

目 录

第 1 章 维护和调试	1-1
1.1 Ping	1-1
1.2 Ping6	1-1
1.3 Traceroute	1-1
1.4 Traceroute6	1-1
1.5 Show	1-2
1.6 Debug	1-3
1.7 系统日志	1-3
1.7.1 系统日志介绍	1-3
1.7.2 系统日志配置	1-5
1.7.3 系统日志配置举例	1-7
第 2 章 定时重启交换机	2-1
2.1 定时重启交换机简介	2-1
2.2 定时重启交换机任务序列	2-1
第 3 章 CPU收发报文调试	3-1
3.1 CPU收发报文简介	3-1
3.2 CPU收发报文任务序列	3-1

第1章 维护和调试

说明：

本章所指的路由器代表了一般意义下的路由器或运行了路由协议的无线控制产品。

当用户配置交换机时，需要查看各项配置是否配置正确，交换机是否符合期望，工作正常；或者当网络出现了故障，用户需要诊断故障，交换机为此提供了 ping、telnet、show、debug 等多种调试命令，帮助用户查看系统配置、运行状态，找到故障原因。

1.1 Ping

Ping 命令主要用于交换机向远端设备发 ICMP 请求包，检测交换机与远端设备之间是否可达。Ping 命令各选项及参数意义请参考命令手册 Ping 命令章节。

1.2 Ping6

Ping6 命令主要用于交换机向远端设备发 ICMPv6 请求包，检测交换机与远端设备之间是否可达。Ping6 命令各选项及参数意义请参考命令手册 Ping6 命令章节。

1.3 Traceroute

Traceroute 命令用于测试数据包从发送设备到目的地设备所经过的网关，检测网络是否可达，定位网络故障所在。

Traceroute 命令的执行过程是：首先向目的地址发送一个 TTL 为 1 的数据包，如果第一跳发送回一个 ICMP 错误消息以指明该数据包不能被发送（因为 TTL 超时），则继续向该地址发送 TTL 为 2 的数据包，同样第二跳也可能返回 TTL 超时，于是这个过程不断进行，直到数据包到达目的地。执行这些过程的目的是记录每一个 ICMP TTL 超时消息的源地址，以提供一个 IP 数据包到达目的地所经历的路径。

Traceroute 命令各选项及参数意义请参考命令手册 traceroute 命令章节。

1.4 Traceroute6

Traceroute6 功能用于测试数据包从发送设备到目的设备所经过的网关，检测网络是否可达，定位网络故障所在。IPv6 下 Traceroute6 的原理和 IPv4 下的 Traceroute 原理是一样的，它利用 ICMPv6 及 IPv6 header 的跳限制字段。首先，Traceroute6 送出一个 HOPLIMIT

是 1 的 IPv6 datagram（包括源地址，目的地址和包发出的时间标签）到目的地，当路径上的第一个路由器（router）收到这个 datagram 时，它将 HOPLIMIT 减 1。此时，HOPLIMIT 变为 0 了，所以该路由器会将此 datagram 丢掉，并送回一个「ICMPv6 time exceeded」消息（包括发 IPv6 包的源地址，IPv6 包的所有内容及路由器的 IPv6 地址），Traceroute6 收到这个消息后，便知道这个路由器存在于这个路径上，接着 Traceroute6 再送出另一个 HOPLIMIT 是 2 的 datagram，发现第 2 个路由器……，Traceroute6 每次将送出的 datagram 的 HOPLIMIT 加 1 来发现另一个路由器，这个重复的动作一直持续到某个 datagram 抵达目的地。

