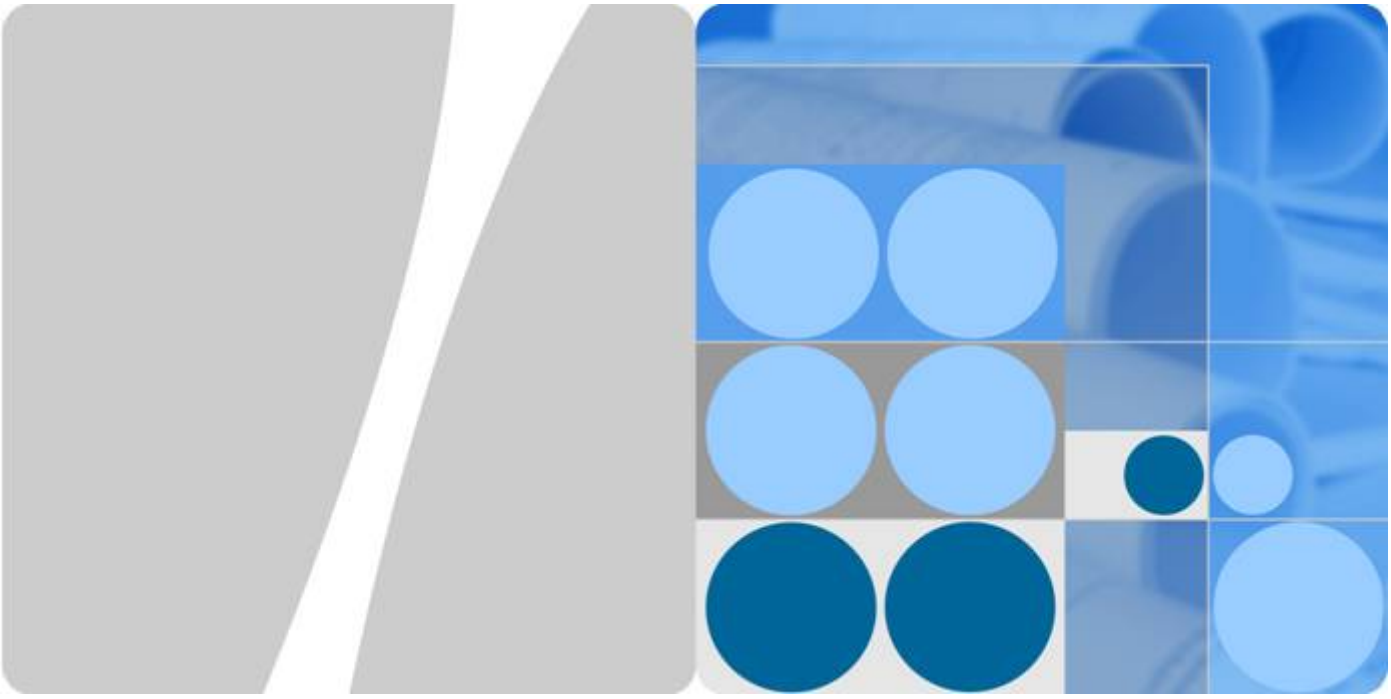


Huawei AR3200 系列企业路由器

V200R002C00

配置指南-网络管理

文档版本　02

发布日期　2012-03-30

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

前 言

读者对象

本文档介绍了 AR3200 中网络管理特性的基本概念、在不同应用场景中的配置过程和配置举例。

本文档提供了网络管理的配置方法。

本文档主要适用于以下工程师：

- 数据配置工程师
- 调测工程师
- 网络监控工程师
- 系统维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
危险	以本标志开始的文本表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。
警告	以本标志开始的文本表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
注意	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
窍门	以本标志开始的文本能帮助您解决某个问题或节省您的时间。
说明	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。

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 | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... } *	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...] *	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&前面的参数可以重复 1 ～ n 次。
#	由“#”开始的行表示为注释行。

接口编号约定

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

修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 02 (2012-03-30)

相对于版本 01（2011-12-30）的变化如下：

修改：

- **1.1.1 SNMP 概述**

文档版本 01 (2011-12-30)

第一次正式发布。

目 录

1 SNMP 配置

关于本章

简单网络管理协议 SNMP（Simple Network Management Protocol）是广泛用于 TCP/IP 网络的网络管理标准协议。SNMP 提供了一种通过运行网络管理软件的中心计算机（即网络管理工作站 NMS）来管理网元的方法。共有三个版本 SNMPv1、SNMPv2c 和 SNMPv3，用户可以根据情况选择同时配置一个或多个版本。

1.1 SNMP 简介
SNMP 为网管和设备间的通信提供一套标准协议，保证网管能够正常的管理设备和接收设备的告警。

1.2 配置设备使用 SNMPv1 与网管通信
配置 SNMPv1 功能后，网管和设备之间将使用 SNMPv1 进行通信。为了保证网管和设备之间的正常通信，需要配置网管侧和 Agent 侧，本节只介绍 Agent 侧的配置，网管侧的配置请参考网管的操作手册。

1.3 配置设备使用 SNMPv2c 与网管通信
配置 SNMPv2c 功能后，网管和设备之间将使用 SNMPv2c 进行通信。为了保证网管和设备之间的正常通信，需要配置网管侧和 Agent 侧，本节只介绍 Agent 侧的配置，网管侧的配置请参考网管的操作手册。

1.4 配置设备使用 SNMPv3 与网管通信
配置 SNMPv3 功能后，网管和设备之间将使用 SNMPv3 进行通信。为了保证网管和设备之间的正常通信，需要配置网管侧和 Agent 侧，本节只介绍 Agent 侧的配置，网管侧的配置请参考网管的操作手册。

1.5 SNMP 配置举例
介绍 SNMP 的配置。请结合配置思路了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

1.1 SNMP 简介

SNMP 为网管和设备间的通信提供一套标准协议，保证网管能够正常的管理设备和接收设备的告警。

1.1.1 SNMP 概述

网管通过在被管理设备中运行的 Agent 客户端上执行 GET-SET 操作来管理设备上的节点，设备上的节点由 MIB（Management Information Base）来唯一标识。

随着网络业务的日益发展，现有的网络中，设备数量日益庞大，且这些设备与网络管理员所在的中心机房距离较远。当这些设备发生故障时，由于设备无法主动上报故障，导致网络管理员无法及时感知、及时定位和排除故障，从而导致网络的维护效率降低，维护工作量大大增加。

为了解决这个问题，设备制造商已经在一些设备中提供了网络管理的功能，这样网管就可以远程询问设备的状态，同样设备能够在特定类型的事件发生时向网络管理工作站发出警告。

SNMP 就是规定网管站和设备之间如何传递管理信息的应用层协议。SNMP 定义了网管管理设备的几种操作，以及设备故障时能向网管主动发送告警。

网管使用 SNMP 协议管理设备时，存在网管站、Agent 和被管理设备三个角色。网管通过管理信息库 MIB 来唯一标识和管理设备上的节点。网管管理设备的操作包括：GetRequest、GetNextRequest、GetResponse、GetBulk、SetRequest、以及设备主动发送告警。关于角色、MIB 和操作的定义和作用请参考下面的具体内容。

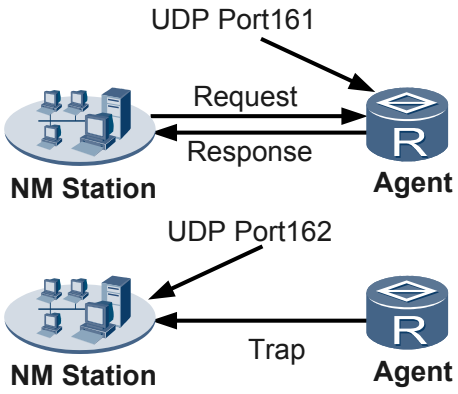
SNMP 定义的三类角色

在网管通过 SNMP 协议管理设备过程中，定义了三类角色：

- 网管站：向被管理设备发送各种查询报文，以及接收被管理设备发送的告警。
- Agent：驻留在被管理设备上的一个进程。Agent 的作用如下：
  - 接收、解析来自网管站的查询报文。
  - 根据报文类型对管理变量进行 Read 或 Write 操作，并生成响应报文，返回给网管站。
  - 根据各协议模块对告警触发条件的定义，在达到触发条件后，如进入、退出系统视图或设备重新启动等，相应的模块通过 Agent 主动向网管站发送告警，报告所发生的事件。
- 被管理设备：接受网管的管理，产生和主动上报告警。

网管站与 Agent 的关系如图 1-1 所示。

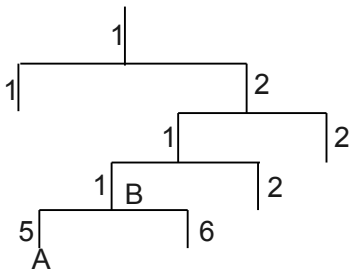
图 1-1 SNMP 结构示意图



MIB

为了在 SNMP 报文中唯一标识设备中的管理对象，SNMP 用层次结构命名方案来识别管理对象，整个层次结构就象一棵树，树的节点表示管理对象，如图 1-2 所示，它可以用从根开始的一条路径进行识别。

图 1-2 MIB 树结构



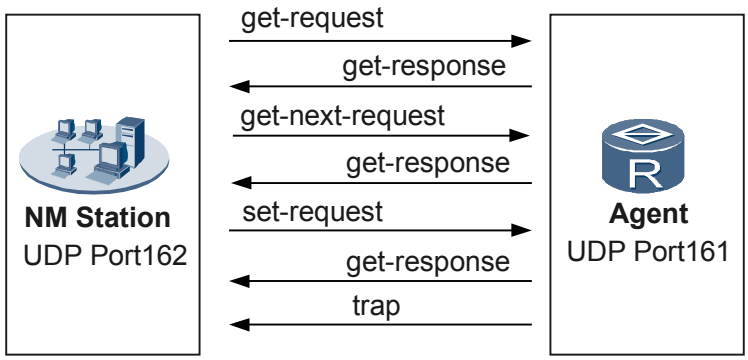
在图 1-2 中，管理对象 B 可以用一串数字{1.2.1.1}唯一确定，这串数字是管理对象的客体标识符（Object Identifier）。而 MIB 的作用就是用来描述树的层次结构，它是所监控网络设备的标准变量定义的集合。

用户可以采用管理信息库标准 MIB，也可以按标准方式定义自己的 MIB。使用标准 MIB 能够降低部署代理部件的成本，从而降低整个网管系统的成本。

SNMP 操作

SNMP 以 GET-SET 操作方式替代复杂的命令集，利用如图 1-3 的操作实现全部功能。

图 1-3 SNMP 操作示意图



SNMP 的操作如表 1-1 所示。

表 1-1 SNMP 的操作

操作	功能
GetRequest	从某变量中取值，获取设备某功能节点状态，是网管向设备发出的请求。
GetNextRequest	在 MIB 表项中取下一项值，获取设备某功能的另一节点状态，是网管向设备发出的请求。
GetResponse	对 GetRequest、GetNextRequest、SetRequest 的响应，是设备向网管的回应。
GetBulk	该操作相当于连续执行多次 GetNextRequest 操作，是网管向设备发出的请求。
SetRequest	设置具体变量的值，对设备功能节点状态进行调整，是网管向设备发出的指令。
Trap	报告事件信息，是设备主动向网管报告事件。

说明

SNMP 协议用于网管对网络设备自身进行监控和管理，不能对网络整体运行情况进行监控和管理。如需要对网络整体运行情况进行监控和管理，比如了解网络性能情况、统计网络数据等，请参考《配置指南 网络管理》中 Netstream 配置、故障和性能管理配置。

1.1.2 AR3200 支持的 SNMP 特性

通过对 SNMP 协议各个版本特性支持情况的对比，以及各个版本适用的应用场景介绍，为用户进行网络部署时选取 SNMP 协议的版本提供参考依据。

AR3200 系统中支持 SNMPv1、SNMPv2c 和 SNMPv3 三个协议版本。各特性的功能如表 1-2 所示，各版本支持的特性列表如表 1-3 所示，SNMP 各版本的应用场景如表 1-4 所示，用户可以根据现网的运营情况，选择需要的版本使网管和被管理设备之间进行通信。

说明

在网络中存在多个网管管理同一设备的情况，各网管站可能选用不同的 SNMP 协议版本与设备进行通信。为了满足这些网管和设备的正常通信，可以在设备上同时部署 SNMPv1、v2c、v3。

表 1-2 SNMP 支持的特性功能介绍

特性	功能描述
访问控制	访问控制主要用来限制管理设备的用户的权限。通过该功能可以限制指定的用户管理设备上的指定节点，从而提升精细化管理。
认证加密	认证加密主要是通过对网管和被管理设备传送的报文进行认证和加密，避免数据报文被窃取或篡改，从而提升数据传输的安全性。
错误码	错误码用来标识特定的故障现象，有助于管理员快速定位和解决故障，因此错误码越丰富越有利于管理员对设备进行管理。
Trap 告警	Trap 告警是被管理设备主动向网管发送告警。以便管理员能够及时发现设备的异常。 被管理设备发送 Trap 告警后，不需要网管进行接收确认。
GetBulk	GetBulk 主要方便管理员进行批量的 Getnext 操作。网络规模较大时，以节省管理员的工作量，提升管理效率。

表 1-3 SNMP 各版本支持的特性概况

特性列表	SNMPv1	SNMPv2c	SNMPv3
访问控制	基于团体名进行访问控制	基于团体名进行访问控制	基于用户和用户组进行访问控制
认证加密	不支持	不支持	支持认证和加密，认证和加密的方式如下： 认证： ● MD5 ● SHA 加密：DES56
错误码	支持 6 个错误码	支持 16 个错误码	支持 16 个错误码
Trap 告警	支持	支持	支持
GetBulk	不支持	支持	支持

表 1-4 SNMP 各版本的应用场景

版本	应用场景
SNMPv1	适用于小型网络，组网简单，对网络安全性要求不高或者网络环境本身比较安全，且比较稳定的网络，比如校园网，小型企业网。
SNMPv2c	适用于大中型网络，对网络安全性要求不高或者网络环境本身比较安全（比如 VPN 网络），但业务比较繁忙，有可能发生流量拥塞的网络。
SNMPv3	适用于各种规模的网络，尤其是对网络的安全性要求较高，确保合法的管理员才能对网络设备进行管理的网络。比如网管和被管理设备间的通信数据需要在公网上进行传输。

如果用户是统一规划建设新网络，建议根据上面的应用场景选择 SNMP 协议的版本。如果用户是网络扩建或升级，建议用户根据网管使用的版本选择在设备上配置对应的 SNMP 协议版本，保证设备和网管的通信。

1.2 配置设备使用 SNMPv1 与网管通信

配置 SNMPv1 功能后，网管和设备之间将使用 SNMPv1 进行通信。为了保证网管和设备之间的正常通信，需要配置网管侧和 Agent 侧，本节只介绍 Agent 侧的配置，网管侧的配置请参考网管的操作手册。

网管管理设备主要体现在两方面：

- 网管主动管理设备，进行 GetRequest、GetNextRequest、GetResponse、GetBulk、SetRequest 操作，获取需要的数据并进行相应设置。
- 网管被动接收被管理设备发送的告警，根据告警定位和处理设备故障。

下面的配置过程中，进行基本功能配置后，网管就可以和被管理设备之间进行上面两种管理方式的操作。如果希望进一步的精细化管理，比如进行精细的访问控制、指定发送告警的模块等，可以参考下面的配置步骤。

1.2.1 建立配置任务

在配置网管使用 SNMPv1 管理设备功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

用户希望通过网管统一管理网络设备时，需要部署 SNMP 协议，保证网管和被管理设备间的正常通信。

当用户的网络规模较小，网络设备较少，且网络设备环境本身比较安全时（比如校园网、小型企业网），可以选择使用 SNMPv1 保证网管和设备间的通信。

前置任务

在完成配置网管使用 SNMPv1 管理设备功能之前，需完成以下任务：

- 配置路由协议，使路由器和网管站之间可达

数据准备

在配置网管使用 SNMPv1 管理设备功能之前，需要准备以下数据：

序号	数据
1	SNMP 协议的版本、SNMP 的团体名、告警目的主机地址、管理员的联系方法和位置
2	（可选）访问控制列表号、网管站的 IP 地址、MIB 的节点
3	（可选）发送告警的模块名称、Trap 报文的源地址、Trap 报文的队列长度、Trap 报文的保存时间

1.2.2 配置 SNMPv1 的基本功能

配置 SNMP 的基本功能后，网管即可与被管理设备间进行基本的监控和管理操作，比如 GET 和 SET 相关数据，被管理设备主动向网管发送告警。

背景信息

配置 SNMP 的基本功能中，步骤 3、步骤 4、步骤 5、步骤 6 为必须配置，配置完成后网管和被管理设备之间可以进行基本通信。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （可选）执行命令 **snmp-agent**，启动 SNMP Agent 服务。

缺省情况下，没有启动 SNMP Agent 服务。执行任意携带 **snmp-agent** 参数的命令都可以触发 SNMP Agent 服务启动，故该步骤可选。

步骤 3 执行命令 **snmp-agent sys-info version v1**，配置 SNMP 的协议版本。

缺省情况下，使能 SNMPv1、SNMPv2c 和 SNMPv3。

步骤 4 执行命令 **snmp-agent community** { **read** | **write** } *community-name*，配置设备的读写团体名。

- 需要网管在指定视图下具有只读权限时（比如级别比较低的管理员），使用 **read** 参数。
- 需要网管在指定视图下具有读写权限时（比如级别比较高的管理员），使用 **write** 参数。

配置设备的读写团体名之后，如果不配置 MIB 视图，使用该团体名的网管拥有 Viewdefault 视图的权限。

步骤 5 执行命令 **snmp-agent target-host trap-paramsname** *paramsname* **v1 securityname** *securityname* [**binding-private-value**] [**private-netmanager**]，配置设备发送 Trap 报文的参数信息。

步骤 6 执行命令 **snmp-agent target-host trap-hostname** *hostname* **address** *ipv4-addr* [**udp-port** *udp-portid*] [**public-net** | **vpn-instance** *vpn-instance-name*] **trap-paramsname** *paramsname*，配置设备发送告警和错误码的目的主机。

请参考下面的说明对参数进行选取：

- 目的 UDP 端口号缺省是 162，如果有特殊需求（比如避免知名端口号被攻击配置了端口镜像），可以配置 **udp-port** 将 UDP 端口号更改为非知名端口号，保证网管和被管理设备的正常通信。
- 如果被管理设备发送的告警需要通过公网传递给网管时，选择参数 **public-net**；如果被管理设备发送的告警需要通过私网传递给网管时，选择参数 **vpn-instance** *vpn-instance-name*，指定告警需要穿越的 VPN 实例。

步骤 7 （可选）执行命令 **snmp-agent sys-info** { **contact** *contact* | **location** *location* }，配置设备管理员的联系方法和位置。

当网管管理较多设备时，为了方便设备管理员记录设备管理员的联系方式和位置，在设备异常时快速联系设备管理员进行故障排除和定位，可配置该功能。

如果需要同时配置设备管理员的联系方法和位置，请执行两次该命令分别配置管理员的联系方法和位置。

----结束

后续处理

如果需要进行更精细化的管理，比如：

- 需要使用该团体名中的指定网管（比如指定 IP 地址的网管）可以管理设备的指定节点，请参考**限制网管对设备的访问权限**进行配置。
- 需要被管理设备上指定模块的告警发送到网管，请参考**配置向网管系统发送告警**进行配置。
- 如果用户使用的网管和被管理设备是华为的设备，可以选择**配置 SNMP 扩展错误码功能**，以便设备可以发送更多类型的错误码，精确定位更多类型的错误，方便用户定位和解决设备故障。

1.2.3 （可选）限制网管对设备的访问权限

通过限定指定地址的网管管理设备，以及限定网管管理的 MIB 节点，可以增强网管和被管理设备使用 SNMP 进行通信时的安全性。

背景信息

当有多个网管使用同一个团体名管理同一设备时：

- 如果需要所有网管拥有 Viewdefault 视图（即 1.3.6.1）的权限时，下面的步骤可以全部省略。

- 如果需要使用该团体名的某些网管拥有 Viewdefault 视图（即 1.3.6.1）的权限时，步骤 5 可以省略。
- 如果需要使用该团体名的所有网管管理设备上的指定节点，步骤 2、步骤 3、步骤 4 可以省略。
- 如果需要使用该团体名的某些网管管理设备上的指定节点，请配置下面的所有步骤。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl** *acl-number*，创建一个基本访问控制列表，过滤管理设备的网管用户。

步骤 3 执行命令 **rule** [*rule-id*] { **deny** | **permit** } **source** { *source-ip-address source-wildcard* | **any** }，配置 ACL 规则。

步骤 4 执行命令 **quit**，退回至系统视图。

步骤 5 执行命令 **snmp-agent mib-view** *view-name* { **include** | **exclude** } *subtree-name* [**mask** *mask*]，创建 MIB 视图并限定网管监控和管理的 MIB 节点。

缺省情况下，拥有视图 Viewdefault（即 1.3.6.1）的权限。

- 需要网管管理设备上的绝大部分 MIB 节点，只有一少部分节点不允许网管管理时，或者在现有的 MIB 视图中希望取消网管对某些节点的访问权限时，使用参数 **exclude**，排除这些 MIB 节点。
- 需要网管管理设备上的一少部分 MIB 节点，绝大部分节点不允许网管管理时，或者在现有的 MIB 视图中添加网管对某些节点的访问权限时，使用参数 **include**，添加这些允许管理的 MIB 节点。

步骤 6 执行命令 **snmp-agent community** { **read** | **write** } *community-name* [**mib-view** *view-name* | **acl** *acl-number*]*，限制网管对设备的访问权限。

- 希望网管在指定视图下具有只读权限时（比如级别比较低的管理员），使用 **read** 参数。希望网管在指定视图下具有读写权限时（比如级别比较高的管理员），使用 **write** 参数。
- 如果需要使用该团体名的某些网管拥有视图 viewdefault（即 1.3.6.1）的权限，参数 **mib-view** *view-name* 可以省略。
- 如果需要使用该团体名的所有网管管理设备上的某些节点，参数 **acl** *acl-number* 可以省略。
- 如果需要使用该团体名的某些网管管理设备上的某些节点，**acl** 和 **mib-view** 都需要配置。

----结束

后续处理

限制网管对设备的访问权限后，尤其是限制网管的 IP 地址后，当网管的 IP 地址发生变更时（比如位置变更、网络调整 IP 地址重新分配等），请修改 ACL 中相关 IP 地址的配置，否则导致网管无法继续访问。

1.2.4 （可选）配置 SNMP 扩展错误码功能

当网管和被管理设备是华为设备时，通过配置 SNMP 扩展错误码，可以扩展标准错误码，扩展更多的错误场景，方便用户能够更加准确和快速的定位和排除故障。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent extend error-code enable**，使能 SNMP 扩展错误码功能。

缺省情况下，SNMP 发送标准错误码，只有使能了扩展错误码功能后，才能向网管发送扩展错误码。

----结束

1.2.5 （可选）配置向网管发送告警

配置向网管发送告警可以设定发送指定的告警，方便用户定位重要的问题。指定发送告警的相关参数，可以增加告警发送的可靠性。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent trap enable**，使能发送 Trap 报文。

步骤 3 执行命令 **snmp-agent trap source** *interface-type interface-number*，指定发送 Trap 的源端接口。

指定源接口后，将以源接口 IP 地址作为发送的 Trap 报文的源 IP 地址。为了保证设备的安全性，发送的源地址最好配置为本地的 loopback 地址。

路由器端配置的 Trap 报文的源接口和网管站配置的路由器发送报文的接口需要一致，否则会引起网管站无法接收 Trap 报文的情况。

步骤 4 执行命令 **snmp-agent trap queue-size** *size*，设置发往目的主机的 Trap 报文的消息队列长度。

为了保证 Trap 报文能够被网管接收到，根据 Trap 报文产生的多少来决定 Trap 队列的长度，在路由器发送 Trap 信息比较频繁时，可以适当的把队列长度加长，减少告警丢失的发生。

步骤 5 执行命令 **snmp-agent trap life** *seconds*，设置 Trap 报文的保存时间。

为了保证 Trap 报文能够被网管接收到，根据 Trap 报文产生的多少来决定保存的时间，在路由器发送 Trap 信息比较频繁时，可以使用此命令配置增加报文的保存时间，减少告警丢失的发生。

----结束

1.2.6 检查配置结果

配置 SNMPv1 成功后，用户可以查看到 SNMPv1 的配置情况。

前提条件

已经完成 SNMPv1 基本功能的所有配置。

操作步骤

- 执行 **display snmp-agent community** { **read** | **write** }命令查看当前配置的团体名。

- 执行 **display snmp-agent sys-info version** 命令查看 SNMP 使能的版本信息。
- 执行 **display acl** *acl-number* 命令显示配置的访问控制列表的规则。
- 执行 **display snmp-agent mib-view** 命令查看 MIB 视图信息。
- 执行 **display snmp-agent sys-info contact** 命令查看管理员的联系方式。
- 执行 **display snmp-agent sys-info location** 命令查看设备的位置。
- 执行 **display current-configuration | include trap** 命令查看 Trap 配置信息。
- 执行 **display snmp-agent extend error-code status** 命令查看 SNMP 扩展错误码功能使能情况。

----结束

任务示例

在配置成功时，执行 **display snmp-agent community read** 命令，查看配置的团体名信息。

```
<Huawei> display snmp-agent community read
   Community name: huawei
   Storage type: nonVolatile
   View name: ViewDefault
   Acl: 2001

   Total number is 1
```

执行 **display snmp-agent sys-info version** 命令，查看当前代理中运行的 SNMP 版本号。

```
<Huawei> display snmp-agent sys-info version
 SNMP version running in the system:
          SNMPv1
```

执行 **display acl** *acl-number* 命令，查看配置的访问控制列表的规则。

```
<Huawei> display acl 2000
Basic ACL  2000, 1 rule
Acl's step is 5
 rule 5 permit source 1.1.1.1 0
```

执行 **display snmp-agent mib-view** 命令查看 MIB 视图。

```
<Huawei> display snmp-agent mib-view
   View name:ViewDefault
   MIB Subtree:internet
   Subtree mask:
   Storage type: nonVolatile
   View Type:included
   View status:active
   View name:ViewDefault
   MIB Subtree:snmpUsmMIB
   Subtree mask:
   Storage type: nonVolatile
   View Type:excluded
   View status:active
   View name:ViewDefault
   MIB Subtree:snmpVacmMIB
   Subtree mask:
   Storage type: nonVolatile
   View Type:excluded
   View status:active
   View name:ViewDefault
   MIB Subtree:snmpModules.18
   Subtree mask:
   Storage type: nonVolatile
   View Type:excluded
   View status:active

   Total number is 1
```

执行 **display snmp-agent sys-info contact** 命令，查看当前设备节点的联系信息。

```
<Huawei> display snmp-agent sys-info contact
  The contact person for this managed node:
          R&D Beijing, Huawei Technologies co.,Ltd.
```

执行 **display snmp-agent sys-info location** 命令，查看当前设备节点的物理位置信息。

```
<Huawei> display snmp-agent sys-info location
  The physical location of this node:
          Beijing China
```

执行 **display current-configuration | include trap** 命令，查看 trap 配置信息。

```
<Huawei> display current-configuration | include trap
 snmp-agent trap enable
```

执行 **display snmp-agent extend error-code status** 命令，查看 SNMP 扩展错误码的使能情况。

```
<Huawei> display snmp-agent extend error-code status
 Extend error-code status:enabled
```

1.3 配置设备使用 SNMPv2c 与网管通信

配置 SNMPv2c 功能后，网管和设备之间将使用 SNMPv2c 进行通信。为了保证网管和设备之间的正常通信，需要配置网管侧和 Agent 侧，本节只介绍 Agent 侧的配置，网管侧的配置请参考网管的操作手册。

网管管理设备主要体现在两方面：

- 网管主动管理设备，进行 GetRequest、GetNextRequest、GetResponse、GetBulk、SetRequest 操作，获取需要的数据并进行相应设置。
- 网管被动接收被管理设备发送的告警，根据告警定位和处理设备故障。

下面的配置过程中，进行基本功能配置后，网管就可以和被管理设备之间进行上面两种管理方式的操作。如果希望进一步的精细化管理，比如进行精细的访问控制、指定发送告警的模块等，可以参考下面的配置步骤。

1.3.1 建立配置任务

在配置网管使用 SNMPv2c 管理设备功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

用户希望通过网管统一管理网络设备时，需要部署 SNMP 协议，保证网管和被管理设备间的正常通信。

当用户的网络规模较大，网络设备较多，对网络安全性要求不高或者网络环境本身比较安全（比如 VPN 网络），但业务比较繁忙，有可能发生流量拥塞时，可以选择使用 SNMPv2c 保证网管和设备间的通信。

前置任务

在完成配置网管使用 SNMPv2c 管理设备功能之前，需完成以下任务：

- 配置路由协议，使路由器和网管站之间可达

数据准备

在配置网管使用 SNMPv2c 管理设备功能之前，需要准备以下数据：

序号	数据
1	SNMP 协议的版本、SNMP 的团体名、告警目的主机地址、管理员的联系方法和位置
2	（可选）访问控制列表号、网管站的 IP 地址、MIB 的节点
3	（可选）发送告警的模块名称、Trap 报文的源地址、Trap 报文的队列长度、Trap 报文的保存时间

1.3.2 配置 SNMPv2c 的基本功能

配置 SNMP 的基本功能后，网管即可与被管理设备间进行基本的监控和管理操作，比如 GET 和 SET 相关数据，被管理设备主动向网管发送告警。

背景信息

配置 SNMP 的基本功能中，步骤 3、步骤 4、步骤 5、步骤 6、步骤 7 为必须配置，配置完成后网管和被管理设备之间可以进行基本通信。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （可选）执行命令 **snmp-agent**，启动 SNMP Agent 服务。

缺省情况下，没有启动 SNMP Agent 服务。执行任意携带 **snmp-agent** 参数的命令都可以触发 SNMP Agent 服务启动，故该步骤可选。

步骤 3 执行命令 **snmp-agent sys-info version v2c**，配置 SNMP 的协议版本。

缺省情况下，使能 SNMPv1、SNMPv2c 和 SNMPv3。

步骤 4 执行命令 **snmp-agent community** { **read** | **write** } *community-name*，配置设备的读写团体名。

- 需要网管在指定视图下具有只读权限时（比如级别比较低的管理员），使用 **read** 参数。
- 需要网管在指定视图下具有读写权限时（比如级别比较高的管理员），使用 **write** 参数。

配置设备的读写团体名之后，如果不配置 MIB 视图，使用该团体名的网管拥有 Viewdefault 视图的权限。

步骤 5 执行命令 **snmp-agent target-host trap-paramsname** *paramsname* **v2c securityname** *securityname* [**binding-private-value**] [**private-netmanager**]，配置设备发送 Trap 报文的参数信息。

步骤 6 执行命令 **snmp-agent target-host trap-hostname** *hostname* **address** *ipv4-addr* [**udp-port** *udp-portid*] [**public-net** | **vpn-instance** *vpn-instance-name*] **trap-paramsname** *paramsname*,配置设备发送告警和错误码的目的主机。

请参考下面的说明对参数进行选取：

- 目的 UDP 端口号缺省是 162，如果有特殊需求（比如避免知名端口号被攻击配置了端口镜像），可以配置 **udp-port** 将 UDP 端口号更改为非知名端口号，保证网管和被管理设备的正常通信。
- 如果被管理设备发送的告警需要通过公网传递给网管时，选择参数 **public-net**；如果被管理设备发送的告警需要通过私网传递给网管时，选择参数 **vpn-instance** *vpn-instance-name*，指定告警需要穿越的 VPN 实例。

步骤 7 （可选）执行命令 **snmp-agent sys-info** { **contact** *contact* | **location** *location* }，配置设备管理员的联系方法和位置。

当网管管理较多设备时，为了方便设备管理员记录设备管理员的联系方式和位置，在设备异常时快速联系设备管理员进行故障排除和定位，可配置该功能。

如果需要同时配置设备管理员的联系方法和位置，请执行两次该命令分别配置管理员的联系方法和位置。

----结束

后续处理

如果需要进行更精细化的管理，比如：

- 需要使用该团体名中的指定网管（比如指定 IP 地址的网管）可以管理设备的指定节点，请参考**限制网管对设备的访问权限**进行配置。
- 需要被管理设备上指定模块的告警发送到网管，请参考**配置向网管系统发送告警**进行配置。
- 如果用户使用的网管和被管理设备是华为的设备，可以选择**配置 SNMP 扩展错误码功能**，以便设备可以发送更多类型的错误码，精确定位更多类型的错误，方便用户定位和解决设备故障。

1.3.3 （可选）限制网管对设备的访问权限

通过限定指定地址的网管管理设备，以及限定网管管理的 MIB 节点，可以增强网管和被管理设备使用 SNMP 进行通信时的安全性。

背景信息

当有多个网管使用同一个团体名管理同一设备时：

- 如果需要所有网管拥有 Viewdefault 视图（即 1.3.6.1）的权限时，下面的步骤可以全部省略。
- 如果需要使用该团体名的某些网管拥有 Viewdefault 视图（即 1.3.6.1）的权限时，**步骤 5** 可以省略。
- 如果需要使用该团体名的所有网管管理设备上的指定节点，**步骤 2**、**步骤 3**、**步骤 4** 可以省略。
- 如果需要使用该团体名的某些网管管理设备上的指定节点，请配置下面的所有步骤。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl** *acl-number*，创建一个基本访问控制列表，过滤管理设备的网管用户。

步骤 3 执行命令 **rule** [*rule-id*] { **deny** | **permit** } **source** { *source-ip-address source-wildcard* | **any** }，配置 ACL 规则。

步骤 4 执行命令 **quit**，退回至系统视图。

步骤 5 执行命令 **snmp-agent mib-view** *view-name* { **include** | **exclude** } *subtree-name* [**mask** *mask*]，创建 MIB 视图并限定网管监控和管理的 MIB 节点。

缺省情况下，拥有视图 Viewdefault（即 1.3.6.1）的权限。

- 需要网管管理设备上的绝大部分 MIB 节点，只有一少部分节点不允许网管管理时，或者在现有的 MIB 视图中希望取消网管对某些节点的访问权限时，使用参数 **exclude**，排除这些 MIB 节点。
- 需要网管管理设备上的一少部分 MIB 节点，绝大部分节点不允许网管管理时，或者在现有的 MIB 视图中添加网管对某些节点的访问权限时，使用参数 **include**，添加这些允许管理的 MIB 节点。

步骤 6 执行命令 **snmp-agent community** { **read** | **write** } *community-name* [**mib-view** *view-name* | **acl** *acl-number*]*，限制网管对设备的访问权限。

- 希望网管在指定视图下具有只读权限时（比如级别比较低的管理员），使用 **read** 参数。希望网管在指定视图下具有读写权限时（比如级别比较高的管理员），使用 **write** 参数。
- 如果需要使用该团体名的某些网管拥有视图 viewdefault（即 1.3.6.1）的权限，参数 **mib-view** *view-name* 可以省略。
- 如果需要使用该团体名的所有网管管理设备上的某些节点，参数 **acl** *acl-number* 可以省略。
- 如果需要使用该团体名的某些网管管理设备上的某些节点，**acl** 和 **mib-view** 都需要配置。

----结束

后续处理

限制网管对设备的访问权限后，尤其是限制网管的 IP 地址后，当网管的 IP 地址发生变更时（比如位置变更、网络调整 IP 地址重新分配等），请修改 ACL 中相关 IP 地址的配置，否则导致网管无法继续访问。

1.3.4 （可选）配置 SNMP 扩展错误码功能

当网管和被管理设备是华为设备时，通过配置 SNMP 扩展错误码，可以扩展标准错误码，扩展更多的错误场景，方便用户能够更加准确和快速的定位和排除故障。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent extend error-code enable**，使能 SNMP 扩展错误码功能。

缺省情况下，SNMP 发送标准错误码，只有使能了扩展错误码功能后，才能向网管发送扩展错误码。

----结束

1.3.5 （可选）配置向网管发送告警

配置向网管发送告警可以设定发送指定的告警，方便用户定位重要的问题。指定发送告警的相关参数，可以增加告警发送的可靠性。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent trap enable**，使能发送 Trap 报文。

步骤 3 执行命令 **snmp-agent trap source** *interface-type interface-number*，指定发送 Trap 的源端接口。

指定源接口后，将以源接口 IP 地址作为发送的 Trap 报文的源 IP 地址。为了保证设备的安全性，发送的源地址最好配置为本地的 loopback 地址。

路由器端配置的 Trap 报文的源接口和网管站配置的路由器发送报文的接口需要一致，否则会引起网管站无法接收 Trap 报文的情况。

步骤 4 执行命令 **snmp-agent trap queue-size** *size*，设置发往目的主机的 Trap 报文的消息队列长度。

为了保证 Trap 报文能够被网管接收到，根据 Trap 报文产生的多少来决定 Trap 队列的长度，在路由器发送 Trap 信息比较频繁时，可以适当的把队列长度加长，减少告警丢失的发生。

步骤 5 执行命令 **snmp-agent trap life** *seconds*，设置 Trap 报文的保存时间。

为了保证 Trap 报文能够被网管接收到，根据 Trap 报文产生的多少来决定保存的时间，在路由器发送 Trap 信息比较频繁时，可以使用此命令配置增加报文的保存时间，减少告警丢失的发生。

----结束

1.3.6 检查配置结果

配置 SNMPv2c 成功后，用户可以查看到 SNMPv2c 的配置情况。

前提条件

已经完成 SNMPv2c 基本功能的所有配置。

操作步骤

- 执行 **display snmp-agent community** { **read** | **write** }命令查看当前配置的团体名。
- 执行 **display snmp-agent sys-info version** 命令查看 SNMP 使能的版本信息。
- 执行 **display acl** *acl-number* 命令显示配置的访问控制列表的规则。
- 执行 **display snmp-agent mib-view** 命令查看 MIB 视图信息。
- 执行 **display snmp-agent sys-info contact** 命令查看管理员的联系方式。
- 执行 **display snmp-agent sys-info location** 命令查看设备的位置。
- 执行命令 **display current-configuration | include trap**,查看 Trap 配置信息。
- 执行 **display snmp-agent target-host** 命令查看目标主机的信息。

- 执行 **display snmp-agent extend error-code status** 命令查看 SNMP 扩展错误码功能使能情况。

----结束

任务示例

在配置成功后，执行 **display snmp-agent community** 命令，查看配置的团体名信息。

```
<Huawei> display snmp-agent community read
   Community name: huawei
   Storage type: nonVolatile
   View name: ViewDefault
   Acl: 2001

   Total number is 1
```

执行 **display snmp-agent sys-info version** 命令，查看当前代理中运行的 SNMP 版本号。

```
<Huawei> display snmp-agent sys-info version
 SNMP version running in the system:
          SNMPv2c
```

执行 **display acl** *acl-number* 命令，查看配置的访问控制列表的规则。

```
<Huawei> display acl 2000
Basic ACL  2000, 1 rule
Acl's step is 5
 rule 5 permit source 1.1.1.1 0
```

执行 **display snmp-agent mib-view** 命令查看 MIB 视图。

```
<Huawei> display snmp-agent mib-view
   View name:ViewDefault
   MIB Subtree:internet
   Subtree mask:
   Storage type: nonVolatile
   View Type:included
   View status:active
   View name:ViewDefault
   MIB Subtree:snmpUsmMIB
   Subtree mask:
   Storage type: nonVolatile
   View Type:excluded
   View status:active
   View name:ViewDefault
   MIB Subtree:snmpVacmMIB
   Subtree mask:
   Storage type: nonVolatile
   View Type:excluded
   View status:active
   View name:ViewDefault
   MIB Subtree:snmpModules.18
   Subtree mask:
   Storage type: nonVolatile
   View Type:excluded
   View status:active

   Total number is 1
```

执行 **display snmp-agent sys-info contact** 命令，查看当前设备节点的联系信息。

```
<Huawei> display snmp-agent sys-info contact
   The contact person for this managed node:
          R&D Beijing, Huawei Technologies co.,Ltd.
```

执行 **display snmp-agent sys-info location** 命令，查看当前设备节点的物理位置信息。

```
<Huawei> display snmp-agent sys-info location
   The physical location of this node:
          Beijing China
```

执行 **display current-configuration | include trap** 命令查看 trap 配置信息。

```
<Huawei> display current-configuration | include trap
 snmp-agent trap enable
```

执行 **display snmp-agent extend error-code status** 命令查看 SNMP 扩展错误码的使能情况。

```
<Huawei> display snmp-agent extend error-code status
 Extend error-code status:enabled
```

执行 **display snmp-agent target-host** 命令查看目标主机的信息。

```
<Huawei> display snmp-agent target-host
   Traphost list:
   Target host name: nsm2
   Traphost address: 1.1.1.2
   Traphost portnumber: 162
   Target host parameter: trapnsm2

   Total number is 1

   Parameter list trap target host:
   Parameter name of the target host: trapnsm2
   Message mode of the target host: SNMPV2C
   Trap version of the target host: v2c
   Security name of the target host: 1.1.3.1

   Total number is 1
```

1.4 配置设备使用 SNMPv3 与网管通信

配置 SNMPv3 功能后，网管和设备之间将使用 SNMPv3 进行通信。为了保证网管和设备之间的正常通信，需要配置网管侧和 Agent 侧，本节只介绍 Agent 侧的配置，网管侧的配置请参考网管的操作手册。

网管管理设备主要体现在两方面：

- 网管主动管理设备，进行 GetRequest、GetNextRequest、GetResponse、GetBulk、SetRequest 操作，获取需要的数据并进行相应设置。
- 网管被动接收被管理设备发送的告警，根据告警定位和处理设备故障。

下面的配置过程中，进行基本功能配置后，网管就可以和被管理设备之间进行上面两种管理方式的操作。如果希望进一步的精细化管理，比如进行精细的访问控制、指定发送告警的模块等，可以参考下面的配置步骤。

1.4.1 建立配置任务

在配置网管使用 SNMPv3 管理设备功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

用户希望通过网管统一管理网络设备时，需要部署 SNMP 协议，保证网管和被管理设备间的正常通信。

当用户的网络对安全性要求较高，只有合法的管理员才能对网络设备进行管理，并且传输的网络数据需要保证其安全性和准确性时，比如网管和被管理设备间的通信数据需要在公网上进行传输，可以部署 SNMPv3，通过 SNMPv3 的认证和加密功能确保数据传输的安全性，保证网管和被管理设备之间的正常通信。

前置任务

在完成配置网管使用 SNMPv3 管理设备功能之前，需完成以下任务：

- 配置路由协议，使路由器和网管站之间可达

数据准备

在配置网管使用 SNMPv3 管理设备功能之前，需要准备以下数据：

序号	数据
1	SNMP 协议的版本、用户和用户组的名称、告警目的主机地址、管理员的联系方法和位置
2	（可选）访问控制列表号、网管站的 IP 地址、MIB 的节点
3	（可选）发送告警的模块名称、Trap 报文的源地址、Trap 报文的队列长度、Trap 报文的保存时间

1.4.2 配置 SNMPv3 的基本功能

配置 SNMP 的基本功能后，网管即可与被管理设备间进行基本的监控和管理操作，比如 GET 和 SET 相关数据，被管理设备主动向网管发送告警。

背景信息

配置 SNMP 的基本功能中，步骤 4、步骤 5、步骤 6 为必须配置，配置完成后网管和被管理设备之间可以进行基本通信。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （可选）执行命令 **snmp-agent**，启动 SNMP Agent 服务。

缺省情况下，没有启动 SNMP Agent 服务。执行任意携带 **snmp-agent** 参数的命令都可以触发 SNMP Agent 服务启动，故该步骤可选。

步骤 3 （可选）执行命令 **snmp-agent sys-info version v3**，配置 SNMP 的协议版本。

缺省情况下，使能 SNMPv1、SNMPv2c 和 SNMPv3。

步骤 4 执行命令 **snmp-agent group v3** *group-name* { **authentication** | **noauth** | **privacy** }，配置 SNMPv3 用户组。

当网管和设备处在不安全的网络环境中时，比如容易遭受攻击等，建议用户配置参数 **authentication** 或 **privacy**，使能数据的认证和加密功能。

用户可以选择的认证加密模式如下：

- 配置 **authentication** 参数：只认证不加密。适用于网络环境安全，但管理员比较多，管理员对设备交叉操作比较频繁的情况下。通过认证可以限制拥有权限的管理员才可以访问该设备。

- 配置 **noauth** 参数：不认证不加密。适用于网络环境安全，且管理员比较固定的情况下。
- 配置 **privacy** 参数：既认证又加密。适用于网络环境不太安全，管理员交叉操作多的情况下。通过认证和加密既可以限制特定的管理员访问设备，并且使网络数据以加密形式发送，避免网络数据被窃取，造成关键数据泄露。

步骤 5 执行命令 **snmp-agent usm-user v3** *user-name group-name* [**authentication-mode** { **md5** | **sha** } *authkey* [**privacy-mode** { **aes128** | **des56** } *prikey* | **plain-text**]] [**acl** *standard-acl*]，配置 SNMPv3 用户信息。

说明

在配置用户的安全级别时，必须确保其安全级别不低于所加入的组的安全级别，否则无法进行正常的通信。如果配置的用户安全级别为不认证不加密，则用户的访问权限限制在 MIB-2 的范围内，且只有只读权限。

用户组和用户配置完成后，使用该用户名的网管拥有 Viewdefault 视图（即 1.3.6.1）的权限。

用户组使能认证和加密功能后，用户可以选择认证和加密的方式，对网络传输的数据进行认证和加密。

- 认证方式
  - MD5（Message Digest 5）：MD5 通过输入任意长度的消息，产生 128bit 的消息摘要。
  - SHA-1（Secure Hash Algorithm）：SHA-1 通过输入长度小于 2 的 64 次方比特的消息，产生 160bit 的消息摘要。

  MD5 算法的计算速度比 SHA-1 算法快，而 SHA-1 算法的安全强度比 MD5 算法高。
- 加密方式
  - AES 使用 128bit 的密钥对一个 128bit 的明文块进行加密。
  - DES 使用 56bit 的密钥对一个 64bit 的明文块进行加密。

步骤 6 执行命令 **snmp-agent target-host trap-paramsname** *paramsname* **v3 securityname** *securityname* { **authentication** | **noauthnopriv** | **privacy** } [**binding-private-value**] [**private-netmanager**]，配置设备发送 Trap 报文的参数信息。

步骤 7 执行命令 **snmp-agent target-host trap-hostname** *hostname* **address** *ipv4-addr* [**udp-port** *udp-portid*] [**public-net** | **vpn-instance** *vpn-instance-name*] **trap-paramsname** *paramsname*,配置设备发送告警和错误码的目的主机。

请参考下面的说明对参数进行选取：

- 目的 UDP 端口号缺省是 162，如果有特殊需求（比如避免知名端口号被攻击配置了端口镜像），可以配置 **udp-port** 将 UDP 端口号更改为非知名端口号，保证网管和被管理设备的正常通信。
- 如果被管理设备发送的告警需要通过公网传递给网管时，选择参数 **public-net**；如果被管理设备发送的告警需要通过私网传递给网管时，选择参数 **vpn-instance** *vpn-instance-name*，指定告警需要穿越的 VPN 实例。

步骤 8（可选）执行命令 **snmp-agent sys-info** { **contact** *contact* | **location** *location* }，配置设备管理员的联系方法和位置。

当网管管理较多设备时，为了方便设备管理员记录设备管理员的联系方式和位置，在设备异常时快速联系设备管理员进行故障排除和定位，可配置该功能。

如果需要同时配置设备管理员的联系方法和位置，请执行两次该命令分别配置管理员的联系方法和位置。

----结束

后续处理

如果需要进行更精细化的管理，比如：

- 需要使用该用户组中的指定网管（比如指定 IP 地址的网管）可以管理设备的指定节点，请参考**限制网管对设备的访问权限**进行配置。
- 需要被管理设备上指定模块的告警发送到网管，请参考**配置向网管系统发送告警**进行配置。
- 如果用户使用的网管和被管理设备是华为的设备，可以选择**配置 SNMP 扩展错误码功能**，以便设备可以发送更多类型的错误码，精确定位更多类型的错误，方便用户定位和解决设备故障。

1.4.3 （可选）限制网管对设备的访问权限

通过限定指定地址的网管管理设备，以及限定网管管理的 MIB 节点，可以增强使用 SNMPv3 进行通信的网管和被管理设备的安全性。

背景信息

当有多个网管使用同一个用户组名管理同一设备时：

- 如果需要所有网管拥有 Viewdefault 视图（即 1.3.6.1）的权限时，下面的步骤可以全部省略。
- 如果需要使用用户组名的某些网管拥有 Viewdefault 视图（即 1.3.6.1）的权限时，**步骤 5** 可以省略。
- 如果需要使用用户组名的所有网管管理设备上的指定节点，**步骤 2**、**步骤 3**、**步骤 4** 可以省略。
- 如果需要使用用户组名的某些网管管理设备上的指定节点，请配置下面的所有步骤。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl** *acl-number*，创建一个基本访问控制列表，过滤管理设备的网管用户。

步骤 3 执行命令 **rule** [*rule-id*] { **deny** | **permit** } **source** { *source-ip-address source-wildcard* | **any** }，配置 ACL 规则。

步骤 4 执行命令 **quit**，退回至系统视图。

步骤 5 执行命令 **snmp-agent mib-view** *view-name* { **include** | **exclude** } *subtree-name* [**mask** *mask*]，创建 MIB 视图并限定网管监控和管理的 MIB 节点。

缺省情况下，拥有视图 viewdefault（即 1.3.6.1）的权限。

- 需要网管管理设备上的绝大部分 MIB 节点，只有一少部分节点不允许网管管理时，或者在现有的 MIB 视图中希望取消网管对某些节点的访问权限时，使用参数 **exclude**，排除这些 MIB 节点。

- 需要网管管理设备上的一少部分 MIB 节点，绝大部分节点不允许网管管理时，或者在现有的 MIB 视图中添加网管对某些节点的访问权限时，使用参数 **include**，添加这些允许管理的 MIB 节点。

步骤 6 执行命令 **snmp-agent group v3** *group-name* { **authentication** | **noauth** | **privacy** } [**read-view** *read-view* | **write-view** *write-view* | **notify-view** *notify-view* | **acl** *acl-number*]*，配置用户组的读写权限。

- 希望网管在指定视图下具有只读权限时（比如级别比较低的管理员），使用 **read-view** 参数。希望网管在指定视图下具有读写权限时（比如级别比较高的管理员），使用 **write-view** 参数。
- 用户希望筛选部分重要告警，过滤掉无关告警时，选择配置 **notify-view** 参数，限制被管理设备向网管发送告警的 MIB 节点。配置该参数后，设备产生的告警中匹配 **notify-view** 指定的 MIB 节点的告警才能发送到该用户的网管。
- 为了加强安全性，用户可以选择配置 **authentication** 或 **privacy** 参数，**authentication** 对用户只认证不加密，**privacy** 对用户既认证又加密，具体请参考**认证和加密选取原则**。
- 如果需要使用该用户组的某些网管拥有视图 viewdefault（即 1.3.6.1）的权限，参数 [**read-view** *read-view* | **write-view** *write-view* | **notify-view** *notify-view*]可以省略。
- 如果需要使用该用户组的所有网管管理设备上的某些节点，参数 **acl** *acl-number* 可以省略。
- 如果需要使用该用户组的某些网管管理设备上的某些节点，ACL 和 MIB 视图都需要配置。

----结束

后续处理

限制网管对设备的访问权限后，尤其是限制网管的 IP 地址后，当网管的 IP 地址发生变更时（比如位置变更、网络调整 IP 地址重新分配等），请修改 ACL 中相关 IP 地址的配置，否则导致网管无法继续访问。

