Continue

您好，用这个 Dropped计数持续增长，表明当前存在拥塞丢包8.1 端口队列统计配置命令8.1.1 display qos queue-statistics interface outbounddisplay qos queue-statistics interface outbound命令用来显示端口队列出方向的统计信息。【命令】（独立运行模式）display qos queue-statistics interface [interface-type interface-number [slot slot-number]] outbound（IRF模式）display qos queue-statistics interface [interface-type interface-number [chassis chassis-number slot slot-number]] outbound【视图】任意视图【缺省用户角色】network-adminnetwork-operator【参数】interface-type interface-number：指定接口类型和接口编号。如果未指定本参数，将显示所有接口的队列出方向统计信息。slot slot-number：显示指定单板上接口队列出方向的统计信息。slot-number表示单板所在的槽位号。如果未指定本参数，将按单板显示接口出方向的队列统计信息。只有当指定接口为聚合接口时才支持此参数。（独立运行模式）chassis chassis-number slot slot-number：显示指定成员设备上指定单板上接口队列出方向的统计信息。chassis-number表示设备在IRF中的成员编号，slot-number表示单板所在的槽位号。如果未指定本参数，将按单板显示接口出方向的队列统计信息。只有当指定接口为聚合接口时才支持此参数。（IRF模式）【使用指导】目前设备仅支持显示绿色报文转发的数据包数目、字节数和红色报文丢弃的数据包数目、字节数的统计情况。对于SPEX-1204单板，仅支持显示转发的数据包数目、字节数的统计情况。【举例】# 显示接口GigabitEthernet3/1/1的队列出方向统计信息。 display qos queue-statistics interface GigabitEthernet 3/1/1 outboundInterface: GigabitEthernet3/1/1 Direction: Outbound Forwarded: 10077 packets, 864466 bytes, 0 pps, 0 bps Dropped: 0 packets, 0 bytes, 0 pps, 0 bps Queue 0 Forwarded: 61 packets, 4758 bytes, 0 pps, 0 bps Forwarded(peak): 0 pps, 0 bps Dropped: 0 packets, 0 bytes, 0 pps, 0 bps Green forwarded: 61 packets, 4758 bytes, 0 pps, 0 bps Green dropped: 0 packets, 0 bytes, 0 pps, 0 bps Yellow forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Yellow dropped: 0 packets, 0 bytes, 0 pps, 0 bps Red forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Red dropped: 0 packets, 0 bytes, 0 pps, 0 bps Total queue length: 0 packets Current queue length: 0 packets Queue 1 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Forwarded(peak): 0 pps, 0 bps Dropped: 0 packets, 0 bytes, 0 pps, 0 bps Green forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Green dropped: 0 packets, 0 bytes, 0 pps, 0 bps Yellow forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Yellow dropped: 0 packets, 0 bytes, 0 pps, 0 bps Red forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Red dropped: 0 packets, 0 bytes, 0 pps, 0 bps Total queue length: 0 packets Current queue length: 0 packets Queue 2 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Forwarded(peak): 0 pps, 0 bps Dropped: 0 packets, 0 bytes, 0 pps, 0 bps Green forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Green dropped: 0 packets, 0 bytes, 0 pps, 0 bps Yellow forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Yellow dropped: 0 packets, 0 bytes, 0 pps, 0 bps Red forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Red dropped: 0 packets, 0 bytes, 0 pps, 0 bps