Traceroute6 命令各选项及参数意义请参考命令手册 traceroute6 命令章节。

1.5 Show

show 命令用来显示交换机的系统信息、端口信息、协议运行情况等。本部分介绍交换机的显示系统信息的 show 命令，其它的 show 命令会在相关章节有介绍。

命令	解释
特权用户配置模式	
show debugging	显示调试开关的状态。
show flash	显示保存在 flash 中的文件及大小。
show history	显示用户最近输入的历史命令。
show history all-users [detail]	显示所有用户最近输入的历史命令，可以使用 clear history all-users 命令清除系统保存的所有用户命令记录，系统保存的最大命令记录数可以通过 history all-users max-length 命令设置。
show memory	显示指定内存区域的内容。
show running-config	显示当前运行状态下生效的交换机参数配置。
show running-config current-mode	显示当前模式下的配置。
show startup-config	显示当前运行状态下写在 Flash Memory 中的交换机参数配置，通常也是交换机下次上电启动时所用的配置文件。
show switchport interface [ethernet <interface-list>]	显示交换机端口的 VLAN 端口模式和所属 VLAN 号及交换机的 Trunk 端口信息。
show tcp show tcp ipv6	显示当前与交换机建立的 TCP 连接情况。
show udp show udp ipv6	显示当前与交换机建立的 UDP 连接情况。

show telnet login	显示当前与交换机建立起 Telnet 连接的 Telnet 客户端的信息。
show tech-support	显示交换机运行的信息和各任务的状态，技术支持人员利用该命令，诊断交换机的运行是否正常。
show version	显示交换机版本信息。
show temperature	显示交换机 CPU 的温度。
show fan	显示交换机风扇情况。

1.6 Debug

交换机支持的每一项协议都有相应的 debug 命令，用户可以通过查看 debug 命令的显示信息诊断网络故障。在以后的章节中会陆续介绍到相应协议的 debug 命令。

1.7 系统日志

1.7.1 系统日志介绍

系统日志接管所有信息输出，并且能够进行细致的分类，从而能够有效地进行信息筛选，它通过与 debug 命令的结合，为网络管理员和开发人员监控网络运行情况和诊断网络故障提供了强有力的支持。

交换机的系统日志具有以下一些特性：

- 支持控制台（console）、Telnet终端和哑终端（monitor）、日志缓冲区（logbuf）、日志主机（loghost）四个方向（也称为日志通道）的日志输出。
- 日志信息按重要性划分为四个严重等级，可按严重等级进行信息过滤。
- 日志信息按严重等级能够自动输出到相应的日志通道。

1.7.1.1 日志输出通道

目前，系统日志可以通过四个通道来输出各种日志信息：

- 通过Console向本地控制台输出日志信息。
- 向远程Telnet终端或哑终端输出日志信息，此功能有助于远程维护。
- 在交换机内部分配适当大小的日志缓冲区，用于永久或临时记录日志信息。
- 配置日志主机，日志系统直接将日志信息发往日志主机，并在其上以文件的形式保存起来，供用户随时查看。

在以上几个日志通道中，用户一般很少通过控制台监视器，而通常选择通过 Telnet 终端来实时监控系统的运行情况，但是通过这些方式输出的信息存在信息量小且无法记录下来供以后查看等缺点。而另外两个通道——交换机内部的日志缓冲区和日志主机通道——则是两个非常重要的通道。

在交换机内部提供了 NVRAM（非易失性随机访问存储器）和 SDRAM（动态随机访问存储器）两部分日志缓冲区。这两部分缓冲区采用环形方式记录日志，即当需要写入的日志信息超过缓冲区的大小时，会擦除最旧的日志信息而写入新的日志信息。保存在 NVRAM 中的日志信息会永久存留，而 SDRAM 中的日志信息在系统重启或掉电后会消失。这些日志缓冲区中的信息对于监控系统的正常运行和异常情况起着非常重要的作用。

注意：在某些交换机上可能不存在 NVRAM 日志缓冲区，而只有 SDRAM 日志缓冲区。我们推荐用户使用系统日志服务器，通过在交换机上配置日志主机，可以将日志信息送到日志服务器上保存下来，供用户随时查看。

1.7.1.2 日志信息的格式与严重等级

日志信息的格式与 BSD syslog 协议兼容，因而可以利用 UNIX/LINUX 上的 syslogd(系统日志守护进程)，以及在 PC 机上运行的类似 syslogd 的一些应用程序来记录并分析日志。

