的 Administrative Distance 值，以 RT1 为例：

```
RT1（config）#router rip
RT1（config-router）#distance 20
```

distance 命令的参数是 1 至 255 之间的任何整数值。RIP 的缺省值是 120。

配置协议时钟

RIP 协议使用四个时钟来确定路由更新时间、路由超时时间、路由保持时间和路由清空时间。这四个时间分别由路由更新计时器、路由超时计时器、路由保持计时器、路由清空计时器来确定。

路由更新计时器记录周期性更新的时间间隔，通常为 30 秒，每当该计时器重置时增加小的随机秒数以防止冲突。

每个路由表项都有相关的路由超时计时器，在本系统中，其缺省时间间隔为 180 秒，当路由超时计时器过期时，该路径就标记为失效的，但仍保存在路由表中，直到路由清空计时器过期才被清掉，其中清空时间间隔为 180 秒。

当路由超时计时器过期时，路由保持计时器也同时被启动，路由保持计时器的缺省值是 120 秒，在这段时间内，路由器不会接收对这条路由的更新信息。

可以适当改变这些时钟来调整路由协议的执行，使之与我们的网络更适应。

在协议配置模式下，利用命令：timers basic <update> <timeout> <hold down> <garbage>

调整路由的更新时钟、超时时钟、保持时钟、清空时钟值。四值范围分别是 <0-4294967295> 、<1-4294967295> 、<1-4294967295>、<1-4294967295>。

【配置案例】

在 RT1 上设置更新时钟、超时时钟、保持时钟、清空时钟时间间隔分别为 40、200、60 、130，键入命令：

```
RT1（config）#router rip
RT1（config-router）#timers basic 40 200 60 130
```

重分布路由（redistribute）

为了能使多种路由协议同时运作，可以将一种路由协议的信息引入到另一种路由协议中，这个过程可以称为重分布路由。例如，可以让 RIP 协议重分布静态路由。将路由信息从一种路由协议引入另一种路由协议的操作适用于所有基于 IP 的路由协议。

将其它路由协议的路由信息引入 RIP，需要在协议配置模式下，进行如下配置：

使用默认的 metric 值引入其它路由协议的路由信息，键入如下命令：

redistribute [connected|static|ospf]

使用命令中指定的 metric 值引入其它路由协议的路由信息，键入如下命令：

redistribute [connected|static|ospf] metric <0-16>

配置缺省 metric

当您需要 RIP 协议发送路由信息的时候，可以指定路由信息的 metric 值，这个值在 RIP 协议中代表跳数。

缺省 metric 与 redistribute 命令是相关的。因为不同的路由协议之间的 metric 意义不完全一样，所以利用这个命令可以为其他路由协议重分布来的路由指定一个 metric。redistribute 命令也可以指定 metric 值，当这两个命令同时配置时，应优先选择 redistribute 命令指定的 metric 值。

【配置案例】

配置 RT1 上的 RIP 路由的缺省 metric 值：

```
RT1（config）#router rip
RT1（config-router）#default-metric 5
```

监控和维护 RIP

您可以查看和显示有关 RIP 协议方面的具体统计信息，例如 RIP 路由信息数据库。

在 HammerOS 中提供的监控和维护命令有：

debug rip rm	打开 RIP 与路由管理相关的信息
debug rip events	打开 RIP 协议处理中的事件信息
debug rip packet recv <detail>	打开 RIP 报文的接收信息
debug rip packet send <detail>	打开 RIP 报文的发送信息

这些命令是在用户配置模式下打开的。配合使用的命令是 monitor [on|off]，用来控制 RIP 信息输出的打开和关闭。

另外，HammerOS 还提供了一些查看状态和数据的命令，包括：

show ip rip protocol-version	查看 RIP 协议的版本相关信息
show ip rip database	查看 RIP 协议路由信息数据库的内容

17.2.3 RIP 故障诊断和排错

RIP 协议无法正常收发报文的常见原因：

运行 RIP 协议的相连端口没有配置相同的认证类型或密码，通过 show running-config 命令查看两端是否一致。

rip 没有在应有的端口上启动， 通过 show running-config 命令查看 RIP 的配置。

相连两端的 RIP 协议版本不一致，通过 show running-config 命令查看两端是否一致。

相连两端的 IP 地址相同，通过 show running-config 命令查看两端是否一致。

单播线路上对端 IP 地址与本机配置不一致，通过 show running-config 命令查看两端是否一致。

对方（或本机）时钟设置不当，造成路由表不稳定，通过 show running-config 命令查看两端是否一致。

水平分割设置不当，造成环路或正常通信受到影响，通过 show running-config 命令查看两端是否一致。

物理链路没有正常连通，通过 ping 命令查看。

17.2.4 RIP 命令参考

- debug rip
- default-metric
- ip rip authentication mode
- ip rip receive version
- ip rip send version
- ip split-horizon
- neighbor
- network
- offset-list
- router rip
- timers basic
- version

debug rip

【命令作用】调试 RIP 信息的开关。关闭相应开关，使用 no 命令。

【命令格式】debug rip [events| packet {recv|send {detail}}]

no debug rip [events| packet]

debug rip RM

no debug rip RM

【参数说明】events 显示 RIP 事件，包括收发包、时钟以及接口变化等。

packet 显示收发的 RIP 数据包。

recv 显示接收的 RIP 数据包。

send 显示发送的 RIP 数据包。

detail 显示接收或发送 RIP 数据包内容的详细信息。

RM 显示路由管理变化信息。

【默认状态】未打开

【命令模式】配置模式

【使用指导】为了在终端显示路由处理信息，需要执行命令 monitor on。注意：当网上流量较大的情况下，如果使能此命令，在 FDB 或 ARP 老化，需要 CPU 重新置表项时，由于此时会在命令行上打印大量信息，占用很多 CPU 资源，导致转发不通，表项置不上甚至死机。因此强烈建议用户，当不必要时，一定要禁用此功能。

【配置实例】在终端显示交换机收发的 RIP 数据包

```
Harbour(config)#debug rip packet
Harbour(config)#monitor on
```

【相关命令】monitor

default-metric

【命令作用】为 RIP 设置从其它路由协议中导入路由的默认的 metric 值，

使用 default-metric 命令。返回默认状态，使用 no 形式命令。

【命令格式】default-metric <number>

no default-metric <number>

no default-metric

【参数说明】<number> 设置为默认的 metric 值，取值范围为 1 至 16。

【默认状态】默认状态下 metric 值为 1。

【命令模式】协议配置模式

【使用指导】命令 default-metric 和 router 配置命令 redistribute 共同作用，使当前路由协议对所有的引入路由使用这个 metric 值。默认 metric 可以解决由于引入矛盾 metric 值的路由而产生的问题。此命令不能改变直连路由的 metric 值（直连路由 metric 值为 0）。

【配置实例】将静态路由引入 RIP 并设定 metric 值为 10

```
Harbour(config)#router rip
Harbour(config-router)#default-metric 10
Harbour(config-router)#redistribute static
```

【相关命令】redistribute

ip rip authentication mode

【命令作用】为 RIPv2 报文指定认证类型。恢复到简单明文认证，使用 no 命令。

【命令格式】ip rip authentication mode {text | md5}

no ip rip authentication mode

【参数说明】text 采用简单明文认证。

md5 采用 md5 认证。

【默认状态】对 RIPv2 报文采用简单明文认证。

【命令模式】接口配置模式

【使用指导】RIPv1 不支持认证。

【配置实例】配置接口使用 md5 认证

```
Harbour(config-if)#ip rip authentication mode md5
```

配置接口使用简单明文认证

```
Harbour(config-if)#ip rip authentication mode text
```

ip rip receive version

【命令作用】指定接口只接收 RIPv1 或 RIPv2 报文。要取消命令 version 的设置，使用 no 形式命令。

【命令格式】ip rip receive version [1][2]

ip rip receive version 1 2

no ip rip receive version

【参数说明】1　　接口只接收 RIPv1 报文。

2　　接口只接收 RIPv2 报文。

1　2　两种都接收。

【默认状态】由命令 version 指定。

【命令模式】接口配置模式。

【使用指导】此命令将覆盖协议配置模式下命令 version 指定的行为。

【配置实例】配置接口接收两个版本的 RIP 报文

```
Harbour(config-if)#ip rip receive version 1 2
```

配置接口只接收 RIPv1 报文

```
Harbour(config-if)#ip rip receive version 1
```

【相关命令】ip rip send version

version

ip rip send version

【命令作用】指定接口发送 RIPv1 或 RIPv2 报文。要恢复命令 version 规则，使用 no 命令形式。

【命令格式】ip rip send version [1] [2]

no ip rip send version

【参数说明】1　　接口发送 RIPv1 报文。

2　　接口发送 RIPv2 报文。

【默认状态】由命令 version 指定。

【命令模式】接口配置模式。

【使用指导】此命令将覆盖 router 配置模式下命令 version 指定的行为。

【配置实例】配置接口只发送 RIPv1 报文

```
Harbour(config-if)#ip rip send version 1
```

【相关命令】ip rip receive version

version

ip rip split-horizon

【命令作用】启动水平分割机制，防止路由环路。关闭水平分割机制，使用 no 命令。

【命令格式】ip split-horizon [simple|poisoned]

no ip split-horizon

【参数说明】simple　　一般的水平分割。

poisoned　具有毒性逆转的水平分割。

【默认状态】RIP 已启动水平分割机制。

【命令模式】接口配置模式。

【使用指导】水平分割机制阻止路由信息返回起初发送的方向。

【配置实例】对接口 v2 设置水平分割机制，对接口 v3 取消水平分割机制

create vlan v2

interface v2

ip split-horizon simple

exit

create vlan v3

interface v3

no ip split-horizon

exit

【相关命令】neighbor

network

【命令作用】为 RIP 协议指定实施 RIP 信息交流的网段。

【命令格式】network <A.B.C.D/M>

no network <A.B.C.D/M>

【参数说明】<A.B.C.D/M> 为与本交换机直连的、要进行 RIP 通信的网络的 IP 地址及子网掩码长度；

【默认状态】未指定任何进行 RIP 通信的网段。

【命令模式】协议配置模式

【配置实例】配置本交换机与子网 11.0.0.0/24 内的路由器进行 RIP 通信

router rip

network 11.0.0.0/24

【相关命令】router rip

offset-list

【命令作用】在接口发送或接收 RIP 报文时给路由增加路由权值(metric)。

【命令格式】offset-list <name> [in| out] <0-16> {<ifname>}

no offset-list <name> [in| out] <0-16> {<ifname>}

【参数说明】<name> access-list 名。

[in|out] access-list 应用于 RIP 数据包的方向：in 对应于将 access list 应用于输入数据包；out 对应于将 access-list 应用于输出数据包。<0-16>对 RIP 路由权值(metric)的增加值，范围从 0 至 16。<ifname> 限定只修改从指定接口收发的路由表项的 metric。

【默认状态】未启动

【命令模式】协议配置模式。

【配置实例】将偏移量 10 运用于通过接口 v1 学到的由 access-list 指定的路由的 metric 值

```
Harbour(config)#access-list route a1 permit 11.0.0.0/8
Harbour(config)#router rip
Harbour(config-router)#offset-list a1 in 10 v1
```

【相关命令】access-list

router rip

【命令作用】启动 RIP 协议并进入协议配置模式；若 RIP 协议已经启动，则直接进入协议配置模式。关闭 RIP，使用 no 命令。

【命令格式】router rip

no router rip

【默认状态】未启动 RIP 进程。

【命令模式】配置模式。

【配置实例】启动 RIP 进程并进入协议配置模式

```
Harbour(config)#router rip
Harbour(config-router)#
```

【相关命令】network

timers basic

【命令作用】调整 RIP 时钟。要恢复到默认状态，使用 no 命令。

【命令格式】timers basic <update> <timeout> <holddown> <garbage>

no timers basic

【参数说明】

<update>路由更新时钟。路由器根据此时钟，定期发送一个包含整个路由表的主动响应信息给所有的相邻路由器。该时钟有效值为 0 至 16777215 秒，默认值为 30 秒。

<timeout> 超时时钟。时钟期满，路由项标志为无效路由，但仍保留在路由表中一段时间，目的是向相邻路由器告知此路由已无效。该时钟有效值为 1 至 16777215 秒，默认值为 180 秒。

<holddown> 若某条路由是因为接收到来自源接口的“路由不可达”信息，而被宣布为 Metric=16。则对此条路由同时启动 Holddown Timer 和 Garbage Timer。在启动两个定时器的同时，按“触发更新”向外广播此路由的 Metric=16，以使“邻居”知道此路由不可达。在 Holddown Timer 超时之前，RIP 不接受任何关于此条路由的路由更新，包括来自源接口的路由更新。该时钟有效值为 1 至 16777215 秒, 默认值为 120 秒。

<garbage> 无效路由保持时钟。此时钟期满，则该项路由将彻底从路由表中删除。该时钟有效值为 1 至 16777215 秒，默认值为 180 秒。

【默认状态】update 为 30 秒。

timeout 为 180 秒。

holddown 为 120 秒

garbage 为 180 秒。

【命令模式】路由协议配置模式

【配置实例】配置四个时钟分别为 31 秒、182 秒、100 秒和 121 秒。

```
Harbour(config)#router rip
Harbour(config-router)#timers basic 31 182 100 121
```

distribute-list

【命令作用】对于接口发送或接受的 RIP，用 access list 对它们进行过滤。

【命令格式】distribute-list <name> [in|out] <IFNAME>

distribute-list <name> [in|out]

no distribute-list <name> [in|out] <IFNAME>
no distribute-list <name> [in|out]

【参数说明】<name>指定用来过滤的 access list 的名字。In 表示于将 access list 应用于输入数据包；

out 表示将 access-list 应用于输出数据包；<IFNAME>将 access-list 引入到某个指定

的接口的名称；没有<IFNAME>表示将 access-list 引入到全部 RIP 接口。

返回默认状态，使用 no 命令，默认状态为如果 access-list 没有配置，结果是 deny ALL。

【命令模式】路由协议配置模式

【配置实例】将 access-list：test1 引入到 V1 上。

```
router rip
distribute-list test1 in v1
exit
```

version

【命令作用】指定 RIP 版本。要恢复到默认值，可以使用 no 命令。

【命令格式】version [1|2]

no version

【语法描述】1　指定 RIPv1。

2　指定 RIPv2。

【默认状态】send v1；recv v1，v2

【命令模式】路由协议配置模式

【使用指导】通过命令 ip rip receive version 和命令 ip rip send version，可以在接口指定收发的 RIP 版本。

【配置实例】指定路由器发送和接收 RIPv2 数据包

```
Harbour(config)#router rip
Harbour(config-router)#version 2
```

【相关命令】ip rip receive version

ip rip send version

show ip rip protocol-version

17.3 OSPF 协议

17.3.1 协议概述

OSPF 是 Open Shortest Path First（即“开放最短路径优先协议”）的缩写。OSPF 是一类内部网关协议 (Interior Gateway Protocol)，它可以计算和设置一个自治系统中各个路由器的路由表。

OSPF 是 IETF 组织开发的一个基于链路状态的路由协议。在 IP 网络上，OSPF 通过收集和传递链路状态（Link State）来动态地发现路由。 每个支持 OSPF 协议的路由器都维护着一份描述整个自治系统网络拓扑结构的数据库（LSDB）——这一数据库是收集所有路由器的链路状态广播（LSA）而得到的。 根据链路状态数据库，各路由器会构建一棵以自己为根的最短路径树（SPF Tree），这棵树给出了到自治系统中各节点的路由。

OSPF 协议有如下优点：

- 适用范围广：从几台到上千台路由器的网络都适合运行 OSPF 协议。
- 没有路由自环：由于链路状态算法自身的优势，从根本上避免了路由自环的产生。
- 网络带宽占用小：OSPF 通过定义“DR”的概念，以及将自治系统划分为不同的区域等措施极大的减少了网络带宽的占用。另外 LSA Update 的时间间隔较长也是很重要的一个原因。
- 同步速度快：当网络的拓扑结构发生变化，OSPF 的 FLOOD 方法可以保证将这一变化迅速可靠的传递到整个自治系统。

HAMMER OS 实现了在 RFC2328 中定义的 OSPF Version 2 的各种特性，包括：

- Stub area —— 利用Stub area来减少协议流量。
- 认证 —— 在OSPF包交换的过程中，支持简单明文认证和MD5认证。
- 配置接口参数 —— 包括认证的密码，邻居的超时时间，hello包的发送时间间隔，重传间隔，接口的输出时延，端口的花费，DR选举的优先级等等……
- virtual link —— 支持virtual link。
- 路由聚合 —— 支持Area之间的路由聚合（area range）以及对外部路由的聚合(summary-address)。
- 与其它路由模块之间共享路由信息 —— 用redistribute命令可以把路由信息从其它模块引入，也可以把路由信息提供给其它动态路由协议，并且有精确的过滤和调整能力。

17.3.2 配置向导

使用 OSPF 的缺省配置，可以适应大多数的网络需求，只要配置 network 命令就可以了。这种配置没有认证功能，接口的各参数都使用缺省值。在下面第一节例子中，我们给出了完成这种配置的步骤。

在其它几个说明中，说明如何配置协议的一些可选的特性，需要特别注意的是，这些特性常常要求路由器之间的配置是协调一致的。下面是目标列表，当您阅读完这一章时，您将能够完成：

基本 OSPF 配置

- 设置接口参数
- 配置区域参数
- 配置路由聚合 area range
- 配置虚拟链路virtual link
- 产生缺省路由default route。

- 配置管理距离Administrative Distances
- 配置路由计算的时间间隔
- 重分布路由的配置 redistribute
- 配置缺省metric
- 监控和维护OSPF
- 故障排除：无法建立邻居关系，邻居无法到达full

基本 OSPF 配置

启动一个 OSPF 进程时，下面的三步是必须要完成的：

- 决定路由器的每一个接口将要连接的区域；
- 使用router ospf命令启动OSPF进程；
- 使用network area命令指定要运行OSPF的接口及其所属的区域

【配置案例】

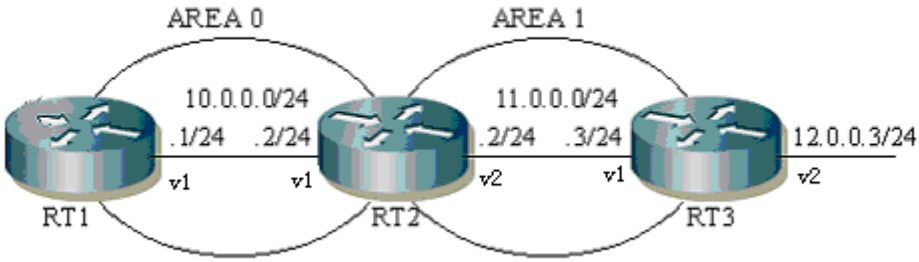


图 17-2 简单的 OSPF 网络

图 17-2 例举了一个简单的 OSPF 网络。在图中的每个路由器可以灵活地使用 network area 命令来进行配置。具体配置如下：

```
RT1#
Router ospf
Network 10.0.0.0/24 area 0


RT2#
Router ospf
Network 10.0.0.0/24 area 0
Network 11.0.0.0/24 area 1


RT3#
```

```
Router ospf
Network 11.0.0.0/24 area 1
```

注意网络配置中的 network area 命令，其中 network 部分为 IP 地址及掩码长度，它定义了一个网段。当 OSPF 运行时，地址在这个网段范围内的接口都将运行 OSPF，接口所属的区域为 area 部分指定的区域。虽然 RT3 在 12.0.0.3/24 接口上没有运行 OSPF，但由于它拥有 RT3 上所有接口中最大的 IP 地址，因此 RT3 的 Router ID 为 12.0.0.3。

注意：

因为在 OSPF 的很多配置中，router ID 都十分重要，但是现在行业内部并没有统一的 router ID 选举方法，所以为了网络配置的清晰和高效，**我们强烈建议您手工指定 router ID**。(在 router ospf 模式下，使用命令 router-id <A.B.C.D>)。

如果没有指定 router ID，我们按照 CISCO 的习惯，从所有配置的 interface 中，选取最大的 IP 地址来作为本机的 router ID。而且一旦选定，即使端口地址改变或端口被删除也不会改变 router ID。

如果您不知道现在的 router ID，可以用 show ip ospf 命令查看。

修改 router ID 后，如果已经配置了区域（area），则必须保存配置，重新启动交换机，设置才能生效。

接口参数的设置

OSPF 允许用户按需改变与某一具体接口相关的参数。但是一些接口参数的设置要求在一个网络中的所有路由器必须一致，否则将无法正确建立邻接关系。这些参数是通过 ip ospf hello-interval, ip ospf dead-interval 和 ip ospf authentication-key 等命令来设置的。因此，如果您确信要配置这些参数，则一个网络中的所有路由器应该有相同的配置。

【配置案例】

如图 17-2 中所示，RT1 和 RT2 在相应接口 v1 配置如下：

```
RT1#
create vlan v1
interface v1
ip ospf hello-interval 15
ip ospf authentication
ip ospf authentication key test


RT2#
create vlan v1
```

```
interface v1
ip ospf hello-interval 15
ip ospf authentication
ip ospf authentication-key test
```