Total queue length: 0 packets Current queue length: 0 packets Queue 3 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Forwarded(peak): 0 pps, 0 bps Dropped: 0 packets, 0 bytes, 0 pps, 0 bps Green forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Green dropped: 0 packets, 0 bytes, 0 pps, 0 bps Yellow forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Yellow dropped: 0 packets, 0 bytes, 0 pps, 0 bps Red forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Red dropped: 0 packets, 0 bytes, 0 pps, 0 bps Total queue length: 0 packets Current queue length: 0 packets Queue 4 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Forwarded(peak): 0 pps, 0 bps Dropped: 0 packets, 0 bytes, 0 pps, 0 bps Green forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Green dropped: 0 packets, 0 bytes, 0 pps, 0 bps Yellow forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Yellow dropped: 0 packets, 0 bytes, 0 pps, 0 bps Red forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Red dropped: 0 packets, 0 bytes, 0 pps, 0 bps Total queue length: 0 packets Current queue length: 0 packets Queue 5 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Forwarded(peak): 0 pps, 0 bps Dropped: 0 packets, 0 bytes, 0 pps, 0 bps Green forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Green dropped: 0 packets, 0 bytes, 0 pps, 0 bps Yellow forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Yellow dropped: 0 packets, 0 bytes, 0 pps, 0 bps Red forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Red dropped: 0 packets, 0 bytes, 0 pps, 0 bps Total queue length: 0 packets Current queue length: 0 packets Queue 6 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Forwarded(peak): 0 pps, 0 bps Dropped: 0 packets, 0 bytes, 0 pps, 0 bps Green forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Green dropped: 0 packets, 0 bytes, 0 pps, 0 bps Yellow forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Yellow dropped: 0 packets, 0 bytes, 0 pps, 0 bps Red forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Red dropped: 0 packets, 0 bytes, 0 pps, 0 bps Total queue length: 0 packets Current queue length: 0 packets Queue 7 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Forwarded(peak): 0 pps, 0 bps Dropped: 0 packets, 0 bytes, 0 pps, 0 bps Green forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Green dropped: 0 packets, 0 bytes, 0 pps, 0 bps Yellow forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Yellow dropped: 0 packets, 0 bytes, 0 pps, 0 bps Red forwarded: 0 packets, 0 bytes, 0 pps, 0 bps Red dropped: 0 packets, 0 bytes, 0 pps, 0 bps Total queue length: 0 packets Current queue length: 0 packets表8-1 