H3C S12500G-AF & S10500X & S10500 & S7500X & S7500E 流量统计专题

S12500G-AF 系列交换机
S10500X 系列交换机
S10500 系列交换机
S7500X 系列交换机
S7500E 系列交换机

资料版本：6W100-20230905

目 录

1 流量统计概述 ····· 1

2 流量统计技术介绍 ····· 1

2.1 命令行 ····· 1

2.2 SNMP ····· 2

2.3 NETCONF ····· 4

2.4 gRPC ····· 6

3 接口流量统计实现 ····· 8

3.1 二层以太网接口/二层聚合组成员接口流量统计 ····· 8

3.1.1 命令行方式实现 ····· 8

3.1.2 SNMP 实现 ····· 14

3.1.3 NETCONF 实现 ····· 19

3.1.4 gRPC 实现 ····· 21

3.2 以太网接口错误报文流量统计 ····· 22

3.2.1 命令行方式实现 ····· 22

3.2.2 SNMP 实现 ····· 24

3.2.3 NETCONF 实现 ····· 26

3.2.4 gRPC 实现 ····· 28

3.3 三层以太网接口/三层以太网子接口/三层聚合成员接口流量统计 ····· 29

3.3.1 命令行方式实现 ····· 29

3.3.2 SNMP 实现 ····· 37

3.3.3 NETCONF 实现 ····· 41

3.3.4 gRPC 实现 ····· 43

3.4 二层聚合接口流量统计 ····· 43

3.4.1 命令行方式实现 ····· 43

3.4.2 SNMP 实现 ····· 45

3.4.3 NETCONF 实现 ····· 47

3.4.4 gRPC 实现 ····· 49

3.5 三层聚合接口流量统计 ····· 49

3.5.1 命令行方式实现 ····· 49

3.5.2 SNMP 实现 ····· 50

3.5.3 NETCONF 实现 ····· 53

3.5.4 gRPC 实现 ····· 55

3.6 接口丢包统计（基于 MQC 实现）……56
3.6.1 需求说明……56
3.6.2 命令行方式实现……56
3.6.3 SNMP 方式实现……57
3.6.4 NETCONF 实现……59
3.6.5 gRPC 方式实现……62
3.7 以太网接口流量统计（基于 MQC 实现）……63
3.7.1 需求说明……63
3.7.2 命令行方式实现……63
3.7.3 SNMP 方式实现……65
3.7.4 NETCONF 实现……67
3.7.5 gRPC 方式实现……68
4 VXLAN 流量统计实现……69
4.1 AC 流量统计……69
4.1.1 需求说明……69
4.1.2 配置限制和指导……69
4.1.3 命令行方式实现……70
4.1.4 SNMP 方式实现……72
4.1.5 NETCONF 方式实现……74
4.1.6 gRPC 方式实现……76
4.2 VSI 流量统计功能……77
4.2.1 需求说明……77
4.2.2 命令行方式实现……77
4.2.3 SNMP 方式实现……78
4.2.4 NETCONF 方式实现……80
4.2.5 gRPC 方式实现……82
4.3 getgetAC 流量统计（基于 MQC 实现）……83
4.3.1 需求说明……83
4.3.2 命令行方式实现……83
4.3.3 SNMP 方式实现……85
4.3.4 NETCONF 实现……87
4.4 gRPC 方式实现……89
4.4.1 配置需求……89
4.4.2 配置步骤……89
4.4.3 查询流量统计数据……89
4.4.4 更多信息……90

5 VLAN 流量统计实现 90
5.1 需求说明 90
5.2 命令行方式实现 90
5.2.1 配置需求 90
5.2.2 配置限制和指导 90
5.2.3 配置步骤 90
5.2.4 查询流量统计数据 90
5.2.5 更多信息 91
5.3 SNMP 方式实现 91
5.3.1 配置需求 91
5.3.2 配置步骤 92
5.3.3 查询流量统计数据示例 92
5.3.4 更多信息 93
5.4 NETCONF 实现 93
5.4.1 配置需求 93
5.4.2 配置步骤 94
5.4.3 查询流量统计数据示例 94
5.4.4 更多信息 95
5.5 gRPC 方式实现 95
5.5.1 配置需求 95
5.5.2 配置步骤 95
5.5.3 查询流量统计数据 96
5.5.4 更多信息 96
6 VPN 实例流量统计实现 96
6.1 需求说明 96
6.2 命令行方式实现 97
6.2.1 配置需求 97
6.2.2 配置限制和指导 97
6.2.3 配置步骤 97
6.2.4 查询流量统计数据 97
6.2.5 更多信息 98
6.3 SNMP 方式实现 98
6.3.1 配置需求 98
6.3.2 配置步骤 98
6.3.3 查询流量统计数据示例 99
6.3.4 更多信息 101

6.4 NETCONF 实现 101
6.4.1 配置需求 101
6.4.2 配置步骤 101
6.4.3 查询流量统计数据示例 101
6.4.4 更多信息 102
6.5 gRPC 方式实现 102
6.5.1 配置需求 102
6.5.2 配置步骤 103
6.5.3 查询流量统计数据 103
6.5.4 更多信息 103
7 队列流量统计实现 104
7.1 接口队列的流量统计 104
7.1.1 需求说明 104
7.1.2 命令行方式实现 104
7.1.3 SNMP 方式实现 105
7.1.4 NETCONF 实现 108
7.1.5 gRPC 方式实现 109
7.2 接口队列丢包统计 110
7.2.1 需求说明 110
7.2.2 命令行方式实现 111
7.2.3 NETCONF 实现 111
7.2.4 gRPC 方式实现 113
8 流量统计应用案例 114
8.1 通过统计 ICMP 流量定位流量不通的位置 114
8.1.1 需求说明 114
8.1.2 定位思路 114
8.1.3 定位步骤 115
8.2 通过统计 DHCP 报文定位终端未成功获取 IP 地址的原因 116
8.2.1 需求说明 116
8.2.2 定位思路 116
8.2.3 定位步骤 116

1 流量统计概述

流量统计是基于设备进出报文的分类统计功能，涉及接口、隧道、VPN、VXLAN 等多个特性。流量统计数据可用于数据分析、流量计费和故障定位等。

为满足不同用户不同场景下的流量统计，H3C 交换机支持多种流量统计方式：

- 命令行：设备提供的用于流量统计方式，无需借助第三方功能。关于命令行流量统计方式更多介绍，请参见 2.1 命令行。
- SNMP：NMS（Network Management System，网络管理系统）通过 SNMP（Simple Network Management Protocol，简单网络管理协议）协议对网络上不同厂商、不同物理特性、采用不同互联技术的设备进行流量统计。关于 SNMP 更多介绍，请参见“2.2 SNMP”。
- NETCONF：NETCONF（Network Configuration Protocol，网络配置协议）是一种基于 XML 的网络管理协议，它提供了一种可编程的、对网络设备进行配置和管理的方法。用户可以通过该协议获取设备的统计信息。关于 NETCONF 更多介绍，请参见“2.3 NETCONF”。
- gRPC：通过在设备上配置 gRPC Dial-out 模式，使设备周期向采集器推送数据统计信息。关于 gRPC 更多介绍，请参见“2.4 gRPC”。

配置流量统计会对设备转发性能产生一定的影响，例如通过 MQC 进行流量统计，当应用 MQC 进行流量统计的接口越多，设备转发性能下降的越多。请在必要的场景下合理使用。

2 流量统计技术介绍

2.1 命令行

命令行流量统计有几种方式：

- 使用 **display interface/display ip interface/display ipv6 interface** 命令直接查看指定接口的流量统计数据，比如二层以太网接口/三层以太网接口/三层以太网子接口/二层聚合接口/三层聚合接口/拆分接口。
- 先在指定接口开启三层流量统计功能，然后在使用 **display interface** 命令查看接口流量统计数据，比如二层以太网接口、三层以太网接口。
- 先配置指定功能，然后在指定位置开启流量统计功能。比如读取 AC、VSI 口流量统计数据。
- 通过 MQC 方式获取指定位置的流量统计数据。MQC（模块化 QoS 配置，Modular QoS Configuration）通过 QoS 策略定义不同类别的流量要采取的动作，并将 QoS 策略应用到不同的目标位置（例如接口、VLAN）来实现对业务流量的统计。相对命令行其他统计方式，MQC 可以统计的流量种类更多。例如您可以通过流分类匹配各种条件的报文，例如内层 VLAN Tag 802.1p 优先级、DSCP、ACL 规则等。统计信息包括通过和丢弃的报文数或字节数，以及丢弃的报文中由过滤动作或者 CAR 动作造成丢弃的报文数或字节数。

不同统计方式可支持统计的数据类型可能不同。如 **display interface/display ip interface/display ipv6 interface** 等命令行，仅支持统计接口的流量统计数据，不支持

统计 VLAN、VPN 的流量数据，MQC 不仅支持统计接口（除 VLAN 接口）的流量数据，还支持统计 VXLAN、VPN、VLAN 流量数据。

2.2 SNMP

1. SNMP 简介

SNMP（Simple Network Management Protocol，简单网络管理协议）广泛用于网络设备的远程管理和操作。SNMP 允许管理员通过 NMS 对网络上不同厂商、不同物理特性、采用不同互联技术的设备进行管理。

H3C 设备通过 SNMP Get 操作实现的流量统计。

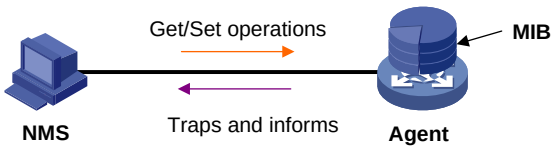
2. SNMP 的网络架构

SNMP（Simple Network Management Protocol，简单网络管理协议）允许管理员通过 NMS（Network Management System，网络管理系统）对网络上不同厂商、不同物理特性、采用不同互联技术的设备进行流量统计

SNMP 网络架构由三部分组成：NMS、Agent 和 MIB。NMS、Agent 和 MIB 之间的关系如图 2-1 所示。

- NMS（Network Management System，网络管理系统）是 SNMP 网络的管理者，能够提供友好的人机交互界面，来获取、设置 Agent 上参数的值，方便网络管理员完成大多数的网络管理工作。
- Agent 是 SNMP 网络的被管理者，负责接收、处理来自 NMS 的 SNMP 报文。在某些情况下，如接口状态发生改变时，Agent 也会主动向 NMS 发送告警信息。
- MIB（Management Information Base，管理信息库）是被管理对象的集合。NMS 管理设备的时候，通常会关注设备的一些参数，比如接口状态、CPU 利用率等，这些参数就是被管理对象，在 MIB 中称为节点。每个 Agent 都有自己的 MIB。MIB 定义了节点之间的层次关系以及对象的一系列属性，比如对象的名称、访问权限和数据类型等。被管理设备都有自己的 MIB 文件，在 NMS 上编译这些 MIB 文件，就能生成该设备的 MIB。NMS 根据访问权限对 MIB 节点进行读/写操作，从而实现对 Agent 的管理。

图2-1 NMS、Agent 和 MIB 关系图

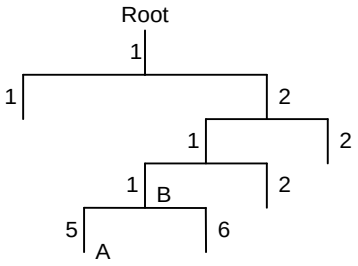


3. MIB 和 MIB 视图

MIB 以树状结构进行存储。树的每个节点都是一个被管理对象，它用从根开始的一条路径唯一地识别（OID）。如图 2-2 所示，被管理对象 B 可以用一串数字{1.2.1.1}唯一确定，这串数字是被管理对象的 OID（Object Identifier，对象标识符）。

MIB 视图是 MIB 的子集合，将团体名/用户名与 MIB 视图绑定，可以限制 NMS 能够访问的 MIB 对象。当用户配置 MIB 视图包含某个 MIB 子树时，NMS 可以访问该子树的所有节点；当用户配置 MIB 视图不包含某个 MIB 子树时，NMS 不能访问该子树的所有节点。

图2-2 MIB 树结构



4. SNMP 版本介绍

目前，设备运行于非 FIPS 模式时，支持 SNMPv1、SNMPv2c 和 SNMPv3 三种版本；设备运行于 FIPS 模式时，只支持 SNMPv3 版本。只有 NMS 和 Agent 使用的 SNMP 版本相同时，NMS 才能和 Agent 建立连接。

- SNMPv1 采用团体名（Community Name）认证机制。团体名类似于密码，用来限制 NMS 和 Agent 之间的通信。如果 NMS 配置的团体名和被管理设备上配置的团体名不同，则 NMS 和 Agent 不能建立 SNMP 连接，从而导致 NMS 无法访问 Agent，Agent 发送的告警信息也会被 NMS 丢弃。
- SNMPv2c 也采用团体名认证机制。SNMPv2c 对 SNMPv1 的功能进行了扩展：提供了更多的操作类型；支持更多的数据类型；提供了更丰富的错误代码，能够更细致地区分错误。
- SNMPv3 采用 USM（User-Based Security Model，基于用户的安全模型）认证机制。网络管理员可以配置认证和加密功能。认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对 NMS 和 Agent 之间的传输报文进行加密，以免被窃听。采用认证和加密功能可以为 NMS 和 Agent 之间的通信提供更高的安全性。

5. SNMP 支持的访问控制方式

SNMP 支持的访问控制方式包括：

- VACM（View-based Access Control Model，基于视图的访问控制模型）：将团体名/用户名与指定的 MIB 视图进行绑定，可以限制 NMS 能够访问哪些 MIB 对象，以及对 MIB 对象不同的操作权限。
- RBAC（Role Based Access Control，基于角色的访问控制）：创建团体名/用户名时，可以指定对应的用户角色，通过用户角色下制定的规则，来限制 NMS 能够访问哪些 MIB 对象，以及对 MIB 对象不同的操作权限。
  - 拥有 network-admin、mdc-admin 或 level-15 用户角色的 SNMP 团体/用户，可以对所有的 MIB 对象进行读写操作；
  - 拥有 network-operator 或 mdc-operator 用户角色的 SNMP 团体/用户，可以对所有的 MIB 对象进行读操作；
  - 拥有自定义用户角色的 SNMP 团体/用户，可以对角色规则中指定的 MIB 对象进行操作。

对于同一 SNMP 用户名/团体名，只能配置一种控制方式，多次使用两种控制方式配置同一用户名/团体名时，以最后一次的配置方式为准。

RBAC 配置方式限制的是 MIB 节点的读写权限，VACM 配置方式限制的是 MIB 视图的读写权限，而一个视图中通常包括多个 MIB 节点。所以，RBAC 配置方式更精准、更灵活。

2.3 NETCONF

1. NETCONF 简介

NETCONF（Network Configuration Protocol，网络配置协议）是一种基于 XML 的网络管理协议，它提供了一种可编程的、对网络设备进行配置和管理的方法。用户可以通过该协议设置属性、获取属性值、获取统计信息等。这使得它在第三方软件的开发上非常便利，很容易开发出在混合不同厂商、不同设备的环境下的特殊定制的网管软件。

2. NETCONF 协议结构

NETCONF 协议采用分层结构，分为内容层（Content）、操作层（Operations）、RPC（Remote Procedure Call，远程调用）层和通信协议层（Transport Protocol）等。

表2-1 XML 分层与 NETCONF 分层模型对应关系

NETCONF 分层	XML 分层	说明
内容层	配置数据、状态数据、统计信息等	被管理对象的集合，可以是配置数据、状态数据、统计信息等 NETCONF协议具体可读写的数据请参见《NETCONF XML API 手册》
操作层	<get>,<get-config>,……	在RPC中应用的基本的原语操作集，这些操作组成NETCONF的基本能力 NETCONF全面地定义了对被管理设备的各种流量统计操作
RPC层	<rpc>,<rpc-reply>	为RPC模块的编码提供了简单的、传输协议无关的机制。通过使用<rpc>和<rpc-reply>元素分别对NETCONF请求和响应数据（即操作层和内容层的内容）进行封装
通信协议层	非FIPS模式下： Console/Telnet/SSH/HTTP/HTTPS/TLS FIPS模式下： Console/SSH/HTTPS/TLS	为NETCONF提供面向连接的、可靠的、顺序的数据链路。 非FIPS模式下： • NETCONF 支持 Telnet、SSH 和 Console 等 CLI 登录方式/协议，即 NETCONF over SSH、NETCONF over Telnet 和 NETCONF over Console • NETCONF 支持封装成 SOAP（Simple Object Access Protocol，简单对象访问协议）报文后通过 HTTP 或 HTTPS 协议传输，即 NETCONF over SOAP over HTTP 和 NETCONF over SOAP over HTTPS FIPS模式下： • NETCONF 支持 SSH 和 Console 等 CLI 方式/协议，即 NETCONF over SSH 和 NETCONF over Console • NETCONF 支持封装成 SOAP 报文后通过 HTTPS 协议传输，即 NETCONF over SOAP over HTTPS

3. NETCONF 报文格式

- NETCONF

NETCONF 命令必须符合 XML 语言的基本格式，格式遵循 RFC 4741。

NETCONF 操作以及可操作的数据项，请参见《NETCONF XML API 手册》。NETCONF 报文的数据合法性都将经过校验才会下发，如果校验失败则会向客户端报错。其中，数据合法性校验通过 XML Schema 的方式完成。

如下为一个 NETCONF 报文示例，用于获取设备上所有接口的所有参数：

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
        <Ifmgr>
          <Interfaces>
                 <Interface/>
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get>
</rpc>
```

- NETCONF over SOAP

NETCONF over SOAP 之后，NETCONF 报文会放在 SOAP 报文的 BODY 元素里，这些报文除了需要遵循纯 NETCONF 报文的规则外，还需要遵循以下规则：

- SOAP 消息必须用 XML 来编码。
- SOAP 消息必须使用 SOAP Envelope 命名空间。
- SOAP 消息必须使用 SOAP Encoding 命名空间。
- SOAP 消息不能包含 DTD（Document Type Definition，文件类型定义）引用。
- SOAP 消息不能包含 XML 处理指令。

如下为一个 NETCONF over SOAP 报文示例，用于获取设备上所有接口的所有参数：

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
  <env:Header>
    <auth:Authentication env:mustUnderstand="1"
xmlns:auth="http://www.h3c.com/netconf/base:1.0">
      <auth:AuthInfo>800207F0120020C</auth:AuthInfo>
    </auth:Authentication>
  </env:Header>
  <env:Body>
    <rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <get>
        <filter type="subtree">
          <top xmlns="http://www.h3c.com/netconf/data:1.0">
            <Ifmgr>
              <Interfaces>
                <Interface/>
              </Interfaces>
            </Ifmgr>
          </top>
        </filter>
      </get>
    </rpc>
  </env:Body>
</env:Envelope>
```

4. 连接方式介绍

本系列交换机支持如下连接方式：

非 FIPS 模式下：

- NETCONF over SSH
- NETCONF over Telnet
- NETCONF over Console
- NETCONF over SOAP over HTTP
- NETCONF over SOAP over HTTPS

FIPS 模式下：

- NETCONF over SSH
- NETCONF over Console
- NETCONF over SOAP over HTTPS

不同配置方式使用的连接方式不同：

- 使用 Telnet 登录到设备并进入 XML 视图即建立 NETCONF over Telnet 连接。
- 使用 Console 登录到设备并进入 XML 视图即建立 NETCONF over Console 连接。建议尽量不使用 NETCONF over Console 方式，因 Console 口的速度限制，且 XML 视图下不输出提示、告警信息，比较容易出现错误。
- 使用 SSH 配置工具或使用 SSH 登录到设备进入 XML 视图执行 NETCONF 配置时需要使用 NETCONF over SSH 连接方式。

使用 SOAP 配置工具下发 NETCONF 指令配置设备时，需要使用 NETCONF over SOAP over HTTP 或 NETCONF over SOAP over HTTPS 方式。

说明

本手册仅介绍 NETCONF over SOAP 方式进行流量统计，其他方式请参见《使用 NETCONF 配置设备操作指导书》。

2.4 gRPC

1. gRPC 简介

gRPC（Google Remote Procedure Call，Google 远程过程调用）是 Google 发布的基于 HTTP 2.0 协议承载的高性能开源软件框架，提供了支持多种编程语言的、对网络设备进行配置和管理的方法。通信双方可以基于该软件框架进行二次开发。

2. gRPC 协议介绍

gRPC 协议栈分层如图 2-3 所示。

表2-2 gRPC 协议栈分层模型

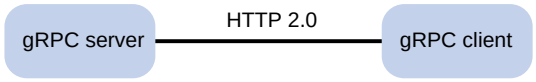
分层	说明
内容层	业务模块的数据

分层	说明
	通信双方需要了解彼此的数据模型，才能正确交互信息
Protocol Buffers编码层	gRPC通过Protocol Buffers编码格式承载数据
gRPC层	远程过程调用，定义了远程过程调用的协议交互格式
HTTP 2.0层	gRPC承载在HTTP 2.0协议上
TCP层	TCP连接提供面向连接的、可靠的、顺序的数据链路

3. gRPC 网络架构

如图 2-3 所示，gRPC 网络采用客户端/服务器模型，使用 HTTP 2.0 协议传输报文。

图2-3 gRPC 网络架构



gRPC 网络的工作机制如下：

(1) 服务器通过监听指定服务端口来等待客户端的连接请求。

(2) 用户通过执行客户端程序登录到服务器。

(3) 客户端调用 proto 文件提供的 gRPC 方法发送请求消息。

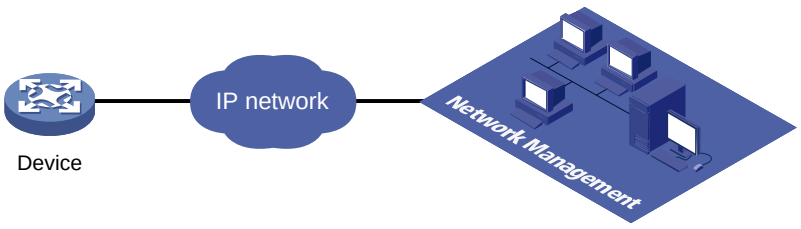
(4) 服务器回复应答消息。

H3C 设备支持作为 gRPC 服务器或者 gRPC 客户端。

4. 基于 gRPC 的 Telemetry 技术

如图 2-4 所示，网络设备和网管系统建立 gRPC 连接后，网管可以订阅设备上指定模块的数据信息。

图2-4 基于 gRPC 的 Telemetry 技术



5. Dial-in 模式和 Dial-out 模式

图 2-4 中，设备支持以下两种 gRPC 对接模式：

- Dial-in 模式：设备作为 gRPC 服务器，采集器作为 gRPC 客户端。由采集器主动向设备发起 gRPC 连接并订阅需要采集的数据信息。

  Dial-in 模式适用于小规模网络和采集器需要向设备下发配置的场景。
- Dial-out 模式：设备作为 gRPC 客户端，采集器作为 gRPC 服务器。设备主动和采集器建立 gRPC 连接，将设备上配置的订阅数据推送给采集器。

  Dial-out 模式适用于网络设备较多的情况下向采集器提供设备数据信息。

H3C 设备通过 Dial-out 方式实现流量统计。

6. Protocol Buffers 编码格式

Protocol Buffers 编码提供了一种灵活、高效、自动序列化结构数据的机制。Protocol Buffers 与 XML、JSON 编码类似，不同之处在于 Protocol Buffers 是一种二进制编码，性能更高。

7. proto 文件

Protocol Buffers 编码通过 proto 文件描述数据结构，用户可以利用 Protoc 等工具软件根据 proto 文件自动生成其他编程语言（例如 Java、C++）代码，然后基于这些生成的代码进行二次开发，以实现 gRPC 设备对接。

H3C 为 Dial-in 模式和 Dial-out 模式分别提供了 proto 文件。

8. Dial-in 模式的 proto 文件

- 公共 proto 文件

grpc_service.proto 文件定义了 Dial-in 模式下的公共 RPC 方法（例如 Login、Logout）。

- 业务模块 proto 文件

Dial-in 模式支持 Device、Ifmgr、IPFW、LLDP、Syslog 等多个业务模块的 proto 文件，描述具体的业务数据格式。

9. Dial-out 模式的 proto 文件

grpc_dialout.proto 文件定义了 Dial-out 模式下的公共 RPC 方法。

10. 获取 proto 文件的方法

请联系 H3C 技术支持。

3 接口流量统计实现

3.1 二层以太网接口/二层聚合组成员接口流量统计

说明

- 本节的二层以太网接口包括设备的固定接口和 100G/400G 接口拆分出来的 25G/10G 接口。
- 二层以太网接口流量统计与二层聚合组成员接口流量统计方式相同，以下以二层以太网接口流量统计为例。

3.1.1 命令行方式实现

1. 配置需求

获取接口 HundredGigE2/0/25 流量统计数据。

2. 配置限制和指导

- 可直接使用 **display interface** 命令获取二层以太网接口的流量统计信息。

- 对于二层聚合组成员接口，统计数据不区分 IPv4 和 IPv6 报文。
- 二层以太网接口支持开启三层流量统计功能。开启三层流量统计功能后，通过 **display interface** 命令可查询接口的 IPv4 和 IPv6 报文流量统计信息。
- 不支持通过 **display ip interface** 或 **display ipv6 interface** 命令查看接口流量统计信息。
- 在某些情况，需要统计某一时段的接口流量统计数据，可以在用户视图通过 **reset counters interface** 命令清除接口原有报文统计信息，重新进行统计。
- **reset counters interface** 命令能够清除 **display interface** 命令行的端口计数但不能清除 MIB 节点计数。

3. 配置步骤

（可选）开启接口 HundredGigE2/0/25 的三层流量统计功能。

```
<Sysname> system-view
[Sysname] interface hundredgige 2/0/25
[Sysname-HundredGigE2/0/25] statistics l3-packet enable inbound
[Sysname-HundredGigE2/0/25] statistics l3-packet enable outbound
```

4. 查询流量统计数据示例

- 未开启三层流量统计功能时，使用 **display interface** 命令进行流量统计。

  # 查询接口 HundredGigE2/0/25 流量统计信息。

```
[Sysname]display interface HundredGigE 2/0/25
HundredGigE2/0/25
........
 Peak input rate: 0 bytes/sec, at 2022-04-07 16:07:11
 Peak output rate: 0 bytes/sec, at 2022-04-07 16:07:11
 Last 300 seconds input: 0 packets/sec 0 bytes/sec 0%
 Last 300 seconds output: 0 packets/sec 0 bytes/sec 0%
 Input (total):  612 packets, 77760 bytes
         606 unicasts, 1 broadcasts, 5 multicasts, 0 pauses
 Input (normal):  612 packets, - bytes
         606 unicasts, 1 broadcasts, 5 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, - overruns, 0 aborts
         - ignored, - parity errors
 Output (total): 614 packets, 77888 bytes
         607 unicasts, 3 broadcasts, 4 multicasts, 0 pauses
 Output (normal): 614 packets, - bytes
         607 unicasts, 3 broadcasts, 4 multicasts, 0 pauses
 Output: 0 output errors, - underruns, 0 buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, - no carrier
```

表3-1 display interface 命令显示信息描述表

字段	描述
HundredGigE2/0/25	接口HundredGigE2/0/25的相关信息
Peak input rate	接口输入流量的峰值速率大小（单位为bytes/sec）以及峰值产生的时间

Peak output rate	接口输出流量的峰值速率大小（单位为bytes/sec）以及峰值产生的时间
Last *interval* seconds input: 0 packets/sec 0 bytes/sec 0% Last *interval* seconds output: 0 packets/sec 0 bytes/sec 0%	端口在最近一个统计周期内接收和发送报文的平均速率，单位分别为数据包/秒和字节/秒，以及实际速率和接口带宽的百分比。统计周期*interval*可以通过**flow-interval**命令设置 如果值显示为“-”，则表示不支持该统计项
Input(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口接收报文的统计值，包括正常报文、异常报文和正常PAUSE帧的报文数、字节数 端口接收的单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
Input(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口接收的正常报文的统计值，包括正常报文和正常PAUSE帧的报文数、字节数 端口接收的正常单播报文、广播报文、组播报文和P AUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
input errors	端口接收的错误报文的统计值
runts	接收到的超小帧的数量 超小帧是指长度小于64字节、格式正确且包含有效的CRC字段的帧
giants	接收到的超大帧的数量 超大帧是指有效长度大于端口允许通过最大报文长度的帧： • 对于禁止长帧通过的以太网端口，超大帧是指有效长度大于 1518 字节（不带 VLAN Tag）或大于 1522 字节（带 VLAN Tag 报文）的帧 • 对于允许长帧通过的以太网端口，超大帧是指有效长度大于指定最大长帧长度的帧
throttles	接收到的长度为非整数字节的帧的个数
CRC	接收到的CRC校验错误、长度正常的帧的数量
frame	接收到的CRC校验错误、且长度不是整字节数的帧的数量
overruns	当端口的接收速率超过接收队列的处理能力时，导致报文被丢弃
aborts	接收到的非法报文总数，非法报文包括： • 报文碎片：长度小于 64 字节（长度可以为整数或非整数）且 CRC 校验错误的帧 • jabber 帧：有效长度大于端口允许通过的最大报文长度，且 CRC 校验错误的帧（长度可以为整字节数或非整字节数）。如对于禁止长帧通过的以太网端口，jabber 帧是指大于 1518（不带 VLAN Tag）或 1522（带 VLAN Tag）字节，且 CRC 校验错误的帧；对于允许长帧通过的以太网端口，jabber 帧是指有效长度大于指定最大长帧长度，且 CRC 校验错误的帧 • 符号错误帧：报文中至少包含 1 个错误的符号 • 操作码未知帧：报文是 MAC 控制帧，但不是 Pause 帧 • 长度错误帧：报文中 802.3 长度字段与报文实际长度（46～1500 字节）不匹配
ignored	由于端口接收缓冲区不足等原因而丢弃的报文数量
parity errors	接收到的奇偶校验错误的帧的数量

Output(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口发送报文的统计值，包括正常报文、异常报文和正常PAUSE帧的报文数、字节数 端口发送的单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
Output(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口发送的正常报文的统计值，包括正常报文和正常PAUSE帧的报文数、字节数 端口发送的正常单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
output errors	各种发送错误的报文总数
underruns	当端口的发送速率超过了发送队列的处理能力，导致报文被丢弃，是一种非常少见的硬件异常
buffer failures	由于端口发送缓冲区不足而丢弃的报文数量
aborts	发送失败的报文总数，即报文已经开始发送，但由于各种原因（如冲突）而导致发送失败
deferred	延迟报文的数量，延迟报文是指发送前检测到冲突而被延迟发送的报文
collisions	冲突帧的数量，冲突帧是指在发送过程中检测到冲突的而停止发送的报文
late collisions	延迟冲突帧的数量，延迟冲突帧是指帧的前512 bits已经被发送，由于检测到冲突，该帧被延迟发送
lost carrier	载波丢失，一般适用于串行WAN接口，发送过程中，每丢失一个载波，此计数器加一
no carrier	无载波，一般适用于串行WAN接口，当试图发送帧时，如果没有载波出现，此计数器加一

- 开启三层流量统计功能后，使用 **display interface** 命令进行流量统计。

  # 查询接口 HundredGigE2/0/25 流量统计信息。

```
[Sysname]display interface HundredGigE 2/0/25
HundredGigE2/0/25
........
 Peak input rate: 0 bytes/sec, at 2022-04-07 16:07:11
 Peak output rate: 0 bytes/sec, at 2022-04-07 16:07:11
 Last 300 seconds input: 0 packets/sec 0 bytes/sec 0%
 Last 300 seconds output: 0 packets/sec 0 bytes/sec 0%
 Input (total):  612 packets, 77760 bytes
         606 unicasts, 1 broadcasts, 5 multicasts, 0 pauses
 Input (normal):  612 packets, - bytes
         606 unicasts, 1 broadcasts, 5 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, - overruns, 0 aborts
         - ignored, - parity errors
 Output (total): 614 packets, 77888 bytes
         607 unicasts, 3 broadcasts, 4 multicasts, 0 pauses
 Output (normal): 614 packets, - bytes
         607 unicasts, 3 broadcasts, 4 multicasts, 0 pauses
```

```
 Output: 0 output errors, - underruns, 0 buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, - no carrier
IPv4 traffic statistics:
 Last 300 seconds input rate: 0 packets/sec, 0 bytes/sec
 Last 300 seconds output rate: 0 packets/sec, 0 bytes/sec
 Input: 300 packets, 38400 bytes
 Output: 300 packets, 38400 bytes
IPv6 traffic statistics:
 Last 300 seconds input rate: 0 packets/sec, 0 bytes/sec
 Last 300 seconds output rate: 0 packets/sec, 0 bytes/sec
 Input: 300 packets, 38400 bytes
 Output: 300 packets, 38400 bytes
```