在路由器 RT1 的设置中，ip ospf hello-interval 命令用来设置接口 v1 上 OSPF 的 hello 间隔，一个网段中的所有 OSPF 接口上，hello 间隔必须相同，才能建立邻居关系。Ip ospf authentication 和 ip ospf authentication-key 用来设置接口 v1 上的认证方式及相应的认证密码。同样，一个网段中的所有 OSPF 接口必须具有相同的认证方式和密码，才能建立邻居关系。

配置区域参数

Hammer OS 的 OSPF 软件允许您配置几个区域参数。这些参数包括认证、定义 STUB 区域、为 ABR 产生的缺省路由设置 metric。

认证提供基于密码的保护，防止与未经授权的路由器交换路由信息。在配置区域认证时，必须对区域的所有接口单独配置认证密码。

STUB 区域是不接受外部路由信息的区域，由 ABR 为 AS 外部路由自动产生一条缺省路由注入 STUB 区域。为了进一步减少发送到 STUB 区域的 LSA 的数量，您可以在 ABR 上配置 no-summary 选项来阻止汇总 LSA（类型 3 LSA）进入到 STUB 区域。

Area 认证的配置案例

如图 17-2 所示，为 area 0 配置 MD5 认证方式：

```
RT1#
Router ospf
Network 10.0.0.0/24 area 0
Area 0 authentication message-digest
create vlan v1
Interface v1
Ip ospf message-digest-key 1 md5 test


RT2#
Router ospf
Network 10.0.0.0/24 area 0
Network 11.0.0.0/24 area 1
Area 0 authentication message-digest
create vlan v1
Interface v1
Ip ospf message-digest-key 1 md5 test
```


在路由器 RT1 的设置中，配置 Area 0 authentication message-digest 表示设置区域 0 为 MD5 认证方式，在接口 v1 上使用 Ip ospf message-digest-key 1 md5 test 配置 MD5 认证密码为 test。在路由器 RT2 上进行相同的配置，就可以在 RT1 和 RT2 之间建立邻居关系了。要注意的是，当接口模式下配置的认证方式和接口所在区域的认证方式不一致时，则优先考虑接口配置的认证方式。

STUB 区域配置案例

如图 17-2 中所示，配置区域 1 为 STUB 区域：

```
RT2#
Router ospf
Network 10.0.0.0/24 area 0
Network 11.0.0.0/24 area 1
Area 1 stub


RT3#
Router ospf
Network 11.0.0.0/24 area 1
Area 1 stub
```

在路由器 RT2 使用命令 area stub 配置区域 1 为 STUB 区域。由于 RT2 为 ABR，因此 RT2 广播一条缺省的 3 类 LSA 进入区域 1。用 show ip ospf database 命令可以看到这条 LSA，见图 17-3。

```
RT3(config)#show ip ospf database

OSPF Router with ID (12.0.0.3)
 5 lsas,    0 external routes.

              Router Link States (Area 0.0.0.1)
Link ID         ADV Router      Age Seq#    CkSum  Link count
11.0.0.2        11.0.0.2         18 0x80000004 0x6fa4 1
12.0.0.3        12.0.0.3         15 0x80000003 0x56ba 1

              Net Link States (Area 0.0.0.1)

Link ID         ADV Router      Age Seq#    CkSum
11.0.0.2        11.0.0.2         19 0x80000001 0x9c89

              Summary Link States (Area 0.0.0.1)
Link ID         ADV Router      Age Seq#    CkSum  Route
0.0.0.0         11.0.0.2        802 0x80000001 0x242d 0.0.0.0/0
10.0.0.0        11.0.0.2        792 0x80000001 0xfb42 10.0.0.0/24
```

图 17-3

用 show ip route 命令可以看到这条缺省路由，见图 17-4。

```
RT3(config)#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP,
       >* - selected route

O>* 0.0.0.0/0 [110/11] via 11.0.0.2, v2, 00:05:41
O>* 10.0.0.0/24 [110/20] via 11.0.0.2, v2, 00:05:41
O   11.0.0.0/24 [110/10] is directly connected, v2, 00:05:51
C>* 11.0.0.0/24 is directly connected, v2
```

图 17-4

默认情况下，ABR 广播一条 cost 值为 1 的缺省路由，这条缺省路由的 cost 值能够通过命令 area default-cost 改变。例如，在 RT2 上的配置改变如下：

```
RT2#
Router ospf
Network 10.0.0.0/24 area 0
Network 11.0.0.0/24 area 1
Area 1 stub
Area 1 default-cost 25
```

此时，在 RT3 上用 show ip route 可以看到这条缺省路由的 cost 值为 35，见图 17-5。

```
RT3(config)#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP,
       >* - selected route

O>* 0.0.0.0/0 [110/35] via 11.0.0.2, v2, 00:00:15
O>* 10.0.0.0/24 [110/20] via 11.0.0.2, v2, 00:16:59
O   11.0.0.0/24 [110/10] is directly connected, v2, 00:17:09
C>* 11.0.0.0/24 is directly connected, v2
```

图 17-5

另外，您也可以使用 area stub no-summary 命令来禁止 ABR 向 STUB 区域广播除了缺省路由以外的其他 summary LSA，在 RT2 上的配置为：

```
RT2#
Router ospf
Network 10.0.0.0/24 area 0
Network 11.0.0.0/24 area 1
Area 1 stub no-summary
```

此时，用 show ip ospf database 命令可以看出在区域 1 的 database 中的 summary LSA 消失了（除了表示缺省路由的 LSA），见图 17-6。

```
RT3(config)#show ip ospf database

      OSPF Router with ID (12.0.0.3)

                       4 lsas,     0 external routes.

             Router Link States (Area 0.0.0.1)

Link ID         ADV Router      Age Seq#     CkSum  Link count
11.0.0.2        11.0.0.2        300 0x80000005 0x6da5 1
12.0.0.3        12.0.0.3        249 0x80000004 0x54bb 1

             Net Link States (Area 0.0.0.1)

Link ID         ADV Router      Age Seq#     CkSum
11.0.0.2        11.0.0.2        253 0x80000002 0x9a8a

             Summary Link States (Area 0.0.0.1)

Link ID         ADV Router      Age Seq#     CkSum  Route
0.0.0.0         11.0.0.2        319 0x80000003 0x202f 0.0.0.0/0
```

图 17-6

配置路由聚合

路由聚合是对被广播的路由进行合并，这个特征使 ABR 仅广播聚合路由到其他区域，如果配置得当，可以减少很多 OSPF 网络流量。在 OSPF 中，ABR 将广播一个区域的网络信息到另一个区域，如果网络地址是连续的，您可以配置一个指定的 area range 来包括所有的这些单个网络。

路由聚合的配置案例

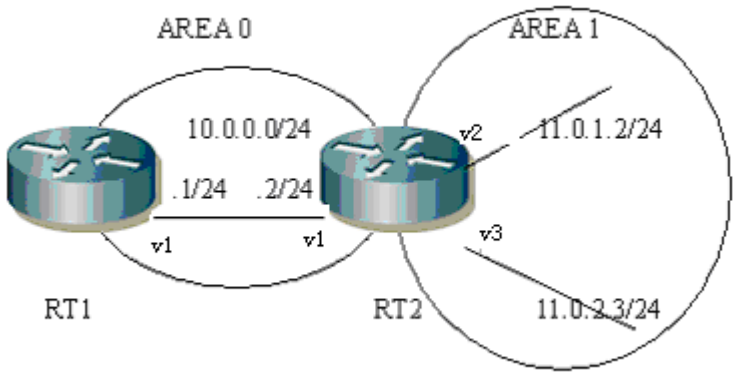


图 17-7

在图 17-7 中，两台路由器的配置如下：

```
RT1#
Router ospf
Network 10.0.0.0/24 area 0


RT2#
Router ospf
Network 10.0.0.0/24 area 0
Network 11.0.0.0/8 area 1
Area 1 range 11.0.0.0/16
```

在 RT2 中增加了 area range 命令，其中 area 指的是要进行聚合的区域，range 为进行聚合的地址范围。这里，我们对属于 11.0.0.0/16 的网段进行了聚合，从 RT1 中可以看到聚合后的路由，详细结果见图 17-8。

```
RT1(config)#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP,
       >* - selected route

O   10.0.0.0/24 [110/10] is directly connected, v1, 00:06:01
C>* 10.0.0.0/24 is directly connected, v1
O>* 11.0.0.0/16 [110/20] via 10.0.0.2, v1, 00:05:51
```

图 17-8

配置虚拟链路 virtual link

在 OSPF 中，规定所有的区域都必须被连接到骨干(backbone)区域。如果骨干区域的连续性被中断，您可以通过创建一个虚拟链路(virtual link)来保持这种连续性。虚拟链路的两端是 ABR，在两端的路由器上都必须进行相应的配置。同时应注意到在 STUB 区域内不能配置虚拟链路。

虚拟链路的配置案例

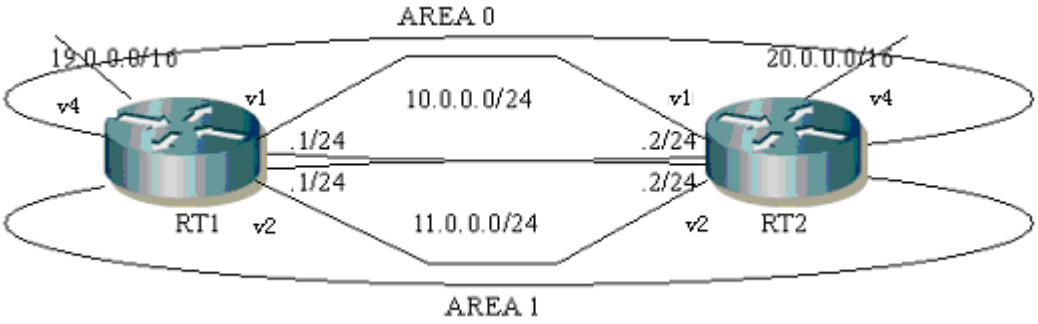


图 17-9

作为一个简单的例子，在图 17-9 例举了一个设计比较差的网络，如果在路由器 RT1 和 RT2 之间的 Area 0 内的链路断开，可能导致网络上的其他路由器的通信受阻。因此，在区域 1 内建立一个虚拟链路来改善网络的脆弱性。两台路由器的配置分别如下：

```
RT1#
Router ospf
Router-id 1.1.1.1
Network 10.0.0.0/24 area 0
Network 11.0.0.0/24 area 1
Area 1 virtual-link 2.2.2.2


RT2#
Router ospf
Router-id 2.2.2.2
Network 10.0.0.0/24 area 0
Network 11.0.0.0/24 area 1
Area 1 virtual-link 1.1.1.1
```

在 area virtual-link 的配置中，area 后面的参数指定 virtual-link 过渡的区域，还要指定对方 ABR 的 router-id。我们可以通过 show ip ospf interface 来查看虚拟链路的接口信息，通过 show ip ospf neighbor 来查看虚拟链路的邻居信息。

配置缺省路由

您可以配置 ASBR，使它产生一条缺省路由。需要注意的是，当您重分布路由进入 OSPF 域时，路由器就自动地成为了 ASBR，然而，ASBR 在默认情况下并不会产生一条缺省路由进入 OSPF 域。

缺省路由的配置案例

以图 17-2 的组网图为例，其中 RT1 和 RT2 分别作如下配置：

```
RT1#
Router ospf
Network 10.0.0.0/24 area 0
Default-information originate always


RT2#
Router ospf
Network 10.0.0.0/24 area 0
```

在 RT1 上 default-information originate always 命令产生一个缺省的外部 LSA，从 RT2 可以看到已经产生了这条缺省路由，见图 17-10。

```
RT2(config)#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP,
```

```
      >* - selected route

O>* 0.0.0.0/0 [110/1] via 10.0.0.2, v1, 00:00:03
O   10.0.0.0/24 [110/10] is directly connected, v1, 00:00:55
C>* 10.0.0.0/24 is directly connected, v1
```

图 17-10 配置 OSPF 的管理距离

管理距离指的是路由信息源的可信度等级。管理距离是一个 0 到 255 的整数，通常情况下，值越高可信度越低。管理距离的值为 255 意味着路由信息源根本不可信，应该被忽略。OSPF 使用了三个不同的管理距离：区域内、区域间和自治系统外部，它们的默认值都是 110。

管理距离的配置案例

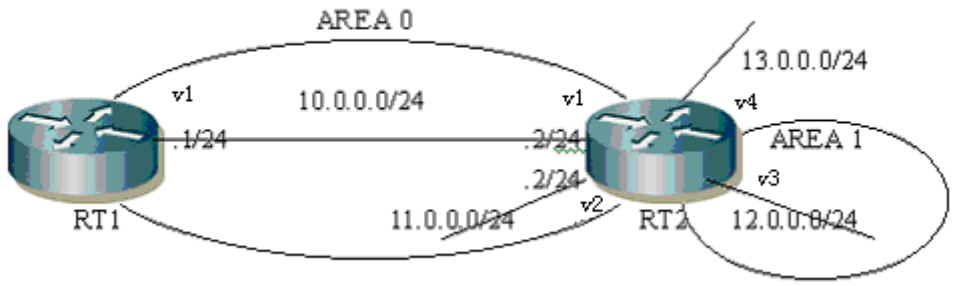


图 17-11

以图 17-11 的组网图为例，对 RT1 和 RT2 分别作如下配置：

```
RT1#
Router ospf
Network 10.0.0.0/24 area 0
Distance ospf intra-area 60 inter-area 90 external 100


RT2#
Router ospf
Redistribute connected
Network 10.0.0.0/24 area 0
Network 11.0.0.0/24 area 0
Network 12.0.0.0/24 area 1
```

在 RT1 上可以看到三种类型 OSPF 路由的管理值的变化，见图 17-12。

```
RT1(config)#sh ip rou
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP,
      >* - selected route

O   10.0.0.0/24 [60/10] is directly connected, v1, 00:07:55
```

```
C>* 10.0.0.0/24 is directly connected, v1
O>* 11.0.0.0/24 [60/20] via 10.0.0.2, v1, 00:07:55
O>* 12.0.0.0/24 [90/20] via 10.0.0.2, v1, 00:07:55
O>* 13.0.0.0/24 [100/20] via 10.0.0.2, v1, 00:07:01
```

图 17-12

配置路由计算的时间间隔

您可以配置从 OSPF 收到一个拓扑变化到开始 SPF 计算之间的延时间隔。您也可以配置两次连续的 SPF 计算之间的保持间隔。

以图 17-2 的组网图为例，对 RT1 作如下配置：

```
RT1#
Router ospf
Network 10.0.0.0/24 area 0
Timers spf 8 16
```

在上面的配置中，第一个数字 8 表示从收到一个拓扑变化到进行 SPF 计算的延时间隔，第二个数字 16 表示相邻两次 SPF 计算的保持间隔。此命令主要用于网络拓扑振荡较频繁的情况下，减少 SPF 计算对路由器的影响，值得注意的是，这样做可能导致路由不能得到及时的更新。

重分布和 route map 的配置

当您需要 OSPF 导入其他路由信息源的路由信息时，则需要完成重分布操作。这里的其它协议可以是静态路由、直连路由和从 RIP 等协议学来的路由。重分布也许可能产生过多的或不需要的路由，这时就需要使用 route map 来进行过滤和控制。

重分布和 route map 的配置案例。

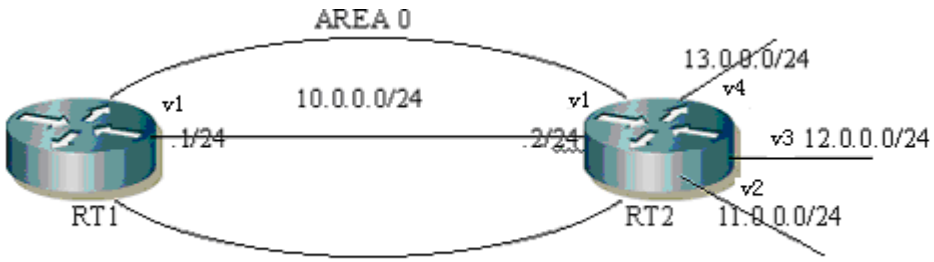


图 17-13

以图 17-13 的组网图为例，对 RT1 和 RT2 分别作如下的配置：

```
RT1#
```

```
Router ospf
Network 10.0.0.0/24 area 0


RT2#
access-list route aclist deny 11.0.0.0/24
access-list route aclist permit any
route-map conmap permit 10
match ip address aclist
set metric 36
exit
Router ospf
Redistribute connected route-map conmap
Network 10.0.0.0/24 area 0
```

在上述的配置中，对被重分布的直连路由应用 route map conmap 进行策略控制，从 RT1 的路由表可以看到没有到达 11.0.0.0/24 网段的路由，说明此条路由已经被 route map 过滤掉了，没有被过滤路由的花费被设置为 36，见图 17-14。

```
RT1(config)#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP,
       >* - selected route

O   10.0.0.0/24 [110/10] is directly connected, v1, 00:13:57
C>* 10.0.0.0/24 is directly connected, v1
O>* 12.0.0.0/24 [110/36] via 10.0.0.2, v1, 00:12:54
O>* 13.0.0.0/24 [110/36] via 10.0.0.2, v1, 00:12:23
```

图 17-14

配置缺省 metric

缺省 metric 与 redistribute 命令是相关的。因为不同的路由协议之间的 metric 意义不完全一样，所以利用这个命令可以为其他路由协议重分布来的路由指定一个 metric。Redistribute 命令也可以指定 metric 值，当这两个命令同时配置时，应优先选择 redistribute 命令指定的 metric 值。以图 17-13 的组网图为例，对 RT1 和 RT2 分别作如下的配置：

```
RT1#
Router ospf
Network 10.0.0.0/24 area 0


RT2#
Router ospf
Redistribute connected
Network 10.0.0.0/24 area 0
Default-metric 88
```

在上述的配置中，设置缺省 metric 值为 88，则从 RT1 的路由表中可以看到这个 metric 值已经生效了，见图 17-15。

```
RT1(config)#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP,
       >* - selected route

O   10.0.0.0/24 [110/10] is directly connected, v1, 00:13:57
C>* 10.0.0.0/24 is directly connected, v1
O>* 11.0.0.0/24 [110/88] via 10.0.0.2, v1, 00:12:54
O>* 12.0.0.0/24 [110/88] via 10.0.0.2, v1, 00:12:54
O>* 13.0.0.0/24 [110/88] via 10.0.0.2, v1, 00:12:23
```

图 17-15

监控和维护 OSPF

您可以查看和显示有关 OSPF 的各种统计信息，例如 IP 路由表，内存和数据库。提供的信息可以用来分析资源的使用情况或者用来解决网络连接问题。

OSPF 监控和维护案例：

组网图见图 17-13，下面介绍一下相关的命令及作用。

Show ip ospf database 主要用来显示 LSA 数据库信息，包括各种类型的 LSA。如果要显示具体的某一类 LSA 信息，可以附加 LSA 的类型参数，显示结果见图 17-16。

```
RT1(config)#show ip ospf database

OSPF Router with ID (12.0.0.3)

 5 lsas,    2 external routes.

 Router Link States (Area 0.0.0.0)

 Link ID         ADV Router      Age Seq#    CkSum  Link count
 12.0.0.3        12.0.0.3        294 0x80000004 0x080a 1
 13.0.0.2        13.0.0.2        296 0x80000007 0x10fb 1

              Net Link States (Area 0.0.0.0)

 Link ID         ADV Router      Age Seq#    CkSum
 10.0.0.2        13.0.0.2        301 0x80000002 0x859a

              AS External Link States

 Link ID         ADV Router    Age   Seq#    CkSum  Route
```

```
12.0.0.0       13.0.0.2     217 0x80000002 0x2c66 V3 12.0.0.0/24 [0x0]
13.0.0.0       13.0.0.2     237 0x80000002 0x1f72 V3 13.0.0.0/24 [0x0]
```

图 17-16

show ip ospf interface 主要用来显示 OSPF 接口信息，可以附加接口名字参数来显示具体的某个接口信息，显示结果见图 17-17。

```
RT1(config)#show ip ospf interface
default is down, line protocol is down
OSPF not enabled on this interface
v1 is up, line protocol is up
Internet Address 10.0.0.1/24, Area 0.0.0.0
Router ID 12.0.0.3, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State Backup, Priority 1
Designated Router (ID) 13.0.0.2, Interface Address 10.0.0.2
Backup Designated Router (ID) 12.0.0.3, Interface Address 10.0.0.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:03
Neighbor Count is 1, Adjacent neighbor count is 1
```

图 17-17

show ip ospf neighbor 主要用来显示 OSPF 的邻居信息，可以附加邻居的 router-id 参数来显示具体的某个邻居信息，显示结果见图 17-18。

```
RT1(config)#show ip ospf neighbor

Neighbor ID  Pri  State  Dead Time  Address    Interface   RXmtL RqstL DBsmL
13.0.0.2     1   Full/DR   00:00:36  10.0.0.2   v1:10.0.0.1  0     0     0
```

图 17-18

show ip ospf route 主要用来显示 OSPF 的路由信息，显示结果见图 17-19。

```
RT1(config)#show ip ospf route
============ OSPF network routing table ============
N    10.0.0.0/24          [10] area: 0.0.0.0
                        directly attached to v1

============ OSPF router routing table =============
```

```
R    13.0.0.2              [10] area: 0.0.0.0, ASBR
                          via 10.0.0.2, v1

============ OSPF external routing table ===========
N V3 12.0.0.0/24           [36/10] tag: 0
                          via 10.0.0.2, v1
N V3 13.0.0.0/24           [36/10] tag: 0
                          via 10.0.0.2, v1
```