1.4.4 （可选）配置 SNMP 扩展错误码功能

当网管和被管理设备是华为设备时，通过配置 SNMP 扩展错误码，可以扩展标准错误码，扩展更多的错误场景，方便用户能够更加准确和快速的定位和排除故障。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent extend error-code enable**，使能 SNMP 扩展错误码功能。

缺省情况下，SNMP 发送标准错误码，只有使能了扩展错误码功能后，才能向网管发送扩展错误码。

----结束

1.4.5 （可选）配置向网管发送告警

配置向网管发送告警可以设定发送指定的告警，方便用户定位重要的问题。指定发送告警的相关参数，可以增加告警发送的可靠性。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent trap enable**，使能发送 Trap 报文。

步骤 3 执行命令 **snmp-agent trap source** *interface-type interface-number*，指定发送 Trap 的源端接口。

指定源接口后，将以源接口 IP 地址作为发送的 Trap 报文的源 IP 地址。为了保证设备的安全性，发送的源地址最好配置为本地的 loopback 地址。

路由器端配置的 Trap 报文的源接口和网管站配置的路由器发送报文的接口需要一致，否则会引起网管站无法接收 Trap 报文的情况。

步骤 4 执行命令 **snmp-agent trap queue-size** *size*，设置发往目的主机的 Trap 报文的消息队列长度。

为了保证 Trap 报文能够被网管接收到，根据 Trap 报文产生的多少来决定 Trap 队列的长度，在路由器发送 Trap 信息比较频繁时，可以适当的把队列长度加长，减少告警丢失的发生。

步骤 5 执行命令 **snmp-agent trap life** *seconds*，设置 Trap 报文的保存时间。

为了保证 Trap 报文能够被网管接收到，根据 Trap 报文产生的多少来决定保存的时间，在路由器发送 Trap 信息比较频繁时，可以使用此命令配置增加报文的保存时间，减少告警丢失的发生。

----结束

1.4.6 检查配置结果

配置 SNMPv3 成功后，用户可以查看到 SNMPv3 的配置情况。

前提条件

已经完成 SNMPv3 基本功能的所有配置。

操作步骤

- 执行 **display snmp-agent usm-user** [*user-name*]命令查看用户信息。
- 执行 **display snmp-agent sys-info version** 命令查看 SNMP 使能的版本信息。
- 执行 **display acl** *acl-number* 命令显示配置的访问控制列表的规则。
- 执行 **display snmp-agent mib-view** 命令查看 MIB 视图信息。
- 执行 **display snmp-agent sys-info contact** 命令查看管理员的联系方式。
- 执行 **display snmp-agent sys-info location** 命令查看设备的位置。
- 执行 **display snmp-agent extend error-code status** 命令查看 SNMP 扩展错误码功能使能情况。

----结束

任务示例

执行 **display snmp-agent usm-user** 命令，查看 SNMP 用户信息。

```
<Huawei> display snmp-agent usm-user
```

```
  User name: testuser
  Engine ID: 000007DB7F00000100004C3F
  Group name: testgroup
  Authentication mode: md5, Privacy mode: des56
  Storage type: nonVolatile
  User status: active

  Total number is 1
```

执行 **display snmp-agent sys-info version** 命令，查看当前代理中运行的 SNMP 版本号。

```
<Huawei> display snmp-agent sys-info version
 SNMP version running in the system:
          SNMPv3
```

执行 **display acl** *acl-number* 命令，查看配置的访问控制列表的规则。

```
<Huawei> display acl 2000
Basic ACL  2000, 1 rule
Acl's step is 5
 rule 5 permit source 1.1.1.1 0
```

执行 **display snmp-agent mib-view** 命令查看 MIB 视图。

```
<Huawei> display snmp-agent mib-view
  View name:ViewDefault
  MIB Subtree:internet
  Subtree mask:
  Storage type: nonVolatile
  View Type:included
  View status:active
  View name:ViewDefault
  MIB Subtree:snmpUsmMIB
  Subtree mask:
  Storage type: nonVolatile
  View Type:excluded
  View status:active
  View name:ViewDefault
  MIB Subtree:snmpVacmMIB
  Subtree mask:
  Storage type: nonVolatile
  View Type:excluded
  View status:active
  View name:ViewDefault
  MIB Subtree:snmpModules.18
  Subtree mask:
  Storage type: nonVolatile
  View Type:excluded
  View status:active

  Total number is 1
```

执行 **display snmp-agent sys-info contact** 命令，查看当前设备节点的联系信息。

```
<Huawei> display snmp-agent sys-info contact
  The contact person for this managed node:
          R&D Beijing, Huawei Technologies co.,Ltd.
```

执行 **display snmp-agent sys-info location** 命令，查看当前设备节点的物理位置信息。

```
<Huawei> display snmp-agent sys-info location
  The physical location of this node:
          Beijing China
```

执行 **display current-configuration | include trap** 命令，查看 trap 配置信息。

```
<Huawei> display current-configuration | include trap
 snmp-agent trap enable
```

执行 **display snmp-agent extend error-code status** 命令，查看 SNMP 扩展错误码的使能情况。

```
<Huawei> display snmp-agent extend error-code status
 Extend error-code status:enabled
```

1.5 SNMP 配置举例

介绍 SNMP 的配置。请结合配置思路了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

1.5.1 配置设备使用 SNMPv1 与网管通信示例

网管在管理设备时使用 SNMPv1 版本保证互通，在互通的过程中限制指定的网管可以管理设备上的部分 MIB 节点。

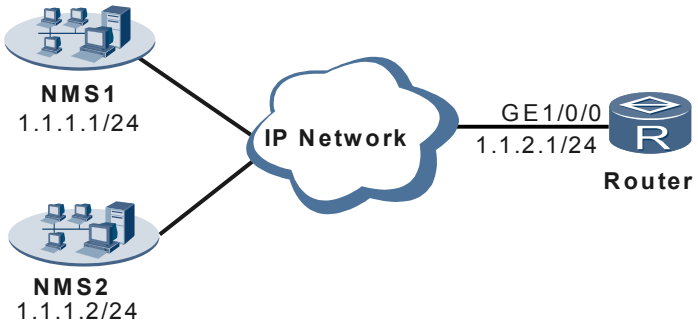
组网需求

如图 1-4 所示，在网络中，用户的两个网管和同一设备通过公网相连，由于业务的需求，用户规划网管 NMS2 仅可以管理该设备上的 DNS 节点，网管站 NMS1 不再管理该设备。

NMS2 管理设备的过程中，为了方便对告警信息进行定位，避免过多的无用告警对处理问题造成干扰，用户只允许缺省打开的模块可以发送告警至 NMS。

由于网管管理员离被管理设备较远，为了使设备出现故障时网管管理员能快速联系上该设备管理员，以便对故障进行快速定位和排除，故要求在设备上配置设备管理员的联系方法。

图 1-4 配置使用 SNMPv1 与网管通信组网图



配置思路

采用如下思路配置网管功能：

1. 使能 SNMP Agent。
2. 配置 SNMP 版本为 SNMPv1。
3. 配置用户访问权限，限制 NMS2 仅可以管理设备上的 DNS 节点。
4. 配置设备的 Trap 功能，使设备产生的告警能够发送至 NMS。
5. 配置管理员的联系方法。
6. 配置网管站。

数据准备

为完成此配置，需要准备如下数据：

- SNMP 版本
- 团体名称
- ACL 号
- NMS 地址
- 管理员联系方法

操作步骤

步骤 1 配置路由器和网管站之间路由可达（略）

步骤 2 使能 SNMP Agent

```
<Huawei> system-view
[Huawei] snmp-agent
```

步骤 3 配置 SNMP 的版本为 v1

```
[Huawei] snmp-agent sys-info version v1
```

查看配置的 SNMP 的版本信息。

```
[Huawei] display snmp-agent sys-info version
  SNMP version running in the system:
          SNMPv1
```

步骤 4 配置用户访问权限

配置 ACL，限制 NMS2 可以管理设备，NMS1 不允许管理设备。

```
[Huawei] acl 2001
[Huawei-acl-basic-2001] rule 5 permit source 1.1.1.2 0.0.0.0
[Huawei-acl-basic-2001] rule 6 deny source 1.1.1.1 0.0.0.0
[Huawei-acl-basic-2001] quit
```

配置 MIB 视图，限制 NMS2 仅可以管理设备上的 DNS 节点。

```
[Huawei] snmp-agent mib-view dnsmib include 1.3.6.1.4.1.2011.5.25.194
```

配置团体名引用 ACL 和 MIB 视图。

```
[Huawei] snmp-agent community write adminnms2 mib-view dnsmib acl 2001
```

步骤 5 配置告警功能

```
[Huawei] snmp-agent target-host trap-paramsname trapnms2 v1 securityname adminnms2
[Huawei] snmp-agent target-host trap-hostname nms2 address 1.1.1.2 trap-paramsname trapnms2
[Huawei] snmp-agent trap queue-size 200
[Huawei] snmp-agent trap life 60
[Huawei] snmp-agent trap enable
```

步骤 6 配置管理员联系方法

```
[Huawei] snmp-agent sys-info contact call Operator at 010-12345678
```

步骤 7 配置网管

网管的配置请根据采用的网管产品参考对应的网管配置手册。

步骤 8 验证配置结果

配置完成后，可以执行下面的命令，检查配置内容是否生效。

查看团体名的配置信息。

```
<Huawei> display snmp-agent community write
   Community name:adminnms2
   Storage type: nonVolatile
   View name: dnsmib
   Acl:2001

   Total number is 1
```

查看 ACL 配置。

```
<Huawei> display acl 2001
Basic ACL 2001, 2 rules
Acl's step is 5
 rule 5 permit source 1.1.1.2 0
 rule 6 deny source 1.1.1.1 0
```

查看 MIB 视图。

```
<Huawei> display snmp-agent mib-view dnsmib
   View name:dnsmib
   MIB Subtree:hwDnsMIB
   Subtree mask:
   Storage type: nonVolatile
   View Type:included
   View status:active
```

查看告警的目标主机。

```
<Huawei> display snmp-agent target-host
   Traphost list:
   Target host name: nms2
   Traphost address: 1.1.1.2
   Traphost portnumber: 162
   Target host parameter: trapnms2

   Total number is 1

   Parameter list trap target host:
   Parameter name of the target host: trapnms2
   Message mode of the target host: SNMPV1
   Trap version of the target host: v1
   Security name of the target host: adminnms2

   Total number is 1
```

当有告警信息产生时，执行命令 **display trapbuffer** 查看告警信息。

```
<Huawei> display trapbuffer
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 98

#Oct 11 2010 18:57:59+00:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011
.5.25.191.3.1 configurations have been changed. The current change number is 95,
 the change loop count is 0, and the maximum number of records is 4095.
```

查看管理员的联系方法。

```
<Huawei> display snmp-agent sys-info contact
The contact person for this managed node:
          call Operator at 010-12345678
```

----结束

配置文件

路由器的配置文件

```
#
acl number 2001
 rule 5 permit source 1.1.1.2 0
 rule 6 deny source 1.1.1.1 0
#
interface GigabitEthernet1/0/0
 ip address 1.1.2.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 1.1.2.0 0.0.0.255
#
 snmp-agent local-engineid 000007DB7FFFFFFF00001AA7
 snmp-agent community write adminnms2 mib-view dnsmib acl 2001
 snmp-agent sys-info contact call Operator at 010-12345678
 snmp-agent sys-info version v1
 snmp-agent target-host trap-hostname nms2 address 1.1.1.2 udp-port 162 trap-paramsname trapnms2
 snmp-agent target-host trap-paramsname trapnms2 v1 securityname adminnms2
 snmp-agent mib-view dnsmib include hwDnsMIB
 snmp-agent trap enable
 snmp-agent trap queue-size 200
 snmp-agent trap life 60
 snmp-agent
#
return
```

1.5.2 配置设备使用 SNMPv2c 与网管通信示例

网管在管理设备时使用 SNMPv2c 版本保证互通，在互通的过程中限制指定的网管可以管理设备上的部分 MIB 节点。

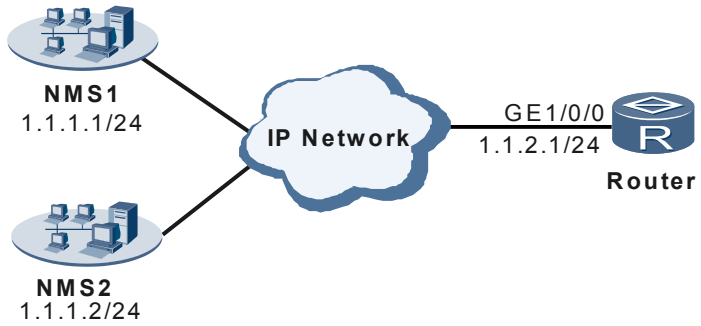
组网需求

如图 1-5 所示，在网络中，用户的两个网管和同一设备通过公网相连，由于业务的需求，用户规划网管 NMS2 仅可以管理设备上的 DNS 节点，网管站 NMS1 不再管理该设备。

NMS2 管理设备的过程中，为了方便对告警信息进行定位，避免过多的无用告警对处理问题造成干扰，用户只允许缺省打开的模块可以发送告警至 NMS。

由于网管管理员离被管理设备较远，为了使设备出现故障时网管管理员能快速联系上被管理设备管理员，以便对故障进行定位和排除，故要求在设备上配置设备管理员的联系方法。

图 1-5 配置使用 SNMPv2c 管通信组网图



配置思路

采用如下思路配置网管功能：

1. 使能 SNMP Agent。
2. 配置 SNMP 版本为 SNMPv2c。
3. 配置用户访问权限，限制 NMS2 仅可以管理设备上的 DNS 节点。
4. 配置管理员的联系方法。
5. 配置网管站。

数据准备

为完成此配置，需要准备如下数据：

- SNMP 版本
- 团体名称
- ACL 号
- NMS 地址
- 管理员联系方法

操作步骤

步骤 1 配置路由器和网管站之间路由可达（略）

步骤 2 使能 SNMP Agent

```
<Huawei> system-view
[Huawei] snmp-agent
```

步骤 3 配置 SNMP 的版本信息为 v2c

```
[Huawei] snmp-agent sys-info version v2c
```

查看配置的 SNMP 的版本信息。

```
[Huawei] display snmp-agent sys-info version
  SNMP version running in the system:
        SNMPv2c
```

步骤 4 配置用户访问权限

配置 ACL，限制 NMS2 可以管理设备，NMS1 不允许管理设备。

```
[Huawei] acl 2001
[Huawei-acl-basic-2001] rule 5 permit source 1.1.1.2 0.0.0.0
[Huawei-acl-basic-2001] rule 6 deny source 1.1.1.1 0.0.0.0
[Huawei-acl-basic-2001] quit
```

配置 MIB 视图。

```
[Huawei] snmp-agent mib-view dnsmib include 1.3.6.1.4.1.2011.5.25.194
```

配置团体名引用 ACL 和 MIB 视图。

```
[Huawei] snmp-agent community write adminnms2 mib-view dnsmib acl 2001
```

步骤 5 配置告警功能

```
[Huawei] snmp-agent target-host trap-paramsname trapnms2 v2c securityname adminnms2
[Huawei] snmp-agent target-host trap-hostname nms2 address 1.1.1.2 trap-paramsname trapnms2
[Huawei] snmp-agent trap queue-size 200
[Huawei] snmp-agent trap life 60
[Huawei] snmp-agent trap enable
```

步骤 6 配置管理员联系方法

```
[Huawei] snmp-agent sys-info contact call Operator at 010-12345678
```

步骤 7 配置网管

网管的配置请根据采用的网管产品参考对应的网管配置手册。

步骤 8 验证配置结果

配置完成后，可以执行下面的命令，检查配置内容是否生效。

查看团体名的配置信息。

```
<Huawei> display snmp-agent community write
   Community name:adminnms2
   Storage type: nonVolatile
   View name: dnsmib
   Acl:2001

   Total number is 1
```

查看 ACL。

```
<Huawei> display acl 2001
Basic ACL 2001, 2 rules
Acl's step is 5
 rule 5 permit source 1.1.1.2 0
 rule 6 deny source 1.1.1.1 0
```

查看 MIB 视图。

```
<Huawei> display snmp-agent mib-view dnsmib
   View name:dnsmib
   MIB Subtree:hwDnsMib
   Subtree mask:
   Storage type: nonVolatile
   View Type:included
   View status:active
```

查看告警的目标主机。

```
<Huawei> display snmp-agent target-host
   Traphost list:
   Target host name: nms2
   Traphost address: 1.1.1.2
   Traphost portnumber: 162
   Target host parameter: trapnms2

   Total number is 1

   Parameter list trap target host:
   Parameter name of the target host: trapnms2
   Message mode of the target host: SNMPV2C
   Trap version of the target host: v2c
   Security name of the target host: adminnms2

   Total number is 1
```

当有告警信息产生时，执行命令 **display trapbuffer** 查看告警信息。

```
<Huawei> display trapbuffer
```

```
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 98

#Oct 11 2010 18:57:59+00:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011
.5.25.191.3.1 configurations have been changed. The current change number is 95,
 the change loop count is 0, and the maximum number of records is 4095.
```

查看管理员的联系方法。

```
<Huawei> display snmp-agent sys-info contact
The contact person for this managed node:
          call Operator at 010-12345678
```

----结束

配置文件

路由器的配置文件

```
#
acl number 2001
 rule 5 permit source 1.1.1.2 0
 rule 6 deny source 1.1.1.1 0
#
interface GigabitEthernet1/0/0
 ip address 1.1.2.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 1.1.2.0 0.0.0.255
#
 snmp-agent local-engineid 000007DB7FFFFFFF00001AA7
 snmp-agent community write adminnms2 mib-view dnsmib acl 2001
 snmp-agent sys-info contact call Operator at 010-12345678
 snmp-agent sys-info version v2c
 snmp-agent target-host trap-hostname nms2 address 1.1.1.2 udp-port 162 trap-paramsname trapnms2
 snmp-agent target-host trap-paramsname trapnms2 v2c securityname adminnms2
 snmp-agent mib-view dnsmib include hwDnsMib
 snmp-agent trap enale
 snmp-agent trap queue-size 200
 snmp-agent trap life 60
 snmp-agent
#
return
```

1.5.3 配置设备使用 SNMPv3 与网管通信示例

网管在管理设备时使用 SNMPv3 版本保证互通，在互通的过程中限制指定的网管可以管理设备上的部分 MIB 节点。

组网需求

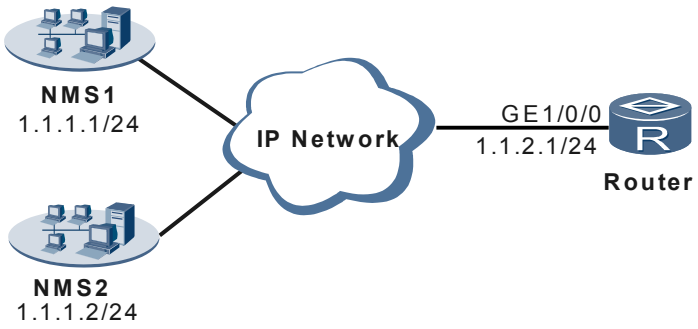
如图 1-6 所示，在网络中，用户的两个网管和同一设备通过公网相连，由于业务的需求，用户规划网管 NMS2 仅可以管理设备上的 DNS 节点，网管站 NMS1 不再管理该设备。

NMS2 管理设备的过程中，为了方便对告警信息进行定位，避免过多的无用告警对处理问题造成干扰，用户只允许缺省打开的模块可以发送告警至 NMS。

由于 NMS2 和设备间的数据需要穿越公网，对用户的数据进行认证和加密。

由于网管管理员离被管理设备较远，为了使设备出现故障时网管管理员能快速联系上被管理设备管理员，以便对故障进行定位和排除，故要求在设备上配置设备管理员的联系方法。

图 1-6 配置使用 SNMPv3 网管通信组网图



配置思路

采用如下思路配置网管功能：

1. 使能 SNMP Agent。
2. 配置 SNMP 版本为 SNMPv3。
3. 配置用户访问权限，限制 NMS2 仅可以管理设备上的 DNS 节点，并对用户进行数据加密。
4. 配置设备的 Trap 功能，使设备产生的告警能够发送至 NMS。
5. 配置管理员的联系方法。
6. 配置网管站。

数据准备

为完成此配置，需要准备如下数据：

- SNMP 版本
- 用户组名称
- 用户名和密码
- 认证和加密算法
- ACL 号
- NMS 地址
- 管理员联系方法

操作步骤

步骤 1 配置路由器和网管站之间路由可达（略）

步骤 2 配置 SNMP Agent

```
<Huawei> system-view
[Huawei] snmp-agent
```

步骤 3 配置 SNMP 的版本信息为 v3

```
[Huawei] snmp-agent sys-info version v3
```

查看配置的 SNMP 的版本信息。

```
[Huawei] display snmp-agent sys-info version
  SNMP version running in the system:
          SNMPv3
```

步骤 4 配置用户访问权限

配置 ACL，限制 NMS2 可以管理设备，NMS1 不允许管理设备。

```
[Huawei] acl 2001
[Huawei-acl-basic-2001] rule 5 permit source 1.1.1.2 0.0.0.0
[Huawei-acl-basic-2001] rule 6 deny source 1.1.1.1 0.0.0.0
[Huawei-acl-basic-2001] quit
```

配置 MIB 视图。

```
[Huawei] snmp-agent mib-view dnsmib include 1.3.6.1.4.1.2011.5.25.194
```

配置用户组和用户，对用户的数据进行认证和加密。

```
[Huawei] snmp-agent usm-user v3 testuser testgroup authentication-mode md5 87654321 privacy-mode
des56 87654321
[Huawei] snmp-agent group v3 testgroup privacy write-view dnsmib notify-view dnsmib acl 2001
```

步骤 5 配置告警功能

```
[Huawei] snmp-agent target-host trap-paramsname trapnms2 v3 securityname testuser privacy
[Huawei] snmp-agent target-host trap-hostname nms2 address 1.1.1.2 trap-paramsname trapnms2
[Huawei] snmp-agent trap queue-size 200
[Huawei] snmp-agent trap life 60
[Huawei] snmp-agent trap enable
```

步骤 6 配置管理员联系方法

```
[Huawei] snmp-agent sys-info contact call Operator at 010-12345678
```

步骤 7 配置 NMS

网管的配置请根据采用的网管产品参考对应的网管配置手册。

步骤 8 验证配置结果

配置完成后，可以执行下面的命令，检查配置内容是否生效。

查看用户组。

```
<Huawei> display snmp-agent group testgroup

  Group name: testgroup
  Security model: v3 noAuthnoPriv
  Readview: ViewDefault
  Writeview: dnsmib
  Notifyview: dnsmib
  Storage type: nonVolatile
  Acl:2001
```

查看用户。

```
<Huawei> display snmp-agent usm-user

  User name: testuser
  Engine ID: 000007DB7F00000100004C3F
  Group name: testgroup
  Authentication mode: md5, Privacy mode: des56
  Storage type: nonVolatile
  User status: active
```

```
   Total number is 1
```

查看 ACL。

```
<Huawei> display acl 2001
Basic ACL 2001, 2 rules
Acl's step is 5
 rule 5 permit source 1.1.1.2 0
 rule 6 deny source 1.1.1.1 0
```

查看 MIB 视图。

```
<Huawei> display snmp-agent mib-view dnsmib
   View name:dnsmib
   MIB Subtree:hwDnsMib
   Subtree mask:
   Storage type: nonVolatile
   View Type:included
   View status:active
```

查看告警的目标主机。

```
<Huawei> display snmp-agent target-host
   Traphost list:
   Target host name: nms2
   Traphost address: 1.1.1.2
   Traphost portnumber: 162
   Target host parameter: trapnms2

   Total number is 1

   Parameter list trap target host:
   Parameter name of the target host: trapnms2
   Message mode of the target host: SNMPV3
   Trap version of the target host: v3
   Security name of the target host: testuser
   Security level of the target host: privacy

   Total number is 1
```

当有告警信息产生时，执行命令 **display trapbuffer** 查看告警信息。

```
<Huawei> display trapbuffer
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 98

#Oct 11 2010 18:57:59+00:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011
.5.25.191.3.1 configurations have been changed. The current change number is 95,
 the change loop count is 0, and the maximum number of records is 4095.
```

查看管理员的联系方法。

```
<Huawei> display snmp-agent sys-info contact
The contact person for this managed node:
          call Operator at 010-12345678
```

----结束

配置文件

路由器的配置文件

```
#
acl number 2001
 rule 5 permit source 1.1.1.2 0
 rule 6 deny source 1.1.1.1 0
#
interface GigabitEthernet1/0/0
 ip address 1.1.2.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 1.1.2.0 0.0.0.255
#
 snmp-agent local-engineid 000007DB7FFFFFFF000004A7
 snmp-agent sys-info contact call Operator at 010-12345678
 snmp-agent sys-info version v3
 snmp-agent group v3 testgroup privacy write-view dnsmib notify-view dnsmib acl 2001
 snmp-agent target-host trap-hostname nms2 address 1.1.1.2 udp-port 162 trap-paramsname trapnms2
 snmp-agent target-host trap-paramsname trapnms2 v3 securityname testuser privacy
 snmp-agent mib-view dnsmib include hwDnsMib
 snmp-agent usm-user v3 testuser testgroup authentication-mode md5 B4B3D731A5006953EDFC9BB83F983497
privacy-mode des56 B4B3D731A5006953EDFC9BB83F983497
 snmp-agent trap enable
 snmp-agent trap queue-size 200
 snmp-agent trap life 60
 snmp-agent
#
return
```

2 RMON 配置

关于本章

通过 RMON(Remote Network Monitoring)可以实现对以太接口的监控。

2.1 RMON 简介
通过 RMON 的简介，用户可以了解到 RMON 的工作原理。

2.2 配置 RMON
通过配置 RMON 可以实现对于网络状况和流量进行监控。

2.3 RMON 配置举例
介绍 RMON 的配置。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

2.1 RMON 简介

通过 RMON 的简介，用户可以了解到 RMON 的工作原理。

2.1.1 RMON 概述

介绍 RMON 的工作原理。

RMON 概述

RMON 基于简单网络管理协议 SNMP 体系结构实现，与现存 SNMP 框架兼容，包括网管工作站 NMS 和运行在各网络设备上的代理 Agent 两部分。

RMON Agent 跟踪统计网络中的各种流量信息，例如，某段时间内某网段上的报文总数，或发往某台主机的正确报文总数等。它使 SNMP 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手段。减少了网管站与代理 Agent 间的通讯流量，从而实现更简单有效地管理大型网络。

RMON 允许有多个监控者，它可用两种方法收集数据。

- 通过专用的 RMON Probe（探测仪）。NMS 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。
- 将 RMON Agent 直接嵌入网络设备（例如路由器）中，使它们成为带 RMON Probe 功能的网络设备。NMS 是用 SNMP 基本命令与其交换数据信息，收集网络管理信息。这种方式受设备资源限制，一般无法获取 RMON MIB 的所有数据，大多数只收集四个组（告警、事件、历史和统计）的信息。

目前只能对网络设备的以太网接口进行监控和统计。

2.1.2 AR3200 支持的 RMON 特性

本节介绍了 AR3200 对 RMON 的支持。

RMON 特性

AR3200 通过把 RMON Agent 模块直接嵌入网络设备中，与其它模块形成一个完整的系统来实现 RMON。网管工作站 NMS 可以完全利用 SNMP NMS，网络管理人员无须进行额外的学习。

AR3200 RMON 支持 RFC2819 规定的统计、历史、告警和事件四个组以及华为规定的私有扩展告警组（PERFORMANCE-MIB）。下面对这几个组分别进行介绍。

- 统计组

  统计组统计被监控的每个子网的基本统计信息。它能统计某一网段的流量和各种类型包的分布，还能统计各种类型的错误帧数、碰撞次数等。

  统计组包含一个以太网统计表（ethernetStatsTable）。

  说明

  RMON 统计结果与 **display interface** 的显示结果不完全一致，虽然两者都是从底层获取数据，但 RMON 搜集的信息更全面。

- 历史组

  历史组定期收集网络状态统计信息并存储，以便后续的处理。

历史组包含两个表：

- 历史控制表（historyControlTable）：主要用来设置采样间隔时间等控制信息。
- 以太网历史表（ethernetHistoryTable）：为网络管理员提供有关网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据。

历史控制表中的每一项控制信息在以太网历史表中最多可以有 10 条历史数据相对应，如果超过指定条数，将循环覆盖。

- 告警组

  告警组允许针对告警变量（可以是本地 MIB 的任意对象）预先定义一组阈值，如果采样数据在相应的方向上越过阈值，监视器会记录日志或者把告警发往网管站。

  按照 RFC2819，告警功能采用一种滞后机制限制告警事件的产生。应用这个机制后，当采样数据以某方向跨过阈值时，将会产生一个事件。直到相反方向的阈值被跨过以前，不会产生更多的事件。

  AR3200 在实现时没有采取这种方式，因为滞后机制可能长时间不会产生告警。在 AR3200 中，只要采样值回到正常阈值后就可以重新告警。

  告警组包括一个告警表（alarmTable）。

- 事件组

  事件组提供关于 RMON 代理所产生的所有事件的表。当某事件发生时，可以记录日志或发送 TRAP 到网管站。

  事件组主要实现 Log、Trap 以及 Log-Trap 三种事件输出，每个日志事件行对应的日志最多可以为 10 条，超过 10 条将循环覆盖。

  事件组包括事件表（eventTable）和日志表（logTable）。

- 扩展告警组

  扩展告警组在 RFC2819 基础上增加了用表达式设定告警对象和告警生存时间的功能。它包括一个扩展告警表（prialarmTable）。

各表项在 AR3200 中，为节约系统资源，每个表记录都有自己的生存时间，规定了当此行状态不是有效状态 VALID 时，此行可以存在的时间。对于一直处于非 VALID 状态的行，其生存时间将递减。当生存时间为 0 时，行被删除。各表的容量和最大生存时间如表 2-1 所示。

表 2-1 各表的生存时间

表名称	表项容量(Byte)	最大生存时间（s）
统计表	100	600
历史控制表	100	600
告警表	60	6000
事件表	60	600
事件日志表	600	-
扩展告警表	50	6000

说明

事件日志表没有最大生存时间，日志事件行对应的日志最多可以为 10 条，超过 10 条将循环覆盖。

当有接口板或接口卡被拔出时，接口对应的统计表和历史控制表状态会变成 INVALID 状态，此时，对应的统计表和历史控制表的生存时间被设置为 1200s。如果表记录的生存时间到达 0，该表记录将被删除。

当接口插入时，如果存在对应的表记录，则把对应表记录的行状态变为 VALID，这一表记录成为有效的正常表记录。

2.2 配置 RMON

通过配置 RMON 可以实现对于网络状况和流量进行监控。

2.2.1 建立配置任务

在配置 RMON 前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

如果要对某一网段的网络状况进行监控、流量统计，可以配置 RMON。

对 RMON 功能的启动时间没有特殊要求，可以预先启动该功能，也可以在怀疑某个接口所连接子网的流量异常时进行配置。

推荐的做法是：预先配置好统计表，对流量有异常的端口配置两条历史控制策略，对某项指标或某几项指标有怀疑时进行告警配置，设定上下阈值，查看告警信息。

说明

RMON 只能提供一些流量统计和异常等信息，并不能防止这些信息尤其是异常情况，要消除异常还需要其它管理手段。

前置任务

在配置 RMON 之前，需完成以下任务：

- 配置以太网接口的参数
- 配置 SNMP 基本功能

数据准备

在配置 RMON 之前，需要准备以下数据：

序号	数据
1	确定要使能统计功能的接口
2	确定要使用的统计表及相关参数
3	确定要使用的历史控制表及相关参数
4	确定要使用的事件表及相关参数
5	确定要使用的告警表及相关参数
6	确定要使用的扩展告警表及相关参数

2.2.2 使能接口的 RMON 统计功能

需要进行流量统计的接口使能统计功能。如果没有使能接口统计功能，RMON 统计表和历史表采集的统计值为零。

背景信息

请在需要进行流量统计的接口上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** { **ethernet** | **gigabitethernet** } *interface-number*，进入接口视图。

步骤 3 执行命令 **rmon-statistics enable**，使能接口的 RMON 统计功能。

如果没有使能接口统计功能，RMON 统计表和历史表采集的统计值为零。

----结束

2.2.3 配置统计表

统计表中记录 RMON 收集到的接口流量信息。

背景信息

请在需要进行流量统计的接口上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** { **ethernet** | **gigabitethernet** } *interface-number*，进入接口视图。

步骤 3 执行命令 **rmon statistics** *entry-number* [**owner** *owner-name*]，配置统计表。

网络管理员监控设备接口的统计信息时，要为相应的接口创建一（表）行，给出接口的 OID、行索引和行的状态。此后，网络管理员可以通过读取本行的方式获取最新统计数据。

----结束

2.2.4 配置历史控制表

历史数据管理功能可以设定对某个接口进行采样、保存数量和采样参数（时间间隔），定期对指定的端口进行数据采集并将采集到的信息保存到历史表中以备查看。

背景信息

RMON 规范建议每个被监视的接口可以有 2 个以上历史控制条目，间隔 30 秒依次采样一次。

短周期取样使监视器能够探测到流量模式的突变，长周期取样则监视接口的稳定状态行为。

目前，AR3200 为每个历史控制条目最多保留 10 条最近的记录，超过 10 条将循环覆盖。

说明

为减少 RMON 对系统性能的影响，历史表的采样间隔应在 10 秒以上，且不要对同一端口配置过多的历史控制表项和告警表项。

请在需要进行流量统计的接口上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** { **ethernet** | **gigabitethernet** } *interface-number*，进入接口视图。

步骤 3 执行命令 **rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *owner-name*]，配置历史控制表。

----结束

2.2.5 配置事件表

通过配置事件表后，当事件超过告警阈值时，设备可以记录日志或者产生告警，或者同时记录日志和产生告警。

背景信息

请在需要进行监控的设备上进行如下的配置。

RMON 事件管理在事件表的指定行添加事件，并定义事件的处理方式：

- **log**：只发送日志
- **log-trap**：既发送日志同时也向 NMS 发送 Trap 消息
- **none**：标记为没有事件发生
- **trap**：只向 NMS 发送 Trap 消息

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rmon event** *entry-number* [**description** *string*] { **log** | **trap** *object* | **log-trap** *object* | **none** } [**owner** *owner-name*]，配置事件表。

----结束

2.2.6 配置告警表

RMON 告警管理可以按照指定的采样间隔对指定的告警变量（用此变量的 OID 指定）进行监视，当被监视数据的值越过定义的阈值时会产生告警事件。

背景信息

RMON 告警管理可以按照指定的采样间隔对指定的告警变量（用此变量的 OID 指定）进行监视，当被监视数据的值越过定义的阈值时会产生告警事件。事件通常会记录在设备的日志表中，或向 NMS 发送 Trap。

如果告警上限和下限所对应事件（*event-entry1*、*event-entry2*）在事件表中均没有配置，即使达到了告警条件也不会产生告警（此时告警记录的状态为 undercreation，不是有效状态 VALID）。

只要事件表中配置了上限和下限其中一个事件，符合条件便会触发相应的告警（告警记录的状态为 VALID）。同理，如果告警变量设置错误，例如设置成一个不存在的 OID，告警记录的状态也为 undercreation，不会正常告警。

请在被监控的设备上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rmon alarm** *entry-number alarm-OID sampling-time* { **absolute** | **changeratio** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *owner-name*]，配置告警表。

----结束

2.2.7 配置扩展告警表

RMON 扩展告警表与 RMON 告警表相比增加了用表达式设定告警对象的功能。

背景信息

在 RFC2819 的告警表基础上，RMON 扩展告警管理增加了用表达式设定告警对象的功能，并且可以限定扩展告警行的总生存时间。

扩展告警表比告警表多了以下几项：

- 扩展告警变量的表达式字符串，可以是若干简单告警变量 OID 组成的四则表达式（＋，－，*，/和小括号）。
- 扩展告警行的描述字符串。
- 采样类型为变化率。
- 扩展告警状态类型，包括两种类型：永远（Forever）和限定时间（cycle）。对于 cycle 类型，当经过了扩展告警状态周期指定时间后，不再产生告警并且此表行被删除。

如果告警上限和下限所对应事件（*event-entry1*、*event-entry2*）在事件表中均没有配置，即使达到了告警条件也不会产生告警。告警记录的状态为 undercreation，不是有效状态 VALID。

只要上限和下限其中一个事件在事件表中配置了，符合条件便会触发相应的告警，告警记录的状态为 VALID。

请在被监控的设备上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **rmon prialarm** *entry-number prialarm-formula description-string sampling-interval* { **absolute** | **changeratio** | **delta** } **rising-threshold** *threshold-value1 event-entry1*

falling-threshold *threshold-value2 event-entry2* **entrytype** { **cycle** *entry-period* | **forever** } [**owner** *owner-name*]，配置扩展告警表。

----结束

2.2.8 检查配置结果

在配置 RMON 功能成功后，可以查看到 RMON 采集的流量信息。

前提条件

已经完成 RMON 功能的所有配置。

操作步骤

- 执行 **display rmon alarm** [*entry-number*]命令查看 RMON 告警信息。
- 执行 **display rmon event** [*entry-number*]命令查看 RMON 事件。
- 执行 **display rmon eventlog** [*entry-number*]命令查看 RMON 事件日志。
- 执行 **display rmon history** [**ethernet** *interface-number* | **gigabitethernet** *interface-number*]命令查看 RMON 历史信息。
- 执行 **display rmon prialarm** [*entry-number*]命令查看 RMON 扩展告警表。
- 执行 **display rmon statistics** [**ethernet** *interface-number* | **gigabitethernet** *interface-number*]命令查看 RMON 统计消息。

----结束

任务示例

配置成功后，执行命令 **display rmon alarm**，查看告警表的信息。

```
<Huawei> display rmon alarm 1
Alarm table 1 owned by Test300 is VALID.
Samples  absolute value   : 1.3.6.1.2.1.16.1.1.1.6.1 <etherStatsBroadcastPkts.1>
Sampling interval         : 30(sec)
Rising threshold          : 500(linked with event 1)
Falling threshold         : 100(linked with event 1)
When startup enables      : risingOrFallingAlarm
Latest value              : 1975
```

执行命令 **display rmon event**，查看事件表信息。

```
<Huawei> display rmon event
Event table 1 owned by Test300 is VALID.
  Description: null.
  Will cause log  when triggered, last triggered at 0days 00h:24m:10s.34th.
Event table 2 owned by Test300 is VALID.
  Description: forUseofPrialarm.
  Will cause snmp-trap when triggered, last triggered at 0days 00h:26m:10s.73th.
```

执行命令 **display rmon eventlog**，查看事件记录的日志信息。

```
<Huawei> display rmon eventlog
Event table 1 owned by Test300 is VALID.
  Generates eventLog 1.1 at 0days 00h:39m:30s.05th
  Description: The 1.3.6.1.2.1.16.1.1.1.6.1 defined in alarm table 1,
     less than or equal to 100 with alarm value 0. Alarm sample type is absolute.
```

执行命令 **display rmon history**，查看 RMON 历史信息。

```
<Huawei> display rmon history
History control entry 1 owned by Test300 is VALID
  Samples interface     : Ethernet1/0/0<ifEntry.402653698>
  Sampling interval     : 30(sec) with 10 buckets max
```

```
  Last Sampling time    : 0days 00h:09m:43s
  Latest sampled values :
  octets              :645       , packets           :7
  broadcast packets   :7         , multicast packets :0
  undersize packets   :6         , oversize packets  :0
  fragments packets   :0         , jabbers packets   :0
  CRC alignment errors :0        , collisions        :0
  Dropped packet:     :0         , utilization       :0
```

执行命令 **display rmon prialarm**，查看 RMON 扩展告警表信息。

```
<Huawei> display rmon prialarm 1
Prialarm table 1 owned by Test300 is VALID.
  Samples delta value       : .1.3.6.1.2.1.16.1.1.1.6.1+.1.3.6.1.2.1.16.1.1.1.7.1
  Sampling interval         : 30(sec)
  Rising threshold          : 1000(linked with event 2)
  Falling threshold         : 0(linked with event 2)
  When startup enables      : risingOrFallingAlarm
  This entry will exist     : forever
  Latest value              : 16
```

执行命令 **display rmon statistics**，查看 RMON 统计信息。

```
<Huawei> display rmon statistics
Statistics entry 1 owned by Test300 is VALID.
  Interface : Ethernet1/0/0<ifEntry.402653698>
  Received  :
  octets              :142915224 , packets          :1749151
  broadcast packets   :11603     , multicast packets:756252
  undersize packets   :0         , oversize packets :0
  fragments packets   :0         , jabbers packets  :0
  CRC alignment errors:0         , collisions       :0
  Dropped packet (insufficient resources):1795
  Packets received according to length (octets):
  64     :150183    ,  65-127  :150183    ,  128-255  :1383
  256-511:3698      ,  512-1023:0         ,  1024-1518:0
```

2.3 RMON 配置举例

介绍 RMON 的配置。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

2.3.1 配置 RMON 示例

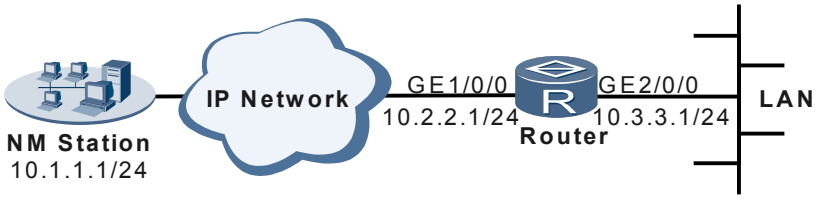
统计接口的流量信息，当流量超过设定值时，记录日志。

组网需求

如图 2-1 所示，要求对 Router 的接口 GE2/0/0 连接的子网进行监控，包括：

- 有关流量和各种类型包数量的实时和历史统计信息。
- 对此接口流量的字节数设置告警监控，当每分钟的流量超过设定值时，记录日志。
- 监控此子网的单播信息流量，对该子网的单播总数进行告警设置，当超过设定值时，主动向网管站 NM Station 上报告警信息。

图 2-1 配置 RMON 组网图



配置思路

采用如下的思路配置 RMON：

1. 使用 SNMP 配置命令允许发送 Trap 报文并设置相应的团体名。
2. 使能统计功能并配置统计表。
3. 配置历史控制表。
4. 配置事件表。
5. 配置告警表及扩展告警表。

数据准备

为完成此配置例，需准备如下的数据：

- 信息采样时间间隔
- 触发告警事件阈值

操作步骤

步骤 1 配置路由器和网管站路由可达（略）

步骤 2 配置允许向网管站发送 Trap

使能 SNMP 发送 Trap 的功能。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] snmp-agent trap enable
```

配置向指定的网管站发送 Trap。

```
[Router] snmp-agent target-host trap-paramsname hw v1 securityname public
[Router] snmp-agent target-host trap-hostname hwnm address 10.1.1.1 trap-paramsname hw
```

步骤 3 配置统计功能

使能 RMON 接口统计功能。

```
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] rmon-statistics enable
```

配置统计表。

```
[Router-GigabitEthernet2/0/0] rmon statistics 1 owner Test300
```

步骤 4 配置历史控制表

设置 RMON 对子网中的流量信息采样，采样间隔为 30 秒钟，并保存最近 10 次数据。

```
[Router-GigabitEthernet2/0/0] rmon history 1 buckets 10 interval 30 owner Test300
```

步骤 5 配置事件表

设置 RMON 的 1 号事件处理方式为记录日志，2 号事件处理方式为向网管站发送 Trap 消息。

```
[Router] rmon event 1 log owner Test300
[Router] rmon event 2 description forUseofPrialarm trap public owner Test300
```

步骤 6 配置告警表

设置采样间隔时间和触发告警事件 1 的阈值。

```
[Router] rmon alarm 1 1.3.6.1.2.1.2.2.1.11.22 30 absolute rising-threshold 10000 1 falling-threshold
100 1 owner Test300
```

步骤 7 检测配置结果

查看配置效果。可以随时查看子网的数据流量信息。

```
<Router> display rmon statistics gigabitethernet 2/0/0
Statistics entry 1 owned by Test300 is VALID.
  Interface : GigabitEthernet2/0/0<ifEntry.22>
  Received  :
  octets              :142915224 , packets          :1749151
  broadcast packets   :11603     , multicast packets:756252
  undersize packets   :0         , oversize packets :0
  fragments packets   :0         , jabbers packets  :0
  CRC alignment errors:0         , collisions       :0
  Dropped packet (insufficient resources):1795
  Packets received according to length (octets):
  64     :150183    ,  65-127  :150183    ,  128-255  :1383
  256-511:3698      ,  512-1023:0         ,  1024-1518:0
```

查看配置效果。

```
<Router> display rmon history gigabitethernet 2/0/0
History control entry 1 owned by Test300 is VALID
  Samples interface     : GigabitEthernet2/0/0<ifEntry.22>
  Sampling interval     : 30(sec) with 10 buckets max
  Last Sampling time    : 0days 00h:19m:43s
  Latest sampled values :
  octets               :645       , packets           :7
  broadcast packets    :7         , multicast packets :0
  undersize packets    :6         , oversize packets  :0
  fragments packets    :0         , jabbers packets   :0
  CRC alignment errors :0         , collisions        :0
  Dropped packet:      :0         , utilization       :0
  History record:
  Record No.1 (Sample time: 0days 00h:02m:30s)
  octets               :0         , packets           :0
  broadcast packets    :0         , multicast packets :0
  undersize packets    :0         , oversize packets  :0
  fragments packets    :0         , jabbers packets   :0
  CRC alignment errors :0         , collisions        :0
  Dropped packet:      :0         , utilization       :0
```

查看事件信息。

```
<Router> display rmon event
Event table 1 owned by Test300 is VALID.
  Description: null.
  Will cause log  when triggered, last triggered at 0days 00h:24m:10s.
Event table 2 owned by Test300 is VALID.
  Description: forUseofPrialarm
  Will cause snmp-trap when triggered, last triggered at 0days 00h:26m:10s.
```

查看告警信息。

```
<Router> display rmon alarm 1
Alarm table 1 owned by Test300 is VALID.
  Samples  absolute value   : 1.3.6.1.2.1.2.2.1.11.22 <ifInUcastPkts.22>
  Sampling interval         : 30(sec)
  Rising threshold          : 500(linked with event 1)
  Falling threshold         : 100(linked with event 1)
  When startup enables      : risingOrFallingAlarm
  Latest value              : 1975
```

查看事件日志信息。

```
<Router> display rmon eventlog
Event table 1 owned by Test300 is VALID.
  Generates eventLog 1.1 at 0days 00h:39m:30s.
  Description: The 1.3.6.1.2.1.16.1.1.1.6.1 defined in alarm table 1,
    less than or equal to 100 with alarm value 0. Alarm sample type is absolute.
```

如果所设置的扩展告警变量超过预定范围，网管站可以接受到告警 Trap 信息。

----结束

配置文件

