新技术专题

技术图解 \ 技术白皮书 \ 配置步骤 \ 配置举例

NQA 技术白皮书

目 录

1 概述

1.1 产生背景

随着 Internet 的高速发展，网络支持的业务和应用日渐增多，传统的网络性能分析方法（如 Ping、Tracert 等）已经不能满足用户对业务多样性和监测实时性的要求。

NQA 通过发送测试报文，对网络性能或服务质量进行分析，为用户提供网络性能参数，如时延抖动、HTTP 的总时延、通过 DHCP 获取 IP 地址的时延、TCP 连接时延、FTP 连接时延和文件传输速率等。利用 NQA 的测试结果，用户可以：

- 及时了解网络的性能状况，针对不同的网络性能，进行相应的处理；
- 对网络故障进行诊断和定位。

NQA 还提供了与 Track 和应用模块联动的功能，实时监控网络状态的变化，及时通知业务模块进行相应处理，从而避免通信的中断或服务质量的降低。

1.2 技术优点

NQA 具有以下几个特点：

- 支持多种测试类型

  传统的 Ping 功能是使用 ICMP（Internet Control Message Protocol，互联网控制报文协议）测试数据包在本端和指定目的端之间的往返时间。NQA 是对 Ping 功能的扩展和增强，它支持 ICMP、UDP、Voice、TCP、DLSw、SNMP、HTTP、FTP、DHCP、DNS、Path-jitter 等多种测试类型。
- 支持多测试组并发

  NQA 模块支持多个测试组同时进行测试，用户可以根据需求手工配置同时进行测试的测试组的个数。但同一时刻，不能有多个 DHCP 类型的测试组进行测试。
- 支持联动功能

  联动功能是指 NQA 提供探测功能，把探测结果通知其他模块，其他模块再根据探测结果进行相应的处理。

2 NQA 技术实现

2.1 概念介绍

1. NQA client

NQA 网络测试的客户端。

2. NQA server

NQA 网络测试的服务器端。狭义上，指 UDP-echo、TCP、UDP-jitter 和 Voice 四种测试中的 NQA server 端。广义上，指所有要被探测的对端设备，如 FTP server、HTTP server 等。

3. SD（Source address to Destination address）

从源端（NQA client）到目的端（NQA server）。

4. DS（Destination address to Source address）

从目的端（NQA server）到源端（NQA client）。

5. 探测

一个能够得到完整探测结果的独立过程。

不同测试一次探测包含的内容不同：

- 对于 ARP、ICMP-echo、UDP-echo 测试，一次探测发送一个探测报文。
- 对于 DLSw、TCP 测试，一次探测是指一次连接。
- 对于 DHCP、DNS、FTP 和 HTTP 测试，一次探测是指完成一次相应的功能。
- 对于 ICMP-jitter、Path-jitter、UDP-jitter 和 Voice 测试，一次探测操作是指向目的端连续发送多个探测报文，一次探测发送探测报文的个数用户可通过命令行配置。
- 对于 SNMP 测试，一次探测会分别发送一个 SNMPv1、v2c、v3 的探测报文。
- 对于 UDP-tracert 测试，一次探测操作是指向一个节点发送一个特定 TTL 值的探测报文。

6. 测试

一次测试由指定次数的连续的探测组成。

7. 测试频率

测试组连续两次测试开始时间的时间间隔。

8. 测试组

NQA 测试功能以测试组的形式进行组织。每一个测试组都具有一系列的属性，例如，测试类型、目的地址、目的端口、发包频率等。

9. 测试组的标识

测试组由管理员名称和操作标签来标识。为了更好地管理 NQA 的测试组，每个测试组都有一个管理员名称和一个操作标签，通过它们可以唯一确定一个测试组。

10. 测试结果

测试结果是针对测试而言的，记录了本次测试中所有探测的统计结果信息。如果测试只完成了部分探测，那么会显示已经完成探测的结果信息。

11. 历史记录

历史记录是针对探测而言的，每次探测都会生成一次历史记录。

2.2 NQA测试机制

2.2.1 UDP-echo 测试机制

UDP-echo 主要用于探测网络可达性和时延。使用 UDP 报文探测网络可达性和时延时，要求对端必须开启 NQA server，并在 NQA server 上打开对应的 UDP 端口。