图 17-19

show ip ospf 主要用来显示 OSPF 总体信息和区域信息，显示结果见图 17-20。

```
RT1(config)#show ip ospf
OSPF Routing Process, Router ID: 12.0.0.3
Supports only single ToS (ToS0) routes
This implementation conforms to RFC2328
RFC1583 Compatibility flag is disabled
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Refresh timer 10 secs
Number of external LSA 2
Number of areas attached to this router: 1

Area ID: 0.0.0.0 (Backbone)
Number of interfaces in this area: Total: 1, Active: 1
Number of fully adjacent neighbors in this area: 1
Area has no authentication
SPF algorithm executed 3 times
Number of LSA 3
```

图 17-20

OSPF 故障诊断和排错

OSPF 邻居关系没有建立的常见原因:

1.路由器上的 OSPF 任务没有启动。可以用 show ip ospf 命令查看。

2.OSPF 在相应的接口上没有启动。可以用 show ip ospf interface 命令查看。

3.OSPF 接口的 hello 间隔和 dead 间隔不一致。可以用 show ip ospf interface 命令查看。

4.在相邻接口上的 OSPF 网络类型不一致。可以用 show ip ospf interface 命令查看。

5.在相邻接口上的认证类型或密钥不一致。可以用 show run 命令查看。

6.OSPF 相邻接口所属区域或区域类型不一致。可以用 show run 和 show ip ospf interface 命令查看。

7.OSPF 邻居与本地 OSPF 实例具有相同的 router-ID。可以用 show ip ospf 查看。

8.OSPF 的 hello 报文由于资源的缺乏而得不到及时的处理（例如，CPU 和内存资源的耗尽）。

9.底层发生问题导致 OSPF 不能正确地收发 hello 报文。可通过 Ping 命令测试，若从本地路由器 ping 对端路由器不通，则表明物理连接和下层协议有问题。

17.3.3 命令参考

area authentication

【命令作用】用这个命令来开启（enable）OSPF 在某个区域（area）中的认证（authentication）功能。使用它的 no 模式，可以禁止（disable）某个区域（area）中的认证。

【命令格式】area [<0-4294967295>|<A.B.C.D>] authentication

area [<0-4294967295>|<A.B.C.D>]

authentication message-digest

no area [<0-4294967295>|<A.B.C.D>] authentication

【参数说明】[<0-4294967295>|<A.B.C.D>] 要开启（enable）认证的区域（Area）的编号，可以是 IP 地址形式或数字形式。

message-digest 可选。如果有，表示采用 MD5 认证。

【缺省状态】没有认证。

【命令模式】router ospf。

【使用指导】OSPF 提供了两种认证模式，一个是简单明文认证（clear text authentication），另一个是 MD5 认证， 这个命令里，MD5 认证用 message-digest 参数来设置。

在同一个 OSPF 区域（area）内，认证模式必须是一致的，如果两个交换机的端口需要交换 OSPF 包，那么这些端口的密码（authentication password）也必须是一致的，这个密码可以在端口模式(interface)下，用命令 ip ospf authentication-key 来设置。如果是 MD5 认证，则用 ip ospf message-digest-key 来设置密码。

【配置实例】在这个例子里创建了 VLAN，启动 OSPF，并且分别为两个 OSPF 区域设置了认证模式，端口（在这里，端口和 VLAN 是一样的。）也配置了密码。在配置模式下输入：

```
create vlan v1
config vlan v1 ipaddress 11.0.0.1 255.255.255.0
config vlan v1 add port 1,2,3,4 untagged
create vlan v2
config vlan v2 ipaddress 12.0.0.1 255.255.255.0
```

```
config vlan v2 add port 9,10,11,12 untagged

router ospf
router-id 11.0.0.1
network 11.0.0.0/24 area 0
network 12.0.0.0/24 area 1
area 0 authentication
area 1 authentication message-digest
exit

create vlan v1
interface v1
ip ospf authentication-key testpass
exit

create vlan v2
interface v2
ip ospf message-digest-key 1 md5 testpass
exit
```

area default-cost

【命令作用】对于 stub 域（stub area），ABR 会产生一条缺省路由（default route），用 area default-cost 命令可以设定这条缺省路由的 cost。 如果需要恢复到缺省状态（缺省 cost 是 1），可以用这个命令的 no 模式。

【命令格式】area [<A.B.C.D>|<0-4294967295>] default-cost <0-16777215>

no area [<A.B.C.D>|<0-4294967295>] default-cost

【参数说明】[<A.B.C.D>|<0-4294967295>] 域（Area）的编号，可以是 IP 地址模式或数字形式。<0-16777215>stub area 缺省路由的 cost。

【缺省状态】是 1

【命令模式】router ospf

【使用指导】这个命令只需要在 stub area 的边界路由器（ABR，Area Border Router）上配置。ABR 会向 stub area 内发送一条缺省路由，这个命令为缺省路由指定 metric 值。area 0 和 virtual-link transmit area（包含 virtual-link 的 area）不能被设置为 stub area，也不能配置这条命令。

【配置实例】下面的配置让路由器加入两个 area（其中一个是 stub area），从而成为边界路由器。用本命令指定缺省路由的 metric 为 10。

```
config vlan default ipaddress 192.168.0.100 255.255.255.0
create vlan v1
config vlan v1 ipaddress 11.0.0.2 255.255.255.0
config vlan v1 add port 1,2,3,4 untagged
create vlan v2
config vlan v2 ipaddress 12.0.0.1 255.255.255.0
config vlan v2 add port 9,10,11,12 untagged
```

```
router ospf
network 11.0.0.0/24 area 1
network 12.0.0.0/24 area 0
area 1 stub
area 1 default-cost 10
exit
```

【相关命令】area stub

area range

【命令作用】这个命令可以让 ABR 对某个 area 的多条路由进行聚合（summarize）。对于聚合范围内的多条路由， ABR 只产生本命令指定的一条聚合路由。使用它的 no 模式，可以禁止（disable）路由聚合。

【命令格式】area [<0-4294967295>|<A.B.C.D>] range

<A.B.C.D/M> {[advertise|not-advertise]}*1

no area [<0-4294967295>|<A.B.C.D>] range <A.B.C.D/M>

{[advertise|not-advertise]}*1

【参数说明】[<0-4294967295>|<A.B.C.D>] area ID 指定对哪个 area 的路由进行聚合。

<A.B.C.D/M>网络地址，用来指定对哪个网段的路由进行聚合。

not-advertise 可选。如果设置了 not-advertise，ABR 就不会发出聚合过的路由，而且聚合前的路由也不会发布，用这个方法可以隐藏起网络信息。相反，如果设置了 advertise，ABR 就会发出聚合过的路由，这与不加选项的默认情况相同。

【缺省状态】不聚合。

【命令模式】router ospf。

【命令指导】这个命令只能在 ABR 上生效。路由聚合的好处是可以减少边界路由器发布的路由条数，而且可以掩盖网络内部的划分细节。一般情况下，没有必要配置这个命令。

【配置实例】下面命令指定对 area 1 的 11.0.0.0/8 网段的路由进行聚合，这样在其它 area 中的路由器将只能收到目标地址为 11.0.0.0/8 的路由。

```
Harbour(config)#router ospf
Harbour(config-router)#area 1 range 11.0.0.0/8
Harbour(config-router)#exit
```

area stub

【命令作用】这个命令可以使某个区域（area）成为 stub area。在 stub area 内，不传播 AS External LSA，这使 OSPF 协议引起的网络负载减少了很多。如果配置了 no-summary 选项，OSPF 会停止传输 summary LSA（第 3 类），从而进一步减少负载流量。使用它的 no 模式可以取消 stub area 的设置。

【命令格式】area [<0-4294967295>|<A.B.C.D>] stub [no-summary]

no area [<0-4294967295>|<A.B.C.D>] stub [no-summary]

【参数说明】[<0-4294967295>|<A.B.C.D>] 区域（Area）的 ID，可以是 IP 地址形式或数字形式。

no-summary 可选的，这个参数只需在 ABR 上设置，如果配置，相应的 area 就成为 totally stub area，ABR 不会向 totally stub area 内部发送 summary LSA（第 3 类 LSA），而用一条缺省路由（全 0 的路由）指明 stub area 的网络出口。

【缺省状态】没有设置 stub area。

【使用指导】如果只需要取消 no-summary 的设置，可以使用命令 no area <A.B.C.D> stub no-summary，这个命令会保留 stub，但是会删除 no-summary 参数。如果要使一个区域（area）成为 stub area，必须把该 area 的所有路由器都配置为 stub，否则这些路由器之间将无法建立邻居或邻接关系。值得注意的是 no-summary 参数只需在 ABR 上设置。设置后 ABR 不会向 stub area 内部发送 summary LSA（第 3 类 LSA），而用一条缺省路由（全 0 的路由）指明 stub area 的网络出口。

【命令模式】router ospf。

【配置实例】参考 area [<A.B.C.D>|<0-4294967295>] default-cost <0-16777215>命令的例子。

area virtual-link

【命令作用】在 OSPF 中，规定所有的 area 必须和骨干区域（backbone area）直接相连，如果因为网络故障或特殊情况而无法做到这一点，也可以用 virtual link 来建立连接。（但是并不推荐总是使用 virtual link）。使用它的 no 模式，可以取消 virtual link 的配置。

【命令格式】area [<0-4294967295>|<A.B.C.D>] virtual-link

<A.B.C.D> [authentication-key] <AUTH_KEY>

area [<0-4294967295>|<A.B.C.D>] virtual-link

<A.B.C.D> [authentication] {[message-digest|null]}*1

area [<0-4294967295>|<A.B.C.D>] virtual-link

<A.B.C.D> [message-digest-key] <1-255> [md5] <KEY>

area [<0-4294967295>|<A.B.C.D>] virtual-link <A.B.C.D> {[hello-interval] <1-65535>}*1{[retransmit-interval]<3-65535>}*1{[transmit-delay]<1-65535>}*1 { [dead-interval] <1-65535>}*1

【参数说明】area <A.B.C.D> 区域（Area）的 ID，可以是 IP 地址形式或数字形式。

message-digest 消息摘要认证，null 不要认证，与默认情况相同。

virtual-link <A.B.C.D> virtual-link 对端邻居的 router id。可以用 show ip ospf 命令查看。

authentication-key <AUTH_KEY> 可选。简单明文认证的密码。有效长度是 8 个字节，而且必须不包含空格，超过的部分会被忽略。当 backbone area 被设定为简单明文验证时发生作用。

message-digest-key <1-255> md5 <KEY>可选。定义 virtual-link 上 MD5 认证的 key ID 和密码。

hello-interval <1-65535>可选。Hello 包从一个端口发出的时间间隔，缺省值是 10 秒。（在每个子网中的各端口必须用统一的设置。）

retransmit-interval <3-65535>可选。两次重传 LSA 之间的时间间隔。缺省值是 5 秒。

transmit-delay <1-65535>可选。在这个端口发出的 LSA 会在 age 域增加这个值，表示在本机的传输过程中经过了这么长的时间。缺省值是 1。

dead-interval <1-65535>可选。缺省值是 40 秒。如果经过这么长时间，还没有从邻居收到 hello 包，OSPF 就认为邻居路由器已经关机了。这个值通常是 hello-interval 的 4 倍。（在每个子网中的各端口必须用统一的设置。）

【使用指导】这个命令比较复杂，但是实际上往往只使用最简单的模式就可以满足大部分需要了，所以请忽略您用不到的部分。如果您的确需 要，可以再回来详细阅读相关内容。如果有必要，可以为 virtual link 设置各种参数，也可以设置简单明文认证和 MD5 认证，和普通的认证很相似，同样需要为 area 和 virtual link 同时配置。在逻辑上，virtual link 属于 backbone area，但是它的认证模式可以和 backbone area 上的认证模式不一致。如果只想删除 virtual link 的某个参数，可以用下面的命令：

no area [<0-4294967295>|<A.B.C.D>] virtual-link <A.B.C.D> [authentication-key]

no area [<0-4294967295>|<A.B.C.D>] virtual-link <A.B.C.D> [authentication]

no area [<0-4294967295>|<A.B.C.D>] virtual-link <A.B.C.D> [message-digest-key] <1-255>

no area [<0-4294967295>|<A.B.C.D>] virtual-link <A.B.C.D> {[hello-interval] <1-65535>}*1 {[retransmit-interval] <3-65535>}*1 {[transmit-delay] <1-65535>}*1 {[dead-interval] <1-65535>}*1

【缺省状态】没有设置 message-digest-key <1-255> md5 <KEY>

hello-interval 10 秒。

retransmit-interval 5 秒。

transmit-delay 1 秒。

dead-interval 40 秒。

【命令模式】router ospf。

【配置实例】下面的例子用缺省值建立一个 virtual link。

```
router ospf
area 1 virtual-link 14.0.0.2
exit
```

下面的例子建立一个有 MD5 认证的 virtual link，而且也在 area 0（backbone area）设置了认证模式。

```
Harbour(config)#router ospf
Harbour(config-router)#area 1 virtual-link 14.0.0.2
Harbour(config-router)#area 1 virtual-link 14.0.0.2 authentication-key her
Harbour(config-router)#area 1 virtual-link 14.0.0.2 authentication
Harbour(config-router)#exit
```

auto-cost reference-bandwidth

【命令作用】在现在的实现里，OSPF 会根据接口的带宽来自动计算 cost。计算公式是：cost = reference-bandwidth / 接口带宽

比如以太网接口的 cost 是 10，FDDI 接口的 cost 是 1。使用它的 no 模式，可以取消 auto-cost reference-bandwidth 的配置。

【命令格式】auto-cost reference-bandwidth <1-4294967>

no auto-cost reference-bandwidth

【参数说明】reference-bandwidth <1-4294967> 接口带宽的大小。

【缺省状态】100Mbps

【命令模式】router ospf。

【使用指导】如果您的 OSPF 网络中有的设备接口的带宽非常大，超过默认的参考带宽（如 STM-1、GE），这时您可以设置一个更大的 reference-bandwidth，使 OSPF 可以准确地反映出路径开销。推荐使用最大的接口带宽作为参考带宽.注意需要在 OSPF 网络中的所有 OSPF 路由器上设置一致.

使用 ip ospf cost <1-65535>命令，可以手工地为某个端口指定 metric，这个设定会覆

盖 OSPF 自动计算的 metric。

【配置实例】把 reference-bandwidth 配成 1000。

```
Harbour(config)#router ospf
Harbour(config-router)#router-id 11.0.0.1
Harbour(config-router)#network 11.0.0.0/24 area 1
Harbour(config-router)#auto-cost reference-bandwidth 1000
Harbour(config-router)#exit
```

clear ip ospf neighbor

【命令作用】使用这个命令相当于重新建立和指定 OSPF 路由器的邻居关系，和这个邻居相关的网络连接状态会被刷新，LSA 会重新发送。

【命令格式】clear ip ospf neighbor <A.B.C.D>

【参数说明】Neighbor <A.B.C.D>指定需要刷新的邻居的 router ID。

【命令模式】配置模式

【使用指导】这个命令和 CISCO 的没有直接关系。当管理员希望从某个邻居重新进行一次数据库同步时，可以使用这个命令。

为了不引起网络的混乱，您需要在整个 AS 统一这个配置。一般情况下请不要修改这个值。

【配置实例】下面的命令刷新来自 12.0.0.2 的 LSA。

clear ip ospf neighbor 12.0.0.2

compatible rfc1583

【命令作用】如果需要和只支持 rfc1583 的路由器互联，请配置这个命令。使用它的 no 模式，可以禁止（disable）rfc1583 兼容功能。

【命令格式】compatible rfc1583

no compatible rfc1583

【缺省状态】compatible rfc1583 被禁止。

【命令模式】router ospf

【使用指导】因为现在的大多数路由器都是支持 rfc2328 的，所以这个命令不太常用。在一个 AS 内部，所有的路由器都必须在这一设置上统一。因为 rfc2328 对 summary route cost 的计算方式和 rfc1583 不一样，所以 AS 内路由器设置不一样的话，可能产生路由环路。

【配置实例】

```
Harbour(config)#router ospf
Harbour(config-router)#compatible rfc1583
Harbour(config-router)#exit
```

default-information originate

【命令作用】这个命令让路由器有能力向整个 OSPF 域（routing domain）发送缺省路由（default route，0.0.0.0/0）。要取消这条命令，可以用它的 no 模式，no default-information originate。

【命令格式】default-information originate{[always]}*1{type<1-2>}*1

{[metric] <0-16777214>}*1 {[route-map] <WORD>}*1

no default-information originate

【参数说明】metric <0-16777214>可选。用来定制缺省路由的 metric。

type <1|2> 可选。限定缺省路由的类型。对 OSPF 来说，外部路由有两种类型。Typv2=Type 1 external route,typv3=type 2 external route。

always 可选。不论是否产生了由其他协议 redistribute 来的缺省路由，都产生一条缺省路由。

route-map <WORD>可选。指定一个 route-map，在发出缺省路由之前会经过 route-map 的过滤。如果缺省路由不符合 route-map 的限定条件，就不发出路由。

【缺省状态】metric 值为 10，type 为 type 2。

【命令模式】router ospf。

【使用指导】任何时候，只要一台路由器上配置了 redistribute 命令，它就自动的成为

ASBR（autonomous system boundary router，自治系统边界路由器）。但是对缺省路由的处理是特殊的。在没有配置 default-information originate 命令的情况下，OSPF 路由器不会产生缺省路由。所以如果需要 OSPF 路由器发出缺省路由，需要先配置该命令。如果配置了 always 参数，不论路由表中是否存在缺省路由，OSPF 都会产生一条缺省路由并通告之。特别要提到的是 route-map 选项，用它可以定义一个对缺省路由的过滤方案，在发出缺省路由之前，会用指定的 route-map 对它进行过滤和设置属性值。

【配置实例】让路由器发出一条缺省路由，metric 100，1 类外部路由。

```
Harbour(config)#router ospf
Harbour(config-router)#default-information originate always type 1 metric
100
Harbour(config-router)#exit
```

default-metric

【命令作用】为 OSPF 设置从其它路由协议中导入路由的默认的 metric 值，使用 default-metric 命令。

使用它的 no 模式，可以使 default-metric 返回缺省状态。

【命令格式】default-metric <0-16777214>

no default-metric

【参数说明】default-metric <0-16777214>指定缺省的 OSPF metric。

【缺省状态】default-metric 为 20。

【命令模式】router ospf。

【使用指导】default-metric 通常是和 redistribute 命令共同使用的。在不同的路由协议之间，常常没有通用的 metric，这个命令就是为了处理这种情况，它可以为转发（redistribute）的路由设置一个缺省的 metric。

【配置实例】下面把 default-metric 设置为 21。

```
Harbour(config)#router ospf
Harbour(config-router)#redistribute static
Harbour(config-router)#default-metric 21
Harbour(config-router)#exit
```

distance

【命令作用】使用这个命令可以设置 OSPF 路由的 administrative distance，这个值越小，表示可信度越高。要取消这个命令的设置，可以用它的 no 模式。

【命令格式】distance <1-255>

no distance <1-255>

【参数说明】distance <1-255>设置 OSPF 路由的 distance。

【缺省状态】ospf distance 缺省是 110

【命令模式】router ospf。

【使用指导】这个命令的配置可以被 distance ospf 命令覆盖。具体内容参考 distance ospf。

【配置实例】下面把 OSPF 可信度设置为 150。

```
Harbour(config)#router ospf
Harbour(config-router)#distance 150
Harbour(config-router)#exit
```

下面是结果的显示：

```
left(config)#show ip route
Codes：  C - connected, S - static, R - RIP
       > - selected route, * - FIB route
O   11.0.0.0/24 [150/10] is directly connected, v1, 00：00：12
C>* 11.0.0.0/24 is directly connected, v1
C>* 12.0.0.0/24 is directly connected, v3
```

distance ospf

【命令作用】这个命令让管理员可以根据 OSPF 的路由类型设置不同的 administrative distance，这个值越小，表示可信度越高。如果可信度是 255，相应的路由将不被采用。要取消这个命令的设置，可以用它的 no 模式。

【命令格式】distance ospf {[intra-area] <1-255>}*1 {[inter-area] <1-255>}*1 {[external] <1-255>}*1

no distance ospf

【参数说明】intra-area <1-255> 可选。设置 intra-area 路由的 distance

inter-area <1-255> 可选。设置 inter-area 路由的 distance。

external <1-255> 可选。设置 external 路由的 distance。

【缺省状态】distance 都是 110。

【使用指导】这个命令和 distance 命令很类似，不过控制范围可以更精确一些。而且这个命令的优先级比 distance 命令高。

通常使用这个命令的目的是为了使内部路由（internal routes）比外部路由（external routes）有更高的可信度。

【命令模式】router ospf

【配置实例】下面把外部路由的 distance 设置成 200，降低其可信度。

```
router ospf
redistribute static
network 11.0.0.0/24 area 1
distance ospf external 200
exit
```

【相关命令】distance

distribute-list

【命令作用】在 OSPF 引入外部路由时，可以用 access list 对它们进行过滤，distribute-list 命令提供了这个接口。要取消这个命令的设置，可以用它的 no 模式。