表3-2 display interface 命令显示信息描述表

字段	描述
HundredGigE2/0/25	接口HundredGigE2/0/25的相关信息
Peak input rate	接口输入流量的峰值速率大小（单位为bytes/sec）以及峰值产生的时间
Peak output rate	接口输出流量的峰值速率大小（单位为bytes/sec）以及峰值产生的时间
Last *interval* seconds input: 0 packets/sec 0 bytes/sec 0% Last *interval* seconds output: 0 packets/sec 0 bytes/sec 0%	端口在最近一个统计周期内接收和发送报文的平均速率，单位分别为数据包/秒和字节/秒，以及实际速率和接口带宽的百分比。统计周期*interval*可以通过**flow-interval**命令设置 如果值显示为“-”，则表示不支持该统计项
Input(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口接收报文的统计值，包括正常报文、异常报文和正常PAUSE帧的报文数、字节数 端口接收的单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
Input(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口接收的正常报文的统计值，包括正常报文和正常PAUSE帧的报文数、字节数 端口接收的正常单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
input errors	端口接收的错误报文的统计值
runts	接收到的超小帧的数量 超小帧是指长度小于64字节、格式正确且包含有效的CRC字段的帧
giants	接收到的超大帧的数量 超大帧是指有效长度大于端口允许通过最大报文长度的帧： • 对于禁止长帧通过的以太网端口，超大帧是指有效长度大于 1518 字节（不带 VLAN Tag）或大于 1522 字节（带 VLAN Tag 报文）的帧 • 对于允许长帧通过的以太网端口，超大帧是指有效长度大于指定最大长帧长度的帧
throttles	接收到的长度为非整数字节的帧的个数
CRC	接收到的CRC校验错误、长度正常的帧的数量

frame	接收到的CRC校验错误、且长度不是整字节数的帧的数量
overruns	当端口的接收速率超过接收队列的处理能力时，导致报文被丢弃
aborts	接收到的非法报文总数，非法报文包括： • 报文碎片：长度小于 64 字节（长度可以为整数或非整数）且 CRC 校验错误的帧 • jabber 帧：有效长度大于端口允许通过的最大报文长度，且 CRC 校验错误的帧（长度可以为整字节数或非整字节数）。如对于禁止长帧通过的以太网端口，jabber 帧是指大于 1518（不带 VLAN Tag）或 1522（带 VLAN Tag）字节，且 CRC 校验错误的帧；对于允许长帧通过的以太网端口，jabber 帧是指有效长度大于指定最大长帧长度，且 CRC 校验错误的帧 • 符号错误帧：报文中至少包含 1 个错误的符号 • 操作码未知帧：报文是 MAC 控制帧，但不是 Pause 帧 • 长度错误帧：报文中 802.3 长度字段与报文实际长度（46～1500 字节）不匹配
ignored	由于端口接收缓冲区不足等原因而丢弃的报文数量
parity errors	接收到的奇偶校验错误的帧的数量
Output(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口发送报文的统计值，包括正常报文、异常报文和正常PAUSE帧的报文数、字节数 端口发送的单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
Output(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口发送的正常报文的统计值，包括正常报文和正常PAUSE帧的报文数、字节数 端口发送的正常单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
output errors	各种发送错误的报文总数
underruns	当端口的发送速率超过了发送队列的处理能力，导致报文被丢弃，是一种非常少见的硬件异常
buffer failures	由于端口发送缓冲区不足而丢弃的报文数量
aborts	发送失败的报文总数，即报文已经开始发送，但由于各种原因（如冲突）而导致发送失败
deferred	延迟报文的数量，延迟报文是指发送前检测到冲突而被延迟发送的报文
collisions	冲突帧的数量，冲突帧是指在发送过程中检测到冲突的而停止发送的报文
late collisions	延迟冲突帧的数量，延迟冲突帧是指帧的前512 bits已经被发送，由于检测到冲突，该帧被延迟发送
lost carrier	载波丢失，一般适用于串行WAN接口，发送过程中，每丢失一个载波，此计数器加一
no carrier	无载波，一般适用于串行WAN接口，当试图发送帧时，如果没有载波出现，此计数器加一
Peak input rate	接口输入流量的峰值速率大小（单位为bytes/sec）以及峰值产生的时间
Peak output rate	接口输出流量的峰值速率大小（单位为bytes/sec）以及峰值产生的时间

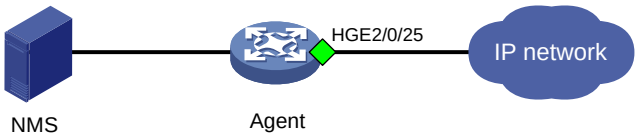
IPv4 traffic statistics	IPv4流量统计信息
IPv6 traffic statistics	IPv6流量统计信息
Last 300 seconds input rate: 0 packets/sec, 0 bytes/sec	端口在最近300秒接收报文的平均速率，单位分别为数据包/秒和字节/秒 如果值显示为“-”，则表示不支持该统计项
Last 300 seconds output rate: 0 packets/sec, 0 bytes/sec	端口在最近300秒发送报文的平均速率，单位分别为数据包/秒和字节/秒 如果值显示为“-”，则表示不支持该统计项
Input: 0 packets, 0 bytes	端口接收报文的统计值，包括报文数、字节数 如果值显示为“-”，则表示不支持该统计项
Output: 0 packets, 0 bytes	端口发送报文的统计值，包括报文数、字节数 如果值显示为“-”，则表示不支持该统计项

3.1.2 SNMP 实现

1. 配置需求

NMS 通过 SNMP 协议读取设备（Agent）的二层以太网接口 HGE2/0/25 入方向流量统计信息。

图3-1 SNMP 功能典型配置组网图



2. 配置限制和指导

- 对于二层以太网接口，端口流量统计主要有五张表：ifEntry（OID 为 1.3.6.1.2.1.2.2.1）、ifXEntry（OID 为 1.3.6.1.2.1.31.1.1）、hh3cIfFlowStatEntry（OID 为 1.3.6.1.4.1.25506.2.40.2.1.2.1.1）、hh3cIfHCFlowStatEntry（OID 为 1.3.6.1.4.1.25506.2.40.2.1.2.3.1）和 hh3cifPortProtocolStatEntry（OID 为 1.3.6.1.4.1.25506.8.35.5.1.13.1）。
- 对于二层居合租成员接口，端口流量统计主要有三张表：ifEntry（OID 为 1.3.6.1.2.1.2.2.1）、ifXEntry（OID 为 1.3.6.1.2.1.31.1.1）和 hh3cifPortProtocolStatEntry（OID 为 1.3.6.1.4.1.25506.8.35.5.1.13.1）。
- 对于 ifEntry 表和 ifXEntry 表，ifEntry 表中的端口流量统计节点数据长度都是 32 位的，ifXEntry 表中的端口流量统计部分节点数据长度是 64 位的。因此在统计端口流量时，ifEntry 表中的端口流量统计节点可能会出溢出现象。ifXEntry 表中的端口流量统计节点不会出现溢出的情况。ifEntry 表和表 ifXEntry 表中的节点不完全一样，二者是相交的关系。因此我们在查看端口流量统计时，如果能在 ifXEntry 表中找到，就以 ifXEntry 表的结果为准，如果在表 ifXEntry 中找不到，再去查看表 ifEntry。
- 可以通过 ifEntry 表、ifXEntry 表、hh3cIfFlowStatEntry 表、hh3cIfHCFlowStatEntry 表和 hh3cifPortProtocolStatEntry 表下的子节点获取不同报文数据。

3. 配置步骤

- 通过 SNMPv1/SNMPv2c 方式实现（基于名称配置 SNMPv1/v2c 团体）

  # 设置 Agent 使用的 SNMP 版本为 v2c、只读团体名为 readtest。

  ```
  <Agent> system-view
  [Agent] snmp-agent sys-info version v2c
  [Agent] snmp-agent community read readtest
  ```

  # 设置设备的联系人和位置信息，以方便维护。

  ```
  [Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
  [Agent] snmp-agent sys-info location telephone-closet,3rd-floor
  ```

  # 配置 NMS 使用的 SNMP 版本为 SNMPv2，只读团体名为 readtest。另外，还可以根据需求配置“超时”时间和“重试次数”。具体配置请参考 NMS 的相关手册。

  
  说明

  NMS 侧的配置必须和 Agent 侧保持一致，否则无法通信。

  不同 NMS 客户端支持的访问控制方式不同，请以 NMS 具体的支持方式为准。

- 通过 SNMPv1/SNMPv2c 方式实现（基于用户配置 SNMPv1/v2c 团体）

  # 在 SNMP 组 readCom 里创建 SNMPv2c 用户 readtest。

  ```
  <Sysname> system-view
  [Sysname] snmp-agent sys-info version v2c
  [Sysname] snmp-agent group v2c readCom
  [Sysname] snmp-agent usm-user v2c readtest readCom
  ```

  # 配置 NMS 使用的 SNMP 版本为 SNMPv2，只读团体名为 readtest。另外，还可以根据需求配置“超时”时间和“重试次数”。具体配置请参考 NMS 的相关手册。

  
  说明

  NMS 侧的配置必须和 Agent 侧保持一致，否则无法通信。

  不同 NMS 客户端支持的访问控制方式不同，请以 NMS 具体的支持方式为准。

- 通过 SNMPv3 方式实现（VACM 方式）

  # 设置 Agent 使用的 SNMP 版本为 v3。

  ```
  <Agent> system-view
  [Agent] snmp-agent sys-info version v3
  ```

  # 配置访问权限：配置用户具有 interfaces（OID 为 1.3.6.1.2.1.2）的读权限。

  ```
  [Agent] snmp-agent mib-view included mibtest 1.3.6.1.2.1.2
  ```

  # 创建 SNMPv3 组 managev3group，并配置与该组绑定的 SNMPv3 用户与 NMS 建立连接时，均进行认证和加密，NMS 可以对设备进行只读的视图为 mibtest。

  ```
  [Agent] snmp-agent group v3 managev3group privacy read-view mibtest
  ```

  # 创建 SNMPv3 用户 managev3user，认证算法为 SHA-1，明文认证密码为 123456TESTauth&!，加密算法为 AES，明文加密密码是 123456TESTencr&!。

  ```
  [Agent] snmp-agent usm-user v3 managev3user managev3group simple authentication-mode
  sha 123456TESTauth&! privacy-mode aes128 123456TESTencr&!
  ```

配置设备的联系人和位置信息，以方便维护。

```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```

配置 NMS 使用的 SNMP 版本为 SNMPv3，用户名为 VACMtest，启用认证和加密功能，认证算法为 SHA-1，认证密码为 123456TESTauth&!，加密协议为 AES，加密密码为 123456TESTencr&!。另外，还可以根据需求配置“超时”时间和“重试次数”。具体配置请参考 NMS 的相关手册。

说明

NMS 侧的配置必须和设备侧保持一致，否则无法进行相应操作。

不同 NMS 客户端支持的访问控制方式不同，请以 NMS 具体的支持方式为准。

- SNMP 实现（RBAC 方式）

  # 设置 Agent 使用的 SNMP 版本为 v3。

  ```
  <Agent> system-view
  [Agent] snmp-agent sys-info version v3
  ```

  # 配置访问权限：配置用户具有 internet（OID 为 1.3.6.1）的读权限。

  ```
  [Agent] role name test
  [Agent-role-test] rule 1 permit read oid 1.3.6.1
  [Agent-role-test] quit
  ```

  # 创建 SNMPv3 用户 RBACtest，为其绑定用户角色 test，认证算法为 SHA-1，明文认证密码为 123456TESTauth&!，加密算法为 AES，明文加密密码是 123456TESTencr&!。

  ```
  [Agent] snmp-agent usm-user v3 RBACtest user-role test simple authentication-mode sha
  123456TESTauth&! privacy-mode aes128 123456TESTencr&!
  ```

  # 配置设备的联系人和位置信息，以方便维护。

  ```
  [Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
  [Agent] snmp-agent sys-info location telephone-closet,3rd-floor
  ```

  # 配置 NMS 使用的 SNMP 版本为 SNMPv3，用户名为 RBACtest，启用认证和加密功能，认证算法为 SHA-1，认证密码为 123456TESTauth&!，加密协议为 AES，加密密码为 123456TESTencr&!。另外，还可以根据需求配置“超时”时间和“重试次数”。具体配置请参考 NMS 的相关手册。

  说明

  NMS 侧的配置必须和设备侧保持一致，否则无法进行相应操作。

  不同 NMS 客户端支持的访问控制方式不同，请以 NMS 设备具体的支持方式为准。

4. 查询流量统计数据示例

说明

- 查询接口流量统计数据前，我们需要获取接口的索引，然后通过索引来查接口的流量统计数据。
- 设备 IRF 成员编号不同时，接口索引值可能不同，具体以实际查询结果为准。
- 以下以通过 MIB Browser 查询 ifXTable 表获取接口 HundredGigE2/0/25 入方向的流量统计数据为例。

如图 3-2 所示，通过 ifName 节点（1.3.6.1.2.1.31.1.1.1.1）查询 HGE2/0/25 口的索引。查询结果会显示在 query results 对话框中，如图 3-3 所示，接口 HGE2/0/25 索引为 220。

图3-2 查询接口索引

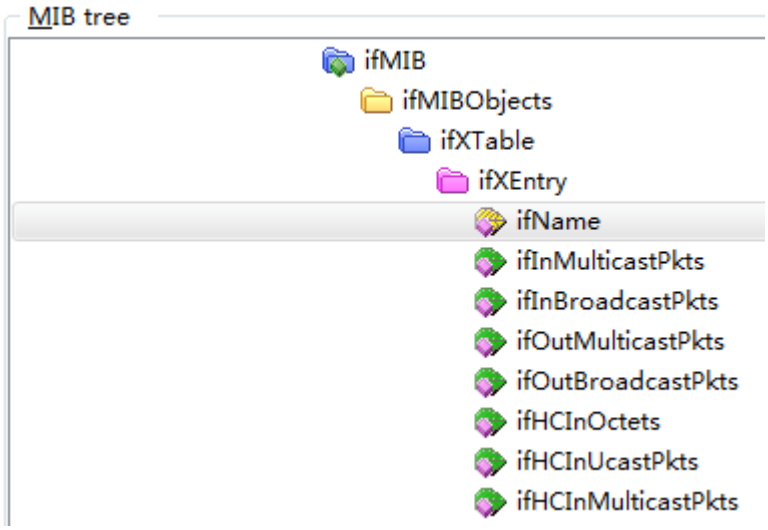
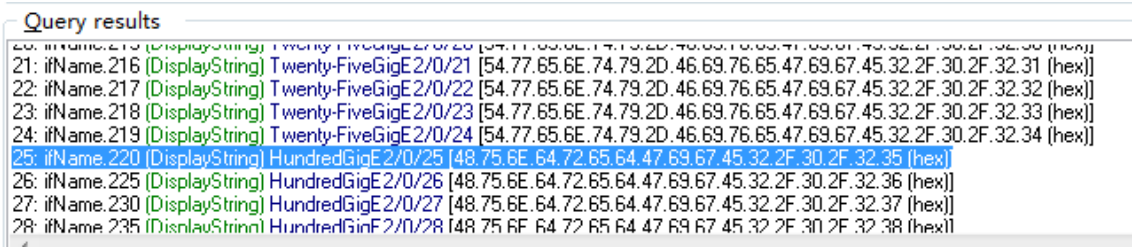


图3-3 索引查询结果



如图 3-4 所示，通过 ifHCInOctets 表（OID 为 1.3.6.1.2.1.31.1.1.1.6）查询接口 HGE2/0/25 入方向以字节为单位的流量统计数据。

查询结果会显示在 query results 对话框中，如图 3-5 所示，

图3-4 查询流量统计数据

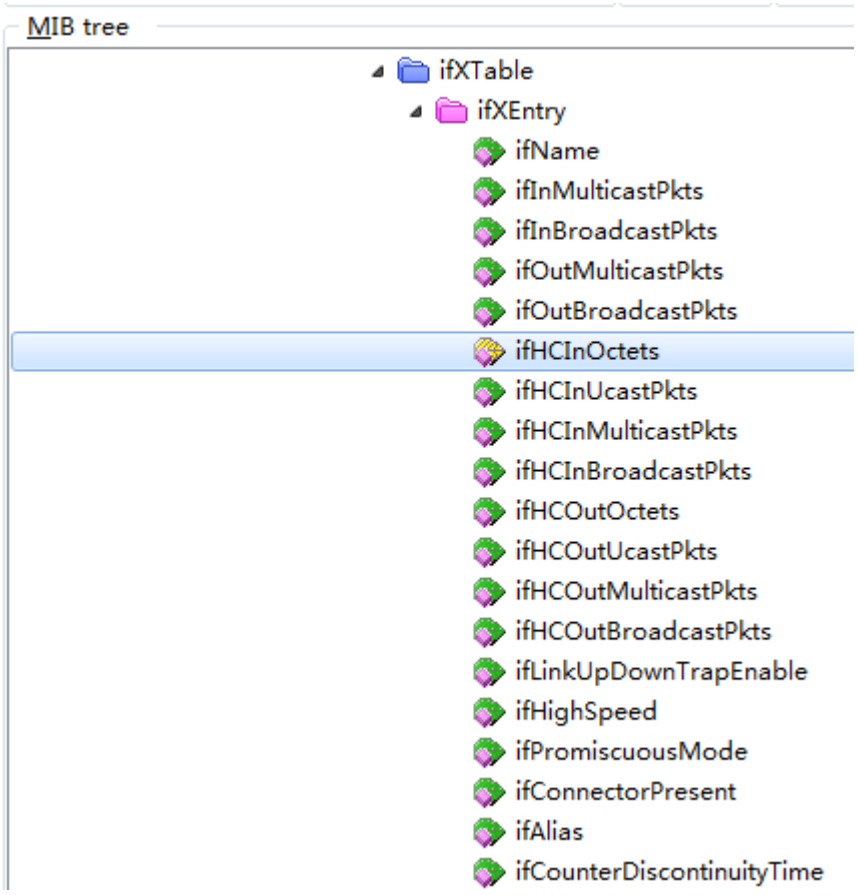
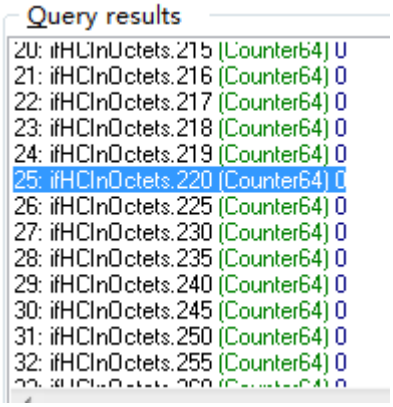


图3-5 流量统计数据查询结果



5. 更多信息

关于 SNMP 的更多配置，请参见对应产品的 SNMP 配置。

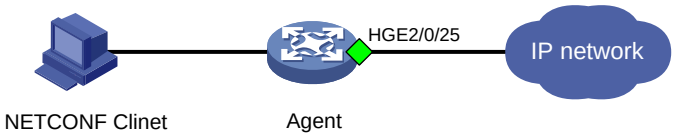
关于 MIB 文件的更多介绍，请参见对应产品的 MIB 参考。

3.1.3 NETCONF 实现

1. 配置需求

在主机上安装 NETCONF 客户端软件，通过 NETCONF 读取设备（Agent）的二层以太网接口 HGE2/0/25 流量统计信息。

图3-6 SNMP 功能典型配置组网图



说明

NETCONF 客户端是通过 Device 设备提供的 NETCONF XML API 获取的接口流量统计信息。

2. 配置步骤

- 开启 NETCONF over SOAP over http 功能。

  # 开启 NETCONF over SOAP 功能。

  ```
  <Sysname> system-view
  [Sysname] netconf soap http enable
  ```

  创建用户 admin，可以通过 NETCONF 操作设备。

  # 创建设备管理类本地用户 admin，设置其密码为 admin、服务类型为 HTTP。

  ```
  [Sysname] local-user admin
  [Sysname-luser-manage-admin] password simple admin
  [Sysname-luser-manage-admin] service-type http
  ```

  # 配置为用户 admin 授权的用户角色为 network-admin。

  ```
  [Sysname-luser-manage-admin] authorization-attribute user-role network-admin
  ```

- 开启 NETCONF over SOAP over https 功能。

  # 开启 NETCONF over SOAP 功能。

  ```
  <Sysname> system-view
  [Sysname] netconf soap https enable
  ```

  创建用户 admin，可以通过 NETCONF 操作设备。

  # 创建设备管理类本地用户 admin，设置其密码为 admin、服务类型为 HTTP。

  ```
  [Sysname] local-user admin
  [Sysname-luser-manage-admin] password simple admin
  [Sysname-luser-manage-admin] service-type https
  ```

  # 配置为用户 admin 授权的用户角色为 network-admin。

  ```
  [Sysname-luser-manage-admin] authorization-attribute user-role network-admin
  ```

3. 查询流量统计数据示例

说明

- 设备提供 2 个表用于进行接口流量统计：Ifmgr/Statistics 和 IPFW/IPStatistic。通过 Ifmgr/Statistics 表可查询接口以字节为单位和以包为单位的统计信息，包括单播报文、非单播报、未知报文、丢弃报文等类型报文的统计数据。通过 IPFW/IPStatistic 表可查询接口以包为单位的 IPv4 或 IPv6 报文的数据。
- 以下使用 Ifmgr/Statistics 表查询接口 HundredGigE2/0/25 统计信息为例，使用 IPFW/IPStatistic 表查询接口统计信息的配置过程相似。

请将以下报文拷贝、粘贴到 NETCONF 客户端。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
        <Ifmgr>
          <Statistics>
           <Interface>
            <IfIndex></IfIndex>
            <Name>HundredGigE2/0/25</Name>
            <AbbreviatedName></AbbreviatedName>
            <InOctets></InOctets>
            <InUcastPkts></InUcastPkts>
            <InNUcastPkts></InNUcastPkts>
            <InDiscards></InDiscards>
            <InErrors></InErrors>
            <InUnknownProtos></InUnknownProtos>
            <InRate></InRate>
            <OutOctets></OutOctets>
            <OutUcastPkts></OutUcastPkts>
            <OutNUcastPkts></OutNUcastPkts>
            <OutDiscards></OutDiscards>
            <OutErrors></OutErrors>
            <OutRate></OutRate>
            <LastClear></LastClear>
           </Interface>
          </Statistics>
        </Ifmgr>
      </top>
    </filter>
  </get>
</rpc>
```

如果客户端收到类似如下的报文，则表示操作成功。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data>
```

```
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
              <Ifmgr>
                 <Statistics>
                    <Interface>
                       <IfIndex>220</IfIndex>
                       <Name>HundredGigE2/0/25</Name>
                       <AbbreviatedName>HGE2/0/25</AbbreviatedName>
                       <InOctets>77760</InOctets>
                       <InUcastPkts>606</InUcastPkts>
                       <InNUcastPkts>6</InNUcastPkts>
                       <InDiscards>0</InDiscards>
                       <InErrors>0</InErrors>
                       <InUnknownProtos>0</InUnknownProtos>
                       <InRate>0</InRate>
                       <OutOctets>77888</OutOctets>
                       <OutUcastPkts>607</OutUcastPkts>
                       <OutNUcastPkts>7</OutNUcastPkts>
                       <OutDiscards>0</OutDiscards>
                       <OutErrors>0</OutErrors>
                       <OutRate>0</OutRate>
                       <LastClear>0000-00-00T00:00:00</LastClear>
                    </Interface>
                 </Statistics>
              </Ifmgr>
      </top>
    </data>
</rpc-reply>
```

4. 更多信息

关于 NETCONF 配置的更多信息，请参见对应产品的“NETCONF 配置”。

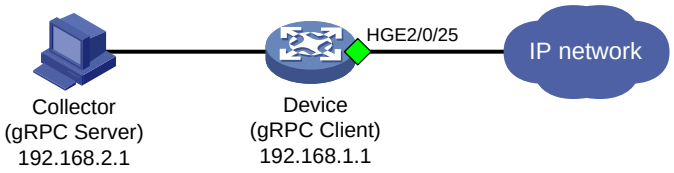
关于 Ifmgr/Statistics 和 IPFW/IPStatistic 的更多信息，请参见《H3C Comware 7 NETCONF XML API Reference 》。

3.1.4 gRPC 实现

1. 配置需求

采集器通过 gRPC 协议读取设备（Device）的二层以太网接口 HGE2/0/25 流量统计信息。

图3-7 gRPC 功能典型配置组网图



2. 配置步骤

在开始下面的配置之前，请确保设备与采集器的 IP 地址都已配置完毕，并且它们之间路由可达。

开启 gRPC 功能。

```
<Sysname> system-view
[Sysname] grpc enable
```

创建传感器组 test，并添加采样路径为 lfmgr/Statistics。

说明

配置采样路径为 lfmgr/Statistics，设备会收集设备所有接口的流量统计数据，并将数据上传给采集器。

```
[Sysname] telemetry
[Sysname-telemetry] sensor-group test
[Sysname-telemetry-sensor-group-test] sensor path ifmgr/statistics
[Sysname-telemetry-sensor-group-test] quit
```

创建目标组 collector1，并配置 IP 地址为 192.168.2.1、端口号为 50050 的采集器。

```
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] ipv4-address 192.168.2.1 port 50050
[Sysname-telemetry-destination-group-collector1] quit
```

创建订阅 A，配置关联传感器组为 test，数据采样和推送周期为 30 秒，关联目标组为 collector1。

```
[Sysname-telemetry] subscription A
[Sysname-telemetry-subscription-A] sensor-group test sample-interval 30
[Sysname-telemetry-subscription-A] destination-group collector1
[Sysname-telemetry-subscription-A] quit
```

3. 查询流量统计数据

采集器每 30 秒收到一次设备推送的接口数据统计信息。

4. 更多信息

关于 gRPC 配置的更多信息，请参见对应产品的“gRPC 配置”。

3.2 以太网接口错误报文流量统计

3.2.1 命令行方式实现

1. 配置需求

获取接口 HundredGigE2/0/25 错误报文流量统计数据。

2. 配置限制和指导

- 可直接使用 **display interface** 命令获取以太网接口的错误报文流量统计信息。
- 错误报文统计仅支持统计入方向，不支持统计出方向。其中 input errors 的统计值等于 runts+giants+throttles+CRC+frame+aborts 等值的和。
- 在某些情况，需要统计某一时段的接口流量统计数据，可以在用户视图通过 **reset counters interface** 命令清除接口原有报文统计信息，重新进行统计。

- **reset counters interface** 命令能够清除 **display interface** 命令行的端口计数但不能清除 MIB 节点计数。

3. 查询流量统计数据示例

使用 **display interface** 命令进行流量统计。

查询接口 HundredGigE2/0/25 流量统计信息。

```
[Sysname]display interface HundredGigE 2/0/25
HundredGigE2/0/25
........
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, - overruns, 0 aborts
         - ignored, - parity errors
........
 Output: 0 output errors, - underruns, 0 buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, - no carrier
```

表3-3 display interface 命令显示信息描述表

字段	描述
HundredGigE2/0/25	接口HundredGigE2/0/25的相关信息
input errors	端口接收的错误报文的统计值
runts	接收到的超小帧的数量 超小帧是指长度小于64字节、格式正确且包含有效的CRC字段的帧
giants	接收到的超大帧的数量 超大帧是指有效长度大于端口允许通过最大报文长度的帧： • 对于禁止长帧通过的以太网端口，超大帧是指有效长度大于 1518 字节（不带 VLAN Tag）或大于 1522 字节（带 VLAN Tag 报文）的帧 • 对于允许长帧通过的以太网端口，超大帧是指有效长度大于指定最大长帧长度的帧
throttles	接收到的长度为非整数字节的帧的个数
CRC	接收到的CRC校验错误、长度正常的帧的数量
frame	接收到的CRC校验错误、且长度不是整字节数的帧的数量
overruns	当端口的接收速率超过接收队列的处理能力时，导致报文被丢弃
aborts	接收到的非法报文总数，非法报文包括： • 报文碎片：长度小于 64 字节（长度可以为整数或非整数）且 CRC 校验错误的帧 • jabber 帧：有效长度大于端口允许通过的最大报文长度，且 CRC 校验错误的帧（长度可以为整字节数或非整字节数）。如对于禁止长帧通过的以太网端口，jabber 帧是指大于 1518（不带 VLAN Tag）或 1522（带 VLAN Tag）字节，且 CRC 校验错误的帧；对于允许长帧通过的以太网端口，jabber 帧是指有效长度大于指定最大长帧长度，且 CRC 校验错误的帧 • 符号错误帧：报文中至少包含 1 个错误的符号 • 操作码未知帧：报文是 MAC 控制帧，但不是 Pause 帧 • 长度错误帧：报文中 802.3 长度字段与报文实际长度（46～1500 字节）不匹

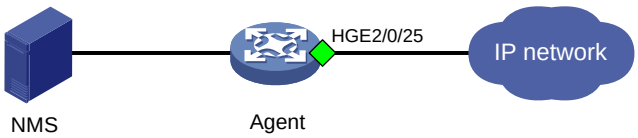
	配
ignored	由于端口接收缓冲区不足等原因而丢弃的报文数量
parity errors	接收到的奇偶校验错误的帧的数量
output errors	各种发送错误的报文总数
underruns	当端口的发送速率超过了发送队列的处理能力，导致报文被丢弃，是一种非常少见的硬件异常
buffer failures	由于端口发送缓冲区不足而丢弃的报文数量
aborts	发送失败的报文总数，即报文已经开始发送，但由于各种原因（如冲突）而导致发送失败
deferred	延迟报文的数量，延迟报文是指发送前检测到冲突而被延迟发送的报文
collisions	冲突帧的数量，冲突帧是指在发送过程中检测到冲突的而停止发送的报文
late collisions	延迟冲突帧的数量，延迟冲突帧是指帧的前512 bits已经被发送，由于检测到冲突，该帧被延迟发送
lost carrier	载波丢失，一般适用于串行WAN接口，发送过程中，每丢失一个载波，此计数器加一
no carrier	无载波，一般适用于串行WAN接口，当试图发送帧时，如果没有载波出现，此计数器加一

3.2.2 SNMP 实现

1. 配置需求

NMS 通过 SNMP 协议读取设备（Agent）的二层以太网接口 HGE2/0/25 错误报文流量统计信息。

图3-8 SNMP 功能典型配置组网图



2. 配置步骤

配置 SNMP，请参见 3.1.3 2. 配置步骤。

3. 查询流量统计数据示例

说明

- 查询接口错误报文流量统计数据前，我们需要获取接口的索引，然后通过索引来查接口错误报文流量统计数据。
- 设备 IRF 成员编号不同时，接口索引值可能不同，具体以实际查询结果为准。
- 我们可以通过 ifInDiscards、ifOutDiscards、ifInErrors 和 ifOutErrors 节点查看接口丢包、错误包统计数据。不同表的统计方式相同，以下以通过 MIB Browser 查询 ifInErrors 节点获取接口 HundredGigE2/0/25 入方向错误包的流量统计数据为例。

如图 3-2 所示，通过 ifName 节点（1.3.6.1.2.1.31.1.1.1.1）查询 HGE2/0/25 口的索引。查询结果会显示在 query results 对话框中，如图 3-3 所示，接口 HGE2/0/25 索引为 220。

图3-9 查询接口索引

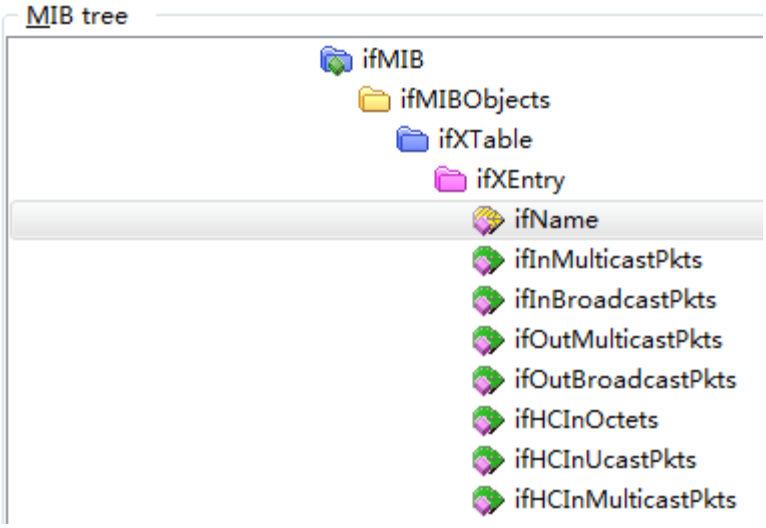
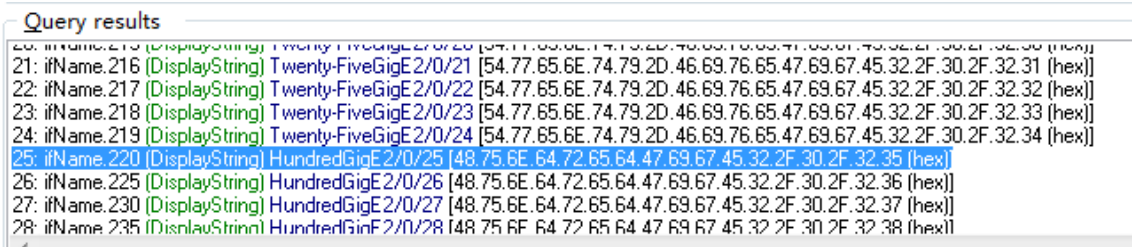
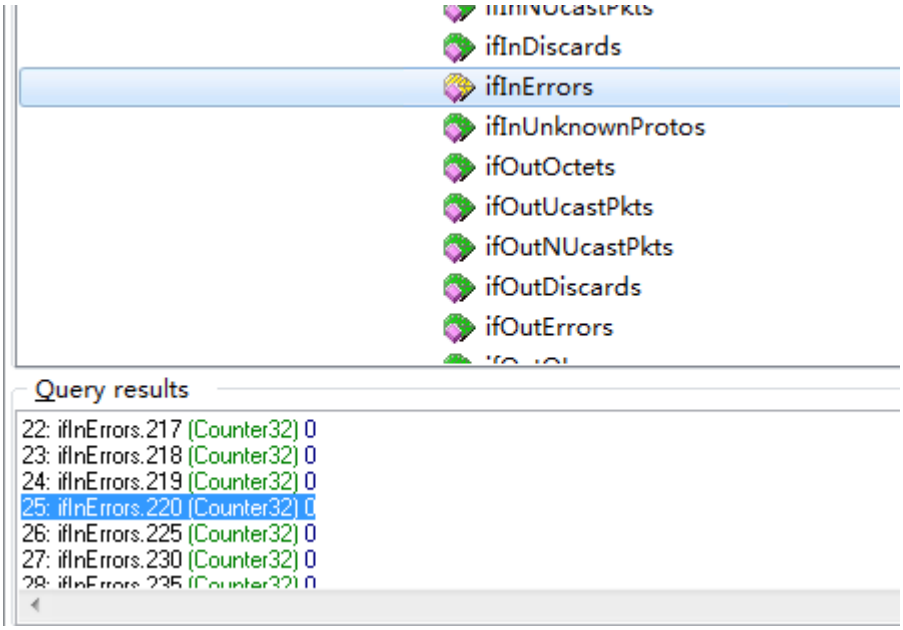


图3-10 索引查询结果



通过 ifInErrors 表（OID 为 1.3.6.1.2.1.31.1.1.1.6）查询接口 HGE2/0/25 入方向错误包的统计数据。查询结果会显示在 query results 对话框中，如图 3-11 所示，

图3-11 查询流量统计数据



4. 更多信息

关于 SNMP 的更多配置，请参见对应产品的 SNMP 配置。

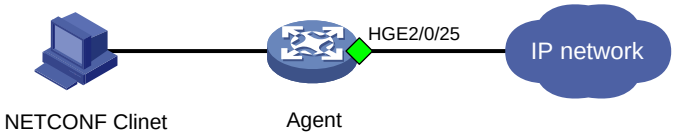
关于 MIB 文件的更多介绍，请参见对应产品的 MIB 参考。

3.2.3 NETCONF 实现

1. 配置需求

在主机上安装 NETCONF 客户端软件，通过 NETCONF 读取设备（Agent）的二层以太网接口 HGE2/0/25 流量统计信息。

图3-12 SNMP 功能典型配置组网图



说明

NETCONF 客户端是通过 Device 设备提供的 NETCONF XML API 获取的接口流量统计信息。

2. 配置步骤

配置 NETCONF，请参见 3.1.3 2. 配置步骤。

3. 查询流量统计数据示例

说明

- 设备提供 2 个表用于进行接口流量统计：Ifmgr/Statistics 和 IPFW/IPStatistic。通过 Ifmgr/Statistics 表可查询接口以字节为单位和以包为单位的统计信息，包括单播报文、非单播报、未知报文、丢弃报文等类型报文的统计数据。通过 IPFW/IPStatistic 表可查询接口以包为单位的 IPv4 或 IPv6 报文的数据。
- 以下使用 Ifmgr/Statistics 表查询接口 HundredGigE2/0/25 统计信息为例，使用 IPFW/IPStatistic 表查询接口统计信息的配置过程相似。

查询接口索引。