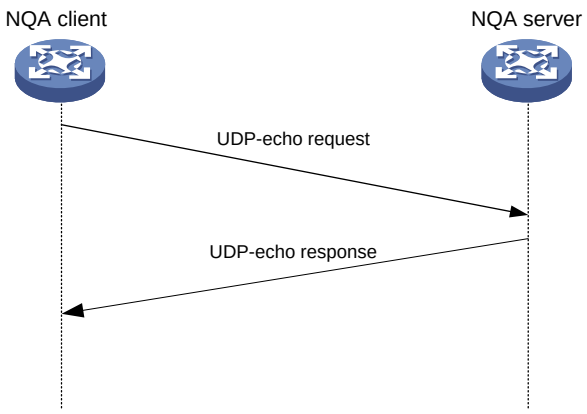
如图 1 所示，UDP-echo 测试机制如下：

(1) NQA 客户端根据配置的探测时间及频率向目的端发送 UDP 报文。

(2) 目的端收到 UDP 报文后，直接利用该报文进行回复。

(3) NQA 客户端根据接收到 UDP 报文的情况，计算到达目的 IP 地址所需的时间及丢包率，以反映当前的网络性能及网络情况。

图1 UDP-echo 测试原理示意图



2.2.2 UDP-tracert 测试机制

UDP-tracert 测试用于发现源端到目的端之间的路径信息。

如图 2 所示，UDP-tracert 测试是基于 ICMP 协议来实现的，和普通 Tracert 流程一致，其原理为：

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

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

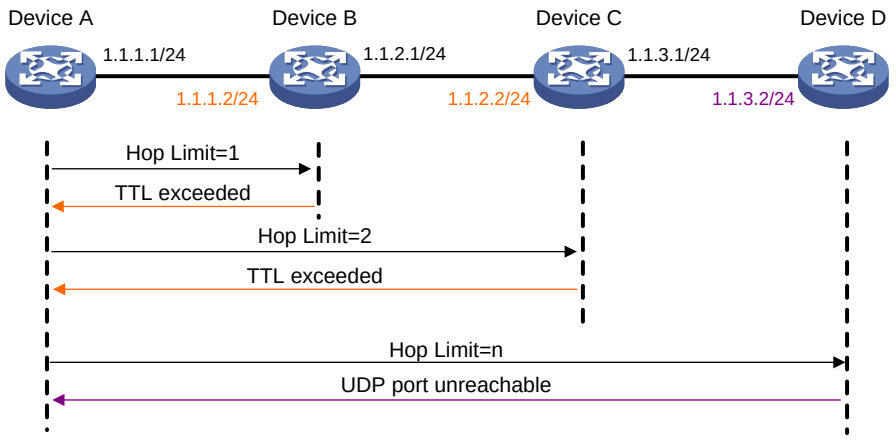
(3) 源端重新向目的端发送一个 IP 数据报文，TTL 值为 2。

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

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

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

图2 UDP-tracert 测试原理示意图



2.2.3 UDP-jitter 测试机制

UDP-jitter 是探测网络状况，监视实时性业务服务质量的重要工具。语音、视频及其它实时业务对时延和时延抖动的要求很高，通过 UDP-jitter 测试可以反映网络的性能，判断网络能否为实时业务提供服务质量保证。

设备还支持高性能模式的 UDP-jitter 测试，用于满足对测试发包数量和时间精度有较高要求的场景。

UDP-jitter 测试报文是私有报文，要求对端必须为 H3C 设备，且开启 NQA server 功能并配置 NQA server 相关参数。

UDP-jitter 测试中每次探测发送一组报文，这组报文只对应一条历史记录。因此，如果想了解 UDP-jitter 测试的结果，建议只查看探测结果，不要查看历史记录。

UDP-jitter 测试结果中存在单向时延信息，如果需要关注此信息，则需要通过时间同步功能（例如 PTP 协议，Precision Time Protocol）保证测试两端设备时间同步到 ms 级；若只关心其他结果，则不要求时间必须同步。