【命令格式】distribute-list <WORD> out [connected|static|rip]

no distribute-list <WORD> out [connected|static|rip]

【参数说明】<WORD>指定用来过滤的 access list 的名字。

[connected|static|rip] 指定对哪个来源的外部路由的引入进行过滤。

【缺省状态】未设置。

【命令模式】router ospf

【使用指导】当 OSPF 引入路由时，会对路由项的目标网段进行分析，如果某个路由的目标网段被

distribute-list 命令中指定的 access list 拒绝（deny），OSPF 将不引入该路由。

【配置实例】下面让 OSPF 只引入 1.1.1.0/24 网段的路由。

配置 access-list

```
access-list a1 permit 1.1.1.0/24
```

配置静态路由。

```
ip route 1.1.1.0/24 10.0.0.99
ip route 1.1.2.0/24 10.0.0.99
ip route 1.1.3.0/24 10.0.0.99
```

指定 OSPF 转发静态路由，并且对它们进行过滤。

```
router ospf
redistribute static
distribute-list a1 out static
exit
```

下面是结果：

```
flex1(config)#show ip ospf database


 OSPF Router with ID (12.0.0.1)  AS External Link States

Link ID        ADV Router      Age Seq#    CkSum  Route
 1.1.1.0        12.0.0.1        158 0x80000001 0xf24e V3 1.1.1.0/24 [0x0]
```

可以看到只引入了 access list 允许的路由。其它的路由都被过滤掉了。

ip ospf authentication-key

【命令作用】用这个命令为某个端口设置简单明文认证的密码（password for clear text authentication）。使用它的 no 模式，可以取消某个端口的密码设置。

【命令格式】ip ospf authentication-key <AUTH_KEY>

no ip ospf authentication-key

【参数说明】<AUTH_KEY>密码。有效字节是 8 个字节，超过的部分会被忽略。

【缺省状态】没有密码（为空字符串）。

【命令模式】interface 模式。

【配置实例】

```
create vlan v1
```

```
interface v1
ip ospf authentication-key testpass
exit
```

【相关命令】area authentication。

ip ospf cost

【命令作用】使用 ip ospf cost <1-65535>命令，可以手工地为某个端口指定 cost，这个设定会覆盖 OSPF 自动计算出的 cost。要取消 cost 设置，可以用这个命令的 no 模式。

【命令格式】ip ospf cost <1-65535>

no ip ospf cost

【参数说明】cost <1-65535>指定某个端口的 metric。

【缺省状态】cost 由计算决定。

【命令模式】interface 模式。

【使用指导】当未手工设置 cost 值时，cost 值由计算得出。

【配置实例】下面的例子里把一个端口的 cost 设为 2。

```
create vlan v1
interface v1
ip ospf cost 2
exit
```

ip ospf dead-interval

【命令作用】用来定义一个时间间隔，如果在这段时间内没有收到某个邻居路由器的 Hello 包，就认为这个邻居已经消失了。使用它的 no 模式，可以恢复到缺省设置。

【命令格式】ip ospf dead-interval <1-65535>

no ip ospf dead-interval

【参数说明】dead-interval <1-65535>以秒为单位定义的时间间隔。

【缺省状态】40 秒

【命令模式】interface 模式

【使用指导】这个值会在 Hello 包中发送。而且在网段中的所有路由器必须一致，否则它们之间将无法建立邻居关系。

【配置实例】设置 OSPF dead-interval 为 60 秒。

```
create vlan v1
interface v1
ip ospf dead-interval 60
```

```
exit
```

ip ospf hello-interval

【命令作用】用这个命令来指定 OSPF 发送 Hello 包的时间间隔（以秒为单位）。

【命令格式】ip ospf hello-interval <1-65535>

no ip ospf hello-interval

【参数说明】Hello-interval <1-65535>指定 OSPF 发送 Hello 包的时间间隔（以秒为单位）。要恢复到缺省值，可以使用它的 no 模式。

【缺省状态】10 秒

【命令模式】interface 模式

【使用指导】在整个网段中的所有路由器的 hello 间隔必须一致，否则它们之间将无法建立邻居关系。这个值越小，网络结构的变化将越快被检测到，但是 OSPF 的 Hello 包也会占用更多的带宽。

【配置实例】把端口 v1 的 ospf hello-interval 设置为 15 秒：

```
create vlan v1
interface v1
ip ospf hello-interval 15
exit
```

ip ospf message-digest-key

【命令作用】为了使能（enable）OSPF 的 MD5 认证，需要用这个命令来配置 MD5 密码。使用它的 no 模式，可以取消一个 MD5 密码设置。

【命令格式】ip ospf message-digest-key <1-255> md5 <KEY>

no ip ospf message-digest-key <1-255>

【参数说明】<1-255>是密码的 ID。<KEY>是密码。有效字节是 16 个字节，超过的部分会被忽略。

【缺省状态】未配置。

【命令模式】interface 模式。

【使用指导】在 CISCO 的路由器里，key ID 是用来在几个密码之间进行过渡而用的，（它的文档说，会为每一个 key ID 发出一个包）但我们只用最新的 key 为发出的包签名。

我们目前的实现和协议的规定基本一致，在填写认证域时，选用最新配置的 key ID 的 key 进行签名。

【配置实例】

```
create vlan v2
```

```
interface v2
ip ospf message-digest-key 1 md5 testpass
exit
```

【相关命令】area authentication

ip ospf mtu-ignore

【命令作用】为了使 OSPF 在交换 DD 报文时忽略接口 MTU 的检查，需要使用这个命令。

使用它的 no 模式，可以取消这个设置。

【命令格式】ip ospf mtu-ignore

no ip ospf mtu-ignore

【缺省状态】未设置

【命令模式】interface 模式

【使用指导】在正常情况下，OSPF 在交换 DD 报文时需要进行接口 MTU 的检查，通过配置这个命令，可以使 OSPF 忽略对接口 MTU 的检查。

【配置实例】

```
create vlan v2
interface v2
ip ospf mtu-ignore
exit
```

ip ospf network

【命令作用】可以使用这个命令配置与缺省网络类型不同的网络类型。使用它的 no 模式，可以回到原来的网络类型。

【命令格式】ip ospf network

[broadcast|non-broadcast|point-to-multipoint|point-to-point]

no ip ospf network

【参数说明】

broadcast	设置网络类型为 broadcast。
non-broadcast	设置网络类型为 NBMA。
point-to-mulpoint	设置网络类型为点对多点。
point-to-point	设置网络类型为点对点。

【缺省状态】依据网络类型。

【命令模式】interface 模式。

【使用指导】使用这个命令，您可以设置 broadcast 网络为 nonbroadcast multi-access(NBMA)网络。

例如在您的网络中某些路由器不支持组播地址。

您同样可以设置 NBMA 网络（如 X.25,Frame Relay 和 SMDS）为 broadcast 网络。这样您就可以不使用 neighbor 命令。

在 NBMA 中，必须使用 neighbor 命令才能建立邻居关系。

【相关命令】neighbor(OSPF)。

frame-relay map。

ip ospf priority

【命令作用】用这个命令来设置 OSPF 的路由器优先级。这个优先级会在网络中选举 DR（designated router）时发生作用。要取消 priority 的设置，可以使用它的 no 模式。

【命令格式】ip ospf priority <0-255>

no ip ospf priority

【参数说明】priority <0-255>优先级，从 0 到 255。

【缺省状态】priority 值为 1

【命令模式】interface 模式。

【命令指导】当同一网段有两台路由器同时试图成为 DR 时，priority 较大的会竞选成功。如果它们的 priority 一样，具有较大的 Router ID 的会成为 DR。如果一台路由器的 priority 为 0，它就不会参与 DR 的竞选。

【配置实例】这个命令设置端口 0 的 priority 为 3。

```
create vlan v1
interface v1
ip ospf priority 3
exit
```

ip ospf retransmit-interval

【命令作用】用这个命令来设置两次 LSA 重传间的时间间隔。要恢复到缺省值，可以使用它的 no 模式。

【命令格式】ip ospf retransmit-interval <3-65535>

no ip ospf retransmit-interval

【参数说明】retransmit-interval <3-65535>两次 LSA 重传间的时间间隔。

【缺省状态】缺省值是 5 秒。

【命令模式】interface 模式

【使用指导】当一台路由器向它的邻居发送 LSA 时，会保留这个 LSA 直到收到对

应的 LS ACK 为止。如果过了 retransmit-interval，还没有收到回应，它会重传这个 LSA。如果这个值被设得很小，将引起不必要的重传。在 virtual link 上，可以把它设置的长一些。

【配置实例】下面的例子里把 v1 端口的 retransmit-interval 设为 10 秒。

```
create vlan v1
interface v1
ip ospf retransmit-interval 10
exit
```

ip ospf transmit-delay

【命令作用】路由器发送一个 LSA 时，要把它的 age 增加一个值，用来标志这个 LSA 已经存在的时间，这个值称为 transmit-delay。用户可以指定 transmit-delay 的大小。要恢复到缺省值，可以使用它的 no 模式。

【命令格式】ip ospf transmit-delay <1-65535>

no ip ospf transmit-delay

【命令参数】transmit-delay <1-65535>指定 transmit-delay，单位是秒。

【缺省状态】1 秒

【命令模式】interface 模式

【使用指导】通常在很慢的链路上才有必要设置这个值，一般情况可以不配置。

【配置实例】下面把 v1 端口的 transmit-delay 设置成 5 秒。

```
create vlan v1
interface v1
ip ospf transmit-delay 5
exit
```

network area

【命令作用】用这个命令可以定义在哪些端口上运行 OSPF，以及这些端口所属 area 的 ID。要取消这个配置，可以使用这个命令的 no 模式。

【命令格式】network <A.B.C.D/M> area [<A.B.C.D>|<0-4294967295>]

no network <A.B.C.D/M> area [<A.B.C.D>|<0-4294967295>]

【参数说明】<A.B.C.D/M>定义执行 OSPF 的网段地址。M 表示掩码长度。

[<A.B.C.D>|<0-4294967295>]设置 area ID。支持 IP 地址模式和数字模式。

【缺省状态】未设置。

【命令模式】router ospf

【使用指导】如果一个端口的地址属于 network 命令定义的网段，就会被加入 area 命令指定的 area 中。使用地址和掩码，可以用一条命令把多个端口加入某个 area。如果几个 network 命令定义的网段是可以互相覆盖的（或者说有交集），那么一个端口会加入最长匹配的 network 命令指定的 area(这与 cisco 的实现有所区别)。

【配置实例】在下面的例子里设置了两个 area，分别是 area 0 和 area 1。

```
router ospf
network 11.0.0.0/24 area 1
network 12.0.0.0/24 area 0
exit
```

passive-interface

【命令作用】用这个命令可以禁止在某些端口上发送 hello 报文。要取消这个配置，可以使用这个命令的 no 模式。

【命令格式】passive-interface <IFNAME>

no passive-interface <IFNAME>

【参数说明】<IFNAME>指定端口，禁止通过这个端口的 OSPF 通讯。

【缺省状态】未设置

【命令模式】router ospf

【使用指导】如果某个端口刚好被包含在 OSPF 的网段内，但是又不想让它和对端建立连接，可以使用这个命令。 如果因为安全的考虑，可以用这个命令来防止对端学习本机的路由，实际通讯的选路可以用静态路由来代替。这个命令的配置会把 OSPF 域分割开来。另外可以将连接 stub network 的 OSPF 接口设为 passive-interface，使 hello 报文不扩散到 stub network，从而减少不必要的流量负载。

【配置实例】

```
router ospf
passive-interface v1
exit
```

redistribute

【命令作用】这个命令让 ospf 重分布从其它协议得到的路由。只有选中到 fib 表中的路由才能被 ospf 重分布。选中的路由在路由表中用一个 >* 号标明。要取消重分布配置，可以使用这个命令的 no 模式。

【命令格式】redistribute [connected|static|rip] {type <1-2>}*1

{[metric] <0-16777214>}*1 {[route-map] <WORD>}*1

no redistribute [connected|static|rip]

【参数说明】connected|static|rip 指定转发路由的来源。分别表示直连路由、静态路由、和 rip 路由。

metric <0-16777214>因为各路由协议之间的 metric 不能通用，所以用这个参数指定转发路由时设置的 metric。

Type <1-2>指定被转发的路由的路径类型。

[route-map] <WORD>指定一个 route-map，用它对转发的路由进行过滤。

【缺省状态】metric 为 20，type 为 type 2。

【命令模式】router ospf。

【配置实例】让 ospf 转发静态路由。

```
router ospf
redistribute static
exit
```

router-id

【命令作用】设置路由器的 router ID。

【命令格式】router-id <A.B.C.D>

no router-id

【参数说明】<A.B.C.D>用 IP 地址格式指定 router ID。要取消这个配置，可以使用这个命令的 no 模式。

【缺省状态】未设置

【命令模式】router ospf

【命令指导】router ID 是用来在网络上标识一台路由器的，所以在一个 AS 内部不能重复。要让设置好的 router ID 生效，必须保存配置并重启交换机。

【配置实例】指定设备的 router ID 为 10.0.0.1

```
router ospf
router-id 10.0.0.1
exit
```

router ospf

【命令作用】这个命令可以启动 OSPF 模块，并进入 OSPF 的配置模式。 如果 OSPF 已经启动，就直接进入 OSPF 配置模式。使用它的 no 模式，可以终止和 OSPF 相关的服务。

【命令格式】router ospf

no router ospf

【缺省状态】未设置

【命令模式】配置模式

【配置实例】用本命令进入 OSPF 配置模式

```
router ospf
exit
```

show ip ospf

【命令作用】显示 OSPF 的各种基本信息。

【命令格式】show ip ospf

【命令模式】配置模式。

【配置实例】

```
Harbour(config)#show ip ospf
OSPF Routing Process, Router ID: 12.0.0.2
Supports only single ToS (ToS0) routes
This implementation conforms to RFC2328
RFC1583Compatibility flag is disabled
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Refresh timer 10 secs
This router is an ASBR (injecting external routing information)
Number of external LSA 0
Number of areas attached to this router: 2

（下面这段是对某个 area 的描述。）
Area ID: 0.0.0.1
Shortcutting mode: Default, S-bit consensus: ok
Number of interfaces in this area: Total: 1, Active: 1
Number of fully adjacent neighbors in this area: 0
Area has no authentication
Number of full virtual adjacencies going through this area: 0
SPF algorithm executed 3 times
Number of LSA 1
```

show ip ospf database

【命令作用】这个命令会显示 OSPF 数据库的内容，有许多不同的选项。

【命令格式】show ip ospf database

show ip ospf database [asbr-summary|external|max-age

|network|router|self-originate|summary] [<A.B.C.D>]

{adv-router <A.B.C.D>}*1

【参数说明】如果不加任何参数，将分类显示数据库中各种 lsa 的概要信息。

[asbr-summary|external| network|router|summary]

<A.B.C.D>可选。显示指定类型的 LSA 的内容。IP 用来指定 LSA 的 link state id。

[self-originate] 可选。显示本机产生的 LSA。

Adv-router <A.B.C.D>可选，显示指定路由器产生的 LSA。IP 用来指定路由器的 router ID。

【缺省状态】未设置

【命令模式】interface 模式

【配置实例】

```
Harbour(config)#show ip ospf database

OSPF Router with ID (12.0.0.2)
Router Link States (Area 0.0.0.1)
Link ID      ADV Router      Age Seq#    CkSum  Link count
12.0.0.2       12.0.0.2        122 0x80000004 0xa379 1
……

Harbour(config)#show ip ospf database router
OSPF Router with ID (12.0.0.2)
Router Link States (Area 0.0.0.1)
LS age: 75
     Options: 2
     Flags: 0x2 : ASBR
     LS Type: router-LSA
     Link State ID: 12.0.0.2
     Advertising Router: 12.0.0.2
LS Seq Number: 80000004
     Checksum: 0xa379
     Length: 36
     Number of Links: 1
     Link connected to: Stub Network
     (Link ID) Network/subnet number: 11.0.0.0
     (Link Data) Network Mask: 255.255.255.0
     Number of ToS metrics: 0
     ToS 0 Metric: 10
```

show ip ospf interface

【命令作用】用来显示运行 OSPF 的端口的信息。

【命令格式】show ip ospf interface {<INTERFACE>}*1

【参数说明】<INTERFACE>可选，用来指定端口名。如果不输入，会显示所有端口的信息。

【缺省状态】未设置

【命令模式】配置模式

【配置实例】下面显示了端口 v1 的信息

```
Harbour(config)#show ip ospf interface v1
```

```
v1 is up, line protocol is up
Internet Address 11.0.0.2/24, Area 0.0.0.1
Router ID 12.0.0.2, Network Type BROADCAST, Cost： 10
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 12.0.0.2, Interface Address 11.0.0.2
No backup designated router on this network
Timer interval configure, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00：00：10
Neighbor Count is 0, Adjacent neighbor count is 0
```

show ip ospf neighbor

【命令作用】这个命令可以显示 OSPF 邻居的信息。

【命令格式】show ip ospf neighbor [<A.B.C.D>]

show ip ospf neighbor detail

【参数说明】<A.B.C.D>用 router ID 来指定邻居。

Detail 显示详细信息。

【命令模式】配置模式。

【配置实例】下面是不加参数的例子：

```
Harbour(config)#show ip ospf neighbor

Neighbor ID  Pri State  Dead Time   Address    Interface   RXmtL RqstL DBsmL
192.168.0.100 1   Full/Backup  00：00：36 11.0.0.1   v1     0     0     0
```

下面是查看某个 neighbor 的细节例子：

```
Harbour(config)#show ip ospf neighbor detail

Neighbor 192.168.0.100, interface address 11.0.0.1
In the area 0.0.0.1 via interface v1
Neighbor priority is 1, State is 2-Way, 2 state changes
DR is 0.0.0.0, BDR is 0.0.0.0
Options 2 *|*|-|-|-|-|E|*
Dead timer due in 00：00：30
Database Summary List 0
Link State Request List 0
Link State Retransmission List 0
Thread Inactivity Timer on
Thread Database Description Retransmision off
Thread Link State Request Retransmission off
Thread Link State Update Retransmission off
```

timers lsa-group-pacing

【命令作用】运行 OSPF 应该每隔 1800 秒刷新一次已有的 LSA，如果两个 LSA 的重发时间很接近，它们将同时被发送，这样可以减少网络上传输的 LS update 包的数量。一般地，这个“比较接近”的时间被设定为 refresh timer。要取消这个配置，可以使用这个命令的 no 模式。

【命令格式】timers lsa-group-pacing <10-1800>

no timers lsa-group-pacing

【参数说明】<10-1800>设置相邻的两次 LSA 刷新的时间间隔。如果两个 LSA 的刷新时间比这个时间短，它们将同时被发送。

【缺省状态】10 秒

【命令模式】router ospf

【使用指导】如果 area 内的 LSA 很少，可以把这个时间设的大一些，进一步减少 OSPF 协议对带宽的占用。

【配置实例】把时间间隔设置为 20 秒。

```
router ospf
timers lsa-group-pacing 20
exit
```

timers spf

【命令作用】使用命令 timers spf，管理员可以设置 spf-delay 和 spf-holdtime 值。要恢复到缺省设置，可以使用它的 no 模式

【命令格式】timers spf <0-65535> <0-65535>

no timers spf

【参数说明】spf-delay 从 OSPF 检测到网络结构的改变，到开始计算最短路径树的时间间隔，单位是秒。

Spf-holdtime 两次 SPF 计算之间的最短时间间隔。

【缺省状态】spf-delay 为 5 秒，spf-holdtime 为 10 秒。

【命令模式】router ospf

【使用指导】OSPF 检测到网络结构的改变后，要经过一个延时才计算最短路径树（SPF tree），这样可以避免因为一些网络抖动而重复计算。另外，在两次路径计算之间，也会有一个最短的间隔，也就是说，一次计算之后，必须要过一定的时间才会进行下一次计算（SPF caculate）。这个命令是为了避免路由计算受到网络抖动的影响，缺省值可以适应大多数的情况。在网络稳定时，路由器不会计算 SPF，所以把时间间隔设置得很长

并不能减少平时的 CPU 时间消耗。

【配置实例】设置这两个值分别为 10 秒和 20 秒。

```
router ospf
timers spf 10 20
exit
```

17.4 路由策略

17.4.1 路由策略配置向导

所谓路由策略，实际上是一种对路由协议收发、引入的路由进行人为干涉的手段，使网络管理员可以在必要时调整、控制特定路由信息。干涉的方式主要是对路由信息做过滤，接受某些路由，拒绝另一些路由。有的手段（routemap）也可以对路由的属性做修改，如人为设置某些路由的下一跳，metric 等。

路由策略属于路由配置工作中的高级内容，只在必要时才使用。由于它是对路由协议的工作进行人为干涉，应该由有经验的网络管理员设计、实施，以免造成网络路由方面的故障。

使用路由策略通常要先定义路由过滤规则，可以使用的方式有访问列表、前缀列表和路由映像。定义过滤规则之后，再把规则应用到路由协议的多种处理环节，从而达到控制路由处理过程的作用。

