

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 Logging.....	1-3
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 4 章 DCP 功能调试	4-1
4.1 DCP 功能简介.....	4-1
4.2 DCP 功能任务序列.....	4-1
4.3 DCP 功能配置举例.....	4-2
4.4 DCP 功能排错帮助.....	4-3
第 5 章 COPP 功能调试	5-1
5.1 COPP 功能简介.....	5-1
5.2 COPP 功能任务序列.....	5-1
5.3 COPP 功能配置举例.....	5-4
5.4 COPP 功能排错帮助.....	5-5

第 1 章 维护和调试

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 原理上是一样的，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	本型号交换机不支持该命令。

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 Logging

交换机支持将用户在 console, telnet 或 ssh 终端执行的命令记录到日志系统 info-center 中。

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

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 <code>no</code> 操作为恢复 cpu 接收报文总限速为默认值。
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 <code>no</code> 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} no 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 {arp bgp dhcp dhcpv6 hsrp http igmp ip ldp mpls ospf pim rip snmp telnet vrrp}

第 4 章 DCP 功能调试

4.1 DCP 功能简介

动态 CPU 防护又称为动态 CPU 限速，当检测到具有某种特定源 IP 的报文上 CPU 的速率超过一定的速率值时，将对该类报文进行限速处理。报文上 CPU 允许的最大速率值被称为限速值，限速值可以采用设定好的默认值，也可以采用用户手工设定的速率值。

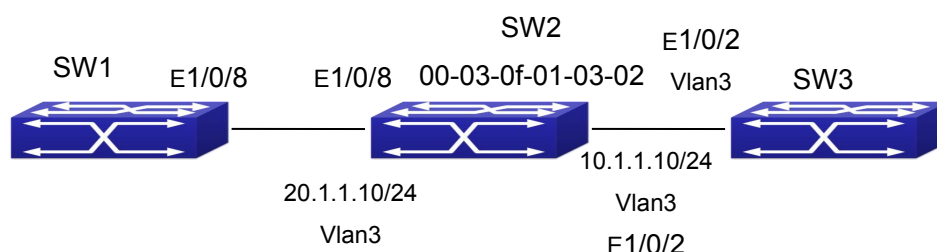
DCP 用来对网段 IP 进行限速，防止单个 IP 占用带宽。DCP (Dynamic CPU Protection) 动态 CPU 防护，是指通过实时监测上 CPU 的 other-ipuc 报文，控制报文上 CPU 的速率，以免速率过快造成 CPU 负载过重，从而达到保护 CPU 的目的。当 5s 内流量低于限速值一半限速取消。DCP 只针对 other-ipuc 报文，对于管理报文或协议报文，不采用这种方式限速。

4.2 DCP 功能任务序列

命令	解释
全局配置模式	
dcp enable dcp disable	使能/去使能 DCP 功能。
dcp limit-rate <20-50> no dcp limit-rate	本命令用于设置 DCP 的限速值，no 操作用于取消限速值，恢复默认限速值。
dcp no-limit-ip <ip_addr> no dcp no-limit-ip <ip_addr>	本命令用于配置进行 DCP 不限速的 IP，no 操作用于取消配置的不限速的 IP。
show dcp limit-rate	本命令用于显示用户配置的限速值。
show cpu ip rate top10 [slot <1-9> member <1-16>]	本命令用于显示 5s 之内上 CPU 速率最大的前 10 个 IP，以及对应的速率值。
show dcp limited ip [slot <1-9> member <1-16>]	显示当前被限速的 IP 节点信息。
特权模式	
clear dcp speed limit rules {member	通过该命令可以清除 DCP 向驱动下发过的限

<1-16>}	速规则，可以指定需要清除规则的板卡号或 ip。
debug dcp packet no debug dcp packet	本命令显示 DCP 功能对上 CPU 报文监测及处理的过程，no 操作是取消 DCP 功能对上 CPU 报文监测及处理的过程。
debug dcp event no debug dcp event	本命令显示 DCP 功能的事件处理过程，no 操作是取消对 DCP 功能处理过程的打印。

4.3 DCP 功能配置举例



如上图所示的网络拓扑中，从 SW1 的 E1/0/8 发到 SW2，目的 mac 为 SW2 的目的 mac 00-03-0f-01-03-02，目的 ip 为 10.1.1.X/24（该 ip 地址不可达）的非协议和管理报文，将会被识别为 other-ipuc 报文。该报文将会被送上 CPU 进行处理。当大量的这种报文被送上 CPU 时，将会使 CPU 负载过重，有可能导致无法处理正常的业务。