```
#
 sysname Router
#
 snmp-agent target-host trap-hostname hwnm address 10.1.1.1 udp-port 162 trap-paramsname hw
 snmp-agent target-host trap-paramsname hw v1 securityname public
 snmp-agent trap enable
#
interface GigabitEthernet1/0/0
 ip address 10.2.2.1 255.255.255.0
interface GigabitEthernet2/0/0
 ip address 10.3.3.1 255.255.255.0
 rmon-statistics enable
 rmon statistics 1 owner Test300
 rmon history 1 buckets 10 interval 30 owner Test300
#
rmon event 1 description null log owner Test300
rmon event 2 description forUseofPrialarm trap public owner Test 300
rmon alarm 1 1.3.6.1.2.1.2.2.1.11.22 30 absolute rising-threshold 10000 1 falling-threshold 100 1
owner Test300
#
return
```

3 LLDP 配置

关于本章

介绍 LLDP 的应用场景、配置步骤以及配置举例。

3.1 LLDP 概述
链路层发现协议 LLDP（Link Layer Discovery Protocol）是 IEEE 802.1ab 中定义的第二层发现协议。

3.2 AR3200 支持的 LLDP 特性
介绍 LLDP 特性的应用场景及 AR3200 支持的 TLV 类型。

3.3 配置 LLDP 功能
介绍如何配置 LLDP 功能。

3.4 维护
维护 LLDP 功能，包括清除 LLDP 统计信息、监控 LLDP 运行状态。

3.5 配置举例
介绍 LLDP 的不同组网中举例。

3.1 LLDP 概述

链路层发现协议 LLDP（Link Layer Discovery Protocol）是 IEEE 802.1ab 中定义的第二层发现协议。

背景

目前以太网技术在局域网、城域网都有非常广泛的应用。随着大规模组网的需求越来越多，对网络管理（以下简写为网管）能力的要求也越来越高，例如获取相连设备的拓扑状态、设备间的配置冲突等。

而现阶段许多网管都使用“自动发现（Automated Discovery）”功能来跟踪拓扑的变化。但是绝大多数网管最多只能分析到第三层网络拓扑结构，将设备分组到各个 IP 子网。这些数据只是一些有关设备增加和移除的基本事件，无法确定设备通过哪些接口跟另外一个设备相连，也无法确定设备间是否存在配置冲突。

第二层发现（Layer 2 Discovery）准确定位了诸如哪些设备附带有哪些接口，以及哪些设备与其他设备相互连接等二层信息，并显示出了客户端、交换机、路由器和应用服务器以及网络服务器之间的路径。这些详细的信息对快速获取相连设备的拓扑状态、设备间的配置冲突、查询网络失败的根源将很有帮助。

链路层发现协议 LLDP（Link Layer Discovery Protocol）就是 IEEE 802.1ab 中定义的第二层发现协议。

LLDP 基本原理

图 3-1 LLDP 结构框图

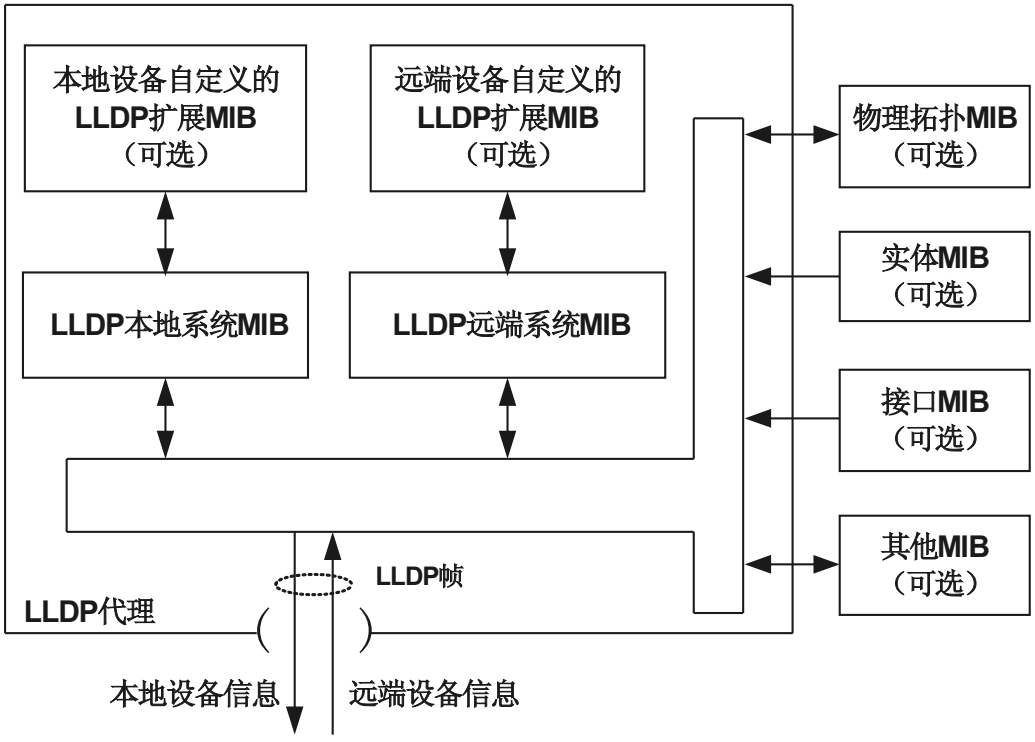


图 3-1 为 LLDP 结构框图。LLDP 与 MIB 密不可分，其基本实现原理为：

- LLDP 模块通过与设备上的 PTOPO MIB、Entity MIB、Interface MIB 以及 Other MIB 的交互，来更新自己的 LLDP local system MIB 库以及自己定义的 LLDP 扩展 MIB（图中的本地设备自定义的 LLDP 扩展 MIB）。
- 然后通过 LLDP 帧，将自己的相关信息通过连接到远端设备的接口，发送给远端设备。
- 同时它接收远端设备发过来的 LLDP 帧，更新自己的 LLDP remote system MIB 即 LLDP 远端系统 MIB 库。

这样，通过 MIB 库，设备就很清楚的知道了自己相邻的设备的信息，包括连接的是远方设备的哪个接口，连接的远端设备的桥 MAC 地址等等。

LLDP 基本概念

MIB

MIB：管理信息数据库，MIB 分为 LLDP Local System MIB 和 LLDP Remote System MIB。

- LLDP Local System MIB：LLDP 本地系统管理信息数据库（以下简称 LLDP 本地 MIB），用来保存本端设备信息。包括设备 ID、接口 ID、系统名称、系统描述、接口描述、设备能力、网络管理地址等等。
- LLDP Remote System MIB：LLDP 远端系统管理信息数据库（以下简称 LLDP 远端 MIB），用来保存相邻设备的信息。包括设备 ID、接口 ID、系统名称、系统描述、接口描述、设备能力、网络管理地址等等。

LLDP Agent

LLDP Agent：LLDP 代理，用于管理接口的 LLDP 操作。

LLDP Agent 要完成下列任务：

- 维护 LLDP 本地 MIB 的信息。
- 在本端状态发生变化的情况下，提取 LLDP 本地 MIB 信息向邻居节点发送。在本端状态没有变化的情况下，按照一定的周期提取 LLDP 本地 MIB 信息向邻居节点发送。
- 识别并处理收到的 LLDP 报文。
- 维护 LLDP 远端 MIB 库。
- LLDP 本地 MIB 库或远端 MIB 库中的信息发生变化的情况下，向网管发送 LLDP 告警。

LLDP 管理地址

LLDP 管理地址（以下简称管理地址）是供网管系统标识 AR3200 并进行管理的地址。管理地址可以明确地标识一台设备，有利于网络拓扑的绘制，更有利于清晰地了解到当前的拓扑状态，便于网络管理。管理地址被封装在 LLDP 报文的 Management Address TLV 字段中传送给邻居节点。

LLDP 告警

LLDP 告警是指 LLDP 本地 MIB 库或远端 MIB 库中的信息发生变化，设备向网管系统发送的更新拓扑的提示信息。触发告警的原因为：

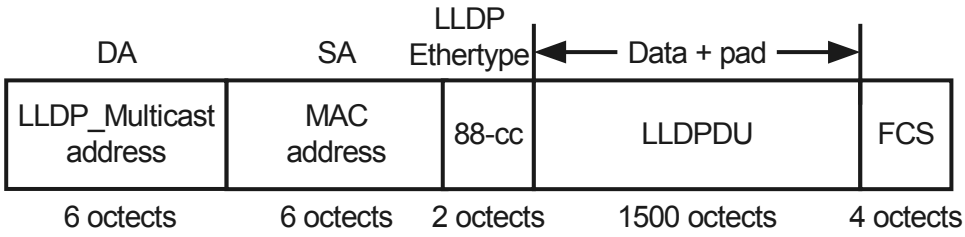
- 全局 LLDP 使能的状态变化
- 本地管理地址改变
- 邻居信息发生变化（邻居管理地址变化，本地不会产生告警信息）

LLDP 告警功能对全局起作用，控制所有接口发送告警的能力。

LLDP 报文

LLDP 报文结构如图 3-2 所示。

图 3-2 LLDP 报文结构

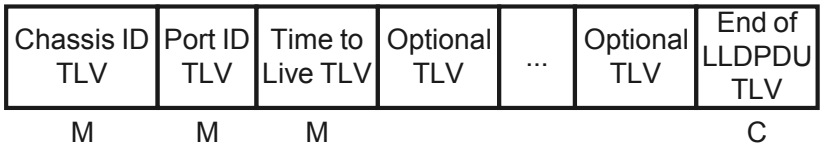


- DA：LLDP 帧的目的地址，它是一个组播地址其值为 01-80-C2-00-00-0E。
- SA：与设备相邻连接设备的桥 MAC。
- LLDP Ethertype：帧类型，设备通过此字节，就可以判断是一个 LLDP 帧，然后交给 LLDP 模块处理，它的值为 0x88CC。
- LLDPDU：LLDP Data Unit，LLDP 数据单元，它是 LLDP 信息交换的主体。
- FCS：帧校验位。

因为 LLDPDU 是 LLDP 信息交换的主体，它决定了通过 LLDP 协议可以发现设备的哪些二层信息，所以下面详细介绍一下该字段。

LLDPDU 结构如图 3-3 所示。

图 3-3 LLDPDU 结构



LLDPDU 中的基本信息单元是 TLV，其中：

- T 指的是信息的类型 TYPE
- L 是指的信息的长度 LENGTH
- V 是指的信息的值，也就是真正所要传输的内容 VALUE

在 LLDP 帧交互的过程中，LLDPDU 往往根据要求包含了很多种不同的 TLV，根据这些不同的 TLV 来传输或者接收自己和邻近设备的信息。

LLDPDU 固定以 Chassis ID TLV、Port ID TLV 和 Time to Live TLV 开始，以 End of LLDPDU TLV 为结束，这四个 TLV 为必选的 TLV。其他均为可选 TLV，可以由设备自行定义是否包含在 LLDPDU 中。

3.2 AR3200 支持的 LLDP 特性

介绍 LLDP 特性的应用场景及 AR3200 支持的 TLV 类型。

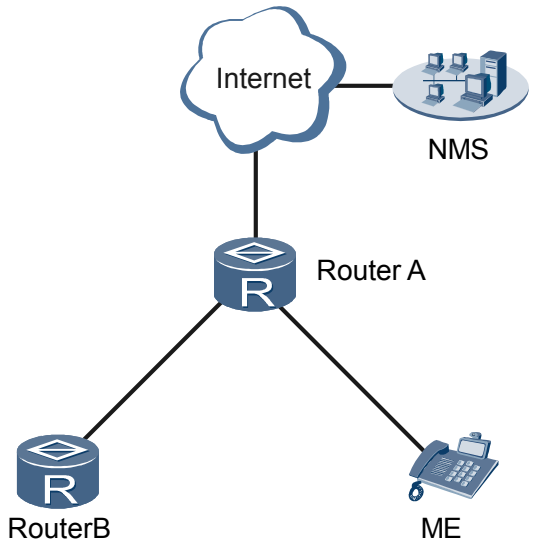
LLDP 应用场景

AR3200 支持在以下三种组网方式下应用 LLDP。

单邻居组网方式

单邻居组网是指路由器设备的端口之间或者路由器与媒体终端 ME（Media Endpoint）的端口之间是直接相连，中间没有跨任何的设备，而且端口只有一个远端邻居设备的情况。单邻居组网如图 3-4 所示，RouterA 和 RouterB 之间以及 RouterA 和 ME 之间均是直接相连，RouterA 和 RouterB 的每一个端口都只有一个远端邻居。

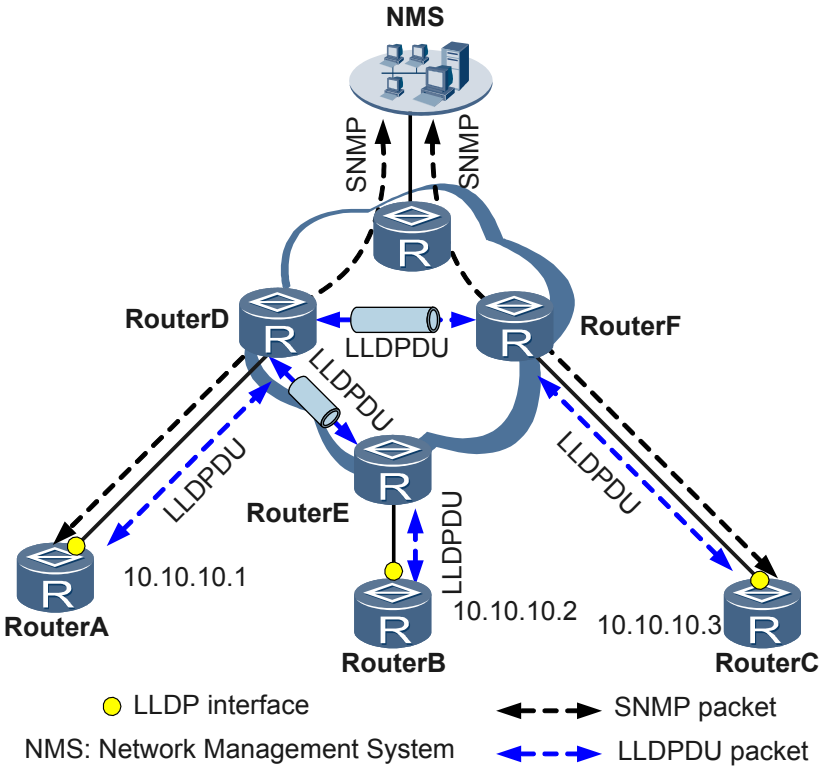
图 3-4 单邻居组网方式



多邻居组网方式

多邻居组网方式是指路由器设备的端口之间不是直接相连，中间跨越了未知网络，这时每个端口的远端邻居不止一个。多邻居组网如图 3-5 所示，RouterA、RouterB 和 RouterC 之间不是直接相连，中间跨越了未知网络，该网络中的设备未使能 LLDP 功能或者无需受 NMS 的管理，但该部分设备可以透传 LLDP 报文。这样 RouterA、RouterB 和 RouterC 的端口都不止有一个远端邻居。

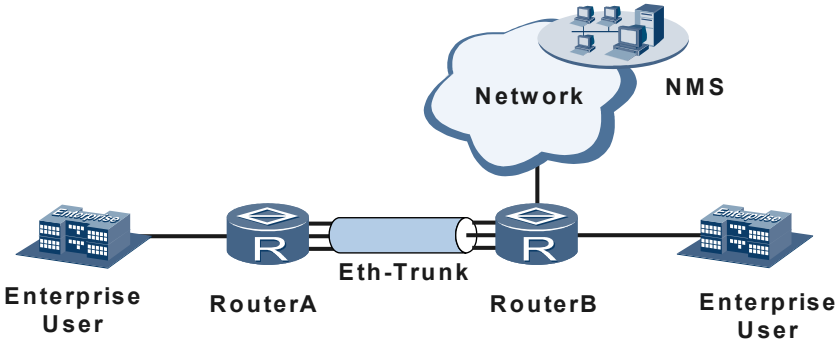
图 3-5 多邻居组网方式



存在链路聚合的组网方式

如图 3-6 所示路由器设备的端口之间存在链路聚合。该情况下，具体到链路聚合之间的每一个端口，都与单邻居组网模式的效果是一样的。

图 3-6 存在链路聚合的组网方式



AR3200 支持的可选 TLV 类型

除了必须支持的 Chassis ID TLV、Port ID TLV、Time to Live TLV 和 End of LLDPDU 以外，AR3200 支持的可选 TLV 类型为：

- 基本 TLV

TLV 类型	说明
Management Address TLV	管理 IP 地址
Port Description TLV	端口描述
System Capabilities TLV	本端设备的支持能力： ● other：其它能力 ● repeater：中继器 ● bridge：桥设备 ● wlanAccessPoint：无线接入点 ● router：路由器 ● telephone：无线设备 ● docsisCableDevice：管理站 ● stationOnly：基站
System Description TLV	设备描述信息
System Name TLV	设备名称

- 802.1 组织定义 TLV

TLV 类型	说明
端口 VLAN TLV	端口的 VLAN ID
端口协议 VLAN TLV	端口的协议 VLAN ID
VLAN Name TLV	VLAN 名称
Protocol identity TLV	端口支持的协议类型

- 802.3 组织定义 TLV

TLV 类型	说明
Link Aggregation TLV	端口是否支持链路聚合以及是否已使能链路聚合
MAC/PHY Configuration/Status TLV	端口的速率和双工状态、是否支持端口速率自动协商、是否已使能自动协商功能以及当前的速率和双工状态
Maximum Frame Size TLV	端口支持的最大帧长度，取端口最大传输单元 MTU（Max Transmission Unit）
Power Via MDI TLV	端口的供电能力，比如是否支持 PoE，是供电设备还是受电设备

- LLDP-MED TLV

TLV 类型	说明
LLDP-MED Capabilities TLV	当前设备的设备类型以及在 LLDPDU 中可封装的 LLDP-MED TLV 类型
Inventory TLV	设备的制造厂商
Location Identification TLV	位置标识信息，供其它设备在基于位置的应用中使用
Network Policy TLV	Voice VLAN 的 VLAN ID、二层优先级以及 DSCP 值等
Extended Power-via-MDI TLV	当前设备的供电能力

缺省情况下，LLDP 发布除 Location Identification TLV 之外所有类型的 TLV。

3.3 配置 LLDP 功能

介绍如何配置 LLDP 功能。

3.3.1 建立配置任务

应用环境

为了方便 NMS 获得网络设备间的拓扑信息、设备的主要能力、管理地址、设备标识、接口标识等信息，可以在网络设备上使能 LLDP 功能。

前置任务

在配置 LLDP 功能之前，需完成以下任务：

- 路由器与 NMS 之间路由可达，且 SNMP 相关参数已经配置完成。
- 需要配置用于 LLDP 管理的 IP 地址。

说明

LLDP 报文中携带的 LLDP 管理地址是用来标识设备的，必须选用网管系统能够唯一标识设备并且方便管理的 IP 地址。要求配置的 LLDP 管理地址必须是设备上已存在的 IP 地址，所以该 IP 地址需要在 **3.3.4 （可选）配置 LLDP 管理地址**之前配置。

数据准备

在配置 LLDP 功能之前，需要准备以下数据。

序号	数据
1	用作 LLDP 管理地址的 IP 地址
2	（可选）发送 LLDP 报文的周期
3	（可选）发送 LLDP 报文的延迟时间
4	（可选）本端信息在邻居节点中保持的时间倍数

序号	数据
5	（可选）接口 LLDP 模块从禁用状态到重新使能的延迟时间
6	（可选）发送邻居信息变化告警的延迟时间

3.3.2 使能全局 LLDP 功能

使能设备 LLDP 功能的情况下，路由器能够向使能 LLDP 功能的邻居节点发送携带本端状态信息的 LLDP 报文，同时也能通过 LLDP 报文获取使能 LLDP 功能的邻居节点的状态信息。网管可从路由器上获取当前设备的二层的连接状态信息并进行网络拓扑的分析。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **lldp enable**，使能全局 LLDP 功能。

----结束

3.3.3 （可选）禁止接口 LLDP 功能

在使能全局 LLDP 功能的情况下，所有接口缺省情况下都处于使能 LLDP 功能的状态。当部分接口需要禁用 LLDP 功能的情况下，执行 **undo lldp enable** 命令禁止 LLDP 功能。

前提条件

已使能全局 LLDP 功能。

背景信息

LLDP 功能有两个开关，一个是全局开关一个是接口下的开关，两者的关系为：

- 使能全局的 LLDP 功能后，缺省情况下所有接口的 LLDP 功能都处于使能状态。
- 去使能全局的 LLDP 功能后，除了 LLDP 告警功能外的所有关于 LLDP 的配置恢复缺省值。所以去使能全局的 LLDP 功能后，接口的 LLDP 功能处于去使能状态。
- 只有全局和接口下的 LLDP 功能都处于使能状态时，该接口才会发送或接收 LLDP 报文。
- 去使能全局 LLDP 功能的情况下，使能和去使能接口的 LLDP 命令无效。
- 当部分接口需要使能 LLDP 功能，而另一部分接口需要去使能 LLDP 功能时，可以全局使能 LLDP 功能，并在需要去使能 LLDP 功能的接口视图下执行 **undo lldp enable** 命令。当禁用 LLDP 功能的接口需要重新使能 LLDP 功能的情况下，在需要重新使能 LLDP 功能的接口视图下执行 **lldp enable** 命令重新使能接口 LLDP 功能。

说明

- 针对二层 Eth-Trunk 接口，LLDP 功能只能在二层 Eth-Trunk 的成员接口上进行配置，并且各成员接口的 LLDP 使能情况互相之间没有影响。
- 接口使能/去使能 LLDP 命令只能在已经全局使能 LLDP 的二层物理端口（Ethernet、GE）的视图中使用，对于如 VLANIF、Eth-Trunk 等逻辑端口的视图中则不能使用。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **undo lldp enable**，禁止接口 LLDP 功能。

----结束

3.3.4 （可选）配置 LLDP 管理地址

配置 LLDP 管理地址，供网管系统标识设备。

前提条件

已使能全局 LLDP 功能。

背景信息

如果指定的 IP 地址不合法，或没有配置管理 IP 地址，系统将自动从 IP 地址列表中查找并指定一个 IP 地址作为 LLDP 的管理 IP 地址。查找的顺序为：Loopback 接口、VLANIF 接口。对于同一种类型接口的 IP 地址，取最小的一个 IP 地址。如果没有找到缺省的 IP 地址，则用系统的桥 MAC。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **lldp management-address** *ip-address*，配置 LLDP 管理地址。

ip-address 必须为一个合法的并且是已经存在于设备上的单播 IP 地址。

----结束

3.3.5 （可选）配置 LLDPDU 发布的 TLV 属性

在 LLDP 帧交互的过程中，LLDPDU 往往根据要求包含了很多种不同的 TLV，根据这些不同的 TLV 来传输或者接收自己和邻近设备的信息。LLDP 可以封装的 TLV 包括基本 TLV、组织定义 TLV 以及媒体终端发现 MED（Media Endpoint Discovery）相关 TLV。

前提条件

- 已使能全局 LLDP 功能。
- 已使能接口的 LLDP 功能。

背景信息

端口发送的 802.3 Power via MDI TLV（通过 **lldp tlv-enable dot3-tlv power** 命令配置是否发布 802.3 Power via MDI TLV）有两种格式：

- 802.1ab 标准规定的格式：[TLV type | TLV information string length | 802.3 OUI | MDI power support | PSE power pair | power class]

- 802.3at 标准规定的格式：[TLV type | TLV information string length | 802.3 OUI | MDI power support | PSE power pair | power class | type/source/priority | PD requested power value | PSE allocated power value]

802.3at 在 802.1 ab 基础上扩展了后面 3 个字段 type/source/priority、PD requested power value 和 PSE allocated power value，用于提供更详细的信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **lldp tlv-enable** { **basic-tlv** { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **protocol-identity** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *Tel-Number* } | **network-policy** | **power-over-ethernet** } }，配置接口发布的 TLV 类型。

缺省情况下，LLDP 发布除 Location Identification TLV 之外所有类型的 TLV。

说明

- 配置发布基本类型 TLV、IEEE 802.1 组织类型 TLV 或 IEEE 802.3 组织类型 TLV 时，指定 **all** 参数，将发布该类型所有可选 TLV；配置发布 LLDP-MED 相关 TLV，指定 **all** 参数将发布除 Location Identification TLV 之外该类型的所有可选 TLV。

  不指定 **all** 参数，每次只能配置发布一种类型的可选 TLV，可以通过多次配置发布多种类型的可选 TLV。
- 必须首先配置发布 LLDP-MED Capabilities TLV，才能配置发布 LLDP-MED 其它类型的 TLV。

  必须首先禁止发布 LLDP-MED 其它类型的 TLV，才能禁止发布 LLDP-MED Capabilities TLV。

  必须首先禁止发布 LLDP-MED Capabilities TLV，才能禁止发布 MAC/PHY Configuration/Status TLV。
- 配置发布 802.3 的 MAC/PHY Configuration/Status TLV，必须通过配置发布 LLDP-MED Capabilities TLV 自动发布。
- 禁止发布 LLDP-MED 相关 TLV，指定 all 参数，不会自动禁止发布 MAC/PHY Configuration/Status TLV。

步骤 4 执行命令 **lldp dot3-tlv power** { **802.1ab** | **802.3at** }，配置端口发送 802.3 Power via MDI TLV 符合的标准。

缺省情况下，端口发送符合 802.1 ab 标准的 802.3 Power via MDI TLV。

说明

在选择发送哪种标准的 802.3 Power via MDI TLV 时，需要注意对端设备对这两种标准的支持情况，本端配置的标准需要对端支持。

----结束

3.3.6 （可选）配置 LLDP 时间属性

可以配置的 LLDP 时间属性包括：发送 LLDP 报文的周期、发送 LLDP 报文的延迟时间、本端信息在邻居节点中保持的时间倍数、接口 LLDP 功能重新使能的延迟时间和邻居信息变化告警的延迟时间。

前提条件

已使能全局 LLDP 功能。

背景信息

发送 LLDP 报文的周期和发送 LLDP 报文的延迟时间

LLDP 报文的发送时间周期是指设备状态一直没有发生变化的情况下接口模块周期性的向邻居节点发送 LLDP 报文的时间周期。设备统一配置该时间周期之后，每一个使能 LLDP 功能的接口都以该间隔为周期向邻居节点发送 LLDP 报文，但是各个接口发送报文的时间点可以不一致。LLDP 报文发送周期的取值要适当，同时要根据网络负载及时调节该参数。

- 取值大，能够减少 LLDP 报文交互频率，从而节省系统资源。但是取值过大会导致设备状态不能及时地通知到邻居节点，从而影响网络拓扑结构的及时发现。
- 取值小，能够增加本端状态信息向邻居节点发送的频率，从而能够及时发现网络拓扑结构。但是取值过小会导致 LLDP 报文交互过于频繁，从而增加系统的负担，造成资源的浪费。

发送 LLDP 报文的延迟时间是指设备状态频繁发生变化的时候，接口模块向邻居节点发送 LLDP 报文的最小延迟时间。设备统一配置该延迟时间之后，每一个使能 LLDP 功能的接口都以该值为最小延迟时间向邻居节点发送 LLDP 报文，但是各个接口发送报文的时间点可以不一致。当设备的状态信息频繁发生变化的时候可以通过延长该延迟时间来减少设备频繁向邻居节点发送信息，以达到抑制拓扑振荡目的。LLDP 报文发送延迟时间的取值要适当，同时要根据网络负载及时调节该参数。

- 取值大，能够减少 LLDP 报文交互频率，从而节省系统资源。但是取值过大会导致设备状态不能及时地通知到邻居节点，从而影响网络拓扑结构的及时发现。
- 取值小，能够增加本端状态信息向邻居节点发送的频率，从而能够及时发现网络拓扑结构。但是取值过小会导致 LLDP 报文交互过于频繁，从而增加系统的负载，造成资源的浪费。

LLDP 报文发送周期 interval 与延迟时间 delay 互相有制约关系，所以调整 interval 的取值时候需要注意与 delay 的取值的配合。

- 增加 *interval* 不受 *delay* 的制约，只要大于等于 5 且小于或等于 32768 就可以。
- 减小 *interval* 的时候，*interval* 的目标取值一定要大于或等于四倍的当前 *delay* 值。所以 *interval* 要取的目标值小于四倍的 *delay* 的时候，需要先将 *delay* 调整到小于或等于 *interval* 目标值的四分之一，然后再将 *interval* 减小到目标值。

说明

在 *interval* 的取值小于四倍的 *delay* 缺省值的情况下，无法用 **undo lldp message-transmission delay** 命令恢复 *delay* 的缺省值，会出现错误提示信息。需要先将 *interval* 的取值调整到大于或等于四倍的 *delay* 的缺省值，然后再执行 **undo lldp message-transmission delay** 命令。

本端信息在邻居节点中保持的时间倍数

本端信息在邻居节点中保持的时间倍数用于计算本次发送报文的有效时间。通过配置这个参数来调整设备信息在邻居节点中储存的有效时间。邻居节点接收到报文后，用这个有效时间更新其邻居节点（即发送端）的信息老化时间。

消息保持有效时间计算公式是：TTL = Min (65535，(*interval* × *hold*))

- TTL 代表 Time to live，表示设备信息在邻居节点中保持的时间，取 65535 和 *interval* × *hold* 中的最小值。

- *interval* 代表设备向邻居节点发送 LLDP 报文的时间周期，通过 **lldp message-transmission interval** 命令配置。
- *hold* 代表设备信息在邻居节点中保持的时间倍数。

当原来使能 LLDP 功能的设备去使能 LLDP 功能后，它的邻居设备不会马上老化掉该设备的信息，而是在等待 TTL 时间后再进行老化，以防止网络拓扑频繁变更。设备信息在邻居节点中保持的时间倍数的取值要适当。

- 取值大，能够减少网络拓扑的频繁变化。但是取值过大会导致设备状态不能及时地通知到邻居节点，从而影响网络拓扑结构的及时发现。
- 取值小，能够及时发现网络拓扑结构。但是取值过小会导致邻居设备频繁刷新该设备的信息，从而增加系统的负担，造成资源的浪费。
- 一般情况下建议使用缺省值。

接口 LLDP 功能重新使能的延迟时间

接口 LLDP 模块重新使能延迟时间是指设备上的接口 LLDP 模块从去使能状态重新使能的延迟时间。通过配置该参数能够抑制由于接口的 LLDP 协议状态频繁改变而导致的邻居节点的拓扑振荡。接口 LLDP 模块从去使能状态重新使能的延迟时间的取值要适当。

- 取值大，能够减少网络拓扑的频繁变化。但是取值过大会导致设备状态不能及时地通知到邻居节点，从而影响网络拓扑结构的及时发现。
- 取值小，能够及时发现网络拓扑结构。但是取值过小会导致邻居设备频繁刷新该设备的信息，从而增加系统的负担，造成资源的浪费。
- 一般情况下建议使用缺省值。

邻居信息变化告警的延迟时间

发送邻居信息变化告警的延迟时间是指在使能 LLDP 告警的情况下，设备向网管系统发送 LLDP 告警的最小延迟时间。当邻居信息频繁发生变化的时候，可以通过延长该延迟时间来减少设备频繁向网管系统发送信息的情况，以达到抑制拓扑振荡目的。设备统一配置该延迟时间之后，每一个使能 LLDP 功能的接口都以该值为最小延迟时间向网管系统发送邻居信息变化告警，但是各个接口发送告警的时间点可以不一致。

该延迟时间只对插入邻居节点数、删除邻居节点数、老化邻居节点数、丢弃邻居节点数等邻居信息变化的告警（LLDP_1.0.8802.1.1.2.0.0.1 lldpRemTablesChange）起作用，对其它告警无影响。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **lldp message-transmission interval** *interval*，配置发送 LLDP 报文的周期。

缺省情况下，LLDP 报文的周期为 30 秒。

步骤 3 执行命令 **lldp message-transmission delay** *delay*，配置发送 LLDP 报文的延迟时间。

缺省情况下，发送 LLDP 报文的延迟时间是 2 秒。

步骤 4 执行命令 **lldp message-transmission hold-multiplier** *hold*，配置本端信息在邻居节点中保持时间的倍数。

缺省值是 4。

说明

- 增加该值能够延长本端信息在邻居节点中保持的时间。
- *hold* 的取值范围是 2 ~ 10，但当 hold**interval* 的值大于 65535 时，配置不生效。

步骤 5 执行命令 **lldp restart-delay** *delay*，配置接口 LLDP 功能重新使能的延迟时间。

缺省值是 2 秒。

在禁止 LLDP 功能的情况下，需要经过该延迟时间才能重新使能接口 LLDP 功能。

步骤 6 执行命令 **lldp trap-interval** *interval*，配置邻居信息变化告警的延迟时间。

缺省值是 5 秒。

----结束

3.3.7 （可选）使能 LLDP 告警

在邻居信息发生变化时，为了向网管系统发送告警信息，需要在路由器上使能告警功能。

背景信息

使能设备的告警功能后，当设备出现以下情况时，设备会向网管系统发送告警。

- 使能或去使能全局 LLDP 功能，对应告警 LLDP_1.3.6.1.4.1.2011.5.25.134.2.1 hwLldpEnabled 和 LLDP_1.3.6.1.4.1.2011.5.25.134.2.2 hwLldpDisabled。
- 本地管理地址改变，对应告警 LLDP_1.3.6.1.4.1.2011.5.25.134.2.5 hwLldpLocManIPAddrChange。
- 邻居信息发生变化（邻居管理地址变化本地不会产生告警信息），对应告警 LLDP_1.0.8802.1.1.2.0.0.1 lldpRemTablesChange。

告警功能对全局起作用，控制所有接口发送告警的能力。使能告警功能不以 LLDP 全局使能为前提。在组网前期网络拓扑变化频繁，可以关闭告警功能，控制告警信息频繁上送网管系统。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent trap enable**，使能告警功能。

缺省情况下，AR3200 的告警功能处于禁用状态。

说明

配置 LLDP 告警功能前，AR3200 与网管系统之间必须要有可达路由，且 SNMP 相关参数已经配置完成。

----结束

3.3.8 检查配置结果

前提条件

已经完成上述所有配置。

操作步骤

- 使用 **display lldp local** [**interface** *interface-type interface-number*]命令查看设备的本地 LLDP 状态。
- 使用 **display lldp neighbor** [**interface** *interface-type interface-number*]命令查看设备接口的邻居信息。
- 使用 **display lldp neighbor brief** 命令查看设备邻居的概要信息。
- 使用 **display lldp tlv-config** 命令查看接口可以发送的 TLV 类型。

----结束

任务示例

在配置成功之后，执行 **display lldp local** 命令查看设备的 LLDP 功能处于 enabled 状态，接口 LLDP 功能处于 enabled 状态、LLDP 管理地址为 10.10.10.1，发送 LLDP 报文的周期和延迟时间、本端信息在邻居节点中保持时间的倍数、LLDP 模块重新使能的延迟时间、邻居信息变化告警的延迟时间等 LLDP 属性的值配置正确。

```
<Huawei> display lldp local
System information
Chassis type   :macAddress
Chassis ID     :00e0-11fc-1710
System name    :Huawei
System description  :Huawei AR3260 Huawei Versatile Routing Platform Software  V
RP (R) software,Version 5.100 (AR3260 V200R002C00) Copyright (C) 2000-2011 Huawei
 Technologies Co., Ltd
System capabilities supported   :bridge
System capabilities enabled     :bridge
LLDP Up time   :2011/6/13 11:40:49

MED system information
Device class   :Network Connectivity
(MED inventory information of master board)
HardwareRev       :AR01SRU1A VER.A
FirmwareRev       :NA
SoftwareRev       :V200R002C00
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO., LTD
Model name        :NA
Asset tracking identifier :NA

System configuration
LLDP Status                     :enabled            (default is disabled)
LLDP Message Tx Interval        :30                 (default is 30s)
LLDP Message Tx Hold Multiplier :4                  (default is 4)
LLDP Refresh Delay              :2                  (default is 2s)
LLDP Tx Delay                   :2                  (default is 2s)
LLDP Notification Interval      :5                  (default is 5s)
LLDP Notification Enable        :enabled            (default is disabled)
Management Address              :IP: 10.10.10.1

Remote Table Statistics:
Remote Table Last Change Time   :0 days, 5 hours, 57 minutes, 32 seconds

Remote Neighbors Added          :15

Remote Neighbors Deleted        :13

Remote Neighbors Dropped        :0

Remote Neighbors Aged           :0

Total Neighbors                 :2
```

```
Port information:

Interface GigabitEthernet0/0/0 currently is L3 interface.
Interface GigabitEthernet0/0/1 currently is L3 interface.
Interface GigabitEthernet0/0/2 currently is L3 interface.
Interface Ethernet2/0/0:
LLDP Enable Status       :enabled             (default is disabled)
Total Neighbors          :1

Port ID subtype     :interfaceName
Port ID             :Ethernet2/0/0
Port description    :HUAWEI, AR Series, Interface

Port And Protocol VLAN ID(PPVID) don't supported
Port VLAN ID(PVID)  :
1
VLAN name of VLAN 1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :9216

MED port information

Media policy type   :Unknown
Unknown Policy      :Yes
VLAN tagged         :No
Media policy VlanID           :0
Media policy L2 priority      :0
Media policy Dscp             :0

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:0
  ---- More ----
```

在配置成功后，执行 **display lldp neighbor** [**interface** *interface-type interface-number*]命令查看设备的 LLDP 功能处于 enabled 状态，接口 LLDP 功能处于 enabled 状态，可以查看到设备 ID、接口 ID、设备名称、设备描述信息、管理地址和老化时间。

```
<Huawei> display lldp neighbor
Ethernet2/0/0 has 1 neighbors:

Neighbor index : 1
Chassis type   :macAddress
Chassis ID     :00e0-11fc-1710
Port ID type   :interfaceName
Port ID        :Ethernet2/0/0
Port description    :HUAWEI, AR Series, Interface
System name         :Huawei
System description  :Huawei AR3260 Huawei Versatile Routing Platform Software  V
RP (R) software,Version 5.100 (AR3260 V200R002C00) Copyright (C) 2000-2011 Huawei
 Technologies Co., Ltd
System capabilities supported   :bridge
System capabilities enabled     :bridge
Management address type  :ipV4
```

```
Management address       : 127.0.0.1
Expired time   :104s


Port VLAN ID(PVID)  :1
VLAN name of VLAN  1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP GVRP

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Signal
Port power classification:Class3

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :1600

MED Device information
Device class   :Network Connectivity

HardwareRev       :AR01SRU1A VER.A
FirmwareRev       :128
SoftwareRev       :V200R002C00
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO., LTD
Model name        :NA
Asset tracking identifier :NA

Media policy type   :Voice
Unknown Policy      :Defined
VLAN tagged         :Yes
Media policy VlanID      :0
Media policy L2 priority :6
Media policy Dscp        :46

Power Type               :PSE
PoE PSE power source     :PSE
Port PSE Priority        :Low
Port Available power value:2
```

在配置成功后，执行 **display lldp neighbor brief** 命令可以查看的概要邻居信息包括：本地接口名、邻居设备名称、邻居接口名、老化时间。

```
<Huawei> display lldp neighbor brief
Local Intf   Neighbor Dev            Neighbor Intf            Exptime
Eth2/0/0     AR                      Eth2/0/0                 103
```

3.4 维护

维护 LLDP 功能，包括清除 LLDP 统计信息、监控 LLDP 运行状态。

3.4.1 清除 LLDP 统计信息

通过执行 reset 命令，清除 LLDP 的统计信息。

操作步骤

- 在用户视图下，使用 **reset lldp statistics** [**interface** *interface-type interface-number*] 命令清除关于 LLDP 报文的统计信息。

----结束

3.4.2 监控 LLDP 运行状态

通过 display 命令监控 LLDP 的运行情况。

操作步骤

- 使用 **display lldp local** [**interface** *interface-type interface-number*]命令查看全局或指定接口的当前 LLDP 状态。
- 使用 **display lldp statistics** [**interface** *interface-type interface-number*]命令查看设备接口收发报文统计信息。
- 使用 **display lldp neighbor** [**interface** *interface-type interface-number*]命令查看设备接口的邻居信息。

----结束

3.5 配置举例

介绍 LLDP 的不同组网中举例。

3.5.1 配置 LLDP 功能示例-单邻居组网

单邻居组网方式下，通过配置 LLDP 功能，使得 NMS 可以获取到网络的拓扑信息。

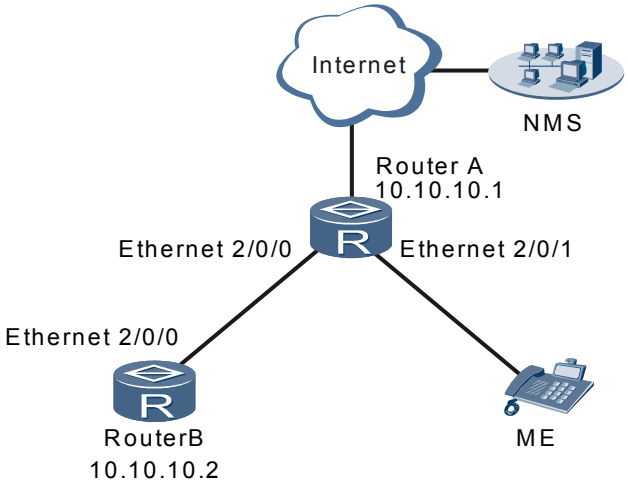
组网需求

如图 3-7 所示，RouterA 和 RouterB 之间、RouterA 和 ME 均为直接相连。这时网络管理员希望在 NMS 上可以获取到 RouterA、RouterB 和 ME 的二层配置信息，用于了解网络的详细拓扑信息和判断网络中是否有配置冲突的情况。这时，可以通过在 RouterA 和 RouterB 上使能 LLDP 功能来实现网络管理员的需求。

另外，管理员希望当 LLDP 管理地址变化、全局 LLDP 功能使能或去使能以及邻居信息发生变化的时候，RouterA、RouterB 能主动向网管系统发送 LLDP 告警，这样便于管理员快速发现网络拓扑的变化。

组网中的 ME 设备支持 LLDP 功能，NMS 与 Router 之间有可达路由且 SNMP 相关功能已经配置完成。

图 3-7 配置 LLDP 功能-单邻居组网图



配置思路

采用如下的思路配置 LLDP 功能：

1. 使能 RouterA 和 RouterB 的全局 LLDP 功能。
2. 配置 RouterA 和 RouterB 的管理 IP 地址方便网管系统进行管理。
3. 使能 RouterA 和 RouterB 的 LLDP 告警。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA 和 RouterB 的管理 IP 地址为 10.10.10.1 和 10.10.10.2。

操作步骤

步骤 1 使能 RouterA 和 RouterB 的全局 LLDP 功能。

配置 RouterA。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] lldp enable
```

配置 RouterB。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] lldp enable
```

步骤 2 配置 RouterA 和 RouterB 的管理 IP 地址。

配置 RouterA。

```
[RouterA] lldp management-address 10.10.10.1
```

配置 RouterB。

```
[RouterB] lldp management-address 10.10.10.2
```

步骤 3 使能 RouterA 和 RouterB 的 LLDP 告警。

配置 RouterA。

```
[RouterA] snmp-agent trap enable
```

配置 RouterB。

```
[RouterB] snmp-agent trap enable
```

步骤 4 验证配置结果。

查看各设备的 LLDP 是否使能、LLDP 管理地址是否配置以及 LLDP 告警功能是否使能。

- 查看 RouterA。

```
<RouterA> display lldp local
System information
Chassis type   :macAddress
Chassis ID     :00e0-11fc-1710
System name    :RouterA
System description  :Huawei AR3260 Huawei Versatile Routing Platform Software  V
RP (R) software,Version 5.100 (AR3260 V200R002C00) Copyright (C) 2000-2011 Huawei
 Technologies Co., Ltd
System capabilities supported   :bridge
System capabilities enabled     :bridge
LLDP Up time   :2011/06/13 11:40:49

MED system information
Device class   :Network Connectivity
(MED inventory information of master board)
HardwareRev       :AR01SRU1A VER.A
FirmwareRev       :NA
SoftwareRev       :V200R002C00
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO.,
LTD
Model name        :NA
Asset tracking identifier :NA

System configuration
LLDP Status                     :enabled            (default is disabled)
LLDP Message Tx Interval        :30                 (default is 30s)
LLDP Message Tx Hold Multiplier :4                  (default is 4)
LLDP Refresh Delay              :2                  (default is 2s)
LLDP Tx Delay                   :2                  (default is 2s)
LLDP Notification Interval      :5                  (default is 5s)
LLDP Notification Enable        :enabled            (default is disabled)
Management Address              :IP: 10.10.10.1  MAC: 00e0-11fc-1710

Remote Table Statistics:
Remote Table Last Change Time   :0 days, 5 hours, 57 minutes, 32 seconds

Remote Neighbors Added          :15

Remote Neighbors Deleted        :13

Remote Neighbors Dropped        :0

Remote Neighbors Aged           :0

Total Neighbors                 :2


Port information:

Interface GigabitEthernet0/0/0 currently is L3 interface.
Interface GigabitEthernet0/0/1 currently is L3 interface.
```

```
Interface GigabitEthernet0/0/2 currently is L3 interface.
Interface Ethernet2/0/0:
LLDP Enable Status       :enabled             (default is disabled)
Total Neighbors          :1

Port ID subtype     :interfaceName
Port ID             :Ethernet2/0/0
Port description    :HUAWEI, AR Series, Ethernet2/0/0 Interface

Port And Protocol VLAN ID(PPVID) don't supported
Port VLAN ID(PVID)  :
1
VLAN name of VLAN 1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :9216

MED port information

Media policy type   :Voice
Unknown Policy      :Defined
VLAN tagged         :Yes
Media policy VlanID           :0
Media policy L2 priority      :6
Media policy Dscp             :46

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:2
```

查看 RouterA 的邻居信息。

```
<RouterA> display lldp neighbor interface ethernet 2/0/0
Ethernet2/0/0 has 1 neighbors:


Neighbor index : 1
Chassis type   :macAddress
Chassis ID     :00e0-11fc-1710
Port ID type   :interfaceName
Port ID        :Ethernet2/0/0
Port description    :HUAWEI, AR Series, Ethernet2/0/0 Interface
System name         :RouterB
System description  :Huawei AR3260 Huawei Versatile Routing Platform Software  V
RP (R) software,Version 5.100 (AR3260 V200R002C00) Copyright (C) 2000-2011 Huawei
 Technologies Co., Ltd
System capabilities supported   :bridge
System capabilities enabled     :bridge
Management address type  :ipV4
Management address       : 10.10.10.2
Expired time   :104s


Port VLAN ID(PVID)  :1
VLAN name of VLAN  1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM
```

```
Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :9216

MED Device information
Device class   :Network Connectivity

HardwareRev       :AR01SRU3A VER.A
FirmwareRev       :100
SoftwareRev       :V200R002C00
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO.,
LTD
Model name        :NA
Asset tracking identifier :NA

Media policy type   :Voice
Unknown Policy      :Defined
VLAN tagged         :Yes
Media policy VlanID      :0
Media policy L2 priority :6
Media policy Dscp        :46

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:2
```

- 查看 RouterB。

  请参见 RouterA 的查看过程。

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 10.10.10.1 255.255.255.0
#
 lldp enable
#
 snmp trap enable
#
 lldp management-address  10.10.10.1
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
```

```
 ip address 10.10.10.2 255.255.255.0
#
 lldp enable
#
 snmp trap enable
#
 lldp management-address 10.10.10.2
#
return
```

3.5.2 配置 LLDP 功能示例-多邻居组网

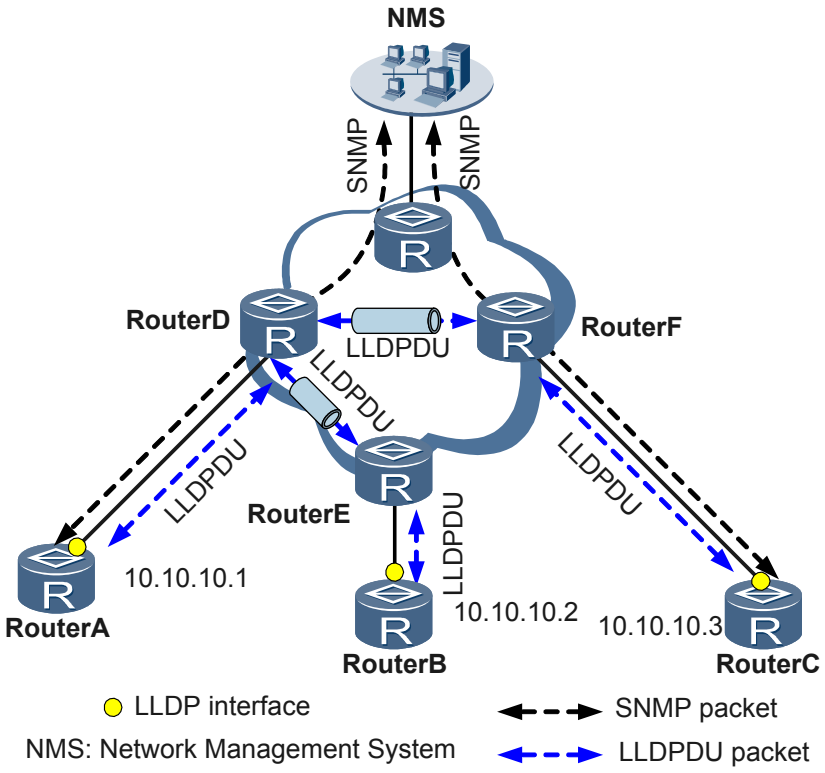
多邻居组网方式下，通过配置 LLDP 功能，使得 NMS 可以获取到网络的拓扑信息。

组网需求

如图 3-8 所示，RouterA、RouterB 和 RouterC 之间通过一个未知网络相连，该未知网络无需 NMS 管理，但该网络可以透传 LLDP 报文。这时网络管理员希望在 NMS 上可以获取到 RouterA、RouterB 和 RouterC 之间的二层配置信息，用于了解网络的详细拓扑信息和判断网络中是否有配置冲突的情况。这时，可以通过在 RouterA、RouterB 和 RouterC 上使能 LLDP 功能来实现网络管理员的需求。

组网中 NMS 与 RouterA、RouterB 和 RouterC 之间有可达路由且 SNMP 相关功能已经配置完成。

图 3-8 配置 LLDP 功能-多邻居组网图



配置思路

采用如下的思路配置 LLDP 功能：

1. 使能 RouterA、RouterB 和 RouterC 的全局 LLDP 功能。
2. 配置 RouterA、RouterB 和 RouterC 的管理 IP 地址方便网管系统进行管理。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA、RouterB 和 RouterC 的管理 IP 地址。

操作步骤

步骤 1 配置 RouterA、RouterB 和 RouterC 的 LLDP 全局使能。

配置 RouterA。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] lldp enable
```

配置 RouterB。

请参见 RouterA 的配置。

配置 RouterC。

请参见 RouterA 的配置。

步骤 2 配置 RouterA、RouterB 和 RouterC 的管理 IP 地址。

配置 RouterA。

```
[RouterA] lldp management-address 10.10.10.1
```

配置 RouterB。

```
[RouterB] lldp management-address 10.10.10.2
```

配置 RouterC。

```
[RouterC] lldp management-address 10.10.10.3
```

步骤 3 验证配置结果。

查看各设备的 LLDP 功能是否使能、LLDP 管理地址是否配置。

- 查看 RouterA 的配置。

```
<RouterA> display lldp local
System information
Chassis type   :macAddress
Chassis ID     :00e0-11fc-1710
System name    :RouterA
System description  :Huawei AR3260 Huawei Versatile Routing Platform Software  V
RP (R) software,Version 5.100 (AR3260 V200R002C00) Copyright (C) 2000-2011 Huawei
 Technologies Co., Ltd
System capabilities supported   :bridge
System capabilities enabled     :bridge
LLDP Up time   :2010/11/13 11:40:49

MED system information
Device class   :Network Connectivity
(MED inventory information of master board)
HardwareRev       :AR01SRU1A VER.A
FirmwareRev       :NA
SoftwareRev       :V200R002C00
```

```
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO.,
LTD
Model name        :NA
Asset tracking identifier :NA

System configuration
LLDP Status                     :enabled            (default is disabled)
LLDP Message Tx Interval        :30                 (default is 30s)
LLDP Message Tx Hold Multiplier :4                  (default is 4)
LLDP Refresh Delay              :2                  (default is 2s)
LLDP Tx Delay                   :2                  (default is 2s)
LLDP Notification Interval      :5                  (default is 5s)
LLDP Notification Enable        :enabled            (default is disabled)
Management Address              :IP: 10.10.10.1  MAC: 00e0-11fc-1710

Remote Table Statistics:
Remote Table Last Change Time   :0 days, 5 hours, 57 minutes, 32 seconds

Remote Neighbors Added          :15

Remote Neighbors Deleted        :13

Remote Neighbors Dropped        :0

Remote Neighbors Aged           :0

Total Neighbors                 :2


Port information:

Interface GigabitEthernet0/0/0 currently is L3 interface.
Interface GigabitEthernet0/0/1 currently is L3 interface.
Interface GigabitEthernet0/0/2 currently is L3 interface.
Interface Ethernet2/0/0:
LLDP Enable Status       :enabled             (default is disabled)
Total Neighbors          :1

Port ID subtype     :interfaceName
Port ID             :Ethernet2/0/0
Port description    :HUAWEI, AR Series, Ethernet2/0/0 Interface

Port And Protocol VLAN ID(PPVID) don't supported
Port VLAN ID(PVID)  :
1
VLAN name of VLAN 1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :9216

MED port information

Media policy type   :Voice
Unknown Policy      :Defined
```

```
VLAN tagged         :Yes
Media policy VlanID           :0
Media policy L2 priority      :6
Media policy Dscp             :46

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:2
  ---- More
----
```

查看 RouterA 的邻居信息。

```
<RouterA> display lldp neighbor interface ethernet 2/0/0
Ethernet2/0/0 has 1 neighbors:

Neighbor index : 1
Chassis type   :macAddress
Chassis ID     :00e0-11fc-1710
Port ID type   :interfaceName
Port ID        :Ethernet2/0/0
Port description    :HUAWEI, AR Series, Ethernet2/0/0 Interface
System name         :RouterB
System description  :Huawei AR3260 Huawei Versatile Routing Platform Software  V
RP (R) software,Version 5.100 (AR3260 V200R002C00) Copyright (C) 2000-2011 Huawei
 Technologies Co., Ltd
System capabilities supported   :bridge
System capabilities enabled     :bridge
Management address type  :ipV4
Management address       : 10.10.10.2
Expired time   :104s


Port VLAN ID(PVID)  :1
VLAN name of VLAN  1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :9216

MED Device information
Device class   :Network Connectivity

HardwareRev       :AR01SRU3A VER.A
FirmwareRev       :100
SoftwareRev       :V200R002C00
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO.,
LTD
Model name        :NA
Asset tracking identifier :NA

Media policy type   :Voice
Unknown Policy      :Defined
VLAN tagged         :Yes
Media policy VlanID      :0
Media policy L2 priority :6
```

```
Media policy Dscp        :46

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:2
```

- 查看 RouterB 的配置。

  请参见 RouterA 的查看过程。

- 查看 RouterC 的配置。

  请参见 RouterA 的查看过程。

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 10.10.10.1 255.255.255.0
#
 lldp enable
#
 lldp management-address 10.10.10.1
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface interface GigabitEthernet1/0/0
 ip address 10.10.10.2 255.255.255.0
#
 lldp enable
#
 lldp management-address 10.10.10.2
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 ip address 10.10.10.3 255.255.255.0
#
 lldp enable
#
 lldp management-address 10.10.10.3
#
return
```

3.5.3 配置 LLDP 功能示例-组网中存在链路聚合

组网中存在链路聚合的情况下，通过配置 LLDP 功能，使得 NMS 可以获取到网络的拓扑信息。

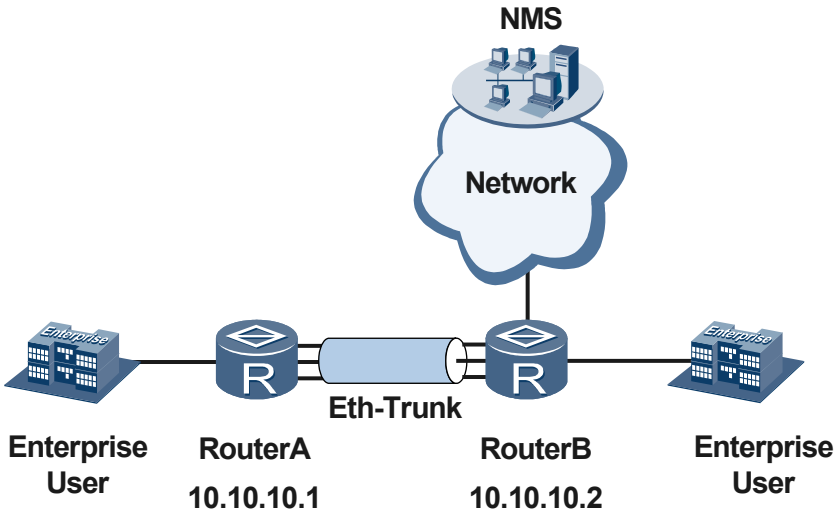
组网需求

如图 3-9 所示，RouterA 与 RouterB 之间通过 Eth-Trunk 相连。网络管理员希望在 NMS 上可以获取到 Router 之间的二层配置信息，用于了解除未知网络以外的设备的详细拓扑