display qos queue-statistics interface outbound命令显示信息描述表字段描述Interface端口队列统计的端口Direction端口队列统计的方向Forwarded转发的数据包数目、字节数和最近一个时间间隔内的平均速率，时间间隔为flow-interval命令配置的接口统计报文信息的时间间隔Forwarded(peak)转发报文的历史峰值速率从上一次执行reset qos queue-statistics interface outbound命令至当前执行display qos queue-statistics interface outbound命令这段时间中的速率最大值Dropped丢弃的数据包数目、字节数和最近一个时间间隔内的平均速率，时间间隔为flow-interval命令配置的接口统计报文信息的时间间隔Queue 0、Queue 1、Queue 2、Queue 3、Queue 4、Queue 5、Queue 6、Queue 7某端口队列统计信息Green forwarded绿色报文转发的数据包数目、字节数和最近一个时间间隔内的平均速率，时间间隔为flow-interval命令配置的接口统计报文信息的时间间隔Green dropped绿色报文丢弃的数据包数目、字节数和最近一个时间间隔内的平均速率，时间间隔为flow-interval命令配置的接口统计报文信息的时间间隔Yellow forwarded黄色报文转发的数据包数目、字节数和最近一个时间间隔内的平均速率，时间间隔为flow-interval命令配置的接口统计报文信息的时间间隔Yellow dropped黄色报文丢弃的数据包数目、字节数和最近一个时间间隔内的平均速率，时间间隔为flow-interval命令配置的接口统计报文信息的时间间隔Red forwarded红色报文转发的数据包数目、字节数和最近一个时间间隔内的平均速率，时间间隔为flow-interval命令配置的接口统计报文信息的时间间隔Red dropped红色报文丢弃的数据包数目、字节数和最近一个时间间隔内的平均速率，时间间隔为flow-interval命令配置的接口统计报文信息的时间间隔Total queue length队列总长度Current queue length当前队列长度 zhiliao_l2b0v 交换机做acl，阻断vlan11的pc（192.168.11.0/24），访问vlan10的pc（192.168.0.0/24），Acl ad 3001 Rule 0 deny ip source 192.168.11.0 0.0.0.255 destination 192.168.0.0 0.0.0.255 Rule 100 permit ip Quit Int v 10 Pa 3001 in Pa 3001 out Quit 实测 acl 应用在inbound无效，应用在outbound有效，请问各位大佬，这是什么原因？如何理解inbound和outbound的区别？ 悲剧塔 楼上是错的。应当站在你调用acl的接口的位置看，这条acl在vlan 10接口调用，那就应该首先站在vlan10接口的角度，再看acl内容，你acl条目写的是禁止vlan 11访问vlan 10，那站在vlan 10的角度，vlan 11就输入vlan 10的外部，它（vlan 11）想访问vlan10的时候，流量是从vlan 11去往vlan 10，所以：站在vlan 10的角度，上面的过程流量就是从outbound方向来的。 2024-11-12回答 评论(17) 举报 编辑答案 ✖ 你的邮箱还未认证，请认证邮箱或绑定手机后进行当前操作 最佳答案 无名之辈 您好，参考1.1.15 packet-filter globalpacket-filter global命令用来全局应用ACL进行报文过滤。undo packet-filter global命令用来取消全局应用ACL进行报文过滤。【命令】packet-filter [ipv6 | mac | user-defined] { acl-number | name acl-name } global { inbound | outbound } [hardware-count]undo packet-filter [ipv6 | mac | user-defined] { acl-number | name acl-name } global { inbound | outbound }【缺省情况】全局不对报文进行过滤。【视图】系统视图【缺省用户角色】network-adminmdc-admin【参数】ipv6：指定ACL类型为IPv6 ACL。mac：指定ACL类型为二层ACL。user-defined：指定ACL类型为用户自定义ACL。acl-number：指定ACL的编号，取值范围及其代表的ACL类型如下：· 2000～2999：表示基本ACL。· 3000～3999：表示高级ACL。· 4000～4999：表示二层ACL。· 5000～5999：表示用户自定义ACL。name acl-name：指定ACL的名称。acl-name表示ACL的名称，为1～63个字符的字符串，不区分大小写。global：表示全局（即所有物理接口）配置。inbound：对收到的报文进行过滤。outbound：对发出的报文进行过滤。hardware-count：表示开启规则匹配硬件统计功能，缺省为关闭。【使用指导】通过编号引用ACL，请遵循如下规则：· 当需要引用IPv4类型ACL时，请直接指定acl-number。· 当需要引用IPv6类型ACL时，必须首先指定ipv6关键字，再指定acl-number。· 当需要引用二层或用户自定义类型ACL时，可首先指定mac或user-defined关键字再指定acl-number，或直接指定acl-number。通过名称引用ACL，请遵循如下规则：· 当需要引用IPv4类型ACL时，请直接指定name acl-name。· 当需要引用IPv6、二层或用户自定义类型ACL时，必须首先指定ipv6、mac或user-defined关键字，再指定name acl-name。