1. UDP-jitter 时延抖动测试

如图 3 所示，UDP-jitter 时延抖动测试原理如下：

(1) NQA client 发送一个 UDP-jitter 报文给 NQA server，并在报文中记录报文离开时间 STxTime。

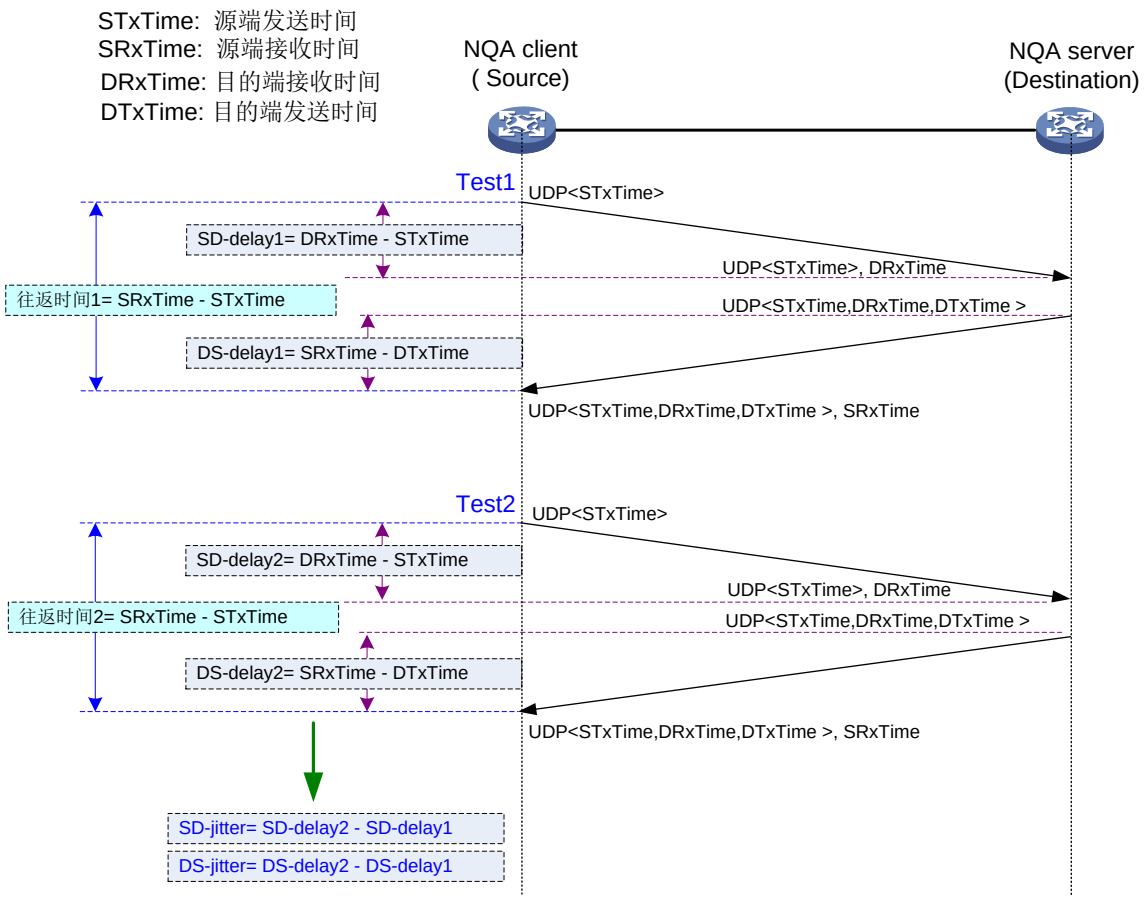
(1) UDP-jitter 报文到达 NQA server，NQA server 在报文中加上接收到该报文的时间 DRxTime。

(2) UDP-jitter 报文离开 NQA server，NQA server 再加上报文离开时的时间 DTxTime。

(3) NQA client 接收到该响应报文，记录接收到响应报文的时间 SRxTime。

(4) NQA client 以固定发包间隔发送多个探测报文，重复上述过程。通过记录的时间戳可以计算出从源端到目的端的时延抖动，以及从目的端到源端的时延抖动。

图3 UDP-jitter 测试时延抖动原理示意图



2. UDP-jitter 单向丢包统计

如图 4 所示，UDP-jitter 客户端和服务器配合，可以统计出报文单向丢包个数。

NQA client 发送的报文中包含报文 ID，每发送一个报文 ID 加 1。NQA server 每收到一个报文，都更新收到的最大报文 ID 和收包个数，并在应答报文中返回给 NQA client；NQA client 记录回应报文个数，并从回应报文中获取 NQA server 端信息。