```
[Sysname-probe]display system internal ifmgr list | in HundredGigE2/0/25
        Bridge-Aggregation2(index:220)
```

请将以下报文拷贝、粘贴到 NETCONF 客户端。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
        <Ifmgr>
          <Statistics>
           <Interface>
            <IfIndex>220</IfIndex>
            <Name>HundredGigE2/0/25</Name>
            <AbbreviatedName></AbbreviatedName>
            <InOctets></InOctets>
            <InUcastPkts></InUcastPkts>
            <InNUcastPkts></InNUcastPkts>
            <InDiscards></InDiscards>
            <InErrors></InErrors>
            <InUnknownProtos></InUnknownProtos>
            <InRate></InRate>
            <OutOctets></OutOctets>
            <OutUcastPkts></OutUcastPkts>
            <OutNUcastPkts></OutNUcastPkts>
            <OutDiscards></OutDiscards>
            <OutErrors></OutErrors>
            <OutRate></OutRate>
            <LastClear></LastClear>
           </Interface>
          </Statistics>
        </Ifmgr>
      </top>
    </filter>
  </get>
</rpc>
```

如果客户端收到类似如下的报文，则表示操作成功。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data>
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
              <Ifmgr>
                 <Statistics>
                    <Interface>
                       <IfIndex>220</IfIndex>
                       <Name>HundredGigE2/0/25</Name>
                       <AbbreviatedName>HGE2/0/25</AbbreviatedName>
                       <InOctets>5090007388288</InOctets>
                       <InUcastPkts>39350156658</InUcastPkts>
                       <InNUcastPkts>0</InNUcastPkts>
                       <InDiscards>0</InDiscards>
                       <InErrors>415526968</InErrors>
                       <InUnknownProtos>0</InUnknownProtos>
                       <InRate>1081146628</InRate>
                       <OutOctets>55212</OutOctets>
                       <OutUcastPkts>0</OutUcastPkts>
                       <OutNUcastPkts>172</OutNUcastPkts>
                       <OutDiscards>0</OutDiscards>
                       <OutErrors>0</OutErrors>
                       <OutRate>0</OutRate>
                       <LastClear>2001-01-01T21:16:23</LastClear>
                    </Interface>
                 </Statistics>
              </Ifmgr>
      </top>
    </data>
</rpc-reply>
```

4. 更多信息

关于 NETCONF 配置的更多信息，请参见对应产品的“NETCONF 配置”。

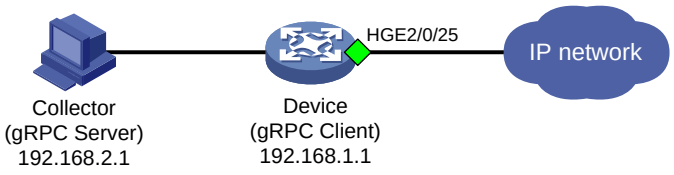
关于 Ifmgr/Statistics 和 IPFW/IPStatistic 的更多信息，请参见《H3C Comware 7 NETCONF XML API Reference 》。

3.2.4 gRPC 实现

1. 配置需求

采集器通过 gRPC 协议读取设备（Device）的二层以太网接口 HGE2/0/25 错误报文的流量统计信息。

图3-13 gRPC 功能典型配置组网图



2. 配置步骤

配置 gRPC，请参见 3.1.4 2. 配置步骤。

3. 查询流量统计数据

采集器每 30 秒收到一次设备推送的接口数据统计信息。

4. 更多信息

关于 gRPC 配置的更多信息，请参见对应产品的“gRPC 配置”。

3.3 三层以太网接口/三层以太网子接口/三层聚合成员接口流量统计

说明

- 本节的三层以太网接口/三层以太网子接口包括设备的固定接口和 100G/40G 接口拆分出来的 25G/10G 接口或者 25G/10G 接口的子接口。
- 三层以太网接口、三层以太网子接口、三层聚合成员接口流量统计方式类似，以下以统计三层以太网接口流量数据为例。

3.3.1 命令行方式实现

1. 配置需求

获取三层以太网接口 HundredGigE2/0/25 流量统计数据。

2. 配置限制和指导

- 可直接使用 **display interface** 命令获取三层以太网接口/三层以太网子接口/三层聚合成员接口的流量统计信息。对于三层聚合成员接口，统计数据不区分 IPv4 和 IPv6 报文。
- 三层以太网接口支持开启三层流量统计功能。开启三层流量统计功能后，通过 **display interface** 命令可查询接口的 IPv4 和 IPv6 报文流量统计信息。
- 三层以太网接口通过 **display ip interface** 或 **display ipv6 interface** 命令查看接口流量统计信息，三层聚合成员接口不支持通过 **display ip interface** 或 **display ipv6 interface** 命令查看接口流量统计信息。
- 如果三层以太网口下面创建了子接口，那么三层以太网口以及子接口的流量统计会累加。例如：te1/0/1 转发转发 1000，te1/0/1.1 转发 1000，te1/0/1.2 转发 1000，那么主接口的统计计数是 3000，子接口 te1/0/1.1 是 3000，子接口 te1/0/1.2 也是 3000
- 在某些情况，需要统计某一时段的接口流量统计数据，可以在用户视图通过 **reset counters interface** 命令清除接口原有报文统计信息，重新进行统计。
- **reset counters interface** 命令能够清除 **display interface** 命令行的端口计数但不能清除 MIB 节点计数。

3. 配置步骤

切换为三层以太网接口。

```
<Sysname> system-view
[Sysname] interface hundredgige 2/0/25
[Sysname-HundredGigE2/0/25] port link-mode route
```

配置 IP 地址（略）。

（可选）开启接口 HundredGigE2/0/25 的三层流量统计功能。

```
[Sysname-HundredGigE2/0/25] statistics l3-packet enable inbound
[Sysname-HundredGigE2/0/25] statistics l3-packet enable outbound
```

4. 查询流量统计数据示例

- 未开启三层流量统计功能时，使用 **display interface** 命令进行流量统计。

  # 查询接口 HundredGigE2/0/25 流量统计信息。

```
[Sysname]display interface HundredGigE 2/0/25
HundredGigE2/0/25
........
 Peak input rate: 0 bytes/sec, at 2022-04-07 16:07:11
 Peak output rate: 0 bytes/sec, at 2022-04-07 16:07:11
 Last 300 seconds input: 0 packets/sec 0 bytes/sec 0%
 Last 300 seconds output: 0 packets/sec 0 bytes/sec 0%
 Input (total):  612 packets, 77760 bytes
         606 unicasts, 1 broadcasts, 5 multicasts, 0 pauses
 Input (normal):  612 packets, - bytes
         606 unicasts, 1 broadcasts, 5 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, - overruns, 0 aborts
         - ignored, - parity errors
 Output (total): 614 packets, 77888 bytes
         607 unicasts, 3 broadcasts, 4 multicasts, 0 pauses
 Output (normal): 614 packets, - bytes
         607 unicasts, 3 broadcasts, 4 multicasts, 0 pauses
 Output: 0 output errors, - underruns, 0 buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, - no carrier
```

表3-4 display interface 命令显示信息描述表

字段	描述
HundredGigE2/0/25	接口HundredGigE2/0/25的相关信息
Peak input rate	接口输入流量的峰值速率大小（单位为bytes/sec）以及峰值产生的时间
Peak output rate	接口输出流量的峰值速率大小（单位为bytes/sec）以及峰值产生的时间
Last *interval* seconds input: 0 packets/sec 0 bytes/sec 0% Last *interval* seconds output: 0 packets/sec 0 bytes/sec 0%	端口在最近一个统计周期内接收和发送报文的平均速率，单位分别为数据包/秒和字节/秒，以及实际速率和接口带宽的百分比。统计周期*interval*可以通过**flow-interval**命令设置 如果值显示为“-”，则表示不支持该统计项
Input(total): 0 packets, 0 bytes 0 unicasts, 0	端口接收报文的统计值，包括正常报文、异常报文和正常PAUSE帧的报文数、字节数 端口接收的单播报文、广播报文、组播报文和PAUSE帧的数量

broadcasts, 0 multicasts, 0 pauses	如果值显示为“-”，则表示不支持该统计项
Input(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口接收的正常报文的统计值，包括正常报文和正常PAUSE帧的报文数、字节数 端口接收的正常单播报文、广播报文、组播报文和P AUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
input errors	端口接收的错误报文的统计值
runts	接收到的超小帧的数量 超小帧是指长度小于64字节、格式正确且包含有效的CRC字段的帧
giants	接收到的超大帧的数量 超大帧是指有效长度大于端口允许通过最大报文长度的帧： • 对于禁止长帧通过的以太网端口，超大帧是指有效长度大于 1518 字节（不带 VLAN Tag）或大于 1522 字节（带 VLAN Tag 报文）的帧 • 对于允许长帧通过的以太网端口，超大帧是指有效长度大于指定最大长帧长度的帧
throttles	接收到的长度为非整数字节的帧的个数
CRC	接收到的CRC校验错误、长度正常的帧的数量
frame	接收到的CRC校验错误、且长度不是整字节数的帧的数量
overruns	当端口的接收速率超过接收队列的处理能力时，导致报文被丢弃
aborts	接收到的非法报文总数，非法报文包括： • 报文碎片：长度小于 64 字节（长度可以为整数或非整数）且 CRC 校验错误的帧 • jabber 帧：有效长度大于端口允许通过的最大报文长度，且 CRC 校验错误的帧（长度可以为整字节数或非整字节数）。如对于禁止长帧通过的以太网端口，jabber 帧是指大于 1518（不带 VLAN Tag）或 1522（带 VLAN Tag）字节，且 CRC 校验错误的帧；对于允许长帧通过的以太网端口，jabber 帧是指有效长度大于指定最大长帧长度，且 CRC 校验错误的帧 • 符号错误帧：报文中至少包含 1 个错误的符号 • 操作码未知帧：报文是 MAC 控制帧，但不是 Pause 帧 • 长度错误帧：报文中 802.3 长度字段与报文实际长度（46～1500 字节）不匹配
ignored	由于端口接收缓冲区不足等原因而丢弃的报文数量
parity errors	接收到的奇偶校验错误的帧的数量
Output(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口发送报文的统计值，包括正常报文、异常报文和正常PAUSE帧的报文数、字节数 端口发送的单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
Output(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口发送的正常报文的统计值，包括正常报文和正常PAUSE帧的报文数、字节数 端口发送的正常单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
output errors	各种发送错误的报文总数

underruns	当端口的发送速率超过了发送队列的处理能力，导致报文被丢弃，是一种非常少见的硬件异常
buffer failures	由于端口发送缓冲区不足而丢弃的报文数量
aborts	发送失败的报文总数，即报文已经开始发送，但由于各种原因（如冲突）而导致发送失败
deferred	延迟报文的数量，延迟报文是指发送前检测到冲突而被延迟发送的报文
collisions	冲突帧的数量，冲突帧是指在发送过程中检测到冲突的而停止发送的报文
late collisions	延迟冲突帧的数量，延迟冲突帧是指帧的前512 bits已经被发送，由于检测到冲突，该帧被延迟发送
lost carrier	载波丢失，一般适用于串行WAN接口，发送过程中，每丢失一个载波，此计数器加一
no carrier	无载波，一般适用于串行WAN接口，当试图发送帧时，如果没有载波出现，此计数器加一

- 开启三层流量统计功能后，使用 **display interface** 命令进行流量统计。

  # 查询接口 HundredGigE2/0/25 流量统计信息。

```
[Sysname]display interface HundredGigE 2/0/25
HundredGigE2/0/25
........
 Peak input rate: 0 bytes/sec, at 2022-04-07 16:07:11
 Peak output rate: 0 bytes/sec, at 2022-04-07 16:07:11
 Last 300 seconds input: 0 packets/sec 0 bytes/sec 0%
 Last 300 seconds output: 0 packets/sec 0 bytes/sec 0%
 Input (total):  612 packets, 77760 bytes
         606 unicasts, 1 broadcasts, 5 multicasts, 0 pauses
 Input (normal):  612 packets, - bytes
         606 unicasts, 1 broadcasts, 5 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, - overruns, 0 aborts
         - ignored, - parity errors
 Output (total): 614 packets, 77888 bytes
         607 unicasts, 3 broadcasts, 4 multicasts, 0 pauses
 Output (normal): 614 packets, - bytes
         607 unicasts, 3 broadcasts, 4 multicasts, 0 pauses
 Output: 0 output errors, - underruns, 0 buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, - no carrier
IPv4 traffic statistics:
 Last 300 seconds input rate: 0 packets/sec, 0 bytes/sec
 Last 300 seconds output rate: 0 packets/sec, 0 bytes/sec
 Input: 300 packets, 38400 bytes
 Output: 300 packets, 38400 bytes
IPv6 traffic statistics:
 Last 300 seconds input rate: 0 packets/sec, 0 bytes/sec
 Last 300 seconds output rate: 0 packets/sec, 0 bytes/sec
```

```
Input: 300 packets, 38400 bytes
Output: 300 packets, 38400 bytes
```

表3-5 display interface 命令显示信息描述表

字段	描述
HundredGigE2/0/25	接口HundredGigE2/0/25的相关信息
Peak input rate	接口输入流量的峰值速率大小（单位为bytes/sec）以及峰值产生的时间
Peak output rate	接口输出流量的峰值速率大小（单位为bytes/sec）以及峰值产生的时间
Last *interval* seconds input: 0 packets/sec 0 bytes/sec 0% Last *interval* seconds output: 0 packets/sec 0 bytes/sec 0%	端口在最近一个统计周期内接收和发送报文的平均速率，单位分别为数据包/秒和字节/秒，以及实际速率和接口带宽的百分比。统计周期*interval*可以通过**flow-interval**命令设置 如果值显示为“-”，则表示不支持该统计项
Input(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口接收报文的统计值，包括正常报文、异常报文和正常PAUSE帧的报文数、字节数 端口接收的单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
Input(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口接收的正常报文的统计值，包括正常报文和正常PAUSE帧的报文数、字节数 端口接收的正常单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
input errors	端口接收的错误报文的统计值
runts	接收到的超小帧的数量 超小帧是指长度小于64字节、格式正确且包含有效的CRC字段的帧
giants	接收到的超大帧的数量 超大帧是指有效长度大于端口允许通过最大报文长度的帧： • 对于禁止长帧通过的以太网端口，超大帧是指有效长度大于 1518 字节（不带 VLAN Tag）或大于 1522 字节（带 VLAN Tag 报文）的帧 • 对于允许长帧通过的以太网端口，超大帧是指有效长度大于指定最大长帧长度的帧
throttles	接收到的长度为非整数字节的帧的个数
CRC	接收到的CRC校验错误、长度正常的帧的数量
frame	接收到的CRC校验错误、且长度不是整字节数的帧的数量
overruns	当端口的接收速率超过接收队列的处理能力时，导致报文被丢弃
aborts	接收到的非法报文总数，非法报文包括： • 报文碎片：长度小于 64 字节（长度可以为整数或非整数）且 CRC 校验错误的帧 • jabber 帧：有效长度大于端口允许通过的最大报文长度，且 CRC 校验错误的帧（长度可以为整字节数或非整字节数）。如对于禁止长帧通过的以太网端口，jabber 帧是指大于 1518（不带 VLAN Tag）或 1522（带 VLAN Tag）字节，且 CRC 校验错误的帧；对于允许长帧通过的以太网端口，jabber 帧是指有效长度大于指定最大长帧长度，且 CRC 校验错误的帧

	• 符号错误帧：报文中至少包含 1 个错误的符号 • 操作码未知帧：报文是 MAC 控制帧，但不是 Pause 帧 • 长度错误帧：报文中 802.3 长度字段与报文实际长度（46～1500 字节）不匹配
ignored	由于端口接收缓冲区不足等原因而丢弃的报文数量
parity errors	接收到的奇偶校验错误的帧的数量
Output(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口发送报文的统计值，包括正常报文、异常报文和正常PAUSE帧的报文数、字节数 端口发送的单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
Output(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口发送的正常报文的统计值，包括正常报文和正常PAUSE帧的报文数、字节数 端口发送的正常单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
output errors	各种发送错误的报文总数
underruns	当端口的发送速率超过了发送队列的处理能力，导致报文被丢弃，是一种非常少见的硬件异常
buffer failures	由于端口发送缓冲区不足而丢弃的报文数量
aborts	发送失败的报文总数，即报文已经开始发送，但由于各种原因（如冲突）而导致发送失败
deferred	延迟报文的数量，延迟报文是指发送前检测到冲突而被延迟发送的报文
collisions	冲突帧的数量，冲突帧是指在发送过程中检测到冲突的而停止发送的报文
late collisions	延迟冲突帧的数量，延迟冲突帧是指帧的前512 bits已经被发送，由于检测到冲突，该帧被延迟发送
lost carrier	载波丢失，一般适用于串行WAN接口，发送过程中，每丢失一个载波，此计数器加一
no carrier	无载波，一般适用于串行WAN接口，当试图发送帧时，如果没有载波出现，此计数器加一
Peak input rate	接口输入流量的峰值速率大小（单位为bytes/sec）以及峰值产生的时间
Peak output rate	接口输出流量的峰值速率大小（单位为bytes/sec）以及峰值产生的时间
IPv4 traffic statistics	IPv4流量统计信息
IPv6 traffic statistics	IPv6流量统计信息
Last 300 seconds input rate: 0 packets/sec, 0 bytes/sec	端口在最近300秒接收报文的平均速率，单位分别为数据包/秒和字节/秒 如果值显示为“-”，则表示不支持该统计项
Last 300 seconds output rate: 0 packets/sec, 0 bytes/sec	端口在最近300秒发送报文的平均速率，单位分别为数据包/秒和字节/秒 如果值显示为“-”，则表示不支持该统计项
Input: 0 packets, 0 bytes	端口接收报文的统计值，包括报文数、字节数 如果值显示为“-”，则表示不支持该统计项

Output: 0 packets, 0 bytes	端口发送报文的统计值，包括报文数、字节数 如果值显示为“-”，则表示不支持该统计项

- IPv4 流量统计。

  # 查询接口 hundredgige2/0/25 的 IPv4 报文流量统计。

```
[Sysname]dis ip interface hundredgige2/0/25
HundredGigE2/0/25 current state: UP
Line protocol current state: UP
Internet Address is 41.41.41.2/24 Primary
Broadcast address: 41.41.41.255
The Maximum Transmit Unit: 1500 bytes
input packets : 300, bytes : 38400, multicasts : 0
output packets : 300, bytes : 38382, multicasts : 0
TTL invalid packet number:         0
ICMP packet input number:          0
  Echo reply:                      0
  Unreachable:                     0
  Source quench:                   0
  Routing redirect:                0
  Echo request:                    0
  Router advert:                   0
  Router solicit:                  0
  Time exceed:                     0
  IP header bad:                   0
  Timestamp request:               0
  Timestamp reply:                 0
  Information request:             0
  Information reply:               0
  Netmask request:                 0
  Netmask reply:                   0
  Unknown type:                    0
```

表3-6 display ip interface 命令显示信息描述表

字段	描述
current state	接口当前的物理状态，可能的状态及含义如下： • Administratively DOWN：表示该接口已经通过 **shutdown** 命令被关闭，即管理状态为关闭 • DOWN：该接口的管理状态为开启，但物理状态为关闭（可能因为未连接好或者线路故障） • UP：该接口的管理状态和物理状态均为开启
Line protocol current state	接口数据链路层协议状态，可能的状态及含义如下： • DOWN：表示接口的数据链路层协议状态为关闭 • UP：表示接口的数据链路层协议状态为开启 • UP (spoofing)：该接口的协议状态为欺骗性开启，即虽然接口的链路层协议状态显示是开启的，但实际可能没有对应的链路，或者所对应的链路不是永久存在而是按需建立的

Internet Address	接口IP地址。IP地址后可携带如下参数： • Primary：手动配置的主地址 • Sub：手动配置的从地址。当配置了主地址时，仅显示主地址；仅配置从地址时，才显示本信息 • DHCP-allocated：通过 DHCP 获取的 IP 地址，详细介绍请参见“三层技术-IP 业务配置指导”中的“DHCP” • BOOTP-allocated：通过 BOOTP 获取的 IP 地址，详细介绍请参见“三层技术-IP 业务配置指导”中的“DHCP” • Unnumbered：借用其他接口的 IP 地址 • Cellular-allocated：通过 Modem 私有协议获取的 IP 地址，详细介绍请参见“二层技术-广域网接入配置指导”中的“3G Modem 和 4G Modem 管理” • MAD：成员设备上配置的 MAD IP 地址，详细介绍请参见“虚拟化技术配置指导”中的“IRF”
Broadcast address	接口所在网段的广播地址
The Maximum Transmit Unit	接口的最大传输单元，单位为字节
input packets, bytes, multicasts output packets, bytes, multicasts	接口上接收和发送的所有报文数、字节数以及组播报文数（设备启动后就开始统计此信息）
TTL invalid packet number	接口上收到的TTL无效的报文个数（设备启动后就开始统计此信息）
ICMP packet input number: Echo reply: Unreachable: Source quench: Routing redirect: Echo request: Router advert: Router solicit: Time exceed: IP header bad: Timestamp request: Timestamp reply: Information request: Information reply: Netmask request: Netmask reply: Unknown type:	接口上收到的ICMP报文的总数（设备启动后就开始统计此信息），包括如下报文： • Echo 应答报文 • 不可达报文 • 源站抑制报文 • 路由重定向报文 • Echo 请求报文 • 路由器通告报文 • 路由器请求报文 • 超时报文 • IP 报文头错误报文 • 时间戳请求报文 • 时间戳响应报文 • 信息请求报文 • 信息响应报文 • 掩码请求报文 • 掩码响应报文 • 未知类型报文

- IPv6 流量统计

  # 查询接口 hundredgige2/0/25 的 IPv4 报文流量统计。

  ```
  [Sysname]dis ipv6 interface H2/0/25
  HundredGigE2/0/25 current state: UP
  ```

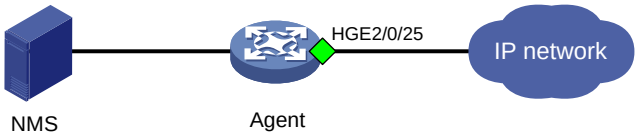
```
Line protocol current state: UP
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE00:6851
  Global unicast address(es):
    41::2, subnet is 41::/64
  Joined group address(es):
    FF02::1
FF02::2
    FF02::1:FF00:2
    FF02::1:FF00:6851
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                   300
  InTooShorts:                  0
  InTruncatedPkts:              0
  InHopLimitExceeds:            0
  InBadHeaders:                 0
  InBadOptions:                 0
  ReasmReqds:                   0
  ReasmOKs:                     0
  InFragDrops:                  0
  InFragTimeouts:               0
  OutFragFails:                 0
  InUnknownProtos:              0
  InDelivers:                   304
  OutRequests:                  4
  OutForwDatagrams:             300
  InNoRoutes:                   0
  InTooBigErrors:               0
  OutFragOKs:                   0
  OutFragCreates:               0
  InMcastPkts:                  0
  InMcastNotMembers:            0
  OutMcastPkts:                 1
  InAddrErrors:                 0
  InDiscards:                   0
  OutDiscards:                  0
```

3.3.2 SNMP 实现

1. 配置需求

NMS 通过 SNMP 协议读取设备（Agent）的三层以太网接口 HGE2/0/25 入方向流量统计信息。

图3-14 SNMP 功能典型配置组网图



2. 配置限制和指导

- 对于三层以太网接口，端口流量统计主要有四张表：ifEntry（OID 为 1.3.6.1.2.1.2.2.1）、ifXEntry（OID 为 1.3.6.1.2.1.31.1.1）、hh3cIfFlowStatEntry（OID 为 1.3.6.1.4.1.25506.2.40.2.1.2.1.1）和 ipIfStatsEntry（OID 为 1.3.6.1.2.1.4.31.3.1）。
- 对于 ifEntry 表和 ifXEntry 表，ifEntry 表中的端口流量统计节点数据长度都是 32 位的，ifXEntry 表中的端口流量统计节点部分节点数据长度是 64 位的。因此在统计端口流量时，ifEntry 表中的端口流量统计节点可能会出溢出现象。ifXEntry 表中的端口流量统计节点不会出现溢出的情况。ifEntry 表和表 ifXEntry 表中的节点不完全一样，二者是相交的关系。因此我们在查看端口流量统计时，如果能在 ifXEntry 表中找到，就以 ifXEntry 表的结果为准，如果在表 ifXEntry 中找不到，再去查看表 ifEntry。
- 可以通过 ifEntry 表、ifXEntry 表、hh3cIfFlowStatEntry 表、hh3cIfHCFlowStatEntry 表和 hh3cifPortProtocolStatEntry 表下的子节点获取不同报文数据。

3. 配置步骤

切换为三层以太网接口。

```
<Sysname> system-view
[Sysname] interface hundredgige 2/0/25
[Sysname-HundredGigE2/0/25] port link-mode route
```

配置 IP 地址（略）。

配置 SNMP，请参见 3.1.3 2. 配置步骤。

4. 查询流量统计数据示例

说明

- 查询接口流量统计数据前，我们需要获取接口的索引，然后通过索引来查接口的流量统计数据。
- 主接口与子接口的索引不同，请分别获取。
- 设备 IRF 成员编号不同时，接口索引值可能不同，具体以实际查询结果为准。
- 以下以通过 MIB Browser 查询 ifXTable 表获取接口 HundredGigE2/0/25 入方向的流量统计数据为例。

通过 ifName 节点（1.3.6.1.2.1.31.1.1.1.1）查询 HGE2/0/25 口的索引。查询结果会显示在 query results 对话框中，如图 3-15 所示，接口 HGE2/0/25 索引为 220。

图3-15 查询接口索引

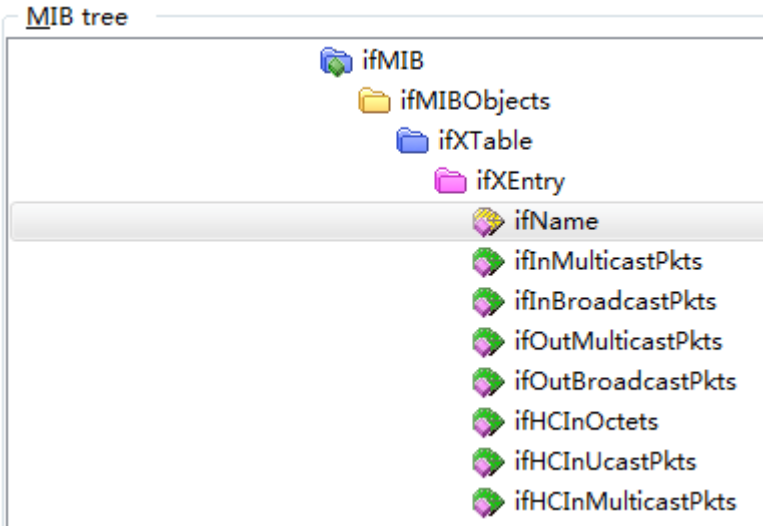
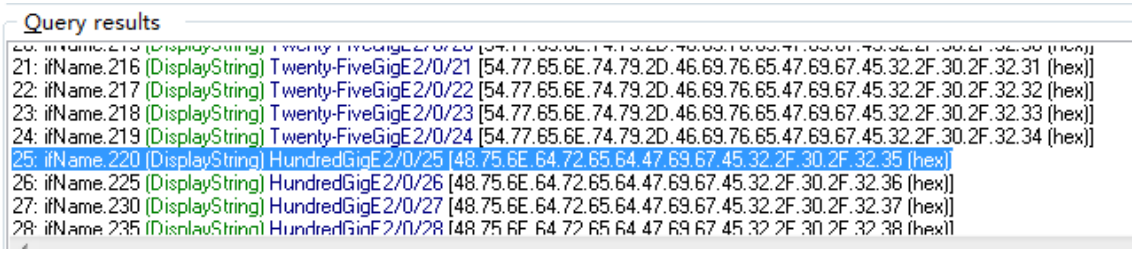


图3-16 索引查询结果



如图 3-17 所示，通过 ifHCInOctets 表（OID 为 1.3.6.1.2.1.31.1.1.1.6）查询接口 HGE2/0/25 入方向以字节为单位的流量统计数据。

查询结果会显示在 query results 对话框中，如图 3-18 所示。

图3-17 查询流量统计数据

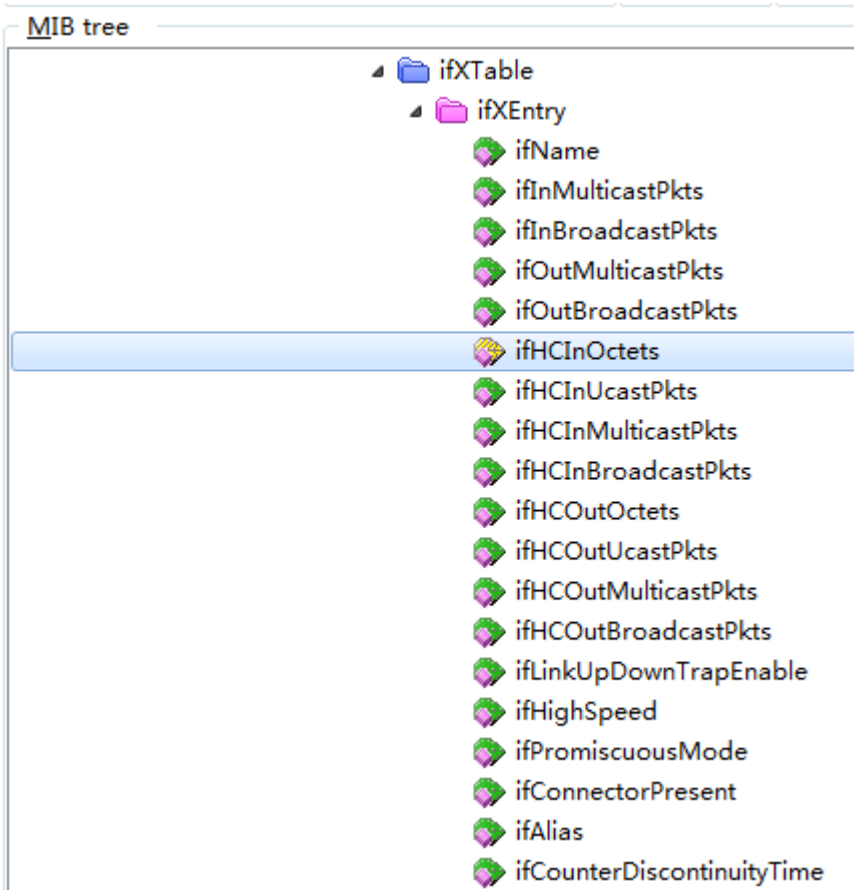
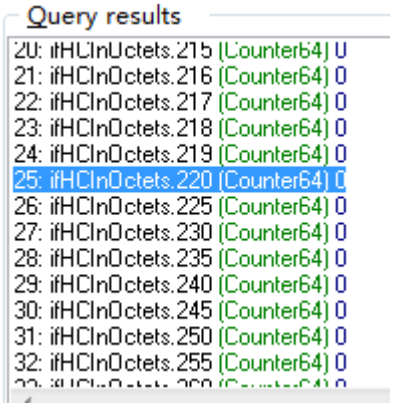


图3-18 流量统计数据查询结果



5. 更多信息

关于 SNMP 的更多配置，请参见对应产品的 SNMP 配置。

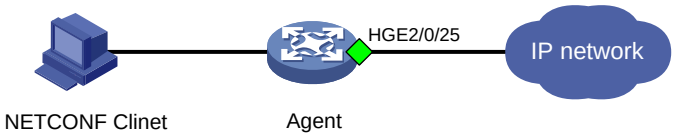
关于 MIB 文件的更多介绍，请参见对应产品的 MIB 参考。

3.3.3 NETCONF 实现

1. 配置需求

在主机上安装 NETCONF 客户端软件，通过 NETCONF 读取设备（Agent）的三层以太网接口 HGE2/0/25 流量统计信息。

图3-19 SNMP 功能典型配置组网图



说明

NETCONF 客户端是通过 Device 设备提供的 NETCONF XML API 获取的接口流量统计信息。

2. 配置步骤

切换为三层以太网接口。

```
<Sysname> system-view
[Sysname] interface hundredgige 2/0/25
[Sysname-HundredGigE2/0/25] port link-mode route
```

配置接口 IP 地址（略）。

配置 NETCONF，请参见 3.1.3 2. 配置步骤。

3. 查询流量统计数据示例

说明

- 设备提供 2 个表用于进行接口流量统计：Ifmgr/Statistics 和 IPFW/IPStatistic。通过 Ifmgr/Statistics 表可查询接口以字节为单位和以包为单位的统计信息，包括单播报文、非单播报、未知报文、丢弃报文等类型报文的统计数据。通过 IPFW/IPStatistic 表可查询接口以包为单位的 IPv4 或 IPv6 报文的数据。
- 以下使用 Ifmgr/Statistics 表查询接口 HundredGigE2/0/25 统计信息为例，使用 IPFW/IPStatistic 表查询接口统计信息的配置过程相似。

```
[Sysname-probe]display system internal ifmgr list | in HundredGigE2/0/25
        Bridge-Aggregation2(index:220)
```

请将以下报文拷贝、粘贴到 NETCONF 客户端。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
        <Ifmgr>
          <Statistics>
```

```
            <Interface>
             <IfIndex>220</IfIndex>
             <Name>HundredGigE2/0/25</Name>
             <AbbreviatedName></AbbreviatedName>
             <InOctets></InOctets>
             <InUcastPkts></InUcastPkts>
             <InNUcastPkts></InNUcastPkts>
             <InDiscards></InDiscards>
             <InErrors></InErrors>
             <InUnknownProtos></InUnknownProtos>
             <InRate></InRate>
             <OutOctets></OutOctets>
             <OutUcastPkts></OutUcastPkts>
             <OutNUcastPkts></OutNUcastPkts>
             <OutDiscards></OutDiscards>
             <OutErrors></OutErrors>
             <OutRate></OutRate>
             <LastClear></LastClear>
            </Interface>
           </Statistics>
         </Ifmgr>
       </top>
     </filter>
   </get>
</rpc>
```