信息和判断 Router 中是否有配置错误的情况。这时，可以通过在 RouterA 与 RouterB 上使能 LLDP功能来实现网络管理员的需求。

组网中 NMS 与 RouterA 和 RouterB 之间有可达路由且 SNMP 相关功能已经配置完成。

图 3-9 配置 LLDP 功能示例组网图-组网中存在链路聚合



配置思路

采用如下的思路配置 LLDP 功能：

1. 将 RouterA 和 RouterB 的以太网物理接口加入到 Eth-Trunk 中。
2. 使能 RouterA 和 RouterB 的全局 LLDP 功能。
3. 配置 RouterA 和 RouterB 的管理 IP 地址方便网管系统进行管理。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA 和 RouterB 的管理 IP 地址为 10.10.10.1 和 10.10.10.2。
- RouterA 和 RouterB 相连的 Eth-Trunk 的编号，加入到该 Eth-Trunk 的成员接口的编号。

操作步骤

步骤 1 配置 RouterA 和 RouterB 的 Eth-Trunk。

配置 RouterA。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] vlan batch 100
[RouterA] interface eth-trunk 1
[RouterA-Eth-Trunk1] trunkport ethernet 2/0/0 to 2/0/2
[RouterA-Eth-Trunk1] port link-type trunk
[RouterA-Eth-Trunk1] port trunk allow-pass vlan 100
[RouterA-Eth-Trunk1] quit
```

配置 RouterB。

请参见 RouterA 的配置。

步骤 2 使能 RouterA 和 RouterB 的全局 LLDP 功能。

配置 RouterA。

```
[RouterA] lldp enable
```

配置 RouterB。

请参见 RouterA 的配置。

步骤 3 配置 RouterA 和 RouterB 的管理 IP 地址以便在邻居设备中标识本端设备。

配置 RouterA。

```
[RouterA] lldp management-address 10.10.10.1
```

配置 RouterB。

```
[RouterB] lldp management-address 10.10.10.2
```

步骤 4 验证配置结果。

- 查看 RouterA 的配置。

  # 查看各设备的成员接口是否已经加入到 Eth-Trunk1。

```
[RouterA] display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL         Hash arithmetic: According to SA-XOR-DA
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 8
Operate status: up          Number Of Up Port In Trunk: 3
--------------------------------------------------------------------------------
PortName                      Status      Weight
Ethernet2/0/0                 Up          1
Ethernet2/0/1                 Up          1
Ethernet2/0/2                 Up          1
```

  #查看设备当前的 LLDP 信息。

```
<RouterA> display lldp local
System information
Chassis type   :macAddress
Chassis ID     :00e0-11fc-1710
System name    :RouterA
System description  :Huawei AR3260 Huawei Versatile Routing Platform Software  V
RP (R) software,Version 5.100 (AR3260 V200R002C00) Copyright (C) 2000-2011 Huawei
 Technologies Co., Ltd
System capabilities supported   :bridge
System capabilities enabled     :bridge
LLDP Up time   :2010/12/13 11:40:49

MED system information
Device class   :Network Connectivity
(MED inventory information of master board)
HardwareRev       :AR01SRU1A VER.A
FirmwareRev       :NA
SoftwareRev       :V200R002C00
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO.,
LTD
Model name        :NA
Asset tracking identifier :NA

System configuration
LLDP Status                    :enabled            (default is disabled)
LLDP Message Tx Interval       :30                 (default is 30s)
LLDP Message Tx Hold Multiplier :4                 (default is 4)
```

```
LLDP Refresh Delay              :2                  (default is 2s)
LLDP Tx Delay                   :2                  (default is 2s)
LLDP Notification Interval      :5                  (default is 5s)
LLDP Notification Enable        :enabled            (default is disabled)
Management Address              :IP: 10.10.10.1  MAC: 00e0-11fc-1710

Remote Table Statistics:
Remote Table Last Change Time   :0 days, 5 hours, 57 minutes, 32 seconds

Remote Neighbors Added          :15

Remote Neighbors Deleted        :13

Remote Neighbors Dropped        :0

Remote Neighbors Aged           :0

Total Neighbors                 :2


Port information:

Interface GigabitEthernet0/0/0 currently is L3 interface.
Interface GigabitEthernet0/0/1 currently is L3 interface.
Interface GigabitEthernet0/0/2 currently is L3 interface.
Interface Ethernet2/0/0:
LLDP Enable Status       :enabled             (default is disabled)
Total Neighbors          :1

Port ID subtype     :interfaceName
Port ID             :Ethernet2/0/0
Port description    :HUAWEI, AR Series, Ethernet2/0/0 Interface

Port And Protocol VLAN ID(PPVID) don't supported
Port VLAN ID(PVID)  :
1
VLAN name of VLAN 1 : VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :9216

MED port information

Media policy type   :Voice
Unknown Policy      :Defined
VLAN tagged         :Yes
Media policy VlanID           :0
Media policy L2 priority      :6
Media policy Dscp             :46

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:2
```

```
Interface Ethernet2/0/1:
LLDP Enable Status       :enabled             (default is disabled)
Total Neighbors          :1

Port ID subtype     :interfaceName
Port ID             :Ethernet2/0/1
Port description    :HUAWEI, AR Series, Ethernet2/0/1 Interface

Port And Protocol VLAN ID(PPVID) don't supported
Port VLAN ID(PVID)  :
1
VLAN name of VLAN 1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :1628

MED port information

Media policy type   :Voice
Unknown Policy      :Defined
VLAN tagged         :Yes
Media policy VlanID           :0
Media policy L2 priority      :6
Media policy Dscp             :46

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:2


Interface Ethernet2/0/2:
LLDP Enable Status       :enabled             (default is disabled)
Total Neighbors          :1

Port ID subtype     :interfaceName
Port ID             :Ethernet2/0/2
Port description    :HUAWEI, AR Series, Ethernet2/0/2 Interface

Port And Protocol VLAN ID(PPVID) don't supported
Port VLAN ID(PVID)  :
1
VLAN name of VLAN 1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
```

```
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :1628

MED port information

Media policy type   :Voice
Unknown Policy      :Defined
VLAN tagged         :Yes
Media policy VlanID           :0
Media policy L2 priority      :6
Media policy Dscp             :46

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:2
```

查看 RouterA 的邻居信息。

```
[RouterA] display lldp neighbor brief
Local Intf   Neighbor Dev            Neighbor Intf            Exptime
Eth2/0/0     RouterB                 Eth2/0/0                 115
Eth2/0/1     RouterB                 Eth2/0/1                 115
Eth2/0/2     RouterB                 Eth2/0/2                 115
```

- 查看 RouterB 的配置。

  请参见 RouterA 的查看过程。

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 vlan batch 100
#
interface GigabitEthernet1/0/0
 ip address 10.10.10.1 255.255.255.0
#
 lldp enable
#
 lldp management-address  10.10.10.1
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface Ethernet2/0/0
 eth-trunk 1
#
interface Ethernet2/0/1
 eth-trunk 1
#
interface Ethernet2/0/2
 eth-trunk 1
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
```

```
 ip address 10.10.10.2 255.255.255.0
#
 vlan batch 100
#
 lldp enable
#
 lldp management-address  10.10.10.2
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface Ethernet2/0/0
 eth-trunk 1
#
interface Ethernet2/0/1
 eth-trunk 1
#
interface Ethernet2/0/2
 eth-trunk 1
#
return
```

4 CWMP 配置

关于本章

介绍 CWMP 的基本概念、配置步骤以及配置举例。

4.1 CWMP 概述
CWMP 定义了 CPE 与 ACS 之间的通信机制，通过 CWMP 可实现 ACS 对 CPE 的集中管理。

4.2 AR3200 支持的 CWMP 特性
AR3200 作为 CPE 设备，为实现 ACS 对 CPE 的管理和维护，首先需要建立 ACS 和 CPE 之间的连接，连接过程中对 CPE 或 ACS 的合法性进行认证，认证成功则允许建立连接。建立连接后，ACS 可通过远程过程调用 RPC（Remote Procedure Call）方法，实现对 CPE 的管理和维护。

4.3 配置 CWMP 功能
介绍如何配置 CWMP 功能。

4.4 配置举例
介绍 CWMP 举例。

4.1 CWMP 概述

CWMP 定义了 CPE 与 ACS 之间的通信机制，通过 CWMP 可实现 ACS 对 CPE 的集中管理。

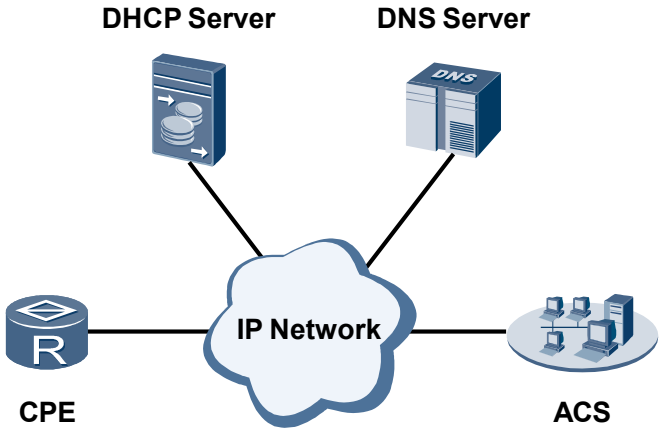
CWMP（TR-069）简介

广域网管理协议 CWMP（CPE WAN Management Protocol）是由数字用户线路 DSL（Digital Subscriber's Line）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 主要应用于 DSL 接入网络环境。在 DSL 接入网络中，由于用户侧设备数量繁多、部署分散，不易进行设备的管理和维护，CWMP 提出通过自动配置服务器 ACS（Auto-Configuration Server）对用户侧设备 CPE（Customer Premises Equipment）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。

CWMP 网络模型

CWMP 网络模型如图 4-1 所示。

图 4-1 CWMP 网络模型图



CWMP 网络模型包括：

- ACS：网络中的管理设备，可以完成对 CPE 设备的管理和维护操作。
- CPE：网络中的被管理设备。
- DNS server：域名服务器。CWMP 协议规定 ACS 和 CPE 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：动态主机配置协议服务器。给 ACS 和 CPE 分配 IP 地址，使用 DHCP 报文中的 option 字段给 CPE 配置参数。

说明

AR3200 作为 CPE 来部署。

4.2 AR3200 支持的 CWMP 特性

AR3200 作为 CPE 设备，为实现 ACS 对 CPE 的管理和维护，首先需要建立 ACS 和 CPE 之间的连接，连接过程中对 CPE 或 ACS 的合法性进行认证，认证成功则允许建立连接。建立连接后，ACS 可通过远程过程调用 RPC（Remote Procedure Call）方法，实现对 CPE 的管理和维护。

ACS 和 CPE 的自动连接

ACS 和 CPE 的自动连接有两种：

- CPE 发起连接
- ACS 发起连接

CPE 和 ACS 都可以发起连接，避免在 CPE 和 ACS 之间维护一个长期的连接，从而节省网络资源和减少开销。

- **CPE 发起连接**

  CPE 通过发送 Inform 报文自动建立与 ACS 的连接，通过 ACS 的认证后，允许与 ACS 建立连接。发起连接的方式有以下几种：

  - CPE 启动，根据获取的 URL 值找到相应的 ACS，自动发起连接。
  - CPE 使能了周期性发送 Inform 报文功能，当周期（如 1 小时）到达时，CPE 会自动发送 Inform 报文来建立连接。
  - CPE 使能了定时发送 Inform 报文功能，当时间点到达时，CPE 会自动发送 Inform 报文来建立连接。
  - 如果当前连接异常中断，而且 CPE 自动重新连接的次数还没有达到上限，此时，CPE 也会自动发起连接。

- **ACS 发起连接**

  ACS 可以在任何时候自动向 CPE 发起连接请求，通过 CPE 的认证后，允许与 CPE 建立连接。

  这种方式需要 ACS 和 CPE 之间通过 CPE 先发送连接请求，与 ACS 进行过至少一次通信。在这次通信中，如果 ACS 希望以后允许 ACS 先发起连接请求，它会将 CPE 的 IP 地址保存在地址列表中。

SSL 功能

传输层安全协议 SSL(Security Socket Layer)是由 Netscape 公司提出的一种安全协议，SSL 协议采用公开密钥技术，保证两个应用间通信的保密性和可靠性，使客户与服务器应用之间的通信不被攻击者窃听。

SSL 协议的优势在于它是与应用层协议独立无关的。高层的应用层协议（例如：Http、FTP、Telnet 等等）能透明的建立于 SSL 协议之上。SSL 协议在应用层协议通信之前就已经完成加密算法、通信密钥的协商以及服务器认证工作。在此之后应用层协议所传送的数据都会被加密，从而保证通信的私密性。

ACS 对 CPE 的管理和维护

CPE 与 ACS 之间建立连接后，ACS 可通过 CWMP 协议规定的 RPC 方法，实现对 CPE 的管理和维护，主要包括以下功能：

- **支持 ACS 对 CPE 的自动配置**

  当 CPE 上线时，ACS 可以自动下发一些配置给 CPE，完成对 CPE 的自动配置。设备支持的自动配置项主要包括：

  - 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 用户名
  - CPE 密码

- **支持 ACS 对 CPE 系统启动文件和配置文件的上传/下载管理**

  网络管理员可以将系统启动文件、配置文件等重要文件保存在文件服务器上。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。

- **支持 ACS 对 CPE 的状态和性能监控**

  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，可执行的功能也有差异，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 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。

说明

ACS 对 CPE 的管理和维护属于 ACS 的配置，此配置任务不做介绍。

4.3 配置 CWMP 功能

介绍如何配置 CWMP 功能。

4.3.1 建立配置任务

应用环境

CWMP 提出通过 ACS 对 CPE 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。

前置任务

在配置 CWMP 功能之前，需完成以下任务：

- 路由器与 ACS 之间路由可达
- 路由器上与 ACS 进行报文交互接口的 IP 地址

数据准备

在配置 CWMP 功能之前，需要准备以下数据。

序号	数据
1	路由器连接到 ACS 的 URL、用户名和密码
2	ACS 连接到路由器的用户名和密码
3	路由器上与 ACS 进行报文交互接口名称和编号
4	周期性发送 Inform 报文的时间间隔
5	定时发送 Inform 报文的日期和时间
6	自动重新连接的次数
7	无数据传输超时时间

4.3.2 使能 CWMP 功能

使能 CWMP 后，CWMP 的其他配置才能生效。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cwmp**，进入 CWMP 视图。

步骤 3 执行命令 **cwmp enable**，使能 CWMP 功能。

----结束

4.3.3 配置 CWMP 自动连接功能

建立 CPE 和 ACS 之间的连接是实现 ACS 对 CPE 管理和维护的前提。

背景信息

CPE 获取 ACS URL 方式

CPE 建立与 ACS 的连接前，需获取 ACS 的 URL，AR3200 支持的获取 ACS URL 方式有以下三种：

CPE 获取 ACS URL 方式	定义	适用场景
DHCP 配置	ACS URL 可以通过在 DHCP server 上配置 option 43 参数来实现。当 CPE 访问 DHCP server 时，DHCP server 会将 ACS URL 发送给 CPE。	适用于 ACS 和 CPE 的 IP 地址均由同一个 DHCP server 分配。

CPE 获取 ACS URL 方式	定义	适用场景
ACS 自动下发	ACS 与 CPE 建立连接后，如果 ACS 的 URL 发生变更，ACS 会自动将新的 URL 下发给 CPE。	适用于 ACS 已经与 CPE 建立连接。
CPE 本地配置	在 CPE 上通过命令行配置 ACS URL。	适用于 CPE 通过命令行配置建立与 ACS 的连接。

说明

这里仅介绍通过 CPE 本地配置的方式配置 ACS URL。

ACS 的 URL 支持 http 和 https 两种格式，如果需要配置 SSL 功能以保证 ACS 与 CPE 之间传输的机密性以及数据的完整性，选择 https 格式的 URL。

ACS 和 CPE 的自动连接

ACS 和 CPE 的自动连接有两种：

- CPE 发起连接
- ACS 发起连接

CPE 和 ACS 都可以发起连接，避免在 CPE 和 ACS 之间维护一个长期的连接，从而节省网络资源和减少开销。这里仅介绍在 CPE 上向 ACS 发起连接的配置步骤。

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。CPE 上发送 Inform 报文的方式有两种：

发送 Inform 报文方式	优点	缺点	应用场景
周期性发送 Inform 报文	周期性发送 Inform 报文可避免在 CPE 和 ACS 之间维护一个长期的连接,节省了网络资源。	如果周期性发送 Inform 报文的时间间隔设置过短，会造成 ACS 和 CPE 间频繁进行会话请求，占用大量网络资源。	维护 CPE 和 ACS 之间周期性的连接，满足 ACS 对 CPE 的日常管理和维护。
定时发送 Inform 报文	更为灵活，可设置在指定时刻与 ACS 建立连接。	仅能发送一次 Inform 报文。	适用于 CPE 需要在指定时刻与 ACS 建立连接的场景。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cwmp**，进入 CWMP 视图。

步骤 3 执行命令 **cwmp acs url** *url*，配置 CPE 连接到 ACS 的 URL。

步骤 4 配置 CPE 发送 Inform 报文的方式有两种：

- 周期性发送 Inform 报文

1. 执行命令 **cwmp cpe inform interval enable**，开启 CPE 周期发送 Inform 报文功能。

   缺省情况下，CPE 周期发送 Inform 报文功能处于关闭状态。

2. 执行命令 **cwmp cpe inform interval**，配置 CPE 周期发送 Inform 报文的时间间隔。

   缺省情况下，CPE 周期发送 Inform 报文的时间间隔为 600 秒。

- 定时发送 Inform 报文

1. 执行命令 **cwmp cpe inform time** *time*，配置 CPE 在指定时刻发送一次 Inform 报文。

   缺省情况下，CPE 周期发送 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。

说明

这两种发送 Inform 报文的方式可同时配置，也可单独配置。

----结束

4.3.4 配置 CWMP 连接参数

可以配置的 CWMP 连接参数包括：CWMP 连接接口,认证参数，重连接次数和无数据传输超时时间。

背景信息

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，通过 ACS 认证（匹配 ACS 用户名和密码）后，可以与 ACS 建立连接，ACS 会将此 IP 地址保存在地址列表中。当 ACS 发起连接时，通过此 IP 地址请求与 CPE 建立连接。

通常情况下，CPE 会自动获取一个 CWMP 连接接口，但如果需要指定 CPE 与 ACS 建立连接的接口时，可通过命令行进行配置。

认证参数

AR3200 支持的 CWMP 认证包含两种：

- ACS 对 CPE 合法性的认证：当 CPE 向 ACS 发送 Inform 报文请求连接时，根据 Inform 报文里携带的 URL 地址，请求与 ACS 建立连接，通过 ACS 的认证（即匹配 ACS 的用户名和密码）后，可以与 ACS 建立连接。
- CPE 对 ACS 合法性的认证：当 ACS 向 CPE 发送 HTTP 报文请求连接时，根据 HTTP 报文里携带的 CPE 的 IP 地址，请求与 CPE 建立连接，通过 CPE 的认证（即匹配 CPE 的用户名和密码）后，可以与 CPE 建立连接。

重连接次数

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时，而且 CPE 自动重新连接的次数还没有达到上限，此时，CPE 会自动发起连接。如果超出重连接次数的上限仍未连接成功，则认为 CPE 与 ACS 连接失败，CPE 将在下一个发送 Inform 报文周期或时间到达时，再次向 ACS 发起连接请求。

无数据传输超时时间

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。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cwmp**，进入 CWMP 视图。

步骤 3 执行命令 **cwmp cpe connect interface** *interface-type interface-number*，设置 CPE 上连接 ACS 的接口。

步骤 4 配置 ACS 对 CPE 合法性的认证。

1. 执行命令 **cwmp acs username** *username*，配置 CPE 连接到 ACS 的用户名。
2. 执行命令 **cwmp acs password** *password*，配置 CPE 连接到 ACS 的密码。

步骤 5 配置 CPE 对 ACS 合法性的认证。

1. 执行命令 **cwmp cpe username** *username*，配置 ACS 连接到 CPE 的用户名。
2. 执行命令 **cwmp cpe password** *password*，配置 ACS 连接到 CPE 的密码。

步骤 6 执行命令 **cwmp cpe connect retry** *times*，配置 CPE 向 ACS 请求连接失败时的重连接次数。

缺省情况下，重连接次数为 3 次。

步骤 7 执行命令 **cwmp cpe wait timeout** *seconds*，配置 CPE 无数据传输超时时间。

缺省情况下，无数据传输超时时间为 30 秒。

----结束

4.3.5 配置 CWMP 的 SSL 功能

CWMP 的 SSL 功能可保证 ACS 与 CPE 间通信的保密性和数据完整性。

背景信息

传输层安全协议 SSL(Security Socket Layer)是由 Netscape 公司提出的一种安全协议，SSL 采用公开密钥技术，保证两个应用间通信的保密性和可靠性，使客户与服务器应用之间的通信不被攻击者窃听。

当 ACS 的 URL 为 https 格式时，CPE 必须对 ACS 进行鉴权，鉴权通过后，可以与 ACS 建立 SSL 连接，以保证 ACS 与 CPE 间通信的保密性以及数据的完整性。

说明

数字证书包含了个人、企业或设备的信息和公钥:

- 公钥：同时拥有一把公共密钥（公钥）对外开放，用于加密和验证签名。
- 私钥：每个用户拥有一把仅为本人所掌握的私有密钥（私钥），用于解密和签名。
- 签名：签字之后表示文件生成的作者，签名后被其他人无权修改，所以也就保证了身份认证和文件的完整性。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cwmp**，进入 CWMP 视图。

步骤 3 执行命令 **cwmp acs url** *url*，配置 CPE 连接到 ACS 的 URL。

说明

ACS 的 URL 必须为 https 格式。

步骤 4 执行命令 **cwmp ssl-client** { **client-root-cert** { *rootcert-path1* } [*rootcert-path2*] | **ssl-policy** *policy-name* }，配置 CPE 鉴权 ACS。

说明

请确认设备的系统时间为正确的当前本地时间，否则有可能出现证书认证失败的情况。如需更换证书，要先卸载当前加载的证书。

当 CPE 使用 SSL 策略对 ACS 鉴权时，需要先使用 **ssl policy** *policy-name* **type client** 命令配置客户端型 SSL 策略。

----结束

4.3.6 检查配置结果

前提条件

已经完成上述所有配置。

操作步骤

- 执行命令 **display cwmp configuration**，查看 AR3200 的 CWMP 配置信息。
- 执行命令 **display cwmp status**，查看 AR3200 的 CWMP 状态信息。

----结束

任务示例

在配置成功之后，执行 **display cwmp configuration** 命令查看 AR3200 的 CWMP 功能是否处于 enabled 状态，连接到 ACS 的 URL、用户名和密码，周期发送 Inform 报文功能处于 enabled 状态，发送 Inform 报文的周期，定时发送 Inform 报文的日期和时间，无数据传输超时时间和重连接次数。

```
<Huawei> display cwmp configuration
  CWMP is enabled
  ACS URL:                          http://www.acs.com:80/acs
  ACS username:                     newacsname
  ACS password:                     newacspsw
  Inform enable status:             enabled
  Inform interval:                  1000s
  Inform time:                      2011-01-01T20:00:00
  Wait timeout:                     100s
  Reconnection times:               5
```

在配置成功之后，执行 **display cwmp status** 命令查看 AR3200 的 CWMP 功能处于 enabled 状态，AR3200 连接到 ACS 的 URL、用户名和密码，AR3200 连接到 ACS 的 URL 的获取方式，AR3200 与 ACS 的连接状态和最后一次成功连接的时间。

```
<Huawei> display cwmp status
 CWMP is enabled
```

```
ACS URL:                              http://www.acs.com:80/acs
ACS information is set by:            user
ACS username:                         newacsname
ACS password:                         newacspsw
Connection status:                    connected
Time of last successful connection:   2010-12-01T20:00:00
```

4.4 配置举例

介绍 CWMP 举例。

4.4.1 配置 CWMP 功能示例

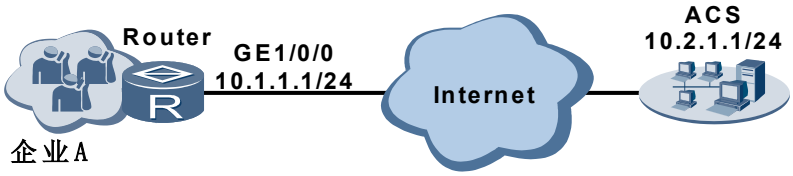
通过配置 CWMP 功能，可实现 ACS 对 CPE 的管理和维护。

组网需求

如图 4-2 所示，企业 A 中多个主机统一接入企业网关 Router，通过 Router 连接互联网。

企业 A 希望运营商提供一种服务，实现对 Router 的软、硬件升级，厂商配置文件的自动下载以及 Router 出现故障或者升级时的远程重启。这时，可通过在 Router 上配置 CWMP 功能，实现对 Router 的管理和维护。

图 4-2 ACS 通过 CWMP 管理 Router



配置思路

采用如下的思路配置 CWMP 功能：

1. 使能 Router 的 CWMP 功能。
2. 配置 Router 的 CWMP 自动连接功能，配置 CPE 向 ACS 发起连接。
3. 配置 Router 的 CWMP 连接参数。

数据准备

为完成此配置例，需准备如下的数据：

- ACS 的 URL 地址。
- Router 的 IP 地址。

操作步骤

步骤 1 按图 4-2 配置 Router 的 IP 地址，配置 Router 和 ACS 路由可达。具体过程略。

步骤 2 使能 Router 的 CWMP 功能

```
<Huawei> system-view
[Huawei] sysname Router
[Router] cwmp
[Router-cwmp] cwmp enable
```

步骤 3 配置 Router 的 CWMP 自动连接功能

配置 Router 连接到 ACS 的 URL。

```
[Router-cwmp] cwmp acs url http://www.acs.com:80/acs
```

使能 Router 发送 Inform 报文功能。

```
[Router-cwmp] cwmp cpe inform interval enable
```

配置 Router 发送 Inform 报文的时间间隔为 1000 秒。

```
[Router-cwmp] cwmp cpe inform interval 1000
```

配置 Router 定时发送 Inform 报文的日期和时间为 2011－01－01T20:00:00。

```
[Router-cwmp] cwmp cpe inform time 2011-01-01T20:00:00
```

步骤 4 配置 Router 的 CWMP 连接参数

配置 Router 上连接 ACS 的接口。

```
[Router-cwmp] cwmp cpe connect interface gigabitethernet 1/0/0
```

配置 ACS 对 Router 的认证。

```
[Router-cwmp] cwmp acs username newacsname
[Router-cwmp] cwmp acs password newacspsw
```

配置 Router 对 ACS 的认证。

```
[Router-cwmp] cwmp cpe username newcpename
[Router-cwmp] cwmp cpe password newcpepsw
```

配置 Router 向 ACS 请求连接失败时的重连接次数为 5 次。

```
[Router-cwmp] cwmp cpe connect retry 5
```

配置 Router 无数据传输超时时间为 100 秒。

```
[Router-cwmp] cwmp cpe wait timeout 100
```

步骤 5 验证配置结果

查看 AR3200 的 CWMP 功能是否处于 enabled 状态，连接到 ACS 的 URL、用户名和密码，周期发送 Inform 报文功能处于 enabled 状态，发送 Inform 报文的周期，定时发送 Inform 报文的日期和时间，无数据传输超时时间和重连接次数。

```
<Router> display cwmp configuration
  CWMP is enabled
  ACS URL:                          http://www.acs.com:80/acs
  ACS username:                     newacsname
  ACS password:                     newacspsw
  Inform enable status:             enabled
  Inform interval:                  1000s
  Inform time:                      2011-01-01T20:00:00
  Wait timeout:                     100s
  Reconnection times:               5
```

查看 AR3200 的 CWMP 功能处于 enabled 状态，AR3200 连接到 ACS 的 URL、用户名和密码，AR3200 连接到 ACS 的 URL 的获取方式，AR3200 与 ACS 的连接状态和最后一次成功连接的时间。

```
<Router> display cwmp status
 CWMP is enabled
 ACS URL:                              http://www.acs.com:80/acs
 ACS information is set by:            user
 ACS username:                         newacsname
 ACS password:                         newacspsw
 Connection status:                    connected
 Time of last successful connection:   2010-12-01T20:00:00
```

----结束

配置文件

Router 的配置文件

```
#
 sysname Router
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
cwmp
 cwmp cpe inform interval enable
 cwmp acs url http://www.acs.com:80/acs
 cwmp acs username newacsname
 cwmp acs password newacspsw
 cwmp cpe username newcpename
 cwmp cpe password newcpepsw
 cwmp cpe inform interval 1000
 cwmp cpe connect retry 5
 cwmp cpe wait timeout 100
 cwmp cpe connect interface GigabitEthernet 1/0/0
#
return
```

5 NTP 配置

关于本章

通过配置 NTP，可以保持网络中各设备的时钟运行一致。

5.1 NTP 简介
本节对 NTP 做了简单的介绍。

5.2 配置 NTP 基本功能
在 NTP 基本配置里，用户可以了解到如何配置 NTP 的基本功能，包括 NTP 的工作模式。

5.3 配置 NTP 安全机制
本节介绍如何配置 NTP 安全模式，从而在对安全要求比较高的网络中，实现可靠的时钟同步。

5.4 NTP 配置举例
本节举例说明如何配置介绍 NTP。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

5.1 NTP 简介

本节对 NTP 做了简单的介绍。

5.1.1 NTP 概述

本节描述了 NTP 的基本原理和运行模式。

NTP（Network Time Protocol）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基本保持一致，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，既可以接收来自其他时钟源的同步，也可以作为时钟源去同步别的时钟，并且可以通过交换 NTP 报文互相同步。

NTP 报文封装在 UDP 报文中传输，使用端口号 123。

NTP 的应用

NTP 主要应用于需要网络中所有主机或路由器时钟保持一致的场景，比如：

- 网络管理：对从不同路由器采集来的日志信息、调试信息进行分析时，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：例如，重启网络中的所有路由器时，要求所有路由器的时钟保持一致。
- 多个系统协同处理同一个复杂事件：为保证正确的执行顺序，多个系统必须参考同一时钟。
- 备份服务器和客户机之间进行增量备份：要求备份服务器和所有客户机之间的时钟同步。
- 用户登录时间：某些应用程序需要知道用户登录系统的时间以及文件修改的时间。

对于网络中的众多设备，如果依靠管理员手工输入命令来修改系统时钟，不仅工作量巨大，也不能保证时钟的精确性。通过配置 NTP，可以很快将网络中设备的时钟同步，同时保证很高的精度。

NTP 的优势：

- 采用分层（Stratum）的方法来定义时钟的准确性，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。
- 支持采用单播、多播或广播方式发送协议报文。

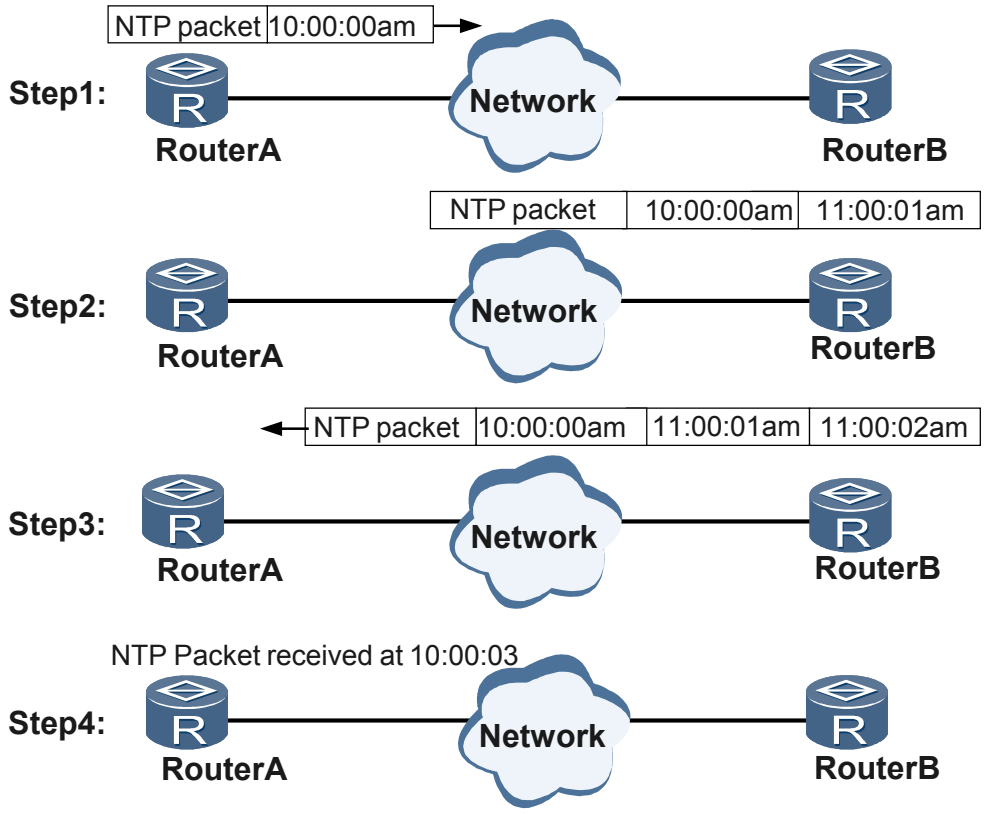
NTP 工作原理

NTP 基本工作原理如图 5-1 所示。Router A 和 Router B 通过广域网相连，它们都有自己独立的系统时钟，通过 NTP 实现系统时钟自动同步。

作如下假设：

- 在 Router A 和 Router B 的系统时钟同步之前，Router A 的时钟设定为 10:00:00am，Router B 的时钟设定为 11:00:00am。
- Router B 充当 NTP 时间服务器。Router A 的时钟与 Router B 的时钟同步。
- 数据包在 Router A 和 Router B 之间单向传输需要 1 秒。
- Router A 和 Router B 处理 NTP 数据包的时间都是 1 秒。

图 5-1 NTP 基本原理图



系统时钟同步的工作过程如下：

1. Router A 发送一个 NTP 消息包给 Router B，该消息包带有它离开 Router A 时的时间戳 10:00:00am（T1）。
2. 此 NTP 消息包到达 Router B 时，Router B 加上到达时间戳 11:00:01am（T2）。
3. 此 NTP 消息包离开 Router B 时，Router B 再加上离开时间戳 11:00:02am（T3）。
4. Router A 接收到该响应消息包时，加上新的时间戳 10:00:03am（T4）。

   至此，Router A 拥有足够信息来计算以下两个重要参数：

   - NTP 消息来回一个周期的时延：Delay=（T4-T1）-（T3-T2）。
   - Router A 相对 Router B 的时间差：Offset=（（T2-T1）+（T3-T4））/2。

   Router A 根据时间差和时延来设定自己的时钟，实现与 Router B 的时钟同步。

   以上是 NTP 工作原理的简略描述，在 RFC1305 中，NTP 使用复杂的算法来确保时钟同步的精确性。

服务器和客户端的概念是相对而言的，提供时间标准的设备称为时间服务器，接收时间服务的设备称为客户端。

5.1.2 AR3200 支持的 NTP 特性

本节介绍 AR3200 支持的 NTP 运行模式。

AR3200 支持如下几种 NTP 工作模式：

- 单播客户端/服务器模式
- 对等体模式
- 广播模式
- 组播模式

单播客户端/服务器模式

这种模式只需要在客户端配置，服务器端除了配置 NTP 主时钟外，不需要进行其他专门配置。

注意只能是客户端同步到服务器，服务器不会同步到客户端。

配置完成后：

1. 客户端向服务器发送同步请求报文，报文中的 Mode 字段设置为 3（客户模式）。
2. 服务器端收到请求报文后，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）。
3. 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端。

对等体模式

在对等体模式中，NTP 只需要在主动对等体（Symmetric active）端进行配置。

对等体模式下，主动对等体和被动对等体可以互相同步，等级低（层数大）的对等体向等级高（层数小）的对等体同步。

配置完成后：

- 主动对等体向被动对等体发送同步请求报文，报文中的 Mode 字段设置为 1（主动对等体）。
- 被动对等体收到请求报文后，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）。

广播模式

在广播模式下，服务器端和客户端都需要配置相关命令。

配置完成后：

- 服务器端周期性向广播地址 255.255.255.255 发送时钟同步报文。
- 客户端侦听来自服务器的广播消息包。
- 客户端接收到第一个广播消息包后，为估计网络延迟，客户端先启用一个短暂的客户端/服务器模式与远程服务器交换消息。

- 客户端进入广播客户模式，继续侦听广播消息包的到来，根据到来的广播消息包对本地时钟进行同步。

组播模式

在组播模式下，服务器端和客户端都需要配置相关命令。

配置完成后：

- 服务器端周期性向配置的组播目的地址发送时钟同步报文。缺省的组播目的地址是224.0.1.1。
- 客户端侦听来自服务器的组播消息包。
- 当客户端接收到第一个组播消息包后，为估计网络延迟，客户端先启用一个短暂的客户端/服务器模式与远程服务器交换消息。
- 客户端进入组播客户端模式，继续侦听组播消息包的到来，根据到来的组播消息包对本地时钟进行同步。

5.2 配置 NTP 基本功能

在 NTP 基本配置里，用户可以了解到如何配置 NTP 的基本功能，包括 NTP 的工作模式。

5.2.1 建立配置任务

在配置 NTP 基本功能前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

NTP 有 5 种工作模式：

- 客户端/服务器模式
- 对等体模式
- 广播模式
- 组播模式
- 多播模式

在实际使用中，应根据网络部署情况选择适当的工作模式，以满足不同情况下的网络时钟同步需求。

对于单播客户端/服务器模式和对等体模式，还可以指定本地发送的所有 NTP 消息都使用同一接口的 IP 地址作为源 IP。

前置任务

在配置 NTP 基本功能之前，需完成以下任务：

- 配置接口的链路层协议
- 配置接口的网络层地址和路由协议，保证 NTP 报文可达

数据准备

在配置 NTP 基本功能之前，需要准备以下数据：

序号	数据
1	NTP 主时钟、主时钟的层数
2	收发 NTP 报文的接口
3	NTP 的版本
4	根据选用的工作模式，准备以下数据： ● 客户端/服务器模式：服务器的 IP 地址、服务器所属的 VPN 实例 ● 对等体模式：被动对等体的 IP 地址、被动对等体所属的 VPN 实例 ● 广播模式：发送和接收 NTP 广播包的接口、客户端允许建立的最大动态会话数目 ● 组播模式：NTP 组播消息包使用的组播组地址、组播消息包的生存周期 TTL、发送和接收 NTP 组播包的接口、客户端允许建立的最大动态会话数目
5	禁止接收 NTP 报文的接口

5.2.2 配置 NTP 主时钟

服务器端主时钟的层数一定要小于客户端时钟的层数，否则客户端无法跟服务器端的时钟进行同步。

背景信息

如果使用路由器提供 NTP 主时钟，请在作为 NTP 服务器的路由器上进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ntp-service refclock-master** [*ip-address*] [*stratum*]配置 NTP 主时钟。

ip-address 是本地参考时钟的 IP 地址 127.127.t.u。t 的取值范围是 0 ～ 37。目前只能取 1，表示本地参考时钟；u 表示 NTP 进程号，取值范围是 0 ～ 3。

当不指定 IP 地址时，默认使用本地时钟 127.127.1.0 为 NTP 主时钟，层数为 8。

----结束

5.2.3 配置单播客户端/服务器模式

服务器/客户端服务方式下，客户端选择与服务器的主时钟进行同步。

背景信息

通常需要在客户端指定 NTP 服务器的 IP 地址。之后，客户端与服务器端才能使用该地址交换 NTP 报文。

如果在服务器端指定了发送 NTP 报文的源地址，该地址必须与在客户端配置的服务端 IP 地址相同。否则，客户端无法处理服务器端发送的 NTP 报文，进而时钟同步失败。

操作步骤

- 配置 NTP 客户端。

  请在作为客户端的路由器上,执行以下配置：

  1. 执行命令 **system-view**，进入系统视图。
  2. （可选）执行命令：

     ntp-service source-interface *interface-type interface-number* [**vpn-instance** *vpn-instance-name*]

     配置用来接收 NTP 报文的本地源接口。
  3. 执行命令:

     ntp-service unicast-server *ip-address* [**version** *number* | **authentication-keyid** *key-id* | **source-interface** *interface-type interface-number* | **vpn-instance** *vpn-instance-name* | **preference**] *

     配置 NTP 服务器的 IP 地址。

     步骤 2 为可选步骤。如果步骤 2 和步骤 3 都指定了源接口（**source-interface**），优先选择步骤 3 指定的源接口。

     参数 *ip-address* 指定了 NTP 服务器的地址。该地址只能是一个 IPv4 或者 IPv6 的主机 IP 地址，而不能是一个广播地址、组播地址、或者是参考时钟的 IP 地址。

     说明

     指定单播 NTP 服务器后，本地路由器自动充当客户端的角色。服务器上只能配置一个主时钟。

- （可选）配置 NTP 服务器上发送 NTP 报文的源接口

  请在作为服务器的路由器上,执行以下配置：

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令:

     ntp-service source-interface *interface-type interface-number* [**vpn-instance** *vpn-instance-name*]

     配置用来发送 NTP 报文的本地源接口。

----结束

5.2.4 配置对等体模式

介绍了如何配置 NTP 对等体模式。两个对等体上的时钟可以分层互相同步，一方既可以主动发送请求消息到对方请求时钟同步，又可以响应对方主动发送来的请求消息去同步对方。

操作步骤

- 配置 NTP 主动对等体
  1. 执行命令 **system-view**，进入系统视图。
  2. （可选）执行命令：

ntp-service source-interface *interface-type interface-number* [**vpn-instance** *vpn-instance-name*]

配置用来发送 NTP 报文的本地源接口。

3. 执行命令:

ntp-service unicast-peer *ip-address* [**version** *number* | **authentication-keyid** *key-id* | **source-interface** *interface-type interface-number* | **vpn-instance** *vpn-instance-name* | **preference**] *

配置 NTP 对等体。

步骤 2 为可选步骤。如果步骤 2 和步骤 3 都指定了源接口(**source-interface**)，优先使用步骤 3 中指定的源接口。

参数 *ip-address* 指定了 NTP 对等体的地址。该地址只能是一个 IPv4 或 IPv6 的主机地址，而不能是一个广播地址、组播地址、或者是参考时钟的 IP 地址。

说明

指定 NTP 对等体后，本地路由器进入对称主动模式。对称被动端不需要配置。

- （可选）配置 NTP 被动对等体的源接口
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令:

ntp-service source-interface *interface-type interface-number* [**vpn-instance** *vpn-instance-name*]

配置用来发送 NTP 报文的本地源接口。

通常需要在客户端指定 NTP 服务器的 IP 地址。之后，客户端与服务器端才能使用该地址交换 NTP 报文。

如果在主动对等体端指定了发送 NTP 报文的源接口，该接口必须与在被动对等体端配置的源接口相同。否则，主动对等体无法处理被动对等体发送的 NTP 报文，进而时钟同步失败。

----结束

5.2.5 配置广播模式

介绍了如何在局域网中配置 NTP 广播模式，实现局域网中的时钟同步。

操作步骤

- 配置一个 NTP 广播服务器

  请在作为 NTP 广播服务器的路由器上,执行以下配置：

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，指定发送 NTP 广播包的接口。
  3. 执行命令 **quit**，返回系统视图。
  4. 执行命令:

ntp-service broadcast-server [**authentication-keyid** *key-id* | **version** *number*]*

配置本地路由器作为 NTP 广播服务器。

配置完成后，本地路由器周期性地向广播地址 255.255.255.255 发送时钟同步报文。

说明

广播模式只能在同一局域网中使用。

- 配置一个 NTP 广播客户端

  请在作为 NTP 广播客户端的路由器上,执行以下配置：

  1. 执行命令 **system-view**，进入系统视图。
  2. （可选）执行命令 **ntp-service max-dynamic-sessions** *number*，配置本地允许建立的动态会话数目。
  3. 执行命令 **interface** *interface-type interface-number*，指定接收 NTP 广播包的接口。
  4. 执行命令 **ntp-service broadcast-client**，将本地路由器配置为 NTP 广播客户端。

     步骤 2 是可选步骤。缺省情况下，最多允许建立 100 个 NTP 动态会话。

     配置完成后，本地路由器接收来自 NTP 服务器的广播 NTP 报文，并同步本地时钟。

     执行 **ntp-service max-dynamic-sessions** 命令不会对现存的 NTP 会话造成影响。当本地的动态 NTP 会话数量超过最大值时，不能建立新会话。

----结束

5.2.6 配置组播模式

介绍如何配置 NTP 组播模式对域内的设备进行时钟同步。

操作步骤

- 配置一个 NTP 组播服务器

  请在作为 NTP 服务器的路由器上,执行以下配置：

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，指定发送 NTP 组播包的接口。
  3. 执行命令 **quit**，返回系统视图。
  4. 执行命令:

     ntp-service multicast-server [*ip-address*] [**authentication-keyid** *key-id* | **ttl** *ttl-number* | **version** *number*] *

     配置本地路由器作为一个 NTP 组播服务器。

     配置完成后，本地路由器周期性地向组播地址 224.0.1.1 发送时钟同步报文。

- 配置一个 NTP 组播客户端

  请在作为客户端的路由器上,执行以下配置：

  1. 执行命令 **system-view**，进入系统视图。
  2. （可选）执行命令 **ntp-service max-dynamic-sessions** *number*，配置本地允许建立的动态会话数目。
  3. 执行命令 **interface** *interface-type interface-number*，指定接收 NTP 组播包的接口。
  4. 执行命令:

```
ntp-service multicast-client [ ip-address ]
```

配置本地路由器作为一个 NTP 组播客户端。

步骤 2 是可选步骤。缺省情况下，最多允许建立 100 个 NTP 动态会话。

配置完成后，本地路由器侦听来自 NTP 服务器的组播 NTP 报文，并同步本地时钟。

执行 **ntp-service max-dynamic-sessions** 命令不会对现存的 NTP 会话造成影响。当本地的动态 NTP 会话数量超过最大值时，不能建立新会话。

----结束

5.2.7 禁止指定接口接收 NTP 报文

当局域网中的某台主机不需要同步指定服务器的时钟时，可以禁止该主机的指定接口接收 NTP 报文。

背景信息

在需要禁止某个接口接收 NTP 报文的路由器上，请进行如下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令:

```
ntp-service in-interface disable
```

禁止路由器上的接口接收 NTP 报文。

----结束

5.2.8 检查配置结果

在配置 NTP 基本功能成功后，可以查看到 NTP 的基本功能的配置情况。

前提条件

已经完成配置 NTP 基本功能的所有配置。

操作步骤

- 执行命令 **display ntp-service status** 查看 NTP 服务的状态。
- 执行命令 **display ntp-service sessions** [**verbose**] 查看 NTP 会话的状态。
- 执行命令 **display ntp-service trace** 查看从本地设备回溯到参考时钟源的各 NTP 服务器的简要信息。

----结束

任务示例

执行命令 **display ntp-service status** 查看 NTP 服务的状态。

```
<Huawei> display ntp-service status
 clock status: synchronized
 clock stratum: 2
 reference clock ID: LOCAL(0)
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 0.0000 ms
 root delay: 0.00 ms
 root dispersion: 0.00 ms
 peer dispersion: 10.00 ms
 reference time: 15:51:36.259 UTC Apr 25 2010(C6179088.426490A3)
```

执行命令 **display ntp-service sessions** [**verbose**]查看 NTP 会话的状态。

```
<Huawei> display ntp-service sessions
              source          reference       stra reach poll  now offset delay disper
********************************************************************************
       [12345]127.127.1.0     LOCAL(0)          7    1   64    2      -    0.0   15.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured,
      6 vpn-instance
```

执行命令 **display ntp-service trace** 查看从本地设备回溯到参考时钟源的各 NTP 服务器的简要信息。

```
<Huawei> display ntp-service trace
server 127.0.0.1,stratum 5, offset 0.024099, synch distance 0.06337
server 171.1.1.2,stratum 4, offset 0.028786, synch distance 0.04575
server 201.1.1.2,stratum 3, offset 0.035199, synch distance 0.03075
server 200.1.7.1,stratum 2, offset 0.039855, synch distance 0.01096
refid 127.127.1.0
```

5.3 配置 NTP 安全机制

本节介绍如何配置 NTP 安全模式，从而在对安全要求比较高的网络中，实现可靠的时钟同步。

5.3.1 建立配置任务

在配置 NTP 安全机制前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

NTP 提供访问权限和 NTP 验证两种安全机制。

- 访问权限

  通过设置访问权限保护本地 NTP 服务是 AR3200 提供的一种比较简单的安全措施。

  AR3200 提供 4 个等级的访问限制。当一个 NTP 访问请求报文到达本地时，按照最小访问限制到最大访问限制对报文进行依次匹配，以第 1 个匹配的为准，匹配顺序如下：

  - **peer**: 表示最小访问限制。远端设备可以给本地设备发送时间请求和控制查询，本地时钟也可以同步到远端服务器。
  - **server**: 远端设备可以对本地设备进行时间请求和控制查询，但本地时钟不会同步到远端服务器。
  - **synchronization**: 只允许远端设备对本地设备提出时间请求。
  - **query**: 表示最大访问限制。只允许远端设备对本地设备进行控制查询。

- NTP 验证

  在安全性要求较高的网络中，可以启用 NTP 验证功能。

  配置 NTP 验证功能分为两部分：配置客户端、配置服务器端。

  在配置 NTP 验证功能时，应注意以下原则：

  - 客户端和服务器端均需要配置 NTP 验证功能。否则，NTP 验证功能不生效。
  - 如果使能了 NTP 验证功能，应同时配置一个可信的密钥。
  - 在服务器端和客户端上配置的密钥必须相同。
  - 在 NTP 对等体模式下，主动对等体相当于客户端，被动对等体相当于服务器端。

前置任务

在配置 NTP 安全机制之前，需完成以下任务：

- 配置接口的链路层协议
- 配置接口的网络层地址和路由协议，保证客户端和路由器端路由可达
- 如果配置访问权限，需要配置用于进行访问控制的 ACL

数据准备

在配置 NTP 安全机制之前，需要准备以下数据：

序号	数据
1	ACL 规则
2	NTP 验证使用的密钥 ID 和密钥
3	NTP 主时钟、主时钟的层数
4	收发 NTP 报文的接口
5	NTP 的版本

5.3.2 配置 NTP 访问控制权限

在接收到一个访问请求报文后，NTP 服务器按照降序（peer, server, synchronization to query）对报文的访问限制进行匹配，以第一个匹配的访问权限为准。

背景信息

请在路由器上进行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令:

```
ntp-service access { peer | query | server | synchronization } acl-number
```

在本地路由器上配置 NTP 服务的访问控制权限。

用户需要根据实际需求决定在哪台设备上配置 **ntp-service access** 命令。

具体描述见表 5-1。

表 5-1 NTP 访问控制权限配置

NTP 工作模式	限制的 NTP 请求类型	进行配置的设备
单播 NTP 客户端/服务器模式	限制客户端同步到服务器端	客户端
单播 NTP 客户端/服务器模式	限制服务器端处理客户端发送的时钟同步请求	服务器端
NTP 对等体模式	限制客户端和服务器端进行时钟同步	主动对等体端
NTP 对等体模式	限制被动对等体端处理主动对等体发送的时钟请求	被动对等体端
NTP 组播模式	限制客户端同步到服务器端	NTP 组播客户端
NTP 广播模式	限制客户端同步到服务器端	NTP 广播客户端