访问列表（access-list）描述一个 IP 地址范围是否可接受，用于 IP 地址的过滤。用户可以指定多个 IP 地址及掩码，并指定接受或拒绝。在本系统中，IP 类型的访问列表（access-list ip）用于防火墙的报文过滤，而路由型访问列表（access-list route）用于路由策略。访问列表规定了一个地址前缀，对匹配它的 IP 地址做判断。在一个访问列表中没有匹配任何地址范围的地址将被当作被拒绝。

地址前缀形如“10.1.0.0/16”。它可以匹配 10.1.1.1、10.1.23.32 等地址，不能匹配 11.1.1.1 等地址。

前缀列表（prefix-list）用于描述一个 IP 前缀范围是否可接受，用于路由目的地址的过滤。用户可以指定多个 IP 前缀范围，并指定接受或拒绝。前缀列表规定了一个地址前缀的范围，对匹配它的 IP 前缀做判断。

一个 IP 前缀范围形如“10.1.0.0/16，掩码范围为 16-24”。它可以匹配 10.1.0.0/16、10.1.128.0/19、10.1.1.0/24 等前缀，不能匹配 10.1.0.0/8、12.1.0.0/16 等前缀。

路由映像（routemap）是专用于路由策略的一种比较复杂的过滤和处理工具。每个 routemap 由一组

match 条件和一组 set 命令构成。其中 match 条件可以匹配路由的多种属性，如目的地址、下一跳、metric 等，而 set 命令则可以修改被匹配路由的很多属性。Routemap 本身又分为允许和拒绝两种类型，可以指定是否接受匹配的路由。

下一节列举了路由策略几种规则的配置命令。而它如何应用用到路由协议，路由协议的某个具体处理环节上可以应用什么类型的规则，则在各协议的章节中说明。

17.4.2 路由策略命令参考

access-list route

【命令作用】定义 access-list 访问列表。删除请使用 no 命令。

【命令格式】access-list route <name> <1-65535> [deny| permit] [<A.B.C.D/M> | any]

no access-list route <name> [deny |permit] [<A.B.C.D/M> | any]

no access-list route <name>

【参数说明】

<name>	access-list 名称，字符串或正整数
<1-65535>	access-list 的级别表示，正整数。
deny	拒绝接受匹配的路由信息。
permit	接受匹配的路由信息。
<A.B.C.D/M>	指定匹配的 IP 地址和掩码长度。
any	指定匹配所有的路由。

【命令模式】配置模式

【使用指导】本命令创建或删除访问列表，之后应使用路由协议的相关命令将其应用到所需要路由过滤的环节。

每一个 access-list 可包含多个元素，它们在 ACL 中各种描述语句的放置顺序很重要，因为它的应用是按照描述语句在 ACL 中的顺序，根据各描述语句的判断条件，对数据包进行检查。一旦找到某一匹配条件，就结束比较过程，不再检查以后的其他条件判断语句。

访问列表可以配置多个地址范围，使用相同的访问列表名称多次使用此命令即可。分以下四种情形：

对于不同的访问控制元素，不同级别，执行结果：按优先级别加入；

对于不同的访问控制元素，相同级别，执行结果：替代以前的元素；

对于同一个访问控制元素，相同级别；执行结果：对于访问控制列表没有影响；

对于同一个访问控制元素，不同级别，执行结果：替代以前的级别后，再按优先级别加入。

在每个 access-list 的最后都有一默认匹配项“deny any”，进行相应配置时需引起注意。

【配置实例】对接口 v2 接收的所有的 RIP 路由进行过滤

```
Harbour(config)#access-list route a1 4 deny 10.1.1.1/16
Harbour(config)#access-list route a1 3 deny 12.1.1.1/16
Harbour(config)#access-list route a1 31 deny 14.1.1.1/16
Harbour(config)#access-list route a1 32 deny 14.1.1.1/16
Harbour(config)#access-list route a1 32 deny 13.1.1.1/16

查看结果：
Harbour(config)#show access-list route
access-list route a1 3 deny 12.1.1.1/16
access-list route a1 4 deny 10.1.1.1/16
access-list route a1 32 deny 13.1.1.1/16
```

【应用实例】

```
Harbour(config)#router rip
Harbour(config-router)#distribute-list a1 in v1
```

【相关命令】distribute-list

access-list description

access-list route description

【命令作用】为 access-list 配置一段说明文字。

【命令格式】access-list route <name> description <desc>

no access-list route <name> description

【参数说明】<name>　　access-list 名称，字符串。

<desc>　　注释字符串。

【命令模式】配置模式。

【配置实例】

```
Harbour(config)#access-list route a1 10 deny any
Harbour(config)#access-list route a1 description acc-deny-all
```

show access-list route

【命令作用】显示路由类型的访问列表配置信息。

【命令格式】show access-list route

【命令模式】配置模式

【使用指导】显示所有访问列表的配置信息。

【配置实例】在如下命令中，显示所有用于路由过滤的访问列表：

```
Harbour(config)#show access-list route
```

ip prefix-list

【命令作用】配置前缀列表。删除前缀列表请使用 no 命令。

【命令格式】{no} ip prefix-list <name> {seq <seq-no>} [[deny|permit] <A.B.C.D/M>

{ge <masklen1>}{le <masklen2>} | any]

【参数说明】

<name>	前缀列表的名称，字符串。
<seq-no>	前缀列表的序号，1-4294967295，缺省为 5。
deny	拒绝指定的地址范围。
permit	接受指定的地址范围。
<A.B.C.D/M>	要匹配的 IP 地址范围。
masklen1	匹配范围要求掩码长度大于等于此数值，取值为 M+1 至 32。缺省为 M。
masklen2	匹配范围要求掩码长度小于等于此数值，取值为 M+1 至 32。缺省为 32。
any	匹配任何 IP 地址。

【默认状态】无前缀列表。

【命令模式】配置模式

【使用指导】本命令创建或删除前缀列表，之后应使用路由协议的相关命令将其应用到所需要路由过滤的环节。

必要时可以通过 ge 和 le 子句给出前缀的掩码范围，要求 M<masklen1<=masklen2。这时可以匹配成功的前缀掩码范围为：

masklen1 <= 被检验的掩码长度 <= masklen2

没有通过 ge 和 le 子句给出前缀的掩码范围时可以匹配成功的前缀掩码范围为：M <= 被检验的掩码长度 <= 32

前缀列表可以由多个地址段构成。创建时应使用相同的前缀列表名称，但配置不同的序列号。较小序列号的地址段将首先被匹配。序号可不连续。

在进行地址匹配时，如果一个地址匹配上一个地址段时，对于 permit 类型的地址段则通过了过滤，对于 deny 类型则没有通过过滤，这时不会检查后面的地址段。如果地

址不在地址段范围中，则检查按序号下一个地址段。

【配置实例】

```
Harbour(config)#ip prefix-list list1 seq 10 permit 10.0.0.0/8 ge 9 le 24
Harbour(config)#ip prefix-list list1 seq 20 permit 20.0.0.0/8 ge 9 le 16
Harbour(config-route-map)#match as-path list1
```

【相关命令】ip prefix-list description

ip prefix-list description

【命令作用】配置前缀列表的说明文字。

【命令格式】ip prefix-list <name> description <desc>

no ip prefix-list <name> description

【参数说明】<name> 前缀列表的名称，字符串。

<desc> 前缀列表的说明文字，字符串。

【默认状态】无前缀列表说明。

【命令模式】配置模式。

【相关命令】ip prefix-list

ip lan_aggregate <A.B.C.D/M>

【命令作用】将几个相邻的子网聚合成一个更大的子网，从而减少网络路由。由于只有 2K 主机表和 16 条网段表，FlexHammer5010 交换机适合于企业网小网络模式，即路由条目（包括静态、直连和动态学习等所有路由）应该小于或等于 16 条（如果存在默认路由，必须小于或等于 15 条，因为默认路由需要占用 2 条网段表项）；否则会有大量的 L3 交换需要软件路由实现，导致 CPU 负载过重。

对于路由条数大于 16 条时的组网，视其情况可以用 ip lan_aggregate A.B.C.D/Mask 这条命令对路由进行汇聚。

【命令格式】{no}ip lan_aggregate <A.B.C.D/M>

【命令模式】配置模式

【使用指导】<A.B.C.D/M>表示聚合后的子网及其掩码,删除聚合的子网请使用 no 命令

【配置实例】交换机上配有 192.168.1.0/24 、192.168.2.0/24 和 192.168.3.0/24 三个子网，执行 ip lan_aggreagte 192.168.0.0/16 将上述两条存在于 def 表中的路由聚合为一条，从而起到减少路由数的目的，满足组网要求。

match interface

【命令作用】配置 route-map 中的接口名匹配条件。

【命令格式】match interface <IFNAME>

no match interface <IFNAME>

【参数说明】<IFNAME>： 接口名

【默认状态】无匹配条件。

【命令模式】route-map 配置模式

【使用指导】在 route-map 匹配过程中，符合至少一个 match 条件的路由将被加以指定的 set 操作。不匹配的路由将被忽略。

Match 过程是按 route-map 序号和 match 条件的顺序有顺序执行的。

【配置实例】在如下例子中，将路由的 next hop 地址是否为接口 v1 作为匹配条件：

```
Harbour(config)#route-map map1 permit 1
Harbour(config)#create vlan v1
Harbour(config-route-map)#match interface v1
```

match ip next-hop

【命令作用】配置 route-map 中的下一跳地址匹配条件，比较下一跳地址是否与 match 命令指定的 access-list 指定网段匹配。

【命令格式】match ip next-hop <ACLName>

no match ip next-hop <ACLName>

【参数说明】<ACLName>：access-list 名字

【默认状态】无匹配条件。

【命令模式】route-map 配置模式

【使用指导】在 route-map 匹配过程中，符合至少一个 match 条件的路由将被加以指定的 set 操作。不匹配的路由将被忽略。

Match 过程是按 route-map 序号和 match 条件的顺序有顺序执行的。

【配置实例】在如下例子中，将路由的 next-hop 地址是否在网段 66.0.0.0/9 作为匹配条件

```
Harbour(config)#access-list a1 permit 66.0.0.0/9
Harbour(config)#route-map map1 permit 1
Harbour(config-route-map)#match ip next-hop a1
```

match ip address

【命令作用】配置 route-map 中的目的地址匹配条件，比较目的地址是否与 match 命令指定的 access-list 指定网段匹配。

【命令格式】match ip address <ACLName>

no match ip address <ACLName>

【参数说明】<ACLName>：access-list 名字

【默认状态】无匹配条件。

【命令模式】route-map 配置模式

【使用指导】在 route-map 匹配过程中，符合至少一个 match 条件的路由将被加以指定的 set 操作。不匹配的路由将被忽略。

Match 过程是按 route-map 序号和 match 条件的顺序有顺序执行的。

【配置实例】在如下例子中，将路由目的地址是否在网段 66.0.0.0/9 作为匹配条件：

```
Harbour(config)#access-list a1 permit 66.0.0.0/9
Harbour(config)#route-map map1 permit 1
Harbour(config-route-map)#match ip address a1
```

match ip address prefix-list

【命令作用】配置 route-map 中的目的地址匹配条件，比较目的地址是否与 match 命令指定的 prefix-list 指定的网段匹配。

【命令格式】match ip address prefix-list <PrefixListName>

no match ip address prefix-list <PrefixListName>

【参数说明】<PrefixListName>：prefix-list 名字

【默认状态】无匹配条件。

【命令模式】route-map 配置模式

【使用指导】在 route-map 匹配过程中，符合至少一个 match 条件的路由将被加以指定的 set 操作。不匹配的路由将被忽略。

Match 过程是按 route-map 序号和 match 条件的顺序有顺序执行的。

【配置实例】在如下例子中，将路由目的地址是否在网段 66.0.0.0/9 作为匹配条件：

```
Harbour(config)#ip prefix-list f1 permit 66.0.0.0/9
Harbour(config)#route-map map1 permit 1
Harbour(config-route-map)#match ip address f1
```

match metric

【命令作用】配置 route-map 中的 metric 匹配条件。

【命令格式】match metric <0-4294967295>

no match metric <0-4294967295>

【参数说明】<0-4294967295>：路由 metric 值

【默认状态】无匹配条件。

【命令模式】route-map 配置模式

【使用指导】在 route-map 匹配过程中，符合至少一个 match 条件的路由将被加以指定的 set 操作。不匹配的路由将被忽略。

Match 过程是按 route-map 序号和 match 条件的顺序有顺序执行的。

【配置实例】在如下命令中，将路由的 metric 值是否为 1 作为匹配条件

```
Harbour(config)#route-map map1 permit 1
Harbour(config-route-map)#match metric 1
```

route-map

【命令作用】创建 route-map 或进入已有 route-map 的配置模式

【命令格式】route-map <name> [deny|permit] <1-65535>

no route-map <name>

no route-map <name> [deny|permit] <1-65535>

【参数说明】<name>：指定 route map 名称。

deny：若 match 匹配，则过滤不通过，将不对指定的路由进行操作。

permit： 若有 match 匹配，则过滤通过，对指定路由将在 set 命令处理后进行操作。否则将忽略路由。默认为 permit。

<1-65535>： 该 route-map 命令的序列号。一般将按照序列号从小到大的顺序执行 route-map 命令。

【默认状态】无 route-map

【命令模式】配置模式

【使用指导】创建 route-map 之后，可使用它进行路由的过滤和更改。Route-map 命令对路由的过滤进行更细致的控制。可以参考下面的例子了解如何配置 route-map。

每个 route-map 命令都包含一个 match 和 set 命令列表。其中 match 命令指定引入路由的匹配条件。Set 命令指定条件匹配时引入路由所进行的操作。

Match 命令有多种格式。相关的 match 命令请参考前面的描述。Match 命令的顺序可

以任意，但所有 match 都必须参与匹配。

一个 route-map 包含多个命令。没有发生任何匹配的路由将被忽略，即这样的路由将被拒绝。如果只是要修改路由的某些值，则应该在第二条 route-map 命令中定义一个准确的 match 命令。

【配置实例】这个例子定义一个 route-map，命名为 r1。将目的地址与 a1 匹配的路由的下一跳地址设置为 192.168.0.176。并将 r1 应用于 RIP 引入的静态路由。

```
Harbour(config)#access-list a1 permit 66.0.0.0/8
Harbour(config)#route-map r1 permit 1
Harbour(config-route-map)#match ip address a1
Harbour(config-route-map)#set ip next-hop 192.168.0.176
Harbour(config)#router rip
Harbour(config-router)#redistribute static route-map r1
```

set ip next-hop

【命令作用】配置 route-map 中的路由下一跳地址。

【命令格式】set ip next-hop <A.B.C.D>

no set ip next-hop {<A.B.C.D>}

【参数说明】<A.B.C.D>：IP 地址

【默认状态】无 set 命令，不更改下一跳地址。

【命令模式】Route-map 模式。

【使用指导】route-map 中的这个 set 配置可以修改匹配到路由的下一跳地址。

【配置实例】在如下命令中，引入静态路由，并将此路由发送的 next hop 地址指定为 12.0.0.1：

```
Harbour(config)#ip route 66.0.0.0 9 192.168.0.115
Harbour(config)#access-list route a1 permit 66.0.0.0/9
Harbour(config)#route-map map1 permit 1
Harbour(config-route-map)#match ip address a1
Harbour(config-route-map)#set ip next-hop 12.0.0.1
Harbour(config-route-map)#exit
Harbour(config)#router rip
Harbour(config-router)#redistribute static route-map r1
```

【相关命令】route-map

set metric

【命令作用】配置 route-map 中的路由 metric 值。

【命令格式】set metric <0-4294967295>

no set metric {<0-4294967295>}

【参数说明】<0-4294967295>：路由 metric 值

【默认状态】无 set 命令，不更改路由 metric 值。

【命令模式】Route-map 模式。

【使用指导】参考 route-map

【配置实例】在如下命令中，为 RIP 引入静态路由，并将路由发送 metric 值指定为 10：

```
Harbour(config)#ip route 66.0.0.0/8 192.168.0.115
Harbour(config)#access-list a1 permit 66.0.0.0/8
Harbour(config)#route-map r1 permit 1
Harbour(config-route-map)#match ip address a1
Harbour(config-route-map)#set metric 10
Harbour(config-route-map)#exit
Harbour(config)#router rip
Harbour(config-router)#redistribute static route-map r1
```

【相关命令】route-map

set metric-type

【命令作用】路由调整命令。改变 OSPF 外部路由 metric 类型。

【命令格式】set metric-type [type-1|type-2]

no set metric-type {[type-1|type-2]}

【参数说明】type-1：路由 metric 类型 1。

type-2：路由 metric 类型 2。

【默认状态】无 set 命令，不更改路由类型。

【命令模式】Route-map 模式。

【使用指导】在 OSPF 协议中，类型 1 的外部 metric 是由 OSPF 接口开销累加得到的。而类型 2 的外部 metric 描述 AS 外部路由 metric，与类型 1 的 metric 不可做数值比较，并且认为所有类型 2 的 metric 都大于类型 1 的 metric。

【配置实例】Harbour(config-route-map)#set metric-type type-1

【相关命令】route-map

show ip lan_aggregate

【命令作用】显示所有聚合的子网

【命令格式】`show ip lan_aggregate`

【命令模式】只读模式或者配置模式

show ip prefix-list

【命令作用】显示前缀列表的配置信息。

【命令格式】show ip prefix-list

show ip prefix-list [<name>|all] <A.B.C.D/M>

show ip prefix-list [<name>|all] seq <1-4294967295>

show ip prefix-list [<name>|all] {[detail | summary]}

【参数说明】

<name>：	前缀列表名称。
all：	代表所有前缀列表。
<A.B.C.D/M>：	前缀地址。
<1-4294967295>：	同一个前缀列表中多个地址段的序列号。
detail：	显示详细信息，包括使用情况统计等。
summary：	显示简要信息，缺省只显示简要信息。

【命令模式】配置模式

【使用指导】不指定前缀列表名称时将显示所有前缀列表的配置信息。

【配置实例】在如下命令中，显示所有前缀列表：

```
Harbour(config)#show ip prefix-list
```

【相关命令】ip prefix-list

show route-map

【命令作用】显示 route-map 的配置信息。

【命令格式】show route-map {<name>}

【参数说明】<name>可选，指定 route map 名。

【命令模式】配置模式

【使用指导】不指定 route-map 名称时将显示所有 route-map 的配置信息。

【配置实例】在如下命令中，显示所有 route-map：

```
Harbour(config)#show route-map
```

config ip route blackhole

【命令作用】黑洞路由是系统把去往某个IP地址的包在硬件中丢弃的一种自动保护机制，使CPU不

受大流量冲击的作用。此命令是用来配置黑洞路由的老化时间

【命令格式】config ip route blackhole timeout <0-1200>

【参数说明】<0-1200>表示老化时间，缺省值为 300 秒。

【命令模式】配置模式

show ip route blackhole

【命令作用】此命令显示了系统中当前黑洞路由信息。

【命令格式】show ip route blackhole

【命令模式】配置模式

第18章 组播路由协议

本章包括如下内容：

组播路由概述

IGMP V2 协议配置指导及命令说明

PIM-SM V2 协议配置指导及命令说明

PIM-DM V2 协议配置指导及命令说明

阅读本章内容前，假定您对 IP 组播路由内容已经熟悉，如果不熟悉，请参阅下面的资料：

RFC 1112 —— Internet Group Management Protocol（IGMP）, Version 1

RFC 2236 —— Internet Group Management Protocol（IGMP）, Version 2

RFC 2362 —— Protocol Independent Multicast-Sparse Mode (PIM-SM) , Version 2

Draft PIM-DM-new —— Protocol Independent Multicast-Dense Mode (PIM-DM) Version 2

本章内容在 FlexHammer5010 上支持，在 FlexHammer5610/5610T 交换机上不支持。

18.1 三层组播

18.1.1 三层组播概述

IP 通讯通常使用单播方式，即 IP 报文的目的地址是一个单播 IP 地址，它说明了应接收这个报文的设备的地址。每个报文只会有唯一的接收者。

在局部网段上，偶尔也使用 IP 广播地址，它的目的地址为 255.255.255.255。在网段内的所有 IP 设备都要接收这个报文。为了避免广播风暴，通常路由器或交换机不会把这个广播报文转发到其它网段。

IP 组播是一种点到多点的通信方式。IP 组播报文的目的地址是一个 D 类 IPv4 地址(即 224.0.0.0 至 239.255.255.255)。它实际上已经不是某个设备的 IP 地址，而是表示一个组。其中 224.0.0.*/24 和 239.0.0.*/24 这两个段一般是被协议保留，不能用于用户数据通讯。

组播报文进入支持三层组播的网络时，将被转发到所有需要接收这个组的设备上。接收者的数量可以是任意多个。网络设备只在必要的网络节点上才复制组播报文，从而以最小的带宽占用将组播报文发送到所有目的地。IP 组播在节省通信带宽、降低服务器和网络负载等方面较单播有许多优越性。

HammerOS 目前支持 IGMP 协议和 PIM-SM 协议，二者配合可以有效支持 IP 组播应用。其中 IGMP 协议用于获得某个网段上是否有终端设备需要接收某个组的报文，而 PIM-SM 协议则用于在网络上计算组播路由，建立组播转发路径。

