H3C S5500-HI 系列以太网交换机

网络管理和监控配置指导

杭州华三通信技术有限公司
http://www.h3c.com.cn

资料版本：6W102-20131220
产品版本：Release 52xx 系列

前 言

H3C S5500-HI 系列以太网交换机配置指导共分为十一本手册，介绍了 S5500-HI 系列以太网交换机 Release52xx 系列软件版本各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例。《网络管理和监控配置指导》主要介绍了网络管理和监控相关功能的原理及具体配置。通过这些功能，您可以对网络进行管理和监控，包括查看系统信息、对网络流量进行统计、对网络质量进行分析、对网络内所有具有时钟的设备进行时钟同步，并可以使用 ping、tracert、debug 等命令来检查、调试当前网络的连接情况。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

新增及修改特性说明

本手册对应 S5500-HI 系列以太网交换机的 Release52xx 系列软件版本，各版本间特性差异如下：

- Release5206 与Release5203 版本相比，新增、修改了部分特性，具体请参见 表 1。
- Release5203 与Release5101 版本相比，新增、修改了部分特性，具体请参见 表 2。

表1 Release5206 与 Release5203 版本间特性差异

配置指导		新增及修改特性
SNMP	SNMP	修改特性：修改SNMP中系统信息描述字符串的最大长度
	MIB	无
报文捕获		报文捕获功能为本版本新增特性

表2 Release5203 与 Release5101 版本间特性差异

配置指导		新增及修改特性
系统维护与调试		新增特性： • 指定 ICMPv6 回显请求报文中的 ToS 域的值 • 指定 tracert 报文中的 ToS 域的值 • 指定 tracert ipv6 报文中的 ToS 域的值
NTP		新增特性： • 配置 NTP 报文的 DSCP 优先级 • NTP 支持 NTPv4 • 设置 NTP 验证密钥
信息中心		新增特性：配置发送到日志主机的报文的DSCP优先级
SNMP	SNMP	新增特性： • 配置SNMP响应报文的DSCP优先级 • 设置SNMP发送的Trap报文的DSCP优先级 • SNMP支持IPv6 ACL • 创建SNMPv3用户时，支持非16进制格式的认证密码和加密密码
	MIB	无
RMON		无
镜像	端口镜像	无
	流镜像	无
NQA		新增特性： • 配置 NQA 服务器 TCP/UDP 监听服务发送报文的 ToS 值 • 进行 FTP 测试时，以密文方式设置 FTP 服务器的登录密码 • 进行 DHCP 测试时，配置 NQA 探测报文 IP 报文头的 ToS 值
sFlow		新增特性：指定 sFlow Collector 所属的 VPN
NetStream		无
IPv6 NetStream		无
Sampler		无
IPC		无
PoE		PoE功能为本版本新增特性
集群管理		无
CWMP		新增特性： • 以密文方式设置 CPE 连接 ACS 的密码 • 以密文方式设置 ACS 连接 CPE 的密码

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。

	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

产品配套资料

H3C S5500-HI 系列以太网交换机的配套资料包括如下部分：

大类	资料名称	内容介绍
产品知识介绍	产品彩页	帮助您了解产品的主要规格参数及亮点
	技术白皮书	帮助您了解产品和特性功能，对于特色及复杂技术从细节上进行介绍
硬件介绍及安装	安全兼容性手册	列出产品的兼容性声明，并对兼容性和安全的细节进行说明
	H3C 设备防雷安装指导手册	帮助您了解防雷接地设计和工程安装方法，以保证交换机具有良好的抗雷击性能
	快速安装指南	指导您对设备进行初始安装，通常针对最常用的情况，减少您的检索时间
	安装指导	帮助您详细了解设备硬件规格和安装方法，指导您对设备进行安装
	风扇安装手册	帮助您了解产品支持的可插拔风扇模块的外观、功能、规格、安装及拆卸方法
	电源手册	帮助您了解产品支持的可插拔电源模块的外观、功能、规格、安装及拆卸方法
	RPS电源用户手册	帮助您了解产品支持的RPS电源的外观、功能、规格
	H3C低端系列以太网交换机RPS电源选购指南	帮助您了解各种RPS电源适用的交换机产品型号及RPS电源配套电缆的相关规格
	接口模块扩展卡用户手册	帮助您了解该接口模块扩展卡的外观、规格、安装及拆卸方法
	H3C低端系列以太网交换机可插拔模块手册	帮助您了解产品支持的可插拔模块类型、外观和规格
	H3C可插拔SFP[SFP+][XFP]模块安装指南	帮助您掌握SFP/SFP+/XFP模块的正确安装方法，避免因操作不当而造成器件损坏
业务配置	配置指导	帮助您掌握设备软件功能的配置方法及配置步骤
	命令参考	详细介绍设备的命令，相当于命令字典，方便您查阅各个命令的功能
运行维护	故障处理手册	指导您快速定位并处理软件故障
	版本说明书	帮助您了解产品版本的相关信息（包括：版本配套说明、兼容性说明、特性变更说明、技术支持信息）及软件升级方法

资料获取方式

您可以通过H3C网站（www.h3c.com.cn）获取最新的产品资料：

H3C 网站与产品资料相关的主要栏目介绍如下：

- [服务支持/文档中心]：可以获取硬件安装类、软件升级类、配置类或维护类等产品资料。
- [产品技术]：可以获取产品介绍和技术介绍的文档，包括产品相关介绍、技术介绍、技术白皮书等。
- [解决方案]：可以获取解决方案类资料。
- [服务支持/软件下载]：可以获取与软件版本配套的资料。

技术支持

用户支持邮箱：service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

010-62982107

网址：http://www.h3c.com.cn

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 系统维护与调试

在日常的系统维护中，用户可以使用 **ping** 命令和 **tracert** 命令来检查当前网络的连接情况；在日常的系统调试中，用户可以使用 **debug** 命令来打开调试信息开关，通过调试信息来诊断系统故障。

1.1 Ping功能

1.1.1 Ping功能简介

通过使用 **ping** 命令，用户可以检查指定地址的设备是否可达，测试网络连接是否出现故障。

Ping 功能是基于 ICMP 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来判断链路的质量，根据 ping 报文的往返时间来判断源端与目的端之间的“距离”。

1.1.2 Ping配置

表1-1 Ping 配置

操作	命令	说明
检查IP网络中的指定地址是否可达	**ping** [**ip**] [**-a** *source-ip* | **-c** *count* | **-f** | **-h** *ttl* | **-i** *interface-type interface-number* | **-m** *interval* | **-n** | **-p** *pad* | **-q** | **-r** | **-s** *packet-size* | **-t** *timeout* | **-tos** *tos* | **-v** | **-vpn-instance** *vpn-instance-name*] * *host*	三者必选其一 • **ping** 命令用于 IPv4 网络环境 • **ping ipv6** 命令用于 IPv6 网络环境 • **ping lsp** 命令用于 MPLS 网络环境 三条命令均可在任意视图下执行 S5500-28SC-HI 和 S5500-52SC-HI不支持**ping lsp** 命令
	ping ipv6 [**-a** *source-ipv6* | **-c** *count* | **-m** *interval* | **-s** *packet-size* | **-t** *timeout* | **-tos** *tos* | **-vpn-instance** *vpn-instance-name*] * *host* [**-i** *interface-type interface-number*]	
	ping lsp [**-a** *source-ip* | **-c** *count* | **-exp** *exp-value* | **-h** *ttl-value* | **-m** *wait-time* | **-r** *reply-mode* | **-s** *packet-size* | **-t** *time-out* | **-v**] * **ipv4** *dest-addr mask-length* [*destination-ip-addr-header*]	

说明

- 如果网络传输速度较慢，用户在配置 **ping** 命令的超时时间参数**-t** 时，可以适当增大超时时间。
- **ping lsp** 命令的详细介绍请参见“MPLS 命令参考”中的“MPLS 基本配置”。

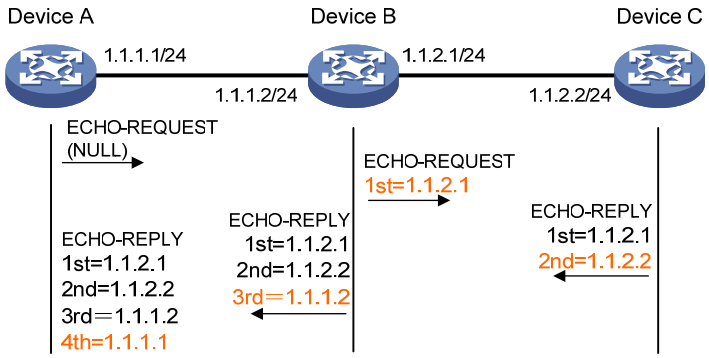
1.1.3 Ping配置举例

1. 组网需求

检查 Device A 与 Device C 之间是否路由可达，如果路由可达，需要了解 Device A 到 Device C 的路由细节。

2. 组网图

图1-1 Ping 应用组网图



3. 配置步骤

使用 ping 命令查看 Device A 和 Device C 之间路由是否可达。

```
<DeviceA> ping 1.1.2.2
  PING 1.1.2.2: 56  data bytes, press CTRL_C to break
    Reply from 1.1.2.2: bytes=56 Sequence=1 ttl=254 time=205 ms
    Reply from 1.1.2.2: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 1.1.2.2: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 1.1.2.2: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 1.1.2.2: bytes=56 Sequence=5 ttl=254 time=1 ms

  --- 1.1.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/41/205 ms
```

了解 Device A 到 Device C 的路由细节。

```
<DeviceA> ping -r 1.1.2.2
  PING 1.1.2.2: 56  data bytes, press CTRL_C to break
    Reply from 1.1.2.2: bytes=56 Sequence=1 ttl=254 time=53 ms
      Record Route:
         1.1.2.1
         1.1.2.2
         1.1.1.2
         1.1.1.1
    Reply from 1.1.2.2: bytes=56 Sequence=2 ttl=254 time=1 ms
      Record Route:
         1.1.2.1
         1.1.2.2
         1.1.1.2
         1.1.1.1
    Reply from 1.1.2.2: bytes=56 Sequence=3 ttl=254 time=1 ms
      Record Route:
         1.1.2.1
         1.1.2.2
         1.1.1.2
         1.1.1.1
    Reply from 1.1.2.2: bytes=56 Sequence=4 ttl=254 time=1 ms
      Record Route:
```

```
        1.1.2.1
        1.1.2.2
        1.1.1.2
        1.1.1.1
  Reply from 1.1.2.2: bytes=56 Sequence=5 ttl=254 time=1 ms
    Record Route:
        1.1.2.1
        1.1.2.2
        1.1.1.2
        1.1.1.1
--- 1.1.2.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/11/53 ms
```

ping -r的原理如 图 1-1 所示：

(1) 源端（Device A）发送 RR 选项（ICMP 报文中的一个字段）为空的 ICMP 回显请求给目的端（Device C）。

(2) 中间设备（Device B）将自己出接口的 IP 地址（1.1.2.1）添加到 ICMP 回显请求报文的 RR 选项中，并转发该报文。

(3) 目的端收到请求报文后，发送 ICMP 回显响应报文，响应报文会拷贝请求报文的 RR 选项，并将自己出接口的 IP 地址（1.1.2.2）添加到 RR 选项中。

(4) 中间设备（Device B）将自己出接口的 IP 地址（1.1.1.2）添加到 RR 选项中，并转发该报文。

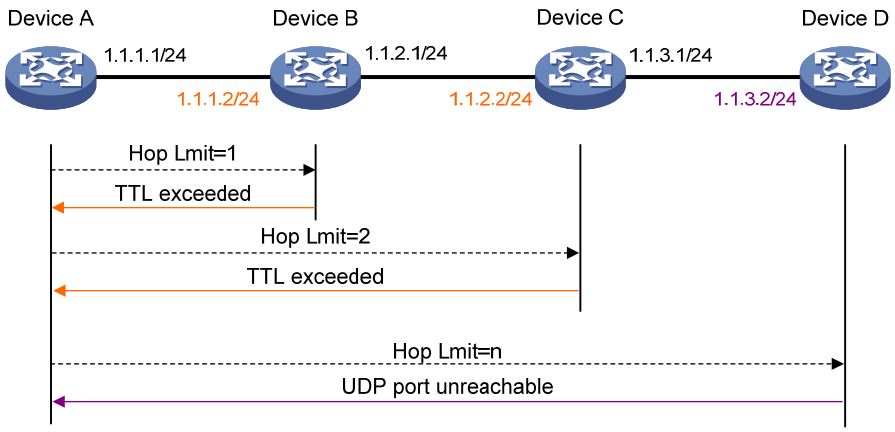
(5) 源端收到 ICMP 回显响应报文，将自己入接口的 IP 地址（1.1.1.1）添加到 RR 选项中。最后得到，Device A 到 Device C 具体路由为 1.1.1.1 <-> {1.1.1.2; 1.1.2.1} <-> 1.1.2.2。

1.2 Tracert功能

1.2.1 Tracert功能简介

通过使用 **tracert** 命令，用户可以查看 IP 报文从源端到达目的端所经过的三层设备，从而检查网络连接是否可用。当网络出现故障时，用户可以使用该命令分析出现故障的网络节点。

图1-2 Tracert 原理示意图



Tracert功能也是基于ICMP协议来实现的，如 图 1-2 所示，Tracert功能的原理为：

(1) 源端（Device A）向目的端（Device D）发送一个 IP 数据报文，TTL 值为 1，报文的 UDP 端口号是目的端的任何一个应用程序都不可能使用的端口号；

(2) 第一跳（Device B）（即该报文所到达的第一个三层设备）回应一个 TTL 超时的 ICMP 错误信息（该报文中含有第一跳的 IP 地址 1.1.1.2），这样源端就得到了第一个三层设备的地址（1.1.1.2）；

(3) 源端重新向目的端发送一个 IP 数据报文，TTL 值为 2；

(4) 第二跳（Device C）回应一个 TTL 超时的 ICMP 错误信息，这样源端就得到了第二个三层设备的地址（1.1.2.2）；

(5) 以上过程不断进行，直到该报文到达目的端，因目的端没有应用程序使用该 UDP 端口，目的端返回一个端口不可达的 ICMP 错误消息（携带了目的端的 IP 地址 1.1.3.2）。

(6) 当源端收到这个端口不可达的 ICMP 错误消息后，就知道报文已经到达了目的端，从而得到数据报文从源端到目的端所经历的路径（1.1.1.2；1.1.2.2；1.1.3.2）。

1.2.2 Tracert配置

1. 配置准备

IPv4 网络环境：

- 需要在中间设备（源端与目的端之间的设备）上开启 ICMP 超时报文发送功能。如果中间设备是 H3C 设备，需要在设备上执行 **ip ttl-expires enable** 命令（该命令的详细介绍请参见“三层技术-IP 业务命令参考”中的“IP 性能优化”）。
- 需要在目的端开启 ICMP 目的不可达报文发送功能。如果目的端是 H3C 设备，需要在设备上执行 **ip unreachables enable** 命令（该命令的详细介绍请参见“三层技术-IP 业务命令参考”中的“IP 性能优化”）。
- 如果源端到目的端路中途经 MPLS 网络，并且在 Tracert 过程中需要显示 MPLS 信息时，还需要在源端和中间设备上使能 ICMP 携带扩展信息功能。如果源端和中间设备是 H3C 设备，需要在设备上执行 **ip icmp-extensions compliant** 命令（该命令的详细介绍请参见“三层技术-IP 业务命令参考”中的“IP 性能优化”）。

IPv6 网络环境：

- 需要在中间设备（源端与目的端之间的设备）上开启设备的 ICMPv6 超时报文的发送功能。如果中间设备是 H3C 设备，需要在设备上执行 **ipv6 hoplimit-expires enable** 命令（该命令的详细介绍请参见“三层技术-IP 业务命令参考”中的“IPv6 基础”）。
- 需要在目的端开启设备的 ICMPv6 目的不可达报文的发送功能。如果目的端是 H3C 设备，需要在设备上执行 **ipv6 unreachables enable** 命令（该命令的详细介绍请参见“三层技术-IP 业务命令参考”中的“IPv6 基础”）。

2. Tracert配置

表1-2 Tracert 配置

操作	命令	说明
查看源端到目的端的路由	**tracert** [**-a** *source-ip* | **-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-tos** *tos* | **-vpn-instance** *vpn-instance-name* | **-w** *timeout*] * *host*	三者必选其一 • **tracert** 命令用于 IPv4 网络环境 • **tracert ipv6** 命令用于 IPv6 网络环境 • **tracert lsp** 命令用于 MPLS 网络环境 三条命令均可在任意视图下执行 S5500-28SC-HI 和 S5500-52SC-HI 不支持 **tracert lsp**命令
	tracert ipv6 [**-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-tos** *tos* | **-vpn-instance** *vpn-instance-name* | **-w** *timeout*] * *host*	
	tracert lsp [**-a** *source-ip* | **-exp** *exp-value* | **-h** *ttl-value* | **-r** *reply-mode* |**-t** *time-out*] * **ipv4** *dest-addr* *mask-length* [*destination-ip-addr-header*]	

说明

tracert lsp 命令的详细介绍请参见“MPLS 命令参考”中的“MPLS 基本配置”。

1.3 系统调试功能

1.3.1 系统调试功能简介

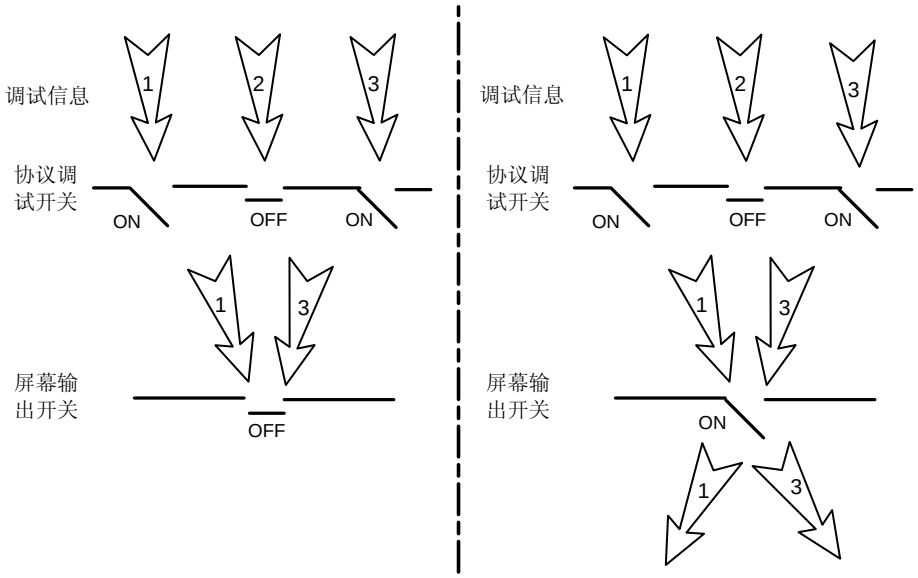
设备提供了种类丰富的调试功能，对于设备所支持的绝大部分协议和功能，系统都提供了相应的调试信息，帮助用户对错误进行诊断和定位。

调试信息的输出可以由两个开关控制：

- 协议调试开关，控制是否生成某协议的调试信息。
- 屏幕输出开关，控制是否在某个用户屏幕上显示调试信息。

如 图 1-3 所示：假设设备可以为 1、2、3 三个模块提供调试信息，用户只有将两个开关都打开，调试信息才会在终端显示出来。

图1-3 系统调试开关关系图



1.3.2 系统调试配置

因为调试信息的生成、输出会影响系统的运行效率，所以，本功能一般在维护人员进行网络故障诊断时使用。调试结束后，请及时关闭相应的调试开关，或者使用 **undo debugging all** 命令，关闭所有模块的调试开关。

调试信息的输出与各协议/功能模块的 **debugging** 命令以及信息中心的配置有关。在访问终端（包括 Console 控制台和 VTY 访问终端）上显示是最常用的调试信息输出方式，用户还可以将调试信息发送到别的输出方向，具体配置请参见“网络管理和监控配置指导”中的“信息中心”。使用以下配置步骤，可以将调试信息输出到访问终端。

表1-3 系统调试操作

操作	命令	说明
开启终端对系统信息的监视功能	**terminal monitor**	可选 缺省情况下，控制台的监视功能处于开启状态，监视终端的监视功能处于关闭状态 该操作在用户视图下执行
开启终端对调试信息的显示功能	**terminal debugging**	必选 缺省情况下，控制台对调试信息的显示功能处于关闭状态 该操作在用户视图下执行
打开系统中指定模块的调试开关	**debugging** *module-name* [*option*]	必选 缺省情况下，所有功能项的调试开关均处于关闭状态 该操作在用户视图下执行
显示系统中已经打开的调试开关	**display debugging** [**interface** *interface-type interface-number*] [*module-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	可选 该操作在任意视图下执行

说明

只有同时配置了 **debugging**、**terminal debugging** 和 **terminal monitor** 命令，才能在终端显示调试信息的具体内容。**terminal debugging** 和 **terminal monitor** 命令的详细介绍请参见“网络管理和监控命令参考”中的“信息中心”。

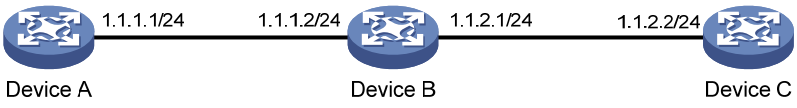
1.4 Ping和Tracert配置举例

1. 组网需求

Device A 使用 Telnet 登录 Device C 失败，现需要确认 Device A 与 Device C 之间是否路由可达，如果路由不可达，需要确定故障的网络节点。

2. 组网图

图1-4 Ping 和 Tracert 应用组网图



3. 配置步骤

(1) 使用 **ping** 命令查看 Device A 和 Device C 之间路由是否可达。

```
<DeviceA> ping 1.1.2.2
  PING 1.1.2.2: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
```

```
  --- 1.1.2.2 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

(2) 路由不可达，使用 **tracert** 命令确定故障的网络节点。

- # 在 Device B 上开启 ICMP 超时报文发送功能。

```
<DeviceB> system-view
[DeviceB] ip ttl-expires enable
```

- # 在 Device C 上开启 ICMP 目的不可达报文发送功能。

```
<DeviceC> system-view
[DeviceC] ip unreachables enable
```

- # 在 Device A 上使用 **tracert** 命令确定故障的网络节点。

```
<DeviceA> tracert 1.1.2.2
 traceroute to 1.1.2.2(1.1.2.2) 30 hops max,40 bytes packet, press CTRL_C to break
 1  1.1.1.2 14 ms 10 ms 20 ms
 2  * * *
 3  * * *
 4  * * *
 5
<DeviceA>
```

从上面结果可以看出，Device A 和 Device C 之间路由不可达，Device A 和 Device B 之间路由可达，Device B 和 Device C 之间的连接出了问题。此时可以在 Device A 和 Device C 上使用 **debugging ip icmp** 命令打开 ICMP 报文的调试开关，查看设备有没有收发指定的 ICMP 报文。或者使用 **display ip routing-table** 查看有没有到对端的路由。

目 录

1 NTP配置

说明

本文中的三层以太网端口是指工作模式被配置成三层模式的以太网端口，有关以太网端口工作模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口配置”部分。

1.1 NTP简介

NTP（Network Time Protocol，网络时间协议）是由 RFC 1305 定义的时间同步协议，用来在分布式时间服务器和客户端之间进行时间同步。NTP 基于 UDP 报文进行传输，使用的 UDP 端口号为 123。

使用 NTP 的目的是对网络内所有具有时钟的设备进行时钟同步，使网络内所有设备的时钟保持一致，从而使设备能够提供基于统一时间的多种应用。

对于运行 NTP 的本地系统，既可以接受来自其他时钟源的同步，又可以作为时钟源同步其他的时钟，并且可以和其他设备互相同步。

1.1.1 NTP的应用

对于网络中的各台设备来说，如果依靠管理员手工输入命令来修改系统时钟是不可能的，不但工作量巨大，而且也不能保证时钟的精确性。通过 NTP，可以很快将网络中设备的时钟同步，同时也能保证很高的精度。

NTP 主要应用于需要网络中所有设备时钟保持一致的场合，比如：

- 在网络管理中，对于从不同设备采集来的日志信息、调试信息进行分析的时候，需要以时间作为参照依据。
- 计费系统要求所有设备的时钟保持一致。
- 完成某些功能，如定时重启网络中的所有设备，此时要求所有设备的时钟保持一致。
- 多个系统协同处理同一个比较复杂的事件时，为保证正确的执行顺序，多个系统必须参考同一时钟。
- 在备份服务器和客户端之间进行增量备份时，要求备份服务器和所有客户端之间的时钟同步。

NTP 的优势如下：

- 采用分层的方法定义时钟的准确性，可以迅速同步网络中各台设备的时间。
- 支持访问控制和 MD5 验证。
- 可以选择采用单播、组播或广播的方式发送协议报文。

说明

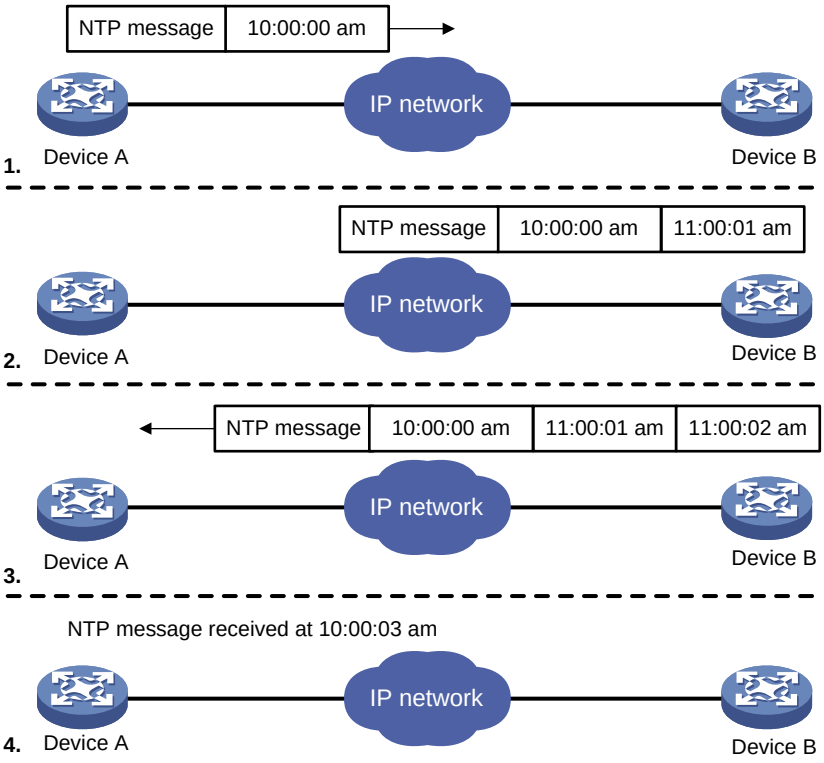
- 时钟的层数决定了时钟的准确度，其取值范围为 1～16。参考时钟的层数取值范围为 1～15，准确度从 1 到 15 依次递减，层数为 16 的时钟处于未同步状态。
- 本系列交换机不支持设置本地时钟为参考时钟，只有当其时钟被同步后，才能作为时钟源去同步其它设备。

1.1.2 NTP工作原理

NTP的基本工作原理如 图 1-1 所示。Device A和Device B通过网络相连，它们都有自己独立的系统时钟，需要通过NTP实现各自系统时钟的自动同步。为便于理解，作如下假设：

- 在 Device A 和 Device B 的系统时钟同步之前，Device A 的时钟设定为 10:00:00am，Device B 的时钟设定为 11:00:00am。
- Device B 作为 NTP 时间服务器，即 Device A 将使自己的时钟与 Device B 的时钟同步。
- NTP 报文在 Device A 和 Device B 之间单向传输所需要的时间为 1 秒。

图1-1 NTP 基本原理图



系统时钟同步的工作过程如下：

- Device A 发送一个 NTP 报文给 Device B，该报文带有它离开 Device A 时的时间戳，该时间戳为 10:00:00am（T_1）。
- 当此 NTP 报文到达 Device B 时，Device B 加上自己的时间戳，该时间戳为 11:00:01am（T_2）。
- 当此 NTP 报文离开 Device B 时，Device B 再加上自己的时间戳，该时间戳为 11:00:02am（T_3）。
- 当 Device A 接收到该响应报文时，Device A 的本地时间为 10:00:03am（T_4）。

至此，Device A 已经拥有足够的信息来计算两个重要的参数：

- NTP 报文的往返时延 Delay=（T_4-T_1）-（T_3-T_2）=2 秒。
- Device A 相对 Device B 的时间差 offset=（（T_2-T_1）+（T_3-T_4））/2=1 小时。

这样，Device A 就能够根据这些信息来设定自己的时钟，使之与 Device B 的时钟同步。

以上内容只是对 NTP 工作原理的一个粗略描述，详细内容请参阅 RFC 1305。

1.1.3 NTP的报文格式

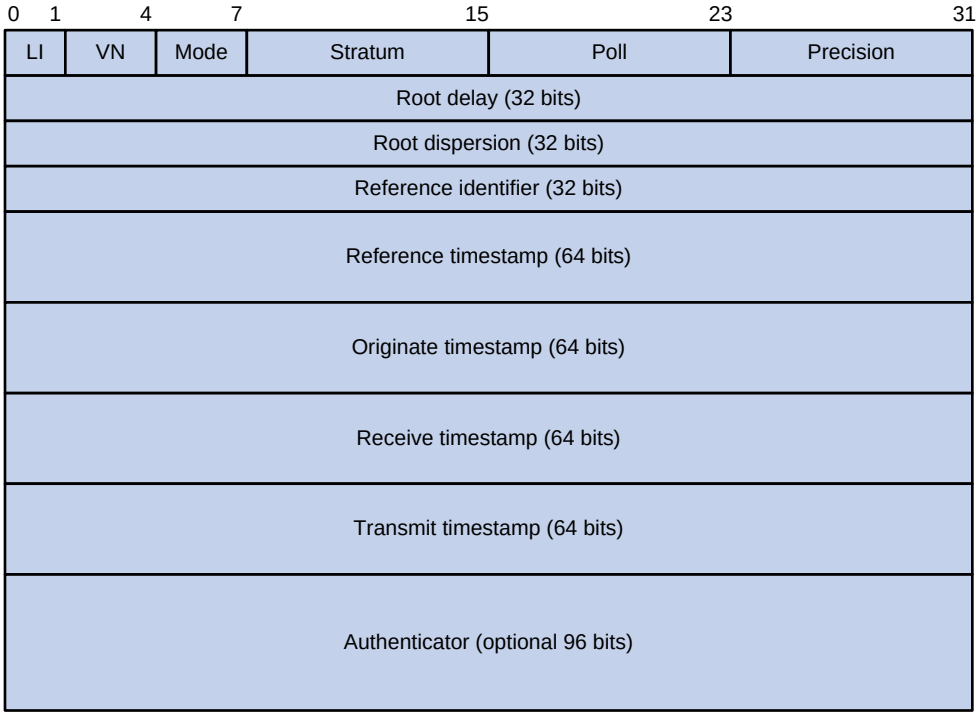
NTP 有两种不同类型的报文，一种是时钟同步报文，另一种是控制报文。控制报文仅用于需要网络管理的场合，它对于时钟同步功能来说并不是必需的，这里不做介绍。

说明

本文中提到的 NTP 报文，均为 NTP 时钟同步报文。

时钟同步报文封装在UDP报文中，其格式如 图 1-2 所示。

图1-2 时钟同步报文格式



主要字段的解释如下：

- LI（Leap Indicator，闰秒提示）：长度为 2 比特，值为“11”时表示告警状态，时钟未被同步。为其他值时 NTP 本身不做处理。
- VN（Version Number，版本号）：长度为 3 比特，表示 NTP 的版本号，目前的最新版本为 4。
- Mode：长度为 3 比特，表示 NTP 的工作模式。不同的值所表示的含义分别是：0 未定义、1 表示主动对等体模式、2 表示被动对等体模式、3 表示客户模式、4 表示服务器模式、5 表示广播模式或组播模式、6 表示此报文为 NTP 控制报文、7 预留给内部使用。
- Stratum：系统时钟的层数，取值范围为 1～16，它定义了时钟的准确度。层数为 1 的时钟准确度最高，准确度从 1 到 16 依次递减，层数为 16 的时钟处于未同步状态。
- Poll：轮询时间，即两个连续 NTP 报文之间的时间间隔。
- Precision：系统时钟的精度。
- Root Delay：本地到主参考时钟源的往返时间。
- Root Dispersion：系统时钟相对于主参考时钟的最大误差。
- Reference Identifier：参考时钟源的标识。
- Reference Timestamp：系统时钟最后一次被设定或更新的时间。
- Originate Timestamp：NTP 请求报文离开发送端时发送端的本地时间。

- Receive Timestamp：NTP 请求报文到达接收端时接收端的本地时间。
- Transmit Timestamp：应答报文离开应答者时应答者的本地时间。
- Authenticator：验证信息。

1.1.4 NTP的工作模式

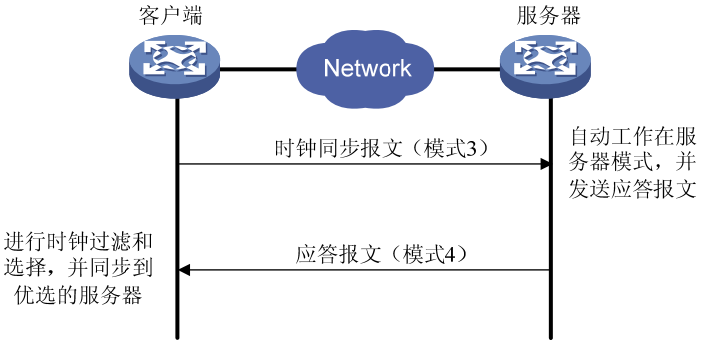
设备可以采用多种 NTP 工作模式进行时间同步：

- 客户端/服务器模式
- 对等体模式
- 广播模式
- 组播模式

用户可以根据需要选择合适的工作模式。在不能确定服务器或对等体 IP 地址、网络中需要同步的设备很多等情况下，可以通过广播或组播模式实现时钟同步；客户端/服务器和对等体模式中，设备从指定的服务器或对等体获得时钟同步，增加了时钟的可靠性。

1. 客户端/服务器模式

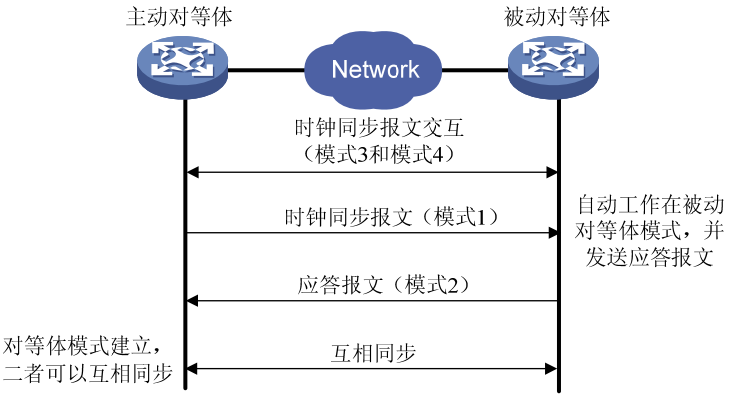
图1-3 客户端/服务器模式



在客户端/服务器模式中，客户端向服务器发送时钟同步报文，报文中的 Mode 字段设置为 3（客户模式）。服务器端收到报文后会自动工作在服务器模式，并发送应答报文，报文中的 Mode 字段设置为 4（服务器模式）。客户端收到应答报文后，进行时钟过滤和选择，并同步到优选的服务器。在该模式下，客户端能同步到服务器，而服务器无法同步到客户端。

2. 对等体模式

图1-4 对等体模式

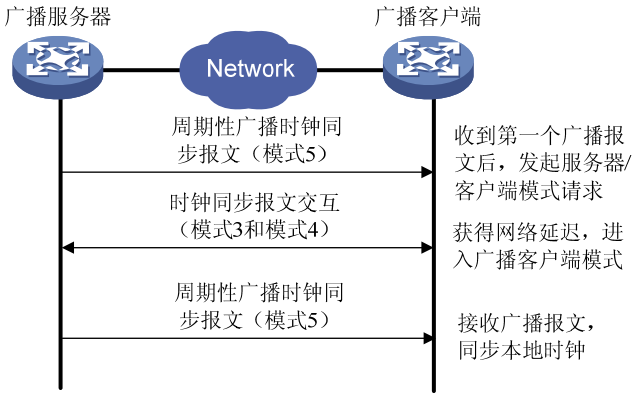


在对等体模式中，主动对等体和被动对等体之间首先交互 Mode 字段为 3（客户端模式）和 4（服务器模式）的 NTP 报文。之后，主动对等体向被动对等体发送时钟同步报文，报文中的 Mode 字

段设置为 1（主动对等体），被动对等体收到报文后自动工作在被动对等体模式，并发送应答报文，报文中的 Mode 字段设置为 2（被动对等体）。经过报文的交互，对等体模式建立起来。主动对等体和被动对等体可以互相同步。如果双方的时钟都已经同步，则以层数小的时钟为准。

3. 广播模式

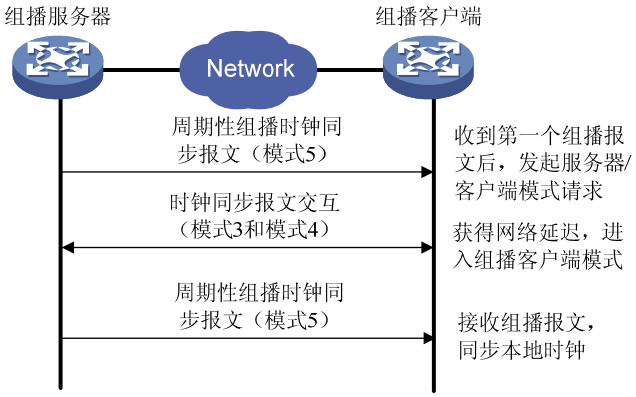
图1-5 广播模式



在广播模式中，服务器端周期性地向广播地址 255.255.255.255 发送时钟同步报文，报文中的 Mode 字段设置为 5（广播模式）。客户端侦听来自服务器的广播报文。当客户端接收到第一个广播报文后，客户端与服务器交互 Mode 字段为 3（客户模式）和 4（服务器模式）的 NTP 报文，以获得客户端与服务器间的网络延迟。之后，客户端就进入广播客户端模式，继续侦听广播报文的到来，根据到来的广播报文对系统时钟进行同步。

4. 组播模式

图1-6 组播模式



在组播模式中，服务器端周期性地向用户配置的组播地址（若用户没有配置组播地址，则使用默认的 NTP 组播地址 224.0.1.1）发送时钟同步报文，报文中的 Mode 字段设置为 5（组播模式）。客户端侦听来自服务器的组播报文。当客户端接收到第一个组播报文后，客户端与服务器交互 Mode 字段为 3（客户模式）和 4（服务器模式）的 NTP 报文，以获得客户端与服务器间的网络延迟。之后，客户端就进入组播客户端模式，继续侦听组播报文的到来，根据到来的组播报文对系统时钟进行同步。

说明

在对等体模式、广播模式和组播模式中，客户端（或主动对等体）和服务器（或被动对等体）之间首先要交互 Mode 字段为 3（客户端模式）和 4（服务器模式）的 NTP 报文，之后，才能进入指定的 NTP 工作模式。在此报文交互过程中，可以实现时钟的同步。

1.1.5 NTP支持MPLS L3VPN

NTP 工作在客户端/服务器模式和对等体模式时支持 MPLS L3VPN，可以实现 MPLS VPN 网络的时间同步，即物理位置不同的网络设备（CE、PE），只要属于同一个 VPN，就可以通过 NTP 来获得时间同步。具体功能如下：

- CE 上的 NTP 客户端可以同步到另一个 CE 上的 NTP 服务器；
- CE 上的 NTP 客户端可以同步到 PE 上的 NTP 服务器；
- PE 上的 NTP 客户端可以通过指定的 VPN 同步到 CE 上的 NTP 服务器；
- PE 上的 NTP 客户端可以通过指定的 VPN 同步到另一个 PE 上的 NTP 服务器；
- PE 上的 NTP 服务器可以同步不同 VPN 内多个 CE 上的 NTP 客户端。

说明

- CE（Customer Edge）设备：用户网络边缘设备，有接口直接与服务提供商（Service Provider，SP）相连。CE“感知”不到 VPN 的存在。
- PE（Provider Edge）设备：服务提供商网络的边缘设备，与用户的 CE 直接相连。
- S5500-28SC-HI 和 S5500-52SC-HI 交换机仅支持作为 CE 设备。

1.2 NTP配置任务简介

表1-1 NTP 配置任务简介

配置任务	说明	详细配置
配置NTP工作模式	必选	1.3
配置NTP可选参数	可选	1.4
配置访问控制权限	可选	1.5
配置NTP验证功能	可选	1.6

1.3 配置NTP工作模式

设备可以采用以下 NTP 工作模式进行时钟同步：

- 客户端/服务器模式
- 对等体模式
- 广播模式
- 组播模式

设备采用客户端/服务器模式或对等体模式时，只需要对客户端或主动对等体进行配置；设备采用广播模式或组播模式时，则需要在服务器端和客户端都进行配置。

说明

同一设备同一时间内存在的连接数目最多为 128 个，其中包括静态连接数和动态连接数。静态连接是用户手动配置 NTP 相关命令而建立的连接；动态连接是系统运行过程中建立的临时连接，若系统长期收不到报文就会删除该临时连接。例如，在客户端/服务器模式中，当用户在客户端配置向服务器端同步的命令的时候，系统会在客户端建立一个静态连接，服务器端在收到报文之后只是被动的响应报文，而不会建立连接（包括静态和动态连接）；在对等体模式中，主动对等体端会建立静态连接，被动对等体端会建立动态连接；在组播和广播模式中，服务器端会建立静态连接，而在客户端会建立动态连接。

1.3.1 配置NTP客户端/服务器模式

当设备采用客户端/服务器模式时，请在客户端进行如下配置。

表1-2 在 NTP 客户端上指定 NTP 服务器

操作	命令	说明
进入系统视图	**system-view**	-
指定设备的NTP服务器	**ntp-service unicast-server** [**vpn-instance** *vpn-instance-name*] { *ip-address* | *server-name* } [**authentication-keyid** *keyid* | **priority** | **source-interface** *interface-type interface-number* | **version** *number*] *	必选 缺省情况下，没有为设备指定NTP服务器

说明

- **ntp-service unicast-server** 命令中的 *ip-address* 是一个单播地址，不能为广播地址、组播地址或本地时钟的 IP 地址。
- 通过 **source-interface** 参数指定 NTP 报文的源接口后，NTP 报文的源 IP 地址将被设置为指定接口的主 IP 地址。
- 服务器端只有当其时钟被同步后，才能作为时间服务器去同步其他设备。当服务器端的时钟层数大于或等于客户端的时钟层数时，客户端将不会向其同步。
- 可以通过多次执行 **ntp-service unicast-server** 命令配置多个服务器，客户端依据时钟优选来选择最优的时钟源。

1.3.2 配置NTP对等体模式

当设备采用对等体模式时，需要在主动对等体上指定被动对等体。

表1-3 在主动对等体上指定被动对等体

操作	命令	说明
进入系统视图	**system-view**	-
指定设备的被动对等体	**ntp-service unicast-peer** [**vpn-instance** *vpn-instance-name*] { *ip-address* | *peer-name* } [**authentication-keyid** *keyid* | **priority** | **source-interface** *interface-type interface-number* | **version** *number*] *	必选 缺省情况下，没有为设备指定被动对等体

说明

- 在对等体模式中，被动对等体上需要执行“1.3 配置NTP工作模式”中的任何一条NTP配置命令来使能NTP，否则被动对等体不会处理来自主动对等体的NTP报文。
- **ntp-service unicast-peer** 命令中的 *ip-address* 是一个单播地址，不能为广播地址、组播地址或本地时钟的 IP 地址。
- 通过 **source-interface** 参数指定 NTP 报文的源接口后，NTP 报文的源 IP 地址将被设置为指定接口的主 IP 地址。
- 通常，主、被动对等体中至少有一个处于同步状态，否则他们将都无法同步。
- 可以通过多次执行 **ntp-service unicast-peer** 命令配置多个被动对等体。

1.3.3 配置NTP广播模式

广播服务器周期性地向广播地址 255.255.255.255 发送 NTP 报文，工作在 NTP 广播客户端模式的设备将回应这个报文，从而开始时钟同步过程。

当设备采用广播模式时，需要在服务器端和客户端都进行配置。由于广播服务器上需要指定一个发送 NTP 广播报文的接口，广播客户端上也需要指定一个接收 NTP 广播报文的接口，所以广播模式的配置只能在具体的接口视图下进行。

1. 配置广播客户端

表1-4 配置广播客户端

操作	命令	说明
进入系统视图	**system-view**	-
进入三层以太网端口视图或者VLAN接口视图	**interface** *interface-type interface-number*	- 进入要接收NTP广播报文的三层以太网端口或者VLAN接口
配置设备工作在NTP广播客户端模式	**ntp-service broadcast-client**	必选

2. 配置广播服务器

表1-5 配置广播服务器

操作	命令	说明
进入系统视图	**system-view**	-
进入三层以太网端口视图或者VLAN接口视图	**interface** *interface-type interface-number*	- 进入要发送NTP广播报文的三层以太网端口或者VLAN接口
配置设备工作在NTP广播服务器模式	**ntp-service broadcast-server** [**authentication-keyid** *keyid* | **version** *number*] *	必选

说明

广播服务器只有当其时钟同步后，才能去同步广播客户端。

1.3.4 配置NTP组播模式

NTP 组播服务器以组播形式周期性地发送时钟同步报文，工作在 NTP 组播客户端模式的设备将回应这个报文，从而开始时钟同步过程。

设备采用组播模式时，需要在服务器端和客户端都进行配置。组播模式的配置只能在具体的接口视图下进行。

1. 配置组播客户端

表1-6 配置组播客户端

操作	命令	说明
进入系统视图	**system-view**	-
进入三层以太网端口视图或者VLAN接口视图	**interface** *interface-type interface-number*	- 进入要接收NTP组播报文的三层以太网端口或者VLAN接口
配置设备工作在NTP组播客户端模式	**ntp-service multicast-client** [*ip-address*]	必选

2. 配置组播服务器

表1-7 配置组播服务器

操作	命令	说明
进入系统视图	**system-view**	-
进入三层以太网端口视图或者VLAN接口视图	**interface** *interface-type interface-number*	- 进入要发送NTP组播报文的三层以太网端口或者VLAN接口
配置设备工作在NTP组播服务器模式	**ntp-service multicast-server** [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*] *	必选

说明

- 组播服务器只有当其时钟同步后，才能去同步组播客户端。
- 目前最多可以配置 1024 个组播客户端，但同时起作用的最多为 128 个。

1.4 配置NTP可选参数

1.4.1 配置NTP报文的源接口

如果指定了 NTP 报文的源接口，则设备在主动发送 NTP 报文时，将报文的源 IP 地址设置为指定接口的主 IP 地址。建议将 Loopback 接口指定为源接口，以避免设备上某个接口的状态变化而导致 NTP 报文无法接收。

设备对接收到的 NTP 请求报文进行应答时，应答报文的源 IP 地址始终为接收到 NTP 请求报文的目的地址。

表1-8 配置 NTP 报文的源接口

操作	命令	说明
进入系统视图	**system-view**	-
配置NTP报文的源接口	**ntp-service source-interface** *interface-type interface-number*	必选 缺省情况下，没有指定NTP报文的源接口，即根据路由选择NTP报文的源IP地址

注意

- 如果在命令 **ntp-service unicast-server** 或 **ntp-service unicast-peer** 中指定了 NTP 报文的源接口，则以 **ntp-service unicast-server** 或 **ntp-service unicast-peer** 指定的为准。
- 如果在接口视图下配置了 **ntp-service broadcast-server** 或 **ntp-service multicast-server**，则 NTP 广播或组播模式报文的源接口为配置了上述命令的接口。

1.4.2 配置禁止接口接收NTP报文

使能 NTP 功能后，缺省情况下所有接口都可以接收 NTP 报文。可以通过本配置，禁止从某个接口接收 NTP 报文。

表1-9 配置禁止接口接收 NTP 报文

操作	命令	说明
进入系统视图	**system-view**	-
进入三层以太网端口视图或者VLAN接口视图	**interface** *interface-type interface-number*	-
配置禁止接口接收NTP报文	**ntp-service in-interface disable**	必选 缺省情况下，允许接口接收NTP报文

1.4.3 配置允许建立的动态会话数目

表1-10 配置允许建立的动态会话数目

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
配置允许建立的动态NTP会话数目	**ntp-service max-dynamic-sessions** *number*	必选 缺省情况下，允许建立的动态NTP会话的数目为100

1.4.4 配置NTP报文的DSCP优先级

表1-11 配置 NTP 报文的 DSCP 优先级

操作	命令	说明
进入系统视图	**system-view**	-
配置NTP报文的DSCP优先级	**ntp-service dscp** *dscp-value*	可选 缺省情况下，NTP报文的DSCP优先级为16

1.5 配置访问控制权限

用户可以配置对本地设备 NTP 服务的访问控制权限。访问控制权限可以分为四种：

- **query**：允许控制查询权限。该权限只允许对端设备对本地设备的 NTP 服务进行控制查询，但是不能向本地设备同步。所谓的控制查询，就是查询 NTP 的一些状态，比如告警信息，验证状态，时钟源信息等。
- **synchronization**：只允许服务器访问权限。该权限只允许对端设备向本地设备同步，但不能进行控制查询。
- **server**：允许服务器访问与查询权限。该权限允许对端设备向本地设备同步和控制查询，但本地设备不会同步到对端设备。
- **peer**：完全访问权限。该权限既允许对端设备向本地设备同步和控制查询，同时本地设备也可以同步到对端设备。

NTP 服务的访问控制权限从高到低依次为 **peer**、**server**、**synchronization**、**query**。当设备接收到 NTP 服务请求报文时，会按照此顺序进行匹配，以第一个匹配的权限为准。如果没有匹配任何权限，则丢弃此 NTP 服务请求报文。

1.5.1 配置准备

在配置对本地设备 NTP 服务的访问控制权限之前，需要创建并配置与访问权限关联的 ACL。ACL 的配置方法请参见“ACL 和 QoS 配置指导”中的“ACL”。

1.5.2 配置访问控制权限

表1-12 配置对本地设备 NTP 服务的访问控制权限

操作	命令	说明
进入系统视图	**system-view**	-
配置对端设备对本地设备NTP服务的访问控制权限	**ntp-service access** { **peer** | **query** | **server** | **synchronization** } *acl-number*	必选 缺省情况下，对端设备对本地设备NTP服务的访问控制权限为**peer**

说明

配置对本地设备 NTP 服务的访问控制权限，仅提供了一种最小限度的安全措施，更安全的方法是进行身份验证。

1.6 配置NTP验证功能

在一些对安全性要求较高的网络中，运行 NTP 协议时需要启用验证功能。通过客户端和服务器端的密码验证，保证客户端只与通过验证的设备进行同步，提高了网络安全性。

1.6.1 配置准备

配置 NTP 验证功能可以分为配置客户端的 NTP 验证和配置服务器端的 NTP 验证两个部分。

在配置 NTP 验证功能时，应注意以下原则：

- 对于所有同步模式，如果使能了 NTP 验证功能，应同时配置验证密钥并将密钥设为可信密钥，即如果执行了 **ntp-service authentication enable** 命令，则必须同时执行 **ntp-service authentication-keyid** 命令和 **ntp-service reliable authentication-keyid** 命令。否则，无法正常启用 NTP 验证功能。
- 对于客户端/服务器模式和对等体模式，还应在客户端（对等体模式中的主动对等体）将指定密钥与对应的 NTP 服务器（对等体模式的被动对等体）关联；对于广播服务器模式和组播服务器模式，应在广播服务器或组播服务器上将指定密钥与对应的 NTP 服务器关联。否则，无法正常启用 NTP 验证功能。
- 对于客户端/服务器同步模式，如果客户端没有成功启用 NTP 验证功能，不论服务器端是否使能 NTP 验证，客户端均可以与服务器端同步；如果客户端上成功启用了 NTP 验证功能，则客户端只会同步到提供可信密钥的服务器，如果服务器提供的密钥不是可信的密钥，那么客户端不会与其同步。
- 对于所有同步模式，服务器端的配置与客户端的配置应保持一致。

1.6.2 配置过程

1. 配置客户端的NTP验证

表1-13 配置客户端的 NTP 验证

操作	命令	说明
进入系统视图	**system-view**	-
使能NTP身份验证功能	**ntp-service authentication enable**	必选 缺省情况下，NTP身份验证功能处于关闭状态
配置NTP验证密钥	**ntp-service authentication-keyid** *keyid* **authentication-mode md5** [**cipher** | **simple**] *value*	必选 缺省情况下，没有配置NTP验证密钥
配置指定密钥为可信密钥	**ntp-service reliable authentication-keyid** *keyid*	必选 缺省情况下，没有指定可信密钥

操作	命令	说明
将指定密钥与对应的NTP服务器关联	客户端/服务器模式： **ntp-service unicast-server** { *ip-address* | *server-name* } **authentication-keyid** *keyid*	必选 可以将不存在的密钥与NTP服务器关联。但是若想成功启用NTP验证功能，则必须在关联密钥后，配置该密钥，并将其指定为可信密钥
	对等体模式： **ntp-service unicast-peer** { *ip-address* | *peer-name* } **authentication-keyid** *keyid*	

说明

客户端使能 NTP 验证功能后，必须配置与服务器端相同的验证密钥，并且必须声明该密钥是可信的，否则无法与服务器同步。

2. 配置服务器端的NTP验证

表1-14 配置服务器端的 NTP 验证

操作	命令	说明
进入系统视图	**system-view**	-
使能NTP验证功能	**ntp-service authentication enable**	必选 缺省情况下，NTP身份验证功能处于关闭状态
配置NTP验证密钥	**ntp-service authentication-keyid** *keyid* **authentication-mode md5** [**cipher** | **simple**] *value*	必选 缺省情况下，没有配置NTP验证密钥
配置指定密钥为可信密钥	**ntp-service reliable authentication-keyid** *keyid*	必选 缺省情况下，没有指定可信密钥
进入三层以太网端口视图或者VLAN接口视图	**interface** *interface-type interface-number*	-
将指定密钥与对应的NTP服务器关联	广播服务器模式： **ntp-service broadcast-server authentication-keyid** *keyid*	必选 可以将不存在的密钥与NTP服务器关联。但是若想成功启用NTP验证功能，则必须在关联密钥后，配置该密钥，并将其指定为可信密钥
	组播服务器模式： **ntp-service multicast-server authentication-keyid** *keyid*	

说明

服务器端的 NTP 验证配置步骤与客户端的相同，并且两端必须配置相同的密钥。

1.7 NTP显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 NTP 的运行情况，通过查看显示信息验证配置的效果。

表1-15 NTP 显示与维护

操作	命令
显示NTP服务的状态信息	**display ntp-service status** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示NTP服务维护的会话信息	**display ntp-service sessions** [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示从本地设备回溯到主参考时钟源的各个NTP时间服务器的简要信息	**display ntp-service trace** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.8 NTP典型配置举例

1.8.1 配置NTP客户端/服务器模式

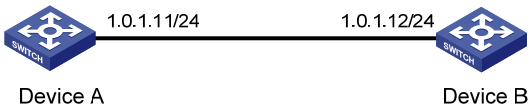
1. 组网需求

为了实现 Device B 的时钟与 Device A 的时钟同步，需要进行以下配置：

- 在 Device A 上设置本地时钟作为参考时钟，层数为 2；
- Device B 工作在客户端模式，指定 Device A 为 NTP 服务器。

2. 组网图

图1-7 配置 NTP 客户端/服务器模式组网图



3. 配置步骤

(1) 按照 图 1-7 配置各接口的IP地址，具体配置过程略。

(2) 配置 Device B

同步前查看 Device B 的 NTP 状态。

```
<DeviceB> display ntp-service status
 Clock status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
 Nominal frequency: 64.0000 Hz
 Actual frequency: 64.0000 Hz
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 0.00 ms
 Root dispersion: 0.00 ms
 Peer dispersion: 0.00 ms
 Reference time: 00:00:00.000 UTC Jan 1 1900 (00000000.00000000)
```

设置 Device A 为 Device B 的 NTP 服务器。

```
<DeviceB> system-view
[DeviceB] ntp-service unicast-server 1.0.1.11
```

以上配置将 Device B 向 Device A 进行时间同步，同步后查看 Device B 的 NTP 状态。

```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 1.0.1.11
 Nominal frequency: 64.0000 Hz
 Actual frequency: 64.0000 Hz
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 31.00 ms
 Root dispersion: 1.05 ms
 Peer dispersion: 7.81 ms
 Reference time: 14:53:27.371 UTC Jan 19 2011 (C6D94F67.5EF9DB22)
```

此时 Device B 已经与 Device A 同步，层数比 Device A 的层数大 1，为 3。

查看 Device B 的 NTP 会话信息，可以看到 Device B 与 Device A 建立了连接。

```
[DeviceB] display ntp-service sessions
      source      reference    stra  reach  poll  now  offset  delay  disper
**************************************************************************
[12345] 1.0.1.11  127.127.1.0    2    63    64    3    -75.5    31.0  16.5
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

1.8.2 配置NTP对等体模式

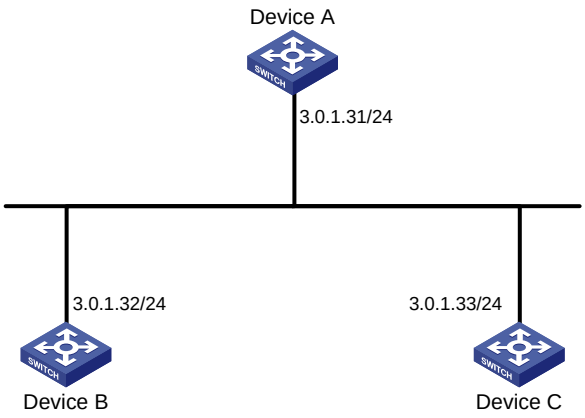
1. 组网需求

为了实现设备之间的时钟同步，需要进行以下配置：

- Device A 设置本地时钟作为参考时钟，层数为 2；
- Device B 工作在客户端模式，指定 Device A 为 NTP 服务器；
- Device B 向 Device A 同步后，配置 Device C 工作在对等体模式，将 Device B 设为对等体。Device C 为主动对等体，Device B 为被动对等体。

2. 组网图

图1-8 配置 NTP 对等体模式组网图



3. 配置步骤

(1) 配置各 VLAN 接口的 IP 地址，具体配置过程略。

(2) 配置 Device B

设置 Device A 为 Device B 的 NTP 服务器。

```
<DeviceB> system-view
[DeviceB] ntp-service unicast-server 3.0.1.31
```

(3) 查看 Device B 的状态（Device B 向 Device A 同步后）。

```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^18
 Clock offset: -21.1982 ms
 Root delay: 15.00 ms
 Root dispersion: 775.15 ms
 Peer dispersion: 34.29 ms
 Reference time: 15:22:47.083 UTC Jan 19 2011 (C6D95647.153F7CED)
```

此时 Device B 已经与 Device A 同步，层数比 Device A 的层数大 1，为 3。

(4) 配置 Device C（Device B 向 Device A 同步后）

本地同步后，设置 Device C 为主动对等体。

```
[DeviceC] ntp-service unicast-peer 3.0.1.32
```

以上配置将 Device B 和 Device C 配置为对等体，Device C 处于主动对等体模式，Device B 处于被动对等体模式，由于 Device C 系统时钟的层数为 16，而 Device B 的层数为 3，所以 Device C 向 Device B 同步。

(5) 同步后查看 Device C 的状态。

```
[DeviceC] display ntp-service status
 Clock status: synchronized
 Clock stratum: 4
 Reference clock ID: 3.0.1.32
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^18
 Clock offset: -21.1982 ms
 Root delay: 15.00 ms
 Root dispersion: 775.15 ms
 Peer dispersion: 34.29 ms
 Reference time: 15:22:47.083 UTC Jan 19 2011 (C6D95647.153F7CED)
```

此时 Device C 已经与 Device B 同步，层数比 Device B 的层数大 1，为 4。

查看 Device C 的 NTP 会话信息，可以看到 Device C 与 Device B 建立了连接。

```
[DeviceC] display ntp-service sessions
      source          reference       stra reach poll  now offset  delay disper
**************************************************************************
[12345] 3.0.1.32       3.0.1.31        3     3    64    16   -6.4    4.8    1.0
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

1.8.3 配置NTP广播模式

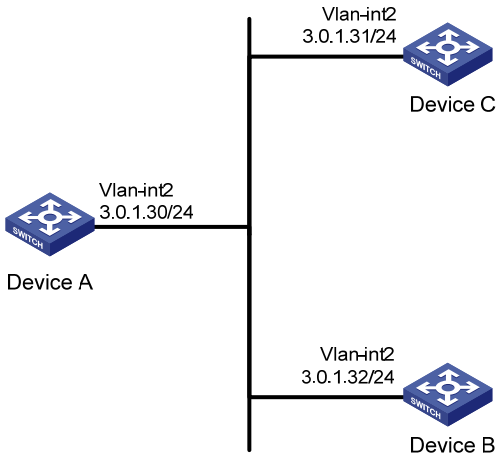
1. 组网需求

Device C 作为同一网段中多个设备的 NTP 服务器，同时同步多个设备的时钟。为了实现该需求，需要进行以下配置：

- 在 Device C 上设置本地时钟作为参考时钟，层数为 2；
- Device C 工作在广播服务器模式，从 VLAN 接口 2 向外发送广播报文；
- Device A 和 Device B 工作在广播客户端模式，分别从各自的 VLAN 接口 2 监听广播报文。

2. 组网图

图1-9 配置 NTP 广播模式组网图



3. 配置步骤

(1) 按照 图 1-9 配置各接口的IP地址，具体配置过程略。

(2) 配置 Device C

设置 Device C 为广播服务器，从 VLAN 接口 2 发送广播报文。