----结束

5.3.3 使能 NTP 验证

该部分描述了如何配置 NTP MD5 认证和自动密钥认证。

背景信息

为了确保网络中时间服务器的可靠性，客户端必须同已通过认证的 NTP 服务器进行同步，防止恶意攻击造成的时钟报文数据的更改。

操作步骤

- 配置 NTP MD5 认证

  说明

  - 客户端与服务器端必须配置相同的验证密钥，并声明该密钥可信，否则无法通过验证。
  - 必须先使能 NTP 验证功能，否则不会进行验证。

  1. 执行 **system-view** 命令，进入系统视图。
  2. 执行 **ntp-service authentication enable** 命令，使能 NTP 验证功能。
  3. 执行 **ntp-service authentication-keyid** *key-id* **authentication-mode md5** *password* 命令，配置 NTP 验证密钥。
  4. 执行 **ntp-service reliable authentication-keyid** *key-id* 命令，声明密钥可信。

----结束

5.3.4 在单播客户端/服务器模式下配置 NTP 验证

通过在 NTP 客户端配置与指定 NTP 服务器同步时使用的密钥 ID，可以在 NTP 服务器/客户端模式下应用 NTP 验证。

背景信息

请在作为 NTP 单播客户端的路由器上，执行以下配置：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令:

ntp-service unicast-server *ip-address* [**authentication-keyid** *key-id* | **version** *number* | **source-interface** *interface-type interface-number* | **vpn-instance** *vpn-instance-name* | **preference**]*

配置用来进行服务器和客户端时钟同步的验证密钥 ID。

----结束

5.3.5 在对等体模式下配置 NTP 验证

通过在本端配置与对等体端同步时使用的密钥 ID，可以在对等体模式下应用 NTP 验证。

背景信息

请在作为主动对等体端的路由器上，执行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令:

ntp-service unicast-peer *ip-address* [**version** *number* | **authentication-keyid** *key-id* | **source-interface** *interface-type interface-number* | **preference**] *

配置用来进行 NTP 对等体时钟同步的验证密钥 ID。

----结束

5.3.6 在广播模式下配置 NTP 验证

通过在本地路由器配置用来与 NTP 组播服务器进行同步时使用的密钥 ID，可以在广播模式下应用 NTP 验证。

背景信息

请在作为 NTP 广播服务器的路由器上，执行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，指定发送 NTP 广播包的接口。

步骤 3 执行命令 **quit**，返回系统视图。

步骤 4 执行命令 **ntp-service broadcast-server** [**authentication-keyid** *key-id* | **version** *number*] *配置本地路由器作为 NTP 广播服务器时使用的密钥 ID。

对于广播客户端的配置，参见“配置广播模式”。

----结束

5.3.7 在组播模式下配置 NTP 验证

通过在本地路由器配置用来与 NTP 组播服务器进行同步时使用的密钥 ID，可以在组播模式下应用 NTP 验证。

背景信息

请在作为 NTP 组播服务器的路由器上，执行以下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，指定发送 NTP 组播包的接口。

步骤 3 执行命令:

ntp-service multicast-server [**authentication-keyid** *key-id* | **version** *number*]*

配置 NTP 组播服务器使用的验证密钥 ID。

对于组播客户端的配置，参见“配置组播模式”。

----结束

5.3.8 检查配置结果

在成功配置 NTP 安全机制后，可以查看到 NTP 安全机制的配置情况。

前提条件

已经完成 NTP 安全机制的所有配置。

操作步骤

- 执行命令 **display ntp-service status** 查看 NTP 服务的状态。
- 执行命令 **display ntp-service sessions** [**verbose**] 查看 NTP 会话的状态。

----结束

任务示例

执行命令 **display ntp-service status** 查看 NTP 服务的状态。

```
<Huawei> display ntp-service status
 clock status: synchronized
 clock stratum: 2
 reference clock ID: LOCAL(0)
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 0.0000 ms
 root delay: 0.00 ms
 root dispersion: 0.00 ms
 peer dispersion: 10.00 ms
 reference time: 15:51:36.259 UTC Apr 25 2010(C6179088.426490A3)
```

执行命令 **display ntp-service sessions** [**verbose**] 查看 NTP 会话的状态。

```
<Huawei> display ntp-service sessions
                source          reference       stra reach poll  now offset delay disper
******************************************************************************
        [12345]127.127.1.0      LOCAL(0)          7    1   64    2      -    0.0   15.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured,
      6 vpn-instance
```

5.4 NTP 配置举例

本节举例说明如何配置介绍 NTP。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

5.4.1 配置带验证的单播 NTP 服务器/客户端模式示例

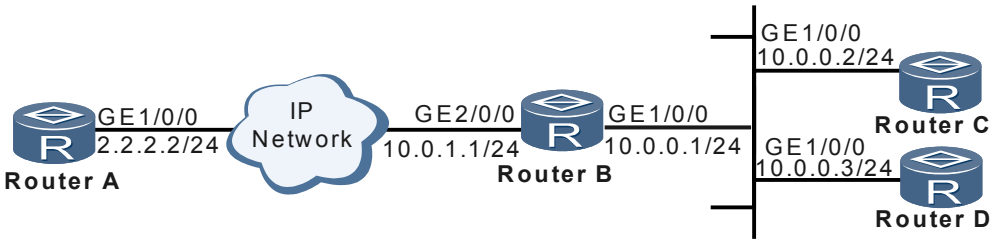
本部分举例说明如何在单播服务器/客户端模式下配置 NTP 验证。客户端必须先使能 NTP 验证，然后再指定 NTP 服务器地址，并同时指定发给服务器的验证密钥。否则将不进行验证，直接同步。客户端和服务器端都需要进行完整的配置，才能验证通过。

组网需求

如图 5-2 所示:

- RouterA 作为 NTP 单播服务器，其本地时钟作为 NTP 主时钟，层数为 2。
- RouterB 作为 NTP 单播客户端，同步远端服务器 RouterA 的时钟。
- RouterC 和 RouterD 作为 NTP 客户端，把 RouterB 作为自己的 NTP 服务器。
- 使能 NTP 验证。

图 5-2 单播 NTP 客户端/服务器模式组网图



配置思路

配置思路如下：

1. 配置 RouterA 作为服务器，提供主时钟。
2. 配置 RouterB 作为 NTP 客户端，同步 RouterA 的时钟。
3. 配置 RouterC、RouterD 作为 NTP 客户端，同步 RouterB 的时钟。
4. 在所有的 Router 上使能 NTP 验证。

说明

- 在单播服务器/客户端模式下配置 NTP 验证时，必须首先在客户端使能 NTP 验证，然后再指定 NTP 服务器地址，并同时指定发给服务器的验证密钥。否则将不进行验证，直接同步。
- 客户端和服务器端都需要进行完整的配置，才能验证通过。

数据准备

为完成此配置例，需准备如下的数据：

- 参考时钟的 IP 地址
- NTP 主时钟的等级
- 验证密钥及其编号
- 密码

操作步骤

步骤 1 根据图 5-2，配置 IP 地址，配置 RouterA,RouterB,RouterC 和 RouterD 路由可达。具体配置过程略。

步骤 2 在 RouterA 上配置 NTP 主时钟并启动 NTP 验证功能。

在 RouterA 上指定使用自己的本地时钟作为参考时钟，层数为 2。

```
<RouterA> system-view
[RouterA] ntp-service refclock-master 2
```

使能 NTP 验证功能、配置验证密钥并声明该密钥可信。

```
[RouterA] ntp-service authentication enable
[RouterA] ntp-service authentication-keyid 42 authentication-mode md5 Hello
[RouterA] ntp-service reliable authentication-keyid 42
```

注意服务器端与客户端必须配置相同的验证密钥。

步骤 3 在 RouterB 上配置 NTP 主时钟并启动 NTP 验证功能。

在 RouterB 上使能 NTP 验证功能、配置验证密钥并声明该密钥可信。

```
<RouterB> system-view
[RouterB] ntp-service authentication enable
[RouterB] ntp-service authentication-keyid 42 authentication-mode md5 Hello
[RouterB] ntp-service reliable authentication-keyid 42
```

指定 RouterA 作为 RouterB 的 NTP 服务器，并使用已配置的验证密钥。

```
[RouterB] ntp-service unicast-server 2.2.2.2 authentication-keyid 42
```

步骤 4 在 Router C 上指定 RouterB 作为 RouterC 的 NTP 服务器。

```
<RouterC> system-view
[RouterC] ntp-service authentication enable
[RouterC] ntp-service authentication-keyid 42 authentication-mode md5 Hello
[RouterC] ntp-service reliable authentication-keyid 42
[RouterC] ntp-service unicast-server 10.0.0.1 authentication-keyid 42
```

步骤 5 在 RouterD 上指定 RouterB 作为 RouterD 的 NTP 服务器。

```
<RouterD> system-view
[RouterD] ntp-service authentication enable
[RouterD] ntp-service authentication-keyid 42 authentication-mode md5 Hello
[RouterD] ntp-service reliable authentication-keyid 42
[RouterD] ntp-service unicast-server 10.0.0.1 authentication-keyid 42
```

步骤 6 验证配置结果。

完成上述配置后，RouterB 可以同步 RouterA 的时钟。

查看 RouterB 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的层数为 3，比服务器 RouterA 低 1 级。

```
[RouterB] display ntp-service status
 clock status: synchronized
 clock stratum: 3
 reference clock ID: 2.2.2.2
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 3.8128 ms
 root delay: 31.26 ms
 root dispersion: 74.20 ms
 peer dispersion: 34.30 ms
 reference time: 11:55:56.833 UTC Mar 2 2006(C7B15BCC.D5604189)
```

完成上述配置后，RouterC 可以同步 RouterB 的时钟。

查看 RouterC 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的层数为 4，比服务器 RouterB 低 1 级。

```
[RouterC] display ntp-service status
 clock status: synchronized
 clock stratum: 4
 reference clock ID: 10.0.0.1
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 3.8128 ms
 root delay: 31.26 ms
 root dispersion: 74.20 ms
 peer dispersion: 34.30 ms
 reference time: 11:55:56.833 UTC Mar 2 2006(C7B15BCC.D5604189)
```

查看 RouterD 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的层数为 4，比服务器 RouterB 低 1 级。

```
[RouterD] display ntp-service status
 clock status: synchronized
 clock stratum: 4
 reference clock ID: 10.0.0.1
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 3.8128 ms
 root delay: 31.26 ms
 root dispersion: 74.20 ms
 peer dispersion: 34.30 ms
 reference time: 11:55:56.833 UTC Mar 2 2006(C7B15BCC.D5604189)
```

查看 Router A 的 NTP 状态。

```
[RouterA] display ntp-service status
 clock status: synchronized
 clock stratum: 2
 reference clock ID: LOCAL(0)
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 0.0000 ms
 root delay: 0.00 ms
 root dispersion: 26.50 ms
 peer dispersion: 10.00 ms
```

```
reference time: 12:01:48.377 UTC Mar 2 2006(C7B15D2C.60A15981)
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 2.2.2.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 2.2.2.0 0.0.0.255
#
ntp-service authentication enable
ntp-service authentication-keyid 42 authentication-mode md5 %@ENC;8HX\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 42
ntp-service refclock-master 2
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 10.0.0.1 255.255.255.0
interface GigabitEthernet2/0/0
 ip address 10.0.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.0.1.0 0.0.0.255
  network 10.0.0.0 0.0.0.255
#
ntp-service authentication enable
ntp-service authentication-keyid 42 authentication-mode md5 %@ENC;8HX\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 42
ntp-service unicast-server 2.2.2.2 authentication-keyid 42
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 ip address 10.0.0.2 255.255.255.0
#
ntp-service authentication enable
ntp-service authentication-keyid 42 authentication-mode md5 %@ENC;8HX\#Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 42
ntp-service unicast-server 10.0.0.1 authentication-keyid 42
#
return
```

- RouterD 的配置文件

```
#
 sysname RouterD
#
interface GigabitEthernet1/0/0
 ip address 10.0.0.3 255.255.255.0
#
ntp-service authentication enable
ntp-service authentication-keyid 42 authentication-mode md5 %@ENC;8HX\#Q=^Q`MAF4<1!!
```

```
ntp-service reliable authentication-keyid 42
ntp-service unicast-server 10.0.0.1 authentication-keyid 42
#
return
```

5.4.2 配置 NTP 对等体模式的示例

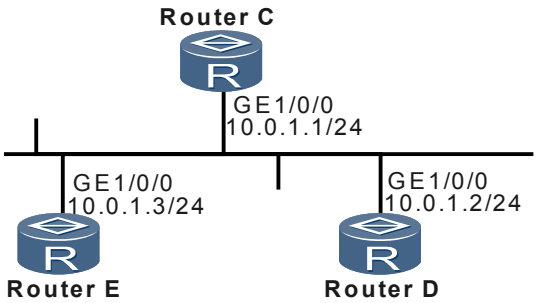
在对等体模式下，对等体双方可以相互同步对方的时钟。

组网需求

如图 5-3 所示。在同一个局域网中有 3 台设备。

- RouterC 的本地时钟设为 NTP 主时钟，层数为 2。
- RouterD 将 RouterC 设为自己的 NTP 服务器。即，RouterD 作为客户端。
- RouterE 将 RouterD 设为自己的被动对等体。即，RouterE 作为主动对等体。

图 5-3 配置 NTP 对等体模式的组网图



配置思路

配置思路如下：

1. 配置 RouterC 的本地时钟作为 NTP 主时钟，RouterD 向 RouterC 请求时钟同步。
2. 配置 RouterE 和 RouterD 为对等体，RouterE 向 RouterD 发起时钟同步请求。
3. 最终实现 RouterC、RouterD、RouterE 的时钟同步。

数据准备

为完成此配置例，需准备如下的数据：

- RouterC 的 IP 地址
- RouterD 的 IP 地址
- NTP 主时钟的层数

操作步骤

步骤 1 配置 RouterC、RouterD、RouterE 的 IP 地址。

按照图 5-3 给每个接口配置 IP 地址。配置完成后，3 台 Router 之间可以互相 ping 通。

具体配置过程略。

步骤 2 配置 NTP 客户端/服务器模式

#将 RouterC 的本地时钟设为 NTP 主时钟，层数为 2。

```
<RouterC> system-view
[RouterC] ntp-service refclock-master 2
```

在 RouterD 上指定 RouterC 作为 RouterD 的 NTP 服务器。

```
<RouterD> system-view
[RouterD] ntp-service unicast-server 10.0.1.1
```

完成上述配置后，Router D 可以同步 Router C 的时钟。

查看 RouterD 的 NTP 状态，可以看到时钟状态为“synchronized”，即，已经完成同步。时钟的层数为 3，比 Router C 低 1 级。

```
[RouterD] display ntp-service status
 clock status: synchronized
 clock stratum: 3
 reference clock ID: 10.0.1.1
 nominal frequency: 64.0029 Hz
 actual frequency: 64.0029 Hz
 clock precision: 2^7
 clock offset: 0.0000 ms
 root delay: 62.50 ms
 root dispersion: 0.20 ms
 peer dispersion: 7.81 ms
 reference time: 06:52:33.465 UTC Mar 7 2006(C7B7AC31.773E89A8)
```

步骤 3 配置 NTP 单播对等体模式

在 RouterE 上指定 RouterD 作为自己的被动对等体。

```
<RouterE> system-view
[RouterE] ntp-service unicast-peer 10.0.1.2
```

由于 RouterE 没有配置主时钟，并且其时钟层数低于 RouterD，所以 RouterE 向 RouterD 同步。

步骤 4 验证配置结果。

同步后观测 RouterE 的状态。RouterE 的时钟状态为“synchronized”，即，已经完成同步。RouterE 的时钟层数为 4，比被动对等体 RouterD 低 1 级。

```
[RouterE] display ntp-service status
 clock status: synchronized
 clock stratum: 4
 reference clock ID: 10.0.1.2
 nominal frequency: 64.0029 Hz
 actual frequency: 64.0029 Hz
 clock precision: 2^7
 clock offset: 0.0000 ms
 root delay: 124.98 ms
 root dispersion: 0.15 ms
 peer dispersion: 10.96 ms
 reference time: 06:55:50.784 UTC Mar 7 2006(C7B7ACF6.C8D002E2)
```

----结束

配置文件

- RouterC 的配置文件

```
#
```

```
 sysname RouterC
#
interface GigabitEthernet1/0/0
 ip address 10.0.1.1 255.255.255.0
#
ntp-service refclock-master 2
#
return
```

- RouterD 的配置文件

```
#
 sysname RouterD
#
interface GigabitEthernet1/0/0
 ip address 10.0.1.2 255.255.255.0
#
 ntp-service unicast-server 10.0.1.1
#
return
```

- Router E 的配置文件

```
#
 sysname RouterE
#
interface GigabitEthernet1/0/0
 ip address 10.0.1.3 255.255.255.0
#
 ntp-service unicast-peer 10.0.1.2
#
return
```

5.4.3 配置带验证的 NTP 广播模式示例

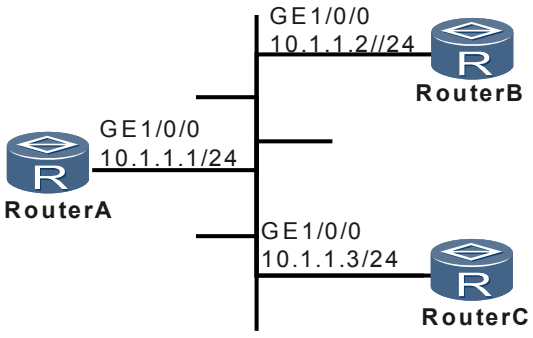
在局域网中，指定时钟精度高的设备作为 NTP 服务器，其他的设备同步服务器的时钟。

组网需求

如图 5-4 所示:

- RouterA、RouterB 与 RouterC 处于同一网段内。
- RouterA 为 NTP 广播服务器，通过 GE1/0/0 接口发送广播报文。RouterA 的本地时钟作为 NTP 主时钟，层级为 3。
- RouterB 和 RouterC 分别从各自的接口 GE1/0/0 监听广播消息。

图 5-4 配置 NTP 广播模式的组网图



配置思路

配置思路如下：

1. 配置 RouterA 为 NTP 广播服务器。
2. 配置 RouterB 与 RouterC 为 NTP 广播客户端。
3. 在 RouterA、RouterB 和 RouterC 上配置 NTP 验证。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA、RouterB 以及 RouterC 的 IP 地址
- NTP 主时钟的层数
- 验证密钥及其编号

操作步骤

步骤 1 配置每台 Router 的 IP 地址。

按照图 5-4 配置 IP 地址,此处不再赘述。

步骤 2 配置 NTP 广播服务器，并启用验证。

配置 RouterA 的本地时钟为 NTP 主时钟，层级为 3。

```
<RouterA> system-view
[RouterA] ntp-service refclock-master 3
```

使能 NTP 验证。

```
[RouterA] ntp-service authentication enable
[RouterA] ntp-service authentication-keyid 16 authentication-mode md5 Hello
[RouterA] ntp-service reliable authentication-keyid 16
```

配置 RouterA 为 NTP 广播服务器，从接口 GE1/0/0 发送 NTP 广播消息包，并指定使用密钥 ID 16 加密。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ntp-service broadcast-server authentication-keyid 16
[RouterA-GigabitEthernet1/0/0] quit
```

步骤 3 配置 RouterB。

使能 NTP 验证。

```
<RouterB> system-view
[RouterB] ntp-service authentication enable
[RouterB] ntp-service authentication-keyid 16 authentication-mode md5 Hello
[RouterB] ntp-service reliable authentication-keyid 16
```

配置 RouterB 作为 NTP 广播客户端，从接口 GE1/0/0 侦听 NTP 广播报文。

```
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ntp-service broadcast-client
[RouterB-GigabitEthernet1/0/0] quit
```

步骤 4 配置 RouterC。

使能 NTP 验证。

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

```
[RouterC] ntp-service authentication-keyid 16 authentication-mode md5 Hello
[RouterC] ntp-service reliable authentication-keyid 16
```

配置 RouterC 作为 NTP 广播客户端，从接口 GE1/0/0 侦听 NTP 广播报文。

```
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] ntp-service broadcast-client
[RouterC-GigabitEthernet1/0/0]quit
```

步骤 5 验证配置结果。

完成以上配置后，RouterB 和 RouterC 能够同步 RouterA 的时钟，

查看 RouterB 的 NTP 时钟状态。结果显示 NTP 时钟的状态为"synchronized"，意味着时钟同步完成。RouterB 的时钟等级为 4，比 RouterA 的时钟低一等级。

```
[RouterB] display ntp-service status
clock status: synchronized
clock stratum: 4
reference clock ID: 10.1.1.2
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 2^18
clock offset: 0.0000 ms
root delay: 0.00 ms
root dispersion: 0.42 ms
peer dispersion: 0.00 ms
reference time: 12:17:21.773 UTC Mar 7 2006(C7B7F851.C5EAF25B)
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
 ntp-service broadcast-server authentication-keyid 16
#
 ntp-service authentication enable
 ntp-service authentication-keyid 16 authentication-mode md5 %@ENC;8HX\#Q=^Q`MAF4<1!!
 ntp-service reliable authentication-keyid 16
 ntp-service refclock-master 3
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
 ntp-service broadcast-client
#
 ntp-service authentication enable
 ntp-service authentication-keyid 16 authentication-mode md5 %@ENC;8HX\#Q=^Q`MAF4<1!!
 ntp-service reliable authentication-keyid 16
#
Return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
```

```
 ip address 10.1.1.3 255.255.255.0
 ntp-service broadcast-client
#
 ntp-service authentication enable
 ntp-service authentication-keyid 16 authentication-mode md5 %@ENC;8HX\#Q=^Q`MAF4<1!!
 ntp-service reliable authentication-keyid 16
#
return
```

5.4.4 配置 NTP 组播模式示例

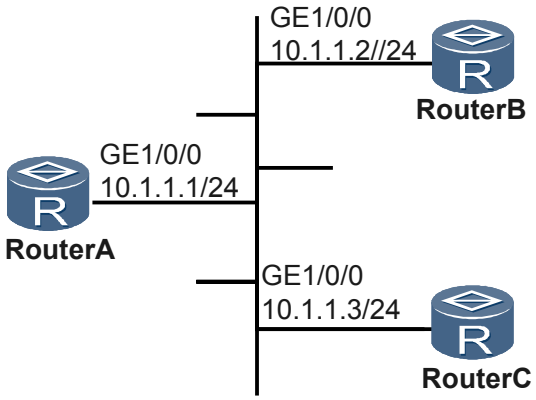
在组播域中，指定时钟精度高的设备作为 NTP 服务器，其他的设备同步服务器的时钟。

组网需求

如图 5-5 所示:

- RouterA、RouterB 与 RouterC 处于同一网段。
- RouterA 为 NTP 组播服务器，通过 GE1/0/0 接口发送组播报文。RouterA 的本地时钟作为 NTP 主时钟，层数为 2。
- RouterB 和 RouterC 分别从各自的接口 GE1/0/0 监听组播报文。

图 5-5 配置 NTP 组播模式的组网图



配置思路

配置思路如下：

1. 配置 RouterA 为 NTP 组播服务器。
2. 配置 RouterB 与 RouterC 作为 NTP 组播客户端。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA、RouterB 以及 RouterC 的 IP 地址
- NTP 主时钟的层数

操作步骤

步骤 1 配置每台 Router 的 IP 地址。

按图 5-5 配置 IP 地址。具体过程略。

步骤 2 配置 NTP 组播服务器。

配置 RouterA 的本地时钟为 NTP 主时钟，层数是 2。

```
<RouterA> system-view
[RouterA] ntp-service refclock-master 2
```

配置 RouterA 作为 NTP 组播服务器，从 GE1/0/0 接口发送 NTP 组播报文。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ntp-service multicast-server
```

步骤 3 配置 RouterB。

配置 RouterB 作为 NTP 组播客户端，从接口 GE1/0/0 侦听 NTP 组播报文。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ntp-service multicast-client
```

步骤 4 配置 RouterC。

配置 RouterC 作为 NTP 组播客户端，从接口 GE1/0/0 侦听 NTP 组播报文。

```
<RouterC> system-view
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] ntp-service multicast-client
```

步骤 5 验证配置结果。

完成以上配置后，RouterB、RouterC 能够同步 RouterA 的时钟。

查看 RouterB 的 NTP 时钟状态。结果显示 NTP 时钟的状态为"synchronized"，意味着时钟同步完成。RouterB 的时钟等级为 3，比 RouterA 的时钟低一等级。

```
[RouterB] display ntp-service status
 clock status: synchronized
 clock stratum: 3
 reference clock ID: 10.1.1.2
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^18
 clock offset: 0.66 ms
 root delay: 24.47 ms
 root dispersion: 208.39 ms
 peer dispersion: 9.63 ms
 reference time: 17:03:32.022 UTC Apr 25 2005(C61734FD.800303C0)
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 ntp-service refclock-master  2
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
```

```
 ntp-service multicast-server
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
 ntp-service multicast-client
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.3 255.255.255.0
 ntp-service multicast-client
#
return
```

6 NQA 配置

关于本章

通过配置 NQA，可以有效的检测网络运行的状态，使运营商能够实时采集到各种网络运行指标。

6.1 NQA 简介
通过 NQA 简介用户可以了解到 NQA 的基本概念及其所实现的功能。

6.2 配置 ICMP 测试
介绍使用 ICMP 测试检测 IP 网络的连通性。

6.3 配置 DHCP 测试
介绍使用 NQA 测试与 DHCP 服务器建立连接及获得地址的速度。

6.4 配置 FTP 下载测试
介绍使用 NQA 测试 FTP 下载的主要性能指标。

6.5 配置 FTP 上载测试
介绍使用 NQA 测试 FTP 上载的主要性能指标。

6.6 配置 HTTP 测试
介绍使用 NQA 测试 HTTP 服务各阶段的响应速度。

6.7 配置 DNS 测试
介绍使用 NQA 测试 DNS 解析速度。

6.8 配置 Traceroute 测试
介绍使用 NQA 进行 Traceroute 测试，查看网络中每一跳的连通情况。

6.9 配置 SNMP 查询测试
介绍使用 NQA 测试主机与 SNMP Agent 之间的通信状况。

6.10 配置 TCP 测试
介绍使用 NQA 测试 TCP 端口的响应速度。

6.11 配置 UDP 测试
介绍使用 NQA 测试 UDP 端口的响应速度。

6.12 配置 Jitter 测试

介绍使用 NQA 测试网络的抖动情况。客户端和服务器端都必须是华为设备才能进行 Jitter 测试。

6.13 配置 NQA 测试例的通用参数
介绍一些 NQA 测试常用的测试参数，并说明各个参数都可以应用到哪些测试例中。

6.14 配置 NQA 双向传输延迟阈值
介绍配置 NQA 双向传输阈值的设定。在测试的结果中将提供超过阈值的测试报文的统计值，为网络管理人员分析指定服务在网络中的运行情况提供依据。

6.15 配置 NQA 单向传输延迟阈值
介绍配置 NQA 单向传输阈值的设定。在测试的结果中将提供超过阈值的测试报文的统计值，为网络管理人员分析指定服务在网络中的运行情况提供依据。

6.16 配置 NQA 测试的 Trap 开关
通过配置 NQA 测试的 Trap 开关可以实现 NQA 测试成功或者失败产生 Trap 消息，可以通过设置 Trap 开关控制是否向网管发送 Trap 消息。

6.17 配置测试结果发送到 FTP 服务器
网管需要了解到设备的测试结果，如果网管不能及时对测试结果进行轮询，测试结果就会丢失。通过配置 FTP 方式保存测试结果到 FTP 服务器，可以最大程度的保存测试结果。

6.18 配置上下限 NQA 阈值告警
在 NQA 的测试结果超出阈值时，向网管发送告警信息，通知设备出现的变化情况。

6.19 维护 NQA
在测试中需要对测试进行维护时，可以通过重新启动测试例，清空测试结果信息实现对测试例的维护。

6.20 NQA 配置举例
介绍 NQA 的配置。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

6.1 NQA 简介

通过 NQA 简介用户可以了解到 NQA 的基本概念及其所实现的功能。

6.1.1 NQA 概述

通过 NQA 概述，用户可以了解到 NQA 的引入及其实现的功能。

随着运营商增值业务的开展，用户和运营商对 QoS 的相关要求越来越高，特别是在传统的 IP 网络承载语音和视频业务后，运营商与客户之间签订 SLA（Service Level Agreement）成为普遍现象。

为了让用户看到承诺的带宽是否达到需求，运营商需要设备侧提供相关的时延、抖动、丢包率等相关的统计参数，以及时了解网络的性能状况。

AR3200 提供 NQA（Network Quality Analysis）功能满足上述需求。

NQA 可以测量网络上运行的各种协议的性能，使运营商能够实时采集到各种网络运行指标，例如：HTTP 的总时延、TCP 连接时延、文件传输速率、FTP 连接时延、DNS 解析时延、DNS 解析错误率等。通过对这些指标进行控制，运营商可以为用户提供不同等级的网络服务，收取不同的费用。

同时，NQA 也是网络故障诊断和定位的有效工具。

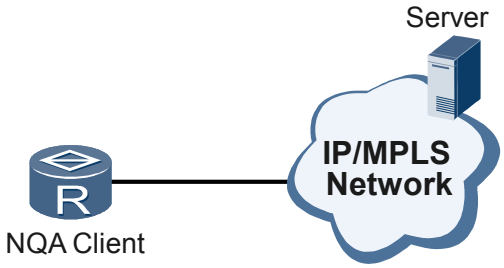
6.1.2 NQA 与 Ping 的比较

通过 NQA 与 Ping 的比较，用户可以了解到 NQA 与 Ping 在测试方式方面的区别。

NQA 是对 Ping 功能的扩展和增强。

Ping 使用 ICMP（Internet Control Message Protocol）测试数据包测试本端和指定目的端之间的往返时间，NQA 不但可以完成这项功能，还可以探测 TCP、UDP、FTP、HTTP、SNMP 服务是否打开，以及测试各种服务的响应时间。如图 6-1 所示。

图 6-1 NQA 测试示意图



与 Ping 不同，NQA 不在控制台终端实时显示每个包的往返时间或是否超时，而是在测试结束后通过 **display nqa results** 命令来查看 NQA 的测试结果。

用户也可以通过网管来设置 NQA 各项操作的参数，并启动测试。

6.1.3 NQA 客户端和服务器

本节介绍到 NQA 客户端、服务器和 NQA 测试例之间的关系。

NQA 测试例和 NQA 客户端

NQA 可以对多个项目进行测试，每个项目都需要创建一个测试例，且每个测试例只能是某一种类型的 NQA 测试。

NQA 测试例在客户端创建。每个测试例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例。

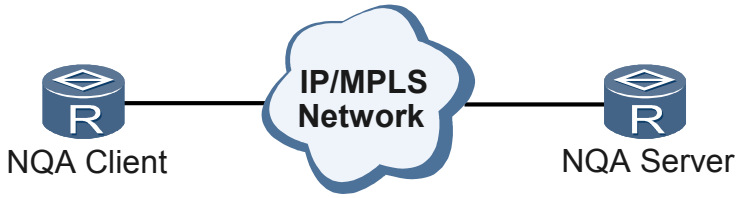
在测试例视图下，需要配置相关的测试参数。其中，有些参数只适用于某种类型的测试例，另外一些则适用于所有类型的测试例。

NQA 服务器

在大多数的测试项中，只需要配置 NQA Client 端。但在进行 TCP、UDP 和 Jitter 类型测试时，必须配置 NQA 服务器。

NQA 服务器负责处理 NQA 客户端发来的测试包，如图 6-2 所示，NQA 服务器通过监听功能对客户端发起的测试进行响应。

图 6-2 NQA 客户端和服务器的关系



可以在一个 NQA 服务器上创建多个 TCP 或 UDP 监听服务，每个监听服务对应一组指定的目的地址和端口号，目的地址和端口号可以重复。

NQA 测试执行

只有在 NQA 服务器上配置了相应的监听地址和端口号后，客户端发起的请求才能得到服务器的响应。并且，服务器监听服务中指定的 IP 地址、端口号要和客户端配置的参数一致。

创建测试例并配置好相关测试项参数之后，必须通过命令 **start** 启动 NQA 测试，并使用 **display nqa results** 命令查看测试结果。

6.1.4 AR3200 支持的 NQA 特性

介绍了 AR3200 支持的 NQA 测试例类型及调度方式。

NQA 提供的特性

- 与网管的配合：
  - 网管可以完全管理 NQA 的所有功能

  - 支持 NQA MIB 用户接口
  - 支持 Disman-traceroute-MIB 用户接口
  - 支持 Disman-NSLookUp-MIB 用户接口
  - 支持 Disman-ping-MIB 用户接口
- 支持多种类型的测试：
  - ICMP 测试
  - DHCP 测试
  - FTP 测试
  - HTTP 测试
  - DNS 测试
  - Traceroute 测试
  - SNMP 测试
  - TCP 测试
  - UDP 测试
  - UDP Jitter 测试
- Jitter 类型的测试例支持最大连续发送报文数目 3000，可模拟语音业务流量。
- 支持配置 256 个测试例。
- 支持测试例的任务调度：

  实现对测试例的调度，降低设备的并发负担。

  对单个测试例，支持多种启动时间、结束时间的设置：
  - 支持立即启动、延迟启动、定时启动
  - 支持报文发送完后自动结束、立即结束、延迟结束、定时结束、生命周期结束

  多个任务同时启动时，设备主动合理分布启动时间和测试间隔。
- 支持自动延时功能。可以最大限度的利用系统的资源，在规定的时间内完成测试例。
- 支持单向延迟统计和双向延迟统计，并且可以通过设定阈值，对测试结果中超过阈值的报文进行统计。
- 支持单向丢包统计。
- 支持动态减少测试例。
- 支持通过 FTP 将测试结果发送到 FTP 服务器。
- 支持灵活告警机制。即，根据被测对象的 OID，为被测对象设置上限和下限阈值，监控被测对象的性能。当测试结果超过阈值时，根据当前事件触发告警。

6.2 配置 ICMP 测试

介绍使用 ICMP 测试检测 IP 网络的连通性。

6.2.1 建立配置任务

在配置 ICMP 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

ICMP 测试提供类似于普通 **ping** 命令的功能，但输出信息更为丰富。

前置任务

在配置 ICMP 测试之前，需配置 NQA 客户端与被测试设备间路由可达。

数据准备

在配置 ICMP 测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	目的地址
3	（可选）VPN 实例名、发送测试报文的源接口、源 IP 地址、Echo Request 报文大小、TTL、ToS、填充字符、测试报文发送间隔、NQA 测试的失败百分比
4	启动方式和结束方式

6.2.2 配置 ICMP 测试参数

在 ICMP 测试时，需要配置的相关参数。

背景信息

请在 NQA 客户端进行下述配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type icmp**，配置测试例类型为 ICMP。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 （可选）根据需要，配置 ICMP 测试其他参数。具体参数配置请参见**配置 NQA 测试例的通用参数**。

- 执行命令 **vpn-instance** *vpn-instance-name*，配置所测试的 VPN 实例。
- 执行命令 **source-interface** *interface-type interface-number*，配置发送测试报文的源接口。
- 执行命令 **source-address ipv4** *ip-address*，配置源地址。该参数相当于 **ping** 命令中的“**-a**”选项。

- 执行命令 **datasize** *size*，配置 Echo Request 报文的大小，不包括 IP 头。该参数相当于 **ping** 命令中的“**-s**”选项。
- 执行命令 **ttl** *number*，配置 TTL 值。该参数相当于 **ping** 命令中的“**-h**”选项。
- 执行命令 **tos** *value*，配置服务类型，即 IP 报文头中 ToS 字段的值。该参数相当于 **ping** 命令中的“**-tos**”选项。
- 执行命令 **datafill** *fillstring*，配置填充字符。该参数相当于 **ping** 命令中的“**-p**”选项。
- 执行命令 **interval seconds** *interval*，配置测试报文的发送间隔。该参数相当于 **ping** 命令中的“**-m**”选项。
- 执行命令 **fail-percent** *percent*，配置 NQA 测试的失败百分比。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

步骤 6 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

6.2.3 检查配置结果

在配置 ICMP 测试成功后，可以查看到测试的结果数据。

前提条件

已经完成 ICMP 测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

步骤 1 执行 **display nqa results** [**test-instance** *admin-name test-name*]命令查看测试结果。

----结束

任务示例

执行 **display nqa results** 命令，如果测试已经成功结束，可以看到以下信息。

- testflag is inactive
- The test is finished
- Completion:success

对于 ICMP 类型的测试，还可以看到接收到响应报文的最小时间、最大时间、RTT（往返时延）。

```
<Huawei> display nqa results
 NQA entry(admin, test) :testflag is inactive ,testtype is icmp
  1 . Test 1 result   The test is finished
   Send operation times: 3              Receive response times: 3
   Completion:success                 RTD OverThresholds number: 0
   Attempts number:1                    Drop operation number:0
   Disconnect operation number:0        Operation timeout number:0
   System busy operation number:0       Connection fail number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   Destination ip address:10.112.58.3
   Min/Max/Average Completion Time: 2/5/3
   Sum/Square-Sum  Completion Time: 9/33
   Last Good Probe Time: 2010-06-21 15:33:09.2
   Lost packet ratio: 0 %
```

6.3 配置 DHCP 测试

介绍使用 NQA 测试与 DHCP 服务器建立连接及获得地址的速度。

6.3.1 建立配置任务

在配置 DHCP 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

通过 NQA DHCP 测试，可以得到以下信息：

- 客户端与 DHCP 服务器之间建立连接的时间。
- 客户端获得地址的时间。

前置任务

在配置 DHCP 测试之前，需完成以下任务：

- 配置 DHCP 服务器或 DHCP Relay
- 配置 NQA 客户端与 DHCP 服务器或 DHCP Relay 间路由可达

数据准备

在配置 DHCP 测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	与 DHCP 服务器相连的出接口
3	（可选）：超时时间、NQA 测试的失败百分比
4	启动方式和结束方式

6.3.2 配置 DHCP 测试参数

在配置 DHCP 测试时，需要配置的相关参数

背景信息

说明

AR3200 支持将路由器配置为 DHCP 服务器，相关配置步骤请参见《Huawei AR3200 系列企业路由器 配置指南 IP 业务》的“DHCP 配置”。

在 NQA 客户端上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type dhcp**，配置测试例类型为 DHCP。

步骤 4 执行命令 **source-interface** *interface-type interface-number*，指定发送 DHCP 请求报文的源接口。

该接口可以是与 DHCP 服务器相连的以太口。

步骤 5 （可选）根据需要，配置 DHCP 测试其他参数。具体参数配置请参见**配置 NQA 测试例的通用参数**。

- 执行命令 **timeout** *time*，配置 NQA 测试例的操作超时时间。

  说明

  对于 DHCP 测试，发送完探测报文后，等待响应的时间可能达到 10 秒。缺省情况下，超时时间是 15 秒，如需要设置为其他的值，建议设置的值在 10 秒以上。

- 执行命令 **fail-percent** *percent*，配置 NQA 测试的失败百分比。

步骤 6 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

6.3.3 检查配置结果

在 DHCP 测试成功后，可以查看到 DHCP 测试的结果数据。

前提条件

已经完成 DHCP 测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

步骤 1 执行 **display nqa results** [**test-instance** *admin-name test-name*]命令查看测试结果。

----结束

任务示例

执行 **display nqa results** 命令，如果测试已经成功结束，可以看到以下信息：

- testflag is inactive
- The test is finished
- Completion:success

对于 DHCP 类型的测试，还可以在扩展结果中看到以下信息：

- 与服务器断开连接的次数；
- 断开连接操作的超时次数；
- 服务器忙的次数；
- 连接失败的次数
- 操作顺序错误次数；
- 丢弃操作次数；
- 操作统计错误次数；

```
<Huawei> display nqa results
NQA entry(admin, dhcp) :testflag is inactive ,testtype is dhcp
1 . Test 1 result   The test is finished
   Send operation times: 3              Receive response times: 3
   Completion:success                   RTD OverThresholds number:  0
   Attempts number:1                    Drop operation number:0
   Disconnect operation number:0        Operation timeout number:0
   System busy operation number:0       Connection fail number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   Destination ip address:10.1.1.3
   Min/Max/Average Completion Time: 1030/1030/1030
   Sum/Square-Sum  Completion Time: 1030/1060900
   Last Good Probe Time: 2007-6-29 16:00:2.2
   Lost packet ratio: 0 %
```

6.4 配置 FTP 下载测试

介绍使用 NQA 测试 FTP 下载的主要性能指标。

6.4.1 建立配置任务

在配置 FTP 下载测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

在 NQA 的 FTP 下载测试中，本地作为 FTP 客户端，从 FTP 服务器下载指定文件。

可以获得 FTP 各个阶段的统计数据，包括：FTP 控制连接建立时间、数据传输时间。

前置任务

在配置 FTP 下载测试之前，需完成以下任务：

- 配置 FTP 服务器，包括 FTP 用户名、密码、登录时的目录
- 配置 NQA FTP 客户端与 FTP 服务器之间路由可达

数据准备

在配置 FTP 下载测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	FTP 服务器的 IP 地址
3	（可选）FTP 操作的源地址、VPN 实例名、FTP 操作的源端口号、FTP 操作的目的端口号
4	FTP 用户名和密码
5	要下载的文件名
6	启动方式和结束方式

6.4.2 配置 FTP 下载测试参数

在配置 FTP 下载测试时，需要配置的相关参数。

背景信息

请在 NQA 客户端进行下列配置，NQA 客户端同时作为 FTP 客户端。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type ftp**，配置测试例类型为 FTP。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 （可选）根据需要，配置 FTP 测试其他参数。具体参数配置请参见**配置 NQA 测试例的通用参数**。

- 执行命令 **source-address ipv4** *ip-address*，配置测试例的源地址。
- 执行命令 **source-port** *port-number*，配置源端口。
- 执行命令 **destination-port** *port-number*，配置目的端口。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

步骤 6 执行命令 **ftp-operation get**，配置操作类型为 Get。

缺省情况下，FTP 操作类型为 Get 操作。

步骤 7 执行命令 **ftp-username** *name*，配置 FTP 用户名。

步骤 8 执行命令 **ftp-password** *password*，配置 FTP 密码。

步骤 9 执行命令 **ftp-filename** *file-name*，配置 FTP 操作文件名。

说明

在进行 FTP 测试时，建议不要选择过大的文件，以免由于超时导致测试失败。

步骤 10 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

6.4.3 检查配置结果

在 FTP 下载成功后，可以查看到 FTP 下载测试的结果数据。

前提条件

已经完成 FTP 下载测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

步骤 1 执行 **display nqa results** [**test-instance** *admin-name test-name*]命令查看测试结果。

----结束

任务示例

对于 FTP 下载测试，如果测试成功，执行 **display nqa results** 命令，可以看到各阶段所用的时间。

- 连接建立时间：CtrlConnTime
- 数据传输时间：DataConnTime
- FTP 操作总时间：SumTime

```
<Huawei> display nqa results
 NQA entry(admin, ftp) :testflag is inactive ,testtype is ftp
  1 . Test 1 result   The test is finished
   SendProbe:1                                  ResponseProbe:1
   Completion :success                          RTD OverThresholds number: 0
   MessageBodyOctetsSum: 448                    Stats errors number: 0
   Operation timeout number: 0                  System busy operation number:0
   Drop operation number:0                      Disconnect operation number: 0
   CtrlConnTime Min/Max/Average: 438/438/438
   DataConnTime Min/Max/Average: 218/218/218
   SumTime Min/Max/Average: 656/656/656
   Average RTT:380
   Lost packet ratio: 0 %
```

6.5 配置 FTP 上载测试

介绍使用 NQA 测试 FTP 上载的主要性能指标。

6.5.1 建立配置任务

在配置 FTP 上载测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

在 NQA 的 FTP 上载测试中，本地作为 FTP 客户端，向 FTP 服务器上载指定文件。

可以获得 FTP 各个阶段的统计数据，包括：FTP 控制连接建立时间、数据传输时间。

进行上载测试时，可以指定要上载的文件，也可以指定要上载的字节数，NQA 客户端自动构造测试文件上载。

前置任务

在配置 FTP 上载测试之前，需完成以下任务：

- 配置 FTP 服务器，包括 FTP 用户名、密码、登录时的目录
- 配置 NQA 客户端与 FTP 服务器之间路由可达

数据准备

在配置 FTP 上载测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	FTP 服务器的 IP 地址
3	FTP 用户名和密码

序号	数据
4	（可选）FTP 操作的源地址、VPN 实例名、FTP 操作的源端口号、FTP 操作的目的端口号
5	要上载的文件名或文件大小
6	启动方式和结束方式

6.5.2 配置 FTP 上载测试参数

在配置 FTP 上载测试参数时，需要配置的相关参数。

背景信息

请在 NQA 客户端进行下列配置，NQA 客户端同时作为 FTP 客户端。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type ftp**，配置测试例类型为 FTP。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 （可选）根据需要，配置 FTP 测试其他参数。具体参数配置请参见**配置 NQA 测试例的通用参数**。

- 执行命令 **source-address ipv4** *ip-address*，配置测试例的源地址。
- 执行命令 **source-port** *port-number*，配置源端口。
- 执行命令 **destination-port** *port-number*，配置目的端口。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

步骤 6 执行命令 **ftp-operation put**，配置操作类型为 Put。

缺省情况下,FTP 的操作类型是 GET。

步骤 7 执行命令 **ftp-username** *name*，配置 FTP 用户名。

步骤 8 执行命令 **ftp-password** *password*，配置 FTP 密码。

步骤 9 指定要上载的文件，有两种方式可以选择。

- 如果要上载指定名称的文件，使用命令 **ftp-filename** *file-name*。

  说明

  - 可以不指定文件路径，系统会在当前路径下查找该文件。如果指定的文件名不存在，则按照指定文件名来构造一个文件，上载文件的大小为 1M。
  - 文件名不能包含字符：“~、*、/、\、'、"、，”，文件路径可以包含这些字符。
  - 文件名中可以包含扩展名，但不能只有扩展名。如.txt。
- 如果要上载指定大小的文件，使用命令 **ftp-filesize** *size*。客户端将自动构建一个名为“nqa-ftp-test.txt”的文件上载。

说明

在进行 FTP 测试时，建议不要选择过大的文件，以免由于超时导致测试失败。

步骤 10 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

6.5.3 检查配置结果

在 FTP 上载测试成功后，可以查看到 FTP 上载测试的结果数据。

前提条件

已经完成 FTP 上载测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

步骤 1 执行 **display nqa results** 命令查看测试结果。

----结束

任务示例

对于 FTP 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到各阶段所用的时间。

- 连接建立时间：CtrlConnTime
- 数据传输时间：DataConnTime
- FTP 操作总时间：SumTime

```
<Huawei> display nqa results
 NQA entry(admin, ftp) :testflag is inactive ,testtype is ftp
  1 . Test 1 result   The test is finished
    SendProbe:1                                 ResponseProbe:1
    Completion :success                         RTD OverThresholds number: 0
    MessageBodyOctetsSum: 448                   Stats errors number: 0
    Operation timeout number: 0                 System busy operation number:0
    Drop operation number:0                     Disconnect operation number: 0
    CtrlConnTime Min/Max/Average: 438/438/438
    DataConnTime Min/Max/Average: 218/218/218
    SumTime Min/Max/Average: 656/656/656
    Average RTT:380
    Lost packet ratio: 0 %
```

6.6 配置 HTTP 测试

介绍使用 NQA 测试 HTTP 服务各阶段的响应速度。

6.6.1 建立配置任务

在配置 HTTP 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

NQA 的 HTTP 测试提供三个阶段的响应速度：

- DNS 解析时间：客户端发送 DNS 报文给名字解析器，将 HTTP 服务器名字解析为 IP 地址，DNS 解析报文返回的时间。
- TCP 建立连接时间：客户端与 HTTP 服务器通过 TCP“三次握手”建立连接所用的时间。
- 交易时间：客户端发送 Get 或 Post 报文给 HTTP 服务器，响应报文到达 HTTP 服务器的时间。

前置任务

在配置 HTTP 测试之前，需完成以下任务：

- 配置 HTTP 服务器
- 配置 NQA 客户端与 HTTP 服务器之间路由可达

数据准备

在配置 HTTP 测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	HTTP 服务器名
3	●（可选）源地址、源端口号 ●（可选）目的端口号 ●（可选）NQA 测试的失败百分比
4	HTTP 操作类型
5	HTTP 测试所访问的页面和版本信息
6	启动方式和结束方式

6.6.2 配置 HTTP 测试参数

在配置 HTTP 测试时，需要配置的相关参数。

背景信息

请在 NQA 客户端进行下列配置，NQA 客户端同时作为 HTTP 客户端。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type http**，配置测试例类型为 HTTP。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 （可选）根据需要，配置 HTTP 测试其他参数。具体参数配置请参见**配置 NQA 测试例的通用参数**。

- 执行命令 **source-address ipv4** *ip-address*，配置源地址。
- 执行命令 **source-port** *port-number*，配置源端口。
- 执行命令 **destination-port** *port-number*，配置目的端口。
- 执行命令 **fail-percent** *percent*，配置 NQA 测试的失败百分比。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

步骤 6 执行命令 **http-operation** { **get** | **post** }，配置 HTTP 操作类型。

缺省情况下，HTTP 操作类型为 Get 操作。

步骤 7 执行命令 **http-url** *deststring* [*verstring*]，配置 HTTP 测试所访问的页面以及 HTTP 版本信息。

说明

在不配置 HTTP 版本信息的情况下，缺省情况下支持 HTTP1.0。通过配置可以支持 HTTP1.1。

步骤 8 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

6.6.3 检查配置结果

在 HTTP 测试成功后，可以查看到 HTTP 测试的结果数据。

前提条件

已经完成 HTTP 测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

步骤 1 执行 **display nqa results** [**test-instance** *admin-name test-name*]命令查看测试结果。

----结束

任务示例

对于 HTTP 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到各阶段的响应速度。

- DNS 查询时间：DNSRTT
- TCP 连接建立时间：TCPConnectRTT
- 数据传输时间 TransactionRTT、HTTP 测试时间 RTT

```
<Huawei> display nqa results
NQA entry (admin, http) :testflag is inactive ,testtype is http
  1 . Test 1 result   The test is finished
   SendProbe:3                          ResponseProbe:3
   Completion:success                   RTD OverThresholdsnumber: 0
   MessageBodyOctetsSum: 411            TargetAddress: 100.2.1.200
   DNSQueryError number: 0              HTTPError number: 0
   TcpConnError number : 0              System busy operation number:0
   DNSRTT Sum/Min/Max:0/0/0             TCPConnectRTT Sum/Min/Max: 6/1/4
   TransactionRTT Sum/Min/Max: 3/1/1
   RTT Sum/Min/Max/Avg: 7/1/5/2
   DNSServerTimeout:0  TCPConnectTimeout:0  TransactionTimeout: 0
   Lost packet ratio:0%
```

6.7 配置 DNS 测试

介绍使用 NQA 测试 DNS 解析速度。

6.7.1 建立配置任务

在配置 DNS 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

DNS 测试用于检测将给定的 DNS 名称解析成 IP 地址的速度。

前置任务

在配置 DNS 测试之前，需完成以下任务：

- 配置 DNS 服务器
- 配置 NQA 客户端与 DNS 服务器之间路由可达

数据准备

在配置 DNS 测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	DNS 服务器的 IP 地址
3	要解析的目的主机名
4	启动方式和结束方式

6.7.2 配置 DNS 测试参数

在配置 DNS 测试时，需要配置的相关参数。

背景信息

请在 NQA 客户端进行下列配置，NQA 客户端同时作为 DNS 客户端。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dns resolve**，使能基于 DNS 的动态域名解析功能。

缺省情况下，动态域名解析功能被禁止。

步骤 3 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 4 执行命令 **test-type dns**，配置测试例类型为 DNS。

步骤 5 执行命令 **dns-server ipv4** *ip-address*，配置 DNS 服务器地址的 IPv4 地址。

说明

具体参数配置请参见**配置 NQA 测试例的通用参数**。

步骤 6 执行命令 **destination-address url** *urlstring*，配置目的主机名。

步骤 7 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

6.7.3 检查配置结果

在 DNS 测试成功后，可以查看到 DNS 测试的结果数据。

前提条件

已经完成 DNS 测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

步骤 1 执行 **display nqa results** [**test-instance** *admin-name test-name*]命令查看测试结果。

----结束

任务示例

对于 DNS 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<Huawei> display nqa results
NQA entry(t, t) :testflag is inactive ,testtype is dns
  1 . Test 1 result   The test is finished
   Send operation times: 1              Receive response times: 1
   Completion:success                   RTD OverThresholds number: 0
   Attempts number:1                    Drop operation number:0
   Disconnect operation number:0        Operation timeout number:0
   System busy operation number:0       Connection fail number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   Destination ip address:10.82.55.191
   Min/Max/Average Completion Time: 4/4/4
   Sum/Square-Sum  Completion Time: 4/16
   Last Good Probe Time: 2010-06-21 15:40:12.6
   Lost packet ratio: 0 %
```