日志信息按严重等级或紧急程度划分为八个等级，每个等级对应一个数值。越紧急的日志信息等级越高，其对应的数值越小；越不紧急的日志信息等级越低，其对应的数值越大。例如 critical 等级对应的数值为 2，warnings 等级对应的数值为 4，debugging 等级对应的数值为 7，因而 critical 的等级高于 warnings，warnings 等级高于 debugging。在按严重等级来进行日志信息过滤时，采用的规则是：只允许等级等于和高于所设等级的日志信息输出，即不允许等级数值高于所设阈值的日志信息输出。因此，当设置严重等级阈值为 debugging 时，所有等级的信息都会输出；当设置严重等级阈值为 critical 时，只有 critical, alerts 和 emergencies 等级的信息才能输出。

下表给出了日志信息的严重等级及简要描述。**注意：**这些严重等级的分类是与标准的 UNIX/LINUX 中的 syslog 一致的。

表 1-1 日志信息的严重等级

严重等级 (Severity)	数值	描述
emergencies	0	System is unusable 极其紧急的错误
alerts	1	Action must be taken immediately 需立即纠正的错误
critical	2	Critical conditions 关键信息
errors	3	Error conditions 需关注但不关键的错误
warnings	4	Warning conditions

		警告，可能存在某种差错
notifications	5	Normal but significant condition 需注意的信息
informational	6	Informational messages 一般提示信息
debugging	7	Debug-level messages 调试信息

交换机目前生成以下四个等级的信息：

- 交换机重启、任务异常、CHASSIS 交换机上板卡的热插拔等信息的级别为 critical。
- 接口的 up/down 切换、拓扑变化、汇聚口状态变化等信息的级别为 notifications。
- 通过 CLI 配置命令的输出信息级别为 informational。
- 通过 CLI 配置命令 debug 开关输出的信息级别为 debugging。

日志信息按严重等级能够自动输出到相应的通道。其中，Debugging 信息只输出到哑终端（monitor）上。Informational 信息只输出到当前监控终端，例如用户通过 Telnet 终端配置命令时输出的信息只输出到该 Telnet 终端。Warnings 信息除了发送到所有终端外，还保存在 SDRAM 日志缓冲区中。而 Critical 信息除了发送到所有终端外，还保存在 SDRAM 和 NVRAM（如果交换机存在 NVRAM 日志缓冲区）中。查看保存在 NVRAM 和 SDRAM 日志缓冲区中的日志信息，可使用 show logging buffered 命令。清除保存在 NVRAM 和 SDRAM 日志缓冲区中的日志信息，可使用 clear logging 命令。

1.7.2 系统日志配置

系统日志配置任务序列如下：

1. 显示和清除日志缓冲区
2. 设置日志主机输出通道
3. 设置本交换机发送日志时使用的源 IPv4 地址或 IPv6 地址
4. 打开或关闭记录用户执行命令的日志开关
5. 显示日志信息的来源
6. 显示记录用户执行命令的日志开关状态

1. 显示和清除日志缓冲区

命令	描述
特权配置模式	

show logging buffered [level {critical warnings} range <begin-index> <end-index>]	显示日志缓冲区通道内日志的详细信息。
clear logging {sdram nvram}	清除日志缓冲区中的信息。

2. 设置日志主机输出通道

命令	描述
全局配置模式	
logging {<ipv4-addr> <ipv6-addr>} [facility <local-number>] [level <severity>] no logging {<ipv4-addr> <ipv6-addr>} [facility <local-number>]	打开日志主机输出通道；在此命令前加“no”将关闭日志主机输出通道的输出。
logging loghost sequence-number no logging loghost sequence-number	为发送到日志主机的日志添加序列号；此命令 no 操作将使得发送到日志主机的日志不包含序列号。

3. 设置本交换机发送日志时使用的源IPv4地址或IPv6地址

命令	描述
全局配置模式	
logging source-ip {<ipv4-address> <ipv6-address>} no logging source-ip {<ipv4-address> <ipv6-address>}	设置本交换机发送日志时所使用源IPv4或IPv6地址；本命令的no操作为删除配置的发送日志使用的源IPv4或IPv6地址。
logging source-ip flags no logging source-ip flags	打开或关闭交换机发送的日志信息中携带发送日志使用的源IPv4或IPv6地址的开关。