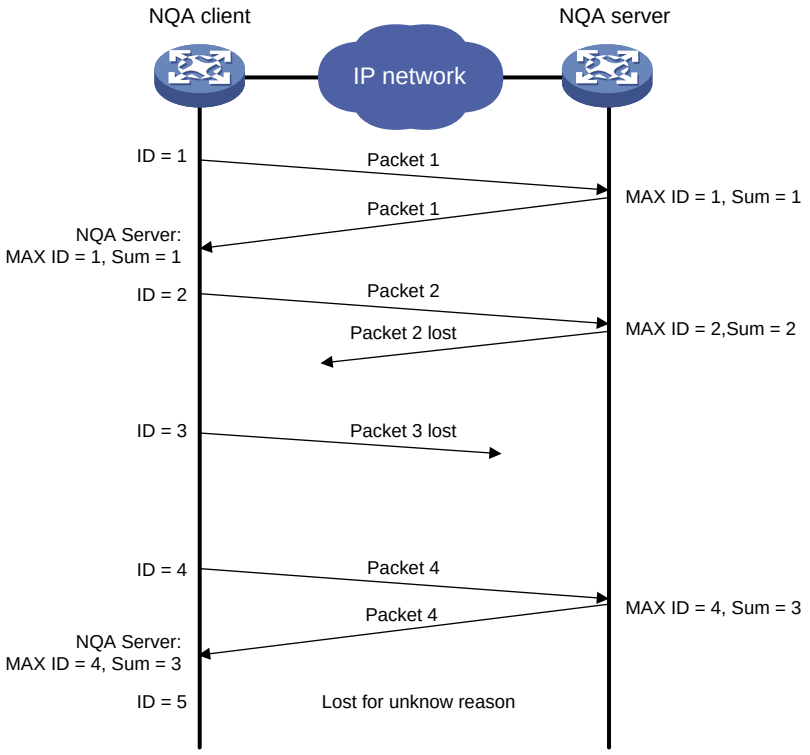
NQA client 可以获取的信息有：

- NQA client 发包个数。
- NQA server 收到的最大报文 ID 和报文个数。
- NQA client 收包个数。

根据这些信息可以计算：

- SD 丢包个数＝NQA server 收到的最大报文 ID－NQA server 端收到报文个数
- DS 丢包个数＝NQA server 端收到报文个数－NQA client 收到报文个数
- 未知方向上丢包个数＝NQA client 发包个数－NQA client 收包个数－SD 丢包个数－DS 丢报个数

图4 UDP-jitter 单向丢包统计原理示意图



2.2.4 Path-jitter 测试机制

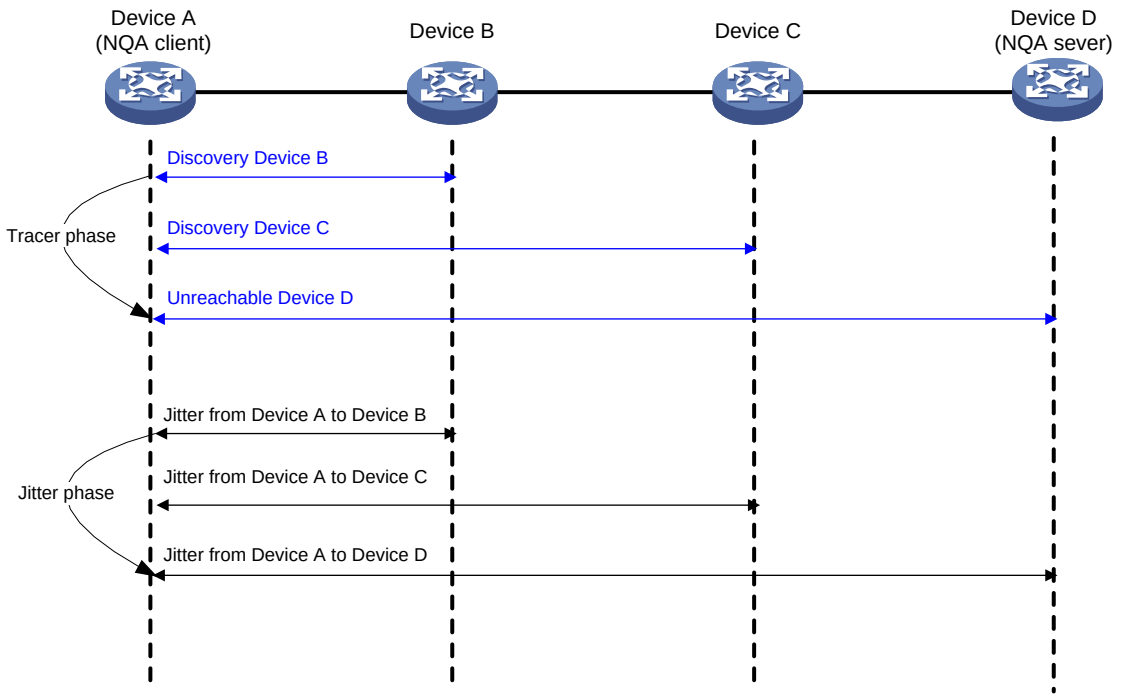
Path-jitter 测试可以作为 UDP-jitter 测试的一种补充，用于在抖动比较大的情况下，进一步探测中间路径的网络质量，以便查找出网络质量差的具体路段。