如果客户端收到类似如下的报文，则表示操作成功。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data>
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
              <Ifmgr>
                 <Statistics>
                    <Interface>
                       <IfIndex>220</IfIndex>
                       <Name>HundredGigE2/0/25</Name>
                       <AbbreviatedName>HGE2/0/25</AbbreviatedName>
                       <InOctets>77760</InOctets>
                       <InUcastPkts>606</InUcastPkts>
                       <InNUcastPkts>6</InNUcastPkts>
                       <InDiscards>0</InDiscards>
                       <InErrors>0</InErrors>
                       <InUnknownProtos>0</InUnknownProtos>
                       <InRate>0</InRate>
                       <OutOctets>77888</OutOctets>
                       <OutUcastPkts>607</OutUcastPkts>
                       <OutNUcastPkts>7</OutNUcastPkts>
                       <OutDiscards>0</OutDiscards>
                       <OutErrors>0</OutErrors>
                       <OutRate>0</OutRate>
```

```
                        <LastClear>0000-00-00T00:00:00</LastClear>
                    </Interface>
                </Statistics>
            </Ifmgr>
        </top>
    </data>
</rpc-reply>
```

4. 更多信息

关于 NETCONF 配置的更多信息，请参见对应产品的“NETCONF 配置”。

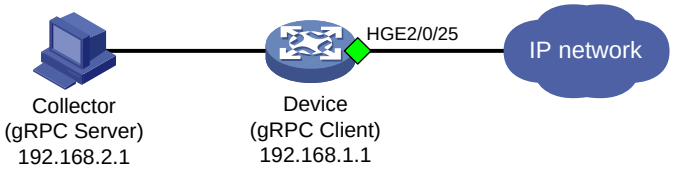
关于 Ifmgr/Statistics 和 IPFW/IPStatistic 的更多信息，请参见《H3C Comware 7 NETCONF XML API Reference 》。

3.3.4 gRPC 实现

1. 配置需求

采集器通过 gRPC 协议读取设备（Device）的三层以太网接口 HGE2/0/25 流量统计信息。

图3-20 gRPC 功能典型配置组网图



2. 配置步骤

配置 gRPC，请参见 3.1.4 2. 配置步骤。

3. 查询流量统计数据

采集器每 30 秒收到一次设备推送的接口数据统计信息。

4. 更多信息

关于 gRPC 配置的更多信息，请参见对应产品的“gRPC 配置”。

3.4 二层聚合接口流量统计

3.4.1 命令行方式实现

1. 配置需求

获取二聚合层接口 Bridge-Aggregation2 流量统计数据。

2. 配置限制和指导

- 可直接使用 **display interface** 命令获取二层聚合接口的流量统计信息，统计数据不区分 IPv4 和 IPv6 报文。
- 二层聚合接口不支持开启三层流量统计功能。

- 不支持通过 **display ip interface** 或 **display ipv6 interface** 命令查看接口流量统计信息。
- 在某些情况，需要统计某一时段的接口流量统计数据，可以在用户视图通过 **reset counters interface** 命令清除接口原有报文统计信息，重新进行统计。
- **reset counters interface** 命令能够清除 **display interface** 命令行的端口计数但不能清除 MIB 节点计数。

3. 查询流量统计数据示例

查询接口 Bridge-Aggregation 流量统计信息。

```
[Sysname]display interface Bridge-Aggregation2
Bridge-Aggregation2
.........
Last 300 seconds input:  1 packets/sec 254 bytes/sec 0%
Last 300 seconds output:  1 packets/sec 254 bytes/sec 0%
Input (total):  610 packets, 77632 bytes
        603 unicasts, 2 broadcasts, 5 multicasts, 0 pauses
Input (normal):  610 packets, - bytes
        603 unicasts, 2 broadcasts, 5 multicasts, 0 pauses
Input:  0 input errors, 0 runts, 0 giants, 0 throttles
        0 CRC, 0 frame, - overruns, 0 aborts
        - ignored, - parity errors
Output (total): 619 packets, 78296 bytes
        605 unicasts, 6 broadcasts, 8 multicasts, 0 pauses
Output (normal): 619 packets, - bytes
        605 unicasts, 6 broadcasts, 8 multicasts, 0 pauses
Output: 0 output errors, - underruns, 0 buffer failures
        0 aborts, 0 deferred, 0 collisions, 0 late collisions
        0 lost carrier, - no carrier
```

表3-7 display interface 命令显示信息描述表

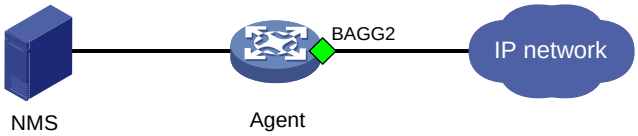
字段	描述
Bridge-Aggregation1	二层聚合接口名
Last clearing of counters	最后一次使用**reset counters interface**命令清除接口统计信息的时间。如果从设备启动一直没有执行**reset counters interface**命令清除过该接口下的统计信息，则显示Never
Last 300 seconds input rate	接口在最近300秒接收报文的平均速率
Last 300 seconds output rate	接口在最近300秒发送报文的平均速率
Input/Output (total)	接口接收/发送的全部报文的统计值
Input/Output (normal)	接口接收/发送的正常报文的统计值

3.4.2 SNMP 实现

1. 配置需求

NMS 通过 SNMP 协议读取设备（Agent）的二聚合层接口 Bridge-Aggregation2 入方向流量统计信息。

图3-21 SNMP 功能典型配置组网图



2. 配置限制和指导

- 对于二层聚合接口，端口流量统计主要有四张表：ifEntry（OID 为 1.3.6.1.2.1.2.2.1）、ifXEntry（OID 为 1.3.6.1.2.1.31.1.1）、hh3cIfFlowStatEntry（OID 为 1.3.6.1.4.1.25506.2.40.2.1.2.1.1）和 ipIfStatsEntry（OID 为 1.3.6.1.2.1.4.31.3.1）。
- 对于 ifEntry 表和 ifXEntry 表，ifEntry 表中的端口流量统计节点数据长度都是 32 位的，ifXEntry 表中的端口流量统计节点的部分节点数据长度是 64 位的。因此在统计端口流量时，ifEntry 表中的端口流量统计节点可能会出溢出现象。ifXEntry 表中的端口流量统计节点不会出现溢出的情况。ifEntry 表和表 ifXEntry 表中的节点不完全一样，二者是相交的关系。因此我们在查看端口流量统计时，如果能在 ifXEntry 表中找到，就以 ifXEntry 表的结果为准，如果在表 ifXEntry 中找不到，再去查看表 ifEntry。
- 可以通过 ifEntry 表、ifXEntry 表、hh3cIfFlowStatEntry 表、hh3cIfHCFlowStatEntry 表和 hh3cifPortProtocolStatEntry 表下的子节点获取不同报文数据。

3. 配置步骤

配置 SNMP，请参见 3.1.3 2. 配置步骤。

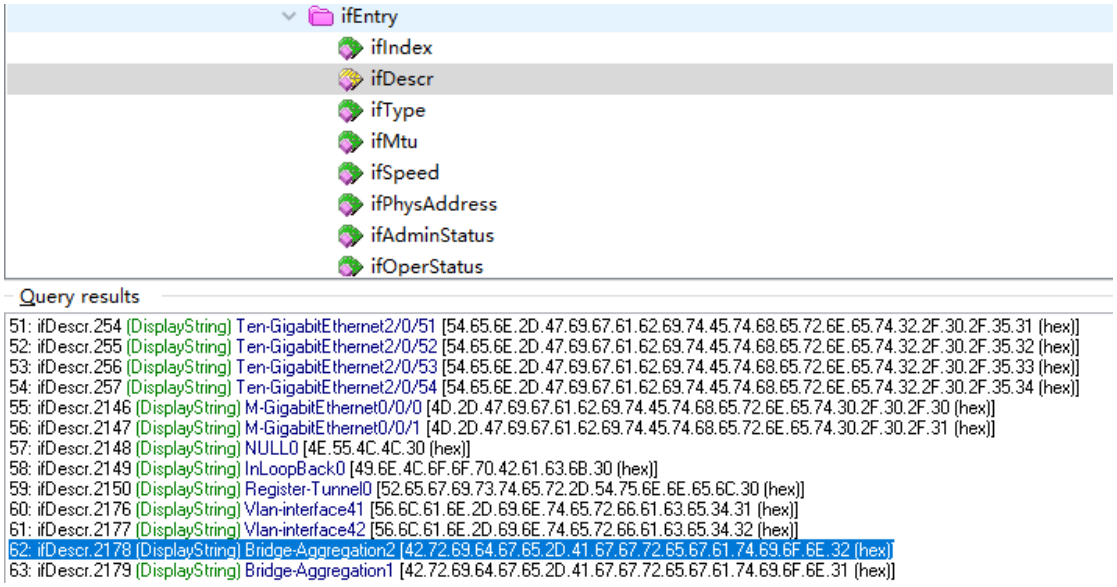
4. 查询流量统计数据示例

说明

- 查询接口流量统计数据前，我们需要获取接口的索引，然后通过索引来查接口的流量统计数据。
- 设备 IRF 成员编号不同时，接口索引值可能不同，具体以实际查询结果为准。
- 以下以通过 MIB Browser 查询 ifXTable 表获取接口 BRGG2 入方向的流量统计数据为例，查询

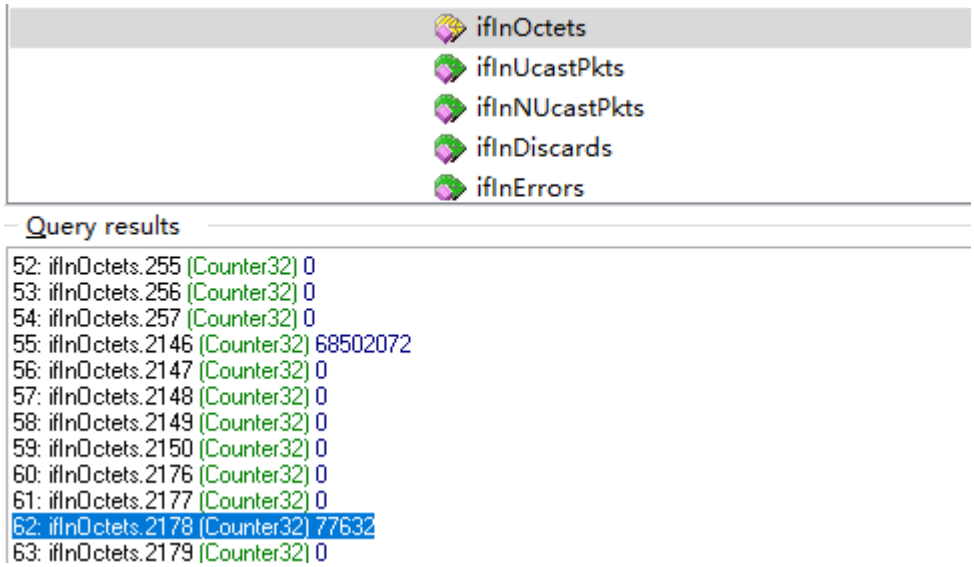
通过 ifName 节点（1.3.6.1.2.1.31.1.1.1.1）查询接口 BRGG2 的索引。查询结果会显示在 query results 对话框中，如图 3-22 所示，接口 BRGG2 索引为 2178。

图3-22 查询接口索引



如图 3-23 所示，通过 ifHCInOctets 表（OID 为 1.3.6.1.2.1.31.1.1.1.6）查询接口 BRGG2 入方向以字节为单位的流量统计数据。

图3-23 查询流量统计数据



5. 更多信息

关于 SNMP 的更多配置，请参见对应产品的 SNMP 配置。

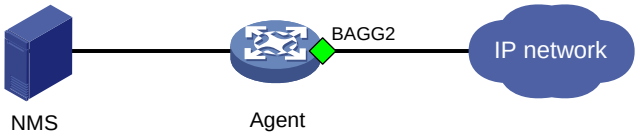
关于 MIB 文件的更多介绍，请参见对应产品的 MIB 参考。

3.4.3 NETCONF 实现

1. 配置需求

在主机上安装 NETCONF 客户端软件，通过 NETCONF 读取设备（Agent）的二聚合层接口 Bridge-Aggregation2 流量统计信息。

图3-24 SNMP 功能典型配置组网图



说明

NETCONF 客户端是通过 Device 设备提供的 NETCONF XML API 获取的接口流量统计信息。

2. 配置步骤

配置 NETCONF，请参见 3.1.3 2. 配置步骤。

3. 查询流量统计数据示例

说明

- 设备提供 2 个表用于进行接口流量统计：Ifmgr/Statistics 和 IPFW/IPStatistic。通过 Ifmgr/Statistics 表可查询接口以字节为单位和以包为单位的统计信息，包括单播报文、非单播报、未知报文、丢弃报文等类型报文的统计数据。通过 IPFW/IPStatistic 表可查询接口以包为单位的 IPv4 或 IPv6 报文的数据。
- 以下使用 Ifmgr/Statistics 表查询接口 BRAGG2 统计信息为例，使用 IPFW/IPStatistic 表查询接口统计信息的配置过程相似。

查询接口索引。

```
[Sysname-probe]display system internal ifmgr list | in Bridge-Aggregation2
        Bridge-Aggregation2(index:2178)
```

请将以下报文拷贝、粘贴到 NETCONF 客户端。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
        <Ifmgr>
          <Statistics>
           <Interface>
            <IfIndex>2178</IfIndex>
            <Name>Bridge-Aggregation2</Name>
            <AbbreviatedName></AbbreviatedName>
```

```
            <InOctets></InOctets>
            <InUcastPkts></InUcastPkts>
            <InNUcastPkts></InNUcastPkts>
            <InDiscards></InDiscards>
            <InErrors></InErrors>
            <InUnknownProtos></InUnknownProtos>
            <InRate></InRate>
            <OutOctets></OutOctets>
            <OutUcastPkts></OutUcastPkts>
            <OutNUcastPkts></OutNUcastPkts>
            <OutDiscards></OutDiscards>
            <OutErrors></OutErrors>
            <OutRate></OutRate>
            <LastClear></LastClear>
           </Interface>
          </Statistics>
        </Ifmgr>
      </top>
    </filter>
  </get>
</rpc>
```

如果客户端收到类似如下的报文，则表示操作成功。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data>
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
              <Ifmgr>
                 <Statistics>
                    <Interface>
                       <IfIndex>2178</IfIndex>
                       <Name>Bridge-Aggregation2</Name>
                       <AbbreviatedName>BAGG2/0/25</AbbreviatedName>
                       <InOctets>77632</InOctets>
                       <InUcastPkts>603</InUcastPkts>
                       <InNUcastPkts>7</InNUcastPkts>
                       <InDiscards>0</InDiscards>
                       <InErrors>0</InErrors>
                       <InUnknownProtos>0</InUnknownProtos>
                       <InRate>0</InRate>
                       <OutOctets>78296</OutOctets>
                       <OutUcastPkts>605</OutUcastPkts>
                       <OutNUcastPkts>14</OutNUcastPkts>
                       <OutDiscards>0</OutDiscards>
                       <OutErrors>0</OutErrors>
                       <OutRate>0</OutRate>
                       <LastClear>0000-00-00T00:00:00</LastClear>
                    </Interface>
                 </Statistics>
              </Ifmgr>
```

```
      </top>
    </data>
</rpc-reply>
```

4. 更多信息

关于 NETCONF 配置的更多信息，请参见对应产品的“NETCONF 配置”。

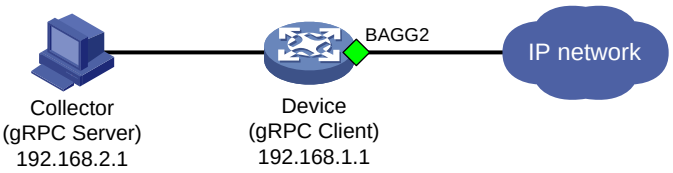
关于 Ifmgr/Statistics 和 IPFW/IPStatistic 的更多信息，请参见《H3C Comware 7 NETCONF XML API Reference 》。

3.4.4 gRPC 实现

1. 配置需求

采集器通过 gRPC 协议读取设备（Device）的二聚合层接口 Bridge-Aggregation2 的流量统计信息。

图3-25 gRPC 功能典型配置组网图



2. 配置步骤

配置 gRPC，请参见 3.1.4 2. 配置步骤。

3. 查询流量统计数据

采集器每 30 秒收到一次设备推送的接口数据统计信息。

4. 更多信息

关于 gRPC 配置的更多信息，请参见对应产品的“gRPC 配置”。

3.5 三层聚合接口流量统计

3.5.1 命令行方式实现

1. 配置需求

获取三层聚合接口 Route-Aggregation2 流量统计数据。

2. 配置限制和指导

- 可直接使用 **display interface** 命令获取三层聚合子接口的流量统计信息，统计数据不区分 IPv4 和 IPv6 报文。
- 三层聚合接口不支持开启三层流量统计功能。
- 如果三层聚合接口下面创建了子接口，那么子接口的流量统计在聚合口上，聚合子接口不支持流量统计。
- 在某些情况，需要统计某一时段的接口流量统计数据，可以在用户视图通过 **reset counters interface** 命令清除接口原有报文统计信息，重新进行统计。

- **reset counters interface** 命令能够清除 **display interface** 命令行的端口计数但不能清除 MIB 节点计数。

3. 配置步骤

创建三层聚合接口 Route-Aggregation2。

```
<Sysname> system-view
[Sysname] interface route-aggregation 2
```

4. 查询流量统计数据示例

查询接口 Route-Aggregation 流量统计信息。

```
[Sysname]display interface route-aggregation 2
Route-Aggregation2
........
Last 300 seconds input rate: 255 bytes/sec, 2040 bits/sec, 2 packets/sec
Last 300 seconds output rate: 255 bytes/sec, 2040 bits/sec, 2 packets/sec
611 packets input, 77696 bytes, 0 drops
627 packets output, 78912 bytes, 0 drops
```

表3-8 display interface 命令显示信息描述表

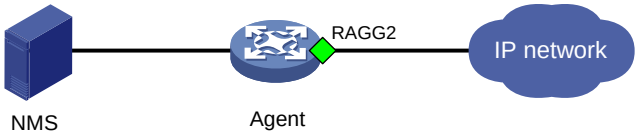
字段	描述
Route-Aggregation	三层聚合接口名
Last 300 seconds input rate	接口在最近300秒接收报文的平均速率
Last 300 seconds output rate	接口在最近300秒发送报文的平均速率
Input	接口接收的全部报文的统计值
output	接口发送的正常报文的统计值

3.5.2 SNMP 实现

1. 配置需求

NMS 通过 SNMP 协议读取设备（Agent）的三层聚合接口 Route-Aggregation2 入方向流量统计信息。

图3-26 SNMP 功能典型配置组网图



2. 配置限制和指导

- 三层聚合接口统计数据不区分 IPv4 和 IPv6 报文。
- 对于三层聚合接口，端口流量统计主要有四张表：ifEntry（OID 为 1.3.6.1.2.1.2.2.1）、ifXEntry（OID 为 1.3.6.1.2.1.31.1.1）、hh3cIfFlowStatEntry（OID 为

1.3.6.1.4.1.25506.2.40.2.1.2.1.1）和 hh3cIfHCFlowStatEntry（OID 为 1.3.6.1.4.1.25506.2.40.2.1.2.3.1）。

- 对于 ifEntry 表和 ifXEntry 表，ifEntry 表中的端口流量统计节点数据长度都是 32 位的，ifXEntry 表中的端口流量统计部分节点数据长度是 64 位的。因此在统计端口流量时，ifEntry 表中的端口流量统计节点可能会出溢出现象。ifXEntry 表中的端口流量统计节点不会出现溢出的情况。ifEntry 表和表 ifXEntry 表中的节点不完全一样，二者是相交的关系。因此我们在查看端口流量统计时，如果能在 ifXEntry 表中找到，就以 ifXEntry 表的结果为准，如果在表 ifXEntry 中找不到，再去查看表 ifEntry。
- 可以通过 ifEntry 表、ifXEntry 表、hh3cIfFlowStatEntry 表和 hh3cIfHCFlowStatEntry 表下的子节点获取不同报文数据。

3. 配置步骤

创建三层聚合接口 Route-Aggregation2。

```
<Sysname> system-view
[Sysname] interface route-aggregation 2
```

分别将接口 hundredgige1/0/25 至 hundredgige1/0/27 加入到聚合组 2 中。

```
[Sysname] interface hundredgige 1/0/25
[Sysname-HundredGigE1/0/25] port link-aggregation group 2
[Sysname] interface hundredgige 1/0/26
[Sysname-HundredGigE1/0/26] port link-aggregation group 2
[Sysname] interface hundredgige 1/0/27
[Sysname-HundredGigE1/0/27] port link-aggregation group 2
```

配置 SNMP，请参见 3.1.3 2. 配置步骤。

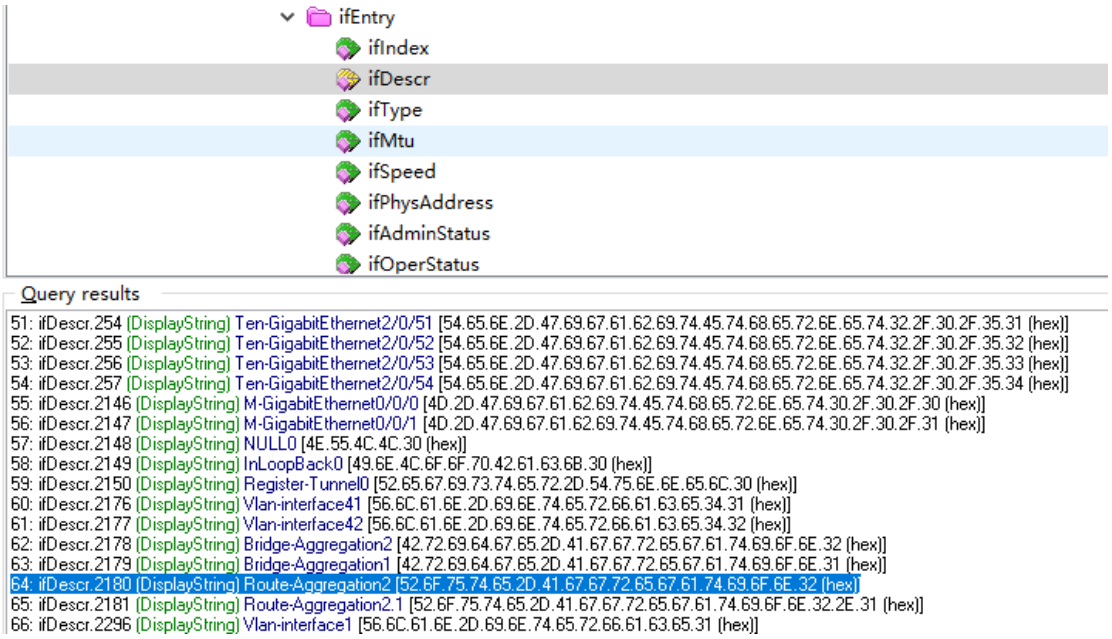
4. 查询流量统计数据示例

说明

- 查询接口流量统计数据前，我们需要获取接口的索引，然后通过索引来查接口的流量统计数据。
- 设备 IRF 成员编号不同时，接口索引值可能不同，具体以实际查询结果为准。
- 以下以通过 MIB Browser 查询 ifXTable 表获取接口 Route-Aggregation2 入方向的流量统计数据为例。

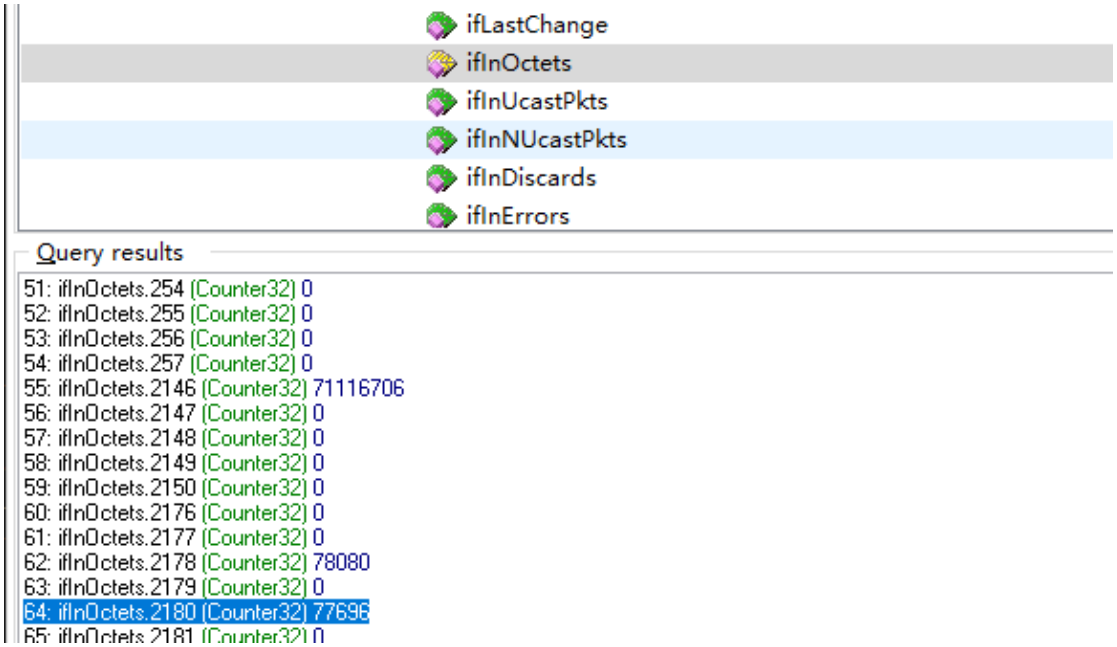
通过 ifDescr 节点（1.3.6.1.2.1.2.2.1.2）查询接口 Route-Aggregation2 的索引。查询结果会显示在 query results 对话框中，如图 3-27 所示，接口 Route-Aggregation2 索引为 2180。

图3-27 查询接口索引



如图 3-28 所示，通过 ifInOctets 表（OID 为 1.3.6.1.2.1.2.2.1.10）查询接口 Route-Aggregation2 入方向以字节为单位的流量统计数据。查询结果会显示在 query results 对话框中。

图3-28 查询流量统计数据



5. 更多信息

关于 SNMP 的更多配置，请参见对应产品的 SNMP 配置。

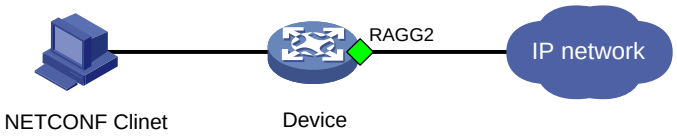
关于 MIB 文件的更多介绍，请参见对应产品的 MIB 参考。

3.5.3 NETCONF 实现

1. 配置需求

在主机上安装 NETCONF 客户端软件，通过 NETCONF 读取设备（Agent）的三层聚合接口 Route-Aggregation2 流量统计信息。

图3-29 SNMP 功能典型配置组网图



说明

- NETCONF 客户端是通过 Device 设备提供的 NETCONF XML API 获取的接口流量统计信息。

2. 配置限制和指导

三层聚合接口统计数据不区分 IPv4 和 IPv6 报文。

3. 配置步骤

创建三层聚合接口 Route-Aggregation2。

```
<Sysname> system-view
[Sysname] interface route-aggregation 2
```

分别将接口 hundredgige1/0/25 至 hundredgige1/0/27 加入到聚合组 2 中。

```
[Sysname] interface hundredgige 1/0/25
[Sysname-HundredGigE1/0/25] port link-aggregation group 2
[Sysname] interface hundredgige 1/0/26
[Sysname-HundredGigE1/0/26] port link-aggregation group 2
[Sysname] interface hundredgige 1/0/27
[Sysname-HundredGigE1/0/27] port link-aggregation group 2
```

配置 NETCONF，请参见 3.1.3 2. 配置步骤。

4. 查询流量统计数据示例

说明

- 通过 Ifmgr/Statistics 表可查询接口以字节为单位和以包为单位的统计信息，包括单播报文、非单播报、未知报文、丢弃报文等类型报文的统计数据。
- 以下使用 Ifmgr/Statistics 表查询三层聚合接口统计信息为例，使用 IPFW/IPStatistic 表查询接口统计信息的配置过程相似。

查询接口索引。

```
[Sysname-probe]display system internal ifmgr list | in Route-Aggregation2
        Route-Aggregation2(index:2180)
```

请将以下报文拷贝、粘贴到 NETCONF 客户端。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
        <Ifmgr>
          <Statistics>
           <Interface>
            <IfIndex>2180</IfIndex>
            <Name>Route-Aggregation2</Name>
            <AbbreviatedName></AbbreviatedName>
            <InOctets></InOctets>
            <InUcastPkts></InUcastPkts>
            <InNUcastPkts></InNUcastPkts>
            <InDiscards></InDiscards>
            <InErrors></InErrors>
            <InUnknownProtos></InUnknownProtos>
            <InRate></InRate>
            <OutOctets></OutOctets>
            <OutUcastPkts></OutUcastPkts>
            <OutNUcastPkts></OutNUcastPkts>
            <OutDiscards></OutDiscards>
            <OutErrors></OutErrors>
            <OutRate></OutRate>
            <LastClear></LastClear>
           </Interface>
          </Statistics>
        </Ifmgr>
      </top>
    </filter>
  </get>
</rpc>
```

如果客户端收到类似如下的报文，则表示操作成功。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data>
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
         <Ifmgr>
             <Statistics>
                 <Interface>
                    <IfIndex>2180</IfIndex>
                    <Name>Route-Aggregation2</Name>
                    <AbbreviatedName>RAGG2</AbbreviatedName>
                    <InOctets>77696</InOctets>
                    <InUcastPkts>603</InUcastPkts>
                    <InNUcastPkts>8</InNUcastPkts>
                    <InDiscards>0</InDiscards>
                    <InErrors>0</InErrors>
                    <InUnknownProtos>0</InUnknownProtos>
```

```
                    <InRate>0</InRate>
                    <OutOctets>78912</OutOctets>
                    <OutUcastPkts>605</OutUcastPkts>
                    <OutNUcastPkts>22</OutNUcastPkts>
                    <OutDiscards>0</OutDiscards>
                    <OutErrors>0</OutErrors>
                    <OutRate>0</OutRate>
                    <LastClear>0000-00-00T00:00:00</LastClear>
                  </Interface>
                </Statistics>
              </Ifmgr>
            </top>
          </data>
</rpc-reply>
```

5. 更多信息

关于 NETCONF 配置的更多信息，请参见对应产品的“NETCONF 配置”。

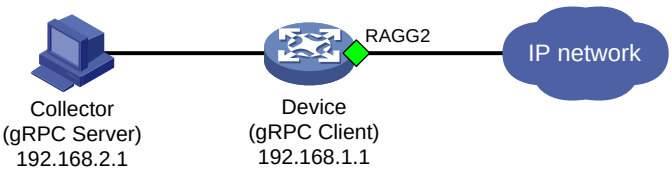
关于 Ifmgr/Statistics 和 IPFW/IPStatistic 的更多信息，请参见《H3C Comware 7 NETCONF XML API Reference 》。

3.5.4 gRPC 实现

1. 配置需求

采集器通过 gRPC 协议读取设备（Device）的三层聚合接口 Route-Aggregation2 流量统计信息。

图3-30 gRPC 功能典型配置组网图



2. 配置限制和指导

三层聚合接口统计数据不区分 IPv4 和 IPv6 报文。

3. 配置步骤

创建三层聚合接口 Route-Aggregation2。

```
<Sysname> system-view
[Sysname] interface route-aggregation 2
```

分别将接口 hundredgige1/0/25 至 hundredgige1/0/27 加入到聚合组 2 中。

```
[Sysname] interface hundredgige 1/0/25
[Sysname-HundredGigE1/0/25] port link-aggregation group 2
[Sysname] interface hundredgige 1/0/26
[Sysname-HundredGigE1/0/26] port link-aggregation group 2
[Sysname] interface hundredgige 1/0/27
[Sysname-HundredGigE1/0/27] port link-aggregation group 2
```

```
[Sysname-HundredGigE1/0/27] quit
```

配置 gRPC，请参见 3.1.4 2. 配置步骤。

4. 查询流量统计数据

采集器每 30 秒收到一次设备推送的接口数据统计信息。

5. 更多信息

关于 gRPC 配置的更多信息，请参见对应产品的“gRPC 配置”。

getgetgetget

3.6 接口丢包统计（基于MQC实现）

3.6.1 需求说明

配置 MQC 获取接口基于 CAR 的丢包统计数据。

说明

接口出方向同时配置MQC方式的CAR和队列调度策略时，设备会先对流量进行队列调度策略处理，然后在进行 CAR 处理，所以即使某些报文被 CAR 染色为红色且被丢弃，这部分报文依然会占用队列调度策略中的调度带宽。

3.6.2 命令行方式实现

1. 配置需求

查询接口 HundredGigE1/0/30 基于 CAR 的丢包统计数据。

2. 配置步骤

创建流分类 car，定义匹配接口所有流量规则。

```
<Sysname> system-view
[Sysname] traffic classifier car
[Sysname-classifier-car] if-match any
[Sysname-classifier-car] quit
```

创建流行为 car，为流行为配置流量监管，报文正常流速为 10000kbps，承诺突发尺寸为 625152bytes。

```
[Sysname]traffic behavior car
[Sysname-behavior-car] car cir 10000 cbs 625152
[Sysname-behavior-car] quit
```

创建 QoS 策略，为流分类 aa 指定流行为 aa。

```
[Sysname]qos policy car
[Sysname-qospolicy-car] classifier car behavior car
[Sysname-qospolicy-car] quit
```

将 QoS 策略应用在接口 HundredGigE1/0/30 的出方向。

```
[Sysname] interface hundredgige 1/0/30
[Sysname-HundredGigE1/0/30] qos apply policy car outbound
```