```
[DeviceC] interface vlan-interface 2
[DeviceC-Vlan-interface2] ntp-service broadcast-server
```

(3) 配置 Device A

设置 Device A 为广播客户端，从 VLAN 接口 2 监听广播报文。

```
<DeviceA> system-view
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ntp-service broadcast-client
```

(4) 配置 Device B

设置 Device B 为广播客户端，从 VLAN 接口 2 监听广播报文。

```
<DeviceB> system-view
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] ntp-service broadcast-client
```

Device A 和 Device B 接收到 Device C 发出的广播报文后，与其同步。

以 Device A 为例，同步后查看 Device A 的状态。

```
[DeviceA-Vlan-interface2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 64.0000 Hz
 Actual frequency: 64.0000 Hz
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 31.00 ms
 Root dispersion: 8.31 ms
 Peer dispersion: 34.30 ms
```

```
 Reference time: 16:01:51.713 UTC Jan 19 2011 (C6D95F6F.B6872B02)
```

此时 Device A 已经与 Device C 同步，层数比 Device C 的层数大 1，为 3。

查看 Device A 的 NTP 会话信息，可以看到 Device A 与 Device C 建立了连接。

```
[DeviceA-Vlan-interface2] display ntp-service sessions
      source    reference    stra  reach  poll  now  offset   delay   disper
**************************************************************************
[1234] 3.0.1.31  127.127.1.0   2   254     64    62   -16.0    32.0   16.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

1.8.4 配置NTP组播模式

1. 组网需求

Device C 作为不同网段中多个设备的 NTP 服务器，同时同步多个设备的时钟。为了实现该需求，需要进行以下配置：

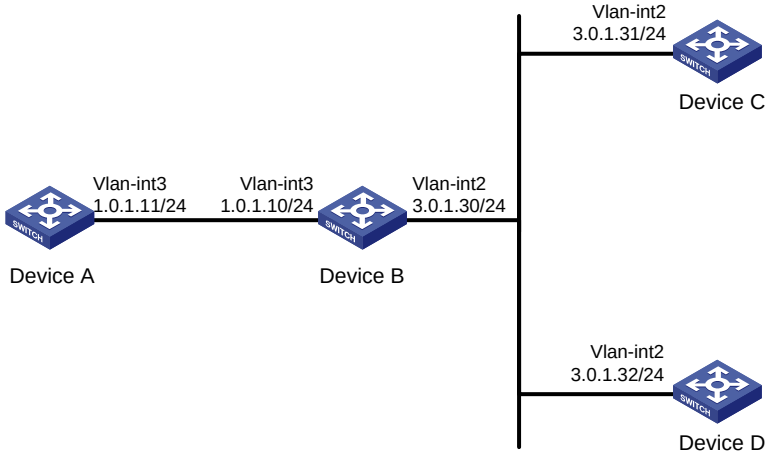
- 在 Device C 上设置本地时钟作为参考时钟，层数为 2；
- Device C 工作在组播服务器模式，从 VLAN 接口 2 向外发送组播报文；
- Device A 和 Device D 工作在组播客户端模式，Device A 从 VLAN 接口 3 监听组播报文，Device D 从 VLAN 接口 2 监听组播报文。

说明

此实例中，Device B 必须为支持组播路由功能的三层交换机。

2. 组网图

图1-10 配置 NTP 组播模式组网图



3. 配置步骤

(1) 按照 图 1-10 配置各接口的IP地址，具体配置过程略。

(2) 配置 Device C

设置 Device C 为组播服务器，从 VLAN 接口 2 发送组播报文。

```
[DeviceC] interface vlan-interface 2
[DeviceC-Vlan-interface2] ntp-service multicast-server
```

(3) 配置 Device D

设置 Device D 为组播客户端，从 VLAN 接口 2 监听组播报文。

```
<DeviceD> system-view
[DeviceD] interface vlan-interface 2
[DeviceD-Vlan-interface2] ntp-service multicast-client
```

由于 Device D 和 Device C 在同一个网段，不需要配置组播功能，Device D 就可以收到 Device C 发出的组播报文，并与其同步。

同步后查看 Device D 的状态。

```
[DeviceD-Vlan-interface2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 64.0000 Hz
 Actual frequency: 64.0000 Hz
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 31.00 ms
 Root dispersion: 8.31 ms
 Peer dispersion: 34.30 ms
 Reference time: 16:01:51.713 UTC Jan 19 2011 (C6D95F6F.B6872B02)
```

此时 Device D 已经与 Device C 同步，层数比 Device C 的层数大 1，为 3。

查看 Device D 的 NTP 会话信息，可以看到 Device D 与 Device C 建立了连接。

```
[DeviceD-Vlan-interface2] display ntp-service sessions
      source    reference    stra  reach  poll  now  offset  delay  disper
**************************************************************************
[1234] 3.0.1.31  127.127.1.0   2   254     64    62   -16.0    31.0   16.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

(4) 配置 Device B

由于 Device A 与 Device C 不在同一网段，所以 Device B 上需要配置组播功能，否则 Device A 收不到 Device C 发出的组播报文。

配置组播功能。

```
<DeviceB> system-view
[DeviceB] multicast routing-enable
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] pim dm
[DeviceB-Vlan-interface2] quit
[DeviceB] vlan 3
[DeviceB-vlan3] port gigabitethernet 1/0/1
[DeviceB-vlan3] quit
[DeviceB] interface vlan-interface 3
[DeviceB-Vlan-interface3] igmp enable
[DeviceB-Vlan-interface3] igmp static-group 224.0.1.1
[DeviceB-Vlan-interface3] quit
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB- GigabitEthernet1/0/1] igmp-snooping static-group 224.0.1.1 vlan 3
```

(5) 配置 Device A

```
<DeviceA> system-view
[DeviceA] interface vlan-interface 3
```

设置 Device A 为组播客户端，从 VLAN 接口 3 监听组播报文。

```
[DeviceA-Vlan-interface3] ntp-service multicast-client
```

同步后查看 Device A 的状态。

```
[DeviceA-Vlan-interface3] display ntp-service status
```

```
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 64.0000 Hz
 Actual frequency: 64.0000 Hz
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 40.00 ms
 Root dispersion: 10.83 ms
 Peer dispersion: 34.30 ms
 Reference time: 16:02:49.713 UTC Jan 19 2011 (C6D95F6F.B6872B02)
```

此时 Device A 已经与 Device C 同步，层数比 Device C 的层数大 1，为 3。

查看 Device A 的 NTP 会话信息，可以看到 Device A 与 Device C 建立了连接。

```
[DeviceA-Vlan-interface3] display ntp-service sessions
      source    reference    stra  reach  poll  now  offset   delay   disper
**************************************************************************
[1234] 3.0.1.31  127.127.1.0    2   255     64    26   -16.0    40.0    16.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

说明

组播功能的详细介绍请参见“IP 组播配置指导”中的“IGMP”和“PIM”。

1.8.5 配置带身份验证的NTP客户端/服务器模式

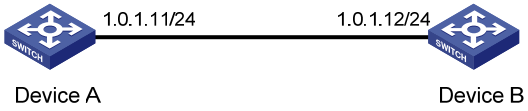
1. 组网需求

为了实现 Device B 的时钟与 Device A 的时钟同步，并保证时钟同步的安全性，需要进行以下配置：

- 在 Device A 上设置本地时钟作为参考时钟，层数为 2；
- Device B 工作在客户端模式，指定 Device A 为 NTP 服务器；
- Device A 和 Device B 上同时配置 NTP 验证。

2. 组网图

图1-11 配置带身份验证的 NTP 客户端/服务器模式组网图



3. 配置步骤

(1) 按照 图 1-11 配置各接口的IP地址，具体配置过程略。

(2) 配置 Device B

```
<DeviceB> system-view
```

在 Device B 上启动身份验证。

```
[DeviceB] ntp-service authentication enable
```

设置密钥。

```
[DeviceB] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

指定密钥为可信密钥。

```
[DeviceB] ntp-service reliable authentication-keyid 42
```

设置 Device A 为 Device B 的 NTP 服务器。

```
[DeviceB] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

以上配置将 Device B 向 Device A 进行时间同步，但由于 Device A 没有使能 NTP 身份验证，所以，Device B 还是无法向 Device A 同步。

现在，向 Device A 增加以下配置：

在 Device A 上启动身份验证。

```
[DeviceA] ntp-service authentication enable
```

设置密钥。

```
[DeviceA] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

指定密钥为可信密钥。

```
[DeviceA] ntp-service reliable authentication-keyid 42
```

此时，Device B 可以向 Device A 同步。

同步后查看 Device B 的状态。

```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 1.0.1.11
 Nominal frequency: 64.0000 Hz
 Actual frequency: 64.0000 Hz
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 31.00 ms
 Root dispersion: 1.05 ms
 Peer dispersion: 7.81 ms
 Reference time: 14:53:27.371 UTC Jan 19 2011 (C6D94F67.5EF9DB22)
```

可以看出，Device B 已经与 Device A 同步，层数比 Device A 的层数大 1，为 3。

查看 Device B 的 NTP 会话信息，可以看到 Device B 与 Device A 建立了连接。

```
[DeviceB] display ntp-service sessions
      source      reference   stra  reach  poll  now  offset  delay  disper
**************************************************************************
[12345] 1.0.1.11  127.127.1.0    2    63    64    3    -75.5    31.0  16.5
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

1.8.6 配置带身份验证的NTP广播模式

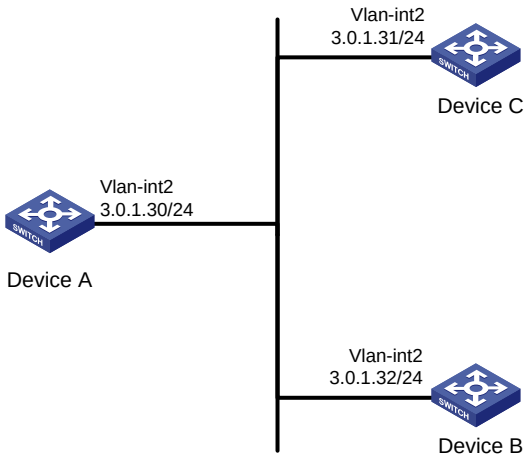
1. 组网需求

Device C 作为同一网段中多个设备的 NTP 服务器，同时同步多个设备的时钟。Device B 要求对时钟源进行验证，以保证时钟同步的安全性。为了实现上述需求，需要进行以下配置：

- 在 Device C 上设置本地时钟作为参考时钟，层数为 3；
- Device C 工作在广播服务器模式，从 VLAN 接口 2 向外发送广播报文；
- Device A 和 Device B 工作在广播客户端模式，从 VLAN 接口 2 监听广播报文；
- 在 Device B 和 Device C 上配置 NTP 验证功能。

2. 组网图

图1-12 配置带身份验证的 NTP 广播模式组网图



3. 配置步骤

(1) 按照 图 1-12 配置各接口的IP地址，具体配置过程略。

(2) 配置 Device A

设置 Device A 为 NTP 广播客户端，从 VLAN 接口 2 监听广播报文。

```
<DeviceA> system-view
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ntp-service broadcast-client
```

(3) 配置 Device B

使能 NTP 验证功能，创建 ID 为 88 的 NTP 验证密钥，密钥值为 123456，并将密钥 88 指定为可信密钥。

```
<DeviceB> system-view
[DeviceB] ntp-service authentication enable
[DeviceB] ntp-service authentication-keyid 88 authentication-mode md5 123456
[DeviceB] ntp-service reliable authentication-keyid 88
```

设置 Device B 为 NTP 广播客户端，从 VLAN 接口 2 监听广播报文。

```
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] ntp-service broadcast-client
```

(4) 配置 Device C

设置 Device C 为 NTP 广播服务器，从 VLAN 接口 2 向外发送广播报文。

```
[DeviceC] interface vlan-interface 2
[DeviceC-Vlan-interface2] ntp-service broadcast-server
[DeviceC-Vlan-interface2] quit
```

Device A 接收到 Device C 发出的广播报文后与其同步。在 Device A 上查看 NTP 服务的状态信息，可以看到 Device A 已经与 Device C 同步，层数比 Device C 的层数大 1，为 4。

```
[DeviceA-Vlan-interface2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 4
 Reference clock ID: 3.0.1.31
 Nominal frequency: 64.0000 Hz
 Actual frequency: 64.0000 Hz
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 31.00 ms
```

```
 Root dispersion: 8.31 ms
 Peer dispersion: 34.30 ms
 Reference time: 16:01:51.713 UTC Jan 19 2011 (C6D95F6F.B6872B02)
```

查看 Device A 的 NTP 会话信息，可以看到 Device A 与 Device C 建立了连接。

```
[DeviceA-Vlan-interface2] display ntp-service sessions
      source    reference    stra  reach  poll  now  offset  delay  disper
**************************************************************************
[1234] 3.0.1.31  127.127.1.0  3   254     64    62   -16.0    32.0   16.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

由于 Device B 上使能了 NTP 验证功能，Device C 上没有使能 NTP 验证功能。因此，Device B 无法向 Device C 同步。

```
[DeviceB-Vlan-interface2] display ntp-service status
 Clock status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^18
 Clock offset: 0.0000 ms
 Root delay: 0.00 ms
 Root dispersion: 0.00 ms
 Peer dispersion: 0.00 ms
 Reference time: 00:00:00.000 UTC Jan 1 1900(00000000.00000000)
```

在 Device C 上使能 NTP 验证功能，创建 ID 为 88 的 NTP 验证密钥，密钥值为 123456，并将密钥 88 指定为可信密钥。

```
[DeviceC] ntp-service authentication enable
[DeviceC] ntp-service authentication-keyid 88 authentication-mode md5 123456
[DeviceC] ntp-service reliable authentication-keyid 88
```

设置 Device C 为 NTP 广播服务器并指定关联的密钥编号为 88。

```
[DeviceC] interface vlan-interface 2
[DeviceC-Vlan-interface2] ntp-service broadcast-server authentication-keyid 88
```

在 Device C 上使能 NTP 验证功能后，Device B 可以向 Device C 同步。在 Device B 上查看 NTP 服务的状态信息，可以看到 Device B 已经与 Device C 同步，层数比 Device C 的层数大 1，为 4。

```
[DeviceB-Vlan-interface2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 4
 Reference clock ID: 3.0.1.31
 Nominal frequency: 64.0000 Hz
 Actual frequency: 64.0000 Hz
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 31.00 ms
 Root dispersion: 8.31 ms
 Peer dispersion: 34.30 ms
 Reference time: 16:01:51.713 UTC Jan 19 2011 (C6D95F6F.B6872B02)
```

查看 Device B 的 NTP 会话信息，可以看到 Device B 与 Device C 建立了连接。

```
[DeviceB-Vlan-interface2] display ntp-service sessions
      source    reference    stra  reach  poll  now  offset  delay  disper
**************************************************************************
[1234] 3.0.1.31  127.127.1.0   3   254     64    62   -16.0    32.0   16.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

```
Total associations :  1
```

在 Device C 上配置 NTP 验证功能后，不会对 Device A 造成影响。Device A 仍然处于同步状态。

```
[DeviceA-Vlan-interface2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 4
 Reference clock ID: 3.0.1.31
 Nominal frequency: 64.0000 Hz
 Actual frequency: 64.0000 Hz
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 31.00 ms
 Root dispersion: 8.31 ms
 Peer dispersion: 34.30 ms
 Reference time: 16:01:51.713 UTC Jan 19 2011 (C6D95F6F.B6872B02)
```

1.8.7 配置采用客户端/服务器模式实现MPLS VPN网络的时间同步

1. 组网需求

PE 1 和 PE 2 上同时存在两个 VPN：VPN 1 和 VPN 2。CE 1 和 CE 3 是 VPN 1 内的设备。为了实现在 VPN 1 内 CE 3 的时钟与 CE 1 的时钟同步，需要进行以下配置：

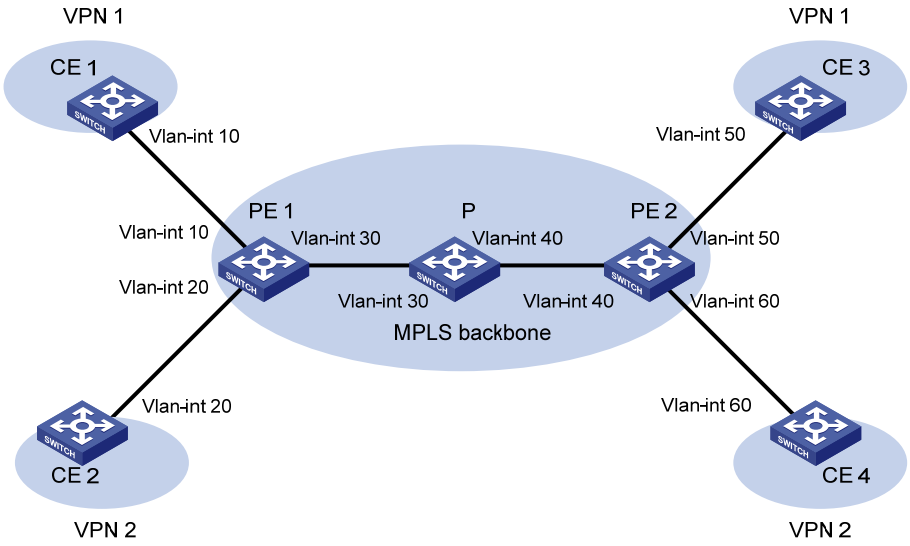
- 在 CE 1 上设置本地时钟作为参考时钟，层数为 1；
- 采用客户端/服务器模式实现 CE 3 向 CE 1 进行时间同步。

说明

目前只有单播方式（客户端/服务器模式或者对等体模式）的 NTP 时间同步支持 MPLS L3VPN，组播和广播模式的时间同步暂时不支持 MPLS L3VPN。

2. 组网图

图1-13 配置 MPLS VPN 网络的时间同步组网图



设备	接口	IP地址	设备	接口	IP地址
CE 1	Vlan-int 10	10.1.1.1/24	PE 1	Vlan-int 10	10.1.1.2/24
CE 2	Vlan-int 20	10.2.1.1/24		Vlan-int 30	172.1.1.1/24
CE 3	Vlan-int 50	10.3.1.1/24		Vlan-int 20	10.2.1.2/24
CE 4	Vlan-int 60	10.4.1.1/24	PE 2	Vlan-int 50	10.3.1.2/24
P	Vlan-int 30	172.1.1.2/24		Vlan-int 40	172.2.1.2/24
	Vlan-int 40	172.2.1.1/24		Vlan-int 60	10.4.1.2/24

3. 配置步骤

说明

在下面的配置之前，MPLS VPN 的相关配置必须完成，CE 1 和 PE 1 之间、PE 1 和 PE 2 之间、PE 2 和 CE 3 之间都必须有路由可达。MPLS VPN 的配置方法请参见“MPLS 配置指导”中的“MPLS L3VPN”。

(1) 按照 图 1-13 配置各接口的IP地址，具体配置过程略。

(2) 配置 CE 3

设置 VPN1 中的 CE 1 为 CE 3 的 NTP 服务器。

```
<CE3> system-view
[CE3] ntp-service unicast-server 10.1.1.1
```

经过一段时间之后在 CE 3 上可以查看 NTP 的会话信息、状态信息等，可以看出 CE 3 已经同步到 CE 1 了，层数为 2。

```
[CE3] display ntp-service status
 Clock status: synchronized
 Clock stratum: 2
 Reference clock ID: 10.1.1.1
 Nominal frequency: 63.9100 Hz
 Actual frequency: 63.9100 Hz
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 47.00 ms
 Root dispersion: 0.18 ms
 Peer dispersion: 34.29 ms
```

```
 Reference time: 02:36:23.119 UTC Jan 19 2011 (BDFA6BA7.1E76C8B4)
[CE3] display ntp-service sessions
source          reference       stra reach poll  now offset  delay disper
********************************************************************************
[12345]10.1.1.1       LOCL          1    7   64   15    0.0   47.0    7.8
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
[CE3] display ntp-service trace
 server 127.0.0.1,stratum 2, offset -0.013500, synch distance 0.03154
 server 10.1.1.1,stratum 1, offset -0.506500, synch distance 0.03429
 refid 127.127.1.0
```

1.8.8 配置采用对等体模式实现MPLS VPN网络的时间同步

1. 组网需求

PE 1 和 PE 2 上同时存在两个 VPN：VPN 1 和 VPN 2。为了实现在 VPN 1 内 PE 2 的时钟与 PE 1 的时钟同步，需要进行以下配置：

- 在 PE 1 上设置本地时钟作为参考时钟，层数为 1；
- 采用对等体模式实现 PE 2 向 PE 1 进行时间同步，并指定 VPN 为 VPN 1。

2. 组网图

如 图 1-13 所示。

3. 配置步骤

(1) 按照 图 1-13 配置各接口的IP地址，具体配置过程略。

(2) 配置 PE 2

设置 VPN 1 中的 PE 1 为 PE 2 的被动对等体。

```
<PE2> system-view
[PE2] ntp-service unicast-peer vpn-instance vpn1 10.1.1.2
```

经过一段时间之后在 PE 2 上可以查看 NTP 的会话信息、状态信息等，可以看出 PE 2 已经同步到 PE 1 了，层数为 2。

```
[PE2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 2
 Reference clock ID: 10.1.1.2
 Nominal frequency: 63.9100 Hz
 Actual frequency: 63.9100 Hz
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 32.00 ms
 Root dispersion: 0.60 ms
 Peer dispersion: 7.81 ms
 Reference time: 02:44:01.200 UTC Jan 19 2011 (BDFA6D71.33333333)
[PE2] display ntp-service sessions
source          reference       stra reach poll  now offset  delay disper
********************************************************************************
[12345]10.1.1.2       LOCL          1    1   64   29   -12.0   32.0    15.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
[PE2] display ntp-service trace
 server 127.0.0.1,stratum 2, offset -0.012000, synch distance 0.02448
 server 10.1.1.2,stratum 1, offset 0.003500, synch distance 0.00781
```

```
refid 127.127.1.0
```

目 录

1 信息中心配置

1.1 信息中心简介

1.1.1 信息中心概述

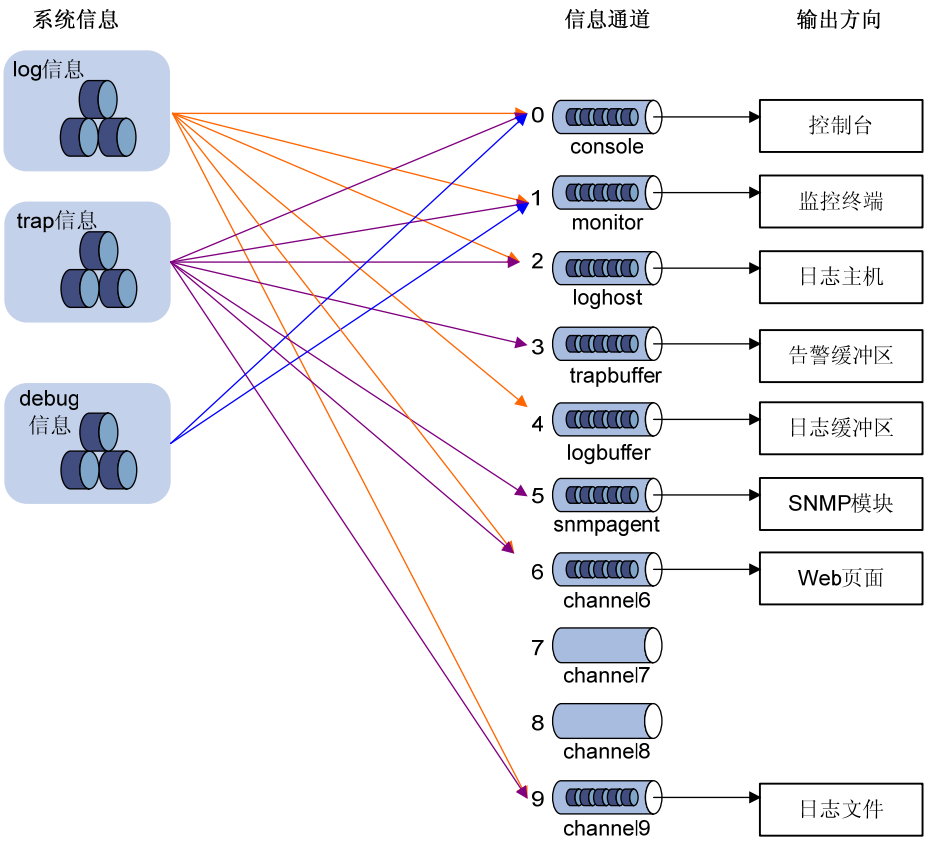
信息中心是系统的信息枢纽，它能够对所有的系统信息进行分类、管理，为网络管理员和开发人员监控网络运行情况和诊断网络故障提供了强有力的支持。

信息中心的工作过程如下：

- 接收各模块生成的日志信息（log）、告警信息（trap）和调试信息（debug）。
- 根据用户设置的输出规则，将信息输出到信息通道。
- 根据信息通道和输出方向的关联，将信息输出到不同方向。

概括来说，信息中心的主要工作就是将三种信息，按照八个严重等级，分配到十个信息通道中，再输出到多个方向，图 1-1 描述了缺省情况下，三种信息分别可以分配到哪些信息通道，每个信息通道对应哪个输出方向。下面将进行详细介绍。

图1-1 信息中心功能示意图（缺省情况下）



说明

信息中心缺省情况下处于开启状态。在信息中心开启时，特别是在处理信息较多时，由于信息分类、输出的原因，对系统性能有一定的影响。

1.1.2 系统信息的分类

信息中心的系统信息共分为三类：

- log 类，日志类信息
- trap 类，告警类信息
- debug 类，调试类信息

1.1.3 系统信息的等级

信息按严重性划分为八个等级，严重性由高到底的顺序依次为：emergencies、alerts、critical、errors、warnings、notifications、informational 和 debugging。根据信息级别输出信息时，将会输出信息级别高于或等于所设置级别的信息。比如，输出规则中指定允许级别为 informational 的信息输出，则级别为 emergencies～informational 的信息均会输出。

表1-1 信息级别列表

信息级别	数值	描述
emergencies	0	系统不可用信息
alerts	1	需要立刻做出反应的信息
critical	2	严重信息
errors	3	错误信息
warnings	4	警告信息
notifications	5	正常出现但是重要的信息
informational	6	需要记录的通知信息
debugging	7	调试过程产生的信息

1.1.4 系统信息的输出方向和通道

系统支持十个通道，缺省情况下，通道 0～6 和通道 9 已经定义了通道名、输出规则和输出方向。可以通过命令改变通道名、输出规则和输出方向，用户还可以在不改变通道 0～6 和通道 9 缺省配置的情况下，配置通道 7 和通道 8，将他们与输出方向关联，以便对输出的系统信息实施配置的过滤规则。

表1-2 信息通道和输出方向

通道编号	通道的缺省名称	通道的缺省输出方向	说明
0	console	控制台	可以接收log、trap、debug信息
1	monitor	监视终端	可以接收log、trap、debug信息，方便远程维护
2	loghost	日志主机	可以接收log、trap、debug信息，通常系统信息在日志主机以文件的方式存储，以便查询
3	trapbuffer	告警缓冲区	可以接收trap信息，是设备内部的一块缓存，用于记录信息
4	logbuffer	日志缓冲区	可以接收log信息，是设备内部的一块缓存，用于记录信息
5	snmpagent	SNMP模块	可以接收trap信息
6	channel6	Web页面	可以接收log信息
7	channel7	未指定	可以接收log、trap、debug信息

通道编号	通道的缺省名称	通道的缺省输出方向	说明
8	channel8	未指定	可以接收log、trap、debug信息
9	channel9	日志文件	可以接收log、trap、debug信息

1.1.5 按来源模块输出系统信息

系统由众多的协议模块、配置模块构成，系统信息可按来源模块进行划分，并过滤输出。系统支持的来源模块可以通过 **info-center source ?** 命令的帮助信息获取。

1.1.6 系统信息的缺省输出规则

缺省输出规则规定了各个输出方向可以输出的信息模块、输出的信息类型以及输出的信息级别，如表 1-3 所示。该表表明，缺省情况下：

- 允许所有模块的所有 log 信息发往 Web 页面和日志文件；允许所有模块的高于或等于 informational 级别的 log 信息发往日志主机；允许所有模块的高于或等于 informational 级别的 log 信息发往控制台、监视终端和日志缓冲区；所有模块的所有 log 信息不允许发往告警缓冲区和 SNMP 模块方向。
- 允许所有模块的所有 Trap 信息发往控制台、监视终端、日志主机、Web 页面和日志文件；允许所有模块的高于或等于 informational 级别的 Trap 信息发往告警缓冲区和 SNMP 模块；所有模块的所有 Trap 信息不允许发往日志缓冲区方向。
- 允许所有模块的所有 debug 信息发往控制台和监视终端；所有模块的所有 debug 信息不允许发往日志主机、告警缓冲区、日志缓冲区、SNMP 模块、Web 页面和日志文件。

表1-3 输出方向的缺省输出规则

输出方向	允许输出的模块	LOG		TRAP		DEBUG	
		开关	级别	开关	级别	开关	级别
控制台	default（所有模块）	开	informational	开	debugging	开	debugging
监视终端	default（所有模块）	开	informational	开	debugging	开	debugging
日志主机	default（所有模块）	开	informational	开	debugging	关	debugging
告警缓冲区	default（所有模块）	关	informational	开	informational	关	debugging
日志缓冲区	default（所有模块）	开	informational	关	debugging	关	debugging
SNMP模块	default（所有模块）	关	debugging	开	informational	关	debugging
Web页面	default（所有模块）	开	debugging	开	debugging	关	debugging
日志文件	default（所有模块）	开	debugging	开	debugging	关	debugging

1.1.7 系统信息的格式

按照系统信息的输出方向不同，系统信息可能有不同格式。

(1) 当输出方向为非日志主机（控制台、监视终端、日志缓冲区、告警缓冲区、SNMP 模块和日志文件）时

系统信息格式大致为：

```
timestamp sysname module/level/digest:content
```

对应的中文格式为：

时间戳 主机名 模块名/信息级别/信息摘要:信息文本

比如，监视终端与设备相连，当有终端登录设备时，在监视终端可以看到格式如下的日志信息：

```
%Jan 26 17:08:35:809 2011 Sysname SHELL/4/LOGIN: VTY login from 1.1.1.1
```

(2) 当输出方向为日志主机时，支持两种输出格式：

- H3C 格式

系统信息格式为：

```
<PRI>timestamp sysname %%vvmodule/level/digest: source content
```

比如，日志主机与设备相连，当有终端登录设备时，在日志主机可以看到格式如下的日志信息：

```
<189>Jan 9 14:59:04 2011 MyDevice %%10SHELL/5/SHELL_LOGIN(l):VTY logged in from 192.168.1.21.
```

- UNICOM 格式

系统信息格式为：

```
<PRI>timestamp sysname vvmodule/level/serial_number: content
```

比如，日志主机与设备相连，当设备端口 Link down 时，在日志主机可以看到格式如下的日志信息：

```
<186>Jan 13 16:48:08 2011 H3C 10IFNET/2/210231a64jx073000020: log_type=port;content=Vlan-interface1 link status is DOWN.
<186>Jan 13 16:48:08 2011 H3C 10IFNET/2/210231a64jx073000020: log_type=port;content=Line protocol on the interface Vlan-interface1 is DOWN.
```

说明

- 以上格式中的尖括号（< >）、空格、斜杠（/）、冒号（:）是必须的。
- 以上格式是设备给各个输出方向发送的原始信息的格式，可能与用户最终看到的信息格式有差异，最终显示格式与用户使用的日志解析工具有关，请以实际情况为准。

下面对每一个字段做详细说明。

1. PRI（优先级）

优先级的计算按如下公式：facility*8+severity。Facility表示工具名称，在设置日志主机相关参数的时候可以设置，参数取值为local0～local7，对应的十进制数值为 16～23，缺省取值为local7。主要用于在日志主机端标志不同的日志来源，查找、过滤对应日志源的日志。severity（信息级别）的取值范围为 0～7，信息级别具体含义请参见 表 1-1。

本字段只有在信息发往日志主机时才有效。

2. timestamp（时间戳）

时间戳记录了系统信息产生的时间，方便用户查看和定位系统事件。发往日志主机的系统信息的时间戳不带毫秒信息，发送到其它方向的系统信息会精确到毫秒；发往日志主机的系统信息的时间戳格式由**info-center timestamp loghost**命令设置，发送到其它方向的时间戳格式由**info-center timestamp**命令统一设置。（各时间戳参数的详细描述请见 表 1-4。）

表1-4 时间戳参数描述表

时间戳参数	说明	举例
boot	系统启动后经历的时间（即设备的本次运行的持续时间），格式为：xxxxxx.yyyyyy，其中xxxxxx是系统自启动后经历时间的毫秒数高32位，yyyyyy是低32位 除日志主机方向外发往其它方向的系统信息均支持该参数	%0.109391473 Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in successfully. 其中0.109391473即为**boot**格式的时间戳

时间戳参数	说明	举例
date	系统当前的日期和时间，格式为“Mmm dd hh:mm:ss:sss yyyy” 发往所有方向的系统信息均支持该参数	%Jan 30 05:36:29:579 2011 Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in successfully. 其中Jan 30 05:36:29:579 2011即为**date**格式的时间戳
iso	ISO 8601中规定的时间戳的格式 只有发往日志主机方向的系统信息支持该参数	<189>2011-05-30T06:42:44 Sysname %%10FTPD/5/FTPD_LOGIN(l): User ftp (192.168.1.23) has logged in successfully. 其中2011-05-30T06:42:44即为**iso**格式的时间戳
none	不带时间信息 发往所有方向的系统信息均支持该参数	% Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in successfully. 其中没有包含时间戳
no-year-date	系统当前日期和时间，但不包含年份信息 只有发往日志主机方向的系统信息支持该参数	<189>Jan 30 06:44:22 Sysname %%10FTPD/5/FTPD_LOGIN(l): User ftp (192.168.1.23) has logged in successfully. 其中Jan 30 06:44:22即为**no-year-date**格式的时间戳

3. sysname（主机名或主机IP地址）

- 当使用 UNICOM 格式将系统信息发送到日志主机，并配置了 **info-center loghost source** 或者在 **info-center loghost** 命令中指定了 **vpn-instance** *vpn-instance-name* 时，该字段会显示为生成该日志的设备的 IP 地址。
- 其它情况下（当使用 H3C 格式将系统信息发送到日志主机或者发往别的方向），该字段均会显示为生成该日志的设备的名称，即本机的系统名。用户可使用 **sysname** 命令修改主机名（具体配置请参见“基础配置命令参考”中的“设备管理”）。

4. %%（厂家标志）

该字段表示本信息由 H3C 设备生成。

本字段只有在使用 H3C 格式将系统信息发往日志主机时才出现。

5. vv（版本信息）

该字段表示 syslog 的版本标识，取值为 10。

本字段只有在信息发往日志主机时才出现。

6. module（模块名）

该字段表示产生信息的功能模块的名称。模块列表可以通过在系统视图下输入命令 **info-center source ?** 查看到。

7. level（信息级别）

系统信息的级别共分为 8 级，从 0～7，它们的定义和说明请参见 表 1-1。各模块生成的系统信息的级别在开发阶段已经确定，用户不能更改，但可以使用**info-center source**命令让指定级别的信息输出，低于该级别的信息不输出。

8. digest（信息摘要）

信息摘要是一个不超过 32 个字符的字符串，表示该信息的内容大意。

- 对于输出方向为日志主机的系统信息，如果该字符串以“(l)”结尾则表示该信息为 Log 信息，如果该字符串以“(t)”结尾则表示该信息为 Trap 信息，如果该字符串以“(d)”结尾则表示该信息为 Debug 信息。
- 对于输出方向为非日志主机的系统信息，时间戳前面会有百分号（%）或井字符号（#）或米字符号（*），分别代表该条信息是日志信息或告警信息或调试信息。

9. serial_number（序列号）

表示生成该日志的设备的序列号。

该信息只有在使用 UNICOM 格式将系统信息发往日志主机时才出现。

10. source（定位信息）

该字段为可选字段，表示该信息的产生者，只有在使用 H3C 格式将系统信息发往日志主机时才出现。该字段的具体内容可能为下面的一种：

- IRF 的成员设备编号；
- 日志发送者的源 IP。

11. content（信息文本）

该字段表示了该条系统信息的具体内容。

1.2 配置信息中心

1.2.1 信息中心配置任务简介

表1-5 信息中心配置任务简介

配置任务	说明	详细配置
配置信息发送到控制台	可选	1.2.2
配置信息发送到监视终端	可选	1.2.3
配置信息发送到日志主机	可选	1.2.4
配置信息发送到告警缓冲区	可选	1.2.5
配置信息发送到日志缓冲区	可选	1.2.6
配置信息发送到SNMP模块	可选	1.2.7
配置信息发送到Web页面	可选	1.2.8
配置信息保存到日志文件	可选	1.2.9
配置安全日志同步保存和管理功能	可选	1.2.10
配置同步信息输出功能	可选	1.2.11
禁止端口生成Link up/Link down日志信息	可选	1.2.12

1.2.2 配置信息发送到控制台

1. 配置信息发送到控制台

表1-6 配置信息发送到控制台

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
开启信息中心	**info-center enable**	可选 缺省情况下，信息中心处于开启状态
为指定编号的信息通道命名	**info-center channel** *channel-number* **name** *channel-name*	可选 通道的缺省名称请参见表1-2
设置系统向控制台输出信息的通道	**info-center console channel** { *channel-number* | *channel-name* }	可选 缺省情况下，系统使用0号（console）通道向控制台输出信息
配置系统信息的输出规则	**info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**debug** { **level** *severity* | **state** *state* } * | **log** { **level** *severity* | **state** *state* } * | **trap** { **level** *severity* | **state** *state* } *] *	可选 缺省情况下，系统信息的输出规则请参见1.1.6
设置时间戳输出格式	**info-center timestamp** { **debugging** | **log** | **trap** } { **boot** | **date** | **none** }	可选 缺省情况下，log、trap和debug信息的时间戳输出格式均为**date**格式

2. 开启控制台对系统信息的显示功能

在配置将系统信息发送到控制台后，为了能在控制台上观察到输出的信息，还要开启控制台对相应信息的显示功能。请在用户视图下进行以下操作。

表1-7 开启控制台对系统信息的显示功能

操作	命令	说明
开启控制台对系统信息的监视功能	**terminal monitor**	可选 缺省情况下，控制台的监视功能处于开启状态，监视终端的监视功能处于关闭状态
开启控制台对调试信息的显示功能	**terminal debugging**	必选 缺省情况下，控制台对调试信息的显示功能处于关闭状态
开启控制台对日志信息的显示功能	**terminal logging**	可选 缺省情况下，控制台对日志信息的显示功能处于开启状态
开启控制台对告警信息的显示功能	**terminal trapping**	可选 缺省情况下，控制台对告警信息的显示功能处于开启状态

1.2.3 配置信息发送到监视终端

系统信息可以发往控制台，也可以发往监视终端。监视终端是指以 VTY 类型用户界面登录的用户终端。

1. 配置信息发送到监视终端

表1-8 配置信息发送到监视终端

操作	命令	说明
进入系统视图	**system-view**	-
开启信息中心	**info-center enable**	可选 缺省情况下，信息中心处于开启状态
为指定编号的信息通道命名	**info-center channel** *channel-number* **name** *channel-name*	可选 通道的缺省名称请参见表1-2
设置系统向监视终端输出系统信息的通道	**info-center monitor channel** { *channel-number* | *channel-name* }	可选 缺省情况下，系统使用1号（monitor）通道向监视终端输出系统信息
配置系统信息的输出规则	**info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**debug** { **level** *severity* | **state** *state* } * | **log** { **level** *severity* | **state** *state* } * | **trap** { **level** *severity* | **state** *state* } *] *	可选 缺省情况下，系统信息的输出规则请参见1.1.6
设置时间戳输出格式	**info-center timestamp** { **debugging | log | trap** } { **boot** | **date** | **none** }	可选 缺省情况下，log、trap和debug信息的时间戳输出格式均为**date**格式

2. 开启监视终端对系统信息的显示功能

在配置将系统信息发送到监视终端后，为了能在监视终端上观察到输出的信息，还要开启监视终端对相应信息的显示功能。

表1-9 开启监视终端对系统信息的显示功能

操作	命令	说明
开启监视终端对系统信息的监视功能	**terminal monitor**	必选 缺省情况下，控制台的监视功能处于开启状态，监视终端的监视功能处于关闭状态
开启监视终端对调试信息的显示功能	**terminal debugging**	必选 缺省情况下，监视终端对调试信息的显示功能处于关闭状态
开启监视终端对日志信息的显示功能	**terminal logging**	可选 缺省情况下，监视终端对日志信息的显示功能处于开启状态
开启监视终端对告警信息的显示功能	**terminal trapping**	可选 缺省情况下，监视终端对告警信息的显示功能处于开启状态

1.2.4 配置信息发送到日志主机

表1-10 配置信息发送到日志主机

操作	命令	说明
进入系统视图	**system-view**	-
开启信息中心	**info-center enable**	可选 缺省情况下，信息中心处于开启状态
为指定编号的信息通道命名	**info-center channel** *channel-number* **name** *channel-name*	可选 通道的缺省名称请参见表1-2
配置系统信息的输出规则	**info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**debug** { **level** *severity* | **state** *state* } * | **log** { **level** *severity* | **state** *state* } * | **trap** { **level** *severity* | **state** *state* } *] *	可选 缺省情况下，系统信息的输出规则请参见1.1.6
配置发送的日志信息的源IP地址	**info-center loghost source** *interface-type interface-number*	可选 缺省情况下，将根据路由来确定发送日志信息的出接口，使用该接口的主IP地址作为发送的日志信息的源IP地址
设置发往日志主机的系统信息的时间戳输出格式	**info-center timestamp loghost** { **date** | **iso** | **no-year-date** | **none** }	可选 缺省情况下，发往日志主机的系统信息的时间戳输出格式为**date**格式
设置发往日志主机的系统信息的输出格式为UNICOM格式	**info-center format unicom**	可选 缺省情况下，发往日志主机的系统信息的格式为H3C格式
指定日志主机并设置相关输出参数	**info-center loghost** [**vpn-instance** *vpn-instance-name*] { *host-ipv4-address* | **ipv6** *host-ipv6-address* } [**port** *port-number*] [**dscp** *dscp-value*] [**channel** { *channel-number* | *channel-name* } | **facility** *local-number*] *	必选 缺省情况下，系统不向日志主机输出信息。如果使能系统向日志主机输出信息，则系统默认使用2号（loghost）通道 *port-number*参数的值需要和日志主机侧的设置一致，否则，日志主机接收不到系统信息

1.2.5 配置信息发送到告警缓冲区

说明

用户可以设置将 log、trap 和 debug 三种类型的信息发送给告警缓冲区，但告警缓冲区只接收 trap 信息，其它类型的信息将被丢弃。

表1-11 配置信息发送到告警缓冲区

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
开启信息中心	**info-center enable**	可选 缺省情况下，信息中心处于开启状态
为指定编号的信息通道命名	**info-center channel** *channel-number* **name** *channel-name*	可选 通道的缺省名称请参见表1-2
设置系统向告警缓冲区输出信息以及相关参数	**info-center trapbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*] *	可选 缺省情况下，系统使用3号（trapbuffer）通道向告警缓冲区输出信息，缓冲区可存储256条信息
配置系统信息的输出规则	**info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**debug** { **level** *severity* | **state** *state* } * | **log** { **level** *severity* | **state** *state* } * | **trap** { **level** *severity* | **state** *state* } *] *	可选 缺省情况下，系统信息的输出规则请参见1.1.6
设置时间戳输出格式	**info-center timestamp** { **debugging** | **log** | **trap** } { **boot** | **date** | **none** }	可选 缺省情况下，log、trap和debug信息的时间戳输出格式均为**date**格式

1.2.6 配置信息发送到日志缓冲区

说明

用户可以设置将 log、trap 和 debug 三种类型的信息发送给日志缓冲区，但日志缓冲区只能接收 log 信息，trap 和 debug 信息将被丢弃。

表1-12 配置信息发送到日志缓冲区

操作	命令	说明
进入系统视图	**system-view**	-
开启信息中心	**info-center enable**	可选 缺省情况下，信息中心处于开启状态
为指定编号的信息通道命名	**info-center channel** *channel-number* **name** *channel-name*	可选 通道的缺省名称请参见表1-2
设置系统向日志缓冲区输出信息以及相关参数	**info-center logbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*] *	可选 缺省情况下，系统使用4号（logbuffer）通道向日志缓冲区输出信息，缓冲区可存储512条信息
配置系统信息的输出规则	**info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**debug** { **level** *severity* | **state** *state* } * | **log** { **level** *severity* | **state** *state* } * | **trap** { **level** *severity* | **state** *state* } *] *	可选 缺省情况下，系统信息的输出规则请参见1.1.6

操作	命令	说明
设置时间戳输出格式	**info-center timestamp { debugging | log | trap } { boot | date | none }**	可选 缺省情况下，log、trap和debug信息的时间戳输出格式均为**date**格式

1.2.7 配置信息发送到SNMP模块

说明

用户可以设置将 log、trap 和 debug 三种类型的信息发送给 SNMP 模块，但 SNMP 模块只接收 trap 信息，其它类型的信息将被丢弃。

为了监控设备的运行状况，通常会将 Trap 信息发送到 SNMP NMS（Network Management System，网络管理系统）。此时，首先需要将信息发送给 SNMP 模块，再设置 SNMP 模块 Trap 发送参数，对 Trap 报文进行进一步的处理（详细介绍请参见“网络管理和监控配置指导”中的“SNMP”）。

表1-13 配置信息发送到 SNMP 模块

操作	命令	说明
进入系统视图	**system-view**	-
开启信息中心	**info-center enable**	可选 缺省情况下，信息中心处于开启状态
为指定编号的信息通道命名	**info-center channel** *channel-number* **name** *channel-name*	可选 通道的缺省名称请参见表1-2
设置系统向SNMP模块输出信息的通道	**info-center snmp channel** { *channel-number* | *channel-name* }	可选 缺省情况下，系统使用5号（snmpagent）通道向SNMP模块送系统信息
配置系统信息的输出规则	**info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**debug** { **level** *severity* | **state** *state* }* | **log** { **level** *severity* | **state** *state* }* | **trap** { **level** *severity* | **state** *state* }*]*	可选 缺省情况下，系统信息的输出规则请参见1.1.6
设置时间戳输出格式	**info-center timestamp { debugging | log | trap } { boot | date | none }**	可选 缺省情况下，log、trap和debug信息的时间戳输出格式均为**date**格式

1.2.8 配置信息发送到Web页面

本特性用于控制是否将系统信息发送到 Web 页面以及哪些系统信息可以发送到 Web 页面。因为 Web 页面提供了丰富的搜索和排序功能，所以，配置该输出方向后，用户通过 Web 页面登录设备，点击相应的页签就可以方便快捷地查看设备的系统信息。

表1-14 配置信息发送到 Web 页面

操作	命令	说明
进入系统视图	**system-view**	-
开启信息中心	**info-center enable**	可选 缺省情况下，信息中心处于开启状态
为指定编号的信息通道命名	**info-center channel** *channel-number* **name** *channel-name*	可选 通道的缺省名称请参见表1-2
设置系统向Web页面输出信息的通道	**info-center syslog channel** { *channel-number* | *channel-name* }	可选 缺省情况下，系统使用6号通道向Web页面发送系统信息
配置系统信息的输出规则	**info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**debug** { **level** *severity* | **state** *state* }* | **log** { **level** *severity* | **state** *state* }* | **trap** { **level** *severity* | **state** *state* }*]*	可选 缺省情况下，系统信息的输出规则请参见1.1.6
设置时间戳输出格式	**info-center timestamp** { **debugging | log | trap** } { **boot** | **date** | **none** }	可选 缺省情况下，log、trap和debug信息的时间戳输出格式均为**date**格式

说明

用户可以配置将 log、trap、debug 信息输出到某个通道，但当该通道和 Web 页面输出方向绑定时，用户登录 Web 页面时，只能显示特定类型的日志信息，其它类型的信息均会被过滤掉。

1.2.9 配置信息保存到日志文件

通过配置信息保存到日志文件（logfile），用户可以将系统产生的日志信息，按照指定的频率保存到该设备的指定路径下，便于用户在本地随时查看历史操作，保障设备的正常运行。

日志在保存到日志文件前，先保存在日志文件缓冲区（logfile buffer）。系统会按照指定的频率将缓冲区的内容写入日志文件，频率一般配置为 24 小时，用户也可以手工触发保存，建议在设备比较空闲的时候进行保存。成功保存后，保存前日志文件缓冲区里的内容会被清空。

日志文件有容量限制，当日志文件的大小达到最大值时，设备会将日志文件中最旧的信息删除，再写入新的信息。

表1-15 配置信息保存到日志文件

操作	命令	说明
进入系统视图	**system-view**	-
开启信息中心	**info-center enable**	可选 缺省情况下，信息中心处于开启状态
开启日志文件特性	**info-center logfile enable**	可选 缺省情况下，日志文件特性处于开启状态
设置自动保存日志文件的频率	**info-center logfile frequency** *freq-sec*	可选 缺省情况下，设备自动保存日志文件的频率缺省值为86400

操作	命令	说明
设置单个日志文件最大能占用的存储空间的大小	**info-center logfile size-quota** *size*	可选 缺省情况下，单个日志文件最大能占用的存储空间的大小为10M
设置存储日志文件的目录	**info-center logfile switch-directory** *dir-name*	可选 缺省情况下，存放日志文件的目录为Flash根目录
手动将日志文件缓冲区中的内容保存到日志文件	**logfile save**	可选 缺省情况下，系统将按照**info-center logfile frequency**命令所设置的频率自动保存日志文件 任意视图均可执行

说明

- 为了保证设备的正常运行，**info-center logfile size-quota** 设置的日志文件的大小最小不能低于 1MB，最大不能超过 10MB。
- **info-center logfile switch-directory** 命令通常用于日志文件的备份或者迁移前的准备工作，其配置会在设备重启或 Master 和 Slave 倒换后失效。

1.2.10 配置安全日志同步保存和管理功能

1. 安全日志同步保存功能简介

查看系统日志是了解设备状态、定位和排除网络问题的一个重要方法，而安全日志是系统日志中与设备安全相关的部分，更是重中之重。但通常情况下，安全日志与其它日志一同输出，被埋没在大量的系统日志中，很难识别、不便于查看。针对这个问题，系统提供了安全日志同步保存功能。使能该功能后，系统将进行如下处理：

- 将安全日志进行集中输出：当生成的系统信息中有安全日志，在不影响系统消息现有输出规则的前提下，系统会将安全日志复制一份同步保存到专用的安全日志文件。这样既实现了安全日志的集中管理，又有利于用户随时快捷地查看安全日志，了解设备状态。
- 安全日志同步保存功能的配置和安全日志文件的管理相互分离，安全日志文件实行专人专管。设备管理员登录设备后可以配置安全日志同步保存功能，执行 表 1-16 所示的命令；只有安全日志管理员通过AAA本地认证登录设备后才能对安全日志文件进行操作（具体操作请参见 表 1-17），其它用户（包括设备管理员）均不能对安全日志文件进行这些操作。

说明

- 本特性中的“安全日志管理员”指的是配置了 **authorization-attribute user-role security-audit** 的本地用户。
- 设备管理员不能对安全日志文件进行查看、拷贝、重命名等文件类操作，操作时会提示“% Execution error”，但可以对除安全日志文件之外的其他文件进行这些操作。
- 本地用户以及 AAA 本地认证的介绍和配置请参见“安全配置指导”中的“AAA”。

2. 配置安全日志同步保存功能

安全日志和其它日志一起被发送到控制台等输出方向时，会被复制一份同步保存在安全日志文件缓冲区（security-logfile buffer）。系统会按照指定的频率（*freq-sec*）将缓冲区的内容写入安全日志文件（安全日志管理员也可以手工触发保存）。安全日志文件缓冲区里的内容成功保存到安全日志文件后，会被立即清空。

安全日志文件有大小限制，当安全日志文件的大小达到最大值（*size*）时，系统会将安全日志文件中最旧的信息删除，再写入新的信息。为了防止安全日志的丢失，用户可以设置安全日志文件使用率告警上限（*usage*）。当达到上限时，系统会输出日志信息提醒管理员，此时，管理员可以使用“安全日志管理员”身份登录设备，将安全日志文件进行备份，以防重要历史数据丢失。

缺省情况下，安全日志同步保存功能没有使能，*freq-sec*、*size*和*usage*参数也有缺省值。如果用户要对这些参数进行修改，请以设备管理员身份登录，使用 表 1-16 所示的命令进行配置。

表1-16 配置安全日志同步保存功能

操作	命令	说明
进入系统视图	**system-view**	-
开启信息中心	**info-center enable**	可选 缺省情况下，信息中心处于开启状态
使能安全日志同步保存功能	**info-center security-logfile enable**	必选 缺省情况下，安全日志同步保存功能没有使能
设置设备自动保存安全日志文件的频率	**info-center security-logfile frequency** *freq-sec*	可选 缺省情况下，设备自动保存日志文件的频率缺省值为600秒
设置单个安全日志文件最大能占用的存储空间的大小	**info-center security-logfile size-quota** *size*	可选 缺省值为1MB
设置安全日志文件使用率的告警上限	**info-center security-logfile alarm-threshold** *usage*	可选 缺省情况下，安全日志文件使用率的告警门限是80（即当安全日志文件使用率达到80%时，系统会发出日志提醒用户）

3. 管理安全日志文件

安全日志管理员通过 AAA 本地认证登录设备后能进行如下操作：

表1-17 管理安全日志文件

操作	命令	说明
显示安全日志文件摘要信息	**display security-logfile summary** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	可选
修改存储安全日志文件的路径	**info-center security-logfile switch-directory** *dir-name*	可选 缺省情况下，存储安全日志文件路径为存储设备根目录下的seclog文件夹。 本命令在用户视图下执行
显示安全日志文件缓冲区的内容	**display security-logfile buffer** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	可选

操作		命令	说明
手动将安全日志文件缓冲区中的内容全部保存到安全日志文件		**security-logfile save**	可选 缺省情况下，系统将按照**info-center security-logfile frequency**命令所设置的频率自动保存安全日志文件，保存的路径可以通过**info-center security-logfile switch-directory**命令设置 本命令在用户视图下执行
对安全日志文件进行操作	显示指定文件的内容	**more** *file-url*	可选 这些命令均在用户视图下执行 关于命令的详细描述请参见“基础配置命令参考”中的“文件系统管理”
	显示文件及文件夹的信息	**dir** [**/all**] [*file-url*]	
	在存储设备的指定目录下创建文件夹	**mkdir** *directory*	
	修改当前的工作路径	**cd** { *directory* | **..** | **/** }	
	显示当前路径	**pwd**	
	删除设备中的指定文件	**delete** [**/unreserved**] *file-url*	
	删除指定文件夹	**rmdir** *directory*	
	格式化存储设备	**format** *device*	
	恢复未被彻底删除（即存放在回收站里）的文件	**undelete** *file-url*	
将安全日志文件上传到SFTP服务器	在IPv4网络环境建立SFTP连接	**sftp** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *	可选 **sftp**命令均在用户视图下执行，其它命令在SFTP客户端视图下执行 关于这些命令的详细介绍请参见“安全命令参考”中的“SSH2.0”
	在IPv6网络环境建立SFTP连接	**sftp ipv6** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *	
	上传本地文件到远程SFTP服务器	**put** *localfile* [*remotefile*]	
	下载SFTP服务器上的文件	**get** *remotefile* [*localfile*]	
	设备作为SFTP客户端支持的其它操作	请参见“安全配置指导/SSH2.0”中的“配置设备作为SFTP客户端”章节	

1.2.11 配置同步信息输出功能

同步信息输出是指当用户在输入时有日志、告警、调试等系统信息输出，则在输出后会回显命令行提示符（在命令编辑状态回显提示符，交互状态回显“[Y/N]”字符串）和用户已有的输入。

此功能用于用户在进行操作（操作还没有完成）却被大量的系统信息打断时，回显用户的上一步操作，用户可以接着执行上一步的操作。

表1-18 配置同步信息输出功能

操作	命令	说明
进入系统视图	**system-view**	-
打开同步信息输出功能	**info-center synchronous**	必选 缺省情况下，同步信息输出功能处于关闭状态

说明

- 在当前命令行提示符下，如果用户没有任何输入，此时若有日志等系统信息输出，输出后将不会回显命令行提示符；
- 当处在交互状态，需要用户输入一些交互信息时（非 Y/N 确认信息），因为情况各异，所以若有系统信息输出，输出后不再回显提示信息，而只是将用户已有的输入换行打印出来。

1.2.12 禁止端口生成Link up/Link down日志信息

缺省情况下，设备的所有端口在端口状态改变时都会生成端口 Link up 和 Link down 的日志信息。如果用户只关心某个或某些端口的状态，这时可以使用该功能，禁止其它端口生成 Link up/Link down 日志信息；或者某个接口的状态不稳定，总在频繁地改变，这时，会生成大量的 Link up/Link down 日志信息，为了屏蔽这些冗余信息，可以使用该功能禁止该端口生成 Link up/Link down 日志信息。

表1-19 禁止端口生成 Link up/Link down 日志信息

操作	命令	说明
进入系统视图	**system-view**	-
进入三层以太网端口视图或者二层以太网端口视图或者VLAN接口视图	**interface** *interface-type interface-number*	-
禁止端口生成Link up/Link down日志信息	**undo enable log updown**	必选 缺省情况下，允许所有端口在状态发生改变时生成端口Link up和Link down的日志信息

说明

使用本特性后，如果端口状态改变，将不再生成端口 Link up 和 Link down 的日志信息。这样，可能会影响用户监控端口状态，所以，一般情况下，建议采用缺省配置。

1.2.13 配置日志文件写保护

使能日志文件写保护功能后，当日志文件达到限额或存储空间不足时，不允许向日志文件中写入新的日志信息。

表1-20 配置日志文件写保护

操作	命令	说明
进入系统视图	**system-view**	-
配置日志文件写保护功能	**info-center logfile overwrite-protection** [**all-port-powerdown**]	必选 缺省情况下，没有配置日志文件写保护功能

说明

- 配置 **all-port-powerdown** 参数时，设备将关闭所有物理以太网端口，管理以太网口、配置了双机热备的端口及配置了 IRF 的端口除外。
- 仅 FIPS 模式下支持日志文件写保护功能。

1.3 信息中心显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后信息中心的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset logbuffer**、**reset trapbuffer** 命令可以分别将日志缓冲区和告警缓冲区的统计信息清除。

表1-21 信息中心显示和维护

操作	命令
显示信息通道的信息	**display channel** [*channel-number* | *channel-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示各个输出方向的信息	**display info-center** [| { **begin** | **exclude** | **include** } *regular-expression*]
显示系统日志缓冲区的状态和缓冲区记录的日志信息	**display logbuffer** [**reverse**] [**level** *severity* | **size** *buffersize* | **slot** *slot-number*] * [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示系统日志缓冲区的概要信息	**display logbuffer summary** [**level** *severity* | **slot** *slot-number*] * [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示日志文件缓冲区内容	**display logfile buffer** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示日志文件配置	**display logfile summary** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示系统告警缓冲区的状态和缓冲区记录的告警信息	**display trapbuffer** [**reverse**] [**size** *buffersize*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除日志缓冲区内的信息	**reset logbuffer**
清除告警缓冲区内的信息	**reset trapbuffer**

1.4 信息中心典型配置举例

1.4.1 日志发送到Unix日志主机的配置举例

1. 组网需求

- 将系统的日志信息发送到 Unix 日志主机；
- 日志主机的 IP 地址为 1.2.0.1/16；
- 信息级别高于等于 informational 的日志信息将会发送到日志主机上；
- 允许输出日志信息的模块为 ARP 和 IP。

2. 组网图

图1-2 配置信息中心组网图（Unix 日志主机）

3. 配置步骤

配置前请确保 Device 和 PC 之间路由可达，具体配置步骤略。

(1) 设备上的配置

开启信息中心。

```
<Sysname> system-view
[Sysname] info-center enable
```

将 IP 地址为 1.2.0.1/16 的主机用作日志主机，使用 loghost 通道发送信息（可选，系统缺省为 loghost 通道），使用 local4 作为日志主机记录工具。

```
[Sysname] info-center loghost 1.2.0.1 channel loghost facility local4
```

关闭 loghost 通道所有模块 log、trap、debug 信息的输出开关。

```
[Sysname] info-center source default channel loghost debug state off log state off trap state off
```