如图 5 所示，对于 Path-jitter 测试，一次探测操作分为两个步骤：

(1) NQA 客户端使用 Tracert 机制发现到达目的地址的路径信息，最大支持 64 跳。

(2) NQA 客户端根据 Tracert 结果，逐跳使用 ICMP 机制探测从本机至该跳设备的路径上报文是否有丢失，同时计算该路径的时延和抖动时间等信息。Path-jitter 测试会记录每一条路径的探测结果，包括平均抖动值、正向抖动值和负向抖动值等信息。

图5 Path-jitter 测试原理示意图



2.2.5 ICMP-echo 测试机制

ICMP-echo 功能是 NQA 最基本的功能，遵循 RFC 2925 来实现，其实现原理是通过发送 ICMP 报文来判断目的地的可达性、计算网络响应时间及丢包率。

ICMP-echo 测试的功能与 Ping 功能类似，二者的不同之处在于：

- ICMP-echo 测试发送的 ICMP 报文的 TTL 值缺省为 20，在复杂组网跳数较多的情况下，用户可以根据实际组网修改 TTL 值。
- ICMP-echo 测试支持多种测试参数，例如，支持指定测试的下一跳地址，当源端和目的端设备之间存在多条路径时，通过配置下一跳地址可以指定测试的路径。

如图 6 所示，ICMP-jitter 测试的原理如下：

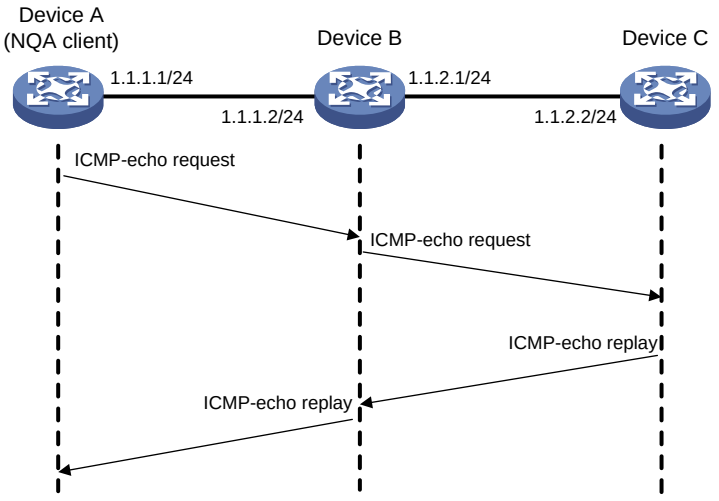
(1) NQA 客户端根据设置的探测时间及频率向探测的目的 IP 地址发送 ICMP echo request 报文。

(2) 目的地址收到 ICMP echo request 报文后，回复 ICMP echo reply 报文。

(3) NQA 客户端根据 ICMP echo reply 报文的接收情况，如接收时间和报文个数，计算出到目的 IP 地址的响应时间及丢包率，从而反映当前的网络性能及网络情况。

ICMP-echo 测试成功的前提条件是目的设备能够正确响应 ICMP echo request 报文。

图6 ICMP-echo 测试原理示意图



2.2.6 ICMP-jitter 测试机制

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

ICMP-jitter 测试和 UDP-jitter 测试原理类似，ICMP-jitter 测试原理如下：

(1) 源端以一定的时间间隔向目的端发送探测报文，并记录报文发送时间。

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

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

需要注意的是，ICMP-jitter 会使用协议规定的 ICMP timestamp 报文，但是该报文曾被国际攻防组织定义为攻击报文，有些防火墙会过滤该报文，导致测试失败。