此时如果使能 DCP 功能，当设备检测到具有某种特定源 IP 的报文上 CPU 的速率超过设定的限速值时，将对该类报文进行限速处理，从而达到保护 CPU 的目的。

配置说明：

1. 使能 DCP
2. 配置限速值
3. 配置不进行限速的 ip 地址
4. 显示配置的限速值
5. 显示 5s 之内上 CPU 速率最大的前 10 个 IP，以及对应的速率值
6. 显示当前被限速 ip 节点信息
7. 清除 DCP 向驱动下发过的限速规则
8. 显示 DCP 功能对上 CPU 报文监测及处理的过程
9. 取消 DCP 功能对上 CPU 报文监测及处理的过程
10. 显示 DCP 功能的事件处理过程
11. 取消对 DCP 功能处理过程的打印

配置步骤如下：

```
Switch(Config)# dcp enable
Switch(Config)# dcp limit-rate 50
Switch(Config)# dcp no-limit-ip 1.1.1.1
Switch(config)#show dcp limit-rate
Switch(config)#show cpu ip rate top10
Switch(config)#show dcp limited ip
Switch#clear dcp speed limit rules
Switch#debug dcp packet
Switch#no debug dcp packet
Switch#debug dcp event
Switch#no debug dcp event
```

4.4 DCP 功能排错帮助

在配置、使用 dcp 时，应该注意一下以下几点：

- ☞ 默认配置下，dcp 功能是不使能的，只有通过 **dcp enable** 使能了以后功能才能生效；
- ☞ Dcp 功能只能对 **other-ipuc** 类型的报文进行限速，对协议报文和管理报文无法限速；
- ☞ Dcp no-limited-ip 能够配置最大数量是 **1024**，超过该值后将无法下发；
- ☞ 默认配置下，dcp 对 **other-ipuc** 报文的限速值为 **20**；
- ☞ 当被限速报文的个数在 **5S** 内低于限速值的一半时，针对该 ip 报文的限速将被放开；
- ☞ 可以通过 **show cpu ip rate top10** 查看上 **5S** 内上 CPU 速率最大的前 **10** 个 ip 及其速率；
- ☞ 可以通过 **show dcp limited ip** 当前被限速 ip 节点信息；其中 **Limited-IP** 是被限速的 ip, **Rate(pkts/s)**是指当前的速率。
- ☞ 如果想查看 dcp 对上 cpu 的 **other-ipuc** 报文的处理过程，可以打开 **debug dcp packet** 或者 **debug dcp event** 开关。**debug dcp packet** 命令查看报文的详细信息，包括源 IP，目的 IP，源 port，目的 port，协议号等。**debug dcp event** 可以打印 dcp 的事件处理过程。

第 5 章 COPP 功能调试

5.1 COPP 功能简介

CPU 是整个设备的大脑，负责处理所有控制层面的信息，因此，需要采取适当的措施，对设备 CPU 提供保护，避免网络攻击。CPU 限速保留了之前的协议限速功能，而且 CPU 协议限速改为硬件限速。新增了 COPP 限速功能，COPP（control plane policing）功能可以满足对控制和管理层面的保护，确保路由功能的稳定性和报文的正常传输。首先配置 ACL 规则，支持多种 ACL 规则，通过 ACL 规则对需要限速或过滤的特定报文进行分类，然后通过配置 COPP 策略表匹配对应的 ACL 规则来过滤特定报文或限制报文上 cpu 的速率。COPP 策略表支持单桶和双桶模式以及多种操作动作。

5.2 COPP 功能任务序列

1. 配置 ACL 规则，以数字标准 IP 访问列表为例
2. 建立分类表
3. 建立 copp 策略表
4. 配置策略
5. 应用到端口

1. 配置ACL规则

命令	解释
全局配置模式	
access-list <num> {deny permit} {{<slpAddr> <sMask>} any-source {host-source <slpAddr>}} no access-list <num>	创建一条数字标准 IP 访问列表，如果已有此访问列表，则增加一条规则（rule）表项；本命令的 no 操作为删除一条数字标准 IP 访问列表。