hardware-count关键字用于开启指定ACL内所有规则的规则匹配硬件统计功能，而rule命令中的counting关键字则用于开启当前规则的匹配统计功能。如果设备资源不足，必须先执行undo packet-filter命令取消报文过滤，然后再配置不携带hardware-count关键字的报文过滤，以此关闭规则匹配硬件统计功能。如果设备资源充足，可通过不携带hardware-count关键字重新配置报文过滤，以此关闭规则匹配硬件统计功能。【举例】# 全局应用IPv4基本ACL 2001对收到的报文进行过滤，并开启规则匹配硬件统计功能。 system-view[Sysname] packet-filter 2001 global inbound hardware-count 叫我靓仔 华三交换机调用ACL IPv6 packet-filter在全局调用的ACL命令是：packet-filter [ipv6] { acl-number | name acl-name } { inbound | outbound } [hardware-count]该命令用来在接口上应用IPv6 ACL进行报文过滤，其中：acl-number 表示ACL的编号，取值范围为2000～2999，表示IPv6基本ACL，或3000～3999，表示IPv6高级ACL。acl-name 表示ACL的名称，为1～63个字符的字符串，不区分大小写，必须以英文字母a～z或A～Z开头。inbound 表示对进入接口的报文进行过滤。outbound 表示对从接口发出的报文进行过滤。hardware-count 表示启用硬件计数器，用于统计匹配规则的报文数。例如，如果您想在GigabitEthernet 1/0/1接口上应用编号为2001的IPv6基本ACL进行入方向的报文过滤，并启用硬件计数器，您可以输入以下命令： system-view [Sysname] interface gigabitethernet 1/0/1 [Sysname-GigabitEthernet1/0/1] packet-filter ipv6 2001 inbound hardware-count希望这些信息对您有所帮助。如果您还有其他问题，欢迎继续与我交流。 ☺ 编辑答案 ✖ 你的邮箱还未认证，请认证邮箱或绑定手机后进行当前操作 ✖ 你的邮箱还未认证，请认证邮箱或绑定手机后进行当前操作 nat static outbound命令用来配置出方向一对一静态地址转换映射。undo nat static outbound命令用来删除出方向一对一静态地址转换映射。【命令】nat static outbound local-ip global-ipundo nat static outbound local-ip【缺省情况】不存在任何地址转换映射。【视图】系统视图【缺省用户角色】network-admin【参数】local-ip：内网IP地址。global-ip：外网IP地址。【使用指导】对于从内网到外网的报文，将其源地址local-ip转换为global-ip；对于从外网到内网的报文，将其目的地址global-ip转换为local-ip。【举例】# 配置内网IP地址192.168.1.1到外网IP地址2.2.2.2的出方向静态地址转换映射。 system-view[Sysname] nat static outbound 192.168.1.1 2.2.2.2【相关命令】 nat static inboundnat static inbound命令用来配置入方向一对一静态地址转换映射。undo nat static inbound命令用来删除指定的入方向一对一静态地址转换映射。【命令】nat static inbound global-ip [vpn-instance global-vpn-instance-name] local-ip [vpn-instance local-vpn-instance-name] [acl [ipv4-acl-number | name ipv4-acl-name] [reversible]] [rule rule-name] [priority priority] [disable] [counting]undo nat static inbound global-ip [vpn-instance global-vpn-instance-name] local-ip [vpn-instance local-vpn-instance-name]【缺省情况】不存在地址转换映射。【视图】系统视图【缺省用户角色】network-admincontext-admin【参数】global-ip：外网IP地址。vpn-instance global-vpn-instance-name：外网IP地址所属的VPN实例。global-vpn-instance-name表示MPLS L3VPN的VPN实例名称，为1～31个字符的字符串，区分大小写。如果未指定本参数，则表示外网IP地址不属于任何一个VPN实例。local-ip：内网IP地址。vpn-instance local-vpn-instance-name：内网IP地址所属的VPN实例。local-vpn-instance-name表示MPLS L3VPN的VPN实例名称，为1～31个字符的字符串，区分大小写。如果未指定本参数，则表示内网IP地址不属于任何一个VPN实例。acl：指定ACL的编号或名称，本参数用于控制指定源地址的内网主机可以访问外网。ipv4-acl-number：ACL的编号，取值范围为2000～3999。name ipv4-acl-name：ACL的名称，为1～63个字符的字符串，不区分大小写，必须以英文字母a～z或A～Z开头。为避免混淆，ACL的名称不允许使用英文单词all。reversible：表示从内网主动访问外网的报文必须通过ACL反向匹配，才能使用该配置进行目的地址转换。rule rule-name：NAT规则的名称，取值范围为1～63个字符的字符串，区分大小写，不能包括“\\”、“/”、“:”、“*”、“?”、“\”、“”、“|”、“””和“@”。如果不指定该参数，则表示该规则无名称。