```
[Sysname-HundredGigE1/0/30] quit
```

3. 查询流量统计数据

查询接口 HundredGigE1/0/30 基于 CAR 的丢包统计数据。

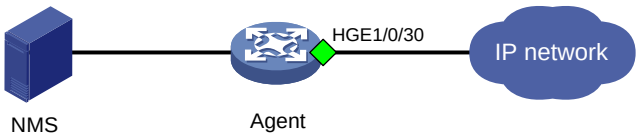
```
[Sysname]display qos policy interface hundredgige1/0/30
Interface: HundredGigE1/0/30
  Direction: Inbound
  Policy: car
   Classifier: car
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: car
      Committed Access Rate:
        CIR 10000 (kbps), CBS 625152 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 208137 (Packets) 26656384 (Bytes)
        Yellow packets: 0 (Packets) 0 (Bytes)
        Red packets   : 43306977 (Packets) 5543306496 (Bytes)
```

3.6.3 SNMP 方式实现

1. 配置需求

NMS 通过 SNMP 协议读取接口 HundredGigE1/0/30 基于 CAR 列表的丢包统计数据。

图3-31 SNMP 功能典型配置组网图



2. 配置步骤

配置基于 CAR 的流量管理，请参见 3.6.2 2. 配置步骤。

配置 SNMP，请参见 3.1.3 2. 配置步骤。

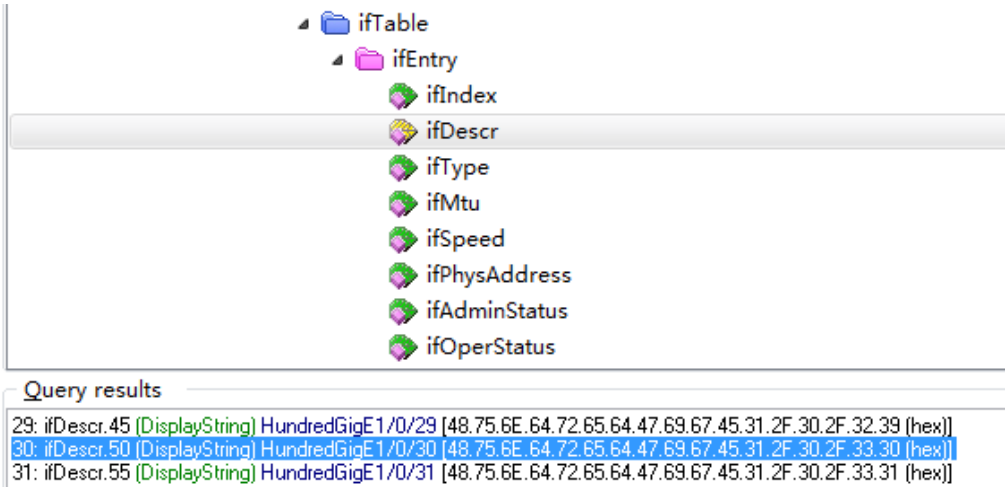
3. 查询流量统计数据示例

说明

本举例以通过 MIB Browser 查询 Agent 设备接口 HundredGigE1/0/30 基于 CAR 的丢包统计数据为例。

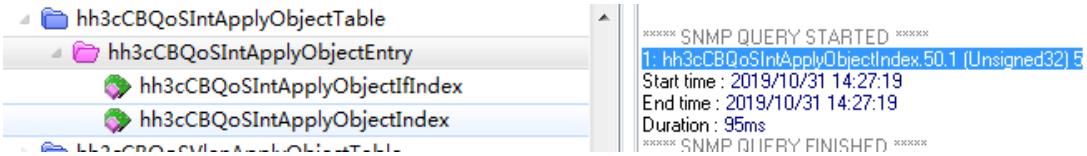
如图 3-32 所示，通过 ifName 节点（1.3.6.1.2.1.31.1.1.1.1）的子节点 ifDescr（1.3.6.1.2.1.31.1.1.1.1.2）查询以太网接口的索引。查询结果会显示在 Query results 对话框中，接口 HundredGigE1/0/30 索引为 50。

图3-32 查询接口索引



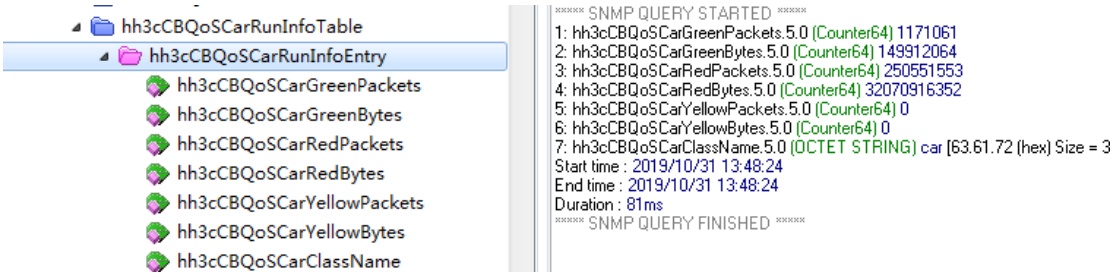
通过接口索引在hh3cCBQoSIntApplyObjectIndex表（ODI为1.3.6.1.4.1.25506.2.65.2.1.5.5.2.1.2）查询应用在接口 QoS 策略的索引。如图 3-33 所示，查询应用在接口 HundredGigE1/0/30 的 QoS 策略索引为 5。

图3-33 查询应用在接口 QoS 策略索引



如通过 hh3cCBQoSCarRunInfoEntry 表（OID 为 1.3.6.1.4.1.25506.2.65.2.1.5.6.3.1）查询接口 HundredGigE1/0/30 基于 CAR 的丢包数据。

图3-34 基于 CAR 的丢包数据



4. 更多信息

关于 SNMP 的更多配置，请参见对应产品的 SNMP 配置。

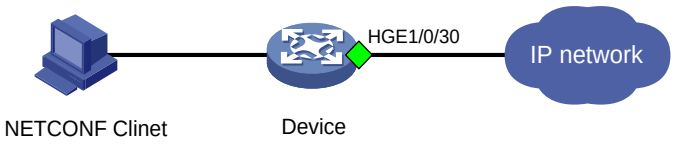
关于 MIB 文件的更多介绍，请参见对应产品的 MIB 参考。

3.6.4 NETCONF 实现

1. 配置需求

在主机上安装 NETCONF 客户端软件，通过 NETCONF 读取设备（Agent）的接口 HGE1/0/30 的队列缓冲区流量统计信息。

图3-35 SNMP 功能典型配置组网图



说明

NETCONF 客户端是通过 Device 设备提供的 NETCONF XML API 获取的接口流量统计信息。

2. 配置步骤

配置 NETCONF，请参见 3.1.3 2. 配置步骤相同。

3. 查询流量统计数据示例

说明

设备提供 QSTAT/QueueStat 表用于统计接口队列流量数据。通过 QSTAT/InterfaceStat 表可查询以字节为单位和以包为单位的统计信息。

以下使用 QSTAT/ QueueStat 表查询 HundredGigE1/0/30 接口统计信息为例。

在设备 Probe 视图使用 **display system internal ifmgr list | include HundredGigE**1/0/30 命令查询接口 HundredGigE1/0/30 的索引。

```
<Sysname> system-view
[Sysname] probe
[Sysname-probe]display system internal ifmgr list | include HundredGigE1/0/30
         HundredGigE1/0/30(index:50)
```

请将以下报文拷贝、粘贴到 NETCONF 客户端。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
        <QSTAT>
          <QueueStat>
            <Statistics>
               <IfIndex>50</IfIndex>
               <Direction></Direction>
               <QueueID></QueueID>
```

```
                <PassPkt></PassPkt>
                <PassByte></PassByte>
                <DropPkt></DropPkt>
                <DropByte></DropByte>
                <PacketRate></PacketRate>
                <BitRate></BitRate>



                <CurrQueLen></CurrQueLen>

            </Statistics>
          </QueueStat>
        </QSTAT>
      </top>
    </filter>
  </get>
</rpc>
```

如果客户端收到类似如下的报文，则表示操作成功。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <data>
     <top xmlns="http://www.h3c.com/netconf/data:1.0">
        <QSTAT>
            <QueueStat>
                 <Statistics>
                    <IfIndex>50</IfIndex>
                    <Direction>1</Direction>
                    <QueueID>0</QueueID>
                    <PassPkt>0</PassPkt>
                    <PassByte>0</PassByte>
                    <DropPkt>0</DropPkt>
                    <DropByte>0</DropByte>
                    <PacketRate>0</PacketRate>
                    <BitRate>0</BitRate>
                    <CurrQueLen>0</CurrQueLen>
                 </Statistics>
                    <Statistics>
                    <IfIndex>50</IfIndex>
                    <Direction>1</Direction>
                    <QueueID>1</QueueID>
                    <PassPkt>0</PassPkt>
                    <PassByte>0</PassByte>
                    <DropPkt>0</DropPkt>
                    <DropByte>0</DropByte>
                    <PacketRate>0</PacketRate>
                    <BitRate>0</BitRate>
                    <CurrQueLen>0</CurrQueLen>
                 </Statistics>
```

```
<Statistics>
   <IfIndex>50</IfIndex>
   <Direction>1</Direction>
   <QueueID>2</QueueID>
   <PassPkt>3983693702452</PassPkt>
   <PassByte>533804491661232</PassByte>
   <DropPkt>2705999003341</DropPkt>
   <DropByte>346367872427648</DropByte>
   <PacketRate>11260285</PacketRate>
   <BitRate>11528004744</BitRate>
   <CurrQueLen>2</CurrQueLen>
</Statistics>
<Statistics>
   <IfIndex>50</IfIndex>
   <Direction>1</Direction>
   <QueueID>3</QueueID>
   <PassPkt>0</PassPkt>
   <PassByte>0</PassByte>
   <DropPkt>0</DropPkt>
   <DropByte>0</DropByte>
   <PacketRate>0</PacketRate>
   <BitRate>0</BitRate>
   <CurrQueLen>0</CurrQueLen>
</Statistics>
<Statistics>
   <IfIndex>50</IfIndex>
   <Direction>1</Direction>
   <QueueID>4</QueueID>
   <PassPkt>0</PassPkt>
   <PassByte>0</PassByte>
   <DropPkt>0</DropPkt>
   <DropByte>0</DropByte>
   <PacketRate>0</PacketRate>
   <BitRate>0</BitRate>
   <CurrQueLen>0</CurrQueLen>
</Statistics>
<Statistics>
   <IfIndex>50</IfIndex>
   <Direction>1</Direction>
   <QueueID>5</QueueID>
   <PassPkt>0</PassPkt>
   <PassByte>0</PassByte>
   <DropPkt>0</DropPkt>
   <DropByte>0</DropByte>
   <PacketRate>0</PacketRate>
   <BitRate>0</BitRate>
   <CurrQueLen>0</CurrQueLen>
 </Statistics>
```

```
                <Statistics>
                  <IfIndex>50</IfIndex>
                  <Direction>1</Direction>
                  <QueueID>6</QueueID>
                  <PassPkt>0</PassPkt>
                  <PassByte>0</PassByte>
                  <DropPkt>0</DropPkt>
                  <DropByte>0</DropByte>
                  <PacketRate>0</PacketRate>
                  <BitRate>0</BitRate>
                  <CurrQueLen>0</CurrQueLen>
                </Statistics>
                <Statistics>
                  <IfIndex>50</IfIndex>
                  <Direction>1</Direction>
                  <QueueID>7</QueueID>
                  <PassPkt>314548</PassPkt>
                  <PassByte>39913188</PassByte>
                  <DropPkt>0</DropPkt>
                  <DropByte>0</DropByte>
                  <PacketRate>0</PacketRate>
                  <BitRate>0</BitRate>
                  <CurrQueLen>0</CurrQueLen>
                </Statistics>
              </QueueStat>
            </QSTAT>
          </top>
        </data>
</rpc-reply>
```

4. 更多信息

关于 NETCONF 配置的更多信息，请参见对应产品的“NETCONF 配置”。

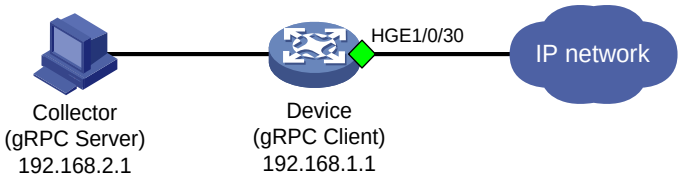
关于 QSTAT/QueueStat 的更多信息，请参见《H3C Comware 7 NETCONF XML API Reference》。

3.6.5 gRPC 方式实现

1. 配置需求

采集器通过 gRPC 协议读取设备（Device）接口 HGE1/0/30 的队列缓冲区流量统计信息。

图3-36 gRPC 功能典型配置组网图



2. 配置步骤

在开始下面的配置之前，请确保设备与采集器的 IP 地址都已配置完毕，并且它们之间路由可达。

开启 gRPC 功能。

```
<Sysname> system-view
[Sysname] grpc enable
```

创建传感器组 test，并添加采样路径为 QSTAT/QueueStat。

说明

配置采样路径为 QSTAT/QueueStat，设备会收集所有接口队列缓冲区的流量数据，并将数据上传给采集器。

```
[Sysname] telemetry
[Sysname-telemetry] sensor-group test
[Sysname-telemetry-sensor-group-test] sensor path qstat/queuestat
[Sysname-telemetry-sensor-group-test] quit
```

创建目标组 collector1，并配置 IP 地址为 192.168.2.1、端口号为 50050 的采集器。

```
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] ipv4-address 192.168.2.1 port 50050
[Sysname-telemetry-destination-group-collector1] quit
```

创建订阅 A，配置关联传感器组为 test，数据采样和推送周期为 30 秒，关联目标组为 collector1。

```
[Sysname-telemetry] subscription A
[Sysname-telemetry-subscription-A] sensor-group test sample-interval 30
[Sysname-telemetry-subscription-A] destination-group collector1
[Sysname-telemetry-subscription-A] quit
```

3. 查询流量统计数据

采集器每 30 秒收到一次设备推送的数据信息。

4. 更多信息

关于 gRPC 配置的更多信息，请参见对应产品的“gRPC 配置”。

3.7 以太网接口流量统计（基于MQC实现）

3.7.1 需求说明

通过 MQC 方式获取以太网接口流量统计数据。

3.7.2 命令行方式实现

1. 配置需求

通过 MQC 获取接口 HundredGigE1/0/30 入方向流量统计数据。

说明

设备支持通过 **accounting [byte | packet]*** 命令配置以包和字节为单位的流量统计动作。byte 和 packet 不能同时配置。

。

2. 配置步骤

创建流分类 aa，定义匹配接口所有流量规则。

```
<Sysname> system-view
[Sysname] traffic classifier aa
[Sysname-classifier-aa] if-match any
[Sysname-classifier-aa] quit
```

创建流行为 aa，为流行为配置以包为单位进行流量统计动作。

```
[Sysname]traffic behavior aa
[Sysname-behavior-aa] accounting packet
[Sysname-behavior-aa] quit
```

创建 QoS 策略，为流分类 aa 指定流行为 aa。

```
[Sysname]qos policy aa
[Sysname-qospolicy-aa] classifier aa behavior aa
[Sysname-qospolicy-aa] quit
```

将 QoS 策略应用在接口 HundredGigE1/0/30 的入方向。

```
[Sysname] interface hundredgige 1/0/30
[Sysname-HundredGigE1/0/30] qos apply policy aa inbound
[Sysname-HundredGigE1/0/30] quit
```

3. 查询流量统计数据

查询接口 HundredGigE1/0/30 的流量统计数据。

```
[Sysname]dis qos policy  interface hun1/0/30
Interface: HundredGigE1/0/30
  Direction: Inbound
  Policy: car
   Classifier: car
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: car
      Accounting enable:
        29287176 (Packets)
```

表3-9 display qos policy interface 命令显示信息描述表

字段	描述
Direction	QoS策略应用的方向
policy	QoS策略名
Classifier	类的名称及其内容，内容可以有多种类型

字段	描述
Operator	分类规则之间的逻辑关系
Rule(s)	分类规则
if-match any	匹配经过接口的所有报文
Behavior	行为的名称及其内容
Accounting enable	流量统计动作

4. 更多信息

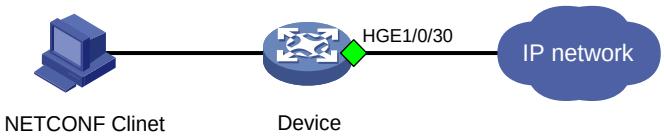
关于 MQC 配置的更多信息，请参见对应产品的“QoS 配置”和“QoS 命令”。

3.7.3 SNMP 方式实现

1. 配置需求

NMS 通过 SNMP 协议读取接口 HundredGigE1/0/30 入方向流量统计信息。

图3-37 SNMP 功能典型配置组网图



2. 配置步骤

配置 MQC 统计以太网接口流量，请参见 3.7.2 2. 配置步骤。

配置 SNMP，请参见 3.1.3 2. 配置步骤。

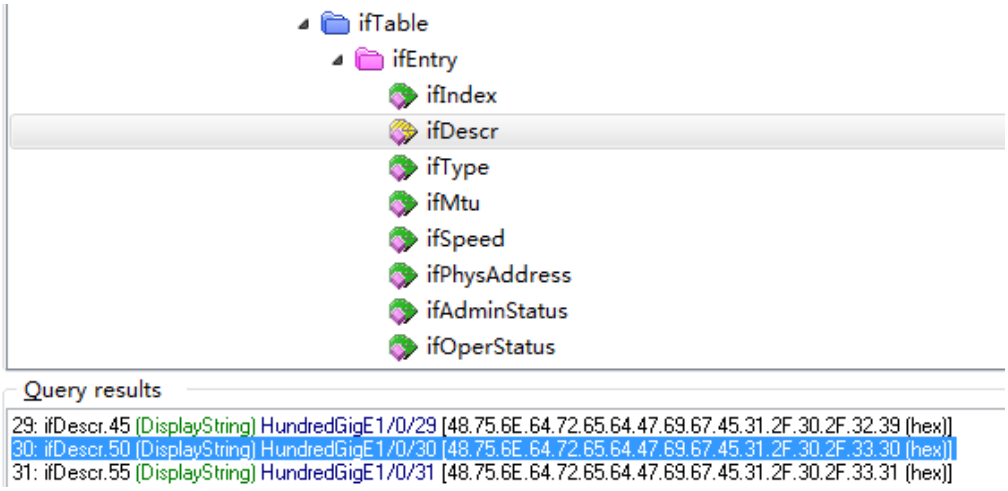
3. 查询流量统计数据示例

说明

- 查询以太网接口流量统计数据前，我们需要获取以太网接口的索引，然后通过索引来查以太网接口的流量统计数据。
- 设备 IRF 成员编号不同时，以太网接口索引值可能不同，具体以实际查询结果为准。
- 查询接口 HundredGigE1/0/30 的流量统计数据时，我们需要通过 ifName 节点（OID 为 1.3.6.1.2.1.31.1.1.1.1）查询接口的索引，然后通过 hh3cCBQoSIntApplyObjectIndex 表（OID 为 1.3.6.1.4.1.25506.2.65.2.1.5.5.2.1.2）获取应用在指定接口上 QoS 策略目标的索引，最后使用应用在指定接口上 QoS 策略目标的索引在 hh3cCBQoSAccountingRunInfoEntry 表（OID 为 1.3.6.1.4.1.25506.2.65.2.1.5.6.8.1）的子表中查询接口的流量统计数据。
- 以下以通过 MIB Browser 查询以太网入方向的流量统计数据为例。

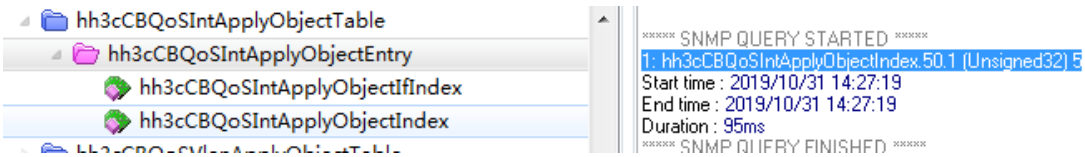
如图 3-38 所示，通过 ifName 节点（OID 为 1.3.6.1.2.1.31.1.1.1.1）的子节点 ifDescr（1.3.6.1.2.1.31.1.1.1.1.2）查询以太网接口的索引。查询结果会显示在 Query results 对话框中，接口 HundredGigE1/0/30 索引为 50。

图3-38 查询接口索引



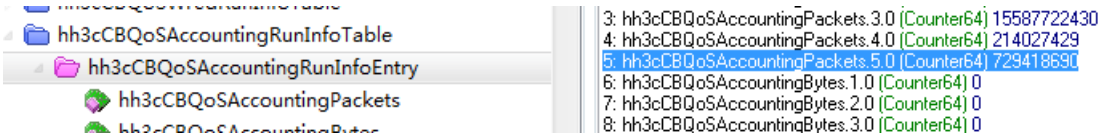
通过接口索引在hh3cCBQoSIntApplyObjectIndex表（ODI为1.3.6.1.4.1.25506.2.65.2.1.5.5.2.1.2）查询应用在接口 QoS 策略的索引。如图 3-39 所示，查询应用在接口 HundredGigE1/0/30 的 QoS 策略索引为 5。

图3-39 查询应用在接口 QoS 策略索引



如图 3-40 所示，通过 hh3cCBQoSAccountingRunInfoEntry 表（OID 为 1.3.6.1.4.1.25506.2.65.2.1.5.6.8.1）查询接口 HundredGigE1/0/30 入方向以包为单位的流量统计数据。

图3-40 查询流量统计数据



4. 更多信息

关于 SNMP 的更多配置，请参见对应产品的 SNMP 配置。

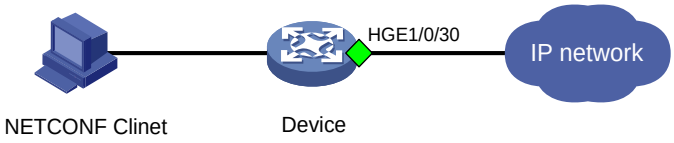
关于 MIB 文件的更多介绍，请参见对应产品的 MIB 参考。

3.7.4 NETCONF 实现

1. 配置需求

在主机上安装 NETCONF 客户端软件，通过 NETCONF 读取设备（Agent）的二层以太网接口 HGE1/0/30 流量统计信息。

图3-41 SNMP 功能典型配置组网图



说明

NETCONF客户端是通过Device设备提供的NETCONF XML API获取的以太网接口流量统计信息。

2. 配置步骤

配置 MQC 统计以太网接口流量，请参见 3.7.2 2. 配置步骤。

设备侧配置与 3.1.3 2. 配置步骤相同。

3. 查询流量统计数据示例

说明

设备提供 MQC/AccountRunInfo 表用于通过 MQC 方式进行流量统计。通过 MQC/AccountRunInfo 表可查询以字节为单位和以包为单位的统计信息。

以下使用 MQC/AccountRunInfo 表查询接口 HundredGigE2/0/25 统计信息为例。

请将以下报文拷贝、粘贴到 NETCONF 客户端。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
        <MQC>
          <AccountRunInfo>
            <AccountRunInfoEntry>
              <AppType></AppType>                    //MQC 应用位置，1 表示接口、2 表示 VLAN
              <AppMainIndex></AppMainIndex>          //MQC 应用位置主索引
              <AppSubIndex></AppSubIndex>            //MQC 子索引
              <AppDirection></AppDirection>          //MQC 应用的方向，1 表示入方向，2 表示出方向
              <CBMapIndex></CBMapIndex>              //流分类和流行为映射索引
              <AccountPkts></AccountPkts>            //以包为单位的统计流量数据
              <AccountBytes></AccountBytes>          //以字节为单位的统计流量数据
            </AccountRunInfoEntry>
```

```
          </AccountRunInfo>
        </MQC>
      </top>
    </filter>
  </get>
</rpc>
```

如果客户端收到类似如下的报文，则表示操作成功。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<data>
   <top xmlns="http://www.h3c.com/netconf/data:1.0">
      <MQC>
        <AccountRunInfo>
           <AccountRunInfoEntry>
              <AppType>1</AppType>
              <AppMainIndex>50</AppMainIndex>
              <AppSubIndex>0</AppSubIndex>
              <AppDirection>1</AppDirection>
              <CBMapIndex>0</CBMapIndex>
              <AccountPkts>150</AccountPkts>
           </AccountRunInfoEntry>
           </AccountRunInfo>
      /MQC>
   </top>
   </data>
</rpc-reply>
```

4. 更多信息

关于 NETCONF 配置的更多信息，请参见对应产品的“NETCONF 配置”。

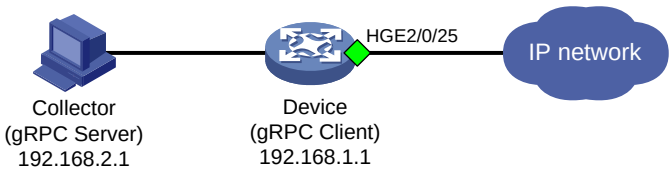
关于MQC/AccountRunInfo的更多信息，请参见《H3C Comware 7 NETCONF XML API Reference》。

3.7.5 gRPC 方式实现

1. 配置需求

采集器通过 gRPC 协议读取设备（Device）的二层以太网接口 HGE2/0/25 流量统计信息。

图3-42 gRPC 功能典型配置组网图



2. 配置步骤

在开始下面的配置之前，请确保设备与采集器的 IP 地址都已配置完毕，并且它们之间路由可达。

配置 MQC 统计以太网接口流量，请参见 3.7.2 2. 配置步骤。

开启 gRPC 功能。

```
<Sysname> system-view
[Sysname] grpc enable
```
创建传感器组 test，并添加采样路径为 MQC/AccountRunInfo。

说明

配置采样路径为 MQC/AccountRunInfo，设备会收集设备所有接口的流量统计数据，并将数据上传给采集器。

```
[Sysname] telemetry
[Sysname-telemetry] sensor-group test
[Sysname-telemetry-sensor-group-test] sensor path mqc/accountruninfo
[Sysname-telemetry-sensor-group-test] quit
```
创建目标组 collector1，并配置 IP 地址为 192.168.2.1、端口号为 50050 的采集器。
```
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] ipv4-address 192.168.2.1 port 50050
[Sysname-telemetry-destination-group-collector1] quit
```
创建订阅 A，配置关联传感器组为 test，数据采样和推送周期为 30 秒，关联目标组为 collector1。
```
[Sysname-telemetry] subscription A
[Sysname-telemetry-subscription-A] sensor-group test sample-interval 30
[Sysname-telemetry-subscription-A] destination-group collector1
[Sysname-telemetry-subscription-A] quit
```
3. 查询流量统计数据

采集器每 30 秒收到一次设备推送的数据信息。

4. 更多信息

关于 gRPC 配置的更多信息，请参见对应产品的“gRPC 配置”。

4 VXLAN 流量统计实现

说明

4.1 AC流量统计

4.1.1 需求说明

获取 AC 的流量统计数据。

4.1.2 配置限制和指导

VTEP 支持采用如下几种方式在数据帧和 VXLAN 之间建立关联：

- 方式一：将以太网服务实例与 VSI 关联：以太网服务实例定义了一系列匹配规则，如匹配指定 VLAN 的报文、匹配接口接收到的所有报文等。从二层以太网接口上接收到的、与规则匹配的数据帧均属于指定的 VSI/VXLAN。
- 方式二：将 VLAN 与 VXLAN 关联：VTEP 接收到的该 VLAN 的数据帧均属于指定的 VXLAN。

只有为以太网服务实例配置了报文匹配方式并绑定了 VSI 实例，以太网服务实例的报文统计功能才会生效。如果在报文统计过程中修改报文匹配方式或绑定的 VSI 实例，则报文统计重新开始。

采用 VLAN 与 VXLAN 关联方式时，开启 VLAN 下对应 AC 的统计功能后，可以对该 VLAN 下自动生成的 AC 进行报文统计。在开启 VLAN 关联 VXLAN 功能，并在 VLAN 视图下配置与该 VLAN 关联的 VXLAN 后，如果存在属于该 VLAN 的接口，则自动在该接口上创建编号为当前 VLAN ID、匹配外层 VLAN tag 为当前 VLAN ID 的以太网服务实例，并将该以太网服务实例与指定 VXLAN 对应的 VSI 关联。

获取 AC 口的流量统计数据，即获取与 VSI 绑定的以太网服务实例的流量统计数据。

AC 对于二层广播报文入方向统计计数也会统计到出方向一份。

在某些情况，需要统计某一时段的 AC 流量统计数据，可以在用户视图通过 **reset l2vpn statistics ac** 命令清除接口原有报文统计信息，重新进行统计。

4.1.3 命令行方式实现

1. 配置需求

获取以太网服务实例 1000 流量统计数据。

2. 配置步骤

- 方式一：

以太网服务实例 1000 与接口 HundredGigE2/0/25 绑定，并在该实例下开启。

```
<Sysname> system-view
[Sysname] interface HundredGigE 2/0/25
[Sysname-HundredGigE2/0/25] service-instance 1000
[Sysname-HundredGigE2/0/25-srv1000] encapsulation s-vid 1000
[Sysname-HundredGigE2/0/25-srv1000] xconnect vsi aa
```

开启 VSI 的报文统计功能。

```
[Sysname-HundredGigE2/0/25-srv1000] statistics enable
[Sysname-HundredGigE2/0/25-srv1000] quit
```

- 方式二：

创建 VSI aa，并进入 VSI 视图。