6.8 配置 Traceroute 测试

介绍使用 NQA 进行 Traceroute 测试，查看网络中每一跳的连通情况。

6.8.1 建立配置任务

在配置 Traceroute 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

NQA 的 Trcaeroute 测试提供类似于 **tracert** 命令的功能，但输出信息更为丰富。

前置任务

在配置 Traceroute 测试之前，需配置 NQA 客户端与被测试设备间路由可达。

数据准备

在配置 Trcaeroute 测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	目的地址
3	（可选）：VPN 实例名、允许的最大跳失败数、报文的初始 TTL 和最大 TTL、源地址、目的端口
4	启动方式和结束方式

6.8.2 配置 Traceroute 测试参数

在配置 Traceroute 测试时，需要配置的相关参数。

背景信息

请在 NQA 客户端进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type trace**，配置测试例类型为 Traceroute。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置 Traceroute 测试的目的地址。

步骤 5 （可选）根据需要，配置 Traceroute 测试其他参数。具体参数配置请参见**配置 NQA 测试例的通用参数**。

- 执行命令 **tracert-hopfailtimes** *times*，配置 NQA 测试 Traceroute 测试例的跳失败数。
- 执行命令 **tracert-livetime first-ttl** *first-ttl* **max-ttl** *max-ttl*，配置报文的初始 TTL 和最大 TTL。
- 执行命令 **source-address ipv4** *ip-address*，配置源地址。
- 执行命令 **destination-port** *port-number*，配置目的端口。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

步骤 6 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。

- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

6.8.3 检查配置结果

在 Traceroute 测试成功后，可以查看到 Traceroute 测试的结果数据。

前提条件

已经完成 Traceroute 测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

步骤 1 执行 **display nqa results** [**test-instance** *admin-name test-name*]命令查看测试结果。

----结束

任务示例

对于 Traceroute 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到每一跳的统计信息。

```
<Huawei> display nqa results
NQA entry(t, t) :testflag is inactive ,testtype is trace
  1 . Test 1 result   The test is finished
   Completion:success                   Attempts number:1
   Disconnect operation number:0        Operation timeout number:0
   System busy operation number:0       Connection fail number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   Drop operation number:0
   Last good path Time:2010-06-21 15:41:01.7
   1 . Hop 1
    Send operation times: 3              Receive response times: 3
    Min/Max/Average Completion Time: 1/2/1
    Sum/Square-Sum  Completion Time: 4/6
    RTD OverThresholds number: 0
    Last Good Probe Time: 2010-06-21 15:41:01.7
    Destination ip address:10.112.58.3
    Lost packet ratio: 0 %
```

6.9 配置 SNMP 查询测试

介绍使用 NQA 测试主机与 SNMP Agent 之间的通信状况。

6.9.1 建立配置任务

在配置 SNMP 查询测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

通过 SNMP 查询测试，可以了解主机与 SNMP Agent 之间通信的统计信息。

前置任务

在配置 SNMP 测试之前，需完成以下任务：

- 配置 SNMP Agent
- 配置 NQA 客户端与 SNMP Agent 之间路由可达

数据准备

在配置 SNMP 查询测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	SNMP Agent 的 IP 地址
3	（可选）源地址、源端口号、发送报文的时间间隔、NQA 测试的失败百分比
4	启动方式和结束方式

6.9.2 配置 SNMP 测试参数

在配置 SNMP 测试时，需要配置的相关参数。

背景信息

请在 NQA 客户端进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **snmp-agent**，启动 SNMP Agent 服务。

步骤 3 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 4 执行命令 **test-type snmp**，配置测试例类型为 SNMP。

步骤 5 执行命令 **destination-address ipv4** *ip-address*，配置目的地址，即 SNMP Agent 的地址。

说明

目的地址所指定的机器上必须启动网管功能，否则将收不到回应包。

步骤 6 （可选）根据需要，配置 SNMP 测试其他参数。具体参数配置请参见**配置 NQA 测试例的通用参数**。

- 执行命令 **vpn-instance** *vpn-instance-name*，配置所测试的 VPN 实例。

- 执行命令 **source-address ipv4** *ip-address*，配置源地址。
- 执行命令 **source-port** *port-number*，配置源端口。
- 执行命令 **interval seconds** *interval*，配置测试报文的发送间隔。
- 执行命令 **fail-percent** *percent*，配置 NQA 测试的失败百分比。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

步骤 7 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

6.9.3 检查配置结果

在 SNMP 查询测试成功后，可以查看到 SNMP 查询测试的结果数据。

前提条件

已经完成 SNMP 查询测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

步骤 1 执行 **display nqa results** [**test-instance** *admin-name test-name*]命令查看测试结果。

----结束

任务示例

对于 SNMP 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<Huawei> display nqa results
 NQA entry(admin, snmp) :testflag is inactive ,testtype is snmp
  1 . Test 1 result   The test is finished
   Send operation times: 3              Receive response times: 3
   Completion:success                   RTD OverThresholds number: 0
   Attempts number:1                    Drop operation number:0
   Disconnect operation number:0        Operation timeout number:0
   System busy operation number:0       Connection fail number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   Destination ip address:10.2.1.2
   Min/Max/Average Completion Time: 63/172/109
   Sum/Square-Sum  Completion Time: 329/42389
   Last Good Probe Time: 2006-8-5 15:33:49.1
```

```
Lost packet ratio: 0 %
```

6.10 配置 TCP 测试

介绍使用 NQA 测试 TCP 端口的响应速度。

6.10.1 建立配置任务

在配置 TCP 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

NQA 支持对 TCP 连接指定端口的响应速度测试。

前置任务

在配置 TCP 测试之前，需配置 NQA 客户端与 TCP 服务器之间路由可达。

数据准备

在配置 TCP 测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	TCP 服务器端监听的 IP 地址和端口号
3	（可选）目的端口号、源地址、源端口号、发送报文的时间间隔、NQA 测试的失败百分比
4	启动方式和结束方式

6.10.2 配置 TCP 服务器端

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

背景信息

请在 NQA 服务器端进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa-server tcpconnect** *ip-address port-number*，配置 TCP 监听服务。

说明

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

----结束

6.10.3 配置 TCP 客户端

在 TCP 客户端配置测试例时，需要配置的相关参数。

背景信息

请在 NQA 客户端进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type tcp**，配置测试例类型为 TCP。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 执行命令 **destination-port** *port-number*，配置目的端口。

步骤 6 （可选）根据需要，配置 TCP 测试其他参数。具体参数配置请参见**配置 NQA 测试例的通用参数**。

- 执行命令 **source-address ipv4** *ip-address*，配置源地址。
- 执行命令 **source-port** *port-number*，配置源端口。
- 执行命令 **interval seconds** *interval*，配置测试报文的发送间隔。
- 执行命令 **fail-percent** *percent*，配置 NQA 测试的失败百分比。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

步骤 7 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

测试类型 TCP Public 和 TCP Private 的不同之处在于：

- TCP Public 测试固定向目的地址的 7 号 TCP 端口发起连接建立请求，客户端不需要配置目的端口，但要在服务器端监听 7 号 TCP 端口。
- TCP Private 测试需要指定目的端口，并且服务器端要对应监听。

----结束

6.10.4 检查配置结果

在 TCP 测试成功后，可以查看到 TCP 测试的结果数据。

前提条件

已经完成 TCP 测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

- 在 NQA 客户端执行 **display nqa results** [**test-instance** *admin-name test-name*]命令查看测试结果。
- 在 NQA 服务器端执行 **display nqa-server** 命令查看服务器信息。

----结束

任务示例

对于 TCP 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<Huawei> display nqa results
 NQA entry(admin, tcp) :testflag is inactive ,testtype is tcp
  1 . Test 1 result   The test is finished
    Send operation times: 3                Receive response times: 3
    Completion:success                     RTD OverThresholds number: 0
    Attempts number:0                      Drop operation number:0
    Disconnect operation number:0          Operation timeout number:0
    System busy operation number:0         Connection fail number:0
    Operation sequence errors number:0     RTT Stats errors number:0
    Destination ip address:10.2.1.2
    Min/Max/Average Completion Time: 31/62/51
    Sum/Square-Sum  Completion Time: 155/8649
    Last Good Probe Time: 2006-8-5 15:55:15.3
    Lost packet ratio: 0 %
```

6.11 配置 UDP 测试

介绍使用 NQA 测试 UDP 端口的响应速度。

6.11.1 建立配置任务

在配置 UDP 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

NQA 支持对 UDP 连接指定端口的响应速度测试。

前置任务

在配置 UDP 测试之前，需配置 NQA 客户端与 UDP 服务器之间路由可达。

数据准备

在配置 UDP 测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	UDP 服务器端监听的 IP 地址和端口号
3	UDP 客户端发送探测报文的目的地址和目的端口号
4	（可选）：源地址、源端口号、发送报文的时间间隔、NQA 测试的失败百分比
5	启动方式和结束方式

6.11.2 配置 UDP 测试服务器端

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

背景信息

请在 NQA 服务器端进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa-server udpecho** *ip-address port-number*，配置 UDP 监听服务。

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

----结束

6.11.3 配置 UDP 测试客户端

在 UDP 客户端配置测试例时，需要配置的相关参数。

背景信息

请在 NQA 客户器端进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type udp**，配置测试例类型为 UDP。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 执行命令 **destination-port** *port-number*，配置目的端口。

步骤 6 （可选）根据需要，配置 UDP 测试其他参数。具体参数配置请参见**配置 NQA 测试例的通用参数**。

- 执行命令 **source-address ipv4** *ip-address*，配置源地址。
- 执行命令 **source-port** *port-number*，配置源端口。
- 执行命令 **interval seconds** *interval*，配置测试报文的发送间隔。
- 执行命令 **fail-percent** *percent*，配置 NQA 测试的失败百分比。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

步骤 7 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

6.11.4 检查配置结果

在 UDP 测试成功后，可以查看到 UDP 测试的结果数据。

前提条件

已经完成 UDP 测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

- 在 NQA 客户端执行 **display nqa results** [**test-instance** *admin-name test-name*]命令查看测试结果。
- 在 NQA 服务器端执行 **display nqa-server** 命令查看服务器信息。

----结束

任务示例

对于 UDP 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<Huawei> display nqa results
 NQA entry(admin, udp) :testflag is inactive ,testtype is udp
  1 . Test 1 result   The test is finished
   Send operation times: 3              Receive response times: 3
   Completion:success                   RTD OverThresholds number: 0
   Attempts number:1                    Drop operation number:0
   Disconnect operation number:0        Operation timeout number:0
   System busy operation number:0       Connection fail number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   Destination ip address:10.2.1.2
   Min/Max/Average Completion Time: 32/109/67
```

```
Sum/Square-Sum  Completion Time: 203/16749
Last Good Probe Time: 2006-8-5 16:9:21.6
Lost packet ratio: 0 %
```

6.12 配置 Jitter 测试

介绍使用 NQA 测试网络的抖动情况。客户端和服务器端都必须是华为设备才能进行 Jitter 测试。

6.12.1 建立配置任务

在配置 Jitter 测试前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

Jitter（抖动时间）是指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。

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数据包。
2. 目的端每收到一个数据包，就给它打上时间戳，然后再把这个数据包发回到源端。
3. 源端收到数据包后通过计算目的端接收数据包时间间隔和源端发送数据包的时间间隔之差，计算出抖动时间。

从源端接收到的信息中计算出，数据包从源端到目的端和从目的端到源端的最大抖动时间、最小抖动时间及平均抖动时间；可以计算出从目的端到源端或从源端到目的端的最大单向延时，从而清晰的反映出网络状况。

Jitter 测试可以设置单个测试例的连续发包数目，通过这项设置，可以在一段时间内模拟某种数据的真实流量。例如，设置 3000 个 UDP 报文以 20 毫秒的间隔发送，可以在一分钟内模拟 G.711 流量。

说明

在客户端和服务器端配置 NTP，可以有效提高测试的精度。

前置任务

在配置 Jitter 测试之前，需配置 NQA 客户端与 UDP 服务器之间路由可达。

数据准备

在配置 Jitter 测试之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	UDP 服务器端监听的 IP 地址和端口号
3	UDP 客户端发送探测报文的目的地址和目的端口号

序号	数据
4	（可选）：VPN 实例名、UDP 客户端发送探测报文的源地址、UDP 客户端发送探测报文的源端口号、每次发送的测试探针个数、每次发送的测试报文个数、发送间隔、NQA 测试的失败百分比、Jitter 报文的版本号
5	启动方式和结束方式

6.12.2 配置 Jitter 测试服务器端

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

背景信息

请在 NQA 服务器端进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa-server udpecho** *ip-address port-number*，配置 UDP 监听服务。

服务器端监听的 IP 地址和端口号必须与客户端的配置一致。

----结束

6.12.3 配置 Jitter 测试客户端

在 UDP 客户端配置测试例时，需要配置的相关参数。

背景信息

说明

系统支持统计 Jitter 测试最大单向延时。

请在 NQA 客户端进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2（可选）执行命令 **nqa-jitter tag-version** *version-number*，配置 Jitter 报文的版本号。

在配置 Jitter 报文的版本号为 2 并配置单向丢包统计后，在测试结果中将可以看到，从源端到目的端、从目的端到源端和未知方向的丢包情况。为网络管理员定位网络故障、检测恶意对网络的攻击提供依据。

步骤 3 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 4 执行命令 **test-type jitter**，配置测试例类型为 Jitter。

步骤 5 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 6 执行命令 **destination-port** *port-number*，配置目的端口。

步骤 7 （可选）根据需要，配置 Jitter 测试其他参数。具体参数配置请参见**配置 NQA 测试例的通用参数**。

- 执行命令 **source-address ipv4** *ip-address*，配置源地址。
- 执行命令 **source-port** *port-number*，配置源端口。
- 执行命令 **probe-count** *number*，配置每次发送的测试探针个数。
- 执行命令 **jitter-packetnum** *number*，配置每次测试所发送的测试包个数。

  Jitter 测试是对 UDP 报文传输的延时变化进行统计分析。为了提高统计结果的准确性，每一次测试系统都会发送多个测试包。每次测试发送的测试包个数越多，统计分析越准确，但完成测试所需的时间也越长。

  说明

  Jitter 测试的次数取决于 **probe-count** 命令的配置，而每次测试所发送的测试包的个数由 **jitter-packetnum** 命令确定。实际配置时，**probe-count** 命令设置的测试次数与 **jitter-packetnum** 命令设置的测试包个数的乘积不能超过 3000。

- 执行命令 **interval** { **milliseconds** *interval* | **seconds** *interval* }，配置发送测试包的时间间隔。

  Jitter 测试包的发送时间间隔越小，完成测试就越快。但由于处理器在数据包发送和接收时处理都会有延时，如果发送测试包的时间间隔很小，Jitter 结果的统计值误差会比较大。

- 执行命令 **fail-percent** *percent*，配置 NQA 测试的失败百分比。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

步骤 8 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

6.12.4 检查配置结果

在 Jitter 测试成功后，可以查看到 Jitter 测试的结果数据。

前提条件

已经完成 Jitter 测试功能的所有配置。

说明

NQA 测试不会在终端自动显示测试结果，必须使用 **display nqa results** 命令查看测试结果。缺省情况下只能显示最近 5 次的测试结果。

操作步骤

- 在 NQA 客户端执行 **display nqa results** [**test-instance** *admin-name test-name*]命令查看测试结果。
- 在 NQA 服务器端执行 **display nqa-server** 命令查看服务器信息。

----结束

任务示例

对于 Jitter 类型的测试，如果测试成功，执行 **display nqa results** 命令，可以看到以下信息。

```
<Huawei> display nqa results test-instance admin jitter
 NQA entry(admin, jitter) :testflag is inactive ,testtype is jitter
  1 . Test 2 result   The test is finished
   SendProbe:60                          ResponseProbe:60
   Completion:success                    RTD OverThresholds number:0
   OWD OverThresholds SD number:0        OWD OverThresholds DS number:0
   Min/Max/Avg/Sum RTT:1/1/1/60          RTT  Square Sum:60
   NumOfRTT:60                           Drop operation number:0
   Operation sequence errors number:0    RTT Stats errors number:0
   System busy operation number:0        Operation timeout number:0
   Min Positive SD:1                     Min Positive DS:1
   Max Positive SD:1                     Max Positive DS:1
   Positive SD Number:15                 Positive DS Number:1
   Positive SD Sum:15                    Positive DS Sum:1
   Positive SD Square Sum:15             Positive DS Square Sum:1
   Min Negative SD:1                     Min Negative DS:1
   Max Negative SD:1                     Max Negative DS:1
   Negative SD Number:15                 Negative DS Number:1
   Negative SD Sum:15                    Negative DS Sum:1
   Negative SD Square Sum:15             Negative DS Square Sum:1
   Min Delay SD:0                        Min Delay DS:0
   Avg Delay SD:0                        Avg Delay DS:0
   Max Delay SD:0                        Max Delay DS:0
   Delay SD Square Sum:27                Delay DS Square Sum:1
   Packet Loss SD:0                      Packet Loss DS:0
   Packet Loss Unknown:0                 Average of Jitter:1
   Average of Jitter SD:1                Average of Jitter DS:1
   jitter out value:0.0312500            jitter in value:0.0020833
   NumberOfOWD:60                        Packet Loss Ratio: 0%
   OWD SD Sum:27                         OWD DS Sum:1
   ICPIF value: 0                        MOS-CQ value: 0
   TimeStamp unit: ms                    Packet Rewrite Number: 0
   Packet Rewrite Ratio: 0%              Packet Disorder Number: 0
   Packet Disorder Ratio: 0%             Fragment-disorder Number: 0
   Fragment-disorder Ratio: 0%
```

6.13 配置 NQA 测试例的通用参数

介绍一些 NQA 测试常用的测试参数，并说明各个参数都可以应用到哪些测试例中。

6.13.1 建立配置任务

在配置 NQA 测试例的通用参数前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

除了不同测试类型的具体配置参数外，NQA 还提供测试例的通用配置项。

对于本节介绍的通用配置，通常情况下，使用缺省值即可。

前置任务

在配置 NQA 通用参数之前，需正确创建 NQA 测试例。

6.13.2 配置测试例的通用参数

指明各个测试在具体测试例中的应用。

背景信息

请在 NQA 客户端进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，进入已建立的 NQA 测试例的测试例视图。

步骤 3 根据需要，配置测试例通用参数。

- 执行命令 **agetime** *hh:mm:ss*，配置 NQA 测试例的老化时间。
- 执行命令 **alarm** *entry-number* { **lost-packet-ratio** | **jitter-average** | **jitter-ds-average** | **jitter-sd-average** | **packet-loss-ds** | **packet-loss-sd** | **rtt-average** } { **absolute** | **delta** } { **falling-threshold** *threshold-value1 event-entry1* | **rising-threshold** *threshold-value2 event-entry2* } * [*description*]，配置 NQA 测试例的告警。
- 执行命令 **datafill** *fillstring*，配置 NQA 测试例的填充字符。

  说明

  只能对 UDP、Jitter、ICMP、Trace 类型的测试例配置填充字符
- 执行命令 **datasize** *size*，配置 NQA 测试例的报文大小。

  说明

  只能对 ICMP、UDP、Jitter、Trace 类型的测试例配置测试报文大小。
- 执行命令 **description** *string*，配置测试例描述。
- 执行命令 **destination-address ipv4** *ip-address*，配置 NQA 测试例的目的 IP 地址。

  说明

  不能对 DNS 和 DHCP 测试配置此参数。
- 执行命令 **destination-address url** *urlstring*，配置 NQA 测试例的目的 url 地址。

  说明

  只能对 DNS 和 HTTP 类型的测试例，配置 NQA 测试例的目的 url 地址。
- 执行命令 **destination-port** *port-number*，配置 NQA 测试例的目的端口号。

  说明

  只能对 UDP、Jitter、TCP、Trace、FTP 和 HTTP 类型的测试例，配置 NQA 测试例的目的端口号。
- 执行命令 **dns-server ipv4** *ip-address*，配置 NQA 测试中 DNS 测试例的 DNS 服务器地址。

说明

只能对 DNS 和 HTTP 类型的测试例，配置 NQA 测试例的 DNS 服务器地址。

- 执行命令 **fail-percent** *percent*，配置 NQA 测试的失败百分比。

  说明

  不能对 Trace、FTP、DNS 测试配置此参数。

- 执行命令 **frequency** *interval*，配置 NQA 测试例的测试周期。
- 执行命令 **ftp-filename** *file-name*，配置 NQA 测试 FTP 测试例的文件名和文件路径。

  说明

  只能对 FTP 类型的测试例，配置 NQA 测试 FTP 测试例的文件名和文件路径。

- 执行命令 **ftp-filesize** *size*，配置 NQA 测试中 FTP 测试例测试的文件大小。

  说明

  只能对 FTP 类型的测试例，配置 NQA 测试中 FTP 测试例测试的文件大小。

- 执行命令 **ftp-operation** { **get** | **put** }，配置 NQA 测试中 FTP 测试例的操作类型。

  说明

  只能对 FTP 类型的测试例，配置 NQA 测试中 FTP 测试例的操作类型。

- 执行命令 **ftp-password** *password*，配置 NQA 测试中 FTP 测试例的用户密码。

  说明

  只能对 FTP 类型的测试例，配置 NQA 测试中 FTP 测试例的用户密码。

- 执行命令 **ftp-username** *name*，配置 NQA 测试的 FTP 测试例使用的用户名。

  说明

  只能对 FTP 类型的测试例，配置 NQA 测试的 FTP 测试例使用的用户名。

- 执行命令 **http-operation** { **get** | **post** }，配置 NQA 测试 HTTP 测试例的测试类型。

  说明

  只能对 HTTP 类型的测试例，配置 NQA 测试 HTTP 测试例的测试类型。

- 执行命令 **http-url** *deststring* [*verstring*]，配置 NQA 测试 HTTP 测试例的相对路径名和版本信息。

  说明

  只能对 HTTP 类型的测试例，配置 NQA 测试 HTTP 测试例的相对路径名和版本信息。

- 执行命令 **interval** { **milliseconds** *interval* | **seconds** *interval* }，配置 NQA 测试例的报文间隔。

  说明

  只能对 ICMP、UDP、SNMP、Jitter、TCP 类型的测试例，配置 NQA 测试例的报文间隔。

- 执行命令 **jitter-packetnum** *number*，配置 NQA 测试例的测试报文个数。

  说明

  只能对 Jitterr 类型的测试例配置测试报文个数。

- 执行命令 **probe-count** *number*，配置一次测试的探针数。

  说明

  不能对 FTP 和 DNS 测试配置此参数。

- 执行命令 **probe-failtimes** *times*，用来配置 NQA 测试例的报文失败数，即，发送 Trap 的阈值。
- 执行命令 **records history** *number*，配置 NQA 测试的最大历史记录数目。
- 执行命令 **records result** *number*，配置 NQA 测试的最大测试结果记录数目。
- 执行命令 **sendpacket passroute**，配置 NQA 测试不查找路由表发送报文。

说明

不能对 DHCP、DNS 测试配置此参数。

- 执行命令 **set-df**，不允许对报文分片。

  说明

  只能对 Trace 类型的测试例，配置不允许对报文分片。

- 执行命令 **send-trap** { **all** | { **owd-ds** | **owd-sd** | **probefailure** | **rtd** | **testcomplete** | **testfailure** } * }，配置 Trap 消息的发送条件。
- 执行命令 **source-address ipv4** *ip-address*，配置 NQA 测试例的源 IP 地址。

  说明

  不能对 DHCP、DNS 测试配置此参数。

- 执行命令 **source-interface** *interface-type interface-number*，配置 NQA 测试例的源接口。

  说明

  只能对 ICMP、DHCP、DHCP、MPing 和 PathMTU 类型的测试例，配置 NQA 测试例的源接口。

- 执行命令 **source-port** *port-number*，配置本次测试的源端口号。

  说明

  不能对 DNS、ICMP、DHCP、Trace 类型的测试配置源端口号。

- 执行命令 **test-failtimes** *times*，配置当 NQA 测试连续测试失败达到一定的次数以后，需要向网管发送 Trap 信息。
- 执行命令 **timeout** *time*，配置测试超时时间。
- 执行命令 **ttl** *number*，配置 NQA 测试例报文中的 TTL 值。

  说明

  不能对 DHCP、DNS、Trace 测试配置此参数。

- 执行命令 **tos** *value*，配置测试包的服务类型 TOS。

  说明

  不能对 DHCP、DNS、Trace 测试配置此参数。

- 执行命令 **tracert-hopfailtimes** *times*，配置 NQA 测试 Trace route 测试例的跳失败数。

  说明

  只能对 Trace 测试例配置此参数。

- 执行命令 **tracert-livetime first-ttl** *first-ttl* **max-ttl** *max-ttl*，配置 NQA 测试 Trace 测试例的生存时间。

  说明

  只能对 Trace 测试例配置生存时间。

- 执行命令 **vpn-instance** *vpn-instance-name*，配置 NQA 测试例的 VPN 实例名。

  说明

  不能对 DHCP、DNS 测试配置此参数。

----结束

6.13.3 检查配置结果

在配置 NQA 测试例的通用参数成功后，可以查看到测试的结果数据。

前提条件

已经完成 NQA 测试例通用参数功能的所有配置。

操作步骤

步骤 1 执行 **display nqa-agent** [*admin-name test-name*] [**verbose**]查看 NQA 测试例配置的通用参数。

----结束

任务示例

```
<Huawei> display nqa-agent
 NQA Tests Max:256           NQA Tests  Number:   2
 NQA Flow  Max:1000          NQA Flow Remained:1000

nqa test-instance a a
 test-type tcp
 destination-address ipv4 10.1.1.1
 source-address ipv4 10.1.1.10
 ttl 100
 tos 50
 interval seconds 30
 timeout 20
 nqa status : normal
```

6.14 配置 NQA 双向传输延迟阈值

介绍配置 NQA 双向传输阈值的设定。在测试的结果中将提供超过阈值的测试报文的统计值，为网络管理人员分析指定服务在网络中的运行情况提供依据。

6.14.1 建立配置任务

在配置 NQA 双向传输延迟阈值前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

配置测试例的双向传输阈值后，在测试的结果中将提供超过阈值的测试报文的统计值，为网络管理人员分析指定服务在网络中的运行情况提供依据。

前置任务

在配置 NQA 阈值之前，需完成以下任务：

- 设备运行正常
- 正确创建 NQA 测试例并配置相关参数

数据准备

在配置阈值功能之前，需要准备以下数据。

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	测试例的双向传输延迟阈值

6.14.2 配置双向传输延迟阈值

配置双向传输延迟阈值，在传输时间超过阈值后，向网管发送 Trap。

背景信息

在运行 NQA 测试例的路由器上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，进入 NQA 视图。

步骤 3 执行命令 **test-type** { **dhcp** | **dns** | **ftp** | **http** | **icmp** | **jitter** | **snmp** | **tcp** | **trace** | **udp** }，配置测试例类型。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 （可选）执行命令 **destination-port** *port-number*，配置目的端口。

步骤 6 执行命令 **threshold rtd** *rtd-value*，配置双向传输延迟阈值。

步骤 7 执行命令 **send-trap rtd**，打开阈值 Trap 开关。

----结束

6.14.3 检查配置结果

在配置 NQA 双向传输延迟阈值成功后，可以查看到 NQA 阈值的配置信息。

前提条件

已经完成 NQA 双向传输延迟阈值测试功能的所有配置。

操作步骤

步骤 1 执行 **display nqa-agent** [*admin-name test-name*] [**verbose**]命令查看 NQA 测试例阈值配置。

----结束

任务示例

执行命令 **display nqa-agent verbose**，可以查看 NQA 阈值的配置信息。例如：

```
<Huawei> display nqa-agent verbose
 NQA Tests Max:256           NQA Tests  Number:   1
```

```
 NQA Flow  Max:1000          NQA Flow Remained:1000

nqa test-instance admin jitter
 test-type jitter
 destination-address ipv4 100.1.1.201
 destination-port 80
 threshold rtd 2000
 send-trap rtd
 nqa status : normal
```

6.15 配置 NQA 单向传输延迟阈值

介绍配置 NQA 单向传输阈值的设定。在测试的结果中将提供超过阈值的测试报文的统计值，为网络管理人员分析指定服务在网络中的运行情况提供依据。

6.15.1 建立配置任务

在配置 NQA 单向传输延迟阈值前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

在进行 Jitter 测试时，网络设定单向传输延迟阈值，通过对测试结果中超过阈值的测试报文统计值进行分析，使网络管理人员能够有效的监控网络的运行情况。

前置任务

在配置 NQA 阈值之前，需完成以下任务：

- 设备运行正常
- 正确创建 NQA 测试例并配置相关参数

数据准备

在配置 NQA 阈值之前，需要准备以下数据。

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	测试例的阈值

6.15.2 配置单向传输延迟阈值

配置单向传输延迟阈值，在传输时间超过阈值后，向网管发送 Trap。

背景信息

在运行 NQA 测试例的路由器上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，进入 NQA 视图。

步骤 3 执行命令 **test-type jitter**，配置测试例类型。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5（可选）执行命令 **destination-port** *port-number*，配置目的端口。

步骤 6 执行命令 **threshold owd-sd** *owd-sd-value*，配置从源到目的的传输延迟阈值。

步骤 7 执行命令 **threshold owd-ds** *owd-ds-value*，配置从目的到源的传输延迟阈值。

----结束

6.15.3 检查配置结果

在配置 NQA 单向传输延迟阈值成功后，可以查看到 NQA 阈值的配置信息。

前提条件

已经完成 NQA 单向传输延迟阈值测试功能的所有配置。

操作步骤

- 执行 **display nqa-agent** [*admin-name test-name*] [**verbose**]命令查看 NQA 测试例阈值配置。

----结束

任务示例

执行命令 **display nqa-agent** [*admin-name test-name*] [**verbose**]，可以查看 NQA 阈值的配置信息。例如：

```
<Huawei> display nqa-agent verbose
 NQA Tests Max:256           NQA Tests  Number:   1
 NQA Flow  Max:1000          NQA Flow Remained:1000

nqa test-instance admin jitter
 test-type jitter
 destination-address ipv4 100.1.1.201
 destination-port 80
 send-trap probefailure
 send-trap testfailure
 send-trap testcomplete
 send-trap rtd
 send-trap owd-sd
 send-trap owd-ds
 threshold owd-sd 2000
 threshold owd-ds 2000
 nqa status : normal
```

6.16 配置 NQA 测试的 Trap 开关

通过配置 NQA 测试的 Trap 开关可以实现 NQA 测试成功或者失败产生 Trap 消息，可以通过设置 Trap 开关控制是否向网管发送 Trap 消息。

6.16.1 建立配置任务

在配置 NQA 测试的 Trap 开关前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

NQA 测试成功或者失败都会产生 Trap 消息，可以通过设置 Trap 开关控制是否向网管发送 Trap 消息。

NQA 支持 DISMAN-PING-MIB 中定义的 3 类 TRAP。

NQA 支持超过单向延迟阈值或超过双向延迟阈值向网管发送 Trap。

- 对于所有的测试例如果双向传输延迟超过设置的阈值时，且 Trap 使能标志为真，则根据配置的网管地址向网管发送告警信息。
- 对于 Jitter 类型的测试例如果从源到目的或从目的到源，任意一个方向的传输延迟超过设置的阈值，且 Trap 使能标志为真，则根据配置的网管地址向网管发送 Trap 信息。

Trap 报文包含目的 IP 地址信息、操作状态信息、结果地址信息、最小和最大 RTT、时间总和、已发送探测数、接收到的相应报文数、RTT 平方和，以及最后一次探测成功的时间。

前置任务

在配置 NQA 测试的 Trap 开关之前，需完成以下任务：

- NQA 客户端与网管站之间路由可达
- 正确创建 NQA 测试例并配置相关参数

数据准备

在配置 NQA 测试的 Trap 开关之前，需要准备以下数据：

序号	数据
1	NQA 测试例的管理者、测试例的测试例名
2	触发 Trap 发送的 NQA 事件类型
3	● 触发 Trap 发送的测试失败次数（可选） ● 触发 Trap 发送的探测失败次数（可选）

6.16.2 配置发送测试失败发送 Trap

在 NQA 测试报文失败后，发送 Trap。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type tcp**，配置测试例类型。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 （可选）执行命令 **destination-port** *port-number*，配置目的端口。

步骤 6 执行命令 **send-trap testfailure**，发送 Trap 开关。

缺省情况下，不发送 Trap 消息。

步骤 7 执行命令 **test-failtimes** *times*，配置发送 Trap 的测试失败次数。

缺省情况下，测试失败一次就会发送一条 Trap 信息。

----结束

6.16.3 配置探测失败发送 Trap

在 NQA 测试失败后，发送 Trap。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type tcp**，配置测试例类型。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 （可选）执行命令 **destination-port** *port-number*，配置目的端口。

步骤 6 执行命令 **probe-failtimes** *times*，配置发送 Trap 的探测失败次数。

缺省情况下，探测失败一次就会发送一条 Trap 信息。

步骤 7 执行命令 **send-trap probefailure**，发送 Trap 开关。

缺省情况下，不发送 Trap 消息。

----结束

6.16.4 配置探测成功发送 Trap

在 NQA 测试成功后，发送 Trap。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type tcp**，配置测试例类型。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 （可选）执行命令 **destination-port** *port-number*，配置目的端口。

步骤 6 执行命令 **send-trap testcomplete**，发送 Trap 开关。

缺省情况下，不发送 Trap 消息。

----结束

6.16.5 配置超过阈值发送 Trap

在 NQA 测试结果超过阈值后，发送 Trap。

背景信息

请在 NQA 客户端进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，建立 NQA 测试例，并进入测试例视图。

步骤 3 执行命令 **test-type tcp**，配置测试例类型。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 （可选）执行命令 **destination-port** *port-number*，配置目的端口。

步骤 6 执行命令 **send-trap rtd**，打开超过阈值发送 Trap 开关。

缺省情况下，不发送 Trap 消息。

----结束

6.16.6 检查配置结果

在配置 NQA 测试的 Trap 开关成功后，可以在 Trapbuffer 中看到告警信息。

前提条件

已经完成 NQA 测试 Trap 开关测试功能的所有配置。

操作步骤

步骤 1 执行命令 **display trapbuffer** [**size** *value*] 查看 NQA 测试例发送的 Trap。

----结束

任务示例

执行命令 **display trapbuffer** [**size** *value*] ，查看产生的告警信息。

例如：

```
<Huawei> display trapbuffer size 2
Trapping buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 11
#May  6 2009 12:54:17+00:00 CBB6-PE3 SINDEX/4/INDEXMAP:OID 1.3.6.1.4.1.2011.5.25.110.2.0.1
ShortIFIndexMapTable changed.
#May  6 2009 11:02:37+00:00 CBB6-PE3 SRM_BASE/4/ENTITYREGSUCCESS: OID
1.3.6.1.4.1.2011.5.25.129.2.1.18 Physical entity register succeeded.
 (EntityPhysicalIndex=17367040, BaseTrapSeverity=2, BaseTrapProbableCause=70144,
BaseTrapEventType=5, EntPhysicalContainedIn=1677721
6, EntPhysicalName="SRU slot 9", RelativeResource="", ReasonDescription="MPU9")
```

6.17 配置测试结果发送到 FTP 服务器

网管需要了解到设备的测试结果，如果网管不能及时对测试结果进行轮询，测试结果就会丢失。通过配置 FTP 方式保存测试结果到 FTP 服务器，可以最大程度的保存测试结果。

6.17.1 建立配置任务

在配置测试结果发送到 FTP 服务器前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

系统默认可以保存最近测试的 5 条测试结果，新产生的测试结果会覆盖最早的测试结果。如果网管不能及时对测试结果进行轮询，测试结果就会丢失。通过配置 FTP 方式保存测试结果，把达到最大条数的测试结果发送统计结果到 FTP 服务器或定时发送统计结果到 FTP 服务器，可以有效避免测试结果丢失，便于网络管理者分析不同时间的测试结果，来综合考虑对网络的管理。

前置任务

在配置测试结果发送到 FTP 服务器之前，需要完成以下任务：

- 配置 FTP 服务器
- 配置 NQA 客户端与网管端路由可达
- 配置测试例

数据准备

在配置测试结果发送到 FTP 服务器之前，需要准备以下数据：

序号	数据
1	FTP 服务器地址

序号	数据
2	登录 FTP 服务器所需的用户名及密码
3	通过 FTP 保存测试结果的条数
4	通过 FTP 保存测试结果的时间

6.17.2 配置连接 FTP 服务器需要的参数

指定接收测试结果的 FTP 服务器地址和登录 FTP 服务器需要的用户名、密码。

背景信息

在 NQA 客户端上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa-ftp-record ip-address** *ip-address* 或 **nqa-ftp-record vpn-instance** *vpn-instance*，配置 FTP 服务器地址。

步骤 3 执行命令 **nqa-ftp-record username** *username*，配置 FTP 的用户名。

步骤 4 执行命令 **nqa-ftp-record password** *password*，配置 FTP 的密码。

步骤 5 执行命令 **nqa-ftp-record filename** *filename*，配置保存的文件名。

----结束

6.17.3 使能通过 FTP 保存 NQA 测试结果功能

只有使能了 FTP 保存 NQA 测试结果功能后，才能向 FTP 服务器发送测试结果。

背景信息

在 NQA 客户端上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa-ftp-record enable**，使能 FTP 保存测试结果。

----结束

6.17.4 （可选）配置通过 FTP 保存测试结果的条数

配置保存在 FTP 服务器文件中的测试结果条目数。

背景信息

在 NQA 客户端上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa-ftp-record item-num** *item-number*，配置保存 FTP 测试结果到文件的条数。

----结束

6.17.5 （可选）配置通过 FTP 保存的测试结果的时间

系统每次能够发送两个测试结果到服务器端，如果 FTP 服务器端不支持文件续写的功能，每次发送的测试结果都将在 FTP 服务器端创建一个新的文件。

背景信息

在 NQA 客户端上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa-ftp-record time** *time*，配置保存 FTP 测试结果到文件的时间。

----结束

6.17.6 （可选）配置 FTP 传送成功向网管端发送 Trap

通过 FTP 保存测试结果成功后，向网管发送 Trap 通知网管测试文件已经保存成功。

背景信息

在 NQA 客户端上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa-ftp-record trap-enable**，配置 FTP 传送成功向网管端发送 Trap。

第一次发送成功后，不会触发告警，从第二次开始，每次发送成功都会触发告警。

----结束

6.17.7 启动测试例

启动测试例，测试结果会定时记录到文件中。

背景信息

在 NQA 客户端上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，进入 NQA 视图。

步骤 3 执行命令 **test-type** { **dhcp** | **dns** | **ftp** | **http** | **icmp** | **jitter** | **snmp** | **tcp** | **trace** | **udp** }，配置测试例类型。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 （可选）执行命令 **destination-port** *port-number*，配置目的端口。

步骤 6 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm* | *dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。
- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

6.17.8 检查配置结果

在配置测试结果发送到 FTP 服务器成功后，可以查看到保存 NQA 测试结果的配置信息。

前提条件

完成测试结果发送到 FTP 服务器的所有配置。

操作步骤

步骤 1 使用命令 **display nqa-ftp-record configuration**，查看保存 NQA 测试结果的配置信息。

----结束

任务示例

执行命令 **display nqa-ftp-record configuration**，可以查看到保存 NQA 测试结果的配置信息。

```
<Huawei> display nqa-ftp-record configuration
---------------NQA FTP SAVE RECORD CONFIGURATION---------------
   FUNCTION: ENABLE    TRAP: DISABLE
   IP-ADDRESS:11.1.1.8
   VPN-INSTANCE:
   USERNAME:wang
   PASSWORD:123
   FILENAME:icmp
   ITEM-NUM:10010
   TIME:2
   LAST FINISHED FILENAME:icmp20080605-150350.txt
```

6.18 配置上下限 NQA 阈值告警

在 NQA 的测试结果超出阈值时，向网管发送告警信息，通知设备出现的变化情况。

6.18.1 建立配置任务

在配置上下限 NQA 阈值告警前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

用户可以通过配置告警阈值的方式来对网络进行监控。在配置监控条件后，当测试的结果中的监控项超出了用户的设定的上限或下限阈值时，设备通过告警方式通知网管站，告知网络出现的情况，便于用户对网络实时的运行情况进行监控。

前置任务

在配置 NQA 阈值告警功能前，需要完成以下任务：

- 配置测试例

数据准备

在配置 NQA 告警阈值之前，需要准备以下数据：

序号	数据
1	阈值相关的事件号
2	阈值告警号
3	上限阈值
4	下限阈值

6.18.2 配置阈值告警相关事件

配置超过阈值时，系统需要采取的动作，可以记录日志、产生告警或者即可以记录日志也可以产生告警。

背景信息

在 NQA 客户端上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa event** *event-entry* { **linkage** *admin-name test-name* | **log** | **trap** | **log-trap** | **none** } [*description*]，配置事件号及相关联的事件。

----结束

6.18.3 配置阈值告警

配置测试结果在超过阈值时产生触发相应的事件。

背景信息

在 NQA 客户端上进行下列配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，进入测试例视图。

步骤 3 执行命令 **test-type** { **dhcp** | **dns** | **ftp** | **http** | **icmp** | **jitter** | **snmp** | **tcp** | **trace** | **udp** }，配置测试例类型。

步骤 4 执行命令 **destination-address ipv4** *ip-address*，配置目的地址。

步骤 5 （可选）执行命令 **destination-port** *port-number*，配置目的端口。

步骤 6 执行命令 **alarm** *entry-number* { **lost-packet-ratio** | **jitter-average** | **jitter-ds-average** | **jitter-sd-average** | **packet-loss-ds** | **packet-loss-sd** | **rtt-average** } { **absolute** | **delta** } { **falling-threshold** *threshold-value1 event-entry1* | **rising-threshold** *threshold-value2 event-entry2* } * [description *description*]，配置告警号及阈值。

说明

目前只支持绝对统计，不支持相对统计。

----结束

6.18.4 启动测试例

启动测试例，在出现超过阈值时，采取和事件对应的动作。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，进入 NQA 视图。

步骤 3 执行命令 **start**，启动 NQA 测试。

命令 **start** 有多种形式，根据实际需要选择其中一种启动方式：

- 执行命令 **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，立即启动测试例。
- 执行命令 **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，在指定时刻启动测试例。

- 执行命令 **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]，延迟指定时间后启动测试例。

----结束

6.18.5 检查配置结果

在配置上下限 NQA 阈值告警成功后，可以查看到上下限 NQA 阈值告警的配置情况。

前提条件

完成上下限 NQA 阈值告警的所有配置。

操作步骤

- 使用命令 **display nqa-event**，查看配置的最大事件数量和已经配置的事件数量。
- 在 NQA 视图下，使用命令 **display nqa alarm**，查看配置的最大告警数量和已经配置的告警数。
- 使用命令 **display nqa-agent** [*admin-name test-name*] [**verbose**]，查看 NQA 客户端配置的测试例状态信息。

----结束

任务示例

执行命令 **display nqa-event**，可以查看到可配置的最大事件数量和已经配置的事件数量。

```
<Huawei> display nqa-event
NQA event information:
------------------------------------------------------
NQA Event Max: 100                  NQA Event Number: 1
------------------------------------------------------
```

执行命令 **display nqa alarm**，可以查看到可配置的最大告警数量和已经配置的告警数。

```
[Huawei-nqa-admin-icmp] display nqa alarm
NQA Alarm Information:
------------------------------------------------------------------
Admin-Name   Operation-Tag   Alarm-Entry   AlarmType   Event-Entry
------------------------------------------------------------------
admin        jitter          10            Rising       10
```

执行命令 **display nqa-agent**，可以查看到 NQA 客户端配置的测试例状态信息。

```
<Huawei> display nqa-agent
 NQA Tests Max:256           NQA Tests  Number:   1
 NQA Flow  Max:1000          NQA Flow Remained:1000
nqa test-instance admin icmp
 test-type icmp
 destination-address ipv4 11.1.1.32
 frequency 5
 alarm 10 rtt-average 2 rising-threshold 200 10 falling-threshold 0 10
 alarm 20 lost-packet-ratio 2 rising-threshold 10 10 falling-threshold 1 10
 nqa status : normal
```

6.19 维护 NQA

在测试中需要对测试进行维护时，可以通过重新启动测试例，清空测试结果信息实现对测试例的维护。

6.19.1 重新启动测试例

在测试不成功时，可以在下一个时间段重新启动测试来尝试。

前提条件

在确认需要重新启动测试例的情况下，请在 NQA 视图下执行以下命令。

背景信息

重新启动测试例，将终止正在运行的测试例。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，进入 NQA 测试例视图。

步骤 3 执行命令 **restart** 重新启动一条 NQA 测试例。

----结束

6.19.2 清除统计信息

当前的测试统计信息已经保存到 FTP 服务器，可以把相关的测试结果清除。

前提条件

在确认需要清除统计信息时，请在 NQA 视图下执行以下的命令。

背景信息

清除统计信息后，以前的统计信息将无法恢复，务必仔细确认。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **nqa test-instance** *admin-name test-name*，进入 NQA 测试例视图。

步骤 3 使用 **clear-records** 命令清除 NQA 测试例的所有历史统计和结果统计。

----结束

6.20 NQA 配置举例

介绍 NQA 的配置。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项、配置思路等。

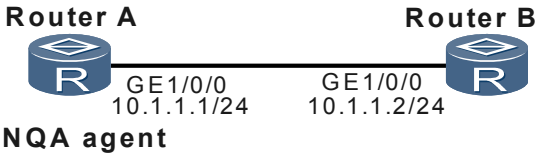
6.20.1 配置 ICMP 测试示例

通过配置 ICMP 测试可以检测到 IP 网络的连通性。

组网需求

如图 6-3 所示，RouterA 作为 NQA 客户端，测试 RouterB 是否可达。

图 6-3 ICMP 测试组网图



配置思路

1. 使用 NQA ICMP 测试功能，测试报文在本端（RouterA）和指定的目的端（RouterB）之间是否可达。
2. 使用 NQA ICMP 测试功能，测试报文在本端（RouterA）和指定的目的端（RouterB）之间的往返时间。

数据准备

为完成此配置例，需准备如下的数据：

- RouterB 的主机地址

操作步骤

步骤 1 配置 IP 地址（略）

步骤 2 使能 NQA 客户端，配置 ICMP 类型的 NQA 测试例

```
<RouterA> system-view
[RouterA] nqa test-instance admin icmp
[RouterA-nqa-admin-icmp] test-type icmp
[RouterA-nqa-admin-icmp] destination-address ipv4 10.1.1.2
```

步骤 3 立即启动测试

```
[RouterA-nqa-admin-icmp] start now
```

步骤 4 验证测试结果

```
[RouterA-nqa-admin-icmp] display nqa results test-instance admin icmp
 NQA entry(admin, icmp) :testflag is inactive ,testtype is icmp
  1 . Test 1 result   The test is finished
```

```
Send operation times: 3                  Receive response times: 3
Completion:success                       RTD OverThresholds number: 0
Attempts number:1                        Drop operation number:0
Disconnect operation number:0            Operation timeout number:0
System busy operation number:0           Connection fail number:0
Operation sequence errors number:0       RTT Stats errors number:0
Destination ip address:10.1.1.2
Min/Max/Average Completion Time: 31/46/36
Sum/Square-Sum  Completion Time: 108/4038
Last Good Probe Time: 2006-8-2 10:7:11.4
Lost packet ratio: 0 %
```

----结束

配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin icmp
 test-type icmp
 destination-address ipv4 10.1.1.2
#
return
```

- RouterB 的配置文件

```
#
sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
#
return
```

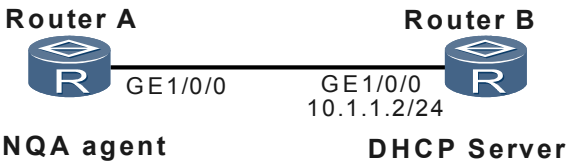
6.20.2 配置 DHCP 测试示例

通过配置 DHCP 测试可以检测到客户端和 DHCP 服务器的连接是否可以建立并可以检测到获取地址的速度。

组网需求

如图 6-4 所示，RouterB 作为 DHCP 服务器，使用 NQA DHCP 功能测试从 DHCP 服务器分配到 IP 地址的时间。

图 6-4 DHCP 测试组网图



配置思路

采用如下思路进行 DHCP 测试的配置：

1. RouterA 作为 NQA 客户端。
2. 在 RouterA 上配置并启动 DHCP 测试例，查看是否能够从 DHCP Server 建立连接并分配到 IP 地址。

数据准备

为完成此配置例，需准备如下的数据：

- DHCP Server 的主机地址
- 源接口
- 超时时间

操作步骤

步骤 1 配置 IP 地址（略）

步骤 2 使能 NQA 客户端，配置 DHCP 类型的 NQA 测试例

```
<RouterA> system-view
[RouterA] nqa test-instance admin dhcp
[RouterA-nqa-admin-dhcp] test-type dhcp
[RouterA-nqa-admin-dhcp] source-interface gigabitethernet 1/0/0
[RouterA-nqa-admin-dhcp] timeout 20
```

步骤 3 启动测试操作

```
[RouterA-nqa-admin-dhcp] start now
```

步骤 4 验证测试结果

```
[RouterA-nqa-admin-dhcp] display nqa results test-instance admin dhcp
NQA entry (admin, dhcp) :testflag is inactive ,testtype is dhcp
  1 . Test 1 result   The test is finished
   Send operation times: 3              Receive response times: 3
   Completion:success                   RTD OverThresholds number: 0
   Attempts number:1                    Drop operation number:0
   Disconnect operation number:0        Operation timeout number:0
   System busy operation number:0       Connection fail number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   Destination ip address:10.1.1.2
   Min/Max/Average Completion Time: 1018/1019/1018
   Sum/Square-Sum  Completion Time: 3055/3111009
   Last Good Probe Time: 2009-3-11 9:26:38.5
   Lost packet ratio: 0 %
```