注意

由于系统对各通道允许输出的系统信息的缺省情况不一样，所以配置前必须将所有模块的需求通道（本例为 loghost）上 log、trap、debug 信息的输出开关关闭，再根据当前的需求配置输出规则，以免输出太多不需要的信息。

配置输出规则：允许 ARP 和 IP 模块的、级别高于等于 informational 的日志信息输出到日志主机（注意：允许输出信息的模块由产品决定）。

```
[Sysname] info-center source arp channel loghost log level informational state on
[Sysname] info-center source ip channel loghost log level informational state on
```

(2) 日志主机上的配置

下面的配置示例是在 Solaris 上完成的，在其它厂商的 Unix 操作系统上的配置操作基本类似。

第一步：以超级用户（root）的身份登录日志主机。

第二步：在/var/log/路径下为 Device 创建同名日志文件夹 Device，在该文件夹创建文件 info.log，用来存储来自 Device 的日志。

```
# mkdir /var/log/Device
# touch /var/log/Device/info.log
```

第三步：编辑文件/etc/syslog.conf，添加以下内容。

```
# Device configuration messages
local4.info     /var/log/Device/info.log
```

以上配置中，local4 表示日志主机接收日志的工具名称，info 表示信息级别。Unix 系统会把级别高于等于 informational 的日志记录到/var/log/Device/info.log 文件中。

说明

在编辑/etc/syslog.conf 时应注意以下问题：

- 注释必须独立成行，并以字符#开头。
- 在文件名之后不得有多余的空格。
- /etc/syslog.conf 中指定的工具名称及信息级别与设备上 **info-center loghost** 和 **info-center source** 命令的相应参数的指定值要保持一致，否则日志信息可能无法正确输出到日志主机上。

第四步：当日志文件 info.log 建立且/etc/syslog.conf 文件被修改之后，应通过执行以下命令查看系统守护进程 syslogd 的进程号，中止 syslogd 进程，并重新用-r 选项在后台启动 syslogd，使修改后配置生效。

```
# ps -ae | grep syslogd
147
# kill -HUP 147
# syslogd -r &
```

进行以上操作之后，系统就可以在相应的文件中记录日志信息了。

1.4.2 日志发送到Linux日志主机的配置举例

1. 组网需求

- 系统的日志信息发送到 Linux 日志主机上，日志主机的 IP 地址为 1.2.0.1/16；
- 信息级别高于等于 informational 的日志信息将会发送到日志主机上；
- 所有模块均允许输出日志信息。

2. 组网图

图1-3 配置信息中心组网图（Linux 日志主机）

3. 配置步骤

配置前请确保 Device 和 PC 之间路由可达，具体配置步骤略。

(1) 设备上的配置

开启信息中心。

```
<Sysname> system-view
[Sysname] info-center enable
```

将 IP 地址为 1.2.0.1/16 的主机用作日志主机，使用 loghost 通道发送信息（可选，系统缺省为 loghost 通道），使用 local5 作为日志主机记录工具。

```
[Sysname] info-center loghost 1.2.0.1 channel loghost facility local5
```

关闭 loghost 通道所有模块 log、trap、debug 信息的输出开关。

```
[Sysname] info-center source default channel loghost debug state off log state off trap state
off
```

注意

由于系统对各通道允许输出的系统信息的缺省情况不一样，所以配置前必须将所有模块的需求通道（本例为 loghost）上 log、trap、debug 信息的输出开关关闭，再根据当前的需求配置输出规则，以免输出太多不需要的信息。

配置输出规则：允许所有模块、级别高于等于 informational 的日志信息输出到日志主机。

```
[Sysname] info-center source default channel loghost log level informational state on
```

(2)　日志主机上的配置

第一步：以超级用户（root）的身份登录日志主机。

第二步：在/var/log/路径下为 Device 创建同名日志文件夹 Device，在该文件夹创建文件 info.log，用来存储来自 Device 的日志。

```
# mkdir /var/log/Device
# touch /var/log/Device/info.log
```

第三步：编辑文件/etc/syslog.conf，添加以下内容。

```
# Device configuration messages
local5.info     /var/log/Device/info.log
```

以上配置中，local5 表示日志主机接收日志的工具名称，info 表示信息级别。Linux 系统会把级别高于等于 informational 的日志记录到/var/log/Device/info.log 文件中。

说明

在编辑/etc/syslog.conf 时应注意以下问题:

- 注释必须独立成行，并以字符#开头。
- 在文件名之后不得有多余的空格。
- /etc/syslog.conf 中指定的工具名称及信息级别与设备上 **info-center loghost** 和 **info-center source** 命令的相应参数的指定值要保持一致，否则日志信息可能无法正确输出到日志主机上。

第四步：当日志文件 info.log 建立且/etc/syslog.conf 文件被修改之后，应通过执行以下命令查看系统守护进程 syslogd 的进程号，中止 syslogd 进程，并重新用-r 选项在后台启动 syslogd，使修改后配置生效。

```
# ps -ae | grep syslogd
147
# kill -9 147
# syslogd -r &
```

说明

对 Linux 日志主机，必须保证 syslogd 进程是以-r 选项启动。

进行以上操作之后，系统就可以在相应的文件中记录日志信息了。

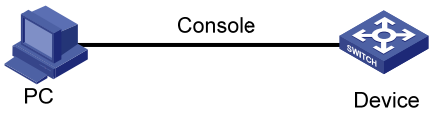
1.4.3 日志发送到控制台的配置举例

1. 组网需求

- 将信息级别高于等于 informational 的日志信息发送到控制台上；
- 允许输出日志信息的模块为 ARP 和 IP。

2. 组网图

图1-4 配置信息中心组网图（控制台）



3. 配置步骤

开启信息中心。

```
<Sysname> system-view
[Sysname] info-center enable
```

使用 console 通道向控制台输出日志信息（可选，缺省情况下系统向控制台输出信息的通道就为 console 通道）。

```
[Sysname] info-center console channel console
```

关闭控制台通道所有模块 log、trap、debug 信息的输出开关。

```
[Sysname] info-center source default channel console debug state off log state off trap state off
```

注意

由于系统对各通道允许输出的系统信息的缺省情况不一样，所以配置前必须将所有模块的需求通道（本例为 console）上 log、trap、debug 信息的输出开关关闭，再根据当前的需求配置输出规则，以免输出太多不需要的信息。

配置输出规则：允许 ARP 和 IP 模块的、级别高于等于 informational 的日志信息输出（注意：允许输出的信息模块由产品决定）。

```
[Sysname] info-center source arp channel console log level informational state on
[Sysname] info-center source ip channel console log level informational state on
[Sysname] quit
```

打开终端显示功能（可选，缺省已经打开了该功能）。

```
<Sysname> terminal monitor
Info: Current terminal monitor is on.
<Sysname> terminal logging
Info: Current terminal logging is on.
```

以上命令配置成功后，如果指定的模块产生了日志信息，信息中心会自动把这些日志发送到控制台，在控制台的屏幕上显示。

1.4.4 安全日志同步保存功能配置举例

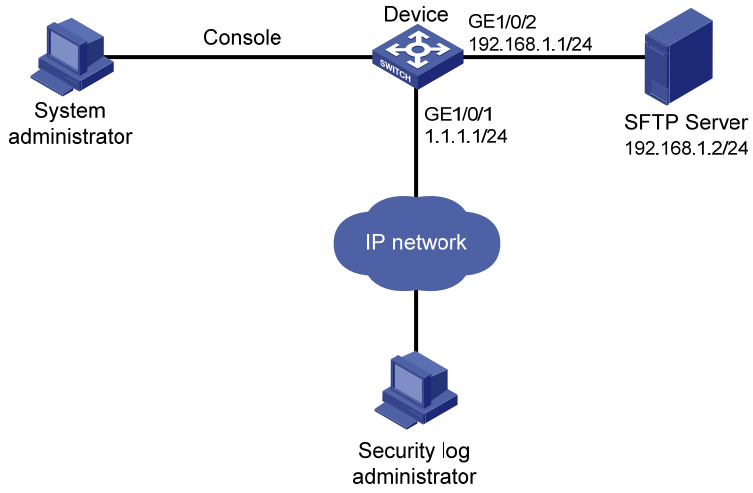
1. 组网需求

为了高效、便捷的查看设备上发生的与安全相关的事件，及时了解设备的安全状态，要求：

- 将安全日志保存到专门的安全日志文件 Flash:/securitylog/seclog.log，保存频率为每小时一次；
- 只有安全日志审计员能够查看安全日志文件内容，其它用户登录设备后都不能对安全日志文件查看、拷贝、重命名等操作。

2. 组网图

图1-5 安全日志功能组网图



3. 配置思路

针对本举例，配置分两大部分：

(1) 以系统管理员身份登录设备

- 使能安全日志同步保存功能，并设置安全日志文件的自动保存频率为 1 小时。
- 创建一个本地用户 seclog，密码为 123123123123。授权用户可以管理安全日志文件，即使用 **authorization-attribute** 命令配置两个授权属性：**level** 为 3 以及 **user-role** 为 **security-audit**；使用 **service-type** 命令配置用户可以使用的登录方式；
- 配置用户界面的认证方式为 **scheme**，保证只有通过 AAA 本地认证的用户才能查看、操作安全日志文件。

(2) 以安全日志管理员身份登录设备

- 设置安全日志文件的保存路径为 Flash:/securitylog/seclog.log。
- 查看安全日志文件内容，了解设备安全状态。

4. 配置步骤

(1) 系统管理员需要执行的配置

使能安全日志同步保存功能，并设置安全日志文件的自动保存频率为 1 小时。

```
<Sysname> system-view
[Sysname] info-center security-logfile enable
[Sysname] info-center security-logfile frequency 3600
```

创建本地用户 seclog，密码为 123123123123。

```
[Sysname] local-user seclog
New local user added.
[Sysname-luser-seclog] password simple 123123123123
```

授权用户可以管理安全日志文件。

```
[Sysname-luser-seclog] authorization-attribute level 3 user-role security-audit
```

设置用户可以使用的登录方式为 SSH、Telnet、Terminal。

```
[Sysname-luser-seclog] service-type ssh telnet terminal
[Sysname-luser-seclog] quit
```

根据组网规划可以看出，用户将使用 SSH 或 Telnet 登录设备，所以配置 VTY 用户界面的认证方式为 scheme。

```
[Sysname] display user-interface vty ?
  INTEGER<0-15>  Specify one user terminal interface
```

以上信息表明，设备支持 16 个 VTY，编号从 0 到 15。

```
[Sysname] user-interface vty 0 15
[Sysname-ui-vty0-15] authentication-mode scheme
[Sysname-ui-vty0-15] quit
```

(2)　安全日志管理员需要执行的配置

使用用户名 seclog 重新登录设备。

```
C:/> telnet 1.1.1.1
******************************************************************************
* Copyright (c) 2004-2011 Hangzhou H3C Tech. Co., Ltd. All rights reserved.  *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************


Login authentication


Username:seclog
Password:
<Sysname>
```

显示安全日志文件摘要信息。

```
<Sysname> display security-logfile summary
  Security-log is enabled.
  Security-log file size quota: 1MB
  Security-log file directory: flash:/seclog
  Alarm-threshold: 80%
  Current usage: 0%
  Writing frequency: 1 hour 0 min 0 sec
```

以上信息表明，安全日志文件当前的存储路径为 flash:/seclog。

设置安全日志文件的保存路径为 Flash:/securitylog。

```
<Sysname> mkdir securitylog
.
%Created dir flash:/securitylog.
<Sysname> info-center security-logfile switch-directory flash:/securitylog/
```

查看安全日志文件缓存区内容。

```
<Sysname> display security-logfile buffer
%@175 Jan  2 17:02:53:766 2011 Sysname SHELL/4/LOGOUT:
 Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.2<hh3cLogOut>: logout from Console
%@176 Jan  2 17:02:53:766 2009 Sysname SHELL/5/SHELL_LOGOUT:Console logged out from aux0.
……其它日志略……
```

以上信息表明，安全日志文件缓存区中还有最新内容没有保存到安全日志文件。

手工触发将安全日志文件缓存区内容保存到安全日志文件。

```
<Sysname> security-logfile save
Info: Save all the contents in the security log buffer into file flash:/securitylog/seclog.log
successfully.
```

查看安全日志文件的内容。

```
<Sysname> more securitylog/seclog.log
%@157 Jan  2 16:12:01:750 2011 Sysname SHELL/4/LOGIN:
 Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1<hh3cLogIn>: login from Console
%@158 Jan  2 16:12:01:750 2011 Sysname SHELL/5/SHELL_LOGIN:Console logged in from aux0.
……其它日志略……
```

目 录

1 SNMP配置

1.1 SNMP简介

SNMP（Simple Network Management Protocol，简单网络管理协议）是因特网中的一种网络管理标准协议，被广泛用于实现管理设备对被管理设备的访问和管理。SNMP 具有以下特点：

- 支持网络设备的智能化管理。利用基于 SNMP 的网络管理平台，网络管理员可以查询网络设备的运行状态和参数，设置参数值，发现故障、完成故障诊断，进行容量规划和生成报告。
- 支持对不同物理特性的设备进行管理。SNMP 只提供最基本的功能集，使得管理任务与被管理设备的物理特性和联网技术相对独立，从而实现对不同厂商设备的管理。

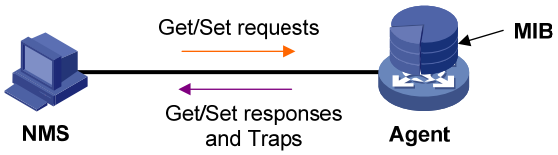
1.1.1 SNMP的工作机制

SNMP 网络环境中包含 NMS 和 Agent 两种元素：

- NMS（Network Management Station，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，方便网络管理员完成网络管理工作。
- Agent 是 SNMP 网络环境中的被管理者，负责接收、处理来自 NMS 的请求报文。在一些紧急情况下，如接口状态发生改变等，Agent 会主动向 NMS 发送告警信息。

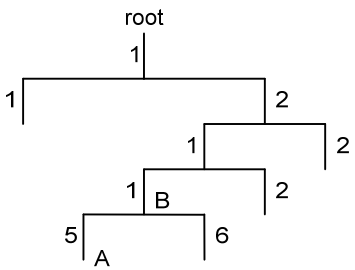
NMS 管理设备的时候通过 MIB（Management Information Base，管理信息库）对设备进行管理。MIB 定义了节点之间的层次关系以及对象的一系列属性，比如对象的名字、访问权限和数据类型等。每个 Agent 都有自己的 MIB。被管理设备都有自己的 MIB 文件，在 NMS 上编译这些 MIB 文件，就能生成该设备的 MIB。NMS 根据访问权限对 MIB 节点进行读/写操作，从而实现对 Agent 的管理。NMS、Agent 和 MIB 之间的关系如下图所示。

图1-1 NMS、Agent 和 MIB 关系图



MIB 是按照树型结构组织的，它由很多个节点组成，每个节点表示被管理对象，被管理对象可以用从根开始的一串表示路径的数字唯一地识别，这串数字称为 OID（Object Identifier，对象标识符）”。如下图所示，被管理对象 B 可以用一串数字{1.2.1.1}唯一确定，这串数字就是被管理对象 B 的 OID。

图1-2 MIB 树结构



SNMP 提供以下基本操作来实现 NMS 和 Agent 的交互：

- GET 操作：NMS 使用该操作查询 Agent MIB 中的一个或多个节点的值。
- SET 操作：NMS 使用该操作设置 Agent MIB 中的一个或多个节点的值。

- Trap 操作：Agent 使用该操作向 NMS 发送告警信息。

1.1.2 SNMP的协议版本

目前 Agent 支持 SNMPv1、SNMPv2c 和 SNMPv3 三种版本：

- 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 对 Agent 的访问。如果 NMS 访问被管理设备时携带的团体名和被管理设备上设置的团体名不同，则不能建立 SNMP 连接，从而导致访问失败。
- 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。网络管理员可以设置认证和加密功能。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。

说明

NMS 和 Agent 成功建立连接的前提条件是 NMS 和 Agent 使用的 SNMP 版本必须相同。

1.2 SNMP配置任务简介

表1-1 SNMP 配置任务简介

配置任务	说明	详细配置
配置SNMP基本参数	必选	1.3
配置接口网管索引	可选	1.4
配置SNMP日志	可选	1.5
配置SNMP Trap	可选	1.6

1.3 配置SNMP基本参数

由于SNMPv3 版本的配置和SNMPv1 版本、SNMPv2c版本的配置有较大区别，所以下面分两种情况进行SNMP基本功能的配置介绍，详见 表 1-2 和 表 1-3。

1.3.1 配置SNMPv3 版本基本参数

使用 SNMPv3 版本时，需要先创建一个 SNMP 组并设置该组的访问权限和认证、加密功能，然后创建一个 SNMPv3 用户并设置该用户的属性。

表1-2 配置 SNMP 基本参数（SNMPv3 版本）

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
启动SNMP Agent服务	**snmp-agent**	可选 缺省情况下，SNMP Agent服务处于关闭状态 执行除**snmp-agent calculate-password**和**snmp-agent ifmib long-ifindex enable**外任何以**snmp-agent**开头的命令，都可以启动SNMP Agent服务
设置系统信息	**snmp-agent sys-info** { **contact** *sys-contact* | **location** *sys-location* | **version** { **all** | { **v1** | **v2c** | **v3** } * } }	可选 缺省情况下，系统维护联系信息为“Hangzhou H3C Tech. Co., Ltd.”。物理位置信息为“Hangzhou, China”。版本为SNMP v3 FIPS模式下不支持**all**、**v1**、**v2c**参数
设置本地SNMP实体的引擎ID	**snmp-agent local-engineid** *engineid*	可选 缺省情况下，设备引擎ID为公司的“企业号＋设备信息”
创建MIB视图或更新MIB视图内容	**snmp-agent mib-view** { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]	可选 缺省情况下，设备上已存在MIB视图ViewDefault，OID为1
创建SNMPv3组	**snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	必选 缺省情况下，不存在任何SNMP组，新创建的SNMP组采用不认证、不加密方式
计算用户给定明文密码通过加密算法处理后的密文密码	**snmp-agent calculate-password** *plain-password* **mode** { **3desmd5** | **3dessha** | **md5** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }	可选 FIPS模式下不支持**3desmd5**、**3dessha**、**md5**参数
创建SNMPv3用户	**snmp-agent usm-user v3** *user-name group-name* [[**cipher**] **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **des56** } *priv-password*]] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	必选 FIPS模式下不支持**md5**、**3des**、**des56**参数
设置Agent能处理的SNMP报文的最大长度	**snmp-agent packet max-size** *byte-count*	可选 缺省情况下，Agent能接收/发送的SNMP消息包长度的最大值为1500字节
配置SNMP响应报文的DSCP优先级	**snmp-agent packet response dscp** *dscp-value*	可选 缺省情况下，SNMP响应报文的DSCP优先级为0

注意

- SNMPv3 版本的用户名、密文密码等的生成都和引擎 ID 相关联，如果更改了引擎 ID，则原引擎 ID 下配置的用户名、密码失效。
- MIB 视图是 MIB 的子集，由视图名和 MIB 子树来唯一确定一个 MIB 视图。视图名相同但包含的子树不同，则认为是不同的视图。除缺省视图外，用户最多可以创建 16 个 MIB 视图。

1.3.2 配置SNMPv1/v2c版本基本参数

说明

FIPS 模式下不支持该功能。

使用 SNMPv1 或 SNMPv2c 版本时，需要先设置 Agent 启用的 SNMP 版本号，然后设置访问权限，访问权限的设置方法有两种：

- 直接设置，即通过指定团体名的方式创建一个 SNMP 团体。
- 间接设置，即先创建一个 SNMP 组，然后为该 SNMP 组添加一个新用户，用户名相当于 SNMPv1 和 SNMPv2c 版本的团体名。

表1-3 配置 SNMP 基本参数（SNMPv1 版本、SNMPv2c 版本）

操作			命令	说明
进入系统视图			**system-view**	-
启动SNMP Agent服务			**snmp-agent**	可选 缺省情况下，SNMP Agent服务处于关闭状态 执行除 **snmp-agent calculate-password** 和 **snmp-agent ifmib long-ifindex enable** 外任何以 **snmp-agent** 开头的命令，都可以启动SNMP Agent服务
设置系统信息			**snmp-agent sys-info** { **contact** *sys-contact* | **location** *sys-location* | **version** { **all** | { **v1** | **v2c** | **v3** } * } }	必选 缺省情况下，系统维护联系信息为“Hangzhou H3C Tech. Co., Ltd.”。物理位置信息为“Hangzhou, China”。版本为SNMP v3
设置本地SNMP实体的引擎ID			**snmp-agent local-engineid** *engineid*	可选 缺省情况下，设备引擎ID为公司的“企业号＋设备信息”。
创建或更新MIB视图内容			**snmp-agent mib-view** { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]	可选 缺省情况下，视图名为ViewDefault，OID为1
设置访问权限	直接设置	创建一个新的SNMP团体	**snmp-agent community** { **read** | **write** } *community-name* [**mib-view** *view-name*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	二者必选其一 直接设置是以指定SNMPv1和SNMPv2c版本的团体名的方式进行设

操作			命令	说明
	间接设置	创建一个SNMP组	**snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	置 间接设置采用与SNMPv3版本类似的命令形式，添加用户到指定的组，用户名相当于SNMPv1和SNMPv2c版本的团体名 缺省情况下，不存在任何SNMP组
		为一个SNMP组添加一个新用户	**snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	
设置Agent能处理的SNMP报文的最大长度			**snmp-agent packet max-size** *byte-count*	可选 缺省情况下，Agent能接收/发送的SNMP消息包长度的最大值为1500字节
配置SNMP响应报文的DSCP优先级			**snmp-agent packet response dscp** *dscp-value*	可选 缺省情况下，SNMP响应报文的DSCP优先级为0

注意

MIB 视图是 MIB 的子集，由视图名和 MIB 子树来唯一确定一个 MIB 视图。视图名相同但包含的子树不同，则认为是不同的视图。除缺省视图外，用户最多可以创建 16 个 MIB 视图。

1.4 配置接口网管索引

1.4.1 接口网管索引简介

接口网管索引是设备提供给 NMS 使用的一个参数，用来标识一个接口。

接口网管索引有两种表达方式：

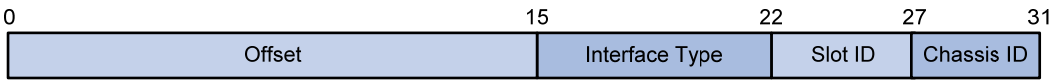
1. 16 比特模式接口网管索引

16 比特模式接口网管索引是一个从 1 开始递增的编号，长度为 16 比特。各个接口的接口网管索引由系统动态分配、顺序递增。16 比特模式接口网管索引仅用来唯一地标识一个接口。

2. 32 比特模式接口网管索引

32 比特模式的接口网管索引长度为 32 比特，如 图 1-3 所示，32 比特模式的接口网管索引由如下几部分信息组成：Offset、Interface Type、Slot ID、Chassis ID。

图1-3 32 比特接口网管索引信息



- Offset：接口偏移量，长度为 16 比特，用于区分同一接口板上相同类型的不同接口。
- Interface Type：接口类型所对应的枚举值，长度为 7 比特，最大支持 128 种接口，目前支持的接口类型有 80 多种。
- Slot ID：接口所在的物理槽位号，长度为 5 比特。
- Chassis ID：长度为 4 比特，对于分布式 IRF 设备，本字段表示接口所在成员设备的编号。对于其它类型的设备，本字段没有意义，取值均为 0。

1.4.2 切换接口网管索引模式

通常情况下，接口网管索引使用缺省模式（16 比特模式）即可。接口网管索引使用模式的选择原则为：

- 如果 NMS 需要使用 32 比特模式的接口网管索引，则可以将接口网管索引切换到 32 比特模式（32 比特模式会携带接口所在的槽位等信息）。
- 如果 NMS 运行的网络协议不支持 32 比特的接口网管索引，则必须将接口网管索引切换到 16 比特模式。

比如 Netstream 版本 5 和 Netstream 版本 8 报文只为接口网管索引预留了 16 个比特，则运行 Netstream 版本 5 或 Netstream 版本 8 时，接口网管索引只能配置为 16 比特模式；Netstream 版本 9 报文为接口网管索引预留了 32 个比特，则运行 Netstream 版本 9 时，接口网管索引可以配置为 16 比特模式或 32 比特模式。

表1-4 切换接口网管索引

操作	命令	说明
进入系统视图	**system-view**	-
切换接口网管索引为32比特模式	**snmp-agent ifmib long-ifindex enable**	可选 缺省情况下，接口网管索引为16比特模式
切换接口网管索引为16比特模式	**undo snmp-agent ifmib long-ifindex enable**	可选 缺省情况下，接口网管索引为16比特模式

注意

对于某些依赖接口网管索引作为参数的配置，切换接口网管索引模式会导致这些配置失效（当接口网管索引切换回原来的模式时，这些配置会重新生效）。此时需要使用新的接口网管索引重新配置，之前的配置才能继续生效。例如在 RMON 告警组、扩展告警组的配置中，当告警变量需要使用“OID/变量名.接口网管索引”来表示，并且接口网管索引模式切换时，会导致配置的 RMON 告警组失效。用户如果需要继续监控此节点，需要使用新的接口网管索引重新配置。

1.5 配置SNMP日志

SNMP 日志可以记录 NMS 对 Agent 的 GET 请求、SET 请求和 SET 响应信息，不能记录 GET 响应信息。

- 当进行 GET 操作时，Agent 会记录 NMS 用户的 IP 地址、GET 操作的节点名和节点 OID。
- 当进行 SET 操作时，Agent 会记录 NMS 用户的 IP 地址、SET 操作的节点名、节点 OID、节点值以及 SET 操作返回的错误码和错误索引。

这些日志将被发送到设备的信息中心，级别为 informational，即作为设备的一般提示信息。通过设置信息中心的参数，最终决定 SNMP 日志的输出规则（即是否允许输出以及输出方向）。

表1-5 配置 SNMP 日志功能

操作	命令	说明
进入系统视图	**system-view**	-
打开SNMP日志开关	**snmp-agent log { all | get-operation | set-operation }**	必选 缺省情况下，SNMP日志开关处于关闭状态

说明

- 大量的日志记录会占用设备的存储空间，影响设备的性能。正常情况下，建议关闭 SNMP 日志功能。
- SNMP 每条日志信息中记录的 node 域（信息内容对应的 MIB 节点名）和 value 域（信息内容对应的 MIB 节点值）的长度之和不能超过 1024 字节，超出的部分将不会被输出。
- 有关日志输出规则、系统信息、信息中心的详细介绍请参见“网络管理和监控配置指导”中的“信息中心”。

1.6 配置SNMP Trap

1.6.1 配置Trap功能

Agent 主动向 NMS 发送 Trap 信息，用于报告一些紧急的重要事件（如被管理设备重新启动等）。Trap 报文有两种：

- 通用 Trap。设备支持的通用 Trap 包括 authentication、coldstart、linkdown、linkup 和 warmstart 五种（其它均为企业自定义 Trap）。
- 企业自定义 Trap。

Trap 信息会占用设备内存较多，影响设备性能，建议用户根据需要开启指定模块的 Trap 功能。

开启模块的 Trap 功能后，该模块生成的 Trap 报文将被发送到设备的信息中心。用户可以根据各模块生成的 Trap 信息的级别设置信息中心参数，决定 Trap 报文的输出规则（即是否允许输出以及输出方向）。

表1-6 配置 Trap 功能

操作	命令	说明
进入系统视图	**system-view**	-
开启Trap功能	**snmp-agent trap enable** [**arp rate-limit** | **bgp** | **configuration** | **default-route** | **flash** | **mpls** | **ospf** [*process-id*] [**ifauthfail** | **ifcfgerror** | **ifrxbadpkt** | **ifstatechange** | **iftxretransmit** | **lsdbapproachoverflow** | **lsdboverflow** | **maxagelsa** | **nbrstatechange** | **originatelsa** | **vifcfgerror** | **virifauthfail** | **virifrxbadpkt** | **virifstatechange** | **viriftxretransmit** | **virnbrstatechange**] * | **pim** [**candidatebsrwinelection** | **electedbsrlostelection** | **interfaceelection** | **invalidjoinprune** | **invalidregister** | **neighborloss** | **rpmappingchange**] * | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] * | **system** | **vrrp** [**authfailure** | **newmaster**]]	必选 缺省情况下，Trap功能处于开启状态
进入二层以太网端口视图或三层以太网端口视图或VLAN接口视图	**interface** *interface-type interface-number*	必选
开启接口状态变化的Trap功能	**enable snmp trap updown**	必选 缺省情况下，接口下接口状态变化的Trap功能处于开启状态

说明

- 如果要求端口在状态发生改变时生成接口状态变化的 Trap 报文，需要在接口下和全局都开启接口状态变化的 Trap 功能。
- 要使各个模块生成相应的 Trap 报文，除了使用 **snmp-agent trap enable** 命令开启 Trap 功能外，还可能需要执行各个模块的相关配置，详情请参见各模块的相关描述。
- 有关信息中心的详细介绍请参见“网络管理和监控配置指导”中的“信息中心”。

1.6.2 配置Trap报文发送参数

如果要将 Trap 发送给 NMS，必须先完成以下配置：

- 完成 SNMP 基本配置（如果使用 SNMPv1 和 SNMPv2c 版本需要设置启用的 SNMP 版本和团体名；如果使用 SNMP v3 版本需要设置用户名和 MIB 视图），这些参数的配置必须和 NMS 上的配置相同。
- 确保设备与 NMS 路由可达。

当收到 Trap 报文后，SNMP 模块有两种处理方式：

- 将 Trap 报文存在消息队列里（在网络出现故障时，消息队列用于缓存 Trap 报文，在网络恢复后，系统会将消息队列中的 Trap 报文依次发出，用户可以设置该队列的长度、Trap 报文在队列里的保存时间）；
- 将 Trap 报文直接发送给指定的目标主机（通常为 NMS）等。

表1-7 配置 Trap 报文发送参数

操作	命令	说明
进入系统视图	**system-view**	-
设置Trap报文的目标主机属性	**snmp-agent target-host trap address udp-domain** { *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] [**dscp** *dscp-value*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]	可选 如果要将Trap信息发送给NMS，该步骤为必选，并将*ip-address*指定为NMS的IP地址 FIPS模式下不支持**v1**、**v2c**参数
设置Trap报文的源地址	**snmp-agent trap source** *interface-type interface-number*	可选 缺省情况下，由SNMP选择一个接口的IP地址作为Trap报文源IP地址
对标准linkUp/linkDown Trap报文进行私有扩展	**snmp-agent trap if-mib link extended**	可选 缺省情况下，使用的是RFC定义的标准linkUp/linkDown Trap报文
设置Trap报文发送队列的长度	**snmp-agent trap queue-size** *size*	可选 缺省情况下，Trap报文的消息队列最多可以存储100条Trap消息
设置Trap报文的保存时间	**snmp-agent trap life** *seconds*	可选 缺省情况下，Trap报文的保存时间为120秒

说明

- 对 linkUp/linkDown Trap 报文进行私有扩展后，设备生成和发送的 linkUp/linkDown Trap 报文由标准 linkUp/linkDown Trap 报文后增加接口描述和接口类型信息构成。如果 NMS 不支持该扩展报文，请禁用私有扩展功能，使设备发送标准的 linkUp/linkDown Trap 报文。
- 如果在 Trap 报文的发送队列已满时系统又收到了新的 Trap 报文，系统会自动删除最先收到的 Trap 报文。
- 如果发送队列中的 Trap 报文到达了已设定的保存时间，系统会自动删除该 Trap 报文。

1.7 SNMP显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 SNMP 的运行情况，通过查看显示信息验证配置的效果。

表1-8 SNMP 显示和维护

操作	命令
显示系统维护联络信息、系统位置信息及SNMP版本信息	**display snmp-agent sys-info** [**contact** | **location** | **version**] * [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示SNMP报文统计信息	**display snmp-agent statistics** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示设备的SNMP实体引擎ID	**display snmp-agent local-engineid** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示SNMP组信息	**display snmp-agent group** [*group-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示Trap消息队列的基本信息	**display snmp-agent trap queue** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示系统当前可以发送Trap消息的模块及其Trap消息的使能状态	**display snmp-agent trap-list** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示SNMPv3用户信息	**display snmp-agent usm-user** [**engineid** *engineid* | **username** *user-name* | **group** *group-name*] * [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示SNMPv1或SNMPv2c团体信息（FIPS模式下不支持该命令）	**display snmp-agent community** [**read** | **write**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示MIB视图的信息	**display snmp-agent mib-view** [**exclude** | **include** | **viewname** *view-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.8 SNMP典型配置举例

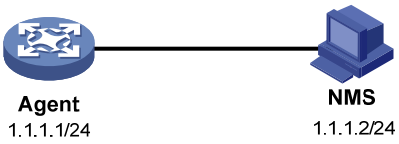
1.8.1 SNMPv1/v2c典型配置举例

1. 组网需求

- NMS 与 Agent 相连，NMS 的 IP 地址为 1.1.1.2/24，Agent 的 IP 地址为 1.1.1.1/24。
- NMS 通过 SNMPv1 或 SNMPv2c 对 Agent 进行监控管理，Agent 在出现故障时能主动向 NMS 发送 Trap 报文。

2. 组网图

图1-4 配置 SNMPv1/v2c 组网图



3. 配置步骤

(1) 配置 Agent

配置 Agent 的 IP 地址为 1.1.1.1/24，并确保 Agent 与 NMS 之间路由可达。（配置步骤略）

设置 Agent 使用的 SNMP 版本为 v1/v2c、只读团体名为 public，读写团体名为 private。

```
<Agent> system-view
[Agent] snmp-agent sys-info version v1 v2c
[Agent] snmp-agent community read public
[Agent] snmp-agent community write private
```

设置 Agent 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
```

设置允许向 NMS 发送 Trap 报文，使用的团体名为 public。

```
[Agent] snmp-agent trap enable
[Agent] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname public
v1
[Agent] quit
```

snmp-agent target-host 命令中指定的版本必须和 NMS 上运行的 SNMP 版本一致，如果 NMS 上运行的是 SNMPv2c 版本，则需要将 **snmp-agent target-host** 命令中的版本参数设置为 v2c。否则，NMS 无法正确接收 Trap 信息。

(2) 配置 NMS

设置 NMS 使用的 SNMP 版本为 SNMPv1/v2c，只读团体名为 public，读写团体名为 private。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，否则无法进行相应操作。

---

(3) 结果验证

通过查询 Agent 上的相应 MIB 节点获取已发送 Trap 信息的数量：

```
Send request to 1.1.1.1/161 ...
Protocol version: SNMPv1
Operation: Get
Request binding:
1: 1.3.6.1.2.1.11.29.0
Response binding:
1: Oid=snmpOutTraps.0 Syntax=CNTR32 Value=18
Get finished
```

当使用错误的团体名获取 Agent 上的 MIB 节点信息时，NMS 上将看到认证失败的 Trap 信息：

```
1.1.1.1/2934 V1 Trap = authenticationFailure
SNMP Version = V1
Community = public
```

```
Command = Trap
Enterprise = 1.3.6.1.4.1.43.1.16.4.3.50
GenericID = 4
SpecificID = 0
Time Stamp = 8:35:25.68
```

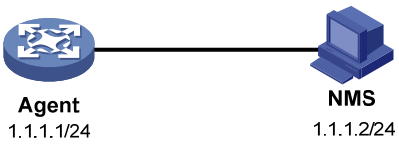
1.8.2 SNMPv3 典型配置举例

1. 组网需求

- NMS 与 Agent 相连，NMS 的 IP 地址为 1.1.1.2/24，Agent 的 IP 地址为 1.1.1.1/24。
- NMS 通过 SNMPv3 只能对 Agent 的 SNMP 报文的相关信息进行监控管理，Agent 在出现问题的时候能够主动向 NMS 发送 Trap 报文。
- NMS 与 Agent 建立 SNMP 连接时，需要认证，认证算法为 MD5，认证密码为 authkey。NMS 与 Agent 之间传输的 SNMP 报文需要加密，使用的加密协议为 DES56，加密密码为 prikey。

2. 组网图

图1-5 配置 SNMPv3 组网图



3. 配置步骤

(1) 配置 Agent

配置 Agent 的 IP 地址为 1.1.1.1/24，并确保 Agent 与 NMS 之间路由可达。（配置步骤略）

设置访问权限：用户只能读写节点 snmp（OID 为 1.3.6.1.2.1.11）下的对象，不可以访问其它 MIB 对象。

```
<Agent> system-view
[Agent] undo snmp-agent mib-view ViewDefault
[Agent] snmp-agent mib-view included test snmp
[Agent] snmp-agent group v3 managev3group read-view test write-view test
```

设置 Agent 使用的用户名为 managev3user，认证算法为 MD5，认证密码为 authkey，加密算法为 DES56，加密密码是 prikey。

```
[Agent] snmp-agent usm-user v3 managev3user managev3group authentication-mode md5 authkey privacy-mode des56 prikey
```

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
```

设置允许向 NMS 发送 Trap 报文，使用的用户名为 managev3user。

```
[Agent] snmp-agent trap enable
[Agent] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname managev3user v3 privacy
```

(2) 配置 NMS

设置 NMS 使用的 SNMP 版本为 SNMPv3，用户名为 managev3user，启用认证和加密功能，认证算法为 MD5，认证密码为 authkey，加密协议为 DES56，加密密码为 prikey。另外，还要设置“超时”时间和“重试次数”。用户可利用网管系统完成对设备的查询和配置操作，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，否则无法进行相应操作。

(3) 结果验证

通过查询 Agent 上的相应 MIB 节点获取已发送 Trap 信息的数量：

```
Send request to 1.1.1.1/161 ...
Protocol version: SNMPv3
Operation: Get
Request binding:
1: 1.3.6.1.2.1.11.29.0
Response binding:
1: Oid=snmpOutTraps.0 Syntax=CNTR32 Value=18
Get finished
```

由于没有权限，无法通过查询 Agent 上的相应 MIB 节点获取设备名称：

```
Send request to 1.1.1.1/161 ...
Protocol version: SNMPv3
Operation: Get
Request binding:
1: 1.3.6.1.2.1.1.5.0
Response binding:
1: Oid=sysName.0 Syntax=noSuchObject Value=NULL
Get finished
```

对设备上某个空闲的接口执行 **shutdown/undo shutdown** 操作，NMS 上将看到相应的 Trap 信息：

```
1.1.1.1/3374 V3 Trap = linkdown
SNMP Version = V3
Community = managev3user
Command = Trap
1.1.1.1/3374 V3 Trap = linkup
SNMP Version = V3
Community = managev3user
Command = Trap
```

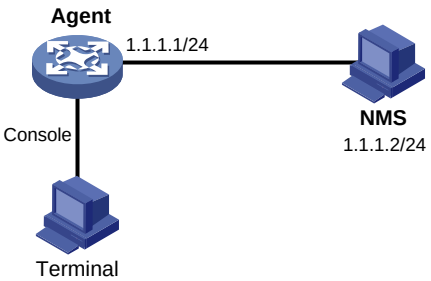
1.8.3 SNMP日志典型配置举例

1. 组网需求

- NMS 与 Agent 相连，NMS 的 IP 地址为 1.1.1.2/24，Agent 的 IP 地址为 1.1.1.1/24。
- 在 Agent 上配置 SNMP 日志功能，以便记录 NMS 对 Agent 进行的操作。

2. 组网图

图1-6 配置 SNMP 日志组网图



3. 配置步骤

说明

下面只列出了与SNMP日志相关的配置，NMS和Agent的SNMP功能配置请参见 1.8.1 和 1.8.2 。

打开控制台对日志信息的显示功能（此步骤可省略，缺省为该功能是开启的）。

```
<Agent> terminal monitor
<Agent> terminal logging
```

配置信息中心允许输出级别高于等于 informational 的系统信息到 Console 口。

```
<Agent> system-view
[Agent] info-center source snmp channel console log level informational
```

打开 Agent 的 SNMP 日志开关，对 NMS 的 GET 和 SET 操作进行记录。

```
[Agent] snmp-agent log all
```

- NMS 对 Agent 进行 GET 操作时，可以在控制台上看到如下日志信息。

```
%Jan 1 02:49:40:566 2011 Sysname SNMP/6/GET:
seqNO = <10> srcIP = <1.1.1.2> op = <get> node = <sysName(1.3.6.1.2.1.1.5.0)> value=<>
```

- NMS 对 Agent 进行 SET 操作时，可以在控制台上看到如下日志信息。

```
%Jan 1 02:59:42:576 2011 Sysname SNMP/6/SET:
seqNO = <11> srcIP = <1.1.1.2> op = <set> errorIndex = <0> errorStatus =<noError> node =
<sysName(1.3.6.1.2.1.1.5.0)> value = <Agent>
```

表1-9 SNMP 日志输出信息描述表

字段	描述
Jan 1 02:49:40:566 2011	表示SNMP日志生成的时间
seqNO	表示该SNMP日志的编号（系统会对记录的SNMP日志进行自动编号，编号从0开始）
srcIP	NMS的IP地址
op	表示SNMP操作类型（GET或者SET）
node	SNMP操作节点的名称和实例的OID
errorIndex	错误索引（0表示没有错误）
errorStatus	错误状态（noError表示没有错误）
value	SET操作时设置的值（GET操作时此域为空，表示不记录GET操作获取的值） 当设置的值为字符串，而且字符串中包含编码范围超出了ASCII 0～127或者包含不可显示的字符时，则以十六进制的方式显示整个字符串，形如：value = <81-43>[hex]

说明

信息中心的系统信息可以输出到控制台或日志缓冲区等方向。本举例是将 SNMP 日志信息输出到控制台，如果要配置别的输出方向，请参见“网络管理和监控配置指导”中的“信息中心”。

2 配置MIB风格

设备的 MIB 分为公有 MIB 和私有 MIB 两大类，私有 MIB 是企业内部开发的。私有 MIB 需要在 MIB 节点 enterprises（1.3.6.1.4.1）下申请一个子节点挂靠。H3C 私有 MIB 有两种风格：

- 一种是设备私有 MIB 在企业 ID 2011 下的 MIB，称为 H3C 兼容风格 MIB；
- 一种是设备私有 MIB 在 H3C 企业 ID 25506 下的 MIB，称为 H3C 新风格 MIB。

这两种风格的MIB在管理功能上完全一致，区别仅在于根节点不同。设备在出厂前都会加载好MIB，设备型号不同，加载的 MIB 风格可能不同。为了支持 NMS 对设备的灵活管理，设备提供了 MIB 风格配置功能，即用户可以任意切换 MIB 的两种风格，但需要保证设备的 MIB 风格和 NMS 的 MIB 风格一致，NMS 才能顺利识别被管理设备。

2.1 配置MIB风格

表2-1 配置 MIB 风格

操作	命令	说明
进入系统视图	**system-view**	-
设置设备的MIB风格	**mib-style** [**compatible** | **new**]	可选 缺省情况下，设备的MIB风格为**new**

说明

修改设备的 MIB 风格后需要重启设备配置才会生效。

2.2 MIB风格显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 MIB 的风格，通过查看显示信息验证配置的效果。

表2-2 MIB 风格显示和维护

操作	命令
查询设备的MIB风格	**display mib-style** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

目 录

1 RMON配置

1.1 RMON简介

1.1.1 RMON概述

RMON（Remote Network Monitoring，远程网络监视）主要实现了统计和告警功能，用于网络中管理设备对被管理设备的远程监控和管理。

统计功能指的是被管理设备可以按周期或者持续跟踪统计其端口所连接的网段上的各种流量信息，比如某段时间内某网段上收到的报文总数，或收到的超长报文的总数等。

告警功能指的是被管理设备能监控指定 MIB 变量的值，当该值达到告警阈值时（比如端口速率达到指定值，或者广播报文的比例达到指定值），能自动记录日志、向管理设备发送 Trap 消息。

RMON 和 SNMP 都用于远程网络管理：

- SNMP 是 RMON 实现的基础，RMON 是 SNMP 功能的增强。RMON 使用 SNMP Trap 报文发送机制向管理设备发送 Trap 消息告知告警变量的异常。虽然 SNMP 也定义了 Trap 功能，但通常用于告知被管理设备上某功能是否运行正常、端口物理状态的变化等，两者监控的对象、触发条件以及报告的内容均不同。
- RMON 使 SNMP 能更有效、更积极主动地监测远程网络设备，为监控子网的运行提供了一种高效的手段。RMON 协议规定达到告警阈值时被管理设备能自动发送 Trap 信息，所以管理设备不需要多次去获取 MIB 变量的值，进行比较，从而能够减少管理设备同被管理设备的通讯流量，达到简便而有力地管理大型互连网络的目的。

1.1.2 RMON工作机制

RMON 允许有多个监控者，监控者可用两种方法收集数据：

- 第一种方法利用专用的 RMON probe（探测仪）收集数据，管理设备直接从 RMON probe 获取管理信息并控制网络资源。这种方式可以获取 RMON MIB 的全部信息；
- 第二种方法是将 RMON Agent 直接植入网络设备（路由器、交换机、HUB 等），使它们成为带 RMON probe 功能的网络设施。管理设备使用 SNMP 的基本操作与 RMON Agent 交换数据信息，收集网络管理信息，但这种方法受设备资源限制，一般不能获取 RMON MIB 的所有数据，大多数只收集四个组的信息。这四个组是：事件组、告警组、历史组和统计组。

H3C 设备采用第二种方法，在设备上实现了 RMON Agent 功能。通过该功能，管理设备可以获得与被管网络设备端口相连的网段上的整体流量、错误统计和性能统计等信息，进而实现对网络的管理。

1.1.3 RMON组

RMON 规范（RFC2819）中定义了多个 RMON 组，设备实现了公有 MIB 中支持的统计组、历史组、事件组和告警组。此外，H3C 还自定义和实现了扩展告警组，以增强告警组的功能。下面将对这五个组作简要介绍。

1. 统计组

统计组规定系统将持续地对端口的各种流量信息进行统计（目前只支持对以太网端口的统计），并将统计结果存储在以太网统计表（etherStatsTable）中以便管理设备随时查看。统计信息包括网络冲突数、CRC 校验错误报文数、过小（或超大）的数据报文数、广播、多播的报文数以及接收字节数、接收报文数等。

在指定接口下创建统计表项成功后，统计组就对当前接口的报文数进行统计，它统计的结果是一个连续的累加值。

2. 历史组

历史组规定系统将按周期对端口的各种流量信息进行统计，并将统计结果存储在历史记录表（etherHistoryTable）中以便管理设备随时查看。统计数据包括带宽利用率、错误包数和总包数等。

历史组统计的是每个周期内端口接收报文的情况，周期的长短可以通过命令行来配置。

3. 事件组

事件组用来定义事件索引号及事件的处理方式。事件组定义的事件用于告警组配置项和扩展告警组配置项中。当监控对象达到告警条件时，就会触发事件，事件有如下几种处理方式：

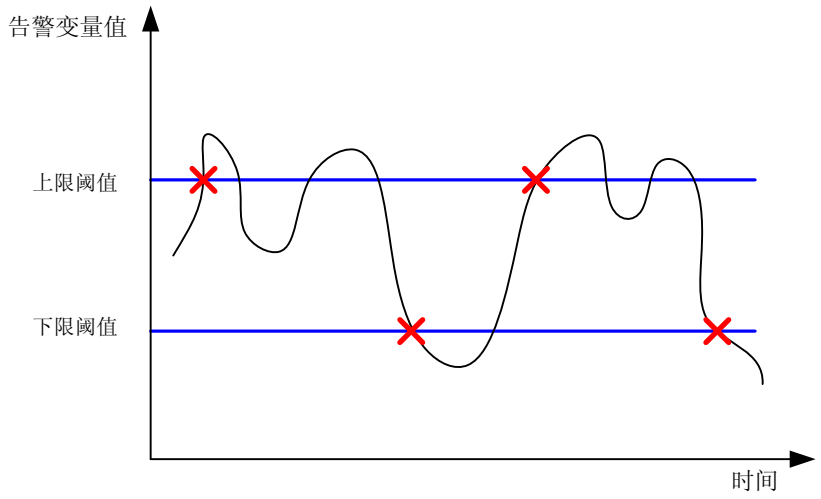
- Log：将事件相关信息（事件发生的事件、事件的内容等）记录在本设备 RMON MIB 的事件日志表中，以便管理设备通过 SNMP GET 操作进行查看。
- Trap：向网管站发送 Trap 消息告知该事件的发生。
- Log-Trap：即在本设备上记录日志，又向网管站发送 Trap 消息。
- None：不做任何处理。

4. 告警组

RMON 告警管理可对指定的告警变量（如端口收到的报文总数 etherStatsPkts）进行监视。用户定义了告警表项后，系统会按照定义的时间周期去获取被监视的告警变量的值，当告警变量的值大于或等于上限阈值时，触发一次上限告警事件；当告警变量的值小于或等于下限阈值，触发一次下限告警事件，告警管理将按照事件的定义进行相应的处理。

当告警变量的采样值在同一方向上连续多次超过阈值时，只会在第一次产生告警事件，后面的几次不会产生告警事件。即上限告警和下限告警是交替产生的，出现了一次上限告警，则下一次必为下限告警。如 图 1-1 所示，告警变量的值（如图中黑色曲线所示）多次超过阈值（如图中蓝色直线所示），产生了多个交叉点，但只有红叉标识的交叉点才会触发告警事件，其它交叉点不会触发告警事件。

图1-1 上下限告警示意图



5. 扩展告警组

扩展告警表项可以对告警变量进行运算，然后将运算结果和设置的阈值比较，实现更为丰富的告警功能。

用户定义了扩展告警表项后，系统对扩展告警表项的处理如下：

(1) 对定义的扩展告警公式中的告警变量按照定义的时间间隔进行采样。

(2) 将采样值按照定义的运算公式进行计算。

(3) 将计算结果和设定的阈值进行比较，越过阈值就触发相应事件。

说明

与告警组一样，当扩展告警组的运算结果在同一方向上连续多次超过阈值时，只会在第一次产生告警事件，后面的几次不会产生告警事件，即上限告警和下限告警是交替产生的。

1.2 配置RMON统计功能

RMON 的统计功能可以通过 RMON 统计组或者 RMON 历史组来实现，但是两者统计的对象不一样，请根据实际需要配置。

- RMON统计组统计的是RMON以太网统计表里定义的变量，记录的是从RMON统计表项创建到当前阶段变量的累加值，具体配置请参见 1.2.1 配置RMON以太网统计功能。
- RMON历史组统计的是RMON历史记录表里定义的变量，记录的是每个周期内变量的累加值，具体配置请参见 1.2.2 配置RMON历史统计功能。

1.2.1 配置RMON以太网统计功能

表1-1 配置 RMON 以太网统计功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图或三层以太网端口视图	**interface** *interface-type interface-number*	-
添加统计表的一个表项	**rmon statistics** *entry-number* [**owner** *text*]	必选

说明

每个接口下只能创建一个统计表项，整个设备允许创建的统计表项最大数目为 100 条。当统计表项的总数大于 100 条时，创建操作失败。

1.2.2 配置RMON历史统计功能

表1-2 配置 RMON 历史统计功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图或三层以太网端口视图	**interface** *interface-type interface-number*	-
添加历史控制表的一个表项	**rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text*]	必选

说明

- 历史表项的 *entry-number* 必须全局唯一，如果已经在别的接口下使用则创建操作失败。
- 同一接口下，可以创建多条历史表项，但要求 *entry-number* 的值必须不同，*sampling-interval* 的值也必须不同，否则创建操作失败。
- 整个设备允许创建的历史表项最大数目为 1000 条。当历史表项的总数大于 1000 条时，创建操作失败。
- 在新建历史控制表项时，如果指定的 **buckets** *number* 参数值超出了设备实际支持的历史表容量时，该历史控制表项会被添加，但该表项对应生效的 **buckets** *number* 的值为设备实际支持的历史表容量。

1.3 配置RMON告警功能

1.3.1 配置准备

- 触发告警事件时，如果需要向管理设备（NMS）发送 Trap 信息，则在配置 RMON 告警功能之前，必须保证 SNMP Agent 已经正确配置。SNMP Agent 的配置请参见“网络管理和监控配置指导”中的“SNMP”。
- 当告警变量是统计组或者历史组中定义的 MIB 变量时，必须在被监控的以太网端口下配置 RMON 以太网统计功能或者 RMON 历史统计功能。否则，虽然会创建告警表项，但不能触发告警事件。

1.3.2 配置过程

表1-3 配置 RMON 告警功能

操作	命令	说明
进入系统视图	**system-view**	-
添加事件表的一个表项	**rmon event** *entry-number* [**description** *string*] { **log** | **log-trap** *log-trapcommunity* | **none** | **trap** *trap-community* } [**owner** *text*]	必选
添加告警表的一个表项	**rmon alarm** *entry-number alarm-variable sampling-interval* { **absolute** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *text*]	二者至少选其一
添加扩展告警表的一个表项	**rmon prialarm** *entry-number prialarm-formula prialarm-des sampling-interval* { **absolute** | **changeratio** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* **entrytype** { **forever** | **cycle** *cycle-period* } [**owner** *text*]	

说明

- 系统不允许创建两个配置完全相同的表项。如果新建表项参数的值和已存在表项对应参数的值完全相同（对于历史表项，只与同一接口下已存在的历史表项进行比较），系统将认为这两个表项的配置相同，创建操作失败。不同表项需要比较的参数请参见 表 1-4。
- 系统对每种类型表项的总数均进行了限制（具体数目请参见 表 1-4），当某种类型表项的总数达到系统允许创建的最大数目时，创建操作失败。

表1-4 RMON 配置约束表

表项名	需要比较的参数	最多可创建的表项数
事件表项	事件描述（**description** *string*）、事件类型（**log**、**trap**、**logtrap**或**none**）和团体名（*trap-community*或*log-trapcommunity*）	60
告警表项	告警变量（*alarm-variable*）、采样间隔（*sampling-interval*）、采样类型（**absolute**或**delta**）、上限阈值（*threshold-value1*）和下限阈值（*threshold-value2*）	60
扩展告警表项	告警变量公式（*prialarm-formula*）、采样间隔（*sampling-interval*）、采样类型（**absolute**、**changeratio**或**delta**）、上限阈值（*threshold-value1*）和下限阈值（*threshold-value2*）	50

1.4 RMON显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 RMON 的运行情况，通过查看显示信息验证配置的效果。

表1-5 RMON 显示和维护

操作	命令
显示RMON统计消息	**display rmon statistics** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示RMON历史控制表及历史采样信息	**display rmon history** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示RMON告警配置信息	**display rmon alarm** [*entry-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示RMON扩展告警配置信息	**display rmon prialarm** [*entry-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示RMON事件配置信息	**display rmon event** [*entry-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示指定事件的记录	**display rmon eventlog** [*entry-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

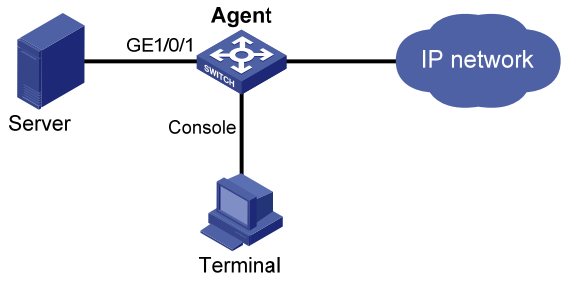
1.5 统计组典型配置举例

1. 组网需求

Agent 通过 console 口连接配置终端，通过以太网线缆连接 Server。现需要通过 RMON 统计表对以太网端口 GigabitEthernet1/0/1 接收的报文进行性能统计，以便管理员能够随时查看统计数据了解接口接收报文的情况。

2. 组网图

图1-2 配置 RMON 组网图



3. 配置步骤

配置 RMON 对接口 GigabitEthernet1/0/1 进行流量统计。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1 owner user1
```

以上配置完成后系统就开始对接口 GigabitEthernet1/0/1 接收的报文进行分类统计了，统计的结果可以通过多种方式查看：

- 使用 display 命令查看接口的统计信息。

```
<Sysname> display rmon statistics gigabitethernet 1/0/1
EtherStatsEntry 1 owned by user1-rmon is VALID.
  Interface : GigabitEthernet1/0/1<ifIndex.3>
  etherStatsOctets         : 21657     , etherStatsPkts          : 307
  etherStatsBroadcastPkts  : 56        , etherStatsMulticastPkts : 34
  etherStatsUndersizePkts  : 0         , etherStatsOversizePkts  : 0
  etherStatsFragments      : 0         , etherStatsJabbers       : 0
  etherStatsCRCAlignErrors : 0         , etherStatsCollisions    : 0
  etherStatsDropEvents (insufficient resources): 0
  Packets received according to length:
  64     : 235       ,  65-127  : 67        ,  128-255  : 4
  256-511: 1         ,  512-1023: 0         ,  1024-1518: 0
```

- 在 NMS 上通过软件执行 get 操作，直接获取 MIB 节点的值。

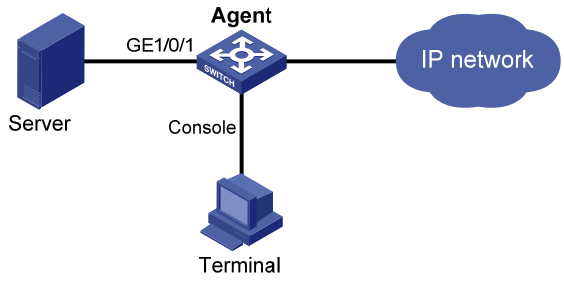
1.6 历史统计典型配置举例

1. 组网需求

Agent 通过 console 口连接配置终端，通过以太网线缆连接 Server。现需要每 1 分钟通过 RMON 历史统计表对以太网端口 GigabitEthernet1/0/1 接收的报文进行周期性统计，以便管理员能够随时了解短时间内接口有没有数据突发。

2. 组网图

图1-3 配置 RMON 组网图



3. 配置步骤

配置 RMON 对接口 GigabitEthernet1/0/1 进行周期性流量统计。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon history 1 buckets 8 interval 60 owner user1
```

以上配置完成后，系统就开始对接口 GigabitEthernet1/0/1 接收的报文进行周期性分类统计了，每 1 分钟统计一次，历史统计列表里会保存最近的 8 次统计的结果，以便管理员查看：

- 使用 display 命令查看接口的历史统计信息。

```
[Sysname-GigabitEthernet1/0/1] display rmon history
HistoryControlEntry 2 owned by null is VALID
  Samples interface     : GigabitEthernet1/0/1<ifIndex.3>
  Sampling interval     : 10(sec) with 8 buckets max
  Sampled values of record 1 :
    dropevents        : 0         , octets              : 834
    packets           : 8         , broadcast packets   : 1
    multicast packets : 6         , CRC alignment errors : 0
    undersize packets : 0         , oversize packets    : 0
    fragments         : 0         , jabbers             : 0
    collisions        : 0         , utilization         : 0
  Sampled values of record 2 :
    dropevents        : 0         , octets              : 962
    packets           : 10        , broadcast packets   : 3
    multicast packets : 6         , CRC alignment errors : 0
    undersize packets : 0         , oversize packets    : 0
    fragments         : 0         , jabbers             : 0
    collisions        : 0         , utilization         : 0
  Sampled values of record 3 :
    dropevents        : 0         , octets              : 830
    packets           : 8         , broadcast packets   : 0
    multicast packets : 6         , CRC alignment errors : 0
    undersize packets : 0         , oversize packets    : 0
    fragments         : 0         , jabbers             : 0
    collisions        : 0         , utilization         : 0
  Sampled values of record 4 :
    dropevents        : 0         , octets              : 933
    packets           : 8         , broadcast packets   : 0
    multicast packets : 7         , CRC alignment errors : 0
    undersize packets : 0         , oversize packets    : 0
    fragments         : 0         , jabbers             : 0
    collisions        : 0         , utilization         : 0
```

```
Sampled values of record 5 :
  dropevents        : 0         , octets               : 898
  packets           : 9         , broadcast packets    : 2
  multicast packets : 6         , CRC alignment errors : 0
  undersize packets : 0         , oversize packets     : 0
  fragments         : 0         , jabbers              : 0
  collisions        : 0         , utilization          : 0
Sampled values of record 6 :
  dropevents        : 0         , octets               : 898
  packets           : 9         , broadcast packets    : 2
  multicast packets : 6         , CRC alignment errors : 0
  undersize packets : 0         , oversize packets     : 0
  fragments         : 0         , jabbers              : 0
  collisions        : 0         , utilization          : 0
Sampled values of record 7 :
  dropevents        : 0         , octets               : 766
  packets           : 7         , broadcast packets    : 0
  multicast packets : 6         , CRC alignment errors : 0
  undersize packets : 0         , oversize packets     : 0
  fragments         : 0         , jabbers              : 0
  collisions        : 0         , utilization          : 0
Sampled values of record 8 :
  dropevents        : 0         , octets               : 1154
  packets           : 13        , broadcast packets    : 1
  multicast packets : 6         , CRC alignment errors : 0
  undersize packets : 0         , oversize packets     : 0
  fragments         : 0         , jabbers              : 0
  collisions        : 0         , utilization          : 0
```