```
<Sysname> system-view
[Sysname] vsi aa
```

创建 VXLAN，并进入 VXLAN 视图。

```
[Sysname-vsi-aa] vxlan 1000
[Sysname-vsi-aa] quit
```

开启 VLAN 关联 VXLAN 功能。

```
[Sysname] vxlan vlan-based
```

创建 VLAN 1000，并进入 VLAN 视图。

```
[Sysname] vlan 1000
```

配置 VLAN 与指定的 VXLAN 关联。

```
[Sysname-vlan1000] vxlan vni 1000
```

开启 VLAN 下对应 AC 的报文统计功能。

```
[Sysname-vlan1000] ac statistics enable
```

3. 查询流量统计数据示例

```
[Sysname]dis l2vpn service-instance verbose
Interface: HGE2/0/25
  Service Instance: 1000
    Type          : Manual
    Encapsulation : s-vid 10
    Bandwidth     : Unlimited
    VSI Name      : aa
    Link ID       : 0
    State         : Up
    Statistics    : Enabled
    Input Statistics:
      Octets   :1142929408
      Packets  :8929136
    Output Statistics:
      Octets   :0
      Packets  :9062436
```

表4-1 display l2vpn service-instance verbose 命令显示信息描述表

字段	描述
Interface	二层以太网接口或二层聚合接口
Service Instance	以太网服务实例ID
Type	以太网服务实例的类型和报文匹配方式，取值包括： • Dynamic (MAC-based)：动态创建，采用 MAC 地址匹配方式 • Dynamic (VLAN-based)：动态创建，采用 VLAN 匹配方式 • Manual：手工创建，采用 VLAN 匹配方式
Encapsulation	以太网服务实例的报文匹配规则，如果未配置报文匹配规则，则不显示本字段
Bandwidth	以太网服务实例对应AC上流量的最大带宽，单位为kbps 取值为“Unlimited”时，表示不限制AC上的流量
VSI Name	与以太网服务实例关联的VSI的名称
Link ID	以太网服务实例在VSI内的链路标识符
State	以太网服务实例的状态，取值包括Up和Down
DF state	接口的EVPN DF（Designated Forwarder）角色，取值包括： • BDF：在 EVPN 多归属组网中，该 AC 转发角色是 BDF （Backup DF） • DF：在 EVPN 多归属组网中，该 AC 转发角色是 DF 若接口未配置ESI（Ethernet Segment Identifier），则不显示该字段

字段	描述
Statistics	是否使能以太网服务实例的统计功能，取值包括： • Enabled：使能了以太网服务实例的统计功能 • Disabled：禁止以太网服务实例的统计功能
Input Statistics	入方向的以太网服务实例报文统计信息，包括入方向接收的字节数（Octets）、接收的报文数（Packets）
Output Statistics	出方向的以太网服务实例报文统计信息，包括出方向发送的字节数（Octets）、发送的报文数（Packets）

4.1.4 SNMP 方式实现

1. 配置需求

获取以太网服务实例 1000 流量统计数据。

2. 配置步骤

VXLAN 相关配置，请参见 4.1.3 2. 配置步骤。

配置 SNMP，请参见 3.1.3 2. 配置步骤。

3. 查询流量统计数据示例

说明

- 查询以太网服务实例流量统计数据前，我们需要获取接口的索引，然后通过接口索引来查询与接口关联的以太网服务实例的流量统计数据。
- 设备 IRF 成员编号不同时，接口索引值可能不同，具体以实际查询结果为准。
- 以下以通过 MIB Browser 查询 hh3cEvcSrvInstStatInfoEntry 表（OID 为 1.3.6.1.4.1.25506.2.106.1.4.1）获取与接口 HGE2/0/25 关联的以太网服务实例 1000 入方向包数统计数据为例。

如图 4-1 所示，通过 ifName 节点（1.3.6.1.2.1.31.1.1.1.1）查询 HGE2/0/25 口的索引。查询结果会显示在 query results 对话框中，如图 4-2 所示，接口 HGE2/0/25 索引为 220。

图4-1 查询接口索引

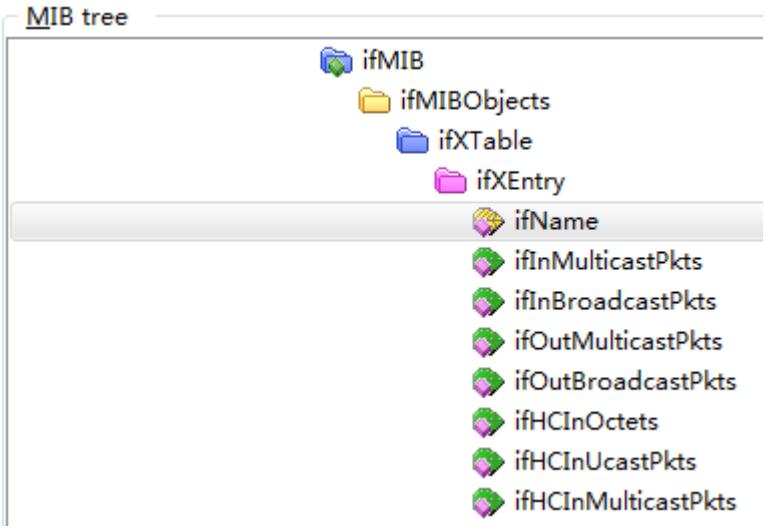


图4-2 索引查询结果

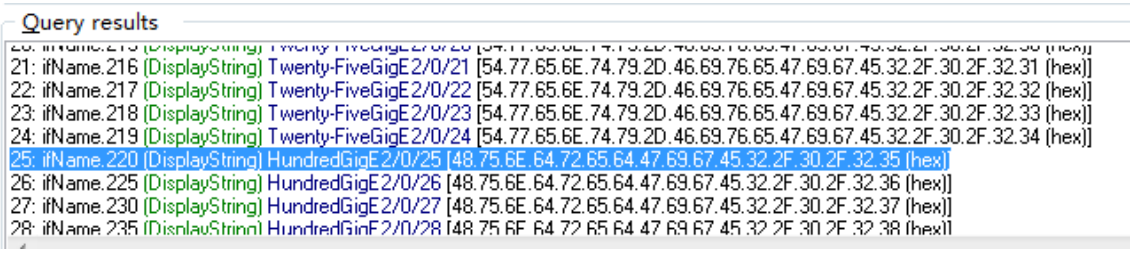
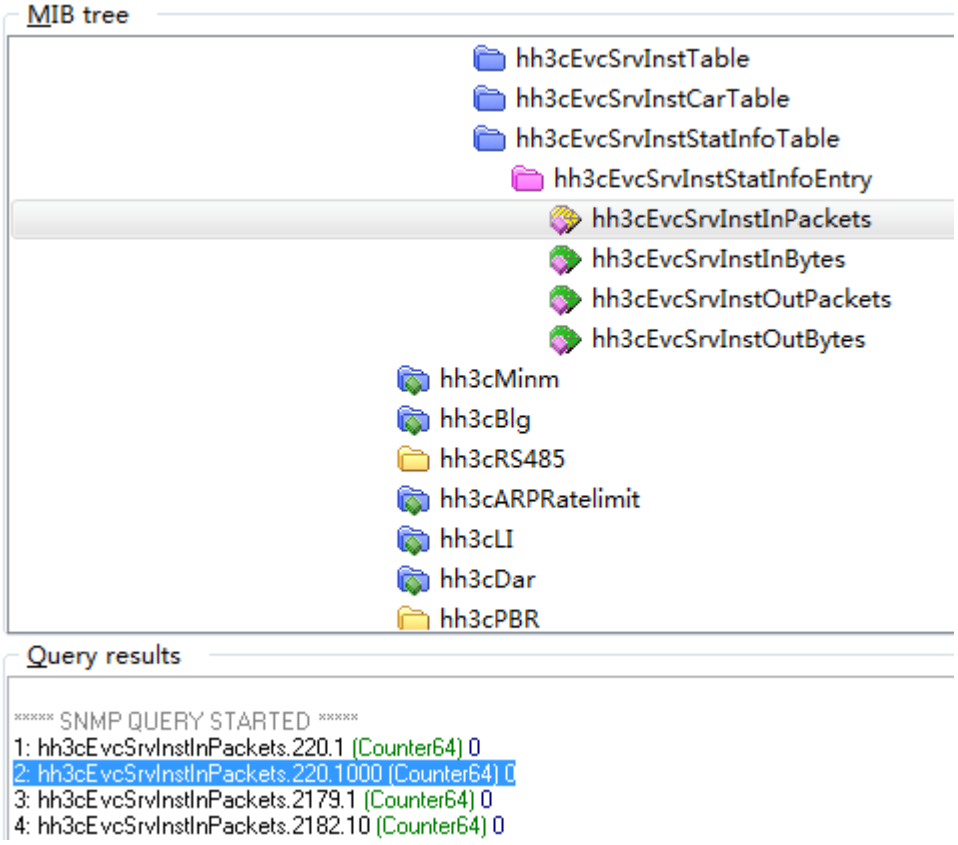


图 4-3 所示，通过 hh3cEvcSrvInstStatInfoEntry 节点子节点 hh3cEvcSrvInstInPackets（OID 为 1.3.6.1.4.1.25506.2.106.1.4.1.1），查询接口 HGE2/0/25 关联的以太网服务实例 1000 的入方向报文统计数据。

图4-3 查询以太网服务实例入方向包数统计数据



4. 更多信息

关于 SNMP 的更多配置，请参见对应产品的 SNMP 配置。

关于 MIB 文件的更多介绍，请参见对应产品的 MIB 参考。

4.1.5 NETCONF 方式实现

1. 配置需求

获取以太网服务实例 1000 流量统计数据。

2. 配置步骤

VXLAN 相关配置，请参见 4.1.3 2. 配置步骤。

NETCONF 配置，请参见 3.1.3 2. 配置步骤。

3. 查询流量统计数据示例

说明

- 用户可通过 L2VPN/VSIStatistics 表查询 VSI 口的流量统计数据，关于 L2VPN/VSIStatistics 表的更多介绍，请参见《NETCONF XML API 手册》。
- 以下以获取以太网服务实例 1000 为例。

请将以下报文拷贝、粘贴到 NETCONF 客户端。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
        <L2VPN>
          <ACs>
            <AC>
              <IfIndex></IfIndex>
              <SrvID>1000</SrvID>
              <VsiName></VsiName>
              <AccessMode></AccessMode>
              <Hub></Hub>
              <Statistics></Statistics>
              <Bandwidth></Bandwidth>
              <LearningMode></LearningMode>
              <InPkts></InPkts>
              <InOctets></InOctets>
              <OutPkts></OutPkts>
              <OutOctets></OutOctets>
              <Flooding></Flooding>
              <FloodType></FloodType>
              <ForwardingMode></ForwardingMode>
              <TrackEntryNumber></TrackEntryNumber>
              <InPktsRate></InPktsRate>
              <InOctetsRate></InOctetsRate>
              <OutPktsRate></OutPktsRate>
              <OutOctetsRate></OutOctetsRate>
              </AC>
          </ACs>
        </L2VPN>
      </top>
    </filter>
  </get>
</rpc>
```

如果客户端收到类似如下的报文，则表示操作成功。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data>
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
         <L2VPN>
            <ACs>
               <AC>
                  <IfIndex>49</IfIndex>
                  <SrvID>1000</SrvID>
                  <VsiName>aa</VsiName>
                  <AccessMode>1</AccessMode>
                  <Statistics>true</Statistics>
                  <Bandwidth>4294967295</Bandwidth>
```

```
                    <LearningMode>0</LearningMode>
                    <Flooding>true</Flooding>
                    <InPkts>12815354350</InPkts>
                    <InOctets>1640365356800</InOctets>
                    <OutPkts>12815447070</OutPkts>
                    <OutOctets>0</OutOctets>
                    <InPktsRate>8261191</InPktsRate>
                    <InOctetsRate>1057432529</InOctetsRate>
                    <OutPktsRate>8261223</OutPktsRate>
                    <OutOctetsRate>0</OutOctetsRate>
                  </AC>
                </ACs>
              </L2VPN>
            </top>
          </data>
</rpc-reply>
```

4.1.6 gRPC 方式实现

1. 配置需求

获取以太网服务实例 1000 流量统计数据。

2. 配置步骤

在开始下面的配置之前，请确保设备与采集器的 IP 地址都已配置完毕，并且它们之间路由可达。

开启 gRPC 功能。

```
<Sysname> system-view
[Sysname] grpc enable
```

创建传感器组 test，并添加采样路径为 L2VPN/VSIStatistics。

```
[Sysname] telemetry
[Sysname-telemetry] sensor-group test
[Sysname-telemetry-sensor-group-test] sensor path l2vpn/vsistatistics
[Sysname-telemetry-sensor-group-test] quit
```

创建目标组 collector1，并配置 IP 地址为 192.168.2.1、端口号为 50050 的采集器。

```
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] ipv4-address 192.168.2.1 port 50050
[Sysname-telemetry-destination-group-collector1] quit
```

创建订阅 A，配置关联传感器组为 test，数据采样和推送周期为 30 秒，关联目标组为 collector1。

```
[Sysname-telemetry] subscription A
[Sysname-telemetry-subscription-A] sensor-group test sample-interval 30
[Sysname-telemetry-subscription-A] destination-group collector1
[Sysname-telemetry-subscription-A] quit
```

3. 查询流量统计数据

采集器每 30 秒收到一次设备推送的数据信息。

4. 更多信息

关于 gRPC 配置的更多信息，请参见对应产品的“gRPC 配置”。

4.2 VSI流量统计功能

4.2.1 需求说明

获取 VSI 流量统计数据。

4.2.2 命令行方式实现

1. 配置需求

获取 vsi vpna 的流量统计数据。

2. 配置限制和指导

- 在 VSI 视图使能 **statistics enable** 使能 VSI 的报文数据统计能。配置完成后，可以通过 **display l2vpn vsi verbose** 查询统计结果。
- 当需要获取多次获取一定时间的流量统计数据时，可以在完成统计后，使用 **reset l2vpn statistics vsi** 命令清除 vsi 的报文统计数据进行重新统计。

3. 配置步骤

开启手工创建隧道接口的报文统计功能

```
<Sysname> system-view
[Sysname] vsi vpna
[Sysname-vsi-vsiaa] statistics enable
```

4. 查询流量统计数据示例

```
[Sysname]display l2vpn vsi verbose
VSI Name: vpna
  VSI Index               : 0
  VSI State               : Up
.........
  Statistics              : Enabled
  Input Statistics        :
    Octets   :6737029504
    Packets  :52633043
    Errors   :0
    Discards :0
  Output Statistics       :
    Octets   :9158149482
    Packets  :105266086
    Errors   :0
    Discards :0
.........
```

表4-2 display l2vpn vsi verbose 命令显示信息描述表

字段	描述
VSI Name	VSI名称
VSI Index	VSI索引

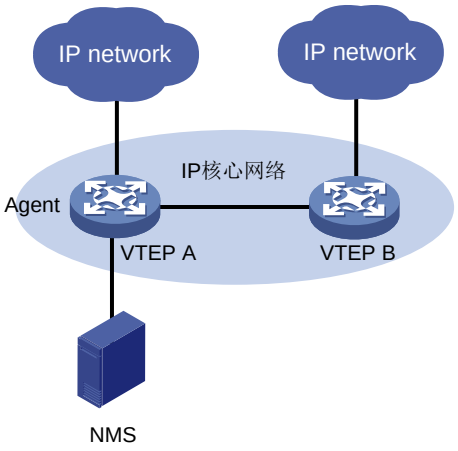
字段	描述
Statistics	是否使能VSI的统计功能，取值包括： • Enabled：使能了 VSI 的统计功能 • Disabled：禁止 VSI 的统计功能
Input statistics	入方向的VSI报文统计信息，包括入方向接收的字节数（Octets）、接收的报文数（Packets）、接收的错误报文数（Errors）和丢弃的报文数（Discards）
Output statistics	出方向的VSI报文统计信息，包括出方向发送的字节数（Octets）、发送的报文数（Packets）、错误报文数（Errors）和丢弃的报文数（Discards）

4.2.3 SNMP 方式实现

1. 配置需求

NMS 通过 SNMP 协议读取设备（Agent）的 vsi vpna 入方向以字节为单位的流量统计信息。

图4-4 SNMP 功能典型配置组网图



2. 配置步骤

参见 3.1.3 2. 配置步骤。

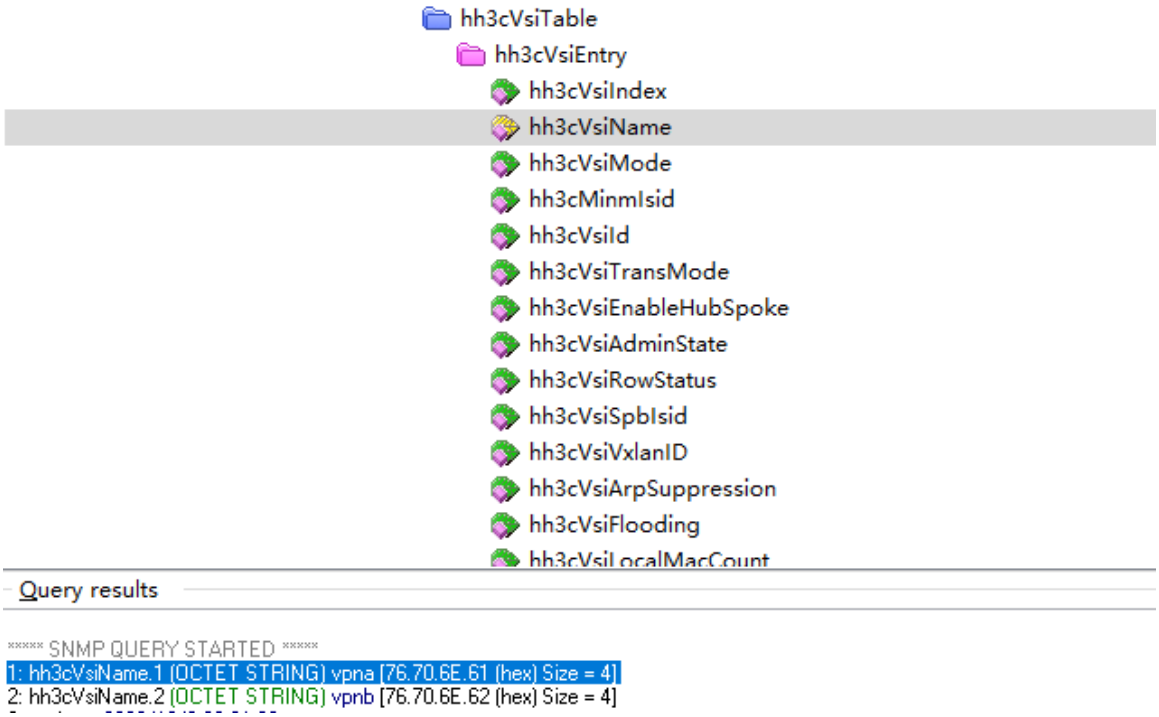
3. 查询流量统计数据示例

说明

- 查询 vsi 流量统计数据前，我们需要获取 vsi vpna 的索引，然后通过索引来查 vsi vpna 的流量统计数据。
- 用户可通过 hh3cVsiEntry（OID 为 1.3.6.1.4.1.25506.2.105.1.2.1）和 hh3cVsiPerfEntry（OID 为 1.3.6.1.4.1.25506.2.105.1.7.1）节点下子节点来获取 VSI 流量统计数据。
- 以下以通过 MIB Browser 查询 vsi vpna 入方向以字节为单位的流量统计数据为例。

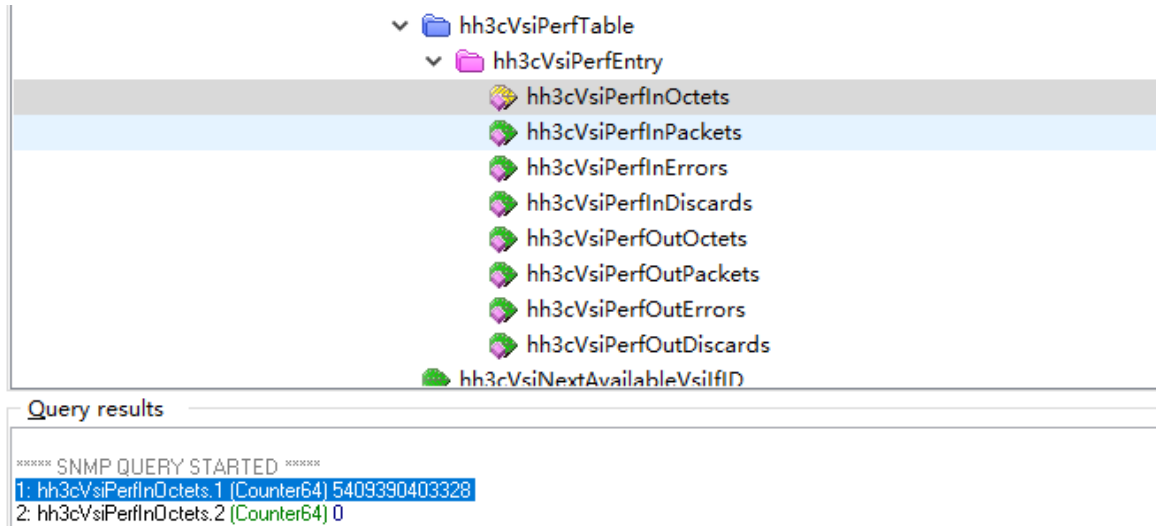
如图 4-5 所示，通过 hh3cVsiEntry（OID 为 1.3.6.1.4.1.25506.2.105.1.2.1）查询 vsi vpna 的索引。查询结果会显示在 query results 对话框中，vsi vpna 索引为 1。

图4-5 查询 VSI 索引



如图 4-6 所示，通过 hh3cVsiPerfEntry（OID 为 1.3.6.1.4.1.25506.2.105.1.7.1）节点查询索引值为 1 入方向以字节为单位的流量统计数据。查询结果会显示在 query results 对话框中。

图4-6 查询流量统计数据



4. 更多信息

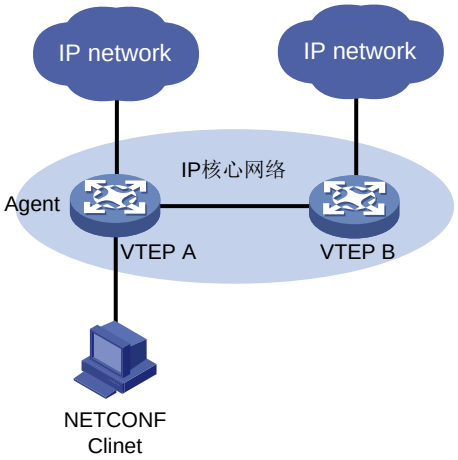
关于 SNMP 的更多配置，请参见对应产品的 SNMP 配置。

关于 MIB 文件的更多介绍，请参见对应产品的 MIB 参考。

4.2.4 NETCONF 方式实现

1. 配置需求

获取 vsi vpna 流量统计数据。



2. 配置步骤

设备侧配置与 3.1.3 2. 配置步骤相同。

3. 查询流量统计数据示例

说明

设备提供 L2VPN/VSIStatistics 表用于统计 VSI 流量数据。通过 L2VPN/VSIStatistics 表可查询接口以字节为单位和以包为单位的统计信息，包括入方向或出方向以字节\包为单位的统计数据，包括正常报文、错误报文、丢弃报文等。

以下使用 L2VPN/VSIStatistics 表查询 vsi vpna 流量统计数据为例。

请将以下报文拷贝、粘贴到 NETCONF 客户端。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
        <L2VPN>
          <VSIStatistics>
            <Statistics>
              <VsiName>vpna</VsiName>                  //VSI 名字
              <InPkts></InPkts>                        //入方向以包为单位的统计数据
              <InOctets></InOctets>                    //入方向以字节为单位的统计数据
              <InErrors></InErrors>                    //入方向以包为单位的错误报文统计数据
              <InDiscards></InDiscards>                //入方向丢包统计数据
              <OutPkts></OutPkts>                      //出方向以包为单位的统计数据
              <OutOctets></OutOctets>                  //出方向以字节为单位的统计数据
              <OutErrors></OutErrors>                  //出方向以包为单位的错误报文统计数据
```

```
              <OutDiscards></OutDiscards>          //出方向丢包统计数据
              <InPktsRate></InPktsRate>            //入方向报文速率（包）
                      <InOctetsRate></InOctetsRate>        //入方向报文速率（字节）
              <OutPktsRate></OutPktsRate>          //出方向报文速率（包）
              <OutOctetsRate></OutOctetsRate>      //出方向报文速率（字节）

            </Statistics>
          </VSIStatistics>
        </L2VPN>
   </top>
  </filter>
</get>
```

如果客户端收到类似如下的报文，则表示操作成功。

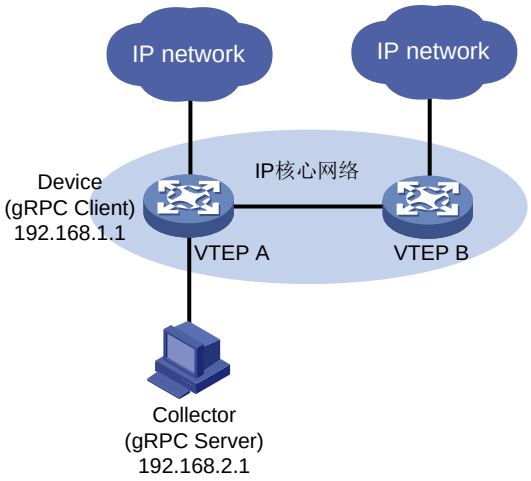
```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
         <data>
            <top xmlns="http://www.h3c.com/netconf/data:1.0">
               <L2VPN>
                  <VSIStatistics>
                     <Statistics>
                        <VsiName>vpna</VsiName>
                        <InPkts>45537431676</InPkts>
                        <InOctets>5828791254528</InOctets>
                        <InErrors>0</InErrors>
                        <InDiscards>0</InDiscards>
                        <OutPkts>91075403010</OutPkts>
                        <OutOctets>7923560061870</OutOctets>
                        <OutErrors>0</OutErrors>
                        <OutDiscards>0</OutDiscards>
                        <InPktsRate>8575395</InPktsRate>
                        <InOctetsRate>1097650645</InOctetsRate>
                        <OutPktsRate>17151031</OutPktsRate>
                        <OutOctetsRate>1492139697</OutOctetsRate>
                        <AcInPkts>0</AcInPkts>
                        <AcInOctets>0</AcInOctets>
                        <AcOutPkts>0</AcOutPkts>
                        <AcOutOctets>0</AcOutOctets>
                        <AcInPktsRate>0</AcInPktsRate>
                        <AcInOctetsRate>0</AcInOctetsRate>
                        <AcOutPktsRate>0</AcOutPktsRate>
                        <AcOutOctetsRate>0</AcOutOctetsRate>
                     </Statistics>
                  </VSIStatistics>
               </L2VPN>
            </top>
         </data>
      </rpc-reply>
      </top>
    </filter>
```

```
  </get>
</rpc>
```

4.2.5 gRPC 方式实现

1. 配置需求

获取 vsi vpna 流量统计数据。



2. 配置步骤

在开始下面的配置之前，请确保设备与采集器的 IP 地址都已配置完毕，并且它们之间路由可达。

开启 gRPC 功能。

```
<Sysname> system-view
[Sysname] grpc enable
```

创建传感器组 test，并添加采样路径为 l2vpn/vsistatistics。

说明

配置采样路径为 l2vpn/vsistatistics，设备会收集设备所有接口的流量统计数据，并将数据上传给采集器。

```
[Sysname] telemetry
[Sysname-telemetry] sensor-group test
[Sysname-telemetry-sensor-group-test] sensor path l2vpn/vsistatistics
[Sysname-telemetry-sensor-group-test] quit
```

创建目标组 collector1，并配置 IP 地址为 192.168.2.1、端口号为 50050 的采集器。

```
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] ipv4-address 192.168.2.1 port 50050
[Sysname-telemetry-destination-group-collector1] quit
```

创建订阅 A，配置关联传感器组为 test，数据采样和推送周期为 30 秒，关联目标组为 collector1。

```
[Sysname-telemetry] subscription A
[Sysname-telemetry-subscription-A] sensor-group test sample-interval 30
[Sysname-telemetry-subscription-A] destination-group collector1
```

```
[Sysname-telemetry-subscription-A] quit
```

3. 查询流量统计数据

采集器每 30 秒收到一次设备推送的数据信息。

4. 更多信息

关于 gRPC 配置的更多信息，请参见对应产品的“gRPC 配置”。

4.3 getgetAC流量统计（基于MQC实现）

4.3.1 需求说明

通过 MQC 获取 AC 流量统计数据。

说明

通过 MQC 获取 AC 流量前，需要在流行为中匹配指定 VLXAN 隧道的规则，并将引用该流行为的 QoS 策略应用在该 VXLAN 隧道出接口对应二层以太网接口上。

4.3.2 命令行方式实现

1. 配置需求

通过 MQC 获取进入接口 HundredGigE1/0/30 的 VXLAN 流量统计数据。

2. 配置限制和指导

设备支持通过 **accounting [byte | packet]*** 命令配置以包和字节为单位的流量统计动作。当设备支持同时按两种方式进行统计，**byte** 和 **packet** 为可选参数，也可以两种统计方式同时指定。如果未指定 **byte** 和 **packet**，设备将以包为单位进行报文统计；如果同时指定了 **byte** 和 **packet**，设备将以包和字节为单位进行报文统计。以下以包为单位进行流量统计。

3. 配置步骤

说明

如果站点间是二层互联，需要匹配内层 mac，如果是三层互联，需要匹配内层 IP。

- 二层互联：

  # 创建二层 ACL 4000，并配置 rule 0 匹配源 MAC 为 0000-0000-0001、目的 MAC 为 0000-0000-0006 的 VXLAN 报文。

  ```
  <Sysname> system-view
  [Sysname] acl mac 4000
  [Sysname-acl-ipv4-adv-4000] rule 0 permit vxlan inner-source-mac 0000-0000-0001
  ffff-ffff-ffff inner-dest-mac 0000-0000-0006 ffff-ffff-ffff
  [Sysname-acl-ipv4-adv-4000] quit
  ```

  # 创建流分类 aa，定义匹配接口所有流量规则。

  ```
  [Sysname] traffic classifier aa
  ```

```
[Sysname-classifier-aa] if-match acl 4000
[Sysname-classifier-aa] quit
```

- 三层互联

  # 创建高级 ACL 3000，并配置 rule 0 匹配 VXLAN ID 为 1、源 IP 为 100.0.0.1、目的 IP 为 101.0.0.1 的 VXLAN 报文。

```
<Sysname> system-view
[Sysname] acl advance 3000
[Sysname-acl-ipv4-adv-3000] rule 0 permit vxlan vxlan-id 1 inner-protocol ip
inner-source 100.0.0.1 0 inner-destination 101.0.0.1 0
[Sysname-acl-ipv4-adv-3000] quit
```

  # 创建流分类 aa，定义匹配接口所有流量规则。

```
[Sysname] traffic classifier aa
[Sysname-classifier-aa] if-match acl 3000
[Sysname-classifier-aa] quit
```

创建流行为 aa，为流行为配置以包为单位进行流量统计动作。

```
[Sysname]traffic behavior aa
[Sysname-behavior-aa] accounting packet
[Sysname-behavior-aa] quit
```

创建 QoS 策略，为流分类 aa 指定流行为 aa。

```
[Sysname]qos policy aa
[Sysname-qospolicy-aa] classifier aa behavior aa
[Sysname-qospolicy-aa] quit
```

将 QoS 策略应用在接口 HundredGigE1/0/30 的入方向。

```
[Sysname] interface hundredgige 1/0/30
[Sysname-HundredGigE1/0/30] qos apply policy aa inbound
[Sysname-HundredGigE1/0/30] quit
```

4. 查询流量统计数据

- # 查询进入接口 HundredGigE1/0/30 的 VXLAN 流量统计数据（二层互联）。

```
[Sysname]display qos policy interface HundredGigE 1/0/30
Interface: HundredGigE1/0/30
  Direction: inbound
  Policy: aa
   Classifier: aa
     Operator: AND
     Rule(s) :
      If-match acl 4000
     Behavior: aa
      Accounting enable:
        98928876 (Packets)
```

- # 查询进入接口 HundredGigE1/0/30 的 VXLAN 流量统计数据（三层互联）。

```
[Sysname]display qos policy interface HundredGigE 1/0/30
Interface: HundredGigE1/0/30
  Direction: inbound
  Policy: aa
   Classifier: aa
     Operator: AND
```

```
    Rule(s) :
     If-match acl 3000
    Behavior: aa
      Accounting enable:
        98928876 (Packets)
```

表4-3 display qos policy interface 命令显示信息描述表

字段	描述
Direction	QoS策略应用的方向
policy	QoS策略名
Classifier	类的名称及其内容，内容可以有多种类型
Operator	分类规则之间的逻辑关系
Rule(s)	分类规则
if-match acl 3000	匹配经过接口的符合ACL 3000规则的报文
Behavior	行为的名称及其内容
Accounting enable	流量统计动作

5. 更多信息

关于 MQC 配置的更多信息，请参见对应产品的“QoS 配置”和“QoS 命令”。

4.3.3 SNMP 方式实现

1. 配置需求

NMS 通过 SNMP 协议进入接口 HundredGigE1/0/30 的 VXLAN 流量统计信息。

2. 配置步骤

配置 MQC 获取进入接口 HundredGigE1/0/30 的 VXLAN 流量统计数据，请参见 4.3.2 3. 配置步骤。

配置 SNMP，请参见 3.1.3 2. 配置步骤。

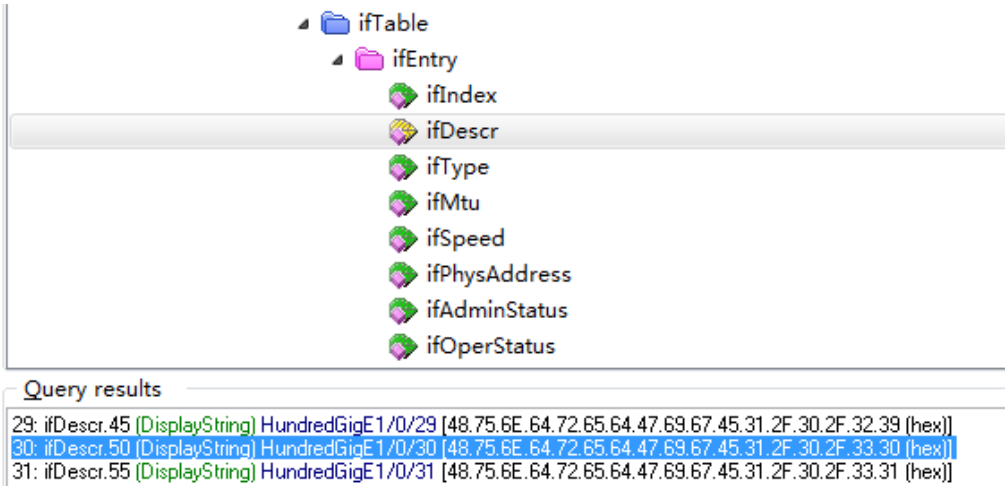
3. 查询流量统计数据示例

说明

- 本举例以通过 MIB Browser 查询 Agen 获取进入接口 HundredGigE1/0/30 的 VXLAN 流量统计为例。
- 查询进入接口 HundredGigE1/0/30 的 VXLAN 流量统计时，我们需要通过 hh3cCBQoSIntApplyObjectIndex 表（OID 为 1.3.6.1.4.1.25506.2.65.2.1.5.5.2.1.2）获取应用在指定接口上 QoS 策略目标的索引，然后使用索引在 hh3cCBQoSAccountingRunInfoEntry 表（OID 为 1.3.6.1.4.1.25506.2.65.2.1.5.6.8.1）的子表中查找指定 VXLAN 隧道出反向的流量统计数据。

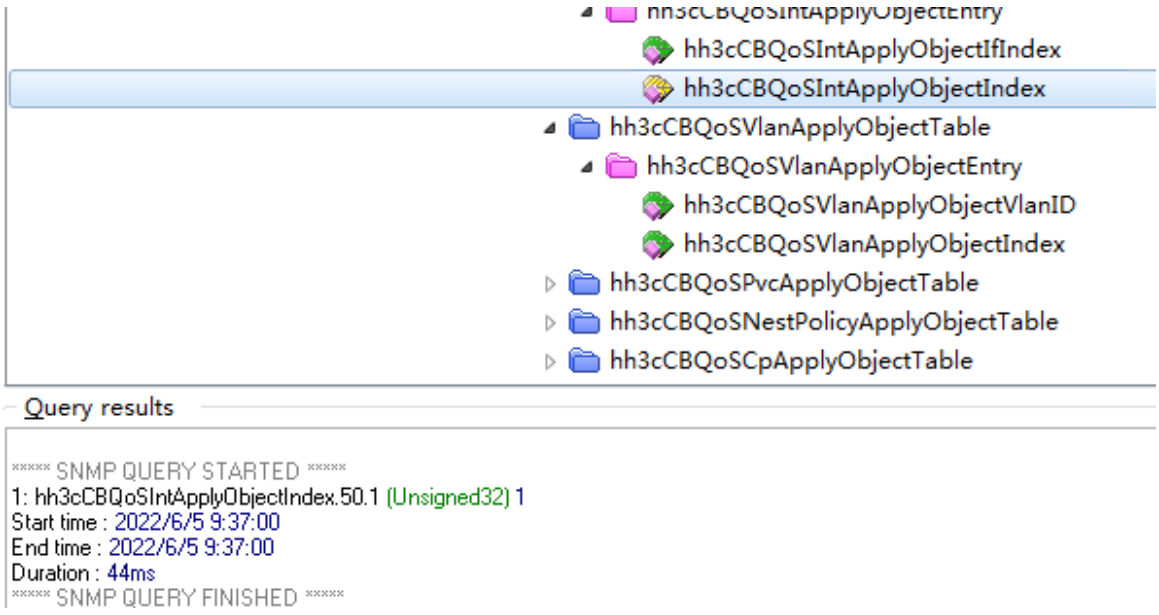
如图 4-7 所示，通过 ifName 节点（1.3.6.1.2.1.31.1.1.1.1）的子节点 ifDescr（1.3.6.1.2.1.31.1.1.1.1.2）查询 HGE1/0/30 接口的索引。查询结果会显示在 Query results 对话框中，HGE1/0/30 口索引为 50。

图4-7 查询接口索引



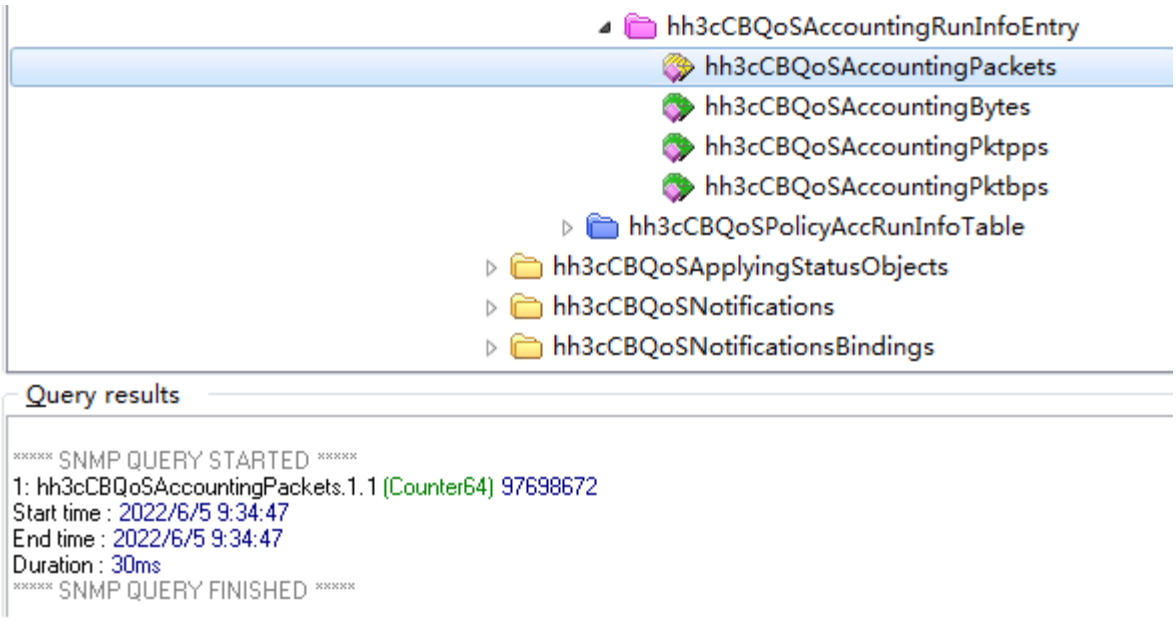
通过接口索引在 hh3cCBQoSIntApplyObjectIndex 表（ODI 为 1.3.6.1.4.1.25506.2.65.2.1.5.5.2.1.2）查询应用在接口 QoS 策略的索引。如图 4-8 所示，查询应用在接口 HundredGigE1/0/30 的 QoS 策略索引为 1。