----结束

配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address dhcp-alloc
#
nqa test-instance admin dhcp
 test-type dhcp
 timeout 20
 source-interface GigabitEthernet1/0/0
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
ip-pool 1
 network 10.1.1.0 mask 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
#
return
```

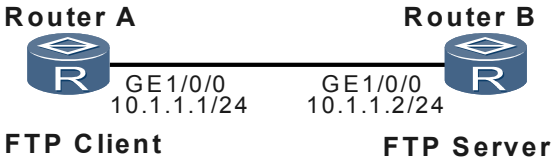
6.20.3 配置 FTP 下载速度测试示例

通过配置 FTP 下载速度测试可以检测到客户端从 FTP 服务器下载文件时的性能。

组网需求

如图 6-5 所示，RouterB 作为 FTP Server，登录 FTP 服务器的用户名为 user1，密码为 hello，要下载的文件名为 test.txt。

图 6-5 FTP 测试组网图



配置思路

为完成此配置例，需准备如下的数据：

1. RouterA 作为 NQA 客户端。
2. 在 RouterA 上配置并启动 FTP 测试例，使用 NQA FTP 功能测试是否可以和指定的 FTP 服务器建立连接，以及从 FTP 服务器得到一个文件的时间。

数据准备

为完成 FTP 下载速度测试，需准备如下数据：

- FTP 服务器的 IP 地址
- 进行测试的源 IP 地址
- FTP 用户名和密码
- FTP 测试操作文件

操作步骤

步骤 1 配置 RouterA 和 RouterB 的 IP 地址（略）

步骤 2 配置 RouterB 作为 FTP 服务器

```
<RouterB> system-view
[RouterB] ftp server enable
[RouterB] aaa
```

```
[RouterB-aaa] local-user user1 password cipher hello
[RouterB-aaa] local-user user1 service-type ftp
[RouterB-aaa] local-user user1 ftp-directory flash:/
[RouterB-aaa] quit
```

步骤 3 在 RouterA 上配置 FTP 类型的 NQA 测试例

```
<RouterA> system-view
[RouterA] nqa test-instance admin ftp
[RouterA-nqa-admin-ftp] test-type ftp
[RouterA-nqa-admin-ftp] destination-address ipv4 10.1.1.2
[RouterA-nqa-admin-ftp] source-address ipv4 10.1.1.1
[RouterA-nqa-admin-ftp] ftp-operation get
[RouterA-nqa-admin-ftp] ftp-username user1
[RouterA-nqa-admin-ftp] ftp-password hello
[RouterA-nqa-admin-ftp] ftp-filename test.txt
```

步骤 4 启动测试操作

```
[RouterA-nqa-admin-ftp] start now
```

步骤 5 验证测试结果

```
[RouterA-nqa-admin-ftp] display nqa results test-instance admin ftp
 NQA entry(admin, ftp) :testflag is inactive ,testtype is  ftp
  1 . Test 1 result   The test is finished
   SendProbe:1                              ResponseProb:1
   Completion :success                      RTD OverThresholds number: 0
   MessageBodyOctetsSum: 448                Stats errors number: 0
   Operation timeout number: 0              System busy operation number:0
   Drop operation number:0                  Disconnect operation number: 0
   CtrlConnTime Min/Max/Average: 438/438/438
   DataConnTime Min/Max/Average: 218/218/218
   SumTime Min/Max/Average: 656/656/656
   Average RTT:656
   Lost packet ratio:0 %
```

----结束

配置文件

- RouterA 的配置文件

```
#
sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin ftp
 test-type  ftp
 destination-address ipv4 10.1.1.2
 source-address ipv4 10.1.1.1
 ftp-filename test.txt
 ftp-username user1
 ftp-password hello
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 FTP server enable
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
#
aaa
 local-user user1 password cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
 local-user user1 service-type ftp
```

```
 local-user user1 ftp-directory flash:/
 #
return
```

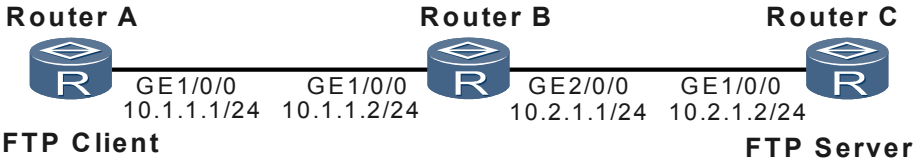
6.20.4 配置 FTP 上载速度测试示例

通过配置 FTP 下载速度测试可以检测到客户端上传文件到 FTP 服务器时的性能。

组网需求

如图 6-6 所示，测试向 FTP Server，即 RouterC 上载文件的速度。

图 6-6 FTP 测试组网图



配置思路

采用如下思路进行 FTP 上载速度的测试：

1. RouterA 作为 NQA 客户端和 FTP Client。在 RouterA 上配置并启动 FTP 测试例，使用 NQA FTP 功能测试是否可以和指定的 FTP 服务器建立连接，以及向 FTP 服务器上载一个文件的时间。
2. 登录 FTP 服务器的用户名为 user1，密码为 hello，构造大小为 10k 的文件上载。

数据准备

为完成此配置例，需准备如下的数据：

- FTP 服务器的 IP 地址
- 进行测试的 FTP 客户端源 IP 地址
- FTP 用户名和密码
- FTP 上载的文件大小

操作步骤

步骤 1 配置 RouterA、RouterB 和 RouterC 之间路由可达（略）

步骤 2 配置 RouterC 作为 FTP 服务器

```
<RouterC> system-view
[RouterC] ftp-server enable
[RouterC] aaa
[RouterC-aaa] local-user user1 password cipher hello
[RouterC-aaa] local-user user1 service-type ftp
[RouterC-aaa] local-user user1 ftp-directory flash:
[RouterC-aaa] quit
```

步骤 3 在 RouterA 上配置 FTP 类型的 NQA 测试例，构造一个大小为 10k 字节的文件上载

```
<RouterA> system-view
```

```
[RouterA] nqa test-instance admin ftp
[RouterA-nqa-admin-ftp] test-type ftp
[RouterA-nqa-admin-ftp] destination-address ipv4 10.2.1.2
[RouterA-nqa-admin-ftp] source-address ipv4 10.1.1.1
[RouterA-nqa-admin-ftp] ftp-operation put
[RouterA-nqa-admin-ftp] ftp-username user1
[RouterA-nqa-admin-ftp] ftp-password hello
[RouterA-nqa-admin-ftp] ftp-filesize 10
```

步骤 4 启动测试操作

```
[RouterA-nqa-admin-ftp] start now
```

步骤 5 验证测试结果

在 RouterA 上查看 NQA 测试结果。

```
[RouterA-nqa-admin-ftp] display nqa results test-instance admin ftp
 NQA entry(admin, ftp) :testflag is inactive ,testtype is  ftp
  1 . Test 1 result   The test is finished
   SendProbe:1                              ResponseProb:1
   Completion :success                      RTD OverThresholds number: 0
   MessageBodyOctetsSum: 10240              Stats errors number: 0
   Operation timeout number: 0              System busy operation number:0
   Drop operation number:0                  Disconnect operation number: 0
   CtrlConnTime Min/Max/Average: 657/657/657
   DataConnTime Min/Max/Average: 500/500/500
   SumTime Min/Max/Average: 1157/1157/1157
   Average RTT:656
   Lost packet ratio:0 %
```

在 RouterC 上可以看到增加了一个名为“nqa-ftp-test.txt”的文件。（以下只显示部分文件）

```
<RouterC> dir
Directory of flash:/
   0   -rw-     331  Jul 06 2007 18:34:34   private-data.txt
   1   -rw-   10240  Jul 06 2007 18:37:06   nqa-ftp-test.txt
2540 KB total (1536 KB free)
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin ftp
 test-type  ftp
 destination-address ipv4 10.2.1.2
 source-address ipv4 10.1.1.1
 ftp-operation put
 ftp-filesize 10
 ftp-username user1
 ftp-password hello
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
```

```
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
  ip address 10.2.1.1 255.255.255.0
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
 FTP server enable
#
interface GigabitEthernet1/0/0
 ip address 10.2.1.2 255.255.255.0
#
aaa
 local-user user1 password cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
 local-user user1 service-type ftp
 local-user user1 ftp-directory flash:
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

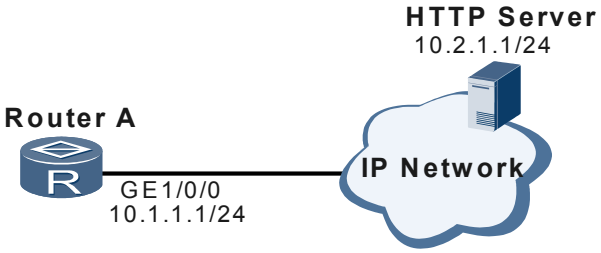
6.20.5 配置 HTTP 测试示例

通过 HTTP 测试可以检测到客户端和 HTTP 服务器交互时的各个阶段的性能。

组网需求

如图 6-7 所示。RouterA 通过广域网和 HTTP Server 相连。

图 6-7 HTTP 测试组网图



配置思路

采用如下思路进行 HTTP 响应速度的测试：

1. RouterA 做为 NQA 客户端。
2. 在 RouterA 上配置并启动 HTTP 测试例，使用 NQA HTTP 功能测试是否可以和指定的 HTTP 服务器建立连接，以及它们之间传输一个文件的时间。

数据准备

为完成此配置例，需准备如下的数据：

- HTTP Server 的主机地址
- HTTP 测试操作类型

操作步骤

步骤 1 配置 IP 地址（略）

步骤 2 使能 NQA 客户端，配置 HTTP 类型的 NQA 测试例

```
<RouterA> system-view
[RouterA] nqa test-instance admin http
[RouterA-nqa-admin-http] test-type http
[RouterA-nqa-admin-http] destination-address ipv4 10.2.1.1
[RouterA-nqa-admin-http] http-operation get
[RouterA-nqa-admin-http] http-url www.huawei.com
```

步骤 3 启动测试操作

```
[RouterA-nqa-admin-http] start now
```

步骤 4 验证测试结果

```
[RouterA-nqa-admin-http] display nqa results test-instance admin http
 NQA entry(admin, http) :testflag is inactive ,testtype is http
  Test 1 result   The test is finished
    SendProbe:3                          ResponseProbe:3
    Completion:success                   RTD OverThresholdsnumber: 0
    MessageBodyOctetsSum: 411            TargetAddress: 10.2.1.1
    DNSQueryError number: 0              HTTPError number: 0
    TcpConnError number : 0              System busy operation number:0
    DNSRTT Sum/Min/Max:0/0/0             TCPConnectRTT Sum/Min/Max: 4/1/2
    TransactionRTT Sum/Min/Max: 3/1/1
    RTT Sum/Min/Max/Avg: 7/2/3/2
    DNSServerTimeout:0  TCPConnectTimeout:0  TransactionTimeout: 0
    Lost packet ratio:0%
```

----结束

配置文件

RouterA 的配置文件

```
#
sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin http
 test-type http
 destination-address ipv4 10.2.1.1
 http-url www.huawei.com
#
return
```

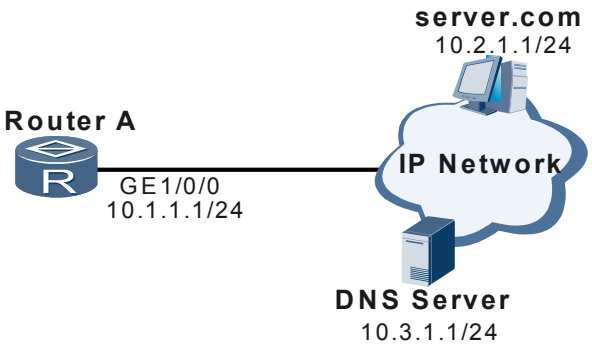
6.20.6 配置 DNS 测试示例

通过 DNS 测试可以检测到客户端和 DNS 服务器交互时的性能参数。

组网需求

如图 6-8 所示，路由器 RouterA 作为 DNS Client 端，通过域名（server.com）访问 IP 地址为 10.2.1.1/24 的主机。

图 6-8 DNS 测试组网图



配置思路

采用如下思路进行 DNS 解析速度的测试：

1. RouterA 作为 NQA 客户端。
2. 在 RouterA 上配置并启动 DNS 测试例，测试是否可以和指定的 DNS 服务器建立连接，以及 DNS 地址解析的响应速度。

数据准备

为完成此配置例，需准备如下的数据：

- DNS Server 的 IP 地址
- 要访问的主机名

操作步骤

步骤 1 配置 RouterA、DNS Server 及所要访问的主机之间网络层可达（略）

步骤 2 配置 DNS 类型的 NQA 测试例

```
<RouterA> system-view
[RouterA] dns resolve
[RouterA] dns server 10.3.1.1
[RouterA] nqa test-instanc admin dns
[RouterA-nqa-admin-dns] test-type dns
[RouterA-nqa-admin-dns] dns-server ipv4 10.3.1.1
[RouterA-nqa-admin-dns] destination-address url server.com
```

步骤 3 启动测试操作

```
[RouterA-nqa-admin-dns] start now
```

步骤 4 验证测试结果

```
[RouterA-nqa-admin-dns] display nqa results test-instance admin dns
 NQA entry(admin, dns) :testflag is inactive ,testtype is dns
  1 . Test 1 result   The test is finished
    Send operation times: 1              Receive response times: 1
    Completion:success                   RTD OverThresholds number: 0
    Attempts number:1                    Drop operation number:0
    Disconnect operation number:0        Operation timeout number:0
    System busy operation number:0       Connection fail number:0
    Operation sequence errors number:0   RTT Stats errors number:0
    Destination ip address: 10.3.1.1
```

```
  Min/Max/Average Completion Time: 1/1/1
  Sum/Square-Sum  Completion Time: 1/1
  Last Good Probe Time: 2007-7-3 10:52:5.7
  Lost packet ratio: 0 %
```

----结束

配置文件

RouterA 的配置文件

```
#
 sysname RouterA
#
 dns resolve
 dns server 10.3.1.1
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin dns
 test-type dns
 destination-address url server.com
 dns-server ipv4 10.3.1.1
#
 ip route-static 10.3.1.0 255.255.255.0 10.1.1.2
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

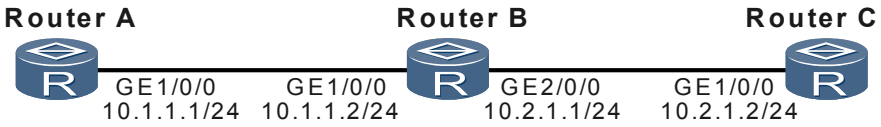
6.20.7 配置 Traceroute 测试示例

通过配置 Traceroute 测试可以检测到报文传输过程中客户端和报文传输路径中的设备的连通性。

组网需求

如图 6-9 所示，在 RouterA 上对 RouterC 接口 GE1/0/0 的 IP 地址进行 Traceroute 测试。

图 6-9 Traceroute 测试组网图



配置思路

采用如下思路进行 Traceroute 测试：

1. RouterA 作为 NQA 客户端。
2. 在 RouterA 上配置并启动 Traceroute 测试例，测试到 RouterC 的每一跳统计信息。

数据准备

为完成此配置例，需准备如下的数据：

- Traceroute 测试的目的地址。

操作步骤

步骤 1 配置 RouterA、RouterB 和 RouterC 之间路由可达（略）

步骤 2 配置在 RouterA 上 Traceroute 类型的 NQA 测试例，目的地址为 10.2.1.2

```
<RouterA> system-view
[RouterA] nqa test-instance admin trace
[RouterA-nqa-admin-trace] test-type trace
[RouterA-nqa-admin-trace] destination-address ipv4 10.2.1.2
```

步骤 3 启动测试操作

```
[RouterA-nqa-admin-trace] start now
```

步骤 4 验证测试结果

在 RouterA 上查看 NQA 测试结果。

```
[RouterA-nqa-admin-trace] display nqa results test-instance admin trace
 NQA entry(admin, trace) :testflag is inactive ,testtype is trace
  1 . Test 1 result   The test is finished
   Completion:success                  Attempts number:1
   Disconnect operation number:0       Operation timeout number:0
   System busy operation number:0      Connection fail number:0
   Operation sequence errors number:0  RTT Stats errors number:0
   Drop operation number:0
   Last good path Time:2009-3-28 10:52:39.9
   1 . Hop 1
    Send operation times: 3             Receive response times: 3
    Min/Max/Average Completion Time: 1/1/1
    Sum/Square-Sum  Completion Time: 3/3
    RTD OverThresholds number: 0
    Last Good Probe Time: 2009-3-28 10:52:39.9
    Destination ip address:10.1.1.2
    Lost packet ratio: 0 %
   2 . Hop 2
    Send operation times: 3             Receive response times: 3
    Min/Max/Average Completion Time: 1/1/1
    Sum/Square-Sum  Completion Time: 3/3
    RTD OverThresholds number: 0
    Last Good Probe Time: 2009-3-28 10:52:39.9
    Destination ip address:10.2.1.2
    Lost packet ratio: 0 %
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin trace
 test-type  trace
 destination-address ipv4 10.2.1.2
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- RouterB 的配置文件

```
#
```

```
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.2.1.1 255.255.255.0
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 ip address 10.2.1.2 255.255.255.0
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

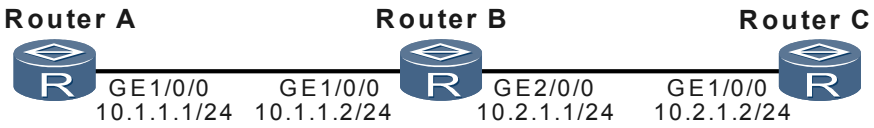
6.20.8 配置 SNMP Query 测试示例

通过配置 SNMP Query 测试可以检测到客户端和网管之间通过 SNMP 通信时的性能。

组网需求

如图 6-10 所示。RouterA 和 RouterC 使能 SNMP Agent，使用 NQA SNMP Query 功能测试从 RouterA 发出一个 SNMP 协议查询报文到收到响应报文所用的时间。

图 6-10 SNMP Query 测试组网图



配置思路

采用如下思路进行 SNMP Query 测试：

1. RouterA 作为 NQA 客户端。
2. 在 RouterA 上使能 SNMP Agent。
3. 在 RouterA 上创建并启动 SNMP Query 类型的测试例。
4. 在 RouterC 上使能 SNMP Agent。

数据准备

为完成此配置例，需准备如下的数据：

- SNMP Agent 的主机地址

操作步骤

步骤 1 配置 RouterA、RouterB 和 RouterC 之间路由可达（略）

步骤 2 在 RouterC 上启动 SNMP Agent 功能

```
<RouterC> system-view
[RouterC] snmp-agent
```

步骤 3 在 RouterA 上启动 SNMP Agent 功能

```
<RouterA> system-view
[RouterA] snmp-agent
[RouterA] quit
```

步骤 4 在 RouterA 上创建 SNMP 类型的测试例

```
<RouterA> system-view
[RouterA] nqa test-instance admin snmp
[RouterA-nqa-admin-snmp] test-type snmp
[RouterA-nqa-admin-snmp] destination-address ipv4 10.2.1.2
```

步骤 5 启动测试操作

```
[RouterA-nqa-admin-snmp] start now
```

步骤 6 验证测试结果

```
[RouterA-nqa-admin-snmp] display nqa results test-instance admin snmp
 NQA entry(admin, snmp) :testflag is inactive ,testtype is snmp
  1 . Test 1 result   The test is finished
   Send operation times: 3                 Receive response times: 3
   Completion:success                      RTD OverThresholds number: 0
   Attempts number:0                       Drop operation number:0
   Disconnect operation number:0           Operation timeout number:0
   System busy operation number:0          Connection fail number:0
   Operation sequence errors number:0      RTT Stats errors number:0
   Destination ip address:10.2.1.2
   Min/Max/Average Completion Time: 63/172/109
   Sum/Square-Sum  Completion Time: 329/42389
   Last Good Probe Time: 2006-8-5 15:33:49.1
   Lost packet ratio: 0 %
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin snmp
 test-type snmp
 destination-address ipv4 10.2.1.2
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
 snmp-agent
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
ip address 10.2.1.1 255.255.255.0
#
```

```
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 ip address 10.2.1.2 255.255.255.0
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
 snmp-agent
 snmp-agent local-engineid 000007DB7F00000100006294
#
return
```

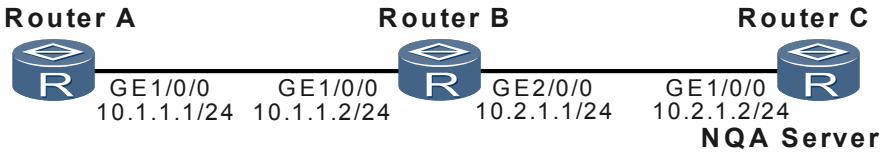
6.20.9 配置 TCP 测试示例

通过配置 TCP 测试可以检测到客户端和服务器端之间 TCP 的连通性。

组网需求

如图 6-11 所示。使用 NQA TCP Private 功能测试 RouterA 到 RouterC 之间建立 TCP 连接的时间。

图 6-11 TCP 测试组网图



配置思路

采用如下思路进行 TCP 测试的配置：

1. RouterA 做为 NQA 客户端，RouterC 做为 NQA 服务器端。
2. 在 NQA 服务器上配置监听端口号，在 NQA 客户端配置 TCP 类型的 NQA 测试例。

数据准备

为完成此配置例，需准备如下的数据：

- 服务器主机地址
- 服务器端 TCP 服务的监听端口号

操作步骤

步骤 1 配置 RouterA、RouterB 和 RouterC 之间路由可达（略）

步骤 2 在 RouterC 上配置 NQA 服务器

配置 NQA 服务器 TCP 连接监听的 IP 地址和端口号。

```
<RouterC> system-view
```

```
[RouterC] nqa-server tcpconnect 10.2.1.2 9000
```

步骤 3 配置 RouterA

使能 NQA 客户端，配置 TCP 类型的测试例。

```
<RouterA> system-view
[RouterA] nqa test-instance admin tcp
[RouterA-nqa-admin-tcp] test-type tcp
[RouterA-nqa-admin-tcp] destination-address ipv4 10.2.1.2
[RouterA-nqa-admin-tcp] destination-port 9000
```

步骤 4 启动测试

```
[RouterA-nqa-admin-tcp] start now
```

步骤 5 验证测试结果

```
[RouterA-nqa-admin-tcp] display nqa results test-instance admin tcp
 NQA entry(admin, tcp) :testflag is inactive ,testtype is tcp
  1 . Test 1 result   The test is finished
   Send operation times: 3                Receive response times: 3
   Completion:success                      RTD OverThresholds number: 0
   Attempts number:1                       Drop operation number:0
   Disconnect operation number:0         Operation timeout number:0
   System busy operation number:0        Connection fail number:0
   Operation sequence errors number:0  RTT Stats errors number:0
   Destination ip address:10.2.1.2
   Min/Max/Average Completion Time: 46/63/52
   Sum/Square-Sum  Completion Time: 156/8294
   Last Good Probe Time: 2006-8-5 15:53:17.8
   Lost packet ratio: 0 %
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
  ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin tcp
 test-type tcp
 destination-address ipv4 10.2.1.2
 destination-port 9000
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.2.1.1 255.255.255.0
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
```

```
interface GigabitEthernet1/0/0
 ip address 10.2.1.2 255.255.255.0
#
 nqa-server tcpconnect 10.2.1.2 9000
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

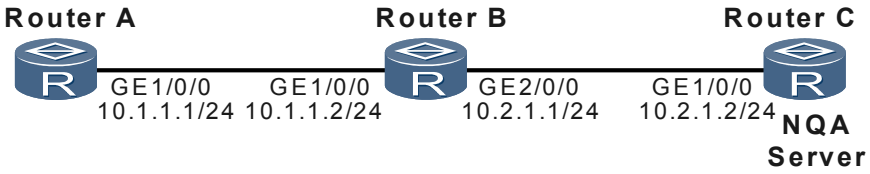
6.20.10 配置 UDP 测试示例

通过配置 UDP 测试可以检测到客户端和服务器端之间 UDP 的连通性。

组网需求

如图 6-12 所示。使用 NQA UDP Public 功能测试 RouterA 与 RouterC 之间 UDP 协议报文的往返时间。

图 6-12 UDP 测试组网图



配置思路

采用如下思路进行 UDP 测试的配置：

1. RouterA 做为 NQA 客户端，RouterC 做为 NQA 服务器端。
2. 在 NQA 服务器上配置监听端口号，在 NQA 客户端配置 UDP 类型的 NQA 测试例。

数据准备

为完成此配置例，需准备如下的数据：

- 服务器端主机地址
- 服务器端 UDP 服务的监听端口号

操作步骤

步骤 1 配置 RouterA、RouterB 和 RouterC 之间路由可达（略）

步骤 2 在 RouterC 上配置 NQA 服务器

配置 NQA 服务器 UDP 监听的 IP 地址和端口号。

```
<RouterC> system-view
[RouterC] nqa-server udpecho 10.2.1.2 6000
```

步骤 3 配置 RouterA

使能 NQA 客户端，配置 UDP 类型的测试例。

```
<RouterA> system-view
[RouterA] nqa test-instance admin udp
[RouterA-nqa-admin-udp] test-type udp
[RouterA-nqa-admin-udp] destination-address ipv4 10.2.1.2
[RouterA-nqa-admin-udp] destination-port 6000
```

步骤 4 启动测试

```
[RouterA-nqa-admin-udp] start now
```

步骤 5 验证测试结果

```
[RouterA-nqa-admin-udp] display nqa results test-instance admin udp
 NQA entry(admin, udp) :testflag is inactive ,testtype is udp
  1 . Test 1 result   The test is finished
   Send operation times: 3              Receive response times: 3
   Completion:success                   RTD OverThresholds number: 0
   Attempts number:1                    Drop operation number:0
   Disconnect operation number:0        Operation timeout number:0
   System busy operation number:0       Connection fail number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   Destination ip address:10.2.1.2
   Min/Max/Average Completion Time: 32/109/67
   Sum/Square-Sum  Completion Time: 203/16749
   Last Good Probe Time: 2006-8-5 16:9:21.6
   Lost packet ratio: 0 %
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin udp
 test-type udp
 destination-address ipv4 10.2.1.2
 destination-port 6000
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.2.1.1 255.255.255.0
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 ip address 10.2.1.2 255.255.255.0
#
 nqa-server udpecho 10.2.1.2 6000
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
```

```
#
return
```

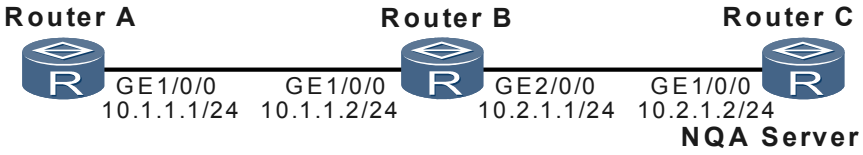
6.20.11 配置 Jitter 测试示例

通过配置 Jitter 测试可以检测到网络中抖动情况。

组网需求

如图 6-13 所示。使用 NQA Jitter 功能测试 RouterA 与 RouterC 之间传送报文的抖动时间。

图 6-13 Jitter 测试组网图



配置思路

采用如下思路进行 Jitter 测试的配置：

1. RouterA 做为 NQA 客户端，RouterC 做为 NQA 服务器端。
2. 在 NQA 服务器上配置监听服务类型和监听端口号。
3. 在 NQA 客户端配置 Jitter 类型的 NQA 测试例。

数据准备

为完成此配置例，需准备如下的数据：

- 服务器端的主机地址
- 服务器端 UDP 服务的监听端口号

操作步骤

步骤 1 配置 RouterA、RouterB 和 RouterC 之间路由可达（略）

步骤 2 在 RouterC 上配置 NQA 服务器

配置 NQA 服务器 UDP 监听的 IP 地址和端口号。

```
<RouterC> system-view
[RouterC] nqa-server udpecho 10.2.1.2 9000
```

步骤 3 配置 RouterA

使能 NQA 客户端，配置 Jitter 类型的 NQA 测试例。

```
<RouterA> system-view
[RouterA] nqa test-instance admin jitter
[RouterA-nqa-admin-jitter] test-type jitter
[RouterA-nqa-admin-jitter] destination-address ipv4 10.2.1.2
```

```
[RouterA-nqa-admin-jitter] destination-port 9000
```

步骤 4 启动测试操作

```
[RouterA-nqa-admin-jitter] start now
```

步骤 5 验证测试结果

```
[RouterA-nqa-admin-jitter] display nqa results test-instance admin jitter
NQA entry(admin, jitter) :testflag is inactive ,testtype is jitter
  1 . Test 1 result   The test is finished
   SendProbe:60                          ResponseProbe:60
   Completion:success                    RTD OverThresholds number:0
   OWD OverThresholds SD number:0        OWD OverThresholds DS number:0
   Min/Max/Avg/Sum RTT:1/4/1/63          RTT  Square Sum:75
   NumOfRTT:60                           Drop operation number:0
   Operation sequence errors number:0    RTT Stats errors number:0
   System busy operation number:0        Operation timeout number:0
   Min Positive SD:1                     Min Positive DS:1
   Max Positive SD:1                     Max Positive DS:3
   Positive SD Number:15                 Positive DS Number:14
   Positive SD Sum:15                    Positive DS Sum:16
   Positive SD Square Sum:15             Positive DS Square Sum:22
   Min Negative SD:1                     Min Negative DS:1
   Max Negative SD:1                     Max Negative DS:4
   Negative SD Number:16                 Negative DS Number:12
   Negative SD Sum:16                    Negative DS Sum:15
   Negative SD Square Sum:16             Negative DS Square Sum:27
   Min Delay SD:0                        Min Delay DS:0
   Max Delay SD:2                        Max Delay DS:1
   Delay SD Square Sum:4                 Delay DS Square Sum:1
   Packet Loss SD:0                      Packet Loss DS:0
   Packet Loss Unknown:0                 Average of Jitter:1
   Average of Jitter SD:1                Average of Jitter DS:1
   jitter out value:0.0322917            jitter in value:0.0322917
   NumberOfOWD:60                        Packet Loss Ratio: 0%
   OWD SD Sum:2                          OWD DS Sum:1
   ICPIF value: 0                        MOS-CQ value: 0
   TimeStamp unit: ms                    Packet Rewrite Number: 0
   Packet Rewrite Ratio: 0%              Packet Disorder Number: 0
   Packet Disorder Ratio: 0%             Fragment-disorder Number: 0
   Fragment-disorder Ratio: 0%
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
nqa test-instance admin jitter
 test-type jitter
 destination-address ipv4 10.2.1.2
 destination-port 9000
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
```

```
#
interface GigabitEthernet2/0/0
 ip address 10.2.1.1 255.255.255.0
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 ip address 10.2.1.2 255.255.255.0
#
  nqa-server udpecho 10.2.1.2 9000
#
 ip route-static 10.1.1.0 255.255.255.0 10.2.1.1
#
return
```

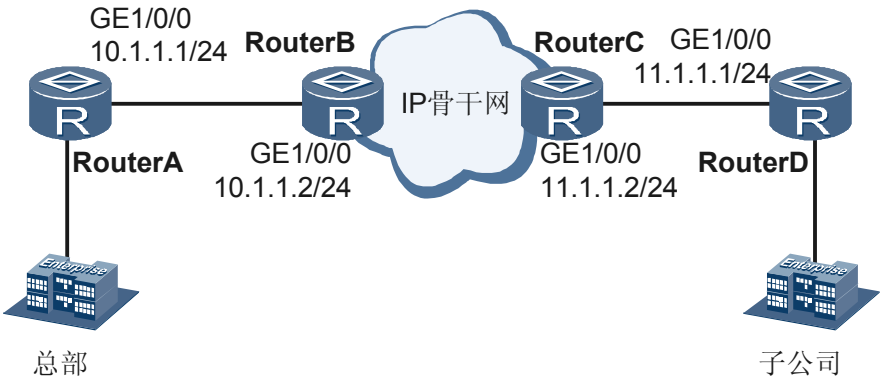
6.20.12 配置 NQA 检测 VoIP 业务抖动示例

本示例通过 UDP jitter 测试检测 VoIP 业务抖动示例。

组网需求

如图 6-14 所示，总部和子公司之间经常要通过 VoIP 进行电话会议，要求双向时延小于250ms，抖动小于 20ms。可以使用 NQA 的 UPD jitter 测试模拟 VoIP 业务。

图 6-14 配置 NQA 检测 VoIP 业务抖动组网图



配置思路

采用如下思路配置 NQA 检测 VoIP 业务抖动：

1. 在 RouterD 上配置 UDP jitter 测试例。RouterD 为 NQA 客户端，RouterA 为 NQA 服务器端。
2. 在 RouterD 上启动测试例。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA 和 RouterD 的 IP 地址
- 模拟 VoIP 业务的编码类型

操作步骤

步骤 1 配置 NQA 服务器端 RouterA

```
<RouterA> system-view
[RouterA] nqa-server udpecho 10.1.1.1 180
```

步骤 2 配置 NQA 客户端 RouterD

1. 配置 UDP Jitter 测试例的报文版本号

```
<RouterD> system-view
[RouterD] nqa-jitter tag-version 2
```

2. 创建 UDP jitter 测试例，并配置目的地址为 RouterA 的 IP 地址

```
[RouterD] nqa test-instance admin udpjitter
[RouterD-nqa-admin-udpjitter] test-type jitter
[RouterD-nqa-admin-udpjitter] destination-address ipv4 10.1.1.1
[RouterD-nqa-admin-udpjitter] destination-port 180
```

3. 配置模拟 VoIP 业务的编码类型

```
[RouterD-nqa-admin-udpjitter] jitter-codec g711a
```

步骤 3 立即启动测试

```
[RouterD-nqa-admin-udpjitter] start now
```

步骤 4 验证测试结果，可以看到双向时延小于 250ms，抖动小于 20ms。

```
[RouterD-nqa-admin-udpjitter] display nqa results test-instance admin udpjitter
NQA entry(admin, udpjitter) :testflag is active ,testtype is jitter
1 . Test 1 result   The test is finished
   SendProbe:1000                        ResponseProbe:1000
   Completion:success                    RTD OverThresholds number:0
   OWD OverThresholds SD number:0        OWD OverThresholds DS number:0
   Min/Max/Avg/Sum RTT:10/38/13/12963    RTT  Square Sum:171925
   NumOfRTT:1000                         Drop operation number:0
   Operation sequence errors number:0    RTT Stats errors number:0
   System busy operation number:0        Operation timeout number:0
   Min Positive SD:1                     Min Positive DS:1
   Max Positive SD:16                    Max Positive DS:27
   Positive SD Number:288                Positive DS Number:287
   Positive SD Sum:427                   Positive DS Sum:485
   Positive SD Square Sum:1317           Positive DS Square Sum:2455
   Min Negative SD:1                     Min Negative DS:1
   Max Negative SD:16                    Max Negative DS:26
   Negative SD Number:292                Negative DS Number:285
   Negative SD Sum:429                   Negative DS Sum:486
   Negative SD Square Sum:1235           Negative DS Square Sum:2714
   Min Delay SD:5                        Min Delay DS:4
   Avg Delay SD:6                        Avg Delay DS:5
   Max Delay SD:19                       Max Delay DS:18
   Delay SD Square Sum:39901             Delay DS Square Sum:33856
   Packet Loss SD:0                      Packet Loss DS:0
   Packet Loss Unknown:0                 Average of Jitter:1
   Average of Jitter SD:1                Average of Jitter DS:1
   jitter out value:0.0535000            jitter in value:0.0606875
   NumberOfOWD:1000                      Packet Loss Ratio: 0%
   OWD SD Sum:6239                       OWD DS Sum:5724
   ICPIF value: 0                        MOS-CQ value: 438
   TimeStamp unit: ms                    Packet Rewrite Number: 0
   Packet Rewrite Ratio: 0%              Packet Disorder Number: 0
   Packet Disorder Ratio: 0%             Fragment-disorder Number: 0
   Fragment-disorder Ratio: 0%
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
 nqa-server udpecho 10.1.1.1 180
#
return
```

- RouterD 的配置文件

```
#
 sysname RouterD
#
interface GigabitEthernet1/0/0
 ip address 11.1.1.1 255.255.255.0
#
nqa-jitter tag-version 2
#
nqa test-instance admin udpjitter
 test-type jitter
 destination-address ipv4 10.1.1.1
 destination-port 180
 jitter-codec g711a
#
return
```

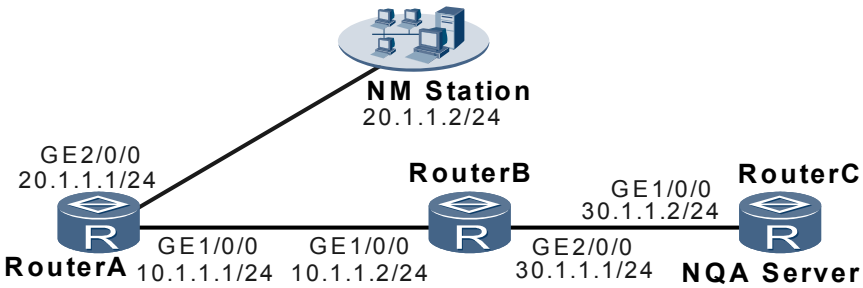
6.20.13 配置向网管端发送 NQA 阈值告警示例

通过向网管端发送 NQA 阈值告警，网络管理人员可以清晰的了解到设备端发生的情况。

组网需求

如图 6-15 所示在配置 Jitter 测试例时，配置阈值并启动告警功能。启动 Jitter 测试例，在测试结束后，当从 RouterA 到 RouterC 或从 RouterC 到 RouteA 的测试报文中，有超过设定的单向传输告警阈值，或测试报文的往返时间超过设定的双向传输阈值时，RouterA 会向网管端发送一次 Trap 消息。通过 NM Station 接收到的 Trap 消息，网络管理人员可以清晰的看到产生告警的原因。

图 6-15 配置 NQA 阈值组网图



说明

关于时钟同步介绍请参见《Huawei AR3200 系列企业路由器 特性描述 系统管理》的“NTP”。

配置思路

采用如下思路进行阈值的配置：配置一个 Jitter 测试例

1. 配置 NQA 阈值功能
2. 开启 Trap 发送开关
3. 配置向网管端发送 Trap

数据准备

为完成此配置例，需准备如下的数据：

- 服务器端的主机地址及端口号
- 监听服务类型及监听端口号
- RTD 阈值和 OWD 阈值
- 网管端地址

操作步骤

步骤 1 配置 RouterA、RouterB 和 RouterC 之间路由可达（略）

步骤 2 配置一个 Jitter 测试例

在 RouterC 上配置 NQA 服务器 UDP 监听的 IP 地址和端口号。

```
<RouterC> system-view
[RouterC] nqa-server udpecho 30.1.1.2 9000
```

在 RouterA 上使能 NQA 客户端，配置 Jitter 类型的 NQA 测试例。

```
<RouterA> system-view
[RouterA] nqa test-instance admin jitter
[RouterA-nqa-admin-jitter] test-type jitter
[RouterA-nqa-admin-jitter] destination-address ipv4 30.1.1.2
[RouterA-nqa-admin-jitter] destination-port 9000
```

步骤 3 配置 NQA 阈值功能

在 RouterA 上配置 RTD 阈值。

```
[RouterA-nqa-admin-jitter] threshold rtd 20
```

在 RouterA 上配置 OWD-DS 阈值。

```
[RouterA-nqa-admin-jitter] threshold owd-ds 100
```

在 RouterA 上配置 OWD-SD 阈值。

```
[RouterA-nqa-admin-jitter] threshold owd-sd 100
```

步骤 4 开启发送 Trap 的功能

```
[RouterA-nqa-test-jitter] send-trap owd-ds owd-sd rtd
[RouterA-nqa-test-jitter] quit
```

步骤 5 配置向网管发送 Trap 的功能

```
[RouterA] snmp-agent target-host trap-paramsname trapnms2 v2c securityname nsmsecurity
[RouterA] snmp-agent target-host trap-hostname nsm2 address 20.1.1.2 trap-paramsname trapnms2
```

步骤 6 启动测试操作

```
[RouterA] nqa test-instance admin jitter
[RouterA-nqa-admin-jitter] start now
```

```
[RouterA-nqa-admin-jitter] quit
[RouterA] quit
```

步骤 7 检查配置结果

显示各路由器的 NQA 测试结果信息。

```
<RouterA> display nqa result
 NQA entry(test, jitter) :testflag is inactive ,testtype is jitter
  1 . Test 1 result   The test is finished
   SendProbe:60                          ResponseProbe:60
   Completion:success                    RTD OverThresholds number:0
   OWD OverThresholds SD number:0        OWD OverThresholds DS number:0
   Min/Max/Avg/Sum RTT:1/1/1/60          RTT  Square Sum:60
   NumOfRTT:60                           Drop operation number:0
   Operation sequence errors number:0    RTT Stats errors number:0
   System busy operation number:0        Operation timeout number:0
   Min Positive SD:0                     Min Positive DS:1
   Max Positive SD:0                     Max Positive DS:1
   Positive SD Number:0                  Positive DS Number:5
   Positive SD Sum:0                     Positive DS Sum:5
   Positive SD Square Sum:0              Positive DS Square Sum:5
   Min Negative SD:0                     Min Negative DS:1
   Max Negative SD:0                     Max Negative DS:1
   Negative SD Number:0                  Negative DS Number:6
   Negative SD Sum:0                     Negative DS Sum:6
   Negative SD Square Sum:0              Negative DS Square Sum:6
   Min Delay SD:0                        Min Delay DS:0
   Max Delay SD:0                        Max Delay DS:0
   Delay SD Square Sum:0                 Delay DS Square Sum:0
   Packet Loss SD:0                      Packet Loss DS:0
   Packet Loss Unknown:0                 Average of Jitter:1
   Average of Jitter SD:0                Average of Jitter DS:1
   jitter out value:0.0000000            jitter in value:0.0114583
   NumberOfOWD:60                        Packet Loss Ratio: 0%
   OWD SD Sum:0                          OWD DS Sum:0
   ICPIF value: 0                        MOS-CQ value: 0
```

在告警缓冲区检查是否产生 Trap 消息。

```
<RouterA> display trapbuffer
Trapping Buffer Configuration and contents:enabled
allowed max buffer size : 1024

actual buffer size : 256
channel number : 3 , channel name : trapbuffer
dropped messages : 0
overwritten messages : 2550
current messages : 256
#Jul  9 00:28:34 2009 Huawei  NQA/4/RTDTHRESHOLD:OID 1.3.6.1.4.1.2011.5.25.111.6.16 NQA entry RTD
over threshold. (OwnerIndex=admin, TestName=jitter)
#Jul  9 00:28:34 2009 Huawei NQA/4/SDTHRESHOLD:OID 1.3.6.1.4.1.2011.5.25.111.6.17 NQA entry OWD-SD
over threshold. (OwnerIndex=admin, TestName=jitter)
#Jul  9 00:28:34 2009 Huawei  NQA/4/DSTHRESHOLD:OID 1.3.6.1.4.1.2011.5.25.111.6.
18 NQA entry OWD-DS over threshold. (OwnerIndex=admin, TestName=jitter)
```

在网管端查看是否可以正确接收到 Trap 消息。(略)

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
```

```
#
interface GigabitEthernet2/0/0
 ip address 20.1.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
nqa test-instance test jitter
 test-type jitter
 destination-address ipv4 30.1.1.2
 destination-port 9000
 threshold rtd 20
 threshold owd-sd 100
 threshold owd-ds 100
 send-trap rtd
 send-trap owd-sd
 send-trap owd-ds
#
 snmp-agent
 snmp-agent local-engineid 000007DB7F00000100007B29
 snmp-agent sys-info version v2c
 snmp-agent target-host trap-hostname nsm2 address 20.1.1.2 udp-port 162 trap-paramsname
trapnms2
 snmp-agent target-host trap-paramsname trapnms2 v2c securityname nsmsecurity
public v2c
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 30.1.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.1
  network 10.1.1.0 0.0.0.255
  network 30.1.1.0 0.0.0.255
#
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 ip address 30.1.1.2 255.255.255.0
#
  nqa-server udpecho 30.1.1.2 9000
#
ospf 1
 area 0.0.0.1
  network 30.1.1.0 0.0.0.255
#
return
```

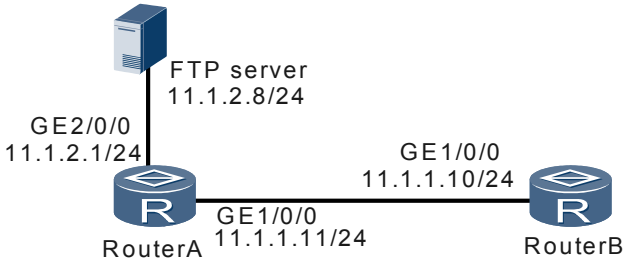
6.20.14 配置测试结果发送到 FTP 服务器示例

通过配置 FTP 方式保存测试结果到 FTP 服务器，可以最大程度的保存测试结果。

组网需求

如图 6-16 所示，RouterA 作为客户端进行 ICMP 测试，测试的结果通过 FTP 发送到 FTP Server。

图 6-16 测试结果发送到 FTP 服务器组网图



配置思路

本例中采用的配置思路如下。

1. 配置连接 FTP 服务器需要的参数。
2. 使能通过 FTP 保存测试结果的功能。
3. 配置 FTP 保存测试结果的条数。
4. 配置 FTP 保存测试结果的时间。
5. 配置发送
6. 启动测试例。
7. 检查配置结果。

数据准备

本例中需要准备的数据如下。

- 登录 FTP 服务器所需的用户名和密码
- FTP 保存测试结果的条数
- 配置 FTP 保存测试结果的时间

操作步骤

步骤 1 配置连接 FTP 服务器需要的参数。

配置连接 FTP 服务器的地址。

```
<RouterA> system-view
[RouterA] nqa-ftp-record ip-address 11.1.2.8
```

配置连接 FTP 服务器所需的用户名。

```
[RouterA] nqa-ftp-record username ftp
[RouterA] nqa-ftp-record password ftp
```

配置测试结果保存的文件名。

```
[RouterA] nqa-ftp-record filename icmp
```

步骤 2 配置通过 FTP 保存测试结果到文件的条数。

```
[RouterA] nqa-ftp-record item-num 10010
```

步骤 3 配置通过 FTP 保存测试结果到文件的时间。

```
[RouterA] nqa-ftp-record time 2
```

步骤 4 配置 FTP 传送成功向网管端发送 Trap

```
[RouterA] nqa-ftp-record trap-enable
```

步骤 5 在 RouterA 使能通过 FTP 保存 NQA 测试结果功能。

```
<RouterA> system-view
[RouterA] nqa-ftp-record enable
```

步骤 6 启动测试例

```
[RouterA] nqa test-instance admin icmp
[RouterA-admin-icmp] start now
```

步骤 7 检查配置结果

显示各路由器的 NQA 测试结果信息。

```
<RouterA> display nqa-ftp-record configuration
---------------NQA FTP SAVE RECORD CONFIGURATION---------------
   FUNCTION: ENABLE    TRAP: ENABLE
   IP-ADDRESS:11.1.1.8
   VPN-INSTANCE:
   USERNAME:ftp
   PASSWORD:ftp
   FILENAME:icmp
   ITEM-NUM:10010
   TIME:2
   LAST FINISHED FILENAME:icmp20080605-150350.txt
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 11.1.1.11 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 11.1.2.1 255.255.255.0
#
interface NULL0
#
aaa
 authentication-scheme default
 #
 authorization-scheme default
 #
 accounting-scheme default
 #
 domain default
#
nqa-ftp-record enable
nqa-ftp-record trap-enable
nqa-ftp-record ip-address 11.1.1.8
nqa-ftp-record username ftp
nqa-ftp-record password ftp
nqa-ftp-record filename icmp
```

```
nqa-ftp-record item-num 10010
nqa-ftp-record time 2
nqa test-instance admin icmp
test-type icmp
 destination-address ipv4 11.1.1.10
 frequency 5
#
 snmp-agent
 snmp-agent local-engineid 000007DB7F000001000021D7
 snmp-agent community read  public
 snmp-agent community write  private
 snmp-agent sys-info version all
 snmp-agent target-host trap-hostname nsm2 address 11.1.1.8 udp-port 162 trap-paramsname
trapnms2
 snmp-agent target-host trap-paramsname trapnms2 v1 securityname wan
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 11.1.1.10 255.255.255.0
#
return
```

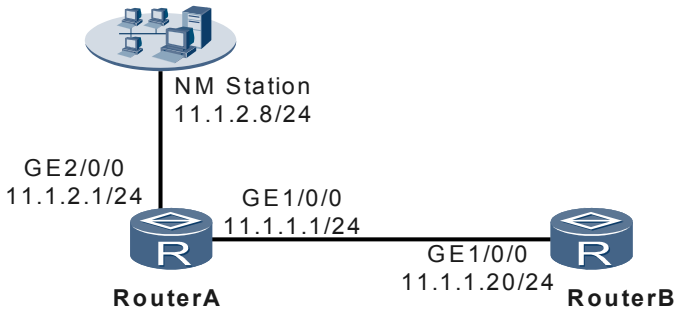
6.20.15 配置 NQA 上下限阈值告警示例

在 NQA 的测试结果超出阈值时，可以发送告警或者生成日志或者既发送告警也生成日志。

组网需求

如图 6-17 所示，RouterA 作为客户端进行 Jitter 测试，对测试结果的丢包率进行监控，在测试结果中的丢包率超过阈值后向网管端发送 Trap。

图 6-17 配置 NQA 阈值告警组网图



配置思路

本例中采用的配置思路如下。

1. 配置阈值告警相关事件。

2. 配置阈值告警。
3. 配置向网管发送告警消息。
4. 启动测试例。

数据准备

本例中需要准备的数据如下。

- 阈值相关事件号
- 阈值告警号
- 阈值上限和下限
- 网管端的地址

操作步骤

步骤 1 配置 RouterA 为 Jitter 测试的客户端。（略）

步骤 2 在 RouterA 配置告警相关事件。

```
<RouterA> system-view
[RouterA] nqa event 10 log-trap
```

步骤 3 配置阈值告警。

```
[RouterA] nqa test-instance admin jitter
[RouterA-nqa-admin-jitter] test-type jitter
[RouterA-nqa-admin-jitter] destination-address ipv4 11.1.1.20
[RouterA-nqa-admin-jitter] frequency 5
[RouterA-nqa-admin-jitter] alarm 10 lost-packet-ratio absolute rising-threshold 100 10 falling-threshold 10 10
[RouterA-nqa-admin-jitter] quit
```

步骤 4 配置向网管发送告警。

配置 SNMP 基本功能。

```
[RouterA] snmp community read public
[RouterA] snmp community write private
[RouterA] snmp sys-info version v2c
```

配置通过 SNMP 向网管端发送 Trap。

```
[RouterA] snmp-agent target-host trap-paramsname trapnms2 v2c securityname alarm
[RouterA] snmp-agent target-host trap-hostname nsm2 address 11.1.2.8 trap-paramsname trapnms2
```

步骤 5 验证配置结果。

```
<RouterA> display nqa-event
NQA event information:
------------------------------------------------------
NQA Event Max: 100                  NQA Event Number: 1
------------------------------------------------------
<Huawei> display nqa alarm
NQA Alarm Information:
----------------------------------------------------------------------
Admin-Name   Operation-Tag   Alarm-Entry   AlarmType   Event-Entry
----------------------------------------------------------------------
admin        jitter          10            Rising       10
<RouterA> display nqa-agent
 NQA Tests Max:256           NQA Tests  Number:   1
 NQA Flow  Max:1000          NQA Flow Remained:1000
nqa test-instance admin jitter
 test-type jitter
 destination-address ipv4 11.1.1.20
```