- 在 NMS 上通过软件执行 get 操作，直接获取 MIB 节点的值。

1.7 告警组典型配置举例

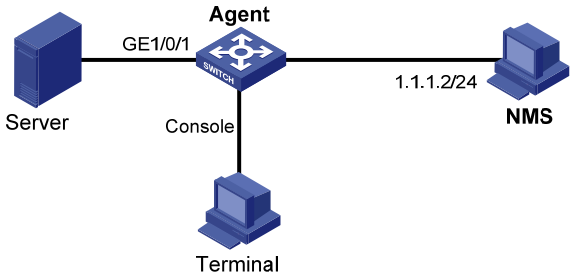
1. 组网需求

Agent 通过 console 口连接配置终端，通过以太网连接 NMS。

- GigabitEthernet1/0/1 接口连接 FTP 服务器，现需要对该服务器的流量进行统计。以 5 秒的采样间隔采样，当流量过大或过低时发送相应的 trap 信息通知 NMS；
- 在 Agent 上通过 **display rmon statistics** 命令查看显示结果，同时在 NMS 上查看统计结果。

2. 组网图

图1-4 配置 RMON 组网图



3. 配置步骤

配置 SNMP Agent。（请注意：这些参数的值应与 NMS 侧的配置一致，假设 NMS 上运行 SNMP v1，访问设备时使用的可读团体名为 public，可写团体名为 private，NMS 的 IP 地址为 1.1.1.2）

```
<Sysname> system-view
[Sysname] snmp-agent
[Sysname] snmp-agent community read public
[Sysname] snmp-agent community write private
[Sysname] snmp-agent sys-info version v1
[Sysname] snmp-agent trap enable
[Sysname] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname public
```

配置 RMON 对以太网端口 GigabitEthernet1/0/1 进行统计。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1 owner user1
[Sysname-GigabitEthernet1/0/1] quit
```

配置 RMON 告警表项。（当节点 1.3.6.1.2.1.16.1.1.1.4.1 的相对采样值超过 100 时或者低于 50 时，都触发事件 1——发起 trap 信息）

```
[Sysname] rmon event 1 trap public owner user1
[Sysname] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 5 delta rising-threshold 100 1 falling-threshold 50 1
```

查看 RMON 告警表信息。

```
<Sysname> display rmon alarm 1
AlarmEntry 1 owned by null is Valid.
  Samples type          : delta
  Variable formula      : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
  Sampling interval     : 5(sec)
  Rising threshold      : 100(linked with event 1)
  Falling threshold     : 50(linked with event 2)
  When startup enables  : risingOrFallingAlarm
  Latest value          : 0
```

查看以太网口的统计信息。

```
<Sysname> display rmon statistics gigabitethernet 1/0/1
EtherStatsEntry 1 owned by user1-rmon is VALID.
  Interface : GigabitEthernet1/0/1<ifIndex.3>
  etherStatsOctets         : 57329     , etherStatsPkts          : 455
  etherStatsBroadcastPkts  : 53        , etherStatsMulticastPkts : 353
  etherStatsUndersizePkts  : 0         , etherStatsOversizePkts  : 0
  etherStatsFragments      : 0         , etherStatsJabbers       : 0
  etherStatsCRCAlignErrors : 0         , etherStatsCollisions    : 0
  etherStatsDropEvents (insufficient resources): 0
  Packets received according to length:
  64     : 7         ,  65-127  : 413       ,  128-255  : 35
  256-511: 0         ,  512-1023: 0         ,  1024-1518: 0
```

完成以上配置后，当告警事件被触发时，在 NMS 的告警管理部分可以查看相应的记录。在设备侧也会有相应信息，如下所示。

```
[Sysname]
#Jan 27 16:31:34:12 2011 Sysname RMON/2/ALARMFALL:Trap 1.3.6.1.2.1.16.0.2 Alarm table 1 monitors 1.3.6.1.2.1.16.1.1.1.4.1 with sample type 2,has sampled alarm value 0 less than(or =) 50.
```

目 录

1 端口镜像配置

1.1 端口镜像简介

端口镜像通过将指定端口或 CPU 的报文复制到与数据监测设备相连的端口，使用户可以利用数据监测设备分析这些复制过来的报文，以进行网络监控和故障排除。

1.1.1 端口镜像的基本概念

1. 镜像源

镜像源是指被监控的对象，经由该对象收发的报文会被复制一份到与数据监测设备相连的端口，用户就可以对这些报文（称为镜像报文）进行监控和分析了。被监控的对象可以是端口或 CPU，我们将之依次称为源端口和源 CPU，这些对象所在的设备就称为源设备。

2. 镜像目的

镜像目的是指镜像报文所要到达的目的地，即与数据监测设备相连的那个端口，我们称之为目的端口，目的端口所在的设备就称为目的设备。目的端口会将其收到的镜像报文转发给与之相连的数据监测设备。

说明

由于一个目的端口可以同时监控多个镜像源，因此在某些配置下，目的端口可能收到对同一报文的多份拷贝。例如，目的端口 Port 1 同时监控源端口 Port 2 和 Port 3（这两个端口在同一台设备上）收发的报文，如果某报文从 Port 2 进入该设备后又从 Port 3 发送出去，那么该报文将被复制两次给 Port 1。

---

3. 镜像方向

镜像方向是指在镜像源上可复制的报文方向，包括：

- 入方向：是指仅复制镜像源收到的报文。
- 出方向：是指仅复制镜像源发出的报文。
- 双向：是指对镜像源收到和发出的报文都进行复制。

4. 镜像组

镜像组是在端口镜像的实现过程中用到的一个逻辑上的概念，镜像源和镜像目的都要属于某一个镜像组。根据具体的实现方式不同，镜像组可分为本地镜像组、远程源镜像组和远程目的镜像组三类，有关这三类镜像组的具体介绍请参见“1.1.2 端口镜像的分类和实现方式”一节。

5. 反射端口、出端口和远程镜像VLAN

反射端口、出端口和远程镜像VLAN都是在二层远程端口镜像的实现过程中用到的概念。远程镜像VLAN是将镜像报文从源设备传送至目的设备的专用VLAN；反射端口和出端口都位于源设备上，都用来将镜像报文发送到远程镜像VLAN中，二者的区别在于前者不必加入远程镜像VLAN中，而后者则必须加入到远程镜像VLAN中。出端口位于源设备上，用来将镜像报文发送到远程镜像VLAN中，且必须加入到远程镜像VLAN中。有关源设备、目的设备、反射端口、出端口和远程镜像VLAN的具体介绍，请参见“1.1.2 端口镜像的分类和实现方式”一节。

说明

反射端口主要用于实现“本地镜像支持多个目的端口”功能。

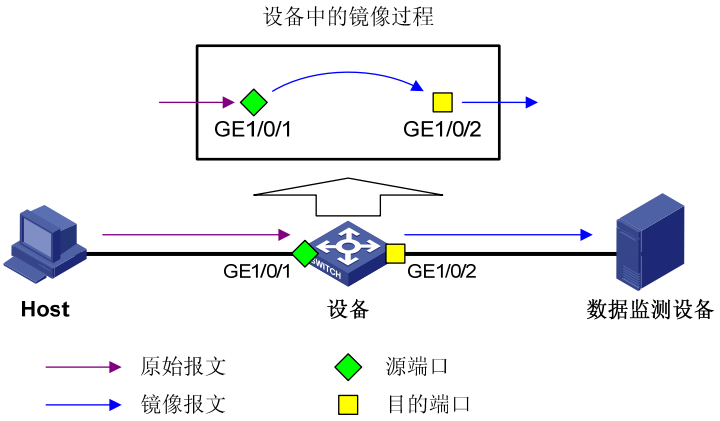
1.1.2 端口镜像的分类和实现方式

根据镜像源与镜像目的所处的相对位置，我们将端口镜像分为本地端口镜像和远程端口镜像两大类：

1. 本地端口镜像

当镜像源和镜像目的位于同一台设备上时，称为本地端口镜像。对于本地端口镜像，镜像源和镜像目的都属于同一台设备上的同一个镜像组，该镜像组就称为本地镜像组。

图1-1 本地端口镜像示意图



如 图 1-1 所示，镜像源为源端口GigabitEthernet1/0/1，镜像目的为目的端口GigabitEthernet1/0/2，这两个端口位于同一台设备上。设备将进入源端口GigabitEthernet1/0/1 的报文复制一份给目的端口GigabitEthernet1/0/2，再由该端口将镜像报文转发给数据监测设备。

2. 远程端口镜像

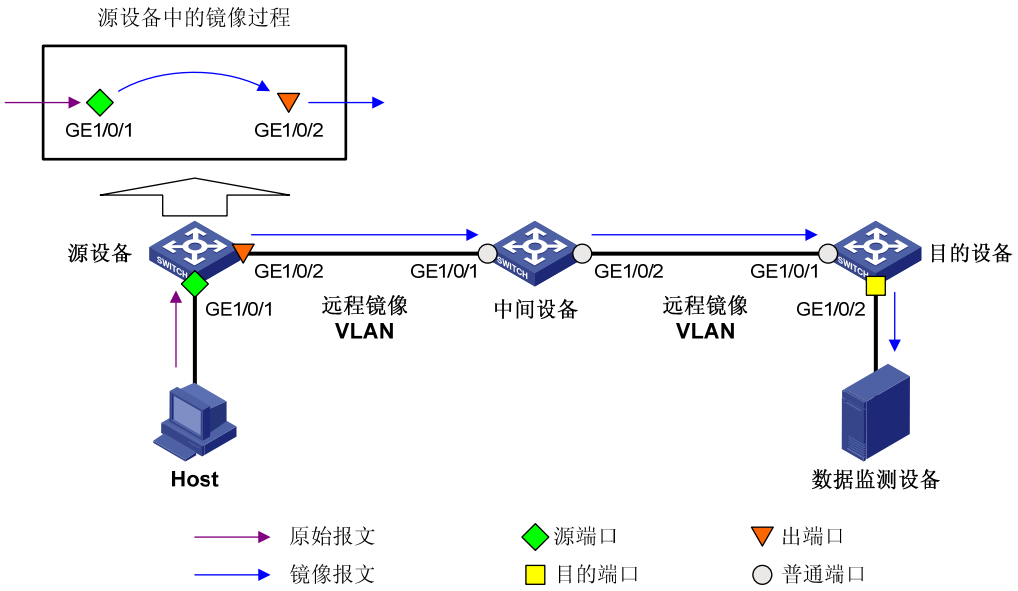
当镜像源和镜像目的分处于两台设备上时，称为远程端口镜像。对于远程端口镜像，镜像源和镜像目的分属于不同设备上的不同镜像组：镜像源所在的设备和镜像组分别称为源设备和远程源镜像组，镜像目的所在的设备和镜像组分别称为目的设备和远程目的镜像组，而位于源设备与目的设备之间的设备则统称为中间设备。

根据源设备与目的设备之间的连接关系，又可将远程端口镜像细分为：

- 二层远程端口镜像：源设备与目的设备之间通过二层网络进行连接。
- 三层远程端口镜像：源设备与目的设备之间通过三层网络进行连接。

(1) 二层远程端口镜像

图1-2 二层远程端口镜像示意图



如 图 1-2 所示，源设备将进入源端口GigabitEthernet1/0/1 的报文复制一份给出端口GigabitEthernet1/0/2，该端口将镜像报文转发给中间设备，再由中间设备在远程镜像VLAN中广播，最终到达目的设备。目的设备收到该报文后判别其VLAN ID，若与远程镜像VLAN的VLAN ID相同，就将其转发至目的端口GigabitEthernet1/0/2，最后由该端口将镜像报文转发给数据监测设备。

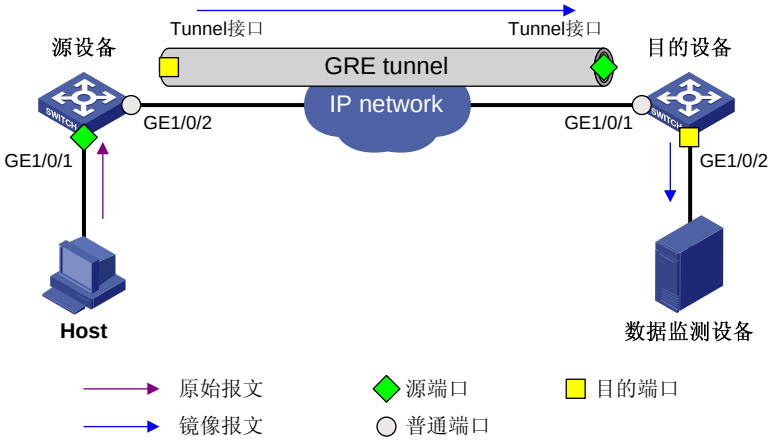
说明

- 中间设备需允许远程镜像 VLAN 通过，以确保源设备与目的设备之间的二层网络畅通。
- 在镜像报文从源设备到达目的设备的过程中，请确保其 VLAN ID 不被修改或删除，否则二层远程镜像功能将失效。
- 在一个镜像组中对同一个端口收发的报文进行双向镜像时，需要在源设备、中间设备和目的设备上通过 **mac-address mac-learning disable** 命令用来关闭远程镜像 VLAN 的 MAC 地址学习功能，以保证镜像功能的正常进行。关于 **mac-address mac-learning disable** 命令的详细信息，请参见“二层技术-以太网交换命令参考”中的“MAC 地址表配置命令”。

(2) 三层远程端口镜像

三层远程端口镜像的实现过程中借用了本地镜像组的概念，即在源设备和目的设备上分别创建各自的本地镜像组，每个本地镜像组也拥有各自的源端口和目的端口。

图1-3 三层远程端口镜像示意图



如 图 1-3 所示，源设备将进入源端口GigabitEthernet1/0/1 的报文复制一份给其Tunnel接口（即目的端口），再经由GRE（Generic Routing Encapsulation，通用路由封装）隧道转发至目的设备端的Tunnel接口。目的设备将从其Tunnel接口（即源端口）收到的镜像报文转发至目的端口GigabitEthernet1/0/2，最后由该端口将镜像报文转发给数据监测设备。

说明

有关 GRE 隧道和 Tunnel 接口的详细介绍，请分别参见“三层技术-IP 业务配置指导”中的“GRE”和“隧道”。

1.2 配置本地端口镜像

1.2.1 配置任务简介

首先创建一个本地镜像组，然后为该镜像组配置源端口（或源 CPU）和目的端口。

表1-1 本地端口镜像配置任务简介

配置任务	说明	详细配置
创建本地镜像组	必选	1.2.2
配置源端口	源端口和源CPU可以只配其一，也可以都配置	1.2.3
配置源CPU		1.2.4
配置目的端口	必选	1.2.5
利用远程镜像VLAN实现本地镜像支持多个目的端口	可选	1.2.6

1.2.2 创建本地镜像组

表1-2 创建本地镜像组

操作	命令	说明
进入系统视图	**system-view**	-
创建本地镜像组	**mirroring-group** *group-id* **local**	必选 缺省情况下，不存在任何本地镜像组

说明

在完成源端口（或源 CPU）和目的端口的配置之后，本地镜像组才能生效。

1.2.3 配置源端口

可以在系统视图下为指定镜像组配置一个或多个源端口，也可以在端口视图下将当前端口配置为指定镜像组的源端口，二者的配置效果相同。

1. 在系统视图下配置源端口

表1-3 在系统视图下配置源端口

操作	命令	说明
进入系统视图	**system-view**	-
为本地镜像组配置源端口	**mirroring-group** *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }	必选 缺省情况下，本地镜像组没有源端口

2. 在端口视图下配置源端口

表1-4 在端口视图下配置源端口

操作	命令	说明
进入系统视图	**system-view**	-
进入端口视图	**interface** *interface-type interface-number*	-
配置本端口为本地镜像组的源端口	[**mirroring-group** *group-id*] **mirroring-port** { **both** | **inbound** | **outbound** }	必选 缺省情况下，端口不是任何本地镜像组的源端口

说明

- 一个镜像组内可以配置多个源端口。
- 在 S5500-28SC-HI 和 S5500-52SC-HI 交换机上，每个端口无论作为单向或双向源端口，均最多只能加入两个镜像组。
- 在其他 S5500-HI 系列交换机上，对源端口的单向数据进行镜像需要占用一个镜像资源，对源端口的双向数据进行镜像需要占用两个镜像资源，对一个源端口最多分配四个镜像资源。即一个端口作为单向源端口最多可以加入四个镜像组，作为双向源端口最多可以加入两个镜像组，或者以一个双向源端口和两个单向源端口的形式加入三个镜像组。

1.2.4 配置源CPU

表1-5 配置源 CPU

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
为本地镜像组配置源CPU	**mirroring-group** *group-id* **mirroring-cpu slot** *slot-number-list* { **both** | **inbound** | **outbound** }	必选 缺省情况下，本地镜像组没有源CPU

说明

一个镜像组内可以配置多个源 CPU。

1.2.5 配置目的端口

可以在系统视图下为指定镜像组配置目的端口，也可以在端口视图下将当前端口配置为指定镜像组的目的端口，二者的配置效果相同。

1. 在系统视图下配置目的端口

表1-6 在系统视图下配置目的端口

操作	命令	说明
进入系统视图	**system-view**	-
为本地镜像组配置目的端口	**mirroring-group** *group-id* **monitor-port** *monitor-port-id*	必选 缺省情况下，本地镜像组没有目的端口

2. 在端口视图下配置目的端口

表1-7 在端口视图下配置目的端口

操作	命令	说明
进入系统视图	**system-view**	-
进入端口视图	**interface** *interface-type interface-number*	-
配置本端口为本地镜像组的目的端口	[**mirroring-group** *group-id*] **monitor-port**	必选 缺省情况下，端口不是任何本地镜像组的目的端口

说明

- 一个镜像组内只能配置一个目的端口。
- 请不要在目的端口上使能生成树协议，否则会影响镜像功能的正常使用。
- 从目的端口发出的报文包括镜像报文和其它端口正常转发来的报文。为了保证数据监测设备只对镜像报文进行分析，请将目的端口只用于端口镜像，不作其它用途。
- 镜像组的目的端口不能配置为已经接入 RRPP 环的端口。

1.2.6 利用远程镜像VLAN实现本地镜像支持多个目的端口

传统的本地镜像配置方式仅支持在一个镜像组中指定一个镜像目的端口，如果用户需要将一份监测数据同时发送到多个目的端口，可以利用远程镜像 VLAN 的原理来实现。

在二层远程端口镜像中，会使用到远程镜像 VLAN，镜像报文在远程镜像 VLAN 中以广播的方式发送。因此，可以利用远程镜像 VLAN 的原理，在本地设备上创建远程源镜像组，并指定远程镜像 VLAN，同时将本设备上连接数据检测设备的多个端口加入该 VLAN。完成以上配置后，镜像报文在远程镜像 VLAN 中广播时便可以从这些端口中发送出去，实现将镜像报文输出至多个端口的需求。

表1-8 利用远程镜像 VLAN 实现本地镜像支持多个目的端口配置

操作		命令	说明
进入系统视图		**system-view**	-
创建远程源镜像组		**mirroring-group** *group-id* **remote-source**	必选 缺省情况下，不存在任何镜像组
为远程源镜像组配置源端口	在系统视图下配置	**mirroring-group** *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }	两种方式必选其一 缺省情况下，镜像组没有源端口
	在端口视图下配置	**interface** *interface-type interface-number*	
		[**mirroring-group** *group-id*] **mirroring-port** { **both** | **inbound** | **outbound** }	
		quit	
为远程源镜像组配置反射端口		**mirroring-group** *group-id* **reflector-port** *reflector-port*	必选 缺省情况下，镜像组没有反射端口
创建远程镜像VLAN并进入VLAN视图		**vlan** *vlan-id*	必选 缺省情况下，镜像组没有远程镜像VLAN
将镜像目的端口加入远程镜像VLAN		**port** *interface-list*	必选 缺省情况下，新建VLAN中不包含任何端口
退出至系统视图		**quit**	-
为远程源镜像组配置远程镜像VLAN		**mirroring-group** *group-id* **remote-probe vlan** *rprobe-vlan-id*	必选 缺省情况下，镜像组没有远程镜像VLAN

说明

- 镜像反射口必须是 Access 类型的端口，且必须属于缺省 VLAN（VLAN1）。
- 建议选择设备上未使用的端口作为镜像反射口，且建议关闭反射口的生成树协议。
- 一个镜像组内可以配置多个源端口。
- 请不要将源端口加入到远程镜像 VLAN 中，否则会影响镜像功能的正常使用。
- 在一个镜像组内，如果已经配置了镜像反射口，则无法再配置镜像出端口。
- 一个 VLAN 只能作为一个远程源镜像组的远程镜像 VLAN，且建议该 VLAN 只用于端口镜像，请不要在该 VLAN 上配置其它业务功能或创建对应的 VLAN 接口。
- 远程镜像 VLAN 必须为静态 VLAN，且在被配置成远程镜像 VLAN 后，该 VLAN 不能直接删除，必须先删除远程镜像 VLAN 的配置才能够删除这个 VLAN。
- 如果镜像组生效后，远程镜像 VLAN 被取消，那么该镜像组将失效。
- 镜像目的端口必须是 Access 类型的端口。

1.3 配置二层远程端口镜像

1.3.1 配置任务简介

二层远程端口镜像的配置需要分别在源设备和目的设备上进行；如果存在中间设备，则需要在中间设备上允许远程镜像 VLAN 通过，以确保源设备与目的设备之间的二层网络畅通。

说明

在配置二层远程端口镜像时不建议启用 GVRP（GARP VLAN Registration Protocol，GARP VLAN 注册协议）功能，否则 GVRP 可能将远程镜像 VLAN 注册到不需要监控的端口上，导致目的端口收到很多不必要的报文。有关 GVRP 的详细介绍，请参见“二层技术-以太网交换配置指导”中的“GVRP”。

首先在目的设备上为远程目的镜像组配置远程镜像 VLAN 和目的端口，然后在源设备上为远程源镜像组配置源端口（或源 CPU）、出端口和远程镜像 VLAN。

表1-9 二层远程端口镜像配置任务简介

配置任务		说明	详细配置
配置远程目的镜像组	创建远程目的镜像组	必选	1.3.2 1.
	配置目的端口	必选	1.3.2 2.
	配置远程镜像VLAN	必选	1.3.2 3.
	将目的端口加入远程镜像VLAN	必选	1.3.2 4.
配置远程源镜像组	创建远程源镜像组	必选	1.3.3 1.
	配置源端口	源端口和源CPU可以只配其一，也可以都配置	1.3.3 2.
	配置源CPU		1.3.3 3.
	配置出端口	必选	1.3.3 4.
	配置远程镜像VLAN	必选	1.3.3 5.

1.3.2 配置远程目的镜像组

请在目的设备上进行如下配置。

1. 创建远程目的镜像组

表1-10 创建远程目的镜像组

操作	命令	说明
进入系统视图	**system-view**	-
创建远程目的镜像组	**mirroring-group** *group-id* **remote-destination**	必选 缺省情况下，不存在任何远程目的镜像组

2. 配置目的端口

可以在系统视图下为指定镜像组配置目的端口，也可以在端口视图下将当前端口配置为指定镜像组的目的端口，二者的配置效果相同。

(1) 在系统视图下配置目的端口

表1-11 在系统视图下配置目的端口

操作	命令	说明
进入系统视图	**system-view**	-
为远程目的镜像组配置目的端口	**mirroring-group** *group-id* **monitor-port** *monitor-port-id*	必选 缺省情况下，远程目的镜像组没有目的端口

(2) 在端口视图下配置目的端口

表1-12 在端口视图下配置目的端口

操作	命令	说明
进入系统视图	**system-view**	-
进入端口视图	**interface** *interface-type interface-number*	-
配置本端口为远程目的镜像组的目的端口	[**mirroring-group** *group-id*] **monitor-port**	必选 缺省情况下，端口不是任何远程目的镜像组的目的端口

说明

- 一个镜像组内只能配置一个目的端口。
- 请不要在目的端口上使能生成树协议，否则会影响镜像功能的正常使用。
- 从目的端口发出的报文包括镜像报文和其它端口正常转发来的报文。为了保证数据监测设备只对镜像报文进行分析，请将目的端口只用于端口镜像，不作其它用途。
- 镜像组的目的端口不能配置为已经接入 RRPP 环的端口。

3. 配置远程镜像VLAN

表1-13 配置远程镜像 VLAN

操作	命令	说明
进入系统视图	**system-view**	-
为远程目的镜像组配置远程镜像VLAN	**mirroring-group** *group-id* **remote-probe vlan** *rprobe-vlan-id*	必选 缺省情况下，远程目的镜像组没有远程镜像VLAN

说明

- 一个 VLAN 只能被一个镜像组使用。
- 当一个 VLAN 已被指定为远程镜像 VLAN 后，请不要在该 VLAN 上配置其它业务功能或创建对应的 VLAN 接口。
- 被配置成远程镜像 VLAN 后，该 VLAN 不能直接删除，必须先删除远程镜像 VLAN 的配置才能够删除这个 VLAN。
- 如果镜像组生效后，远程镜像 VLAN 被取消，那么该镜像组将失效。

4. 将目的端口加入远程镜像VLAN

表1-14 将目的端口加入远程镜像 VLAN

操作		命令	说明
进入系统视图		**system-view**	-
进入目的端口视图		**interface** *interface-type interface-number*	-
将目的端口加入远程镜像VLAN	目的端口为Access端口	**port access vlan** *vlan-id*	三者必选其一
	目的端口为Trunk端口	**port trunk permit vlan** *vlan-id*	
	目的端口为Hybrid端口	**port hybrid vlan** *vlan-id* { **tagged** | **untagged** }	

说明

有关 **port access vlan**、**port trunk permit vlan** 和 **port hybrid vlan** 命令的详细介绍，请参见“二层技术-以太网交换命令参考”中的“VLAN”。

1.3.3 配置远程源镜像组

请在源设备上进行如下配置。

1. 创建远程源镜像组

表1-15 创建远程源镜像组

操作	命令	说明
进入系统视图	**system-view**	-
创建远程源镜像组	**mirroring-group** *group-id* **remote-source**	必选 缺省情况下，不存在任何远程源镜像组

2. 配置源端口

可以在系统视图下为指定镜像组配置一个或多个源端口，也可以在端口视图下将当前端口配置为指定镜像组的源端口，二者的配置效果相同。

(1) 在系统视图下配置源端口

表1-16 在系统视图下配置源端口

操作	命令	说明
进入系统视图	**system-view**	-
为远程源镜像组配置源端口	**mirroring-group** *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }	必选 缺省情况下，远程源镜像组没有源端口

(2) 在端口视图下配置源端口

表1-17 在端口视图下配置源端口

操作	命令	说明
进入系统视图	**system-view**	-
进入端口视图	**interface** *interface-type interface-number*	-
配置本端口为远程源镜像组的源端口	[**mirroring-group** *group-id*] **mirroring-port** { **both** | **inbound** | **outbound** }	必选 缺省情况下，端口不是任何远程源镜像组的源端口

说明

- 一个镜像组内可以配置多个源端口。
- 在 S5500-28SC-HI 和 S5500-52SC-HI 交换机上，每个端口无论作为单向或双向源端口，均最多只能加入两个镜像组。
- 在其他 S5500-HI 系列交换机上，对源端口的单向数据进行镜像需要占用一个镜像资源，对源端口的双向数据进行镜像需要占用两个镜像资源，对一个源端口最多分配四个镜像资源。即一个端口作为单向源端口最多可以加入四个镜像组，作为双向源端口最多可以加入两个镜像组，或者以一个双向源端口和两个单向源端口的形式加入三个镜像组。

3. 配置源CPU

表1-18 配置源 CPU

操作	命令	说明
进入系统视图	**system-view**	-
为远程源镜像组配置源CPU	**mirroring-group** *group-id* **mirroring-cpu slot** *slot-number-list* { **both** | **inbound** | **outbound** }	必选 缺省情况下，远程源镜像组没有源CPU

说明

一个镜像组内可以配置多个源 CPU。

4. 配置出端口

可以在系统视图下为指定镜像组配置出端口，也可以在端口视图下将当前端口配置为指定镜像组的出端口，二者的配置效果相同。

(1) 在系统视图下配置出端口

表1-19 在系统视图下配置出端口

操作	命令	说明
进入系统视图	**system-view**	-
为远程源镜像组配置出端口	**mirroring-group** *group-id* **monitor-egress** *monitor-egress-port*	必选 缺省情况下，远程源镜像组没有出端口

(2) 在端口视图下配置出端口

表1-20 在端口视图下配置出端口

操作	命令	说明
进入系统视图	**system-view**	-
进入端口视图	**interface** *interface-type interface-number*	-
配置本端口为远程源镜像组的出端口	**mirroring-group** *group-id* **monitor-egress**	必选 缺省情况下，端口不是任何远程源镜像组的出端口

说明

- 一个镜像组内只能配置一个出端口。
- 出端口不能是现有镜像组的成员端口。
- 请不要在出端口上配置下列功能：生成树协议、802.1X、IGMP Snooping、静态 ARP 和 MAC 地址学习，否则会影响镜像功能的正常使用。

5. 配置远程镜像VLAN

(1) 配置准备

在配置远程镜像 VLAN 之前，需完成以下任务：

- 配置远程镜像 VLAN 所使用的静态 VLAN

(2) 配置过程

表1-21 配置远程镜像 VLAN

操作	命令	说明
进入系统视图	**system-view**	-
为远程源镜像组配置远程镜像VLAN	**mirroring-group** *group-id* **remote-probe vlan** *rprobe-vlan-id*	必选 缺省情况下，远程源镜像组没有远程镜像 VLAN

说明

- 一个 VLAN 只能被一个镜像组使用。
- 被配置成远程镜像 VLAN 后，该 VLAN 不能直接删除，必须先删除远程镜像 VLAN 的配置才能够删除这个 VLAN。
- 如果镜像组生效后，远程镜像 VLAN 被取消，那么该镜像组将失效。
- 当一个 VLAN 已被指定为远程镜像 VLAN 后，请不要在该 VLAN 上配置其它业务功能或创建对应的 VLAN 接口。
- 源设备和目的设备上的远程镜像组必须使用相同的远程镜像 VLAN。

1.4 配置三层远程端口镜像

1.4.1 配置任务简介

三层远程端口镜像的配置需要分别在源设备和目的设备上进行；如果存在中间设备，则需要在中间设备上配置单播路由协议，以确保源设备与目的设备之间的三层网络畅通。

分别在源设备和目的设备上先创建一个本地镜像组，然后为该镜像组配置源端口（或源 CPU）和目的端口，不同的是：

- 在源设备上，需要将源端口（或源 CPU）指定为待监控的端口（或 CPU），目的端口指定为 Tunnel 接口；
- 在目的设备上，需要将源端口指定为 Tunnel 接口对应的物理端口，目的端口指定为连接数据监测设备的端口。

表1-22 三层远程端口镜像配置任务简介

配置任务		说明	详细配置
源设备上的配置	创建本地镜像组	必选	1.4.3
	配置源端口	源端口和源CPU可以只配其一，也可以都配置	1.4.4
	配置源CPU		1.4.5
	配置目的端口	必选	1.4.6
目的设备上的配置	创建本地镜像组	必选	1.4.3
	配置源端口	必选	1.4.4

配置任务		说明	详细配置
	配置目的端口	必选	1.4.6

1.4.2 配置准备

在配置三层远程端口镜像之前，需完成以下任务：

- 配置 Tunnel 接口和 GRE 隧道

1.4.3 创建本地镜像组

请分别在源设备和目的设备上进行如下配置。

表1-23 创建本地镜像组

操作	命令	说明
进入系统视图	**system-view**	-
创建本地镜像组	**mirroring-group** *group-id* **local**	必选 缺省情况下，不存在任何本地镜像组

1.4.4 配置源端口

在源设备上，请将源端口指定为待监控的端口；而在目的设备上，请将源端口指定为 Tunnel 接口对应的物理端口。

可以在系统视图下为指定镜像组配置一个或多个源端口，也可以在端口视图下将当前端口配置为指定镜像组的源端口，二者的配置效果相同。

1. 在系统视图下配置源端口

表1-24 在系统视图下配置源端口

操作	命令	说明
进入系统视图	**system-view**	-
为本地镜像组配置源端口	**mirroring-group** *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }	必选 缺省情况下，本地镜像组没有源端口

2. 在端口视图下配置源端口

表1-25 在端口视图下配置源端口

操作	命令	说明
进入系统视图	**system-view**	-
进入端口视图	**interface** *interface-type interface-number*	-
配置本端口为本地镜像组的源端口	[**mirroring-group** *group-id*] **mirroring-port** { **both** | **inbound** | **outbound** }	必选 缺省情况下，端口不是任何本地镜像组的源端口

说明

- 一个镜像组内可以配置多个源端口。
- 在 S5500-28SC-HI 和 S5500-52SC-HI 交换机上，每个端口无论作为单向或双向源端口，均最多只能加入两个镜像组。
- 在其他 S5500-HI 系列交换机上，对源端口的单向数据进行镜像需要占用一个镜像资源，对源端口的双向数据进行镜像需要占用两个镜像资源，对一个源端口最多分配四个镜像资源。即一个端口作为单向源端口最多可以加入四个镜像组，作为双向源端口最多可以加入两个镜像组，或者以一个双向源端口和两个单向源端口的形式加入三个镜像组。

1.4.5 配置源CPU

在源设备上，请将源 CPU 指定为待监控设备上的 CPU；而在目的设备上，不支持配置源 CPU。

表1-26 配置源 CPU

操作	命令	说明
进入系统视图	**system-view**	-
为本地镜像组配置源CPU	**mirroring-group** *group-id* **mirroring-cpu slot** *slot-number-list* { **both** | **inbound** | **outbound** }	必选 缺省情况下，本地镜像组没有源 CPU

说明

一个镜像组内可以配置多个源 CPU。

1.4.6 配置目的端口

在源设备上，请将目的端口指定为 Tunnel 接口；而在目的设备上，请将目的端口指定为连接数据监测设备的端口。

可以在系统视图下为指定镜像组配置目的端口，也可以在端口视图下将当前端口配置为指定镜像组的目的端口，二者的配置效果相同。

1. 在系统视图下配置目的端口

表1-27 在系统视图下配置目的端口

操作	命令	说明
进入系统视图	**system-view**	-
为本地镜像组配置目的端口	**mirroring-group** *group-id* **monitor-port** *monitor-port-id*	必选 缺省情况下，本地镜像组没有目的端口

2. 在端口视图下配置目的端口

表1-28 在端口视图下配置目的端口

操作	命令	说明
进入系统视图	**system-view**	-
进入端口视图	**interface** *interface-type interface-number*	-
配置本端口为本地镜像组的目的端口	[**mirroring-group** *group-id*] **monitor-port**	必选 缺省情况下，端口不是任何本地镜像组的目的端口

说明

- 一个镜像组内只能配置一个目的端口。
- 在目的设备上，请不要在目的端口上使能生成树协议，否则会影响镜像功能的正常使用。
- 从目的端口发出的报文包括镜像报文和其它端口正常转发来的报文。为了保证数据监测设备只对镜像报文进行分析，请将目的端口只用于端口镜像，不作其它用途。
- 镜像组的目的端口不能配置为已经接入 RRPP 环的端口。

1.5 端口镜像显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后镜像组的运行情况，通过查看显示信息验证配置的效果。

表1-29 端口镜像显示和维护

操作	命令
显示镜像组的配置信息	**display mirroring-group** { *group-id* | **all** | **local** | **remote-destination** | **remote-source** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.6 端口镜像典型配置举例

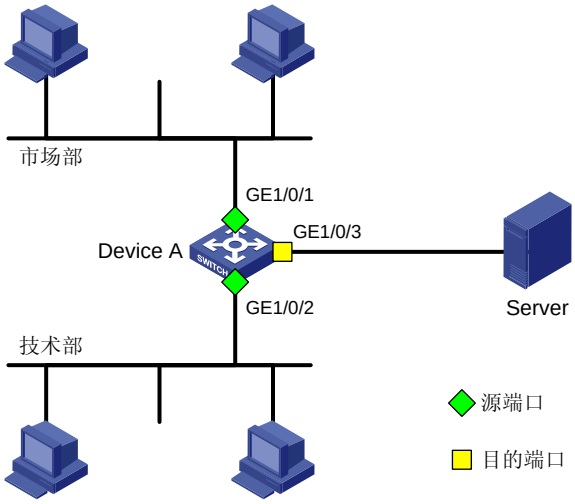
1.6.1 本地端口镜像配置举例

1. 组网需求

- Device A 通过端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别连接市场部和技术部，并通过端口 GigabitEthernet1/0/3 连接 Server。
- 通过配置源端口方式的本地端口镜像，使 Server 可以监控所有进、出市场部和技术部的报文。

2. 组网图

图1-4 本地端口镜像配置组网图



3. 配置步骤

(1) 配置本地镜像组

创建本地镜像组 1。

```
<DeviceA> system-view
[DeviceA] mirroring-group 1 local
```

配置本地镜像组 1 的源端口为 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2，目的端口为 GigabitEthernet1/0/3。

```
[DeviceA] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 gigabitethernet 1/0/2 both
[DeviceA] mirroring-group 1 monitor-port gigabitethernet 1/0/3
```

在目的端口 GigabitEthernet1/0/3 上关闭生成树协议。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] undo stp enable
[DeviceA-GigabitEthernet1/0/3] quit
```

(2) 检验配置效果

显示所有镜像组的配置信息。

```
[DeviceA] display mirroring-group all
mirroring-group 1:
    type: local
    status: active
    mirroring port:
        GigabitEthernet1/0/1  both
        GigabitEthernet1/0/2  both
    mirroring CPU:
    monitor port: GigabitEthernet1/0/3
```

配置完成后，用户可以通过 Server 监控所有进、出市场部和技术部的报文。

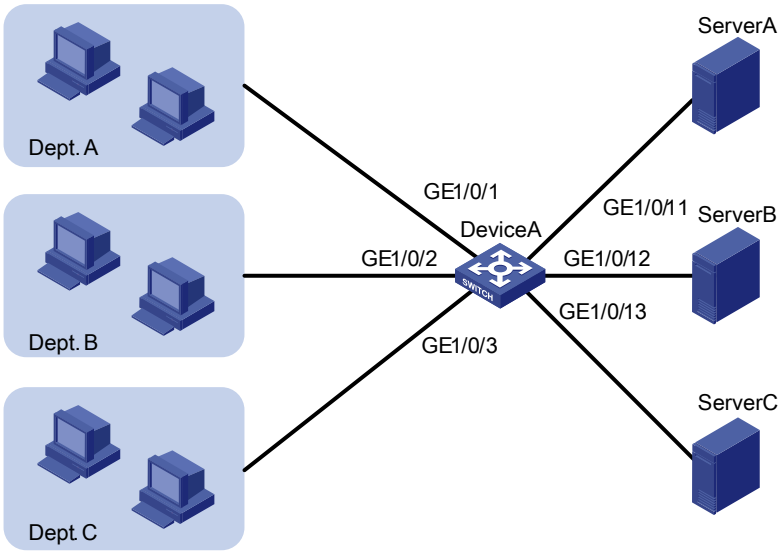
1.6.2 利用远程镜像VLAN实现本地镜像支持多个目的端口典型配置举例

1. 组网需求

三个部门 A、B、C 分别使用 GigabitEthernet1/0/1～GigabitEthernet1/0/3 端口接入 DeviceA，现要求通过镜像功能，使三台数据检测设备 ServerA、ServerB、ServerC 都能够对三个部门发送和接收的报文进行镜像。

2. 组网图

图1-5 利用远程镜像 VLAN 实现本地镜像支持多个目的端口组网图



3. 配置步骤

创建远程源镜像组 1。

```
<DeviceA> system-view
[DeviceA] mirroring-group 1 remote-source
```

将接入部门 A、B、C 的三个端口配置为远程源镜像组 1 的源端口。

```
[DeviceA] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
both
```

将设备上任意未使用的端口（此处以 GigabitEthernet1/0/5 为例）配置为镜像组 1 的反射口。

```
[DeviceA] mirroring-group 1 reflector-port GigabitEthernet 1/0/5
```

创建 VLAN10 作为镜像组 1 的远程镜像 VLAN，并将接入三台数据检测设备的端口加入 VLAN10。

```
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 1/0/11 to gigabitethernet 1/0/13
[DeviceA-vlan10] quit
```

配置 VLAN10 作为镜像组 1 的远程镜像 VLAN。

```
[DeviceA] mirroring-group 1 remote-probe vlan 10
```

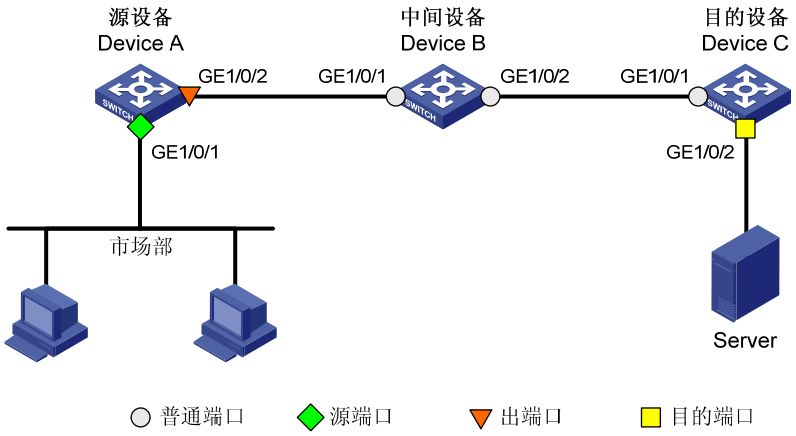
1.6.3 二层远程端口镜像配置举例

1. 组网需求

- 在一个二层网络中，Device A 通过端口 GigabitEthernet1/0/1 连接市场部，并通过 Trunk 端口 GigabitEthernet1/0/2 与 Device B 的 Trunk 端口 GigabitEthernet1/0/1 相连；Device C 通过端口 GigabitEthernet1/0/2 连接 Server，并通过 Trunk 端口 GigabitEthernet1/0/1 与 Device B 的 Trunk 端口 GigabitEthernet1/0/2 相连。
- 通过配置二层远程端口镜像，使 Server 可以监控所有进、出市场部的报文。

2. 组网图

图1-6 二层远程端口镜像配置组网图



3. 配置步骤

(1) 配置 Device C

配置端口 GigabitEthernet1/0/1 为 Trunk 口，并允许 VLAN 2 的报文通过。

```
<DeviceC> system-view
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 2
[DeviceC-GigabitEthernet1/0/1] quit
```

创建远程目的镜像组 1。

```
[DeviceC] mirroring-group 1 remote-destination
```

创建 VLAN 2 作为远程镜像 VLAN。

```
[DeviceC] vlan 2
```

关闭远程镜像 VLAN 的 MAC 地址学习功能

```
[DeviceC-vlan2] mac-address mac-learning disable
[DeviceC-vlan2] quit
```

配置远程目的镜像组 1 的远程镜像 VLAN 为 VLAN 2，目的端口为 GigabitEthernet1/0/2，在该端口上关闭生成树协议并将其加入 VLAN 2。

```
[DeviceC] mirroring-group 1 remote-probe vlan 2
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] mirroring-group 1 monitor-port
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port access vlan 2
[DeviceC-GigabitEthernet1/0/2] quit
```

(2) 配置 Device B

创建 VLAN 2 作为远程镜像 VLAN。

```
<DeviceB> system-view
[DeviceB] vlan 2
```

关闭远程镜像 VLAN 的 MAC 地址学习功能

```
[DeviceB-vlan2] mac-address mac-learning disable
[DeviceB-vlan2] quit
```

配置端口 GigabitEthernet1/0/1 为 Trunk 口，并允许 VLAN 2 的报文通过。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 2
```

```
[DeviceB-GigabitEthernet1/0/1] quit
```

配置端口 GigabitEthernet1/0/2 为 Trunk 口，并允许 VLAN 2 的报文通过。

```
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 2
[DeviceB-GigabitEthernet1/0/2] quit
```

(3) 配置 Device A

创建远程源镜像组 1。

```
<DeviceA> system-view
[DeviceA] mirroring-group 1 remote-source
```

创建 VLAN 2 作为远程镜像 VLAN。

```
[DeviceA] vlan 2
```

关闭远程镜像 VLAN 的 MAC 地址学习功能

```
[DeviceA-vlan2] mac-address mac-learning disable
[DeviceA-vlan2] quit
```

配置远程源镜像组 1 的远程镜像 VLAN 为 VLAN 2，源端口为 GigabitEthernet1/0/1，出端口为 GigabitEthernet1/0/2。

```
[DeviceA] mirroring-group 1 remote-probe vlan 2
[DeviceA] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 both
[DeviceA] mirroring-group 1 monitor-egress gigabitethernet 1/0/2
```

配置出端口 GigabitEthernet1/0/2 为 Trunk 口，允许 VLAN 2 的报文通过，并在该端口上关闭生成树协议。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 2
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

(4) 检验配置效果

配置完成后，用户可以通过 Server 监控所有进、出市场部的报文。

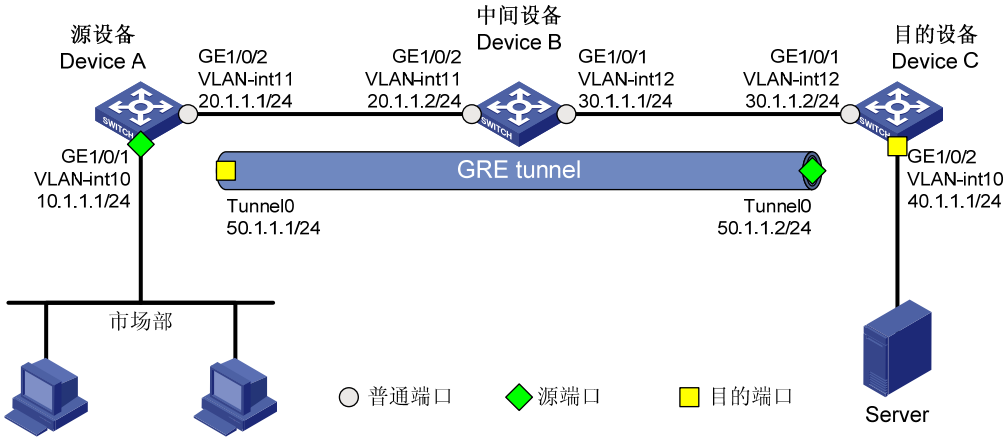
1.6.4 三层远程端口镜像配置举例

1. 组网需求

- 在一个三层网络中，Device A 通过端口 GigabitEthernet1/0/1 连接市场部，并通过端口 GigabitEthernet1/0/2 与 Device B 的端口 GigabitEthernet1/0/1 相连；Device C 通过端口 GigabitEthernet1/0/2 连接 Server，并通过端口 GigabitEthernet1/0/1 与 Device B 的端口 GigabitEthernet1/0/2 相连。
- 通过配置三层远程端口镜像，使 Server 可以通过 GRE 隧道穿越三层网络监控所有进、出市场部的报文。

2. 组网图

图1-7 三层远程端口镜像配置组网图



3. 配置步骤

(1) 配置 IP 地址

请按照 图 1-7 配置VLAN，并将相应端口加入VLAN，配置各接口的IP地址和子网掩码，具体配置过程略。

(2) 配置 Device A

创建接口 Tunnel0，并为其配置 IP 地址和掩码。

```
<DeviceA> system-view
[DeviceA] interface tunnel 0
[DeviceA-Tunnel0] ip address 50.1.1.1 24
```

配置 Tunnel0 接口采用 GRE 隧道模式，并为该接口指定源地址和目的地址。

```
[DeviceA-Tunnel0] tunnel-protocol gre
[DeviceA-Tunnel0] source 20.1.1.1
[DeviceA-Tunnel0] destination 30.1.1.2
[DeviceA-Tunnel0] quit
```

创建并配置业务环回组 1，服务类型为 tunnel。

```
[DeviceA] service-loopback group 1 type tunnel
```

将设备上的任意端口（此处以 GigabitEthernet1/0/3 为例）加入业务环回组 1。

```
[DeviceA] interface GigabitEthernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] undo stp enable
[DeviceA-GigabitEthernet1/0/3] port service-loopback group 1
```

在 Tunnel 接口视图下指定隧道引用的业务环回组 1。

```
[DeviceA-GigabitEthernet1/0/3] quit
[DeviceA] interface tunnel 0
[DeviceA-Tunnel0] service-loopback-group 1
```

配置 OSPF 协议。

```
[DeviceA] ospf 1
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 50.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] quit
```

创建本地镜像组 1。

```
[DeviceA] mirroring-group 1 local
```

配置本地镜像组 1 的源端口为 GigabitEthernet1/0/1，目的端口为 Tunnel0。

```
[DeviceA] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 both
[DeviceA] mirroring-group 1 monitor-port tunnel 0
```

(3) 配置 Device B

配置 OSPF 协议。

```
<DeviceB> system-view
[DeviceB] ospf 1
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

(4) 配置 Device C

创建接口 Tunnel0，并为其配置 IP 地址和掩码。

```
<DeviceC> system-view
[DeviceC] interface tunnel 0
[DeviceC-Tunnel0] ip address 50.1.1.2 24
```

配置 Tunnel0 接口采用 GRE 隧道模式，并为该接口指定源地址和目的地址。

```
[DeviceC-Tunnel0] tunnel-protocol gre
[DeviceC-Tunnel0] source 30.1.1.2
[DeviceC-Tunnel0] destination 20.1.1.1
[DeviceC-Tunnel0] quit
```

创建并配置业务环回组 1，服务类型为 tunnel。

```
[DeviceC] service-loopback group 1 type tunnel
```

将设备上的任意端口（此处以 GigabitEthernet1/0/3 为例）加入业务环回组 1。

```
[DeviceC] interface GigabitEthernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] undo stp enable
[DeviceC-GigabitEthernet1/0/3] port service-loopback group 1
```

在 Tunnel 接口视图下指定隧道引用的业务环回组 1。

```
[DeviceC-GigabitEthernet1/0/3] quit
[DeviceC] interface tunnel 0
[DeviceC-Tunnel0] service-loopback-group 1
[DeviceC-Tunnel0] quit
```

配置 OSPF 协议。

```
[DeviceC] ospf 1
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 40.1.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 50.1.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] quit
[DeviceC-ospf-1] quit
```

创建本地镜像组 1。

```
[DeviceC] mirroring-group 1 local
```

配置本地镜像组 1 的源端口为 GigabitEthernet1/0/1，目的端口为 GigabitEthernet1/0/2。

```
[DeviceC] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 inbound
[DeviceC] mirroring-group 1 monitor-port gigabitethernet 1/0/2
```

在目的端口 GigabitEthernet1/0/2 上关闭生成树协议。

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] quit
```

(5) 检验配置效果

配置完成后，用户可以通过 Server 监控所有进、出市场部的报文。

2 流镜像配置

说明

流镜像功能中提到的端口包括二层以太网端口和三层以太网端口。三层以太网端口是指被配置为三层模式的以太网端口，有关以太网端口模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口配置”。

2.1 流镜像简介

流镜像是指将指定报文复制到指定目的地，用于报文的分析和监控。流镜像通过 QoS 策略来实现，即使用流分类技术为待镜像报文定义匹配条件，再通过配置流行为将符合条件的报文镜像至指定目的地。其优势在于用户通过流分类技术可以灵活地制订匹配条件，从而对报文类型进行精细区分，以获取更加精确的统计信息。根据报文镜像的目的地不同，流镜像可分为以下几种类型：

- 流镜像到端口：将符合要求的报文复制后转发到指定端口。
- 流镜像到 CPU：将符合要求的报文复制后转发到 CPU（这里的 CPU 是指配置了流镜像的源端口所在设备上的 CPU）。

说明

有关 QoS 策略、流分类和流行为的详细介绍，请参见“ACL 和 QoS 配置指导”中的“QoS 配置方式”。

2.2 流镜像配置任务简介

表2-1 流镜像配置任务简介

配置任务		说明	详细配置
配置报文匹配规则		必选	2.3.1
配置流镜像类型	配置流镜像到端口	二者必选其一	2.3.2 1.
	配置流镜像到CPU		2.3.2 2.
配置QoS策略		必选	2.3.3
应用QoS策略	基于端口应用	四者必选其一	2.3.4 1.
	基于VLAN应用		2.3.4 2.
	基于全局应用		2.3.4 3.
	基于控制平面应用		2.3.4 4.

2.3 配置流镜像

2.3.1 配置报文匹配规则

表2-2 配置报文匹配规则

操作	命令	说明
进入系统视图	**system-view**	-
定义流分类，并进入流分类视图	**traffic classifier** *tcl-name* [**operator** { **and** | **or** }]	必选 缺省情况下，不存在任何流分类
配置报文匹配规则	**if-match** *match-criteria*	必选 缺省情况下，流分类中不存在任何报文匹配规则

说明

有关 **traffic classifier** 和 **if-match** 命令的详细介绍，请参见“ACL 和 QoS 命令参考”中的“QoS 策略”。

2.3.2 配置流镜像类型

说明

在同一流行为中只能配置一种类型的流镜像。

1. 配置流镜像到端口

表2-3 配置流镜像到端口

操作	命令	说明
进入系统视图	**system-view**	-
定义流行为，并进入流行为视图	**traffic behavior** *behavior-name*	必选 缺省情况下，不存在任何流行为
配置流镜像到指定端口	**mirror-to interface** *interface-type interface-number*	必选 缺省情况下，流行为中未配置任何流镜像

说明

- 有关 **traffic behavior** 命令的详细介绍，请参见“ACL 和 QoS 命令参考”中的“QoS 策略”。
- 通过多次执行 **mirror-to interface** 命令，最多可以将报文镜像至四个目的端口。

2. 配置流镜像到CPU

表2-4 配置流镜像到 CPU

操作	命令	说明
进入系统视图	**system-view**	-
定义流行为，并进入流行为视图	**traffic behavior** *behavior-name*	必选 缺省情况下，不存在任何流行为
配置流镜像到CPU	**mirror-to cpu**	必选 缺省情况下，流行为中未配置任何流镜像

说明

- 有关 **traffic behavior** 命令的详细介绍，请参见“ACL 和 QoS 命令参考”中的“QoS 策略”。
- 上述 CPU 是指配置了流镜像的端口所在设备上的 CPU。

2.3.3 配置QoS策略

表2-5 配置 QoS 策略

操作	命令	说明
进入系统视图	**system-view**	-
定义QoS策略，并进入QoS策略视图	**qos policy** *policy-name*	必选 缺省情况下，不存在任何策略
为流分类指定采用的流行为	**classifier** *tcl-name* **behavior** *behavior-name*	必选 缺省情况下，没有为流分类指定采用的流行为

说明

有关 **qos policy** 和 **classifier behavior** 命令的详细介绍，请参见“ACL 和 QoS 命令参考”中的“QoS 策略”。

2.3.4 应用QoS策略

说明

有关应用 QoS 策略的详细介绍，请参见“ACL 和 QoS 配置指导”中的“QoS 配置方式”。

1. 基于端口应用

将 QoS 策略应用到某端口，可以对该端口指定方向上的流量进行镜像。一个 QoS 策略可以应用于多个端口，而端口在每个方向上只能应用一个 QoS 策略。

表2-6 基于端口应用

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	进入端口视图	**interface** *interface-type interface-number*	二者必选其一 端口视图下的配置只对当前端口生效；端口组视图下的配置将对端口组中的所有端口生效
	进入端口组视图	**port-group manual** *port-group-name*	
应用QoS策略到端口		**qos apply policy** *policy-name* { **inbound** | **outbound** }	必选

说明

有关 **qos apply policy** 命令的详细介绍，请参见“ACL 和 QoS 命令参考”中的“QoS 策略”。

2. 基于VLAN应用

将 QoS 策略应用到某 VLAN，可以对该 VLAN 内各端口指定方向上的流量进行镜像。

表2-7 基于 VLAN 应用

操作	命令	说明
进入系统视图	**system-view**	-
应用QoS策略到指定VLAN	**qos vlan-policy** *policy-name* **vlan** *vlan-id-list* { **inbound** | **outbound** }	必选

说明

有关 **qos vlan-policy** 命令的详细介绍，请参见“ACL 和 QoS 命令参考”中的“QoS 策略”。

3. 基于全局应用

将 QoS 策略应用到全局，可以对设备各端口指定方向上的流量进行镜像。

表2-8 基于全局应用

操作	命令	说明
进入系统视图	**system-view**	-
应用QoS策略到全局	**qos apply policy** *policy-name* **global** { **inbound** | **outbound** }	必选

说明

有关 **qos apply policy** 命令的详细介绍，请参见“ACL 和 QoS 命令参考”中的“QoS 策略”。

4. 基于控制平面应用

将 QoS 策略应用到控制平面，可以对控制平面入方向上的流量进行镜像。

表2-9 基于控制平面应用

操作	命令	说明
进入系统视图	**system-view**	-
进入控制平面视图	**control-plane slot** *slot-number*	-
应用QoS策略到控制平面	**qos apply policy** *policy-name* **inbound**	必选

说明

有关 **control-plane** 和 **qos apply policy** 命令的详细介绍，请参见“ACL 和 QoS 命令参考”中的“QoS 策略”。

2.4 流镜像典型配置举例

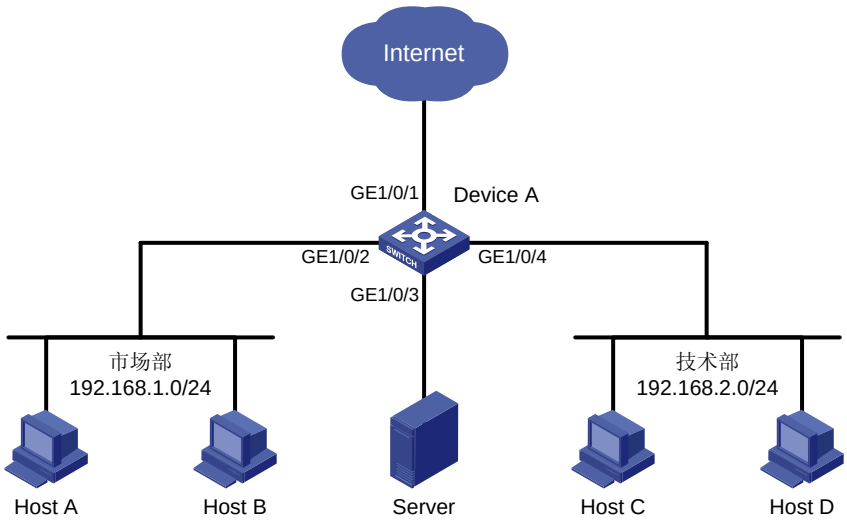
2.4.1 流镜像典型配置举例

1. 组网需求

- 某公司内的各部门之间使用不同网段的IP地址，其中市场部和技术部分别使用192.168.1.0/24和192.168.2.0/24网段，该公司的工作时间为每周工作日的8点到18点。
- 通过配置流镜像，使Server可以监控技术部访问互联网的WWW流量，以及技术部在工作时间发往市场部的IP流量。

2. 组网图

图2-1 流镜像典型配置组网图



3. 配置步骤

(1) 配置监控技术部访问互联网的流量

创建 ACL 3000，并定义如下规则：匹配技术部（192.168.2.0/24 网段）访问 WWW 的报文。

```
<DeviceA> system-view
[DeviceA] acl number 3000
[DeviceA-acl-adv-3000] rule permit tcp source 192.168.2.0 0.0.0.255 destination-port eq www
[DeviceA-acl-adv-3000] quit
```

创建流分类 tech_c，并配置报文匹配规则为 ACL 3000。

```
[DeviceA] traffic classifier tech_c
[DeviceA-classifier-tech_c] if-match acl 3000
[DeviceA-classifier-tech_c] quit
```

创建流行为 tech_b，并配置流镜像到端口 GigabitEthernet1/0/3。

```
[DeviceA] traffic behavior tech_b
[DeviceA-behavior-tech_b] mirror-to interface gigabitethernet 1/0/3
[DeviceA-behavior-tech_b] quit
```

创建 QoS 策略 tech_p，并指定流分类 tech_c 采用流行为 tech_b。

```
[DeviceA] qos policy tech_p
[DeviceA-qospolicy-tech_p] classifier tech_c behavior tech_b
[DeviceA-qospolicy-tech_p] quit
```

将 QoS 策略 tech_p 应用到端口 GigabitEthernet1/0/1 的出方向上。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] qos apply policy tech_p outbound
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 配置监控技术部发往市场部的流量

定义工作时间：创建名为 work 的时间段，其时间范围为每周工作日的 8 点到 18 点。

```
[DeviceA] time-range work 8:0 to 18:0 working-day
```

创建 ACL 3001，并定义如下规则：匹配在工作时间由技术部（192.168.2.0/24 网段）发往市场部（192.168.1.0/24 网段）的 IP 报文。

```
[DeviceA] acl number 3001
[DeviceA-acl-adv-3001] rule permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0
0.0.0.255 time-range work
[DeviceA-acl-adv-3001] quit
```

创建流分类 mkt_c，并配置报文匹配规则为 ACL 3001。

```
[DeviceA] traffic classifier mkt_c
[DeviceA-classifier-mkt_c] if-match acl 3001
[DeviceA-classifier-mkt_c] quit
```

创建流行为 mkt_b，并配置流镜像到端口 GigabitEthernet1/0/3。

```
[DeviceA] traffic behavior mkt_b
[DeviceA-behavior-mkt_b] mirror-to interface gigabitethernet 1/0/3
[DeviceA-behavior-mkt_b] quit
```

创建 QoS 策略 mkt_p，并指定流分类 mkt_c 采用流行为 mkt_b。