图4-8 查询应用在接口 QoS 策略索引



如图 4-9 所示，通过 hh3cCBQoSAccountingRunInfoEntry 表（OID 为 1.3.6.1.4.1.25506.2.65.2.1.5.6.8.1）查询进入接口 HundredGigE1/0/30 的 VXLAN 流量统计数据。

图4-9 查询流量统计数据



4. 更多信息

关于 SNMP 的更多配置，请参见对应产品的 SNMP 配置。

关于 MIB 文件的更多介绍，请参见对应产品的 MIB 参考。

4.3.4 NETCONF 实现

1. 配置需求

在主机上安装 NETCONF 客户端软件，通过 NETCONF 读取进入接口 HundredGigE1/0/30 的 VXLAN 流量统计信息。

说明

NETCONF 客户端是通过 Device 设备提供的 NETCONF XML API 获取的接口流量统计信息。

2. 配置步骤

配置 MQC 获取进入接口 HundredGigE1/0/30 的 VXLAN 流量统计数据，请参见 4.3.2 3. 配置步骤。

配置 NETCONF，请参见 3.1.3 2. 配置步骤相同。

3. 查询流量统计数据示例

说明

设备提供 MQC/IfPolicyAccount 表用于统计 VXLAN 流量数据。通过 MQC/IfPolicyAccount 表可查询以字节为单位和以包为单位的统计信息

以下使用 MQC/AccountRunInfo 表查询接口 HundredGigE1/0/30 统计信息为例。

在设备 Probe 视图使用 **display system internal ifmgr list | include HundredGigE**1/0/30 命令查询接口 HundredGigE1/0/30 的索引。

```
<Sysname> system-view
[Sysname] probe
[Sysname-probe]display system internal ifmgr list | include HundredGigE1/0/30
        HundredGigE1/0/30(index:50)
```

请将以下报文拷贝、粘贴到 NETCONF 客户端。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
        <MQC>
          <IfPolicyAccount>
            <Interface>
              <IfIndex>50</IfIndex>            //接口索引
              <Direction></Direction>          //QoS 策略应用方向
              <ClassName></ClassName>          //流分类名字
              <Packets></Packets>              //以包为单位的流量统计数据
              <Bytes></Bytes>                  //以字节为单位的流量统计数据
              <pps></pps>                      //每秒以包为单位的流量统计数据
              <bps></bps>                      //每秒以字节为单位的流量统计数据
            </Interface>
          </IfPolicyAccount>
        </MQC>
      </top>
    </filter>
  </get>
</rpc>
```

如果客户端收到类似如下的报文，则表示操作成功。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<data>
   <top xmlns="http://www.h3c.com/netconf/data:1.0">
      <MQC>
         <IfPolicyAccount>
            <Interface>
               <IfIndex>50</IfIndex>
               <Direction>0</Direction>
               <ClassName>aa</ClassName>
               <Packets>98928876</Packets>
               <pps>0</pps>
            </Interface>
         </IfPolicyAccount>
      </MQC>   </top>
   </data>
</rpc-reply>
```

4. 更多信息

关于 NETCONF 配置的更多信息，请参见对应产品的“NETCONF 配置”。

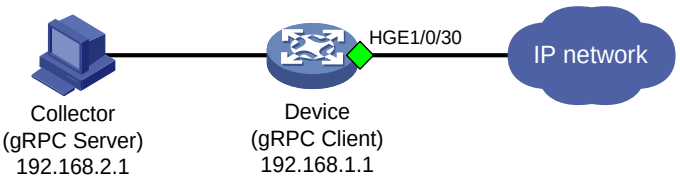
关于 MQC/IfPolicyAccount 的更多信息，请参见《H3C Comware 7 NETCONF XML API Reference 》。

4.4 gRPC方式实现

4.4.1 配置需求

采集器通过 gRPC 协议读取设备（Device）进入接口 HundredGigE1/0/30 的 VXLAN 流量统计信息。

图4-10 gRPC 功能典型配置组网图



4.4.2 配置步骤

在开始下面的配置之前，请确保设备与采集器的 IP 地址都已配置完毕，并且它们之间路由可达。

开启 gRPC 功能。

```
<Sysname> system-view
[Sysname] grpc enable
```

创建传感器组 test，并添加采样路径为 MQC/IfPolicyAccount。

说明

配置采样路径为 MQC/IfPolicyAccount，设备会收集设备所有接口通过 MQC 统计的流量数据，并将数据上传给采集器。

```
[Sysname] telemetry
[Sysname-telemetry] sensor-group test
[Sysname-telemetry-sensor-group-test] sensor path mqc/ifpolicyaccount
[Sysname-telemetry-sensor-group-test] quit
```

创建目标组 collector1，并配置 IP 地址为 192.168.2.1、端口号为 50050 的采集器。

```
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] ipv4-address 192.168.2.1 port 50050
[Sysname-telemetry-destination-group-collector1] quit
```

创建订阅 A，配置关联传感器组为 test，数据采样和推送周期为 30 秒，关联目标组为 collector1。

```
[Sysname-telemetry] subscription A
[Sysname-telemetry-subscription-A] sensor-group test sample-interval 30
[Sysname-telemetry-subscription-A] destination-group collector1
[Sysname-telemetry-subscription-A] quit
```

4.4.3 查询流量统计数据

采集器每 30 秒收到一次设备推送的数据信息。

4.4.4 更多信息

关于 gRPC 配置的更多信息，请参见对应产品的“gRPC 配置”。

5 VLAN 流量统计实现

5.1 需求说明

通过 MQC 方式获取 VLAN 流量统计数据。

5.2 命令行方式实现

5.2.1 配置需求

通过 MQC 获取 VLAN 2 入方向和出方向流量统计数据。

5.2.2 配置限制和指导

设备支持通过 **accounting [byte | packet]*** 命令配置以包和字节为单位的流量统计动作。byte 和 packet 不能同时配置。

5.2.3 配置步骤

创建流分类 aa，定义匹配接口所有流量规则。

```
<Sysname> system-view
[Sysname] traffic classifier aa
[Sysname-classifier-aa] if-match any
[Sysname-classifier-aa] quit
```

创建流行为 aa，为流行为配置以包为单位进行流量统计动作。

```
[Sysname]traffic behavior aa
[Sysname-behavior-aa] accounting packet
[Sysname-behavior-aa] quit
```

创建 QoS 策略，为流分类 aa 指定流行为 aa。

```
[Sysname]qos policy aa
[Sysname-qospolicy-aa] classifier aa behavior aa
[Sysname-qospolicy-aa] quit
```

将 QoS 策略应用在 VLAN 的入方向和出方向。

```
[Sysname] qos vlan-policy aa vlan 2 inbound
[Sysname] qos vlan-policy aa vlan 2 outbound
```

5.2.4 查询流量统计数据

查询 VLAN 2 的流量统计数据。

```
[Sysname] dis qos vlan-policy vlan 20
Vlan 2
```

```
  Direction: Inbound
  Policy: test
   Classifier: test
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: test
      Accounting enable:
        1193773738 (Packets)
Vlan 2
  Direction: Outbound
  Policy: test
   Classifier: test
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: test
      Accounting enable:
        250116562 (Packets)
```

表5-1 display qos policy interface 命令显示信息描述表

字段	描述
Direction	QoS策略应用的方向
policy	QoS策略名
Classifier	类的名称及其内容，内容可以有多种类型
Operator	分类规则之间的逻辑关系
Rule(s)	分类规则
if-match any	匹配经过接口的所有报文
Behavior	行为的名称及其内容
Accounting enable	流量统计动作

5.2.5 更多信息

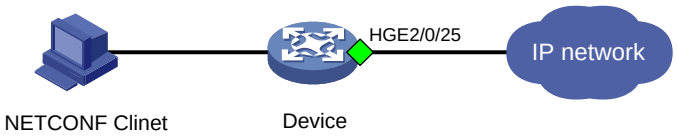
关于 MQC 配置的更多信息，请参见对应产品的“QoS 配置”和“QoS 命令”。

5.3 SNMP方式实现

5.3.1 配置需求

NMS 通过 SNMP 协议读取 VLAN 2 接收的流量统计信息。

图5-1 SNMP 功能典型配置组网图



5.3.2 配置步骤

配置 MQC 获取 VLAN 流量统计数据，请参见 5.2.3 配置步骤。

配置 SNMP，请参见 3.1.3 2. 配置步骤。

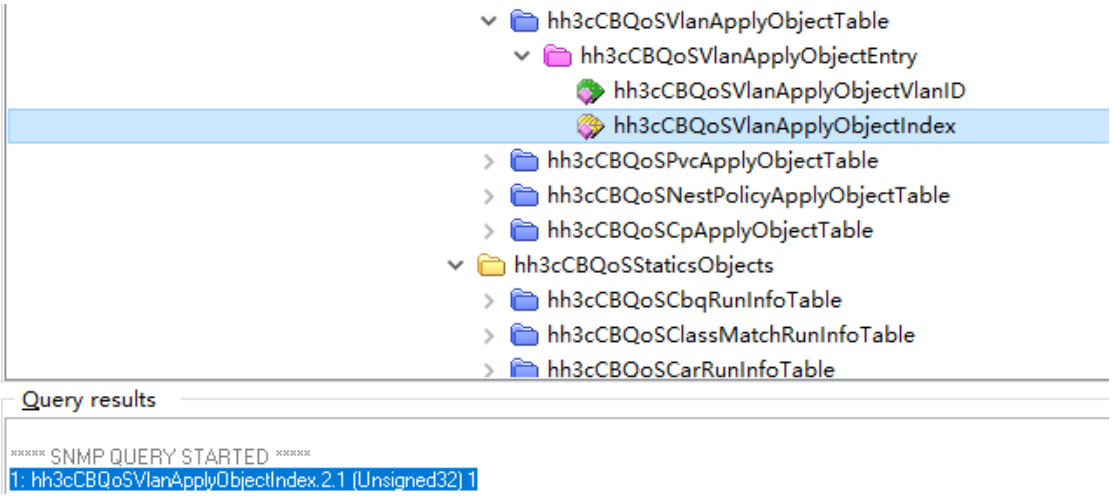
5.3.3 查询流量统计数据示例

说明

- 本举例以通过 MIB Browser 查询 tunnel0 入方向的流量统计数据为例。
- 假设已在设备上配置好 QoS 策略，并应用在 VLAN2 的入方向。
- 查询 VLAN 流量统计数据时，我们需要通过 hh3cCBQoSVlanApplyObjectIndex 表（OID 为 1.3.6.1.4.1.25506.2.65.2.1.5.5.3.1.2）获取应用在指定 VLAN 上 QoS 策略目标的索引，然后使用索引在 hh3cCBQoSAccountingRunInfoEntry 表（OID 为 1.3.6.1.4.1.25506.2.65.2.1.5.6.8.1）的子表中查找指定 VLAN 的流量统计数据。

通过 hh3cCBQoSVlanApplyObjectIndex 表（OID 为 1.3.6.1.4.1.25506.2.65.2.1.5.5.3.1.2）获取应用在 VLAN 2 上 QoS 策略对象的索引。查询结果会显示在 query results 对话框中，如图 5-2 所示，应用在 VLAN 2 上 QoS 策略对象的索引为 1。

图5-2 查询接口索引

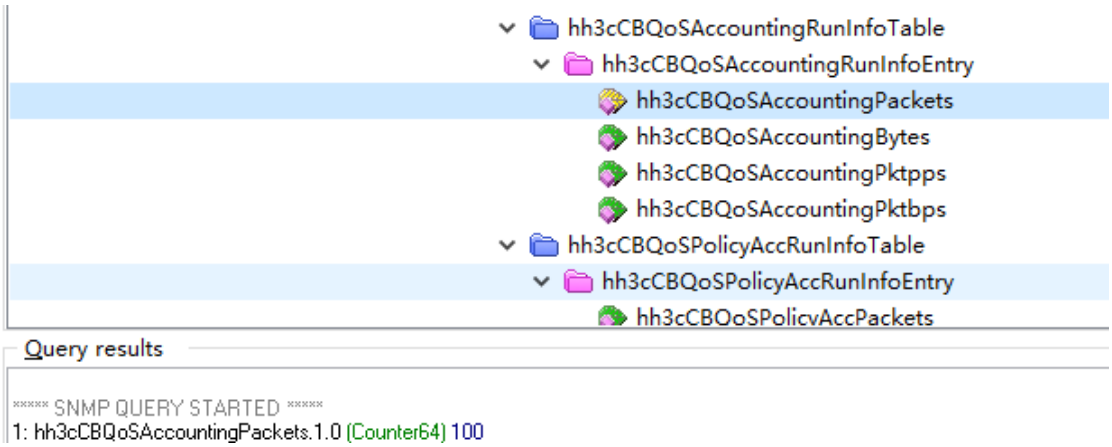


说明

图 5-2 中，hh3cCBQoSVlanApplyObjectIndex 表查询的结果中，2.1 表示 QoS 策略应用在了 VLAN 2 的入方向，1 为应用在 VLAN 2 上 QoS 策略对象的索引值。

在 hh3cCBQoSAccountingRunInfoEntry 表（OID 为 1.3.6.1.4.1.25506.2.65.2.1.5.6.8.1）的子表中使用上一步查询出的索引值查找 VLAN 2 的流量统计数据。如图 5-3 所示，查询以包为单位的统计数据，Query results 对话框中显示 VLAN 2 入方向统计了 100 个包。

图5-3 查询流量统计数据



5.3.4 更多信息

关于 SNMP 的更多配置，请参见对应产品的 SNMP 配置。

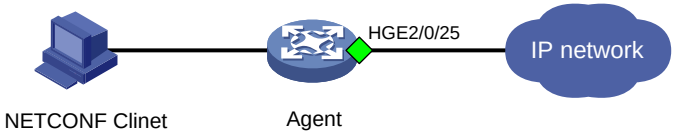
关于 MIB 文件的更多介绍，请参见对应产品的 MIB 参考。

5.4 NETCONF实现

5.4.1 配置需求

在主机上安装 NETCONF 客户端软件，通过 NETCONF 读取设备（Agent）的 VLAN 2 的流量统计信息。

图5-4 SNMP 功能典型配置组网图



说明

NETCONF 客户端是通过 Device 设备提供的 NETCONF XML API 获取的接口流量统计信息。

5.4.2 配置步骤

配置 MQC 获取 VLAN 流量统计数据，请参见 5.2.3 配置步骤。

配置 NETCONF，请参见 3.1.3 2. 配置步骤。

5.4.3 查询流量统计数据示例

说明

设备提供 MQC/VLANPolicyAccount 表用于统计 VLAN 流量数据。通过 MQC/VLANPolicyAccount 表可查询以字节为单位和以包为单位的统计信息。

以下使用 MQC/AccountRunInfo 表查询 VLAN 2 流量统计信息为例。

请将以下报文拷贝、粘贴到 NETCONF 客户端。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
        <MQC>
          <VLANPolicyAccount>
            <VLAN>
              <VLANID>2</VLANID>
              <Direction></Direction>
              <ClassName></ClassName>
              <Packets></Packets>
              <Bytes></Bytes>
              <pps></pps>
              <bps></bps>
            </VLAN>
          </VLANPolicyAccount>
        </MQC>
      </top>
    </filter>
  </get>
</rpc>
```

如果客户端收到类似如下的报文，则表示操作成功。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<data>
   <top xmlns="http://www.h3c.com/netconf/data:1.0">
      <MQC>
```

```
            <VLANPolicyAccount>
               <VLAN>
                    <VLANID>2</VLANID>                  //VLAN ID
                    <Direction>0</Direction>            //0 代表入方向，1 代表出方向
                    <ClassName>test</ClassName>         //流分类名
                    <Packets>52133621124</Packets>      //以包为单位的统计数据
                    <Bytes></Bytes>                     //以字节为单位的统计数据
                    <pps>12668937</pps>                 //每秒钟统计的包书
                    <bps></bps>                         //每秒钟统计的字节数
                    </VLAN>
            </VLANPolicyAccount>
         /MQC>
      </top>
      </data>
</rpc-reply>
```

5.4.4 更多信息

关于 NETCONF 配置的更多信息，请参见对应产品的“NETCONF 配置”。

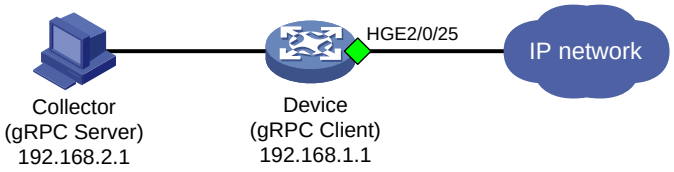
关于 MQC/AccountRunInfo 的更多信息，请参见《H3C Comware 7 NETCONF XML API Reference》。

5.5 gRPC方式实现

5.5.1 配置需求

采集器通过 gRPC 协议读取设备（Device）的 VLAN 2 流量统计信息。

图5-5 gRPC 功能典型配置组网图



5.5.2 配置步骤

在开始下面的配置之前，请确保设备与采集器的 IP 地址都已配置完毕，并且它们之间路由可达。

配置 MQC 获取 VLAN 流量统计数据，请参见 5.2.3 配置步骤。

开启 gRPC 功能。

```
<Sysname> system-view
[Sysname] grpc enable
```

创建传感器组 test，并添加采样路径为 MQC/VLANPolicyAccount。

说明

配置采样路径为 MQC/VLANPolicyAccount，设备会收集所有应用了 QoS 策略的 VLAN 的流量统计数据，并将数据上传给采集器。

```
[Sysname] telemetry
[Sysname-telemetry] sensor-group test
[Sysname-telemetry-sensor-group-test] sensor path mqc/vlanpolicyaccount
[Sysname-telemetry-sensor-group-test] quit
```

创建目标组 collector1，并配置 IP 地址为 192.168.2.1、端口号为 50050 的采集器。

```
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] ipv4-address 192.168.2.1 port 50050
[Sysname-telemetry-destination-group-collector1] quit
```

创建订阅 A，配置关联传感器组为 test，数据采样和推送周期为 30 秒，关联目标组为 collector1。

```
[Sysname-telemetry] subscription A
[Sysname-telemetry-subscription-A] sensor-group test sample-interval 30
[Sysname-telemetry-subscription-A] destination-group collector1
[Sysname-telemetry-subscription-A] quit
```

5.5.3 查询流量统计数据

采集器每 30 秒收到一次设备推送的数据信息。

5.5.4 更多信息

关于 gRPC 配置的更多信息，请参见对应产品的“gRPC 配置”。

6 VPN 实例流量统计实现

6.1 需求说明

通过 MQC 获取指定 VPN 实例流量统计数据。

说明

- 通过 MQC 获取 VPN 流量前，需要在流行为中匹配指定 VPN 的规则，并将引用该流行为的 QoS 策略应用在与 VPN 关联的接口上。设备支持命令行、SNMP、NETCONF 和 gRPC 四种方式查询 MQC 流量统计数据。

6.2 命令行方式实现

6.2.1 配置需求

通过 MQC 获取 VPN vpn1 入方向流量统计数据。

6.2.2 配置限制和指导

设备支持通过 **accounting [byte | packet]*** 命令配置以包和字节为单位的流量统计动作。当设备支持同时按两种方式进行统计，**byte** 和 **packet** 为可选参数，也可以两种统计方式同时指定。如果未指定 **byte** 和 **packet**，设备将以包为单位进行报文统计；如果同时指定了 **byte** 和 **packet**，设备将以包和字节为单位进行报文统计。以下以包为单位进行流量统计。

6.2.3 配置步骤

创建高级 ACL 3000，并配置 rule 0 匹配 VPN vpn1 入方向 IP 报文。

```
<Sysname> system-view
[Sysname] acl advance 3000
[Sysname-acl-ipv4-adv-3000] rule 0 permit ip vpn-instance vpn1
[Sysname-acl-ipv4-adv-3000] quit
```

创建流分类 aa，定义匹配接口所有流量规则。

```
[Sysname] traffic classifier aa
[Sysname-classifier-aa] if-match any
[Sysname-classifier-aa] quit
```

创建流行为 aa，为流行为配置以包为单位进行流量统计动作。

```
[Sysname]traffic behavior aa
[Sysname-behavior-aa] accounting packet
[Sysname-behavior-aa] quit
```

创建 QoS 策略，为流分类 aa 指定流行为 aa。

```
[Sysname]qos policy aa
[Sysname-qospolicy-aa] classifier aa behavior aa
[Sysname-qospolicy-aa] quit
```

将 QoS 策略应用在接口 HundredGigE1/0/30 的入方向。

```
[Sysname] interface hundredgige 1/0/30
[Sysname-HundredGigE1/0/30] qos apply policy aa inbound
[Sysname-HundredGigE1/0/30] quit
```

6.2.4 查询流量统计数据

查询接口 HundredGigE1/0/30 的流量统计数据。

```
[Sysname]display qos policy interface HundredGigE 1/0/30
Interface: HundredGigE1/0/30
  Direction: Inbound
  Policy: aa
   Classifier: aa
     Operator: AND
```

```
    Rule(s) :
     If-match acl 3000
    Behavior: aa
     Accounting enable:
       98928876 (Packets)
```

表6-1 display qos policy interface 命令显示信息描述表

字段	描述
Direction	QoS策略应用的方向
policy	QoS策略名
Classifier	类的名称及其内容，内容可以有多种类型
Operator	分类规则之间的逻辑关系
Rule(s)	分类规则
if-match acl 3000	匹配经过接口的符合ACL 3000规则的报文
Behavior	行为的名称及其内容
Accounting enable	流量统计动作

6.2.5 更多信息

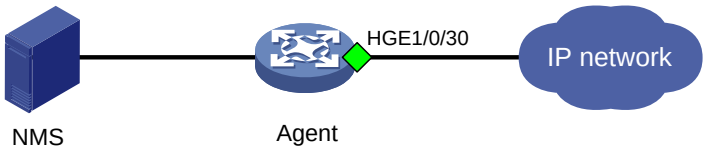
关于 MQC 配置的更多信息，请参见对应产品的“QoS 配置”和“QoS 命令”。

6.3 SNMP方式实现

6.3.1 配置需求

NMS 通过 SNMP 协议读取 VPN vpn1 入方向流量统计信息。

图6-1 SNMP 功能典型配置组网图



6.3.2 配置步骤

配置 MQC 获取 VPN vpn1 入方向流量统计数据，请参见 6.2.3 配置步骤。

配置 SNMP，请参见 3.1.3 2. 配置步骤。

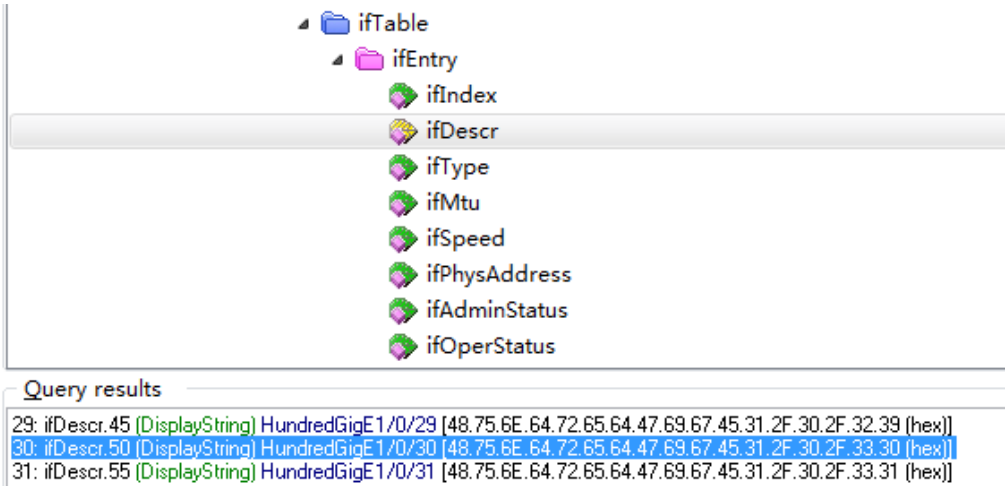
6.3.3 查询流量统计数据示例

说明

- 本举例以通过 MIB Browser 查询 VPN vpn1 入方向的流量统计数据为例。
- 查询 VLAN 流量统计数据时，我们需要通过 hh3cCBQoSIntApplyObjectIndex 表（OID 为 1.3.6.1.4.1.25506.2.65.2.1.5.5.2.1.2）获取应用在指定接口上 QoS 策略目标的索引，然后使用索引在 hh3cCBQoSAccountingRunInfoEntry 表（OID 为 1.3.6.1.4.1.25506.2.65.2.1.5.6.8.1）的子表中查找指定 VPN 的流量统计数据。

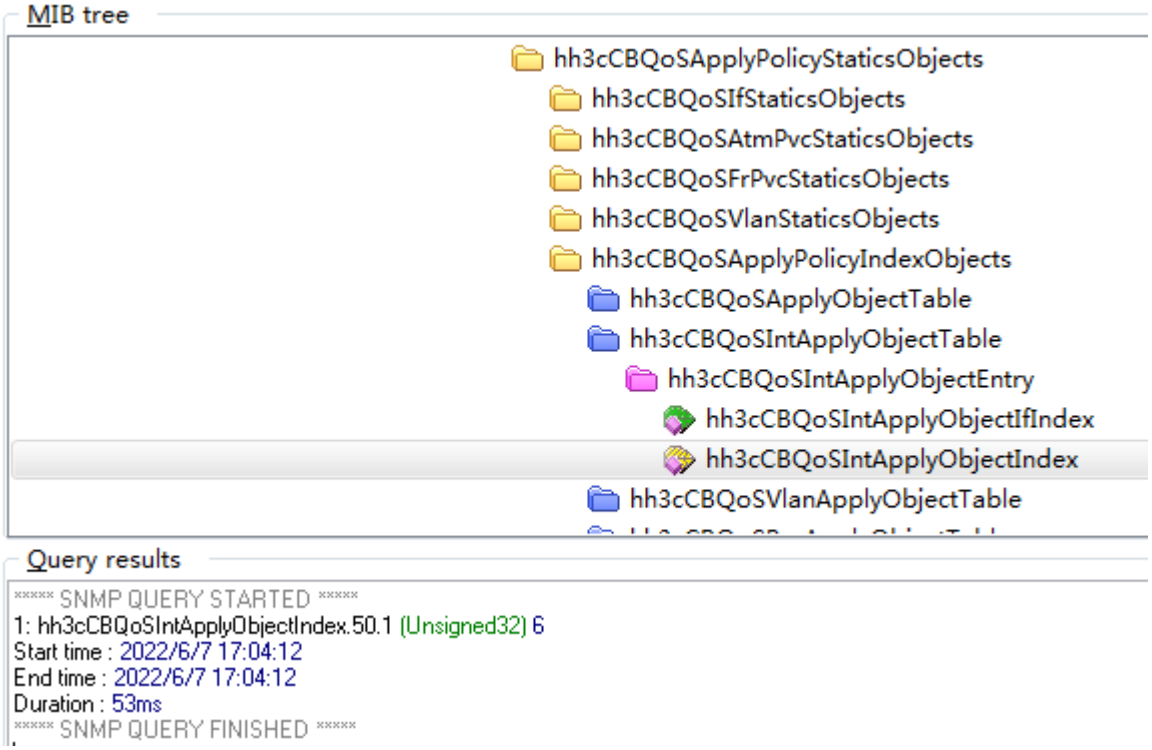
如图 6-2 所示，通过 ifName 节点（1.3.6.1.2.1.31.1.1.1.1）的子节点 ifDescr（1.3.6.1.2.1.31.1.1.1.1.2）查询 HGE1/0/30 接口的索引。查询结果会显示在 Query results 对话框中，HGE1/0/30 口索引为 51。

图6-2 查询接口索引



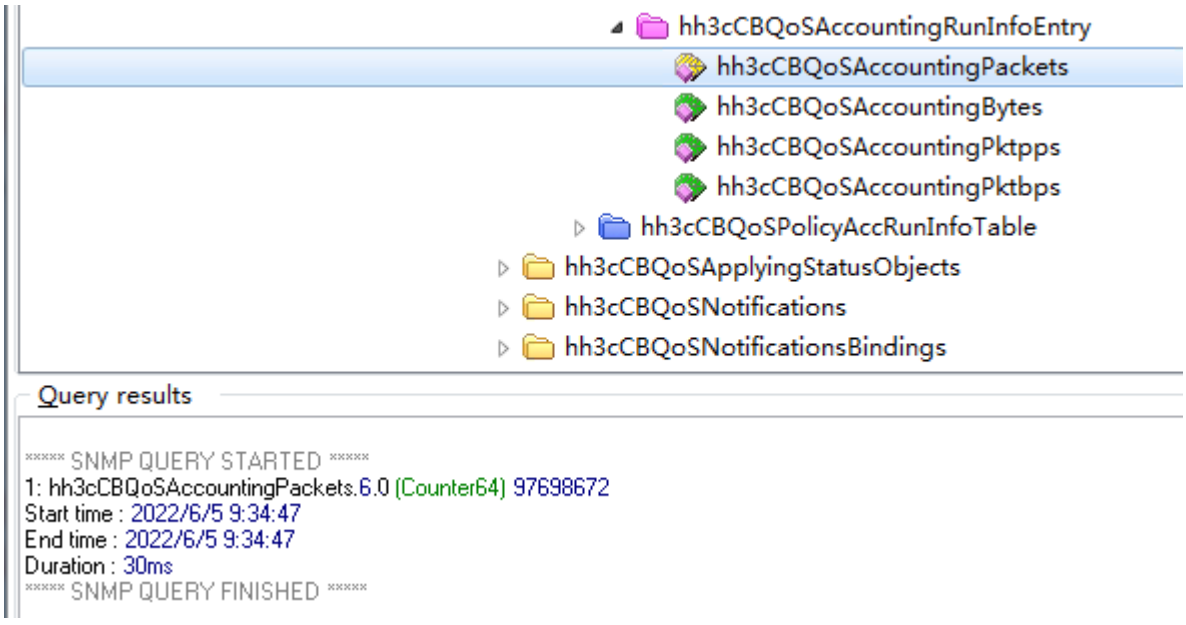
通过接口索引在 hh3cCBQoSIntApplyObjectIndex 表（ODI 为 1.3.6.1.4.1.25506.2.65.2.1.5.5.2.1.2）查询应用在接口 QoS 策略的索引。如图 6-3 所示，查询应用在接口 HundredGigE1/0/30 的 QoS 策略索引为 6。

图6-3 查询应用在接口 QoS 策略索引



如图 6-4 所示，通过 hh3cCBQoSAccountingRunInfoEntry 表（OID 为 1.3.6.1.4.1.25506.2.65.2.1.5.6.8.1）查询 VPN vpn1 入方向以字节为单位的流量统计数据。

图6-4 查询流量统计数据



6.3.4 更多信息

关于 SNMP 的更多配置，请参见对应产品的 SNMP 配置。

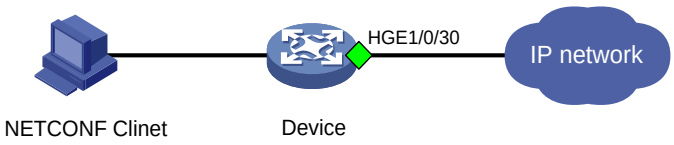
关于 MIB 文件的更多介绍，请参见对应产品的 MIB 参考。

6.4 NETCONF实现

6.4.1 配置需求

在主机上安装 NETCONF 客户端软件，通过 NETCONF 读取设备（Agent）的二层以太网接口 HGE2/0/25 流量统计信息。

图6-5 SNMP 功能典型配置组网图



说明

NETCONF 客户端是通过 Device 设备提供的 NETCONF XML API 获取的接口流量统计信息。

6.4.2 配置步骤

配置 MQC 获取 VPN vpn1 入方向流量统计数据，请参见 6.2.3 配置步骤。

配置 NETCONF，请参见 3.1.3 2. 配置步骤相同。

6.4.3 查询流量统计数据示例

说明

设备提供 MQC/IfPolicyAccount 表用于统计接口流量数据。通过 MQC/IfPolicyAccount 表可查询以字节为单位和以包为单位的统计信息

以下使用 MQC/AccountRunInfo 表查询接口 HundredGigE2/0/25 统计信息为例。

请将以下报文拷贝、粘贴到 NETCONF 客户端。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
        <MQC>
          <IfPolicyAccount>
            <Interface>
```

```
                <IfIndex>50</IfIndex>            //接口索引
                <Direction></Direction>          //QoS 策略应用方向
                <ClassName></ClassName>          //流分类名字
                <Packets></Packets>              //以包为单位的流量统计数据
                <Bytes></Bytes>                  //以字节为单位的流量统计数据
                <pps></pps>                      //每秒以包为单位的流量统计数据
                <bps></bps>                      //每秒以字节为单位的流量统计数据
              </Interface>
            </IfPolicyAccount>
          </MQC>
        </top>
      </filter>
    </get>
</rpc>
```

如果客户端收到类似如下的报文，则表示操作成功。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<data>
   <top xmlns="http://www.h3c.com/netconf/data:1.0">
      <MQC>
         <IfPolicyAccount>
            <Interface>
               <IfIndex>50</IfIndex>
               <Direction>0</Direction>
               <ClassName>aa</ClassName>
               <Packets>98928876</Packets>
               <pps>0</pps>
            </Interface>
         </IfPolicyAccount>
      </MQC>   </top>
   </data>
</rpc-reply>
```

6.4.4 更多信息

关于 NETCONF 配置的更多信息，请参见对应产品的“NETCONF 配置”。

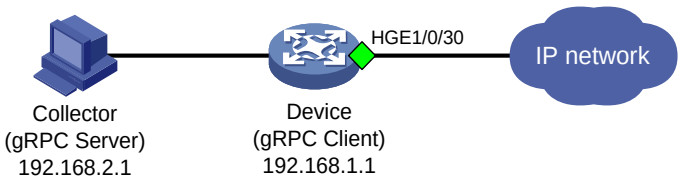
关于MQC/AccountRunInfo的更多信息，请参见《H3C Comware 7 NETCONF XML API Reference 》。