```
 frequency 5
 alarm 10 lost-packet-ratio absolute rising-threshold 100 10 falling-threshold 1
0 10
 nqa status : normal
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 11.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 11.1.2.1 255.255.255.0
#
interface NULL0
#
aaa
 authentication-scheme default
 #
 authorization-scheme default
 #
 accounting-scheme default
 #
 domain default
 #
#
nqa-jitter tag-version 2
nqa event 10 log-trap
nqa test-instance admin jitter
 test-type jitter
 destination-address ipv4 11.1.1.20
 frequency 5
 alarm 10 lost-packet-ratio absolute rising-threshold 100 10 falling-threshold 1
0 10
#
 snmp-agent
 snmp-agent local-engineid 000007DB7F00000100000B31
 snmp-agent sys-info version v2c v3
 snmp-agent target-host trap-hostname nsm2 address 11.1.2.8 udp-port 162 trap-paramsname
trapnms2
 snmp-agent target-host trap-paramsname trapnms2 v2c securityname alarm
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
 aps fast-interval 0
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 11.1.1.20 255.255.255.0
#
return
```

7 NetStream 配置

关于本章

介绍了 NetStream 的基本原理，并提供配置举例。

7.1 NetStream 概述
简要介绍 Netstream 的基本概念及应用。

7.2 AR3200 中支持的 NetStream 特性
AR3200 可以实现对 IPv4 报文的采样，可以支持 v5、v8 和 v9 报文的输出。

7.3 配置 IPv4 单播原始流统计
配置对经过接口的 IPv4 单播流量的统计。

7.4 配置 IPv4 组播原始流统计
通过配置 IPv4 组播原始流统计，可以实现对于 IPv4 组播流量的统计。

7.5 配置 IPV4 聚合流统计
配置对经过接口的 IPv4 聚合流量的统计。

7.6 配置 IPV4 灵活流统计
配置根据记录灵活创建 Netstream 统计。

7.7 配置 RPF 流量统计
通过配置 RPF 流量统计，可以实现对 RPF 检查失败的异常流量的统计。

7.8 维护 NetStream
清除 NetStream 的统计信息。

7.9 NetStream 配置举例
介绍 NetStream 的各种组网举例。

7.1 NetStream 概述

简要介绍 Netstream 的基本概念及应用。

Netstream 基本概念

NetStream 是一种基于网络流信息的统计与发布技术，可以对网络中的通信量和资源使用情况进行分类和统计，基于各种业务和不同的 QoS 进行管理和计费。

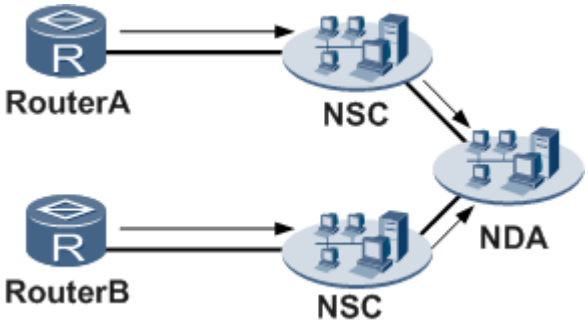
NetStream 主要包括三个设备 NDE（Netstream Data Exporter）、NSC(Netstream Collector)、NDA(Netstream Data Analyse)。

- NDE 负责流量采集和发送流量统计数据信息。
- NSC 设备负责收集和存储 NDE 发来的流量统计数据信息。
- NDA 负责对统计信息分析，分析的结果为网络计费、网络规划、网络监控、应用监控和分析等提供依据。

Netstream 的应用

由于 IP 网络的非面向连接特性，网络中不同类型业务的通信可能是任意一台终端设备向另一台终端设备发送的一组 IP 数据包，这组数据包实际上构成了网络中某种业务的一个数据流。绝大部分的数据流量都是短暂、阵发的双向数据流。NetStream 主要根据一个报文的目的 IP 地址、源 IP 地址、目的端口号、源端口号、协议号、ToS（Type of Service）、输入/输出接口组成的 7 元组来区分不同的流，针对这些流做独立的数据统计。路由器将获得的统计信息定期向 NSC 发送，由 NSC 进行进一步的处理，然后交给后续的 NDA 进行数据分析并形成报表，通过报表进行计费、网络规划等。如图 7-1 所示。

图 7-1 NetStream 数据采集和分析图



7.2 AR3200 中支持的 NetStream 特性

AR3200 可以实现对 IPv4 报文的采样，可以支持 v5、v8 和 v9 报文的输出。

IPv4 网络流量的采样和统计

AR3200 支持对 IPv4 网络流量报文的原始流量进行采样和统计。包括：单播、组播报文和 RPF 检查失败报文。原始流统计信息中除了提供 7 元组外，统计信息还包括源 AS、目的 AS 和 BGP 下一跳的信息。

采样方式

AR3200 支持四种采样方式：固定报文间隔采样、随机报文间隔采样、固定时间间隔采样和随机时间间隔采样。

- 固定报文间隔采样

  固定报文间隔表示每隔一定的报文间隔对报文进行一次采样。
- 随机报文间隔采样

  随机报文间隔采样表示在指定的报文间隔内随机对报文进行一次采样。
- 固定时间间隔采样

  固定时间间隔采样表示每隔一定的时间对报文进行一次采样。
- 随机采样的时间间隔

  随机时间间隔采样表示在指定的时间内随机对报文进行一次采样。

原始流和聚合流版本

Huawei AR3200 系列支持原始流、聚合流和 Flexible 流三种输出方式。原始流按 V5/V9 版本输出，聚合流按 V8/V9 版本输出，Flexible 流按 V9 版本输出。

统计信息的聚合

AR3200 支持 as、as-tos、protocol-port、protocol-port-tos、source-prefix、source-prefix-tos、destination-prefix、destination-prefix-tos、prefix、prefix-tos 这 10 种 IPv4 聚合方式的输出。

老化方式

AR3200 支持 NetStream 流的老化方式有：活跃时间超时老化、非活跃时间超时老化、TCP 连接断开老化、计数溢出老化。

- 非活跃时间老化

  非活跃时间是指从最后一个报文到达时间与当前时间的时间间隔，在超过此间隔时间后，系统立即对流进行老化。
- 活跃时间老化

  活跃时间是指从第一个报文到达时间到当前时间的时间间隔。当缓存区中的流超过此间隔时间后，系统对缓存区的流进行老化。
- TCP 连接断开老化

  对于 TCP 连接，当有标志位 FIN 或 RST 的报文发送时，标志位被置位时，表示一次会话结束。当一条已经存在的 TCP 协议流中采集到一条标志为 FIN 或 RST 的报文时，系统就会把相应的流进行老化。
- 计数溢出老化

  当进入流缓冲区中的流的数量，超过了系统默认的流缓存区中容纳的流的最大数量，系统就会自动对流进行老化。

7.3 配置 IPv4 单播原始流统计

配置对经过接口的 IPv4 单播流量的统计。

7.3.1 建立配置任务

在配置 IPv4 单播流量统计前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

在接口上配置 NetStream 单播统计功能，可以对流入、流出接口的 IPv4 单播报文分别进行统计，并把统计结果发送到网管。网管通过对统计信息的分析，可以了解到网络的流量状况，从而可以对网络进行有效管理。

前置任务

在配置 IPv4 单播原始流统计之前，需要完成以下任务：

- 配置接口的物理参数
- 配置接口的链路层属性

数据准备

在配置 IPv4 单播原始流统计之前，需要准备以下数据：

序号	数据
1	需要统计流量的接口名及编号
2	NetStream 流量输出的版本号
3	NSC 的 IP 地址及端口号

7.3.2 配置输出报文的格式

对于原始流可以配置 v5 和 v9 格式的报文输出。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream export version** *version* [**origin-as** | **peer-as**] [**bgp-nexthop**]，配置输出报文的格式。

缺省情况下，按照版本 5 格式输出，无自治系统选项，输出中不携带 BGP 下一跳。

说明

目前只有版本 9 支持 BGP 下一跳。

----结束

7.3.3 配置统计信息的输出

通过配置统计信息的输出，可以把统计到的流量信息输出到网管进行分析。

背景信息

需要先配置源地址和一个目的地址，Netstream 才能成功输出统计信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream export source** *ip-address*，配置统计信息输出的源地址。

步骤 3 执行命令 **ip netstream export host** *ip-address port-number*，配置统计信息输出的目的地址，即 NSC 的 IP 地址。

最多可以配置两个目的地址，以支持两个 NSC 的相互备份。

----结束

7.3.4 （可选）配置 TCP 流根据 FIN 或 RST 标志位老化

背景信息

对于 TCP 流，可以配置根据 FIN 或 RST 标志位老化。当 AR3200 收到的流含有 TCP 报文的 FIN 或 RST 标志位，则认为该流已经老化，结束统计并将结果上送至 NSC。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream tcp-flag enable**，配置 TCP 流根据 TCP 报文头的 FIN 或 RST 标志位老化。

缺省情况下，TCP 流不根据 TCP 报文头的 FIN 或 RST 标志位老化。

说明

在 AR3200 上同时配置多种老化方式后，当某一流满足任一老化条件时，该流老化。

----结束

7.3.5 （可选）配置非活跃老化时间

非活跃时间是指从最后一个报文到达时间与当前时间的时间间隔，在超过此间隔时间后，系统立即对流进行老化。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream timeout inactive** *inactive-interval*，配置原始流非活跃老化时间。

缺省情况下，原始流的非活跃老化时间为 30s。

----结束

7.3.6 （可选）配置活跃老化时间

活跃时间是指从第一个报文到达时间到当前时间的时间间隔。当缓存区中的流超过此间隔时间后，系统对缓存区的流进行老化。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream timeout active** *active-interval*，配置活跃老化时间。

缺省情况下，活跃老化时间是 30 分钟。

----结束

7.3.7 使能接口的 NetStream 功能

只有在接口下使能了 NetStream 流量统计后，才能实现对流量的采集。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 （可选）执行命令 **ip netstream sampler** { **fix-packets** *packet-interval* | **fix-time** *time-interval* | **random-packets** *packet-interval* | **random-time** *time-interval* } { **inbound** | **outbound** }，配置采样功能。

缺省情况下，接口按照固定报文间隔采样，采样比值为 100。

步骤 4 执行命令 **ip netstream** { **inbound** | **outbound** }，使能接口的 IPv4 单播流量的 NetStream 统计功能。

缺省情况下，不使能 IPv4 流量的统计功能。

----结束

7.3.8 检查配置结果

在配置 IPv4 单播流量统计成功后，可以查看 NetStream 流量统计的配置情况。

前提条件

已经完成上述所有配置。

操作步骤

- 执行命令 **display ip netstreamall** 查看 Netstream 当前配置。
- 执行命令 **display ip netstreamstatistic** 查看 Netstream 统计信息。

----结束

任务示例

配置成功后，执行命令 **display ip netstreamall** 查看 Netstream 当前配置。

```
<Huawei> display ip netstream all
ip netstream timeout inactive 100
ip netstream export source 100.1.10.10
ip netstream export host 100.1.10.1 100
GigabitEthernet1/0/0
 ip netstream inbound
 ip netstream outbound
```

配置成功后，执行命令 **display ip netstreamstatistic** 查看 Netstream 统计信息。

```
<Huawei> display ip netstream statistic
 Origin ingress entries           : 30000
 Origin ingress packets           : 30000
 Origin ingress octets            : 1380000
 Origin egress entries            : 0
 Origin egress packets            : 0
 Origin egress octets             : 0
 Origin total entries             : 30000
 Agility ingress entries          : 0
 Agility ingress packets          : 0
 Agility ingress octets           : 0
 Agility egress entries           : 0
 Agility egress packets           : 0
 Agility egress octets            : 0
 Agility total entries            : 0
 Handle origin entries            : 0
 Handle agility entries           : 0
 Handle As aggre entries          : 0
 Handle ProtPort aggre entries    : 0
 Handle SrcPrefix aggre entries   : 0
 Handle DstPrefix aggre entries   : 0
 Handle Prefix aggre entries      : 0
 Handle AsTos aggre entries       : 0
 Handle ProtPortTos aggre entries : 0
 Handle SrcPreTos aggre entries   : 0
 Handle DstPreTos aggre entries   : 0
 Handle PreTos aggre entries      : 0
```

7.4 配置 IPv4 组播原始流统计

通过配置 IPv4 组播原始流统计，可以实现对于 IPv4 组播流量的统计。

7.4.1 建立配置任务

在配置 IPv4 组播原始流统计前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

在接口上配置 NetStream 组播统计功能，可以对流入、流出接口的 IPv4 组播报文分别进行统计，并把统计结果发送到网管。网管通过对统计信息的分析，可以了解到网络的操作行为，从而对网络进行有效的管理。

前置任务

在配置 IPv4 组播原始流统计之前，需要完成以下任务：

- 配置接口的物理参数
- 配置接口的链路层属性
- 配置接口的 IP 地址

数据准备

在配置 IPv4 组播原始流统计之前，需要准备以下数据。

序号	数据
1	需要统计流量的接口名及编号
2	NetStream 流量输出的版本号
3	NSC&NDA 的 IP 地址及端口号

7.4.2 配置报文输出的格式

对于原始流可以配置 v5 和 v9 格式的报文输出。

背景信息

在统计需要统计流的路由器上，进行以下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream export version** *version* [**origin-as** | **peer-as**] [**bgp-nexthop**]，配置输出报文的格式。

缺省情况下，按照版本 5 格式输出，无自治系统选项，输出中不携带 BGP 下一跳。

说明

目前只有版本 9 支持 BGP 下一跳。

----结束

7.4.3 配置统计信息的输出

通过配置统计信息的输出，可以把统计到的流量信息输出到网管进行分析。

背景信息

请在需要统计流的路由器上执行以下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream export source** *ip-address*，配置统计信息输出的源地址。

步骤 3 执行命令 **ip netstream export host** *ip-address port-nubmer*，配置统计信息输出的目的地址。

最多可以配置两个目的地址，以支持两个 NSC 的相互备份。

----结束

7.4.4 （可选）配置非活跃老化时间

非活跃时间是指从最后一个报文到达时间与当前时间的时间间隔，在超过此间隔时间后，系统立即对流进行老化。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream timeout inactive** *inactive-interval*，配置原始流非活跃老化时间。

缺省情况下，原始流的非活跃老化时间为 30s。

----结束

7.4.5 （可选）配置活跃老化时间

活跃时间是指从第一个报文到达时间到当前时间的时间间隔。当缓存区中的流超过此间隔时间后，系统对缓存区的流进行老化。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream timeout active** *active-interval*，配置活跃老化时间。

缺省情况下，活跃老化时间是 30 分钟。

----结束

7.4.6 使能接口组播流的 NetStream 功能

只有在接口下使能了 NetStream 流量统计后，才能实现对流量的采集。

背景信息

请在需要统计流的路由器上执行以下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **ip netstream multicast** { **inbound** | **outbound** }，使能接口组播流的 NetStream 功能。

缺省情况下，不使能 NetStream 组播流入统计功能和出统计功能。

NetStream 特性可以同时进行报文的入统计和出统计，而且可互不干扰地独立运行。

----结束

7.4.7 检查配置结果

在配置 IPv4 组播流量统计成功后，可以查看 NetStream 流量统计的配置情况。

前提条件

已经完成上述所有配置。

操作步骤

- 执行命令 **display ip netstream all** 查看 Netstream 当前配置。
- 执行命令 **display ip netstream statistic** 查看 Netstream 统计信息。

----结束

任务示例

配置成功后，执行命令 **display ip netstream all** 查看 Netstream 当前配置。

```
<Huawei> display ip netstream all
ip netstream timeout inactive 100
ip netstream export source 100.1.10.10
ip netstream export host 100.1.10.1 100
GigabitEthernet1/0/0
 ip netstream multicast inbound
 ip netstream multicast outbound
```

配置成功后，执行命令 **display ip netstream statistic** 查看 Netstream 统计信息。

```
<Huawei> display ip netstream statistic
 Origin ingress entries           : 30000
 Origin ingress packets           : 30000
 Origin ingress octets            : 1380000
 Origin egress entries            : 0
 Origin egress packets            : 0
 Origin egress octets             : 0
 Origin total entries             : 30000
 Origin total entries             : 0
 Agility ingress entries          : 30000
 Agility ingress packets          : 30000
 Agility ingress octets           : 3960000
 Agility egress entries           : 0
 Agility egress packets           : 0
 Agility egress octets            : 0
 Agility total entries            : 30000
 Handle origin entries            : 29035
 Handle agility entries           : 29050
 Handle As aggre entries          : 1
 Handle ProtPort aggre entries    : 1
 Handle SrcPrefix aggre entries   : 118
 Handle DstPrefix aggre entries   : 1
 Handle Prefix aggre entries      : 118
 Handle AsTos aggre entries       : 1
 Handle ProtPortTos aggre entries : 1
 Handle SrcPreTos aggre entries   : 118
 Handle DstPreTos aggre entries   : 1
 Handle PreTos aggre entries      : 118
```

7.5 配置 IPV4 聚合流统计

配置对经过接口的 IPv4 聚合流量的统计。

7.5.1 建立配置任务

在配置 IPv4 流量的聚合统计前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

在配置 NetStream 时，若要对报文按照某种规则分类统计，需要配置聚合流统计方式。

前置任务

在配置 Netstream 聚合流量统计之前，需要完成以下任务：

- 配置接口的物理参数
- 配置接口的链路层属性
- 配置接口的 IP 地址

数据准备

在配置 Netstream 聚合流量统计之前，需要准备以下数据：

序号	数据
1	需要统计流量的接口名及编号
2	NetStream 流量输出的版本号
3	NSC 地址和端口号

7.5.2 配置 Netstream 聚合功能

可以根据 as、as-tos、protocol-port、protocol-port-tos、source-prefix、source-prefix-tos、destination-prefix、destination-prefix-tos、prefix 和 prefix-tos 对网络流量进行聚合。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream aggregation** { **as** | **as-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos** }，进入 NetStream 聚合视图。

步骤 3 执行命令 **enable**，使能聚合模式。

----结束

7.5.3 配置输出报文的格式

对于聚合流可以支持 v8 和 v9 版本的输出。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream aggregation** { **as** | **as-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos** }，进入 NetStream 聚合视图。

步骤 3 （可选）执行命令 **export version** *version*，配置输出报文的格式。

缺省情况下，输出报文格式版本号为 V8。

----结束

7.5.4 配置统计信息的输出

通过配置统计信息的输出，可以把统计到的流量信息输出到网管进行分析。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream aggregation** { **as** | **as-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos** }，进入 NetStream 聚合视图。

步骤 3 执行命令 **ip netstream export source** *ip-address*，配置统计信息输出的源地址。

步骤 4 执行命令 **ip netstream export host** *ip-address port-number*，配置统计信息输出的目的 NSC 地址。

系统视图、NetStream 聚合视图都可以配置统计信息输出的目的 NSC 地址。最多可以配置两个目的地址，以支持两个 NSC 的相互备份。

聚合视图下配置的目的 NSC 地址的优先级高于系统视图下配置的目的 NSC 地址。成功配置目的 NSC 地址后，

- 原始流只能被送往系统视图下配置的目的 NSC 地址。
- 聚合流被送往相应的聚合视图下配置的目的 NSC 地址。

----结束

7.5.5 （可选）配置非活跃老化时间

非活跃时间是指从最后一个报文到达时间与当前时间的时间间隔，在超过此间隔时间后，系统立即对流进行老化。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream aggregation timeout inactive** *inactive-interval*，配置聚合流非活跃老化时间。

缺省情况下，聚合流的非活跃老化时间为 30s。

----结束

7.5.6 （可选）配置活跃老化时间

活跃时间是指从第一个报文到达时间到当前时间的时间间隔。当缓存区中的流超过此间隔时间后系统对缓存区的流进行老化。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream aggregation timeout active** *active-interval*，配置聚合流活跃老化时间。

缺省情况下，聚合流的活跃老化时间为 30 分钟。

----结束

7.5.7 使能接口的 NetStream 功能

只有在接口下使能了 NetStream 流量统计后，才能实现对流量的采集。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 （可选）执行命令 **ip netstream sampler** { **fix-packets** *packet-interval* | **fix-time** *time-interval* | **random-packets** *packet-interval* | **random-time** *time-interval* } { **inbound** | **outbound** }，配置接口报文采样比。

缺省情况下，接口按照固定报文间隔采样，采样比值为 100。

步骤 4 如果聚合方式配置为 as-tos、destination-prefix-tos、prefix-tos、protocol-port-tos 或 source-prefix-tos 时，执行命令 **trust dscp override**,配置接口下的报文按照 DSCP 优先级进行映射。

步骤 5 执行命令 **ip netstream** { **inbound** | **outbound** }，使能接口的 IPv4 单播流量的 NetStream 统计功能。

缺省情况下，不使能 IPv4 流量的统计功能。

----结束

7.5.8 检查配置结果

在配置 IPv4 流量的聚合统计成功后，可以查看 NetStream 流量统计的配置情况。

前提条件

已经完成上述所有配置。

操作步骤

- 执行命令 **display ip netstream all** 查看 Netstream 当前配置。
- 执行命令 **display ip netstream statistic** 查看 Netstream 统计信息。

----结束

任务示例

配置成功后，执行命令 **display ip netstream all** 查看 Netstream 当前配置。

```
<Huawei> display ip netstream all
ip netstream aggregation timeout inactive 100
ip netstream aggregation as
 enable
 ip netstream export source 100.1.10.10
 ip netstream export host 100.1.10.1 100
GigabitEthernet1/0/0
 ip netstream inbound
 ip netstream outbound
```

配置成功后，执行命令 **display ip netstream statistic** 查看 Netstream 统计信息。

```
<Huawei> display ip netstream statistic
 Origin ingress entries           : 30000
 Origin ingress packets           : 30000
 Origin ingress octets            : 1380000
 Origin egress entries            : 0
 Origin egress packets            : 0
 Origin egress octets             : 0
 Origin total entries             : 30000
 Origin total entries             : 0
 Agility ingress entries          : 30000
 Agility ingress packets          : 30000
 Agility ingress octets           : 3960000
 Agility egress entries           : 0
 Agility egress packets           : 0
 Agility egress octets            : 0
 Agility total entries            : 30000
 Handle origin entries            : 29035
 Handle agility entries           : 29050
 Handle As aggre entries          : 1
 Handle ProtPort aggre entries    : 1
 Handle SrcPrefix aggre entries   : 118
 Handle DstPrefix aggre entries   : 1
 Handle Prefix aggre entries      : 118
 Handle AsTos aggre entries       : 1
 Handle ProtPortTos aggre entries : 1
 Handle SrcPreTos aggre entries   : 118
 Handle DstPreTos aggre entries   : 1
 Handle PreTos aggre entries      : 118
```

7.6 配置 IPV4 灵活流统计

配置根据记录灵活创建 Netstream 统计。

7.6.1 建立配置任务

应用环境

在网络中，若要对报文按照协议类型、TOS、源 IP 地址、目的 IP 地址、源端口号、目的端口号统计，请配置灵活流统计。

前置任务

在配置 IPV4 灵活流统计之前，需要完成以下任务：

- 配置接口的物理参数
- 配置接口的链路层属性
- 配置接口的 IP 地址

数据准备

在配置 IPV4 灵活流统计之前，需要准备以下数据：

序号	数据
1	需要统计流量的接口名及编号
2	NSC 的 IP 地址及端口号

7.6.2 配置灵活流统计模板

使能接口的灵活流统计之前，需要配置灵活流统计的模板。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream record** *record-name*，创建并进入一个 Record 记录视图。

步骤 3 执行命令 **match ipv4** { **protocol** | **tos** | **source-address** | **destination-address** | **source-port** | **destination-port** }，配置记录的 IPv4 聚合关键字。

步骤 4 执行命令 **collect counter** { **bytes** | **packets** }，配置上送流的统计方式。

步骤 5 执行命令 **collect interface** { **input** | **output** }，配置发送至 NSC 的流量统计信息中包含流量入、出接口的索引。

----结束

7.6.3 配置输出报文的格式

输出 IPV4 灵活流统计时，需要配置输出报文的格式为 V9。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream export version** 9 [**origin-as** | **peer-as**] [**bgp-nexthop**]，配置以 V9 格式输出。

缺省情况下，按照版本 5 格式输出，无自治系统选项，输出中不携带 BGP 下一跳。

说明

目前只有版本 9 支持 BGP 下一跳。

----结束

7.6.4 配置统计信息的输出

通过配置统计信息的输出，可以把统计到的流量信息输出到网管进行分析。

背景信息

需要先配置源地址和一个目的地址，Netstream 才能成功输出统计信息。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream export source** *ip-address*，配置统计信息输出的源地址。

步骤 3 执行命令 **ip netstream export host** *ip-address port-number*，配置统计信息输出的目的地址，即 NSC 的 IP 地址。

最多可以配置两个目的地址，以支持两个 NSC 的相互备份。

----结束

7.6.5 （可选）配置非活跃老化时间

非活跃时间是指从最后一个报文到达时间与当前时间的时间间隔，在超过此间隔时间后，系统立即对流进行老化。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream timeout inactive** *inactive-interval*，配置原始流非活跃老化时间。

缺省情况下，原始流的非活跃老化时间为 30s。

----结束

7.6.6 （可选）配置活跃老化时间

活跃时间是指从第一个报文到达时间到当前时间的时间间隔。当缓存区中的流超过此间隔时间后，系统对缓存区的流进行老化。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream timeout active** *active-interval*，配置活跃老化时间。

缺省情况下，活跃老化时间是 30 分钟。

----结束

7.6.7 使能接口的 IPV4 灵活流统计

只有在接口下使能了 NetStream 流量统计后，才能实现对流量的采集。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **port ip netstream record** *record-name*，配置记录应用到接口。

说明

每个接口只可以配置一个记录。同一接口视图下，如需改变记录，需要先执行 **undo port ip netstream record** 命令删除原有配置。

步骤 4 （可选）执行命令 **ip netstream sampler** { **fix-packets** *packet-interval* | **fix-time** *time-interval* | **random-packets** *packet-interval* | **random-time** *time-interval* } { **inbound** | **outbound** }，配置采样功能。

缺省情况下，接口按照固定报文间隔采样，采样比值为 100。

步骤 5 执行命令 **ip netstream** { **inbound** | **outbound** }，使能接口的 IPv4 流量统计功能。

----结束

7.6.8 检查配置结果

在配置 IPv4 流量灵活统计成功后，可以查看 NetStream 流量统计的配置情况。

前提条件

已经完成上述所有配置。

操作步骤

- 执行命令 **display ip netstream all** 查看 Netstream 当前配置。
- 执行命令 **display ip netstream statistic** 查看 Netstream 统计信息。

----结束

任务示例

配置成功后，执行命令 **display ip netstream all** 查看 Netstream 当前配置。

```
<Huawei> display ip netstream all
ip netstream timeout inactive 100
ip netstream export source 100.1.10.10
ip netstream export host 100.1.10.1 100
ip netstream record hwrecord
 match ipv4 destination-address
 collect counter packets
 collect interface input
 collect interface output
GigabitEthernet1/0/0
 port ip netstream record hwrecord
 ip netstream inbound
 ip netstream outbound
```

配置成功后，执行命令 **display ip netstream statistic** 查看 Netstream 统计信息。

```
<Huawei> display ip netstream statistic
 Origin ingress entries           : 30000
 Origin ingress packets           : 30000
 Origin ingress octets            : 1380000
 Origin egress entries            : 0
 Origin egress packets            : 0
 Origin egress octets             : 0
 Origin total entries             : 30000
 Origin total entries             : 0
 Agility ingress entries          : 30000
 Agility ingress packets          : 30000
 Agility ingress octets           : 3960000
 Agility egress entries           : 0
 Agility egress packets           : 0
 Agility egress octets            : 0
 Agility total entries            : 30000
 Handle origin entries            : 29035
 Handle agility entries           : 29050
 Handle As aggre entries          : 1
 Handle ProtPort aggre entries    : 1
 Handle SrcPrefix aggre entries   : 118
 Handle DstPrefix aggre entries   : 1
 Handle Prefix aggre entries      : 118
 Handle AsTos aggre entries       : 1
 Handle ProtPortTos aggre entries : 1
 Handle SrcPreTos aggre entries   : 118
 Handle DstPreTos aggre entries   : 1
 Handle PreTos aggre entries      : 118
```

7.7 配置 RPF 流量统计

通过配置 RPF 流量统计，可以实现对 RPF 检查失败的异常流量的统计。

7.7.1 建立配置任务

在配置 RPF 流量统计前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

对于配置了 RPF 后，部分 IPv4 组播报文由于检测不通过，而被丢弃。可以配置对于此部分的报文进行统计，就可以更加全面的了解网络中的组播流量信息。

前置任务

在配置 RPF 流量统计前，需要完成以下任务：

- 配置接口的物理参数
- 配置接口的链路层属性
- 配置接口的 IP 地址

数据准备

在完成配置 RPF 统计之前，需要准备以下数据。

序号	数据
1	需要统计流量的接口名及编号
2	NetStream 流量输出的版本号
3	NSC&NDA 的 IP 地址及端口号

7.7.2 配置报文输出的格式

对于原始流可以配置 v5 和 v9 格式的报文输出。

背景信息

请在需要统计丢弃报文的路由器上执行以下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream export version** { **5** | **9** } [**origin-as** | **peer-as**] [**bgp-nexthop**]，配置输出报文的格式。

缺省情况下，按照版本 5 格式输出，无自治系统选项，输出中不携带 BGP 下一跳。

说明

目前只有版本 9 支持 BGP 下一跳。

----结束

7.7.3 配置统计信息的输出

通过配置统计信息的输出，可以把统计到的流量信息输出到网管进行分析。

背景信息

请在需要统计丢弃报文的路由器上执行以下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream export source** *ip-address*，配置统计信息输出的源地址。

步骤 3 执行命令 **ip netstream export host** *ip-address port-number*，配置统计信息输出的目的地址。

最多可以配置两个目的地址，以支持两个 NSC 的相互备份。

----结束

7.7.4 （可选）配置非活跃老化时间

非活跃时间是指从最后一个报文到达时间与当前时间的时间间隔，在超过此间隔时间后，系统立即对流进行老化。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream timeout inactive** *inactive-interval*，配置原始流非活跃老化时间。

缺省情况下，原始流的非活跃老化时间为 30s。

----结束

7.7.5 （可选）配置活跃老化时间

活跃时间是指从第一个报文到达时间到当前时间的时间间隔。当缓存区中的流超过此间隔时间后，系统对缓存区的流进行老化。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ip netstream timeout active** *active-interval*，配置活跃老化时间。

缺省情况下，活跃老化时间是 30 分钟。

----结束

7.7.6 使能 RPF 统计功能

使能 RPF 对组播异常流量的检测。

背景信息

请在需要统计丢弃报文的路由器上执行以下的配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **ip netstream rpf-failure inbound**，使能 RPF 统计功能。

缺省情况下，不使能 NetStream RPF 统计功能。

NetStream 特性仅支持对报文的入方向统计。

----结束

7.7.7 检查配置结果

在配置 RPF 流量统计成功后，可以查看 NetStream 流量统计的配置情况。

前提条件

已经完成 RPF 流量统计功能的所有配置。

操作步骤

- 执行命令 **display ip netstream all** 查看 Netstream 当前配置。
- 执行命令 **display ip netstream statistic** 查看 Netstream 统计信息。

----结束

任务示例

配置成功后，执行命令 **display ip netstream all** 查看 Netstream 当前配置。

```
<Huawei> display ip netstream all
ip netstream timeout inactive 100
ip netstream export source 100.1.10.10
ip netstream export host 100.1.10.1 100
GigabitEthernet1/0/0
 ip netstream rpf-failure inbound
```

配置成功后，执行命令 **display ip netstream statistic** 查看 Netstream 统计信息。

```
<Huawei> display ip netstream statistic
 Origin ingress entries           : 30000
 Origin ingress packets           : 30000
 Origin ingress octets            : 1380000
 Origin egress entries            : 0
 Origin egress packets            : 0
 Origin egress octets             : 0
 Origin total entries             : 30000
 Origin total entries             : 0
 Agility ingress entries          : 30000
 Agility ingress packets          : 30000
 Agility ingress octets           : 3960000
 Agility egress entries           : 0
 Agility egress packets           : 0
 Agility egress octets            : 0
 Agility total entries            : 30000
 Handle origin entries            : 29035
 Handle agility entries           : 29050
 Handle As aggre entries          : 1
 Handle ProtPort aggre entries    : 1
 Handle SrcPrefix aggre entries   : 118
 Handle DstPrefix aggre entries   : 1
 Handle Prefix aggre entries      : 118
 Handle AsTos aggre entries       : 1
 Handle ProtPortTos aggre entries : 1
 Handle SrcPreTos aggre entries   : 118
 Handle DstPreTos aggre entries   : 1
 Handle PreTos aggre entries      : 118
```

7.8 维护 NetStream

清除 NetStream 的统计信息。

7.8.1 清除 NetStream 的统计信息

当确认清除 NetStream 的统计信息，可以执行命令 reset ip netstream statistics 进行清除。执行清除命令后，信息将无法恢复。

背景信息

> **注意**
>
> 清除统计信息后，以前的统计信息将无法恢复，务必仔细确认。

操作步骤

步骤 1 执行 **reset ip netstream statistic** 命令清除 NetStream 统计信息和输出统计信息，同时执行 **reset ip netstream cache** 命令将流缓存区中所有流老化。

----结束

7.9 NetStream 配置举例

介绍 NetStream 的各种组网举例。

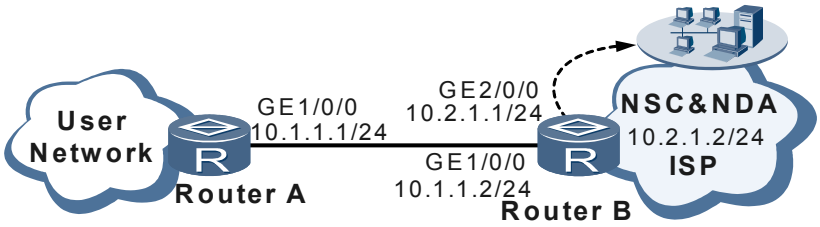
7.9.1 配置 IPv4 单播流统计示例

通过配置 IPv4 单播流统计，可以实现 IPv4 单播流量的统计。

组网需求

如图 7-2 所示，企业用户网络通过 RouterA 接入到运营商的路由器 RouterB 上，在 RouterB 上使能 NetStream 统计功能。运营商通过对流入和流出 RouterB 的 GE1/0/0 接口的流量进行统计，为网络计费提供依据。

图 7-2 配置 IPv4 单播流量统计组网图



配置思路

采用如下的思路配置 IPv4 单播流量统计：

1. 配置路由器接口的 IP 地址。
2. 在 RouterB 上启动 NetStream 的入、出统计功能。

数据准备

完成此配置举例，需要准备如下数据：

- 接口的 IP 地址
- NetStream 信息输出的目的地址、目的端口、源地址

操作步骤

步骤 1 配置 RouterA、RouterB 的接口 IP 地址（略）

步骤 2 在 RouterB 上的使能 NetStream 出、入统计功能

RouterB 上的使能 NetStream 出统计功能。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ip netstream outbound
```

RouterB 上的使能 NetStream 入统计功能。

```
[RouterB-GigabitEthernet1/0/0] ip netstream inbound
```

在 RouterB 配置输出的版本。

```
[RouterB] ip netstream export version 9
```

缺省情况下，原始 IPv4 流按照版本 5 进行输出。

在 RouterB 上配置统计信息输出到 NSC&NDA。

```
[RouterB] ip netstream export host 10.2.1.2 6000
```

在 RouterB 上配置统计信息输出的源地址。

```
[RouterB] ip netstream export source 10.2.1.1
```

步骤 3 验证配置效果

配置成功后，在用户视图下执行命令 **display ip netstream all**，查看配置。

```
<RouterB> display ip netstream all
ip netstream export source 10.2.1.1
ip netstream export host 10.2.1.2 6000
GigabitEthernet1/0/0
 ip netstream inbound
 ip netstream outbound
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 ip netstream export version 9
 ip netstream export source 10.2.1.1
```

```
 ip netstream export host 10.2.1.2 6000
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
 ip netstream inbound
 ip netstream outbound
#
interface GigabitEthernet2/0/0
 ip address 10.2.1.1 255.255.255.0
#
return
```

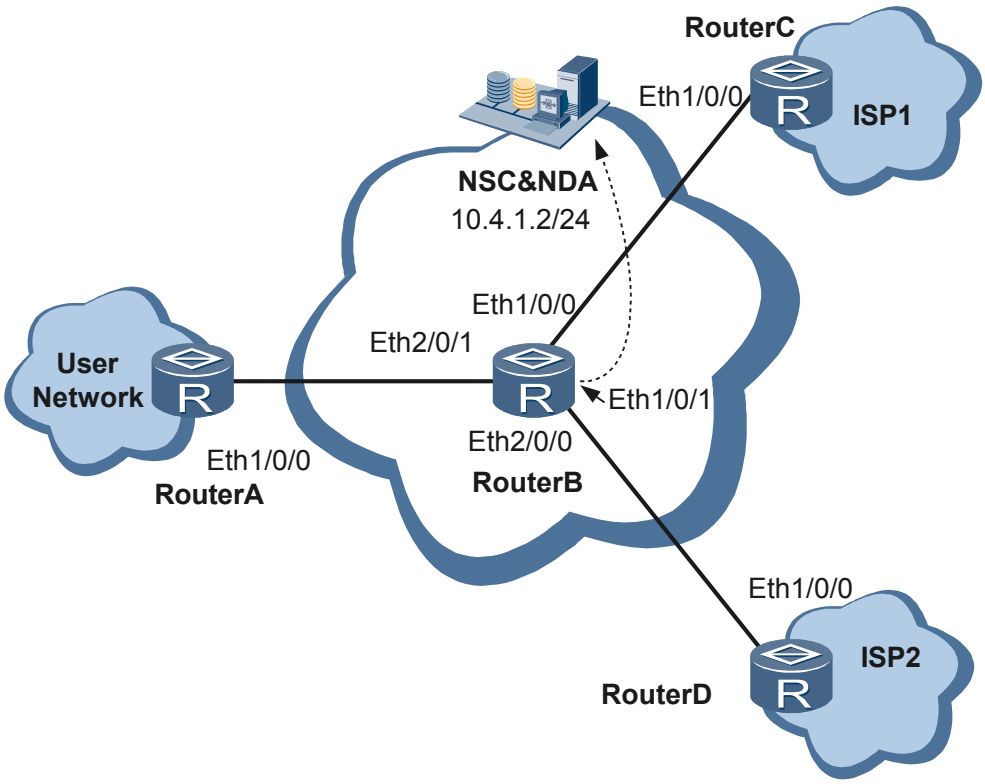
7.9.2 配置 IPv4 聚合流统计示例

通过配置 IPv4 聚合流统计，可以实现 IPv4 聚合流量的统计。

组网需求

如图 7-3 所示，在 RouterB 上部署 NetStream，可以统计出从用户网络到不同 ISP 的流量，为网络计费提供依据。

图 7-3 Netstream 聚合组网图



Router	接口	IP 地址
RouterA	Ethernet1/0/0	10.1.1.1/24
RouterB	Ethernet1/0/0	10.2.1.1/24
	Ethernet1/0/1	10.4.1.1/24
	Ethernet2/0/0	10.3.1.1/24
	Ethernet2/0/1	10.1.1.2/24
RouterC	Ethernet1/0/0	10.2.1.2/24
RouterD	Ethernet1/0/0	10.3.1.2/24

配置思路

采用如下的思路配置 IPv4 聚合流统计：

1. 在 RouterB 的 Eth2/0/1 接口下使能 NetStream 的入、出统计功能并在该接口下配置采样功能。
2. 在 RouterB 上使能聚合功能，减少网管的数据流量。
3. 在 RouterB 配置 NetStream 报文输出版本。
4. 在 RouterB 配置流输出的目的地址与端口号（即 NSC&NDA 的 IP 地址和端口号）。
5. 在 RouterB 配置流输出的源地址（即 Eth1/0/1 接口的 IP 地址）。

数据准备

完成该配置需要准备如下数据：

- 接口的 IP 地址
- NSC 地址和端口号
- 采样比例
- 输出统计信息版本号

操作步骤

步骤 1 配置用户网络、ISP1 和 ISP2 与接入网络之间路由可达。（略）。

步骤 2 在 RouterB 上配置 Netstream。

配置聚合流的输出和版本号。

```
[RouterB] ip netstream aggregation as
[RouterB-aggregation-as] export version 9
[RouterB-aggregation-as] ip netstream export host 10.4.1.2 6000
[RouterB-aggregation-as] ip netstream export source 10.4.1.1
[RouterB-aggregation-as] enable
[RouterB-aggregation-as] quit
```

配置报文采样比及使能接口流量统计。

```
[RouterB] interface ethernet 2/0/1
[RouterB-Ethernet2/0/1] ip netstream sampler fix-packets 100 inbound
[RouterB-Ethernet2/0/1] ip netstream sampler fix-packets 100 outbound
[RouterB-Ethernet2/0/1] ip netstream inbound
[RouterB-Ethernet2/0/1] ip netstream outbound
[RouterB-Ethernet2/0/1] quit
[RouterB] quit
```

步骤 3 验证配置结果

配置成功后，在 RouterB 的用户视图下执行命令 **display ip netstream all**，查看配置信息。

```
<RouterB> display ip netstream all
ip netstream aggregation as
 enable
 export version 9
 ip netstream export source 10.4.1.1
 ip netstream export host 10.4.1.2 6000
Ethernet2/0/1
```

```
 ip netstream inbound
 ip netstream outbound
```

----结束

配置文件

RouterA 的配置文件。

```
#
 sysname RouterA
#
 interface Ethernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
return
```

RouterB 的配置文件。

```
#
 sysname RouterB
#
interface Ethernet1/0/0
 ip address 10.2.1.1 255.255.255.0
#
interface Ethernet1/0/1
 ip address 10.4.1.1 255.255.255.0
#
interface Ethernet2/0/0
 ip address 10.3.1.1 255.255.255.0
#
interface Ethernet2/0/1
 ip address 10.1.1.2 255.255.255.0
 ip netstream inbound
 ip netstream outbound
#
ip netstream aggregation as
 enable
 export version 9
 ip netstream export source 10.4.1.1
 ip netstream export host 10.4.1.2 6000
#
return
```

RouterC 的配置文件。

```
#
 sysname RouterC
#
interface Ethernet1/0/0
 ip address 10.2.1.2 255.255.255.0
#
return
```

RouterD 的配置文件。

```
#
 sysname RouterD
#
interface Ethernet1/0/0
 ip address 10.3.1.2 255.255.255.0
#
return
```

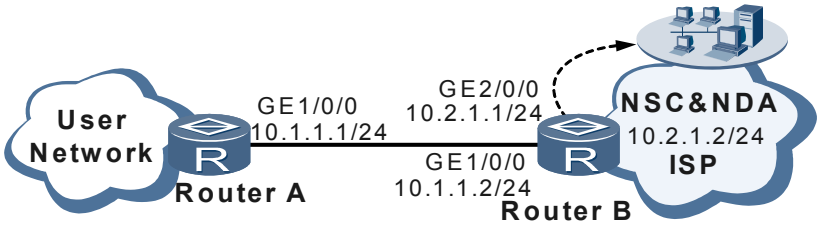
7.9.3 配置 IPV4 灵活流统计示例

通过配置 IPv4 灵活流统计，可以实现对报文按照协议类型、TOS、源 IP 地址、目的 IP 地址、源端口号、目的端口号统计。

组网需求

如图 7-4 所示，企业用户网络通过 RouterA 接入到运营商接入交换机 RouterB 上。在 RouterB 上使能 IPV4 灵活流统计功能，使用户可以根据目的 IP 地址和目的端口号聚合，统计接口的入、出方向的流量信息，并上送至 NSC。

图 7-4 Flexible Netstream 组网图



配置思路

采用如下思路配置 IPV4 灵活流统计功能。

1. 配置 RouterA 和 RouterB 的接口 IP 地址。
2. 配置输出报文的版本。
3. 配置输出报文的源地址、目的地址、目的端口号。
4. 在 RouterB 的 GE1/0/0 上使能 IPV4 灵活流统计功能。

数据准备

完成此配置，需要准备如下数据：

- 接口的 IP 地址。
- 输出报文的版本
- NSC 的地址、端口号，报文携带的源地址。
- 需要上送至 NSC 的统计信息。

操作步骤

步骤 1 如图 7-4 标注所示，配置 RouterA 及 RouterB 的接口 IP 地址（略）。

步骤 2 配置统计报文输出的版本。

配置统计报文输出的版本为 V9。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] ip netstream export version 9
```

步骤 3 配置统计报文输出的目的地址、目的端口号、源地址。

配置统计报文输出目的地址和目的端口号。

```
[RouterB] ip netstream export host 10.2.1.2 6000
```

配置统计报文输出的源地址。

```
[RouterB] ip netstream export source 10.2.1.1
```

步骤 4 在 RouterB 上使能 Flexible 流量统计功能。

创建并进入一个名为“test”的记录视图。

```
[RouterB] ip netstream record test
[RouterB-record-test]
```

配置“test”记录的聚合关键字。

```
[RouterB-record-test] match ipv4 destination-address
[RouterB-record-test] match ipv4 destination-port
```

配置将“test”记录的入、出接口索引发送至 NSC。

```
[RouterB-record-test] collect interface input
[RouterB-record-test] collect interface output
```

配置将出、入接口的流的报文数和字节数送至 NSC。

```
[RouterB-record-test] collect counter bytes
[RouterB-record-test] collect counter packets
[RouterB-record-test] quit
```

步骤 5 使能 GE1/0/0 接口的 IPV4 灵活流统计功能。

使能 GE1/0/0 接口的 IPV4 灵活流统计功能。

```
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] port ip netstream record test
```

配置 GE1/0/0 接口的入、出方向固定报文间隔采样比为 100。

```
[RouterB-GigabitEthernet1/0/0] ip netstream sampler fix-packets 100 inbound
[RouterB-GigabitEthernet1/0/0] ip netstream sampler fix-packets 100 outbound
```

使能 GE1/0/0 接口的入、出方向 Netstream 功能。

```
[RouterB-GigabitEthernet1/0/0] ip netstream inbound
[RouterB-GigabitEthernet1/0/0] ip netstream outbound
[RouterB-GigabitEthernet1/0/0] quit
```

步骤 6 验证配置结果

配置成功后，在 RouterB 的用户视图下执行命令 **display ip netstream all** 查看配置。

```
<RouterB> display ip netstream all
ip netstream export source 10.2.1.1
ip netstream export host 10.2.1.2 6000
ip netstream export version 9
ip netstream record test
 match ipv4 destination-address
 match ipv4 destination-port
 collect counter packets
 collect counter bytes
 collect interface input
 collect interface output
GigabitEthernet1/0/0
 port ip netstream record test
 ip netstream inbound
 ip netstream outbound
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
```

```
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
 ip netstream export source 10.2.1.1
 ip netstream export host 10.2.1.2 6000
 ip netstream record test
 ip netstream export version 9
#
ip netstream record test
 match ipv4 destination-address
 match ipv4 destination-port
 collect counter packets
 collect interface input
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
 ip netstream inbound
 ip netstream outbound
#
interface GigabitEthernet2/0/0
 ip address 10.2.1.1 255.255.255.0
#
return
```

8 Ping 和 Tracert

关于本章

通过 Ping 和 Tracert 可以检测网络的连通性。

8.1 ping 和 tracert 简介
通过 Ping 和 Tracert 用户可以了解到 Ping 和 Tracert 的基本原理和 AR3200 系统对 Ping 和 Tracert 特性的支持情况。

8.2 配置 ping 和 tracert 检测网络
通过 ping 和 tracert 可以检测到网络的连通情况。

8.1 ping 和 tracert 简介

通过 Ping 和 Tracert 用户可以了解到 Ping 和 Tracert 的基本原理和 AR3200 系统对 Ping 和 Tracert 特性的支持情况。

8.1.1 ping 和 tracert

当设备出现故障时，可以首先使用 Ping 与 Tracert 命令测试网络连接是否正常工作。

ping 命令主要用于检查网络连接及主机是否可达。

tracert 命令用于测试数据包从发送主机到目的地所经过的网关，它主要检查网络连接是否可达，以及分析网络什么地方发生了故障。

tracert 的执行过程如下：

1. 首先发送一个 TTL 为 1 的数据包。
2. 到达第一跳时 TTL 超时，第一跳路由器发回一个 ICMP 错误消息，指明此数据包不能被发送。
3. 发送主机将 TTL 加 1，重新发送此数据包。
4. 第二跳路由器返回 TTL 超时。

   以上步骤循环进行，直到到达目的地。这样，发送主机就能够记录每一个 ICMP TTL 超时消息的源地址，得到 IP 数据包到达目的地所经历的路径。

8.2 配置 ping 和 tracert 检测网络

通过 ping 和 tracert 可以检测到网络的连通情况。

8.2.1 建立配置任务

在配置 ping 和 tracert 检测网络前了解它的应用环境、配置此特性的前置任务和数据准备，可以帮助用户快速、准确地完成配置任务。

应用环境

客户端无法正常上网，需要使用 **ping** 和 **tracert** 检测网络连接是否正常。

前置任务

在配置 Ping 和 Tracert 测试之前，需完成以下任务：

- 客户端的网络连接线连接正确。
- 客户端正确配置了 IP 地址。

数据准备

在配置 ping 和 tracert 检测网络之前，需要准备以下数据。

序号	数据
1	客户端的 IP 地址。
2	网关的 IP 地址。

8.2.2 使用 ping 检测网络连接是否正常

使用 Ping 检测网络中两个节点之间的连通性。

背景信息

在客户端进行如下的配置。

操作步骤

步骤 1 执行命令 **ping** [**ip**] [**-a** *source-ip-address* | **-c** *count* | **-d** | **-f** | **-h** *ttl-value* | **-i** *interface-type interface-number* | **-si** *source-interface-type source-interface-number* | **-m** *time* | **-n** | **-name** | **-p** *pattern* | **-q** | **-r** | **-s** *packetsize* | **-system-time** | **-t** *timeout* | **-tos** *tos-value* | **-v** | **-vpn-instance** *vpn-instance-name*] * *host* [**ip-forwarding**]，测试网络连接是否正常。

以上 **ping** 命令只列出了部分参数，各参数意义请参见《Huawei AR3200 系列企业路由器 命令参考》。

命令执行结果输出包括：

- 对每一个 **ping** 报文的响应情况，如果超时后仍没有收到响应报文，则输出“Request time out”，否则显示响应报文中数据字节数、报文序号、TTL 和响应时间等。
- 最后的统计信息，包括发送报文数、接收报文数、未响应报文百分比和响应时间的最小、最大和平均值。

说明

如果 **ping** 的目的地址是广播地址，则回应报文中的源地址是广播地址。

```
<Huawei> ping 202.20.36.25
  PING 202.20.36.25: 56  data bytes, press CTRL_C to break
    Reply from 202.20.36.25: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 202.20.36.25: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 202.20.36.25: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 202.20.36.25: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 202.20.36.25: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 202.20.36.25 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

----结束

8.2.3 使用 tracert 检测网络发生故障的位置

使用 Tracert 检测网络中各个节点之间的连通性。

背景信息

在客户端进行如下的配置。下列操作可在所有视图下进行。当使用 **tracert** 命令检查网络连接是否可达时，可以使用 **icmp time-exceed** 命令指定 ICMP Time Exceeded 报文的格式。

操作步骤

步骤 1 （可选）执行命令 **icmp time-exceed** { **extension** { **compliant** | **non-compliant** } | **classic** }，指定 ICMP Time Exceeded 报文的格式。

说明
请在系统视图下执行该命令。

步骤 2 执行命令 **tracert** [**-a** *source-ip-address* | **-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *nqueries* | **-v** | **-vpn-instance** *vpn-instance-name* | **-w** *timeout*] * *host*，测试故障发生的位置。

以上 **tracert** 命令只列出了部分参数，该命令各选项及参数意义请参见《Huawei AR3200 系列企业路由器 命令参考》。

下面是应用 **tracert** 分析网络情况的例子。

```
<Huawei> tracert -m 10 35.1.1.48
traceroute to 35.1.1.48 (35.1.1.48), max hops: 30, packet length: 40, press CTRL_C to break
1  128.3.112.1    19 ms   19 ms   0 ms
2  128.32.216.1   39 ms   39 ms   19 ms
3  128.32.136.23  39 ms   40 ms   39 ms
4  128.32.168.22  39 ms   39 ms   39 ms
5  128.32.197.4   40 ms   59 ms   59 ms
6  131.119.2.5    59 ms   59 ms   59 ms
7  129.140.70.13  99 ms   99 ms   80 ms
8  129.140.71.6   139 ms  239 ms  319 ms
9  129.140.81.7   220 ms  199 ms  199 ms
10  35.1.1.48     239 ms  239 ms  239 ms
```

----结束