priority priority：NAT规则的匹配优先级，取值范围为0～2147483647，数值越小，优先级越高。如果不指定该参数，那么相应的NAT规则在同类NAT规则中，其匹配优先级最低。disable：表示禁用该地址转换映射。如果不指定该参数，则地址转换映射处于启用状态。counting：开启NAT转换计数功能，即对每一次首报文地址转换进行计数。【使用指导】对于从外网到内网的报文，将其源地址global-ip转换为local-ip；对于从内网到外网的报文，将其目的地址local-ip转换为global-ip。指定引用的ACL时，需要注意：· 如果没有指定ACL，则所有从外网到内网的报文都可以使用该配置进行源地址转换；所有从内网到外网的报文都可以使用该配置进行目的地址转换。· 如果仅指定了ACL，没有指定ACL反向匹配（即没有配置reversible），对于从外网到内网的报文，只有报文符合ACL permit规则，才能使用该配置进行源地址转换；对于从内网主动访问外网的报文，不能使用该配置进行目的地址转换。· 如果既指定了ACL，又指定了ACL反向匹配（即配置了reversible），对于外网到内网的报文，只有报文符合ACL permit规则，才能使用该配置进行源地址转换；对于从内网主动访问外网的报文，需要进行ACL反向匹配（提取报文的源地址/端口和目的地址/端口，并根据配置转换目的地址，然后将源地址/端口和目的地址/端口互换去匹配ACL），只有反向匹配ACL的报文才能使用该配置进行转换，否则不予转换。如果接口下既配置了NAT动态地址转换，又配置了NAT静态地址转换，则优先使用静态地址转换。设备可支持配置多条入方向静态地址转换映射（包括nat static inbound和nat static inbound net-to-net）。在VPN组网中，配置入方向静态地址转换时需要指定vpn-instance参数，且VPN实例的名称必须与该接口关联的VPN实例一致。对于引用了ACL的入方向一对一静态地址转换映射，当NAT规则的匹配优先级相同时，设备将按照ACL名称或ACL编号进行匹配，且ACL名称的优先级高于ACL编号的优先级，具体规则如下：· 对于ACL名称，设备将根据名称的字符序对NAT规则进行排序，在字符序中的位置越靠前，相应的NAT规则的匹配优先级越高。· 对于ACL编号，编号越大，优先级越高，设备将优先进行匹配。【举例】# 配置外网IP地址2.2.2.2到内网IP地址192.168.1.1的入方向静态地址转换。 system-view[Sysname] nat static inbound 2.2.2.2 192.168.1.1【相关命令】· display nat all· display nat static· nat static enable 组网如图，配置如下。内网终端相同，想要通过acl匹配不同目的地址，nat outbound转换成不同的源地址。但是测试发现，如果同时访问两个目的地址的话，只会转换成同一个源地址 #nat address-group 1 address 3.3.3.10 3.3.3.20#nat address-group 2 address 3.3.3.40 3.3.3.50##interface GigabitEthernet0/1 port link-mode route combo enable copper ip address 3.3.3.3 255.255.255.0 nat outbound 3001 address-group 2 no-pat nat outbound 3000 address-group 1 no-pat# acl advanced 3000 rule 5 permit ip source 10.0.0.1 0 destination 40.0.0.1 0 acl advanced 3001 rule 0 permit ip source 10.0.0.1 0 destination 30.0.0.1 0 设备上debug nat packet发现，10.0.0.1访问30.0.0.1和40.0.0.1确实都转换成了address-group 1中相同的地址 [H3C-acl-ipv4-adv-3000]*Dec 17 12:54:22:042 2024 H3C NAT/7/COMMON: PACKET: (GigabitEthernet0/1-out-config) Protocol: ICMP 10.0.0.1:10987 - 30.0.0.1: 2048(VPN: 0) ------> 3.3.3.15:10987 - 30.0.0.1: 2048(VPN: 0)*Dec 17 12:54:22:043 2024 H3C NAT/7/COMMON: PACKET: (GigabitEthernet0/1-in-session) Protocol: ICMP 30.0.0.1:10987 - 3.3.3.15: 0(VPN: 0) ------> 30.0.0.1:10987 - 10.0.0.1: 0(VPN: 0)*Dec 17 12:54:26:739 2024 H3C NAT/7/COMMON: PACKET: (GigabitEthernet0/1-out-config) Protocol: ICMP 10.0.0.1:10988 - 40.0.0.1: 2048(VPN: 0) ------> 3.3.3.15:10988 - 40.0.0.1: 2048(VPN: 0)*Dec 17 12:54:26:739 2024 H3C NAT/7/COMMON: PACKET: (GigabitEthernet0/1-in-session) Protocol: ICMP 40.0.0.1:10988 - 3.3.3.15: 0(VPN: 0) ------> 40.0.0.1:10988 - 10.0.0.1: 0(VPN: 0) 经确认，no-pat方式只会匹配源ip，当已经有了一个会话的时候，后面所有相同的源ip都会转换成相同的地址，去掉no-pat之后可以正常匹配acl，转换成对应address-group中的地址 ✖ 你的邮箱还未认证，请认证邮箱或绑定手机后进行当前操作