4. 打开或关闭记录用户执行命令的日志开关

命令	描述
全局配置模式	
logging executed-commands {enable disable}	打开或关闭记录用户执行命令的日志开关

5. 显示日志信息的来源

命令	描述
特权和配置模式	
show logging source mstp	显示设备 MSTP 模块的日志信息的来源。

6. 显示记录用户执行命令的日志开关状态

命令	描述
特权和配置模式	
show logging executed-commands state	显示用于记录用户执行命令的日志开关状态

1.7.3 系统日志配置举例

举例 1：交换机的管理 VLAN 的 IPv4 地址为 100.100.100.1，远端日志服务器的 IPv4 地址为 100.100.100.5。需要能够将交换机中严重级别等于和高于 warnings 的日志信息发送到该日志服务器，并保存到其日志记录设备 local1 中。

配置步骤如下：

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 100.100.100.1 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#logging 100.100.100.5 facility local1 level warnings
```

举例 2：交换机的管理 VLAN 的 IPv6 地址为 3ffe:506::1，远端日志服务器的 IPv6 地址为 3ffe:506::4。需要能够将交换机中严重级别等于和高于 critical 的日志信息发送到该日志服务器，并保存到其日志记录设备 local7 中。

配置步骤如下：

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 address 3ffe:506::1/64
Switch(Config-if-Vlan1)#exit
Switch(config)#logging 3ffe:506::4 facility local7 level critical
```

第2章 定时重启交换机

2.1 定时重启交换机简介

定时重启交换机是在不关闭电源的情况下，经过指定的时间以后，重新启动交换机。本功能一般用于版本升级。当升级完版本以后，可以不立刻重启交换机，而是指定经过一段时间以后再重启交换机。

2.2 定时重启交换机任务序列

1. 定时热启动交换机

命令	解释
特权用户配置模式	
reload after {[<HH:MM:SS>] [days <days>]}	定时热启动交换机。
reload cancel	取消定时热启动交换机。

第3章 CPU收发报文调试

3.1 CPU收发报文简介

CPU 收发报文调试命令用于对各种送往交换机 **cpu** 的报文的诊断调试，这部分命令的使用必须在厂商技术人员的指导下使用。

3.2 CPU收发报文任务序列

命令	解释
全局配置模式	
cpu-rx-ratelimit total <packets> no cpu-rx-ratelimit total	设置 cpu 接收报文总限速值，本命令的 no 操作为恢复 cpu 接收报文总限速为默认值。
cpu-rx-ratelimit queue-length <queue-id> <qlen-value> no cpu-rx-ratelimit queue-length [<queue-id>]	设置 cpu 各队列接收报文的队列长度，本命令的 no 操作为恢复 cpu 各队列接收报文的队列长度为默认值。
cpu-rx-ratelimit protocol <protocol-type> <packets> no cpu-rx-ratelimit protocol [<protocol-type>]	设置协议报文每秒允许送 CPU 的个数，本命令的 no 操作为恢复协议报文每秒允许送 CPU 的个数为默认值。
clear cpu-rx-stat protocol [<protocol-type>]	将某类型协议报文的收包统计清 0。
特权模式	
show cpu-rx protocol [<protocol-type>]	显示某板卡的指定类型报文的接收信息。
debug driver {receive send} [interface {<interface-name> all}] [protocol {<protocol-type> discard all}][detail]	打开指定端口指定类型报文驱动接收或发送信息的显示。
no debug driver {receive send}	关闭驱动收发包信息的显示。

命令	解释
特权模式	

protocol filter {protocol-type}	开启/关闭针对具名协议报文的处理,目前该具名协议包括
no Protocol filter {protocol-type}	{arp bgp dhcp dhcpv6 hsrp http igmp ip ldp mpls ospf pim rip snmp telnet vrrp}