2.2.7 Voice 测试机制

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

Voice 测试的原理如下：

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

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

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

除了抖动时间等参数，Voice 测试还可以计算出反映 VoIP 网络状况的语音参数值：

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

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

2.2.8 TCP 测试机制

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

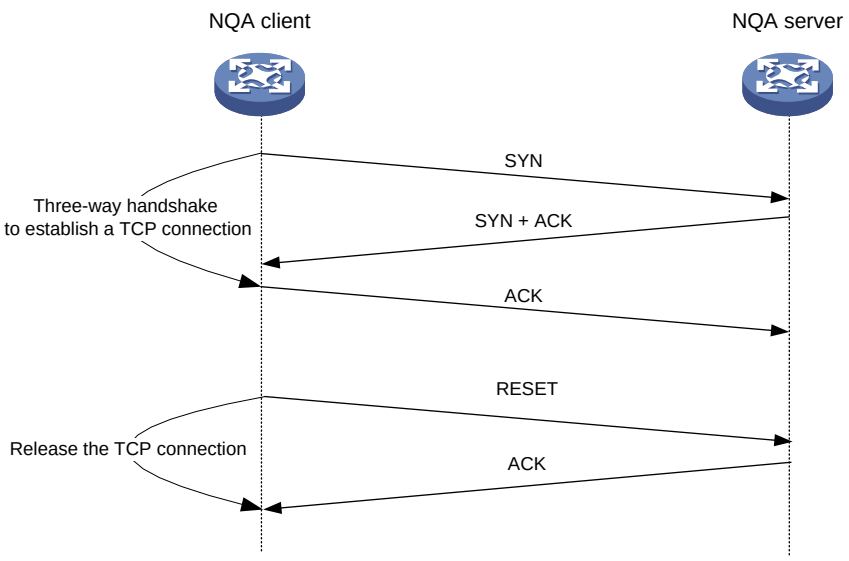
需要注意的是，不能太频繁地发起 TCP 探测，以免占用过多资源，影响目的设备上的正常服务。

如图 7 所示，TCP 测试分为两个步骤：

- 使用三次握手机制建立 TCP 连接。
- 通过 RESET 报文释放 TCP 连接。

能正常建立并释放一次 TCP 连接，则认为本次测试成功。

图7 TCP 测试原理示意图



2.2.9 DHCP 测试机制

DHCP 测试主要用来测试网络上的 DHCP 服务器能否响应客户端请求，以及为客户端分配 IP 地址所需的时间。

测试过程中，NQA 客户端模拟 DHCP 中继转发 DHCP 请求报文，向 DHCP 服务器申请 IP 地址。DHCP 测试完成后，NQA 客户端会主动发送报文释放申请到的 IP 地址。

2.2.10 DLSw 测试机制

DLSw 测试通过向对端设备的 DLSw 协议指定端口发起 TCP 连接，根据连接是否建立，来确认对端设备是否使能了 DLSw 功能。DLSw 测试实现上和 TCP 测试基本一样，可以看作固定目的端口号的 TCP 测试。

2.2.11 DNS 测试机制

DNS 测试通过模拟 DNS client 向指定的 DNS 服务器发送域名解析请求，根据域名解析是否成功及域名解析需要的时间，来判断 DNS 服务器是否可用，及域名解析速度。

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

2.2.12 FTP 测试机制

FTP 测试主要用来测试 NQA 客户端是否可以与指定的 FTP 服务器建立连接，以及与 FTP 服务器之间传送文件的时间，从而判断 FTP 服务器的连通性及性能。

FTP 测试支持 GET 和 PUT 操作，一次探测是指向 FTP 服务器上传一个文件或从 FTP 服务器下载一个文件。

- GET 操作临时将文件下载到本地的文件系统，计算下载该文件所需要的时间，取得数据后立即删除该文件，自动释放占用的内存。如果下载的文件名和 NQA 客户端上已有的文件重名，则覆盖 NQA 客户端原来的文件。
- PUT 操作是上传固定大小及内容的文件到 FTP 服务器。用户可以配置上传的文件的名称，文件内容为系统内部指定的固定数据。如果配置的文件名和 FTP 服务器上已有的文件重名，则覆盖 FTP 服务器原来的文件。