2. 建立分类表

命令	解释
全局配置模式	
class-map <class-map-name> no class-map <class-map-name>	建立一个 class-map（分类表），并进入 class-map 模式；本命令的 no 操作为删除指定的 class-map。
match {access-group <acl-index-or-name> ip dscp <dscp-list> ip precedence	设置分类表中的匹配标准，可以根据 ACL 对数据流进行分类；本命令的 no 操作为删除指定的匹配标准。

<pre> <ip-precedence-list> ipv6 access-group <acl-index-or-name> ipv6 dscp <dscp-list> ipv6 flowlabel <flowlabel-list> vlan <vlan-list> cos <cos-list> vlan range <vlan-list>} no match {access-group ip dscp ip precedence ipv6 access-group ipv6 dscp ipv6 flowlabel vlan cos vlan range} </pre>	
--	--

3. 配置策略表

命令	解释
全局配置模式	
<pre> copp-policy-map <policy-map name> no policy-map <policy-map-name> </pre>	建立一个 copp-policy-map（策略表），并进入 copp-policy-map（策略表）模式；本命令的 no 操作为删除指定的 copp-policy-map。
<pre> class <class-map-name> no class <class-map-name> </pre>	建立一个 copp-policy-map（策略表）之后，可以将其对应于一个 class（策略分类表），并进入策略分类表模式,之后就可以对不同的数据流采取不同的策略；本命令的 no 操作为删除指定策略分类表。
pps 限速模式： <pre> policy packets-per-second <pps> normal-burst-packets <pps> { conform-action exceed-action } <ACTION> no policy </pre> bps 限速模式： 1、单桶模式： <pre> Policy <bits_per_second> <normal_burst_bytes> ({action{{policied-cos-to-cos-transmit{ policied-cos-to-dscp-transmit violate-a ction}}policied-cos-to-dscp-transmit{p olicied-cos-to-cos-transmit violate-acti on }} policied-dscp-exp-to-cos-transmit{poli cied-dscp-exp-to-dscp-transmit violate </pre>	pps限速模式： 支持单桶双色 Policy 命令，限速为 pps 模式，可以根据配置将报文分为不同颜色的报文，并且给不同颜色报文设置相应动作。no 命令删除模式配置。 bps限速模式： 为分类后的流量配置一个策略，支持三色 color 的非聚合 Policy 命令，根据配置参数解析出令牌桶的工作模式，是单速单桶、单速双桶还是双速双桶，并且给不同颜色报文设置相应动作。no 命令删除模式配置。

-action}} policed-dscp-exp-to-dscp-transmit{policed-dscp-exp-to-cos-transmit violate-action }}violate-action {drop transmit}} exceed-action ACTION }) 2、双桶模式: policy <bits_per_second> <normal_burst_bytes> [pir <peak_rate_bps>] <maximum_burst_bytes> [{action{{policed-cos-to-cos-transmit{ policed-cos-to-dscp-transmit violate-action}} policed-cos-to-dscp-transmit{policed-cos-to-cos-transmit violate-action }} policed-dscp-exp-to-cos-transmit{policed-dscp-exp-to-dscp-transmit violate-action}} policed-dscp-exp-to-dscp-transmit{policed-dscp-exp-to-cos-transmit violate-action }} exceed-action violate-action ACTION }] ACTION 定义: drop transmit set-internal-priority <intp_value> policed-intp-transmit no policy	
策略分类表配置模式	
drop no drop transmit no transmit	对分类后的流量可以选择丢弃、通过动作；本命令的 no 操作为取消分配的动作。

4. 应用策略表到端口

命令	解释
端口配置模式	
service-policy output <policy-map name>	在交换机端口出方向上应用一个策略表；本命令的 no 操作为删除应用到交换机端口的某