```
[DeviceA] qos policy mkt_p
[DeviceA-qospolicy-mkt_p] classifier mkt_c behavior mkt_b
[DeviceA-qospolicy-mkt_p] quit
```

将 QoS 策略 mkt_p 应用到端口 GigabitEthernet1/0/2 的出方向上。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] qos apply policy mkt_p outbound
```

(3) 检验配置效果

配置完成后，用户可以通过 Server 监控技术部访问互联网的 WWW 流量，以及技术部在工作时间发往市场部的 IP 流量。

目 录

1 NQA配置

1.1 NQA简介

1.1.1 NQA概述

NQA 是 Network Quality Analyzer（网络质量分析）的简称。NQA 通过发送探测报文，对网络性能、网络提供的服务及服务质量进行分析，并为用户提供网络性能和服务质量的参数，如时延抖动、TCP 连接建立时间、FTP 连接建立时间和文件传输速率等。

利用 NQA 的测试结果，用户可以：

(1) 及时了解网络的性能状况，针对不同的网络性能进行相应处理。

(2) 对网络故障进行诊断和定位。

1.1.2 NQA的特点

1. 支持多种测试类型

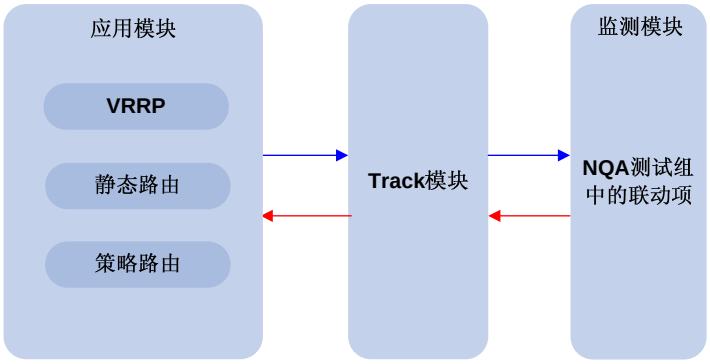
以往的 Ping 功能是使用 ICMP（Internet Control Message Protocol，互联网控制消息协议）测试数据包在本端和指定目的端之间的往返时间。NQA 是对 Ping 功能的扩展和增强，它增加了多种测试类型，提供了更多的功能。

目前 NQA 支持 11 种测试类型：ICMP-echo、DHCP、DNS、FTP、HTTP、UDP-jitter、SNMP、TCP、UDP-echo、Voice 和 DLSw 测试。客户端向对端发送不同类型的探测报文，统计对端是否回应报文以及报文的往返时间等参数，以便用户根据统计结果判断协议的可用性和网络的性能。

2. 支持联动功能

联动功能是指通过建立联动项，对NQA探测结果进行监测，当连续探测失败次数达到一定数目时，就通过Track模块触发应用模块联动。联动功能的实现如 图 1-1 所示。

图1-1 联动功能实现示意图



联动功能由监测模块、Track 模块和应用模块三部分组成：

- 监测模块负责对链路状态、网络性能等进行监测，并将探测结果通知给 Track 模块。
- Track 模块接收到监测模块的探测结果后，及时改变 Track 项的状态，并通知应用模块。Track 模块位于应用模块和监测模块之间，可以屏蔽不同监测模块的差异，为应用模块提供统一的接口。
- 应用模块根据 Track 项的状态，进行相应的处理，从而实现联动。

以静态路由为例，用户配置了一条静态路由，下一跳为 192.168.0.88，如果 192.168.0.88 可达，那么该静态路由有效；如果 192.168.0.88 不可达，则该静态路由无效。通过在 NQA、Track 模块和静态路由模块之间建立联动，可以实现静态路由有效性的实时判断：

(1) 通过 NQA 监测地址 192.168.0.88 是否可达。

(2) 如果 NQA 发现 192.168.0.88 不可达，则通知 Track 模块改变 Track 项的状态。

(3) Track 项将改变后的状态通知给静态路由模块。静态路由模块据此可以判断该静态路由项无效。

说明

联动功能和 Track 模块的详细介绍，请参见“可靠性配置指导”中的“Track”。

3. 支持阈值告警功能

NQA 可以对探测结果进行监测，通过向网管服务器发送 Trap 消息，及时将监测结果通知给网管服务器，以便网络管理员根据 Trap 消息了解测试运行状况和网络性能。

(1) 监测对象

NQA阈值告警功能支持的监测对象及对应的测试类型，如 表 1-1 所示：

表1-1 NQA 阈值告警功能支持的监测对象

监测对象	支持的测试类型
探测持续时间	除UDP-jitter和Voice之外的测试类型
探测失败次数	除UDP-jitter和Voice之外的测试类型
报文往返时间	UDP-jitter和Voice测试类型
丢弃报文数目	UDP-jitter和Voice测试类型
源到目的和目的到源的单向时延抖动	UDP-jitter和Voice测试类型
源到目的和目的到源的单向时延	UDP-jitter和Voice测试类型
ICPIF（Calculated Planning Impairment Factor，计算计划损伤元素）值 ICPIF的详细介绍请参见“1.6.10 配置Voice测试”	Voice测试类型
MOS（Mean Opinion Scores，平均意见得分）值 MOS的详细介绍请参见“1.6.10 配置Voice测试”	Voice测试类型

(2) 阈值类型

NQA 阈值告警功能支持的阈值类型包括：

- **average**：阈值类型为平均值，即：监测一次测试中探测结果的平均值，如果平均值不在指定的范围内，则该监测对象超出阈值。例如，监测一次测试中探测持续时间的平均值。
- **accumulate**：阈值类型为累计数目，即：监测一次测试中探测结果不在指定范围内的累计数目，如果累计数目达到或超过设定的值，则该监测对象超出阈值。
- **consecutive**：阈值类型为连续次数，即：NQA 测试组启动后，监测探测结果连续不在指定范围内的次数，如果该次数达到或超过设定的值，则该监测对象超出阈值。

说明

阈值类型为 **average** 和 **accumulate** 时，以每次测试为界限监测探测结果；阈值类型为 **consecutive** 时，不以测试为界限监测探测结果。

(3) 触发动作

NQA 阈值告警功能可以触发如下动作：

- **none**：只在显示信息中记录监测结果，不向网管发送 Trap 消息。
- **trap-only**：在显示信息中记录监测结果的同时，向网管发送 Trap 消息。

说明

DNS 测试不支持发送 Trap 消息，即对于 DNS 测试，触发动作只能配置为 **none**。

(4) 阈值告警组

NQA 通过创建阈值告警组、在阈值告警组中配置监测的对象、阈值类型及触发的动作，来实现阈值告警功能。

阈值告警组包括 invalid、over-threshold 和 below-threshold 三种状态：

- NQA 测试组未启动时，阈值告警组的状态为 invalid。
- NQA 测试组启动后，每次测试或探测结束时，检查监测的对象是否超出阈值。如果超出阈值，则阈值告警组的状态变为 over-threshold；如果未超出阈值，则状态变为 below-threshold。

若配置阈值告警组的触发动作为 **trap-only**，则当阈值告警组的状态改变时，向网管发送 Trap 消息。

1.1.3 NQA的基本概念

1. 测试组

NQA 可以对多个目标（例如，目的主机或服务器）进行测试。NQA 通过测试组管理和调度针对某一目标的 NQA 测试。进行 NQA 测试前，需要先创建 NQA 测试组。在 NQA 测试组中配置 NQA 测试的参数，如测试类型，测试目的地址，测试目的端口等。

每个测试组都有一个管理员名称和一个操作标签，管理员名称和操作标签可以唯一确定一个测试组。

2. 测试和探测

启动 NQA 测试组后，每隔一段时间进行一次测试，测试的时间间隔可以由用户来设定。

一次 NQA 测试由若干次连续的探测组成，探测的次数可以由用户来设定。

说明

对于 Voice 测试，一次测试中只能进行一次探测。

不同测试类型中，探测的含义不同：

- 对于 TCP 和 DLSw 测试，一次探测操作是指建立一次连接；
- 对于 UDP-jitter 和 Voice 测试，一次探测操作是指连续发送多个探测报文，发送探测报文的个数由用户来设定；
- 对于 FTP、HTTP、DHCP 和 DNS 测试，一次探测操作是指完成一次相应的功能，例如上传或下载一个文件，获取一个 Web 页面，为接口申请一个 IP 地址，将一个域名解析为 IP 地址；
- 对于 ICMP-echo 和 UDP-echo 测试，一次探测操作是指发送一个探测报文；
- 对于 SNMP 测试，一次探测操作是指发送三个 SNMP 协议报文，分别对应 SNMP v1、SNMP v2c 和 SNMP v3 三个版本。

3. NQA客户端和服务器

NQA 客户端是发起 NQA 测试的设备，NQA 测试组在客户端创建。

NQA服务器负责处理NQA客户端发来的探测报文，如 图 1-2 所示。NQA服务器监听指定IP地址和端口的报文，并对客户端发送的探测报文进行响应。

图1-2 NQA 客户端与服务器之间的关系

在大多数的测试中，只需要配置 NQA 客户端。但在进行 TCP、UDP-echo、UDP-jitter 和 Voice 类型测试时，必须配置 NQA 服务器。

在一个 NQA 服务器上可以创建多个 TCP 或 UDP 监听服务，每个监听服务对应一个目的地址和一个端口号，配置的目的地址和端口号必须与 NQA 客户端的配置一致，且不能与已有的监听服务冲突。

1.1.4 NQA测试操作

NQA 测试操作的过程为：

(1) NQA 客户端构造指定测试类型的探测报文，并发送给对端；

(2) 对端收到探测报文后，回复带有时间戳的应答报文；

(3) NQA 客户端根据是否收到应答报文，以及应答报文中的时间戳，计算报文丢失率、往返时间等参数。

1.2 NQA配置任务简介

表1-2 NQA 服务器配置任务简介

配置任务	说明	详细配置
配置NQA服务器	对于TCP、UDP-echo、UDP-jitter和Voice四种测试类型，为必选	1.3

要成功进行某项测试，NQA 客户端上需要进行如下操作：

(1) 使能 NQA 客户端功能。

(2) 创建测试组，根据测试类型进行相应测试参数的配置。不同测试类型对应的测试参数不同，详见下面具体的配置过程。

(3) 启动 NQA 测试组。

表1-3 NQA 客户端配置任务简介

配置任务		说明	详细配置
使能NQA客户端功能		必选	1.4
创建NQA测试组		必选	1.5
配置NQA测试组	配置ICMP-echo测试	必选其一	1.6.1
	配置DHCP测试		1.6.2
	配置DNS测试		1.6.3
	配置FTP测试		1.6.4
	配置HTTP测试		1.6.5
	配置UDP-jitter测试		1.6.6
	配置SNMP测试		1.6.7

配置任务		说明	详细配置
	配置TCP测试		1.6.8
	配置UDP-echo测试		1.6.9
	配置Voice测试		1.6.10
	配置DLSw测试		1.6.11
配置联动功能		可选	1.7
配置阈值告警功能		可选	1.8
配置NQA统计功能		可选	1.9
配置NQA历史记录功能		可选	1.10
配置NQA测试组通用可选参数		可选	1.11
调度NQA测试组		必选	1.12

1.3 配置NQA服务器

在进行 TCP、UDP-echo、UDP-jitter 和 Voice 类型测试前，必须在对端设备上配置 NQA 服务器。NQA 服务器监听指定 IP 地址和端口的报文，并对客户端发送的探测报文进行响应。

表1-4 配置 NQA 服务器

操作	命令	说明
进入系统视图	**system-view**	-
开启NQA服务器功能	**nqa server enable**	必选 缺省情况下，NQA服务器功能处于关闭状态
在NQA服务器上配置监听服务	**nqa server** { **tcp-connect** | **udp-echo** } *ip-address port-number*	必选 配置的IP地址和端口号必须与NQA客户端的配置一致，且不能与已有的监听服务冲突
配置NQA服务器监听服务发送报文的ToS值	**nqa server** { **tcp-connect** | **udp-echo** } **tos** *tos*	可选 缺省情况下，NQA服务器监听服务发送报文的ToS值为0

1.4 使能NQA客户端功能

只有使能 NQA 客户端功能后，NQA 客户端的相关配置才会生效。

表1-5 使能 NQA 客户端功能

操作	命令	说明
进入系统视图	**system-view**	-
开启NQA客户端功能	**nqa agent enable**	可选 缺省情况下，NQA客户端功能处于开启状态

1.5 创建NQA测试组

进行 NQA 测试前，需要先创建 NQA 测试组。创建测试组并进入测试组视图后，可以配置测试的类型。

表1-6 创建 NQA 测试组

操作	命令	说明
进入系统视图	**system-view**	-
创建NQA测试组，并进入NQA测试组视图	**nqa entry** *admin-name operation-tag*	必选

说明

执行 **nqa entry** 命令进入已经配置测试类型的测试组视图时，将直接进入测试组测试类型视图。

1.6 配置NQA测试组

1.6.1 配置ICMP-echo测试

ICMP-echo 测试利用 ICMP 协议，根据是否接收到应答报文判断目的主机的可达性。ICMP-echo 测试的功能与 Ping 命令类似，但 ICMP-echo 测试中可以指定测试的下一跳设备，并且 ICMP-echo 测试的输出信息更为丰富。网络中出现连通性故障时，可以通过 ICMP-echo 测试对故障进行定位。

表1-7 配置 ICMP-echo 测试

操作	命令	说明
进入系统视图	**system-view**	-
进入NQA测试组视图	**nqa entry** *admin-name operation-tag*	-
配置测试类型为ICMP-echo，并进入测试类型视图	**type icmp-echo**	必选
配置测试操作的目的地址	**destination ip** *ip-address*	必选 缺省情况下，未配置测试操作的目的IP地址
配置发送的探测报文的大小	**data-size** *size*	可选 缺省情况下，发送的探测报文为100字节
配置发送的探测报文的填充字符串	**data-fill** *string*	可选 缺省情况下，探测报文的填充内容为十六进制数值00010203040506070809
指定测试操作所属的VPN	**vpn-instance** *vpn-instance-name*	可选 缺省情况下，未指定测试操作所属的VPN，NQA用来测试公网的连通性

操作	命令	说明
配置探测报文的源接口	**source interface** *interface-type interface-number*	可选 缺省情况下，未配置探测报文的源接口 如果使用**source ip**命令配置了ICMP-echo测试的源地址，则此配置无效；否则，指定的源接口的IP地址将作为ICMP-echo探测报文的源IP地址 该命令指定的接口必须为up状态，否则探测将会失败
配置探测报文的源IP地址	**source ip** *ip-address*	可选 缺省情况下，未指定源IP地址 如果没有指定源IP地址，但是配置了**source interface**，则该源接口的IP地址将作为探测报文中的源IP地址 该命令指定的源IP地址必须是设备上接口的IP地址，且接口为up状态，否则探测将会失败
配置探测报文的下一跳IP地址	**next-hop** *ip-address*	可选 缺省情况下，未配置下一跳IP地址
配置通用的可选参数	参见表1-22	可选

说明

ICMP-echo 测试不支持在 IPv6 网络中使用，如果要测试 IPv6 网络中目的主机的可达性，可以使用 **ping ipv6** 命令。**ping ipv6** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“系统维护与调试”。

1.6.2 配置DHCP测试

DHCP 测试主要用来测试网络上是否有 DHCP 服务器，以及 DHCP 服务器响应客户端请求、为客户端分配 IP 地址所需的时间。

1. 配置准备

在进行 DHCP 测试之前，需要完成 DHCP 服务器的配置。如果 NQA 客户端（即 DHCP 客户端）和 DHCP 服务器在不同的网段，还需要配置 DHCP 中继。DHCP 服务器和 DHCP 中继的配置方法，请参见“三层技术-IP 业务配置指导”中的“DHCP 服务器”和“DHCP 中继”。

2. 配置DHCP测试

表1-8 配置 DHCP 测试

操作	命令	说明
进入系统视图	**system-view**	-
进入NQA测试组视图	**nqa entry** *admin-name operation-tag*	-
配置测试类型为DHCP，并进入测试类型视图	**type dhcp**	必选

操作	命令	说明
指定进行DHCP测试的接口	**operation interface** *interface-type interface-number*	必选 缺省情况下，没有指定进行DHCP测试的接口 该命令指定的接口必须为up状态，否则会导致测试失败
配置通用的可选参数	参见表1-22	可选

说明

- DHCP 测试只是模拟 DHCP 申请地址的过程，进行 DHCP 测试的接口 IP 地址不会改变。
- DHCP 测试完成后，NQA 客户端将主动发送 DHCP-RELEASE 报文释放申请到的 IP 地址。

1.6.3 配置DNS测试

DNS 测试主要用来测试 NQA 客户端是否可以通过指定的 DNS 服务器将域名解析为 IP 地址，以及域名解析过程需要的时间。

1. 配置准备

在进行 DNS 测试之前，需要在 DNS 服务器上创建域名和 IP 地址的映射关系。

2. 配置DNS测试

表1-9 配置 DNS 测试

操作	命令	说明
进入系统视图	**system-view**	-
进入NQA测试组视图	**nqa entry** *admin-name operation-tag*	-
配置测试类型为DNS，并进入测试类型视图	**type dns**	必选
将DNS服务器的IP地址配置为测试操作的目的地址	**destination ip** *ip-address*	必选 缺省情况下，未配置测试操作的目的IP地址
配置要解析的域名	**resolve-target** *domain-name*	必选 缺省情况下，没有配置要解析的域名
配置通用的可选参数	参见表1-22	可选

说明

DNS 测试只是模拟域名解析的过程，设备上不会保存要解析的域名与 IP 地址的对应关系。

1.6.4 配置FTP测试

FTP 测试主要用来测试 NQA 客户端是否可以与指定的 FTP 服务器建立连接，以及与 FTP 服务器之间传送文件的时间。

1. 配置准备

在进行 FTP 测试之前，需要在 FTP 服务器上进行相应的配置，包括 FTP 客户端登录 FTP 服务器的用户名、密码等。FTP 服务器的配置方法，请参见“基础配置指导”中的“FTP”。

2. 配置FTP测试

表1-10 配置 FTP 测试

操作	命令	说明
进入系统视图	**system-view**	-
进入NQA测试组视图	**nqa entry** *admin-name operation-tag*	-
配置测试类型为FTP，并进入测试类型视图	**type ftp**	必选
将FTP服务器的IP地址配置为测试操作的目的地址	**destination ip** *ip-address*	必选 缺省情况下，未配置测试操作的目的IP地址
配置探测报文的源IP地址	**source ip** *ip-address*	必选 缺省情况下，未指定源IP地址 该命令指定的源IP地址必须是设备上接口的IP地址，且接口为up状态，否则测试将会失败
配置FTP测试的操作类型	**operation** { **get** | **put** }	可选 缺省情况下，FTP操作方式为**get**操作，即从FTP服务器获取文件
配置FTP登录用户名	**username** *name*	必选 缺省情况下，未配置FTP登录用户名
配置FTP登录密码	**password** [**cipher** | **simple**] *password*	必选 缺省情况下，未配置FTP登录密码
配置FTP服务器和客户端传送文件的文件名	**filename** *file-name*	必选 缺省情况下，未配置FTP服务器和客户端之间传送文件的文件名
配置FTP测试的数据传输方式	**mode** { **active** | **passive** }	可选 缺省情况下，FTP测试的数据传输方式为主动方式
配置通用的可选参数	参见表1-22	可选

说明

- 进行 **put** 操作时，NQA 客户端将在 FTP 服务器会创建以 *file-name* 为文件名的固定大小的测试文件，此文件与 NQA 客户端存储设备中保存的文件无关；进行 **get** 操作时，设备上不会保存从服务器获取的文件。
- 进行 **get** 操作时，如果 FTP 服务器上没有以 *file-name* 为名字的文件，则测试不会成功。
- 进行 FTP 测试时，建议选用较小的测试文件并将 NQA 探测超时时间调大，如果测试文件太大或探测超时时间太小，可能会导致探测超时。

1.6.5 配置HTTP测试

HTTP 测试主要用来测试 NQA 客户端是否可以与指定的 HTTP 服务器建立连接，以及从 HTTP 服务器获取数据所需的时间，从而判断 HTTP 服务器的连通性及性能。

1. 配置准备

在进行 HTTP 测试之前，需要完成 HTTP 服务器的配置。

2. 配置HTTP测试

表1-11 配置 HTTP 测试

操作	命令	说明
进入系统视图	**system-view**	-
进入NQA测试组视图	**nqa entry** *admin-name operation-tag*	-
配置测试类型为HTTP，并进入测试类型视图	**type http**	必选
将HTTP服务器的IP地址配置为测试操作的目的地址	**destination ip** *ip-address*	必选 缺省情况下，未配置测试操作的目的IP地址
配置探测报文的源IP地址	**source ip** *ip-address*	可选 缺省情况下，未指定源IP地址 该命令指定的源IP地址必须是设备上接口的IP地址，且接口为up状态，否则测试将会失败
配置HTTP测试的操作类型	**operation { get | post }**	可选 缺省情况下，HTTP操作方式为**get**操作，即从HTTP服务器获取数据
配置HTTP测试访问的网址	**url** *url*	必选
配置HTTP测试所使用的协议版本	**http-version v1.0**	可选 缺省情况下，HTTP测试使用的版本为1.0
配置通用的可选参数	参见表1-22	可选

说明

HTTP 测试中，HTTP 服务器的 TCP 端口号只能为 80。如果 HTTP 服务器采用其他 TCP 端口，测试将会失败。

1.6.6 配置UDP-jitter测试

说明

建议不要对知名端口，即 1～1023 之间的端口，进行 UDP-jitter 测试，否则可能导致 NQA 测试失败或该知名端口对应的服务不可用。

语音、视频等实时性业务对 Delay jitter（时延抖动）的要求较高。通过 UDP-jitter 测试，可以获得网络的单向和双向时延抖动，从而判断网络是否可以承载实时性业务。

UDP-jitter 测试的过程如下：

(1) 源端以一定的时间间隔向目的端发送探测报文。

(2) 目的端收到探测报文后，为它打上时间戳，并把带有时间戳的报文发送给源端。

(3) 源端收到报文后，根据报文上的时间戳，计算出时延抖动，从而清晰地反映出网络状况。时延抖动的计算方法为相邻两个报文的接收时间间隔减去这两个报文的发送时间间隔。

1. 配置准备

UDP-jitter测试需要NQA服务器和客户端配合才能完成。进行UDP-jitter测试之前，必须保证NQA服务器端配置了UDP监听功能，配置方法请参见“1.3 配置NQA服务器”。

2. 配置UDP-jitter测试

表1-12 配置 UDP-jitter 测试

操作	命令	说明
进入系统视图	**system-view**	-
进入NQA测试组视图	**nqa entry** *admin-name operation-tag*	-
配置测试类型为UDP-jitter，并进入测试类型视图	**type udp-jitter**	必选
配置测试操作的目的地址	**destination ip** *ip-address*	必选 缺省情况下，未配置测试操作的目的IP地址 测试操作的目的地址必须与NQA服务器上所配置的监听服务的IP地址一致
配置测试操作的目的端口	**destination port** *port-number*	必选 缺省情况下，未配置测试操作的目的端口号 测试操作的目的端口号必须与NQA服务器上所配置的监听服务的端口号一致
配置探测报文的源端口号	**source port** *port-number*	可选 缺省情况下，未指定源端口号

操作	命令	说明
配置发送的探测报文的大小	**data-size** *size*	可选 缺省情况下，发送的探测报文为100字节
配置发送的探测报文的填充字符串	**data-fill** *string*	可选 缺省情况下，探测报文的填充内容为十六进制数值00010203040506070809
配置一次UDP-jitter探测中发送探测报文的个数	**probe packet-number** *packet-number*	可选 缺省情况下，一次UDP-jitter探测中发送10个探测报文
配置UDP-jitter测试中发送探测报文的时间间隔	**probe packet-interval** *packet-interval*	可选 缺省情况下，UDP-jitter测试中发送探测报文的时间间隔为20毫秒
配置UDP-jitter测试中等待响应报文的超时时间	**probe packet-timeout** *packet-timeout*	可选 缺省情况下，UDP-jitter测试中等待响应报文的超时时间为3000毫秒
配置探测报文的源IP地址	**source ip** *ip-address*	可选 缺省情况下，未指定源IP地址 该命令指定的源IP地址必须是设备上接口的IP地址，且接口为up状态，否则测试将会失败
配置通用的可选参数	参见表1-22	可选

说明

一次 UDP-jitter 测试中探测的次数取决于 **probe count** 命令的配置，而每次探测所发送的探测包的个数由 **probe packet-number** 命令配置决定。

1.6.7 配置SNMP测试

SNMP 查询测试主要用来测试从 NQA 客户端向 SNMP agent 设备发出一个 SNMP 协议查询报文到接收响应报文的时间。

1. 配置准备

在进行 SNMP 测试之前，需要在作为 SNMP agent 的设备上启动 SNMP agent 功能。SNMP agent 的配置方法，请参见“网络管理和监控配置指导”中的“SNMP”。

2. 配置SNMP测试

表1-13 配置 SNMP 测试

操作	命令	说明
进入系统视图	**system-view**	-
进入NQA测试组视图	**nqa entry** *admin-name operation-tag*	-
配置测试类型为SNMP，并进入测试类型视图	**type snmp**	必选

操作	命令	说明
配置测试操作的目的地址	**destination ip** *ip-address*	必选 缺省情况下，未配置测试操作的目的IP地址
配置探测报文的源端口号	**source port** *port-number*	可选 缺省情况下，未指定源端口号
配置探测报文的源IP地址	**source ip** *ip-address*	可选 缺省情况下，未指定源IP地址 该命令指定的源IP地址必须是设备上接口的IP地址，且接口为up状态，否则测试将会失败
配置通用的可选参数	参见表1-22	可选

1.6.8 配置TCP测试

TCP 测试用来测试客户端和服务器指定端口之间是否能够建立 TCP 连接，以及建立 TCP 连接所需的时间，从而判断服务器指定端口上提供的服务是否可用，及服务性能。

1. 配置准备

TCP测试需要NQA服务器和客户端配合才能完成。在TCP测试之前，需要在NQA服务器端配置TCP监听功能，配置方法请参见“1.3 配置NQA服务器”。

2. 配置TCP测试

表1-14 配置 TCP 测试

操作	命令	说明
进入系统视图	**system-view**	-
进入NQA测试组视图	**nqa entry** *admin-name operation-tag*	-
配置测试类型为TCP，并进入测试类型视图	**type tcp**	必选
配置测试操作的目的地址	**destination ip** *ip-address*	必选 缺省情况下，未配置测试操作的目的IP地址 必须与NQA服务器上配置的监听服务的IP地址一致
配置测试操作的目的端口	**destination port** *port-number*	必选 缺省情况下，未配置测试操作的目的端口号 必须与NQA服务器上配置的监听服务的端口号一致
配置探测报文的源IP地址	**source ip** *ip-address*	可选 缺省情况下，未指定源IP地址 该命令指定的源IP地址必须是设备上接口的IP地址，且接口为up状态，否则测试将会失败
配置通用的可选参数	参见表1-22	可选

1.6.9 配置UDP-echo测试

UDP-echo 测试可以用来测试客户端和服务器指定 UDP 端口之间的连通性以及 UDP 报文的往返时间。

1. 配置准备

UDP-echo测试需要NQA服务器和客户端配合才能完成。在进行UDP-echo测试之前，需要在NQA服务器端配置UDP监听功能，配置方法请参见“1.3 配置NQA服务器”。

2. 配置UDP-echo测试

表1-15 配置 UDP-echo 测试

操作	命令	说明
进入系统视图	**system-view**	-
进入NQA测试组视图	**nqa entry** *admin-name operation-tag*	-
配置测试类型为UDP-echo，并进入测试类型视图	**type udp-echo**	必选
配置测试操作的目的地址	**destination ip** *ip-address*	必选 缺省情况下，未配置测试操作的目的IP地址 必须与NQA服务器上配置的监听服务的IP地址一致
配置测试操作的目的端口	**destination port** *port-number*	必选 缺省情况下，未配置测试操作的目的端口号 必须与NQA服务器上配置的监听服务的端口号一致
配置发送的探测报文的大小	**data-size** *size*	可选 缺省情况下，UDP-echo测试中发送的探测报文为100字节
配置发送的探测报文的填充字符串	**data-fill** *string*	可选 缺省情况下，探测报文的填充内容为十六进制数值00010203040506070809
配置探测报文的源端口号	**source port** *port-number*	可选 缺省情况下，未指定源端口号
配置探测报文的源IP地址	**source ip** *ip-address*	可选 缺省情况下，未指定源IP地址 该命令指定的源IP地址必须是设备上接口的IP地址，且接口为up状态，否则测试将会失败
配置通用的可选参数	参见表1-22	可选

1.6.10 配置Voice测试

说明

建议不要对知名端口，即 1～1023 之间的端口，进行 Voice 测试，否则可能导致 NQA 测试失败或该知名端口对应的服务不可用。

Voice 测试主要用来测试 VoIP（Voice over IP，在 IP 网络上传送语音）网络情况，统计 VoIP 网络参数，以便用户根据网络情况进行相应的调整。

Voice 测试的过程如下：

(1) 源端（NQA 客户端）以一定的时间间隔向目的端（NQA 服务器）发送 G.711 A 律、G.711 μ 律或 G.729 A 律编码格式的语音数据包。

(2) 目的端收到语音数据包后，为它打上时间戳，并把带有时间戳的数据包发送给源端。

(3) 源端收到数据包后，根据数据包上的时间戳等信息，计算出时延抖动、单向延迟等网络参数，从而清晰地反映出网络状况。

Voice 测试还可以计算出反映 VoIP 网络状况的语音参数值，包括：

- ICPIF（Calculated Planning Impairment Factor，计算计划损伤元素）：用来量化网络中语音数据的衰减，由单向网络延迟和丢包率等决定。数值越大，表明语音网络质量越差。
- MOS（Mean Opinion Scores，平均意见得分）：语音网络的质量得分。MOS 值的范围为 1～5，该值越高，表明语音网络质量越好。通过计算网络中语音数据的衰减——ICPIF 值，可以估算出 MOS 值。

对语音质量的评价具有一定的主观性，不同用户对语音质量的容忍程度不同，因此，衡量语音质量时，需要考虑用户的主观因素。对语音质量容忍程度较强的用户，可以通过 **advantage-factor** 命令配置补偿因子，在计算 ICPIF 值时将减去该补偿因子，修正 ICPIF 和 MOS 值，以便在比较语音质量时综合考虑客观和主观因素。

1. 配置准备

Voice测试需要NQA服务器和客户端配合才能完成。进行Voice测试之前，必须保证NQA服务器端配置了UDP监听功能，配置方法请参见“1.3 配置NQA服务器”。

2. 配置Voice测试

表1-16 配置 Voice 测试

操作	命令	说明
进入系统视图	**system-view**	-
进入NQA测试组视图	**nqa entry** *admin-name operation-tag*	-
配置测试类型为Voice，并进入测试类型视图	**type voice**	必选
配置测试操作的目的地址	**destination ip** *ip-address*	必选 缺省情况下，未配置测试操作的目的IP地址 测试操作的目的地址必须与NQA服务器上所配置的监听服务的IP地址一致

操作	命令	说明
配置测试操作的目的端口	**destination port** *port-number*	必选 缺省情况下，未配置测试操作的目的端口号 测试操作的目的端口号必须与NQA服务器上所配置的监听服务的端口号一致
配置Voice测试的编码格式	**codec-type** { **g711a** | **g711u** | **g729a** }	可选 缺省情况下，语音编码格式为G.711 A律
配置用于计算MOS值和ICPIF值的补偿因子	**advantage-factor** *factor*	可选 缺省情况下，补偿因子取值为0
配置探测报文的源IP地址	**source ip** *ip-address*	可选 缺省情况下，未指定源IP地址 该命令指定的源IP地址必须是设备上接口的IP地址，且接口为up状态，否则测试将会失败
配置探测报文的源端口号	**source port** *port-number*	可选 缺省情况下，未指定源端口号
配置发送的探测报文的大小	**data-size** *size*	可选 缺省情况下，发送的探测报文大小与配置的编码格式有关，编码格式为**g.711a**和**g.711u**时缺省报文大小为172字节，**g.729a**时为32字节
配置发送的探测报文的填充字符串	**data-fill** *string*	可选 缺省情况下，探测报文的填充内容为十六进制数值00010203040506070809
配置一次Voice探测中发送探测报文的个数	**probe packet-number** *packet-number*	可选 缺省情况下，一次Voice探测中发送1000个探测报文
配置Voice探测中发送探测报文的时间间隔	**probe packet-interval** *packet-interval*	可选 缺省情况下，Voice探测中发送探测报文的时间间隔为20毫秒
配置Voice测试中等待响应报文的超时时间	**probe packet-timeout** *packet-timeout*	可选 缺省情况下，Voice测试中等待响应报文的超时时间为5000毫秒
配置通用的可选参数	参见表1-22	可选

说明

一次 Voice 测试只能进行一次探测，而每次探测所发送的探测报文的个数由 **probe packet-number** 命令配置决定。

1.6.11 配置DLSw测试

DLSw 测试主要用来测试 DLSw 设备的响应时间。

1. 配置准备

在进行 DLSw 测试之前，需要在对端设备上使能 DLSw 功能。

2. 配置DLSw测试

表1-17 配置 DLSw 测试

操作	命令	说明
进入系统视图	**system-view**	-
进入NQA测试组视图	**nqa entry** *admin-name operation-tag*	-
配置测试类型为DLSw，并进入测试类型视图	**type dlsw**	必选
配置测试操作的目的地址	**destination ip** *ip-address*	必选 缺省情况下，未配置测试操作的目的IP地址
配置探测报文的源IP地址	**source ip** *ip-address*	可选 缺省情况下，未指定源IP地址 该命令指定的源IP地址必须是设备上接口的IP地址，且接口为up状态，否则测试将会失败
配置通用的可选参数	参见表1-22	可选

1.7 配置联动功能

联动功能是通过建立联动项，对当前所在测试组中的探测进行监测，当连续探测失败次数达到阈值时，就触发配置的动作类型。

表1-18 配置联动功能

操作	命令	说明
进入系统视图	**system-view**	-
进入NQA测试组视图	**nqa entry** *admin-name operation-tag*	-
进入测试组测试类型视图	**type** { **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** }	- UDP-jitter和Voice测试不支持联动功能
建立联动项	**reaction** *item-number* **checked-element probe-fail threshold-type consecutive** *consecutive-occurrences* **action-type trigger-only**	必选 缺省情况下，未配置联动项
退回系统视图	**quit**	-
创建与NQA测试组中指定联动项关联的Track项	**track** *entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-number*	必选 缺省情况下，未配置Track项

说明

- 联动项创建后，不能再通过 **reaction** 命令修改该联动项的内容。
- UDP-jitter 和 Voice 测试不支持联动功能。

1.8 配置阈值告警功能

1. 配置准备

在配置阈值告警功能之前，需要执行以下操作：

- 通过 **snmp-agent target-host** 命令配置 Trap 消息的目的地址。**snmp-agent target-host** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“SNMP”。
- 正确创建 NQA 测试组并配置相关参数。

2. 配置阈值告警功能

表1-19 配置阈值告警功能

操作	命令	说明
进入系统视图	**system-view**	-
进入NQA测试组视图	**nqa entry** *admin-name operation-tag*	-
进入测试组测试类型视图	**type** { **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** | **voice** }	-
配置在指定条件下向网管服务器发送Trap消息	**reaction trap** { **probe-failure** *consecutive-probe-failures* | **test-complete** | **test-failure** *cumulate-probe-failures* }	根据实际需要，选择配置发送Trap消息的方法 缺省情况下，不向网管服务器发送Trap消息
创建监测探测持续时间的阈值告警组（除UDP-jitter和Voice测试外，均支持）	**reaction** *item-number* **checked-element probe-duration threshold-type** { **accumulate** *accumulate-occurrences* | **average** | **consecutive** *consecutive-occurrences* } **threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]	
创建监测探测失败次数的阈值告警组（除UDP-jitter和Voice测试外，均支持）	**reaction** *item-number* **checked-element probe-fail threshold-type** { **accumulate** *accumulate-occurrences* | **consecutive** *consecutive-occurrences* } [**action-type** { **none** | **trap-only** }]	
创建监测报文往返时延的阈值告警组（仅UDP-jitter和Voice测试支持）	**reaction** *item-number* **checked-element rtt threshold-type** { **accumulate** *accumulate-occurrences* | **average** } **threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]	
创建监测每次测试中丢包数的阈值告警组（仅UDP-jitter和Voice测试支持）	**reaction** *item-number* **checked-element packet-loss threshold-type accumulate** *accumulate-occurrences* [**action-type** { **none** | **trap-only** }]	
创建监测单向时延抖动的阈值告警组（仅UDP-jitter和Voice测试支持）	**reaction** *item-number* **checked-element** { **jitter-ds** | **jitter-sd** } **threshold-type** { **accumulate** *accumulate-occurrences* | **average** } **threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]	

操作	命令	说明
创建监测单向时延的阈值告警组（仅UDP-jitter和Voice测试支持）	**reaction** *item-number* **checked-element** { **owd-ds** | **owd-sd** } **threshold-value** *upper-value lower-value*	
创建监测Voice测试ICPIF值的阈值告警组（仅Voice测试支持）	**reaction** *item-number* **checked-element icpif threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]	
创建监测Voice测试MOS值的阈值告警组（仅Voice测试支持）	**reaction** *item-number* **checked-element mos threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]	

说明

- DNS 测试不支持发送 Trap 消息，即对于 DNS 测试，触发动作只能配置为 **none**。
- 在 Voice 测试类型视图下执行 **reaction trap** 命令时，只支持 **reaction trap test-complete**。

1.9 配置NQA统计功能

NQA 将在指定时间间隔内完成的 NQA 测试归为一组，计算该组测试结果的统计值，这些统计值构成一个统计组。通过 **display nqa statistics** 命令可以显示该统计组的信息。通过 **statistics interval** 命令可以设置统计的时间间隔。

当保留的统计组数目达到最大值时，如果形成新的统计组，保存时间最久的统计组将被删除。通过 **statistics max-group** 命令可以设置保留的最大统计组个数。

指定时间间隔内最后一次测试结束后，形成一个统计组。统计组具有老化功能，即统计组保存一定时间后，将被删除。通过 **statistics hold-time** 命令可以设置统计组的保留时间。

表1-20 配置 NQA 统计功能

操作	命令	说明
进入系统视图	**system-view**	-
进入NQA测试组视图	**nqa entry** *admin-name operation-tag*	-
进入测试组测试类型视图	**type** { **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** | **voice** }	-
配置对测试结果进行统计的时间间隔	**statistics interval** *interval*	可选 缺省情况下，对测试结果进行统计的时间间隔为60分钟
配置能够保留的最大统计组个数	**statistics max-group** *number*	可选 缺省情况下，能够保留的最大统计组数为2 最大统计组个数为0时，不进行统计
配置统计组的保留时间	**statistics hold-time** *hold-time*	可选 缺省情况下，统计组的保留时间为120分钟

说明

- DHCP 测试不支持配置 NQA 统计功能。
- 如果通过 **frequency** 命令指定连续两次测试开始时间的时间间隔为 0，则不生成统计组信息。

1.10 配置NQA历史记录功能

开启 NQA 测试组的历史记录保存功能后，系统将记录 NQA 测试的历史信息，通过 **display nqa history** 命令可以查看该测试组的历史记录信息。

通过本配置任务还可以指定：

- 历史记录的保存时间：历史记录保存时间达到配置的值后，将删除该历史记录。
- 一个测试组中能够保存的最大历史记录个数：如果历史记录个数超过设定的最大数目，则最早的历史记录将会被删除。

表1-21 配置 NQA 历史记录功能

操作	命令	说明
进入系统视图	**system-view**	-
进入NQA测试组视图	**nqa entry** *admin-name operation-tag*	-
进入测试组测试类型视图	**type** { **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** | **voice** }	-
开启NQA测试组的历史记录保存功能	**history-record enable**	必选 缺省情况下，NQA测试组的历史记录保存功能处于关闭状态
配置NQA测试组中历史记录的保存时间	**history-record keep-time** *keep-time*	可选 缺省情况下，NQA测试组中历史记录的保存时间为120分钟
配置在一个测试组中能够保存的最大历史记录个数	**history-record number** *number*	可选 缺省情况下，一个测试组中能够保存的最大历史记录个数为50

1.11 配置NQA测试组通用可选参数

NQA 测试组的通用可选参数，只对该测试组中的测试有效。

除特别说明外，所有测试类型都可以配置通用可选参数，可以根据实际情况选择配置测试组的参数。

表1-22 配置 NQA 测试组的通用可选参数

操作	命令	说明
进入系统视图	**system-view**	-
进入NQA测试组视图	**nqa entry** *admin-name operation-tag*	-
进入测试组测试类型视图	**type** { **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** | **voice** }	-

操作	命令	说明
配置测试组的描述字符串	**description** *text*	可选 缺省情况下，测试组没有描述字符串
配置测试组连续两次测试开始时间的时间间隔	**frequency** *interval*	可选 缺省情况下，测试组连续两次测试开始时间的时间间隔为0毫秒，即只进行一次测试 如果到达**frequency**指定的时间间隔时，上次测试尚未完成，则不启动新一轮测试
配置一次NQA测试中进行探测的次数	**probe count** *times*	可选 缺省情况下，一次测试中的探测次数为1次 Voice测试中探测次数只能为1，不支持该命令
配置NQA探测超时时间	**probe timeout** *timeout*	可选 缺省情况下，探测的超时时间为3000毫秒 UDP-jitter测试不能配置该参数
配置探测报文在网络中可以经过的最大跳数	**ttl** *value*	可选 缺省情况下，探测报文在网络中可以经过的最大跳数为20跳 DHCP测试不能配置该参数
配置NQA探测报文IP报文头中服务类型域的值	**tos** *value*	可选 缺省情况下，NQA探测报文IP报文头中服务类型域的值为0
启动路由表旁路功能	**route-option bypass-route**	可选 缺省情况下，路由表旁路功能处于关闭状态 DHCP测试不能配置该参数

1.12 调度NQA测试组

通过本配置，可以设置测试组进行测试的启动时间和持续时间。启动时间取值可以是具体的时间值和 **now**，**now** 表示立即启动测试；持续时间取值可以是具体的时间值和 **forever**，**forever** 表示一直进行测试，直到用户通过 **undo nqa schedule** 命令手动停止测试。

系统时间在<启动时间>到<启动时间＋持续时间>范围内时，测试组进行测试。执行 **nqa schedule** 命令时，如果系统时间尚未到达启动时间，则到达启动时间后，启动测试；如果系统时间在启动时间～启动时间＋持续时间之间，则立即启动测试；如果系统时间已经超过启动时间＋持续时间，则不会启动测试。通过 **display clock** 命令可以查看系统的当前时间。

1. 配置准备

在调度 NQA 测试组之前，需要保证：

- 测试类型相应的测试参数配置完整；
- 对于需要与 NQA 服务器配合的测试类型，已经完成 NQA 服务器端的配置。

2. 调度NQA测试组

表1-23 调度 NQA 测试组

操作	命令	说明
进入系统视图	**system-view**	-
调度NQA测试组	**nqa schedule** *admin-name operation-tag* **start-time** { *hh:mm:ss* [*yyyy/mm/dd*] | **now** } **lifetime** { *lifetime* | **forever** }	必选
配置处于测试状态的NQA测试的最大个数	**nqa agent max-concurrent** *number*	可选 缺省情况下，设备允许配置处于测试状态的NQA测试的最大个数为2

注意

- 测试组被调度后就不能再进入该测试组视图和测试类型视图。
- 对于已启动的测试组或已经完成测试的测试组，不受系统时间调整的影响，只有等待测试的测试组受系统时间调整的影响。

1.13 NQA显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 NQA 的运行情况，通过查看显示信息验证配置的效果。

表1-24 NQA 显示和维护

操作	命令
显示NQA测试组的历史记录	**display nqa history** [*admin-name operation-tag*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示NQA阈值告警功能的当前监测结果	**display nqa reaction counters** [*admin-name operation-tag* [*item-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示最近一次NQA测试的结果	**display nqa result** [*admin-name operation-tag*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示NQA测试的统计信息	**display nqa statistics** [*admin-name operation-tag*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示服务器的状态信息	**display nqa server status** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.14 NQA典型配置举例

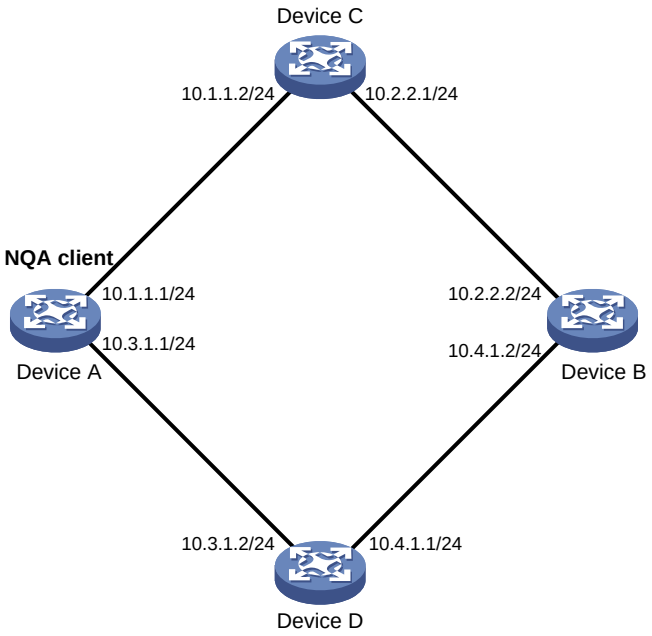
1.14.1 ICMP-echo测试配置举例

1. 组网需求

使用 NQA 的 ICMP-echo 测试功能，测试本端（Device A）发送的报文是否可以经过指定的下一跳设备（Device C）到达指定的目的端（Device B），以及报文的往返时间。

2. 组网图

图1-3 ICMP-echo 测试组网图



3. 配置步骤

说明

进行下面的配置之前，需要确保各设备之间路由可达。

创建 ICMP-echo 类型的 NQA 测试组，并配置测试操作的目的地址为 10.2.2.2。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type icmp-echo
[DeviceA-nqa-admin-test-icmp-echo] destination ip 10.2.2.2
```

配置下一跳地址为 10.1.1.2，以便测试报文经过指定的下一跳设备（Device C）到达目的端，而不是通过 Device D 到达目的端。

```
[DeviceA-nqa-admin-test-icmp-echo] next-hop 10.1.1.2
```

配置可选参数：一次 NQA 测试中探测的次数为 10，探测的超时时间为 500 毫秒，测试组连续两次测试开始时间的时间间隔为 5000 毫秒。

```
[DeviceA-nqa-admin-test-icmp-echo] probe count 10
[DeviceA-nqa-admin-test-icmp-echo] probe timeout 500
[DeviceA-nqa-admin-test-icmp-echo] frequency 5000
```

开启 NQA 历史记录保存功能，并配置一个测试组中能够保存的最大历史记录个数为 10。

```
[DeviceA-nqa-admin-test-icmp-echo] history-record enable
[DeviceA-nqa-admin-test-icmp-echo] history-record number 10
[DeviceA-nqa-admin-test-icmp-echo] quit
```

启动 ICMP-echo 测试操作。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

测试执行一段时间后，停止 ICMP-echo 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

显示 ICMP-echo 测试中最后一次测试的结果。

```
[DeviceA] display nqa result admin test
```

```
  NQA entry (admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 10              Receive response times: 10
      Min/Max/Average round trip time: 2/5/3
      Square-Sum of round trip time: 96
      Last succeeded probe time: 2011-08-23 15:00:01.2
    Extended results:
      Packet loss in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
```

显示 ICMP-echo 测试的历史记录。

```
[DeviceA] display nqa history admin test
  NQA entry (admin admin, tag test) history record(s):
    Index      Response     Status           Time
    370        3            Succeeded        2011-08-23 15:00:01.2
    369        3            Succeeded        2011-08-23 15:00:01.2
    368        3            Succeeded        2011-08-23 15:00:01.2
    367        5            Succeeded        2011-08-23 15:00:01.2
    366        3            Succeeded        2011-08-23 15:00:01.2
    365        3            Succeeded        2011-08-23 15:00:01.2
    364        3            Succeeded        2011-08-23 15:00:01.1
    363        2            Succeeded        2011-08-23 15:00:01.1
    362        3            Succeeded        2011-08-23 15:00:01.1
    361        2            Succeeded        2011-08-23 15:00:01.1
```

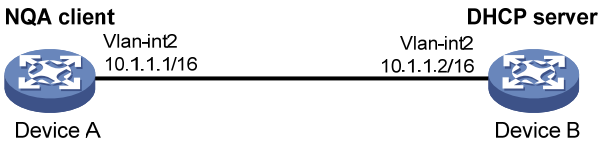
1.14.2 DHCP测试配置举例

1. 组网需求

使用 NQA 的 DHCP 测试功能，测试 Device A 从 DHCP 服务器 Device B 申请到 IP 地址所需的时间。

2. 组网图

图1-4 配置 DHCP 组网图



3. 配置步骤

创建 DHCP 类型的 NQA 测试组，并指定进行 DHCP 测试的接口为 VLAN 接口 2。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type dhcp
[DeviceA-nqa-admin-test-dhcp] operation interface vlan-interface 2
```

开启 NQA 测试组的历史记录保存功能。

```
[DeviceA-nqa-admin-test-dhcp] history-record enable
```

```
[DeviceA-nqa-admin-test-dhcp] quit
```

启动 DHCP 测试操作。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

测试执行一段时间后，停止 DHCP 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

显示 DHCP 测试中最后一次测试的结果。

```
[DeviceA] display nqa result admin test
  NQA entry (admin admin, tag test) test results:
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 624/624/624
      Square-Sum of round trip time: 389376
      Last succeeded probe time: 2011-01-22 09:56:03.2
    Extended results:
      Packet loss in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
```

显示 DHCP 测试的历史记录。

```
[DeviceA] display nqa history admin test
  NQA entry (admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          624          Succeeded        2011-01-22 09:56:03.2
```

1.14.3 DNS测试配置举例

1. 组网需求

使用 NQA 的 DNS 测试功能，测试 Device A 是否可以通过指定的 DNS 服务器将域名 host.com 解析为 IP 地址，并测试域名解析所需的时间。

2. 组网图

图1-5 配置 DNS 组网图

3. 配置步骤

说明

进行下面的配置之前，需要确保各设备之间路由可达。

创建 DNS 类型的 NQA 测试组。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type dns
```

配置测试操作的目的地址为 DNS 服务器的 IP 地址 10.2.2.2，要解析的域名为 host.com。

```
[DeviceA-nqa-admin-test-dns] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-dns] resolve-target host.com
```

开启 NQA 测试组的历史记录保存功能。

```
[DeviceA-nqa-admin-test-dns] history-record enable
[DeviceA-nqa-admin-test-dns] quit
```

启动 DNS 测试操作。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

测试执行一段时间后，停止 DNS 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

显示 DNS 测试中最后一次测试的结果。

```
[DeviceA] display nqa result admin test
  NQA entry (admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 62/62/62
      Square-Sum of round trip time: 3844
      Last succeeded probe time: 2011-01-23 10:49:37.3
    Extended results:
      Packet loss in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
```

显示 DNS 测试的历史记录。

```
[DeviceA] display nqa history admin test
  NQA entry (admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          62           Succeeded        2011-01-23 10:49:37.3
```

1.14.4 FTP测试配置举例

1. 组网需求

使用 NQA 的 FTP 测试功能，测试 Device A 是否可以和指定的 FTP 服务器 Device B 建立连接，以及往 FTP 服务器上传一个文件的时间。登录 FTP 服务器的用户名为 admin，密码为 systemtest，要传送到服务器的文件名为 config.txt。

2. 组网图

图1-6 配置 FTP 组网图

3. 配置步骤

说明

进行下面的配置之前，需要确保各设备之间路由可达。

创建 FTP 类型的 NQA 测试组。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type ftp
```

配置测试操作的目的地址为 FTP 服务器的 IP 地址 10.2.2.2。

```
[DeviceA-nqa-admin-test-ftp] destination ip 10.2.2.2
```

配置探测报文的源 IP 地址为 10.1.1.1。

```
[DeviceA-nqa-admin-test-ftp] source ip 10.1.1.1
```

配置登录 FTP 服务器的用户名为 admin，密码为 systemtest。

```
[DeviceA-nqa-admin-test-ftp] username admin
[DeviceA-nqa-admin-test-ftp] password systemtest
```

配置测试执行的操作为向 FTP 服务器上传文件 config.txt。

```
[DeviceA-nqa-admin-test-ftp] operation put
[DeviceA-nqa-admin-test-ftp] filename config.txt
```

开启 NQA 测试组的历史记录保存功能。

```
[DeviceA-nqa-admin-test-ftp] history-record enable
[DeviceA-nqa-admin-test-ftp] quit
```

启动 FTP 测试操作。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

测试执行一段时间后，停止 FTP 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

显示 FTP 测试中最后一次测试的结果。

```
[DeviceA] display nqa result admin test
  NQA entry (admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 173/173/173
      Square-Sum of round trip time: 29929
      Last succeeded probe time: 2011-01-22 10:07:28.6
    Extended results:
      Packet loss in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
```

显示 FTP 测试的历史记录。

```
[DeviceA] display nqa history admin test
  NQA entry (admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          173          Succeeded        2011-01-22 10:07:28.6
```

1.14.5 HTTP测试配置举例

1. 组网需求

使用 NQA 的 HTTP 测试功能，测试是否可以和指定的 HTTP 服务器之间建立连接，以及从 HTTP 服务器获取数据的时间。

2. 组网图

图1-7 HTTP 测试组网图

3. 配置步骤

说明

进行下面的配置之前，需要确保各设备之间路由可达。

创建 HTTP 类型的 NQA 测试组。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type http
```

配置测试操作的目的地址为 HTTP 服务器的 IP 地址 10.2.2.2。

```
[DeviceA-nqa-admin-test-http] destination ip 10.2.2.2
```

配置 HTTP 测试的操作方式为 get 操作。（get 操作为缺省操作方式，因此，可以不执行本配置）

```
[DeviceA-nqa-admin-test-http] operation get
```

配置 HTTP 测试访问的网址为/index.htm。

```
[DeviceA-nqa-admin-test-http] url /index.htm
```

配置 HTTP 测试使用的版本为 1.0。（缺省情况下使用的版本为 1.0，因此，可以不执行本配置）

```
[DeviceA-nqa-admin-test-http] http-version v1.0
```

开启 NQA 测试组的历史记录保存功能。

```
[DeviceA-nqa-admin-test-http] history-record enable
[DeviceA-nqa-admin-test-http] quit
```

启动 HTTP 测试操作。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

测试执行一段时间后，停止 HTTP 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

显示 HTTP 测试中最后一次测试的结果。

```
[DeviceA] display nqa result admin test
  NQA entry (admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 64/64/64
      Square-Sum of round trip time: 4096
      Last succeeded probe time: 2011-01-22 10:12:47.9
    Extended results:
      Packet loss in test: 0%
      Failures due to timeout: 0
```

```
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
```

显示 HTTP 测试的历史记录。

```
[DeviceA] display nqa history admin test
  NQA entry (admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          64           Succeeded        2011-01-22 10:12:47.9
```

1.14.6 UDP-jitter测试配置举例

1. 组网需求

使用 NQA 的 UDP-jitter 测试功能，测试本端（Device A）和指定目的端（Device B）的端口 9000 之间传送报文的时延抖动。

2. 组网图

图1-8 UDP-jitter 测试组网图

3. 配置步骤

说明

进行下面的配置之前，需要确保各设备之间路由可达。

(1) 配置 Device B

使能 NQA 服务器，配置监听的 IP 地址为 10.2.2.2，UDP 端口号为 9000。

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server udp-echo 10.2.2.2 9000
```

(2) 配置 Device A

创建 UDP-jitter 类型的 NQA 测试组。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type udp-jitter
```

配置测试操作的目的地址为 10.2.2.2，目的端口号为 9000。

```
[DeviceA-nqa-admin-test-udp-jitter] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-udp-jitter] destination port 9000
```

配置可选参数：测试组连续两次测试开始时间的时间间隔为 1000 毫秒。

```
[DeviceA-nqa-admin-test-udp-jitter] frequency 1000
[DeviceA-nqa-admin-test-udp-jitter] quit
```

启动 UDP-jitter 测试操作。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

测试执行一段时间后，停止 UDP-jitter 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

显示 UDP-jitter 测试中最后一次测试的结果。

```
[DeviceA] display nqa result admin test
  NQA entry (admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 10             Receive response times: 10
      Min/Max/Average round trip time: 15/32/17
      Square-Sum of round trip time: 3235
      Last succeeded probe time: 2011-01-29 13:56:17.6
    Extended results:
      Packet loss in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
    UDP-jitter results:
     RTT number: 10
      Min positive SD: 4                   Min positive DS: 1
      Max positive SD: 21                  Max positive DS: 28
      Positive SD number: 5                Positive DS number: 4
      Positive SD sum: 52                  Positive DS sum: 38
      Positive SD average: 10              Positive DS average: 10
      Positive SD square sum: 754          Positive DS square sum: 460
      Min negative SD: 1                   Min negative DS: 6
      Max negative SD: 13                  Max negative DS: 22
      Negative SD number: 4                Negative DS number: 5
      Negative SD sum: 38                  Negative DS sum: 52
      Negative SD average: 10              Negative DS average: 10
      Negative SD square sum: 460          Negative DS square sum: 754
    One way results:
      Max SD delay: 15                     Max DS delay: 16
      Min SD delay: 7                      Min DS delay: 7
      Number of SD delay: 10               Number of DS delay: 10
      Sum of SD delay: 78                  Sum of DS delay: 85
      Square sum of SD delay: 666          Square sum of DS delay: 787
      SD lost packet(s): 0                 DS lost packet(s): 0
      Lost packet(s) for unknown reason: 0
```

显示 UDP-jitter 测试的统计结果。

```
[DeviceA] display nqa statistics admin test
  NQA entry (admin admin, tag test) test statistics:
    NO. : 1
    Destination IP address: 10.2.2.2
      Start time: 2011-01-29 13:56:14.0
      Life time: 47 seconds
      Send operation times: 410            Receive response times: 410
      Min/Max/Average round trip time: 1/93/19
      Square-Sum of round trip time: 206176
    Extended results:
      Packet loss in test: 0%
```

```
  Failures due to timeout: 0
  Failures due to disconnect: 0
  Failures due to no connection: 0
  Failures due to sequence error: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packet(s) arrived late: 0
UDP-jitter results:
 RTT number: 410
  Min positive SD: 3                    Min positive DS: 1
  Max positive SD: 30                   Max positive DS: 79
  Positive SD number: 186               Positive DS number: 158
  Positive SD sum: 2602                 Positive DS sum: 1928
  Positive SD average: 13               Positive DS average: 12
  Positive SD square sum: 45304         Positive DS square sum: 31682
  Min negative SD: 1                    Min negative DS: 1
  Max negative SD: 30                   Max negative DS: 78
  Negative SD number: 181               Negative DS number: 209
  Negative SD sum: 181                  Negative DS sum: 209
  Negative SD average: 13               Negative DS average: 14
  Negative SD square sum: 46994         Negative DS square sum: 3030
One way results:
  Max SD delay: 46                      Max DS delay: 46
  Min SD delay: 7                       Min DS delay: 7
  Number of SD delay: 410               Number of DS delay: 410
  Sum of SD delay: 3705                 Sum of DS delay: 3891
  Square sum of SD delay: 45987         Square sum of DS delay: 49393
  SD lost packet(s): 0                  DS lost packet(s): 0
  Lost packet(s) for unknown reason: 0
```

说明

display nqa history 命令的显示信息无法反映 UDP-jitter 测试的结果，如果想了解 UDP-jitter 测试的结果，建议通过 **display nqa result** 命令查看最近一次 NQA 测试的结果，或通过 **display nqa statistics** 命令查看 NQA 测试的统计信息。

1.14.7 SNMP测试配置举例

1. 组网需求

使用 NQA 的 SNMP 测试功能，测试从 Device A 发出一个 SNMP 协议查询报文到收到 SNMP agent（Device B）响应报文所用的时间。

2. 组网图

图1-9 SNMP 配置测试组网图

3. 配置步骤

说明

进行下面的配置之前，需要确保各设备之间路由可达。

(1) 配置 SNMP agent（Device B）

启动 SNMP agent 服务，设置 SNMP 版本为 all、只读团体名为 public、读写团体名为 private。

```
<DeviceB> system-view
[DeviceB] snmp-agent
[DeviceB] snmp-agent sys-info version all
[DeviceB] snmp-agent community read public
[DeviceB] snmp-agent community write private
```

(2) 配置 Device A

创建 SNMP 类型的测试组，并配置测试操作的目的地址为 SNMP agent 的 IP 地址 10.2.2.2。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type snmp
[DeviceA-nqa-admin-test-snmp] destination ip 10.2.2.2
```

开启 NQA 测试组的历史记录保存功能。

```
[DeviceA-nqa-admin-test-snmp] history-record enable
[DeviceA-nqa-admin-test-snmp] quit
```