2.2.13 HTTP 测试机制

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

HTTP 测试支持如下操作类型：

- GET：从 HTTP 服务器获取数据。
- POST：向 HTTP 服务器提交数据。
- RAW：向 HTTP 服务器发送 RAW 请求报文。

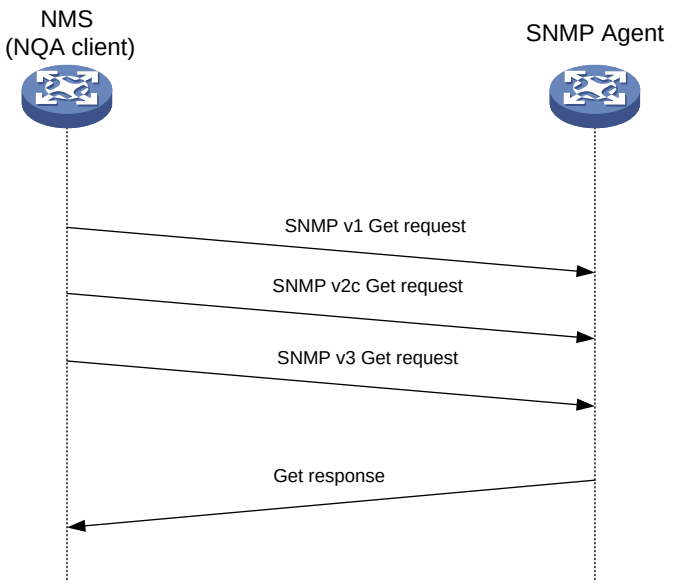
HTTP 测试时，NQA 客户端会向指定地址的 HTTP 服务器发送 GET 请求或者 POST 请求，在接收到回应信息以后，计算整个测试的时间。整个过程只是和 HTTP 服务器建立连接，如果建立连接成功即认为测试成功。

2.2.14 SNMP 测试机制

SNMP 测试由 NQA 客户端向 SNMP Agent 设备发出一个 SNMP Get 请求，根据能否收到应答报文判断 SNMP Agent 上提供的 SNMP 服务是否可用。

目前，网络设备广泛使用的 SNMP 主流版本为 v1、v2c 和 v3。每次测试时，NQA 客户端会对 SNMP v1/v2c/v3 三个版本都进行测试，收到任何一个版本的回复，即认为测试成功，如图 8 所示。

图8 SNMP 测试原理示意图



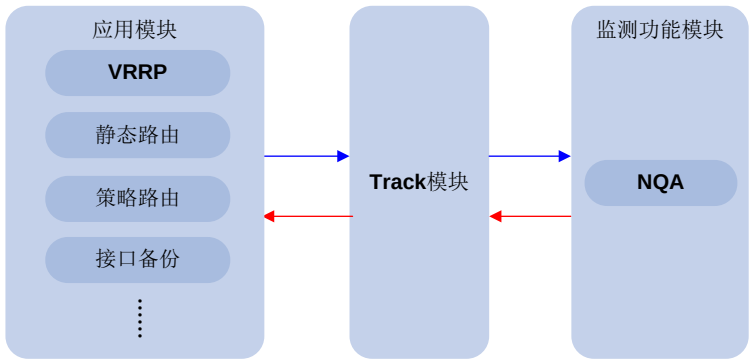
2.2.15 ARP 测试机制

ARP 测试通过向目的端设备发送 ARP 请求报文，根据能否收到应答报文判断目的端设备的 ARP 服务是否可用。

2.3 联动功能机制

如图 9 所示，联动功能是指在监测模块、Track 模块和应用模块之间建立关联，实现这些模块之间的联合动作。NQA 可以作为联动功能的监测模块，对 NQA 探测结果进行监测，当连续探测失败次数达到一定数目时，就通过 Track 模块触发应用模块进行相应的处理。

图9 联动功能原理示意图



目前，NQA 可以通过 Track 模块建立关联的应用模块包括：

- VRRP（Virtual Router Redundancy Protocol，虚拟路由器冗余协议）
- 多机备份
- 静态路由
- 策略路由
- 接口备份
- 流量重定向
- WLAN（Wireless Local Area Network，无线局域网）上行链路检测
- Smart Link

以静态路由为例，用户配置了一条静态路由，下一跳为 192.168.0.88。通过在 NQA、Track 模块和静态路由模块之间建立联动，可以实现静态路由有效性的判断：

(1) 通过 NQA 监测地址 192.168.0.88 是否可达。

(2) 如果 192.168.0.88 可达，则认为该静态路由有效，NQA 不通知 Track 模块改变 Track 项的状态；如果 NQA 发现 192.168.0.88 不可达，则通知 Track 模块改变 Track 项的状态。

(3) Track 模块将改变后的 Track 项状态通知给静态路由模块。静态路由模块据此可以判断该静态路由项是否有效。

2.4 阈值告警功能机制

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

NQA 阈值告警功能支持的阈值类型包括：

- 平均值（average）：监测一次测试中探测结果的平均值，如果平均值不在指定的范围内，则该监测对象超出阈值。例如，监测一次测试中探测持续时间的平均值。
- 累计数目（accumulate）：监测一次测试中探测结果不在指定范围内的累计数目，如果累计数目达到或超过设定的值，则该监测对象超出阈值。