IP 组播又称为三层组播，以区别与二层组播功能。通常交换机做二层转发时，对于目的 MAC 地址为组播地址的帧只能采用广播方法，将它们转发到所有端口。某些交换机支持二层组播功能，主要是在二层转发的过程中，通过 IGMP-SNOOPING 等手段获得 IP 组播的某些信息，用有选择的转发代替二层广播，达到优化的目的。由于 IGMP 本身是三层协议，所以这里对 IGMP 使用称为侦听（SNOOPING）。二层组播只能应用在终端设备和三层设备之间的二层设备上，适用范围很有限。

三层组播与二层组播的主要区别在于它使用 IP 组播路由协议，从而可以在跨越多个三层设备，在多个网段之间选择组播转发路由，控制组播数据有效地转发到需要数据的网段，避免转发到不需要的网段，并可以抑制数据重复转发到一个网段上。

三层组播的上层应用通常包括：视频点播、视频会议、远程教学、电子白板、数据公告（如股市行情）等。

18.1.2 基本命令参考

clear ip mroute

【命令作用】删除组播路由表。

【命令原型】clear ip mroute {<group> {<source>}}

【参数说明】<group>　　组地址，点分形式。

<source>　　源地址，点分形式。

【命令模式】配置模式

【使用指导】无参数时表示删除整个组播路由表，将停止所有组播路由转发。

只输入组地址时，表示删除所有组地址为 G 的组播路由项，停止对相关组的组播转发。

输入组地址和源地址时，表示删除一个(S,G)路由。

在协议的作用下，可能很快路由将得到恢复。

【配置实例】

```
Harbour(config)# clear ip mroute 224.1.1.1 100.1.0.1
Harbour(config)# clear ip mroute
```

【相关命令】show ip mroute

ip multicast-routing

【命令作用】启动或停止三层组播转发功能。

【命令原型】{no} ip multicast-routing

【默认状态】不启动三层组播转发功能。

【命令模式】配置模式

【使用指导】在启动组播路由协议或 IGMP 协议之前，要先通过这个命令启动组播转发功能。

No 命令用于停止组播路由协议。

【相关命令】ip pim sparse-mode

ip pim dense-mode

show ip mroute

【命令作用】显示组播路由表。

【命令原型】show ip mroute {<group>| summary}

【参数说明】<group> 组播的组地址，D 类的 IP 地址

summary 按种类统计路由数量

【命令模式】配置模式

【使用指导】此命令可显示组播路由表的内容。组播路由是组播路由协议和 IGMP 协议运行的结果，用于指示组播报文的转发。

不带参数则显示所有的组播路由项和按种类统计路由数量；输入参数<group>则显示特定组的(*,G)和(S,G)路由；输入参数 summary 则按种类统计路由数量。

show ip rpf

【命令作用】显示到指定组播源的反向路径转发信息。

【命令原型】show ip rpf <A.B.C.D>

【参数说明】<A.B.C.D>反向路径转发的组播源 IP 地址

【命令模式】配置模式

【使用指导】此命令主要显示指定组播源的反向路径转发（RPF）信息，如 RPF 上游邻居、对应于该源的入接口名称和 IP 地址等。

18.2 IGMP 协议

18.2.1 协议概述

IGMP(Internet Group Management Protocol)的功能是管理组播成员信息。该协议一般运行在组播域中直接与接收者连接的设备上，它动态的建立、维护组播组成员关系，是组播路由体系中的基础协议。

目前常用的 IGMP 协议有两个版本：IGMP v1 和 IGMP v2。本系统在全面实现 IGMP v2 的基础上，考虑到向下兼容性问题，可以接收 IGMP v1 的报文，但不发送 IGMP v1 报文。

IGMP v2 有 3 种主要报文：

Memebership Query：是运行 IGMP 协议的 Internet Group Management Protocol 发送给组播接收者（主机）的，根据报文中组播组地址的不同，分为常规查询和特定组查询。当查询报文中的组播组地址为 0.0.0.0 时，用于确定当前的接口所在的网段上存在哪些组播组的接收者；当组播组地址为特定的合法组播组地址时，用于确定当前接口所在的网段上是否存在该组的接收者。

Memebership Report：是支持 IGMP 协议的主机向组播路由设备汇报网络上存在特定组播组的活动成员时使用的报文。本系统支持两种报告报文：版本 1 和版本 2 的成员报告。

Leave Group：当主机离开一个组播组时，向所有组播路由器发送一个成员离开报文。

IGMP 的容量说明：设备的每个接口上最多可请求组播组的数量为 512。

18.2.2 配置向导

IGMP 配置的步骤是：

在配置模式下启动组播：配置命令为 ip multicast-routing

在相关的接口上启动 IGMP：在接口上启动 IGMP 有两种方式：同时启动 PIM 等组播协议和 IGMP 协议，或只启动 IGMP 协议。对于面向只接收组播数据流的最终用户的接口，可以使用 ip pim <mode> passive 命令配置该接口只运行 IGMP，以减小协议复杂度和增加网络安全性。而 ip pim 命令则在接口上同时启动了 PIM 和 IGMP。

加入组播组：有两种方式：动态和静态加入。动态加入不需配置，通过接收者发送 IGMP Memebership Report 报文实现；静态配置一般是为了保证在特定接口上有一个稳定的流输出，配置方法是在特定接口下使用 ip igmp static-group 命令。

18.2.3 命令参考

clear ip igmp group

【命令作用】清除当前的 IGMP 成员。

【命令原型】clear ip igmp group {<group>|<ifname>}

【参数说明】<group> IGMP 组地址 点分格式(A.B.C.D)

<ifname>接口名称 大小写敏感

【命令模式】配置模式

【使用指导】这个命令将清除动态获得的 IGMP 组成员信息，若要删除静态配置的 IGMP 成员，使用 no ip igmp static-group 命令。

无参数时表示删除所有的 IGMP 成员组。

输入组地址时，表示删除所有组地址为 G 的 IGMP 成员组。

输入接口名称时，表示删除该接口上的所有 IGMP 成员组。

在协议或 IGMP 报文的作用下，IGMP 成员组可能很快将得到恢复。

【配置实例】

```
Harbour(config)# clear ip igmp group
Harbour(config)# clear ip igmp group 225.1.1.100
Harbour(config)# clear ip igmp group vlan1
```

【相关命令】show ip igmp group

ip igmp static-group

debug igmp

【命令作用】打开 IGMP 调试信息开关。

【命令原型】debug igmp [packet|member]

no debug igmp [packet|member|all]

【参数说明】packet 显示 IGMP 报文收发信息。

member 显示 IGMP 组成员变化信息。

all 所有 IGMP 调试信息。

【默认状态】所有调试开关都关闭。

【命令模式】配置模式

【使用指导】有经验的用户可根据需要打开某些调试开关查看协议运行中输出的调试信息，帮助分析协议运行状态，解决网络运行问题。

打开终端监视开关后（monitor on），调试信息将输出到控制台。

No 命令用于取消相关调试设置。

【配置实例】

```
Harbour(config)# debug igmp packet
```

【相关命令】monitor

show debug igmp

ip igmp access-group

【命令作用】用访问列表控制特定组播组的成员报告。

【命令原型】ip igmp access-group <access_list>

no ip igmp access-group

【参数说明】<access_list>　　访问列表的名称

【默认状态】本设备不过滤，即接收所有组播组的成员报告。

【命令模式】接口配置模式。

【使用指导】在组播域的边缘路由设备的特定接口上启动该过滤机制后，会对接收到的 IGMP 成员报告报文进行过滤，以保证接受或不接受特定范围内的组播组成员报告。

No 命令用于清除该过滤策略。

【配置实例】下例中，通过使用访问列表 igmpgrp_acl 使得源 DR 的接口 v2 仅接收组地址范围为 226.0.0.0～226.255.255.255 的组成员报告。

```
Harbour(config)#access-list route igmpgrp_acl 10 permit 226.0.0.0/8
Harbour(config)#create vlan v2
Harbour(config)#interface v2
Harbour(config-if)#ip pim access-group igmpgrp_acl
```

【相关命令】access-list route

ip igmp member-timeout

【命令作用】设置 IGMP 成员超时时间。

【命令原型】ip igmp member-timeout <70-65535>

no ip igmp member-timeout

【参数说明】<70-65535>　　成员超时时间（秒）

【默认状态】成员超时时间缺省为 260 秒。

【命令模式】配置模式

【使用指导】按协议规定，成员超时时间为可靠系数*查询间隔+响应时间，缺省为 2*125+10 秒，

即 260 秒。

注意，查询间隔是可以配置的。当查询时间被修改后，成员超时时间会按这个公式重新计算，可能会不再是原来配置的成员超时时间。

No 命令用于将成员超时时间恢复成默认值。

【配置实例】

```
Harbour(config)# ip igmp member-timeout 300
```

【相关命令】ip igmp querier-timeout

ip igmp query-interval

ip igmp querier-timeout

【命令作用】配置 IGMP 查询者超时时间。

【命令原型】ip igmp querier-timeout <65-6005>

no ip igmp querier-timeout

【参数说明】<65-6005>IGMP 查询者超时时间（秒）。

【默认状态】IGMP 查询者超时时间缺省为 255 秒。

【命令模式】配置模式

【使用指导】IGMP 查询者超时时间用于网段上有多个 IGMP 路由器时，它们之间要竞争由谁发出 IGMP 查询报文。竞争结果的有效时间就是这个查询者超时时间。即非查询者路由器过了这么长时间没有收到查询报文，就会认为查询者已经退出，将再次发出查询报文，并以此竞争查询者。

按协议规定，查询者超时时间为可靠系数*查询间隔+响应时间/2，缺省为 2*125+10/2 秒，即 255 秒。

注意，查询间隔是可以配置的。当查询时间被修改后，查询者超时时间会按这个公式重新计算，可能会不再是原来配置的查询者超时时间。

No 命令用于将 IGMP 查询者超时时间恢复成默认值。

【配置实例】

```
Harbour(config)# ip igmp querier-timeout 200
```

【相关命令】ip igmp member-timeout

ip igmp query-interval

ip igmp query-interval

【命令作用】配置 IGMP 查询间隔。

【命令原型】ip igmp query-interval <30-3000>

no ip igmp query-interval

【参数说明】<30-3000>　　IGMP 查询间隔（秒）。

【默认状态】IGMP 查询间隔缺省为 125 秒。

【命令模式】配置模式

【使用指导】IGMP 查询间隔是协议的一个重要参数，它控制着 IGMP 发出查询的频率，同时也影响其它一些系统时间参数，如成员超时时间=可靠系数*查询间隔+响应时间，查询者超时时间=可靠系数*查询间隔+响应时间/2。

No 命令用于将 IGMP 查询间隔恢复成默认值。

【配置实例】

```
Harbour(config)# ip igmp query-interval 100
```

【相关命令】ip igmp member-timeout

ip igmp querier-timeout

ip igmp static-group

【命令作用】在接口上配置 IGMP 静态成员。

【命令原型】{no} ip igmp static-group <A.B.C.D>

【参数说明】<A.B.C.D>　组地址。

【默认状态】无静态成员。

【命令模式】接口配置模式。

【使用指导】必要时可以在接口上配置静态的 IGMP 成员，它不会超时被删除。

例如需要保证一个稳定的流输出，或用于简便的系统测试。

只有在该网段中充当 DR 的接口上配置的 ip igmp static-group，命令才会生效。

No 命令用于删除该静态成员。

【配置实例】

```
Harbour(config)# create vlan v2
Harbour(config)# interface v2
Harbour(config-if)# ip igmp static-group 224.1.1.1
```

【相关命令】show ip igmp groups

show debug igmp

【命令作用】显示已经打开的 IGMP 调试信息开关。

【命令原型】show debug igmp

【命令模式】配置模式

【使用指导】此命令显示当前打开的 IGMP 调试信息开关的情况。

【相关命令】debug igmp

show ip igmp group

【命令作用】显示 IGMP 当前的组成员信息。

【命令原型】show ip igmp group {interface <ifname>}

【参数说明】<interface>　接口(关键字)。

<ifname>　接口名称。

【命令模式】配置模式

【使用指导】此命令显示内容包括 IGMP 协议收到的组成员加入信息，以及通过静态组成员配置命令加入的成员信息。静态信息无论目前是否生效都可以显示，并说明了当前状态。如果不使用参数，则显示当前的所有 IGMP 成员信息。如果输入接口名称参数，则显示该接口上的当前 IGMP 成员信息。

【配置实例】

```
Harbour(config)# show ip igmp group interface v1
```

显示 v1 接口上通过 igmp 协议收到的组播组信息

【相关命令】ip igmp static-group

show ip igmp timer

【命令作用】显示 IGMP 协议中定时器的默认值和当前值。

【命令原型】show ip igmp timer

【命令模式】配置模式

【使用指导】 IGMP 协议中有三个重要的定时器:IGMP 查询者超时、IGMP 成员超时和 IGMP 查询间隔。此命令显示了三个定时器的默认值、推荐值和当前值，时间单位是秒。

【配置实例】Harbour(config)# show ip igmp group

【相关命令】ip igmp member-timeout

ip igmp querier-timeout

ip igmp query-interval

18.3 PIM-SM 协议

18.3.1 协议概述

组播路由建立了一条沟通数据源和接收者之间的无环数据传输路径；路由项的由两部分组成：匹配条件和接口信息。匹配条件有三种格式：

（S，G）路由　　路由匹配条件为源地址和组地址。

（*，G）路由　　路由匹配条件为组地址。

（*，*，RP）路由　路由匹配条件为集中点(RP)地址。

接口信息包括入接口(iif)和出接口列表(oifs)。所有组播路由协议都使用 RPF(反向路径转发)机制来决定是否转发或者丢弃组播数据包。当组播数据包到达路由设备时，路由器根据数据包的源地址反向查找单播路由表以确定该数据包是否从正确的接口进入的，如果检查成功则转发，检查失败则丢弃。

PIM(Protocol Independent Multicast)协议是一种独立于单播路由协议的组播协议，按照应用场合和处理机制的不同，可以分为密集模式(Dense Mode)和稀疏模式(Sparse Mode)两种。密集模式适合于组播源和接收者物理距离近、数据报文流量大而且持续、接收者密度较大的网络，典型的例子是局域网；稀疏模式适合于组播源和接收者散布在很大地域且带宽有限的网络中，典型的例子如 Internet。

在 PIM-SM 协议中，每个设备可能充当以下几种角色：DR(指定路由器) 、RP(集中点)、BSR(启动消息发出者)。在一个网段上的 PIM 设备将通过竞争产生出 DR 来负责这个网段上的组播数据收发。竞争 DR 的原则是：首先，按照优先级次序，高优先级路由器成功；然后，对于 DR 优先级相同的路由器，将根据协议选择接口 IP 地址最大的作为 DR。RP 是一个组播域中公认的中间节点，是 PIM 网络中共享路径转发树（RPT）的根。对一个特定的组播组 G，必须在整个组播域中映射到同一个 RP。BSR 是一个组播域中 bootstrap 信息的收集和定期发送者，它接受来自候选 RP 的候选通告报文，并定期将它掌握的候选 RP 信息向全网公布。在边界 DR 上，通过运行 IGMP 协议来管理接收者对特定组 G 的加入/退出信息的。

PIM-SM 协议中，通过维护组播域中各个设备上的组播路由表而形成了转发路径树，根据根节点的位置可以将转发树分成两类：以集中点 RP 为根的共享路径树(RPT)和以源 DR 为根的最优树(SPT)。为了优化组播数据包的转发路径，可以在通信流量达到某个阀值后从共享路径转发树切换到以源 DR 为根的转发树。本系统中该切换的流量阈值为 0，即只要有 RPT 数据流到达就会立刻切换到 SPT。PIM-SM v2 协议中的主要协议报文有 7 种，包括：

Hello: 运行 PIM-SM 的接口定期发送 Hello，以便与同网段上的 PIM 设备建立和维持邻居关系；同时通过 PIM 竞争产生本网段的 DR。

Register: 组播源网段内的 DR(简称源 DR)在收到组播服务器发出的组播报文后，将该报文封装在注册(register)报文中，用单播方式发送给对应于该组的 RP。

Register-Stop: 当不需要再用 RPT 转发时，RP 向源 DR 发送一个 Register-stop 报文，告知源 DR 停止发送 register 报文。

Join/Prune: 是从下游路由器发往源或者 RP 方向的报文，用于将一个接口加入到组播路径转发树或将一个接口从组播转发树中剪枝。

Bootstrap: 是 BSR 定期向组播域中其它设备通告候选 RP 时使用的报文。

Assert: 在多介质访问网络(如以太网)中，存在一个以上并列的设备，导致其中一设备的出接口收到组播数据包时，会引发发送断言报文，竞争产生获胜者。

Cand-RP-Adv: 候选 RP 会定期向 BSR 报告其上配置的候选 RP 信息时使用的报文。

PIM-SM 协议的标准过程：起始时，BSR 会在全网上发布候选 RP 信息，以便形成全组播域内的 BSR 地址和 RP 映射的一致。源 DR 将组 G 的组播数据包用 Register 封装，用单播发布给映射到的 RP；接收者会通过 IGMP 协议向 DR 发出对组 G 的加入请求，DR 使用 Join/Prune 报文向 RP 方向发送加入请求，多个接收者对同一个组 G 的加入请求就导致共享路径转发树的建立。RP 收到 Register 报文后，如果有关于该组 G 的组播路由，则拆封 Register 报文，沿路由的出接口发送组播数据包；如果没有关于组 G 的组播路由，则向源 DR 发送 Register-Stop。当组播数据报到达接收者后，如果流量达到阀值(本系统为 0，立即切换)，则启动 RPT 到 SPT 的切换。

PIM-SM 的容量说明：每个 Flex5010 最多可请求组播组的数量为 1024 组；可创建组播路由的最大数量为 2048 条；可交互的邻居最大数量为 128 个。

18.3.2 配置向导

PIM-SM 配置的步骤

启动组播：

(1) 在配置模式下执行命令 ip multicast-routing

(2) 指定集中点（RP）：有两种方式：静态配置；使用 Bootstrap 动态发布。如果使用静态配置，必

须保证整个组播域中各组播设备上 RP 配置的一致性，配置方法是在配置模式下使用 ip pim rp-address 命令。如果使用动态发布的方式，则需要指定 BSR 和候选 RP：在一个组播域中必须保证至少有一个激活的候选 BSR，对每个组播组必须保证至少存在一个可以映射到的 RP。配置方法是选定的设备上，在配置模式下运行 ip pim bsr 和 ip pim rp-candidate 命令。

(3) 在接口上启动组播：有两种方式：同时启动 PIM 等组播协议和 IGMP 协议，或只启动 IGMP 协议。对于面向只接收组播数据流的最终用户的接口，可以使用 ip pim sparse-mode passive 命令配置该接口只运行 IGMP，以减小协议复杂度和增加网络安全性。而 ip pim sparse-mode 命令则在接口上同时启动了 PIM-SM 和 IGMP。

注意事项：

（1）为了配置组播网络，必须先保证单播路由畅通！

（2）由于静态配置 RP 需要整个组播域的一致性，建议使用动态 RP 发布机制。

配置专题 1：动态 RP 发现的配置

PIM-SM 协议支持静态 RP 配置和动态 RP 配置两种模式。由于 RP--组 G 映射关系是 PIM-SM 协议能否正常工作的一个重要前提，为了保证全组播域映射的一致性，建议使用动态 RP 发现。

为了支持动态 RP，组播域中至少需要有一个候选 BSR 和至少一个候选 RP。典型配置如下：

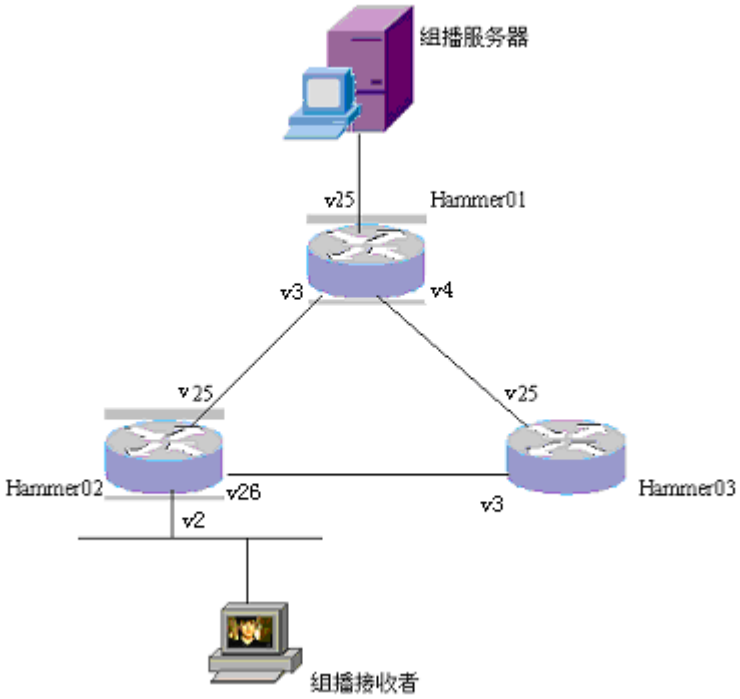
```
Hammer01(config)# create vlan v2
Hammer01(config)# interface v2
Hammer01(config-if)# ip pim sparse-mode
Hammer01(config-if)# exit
Hammer01(config)# interface default
Hammer01(config-if)#ip pim-sparse-mode passive
Hammer01(config-if)# exit
Hammer01(config)# ip pim rp-candidate default group 225.0.0.0/8
Hammer01(config)# ip pim bsr-candidate v2 hash-mask-length 30 priority 20
```