启动测试操作。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

测试执行一段时间后，停止 SNMP 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

显示 SNMP 测试中最后一次测试的结果。

```
[DeviceA] display nqa result admin test
  NQA entry (admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 50/50/50
      Square-Sum of round trip time: 2500
      Last succeeded probe time: 2011-01-22 10:24:41.1
    Extended results:
      Packet loss in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
```

显示 SNMP 测试的历史记录。

```
[DeviceA] display nqa history admin test
  NQA entry (admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          50           Timeout          2011-01-22 10:24:41.1
```

1.14.8 TCP测试配置举例

1. 组网需求

使用 NQA 的 TCP 测试功能，测试本端（Device A）和指定目的端（Device B）的端口 9000 之间建立 TCP 连接所需的时间。

2. 组网图

图1-10 TCP 测试组网图

3. 配置步骤

说明

进行下面的配置之前，需要确保各设备之间路由可达。

(1) 配置 Device B

使能 NQA 服务器，配置监听的 IP 地址为 10.2.2.2，TCP 端口号为 9000。

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server tcp-connect 10.2.2.2 9000
```

(2) 配置 Device A

创建 TCP 类型的测试组。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type tcp
```

配置测试操作的目的地址为 10.2.2.2，目的端口号为 9000。

```
[DeviceA-nqa-admin-test-tcp] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-tcp] destination port 9000
```

开启 NQA 测试组的历史记录保存功能。

```
[DeviceA-nqa-admin-test-tcp] history-record enable
[DeviceA-nqa-admin-test-tcp] quit
```

启动测试操作。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

测试执行一段时间后，停止 TCP 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

显示 TCP 测试中最后一次测试的结果。

```
[DeviceA] display nqa result admin test
  NQA entry (admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 13/13/13
      Square-Sum of round trip time: 169
      Last succeeded probe time: 2011-01-22 10:27:25.1
    Extended results:
      Packet loss in test: 0%
```

```
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
```

显示 TCP 测试的历史记录。

```
[DeviceA] display nqa history admin test
  NQA entry (admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          13           Succeeded        2011-01-22 10:27:25.1
```

1.14.9 UDP-echo测试配置举例

1. 组网需求

使用 NQA 的 UDP-echo 测试功能，测试本端（Device A）和指定目的端（Device B）的端口 8000 之间 UDP 协议报文的往返时间。

2. 组网图

图1-11 UDP-echo 测试组网图

3. 配置步骤

说明

进行下面的配置之前，需要确保各设备之间路由可达。

(1) 配置 Device B

使能 NQA 服务器，配置监听的 IP 地址为 10.2.2.2，UDP 端口号为 8000。

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server udp-echo 10.2.2.2 8000
```

(2) 配置 Device A

创建 UDP-echo 类型的测试组。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type udp-echo
```

配置测试操作的目的地址为 10.2.2.2，目的端口号为 8000。

```
[DeviceA-nqa-admin-test-udp-echo] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-udp-echo] destination port 8000
```

开启 NQA 测试组的历史记录保存功能。

```
[DeviceA-nqa-admin-test-udp-echo] history-record enable
[DeviceA-nqa-admin-test-udp-echo] quit
```

启动测试操作。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

测试执行一段时间后，停止 UDP-echo 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

显示 UDP-echo 测试中最后一次测试的结果。

```
[DeviceA] display nqa result admin test
  NQA entry (admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 25/25/25
      Square-Sum of round trip time: 625
      Last succeeded probe time: 2011-01-22 10:36:17.9
    Extended results:
      Packet loss in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
```

显示 UDP-echo 测试的历史记录。

```
[DeviceA] display nqa history admin test
  NQA entry (admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          25           Succeeded        2011-01-22 10:36:17.9
```

1.14.10 Voice测试配置举例

1. 组网需求

使用 NQA 的 Voice 测试功能，测试本端（Device A）和指定的目的端（Device B）之间传送语音报文的时延抖动和网络语音质量参数。

2. 组网图

图1-12 Voice 测试组网图

3. 配置步骤

说明

进行下面的配置之前，需要确保各设备之间路由可达。

(1) 配置 Device B

使能 NQA 服务器，配置监听的 IP 地址为 10.2.2.2，UDP 端口号为 9000。

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server udp-echo 10.2.2.2 9000
```

(2) 配置 Device A

创建 Voice 类型的 NQA 测试组。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type voice
```

配置测试操作的目的地址为 10.2.2.2，目的端口号为 9000。

```
[DeviceA-nqa-admin-test-voice] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-voice] destination port 9000
[DeviceA-nqa-admin-test-voice] quit
```

启动 Voice 测试操作。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

测试执行一段时间后，停止 Voice 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

显示 Voice 测试中最后一次测试的结果。

```
[DeviceA] display nqa result admin test
  NQA entry (admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1000          Receive response times: 1000
      Min/Max/Average round trip time: 31/1328/33
      Square-Sum of round trip time: 2844813
      Last succeeded probe time: 2011-01-13 09:49:31.1
    Extended results:
      Packet loss in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
    Voice results:
     RTT number: 1000
      Min positive SD: 1                  Min positive DS: 1
      Max positive SD: 204                Max positive DS: 1297
      Positive SD number: 257             Positive DS number: 259
      Positive SD sum: 759                Positive DS sum: 1797
      Positive SD average: 2              Positive DS average: 6
      Positive SD square sum: 54127       Positive DS square sum: 1691967
      Min negative SD: 1                  Min negative DS: 1
      Max negative SD: 203                Max negative DS: 1297
      Negative SD number: 255             Negative DS number: 259
      Negative SD sum: 759                Negative DS sum: 1796
      Negative SD average: 2              Negative DS average: 6
      Negative SD square sum: 53655       Negative DS square sum: 1691776
    One way results:
      Max SD delay: 343                   Max DS delay: 985
      Min SD delay: 343                   Min DS delay: 985
      Number of SD delay: 1               Number of DS delay: 1
      Sum of SD delay: 343                Sum of DS delay: 985
      Square sum of SD delay: 117649      Square sum of DS delay: 970225
      SD lost packet(s): 0                DS lost packet(s): 0
      Lost packet(s) for unknown reason: 0
    Voice scores:
```

```
      MOS value: 4.38                         ICPIF value: 0
```

显示 Voice 测试的统计结果。

```
[DeviceA] display nqa statistics admin test
  NQA entry (admin admin, tag test) test statistics:
    NO. : 1
    Destination IP address: 10.2.2.2
      Start time: 2011-06-13 09:45:37.8
      Life time: 331 seconds
      Send operation times: 4000           Receive response times: 4000
      Min/Max/Average round trip time: 15/1328/32
      Square-Sum of round trip time: 7160528
    Extended results:
      Packet loss in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
    Voice results:
     RTT number: 4000
      Min positive SD: 1                      Min positive DS: 1
      Max positive SD: 360                    Max positive DS: 1297
      Positive SD number: 1030                Positive DS number: 1024
      Positive SD sum: 4363                   Positive DS sum: 5423
      Positive SD average: 4                  Positive DS average: 5
      Positive SD square sum: 497725          Positive DS square sum: 2254957
      Min negative SD: 1                      Min negative DS: 1
      Max negative SD: 360                    Max negative DS: 1297
      Negative SD number: 1028                Negative DS number: 1022
      Negative SD sum: 1028                   Negative DS sum: 1022
      Negative SD average: 4                  Negative DS average: 5
      Negative SD square sum: 495901          Negative DS square sum: 5419
    One way results:
      Max SD delay: 359                       Max DS delay: 985
      Min SD delay: 0                         Min DS delay: 0
      Number of SD delay: 4                   Number of DS delay: 4
      Sum of SD delay: 1390                   Sum of DS delay: 1079
      Square sum of SD delay: 483202          Square sum of DS delay: 973651
      SD lost packet(s): 0                    DS lost packet(s): 0
      Lost packet(s) for unknown reason: 0
    Voice scores:
      Max MOS value: 4.38                     Min MOS value: 4.38
      Max ICPIF value: 0                      Min ICPIF value: 0
```

说明

display nqa history 命令的显示信息无法反映 Voice 测试的结果，如果想了解 Voice 测试的结果，建议通过 **display nqa result** 命令查看最近一次 NQA 测试的结果，或通过 **display nqa statistics** 命令查看 NQA 测试的统计信息。

1.14.11 DLSw测试配置举例

1. 组网需求

使用 NQA 的 DLSw 测试功能，测试 DLSw 设备的响应时间。

2. 组网图

图1-13 DLSw 测试组网图

3. 配置步骤

说明

进行下面的配置之前，需要确保各设备之间路由可达。

创建 DLSw 类型的测试组，并配置测试操作的目的地址为 10.2.2.2。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type dlsw
[DeviceA-nqa-admin-test-dlsw] destination ip 10.2.2.2
```

开启 NQA 测试组的历史记录保存功能。

```
[DeviceA-nqa-admin-test-dlsw] history-record enable
[DeviceA-nqa-admin-test-dlsw] quit
```

启动测试操作。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

测试执行一段时间后，停止 DLSw 测试操作。

```
[DeviceA] undo nqa schedule admin test
```

显示 DLSw 测试中最后一次测试的结果。

```
[DeviceA] display nqa result admin test
  NQA entry (admin admin, tag test) test results:
    Destination IP address: 10.2.2.2
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 19/19/19
      Square-Sum of round trip time: 361
      Last succeeded probe time: 2011-01-22 10:40:27.7
    Extended results:
      Packet loss in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
```

显示 DLSw 测试的历史记录。

```
[DeviceA] display nqa history admin test
  NQA entry (admin admin, tag test) history record(s):
```

```
Index       Response     Status          Time
1           19           Succeeded       2011-01-22 10:40:27.7
```

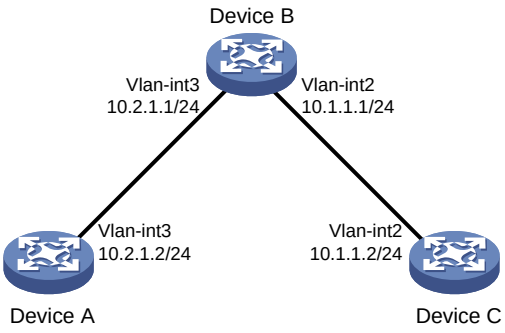
1.14.12 NQA联动配置举例

1. 组网需求

- Device A 到达 Device C 的静态路由下一跳为 Device B。
- 在 Device A 上通过静态路由、Track 与 NQA 联动，对到达 Device C 的静态路由有效性进行实时判断。

2. 组网图

图1-14 NQA 联动配置组网图



3. 配置步骤

(1) 按照 图 1-14 配置各接口的IP地址，具体配置过程略。

(2) 在 Device A 上配置静态路由，并与 Track 项关联

配置到达 Device C 的静态路由下一跳地址为 10.2.1.1，并配置静态路由与 Track 项 1 关联。

```
<DeviceA> system-view
[DeviceA] ip route-static 10.1.1.2 24 10.2.1.1 track 1
```

(3) 在 Device A 上配置 NQA 测试组

创建管理员名为 admin、操作标签为 test 的 NQA 测试组。

```
[DeviceA] nqa entry admin test
```

配置测试类型为 ICMP-echo。

```
[DeviceA-nqa-admin-test] type icmp-echo
```

配置目的地址为 10.2.1.1。

```
[DeviceA-nqa-admin-test-icmp-echo] destination ip 10.2.1.1
```

测试频率为 100ms。

```
[DeviceA-nqa-admin-test-icmp-echo] frequency 100
```

配置联动项 1（连续失败 5 次触发联动）。

```
[DeviceA-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type
consecutive 5 action-type trigger-only
[DeviceA-nqa-admin-test-icmp-echo] quit
```

启动探测。

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

(4) 在 Device A 上配置 Track 项

配置 Track 项 1，关联 NQA 测试组（管理员为 admin，操作标签为 test）的联动项 1。

```
[DeviceA] track 1 nqa entry admin test reaction 1
```

(5) 验证配置结果

显示 Device A 上 Track 项的信息。

```
[DeviceA] display track all
Track ID: 1
  Status: Positive
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    NQA entry: admin test
    Reaction: 1
```

显示 Device A 的路由表。

```
[DeviceA] display ip routing-table
Routing Tables: Public
         Destinations : 5        Routes : 5

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

10.1.1.0/24         Static 60   0            10.2.1.1        Vlan3
10.2.1.0/24         Direct 0    0            10.2.1.2        Vlan3
10.2.1.2/32         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

以上显示信息表示，NQA 测试的结果为下一跳地址 10.2.1.1 可达（Track 项状态为 Positive），配置的静态路由生效。

在 Device B 上删除 VLAN 接口 3 的 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface vlan-interface 3
[DeviceB-Vlan-interface3] undo ip address
```

显示 Device A 上 Track 项的信息。

```
[DeviceA] display track all
Track ID: 1
  Status: Negative
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    NQA entry: admin test
    Reaction: 1
```

显示 Device A 的路由表。

```
[DeviceA] display ip routing-table
Routing Tables: Public
         Destinations : 4        Routes : 4

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

10.2.1.0/24         Direct 0    0            10.2.1.2        Vlan3
10.2.1.2/32         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

以上显示信息表示，NQA 测试的结果为下一跳地址 10.2.1.1 不可达（Track 项状态为 Negative），配置的静态路由无效。

目 录

1 sFlow配置

1.1 sFlow简介

1.1.1 sFlow简介

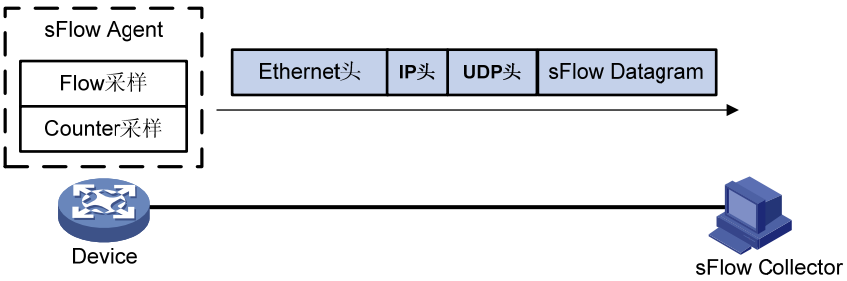
sFlow（Sampled Flow，采样流）是一种基于报文采样的网络流量监控技术，主要用于对网络流量进行统计分析。

如 图 1-1 所示，sFlow系统包含一个嵌入在设备中的sFlow Agent和远端的sFlow Collector。其中，sFlow Agent用于获取端口的统计信息和数据信息，将信息封装成sFlow报文，当sFlow报文缓冲区满或是在sFlow报文老化时间（老化时间为 1 秒）超时后，sFlow Agent会将sFlow报文发送到指定的sFlow Collector。sFlow Collector会对sFlow报文进行分析，并显示分析结果。

sFlow 包括以下两种采样机制：

- Flow 采样：基于数据包的采样，用于获取数据内容的相关信息。
- Counter 采样：基于时间的端口统计信息采样，用于获取端口的统计信息。

图1-1 sFlow 示意图



作为一种网络流量监控技术，sFlow 具有如下优点：

- 支持在千兆或更高速的网络上精确地监控网络流量。
- 一个 sFlow Collector 能够监控多个 sFlow Agent，具有良好的扩展性。
- sFlow Agent 可以内嵌在设备中，不需要专门的 sFlow Agent 设备，节省了成本。

说明

目前设备只支持 sFlow Agent，不支持 sFlow Collector。

1.1.2 sFlow的启动和运行过程

sFlow 启动和运行的整个过程如下：

(1) 在设备上配置 sFlow Agent 和 sFlow Collector 信息。

(2) 在以太网端口上配置Flow采样后，sFlow Agent会收集采样报文，然后将采样报文封装为sFlow报文。具体配置可参见“1.2.2 配置Flow采样”。

(3) 在以太网端口上配置Counter采样后，sFlow Agent会定时查询该端口下的统计信息，然后将统计信息封装为sFlow报文。具体配置可参见“1.2.3 配置Counter采样”。

1.2 配置sFlow

在设备和 sFlow Collector 上完成 sFlow 相关配置后，sFlow 功能才能正常工作。

- 在设备上必须配置 sFlow Collector 的 IP 地址、Flow 采样和 Counter 采样。
- 在 sFlow Collector 上完成相关配置。

1.2.1 配置sFlow Agent和sFlow Collector信息

本配置用于设置设备的 sFlow 特性，使远端的 sFlow Collector 能够监控网络，并对 sFlow 报文进行分析。

表1-1 配置 sFlow Agent 和 sFlow Collector 信息

操作	命令	说明
进入系统视图	**system-view**	-
配置sFlow Agent的IP地址	**sflow agent** { **ip** *ip-address* | **ipv6** *ipv6-address* }	可选 缺省情况下，未配置sFlow Agent的IP地址。设备会定期检查是否存在sFlow Agent的IP地址，如果不存在，设备会自动查找一个IPv4地址作为sFlow Agent的IP地址。自动查找的IP地址信息不会保存在设备上 需要注意的是： • 建议用户手工配置 sFlow Agent 的 IP 地址 • 在设备上只能配置一个 sFlow Agent 的 IP 地址
配置sFlow Collector的信息	**sflow collector** *collector-id* { [**vpn-instance** *vpn-instance-name*] { **ip** *ip-address* | **ipv6** *ipv6-address* } | **datagram-size** *size* | **description** *text* | **port** *port-number* | **time-out** *seconds* } *	必选 缺省情况下，设备会预先创建一定数目的sFlow Collector。设备预先创建的sFlow Collector中的参数情况可以使用**display sflow**命令查看
配置sFlow报文的源地址	**sflow source** { **ip** *ip-address* | **ipv6** *ipv6-address* } *	可选 缺省情况下，没有配置sFlow报文的源地址

1.2.2 配置Flow采样

表1-2 配置 Flow 采样

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图或者三层以太网端口视图	**interface** *interface-type interface-number*	-
设置Flow采样的采样模式	**sflow sampling-mode** { **determine** | **random** }	可选 缺省情况下，数据流信息的采样模式为**random**
配置报文的采样间隔，即在*interval*个报文中抽取一个报文进行采样	**sflow sampling-rate** *interval*	必选 缺省情况下，不对报文进行采样

操作	命令	说明
配置从原始报文的头开始，允许拷贝的最大字节数	**sflow flow max-header** *length*	可选 缺省情况下，从原始报文的头开始，允许拷贝的最大字节数为128字节。建议用户使用缺省配置
配置经过Flow采样后，sFlow Agent输出sFlow报文的目的sFlow Collector编号	**sflow flow collector** *collector-id*	必选 缺省情况下，Flow采样和sFlow Collector没有绑定关系，即没有指定目的sFlow Collector编号

说明

目前本系列交换机不支持配置 sFlow 采样模式为 **determine**。

1.2.3 配置Counter采样

表1-3 配置 Counter 采样

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图或者三层以太网端口视图	**interface** *interface-type interface-number*	-
配置Counter采样的时间间隔	**sflow counter interval** *seconds*	必选 缺省情况下，不进行Counter采样
配置经过Counter采样后，sFlow Agent输出sFlow报文的目的sFlow Collector编号	**sflow counter collector** *collector-id*	必选 缺省情况下，Counter采样和sFlow Collector没有绑定关系，即没有指定目的sFlow Collector编号

1.3 sFlow显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令，可以显示配置的 sFlow 特性运行情况，通过查看显示信息验证配置的效果。

表1-4 sFlow 显示和维护

操作	命令
显示sFlow配置信息	**display sflow** [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

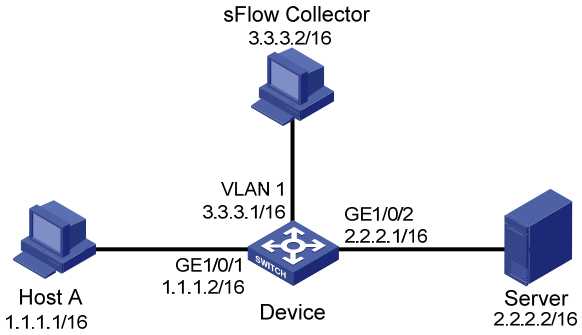
1.4 sFlow典型配置举例

1.4.1 sFlow典型配置举例

1. 组网需求

Host A 与远端服务器 Server 通过 Device 相连。在 Device 上运行 sFlow Agent，并在 GigabitEthernet1/0/1 上开启 sFlow 功能（包括 Flow 采样和 Counter 采样），使 Agent 能够对该端口的网络流量进行监控。Device 将 sFlow 报文通过 GigabitEthernet1/0/3 发送给 sFlow Collector，sFlow Collector 再对 sFlow 报文进行分析并显示。

图1-2 sFlow 典型配置组网图



2. 配置步骤

(1) 配置 sFlow Agent 和 sFlow Collector 信息

配置接口 IP 地址。

```
<Device> system-view
[Device] interface vlan-interface 1
[Device-Vlan-interface1] ip address 3.3.3.1 16
[Device-Vlan-interface1] quit
```

配置 sFlow Agent 的 IP 地址。

```
[Device] sflow agent ip 3.3.3.1
```

配置 sFlow Collector 信息：sFlow Collector 的 ID 为 2，IP 地址为 3.3.3.2，端口号保持缺省值，描述信息为 netserver。

```
[Device] sflow collector 2 ip 3.3.3.2 description netserver
```

(2) 配置 Counter 采样

配置 Counter 采样时间间隔为 120 秒。

```
[Device] interface gigabitethernet 1/0/1
[Device- GigabitEthernet1/0/1] sflow counter interval 120
```

配置经过 Counter 采样后，sFlow Agent 输出 sFlow 报文的目的 sFlow Collector 编号为 2。

```
[Device-GigabitEthernet1/0/1] sflow counter collector 2
```

(3) 配置 Flow 采样

配置采样模式为随机采样。报文的采样间隔为 4000，即在 4000 个报文中抽取一个报文进行采样。

```
[Device-GigabitEthernet1/0/1] sflow sampling-mode random
[Device-GigabitEthernet1/0/1] sflow sampling-rate 4000
```

配置经过 Flow 采样后，sFlow Agent 输出 sFlow 报文的目的 sFlow Collector 编号为 2。

```
[Device-GigabitEthernet1/0/1] sflow flow collector 2
```

显示 sFlow 的配置和运行信息。

```
[Device-GigabitEthernet1/0/1] display sflow
```

```
sFlow Version: 5
sFlow Global Information:
Agent          IP:3.3.3.1(CLI)
Source  Address:
Collector Information:
ID    IP                                    Port    Aging    Size  VPN-instance Description
1                                           6343    0        1400
2     3.3.3.2                               6543    N/A      1400                 netserver
3                                           6343    0        1400
4                                           6343    0        1400
5                                           6343    0        1400
6                                           6343    0        1400
7                                           6343    0        1400
8                                           6343    0        1400
9                                           6343    0        1400
10                                          6343    0        1400
sFlow Port Information:
Interface CID   Interval(s) FID  MaxHLen   Rate       Mode     Status
GE1/0/1    2      120         2    128       4000       Random   Active
```

从上面的显示信息中可以看到开启 sFlow 功能的 GigabitEthernet1/0/1 端口的处于“Active”状态，Counter 采样时间间隔为 120 秒，报文的采样间隔为 4000，表示 sFlow 功能正在正常运行。

1.5 常见配置错误举例

1.5.1 远端的sFlow Collector无法收到sFlow报文

1. 故障现象

远端的 sFlow Collector 无法收到 sFlow 报文。

2. 故障分析

可能有以下几个原因：

- 没有配置 sFlow Collector 的 IP 地址；
- 端口没有配置 sFlow 采样，导致没有端口提供采样数据；
- 配置的 sFlow Collector 的 IP 地址和远端的 sFlow Collector 的 IP 地址不同，导致远端的 sFlow Collector 无法收到 sFlow 报文；
- 如果设备没有配置三层接口的 IP 地址，或配置了 IP 地址但是以此 IP 为源 IP 地址的 UDP 报文无法到达 sFlow Collector；
- 设备和 sFlow Collector 之间的网络物理中断。

3. 故障排除

(1) 执行 **display sflow** 命令，查看当前的 sFlow 配置信息，检查是否为 sFlow 特性配置错误；

(2) 检查设备是否已经配置可以和 sFlow Collector 通讯的 IP 地址；

(3) 检查设备和 sFlow Collector 之间的物理连接是否正常。

目 录

1 NetStream配置


说明

S5500-28SC-HI 和 S5500-52SC-HI 不支持 NetStream 相关配置。

1.1 NetStream技术应用背景

Internet 的高速发展为用户提供了更高的带宽，支持的业务和应用日渐增多，传统流量统计如 SNMP、端口镜像等，由于统计流量方式不灵活或是需要投资专用服务器成本高等原因，无法满足对网络进行更细致的管理，需要一种新技术来更好的支持网络流量统计。

NetStream 技术是一种基于网络流信息的统计技术，可以对网络中的业务流量情况进行统计和分析。在网络的接入层、汇聚层、核心层上，都可以部署 NetStream。

NetStream 技术的应用有以下几种。

- 计费：NetStream 为基于资源（如线路、带宽、时段等）占用情况的计费提供了精细的数据。Internet 服务提供商可以利用这些信息来实行灵活的计费策略，如基于时间、带宽、应用、服务质量等。企业客户可以使用这些信息计算部门费用或分配成本，以便有效利用资源。
- 网络规划：NetStream 可以为网络管理工具提供关键信息，比如各设备之间的网络流量情况，以便优化网络设计和规划，实现以最小的网络运营成本达到最佳的网络性能和可靠性。
- 网络监控：通过在出口部署 NetStream，对连接 Internet 网络的接口进行实时的流量监控，可以分析各种业务占用出口带宽的情况。网管人员可以根据这些信息判断网络的运行情况，尽早发现不合理的网络结构或是网络中的性能瓶颈，方便网管人员规划和分配网络资源。
- 用户监控和分析：通过 NetStream 技术可以使网络管理者轻松获取用户使用网络和应用资源的详细情况，进而高效地规划以及分配网络资源，并保障网络的安全运行。

1.2 NetStream的基本概念

1.2.1 NetStream流定义

NetStream 是一项基于“流”来提供报文统计的技术。它根据 IPv4 报文的目的 IP 地址、源 IP 地址、目的端口号、源端口号、协议号、ToS（Type of Service，服务类型）、输入接口或输出接口来定义流，相同的八元组标识为同一条流。

1.2.2 NetStream系统组成

一个典型的 NetStream 系统由 NDE（NetStream Data Exporter，网络流数据输出）、NSC（NetStream Collector，网络流数据收集）和 NDA（NetStream Data Analyzer，网络流数据分析）三部分组成。

- NDE

NDE 负责对网络流进行分析处理，提取符合条件的流进行统计，并将统计信息输出给 NSC 设备。输出前也可对数据进行一些处理，比如聚合。配置了 NetStream 功能的设备在 NetStream 系统中担当 NDE 角色。

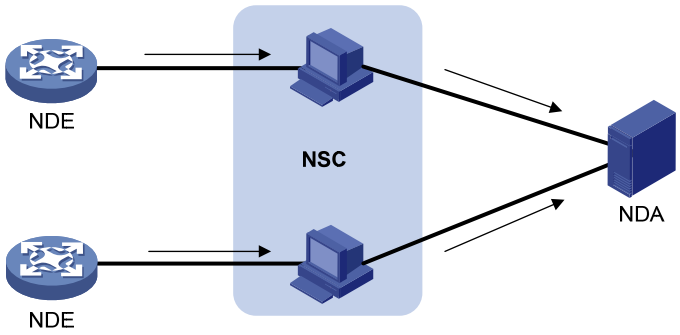
- NSC

NSC 通常为运行于 Unix 或者 Windows 上的一个应用程序，负责解析来自 NDE 的报文，把统计数据收集到数据库中，可供 NDA 进行解析。NSC 可以采集多个 NDE 设备输出的数据，对数据进行进一步的过滤和聚合。

- NDA

NDA 是一个网络流量分析工具，它从 NSC 中提取统计数据，进行进一步的加工处理，生成报表，为各种业务提供依据（比如流量计费、网络规划，攻击监测）。通常，NDA 具有图形化用户界面，可以使用户方便地获取、显示和分析收集到的数据。

图1-1 NetStream 系统中的设备角色



如 图 1-1 所示，NetStream进行数据采集和分析的过程如下：

(1) 配置了 NetStream 功能的设备（即 NDE）把采集到的关于流的详细信息定期发送给 NSC；

(2) 信息由 NSC 初步处理后发送给 NDA；

(3) NDA 对数据进行分析，以用于计费、网络规划等应用。

说明

- 由于设备在 NetStream 系统中担任 NDE 角色，所以本文档重点介绍 NDE 的实现以及配置。
- NSC 和 NDA 一般集成在一台 NetStream 服务器上。

1.3 NetStream关键技术

1.3.1 流老化

NetStream流老化是设备向NetStream服务器输出流统计信息的一种手段。当设备启用NetStream功能后，流统计信息首先会被存储在设备的NetStream缓冲区中。当存储在设备上的NetStream流信息老化后，设备会把缓冲区中的流统计信息通过指定版本的NetStream输出报文发送给NetStream服务器。流老化的三种方式及其配置请参见“1.10 配置NetStream的流老化”。

1.3.2 流输出

1. 普通流输出

普通流输出是指所有流的统计信息都要被统计。在流老化时间超时后，每条流的统计信息都要输出到 NetStream 服务器。

普通流的优点是：NetStream 服务器可以得到每条流的详细统计信息。但是缺点也是很明显的，这种方式增加了网络带宽和设备的 CPU 占有率，而且为了存储这些信息，需要大量的存储介质空间，而很多情况下，用户并不需要获取所有流的统计信息。

2. 聚合流输出

聚合流输出是指采用聚合流输出功能后，设备对与聚合关键项完全相同的流统计信息进行汇总，从而得到对应的聚合流统计信息，并且将该聚合统计信息发送到相应的接收聚合统计信息的NetStream服务器。

例如，发送四条TCP流，其目的地址相同、源地址不同，源端口、目的端口均为 10，选择 表 1-1 中的“协议-端口聚合”方式，该聚合方式的依据为“协议号、源端口、目的端口”。因为这四条TCP流的源端口、目的端口和协议号相同，所以在聚合流统计表项中只会记录一条聚合流统计信息。设备只将聚合统计信息发送给相应的接收聚合统计信息的NetStream服务器。由此可见，聚合的最大好处是可以减少对网络带宽的占用。

在目前的实现中，聚合流输出支持的 9 种方式如 表 1-1 所示。系统根据选择聚合方式的聚合关键项，将符合对应聚合方式的多条流合并为一条聚合流，对应一条聚合记录。9 种聚合方式相互独立，可以同时配置。

表1-1 聚合流输出支持的 9 种方式

聚合方式	聚合关键项
协议-端口聚合（**protocol-port**）	协议号、源端口、目的端口
源前缀聚合（**source-prefix**）	源掩码长度、源前缀、输入接口索引
目的前缀聚合（**destination-prefix**）	目的掩码长度、目的前缀、输出接口索引
源和目的前缀聚合（**prefix**）	源掩码长度、目的掩码长度、源前缀、目的前缀、输入接口索引、输出接口索引
前缀-端口聚合（**prefix-port**）	源前缀、目的前缀、源掩码长度、目的掩码长度、ToS、协议号、源端口、目的端口、输入接口索引、输出接口索引
服务类型-源前缀聚合（**tos-source-prefix**）	ToS、源前缀、源掩码长度、输入接口索引
服务类型-目的前缀聚合（**tos-destination-prefix**）	ToS、目的掩码长度、目的前缀、输出接口索引
服务类型-前缀聚合（**tos-prefix**）	ToS、源前缀、源掩码长度、目的掩码长度、目的前缀、输入接口索引和输出接口索引
服务类型-协议-端口聚合（**tos-protocol-port**）	ToS、协议类型、源端口、目的端口、输入接口索引、输出接口索引

1.3.3 输出报文的版本格式

目前 Netstream 输出的报文主要有 5、8、9 三个版本。其中版本 9 为用户提供了可定义统计元素的模板，用户可根据实际需求设计该模板，使统计信息的输出更为灵活。

- 版本 5：根据七元组产生原始的数据流，但报文格式固定，不易扩展。
- 版本 8：支持聚合输出格式，但报文格式固定，不易扩展。
- 版本 9：基于模板方式，使统计信息的输出更为灵活，可以用来灵活输出各种组合格式的数据。

1.4 NetStream采样过滤功能

1.4.1 NetStream采样

NetStream 可以与 Sampler（采样器）配合使用。通过设定适当的采样间隔，不但减少了统计的报文数量，收集到的统计信息也可以保证基本正确地反映整个网络流的状况。另外，采样还可以减小对设备转发性能造成的影响。与采样有关的内容请参见“网络管理和监控配置指导”中的“Sampler”。

1.4.2 NetStream过滤

NetStream 可以与 ACL（Access Control List，访问控制列表）和 QoS（Quality of Service，服务质量）配合使用，NetStream 只统计符合 ACL 和 QoS 筛选出的特定报文。通过这种方式可以使 NetStream 对用户关注的数据进行统计，更能满足用户多样的统计要求。

NetStream 无论是和 ACL 或是和 QoS 配合使用，都是为了先对数据流进行过滤，这样 NetStream 就可以“只对某些符合条件的流”进行统计。两者方式的区别是：QoS 可以更加灵活的指定流，且应用方式多样。

1.5 NetStream配置任务简介

在配置 NetStream 之前，可根据以下需求选择相应的配置环节：

- 部署 NetStream 的具体位置，也就是明确需要在网络环境中的哪台设备上开启 NetStream 功能。
- 如果网络上有各种业务流，可以考虑使用 ACL 或 QoS 筛选出需要统计的特定数据。
- 如果网络上的流量很大，可以考虑对数据流进行采样。
- 确定采用哪种输出报文的版本，对 NetStream 统计输出报文的版本进行设置。
- 根据实际网络情况和需求，对 NetStream 的流老化时间进行设置。
- 如果统计输出的报文过多，可以配置聚合输出统计信息，避免重复的流输出信息占用网络带宽。

具体的配置步骤可以参考 图 1-2。

图1-2 NetStream 配置步骤流程图

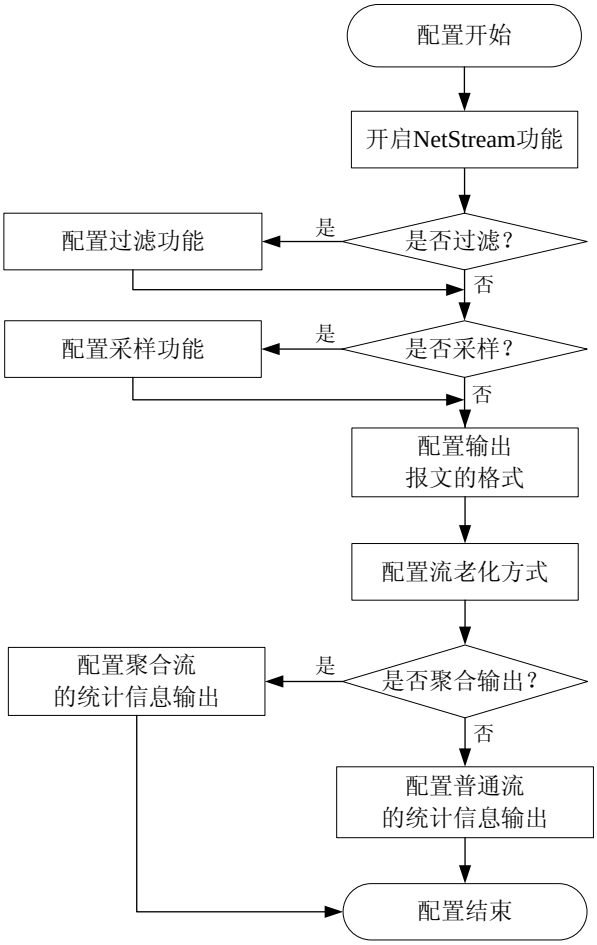


表1-2 NetStream 配置任务简介

配置任务		说明	详细配置
开启NetStream功能		必选	1.6
配置NetStream过滤功能		可选	1.7.1
配置NetStream采样功能		可选	1.7.2
配置NetStream统计信息的输出	配置NetStream普通流的统计信息输出	请根据实际需要进行选择	1.8
	配置NetStream聚合流的统计信息输出		
配置NetStream输出报文的格式		可选	1.9
配置NetStream的流老化		可选	1.10

1.6 开启NetStream功能

1.6.1 开启端口的NetStream功能

表1-3 开启端口的 NetStream 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图/三层以太网端口视图	**interface** *interface-type interface-number*	-
开启端口的NetStream功能	**ip netstream** { **inbound** | **outbound** }	必选 缺省情况下，NetStream功能处于关闭状态

1.7 配置NetStream过滤采样功能

配置 NetStream 过滤采样功能前，请先使用 **ip netstream** 命令开启 NetStream 功能。

1.7.1 配置NetStream过滤功能

1. 使用ACL方式进行过滤

表1-4 配置根据指定条件对 NetStream 过滤功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图	**interface** *interface-type interface-number*	-
配置根据指定条件对NetStream过滤功能	**ip netstream filter acl** *acl-number* { **inbound** | **outbound** }	可选 缺省情况下， NetStream统计所有IPv4报文，不启用过滤功能

说明

- 如果在设备上同时配置过滤和采样，设备会先过滤后采样报文。
- 配置过滤时，要求 ACL 规则必须存在且不为空。ACL 被引用后，不允许删除或修改 ACL 规则。关于 ACL 的相关内容请参见“ACL 和 QoS 配置指导”中的“ACL”。

2. 使用QoS方式进行过滤

使用 **netstream filter** 命令可以对匹配到的具体报文进行 NetStream 统计。

- **deny**：不对报文进行 NetStream 统计，直接转发。
- **permit**：对报文进行 NetStream 统计。

表1-5 使用 QoS 方式进行过滤

操作	命令	说明
进入系统视图	**system-view**	-

操作		命令	说明
定义类并进入类视图		**traffic classifier** *tcl-name* [**operator** { **and** | **or** }]	-
定义匹配数据包的规则		**if-match** *match-criteria*	-
退出类视图		**quit**	-
定义一个流行为并进入流行为视图		**traffic behavior** *behavior-name*	-
配置NetStream过滤动作		**netstream filter** { **deny** | **permit** }	必选
退出流行为视图		**quit**	-
定义策略并进入策略视图		**qos policy** *policy-name*	-
在策略中为类指定采用的流行为		**classifier** *tcl-name* **behavior** *behavior-name*	-
退出策略视图		**quit**	-
应用QoS策略	基于端口	进入二层以太网端口视图或三层以太网端口视图、端口组视图 **qos apply policy** *policy-name* { **inbound** | **outbound** }	-
	基于VLAN	进入系统视图 **qos vlan-policy** *policy-name* **vlan** *vlan-id-list* { **inbound** | **outbound** }	-
	基于全局	进入系统视图 **qos apply policy** *policy-name* **global** { **inbound** | **outbound** }	-
	基于控制平面	进入控制平面视图 **qos apply policy** *policy-name* **inbound**	-

说明

关于类、流行为、策略的详细介绍和相关配置，请参见“ACL 和 QoS 配置指导”中的“QoS 配置方式”。

1.7.2 配置NetStream采样功能

表1-6 配置 NetStream 的采样功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图或三层以太网端口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
配置NetStream采样功能	**ip netstream sampler** *sampler-name* { **inbound** | **outbound** }	必选 缺省情况下，NetStream统计所有IPv4报文，不启用采样功能

说明

- 如果在设备上同时配置过滤和采样，设备会先过滤后采样报文。
- 配置采样时，要求采样器必须存在（即需要 **sampler** 命令先创建采样器），然后使用 **ip netstream sampler** 引用采样器。采样器引用后不允许删除。关于 Sampler 的内容请参见“网络管理和监控配置指导”中的“Sampler”。

1.8 配置NetStream统计信息的输出

在配置 NetStream 统计信息的输出时，需要对 NetStream 统计信息输出的源端口和目的地址进行设置，后者为必选配置。

1.8.1 配置NetStream普通流的统计信息输出

表1-7 配置 NetStream 普通流的统计信息输出

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图/三层以太网端口视图	**interface** *interface-type interface-number*	-
使能端口的NetStream统计功能	**ip netstream** { **inbound** | **outbound** }	必选 缺省情况下，NetStream统计功能处于关闭状态
退回系统视图	**quit**	-
配置NetStream普通流统计信息输出的目的地址和目的UDP端口号	**ip netstream export host** *ip-address udp-port* [**vpn-instance** *vpn-instance-name*]	必选 缺省情况下，系统视图下没有配置目的地址和目的UDP端口号
配置NetStream统计信息输出的源端口	**ip netstream export source interface** *interface-type interface-number*	可选 缺省情况下，采用统计输出报文的出端口（即与服务器相连的端口）作为源端口 建议使用网管口作为源端口，与服务器相连，并向服务器输出统计信息
配置输出速率限制	**ip netstream export rate** *rate*	可选 缺省情况下，NetStream统计输出报文的输出速率不受限制

1.8.2 配置NetStream聚合流的统计信息输出

设备支持两种聚合方式：软件聚合和硬件聚合。若未配置硬件流聚合功能，则设备会通过软件对与聚合关键项完全相同的流统计信息进行汇总；配置采用硬件流聚合功能后，设备会通过硬件直接对与聚合关键项完全相同的流统计信息进行汇总，从而得到对应的聚合流统计信息。因此通过配置硬件流聚合功能，能够有效降低流聚合对设备资源的消耗。

表1-8 配置 NetStream 聚合流的统计信息输出

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图/三层以太网端口视图	**interface** *interface-type interface-number*	-
使能端口的NetStream统计功能	**ip netstream** { **inbound** | **outbound** }	必选 缺省情况下，NetStream统计功能处于关闭状态
退回系统视图	**quit**	-
配置NetStream硬件流聚合功能	**ip netstream aggregation advanced**	可选 缺省情况下，NetStream硬件流聚合功能处于关闭状态
进入NetStream聚合视图	**ip netstream aggregation** { **destination-prefix** | **prefix** | **prefix-port** | **protocol-port** | **source-prefix** | **tos-destination-prefix** | **tos-prefix** | **tos-protocol-port** | **tos-source-prefix** }	必选
配置NetStream聚合统计信息输出的目的地址和目的UDP端口号	**ip netstream export host** *ip-addrress udp-port* [**vpn-instance** *vpn-instance-name*]	必选 缺省情况下，聚合视图下没有配置目的地址和目的UDP端口号。为了减少对网络带宽的占用，可以只在聚合视图下配置**ip netstream export host**命令，此时设备只会输出聚合流信息
配置NetStream聚合统计信息输出的源端口	**ip netstream export source interface** *interface-type interface-number*	可选 缺省情况下，采用统计输出报文的出端口（即与服务器相连的端口）作为源端口 • 不同聚合视图下可以配置不同的源端口 • 聚合视图下若没有配置源端口，则使用系统视图下的配置 • 建议使用网管口作为源端口，与服务器相连，并向服务器输出统计信息
使能NetStream聚合功能	**enable**	必选 缺省情况下，NetStream聚合功能处于关闭状态

说明

- 硬件流聚合不能和系统视图下的 **ip netstream export host** 同时配置。在系统视图下配置的 **ip netstream export host** 命令后硬件聚合功能失效。
- 硬件聚合流表项的老化与普通流表项的老化相同。
- 在聚合视图下，用户配置的 NetStream 统计输出报文的输出属性，仅对聚合报文生效；而系统视图下的配置对普通报文生效，并且当聚合视图下没有配置以上属性时，也会对聚合报文生效。

1.9 配置NetStream输出报文的属性

1.9.1 配置NetStream输出报文的格式

用户可以通过配置 NetStream 输出报文的格式，进一步明确需要统计的选项。

表1-9 配置 NetStream 输出报文的格式

操作	命令	说明
进入系统视图	**system-view**	-
配置NetStream统计输出报文版本	**ip netstream export version** { **5** | 9 }	可选 缺省情况下，IPv4普通流信息通过版本5的NetStream统计输出报文

1.9.2 配置NetStream输出报文版本 9 模板的刷新率

由于 V9 版本是基于模板方式的、可支持自定义格式，所以设备上需要定期刷新模板，并通知 NetStream 服务器最新的 V9 模版格式。用户可以根据实际情况，配置版本 9 模板的刷新率，及时更新模板。

表1-10 配置 NetStream 输出报文版本 9 模板的刷新率

操作	命令	说明
进入系统视图	**system-view**	-
配置NetStream统计输出报文版本9模板的包刷新率	**ip netstream export v9-template refresh-rate packet** *packets*	可选 缺省情况下，每隔20个包发送一次版本9模板
配置NetStream统计输出报文版本9模板的时间刷新率	**ip netstream export v9-template refresh-rate time** *minutes*	可选 缺省情况下，每隔30分钟发送一次版本9模板

说明

可以同时配置包刷新率和时间刷新率，只要满足任意一个刷新条件，设备就会将符合条件的模板发送给 NetStream 服务器。

1.10 配置NetStream的流老化

1.10.1 流老化的三种机制

NetStream 流老化有以下三种机制：

- 按时老化
- 强制老化
- TCP 的 FIN 和 RST 报文触发老化（该形式的老化在 TCP 连接拆除时自动进行）。

1. 按时老化

按时老化分为以下两种方式：

- 不活跃的流老化：从最后一个报文开始，该流在 **ip netstream timeout inactive** 指定的时间内没有被采集到（即在设定的 **inactive** 时长内统计到的流数目没有增加），那么设备会向 NetStream 服务器输出该流的统计信息，这种老化称为不活跃的流老化。通过这种老化，可以清除设备上 NetStream 缓冲区中的无用表项（此时使用 **display ip netstream cache** 命令无法看到这条老化的流），充分利用统计表项资源。
- 活跃的流老化：从第一个报文开始，该流在 **ip netstream timeout active** 指定的时间内一直能被采集到。活跃时间超过设定的 **active** 时长后，需要输出该流的统计信息，这种老化称为活跃的流老化。设备向 NetStream 服务器输出活跃流的统计信息后，因为该流实际上还存在，所以在设备上 NetStream 缓冲区会继续统计该流（此时使用 **display ip netstream cache** 可以看到这条流的统计表项）。这种老化方式是设备为了向 NetStream 服务器输出活跃流统计信息的一种机制。

2. 强制老化

用户可以执行 **reset ip netstream statistics** 命令强制将 NetStream 缓冲区中所有流老化，并清除 NetStream 缓冲区信息。

3. TCP的FIN和RST报文触发老化

对于 TCP 连接，当有标志为 FIN 或 RST 的报文发送时，表示一次会话结束。因此当一条已经存在的 TCP 协议 NetStream 流中流过一条标志为 FIN 或 RST 的报文时，可以立即老化相应的 NetStream 流。但是假如一条流的第一个报文就是 TCP 的 FIN 或 RST 报文，则会按正常的流程创建一条新流，不进行老化。这种方式在设备上缺省开启，不能通过执行命令开启或关闭该老化方式。

1.10.2 配置NetStream的流老化

表1-11 配置 NetStream 的流老化

操作		命令	说明
进入系统视图		**system-view**	-
配置按时老化	配置活跃流的老化时间	**ip netstream timeout active** *minutes*	可选 缺省情况下，活跃流的老化时间为5分钟
	配置不活跃流的老化时间	**ip netstream timeout inactive** *seconds*	可选 缺省情况下，不活跃流的老化时间为30秒
配置强制老化	退回用户视图	**quit**	-

操作		命令	说明
	强制老化	**reset ip netstream statistics**	可选 执行该命令会强制老化流缓存区中所有流，并清除NetStream缓冲区的状态信息和输出报文信息

1.11 NetStream显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 IPv4 NetStream 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 NetStream 的统计信息。

表1-12 NetStream 显示和维护

操作	命令
查看NetStream流缓存区的配置和状态信息	**display ip netstream cache** [**verbose**] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
查看NetStream统计输出报文信息	**display ip netstream export** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
查看NetStream模板的配置和状态信息	**display ip netstream template** [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
将流缓存区中所有流强制老化，并清除NetStream缓冲区的状态信息和输出报文信息	**reset ip netstream statistics**

1.12 NetStream典型配置举例

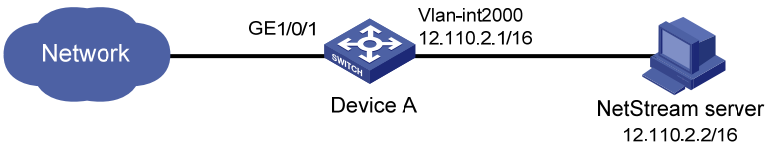
1.12.1 NetStream普通流的统计信息输出配置举例

1. 组网需求

如图所示，在 Device A 上配置 NetStream，对接收的报文进行统计，并将 NetStream 普通流的统计信息输出到 NetStream 服务器。NetStream 服务器的 IP 地址为 12.110.2.2/16，UDP 端口号为 5000。

2. 组网图

图1-3 NetStream 普通流的统计信息输出配置组网图



3. 配置步骤

在端口 GigabitEthernet1/0/1 上启动 NetStream 入统计。

```
<DeviceA> system-view
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip netstream inbound
[DeviceA-GigabitEthernet1/0/1] quit
```

在 VLAN 接口 2000 上配置 IP 地址。

```
[DeviceA] vlan 2000
[DeviceA-vlan2000] quit
[DeviceA] interface vlan-interface 2000
[DeviceA-Vlan-interface2000] ip address 12.110.2.1 255.255.0.0
[DeviceA-Vlan-interface2000] quit
[DeviceA] ip netstream export source interface Vlan-interface 2000
```

配置 NetStream 普通流统计信息输出的目的地址。

```
[DeviceA] ip netstream export host 12.110.2.2 5000
```

1.12.2 NetStream聚合流的统计信息输出配置举例

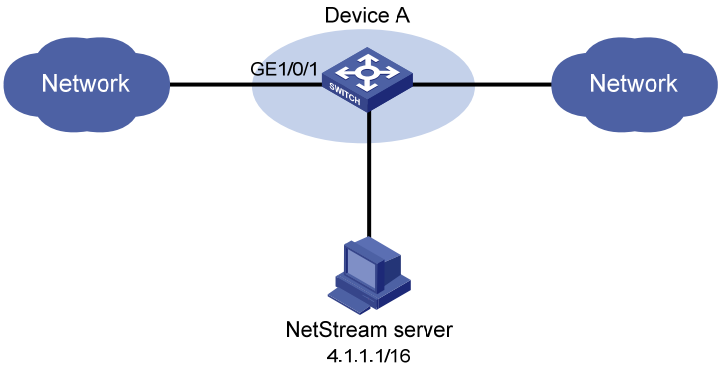
1. 组网需求

在 Device A 上配置 NetStream，具体要求为：

- 普通流的统计信息使用版本 5 格式输出到 NetStream 服务器。NetStream 服务器的 IP 地址为 4.1.1.1/16，UDP 端口号为 5000；
- 使用版本 8 格式对 4 种聚合流（**protocol-port**、**source-prefix**、**destination-prefix** 和 **prefix**）进行统计，并将各聚合流分别输出到该 NetStream 服务器的 3000、4000、6000 和 7000 端口。

2. 组网图

图1-4 NetStream 聚合流的统计信息输出配置组网图



3. 配置步骤

在出、入方向启用 NetStream 统计功能。

```
<DeviceA> system-view
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip netstream inbound
[DeviceA-GigabitEthernet1/0/1] ip netstream outbound
[DeviceA-GigabitEthernet1/0/1] quit
```

配置普通流统计信息输出的目的地址。

```
[DeviceA] ip netstream export host 4.1.1.1 5000
```

配置协议－端口聚合模式，以及该聚合模式聚合流统计信息输出的目的地址。

```
[DeviceA] ip netstream aggregation protocol-port
[DeviceA-ns-aggregation-protport] enable
[DeviceA-ns-aggregation-protport] ip netstream export host 4.1.1.1 3000
[DeviceA-ns-aggregation-protport] quit
```

配置源前缀聚合模式，以及该聚合模式聚合流统计信息输出的目的地址。

```
[DeviceA] ip netstream aggregation source-prefix
[DeviceA-ns-aggregation-srcpre] enable
```

```
[DeviceA-ns-aggregation-srcpre] ip netstream export host 4.1.1.1 4000
[DeviceA-ns-aggregation-srcpre] quit
```

配置目的前缀聚合模式，以及该聚合模式聚合流统计信息输出的目的地址。

```
[DeviceA] ip netstream aggregation destination-prefix
[DeviceA-ns-aggregation-dstpre] enable
[DeviceA-ns-aggregation-dstpre] ip netstream export host 4.1.1.1 6000
[DeviceA-ns-aggregation-dstpre] quit
```

配置前缀聚合模式，以及该聚合模式聚合流统计信息输出的目的地址。

```
[DeviceA] ip netstream aggregation prefix
[DeviceA-ns-aggregation-prefix] enable
[DeviceA-ns-aggregation-prefix] ip netstream export host 4.1.1.1 7000
[DeviceA-ns-aggregation-prefix] quit
```

目 录

1 IPv6 NetStream配置

说明

S5500-28SC-HI 和 S5500-52SC-HI 不支持 IPv6 NetStream 相关配置。

1.1 IPv6 NetStream技术应用背景

IPv6 NetStream 技术应用背景 Internet 的高速发展为用户提供了更高的带宽，支持的业务和应用日渐增多，传统流量统计如 SNMP、端口镜像等，由于统计流量方式不灵活或是需要投资专用服务器成本高等原因，无法满足对网络进行更细致的管理，需要一种新技术来更好的支持网络流量统计。

IPv6 NetStream 技术是一种基于网络流信息的统计技术，可以对网络中的业务流量情况进行统计和分析。在网络的接入层、汇聚层、核心层上，都可以部署 IPv6 NetStream。

IPv6 NetStream 技术的应用有以下几种。

- 计费：IPv6 NetStream 为基于资源（如线路、带宽、时段等）占用情况的计费提供了精细的数据。ISP（Internet Service Provider，互联网服务提供商）可以利用这些信息来实行灵活的计费策略，如基于时间、带宽、应用、服务质量等。企业客户可以使用这些信息计算部门费用或分配成本，以便有效利用资源。
- 网络规划：IPv6 NetStream 可以为网络管理工具提供关键信息，比如各设备之间的网络流量情况，以便优化网络设计和规划，实现以最小的网络运营成本达到最佳的网络性能和可靠性。
- 网络监控：通过在出口部署 IPv6 NetStream，对连接 Internet 网络的接口进行实时的流量监控，可以分析各种业务占用出口带宽的情况。网管人员可以根据这些信息判断网络的运行情况，尽早发现不合理的网络结构或是网络中的性能瓶颈，方便网管人员规划和分配网络资源。
- 用户监控和分析：通过 IPv6 NetStream 技术可以使网络管理者轻松获取用户使用网络和应用资源的详细情况，进而高效地规划以及分配网络资源，并保障网络的安全运行。

1.2 IPv6 NetStream的基本概念

1.2.1 IPv6 NetStream流定义

IPv6 NetStream 是一项基于“流”来提供报文统计的技术功能。它根据 IPv6 报文的目的 IP 地址、源 IP 地址、目的端口号、源端口号、协议号、流量分类、流标签、输入接口或输出接口来定义流，相同的八元组标识为同一条流。

1.2.2 IPv6 NetStream系统组成

一个典型的 IPv6 NetStream 系统由 NDE（NetStream Data Exporter，网络流数据输出）、NSC（NetStream Collector，网络流数据收集）和 NDA（NetStream Data Analyzer，网络流数据分析）三部分组成。

- NDE

NDE 负责对网络流进行分析处理，提取符合条件的流进行统计，并将统计信息输出给 NSC 设备。输出前也可对数据进行一些处理，比如聚合。配置了 IPv6 NetStream 功能的设备在 IPv6 NetStream 系统中担当 NDE 角色。

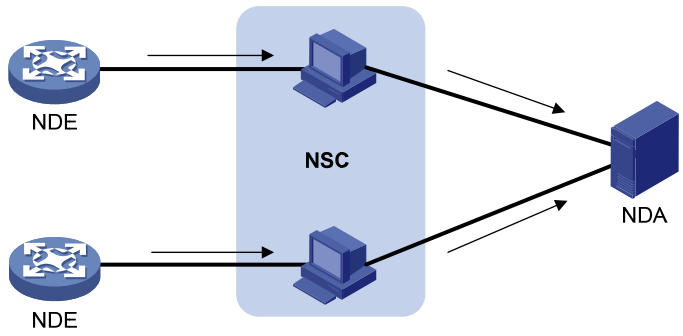
- NSC

NSC 通常为运行于 Unix 或者 Windows 上的一个应用程序，负责解析来自 NDE 的报文，把统计数据收集到数据库中，可供 NDA 进行解析。NSC 可以采集多个 NDE 设备输出的数据。

- NDA

NDA 是一个网络流量分析工具，它从 NSC 中提取统计数据，进行进一步的加工处理，生成报表，为各种业务提供依据（比如流量计费、网络规划，攻击监测）。通常，NDA 具有图形化用户界面，可以使用户方便地获取、显示和分析收集到的数据。

图1-1 IPv6 NetStream 系统中的设备角色



如 图 1-1 所示，IPv6 NetStream进行数据采集和分析的过程如下：

(1) 配置了 IPv6 NetStream 功能的设备（即 NDE）把采集到的关于流的详细信息定期发送给 NSC；

(2) 信息由 NSC 初步处理后发送给 NDA；

(2) NDA 对数据进行分析，以用于计费、网络规划等应用。

说明

- 由于设备在 NetStream 系统中担任 NDE 角色，所以本文档重点介绍 NDE 的实现以及配置。
- NSC 和 NDA 一般集成在一台 NetStream 服务器上。

1.3 IPv6 NetStream关键技术

1.3.1 流老化

IPv6 NetStream 流老化是设备向 NetStream 服务器输出流统计信息的一种手段。当设备启用 IPv6 NetStream 功能后，流统计信息首先会被存储在设备的 IPv6 NetStream 缓冲区中。当存储在设备上的 IPv6 NetStream 流信息老化后，设备会把缓冲区中的流统计信息通过指定版本的 IPv6 NetStream 输出报文发送给 NetStream 服务器。

说明

IPv6 NetStream 流老化采用和 IPv4 NetStream 相同的老化时间，关于流老化的三种方式及其配置请参见“网络管理和监控配置指导”中的“NetStream”。

1.3.2 流输出

1. 普通流输出

普通流输出是指所有流的统计信息都要被统计，并且每条流的统计信息都要输出到 NetStream 服务器。

普通流的优点是：NetStream 服务器可以得到每条流的详细统计信息。但是缺点也是很明显的，这种方式增加了网络带宽和设备的 CPU 占有率，而且为了存储这些信息，需要大量的存储介质空间，而很多情况下，用户并不需要获取所有流的统计信息。

2. 聚合流输出

聚合流输出是指采用聚合流输出功能后，设备对与聚合关键项完全相同的流统计信息进行汇总，从而得到对应的聚合流统计信息，并且将该聚合统计信息发送到相应的接收聚合统计信息的 NetStream 服务器。聚合的最大好处是可以减少对网络带宽的占用。

在目前的实现中，支持 4 种聚合方式，如 表 1-1 所示。系统根据选择聚合方式的聚合关键项，将符合对应聚合方式的多条流合并为一条聚合流，对应一条聚合记录。4 种聚合方式相互独立，可以同时配置。

表1-1 IPv6 NetStream 聚合流输出支持的 4 种方式

聚合方式	聚合关键项
协议-端口聚合（**protocol-port**）	协议号、源端口、目的端口
源前缀聚合（**source-prefix**）	源掩码长度、源前缀、输入接口索引
目的前缀聚合（**destination-prefix**）	目的掩码长度、目的前缀、输出接口索引
源和目的前缀聚合（**prefix**）	源掩码长度、目的掩码长度、源前缀、目的前缀、输入接口索引、输出接口索引

1.3.3 输出报文的版本格式

版本 9 是一种基于模板方式的版本格式，使统计信息的输出更为灵活，可以用来灵活输出各种组合格式的数据。

目前 IPv6 NetStream 输出的统计信息只能使用版本 9 格式。

1.4 IPv6 NetStream配置任务简介

在配置 IPv6 NetStream 之前，可根据以下需求选择相应的配置环节：

- 部署 IPv6 NetStream 的具体位置，也就是明确需要在网络环境中的哪台设备上开启 IPv6 NetStream 功能。
- 根据实际网络情况和需求，对 IPv6 NetStream 的流老化时间进行设置。
- 如果统计输出的报文过多，可以配置聚合输出统计信息，避免重复的流输出信息占用网络带宽。

表1-2 IPv6 NetStream 配置任务简介

配置任务	说明	详细配置
开启IPv6 NetStream功能	必选	1.5

配置任务		说明	详细配置
配置IPv6 NetStream统计信息的输出	配置IPv6 NetStream普通流的统计信息输出	请根据实际需要进行选择	1.6
	配置IPv6 NetStream聚合流的统计信息输出		
配置IPv6 NetStream输出报文的格式		可选	1.7

1.5 开启IPv6 NetStream功能

表1-3 开启 IPv6 NetStream 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口/三层以太网端口视图	**interface** *interface-type interface-number*	-
开启IPv6 NetStream功能	**ipv6 netstream** { **inbound** | **outbound** }	必选 缺省情况下，IPv6 NetStream功能处于关闭状态