6.5 gRPC方式实现

6.5.1 配置需求

采集器通过 gRPC 协议读取设备（Device）的二层以太网接口 HGE1/0/30 流量统计信息。

图6-6 gRPC 功能典型配置组网图



6.5.2 配置步骤

在开始下面的配置之前，请确保设备与采集器的 IP 地址都已配置完毕，并且它们之间路由可达。

配置 MQC 获取 VPN vpn1 入方向流量统计数据，请参见 6.2.3 配置步骤。

开启 gRPC 功能。

```
<Sysname> system-view
[Sysname] grpc enable
```

创建传感器组 test，并添加采样路径为 MQC/IfPolicyAccount。

说明

配置采样路径为 MQC/IfPolicyAccount，设备会收集设备所有接口通过 MQC 统计的流量数据，并将数据上传给采集器。

```
[Sysname] telemetry
[Sysname-telemetry] sensor-group test
[Sysname-telemetry-sensor-group-test] sensor path mqc/ifpolicyaccount
[Sysname-telemetry-sensor-group-test] quit
```

创建目标组 collector1，并配置 IP 地址为 192.168.2.1、端口号为 50050 的采集器。

```
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] ipv4-address 192.168.2.1 port 50050
[Sysname-telemetry-destination-group-collector1] quit
```

创建订阅 A，配置关联传感器组为 test，数据采样和推送周期为 30 秒，关联目标组为 collector1。

```
[Sysname-telemetry] subscription A
[Sysname-telemetry-subscription-A] sensor-group test sample-interval 30
[Sysname-telemetry-subscription-A] destination-group collector1
[Sysname-telemetry-subscription-A] quit
```

6.5.3 查询流量统计数据

采集器每 30 秒收到一次设备推送的数据信息。

6.5.4 更多信息

关于 gRPC 配置的更多信息，请参见对应产品的“gRPC 配置”。

7 队列流量统计实现

说明

本节介绍通过命令行、SNMP、NETCONF、gRPC 四种方式查询队列流量统计。配置时需要先在设备上配置 QoS 策略，并设置好流分类和流行为，然后将 QoS 策略应用在指定位置，如接口、VLAN 等。

7.1 接口队列的流量统计

7.1.1 需求说明

获取接口队列出方向流量统计数据。

说明

- 接口队列只能统计出方向流量统计数据。
- 支持统计转发报文数、丢弃报文数，并显示当前队列长度。

7.1.2 命令行方式实现

1. 配置需求

查询接口 HundredGigE1/0/29 的队列出方向统计信息。

2. 查询流量统计数据

查询接口 HGE1/0/29 队列的流量统计数据。

```
<Sysname> display qos queue-statistics interface hundredgige 1/0/29 outbound
Interface: HundredGigE1/0/29
 Direction: outbound
 Forwarded: 8614890247 packets, 1498990957070 bytes
 Dropped: 22096410 packets, 2828340480 bytes
 Queue 0
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 1
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 2
  Forwarded: 8614889788 packets, 1498990823112 bytes, 7184 pps, 10001024 bps
  Dropped: 22096410 packets, 2828340480 bytes
```

```
 Current queue length: 26142 packets
Queue 3
 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 4
 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 5
 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 6
 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 7
 Forwarded: 459 packets, 133958 bytes, 0 pps, 0 bps
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
```

表7-1 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	转发的数据包数目和字节数
Dropped	丢弃的数据包数目和字节数 S9850-4C、S9850-32H和S6850-56HF后面板的2个1G SFP接口不支持丢弃的数据包数目和字节数
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
Current queue length	当前队列长度

3. 更多信息

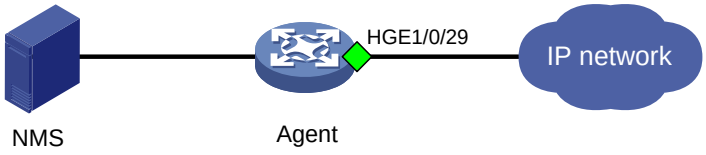
关于 MQC 配置的更多信息，请参见对应产品的“QoS 配置”和“QoS 命令”。

7.1.3 SNMP 方式实现

1. 配置需求

NMS 通过 SNMP 协议读取接口 HundredGigE1/0/29 队列出方向统计信息。

图7-1 SNMP 功能典型配置组网图



2. 配置步骤

配置 SNMP，请参见 3.1.3 2. 配置步骤。

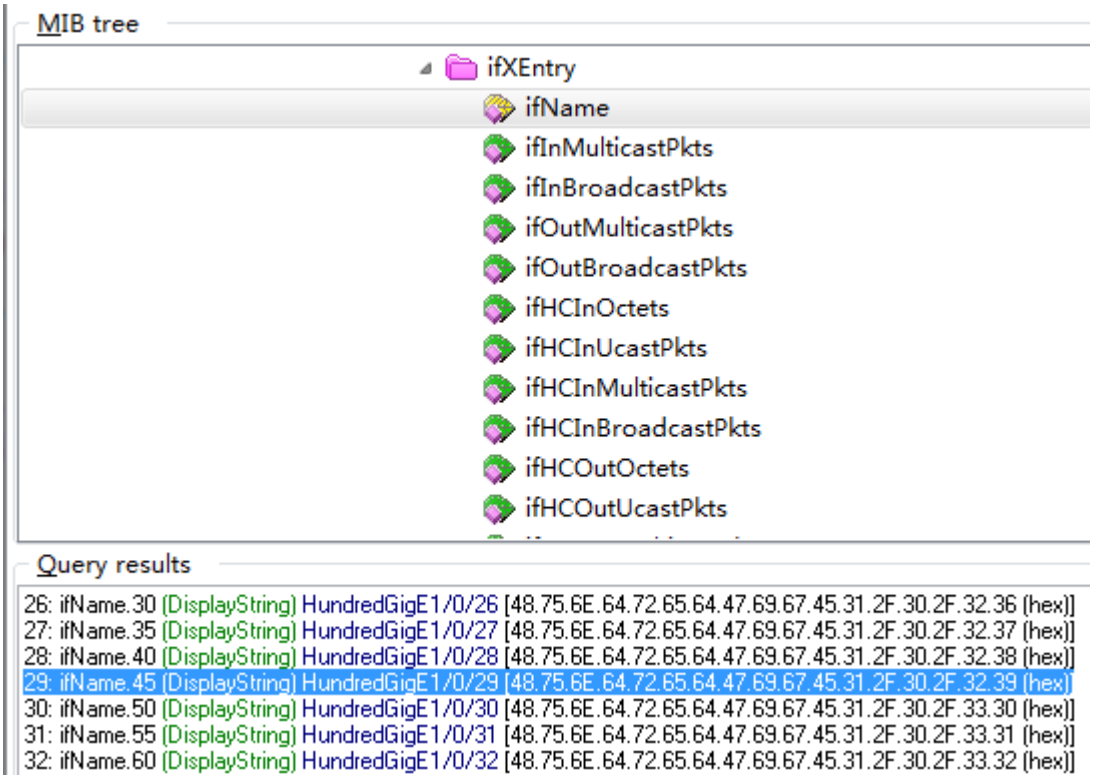
3. 查询流量统计数据示例

说明

- 本举例以通过 MIB Browser 查询 Agent 设备接口队列的流量统计数据为例。
- 查询接口队列丢包流量统计数据，先通过 ifDescr 表（OID1.3.6.1.2.1.2.2.1.2）获取接口索引，然后使用索引查找。
- 设备 IRF 成员编号不同时，接口索引值可能不同，具体以实际查询结果为准。

如图 7-2 所示，通过 ifName 节点（1.3.6.1.2.1.31.1.1.1.1）的子节点 ifDescr（1.3.6.1.2.1.31.1.1.1.1.2）查询 HGE1/0/29 接口的索引。查询结果会显示在 Query results 对话框中，HGE1/0/30 口索引为 45。

图7-2 查询接口索引



使用接口索引在 hh3cIfQoSHardwareQueueRunInfoEntry 表（ODI 为 1.3.6.1.4.1.25506.2.65.1.1.2.1.1）中查询该接口队列统计，如图 7-3 所示。

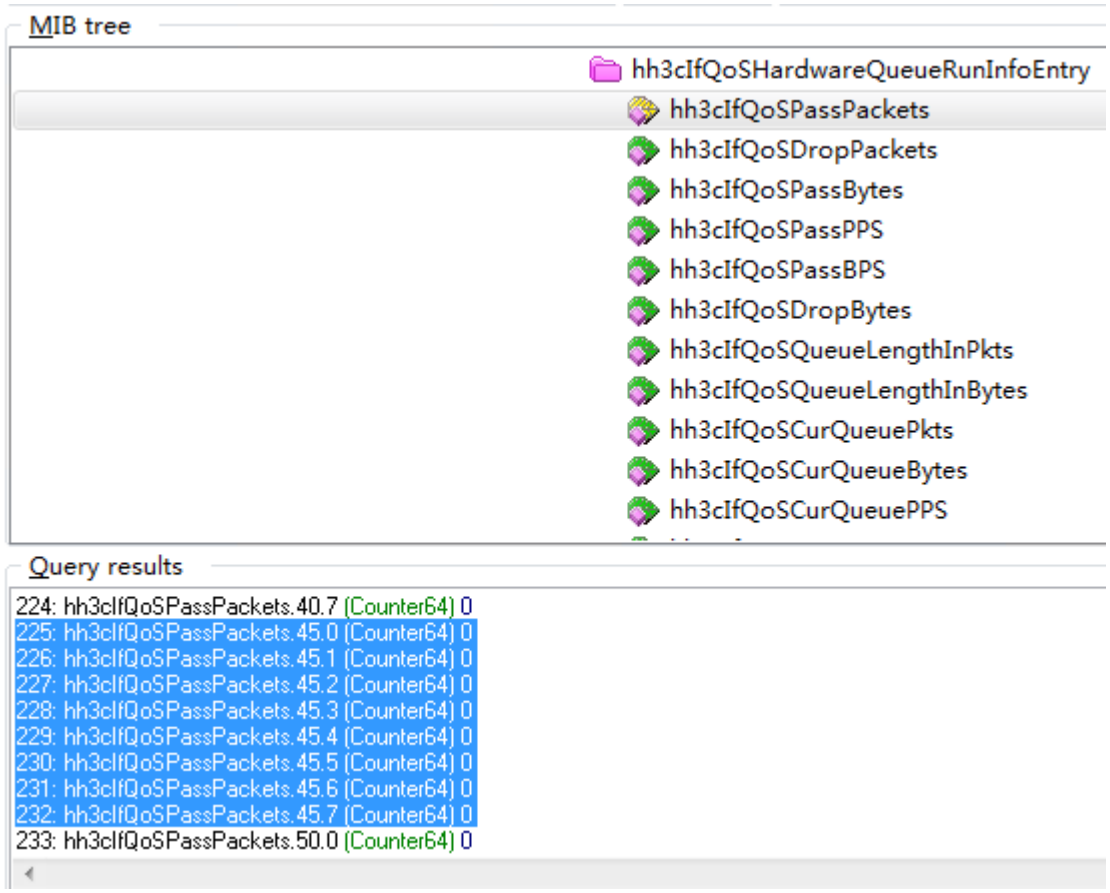
说明

通过 hh3cIfQoSHardwareQueueRunInfoEntry 表（ODI 为 1.3.6.1.4.1.25506.2.65.1.1.2.1.1）可查询端口队列如下统计信息:

- 端口队列转发报文包数，表名为 hh3cIfQoSPassPackets（ODI 为 1.3.6.1.4.1.25506.2.65.1.1.2.1.1.1）
- 端口队列丢弃报文包数，表名为 hh3cIfQoSDropPackets（ODI 为 1.3.6.1.4.1.25506.2.65.1.1.2.1.1.2）
- 端口队列转发报文字节数，表名为 hh3cIfQoSPassBytes（ODI 为 1.3.6.1.4.1.25506.2.65.1.1.2.1.1.3）
- 端口队列丢弃报文包数，表名为 hh3cIfQoSDropBytes（ODI 为 1.3.6.1.4.1.25506.2.65.1.1.2.1.1.6）
- 当前队列长度，表名为 hh3cIfQoSCurQueuePkts（ODI 为 1.3.6.1.4.1.25506.2.65.1.1.2.1.1.9）和表名为 hh3cIfQoSCurQueueBytes（ODI 为 1.3.6.1.4.1.25506.2.65.1.1.2.1.1.10）。

以下以查询接口队列转发报文数为例，更多可查询数据，请参见对应产品的 MIB 参考。

图7-3 查询接口队列转发报文数



4. 更多信息

关于 SNMP 的更多配置，请参见对应产品的 SNMP 配置。

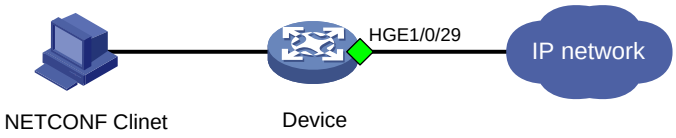
关于 MIB 文件的更多介绍，请参见对应产品的 MIB 参考。

7.1.4 NETCONF 实现

1. 配置需求

在主机上安装 NETCONF 客户端软件，通过 NETCONF 读取设备（Agent）的接口 HGE1/0/29 队列流量统计信息。

图7-4 SNMP 功能典型配置组网图



说明

NETCONF 客户端是通过 Device 设备提供的 NETCONF XML API 获取的接口流量统计信息。

2. 配置步骤

配置 NETCONF，请参见 3.1.3 2. 配置步骤相同。

3. 查询流量统计数据示例

说明

设备提供 QSTAT/InterfaceStat 表用于统计接口队列流量数据。通过 QSTAT/InterfaceStat 表可查询以字节为单位和以包为单位的统计信息。

以下使用 QSTAT/InterfaceStat 表查询 HundredGigE1/0/29 接口统计信息为例。

在设备 Probe 视图使用 **display system internal ifmgr list | include HundredGigE**1/0/29 命令查询接口 HundredGigE21/0/29 的索引。

```
[Sysname-probe]display system internal ifmgr list | include HundredGigE1/0/29
        HundredGigE1/0/29(index:45)
```

请将以下报文拷贝、粘贴到 NETCONF 客户端。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
        <QSTAT>
          <InterfaceStat>
            <Statistics>
```

```
              <IfIndex>45</IfIndex>
              <Direction></Direction>
              <PassPacket></PassPacket>
              <PassByte></PassByte>
              <DropPacket></DropPacket>
              <DropByte></DropByte>
              <AgingPacket></AgingPacket>
              <AgingByte></AgingByte>
            </Statistics>
          </InterfaceStat>
        </QSTAT>
      </top>
    </filter>
  </get>
</rpc>
```

如果客户端收到类似如下的报文，则表示操作成功。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <data>
     <top xmlns="http://www.h3c.com/netconf/data:1.0">
        <QSTAT>
          <InterfaceStat>
            <Statistics>
              <IfIndex>45</IfIndex>
              <Direction>1</Direction>
              <PassPacket>578853253273</PassPacket>
              <PassByte>97793557880219</PassByte>
              <DropPacket>67748792372</DropPacket>
              <DropByte>8671845423616</DropByte>
              <AgingPacket></AgingPacket>
              <AgingByte></AgingByte>
            </Statistics>
          </InterfaceStat>
        </QSTAT>
     </top>
   </data>
</rpc-reply>
```

4. 更多信息

关于 NETCONF 配置的更多信息，请参见对应产品的“NETCONF 配置”。

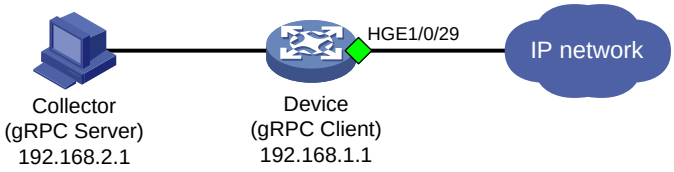
关于 QSTAT/InterfaceStat 的更多信息，请参见《H3C Comware 7 NETCONF XML API Reference 》。

7.1.5 gRPC 方式实现

1. 配置需求

采集器通过 gRPC 协议读取设备（Device）接口 HGE1/0/29 的出方向流量统计信息。

图7-5 gRPC 功能典型配置组网图



2. 配置步骤

在开始下面的配置之前，请确保设备与采集器的 IP 地址都已配置完毕，并且它们之间路由可达。

开启 gRPC 功能。

```
<Sysname> system-view
[Sysname] grpc enable
```

创建传感器组 test，并添加采样路径为 QSTAT/InterfaceStat。

说明

配置采样路径为 QSTAT/InterfaceStat，设备会收集设备所有接口通过 MQC 统计的流量数据，并将数据上传给采集器。

```
[Sysname] telemetry
[Sysname-telemetry] sensor-group test
[Sysname-telemetry-sensor-group-test] sensor path qstat/interfacestat
[Sysname-telemetry-sensor-group-test] quit
```

创建目标组 collector1，并配置 IP 地址为 192.168.2.1、端口号为 50050 的采集器。

```
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] ipv4-address 192.168.2.1 port 50050
[Sysname-telemetry-destination-group-collector1] quit
```

创建订阅 A，配置关联传感器组为 test，数据采样和推送周期为 30 秒，关联目标组为 collector1。

```
[Sysname-telemetry] subscription A
[Sysname-telemetry-subscription-A] sensor-group test sample-interval 30
[Sysname-telemetry-subscription-A] destination-group collector1
[Sysname-telemetry-subscription-A] quit
```

3. 查询流量统计数据

采集器每 30 秒收到一次设备推送的数据信息。

4. 更多信息

关于 gRPC 配置的更多信息，请参见对应产品的“gRPC 配置”。

7.2 接口队列丢包统计

7.2.1 需求说明

获取接口队列丢包统计数据。

7.2.2 命令行方式实现

1. 配置需求

查询接口 HundredGigE1/0/29 队列丢包的统计信息。

2. 配置步骤

无需配置。

3. 查询流量统计数据

查询接口 HGE1/0/29 队列丢包的统计信息。

```
[Sysname]display packet-drop interface hundredgige1/0/29
HundredGigE1/0/29:
   Packets dropped due to full GBP or insufficient bandwidth: 0
  Packets dropped due to Fast Filter Processor (FFP): 51725218317
  Packets dropped due to STP non-forwarding state: 0
```

表7-2 display packet-drop 命令显示信息描述表

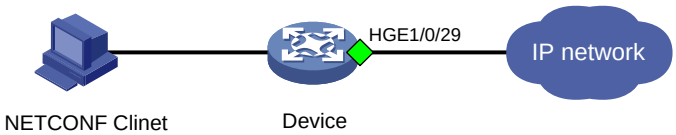
字段	描述
Packets dropped due to full GBP or insufficient bandwidth	由于芯片缓存满或者带宽不够导致的丢包数
Packets dropped due to Fast Filter Processor (FFP)	由于接口入方向数据包被过滤所导致的丢包数
Packets dropped due to STP non-forwarding state	由于STP协议状态为discarding导致的丢包数

7.2.3 NETCONF 实现

1. 配置需求

在主机上安装 NETCONF 客户端软件，通过 NETCONF 读取设备（Agent）的接口 HGE1/0/29 队列丢包统计信息。

图7-6 SNMP 功能典型配置组网图



说明

NETCONF 客户端是通过 Device 设备提供的 NETCONF XML API 获取的接口队列丢包统计信息。

2. 配置步骤

配置 NETCONF，请参见 3.1.3 2. 配置步骤相同。

3. 查询流量统计数据示例

说明

设备提供 QSTAT/InterfaceStat 表用于统计接口队列丢包流量数据。通过 QSTAT/InterfaceStat 表可查询以字节为单位和以包为单位的统计信息。

以下使用 QSTAT/InterfaceStat 表查询接口 HundredGigE1/0/29 队列丢包统计信息为例。

在设备 Probe 视图使用 **display system internal ifmgr list | include HundredGigE**1/0/29 命令查询接口 HundredGigE21/0/29 的索引。

```
[Sysname-probe]display system internal ifmgr list | include HundredGigE1/0/29
         HundredGigE1/0/29(index:45)
```

请将以下报文拷贝、粘贴到 NETCONF 客户端。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.h3c.com/netconf/data:1.0">
        <QSTAT>
          <InterfaceStat>
            <Statistics>
              <IfIndex>45</IfIndex>
              <Direction></Direction>
              <PassPacket></PassPacket>
              <PassByte></PassByte>
              <DropPacket></DropPacket>
              <DropByte></DropByte>
            </Statistics>
          </InterfaceStat>
        </QSTAT>
      </top>
    </filter>
  </get>
</rpc>
```

如果客户端收到类似如下的报文，则表示操作成功。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <data>
     <top xmlns="http://www.h3c.com/netconf/data:1.0">
        <QSTAT>
          <InterfaceStat>
            <Statistics>
              <IfIndex>45</IfIndex>
              <Direction>1</Direction>
              <PassPacket>578853253273</PassPacket>
              <PassByte>97793557880219</PassByte>
              <DropPacket>67748792372</DropPacket>
              <DropByte>8671845423616</DropByte>
```

```
            </Statistics>
          </InterfaceStat>
        </QSTAT>
      </top>
    </data>
</rpc-reply>
```

4. 更多信息

关于 NETCONF 配置的更多信息，请参见对应产品的“NETCONF 配置”。

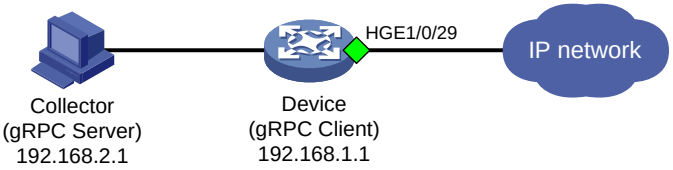
关于 QSTAT/InterfaceStat 的更多信息，请参见《H3C Comware 7 NETCONF XML API Reference 》。

7.2.4 gRPC 方式实现

1. 配置需求

采集器通过 gRPC 协议读取设备（Device）接口 HGE1/0/29 队列丢包统计信息。

图7-7 gRPC 功能典型配置组网图



2. 配置步骤

在开始下面的配置之前，请确保设备与采集器的 IP 地址都已配置完毕，并且它们之间路由可达。

开启 gRPC 功能。

```
<Sysname> system-view
[Sysname] grpc enable
```

创建传感器组 test，并添加采样路径为 QSTAT/InterfaceStat。

说明

配置采样路径为 QSTAT/InterfaceStat，设备会收集设备所有接口队列丢包统计数据，并将数据上传给采集器。

```
[Sysname] telemetry
[Sysname-telemetry] sensor-group test
[Sysname-telemetry-sensor-group-test] sensor path qstat/interfacestat
[Sysname-telemetry-sensor-group-test] quit
```

创建目标组 collector1，并配置 IP 地址为 192.168.2.1、端口号为 50050 的采集器。

```
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] ipv4-address 192.168.2.1 port 50050
[Sysname-telemetry-destination-group-collector1] quit
```

创建订阅 A，配置关联传感器组为 test，数据采样和推送周期为 30 秒，关联目标组为 collector1。

```
[Sysname-telemetry] subscription A
```

```
[Sysname-telemetry-subscription-A] sensor-group test sample-interval 30
[Sysname-telemetry-subscription-A] destination-group collector1
[Sysname-telemetry-subscription-A] quit
```

3. 查询流量统计数据

采集器每 30 秒收到一次设备推送的数据信息。

4. 更多信息

关于 gRPC 配置的更多信息，请参见对应产品的“gRPC 配置”。

8 流量统计应用案例

8.1 通过统计ICMP流量定位流量不通的位置

8.1.1 需求说明

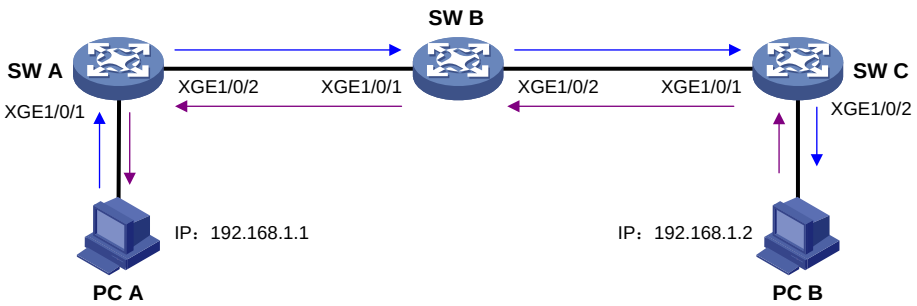
通过使用 Ping 功能，用户可以检查指定地址的设备是否可达，测试链路是否通畅。

Ping 功能是基于 ICMP（Internet Control Message Protocol，互联网控制消息协议）协议来实现的：源端向目的端发送 ICMP 回显请求（ECHO-REQUEST）报文后，根据是否收到目的端的 ICMP 回显应答（ECHO-REPLY）报文来判断目的端是否可达，对于可达的目的端，再根据发送报文个数、接收到响应报文个数以及 Ping 过程报文的往返时间来判断链路的质量。

当源端和目的端之间出现流量不通时，我们可以在沿途设备上部署流量统计功能，对 ICMP 报文的收、发进行统计，判断流量不通的位置。

如图 8-1 所示，PC A Ping PC B 不通，我们在 SW A、SW B、SW C 上部署 ICMP 报文流量统计，判断哪台设备存在流量不通。

图8-1 通过统计 ICMP 流量定位流量不通的位置



8.1.2 定位思路

我们以 SW B 上的定位为例，SW A 和 SW C 同理。

以 PC A（192.168.1.1）主动 Ping PC B（192.168.1.2）为例，ICMP Request 报文从 SW B 的 Ten-GigabitEthernet1/0/1 进入、Ten-GigabitEthernet1/0/2 发出，我们部署流量统计功能，统计 Ten-GigabitEthernet1/0/1 入方向的 ICMP 报文与 Ten-GigabitEthernet1/0/2 出方向的 ICMP 报文包

数是否相同，如果 Ten-GigabitEthernet1/0/2 出方向比 Ten-GigabitEthernet1/0/1 入方向 ICMP 报文少，则存在丢包。反向同理。

8.1.3 定位步骤

定义高级 ACL 3000，匹配源 IP 为 192.168.1.1、目的 IP 为 192.168.1.2 的 ICMP Request 报文。

```
<SWB> system-view
[SWB] acl advanced 3000
[SWB-acl-ipv4-adv-3000] rule permit icmp source 192.168.1.1 0 destination 192.168.1.2 0
```

创建流分类 classifier_1，匹配 ACL 3000。创建流行为 behavior_1，动作为 accounting。

```
[SWB] traffic classifier classifier_1
[SWB-classifier-classifier_1] if-match acl 3000
[SWB-classifier-classifier_1] quit
[SWB] traffic behavior behavior_1
[SWB-behavior-behavior_1] accounting packet
[SWB-behavior-behavior_1] quit
```

创建 QoS 策略 policy_1 的，将流分类 classifier_1 和流行为 behavior_1 关联。

```
[SWB] qos policy policy_1
[SWB-qos-policy-policy_1] classifier classifier_1 behavior behavior_1
[SWB-qos-policy-policy_1] quit
```

将 QoS 策略 policy_1 应用到 Ten-GigabitEthernet1/0/1 的入方向和 Ten-GigabitEthernet1/0/2 的出方向。

```
[SWB]interface ten-gigabitethernet 1/0/1
[SWB-Ten-GigabitEthernet1/0/1] qos apply policy policy_1 inbound
[SWB-Ten-GigabitEthernet1/0/1] quit
[SWB] interface ten-gigabitethernet 1/0/2
[SWB-Ten-GigabitEthernet1/0/2] qos apply policy policy_1 outbound
[SWB-Ten-GigabitEthernet1/0/2] quit
```

通过 **display qos policy interface inbound/display qos policy interface outbound** 命令查看流量统计结果，Ten-GigabitEthernet1/0/1 的 inbound 方向收到了 5 个 ICMP Request 报文，Ten-GigabitEthernet1/0/2 的 outbound 方向发出了 5 个 ICMP Request 报文，由此说明 SW B 并没有丢弃 ICMP Request 报文。

```
[SWB] display qos policy interface ten-gigabitethernet 1/0/1 inbound
Interface: Ten-GigabitEthernet1/0/1
  Direction: Inbound
  Policy: policy_1
   Classifier: classifier_1
     Operator: AND
     Rule(s) :
      If-match acl 3000
     Behavior: behavior_1
      Accounting enable:
        5 (Packets)
[SWB] display qos policy interface ten-gigabitethernet 1/0/2 outbound
Interface: Ten-GigabitEthernet1/0/2
  Direction: Outbound
```

```
  Policy: policy_1
   Classifier: classifier_1
     Operator: AND
     Rule(s) :
      If-match acl 3000
     Behavior: behavior_1
      Accounting enable:
        5 (Packets)
```

下次统计前通过 **reset counters interface** 命令清除接口计数，清除后可以再次进行 Ping 测试和流量统计。

```
[SWB] quit
<SWB> reset counters interface ten-gigabitethernet 1/0/1
<SWB> reset counters interface ten-gigabitethernet 1/0/2
```

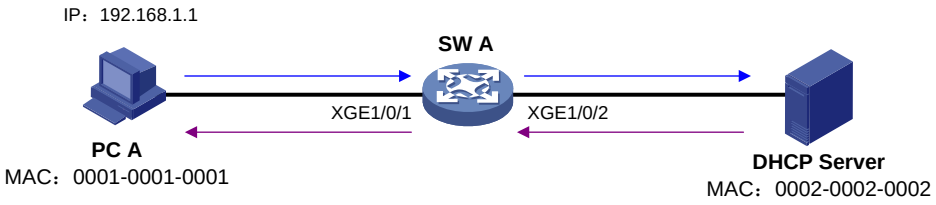
8.2 通过统计DHCP报文定位终端未成功获取IP地址的原因

8.2.1 需求说明

在网络中，DHCP 协议主要用于分配 IP 地址给终端设备。当终端未能成功通过 DHCP 获得 IP 地址时，可以在终端到 DHCP Server 的沿途设备上部署流量统计，确认每台沿途设备上 DHCP 报文的传输是否正常。

如图 8-2 所示，在 SW A 上部署 DHCP 报文流量统计，确认 SW A 是否能正常收发 DHCP 报文。

图8-2 通过统计 DHCP 报文定位终端未成功获取 IP 地址的原因



8.2.2 定位思路

终端通过 DHCP 获取 IP 地址时，终端先发出 DHCP Discovery 报文，服务器收到后会进行地址的分配并回复 DHCP Offer 报文，终端收到后会再次发送 DHCP Request 报文进行确认，服务器最后回复 DHCP ACK 给终端。

DHCP 报文均为 UDP 报文，终端发出的 DHCP 报文 UDP 源端口号为 68（bootpc），DHCP Server 发出的 DHCP 报文源端口号 67（bootps），我们可以根据报文的源 MAC 及 UDP 端口号匹配 DHCP 报文。

8.2.3 定位步骤

定义 ACL 3010 匹配终端发出的 DHCP 报文。

```
<SWA> system-view
[SWA] acl advanced 3010
[SWA-acl-ipv4-adv-3010] rule 0 permit udp source-port eq bootpc destination-port eq bootps
```

```
[SWA-acl-ipv4-adv-3010] quit
```
定义 ACL 3011 匹配服务器发出的 DHCP 报文。
```
[SWA] acl advanced 3011
[SWA-acl-ipv4-adv-3011] rule 0 permit udp source-port eq bootps destination-port eq bootpc
[SWA-acl-ipv4-adv-3011] quit
```
创建流分类 client，匹配 ACL 3010 和 PC A 的 MAC，创建流行为 client，动作为 accounting packet，创建 QoS 策略 client，将流分类 client 和流行为 client 关联。
```
[SWA] traffic classifier client
[SWA-classifier-client] if-match acl 3010
[SWA-classifier-client] if-match source-mac 1-1-1
[SWA-classifier-client] quit
[SWA] traffic behavior client
[SWA-behavior-client] accounting packet
[SWA-behavior-client] quit
[SWA] qos policy client
[SWA-qos-policy-client] classifier client behavior client
[SWA-qos-policy-client] quit
```
创建流分类 server，匹配 ACL 3011 和 DHCP Server 的 MAC，创建流行为 server，动作为 accounting packet，创建 QoS 策略 server，将流分类 server 和流行为 server 关联。
```
[SWA] traffic classifier server
[SWA-classifier-server] if-match acl 3011
[SWA-classifier-server] if-match source-mac 2-2-2
[SWA-classifier-server] quit
[SWA] traffic behavior server
[SWA-behavior-server] accounting packet
[SWA-behavior-server] quit
[SWA] qos policy server
[SWA-qos-policy-server] classifier server behavior server
[SWA-qos-policy-server] quit
```
将 QoS 策略应用到 DHCP 终端所在端口的入方向和 DHCP 服务器所在端口的出方向。
```
[SWA] interface ethernet 1/1/1
[SWA-Ethernet1/1/1] qos apply policy policy_1 inbound
[SWA] interface ethernet 1/1/2
[SWA-Ethernet1/1/2] qos apply policy policy_1 outbound
```
将 QoS 策略 client 应用到 Ten-GigabitEthernet1/0/1 的入方向和 Ten-GigabitEthernet1/0/2 的出方向。
```
[SWA]interface ten-gigabitethernet 1/0/1
[SWA-Ten-GigabitEthernet1/0/1] qos apply policy client inbound
[SWA-Ten-GigabitEthernet1/0/1] quit
[SWA] interface ten-gigabitethernet 1/0/2
[SWA-Ten-GigabitEthernet1/0/2] qos apply policy client outbound
[SWA-Ten-GigabitEthernet1/0/2] quit
```
将 QoS 策略 server 应用到 Ten-GigabitEthernet1/0/2 的入方向和 Ten-GigabitEthernet1/0/1 的出方向。
```
[SWA] interface ten-gigabitethernet 1/0/2
[SWA-Ten-GigabitEthernet1/0/2] qos apply policy server inbound
```

```
[SWA-Ten-GigabitEthernet1/0/2] quit
[SWA]interface ten-gigabitethernet 1/0/1
[SWA-Ten-GigabitEthernet1/0/1] qos apply policy server outbound
[SWA-Ten-GigabitEthernet1/0/1] quit
```

通过 **display qos policy interface inbound/display qos policy interface outbound** 命令查看 Ten-GigabitEthernet1/0/1 和 Ten-GigabitEthernet1/0/2 流量统计结果，可以分别查看终端到 DHCP Server 之间、DHCP Server 到终端之间是否存在 DHCP 报文丢包。