如上配置以后，设备 Hammer01 的 default 接口就成为组播组 225.0.0.0/8 的候选 RP；v2 接口成为该组播域中一个候选 BSR，计算 RP 映射时的掩码长度为 30，在 BSR 选举中优先级为 20。

⚠注意事项：做为候选 RP 和 BSR 的接口只有处于 UP 状态且启动了组播才能生效。接口启动组播的方式有两种：在 interface 模式下视情况运行 ip pim sparse-mode 或 ip pim sparse-mode passive！

配置专题 2：配置实例

单播路由畅通是组播协议正常运行的前提条件，但由于 PIM 协议独立于任何的单播路由协议，在下面的配置例中将不列出单播路由的配置。



如上图，Hammer01 做为组播源 DR 出现，Hammer02 做为目的 DR，Hammer03 的两个接口分别作为候选 RP 和 BSR。由于图中 Hammer02 的接口 v2 并不与其它组播路由器交互，该接口上可以只运行 IGMP 的方式启动组播。

Hammer01 的配置：

```
Hammer01 (config)# ip multicast-routing
Hammer01 (config)# create vlan v25
Hammer01 (config)# interface v25
Hammer01 (config-if)# ip pim sparse-mode
Hammer01 (config-if)# exit
Hammer01 (config)# create vlan v3
Hammer01 (config)# interface v3
Hammer01 (config-if)# ip pim sparse-mode
Hammer01 (config-if)# exit
Hammer01 (config)# create vlan v4
Hammer01 (config)# interface v4
Hammer01 (config-if)# ip pim sparse-mode
Hammer01 (config-if)# exit
```

Hammer02 的配置：

```
Hammer02 (config)# ip multicast-routing
```

```
Hammer02 (config)# create vlan v25
Hammer02 (config)# interface v25
Hammer02 (config-if)# ip pim sparse-mode
Hammer02 (config-if)# exit
Hammer02 (config)# create vlan v26
Hammer02 (config)# interface v26
Hammer02 (config-if)# ip pim sparse-mode
Hammer02 (config-if)# exit
Hammer02 (config)# create vlan v2
Hammer02 (config)# interface v2
Hammer02 (config-if)# ip pim sparse-mode passive
Hammer02 (config-if)# exit
```

Hammer03 的配置：

```
Hammer03 (config)# ip multicast-routing
Hammer03 (config)# create vlan v25
Hammer03 (config)# interface v25
Hammer03 (config-if)# ip pim sparse-mode
Hammer03 (config-if)# exit
Hammer03 (config)# create vlan v3
Hammer03 (config)# interface v3
Hammer03 (config-if)# ip pim sparse-mode
Hammer03 (config-if)# exit
Hammer03 (config)# ip pim bsr-candiate v3
Hammer03 (config)# ip pim rp-candidate v25
```

配置专题 3：路由策略

现在使用访问控制列表对上例进行控制，假设如下的限制条件

使源 DR Hammer01 的 v3、v4 接口仅发布组播组为 225.0.0.0/8、源 IP 为 16.1.1.99 的组播报文；

使 Hammer03 的 v25 不能与 23.0.0.0/8 网段内的路由设备建立邻居关系；

使 Hammer03 的 v3 只接受下游设备对组 225.0.3.15 的加入；

使 Hammer02 的 v2 只接受组 225.0.3.15 的成员报告。

Hammer01 的配置：

```
Hammer01(config)# access-list route sdrgrp_acl 10 permit 225.0.0.0/8
Hammer01(config)# access-list route sdrsrc_acl 10 permit 16.1.1.99/32
Hammer01(config)# create vlan v3
Hammer01(config)# interface v3
Hammer01(config-if)# ip pim source-dr-filter group sdrgrp_acl
Hammer01(config-if)# ip pim source-dr-filter source sdrsrc_acl
Hammer01(config-if)# exit
Hammer01(config)# create vlan v4
Hammer01(config)# interface v4
Hammer01(config-if)# ip pim source-dr-filter group sdrgrp_acl
```

```
Hammer01(config-if)# ip pim source-dr-filter source sdrsrc_acl
Hammer01(config-if)# exit
```

Hammer03 的配置：

```
Hammer03(config)# access-list route neig_acl 10 deny 23.0.0.0/8
Hammer03(config)# access-list route down_acl 10 permit 225.0.3.15/32
Hammer03(config)# create vlan v25
Hammer03(config)# interface v25
Hammer03(config-if)# ip pim neighbor-filter neig_acl
Hammer03(config-if)# exit
Hammer03(config)# create vlan v3
Hammer03(config)# interface v3
Hammer03(config-if)# ip pim downstream-filter down_acl
```

Hammer02 的配置：

```
Hammer02(config)# access-list route igmpgrp_acl 10 permit 225.0.3.15/32
Hammer02(config)# create vlan v2
Hammer02(config)# interface v2
Hammer02(config-if)# ip igmp access-group igmpgrp_acl
Hammer02(config-if)# exit
```

⚠注意事项：路由策略配置后，不能对已有转发行为和路由项产生作用。因此，推荐配置完成后，使用 clear ip mroute 清除已有路由表项，以便设备按照新的策略重新学习。

18.3.3 命令参考

debug pim

【命令作用】打开/关闭 PIM 调试信息开关。

【命令原型】debug pim [packet [hello|register|join-prune|bootstrap|assert|graft|cand-rp

|all|summary] | mroute]

no debug pim [packet [hello|register|join-prune|bootstrap|assert|graft|cand-rp |summary| all] | mroute | all]

【参数说明】

packet	显示 PIM 报文收发信息。
hello	显示 PIM hello 报文收发信息。
register	显示 PIM register 报文收发信息。
join-prune	显示 PIM join-prune 报文收发信息。

bootstrap	显示 PIM bootstrap 报文收发信息。
assert	显示 PIM assert 报文收发信息。
graft	显示 PIM graft/graft-ack 报文收发信息。
cand-rp	显示 PIM cand-rp 报文收发信息。
summary	显示 PIM 收发报文的基本信息
all	显示 PIM 所有报文收发信息。
mroute	显示组播路由表更新信息。
all	显示所有 PIM 调试信息（仅在 no debug pim 中使用）。

【默认状态】所有调试开关都关闭。

【命令模式】配置模式

【使用指导】有经验的用户可根据需要打开某些调试开关查看协议运行中输出的调试信息，帮助分析协议运行状态，解决网络运行问题。打开终端监视开关后（monitor on），调试信息将输出到控制台。No 命令用于取消相关调试设置。

【配置实例】

```
Harbour(config)#debug pim packet join-prune
```

【相关命令】monitor

show debug pim

ip pim bsr-border

【命令作用】配置相应接口为 PIM Bootstrap 消息的边界。

【命令原型】{no} ip pim bsr-border

【默认状态】该接口不作为 PIM Bootstrap 边界，即转发 Bootstrap 消息。

【命令模式】接口配置模式

【使用指导】将一个接口配置为 BSR 边界后，Bootstrap 消息就不能穿过该接口转发，但其它组播报文仍然可以穿越。

No 命令用于取消该设置。

ip pim bsr-candidate

【命令作用】配置本机为候选 BSR。

【命令原型】ip pim bsr-candidate <interface> {hash-mask-length <0-32> priority <0-255>}

no ip pim bsr-candidate

【参数说明】<interface> 选择候选 BSR IP 地址的接口名称 。

<0-32> BSR 计算 RP 映射时的掩码长度，缺省为 0。

<0-255> 候选 BSR 竞争 BSR 的优先级，缺省为 0(最小)。

【默认状态】本设备不作为候选 BSR。

【命令模式】配置模式

【使用指导】BSR（Bootstrap Router）是 PIM 网络中的启动消息（bootstrap）发出者。在 PIM 网络中必须存在一个唯一的 BSR 设备。它接受候选 RP 的消息通告，并发出 bootstrap 把当前的 RP 表通知给域中的所有路由器。

在 PIM 网络中，必须通过这个命令配置至少一个候选 BSR。

No 命令用于取消该设置。

【配置实例】

```
Harbour(config)# ip pim bsr-candidate v2
Harbour(config)# ip pim bsr-candidate v2 hash-mask-length 24 priority 20
```

【相关命令】ip pim rp-candidate

ip pim downstream-filter

【命令作用】用访问列表控制下游设备加入特定组播组。

【命令原型】ip pim downstream-filter <access_list>

no ip pim downstream-filter

【参数说明】<access_list> 访问列表的名称

【默认状态】本设备不过滤，即接受来自下游的所有组播组的加入请求。

【命令模式】接口配置模式

【使用指导】在特定的接口上启动该过滤机制，可以对收到的 PIM Join/Prune 报文中的组播组进行过滤，以确定接受或者拒绝特定范围内的组。

No 命令用于清除该过滤策略。

【配置实例】下例中，通过使用访问列表 down_acl 使得接口 v2 仅接受下游设备对 226.0.0.0～226.255.255.255 范围内组播组的加入。

```
Harbour(config)# access-list route down_acl 10 permit 226.0.0.0/8
Harbour(config)# create vlan v2
Harbour(config)# interface v2
Harbour(config-if)# ip pim downstream-filter down_acl
```

【相关命令】access-list route

ip pim dr-priority

【命令作用】配置接口上的 DR 优先级。

【命令原型】ip pim dr-priority <0-4294967294>

no ip pim dr-priority

【参数说明】<0-4294967294> DR 优先级。

【默认状态】DR 优先级缺省为 0（最小）。

【命令模式】接口配置模式。

【使用指导】一个网段上有多个 PIM 路由器时，通过发送 hello 报文竞争 DR。竞争成功的 DR 将负责这个网段上的用户数据收发。竞争 DR 的原则是：首先按照优先级次序，高优先级路由器成功；对于 DR 优先级相同的路由器，将根据协议选择接口 IP 地址最大的作为 DR。

No 命令用于取消该设置。

【配置实例】

```
Harbour(config)# create vlan v2
Harbour(config)# interface v2
Harbour(config-if)# ip pim dr-priority 100
```

【相关命令】show ip pim interface

ip pim enforce-bsr-neighbor

【命令作用】配置 PIM 对发送 BootStrap 报文的路由器是否是其 PIM 邻居做检查。

【命令原型】{no} ip pim enforce-bsr-neighbor

【默认状态】对发送 BootStrap 报文的路由器不做是否是 PIM 邻居检查

【命令模式】接口配置模式

【使用指导】该命令主要用于和其它厂家的设备互联时兼容互通时使用。

No 命令用于设置对发送 BootStrap 报文的路由器不做是否是 PIM 邻居检查。

ip pim message-interval

【命令作用】配置 PIM 的 JOIN-PRUNE 消息发送间隔。

【命令原型】ip pim message-interval <1-65535>

no ip pim message-interval

【参数说明】<1-65535> JOIN-PRUNE 消息发送间隔（秒）。

【默认状态】JOIN-PRUNE 消息发送间隔缺省为 60 秒。

【命令模式】配置模式

【使用指导】必要时可以修改 PIM 的 JOIN-PRUNE 消息发送间隔。

该命令的配置直接影响网络负载和协议性能，建议使用默认值，如需配置请谨慎考虑。

No 命令用于将 JOIN-PRUNE 消息发送间隔恢复成默认值。

【配置实例】

```
Harbour(config)# ip pim message-interval 40
```

【相关命令】ip pim query-interval

ip pim mode

【命令作用】启动 PIM 协议。

【命令原型】{no} ip pim [dense-mode | sparse-mode] {passive}

【参数说明】

sparse-mode	以密集模式启动 PIM
dense-mode	以稀疏模式启动 PIM
passive	以被动方式启动 PIM，即只接收 IGMP 报文

【默认状态】不启动 PIM 协议。

【命令模式】接口配置模式。

【使用指导】将接口加入三层组播转发有两种方式：启动 PIM 等组播协议和 IGMP，或只启动 IGMP 协议。本命令在对应的接口上启动 PIM-SM 协议和 IGMP 协议。

使用 PIM 协议必须通过此命令在至少 1 个接口上启动 PIM 协议。

在配置这个命令前，必须先用 ip multicast-routing 命令启动组播转发。

以 sparse-dense-mode 启动 PIM 协议的接口，将根据组播组 G 与 RP 的映射关系决定以密集或稀疏模式启动 PIM：对特定组，若能映射到 RP，则使用稀疏模式，否则使用密集模式启动 PIM

No 命令用于该接口退出三层组播。

【配置实例】

```
Harbour(config-if)# ip pim sparse-mode
```

【相关命令】ip multicast-routing

ip pim neighbor-filter

【命令作用】用访问列表设置邻居关系的建立规则。

【命令原型】ip pim neighbor-filter <access_list>

no ip pim neighbor-filter

【参数说明】<access_list>　　访问列表的名称

【默认状态】本设备不过滤，即可与任一相连组播路由器建立邻居关系。

【命令模式】接口配置模式。

【使用指导】在特定的接口上启动该过滤机制，可以对收到的 PIM Hello 报文进行过滤，以确定接受或者拒绝与特定范围内的邻接设备建立邻居关系。No 命令用于清除该过滤策略。

【配置实例】下例中，通过使用访问列表 neig_acl 使得接口 v2 仅与 ip 地址在 16.0.0.0～16.255.255.255 范围内的组播路由设备建立邻居关系。

```
Harbour(config)# access-list route neig_acl 10 permit 16.0.0.0/8
Harbour(config)# create vlan v2
Harbour(config)# interface v2
Harbour(config-if)# ip pim neighbor-filter neig_acl
```

【相关命令】access-list route

ip pim query-interval

【命令作用】配置相应接口的 PIM hello 消息发送间隔。

【命令原型】ip pim query-interval <1-18724>

no ip pim query-interval

【参数说明】<1-18724>　　hello 消息发送间隔（以秒为单位，默认值为 30 秒）。

【命令模式】接口配置模式

【使用指导】必要时可以修改接口的 PIM hello 消息发送间隔。

该命令的配置直接影响网络负载和协议性能，建议使用默认值，如需配置请谨慎考虑。

No 命令用于将该接口的 PIM hello 消息发送间隔恢复成默认值。

【配置实例】

```
Harbour(config)# create vlan v2
Harbour(config)# interface v2
Harbour(config-if)# ip pim query-interval 25
```

【相关命令】ip pim message-interval

ip pim rp-address

【命令作用】配置静态 RP 地址。

【命令原型】ip pim rp-address <A.B.C.D> {group <A.B.C.D/M> {[priority <0-254>| override]}}

no ip pim rp-address <A.B.C.D> {group <A.B.C.D/M>}

【参数说明】<A.B.C.D> 静态 RP 地址 。

group <A.B.C.D/M> RP 可以负责的组地址范围。缺省为所有组：224.0.0.0/4。

priority <0-254> 静态 RP 的优先级。缺省为 0（最低）。

override 覆盖 bootstrap 消息申明的 RP 表。

【默认状态】无静态 RP。

【命令模式】配置模式

【使用指导】RP（Rendezvous Point）是 PIM 网络中共享树转发路径（RPT）的根节点。在 PIM 网络中必须存在一个唯一的 RP 设备。它接受源 DR 发来的 REGISTER 报文，并将数据沿共享树向下转发。每个边缘 PIM 路由器收到 IGMP 请求后，都会向 RP 发送组加入报文，请求接收对应组的数据流。

在 PIM 网络中，必要时可以通过这个命令配置一个或多个静态的 RP 地址。

No 命令用于取消该 RP 设置，若优先级和组播组地址范围相同，则静态配置的 rp 将覆盖通过 bootstrap 动态学习的 rp。

【配置实例】

```
Harbour(config)# ip pim rp-address 100.1.0.1 group 225.0.0.0/8
Harbour(config)# ip pim rp-address 100.1.0.2 group 230.0.0.0/16 override
```

【相关命令】ip pim bsr-candidate

ip pim rp-address

ip pim rp-candidate

【命令作用】配置本机为 PIM 候选 RP。

【命令原型】{no} ip pim rp-candidate <interface> {group <A.B.C.D/M>}

【参数说明】<interface> 选择候选 RP IP 地址的接口名称 。

<A.B.C.D/M> RP 可以负责的组地址范围。缺省为所有组：224.0.0.0/4。

【默认状态】本机不作为候选 RP。

【命令模式】配置模式

【使用指导】RP（Rendezvous Point）是 PIM 网络中共享路径转发树（RPT）的根节点。在 PIM 组播域中对特定组必须存在一个唯一的 RP 设备。它接受源 DR 发来的 REGISTER 报文，并将数据沿共享树向下转发。每个边缘 PIM 路由器收到 IGMP 请求后，都会向 RP 发送组加入报文，请求接收对应组的数据流。

在 PIM 协议中，为了优化数据流路径，可以在通信流量达到某个阀值后从共享路径转发树切换到以源 DR 为根的转发树（SPT）。本软件中这个切换的流量阈值为 0，即

只要有 RPT 数据流到达就会立刻切换到 SPT。在与其它厂商设备互联时可能需要设置它们的切换流量阈值为 0。

在 PIM 网络中，必须通过这个命令配置至少一个候选 RP。

No 命令用于取消该 RP 设置。

【配置实例】

```
Harbour(config)# ip pim rp-candidate v2 group 232.0.0.0/16
```

【相关命令】ip pim bsr-candidate

ip pim rp-address

ip pim source-dr-filter group

【命令作用】在源 DR 上，用访问列表设置组播数据包的组过滤规则。

【命令原型】ip pim source-dr-filter group <access_list>

no ip pim source-dr-filter group

【参数说明】<access_list>　　访问列表的名称

【默认状态】本设备不过滤，即发布所有组地址的组播数据包。

【命令模式】接口配置模式。

【使用指导】在源 DR 的特定的接口上启动该过滤机制，在发布组播数据报文时进行过滤，以保证发布或不发布组播组地址在特定范围内的组播数据包。

No 命令用于清除该过滤策略。

【配置实例】下例中，通过使用访问列表 sdrgrp_acl 使得源 DR 的接口 v2 仅发送组地址范围为 226.0.0.0～226.255.255.255 的组播数据包。

```
Harbour(config)# access-list route sdrgrp_acl 10 permit 226.0.0.0/8
Harbour(config)# create vlan v2
Harbour(config)# interface v2
Harbour(config-if)# ip pim source-dr-filter group sdrgrp_acl
```

【相关命令】access-list route

ip pim source-dr-filter source

【命令作用】在源 DR 上，用访问列表设置组播数据包的源过滤规则。

【命令原型】ip pim source-dr-filter source <access_list>

no ip pim source-dr-filter source

【参数说明】<access_list>　　访问列表的名称

【默认状态】本设备不过滤，即发布所有源的组播数据包。

【命令模式】接口配置模式

【使用指导】在源 DR 的特定的接口上启动该过滤机制，在发布组播数据报文时进行过滤，以保证发布或不发布源地址在特定范围内的组播数据包。

No 命令用于清除该过滤策略。

【配置实例】下例中，通过使用访问列表 sdrsrc_acl 使得源 DR 的接口 v2 仅发送源地址范围为 16.0.0.0～16.255.255.255 的组播数据包。

```
Harbour(config)# access-list route sdrsrc_acl 10 permit 16.0.0.0/8
Harbour(config)# create vlan v2
Harbour(config)# interface v2
Harbour(config-if)# ip pim source-dr-filter source  sdrsrc_acl
```

【相关命令】access-list route

show debug pim

【命令作用】显示已经打开的 PIM 调试信息开关。

【命令原型】show debug pim

【命令模式】配置模式

【使用指导】此命令显示当前打开的 PIM 调试信息开关的情况。

【相关命令】debug pim

show ip pim bsr-router

【命令作用】显示 PIM 协议的 BSR 选择信息。

【命令原型】show ip pim bsr-router

【命令模式】配置模式

【使用指导】此命令显示当前采用的 BSR 地址、优先级、RP 映射掩码等信息。

【配置实例】

```
Harbour(config)# show ip pim bsr-router
```

【相关命令】ip pim bsr-candidate

show ip pim interface

【命令作用】显示运行 PIM 的接口信息。

【命令原型】show ip pim interface {<ifname>}

【参数说明】<ifname>　　接口名称。

【命令模式】配置模式

【使用指导】此命令显示运行 PIM 的接口表和相应的状态。

不带参数时，将显示所有的 PIM 接口信息；带接口名称参数时，显示特定接口的 PIM 信息。

【配置实例】

```
Harbour(config)# show ip pim interface
```

【相关命令】show ip multicast interface

ip pim sparse

show ip pim neighbor

【命令作用】显示 PIM 邻居信息。

【命令原型】show ip pim neighbor {<ifname> }

【参数说明】<ifname>接口名称。

【命令模式】配置模式

【使用指导】此命令显示协议当前已经获得的 PIM 邻居情况。PIM 邻居是通过 hello 报文发现的。不带参数时，将显示所有的 PIM 邻居信息；带接口名称参数时，显示特定接口上的 PIM 邻居。