no	service-policy	output	个指定策略表。
<policy-map-name>			

5.3 COPP 功能配置举例

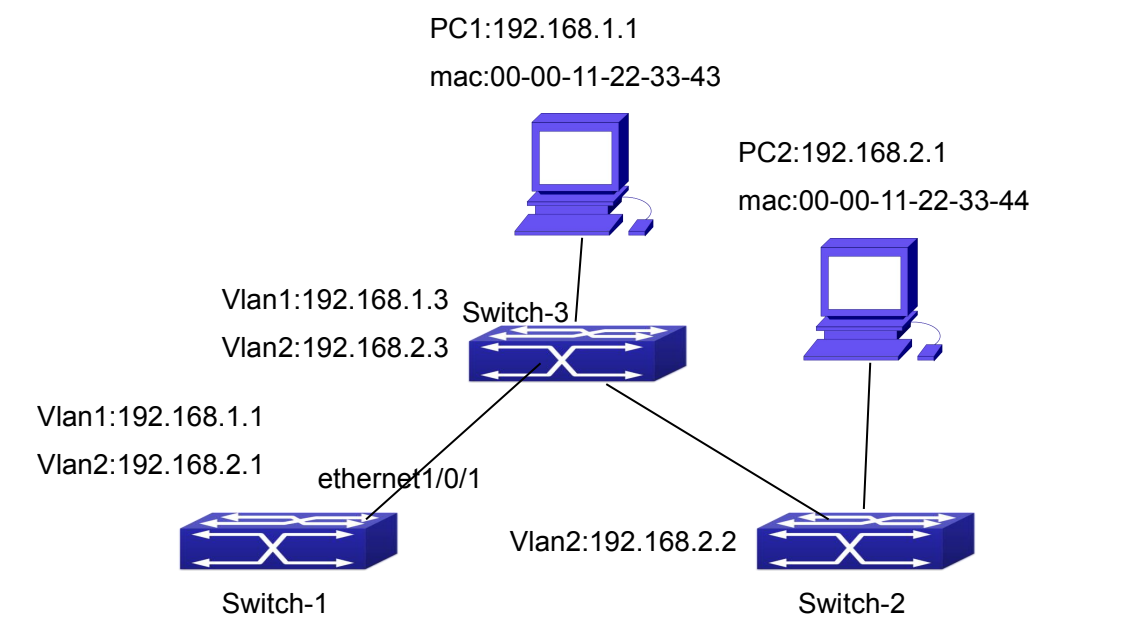


图 4-1 COPP 功能示意图

举例 1：在 Switch-1 端口 ethernet1/0/1 上配置 COPP 策略表，将属于网段 192.168.1.0 内的报文上 cpu 的报文限制为 10pps，突发值设为 20pps，超过带宽的该网段内的报文一律丢弃。

配置步骤如下：

```
Switch#config
Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch(config)#class-map c1
Switch(config-classmap-c1)#match access-group 1
Switch(config-classmap)# exit
Switch(config)#copp-policy-map p1
Switch(config-copp-policymap-p1)#class c1
Switch(config-copp-policymap-p1-class-c1)#policy          packets-per-second          10
normal-burst-packets 20 exceed-action drop
Switch(config-copp-policymap-p1-class-c1)#exit
Switch(config-copp-policymap-p1)# #exit
Switch(config)#interface ethernet 1/0/1
```

```
Switch(config-if-ethernet1/0/1)# service-policy output p1
```

举例 2：在 Switch-1 端口 ethernet1/0/1 上配置 COPP 策略表，将属于源 mac 地址为 00-00-11-22-33-44 的报文上 cpu 的报文限制为 10pps，突发值设为 20pps，超过带宽的该源 mac 地址的报文设置内部优先级为 1 后转发。

配置步骤如下：

```
Switch#config
Switch(config)#access-list 1100 permit host-source-mac 00-00-11-22-33-44
any-destination-mac
Switch(config)#class-map c1
Switch(config-classmap-c1)#match access-group 1100
Switch(config)#copp-policy-map p1
Switch(config-copp-policymap-p1)#class c1
Switch(config-copp-policymap-p1-class-c1)# policy packets-per-second 10
normal-burst-packets 20 exceed-action set-internal-priority 1 transmit
Switch(config-copp-policymap-p1-class-c1)#exit
Switch(config-copp-policymap-p1)# #exit
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# service-policy output p1
```

5.4 COPP 功能排错帮助

- ☞ 属于该网段的报文是否正确上了 cpu，该功能是对上 cpu 的报文限速，可以通过 debug driver receive 查看报文是否上了 cpu。
- ☞ ACL 匹配是否正确，ACL 规则必须是 permit。
- ☞ COPP 策略表是否配置正确，COPP 在端口应用必须是出方向，不支持入方向。
- ☞ 可以通过 show cpu-rx protocol all 命令查看报文统计，确定限速是否生效。