1.6 配置IPv6 NetStream统计信息的输出

在配置 IPv6 NetStream 统计信息的输出时，需要对 IPv6 NetStream 统计信息输出的源接口和目的地址进行设置，后者为必选配置。

1.6.1 配置IPv6 NetStream普通流的统计信息输出

表1-4 配置 IPv6 NetStream 普通流的统计信息输出

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图/三层以太网端口视图	**interface** *interface-type interface-number*	-
使能IPv6 NetStream功能	**ipv6 netstream** { **inbound** | **outbound** }	必选 缺省情况下，IPv6 NetStream统计功能处于关闭状态
退回系统视图	**quit**	-
配置IPv6 NetStream普通流统计信息输出的目的地址和目的UDP端口号	**ipv6 netstream export host** *ip-address udp-port* [**vpn-instance** *vpn-instance-name*]	必选 缺省情况下，系统视图下没有配置目的地址和目的UDP端口号
配置IPv6 NetStream统计信息输出的源接口	**ipv6 netstream export source interface** *interface-type interface-number*	可选 缺省情况下，采用统计输出报文的出接口（即与服务器相连的接口）作为源接口 建议使用网管口作为源接口与服务器相连，并向服务器输出统计信息

操作	命令	说明
配置输出速率限制	**ipv6 netstream export rate** *rate*	可选 缺省情况下，IPv6 NetStream统计输出报文的输出速率不受限制

1.6.2 配置IPv6 NetStream聚合流的统计信息输出

设备支持两种聚合方式：软件聚合和硬件聚合。若未配置硬件流聚合功能，则设备会通过软件对与聚合关键项完全相同的流统计信息进行汇总；配置采用硬件流聚合功能后，设备会通过硬件直接对与聚合关键项完全相同的流统计信息进行汇总，从而得到对应的聚合流统计信息。因此通过配置硬件流聚合功能，能够有效降低流聚合对设备资源的消耗。

表1-5 配置 IPv6 NetStream 聚合流的统计信息输出

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图/三层以太网端口视图	**interface** *interface-type interface-number*	-
使能IPv6 NetStream功能	**ipv6 netstream** { **inbound** | **outbound** }	必选 缺省情况下，IPv6 NetStream功能处于关闭状态
退回系统视图	**quit**	-
配置IPv6 NetStream硬件流聚合功能	**ipv6 netstream aggregation advanced**	可选 缺省情况下，NetStream硬件流聚合功能处于关闭状态
进入IPv6 NetStream聚合视图	**ipv6 netstream aggregation** { **destination-prefix** | **prefix** | **protocol-port** | **source-prefix** }	必选
配置IPv6 NetStream聚合统计信息输出的目的地址和目的UDP端口号	**ipv6 netstream export host** *ip-address udp-port* [**vpn-instance** *vpn-instance-name*]	必选 缺省情况下，聚合视图下没有配置目的地址. 和目的UDP端口号。为了减少对网络带宽的占用，可以只在聚合视图下配置**ipv6 netstream export host**命令，此时设备只会输出聚合流信息
配置IPv6 NetStream聚合统计信息输出的源接口	**ipv6 netstream export source interface** *interface-type interface-number*	可选 缺省情况下，采用统计输出报文的出接口（即与服务器相连的接口）作为源接口 • 不同聚合视图下可以配置不同的源接口 • 聚合视图下若没有配置源接口，则使用系统视图下的配置 • 建议使用网管口作为源接口与服务器相连，并向服务器输出统计信息
使能该类的IPv6 NetStream聚合功能	**enable**	必选 缺省情况下，IPv6 NetStream聚合功能处于关闭状态

说明

- 硬件流聚合不能和系统视图下的 **ipv6 netstream export host** 同时配置。在系统视图下配置的 **ipv6 netstream export host** 命令后硬件聚合功能失效。
- 硬件聚合流表项的老化与普通流表项的老化相同。
- 在聚合视图下，用户配置的 IPv6 NetStream 统计输出报文的输出属性，仅对聚合报文生效；而系统视图下的配置对普通报文生效，并且当聚合视图下没有配置以上属性时，也会对聚合报文生效。

1.7 配置IPv6 NetStream输出报文的属性

表1-6 配置 IPv6 NetStream 输出报文的属性

操作	命令	说明
进入系统视图	**system-view**	-
配置IPv6 NetStream统计输出报文版本9模板的包刷新率	**ipv6 netstream export v9-template refresh-rate packet** *packets*	可选 缺省情况下，每隔20个包发送一次模板
配置IPv6 NetStream统计输出报文版本9模板的时间刷新率	**ipv6 netstream export v9-template refresh-rate time** *minutes*	可选 缺省情况下，每隔30分钟发送一次模板

注意

- 由于 V9 版本是基于模板方式的、可支持自定义格式，所以设备上需要定期刷新模板，通知 NetStream 服务器最新的 V9 模版格式。用户可以根据实际情况，配置版本 9 模板的刷新率，及时更新模板。
- 可以同时配置包刷新率和时间刷新率，只要满足任意一个刷新条件，设备会发送模板给 NetStream 服务器。

1.8 IPv6 NetStream显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 IPv6 NetStream 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 IPv6 NetStream 的统计信息。

表1-7 IPv6 NetStream 显示和维护

操作	命令
查看IPv6 NetStream流缓存区的配置和状态信息	**display ipv6 netstream cache** [**verbose**] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
查看IPv6 NetStream统计输出报文信息	**display ipv6 netstream export** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

操作	命令
查看IPv6 NetStream模板的配置和状态信息	**display ipv6 netstream template** [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
将流缓存区中所有流强制老化，并清除IPv6 NetStream缓冲区的状态信息和输出报文信息	**reset ipv6 netstream statistics**

1.9 IPv6 NetStream典型配置举例

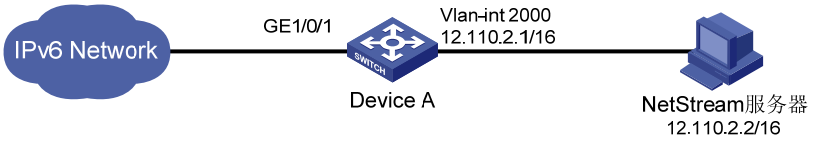
1.9.1 IPv6 NetStream普通流的统计信息输出配置举例

1. 组网需求

如图所示，在 Device A 上配置 IPv6 NetStream，对接收的报文进行统计，并将 IPv6 NetStream 普通流的统计信息输出到 NetStream 服务器。NetStream 服务器的 IP 地址为 12.110.2.2/16，UDP 端口号为 5000。

2. 组网图

图1-2 IPv6 NetStream 普通流的统计信息输出配置组网图



3. 配置步骤

在端口 GigabitEthernet1/0/1 上启用 NetStream 入统计功能。

```
<DeviceA> system-view
[DeviceA] ipv6
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ipv6 netstream inbound
[DeviceA-GigabitEthernet1/0/1] quit
```

在 VLAN 接口 2000 上配置 IP 地址。

```
[DeviceA] vlan 2000
[DeviceA-vlan2000] quit
[DeviceA] interface vlan-interface 2000
[DeviceA-Vlan-interface2000] ip address 12.110.2.1 255.255.0.0
[DeviceA-Vlan-interface2000] quit
```

配置 IPv6 NetStream 普通流统计信息输出的目的地址。

```
[DeviceA] ipv6 netstream export host 12.110.2.2 5000
```

1.9.2 IPv6 NetStream聚合流的统计信息输出配置举例

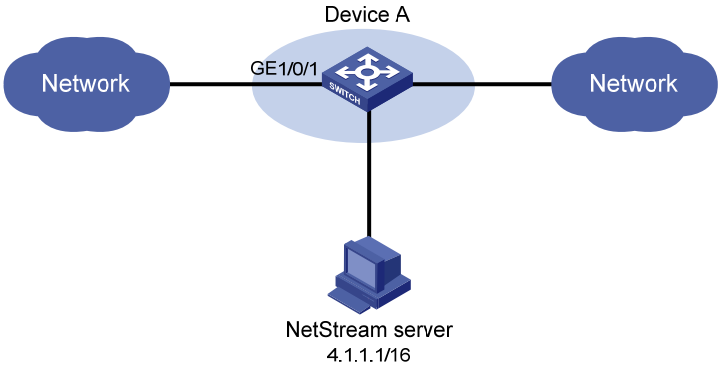
1. 组网需求

在 Device A 上配置 IPv6 NetStream，具体要求为：

- 普通流的统计信息使用输出到 NetStream 服务器。NetStream 服务器的 IP 地址为 4.1.1.1/16，UDP 端口号为 5000；
- 4 种聚合流（**protocol-port**、**source-prefix**、**destination-prefix** 和 **prefix**）的统计信息输出到该 NetStream 服务器的 3000、4000、6000 和 7000 端口。

2. 组网图

图1-3 IPv6 NetStream 聚合流的统计信息输出配置组网图



3. 配置步骤

配置端口 GigabitEthernet1/0/1，在出、入方向启动 NetStream 统计。

```
<DeviceA> system-view
[DeviceA] ipv6
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ipv6 netstream inbound
[DeviceA-GigabitEthernet1/0/1] ipv6 netstream outbound
[DeviceA-GigabitEthernet1/0/1] quit
```

配置普通流统计信息输出的目的地址。

```
[DeviceA] ipv6 netstream export host 4.1.1.1 5000
```

配置协议—端口聚合模式，以及该聚合流统计信息输出的目的地址。

```
[DeviceA] ipv6 netstream aggregation protocol-port
[DeviceA-ns6-aggregation-protport] ipv6 netstream export host 4.1.1.1 3000
[DeviceA-ns6-aggregation-protport] enable
[DeviceA-ns6-aggregation-protport] quit
```

配置源前缀聚合模式，以及该聚合流统计信息输出的目的地址。

```
[DeviceA] ipv6 netstream aggregation source-prefix
[DeviceA-ns6-aggregation-srcpre] ipv6 netstream export host 4.1.1.1 4000
[DeviceA-ns6-aggregation-srcpre] enable
[DeviceA-ns6-aggregation-srcpre] quit
```

配置目的前缀聚合模式，以及该聚合流统计信息输出的目的地址。

```
[DeviceA] ipv6 netstream aggregation destination-prefix
[DeviceA-ns6-aggregation-dstpre] ipv6 netstream export host 4.1.1.1 6000
[DeviceA-ns6-aggregation-dstpre] enable
[DeviceA-ns6-aggregation-dstpre] quit
```

配置前缀聚合模式，以及该聚合流统计信息输出的目的地址。

```
[DeviceA] ipv6 netstream aggregation prefix
[DeviceA-ns6-aggregation-prefix] ipv6 netstream export host 4.1.1.1 7000
[DeviceA-ns6-aggregation-prefix] enable
[DeviceA-ns6-aggregation-prefix] quit
```

目 录

1 Sampler配置

说明

S5500-28SC-HI 和 S5500-52SC-HI 不支持 Sampler 相关配置。

1.1 Sampler简介

Sampler 即报文采样功能，用来从一组固定数量的报文中选出一个报文，送交后续业务模块处理。Sampler 支持固定采样和随机采样两种方式：

- 固定采样：每组报文中的第一个报文被选中。
- 随机采样：每组报文中，任意一个报文都有可能被选中。

目前 Sampler 可以和 NetStream 达到以下目的：

- 对网络流量先进行采样，然后将采样后的流量发送给流量监控系统进行流量统计。通过设定适当的采样间隔，在减少统计的报文数量的前提下，同样可以使流量监控系统收集到的统计信息能基本反映整个网络的状况。
- 通过采样可以减少网络的流量，避免网络中的大流量对设备转发性能造成影响。

说明

- 有关 NetStream 的详细介绍，请参见“网络管理和监控配置指导”中的“NetStream”。
- 本系列交换机仅支持固定采样模式。

1.2 创建采样器

表1-1 创建采样器功能

操作	命令	说明
进入系统视图	**system-view**	-
创建采样器	**sampler** *sampler-name* **mode fixed packet-interval** *rate*	必选 需要注意的是，参数*rate*表示采样率，按照2的rate次方进行计算。例如，该参数设为8，表示在256（2的8次方）个报文中采样1个报文；该参数设为10，表示在1024（2的10次方）个报文中采样1个报文。

1.3 Sampler显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 Sampler 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 Sampler 的统计信息。

表1-2 Sampler 显示和维护

操作	命令
查看Sampler配置和运行信息	**display sampler** [*sampler-name*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.4 Sampler典型配置举例

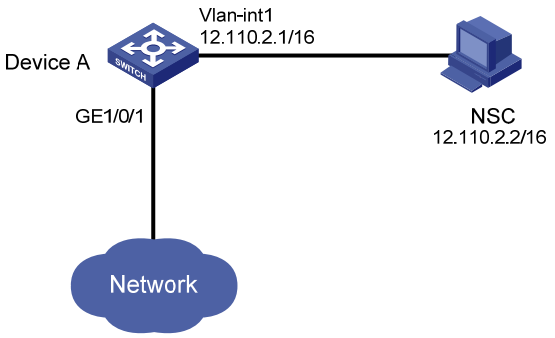
1.4.1 Sampler与NetStream配合使用

1. 组网需求

如 图 1-1 所示，在Device A上配置IPv4 NetStream入统计，并将统计结果发送到NSC 12.110.2.2/16 的 5000 端口。要求入方向采用固定采样，每 256 个报文选中一个进行NetStream统计。

2. 组网图

图1-1 Sampler 与 NetStream 配合使用组网图



3. 配置步骤

(1) 配置 Device A

创建一个名为 256 的采样器，采用固定采样方式，设置采样率为 8，即 256（2 的 8 次方）个报文中采样 1 个报文。

```
<DeviceA> system-view
[DeviceA] sampler 256 mode fixed packet-interval 8
```

配置 GigabitEthernet1/0/1，在此端口上启动 IPv4 NetStream 入统计并使用采样器 256。

```
[DeviceA] interface GigabitEthernet1/0/1
[DeviceA-GigabitEthernet1/0/1] ip netstream inbound
[DeviceA-GigabitEthernet1/0/1] ip netstream sampler 256 inbound
[DeviceA-GigabitEthernet1/0/1] quit
```

配置 IPv4 NetStream 统计输出报文的目的 IP 地址和目的端口（即 NSC 的地址以及端口），源接口采用缺省配置。

```
[DeviceA] ip netstream export host 12.110.2.2 5000
```

目 录

1 IPC配置

1.1 IPC简介

1.1.1 IPC概述

IPC（Inter-process Communication，进程间通信）是不同节点间的一种可靠通讯机制。下面先介绍 IPC 模块的基本概念。

1. 节点

节点指的是支持 IPC 通信的物理实体，是一个独立的处理单元。在实际应用中，一般情况下，一个节点对应于一个 CPU。

- 集中式设备只有一个 CPU，因此，集中式设备对应一个节点；
- 分布式设备一般配有多个单板，每个单板都有一个 CPU，甚至一块单板有多个 CPU（比如业务 CPU 和 OAM CPU 等），因此，分布式设备是多个节点的集合；
- IRF 是多台设备的互联形成的虚拟设备，每一个成员设备对应一个或多个节点，因此，IRF 是多个节点的集合。

因此，在具体应用中，IPC 主要应用于 IRF 和分布式设备，它为不同的设备之间、不同的单板之间提供了一种可靠的传输机制。

2. 链路

链路就是两个节点之间的连接。它可以存在于任意两个 IPC 节点之间，任意两个节点之间有且仅有一条链路用于收发报文。链路基于节点而存在，各节点间的链路是全连接结构。

链路在系统初始化时创建：节点启动时，会主动同其它节点进行握手，如果握手成功，会建立连接。

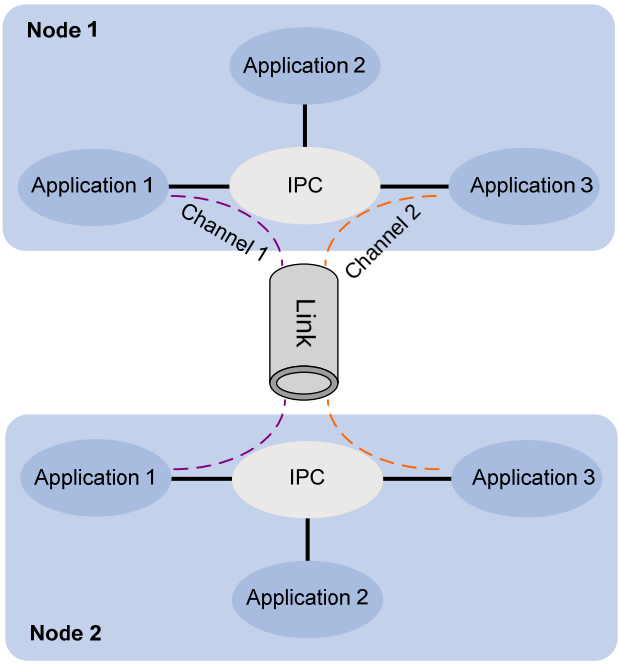
系统用链路状态来表示两个节点之间链路的连通情况。一个 IPC 节点可以有多条链路，每条链路都有对应的状态。

3. 通道

通道是不同节点的上层应用模块之间的通信接口。每个节点会给上层应用模块分配一个本地唯一的通道号来标志该模块。

上层应用模块的数据通过通道将数据发送给IPC模块，IPC模块通过底层的链路将数据发送给对端节点。节点、链路和通道之间的关系请参见 图 1-1。

图1-1 节点、链路和通道关系图



4. 报文发送方式

IPC 有三种报文发送方式：单播、组播（广播被视为特殊的组播）和混播，每种发送方式都有对应的队列，上层应用模块可以根据需要自动选择其中的任何一种方式。

- 单播即单个节点对单个节点的发送方式。
- 组播即单个节点对多个节点的发送方式。当选择组播发送方式的时候，需要先创建一个组播组，组播报文会发送到这个组播组内的所有节点。一个应用模块可以创建多个组播组，组播组何时创建/删除以及组播组的成员由应用模块决定。
- 混播，即同时支持单播和组播的发送方式。

1.2 开启IPC性能统计功能

开启 IPC 性能统计功能后，系统将统计节点在指定时间段内（最近 10 秒、最近 1 分钟等）收发报文的情况，通过 **display** 命令可以查看这些信息。关闭性能统计开关后，将停止统计，统计数据将不再发生变化。此时，如果使用 **display** 命令，显示的将是开关关闭时刻的统计数据。

表1-1 开启 IPC 性能统计功能

操作	命令	说明
打开IPC性能统计开关	**ipc performance enable** { **node** *node-id* | **self-node** } [**channel** *channel-id*]	必选 缺省情况下，IPC性能统计开关是关闭的 该操作在用户视图下执行

1.3 IPC显示和维护

完成上述配置后，在任意视图下执行 **display** 命令可以显示 IPC 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可以清除相关统计信息。

表1-2 IPC 显示和维护

操作	命令
显示IPC节点信息	**display ipc node** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示节点的通道信息	**display ipc channel** { **node** *node-id* | **self-node** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示节点的队列信息	**display ipc queue** { **node** *node-id* | **self-node** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示节点的组播组信息	**display ipc multicast-group** { **node** *node-id* | **self-node** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示节点的报文信息	**display ipc packet** { **node** *node-id* | **self-node** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示节点的链路状态信息	**display ipc link** { **node** *node-id* | **self-node** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示节点的性能统计信息	**display ipc performance** { **node** *node-id* | **self-node** } [**channel** *channel-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除节点的性能统计信息	**reset ipc performance** [**node** *node-id* | **self-node**] [**channel** *channel-id*]

目　录

1 PoE配置

1.1 PoE简介

1.1.1 PoE概述

PoE（Power over Ethernet，以太网供电，又称远程供电）是指设备通过以太网电口，利用双绞线对外接 PD（Powered Device，受电设备）进行远程供电。

1. PoE的优点

- 可靠：电源集中供电，备份方便；
- 连接简捷：网络终端不需外接电源，只需要一根网线；
- 标准：符合 IEEE 802.3af 和 802.3at 标准，使用全球统一的电源接口；
- 应用前景广泛：可以用于 IP 电话、无线 AP（Access Point，接入点）、便携设备充电器、刷卡机、网络摄像头、数据采集等。

2. PoE相关概念

PoE系统如 图 1-1 所示，包括PoE电源、PSE（Power Sourcing Equipment，供电设备）、PI（Power Interface，电源接口）和PD。

(1) PoE 电源为整个 PoE 系统提供功率。

(2) PSE：直接给 PD 供电的设备。PSE 分为内置（Endpoint）和外置（Midspan）两种：内置指的是 PSE 集成在设备内部，外置指的是 PSE 与设备相互独立。本系列设备 PSE 均采用内置方式，系统使用 PSE ID 来识别不同 PSE，使用 **display poe device** 命令可以查看 PSE ID 和成员设备的对应关系。PSE 支持的主要功能包括寻找、检测 PD，对 PD 分类，并向其供电，进行功率管理，实时监控，检测与 PD 的连接是否断开等。

说明

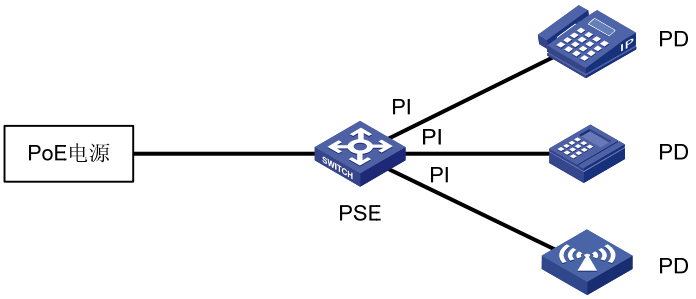
PSE ID 的计算方法为：设备的成员编号 × 3 + 1，例如：设备的成员编号为 3，其 PSE ID 为 3 × 3 + 1 = 10。

---

(3) PI：具备 PoE 供电能力的以太网端口，也称为 PoE 接口。

(4) PD：接受 PSE 供电的设备，如 IP 电话、无线 AP（Access Point，接入点）、便携设备充电器、刷卡机、网络摄像头等。PD 设备在接受 PoE 电源供电的同时，可以连接其它电源，进行电源冗余备份。

图1-1 PoE 系统示意图



1.1.2 协议规范

与 PoE 相关的协议规范为：IEEE 802.3af、802.3at。

1.2 PoE配置任务简介

配置 PoE 接口有两种方式：

- 通过命令行配置；
- 通过配置 PoE Profile，并将 PoE Profile 应用到指定的 PoE 接口。

两种方式的作用一样，可以根据具体的需求选择：配置单独 PoE 接口时，一般采用命令行配置；而批量配置 PoE 接口时，一般采用 PoE Profile 配置。对于同一 PoE 接口下的同一 PoE 配置参数，只能选择一种方式进行配置（包括修改和删除）。

表1-1 PoE 配置任务简介

配置任务		说明	详细配置
使能PoE功能	使能PoE接口的PoE功能	必选	1.3.1
检测PD	使能非标准PD检测功能	可选	1.4.1
配置PoE功率	配置PoE接口的最大功率	可选	1.5.1
配置PoE功率管理	配置PoE接口功率管理	可选	1.6.1
PoE监控功能	监控PSE	可选	1.7.1
	监控PD	可选 设备给PD供电时会自动监控PD，不需要通过命令行来配置	1.7.2
通过PoE Profile配置PoE接口	定义PoE Profile的内容	可选	1.8.1
	应用PoE Profile	可选	1.8.2
在线升级PSE处理软件		可选	1.9

注意

- 在配置 PoE 功能前，请确保 PoE 电源和 PSE 已经处于正常工作状态，否则，可能无法进行 PoE 配置或者配置的 PoE 功能不能生效；
- 如果在设备启动过程中不慎关闭 PoE 电源，可能会导致 PoE Profile 中的 PoE 配置无法生效。

1.3 使能PoE功能

1.3.1 使能PoE接口的PoE功能

如果没有使能 PoE 接口的 PoE 功能，系统不会给 PoE 接口下挂的 PD 供电，也不会给 PD 预留功率。

使能PoE接口的PoE功能时，如果该PoE接口的加入不会导致PSE功率过载，则允许使能。否则，由该PoE接口是否使能PoE功率管理功能决定（PoE接口功率管理的详细介绍请参见 1.6.1 配置PoE接口功率管理）：

- 如果该 PoE 接口没有使能 PoE 功率管理功能，则不允许使能该 PoE 接口的 PoE 功能；
- 如果该 PoE 接口已经使能了 PoE 功率管理功能，则允许使能该 PoE 接口的 PoE 功能（使能后 PD 是否能够获得供电由其它因素决定，比如 PoE 接口的供电优先级）。

PoE 接口远程供电有两种模式：

- 信号线供电模式：PSE 使用 3/5 类双绞线中传输数据所用的线对（1、2、3、6）向 PD 传输数据的同时传输直流电。
- 空闲线供电模式：PSE 使用 3/5 类双绞线中没有被使用的线对（4、5、7、8）向 PD 来传输直流电。

说明

- PSE 功率过载：当 PSE 上已经获得供电的端口的最大功率之和大于 PSE 最大功率时，系统将认为 PSE 功率过载（PSE 最大功率由用户的配置决定）。
- PSE 和 PD 必须使用相同的模式，才能正常供电。如果 PSE 和 PD 支持的供电模式不同（比如 PSE 不支持空闲线供电式，PD 只支持空闲线供电），则需要转接才能给 PD 供电。
- 本系列设备 PoE 接口仅支持使用信号线供电模式为 PD 设备进行远程供电。

表1-2 使能 PoE 接口的 PoE 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入PoE接口视图	**interface** *interface-type interface-number*	-
使能PoE接口远程供电功能	**poe enable**	必选 缺省情况下，PoE接口远程供电功能为禁用状态
配置PoE接口连接PD的描述信息	**poe pd-description** *text*	可选 缺省情况下，PoE接口连接PD的描述信息为空，即没有描述信息

1.4 检测PD

1.4.1 使能非标准PD检测功能

PD 设备分为标准 PD 和非标准 PD，标准 PD 是指符合 IEEE 802.3af 标准的 PD 设备。通常情况下，PSE 只能检测到标准 PD，并为其供电。只有在使能 PSE 检测非标准 PD 功能后，PSE 才能检测到非标准 PD，并为其供电。

表1-3 使能 PSE 检测非标准 PD 功能

操作	命令	说明
进入系统视图	**system-view**	-
使能PSE检测非标准PD功能	**poe legacy enable pse** *pse-id*	必选 缺省情况下，PSE只能检测到标准PD，不能检测非标准PD

1.5 配置PoE功率

1.5.1 配置PoE接口的最大功率

PoE 接口的最大功率指的是 PoE 接口能够提供给下挂 PD 的最大功率。当 PD 要求的功率大于 PoE 接口的最大功率时，则不会给 PD 供电。

表1-4 配置 PoE 接口的最大功率

操作	命令	说明
进入系统视图	**system-view**	-
进入PoE接口视图	**interface** *interface-type interface-number*	-
配置PoE接口的最大供电功率	**poe max-power** *max-power*	可选 缺省情况下，PoE接口最大供电功率为30000毫瓦

1.6 PoE功率管理

PoE 功率管理分为两个部分：PSE 功率管理和 PoE 接口功率管理。

1.6.1 配置PoE接口功率管理

PD 供电优先级取决于 PoE 接口的优先级。PoE 接口的优先级按照高低顺序为：Critical、High 和 Low。PD 能否得到供电要受 PoE 接口功率管理策略的控制。

所有 PSE 都执行相同的 PoE 接口功率管理策略。PSE 对接入的 PD 设备进行供电时：

- 在没有使能 PoE 接口功率管理的情况下，如果 PSE 功率过载，则不对新接入的 PD 供电；
- 在使能 PoE 接口功率管理优先级策略的情况下，如果 PSE 功率过载，接入新的 PD，将对优先级低的 PD 断电，保证优先级高的 PD 供电。

说明

- 设备给每个 PoE 接口预设了 19W 的保护功率，以便适应 PD 设备的功率波动，从而防止由于 PD 的瞬间功率过大而导致 PD 断开。当接口所在 PSE 剩余功率小于 19W，而且 PoE 接口没有配置优先级时，将不能给新增的 PD 供电；当接口所在 PSE 剩余功率小于 19W，但 PoE 接口配置了优先级时，高优先级端口将抢占低优先级端口的功率，优先保证高优先级端口的正常工作。
- 如果已接入的 PD 功率突然增加，造成 PSE 功率过载时，将停止对连接在低优先级 PoE 接口上的 PD 的供电，以便保证给优先级高的 PD 供电。

当 PSE 剩余保证功率（PSE 最大功率减去该 PSE 中优先级为 Critical 的 PoE 接口的最大功率，与 PoE 接口是否使能 PoE 功能无关）小于该 PoE 接口最大功率时，设置 Critical 优先级不成功；否则，该 PoE 接口优先级成功设为 Critical，并将抢占部分低优先级 PD 的功率，被抢占的 PD 断电，但是这些 PoE 接口的配置不变。将某个 PoE 接口的优先级从 Critical 降为其它优先级，可能导致其它 PoE 接口的 PD 得到供电。

1. 配置准备

使能 PoE 接口远程供电功能。

2. 配置PoE接口功率管理

表1-5 配置 PoE 接口功率管理

操作	命令	说明
进入系统视图	**system-view**	-
使能PoE接口功率管理优先级策略	**poe pd-policy priority**	必选 缺省情况下，没有使能PoE接口功率管理优先级策略
进入PoE接口视图	**interface** *interface-type interface-number*	-
配置PoE接口供电优先级	**poe priority** { **critical** | **high** | **low** }	可选 缺省情况下，PoE接口供电优先级为**low**

1.7 PoE监控功能

当使能 PoE 监控功能后，系统就会实时监控一些参数的值，当这些值超出限定范围时，系统会自动采取一些措施来进行自我保护。PoE 监控功能包括对 PoE 电源、PSE 和 PD 的监控以及对设备温度的监控。

1.7.1 监控PSE

当 PSE 在当前功率利用率首次超过或低于设置的功率阈值时，系统会发送 Trap 告警信息。

表1-6 配置 PSE 的功率告警阈值

操作	命令	说明
进入系统视图	**system-view**	-
配置PSE的功率告警阈值	**poe utilization-threshold** *utilization-threshold-value* **pse** *pse-id*	可选 缺省情况下，PSE的功率告警阈值为80%

1.7.2 监控PD

当 PSE 开始或终止给 PD 供电时，系统会发送 Trap 信息。

1.8 通过PoE Profile配置PoE接口

配置 PoE 接口有两种方式，两种方式的作用一样，可以根据具体的需求选择，具体方式为：

- 通过命令行配置。该方式通常用于对单个 PoE 端口的配置。
- 通过 PoE Profile 配置，并将 PoE Profile 应用到指定的 PoE 接口。该方式通常用于批量配置 PoE 接口，可以简化用户的操作。

PoE Profile 是一组配置的集合，一个 PoE Profile 中可以配置多个 PoE 特性。在用大型网络中，将 PoE Profile 应用到多个 PoE 接口，则这些接口就具有相同的 PoE 特性；如果 PD 的接入接口变更，则把原接口上应用的 PoE Profile 应用到新的接入接口即可，不再需要重新逐条配置，从而方便了网管人员对 PoE 特性的配置。

设备支持创建多个 PoE Profile，针对不同 PD 定义不同的 PoE 配置存放在不同的 PoE Profile 中，并在 PD 的接入接口应用相应的 PoE Profile 即可。

1.8.1 定义PoE Profile的内容

表1-7 定义 PoE Profile 的内容

操作	命令	说明
进入系统视图	**system-view**	-
创建PoE Profile，并进入PoE Profile视图	**poe-profile** *profile-name* [*index*]	必选
使能PoE接口远程供电功能	**poe enable**	必选 缺省情况下，PoE接口远程供电功能处于禁用状态
配置PoE接口的最大供电功率	**poe max-power** *max-power*	可选 缺省情况下，PoE接口最大供电功率为30000毫瓦
配置PoE接口供电优先级	**poe priority** { **critical** | **high** | **low** }	可选 缺省情况下，PoE接口供电优先级为**low**

注意

- 如果 PoE Profile 已经应用，必须先取消 PoE Profile 的应用后，才能删除或修改该 PoE Profile。
- 命令 **poe max-power** *max-power* 和 **poe priority** { **critical** | **high** | **low** }必须保证用同一种方式配置，即只能通过命令行配置或只能通过 PoE Profile 配置。
- 对于同一 PoE 接口下的同一 PoE 配置参数，只能选择一种方式进行配置（包括修改和删除），先配置的生效。如果对命令行已经配置过的参数再通过 PoE Profile 配置，则 PoE Profile 会应用失败；如果对 PoE Profile 已经配置过的参数再通过命令行配置，则命令行执行失败。必须先取消现有配置，新的配置才能成功。

1.8.2 应用PoE Profile

应用 PoE Profile 有两种方式：方式一是在系统视图下应用 PoE Profile，方式二是在接口视图下应用 PoE Profile。两种方式配置效果一样，后配置的生效。如果需要将 PoE Profile 应用到多个 PoE 接口，使用方式一更为简便。

表1-8 应用 PoE Profile（方式一）

操作	命令	说明
进入系统视图	**system-view**	-
将PoE Profile应用到指定一个或多个PoE接口	**apply poe-profile** { **index** *index* | **name** *profile-name* } **interface** *interface-range*	必选

表1-9 应用 PoE Profile（方式二）

操作	命令	说明
进入系统视图	**system-view**	-
进入PoE接口视图	**interface** *interface-type interface-number*	-
将PoE Profile应用到当前PoE接口	**apply poe-profile** { **index** *index* | **name** *profile-name* }	必选

注意

PoE Profile 可以应用于多个 PoE 接口，但一个 PoE 接口下只能应用一个 PoE Profile。

1.9 在线升级PSE处理软件

用户可以通过以下操作在线升级 PSE 处理软件，在线升级指的是不用重启 PSE 就能完成升级。升级有两种模式：

- refresh 模式，该模式是在 PSE 中原有处理软件的基础上对其进行升级更新。一般情况下使用 refresh 模式来升级 PSE 处理软件。

- full 模式，该模式是将 PSE 中原有处理软件彻底删除，再重新装入。PSE 处理软件被损坏的情况下（表现为所有的 PoE 命令执行不成功），可用 full 模式进行升级，使软件恢复。

如果 PSE 处理软件的升级过程因意外而中断（例如发生错误导致设备重启），重启后用 full 方式升级失败时，请将设备断电重启后再用 full 方式升级即可成功。升级后重启设备，新的 PSE 处理软件就会生效。

表1-10 在线升级 PSE 处理软件

操作	命令	说明
进入系统视图	**system-view**	-
升级PSE处理软件	**poe update** { **full** | **refresh** } *filename* **pse** *pse-id*	必选

1.10 PoE显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 PoE 的运行情况，通过查看显示信息验证配置的效果。

表1-11 PoE 显示和维护

操作	命令
显示所有PSE的相关信息	**display poe device** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示设备指定PoE接口的供电状态	**display poe interface** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示PoE接口的功率信息	**display poe interface power** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示PSE信息	**display poe pse** [*pse-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示PSE连接的所有PoE接口的供电状态	**display poe pse** *pse-id* **interface** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示PSE连接的PoE接口的功率信息	**display poe pse** *pse-id* **interface power** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示PoE Profile的配置和应用的所有信息	**display poe-profile** [**index** *index* | **name** *profile-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示指定PoE接口当前生效的PoE Profile配置项和应用的所有信息	**display poe-profile interface** *interface-type interface-number* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.11 PoE典型配置举例

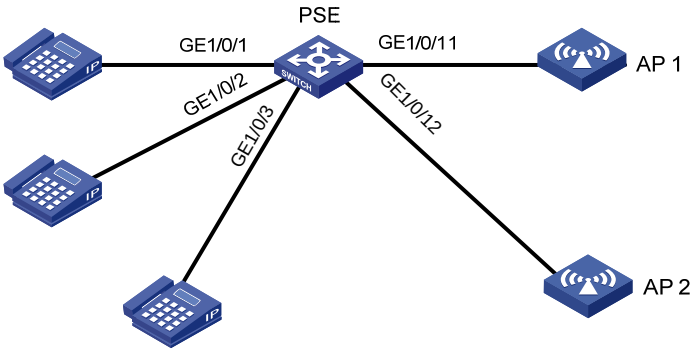
1. 组网需求

- GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 接入 IP 电话。

- GigabitEthernet1/0/11、GigabitEthernet1/0/12 接入 AP 设备。
- IP 电话的供电优先级高于 AP 设备，当 PSE 功率过载时，优先给 IP 电话供电。
- GigabitEthernet1/0/12 下接的 AP 2 的功率最大不能超过 9000 毫瓦。

2. 组网图

图1-2 PoE 组网图



3. 配置步骤

使能 PoE 接口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 的远程供电功能，并且供电优先级为 critical。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe enable
[Sysname-GigabitEthernet1/0/1] poe priority critical
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] poe enable
[Sysname-GigabitEthernet1/0/2] poe priority critical
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] poe enable
[Sysname-GigabitEthernet1/0/3] poe priority critical
[Sysname-GigabitEthernet1/0/3] quit
```

使能 PoE 接口 GigabitEthernet1/0/11 和 GigabitEthernet1/0/12 的远程供电功能，并配置 PoE 接口 GigabitEthernet1/0/12 的最大供电功率为 9000 毫瓦。

```
[Sysname] interface gigabitethernet 1/0/11
[Sysname-GigabitEthernet1/0/11] poe enable
[Sysname-GigabitEthernet1/0/11] quit
[Sysname] interface gigabitethernet 1/0/12
[Sysname-GigabitEthernet1/0/12] poe enable
[Sysname-GigabitEthernet1/0/12] poe max-power 9000
```

配置完成后，IP 电话和 AP 设备被供电，能够正常工作。

1.12 常见配置错误举例

1.12.1 配置PoE接口优先级为critical不成功

1. 原因分析

- PoE 接口所在 PSE 剩余保证功率小于 PoE 接口的最大供电功率。
- PoE 接口的优先级已经通过其他方式进行配置。

2. 解决方法

- 对于第一种情况可以通过增大 PSE 的最大供电功率来解决，或者在 PSE 剩余保证功率不可调整时减小 PoE 接口的最大供电功率。
- 对于第二种情况需先取消其他方式的配置。

1.12.2 应用PoE Profile到PoE接口不成功

1. 原因分析

- 该 PoE Profile 的某些配置项已经通过其他方式进行配置。
- 该 PoE Profile 的某些配置项不符合 PoE 接口的配置要求。
- 已经存在 PoE Profile 在该 PoE 接口的应用。

2. 解决方法

- 对于第一种情况，可以通过取消其他方式的配置来解决。
- 对于第二种情况，需修改该 PoE Profile 的某些配置项。
- 对于第三种情况，先取消其他 PoE Profile 在该 PoE 接口的应用。

目 录

1 集群管理配置

说明

设备运行于 FIPS 模式时，不支持集群管理功能。有关 FIPS 模式的详细介绍请参见“安全配置指导”中的“FIPS”。

1.1 集群管理简介

随着网络规模的增加，网络边缘需要使用大量的接入设备，这使对这些设备的管理工作非常繁琐，同时要为这些设备逐一配置 IP 地址，在目前 IP 地址资源日益紧张的情况下无疑也是一种浪费，而集群管理则可以解决上述问题。

集群（Cluster）是指一组网络设备的集合，集群管理的主要目的就是解决大量分散的网络设备的集中管理问题，其具有以下优点：

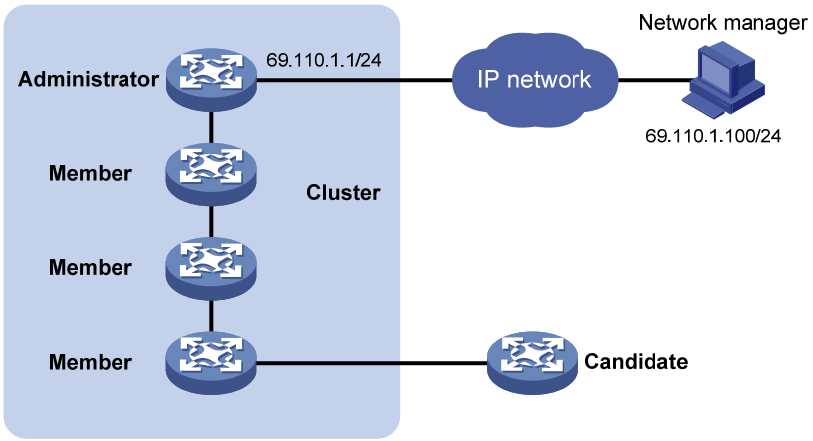
- 节省公网 IP 地址。
- 简化配置管理任务。网络管理员只需在一台设备上配置公网 IP 地址就可实现对集群中所有设备的管理和维护，而无需登录到每台设备上进行配置。
- 提供拓扑发现和显示功能，有助于监视和调试网络。
- 可同时对多台设备进行软件升级和参数配置，且不受网络拓扑和距离限制。

1.1.1 集群角色

根据在集群中所处的地位和功能的不同，可把集群中的设备分为以下三种角色：

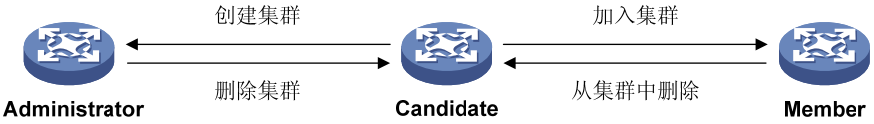
- 管理设备（Administrator）：在集群中对整个集群管理发挥接口作用的设备，也是集群中唯一配置公网 IP 地址的设备。每个集群必须（且只能）指定一个管理设备。对集群中的其它设备进行配置、管理和监控都必须通过管理设备来进行，管理设备通过收集相关信息来发现和确定候选设备。
- 成员设备（Member）：在集群中处于被管理状态的设备。
- 候选设备（Candidate）：指没有加入任何集群但具备集群能力、能够成为集群成员的设备。它与成员设备的区别在于：其拓扑信息已被管理设备收集到但尚未加入集群。

图1-1 集群典型组网图



如 图 1-1 所示，配置有公网IP地址并执行管理功能的设备就是管理设备，其它被管理的设备是成员设备，尚未加入任何集群但具备集群能力的设备是候选设备。由管理设备和成员设备共同组成了一个集群。

图1-2 集群角色转换示意图



如 图 1-2 所示，各角色可按如下规则相互转换：

- 当在某候选设备上创建集群时，该设备就成为了这个集群的管理设备；管理设备只有在删除集群时才能恢复为候选设备。
- 当把某候选设备加入到集群中后，该设备便成为成员设备；当从集群中删除某成员设备后，该设备又恢复为候选设备。

1.1.2 集群工作原理

集群管理通过 HGMPv2（HW Group Management Protocol version 2，HW 组管理协议版本 2）来实现，它由以下三个协议组成：

- NDP（Neighbor Discover Protocol，邻居发现协议）
- NTDP（Neighbor Topology Discover Protocol，邻居拓扑发现协议）
- Cluster（集群管理协议）

集群通过以上三个协议，对集群内部的设备进行配置和管理，其工作过程包括拓扑收集以及集群的建立和维护。拓扑收集过程和集群维护过程相对独立，拓扑收集过程在集群建立之前就开始启动，工作原理如下：

- 所有设备通过 NDP 来获取邻居设备的信息，包括邻居设备的软件版本、主机名、MAC 地址和端口名称等信息。
- 管理设备通过 NTDP 来收集用户指定跳数范围内的设备信息以及各个设备的连接信息，并从收集到的拓扑信息中确定集群的候选设备。
- 管理设备根据 NTDP 收集到的候选设备信息完成将候选设备加入集群、成员设备离开集群的操作。

1. NDP简介

NDP 用来获取直接相连的邻居设备的信息，包括连接端口、设备名称、软件版本等信息，工作原理如下：

- 运行 NDP 的设备周期性地向邻居发送 NDP 报文，其中包含 NDP 信息（包括当前设备的名称、软件版本和连接端口等信息）以及 NDP 信息在接收设备上的老化时间。同时会接收（但不转发）邻居设备发送的 NDP 报文。
- 运行 NDP 的设备都会存储和维护 NDP 邻居信息表，在该表中为每台邻居设备创建一个表项。当新发现了一个邻居，即第一次收到它发送的 NDP 报文时，为其新增一个表项。如果收到的邻居设备 NDP 信息与旧信息不同，则更新相应的表项及其老化时间；如果相同，则只更新老化时间；如果老化时间超时后仍未收到邻居的 NDP 信息，将自动删除相应的表项。

NDP 协议运行在数据链路层，因此可以支持不同的网络层协议。

2. NTDP简介

NTDP 为管理设备提供可加入集群的设备信息，收集指定跳数内设备的拓扑信息。NDP 为 NTDP 提供邻接表信息，NTDP 根据邻接信息发送和转发 NTDP 拓扑收集请求，收集一定网络范围内所有

设备的 NDP 信息以及这些设备间的连接信息。收集完这些信息后，管理设备或网管可使用这些信息完成所需功能。

当成员设备上的 NDP 发现邻居有变化时，通过握手报文将邻居改变的消息通知给管理设备，管理设备可以启动 NTDP 收集指定拓扑，从而使 NTDP 能够及时反映网络拓扑的变化。

管理设备可以定时在网络内进行拓扑收集，用户也可以通过手工配置启动一次拓扑收集。管理设备收集拓扑信息过程如下：

- 管理设备从使能 NTDP 的端口周期性发送 NTDP 拓扑收集请求报文。
- 收到请求报文的设备立即发送拓扑响应报文至管理设备，并在已使能 NTDP 的端口复制此请求报文并发送到邻接设备；拓扑响应报文包含本设备的基本信息和所有邻接设备的 NDP 信息。
- 邻接设备收到请求报文后将执行同样操作，直至拓扑收集请求报文扩散到指定跳数范围内的所有设备。

当拓扑收集请求报文在网络内扩散时，大量网络设备同时收到拓扑收集请求并同时发送拓扑收集响应报文。为了避免网络拥塞和管理设备任务繁忙，可采取以下措施控制拓扑收集请求报文的扩散速度：

- 每台被收集设备收到拓扑收集请求报文后，并不立即转发该报文，而是延迟一段时间再由其第一个端口转发。
- 在同一台设备上，除第一个端口外，其它端口在上一个端口转发了拓扑收集请求报文后，都将延迟一段时间再继续转发该报文。

3. 集群管理维护

(1) 候选设备加入集群

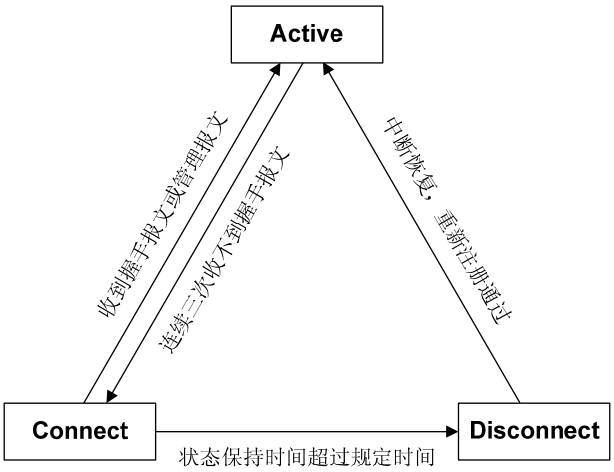
用户在建立集群时应首先指定管理设备，管理设备可以通过 NDP 和 NTDP 协议发现和确定候选设备并将其自动加入集群，也可以通过手工配置将候选设备加入集群。

当候选设备成功加入集群后，将获得管理设备为其分配的集群成员序列号、集群管理使用的私有 IP 地址等。

(2) 集群内部通讯

在集群内部，管理设备与成员设备通过握手报文实时通信，以维护它们之间的连接状态，管理设备和成员设备的连接状态如 图 1-3 所示。

图1-3 管理/成员设备状态转换



- 集群建立成功、候选设备加入集群成为成员设备后，管理设备将其状态信息保存到本地，并将其状态标识为 Active；成员设备也将自身的状态信息保存到本地，并将其自身状态标识为 Active。

- 管理设备和成员设备定时互发握手报文。管理设备收到成员设备的握手报文后不应答，仍将其状态保持为 Active；成员设备收到管理设备的握手报文后也不应答，仍将其自身状态保持为 Active。
- 当管理设备发送握手报文后，在三倍握手报文发送时间间隔内仍没收到成员设备的握手报文，则将其状态由 Active 迁移为 Connect；同样，当成员设备发送握手报文后，在三倍握手报文发送时间间隔内仍没收到管理设备的握手报文，其自身状态也将从 Active 迁移为 Connect。
- 若管理设备收到了处于 Connect 状态的成员设备在有效保留时间内发送的握手或管理报文，则将其状态迁移回 Active，否则迁移为 Disconnect——此时管理设备会认为已与该成员设备断开；而处于 Connect 状态的成员设备若在有效保留时间内收到了管理设备发送的握手或管理报文，则将其自身状态迁移至 Active，否则迁移为 Disconnect。
- 当管理设备与成员设备的通信恢复时，处于 Disconnect 状态的成员设备将重新加入集群。加入成功后，成员设备在管理设备以及其本地的状态都将恢复为 Active。

如果发现拓扑改变，成员设备也通过握手报文向管理设备传递变化信息。

4. 管理VLAN

管理VLAN是指集群协议报文通讯所使用的VLAN，它限制了集群管理的范围，通过配置管理VLAN，可实现如下功能：

- 集群的管理报文（包括 NDP、NTDP 和握手报文）都将限制在管理 VLAN 内，实现了与其它报文的隔离，增加了安全性。
- 管理设备和成员设备通过管理 VLAN 实现了内部通讯。

集群管理要求管理设备与成员/候选设备相连的端口（包括级联端口）都要允许管理 VLAN 通过。如果端口不允许管理 VLAN 通过，该端口所连的设备将不能加入集群，因此当候选设备与管理设备相连的端口包括级联端口不允许管理 VLAN 通过时，可通过管理 VLAN 自协商修改候选设备的端口以允许管理 VLAN 通过。只有当管理设备与成员/候选设备相连接的端口（包括级联端口）的缺省 VLAN ID 都是管理 VLAN 时，才允许配置管理 VLAN 的报文不带 Tag 通过，否则管理 VLAN 的报文都必须带 Tag 通过。

说明

- 级联端口是指当候选设备通过另外一台候选设备与管理设备相连时，这两台候选设备之间的连接端口。
- 有关 VLAN 和 Tag 的相关介绍，请参见“二层技术-以太网交换配置指导”中的“VLAN”。

1.2 集群管理配置任务简介

用户配置集群前，需要明确集群内各个设备的角色以及功能，另外还要配置相关的功能，做好与集群内部设备进行通信的规划工作。

表1-1 集群管理配置任务简介

配置任务		说明	详细配置
配置管理设备	使能NDP功能	可选	1.3.1
	配置NDP参数	可选	1.3.2
	使能NTDP功能	可选	1.3.3
	配置NTDP参数	可选	1.3.4
	手动收集拓扑信息	可选	1.3.5
	使能集群功能	可选	1.3.6
	建立集群	必选	1.3.7
	使能管理VLAN自协商功能	必选	1.3.8
	配置集群成员交互	可选	1.3.9
	配置集群管理协议报文	可选	1.3.10
	集群成员管理	可选	1.3.11
配置成员设备	使能NDP功能	可选	1.4.1
	使能NTDP功能	可选	1.4.2
	手动收集拓扑信息	可选	1.4.3
	使能集群功能	可选	1.4.4
	配置成员设备退出集群	可选	1.4.5
配置集群成员互访		可选	1.5
配置候选设备加入集群		可选	1.6
配置集群管理高级功能	配置集群拓扑管理	可选	1.7.1
	配置集群内外交互	可选	1.7.2
	SNMP配置同步功能	可选	1.7.3
	批量配置Web账户	可选	1.7.4

注意

- 集群建立后，在管理设备和成员设备上关闭 NDP 或者 NTDP 功能后，集群不会解散，但是会影响已经建立的集群的正常运行。
- 在一个集群中，当使能了 802.1X 或 MAC 地址认证功能的成员设备还连接有其它成员设备时，必须在该成员设备上开启 HABP server 功能，否则管理设备将无法对其连接的成员设备进行管理。有关 HABP（HW Bypass Protocol，HW 旁路认证协议）的详细介绍，请参见“安全配置指导”中的“HABP”。
- 如果集群建立时管理设备的路由表已满，即无法向路由表中添加目的地址为候选设备的路由条目，将导致所有候选设备反复加入退出集群。
- 如果候选设备加入集群时候选设备的路由表已满，即无法向路由表中添加目的地址为管理设备的路由条目，也将导致本设备反复加入退出集群。

1.3 配置管理设备

1.3.1 使能NDP功能

当全局和端口的 NDP 功能都使能时，NDP 才能正常运行。

表1-2 使能 NDP 功能

操作		命令	说明
进入系统视图		**system-view**	-
使能全局的NDP功能		**ndp enable**	可选 缺省情况下，全局的NDP功能处于使能状态
使能端口的NDP功能	系统视图下	**ndp enable interface** *interface-list*	二者可选其一 缺省情况下，所有端口的NDP功能都处于使能状态
	以太网接口或二层聚合接口视图下	**interface** *interface-type interface-number* **ndp enable**	

说明

为避免管理设备收集到不需要加入集群的设备的拓扑信息并将其误加入集群，建议在与这些设备相连的端口上关闭 NDP 功能。

1.3.2 调整NDP参数

使能了 NDP 功能的端口会周期性地向外发送 NDP 报文。当 NDP 报文在接收设备上的老化时间超时后，接收设备仍未收到本设备发送的 NDP 报文，接收设备将自动删除本设备所对应的邻居表项。

表1-3 调整 NDP 参数

操作	命令	说明
进入系统视图	**system-view**	-
配置发送NDP报文的时间间隔	**ndp timer hello** *hello-time*	可选 缺省情况下，发送NDP报文的时间间隔为60秒
配置NDP报文在接收设备上的老化时间	**ndp timer aging** *aging-time*	可选 缺省情况下，NDP报文在接收设备上的老化时间为180秒

注意

NDP 报文在接收设备上的老化时间应不小于发送 NDP 报文的时间间隔，否则将引起 NDP 端口邻居信息表的不稳定。

1.3.3 使能NTDP功能

当全局和端口的 NTDP 功能都使能时，NTDP 才能正常运行。

表1-4 使能 NTDP 功能

操作	命令	说明
进入系统视图	**system-view**	-
使能全局的NTDP功能	**ntdp enable**	可选 缺省情况下，全局的NTDP功能处于使能状态
进入以太网接口或二层聚合接口视图	**interface** *interface-type interface-number*	-
使能端口的NTDP功能	**ntdp enable**	可选 缺省情况下，所有端口的NTDP功能都处于使能状态

为避免管理设备收集到不需要加入集群的设备的拓扑信息并将其误加入集群，建议在与这些设备相连的端口上关闭 NTDP 功能。

1.3.4 调整NTDP参数

通过配置拓扑收集范围（即最大跳数）可以收集确定范围内设备的拓扑信息，从而避免无限的扩展收集过程。控制收集范围采用从收集发起者开始、控制允许发现的跳数的方法。

在配置了拓扑收集的时间间隔后，设备将以此间隔为周期进行拓扑信息的收集。

为了避免拓扑收集设备由于同时收到大量拓扑响应报文而导致的拥塞：

- 每台被收集设备在收到拓扑收集请求报文后，都将延迟一段时间再由其第一个端口转发该报文；
- 在同一台设备上，除第一个端口外，其它端口在上一个端口转发了拓扑收集请求报文后，都将延迟一段时间再继续转发该报文。

表1-5 调整 NTDP 参数

操作	命令	说明
进入系统视图	**system-view**	-
配置拓扑收集的最大跳数	**ntdp hop** *hop-value*	可选 缺省情况下，拓扑收集的最大跳数为3跳
配置拓扑收集的时间间隔	**ntdp timer** *interval*	可选 缺省情况下，拓扑收集的时间间隔为1分钟
配置首个端口转发拓扑收集请求报文的延迟时间	**ntdp timer hop-delay** *delay-time*	可选 缺省情况下，首个端口转发拓扑收集请求报文的延迟时间为200毫秒
配置其它端口转发拓扑收集请求报文的延迟时间	**ntdp timer port-delay** *delay-time*	可选 缺省情况下，其它端口转发拓扑收集请求报文延迟时间为20毫秒

说明

首个/其它端口转发拓扑收集请求报文的延迟时间都需配置在拓扑收集设备上：拓扑收集设备在其发送的拓扑收集请求报文中携带了这两种延迟时间值，被收集设备依据该值来延迟拓扑收集请求报文的转发。

1.3.5 手动收集拓扑信息

集群建立后，管理设备会周期性地收集拓扑信息。用户还可以在管理设备或使能 NTDP 功能的设备上手动发起拓扑信息的收集过程（不论集群是否已建立），从而更有效地对设备进行实时管理与监控。

请在用户视图下进行下列配置。

表1-6 手动收集拓扑信息

操作	命令	说明
手动收集拓扑信息	**ntdp explore**	必选

1.3.6 使能集群功能

表1-7 使能集群功能

操作	命令	说明
进入系统视图	**system-view**	-
使能集群功能	**cluster enable**	可选 缺省情况下，集群功能处于使能状态

1.3.7 建立集群

建立集群前，须指定管理 VLAN，成员设备加入集群后就不能再修改管理 VLAN。

建立集群前，还须在欲配置为管理设备的设备上配置成员设备所使用的私有 IP 地址范围，且管理设备和成员设备的 VLAN 接口的 IP 地址和集群地址池不能配置在同一网段内，否则集群将不能正常工作。当候选设备加入时，管理设备为候选设备动态分配一个能够在集群内使用的私有 IP 地址，用于集群内部的通信。

建立集群有两种方式：手工创建和自动创建。其中，在自动创建集群的过程中，用户可根据系统提示自动创建集群：

(1) 首先，系统提示输入集群名称；

(2) 接着，系统将列出指定的跳数范围内发现的所有候选设备；

(3) 系统将把所有列出的候选设备自动加入到所创建的集群中。

在自动创建过程中，允许用户输入<Ctrl+C>取消当前操作，并退出自动创建过程。该操作只能停止加入新的设备，已加入集群的设备仍将保留在集群中。

表1-8 手动建立集群

操作	命令	说明
进入系统视图	**system-view**	-

操作		命令	说明
指定管理VLAN		**management-vlan** *vlan-id*	可选 缺省情况下，管理VLAN为VLAN 1
进入集群视图		**cluster**	-
配置成员设备的私有IP地址范围		**ip-pool** *ip-address* { *mask* | *mask-length* }	必选 缺省情况下，没有指定成员设备的私有IP地址范围
创建集群	手动创建集群	**build** *cluster-name*	二者必选其一 缺省情况下，设备不是管理设备
	自动创建集群	**auto-build** [**recover**]	

注意

由于握手报文使用的 UDP 端口号为 40000，因此建立集群前需确保该端口未被占用，否则将导致集群建立失败。

1.3.8 使能管理VLAN自协商功能

管理 VLAN 限制了集群管理的范围，当管理设备发现的新设备在管理 VLAN 之外即与管理设备相连的端口及级联端口不允许管理 VLAN 通过时，新设备将无法加入集群。通过在管理设备上使能管理 VLAN 自动协商功能，可以将与管理设备相连的端口及级联端口自动加入管理 VLAN。

表1-9 使能管理 VLAN 自协商功能

操作	命令	说明
进入系统视图	**system-view**	-
进入集群视图	**cluster**	-
使能管理VLAN自协商功能	**management-vlan synchronization enable**	必选 缺省情况下，管理VLAN自协商功能处于关闭状态

说明

在开启了管理 VLAN 自协商功能后，各成员设备之间相连的端口将会发生以下转换过程：

- 如果该端口之前为 Access 端口，则转换为 Hybrid 端口，且将不再允许除管理 VLAN 外的其他 VLAN 通过（管理 VLAN 以 tagged 形式通过）。
- 如果该端口之前为 Trunk 或 Hybrid 端口，则转换过程对端口类型和已经允许通过的 VLAN 没有影响，只是增加允许管理 VLAN 通过（对于 Hybrid 端口为 tagged 形式）。

请用户在配置本功能之前，确认成员设备之间连接端口的端口类型和允许通过的 VLAN，避免转换过程对网络产生影响。

1.3.9 配置集群成员交互

在集群内部，管理设备与成员设备通过握手报文进行实时通信，以维护它们之间的连接状态。可以在管理设备上配置发送握手报文的时间间隔和有效保留时间，该配置将对集群内部所有成员设备同时生效。对于处于 Connect 状态的成员设备来说：

- 如果管理设备在有效保留时间内未收到来自该成员设备的消息，则将其状态迁移为 Disconnect。当通讯恢复后，该成员设备需要重新加入（成员重新加入过程是自动进行的）。
- 如果管理设备在有效保留时间内收到了来自该成员设备的消息，则将其状态迁移回 Active。

表1-10 配置集群成员交互

操作	命令	说明
进入系统视图	**system-view**	-
进入集群视图	**cluster**	-
配置发送握手报文的时间间隔	**timer** *interval*	可选 缺省情况下，发送握手报文的时间间隔为10秒
配置有效保留时间	**holdtime** *hold-time*	可选 缺省情况下，有效保留时间为60秒

1.3.10 配置集群管理协议报文

集群管理协议报文（包括 NDP、NTDP 和 HABP 报文）的缺省目的 MAC 地址是 IEEE 保留的组播 MAC 地址 0180-C200-000A，而部分现有设备对目的 MAC 地址为此类地址的报文不能正常转发，从而导致集群管理协议报文无法穿越这些设备。针对这种情况，在不改变现有组网的前提下，可将集群管理协议报文的目的 MAC 地址修改为其它 MAC 地址来避免影响集群的正常运行。

管理设备通过周期性地向成员/侯选设备发送 MAC 地址协商广播报文来通告集群管理协议报文的目的 MAC 地址。

表1-11 配置集群管理协议报文

操作	命令	说明
进入系统视图	**system-view**	-
进入集群视图	**cluster**	-
配置集群管理协议报文的目的MAC地址	**cluster-mac** *mac-address*	必选 缺省情况下，集群管理协议报文的目的MAC地址为0180-C200-000A 可以配置的MAC地址包括：0180-C200-0000，0180-C200-000A，0180-C200-0020～0180-C200-002F或010F-E200-0002
配置发送MAC地址协商广播报文的时间间隔	**cluster-mac syn-interval** *interval*	可选 缺省情况下，发送MAC地址协商广播报文的时间间隔为1分钟

注意

在配置集群管理协议报文的目的 MAC 地址时：

- 若发送 MAC 地址协商广播报文的时间间隔为零，系统会自动将其修改为 1 分钟；
- 若发送 MAC 地址协商广播报文的时间间隔非零，则该时间间隔将保持不变。

1.3.11 集群成员管理

用户可以在管理设备上手工指定要加入集群中的候选设备，也可以手工删除集群中指定的成员设备。当成员设备由于软件版本升级、配置更新等原因需要重启时，可以通过管理设备对其进行远程重启。

1. 添加成员设备

表1-12 添加成员设备

操作	命令	说明
进入系统视图	**system-view**	-
进入集群视图	**cluster**	-
将候选设备加入集群	**add-member** [*member-number*] **mac-address** *mac-address* [**password** *password*]	必选

2. 删除成员设备

表1-13 删除成员设备

操作	命令	说明
进入系统视图	**system-view**	-
进入集群视图	**cluster**	-
将成员设备从集群中删除	**delete-member** *member-number* [**to-black-list**]	必选

3. 重启成员设备

表1-14 重启成员设备

操作	命令	说明
进入系统视图	**system-view**	-
进入集群视图	**cluster**	-
重新启动指定的成员设备	**reboot member** { *member-number* | mac-address *mac-address* } [**eraseflash**]	必选

1.4 配置成员设备

1.4.1 使能NDP功能

请参见“1.3.1 使能NDP功能”。

1.4.2 使能NTDP功能

请参见“1.3.3 使能NTDP功能”。

1.4.3 手动收集拓扑信息

请参见“1.3.5 手动收集拓扑信息”。

1.4.4 使能集群功能

请参见“1.3.6 使能集群功能”。

1.4.5 配置成员设备退出集群

表1-15 配置成员设备退出集群

操作	命令	说明
进入系统视图	**system-view**	-
进入集群视图	**cluster**	-
配置成员设备退出集群	**undo administrator-address**	必选

1.5 配置集群成员互访

当 NDP、NTDP 和集群功能的配置完成后，可通过管理设备对成员设备进行配置、管理和监控：既可在管理设备上切换到指定成员设备的操作界面上对该成员设备进行配置管理；也可从成员设备切换回管理设备的操作界面上对管理设备进行配置。

请在用户视图下进行下列配置。

表1-16 配置集群成员互访

操作	命令	说明
从管理设备操作界面切换到成员设备操作界面	**cluster switch-to** { *member-number* | **mac-address** *mac-address* | **sysname** *member-sysname* }	必选
从成员设备操作界面切换到管理设备操作界面	**cluster switch-to administrator**	必选

注意

管理设备和成员设备间的切换均使用了 Telnet 连接，进行切换时需要注意：

- 成员设备切换到管理设备上需要认证，认证不通过将会导致切换失败，切换成功后用户权限根据管理设备预定的级别分配。
- 候选设备加入集群成为成员设备后，其级别为 3 的 super password 会自动同步与管理设备保持一致。集群建立以后，建议用户不要修改集群成员（包括管理设备和成员设备）的 super password，以免切换时由于认证不通过而失败。
- 从管理设备切换到成员设备，如果指定的成员不存在，将显示出错信息；切换成功后在成员设备上继承管理设备上的当前级别。
- 如果被请求登录的设备 Telnet 用户已满将会导致切换失败。

1.6 配置候选设备加入集群

用户可以在候选设备上进行配置，将候选设备自身加入某个已建立的集群。

表1-17 配置候选设备加入集群

操作	命令	说明
进入系统视图	**system-view**	-
进入集群视图	**cluster**	-
配置候选设备加入集群	**administrator-address** *mac-address* **name** *name*	必选

1.7 配置集群管理高级功能

1.7.1 配置集群拓扑管理

白名单与黑名单是拓扑管理的依据，网络管理员可通过将当前网络拓扑（即集群当前的拓扑节点和邻接关系等信息，记录了当前的网络拓扑状况）与标准拓扑进行比较对当前的网络状况进行诊断，两者的含义如下：

- 拓扑管理白名单：即标准拓扑，是网络管理员对当前网络拓扑进行确认之后认为正确的网络拓扑信息。可根据当前网络拓扑状况实现对白名单的维护，包括添加、删除和修改结点。
- 拓扑管理黑名单：列入黑名单中的设备不允许自动加入集群。黑名单信息包括设备的 MAC 地址，若该设备通过非黑名单中的设备接入，则还包括接入设备的 MAC 地址和接入端口。被列入黑名单的候选设备，需要网络管理员手工将其从黑名单删除后，方可加入集群

白名单与黑名单具有互斥性：白名单中的节点必定不在黑名单中；黑名单中的节点也不能加入白名单。拓扑节点可以既不在白名单也不在黑名单中，这类节点通常属于新增结点，其身份还有待网络管理员的确认。

用户可以对白名单和黑名单进行备份和恢复，有以下两种方式：

- 备份在集群公用的 FTP 服务器上：白名单与黑名单可以手动从 FTP 服务器上恢复。
- 备份在管理设备的 Flash 中：当管理设备重启时，白名单与黑名单会自动从管理设备的 Flash 中恢复；当集群重新创建时，可根据用户的选择决定是否从管理设备的 Flash 中恢复，也可手动从管理设备的 Flash 中恢复。

表1-18 配置集群拓扑管理

操作	命令	说明
进入系统视图	**system-view**	-
进入集群视图	**cluster**	-
将设备加入黑名单	**black-list add-mac** *mac-address*	可选
将设备从黑名单中删除	**black-list delete-mac** { **all** | *mac-address* }	可选
确认集群当前的拓扑信息，并存为标准拓扑	**topology accept** { **all** [**save-to** { **ftp-server** | **local-flash** }] | **mac-address** *mac-address* | **member-id** *member-number* }	可选
保存标准拓扑信息到FTP服务器或者本地Flash中	**topology save-to** { **ftp-server** | **local-flash** }	可选
获取标准拓扑信息进行恢复	**topology restore-from** { **ftp-server** | **local-flash** }	可选

1.7.2 配置集群内外交互

集群建立后，可以在管理设备上为集群统一配置 FTP/TFTP 服务器、网管主机和日志主机：

- 为集群统一配置 FTP/TFTP 服务器后，成员设备通过管理设备来访问配置的 FTP/TFTP 服务器（即在成员设备上通过 **ftp** 或 **tftp** 命令指定管理设备的私有 IP 地址。有关 **ftp** 和 **tftp** 命令的详细介绍，请参见“基础配置命令参考”中的“FTP 和 TFTP”）。
- 为集群统一配置日志主机后，成员设备的所有日志信息都将输出到该日志主机上：当成员设备输出日志信息时，日志信息将直接发送给管理设备，并由管理设备对这些日志信息进行地址转换，然后发送到该日志主机上。
- 为集群统一配置网管主机后，成员设备通过管理设备向公用的 SNMP 网管站发送 Trap 信息。

如果接入网管设备（包括 FTP/TFTP 服务器、网管主机和日志主机）的端口不允许管理 VLAN 通过，网管设备将无法通过管理设备对集群内部的设备进行管理。这时需在管理设备上将这些接入网管设备的 VLAN 接口配置为网管接口。

表1-19 配置集群内外交互

操作	命令	说明
进入系统视图	**system-view**	-
进入集群视图	**cluster**	-
配置集群公用的FTP服务器	**ftp-server** *ip-address* [**user-name** *username* **password** { **simple** | **cipher** } *password*]	必选 缺省情况下，集群没有公用的FTP服务器
配置集群公用的TFTP服务器	**tftp-server** *ip-address*	必选 缺省情况下，集群没有公用的TFTP服务器
配置集群公用的日志主机	**logging-host** *ip-address*	必选 缺省情况下，集群没有公用的日志主机
配置集群公用的SNMP网管站	**snmp-host** *ip-address* [**community-string read** *string1* **write** *string2*]	必选 缺省情况下，集群没有公用的SNMP网管站
配置管理设备的网管接口	**nm-interface vlan-interface** *interface-name*	可选

注意

为了将集群的管理协议报文与集群外部网络的报文隔离，建议管理设备与集群网络外部的设备相连的端口不要允许管理 VLAN 通过，并配置管理设备的网管接口。

1.7.3 SNMP配置同步功能

SNMP 配置同步功能方便了集群管理，可以在管理设备上进行 SNMP 的相关配置操作并将其同步到白名单中的成员设备上，相当于对成员设备进行批量配置，极大地简化配置过程。

表1-20 SNMP 配置同步功能

操作	命令	说明
进入系统视图	**system-view**	-
进入集群视图	**cluster**	-
配置集群公用的SNMP团体	**cluster-snmp-agent community** { **read** | **write** } *community-name* [**mib-view** *view-name*]	必选
配置集群公用的SNMP v3组	**cluster-snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*]	必选
创建或者更新集群公用的MIB视图信息	**cluster-snmp-agent mib-view included** *view-name oid-tree*	必选 缺省情况下，集群公用的MIB视图名为ViewDefault，可访问ISO子树
为集群公用的SNMP v3组添加一个新用户	**cluster-snmp-agent usm-user v3** *user-name group-name* [**authentication-mode** { **md5** | **sha** } *auth-password*] [**privacy-mode des56** *priv-password*]	必选

说明

- 集群解散或成员设备从白名单中删除时，SNMP 相关配置都将继续保留。
- 有关 SNMP 的相关介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

1.7.4 批量配置Web账户

批量配置 Web 账户功能提供了一种便捷的方法，用户可以在管理设备上配置通过 Web 方式登录到集群内部设备（包括管理设备和成员设备）的用户名和密码，并将配置同步到白名单中的成员设备上。当用户通过 Web 方式登录到集群内部设备上进行相关操作时，需要输入用户名和密码。

表1-21 批量配置 Web 账户

操作	命令	说明
进入系统视图	**system-view**	-
进入集群视图	**cluster**	-
批量配置Web账户	**cluster-local-user** *user-name* **password** { **cipher** | **simple** } *password*	必选

说明

集群解散或成员设备从白名单中删除时，Web 账户的配置将继续保留。

1.8 集群管理显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后集群的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 NDP 的统计信息。

表1-22 集群管理显示和维护

操作	命令
显示NDP的配置信息	**display ndp** [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示NTDP的配置信息	**display ntdp** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示NTDP收集到的设备信息	**display ntdp device-list** [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示指定设备的NTDP详细信息	**display ntdp single-device mac-address** *mac-address* [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示设备所属集群的信息	**display cluster** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示集群的标准拓扑信息	**display cluster base-topology** [**mac-address** *mac-address* | **member-id** *member-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示集群当前的黑名单	**display cluster black-list** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示候选设备的信息	**display cluster candidates** [**mac-address** *mac-address* | **verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示集群当前的拓扑信息	**display cluster current-topology** [**mac-address** *mac-address* [**to-mac-address** *mac-address*] | **member-id** *member-number* [**to-member-id** *member-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示成员设备的信息	**display cluster members** [*member-number* | **verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除NDP的统计信息	**reset ndp statistics** [**interface** *interface-list*]

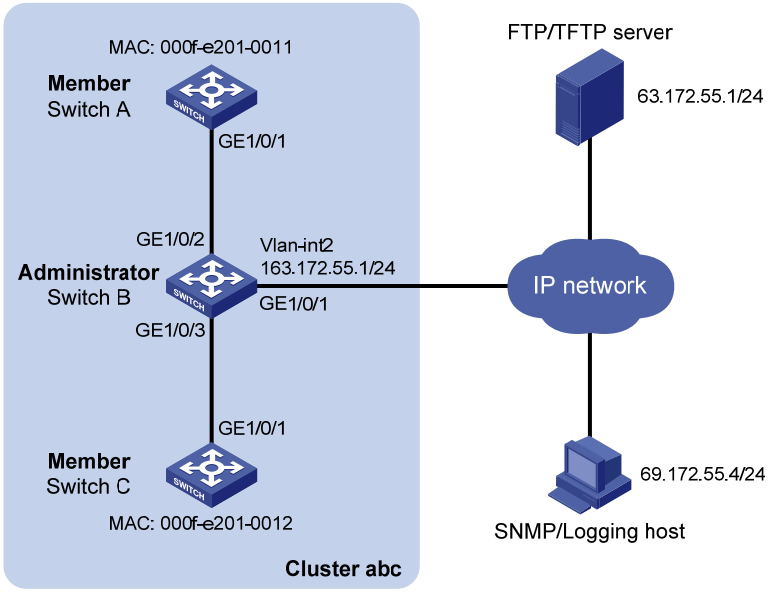
1.9 集群管理典型配置举例

1. 组网需求

- 由三台设备组成的集群 abc，其管理 VLAN 为 VLAN 10。其中，Switch B 为管理设备（Administrator），其网管接口为 Vlan-interface2；Switch A 和 Switch C 为成员设备（Member）。
- 整个集群将 IP 地址为 63.172.55.1/24 设备作为 FTP 服务器和 TFTP 服务器，SNMP 网管站及日志主机的 IP 地址为 69.172.55.4/24。
- 通过配置，将 MAC 地址为 000f-e201-0013 的设备加入黑名单。

2. 组网图

图1-4 集群管理配置组网图



3. 配置步骤

(1) 配置成员设备 Switch A

使能全局 NDP 功能和端口 GigabitEthernet1/0/1 上的 NDP 功能。