【配置实例】

```
Harbour(config)# show ip pim neighbor
```

【相关命令】show ip multicast interface

show ip pim interface

show ip pim rp

【命令作用】显示当前 RP 列表。

【命令原型】show ip pim rp

【命令模式】配置模式

【使用指导】此命令显示的内容包括两部分：当前获得的 RP 列表（包括 RP 地址、管理的组地址范围、来源、超时时间等）以及该设备上的组播组与 RP 的映射表。

【配置实例】

```
Harbour(config)# show ip pim rp
```

【相关命令】ip pim rp-candidate

show ip pim rp-hash

show ip pim rp-candidate

【命令作用】显示当前候选 RP 列表。

【命令原型】show ip pim rp-candidate

【命令模式】配置模式

【使用指导】可以在候选 RP 或 BSR 上通过这个命令显示本设备上已配置的候选 RP 信息。

【配置实例】

```
Harbour(config)# show ip pim rp-candidate
```

【相关命令】ip pim rp-candidate

show ip pim rp

show ip pim rp-hash

【命令作用】查询一个组的 RP 映射结果。

【命令原型】show ip pim rp-hash <A.B.C.D>

【命令模式】配置模式

【使用指导】可通过命令计算任意一个组的 RP 映射，了解系统中对 RP 的选择。

【配置实例】

```
Harbour(config)# show ip pim rp-hash 224.1.1.1
```

【相关命令】ip pim rp-candidate

show ip pim rp

show ip rpf

附录 命令索引

普通用户命令一览表：

命令名称	命令功能描述
clear	清除屏幕
enable	进入配置模式，可以对交换机进行配置和写操作
exit	结束当前模式，返回前一模式
help	显示系统的帮助信息
list	列出当前模式下的所有命令
logout	断开与交换机的连接，并退出系统
ping {[-t]}*1 {[-count] <1-65535>}*1 {[-size] <0-6400>}*1 {[-waittime] <1-255>}*1 {[-ttl] <1-255>}*1 {[-pattern] <user_pattern>}*1 <A.B.C.D>	用于检测网络连接是否正常。
quit	断开与交换机的连接并退出系统
show ACL [<name>|all]	查看 ACL 策略
show arp {[<A.B.C.D>|permanent]}*1	查看 arp 地址表项
show fdb {[mac] <macaddr>}*1 {[vlan] <name>}*1	显示 mac 地址为<macaddr>，vlan 名为<vlan>的 FDB 信息
show fdb agetime	显示地址表老化时间
show fdb permanent {[mac] <macaddr>}*1 {[vlan] <name>}*1	显示永久的 FDB 信息
show history	显示历史命令
show idle-timeout	显示经过多长的空闲等待时间系统自动进入登录前的状态
show interface {<IFNAME>}*1	显示接口状态和配置信息
show ip route	显示 RIB 路由表所有路由信息
show ip route <A.B.C.D/M>	显示 RIB 表中目的 IP 地址和子网掩码长度与<A.B.C.D/M>匹配的路由信息
show ip route <A.B.C.D>	显示 RIB 表中目的 IP 地址与<A.B.C.D>匹配的路由信息
show ip route [connected|static]	显示 RIB 表中指定协议的路由信息
show ip route summary	查看路由表的详细信息
show mirroring	查看系统镜像信息

show port [<portlist>|all] {[configuration|stats]}*1	显示系统指定端口的配置信息或状态
show services	显示系统服务的状态，包括 telnet，snmp， 和 web manage 三个服务
show sharing	显示系统 sharing 信息
show stpd default	显示 STP 域缺省信息
show stpd default port [<portlist> | all]	显示指定端口的 stp 信息
show syscontact	显示管理本主机的用户，以及如何联系该用户
show syslocation	显示主机所在的物理位置
show time	显示系统日期
show version	显示 HammerOS 系统版本信息
show vlan {<name>}*1	显示系统 VLAN 信息
telnet <A.B.C.D>	登录其他主机或者交换机
terminal length <0-512>	设置终端屏幕上所显示的行数
who	显示连接在交换机上的所有用户
who am I	仅仅显示用户自己的连接信息

管理员用户命令一览表：

命令	功能描述
clear	清除屏幕
clear counter [<name>|all]	清空指定名称（name）或所有（all）ACL 计数器的统计信息
clear igmp snooping vlan [name|all]	清除 VLAN 内的组播
clear ip route static	清除静态路由
clear stats port [<portlist>|all]	清除端口统计信息，选择 portlist 对指定端口进行操作，选择 all 对所有端口进行操作
config ACL <name> priority <0-7>	配置 ACL 策略的数据流的优先级的重新映射
config access-control { [telnet|web|snmp] }*1 [on|off]	打开或关闭访问控制。选择 on 表示打开；选择 off 表示关闭。
config WRR-queue bandwidth <low,normal,medium,high>	配置队列加权轮循的权重
config access-control {[telnet|web|snmp]}*1 [on|off]	激活或禁止对 telnet、web 和 snmp 的访问控制功能。
config acl <name> counter <name>	设置 ACL 计数器

config igmp snooping host_timeout <10-2147483647>	设置主机超时时间间隔
config igmp snooping router_timeout <10-2147483647>	设置路由器超时时间间隔
config loopDetect [enable|disable]	设置端口的下行环路检测。enable 表示允许，disable 表示禁止。
config mirroring [add|delete] port [<portlist>|all] [egress|ingress]	增加或删除镜像端口的发送或接收包，选择 add 为增加镜像端口，选择 delete 为删除端口，选择 egress 为对发送包进行镜像，选择 ingress 为对接收包进行镜像
config mirroring disable	取消端口镜像
config mirroring to <1-50>	配置镜像目标端口
config fdb agingtime [0|<10-1000000>	修改 fdb 表老化时间
create nms-access-profile <access_profile_name>	创建一个访问控制配置。
delete nms-access-profile <access_profile_name>	删除特定的访问控制配置。
config nms-access-profile <access_profile_name> telnet [enable|disable]	允许或禁止 telnet 访问控制。
config nms-access-profile <access_profile_name> web [enable|disable]	允许或禁止 web 访问控制。
config nms-access-profile <access_profile_name> snmp [enable|disable]	允许或禁止 snmp 访问控制。
config nms-access-profile <access_profile_name> add ipaddress <A.B.C.D/M>	在指定的配置表里添加 IP 地址。
config nms-access-profile <access_profile_name> add ipaddress <A.B.C.D> <A.B.C.D>	在指定的配置表里添加 IP 地址。
config nms-access-profile <access_profile_name> delete ipaddress [all |<A.B.C.D/M>]	在指定的配置表里删除 IP 地址。
config nms-access-profile <access_profile_name> delete ipaddress <A.B.C.D> <A.B.C.D>	在指定的配置表里删除 IP 地址。
show access-control {[telnet|web|snmp]}*1	查看访问控制功能是否打开。
show nms-access-profile {<access_profile_name>}*1	查看特定配置表的配置情况。

config port [<portlist>|all] [enable|disable]	修改端口状态（开/关），enable 为打开端口，disable 为关闭端口
config port [<portlist>|all] auto [on|off]	修改端口自适应状态（开/关），on 为打开端口自适应功能，off 为关闭端口自适应功能
config port [<portlist>|all] duplex [full|half]	修改端口工作方式（全双工/半双工），full 为全双工方式，half 为半双工方式
config port [<portlist>|all] flowcontrol [on|off]	修改端口流控状态（开/关），on 为打开端口流控功能，off 为关闭端口流控功能
config port [<portlist>|all] speed [10|100|1000]	修改端口速度，10 为 10Mbps，100 为 100Mbps，1000 为 1000Mbps
config port [<portlist>|all] learn [on|off]	使能或者禁止端口的地址学习功能
config port [<portlist>|all] mode [master|slave]	千兆电口工作在强制千兆模式下，需要一端设置成主模式，另一端设置从模式。
config port [<portlist>|all] remap-priority <0-7>	配置相应端口对 802.1p 优先级的重新映射
config port [<portlist>|all] remap-priority [on|off]	使能/禁止端口对 802.1p 优先级的重新映射功能
config priority <0-7> qosqueue [Low|Normal|Medium|High]	配置 802.1p 优先级到 CoS 队列的映射关系
config proxyarp [supervlan|subvlan] <vlanname> [enable|disable]	使能或关闭 PROXYARP 功能
show proxyarp [supervlan|subvlan] <vlanname>	显示 PROXYARP 状态信息
config proxyarp searchtime <0-196605>	配置主机搜索表老化时间
config proxyarp agetime <0-196605>	配置 ProxyArp 表老化时间
config proxyarp delete <A.B.C.D>	删除 ProxyArp 表项
show proxyarp table {<A.B.C.D >}*1	显示 ProxyArp 表项
config sharing <1-50> select-mode <rtag>	配置 Load sharing 成员端口的转发策略
config snmp community [readonly|readwrite] <string>	设置 community 的 readonly/readwirte 字符串信息
Config snmp trapagent-address [<A.B.C.D>|auto]	配置 SNMP 的 trapagent-address
config snmp trapreceiver add <A.B.C.D> version [v1|v2c] {community <string>}*1	添加一个 trap 接收服务器 Ip 地址
config snmp trapreceiver delete <A.B.C.D>	删除一个 trap 接收服务器 Ip 地址
Config sntp-client [enabler|disable]	使能或关闭 SNTP 协议的客户端软件

Config sntp-server [enabler|disable]	使能或关闭 SNTP 协议的服务器端软件
config sntp-client mode <1-3>	配置 SNTP 协议客户端的工作模式，即 unicast，multicast，anycast 三种模式的任意一种。
config sntp-server mode <1-3>	配置 SNTP 协议服务器的工作模式，即 unicast，multicast，anycast 三种模式的任意一种。
config sntp-client server ipaddr <A.B.C.D>	配置 SNTP 协议客户端的时间服务器的 IP 地址。
config sntp-client update-interval <64-1024>	配置 SNTP 客户端的时间更新周期
config sntp-server broadcast-interval <64-1024>	当 SNTP 服务器工作在 multicast 模式下时，配置 SNTP 服务器的时间广播周期。
show sntp-client	显示 SNTP 客户端的状态。
show sntp-server	显示 SNTP 服务器端的状态。
config stpd default [enable|disable]	打开或关闭 stpd 功能
config stpd default port [<portlist> | all] cost <1-65535>	修改端口 STP 路径开销值
config stpd default port [<portlist> | all] priority <0-255>	修改端口 STP 优先级
config stpd default port [<portlist>|all] [enable|disable]	修改端口 STP 状态（参加 STP 计算/不参加 STP 计算）
config stpd default [enable | disable]	修改 STP 状态（打开/关闭）
config stpd default forwarddelay <4-30>	修改 STP 延迟时间
config stpd default hellotime <1-10>	修改 STP 响应时间
config stpd default maxage <6-40>	修改 STP 最长计算时间
config stpd default priority <0-65535>	修改 STP 优先级
config syscontact <.contact>	描述主机管理员的信息，包括用户名、联系方式等（根据需要来设定）
config syslocation <.location>	描述主机的位置
config time <1970-2100> <1-12> <1-31> <HH:MM:SS>	修改日期时间，依次为年、月、日、时、分、秒
config vlan <name> [add|delete] port <portlist> [tagged|untagged]	配置名为<name>的 VLAN 的端口为 tagged 或 untagged
config vlan <name> ipaddress <A.B.C.D/M>	配置名为<name>的 VLAN 的 IP 地址和网络掩码长度

	长度
config vlan <name> ipaddress <A.B.C.D> <A.B.C.D>	配置名为<name>的 VLAN 的 IP 地址和网络掩码
config vlan <name> priority <0-7>	通过改变 VLAN 的优先级属性来实现属于某一个 VLAN 的数据流的优先级的重新映射
config vlan <name> tag <1-4094>	配置名为<name>的 VLAN 的标签（即 VLAN ID）
create ACL <name> ip DIP [<A.B.C.D/M>|any] SIP [<A.B.C.D/M>|any] [permit|deny] ports [<portlist>|any] {precedence <0-255>}	创建基于 IP 的 ACL 策略
create ACL <name> udp DIP [<A.B.C.D/M>|any] ip-port [<dst_port>|any] SIP [<A.B.C.D/M>|any] ip-port [<src_port>|any] [permit|deny] ports [<portlist>|any] {precedence <0-255>}	创建基于 UDP 的 ACL 策略
create ACL <name> tcp DIP [<A.B.C.D/M>|any]ip-port [<dst_port>| any] SIP [<A.B.C.D/M>|any]ip-port [<src_port>|any] [permit|deny] ports [<portlist>|any]{precedence <0-255>}*1	创建基于 TCP 的 ACL 策略
create ACL <name> mac-ip destination [<dst_mac> |any] [<A.B.C.D/M> |any] source [<src_mac> |any] [<A.B.C.D/M>|any] [permit|deny] ports [<portlist>|any] {precedence <0-255>}*1	创建基于 MAC+IP 的 ACL 策略
create ACL <name> icmp DIP [<A.B.C.D/M>|any] SIP [<A.B.C.D/M>|any] type [<icmp_type>|any] code [<icmp_code>|any] [permit|deny] ports [<portlist>|any] {precedence <0-255>}*1	创建基于 ICMP 的 ACL 策略
create counter <name>	创建一个计数器
create fdbentry <mac_address> vlan <name> port <portno> {priority <0-7>}*1	创建 FDB 地址表项
create sharing <1-50> grouping <portlist>	创建特定 Load Sharing，这一 Load Sharing 由端口<portlist>组成
create vlan <name>	创建一个名为<name>的 VLAN
delete ACL [<name>|all]	删除一个或所有 ACL 策略

delete counter [<name>|all]	删除一个或所有 ACL 计数器
delete fdbentry {mac <mac_address> vlan <name>}*1	删除转发表中指定的 MAC 地址的入口
delete nms-access-profile <access_profile_name>	删除一个 NMS 访问控制组
delete sharing <1-50>	删除指定的 Load Sharing
delete vlan [<name>|all]	删除名为<name>的 VLAN 或所有的 VLAN
download ftp [hammeros|config-file] <A.B.C.D> <username> <password> <filename>	利用 FTP 下载 HammerOS 文件或 config-file 到 FLASH 中
download xmodem [hammeros|config-file] {baudrate [9600|115200]}*1	利用 xmodem 协议下载 HammerOS 文件或 config-file 到 FLASH 中并可以选择下载带宽为 9600 或 115200
enable-password	修改进入配置模式的密码，必须大于或者等于 6 个字符
erase {startup-config}*1	删除交换机启动配置
exit	关闭当前模式，返回到上一个模式
help	显示系统帮助信息
hostname <hostname>	设置系统的网络名称，例如，在本手册中，网络名称为 HammerOS
idle-timeout <0-35791>	设置经过多长的空闲等待系统自动进入登录前的状态
interface <IFNAME>	进入要配置的 vlan 接口名称
ip route <A.B.C.D/M> [<A.B.C.D>] {<1-255>}*1	建立一条静态路由,目的 IP 地址和子网掩码长度为<A.B.C.D/M>， 下一跳 IP 地址为<A.B.C.D>，distance 值为<1-255>
ip route <A.B.C.D> <A.B.C.D> [<A.B.C.D>] {<1-255>}*1	建立一条静态路由,目的 IP 地址为第一个<A.B.C.D>,子网掩码为第二个<A.B.C.D>,下一跳地址为第三个<A.B.C.D>，distance 值为<1-255>
kill session <1-24>	强制断开特定 telnet 连接
list	列出当前模式下的所有命令
List<pattern>	根据关键字查找命令行
login-password	设置登录密码
logout	断开与交换机的连接并退出系统
monitor [on|off]	打开或关闭在本终端显示日志信息的功能
monitor lowest-level <0-7>	配置在终端可以显示的日志信息的最低级别
monitor timestamp [none|time|datetime]	配置是否显示时间信息

monitor type [<typename>|all] [on|off]	配置在终端可以显示的日志信息的类型
no acl <name> priority	取消已经配置的 ACL 优先级配置信息
no ip route <A.B.C.D/M> <A.B.C.D> {<1-255>}*1	删除目的网段 IP 地址和子网掩码长度为<A.B.C.D/M>、下一跳地址为<A.B.C.D>、distance 值(如果有)为<1-255>的静态路由
no ip route <A.B.C.D> <A.B.C.D> <A.B.C.D> {<1-255>}*1	删除目的网段 IP 地址为第一个<A.B.C.D>、子网掩码为第二个<A.B.C.D>、下一跳地址为第三个<A.B.C.D>、 distance 值(如果有)为<1-255>的静态路由
no vlan-priority <name>	取消已经配置的 vlan 优先级配置信息
no vlan <name> ip	删除指定 vlan 的 ip 地址
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>	用于检测网络连接是否正常
quit	断开与交换机的连接并退出系统
reboot	重新启动交换机
record command-line [enable|disable]	打开命令行操作日志记录功能
save configuration	保存系统配置信息
service acl [enable|disable]	启用或者禁止 acl 功能
service igmp snooping [enable|disable]	启用/禁止 IGMP Snooping 功能
service qos [enable|disable]	启用或者禁止 QoS 功能
service snmp [enable|disable]	启用或者禁止 snmp 功能
service snmp rmon [enable|disable]	启用或者禁止 rmon 功能
service snmp trap [enable|disable]	启用或者禁止 snmp trap 功能
service telnet [enable|disable]	配置 telnet 服务，打开或关闭服务，enable 为打开 telnet 服务，disable 为关闭 telnet 服务
show ACL [<name>|all]	查看一个或所有 ACL 策略
show WRR-queue	显示 4 个优先级队列与权重的对应关系
show arp {[<A.B.C.D>|permanent]}*1	查看 arp 地址表项信息
show acl counter	查看 ACL 计数信息
show counter [<name>|all]	查看一个或所有的计数器统计信息
show dot1p-QosQueue-mapping	显示 802.1p 优先级到 CoS 队列的映射关系
show arp [{<A.B.C.D>}*1 |{permanent}*1]	显示 IP 地址为<A.B.C.D>的 Arp 表项

show fdb {[mac] <macaddr>}*1 {[vlan] <name>}*1	显示 mac 地址为<macaddr>，vlan 名为<vlan>的 mac 地址入口信息
show fdb agingtime	显示 fdb 表的老化时间
show fdb permanent {[mac] <macaddr>}*1 {[vlan] <name>}*1	显示指定的静态 mac 地址信息
Show fdb summary	显示 FDB 统计信息，包括静态和动态 FDB 信息
Show filter	显示系统 IRULE 和 IMASK 表的信息
show history	显示最近用户输入的 20 个历史命令
show idle-timeout	显示经过多长的空闲等待系统自动进入登录前的状态
show igmp snooping timer	显示 IGMP Snooping 定时信息
show igmp snooping vlan <name>	显示 VLAN 中的 IGMP Snooping
show interface {<IFNAME>}*1	显示接口名称
show ip fib	显示系统当前有效地 IP 转发表
show ip route	显示 RIB 表中所有路由信息
show ip route <A.B.C.D/M>	显示 RIB 表中目的 IP 地址和子网掩码长度与<A.B.C.D/M>匹配的路由信息
show ip route <A.B.C.D>	显示在此 RIB 表中的制定目的 IP 地址（不含子网掩码）的路由信息
show ip route [connected|static]	显示 RIB 表中指定路由协议的路由信息：直连的，通过 rip 协议学到的和静态的
show ip route summary	显示 RIP 路由表概要信息
Show macgroup-info	显示 MAC groupr 的信息
show mirroring	显示镜像配置信息
show monitor{configuration}*1	显示 monitor 的状态是打开还是关闭
show nms-access-profile {<access_profile_name>}*1	显示 NMS 访问控制组的内容
show port [<portlist>|all] {[configuration|stats]}*1	显示系统指定端口的配置信息
show qos [port|mac|vlan|acl|all]	显示不同类型的 QoS 优先级配置信息
show running-config	显示系统的运行配置
show services	显示系统服务的状态，包括 telnet，snmp， 和 web manage 三个服务
show sharing	显示系统 sharing 信息
show snmp community-string	显示 community-string 的 get/set 字符串信息
Show snmp trapagent-address	显示 SNMP 的 trapagent-address 信息
show snmp trapreceiver	查看 snmp trapreceiver 的信息
show startup-config	显示启动配置

show stpd default	显示 STP 域端口信息
show stpd default port [<portlist>| all]	显示指定/全部端口的生成树协议信息
show syscontact	显示描述主机管理员的信息
show syslocation	显示描述主机的位置的信息
show syslog {configuration}*1	显示系统日志信息
show time	显示系统时间信息
show version	显示系统版本信息
show vlan {<name>}*1	显示 VLAN 的信息
telnet <A.B.C.D>	远程登录 IP 地址为<A.B.C.D>的主机或交换机
terminal length <0-512>	设置终端屏幕所显示的行数
upload ftp [hammeros|config-file] <A.B.C.D> <username> <password> <filename>	利用 FTP 上传 HammerOS 文件或 config-file 到文件服务器中
upload xmodem [hammeros|config-file] {baudrate [9600|115200]}*1	利用 xmodem 协议上传 HammerOS 文件或 config-file 到文件服务器中并可以选择下载带宽为 9600 或 115200
user add <username> login-password <login_password>	添加登录密码为<login_password>的用户<username>到系统中
user delete <username>	从系统中删除用户<username>
user enable-password <username>	设置用户<username>的配置密码
user list	显示所有系统用户
user login-password <username>	设置系统用户<username>的登录密码
user role <username> ADMIN enable-password <enable_password>	把用户<username>转变为系统管理员，且密码为<enable_password>
user role <username> NORMAL	把用户<username>转变为普通用户
who	显示连接在交换机上的所有用户
who am i	仅仅显示用户自己的连接信息