```
<SwitchA> system-view
[SwitchA] ndp enable
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] ndp enable
[SwitchA-GigabitEthernet1/0/1] quit
```

使能全局 NTDP 功能和端口 GigabitEthernet1/0/1 上的 NTDP 功能。

```
[SwitchA] ntdp enable
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] ntdp enable
[SwitchA-GigabitEthernet1/0/1] quit
```

使能集群功能。

```
[SwitchA] cluster enable
```

(2) 配置成员设备 Switch C

由于成员设备的配置相同，因此 Switch C 上的配置与 Switch A 相似，配置过程略。

(3) 配置管理设备 Switch B

使能全局 NDP 功能，并分别使能端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 上的 NDP 功能。

```
<SwitchB> system-view
[SwitchB] ndp enable
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] ndp enable
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] ndp enable
[SwitchB-GigabitEthernet1/0/3] quit
```

配置本设备发送的 NDP 报文在接收设备上的老化时间为 200 秒。

```
[SwitchB] ndp timer aging 200
```
配置 NDP 报文发送的时间间隔为 70 秒。
```
[SwitchB] ndp timer hello 70
```
使能全局 NTDP 功能，并分别使能端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 上的 NTDP 功能。
```
[SwitchB] ntdp enable
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] ntdp enable
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] ntdp enable
[SwitchB-GigabitEthernet1/0/3] quit
```
配置拓扑收集的最大跳数为 2 跳。
```
[SwitchB] ntdp hop 2
```
配置被收集设备首个端口转发拓扑收集请求报文的延迟时间为 150ms。
```
[SwitchB] ntdp timer hop-delay 150
```
配置被收集设备其它端口转发拓扑收集请求报文的延迟时间为 15ms。
```
[SwitchB] ntdp timer port-delay 15
```
配置拓扑收集的时间间隔为 3 分钟。
```
[SwitchB] ntdp timer 3
```
配置集群的管理 VLAN 为 VLAN 10。
```
[SwitchB] vlan 10
[SwitchB-vlan10] quit
[SwitchB] management-vlan 10
```
将端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 都配置为 Trunk 口，并允许管理 VLAN 通过。
```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-GigabitEthernet1/0/2] port trunk permit vlan 10
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port link-type trunk
[SwitchB-GigabitEthernet1/0/3] port trunk permit vlan 10
[SwitchB-GigabitEthernet1/0/3] quit
```
使能集群功能。
```
[SwitchB] cluster enable
```
配置成员设备的私有 IP 地址范围为 172.16.0.1～172.16.0.7。
```
[SwitchB] cluster
[SwitchB-cluster] ip-pool 172.16.0.1 255.255.255.248
```
配置当前设备为管理设备，并建立名为 abc 的集群。
```
[SwitchB-cluster] build abc
Restore topology from local flash file,for there is no base topology.
(Please confirm in 30 seconds, default No). (Y/N)
N
```
使能管理 VLAN 自协商功能。
```
[abc_0.SwitchB-cluster] management-vlan synchronization enable
```
配置成员设备信息的有效保留时间为 100 秒。
```
[abc_0.SwitchB-cluster] holdtime 100
```
配置发送握手报文的时间间隔为 10 秒。
```
[abc_0.SwitchB-cluster] timer 10
```
分别指定集群公用的 FTP 服务器、TFTP 服务器、日志主机和 SNMP 网管站。

```
[abc_0.SwitchB-cluster] ftp-server 63.172.55.1
[abc_0.SwitchB-cluster] tftp-server 63.172.55.1
[abc_0.SwitchB-cluster] logging-host 69.172.55.4
[abc_0.SwitchB-cluster] snmp-host 69.172.55.4
```

将 MAC 地址为 000f-e201-0013 的设备加入黑名单。

```
[abc_0.SwitchB-cluster] black-list add-mac 000f-e201-0013
[abc_0.SwitchB-cluster] quit
```

将端口 GigabitEthernet1/0/1 加入 VLAN 2，并为接口 Vlan-interface2 配置 IP 地址。

```
[abc_0.SwitchB] vlan 2
[abc_0.SwitchB-vlan2] port gigabitethernet 1/0/1
[abc_0.SwitchB] quit
[abc_0.SwitchB] interface vlan-interface 2
[abc_0.SwitchB-Vlan-interface2] ip address 163.172.55.1 24
[abc_0.SwitchB-Vlan-interface2] quit
```

将接口 Vlan-interface2 配置为网管接口。

```
[abc_0.SwitchB] cluster
[abc_0.SwitchB-cluster] nm-interface vlan-interface 2
```

目 录

1 CWMP配置

1.1 CWMP简介

1.1.1 CWMP协议

CWMP（CPE WAN Management Protocol，CPE 广域网管理协议）是由 DSL（Digital Subscriber's Line，数字用户线路）论坛发起开发的技术规范之一，编号为 TR-069，所以又被称为 TR-069 协议。CWMP 在设计时主要针对 DSL 接入网络环境。在 DSL 接入网络中，由于用户设备数量繁多、部署分散，通常位于用户侧，不易进行设备的管理和维护，CWMP 提出通过 ACS（Auto-Configuration Server，自动配置服务器）对 CPE（Customer Premises Equipment，用户侧设备）进行远程集中管理，解决 CPE 设备的管理困难，节约维护成本，提高问题解决效率。

大型数据中心的网络环境与 DSL 环境具有类似的特征，即接入交换机数量众多，而且随着规模的扩张，会经常出现在网络的某个层级大量增加新设备的情况。这些新设备的业务功能基本相同，如果能够利用 CWMP 协议的特点进行远程集中管理和配置，便可以快速完成部署，并且后期的维护和管理也将变得更加便捷。

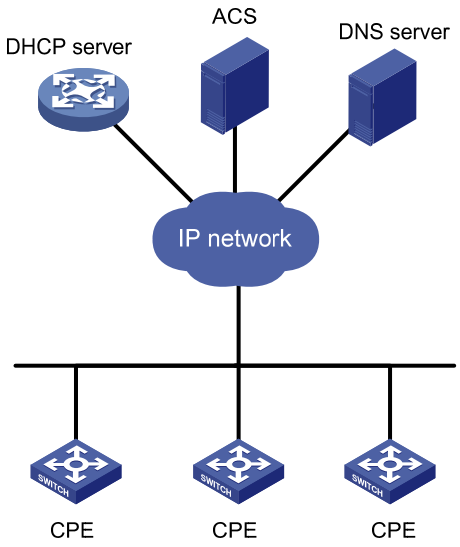
设备提供了对 CWMP 协议的支持，在空配置接入网络时可以作为 CPE 设备，自动从 ACS 下载配置文件。相对于传统的手工配置方式，利用 CWMP 进行远程统一配置具有以下优点：

- 对于业务相同的新设备统一下发配置，减少重复工作，提高部署效率
- 设备开箱后即可直接接入网络，不需要工程师现场配置，降低人力成本
- 配置文件预先生成，降低人工配置错误几率

1.1.2 CWMP网络框架

CWMP网络的基本框架如 图 1-1 所示：

图1-1 CWMP 网络基本框架示意图



说明

图 1-1 中的DHCP服务器、DNS服务器、ACS仅作为角色示意，实际应用中这些功能可以集中在一台服务器上。

CWMP 环境中的角色主要包括：

- CPE：网络中的被管理设备，可以向 ACS 上报自身信息并获取相应的配置。
- ACS：自动配置服务器，用于向 CPE 设备下发配置并提供 CPE 设备的管理服务。本文中的 ACS 是指安装了 H3C iMC 分支网点智能管理系统（简称 iMC BIMS）的服务器。
- DNS server：域名服务器。ACS 和 CPE 之间可以使用 URL 地址来互相识别和访问，DNS 用于帮助解析 URL 参数。
- DHCP server：DHCP 服务器，用于为 CPE 分配 IP 地址，并使用 DHCP 报文中的 option 字段为 CPE 提供访问 ACS 所使用的 URL 等参数。

1.2 CWMP的基本功能

1.2.1 通过ACS向CPE自动下发配置文件

为了便于对提供相同业务功能的新设备进行快速配置，网络管理员可以在 ACS 上创建针对该类设备的配置文件。当 CPE 设备与 ACS 建立连接后，ACS 可以判断 CPE 设备所属类别，并将对应该类设备的配置文件下发给 CPE 设备，从而可以使相同类型的大量 CPE 设备获得相同的业务配置。目前 ACS 可以通过产品型号和序列号等将 CPE 划分为不同的类别。

ACS 向 CPE 下发配置文件时，可以通过以下两种方式进行：

- 部署为启动配置：ACS 向 CPE 发送配置文件，覆盖 CPE 本地的缺省配置文件，当 CPE 重启之后，便可以使用新的配置运行。
- 部署为运行配置：ACS 将配置内容直接发给 CPE，并写入到 CPE 的当前配置中，配置内容即时生效，但是需要再执行保存配置的操作，以保证重启后配置不会丢失。

1.2.2 通过ACS管理CPE设备的系统文件

网络管理员可以将 CPE 设备的应用程序文件和配置文件等重要文件保存在 ACS 上，当 ACS 发现某个文件的版本有更新，将会通知 CPE 进行下载。CPE 收到 ACS 的下载请求后，能够根据 ACS 报文中提供的下载地址和文件名，自动到指定的文件服务器下载文件。下载完成后，对下载文件的合法性做相应的检查，并将下载结果（成功或失败）反馈给 ACS。目前 CPE 可以通过 ACS 下载的文件类型包括设备应用程序文件和配置文件。

同样，为了实现对重要数据的备份，CPE 将根据 ACS 的要求将当前的配置文件和日志文件上传到指定的服务器。

1.2.3 通过ACS监控CPE的状态和性能

ACS 可以监控与其相连的 CPE 的各种参数。由于不同的 CPE 具有不同的性能，可执行的功能也各异，因此 ACS 必须能识别不同类型 CPE 的性能，并监控到 CPE 的当前配置以及配置的变更。CWMP 还允许网络管理人员自定义监控参数并通过 ACS 获取这些参数，以便了解 CPE 的状态和统计信息。

ACS 能够监控的状态和性能有：厂商名称（Manufacturer）、厂商标识 OUI（ManufacturerOUI）、序列号（SerialNumber）、硬件版本号（HardwareVersion）、软件版本号（SoftwareVersion）、设备状态（DeviceStatus）、启动时间（UpTime）、配置文件、ACS 地址、ACS 用户名、ACS 密码、Inform 报文自动发送使能标志、Inform 报文周期发送时间间隔、Inform 报文定期发送日期、CPE 地址、CPE 用户名、CPE 密码等。

1.3 CWMP的实现机制

1.3.1 ACS和CPE的自动连接

CPE 在第一次上电启动时，会通过 DHCP 自动获取 IP 地址，DHCP 服务器在分配 IP 地址的同时，将向 CPE 通告以下内容：

- ACS 的 URL 地址（通过 option 43 选项分配）
- 连接 ACS 所需要的用户名和密码（通过 option 43 选项分配）
- DNS 服务器地址（直接分配）

CPE 设备得到以上信息后，通过 DNS 服务器解析出 ACS 的 IP 地址，向 ACS 发起连接请求，如果用户名和密码验证通过，CPE 和 ACS 之间将成功建立连接。

如果当前会话没有结束，但是连接异常中断，CPE 将自动尝试重新连接，直至重新连接的次数达到上限。

在运行过程中，CPE 设备还可以根据配置周期性或者定时向 ACS 服务器发起连接。ACS 也可以在任何时候自动向 CPE 发起连接请求，通过 CPE 的认证（即 CPE 用户名、CPE 密码）后，可以与 CPE 建立连接。

1.3.2 ACS向CPE下发配置项参数

CPE与ACS建立连接之后，ACS可以自动下发一些配置给CPE，完成对CPE的自动配置。CPE可以从ACS获取的自动配置项参数如 表 1-1 所示：

表1-1 CPE 可以从 ACS 获取的配置项

配置项	用途
配置文件（ConfigFile）	用于更新CPE的本地配置文件，ACS可以使用文件形式和当前配置形式向CPE下发配置文件
ACS地址（URL）	更新CPE记录的ACS地址，可用于主备ACS服务器之间的切换
ACS用户名（Username）	当ACS上连接用户名和密码发生变更时，可以自动同步到CPE设备，也可用于主备ACS服务器切换时向CPE通告备用ACS服务器的验证信息
ACS密码（Password）	
Inform报文自动发送使能标志（PeriodicInformEnable）	开启CPE设备发送Inform报文的功能
Inform报文周期发送时间间隔（PeriodicInformInterval）	配置CPE周期性向ACS发送Inform报文建立连接，用于定期查询更新和信息备份
Inform报文定期发送日期（PeriodicInformTime）	配置CPE在指定时间点向ACS发送Inform报文建立连接，用于在指定时间查询更新和信息备份
CPE用户名（ConnectionRequestUsername）	配置CPE在接受ACS发起的连接时所需要的验证信息
CPE密码（ConnectionRequestPassword）	

1.3.3 ACS对CPE的管理方式

ACS 对 CPE 的管理和监控是通过一系列的操作来实现的，这些操作在 CWMP 协议里称为 RPC 方法。主要方法的描述如下：

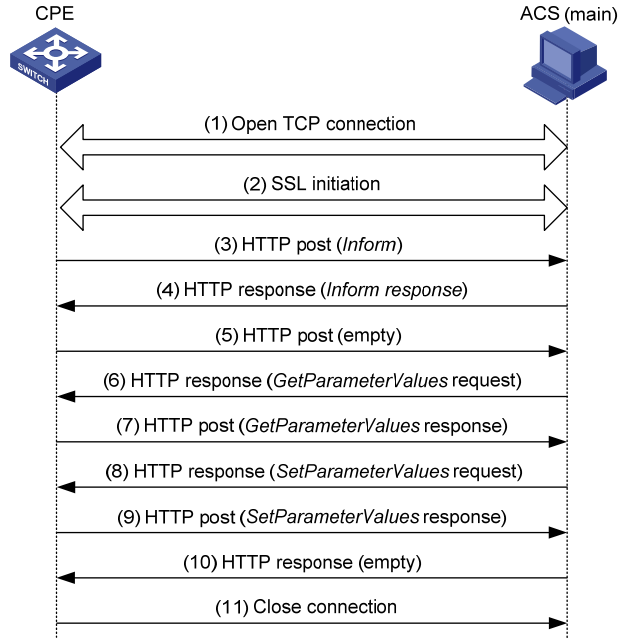
- Get：ACS 使用该方法可以获取 CPE 上参数的值。
- Set：ACS 使用该方法可以设置 CPE 上参数的值。

- Inform：当 CPE 与 ACS 建立连接时，或者底层配置发生改变时，或者 CPE 周期性发送本地信息到 ACS 时，CPE 都要通过该方法向 ACS 发起通告信息。
- Download：为了保证 CPE 端软件的升级以及厂商配置文件的自动下载，ACS 使用该方法可以要求 CPE 到指定的 URL 下载指定的文件来更新 CPE 的本地文件。
- Upload：为了方便 ACS 对 CPE 端的管理，ACS 使用该方法可以要求 CPE 将指定的文件上传到 ACS 指定的位置。
- Reboot：当 CPE 故障或者需要软件升级的时候，ACS 使用该方法可以对 CPE 进行远程重启。

1.3.4 主备ACS切换时的操作方式

下面以一个具体的例子来描述主备 ACS 切换时的实现过程，应用场景如下：区域内有主、备两台 ACS，主 ACS 系统升级，需要重启。为了连续监控，主 ACS 需要将区域内的 CPE 都连接到备用 ACS 上，处理流程如下：

图1-2 主备 ACS 切换时主 ACS 与 CPE 的消息交互举例



(1) 建立 TCP 连接。

(2) SSL 初始化，建立安全机制。

(3) CPE 发送 Inform 报文，开始建立 CWMP 连接。Inform 报文使用 Eventcode 字段描述发送 Inform 报文的原因，该举例为“6 CONNECTION REQUEST”，表示 ACS 要求建立连接。

(4) 如果 CPE 通过 ACS 的认证，ACS 将返回 Inform 响应报文，连接建立。

(5) 如果 CPE 没有别的请求，就会发送一个空报文，以满足 HTTP 报文请求/响应报文交互规则（CWMP 是基于 HTTP 协议的，CWMP 报文作为 HTTP 报文的数据部分封装在 HTTP 报文中）。

(6) ACS 查询 CPE 上设置的 ACS URL 的值。

(7) CPE 把获取到的 ACS URL 的值回复给 ACS。

(8) ACS 发现 CPE 的 ACS URL 是本机 URL 的值，于是发起 Set 请求，要求将 CPE 的 ACS URL 设置为备用 ACS 的 URL 的值。

(9) 设置成功，CPE 发送响应报文。

(10) ACS 发送空报文通知 CPE，表示不再请求其他内容。

(11) CPE 关闭连接。

之后，CPE 将向备用 ACS 发起连接。

1.4 CWMP配置任务简介

1.4.1 DHCP服务器的配置

在 CWMP 网络中，DHCP 服务器主要用于向 CPE 通告 ACS 的位置和验证信息，因此 DHCP 服务器上的配置主要包含以下内容：

- 配置地址池，为 CPE 设备分配 IP 地址
- 配置 DNS 服务器
- 配置 option 43 选项，向 CPE 通告 ACS 信息

这里主要介绍 option 43 选项的配置方法，关于地址池和 DNS 服务器的配置请参见“三层技术-IP 业务配置指导”中的“DHCP 服务器”。

当使用 H3C 设备作为 DHCP server 时，可以使用命令行配置包含 ACS 参数的 option 43 信息，命令格式为：**option 43 hex 01***length URL username password*

- *length*：表示关键字 **option 43 hex 01** 后面参数的总长度，用十六进制数表示。
- *URL*：ACS 的地址。
- *username*：ACS 的用户名。
- *password*：ACS 的密码。

ACS 的 URL、用户名和密码参数需要用空格隔开，参数的格式必须为字符对应的 ASCII 码的十六进制值格式。输入时，可以 2、4、6 或者 8 个十六进制值为一组，组间用空格隔开。比如，要将 ACS 地址配置为 http://169.254.76.31:7547/acs（http://对应的 ASCII 码的十六进制值为 68 74 74 70 3A 2F 2F，169.254.76.31 对应的 ASCII 码的十六进制值为 31 36 39 2E 32 35 34 2E 37 36 2E 33 31，:7547 对应的 ASCII 码的十六进制值为 3A 37 35 34 37，/acs 对应的 ASCII 码的十六进制值为 2F 61 63 73）、用户名配置为 1234（对应的 ASCII 码的十六进制值为 31 32 33 34）、密码配置为 5678（对应的 ASCII 码的十六进制值为 35 36 37 38），空格对应的 ASCII 码的十六进制值为 20，（*URL*＋1 个空格＋*username*＋1 个空格＋*password*）一共为 39 个字符（39 对应的十六进制为 27），所以 *length* 值为 0x27，可使用以下配置步骤：

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] option 43 hex 0127 68747470 3A2F2F31 36392E32 35342E37 362E3331
3A373534 372F6163 73203132 33342035 3637 38
```

说明

关于 DHCP 技术、option 43 参数以及 **option** 命令的详细介绍请参见“三层技术-IP 业务配置指导”中的“DHCP 概述”和“DHCP 服务器”。

1.4.2 DNS服务器的配置

在 DNS 服务器上，需要事先配置 ACS 服务器的 URL 和 IP 地址的对应，以便 CPE 设备可以通过域名解析功能得到 ACS 的 IP 地址。

1.4.3 ACS服务器的配置

由ACS远程管理，对CPE进行自动配置。可配置的主要参数请参见 1.3.2 。ACS服务器上的配置请参见您所选ACS服务器的软件使用说明。

1.4.4 CPE设备的配置

即通过命令行手工指定CWMP参数，可配置的内容如 表 1-2 所示。

说明

设备在 CWMP 环境中充当 CPE，因此下文中只介绍 CPE 设备上进行的配置。

表1-2 CWMP 配置任务简介

配置任务		说明	详细配置
使能CWMP功能		必选	1.5
配置ACS服务器信息	配置ACS的URL值	必选	1.6.1
	配置ACS的用户名和密码	可选	1.6.2
配置CPE设备属性	配置CPE的用户名和密码	可选	1.7.1
	配置CWMP接口	可选	1.7.2
	发送Inform报文	可选	1.7.3
	配置CPE自动重新连接的次数	可选	1.7.4
	配置CPE无数据传输的超时时间	可选	1.7.5
	配置CPE的工作模式	可选	1.7.6
	配置CWMP引用的SSL客户端策略	可选	1.7.7

1.5 使能CWMP功能

使能 CWMP 后，CWMP 的其它配置才能生效。

表1-3 使能 CWMP 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入CWMP视图	**cwmp**	-
使能CWMP功能	**cwmp enable**	可选 缺省情况下，CWMP功能处于使能状态

1.6 配置ACS服务器信息

ACS 服务器信息包括 ACS 的 URL、用户名和密码，当 CPE 发起连接请求时，连接请求报文里会携带 ACS 的 URL、用户名和密码。当 ACS 收到该报文后，如果这个参数的值和本地配置的值一致，则验证成功，允许建立连接；如果不一致，则验证失败，禁止建立连接。

1.6.1 配置ACS的URL值

表1-4 配置 ACS 的 URL 值

操作	命令	说明
进入系统视图	**system-view**	-
进入CWMP视图	**cwmp**	-
配置ACS的URL值	**cwmp acs url** *url*	必选 缺省情况下，没有配置ACS的URL

说明

一个 CPE 只能配置一个 ACS，多次配置 ACS 的 URL 值时，最新的配置生效。

1.6.2 配置ACS的用户名和密码

表1-5 配置 ACS 的用户名和密码

操作	命令	说明
进入系统视图	**system-view**	-
进入CWMP视图	**cwmp**	-
配置连接到ACS的用户名	**cwmp acs username** *username*	必选 缺省情况下，没有配置连接到ACS的用户名
配置连接到ACS的密码	**cwmp acs password** [**cipher** | **simple**] *password*	可选，可以只用用户名验证，但ACS和CPE上的配置必须一致 缺省情况下，没有配置连接到ACS的密码

说明

请使用 ACS 上合法的用户名和密码来配置 *username* 和 *password* 参数，否则，CPE 将不能通过 ACS 的认证。

1.7 配置CPE设备属性

在 CPE 上还可以配置 CPE 的用户名和密码，这些属性用于 CPE 对 ACS 的合法性进行验证。当连接由 ACS 发起时，会话请求报文里会携带 CPE 用户名和密码。CPE 设备收到该报文后，会与本地设置的 CPE 用户名和密码比较，如果相同则通过认证，进入连接建立的下一阶段，否则，认证失败，退出连接建立过程。

1.7.1 配置CPE的用户名和密码

表1-6 配置 CPE 用户名和密码

操作	命令	说明
进入系统视图	**system-view**	-
进入CWMP视图	**cwmp**	-
配置ACS连接到CPE时用来认证的用户名	**cwmp cpe username** *username*	必选 缺省情况下，没有设置CPE的用户名
配置ACS连接到CPE时用来认证的密码	**cwmp cpe password** [**cipher** | **simple**] *password*	可选，可以只用用户名验证，但ACS和CPE上的配置必须一致 缺省情况下，没有设置CPE的密码

1.7.2 配置CWMP连接接口

CWMP 连接接口指的是 CPE 上用于连接 ACS 的接口。CPE 会在 Inform 报文中携带 CWMP 连接接口的 IP 地址，要求 ACS 通过此 IP 地址和自己建立连接；相应的，ACS 会向该 IP 地址回复 Inform 响应报文。

通常情况下，系统会采用一定的机制去自动获取一个 CWMP 连接接口，但如果获取的 CWMP 连接接口不是 CPE 和 ACS 实际相连的接口时，就会导致 CWMP 连接建立失败。因此，在这种情况下需要手工指定 CWMP 连接接口。

表1-7 配置 CWMP 连接接口

操作	命令	说明
进入系统视图	**system-view**	-
进入CWMP视图	**cwmp**	-
设置CPE上用于连接ACS的接口	**cwmp cpe connect interface** *interface-type interface-number*	必选 缺省情况下，没有配置CPE上用于连接ACS的接口

1.7.3 发送Inform报文

CPE 与 ACS 之间连接的建立过程需要发送 Inform 报文。通过设置 Inform 报文发送参数，可以触发 CPE 向 ACS 自动发起连接。

1. 配置周期性发送Inform报文

表1-8 配置周期性发送 Inform 报文

操作	命令	说明
进入系统视图	**system-view**	-
进入CWMP视图	**cwmp**	-
使能CPE周期发送Inform报文功能	**cwmp cpe inform interval enable**	必选 缺省情况下，CPE周期发送Inform报文功能处于关闭状态

操作	命令	说明
配置CPE发送Inform报文的周期	**cwmp cpe inform interval** *seconds*	可选 缺省情况下，CPE每隔600秒发送一次Inform报文

2. 配置定时发送Inform报文

表1-9 配置定时发送 Inform 报文

操作	命令	说明
进入系统视图	**system-view**	-
进入CWMP视图	**cwmp**	-
配置CPE在指定时刻发送一次Inform报文	**cwmp cpe inform time** *time*	必选 缺省情况下，CPE发送Inform报文的日期和时间为空，即没有配置CPE定时发送Inform报文的时间

1.7.4 配置CPE自动重新连接的次数

当 CPE 向 ACS 请求建立连接失败，或者在会话过程中连接异常中止（CPE 没有收到表示会话正常结束的报文）时，设备可以自动重新发起连接。

表1-10 配置 CPE 自动重新连接的次数

操作	命令	说明
进入系统视图	**system-view**	-
进入CWMP视图	**cwmp**	-
配置当创建连接失败时自动重新连接的次数	**cwmp cpe connect retry** *times*	可选 缺省情况下，自动重新连接的次数为无限次，即设备会一直按照一定周期给ACS发送连接请求

1.7.5 配置CPE无数据传输超时的时间

无数据传输超时时间主要用于以下两种情况：

- 在连接建立过程中，CPE 向 ACS 发送连接请求，但是经过无数据传输超时时间还没有收到响应报文，CPE 将认为连接失败。
- 连接建立后，如果 CPE 与 ACS 在无数据传输超时时间内没有报文交互，CPE 将认为连接失效，并断开连接。

表1-11 配置 CPE 无数据传输超时的时间

操作	命令	说明
进入系统视图	**system-view**	-
进入CWMP视图	**cwmp**	-
配置CPE无数据传输超时的时间	**cwmp cpe wait timeout** *seconds*	可选 缺省情况下，无数据传输超时的时间为30秒

1.7.6 配置CPE的工作模式

当设备作为 CPE 被 ACS 管理时，需要根据设备在网络中的位置，设置设备的工作模式。

- 当设备部署在网吧、小型企业的广域网出口，并且设备下层级联了其它 CPE。此时，如果要求 ACS 能够管理本设备以及下层 CPE，则需要配置设备工作在 gateway 模式。
- 如果设备下层没有级联 CPE 时，可以配置设备工作在 device 模式。

表1-12 配置 CPE 的工作模式

操作	命令	说明
进入系统视图	**system-view**	-
进入CWMP视图	**cwmp**	-
配置CPE的工作模式	**cwmp device-type** { **device** | **gateway** }	可选 缺省情况下，设备作为CPE时工作在gateway模式

注意

切换工作模式前，须关闭 CWMP 功能。否则，不能切换。

1.7.7 配置CWMP引用的SSL客户端策略

CWMP 是基于 HTTP/HTTPS 协议的，CWMP 报文作为 HTTP/HTTPS 报文的数据部分封装在 HTTP/HTTPS 报文中。如果 ACS 的 URL 以“http://”开头，则使用 HTTP 协议，如果 ACS 的 URL 以“https://”开头，则使用 HTTPS 协议。使用 HTTPS 协议时，需要配置该命令，来对 ACS 的身份进行认证，关于 SSL 客户端策略的详细介绍和配置请参见“安全配置指导”中的“SSL”。

表1-13 配置 CWMP 引用的 SSL 客户端策略

操作	命令	说明
进入系统视图	**system-view**	-
进入CWMP视图	**cwmp**	-
配置CWMP引用的SSL客户端策略	**ssl client-policy** *policy-name*	必选 缺省情况下，CWMP没有引用SSL客户端策略

1.8 CWMP显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 CWMP 的运行情况，通过查看显示信息验证配置的效果。

表1-14 cwmp 显示和维护

操作	命令
显示CWMP的当前配置信息	**display cwmp configuration** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

操作	命令
显示CWMP的当前状态信息	**display cwmp status** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.9 CWMP典型配置案例

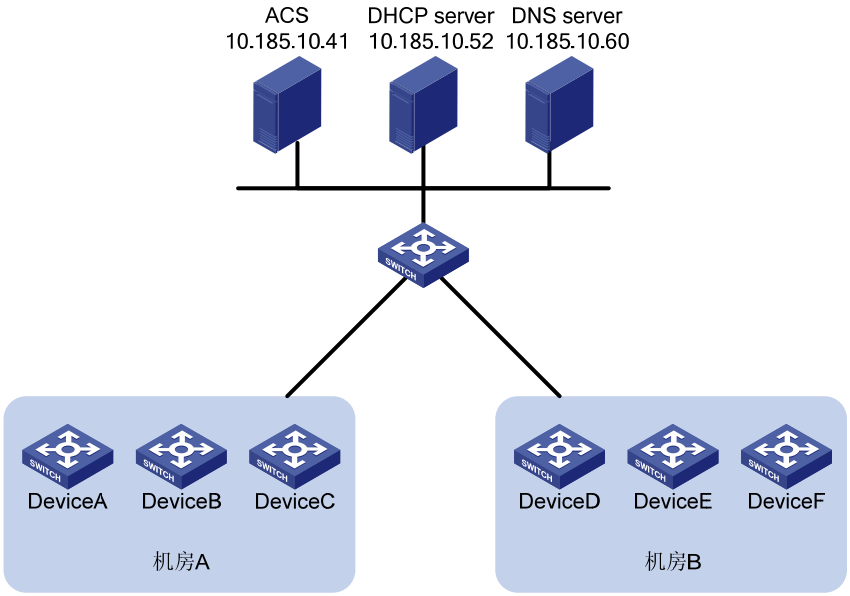
说明

下文中 ACS 的配置需要在安装了 H3C iMC BIMS 软件的服务器上进行。随着软件版本的更新，BIMS 的功能和界面可能会有变化，如您所使用的软件界面与本例中不同，请参阅对应您使用版本的软件用户手册进行配置。

1.9.1 组网需求

某数据中心有两个机房（A 和 B）需要部署大量的设备，目前网络中已存在 ACS 服务器/DHCP 服务器/DNS 服务器，为提高部署效率，要求利用 CWMP 功能为两个机房中的设备分别自动下发不同的配置文件。下面以每个机房内的三台设备为例介绍 CWMP 功能的配置方法。

图1-3 CWMP 典型配置案例组网图



其中部署到两个机房的设备及序列号如 表 1-15 所示：

表1-15 部署到机房的设备列表

机房	设备	序列号
A	DeviceA	210235AOLNH12000008
	DeviceB	210235AOLNH12000010
	DeviceC	210235AOLNH12000015
B	DeviceD	210235AOLNH12000017
	DeviceE	210235AOLNH12000020
	DeviceF	210235AOLNH12000022

网络管理员已经事先为两个机房的设备分别创建了配置文件 sys_a.cfg 和 sys_b.cfg，ACS 服务器的访问用户名和密码分别为“vicky”和“12345”，URL 地址为 http://acs.database:9090/acs。

1.9.2 配置步骤

1. ACS服务器上的配置

在本例中，ACS 服务器上的配置包括以下几项：

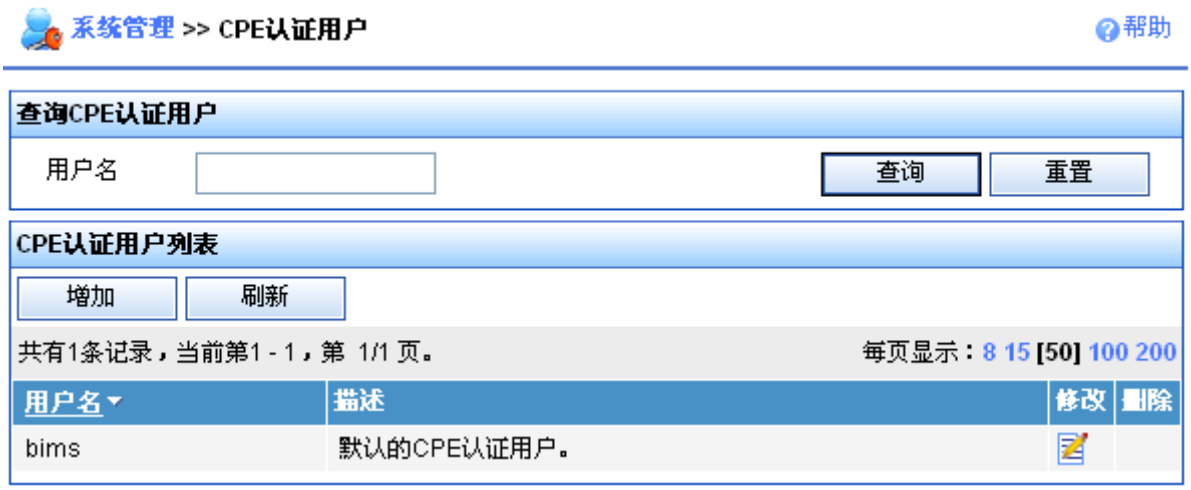
- 访问 ACS 服务器的用户名和密码
- 增加 CPE 设备的信息并将 CPE 划分到不同的组别
- 为不同的 CPE 设备组绑定不同的配置文件

ACS 服务器上的其余配置保持缺省值即可。

在 ACS 服务器上配置用户名和密码。

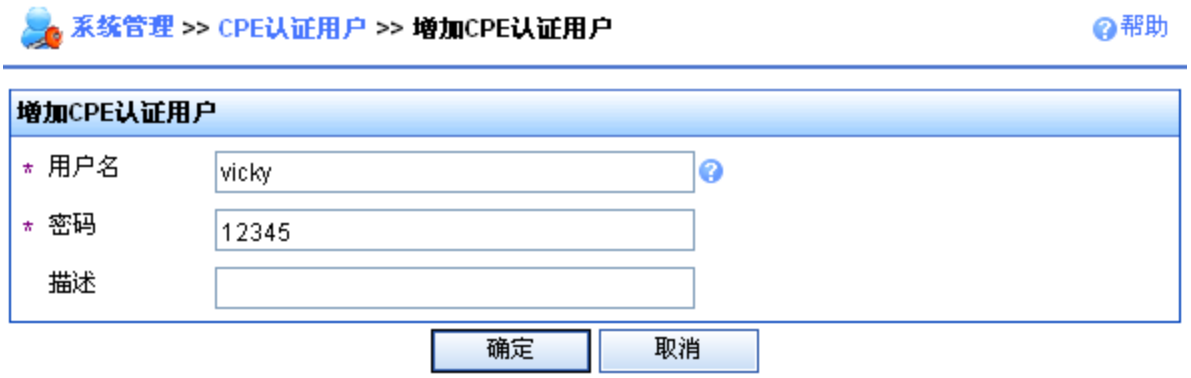
选择“系统管理”页签，单击导航树中的[CPE 认证用户]菜单项，进入 CPE 认证用户管理页面。

图1-4 CPE 认证用户管理页面



单击<增加>按钮，进入增加 CPE 认证用户页面。

图1-5 增加 CPE 认证用户页面



设置用户名、密码及描述后，单击<确定>按钮完成增加操作。

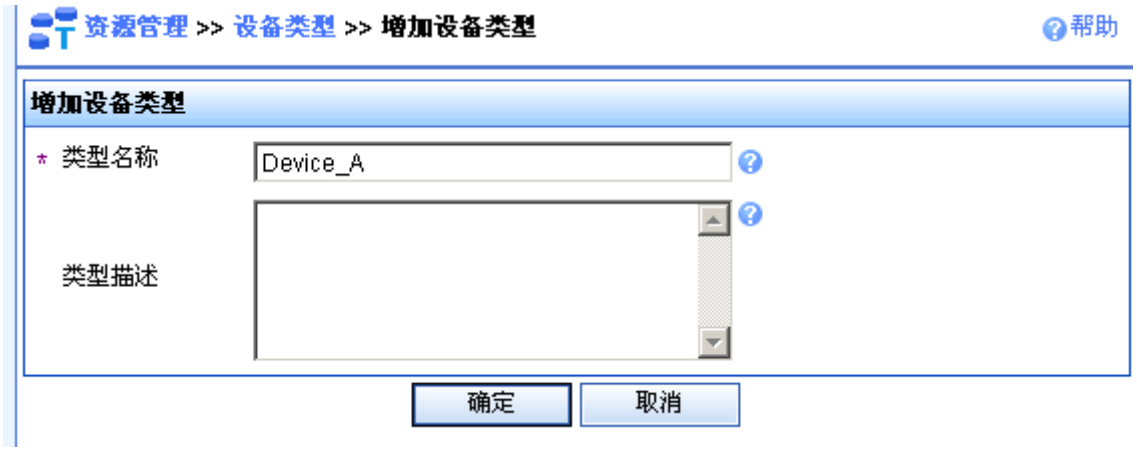
在 ACS 上增加 CPE 设备分组和类型，这里以增加 DeviceA 设备到“DB_1”组的“Device_A”类型为例。选择“资源管理”页签，单击导航树中的[分组管理/设备分组]菜单项，进入设备分组页面后单击<增加>按钮，进入增加设备分组页面。

图1-6 增加设备分组页面

设置分组名称后，单击<确定>按钮完成增加操作。

单击导航树中的[设备类型]菜单项，进入设备类型页面后单击<增加>按钮，进入增加设备类型页面。

图1-7 增加设备类型页面



设置设备类型名称后，单击<确定>按钮完成增加操作。

单击导航树中的[增加设备]菜单项，进入增加设备页面。

图1-8 增加设备页面

设置设备名称及相关信息，并选择设备类型和设备分组后，单击<确定>按钮完成增加操作。

图1-9 增加设备成功页面

重复以上步骤，将 DeviceB 和 DeviceC 设备的信息输入，完成机房 A 中的设备添加任务。

在 ACS 上将配置文件与不同组别的 CPE 设备绑定，实现自动部署。选择导航树中的[部署向导]菜单项，选择[自动部署设备配置/按设备类型]进行自动部署。

图1-10 部署向导页面

在自动部署设备配置页面，选择要部署的配置文件，并将其选择部署为“启动配置”。

图1-11 自动部署设备配置页面

单击[选取类型]按钮，进入设备类型选择页面，选取之前创建的 Device_A 类型，单击<确定>按钮完成选择操作。

图1-12 选取设备类型页面

完成选择页面后将返回自动部署设备配置页面，单击<确定>按钮完成部署任务的创建。

图1-13 部署任务创建成功页面

对于机房 B 中的三台设备，配置步骤基本类似，主要区别如下：

- 需要为机房 B 的设备创建新的设备类型，例如“Device_B”。
- 在增加设备时，将机房 B 中的三台设备加入到 Device_B 类型中。
- 创建部署配置的任务时，将对应机房 B 的配置文件与 Device_B 进行关联。

2. DHCP服务器上的配置

说明

DHCP 服务器的配置以支持 option 43 功能的 H3C 交换机为例进行介绍。如果您使用的是其他 DHCP 服务器，请参阅软件的使用手册。

- 配置地址池，为 CPE 设备分配 IP 地址和 DNS 服务器，此处以分配 10.185.10.0/24 网段的地址为例。

使能 DHCP 服务。

```
<DHCP_server> system-view
[DHCP_server] dhcp enable
```

配置 VLAN 接口 1 工作在 DHCP 服务器模式。

```
[DHCP_server] interface vlan-interface 1
[DHCP_server-Vlan-interface1] dhcp select server global-pool
[DHCP_server-Vlan-interface1] quit
```

配置不参与自动分配的 IP 地址（此处包括 DNS 服务器、ACS 服务器）。

```
[DHCP_server] dhcp server forbidden-ip 10.185.10.41
[DHCP_server] dhcp server forbidden-ip 10.185.10.60
```

配置 DHCP 地址池 0 的共有属性（网段、DNS 服务器地址）。

```
[DHCP_server] dhcp server ip-pool 0
[DHCP_server-dhcp-pool-0] network 10.185.10.0 mask 255.255.255.0
[DHCP_server-dhcp-pool-0] dns-list 10.185.10.60
```

- 配置 option 43 选项。选项内容包括 ACS 的地址、用户名和密码。

将 ACS 的地址、用户名和密码转换成 ASCII 码。其中 URL 地址对应的 ASCII 码为 68 74 74 70 3A 2F 2F 61 63 73 2E 64 61 74 61 62 61 73 65 3A 39 30 39 30 2F 61 63 73。用户名 vicky 对应的 ASCII 码为 76 69 63 6B 79，密码 12345 对应的 ASCII 码为 31 32 33 34 35。

```
[DHCP_server-dhcp-pool-0] option 43 hex 0140 68747470 3A2F2F61 63732E64 61746162 6173653A
39303930 2F616373 20766963 6B792031 32333435
```

3. DNS服务器上的配置

在 DNS 服务器上需要配置域名和地址的映射，将 http://acs.database:9090/acs 地址映射为 http://10.185.1.41:9090/acs。具体配置方法请参见您使用的 DNS 服务器软件手册。

4. 将CPE接入网络

将 CPE 上电并连接网线后，CPE 将按照 CWMP 协议的流程自动从 ACS 处获取配置文件。

5. 在ACS上查看配置效果

选择“资源管理”页签，单击导航树中的[设备交互记录]菜单项，进入设备交互记录查询页面，查看与序列号对应的设备是否已经完成部署配置的操作。

图1-14 设备交互记录界面

目 录

1 报文捕获

仅 R5206 及以上版本支持报文捕获功能。

1.1 报文捕获简介

报文捕获功能使设备能够捕获其收到的报文，提供了一种定位网络问题的途径。使用该功能可以简化报文分析设备和网络监控设备的部署。

捕获的报文存放在设备的缓冲区中，用户可以通过命令行查看捕获的报文，也可以将捕获的报文输出为*.pcap 格式文件，再用报文分析软件（如 Ethereal、Wireshark）进行分析。

1.2 配置报文捕获

配置报文捕获功能时，需要注意：

- 如果报文捕获时引用了 ACL，启动报文捕获后，不能再对 ACL 规则进行修改（包括向该 ACL 中添加、删除和修改规则）。
- 如果报文捕获时引用了 ACL，则忽略 ACL 规则的动作，报文匹配只使用 ACL 中的分类域。
- 完成报文捕获后，建议使用 **undo packet capture** 命令停止本功能，以释放系统资源。

表1-1 配置报文捕获

操作		命令	说明
设置报文捕获参数		**packet capture** { **acl** { *acl-number* | **ipv6** *acl6-number* } | **buffer-size** *size* | **length** *capture-length* | **mode** { **circular** | **linear** } }*	可选
启动报文捕获	立刻启动报文捕获（可同时设置报文捕获参数）	**packet capture start** [**acl** { *acl-number* | **ipv6** *acl6-number* } | **buffer-size** *size* | **length** *capture-length* | **mode** { **circular** | **linear** } | [**packets** *packet-number* | **seconds** *second-number*]]*	二者必选其一 缺省情况下，报文捕获功能处于停止状态，报文捕获计划未设置 如果使用**packet capture start**命令，已配置的报文捕获计划将被取消
	配置报文捕获计划	**packet capture schedule datetime** *time date*	
暂停报文捕获		**packet capture stop**	可选 在查看、保存或清除报文缓冲区中的内容之前，需要暂停报文捕获 系统会在以下任何一种情况下自动暂停报文捕获： • 报文捕获模式为缺省的线性模式，且报文缓冲区写满； • 捕获的报文数量超过上限； • 报文捕获持续时间超过上限
保存报文捕获缓冲区中的内容		**packet capture buffer save** [*filename*]	可选 请将.pcap作为保存的文件名后缀

1.3 报文捕获显示和维护

在任意视图下执行 **display packet capture status** 命令可以即时查看当前报文捕获状态和已使用的缓冲区长度。

执行 **packet capture stop** 命令后，可以在任意视图下使用 **display packet capture buffer** 命令查看缓冲区中的内容，也可以在用户视图下执行 **reset packet capture buffer** 命令来清除缓冲区中的内容，以便进行新的报文捕获任务。

表1-2 报文捕获显示和维护

操作	命令
查看当前报文捕获状态	**display packet capture status**
查看当前报文捕获缓冲区中的内容	**display packet capture buffer** [*start-index* [*end-index*]] [**length** *display-length*]
清除报文捕获缓冲区中的内容	**reset packet capture buffer**

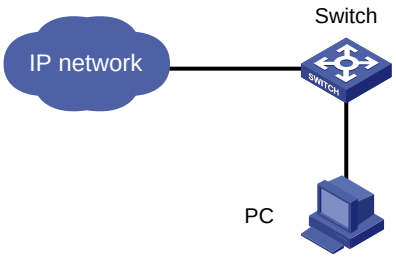
1.4 报文捕获典型配置举例

1. 组网需求

在 Switch 上捕获该设备收到的来自 192.168.1.0/24 网段的报文，通过命令行将报文捕获结果保存为*.pcap 文件，以便连接到 Switch 的 PC 下载该文件，再用报文分析软件进行分析。

2. 组网图

图1-1 报文捕获应用组网图



3. 配置步骤

(1) 启动报文捕获

为 IPv4 基本 ACL 2000 创建规则：匹配来自 192.168.1.0/24 网段的报文。

```
<Switch> system-view
[Switch] acl number 2000
[Switch-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Switch-acl-basic-2000] quit
[Switch] quit
```

设置 Switch 捕获按 ACL 2000 过滤的报文，并启动报文捕获。

```
<Switch> packet capture start acl 2000
```

查看报文捕获状态。

```
<Switch> display packet capture status
```

```
  Current status :          In process
  Mode :                    Linear
  Buffer size :             2097152 (bytes)
  Buffer used :             1880 (bytes)
  Max capture length :      68 (bytes)
  ACL information :         Basic or advanced IPv4 ACL 2000
  Schedule datetime:        Unspecified
  Upper limit of duration : Unspecified (seconds)
  Duration :                13 (seconds)
  Upper limit of packets :  Unspecified
  Packets count :           10
```

由此可见，报文捕获正在进行。

(2) 保存报文捕获结果

暂停报文捕获。

```
<Switch> packet capture stop
```

将报文缓冲区中的内容保存为 test.pcap 文件。

```
<Switch> packet capture buffer save test.pcap
```

显示当前目录下的目录和文件信息。

```
<Switch> dir
Directory of flash:/

   0     -rw-      1860  Sep 21 2012 12:52:58   test.pcap
   1     drw-         -  Apr 26 2012 12:00:38   seclog
   2     -rw-  10479398  Apr 26 2012 12:26:39   logfile.log
```

由此可见，报文捕获缓冲区的内容已成功保存。

完成报文捕获后，停止报文捕获功能，释放系统资源。

```
<Switch> undo packet capture
```

连接到 Switch 的 PC 可以通过 FTP 或者 TFTP 工具访问设备，将*.pcap 文件复制到 PC 上，再用 Wireshark 等报文分析软件进行处理。