- 连续次数（consecutive）：NQA 测试组启动后，监测探测结果连续不在指定范围内的次数，如果该次数达到或超过设定的值，则该监测对象超出阈值。

NQA 阈值告警功能可以触发如下动作：

- none：只在本地记录监测结果，监测结果可通过显示命令查看，不向网络管理系统发送 Trap 消息。
- trap-only：不仅在本地记录监测结果，当阈值告警项的状态改变时，还可以通过 SNMP 功能向网络管理系统发送 Trap 消息。
- trigger-only：不仅在本地记录监测结果，当阈值告警项的状态改变时，触发其他模块联动。

阈值告警项包括 invalid、over-threshold 和 below-threshold 三种状态：

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

2.5 NQA统计功能

NQA 将在指定时间间隔内完成的 NQA 测试归为一组，计算该组测试结果的统计值，这些统计值构成一个统计组，通过命令可以显示该统计组的信息。

统计组具有老化功能，即统计组保存一定时间后，将被删除。

当 NQA 设备上保留的统计组数目达到最大值时，如果形成新的统计组，保存时间最久的统计组将被删除。

2.6 NQA历史记录功能

开启 NQA 测试组的历史记录保存功能后，系统会将 NQA 测试结果保存在历史记录缓冲区，方便用户查看历史测试的结果。

2.7 NQA server处理机制

进行 UDP-jitter、UDP-echo、TCP 和 Voice 测试时，需要对端设备支持 NQA server 功能，才能完成测试。H3C 设备既支持作为 NQA client，又支持作为 NQA server。当作为 NQA server 时：

- 对于 UDP-echo 测试，NQA server 把接收的报文直接传回客户端。
- 对于 TCP 测试，NQA server 建立监听端口，和客户端建立连接。
- 对于 UDP-jitter 和 Voice 测试，NQA server 需要在报文中打上时间戳，并且记录当前 NQA server 接收到的最大报文 ID、报文个数，并发送给客户端。

3 典型组网案例

NQA 通常应用在联动功能中。NQA 可以通过 Track 模块，实现与 VRRP、静态路由、备份中心、策略路由联动，以便及时发现网络中的故障，避免通信中断或服务质量降低。

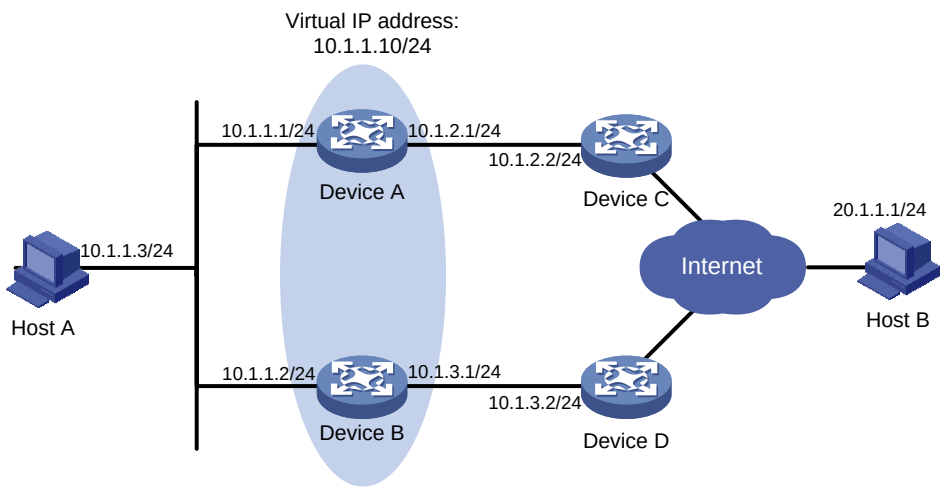
3.1 NQA与VRRP联动

通过 NQA 与 VRRP 联动，可以实现对上行链路的监控。当上行链路出现故障，局域网内的主机无法通过路由器访问外部网络时，NQA 会通过 Track 模块通知 VRRP 将路由器的优先级降低指定的数额。从而，使得备份组内其它路由器的优先级高于这个路由器的优先级，成为 Master 设备，保证局域网内主机与外部网络的通信不会中断。上行链路恢复后，NQA 通过 Track 模块通知 VRRP 恢复路由器的优先级。

如图 10 所示，Device A 和 Device B 组成一台虚拟设备，局域网内的主机 Host A 将虚拟设备设置为默认网关。Device A 和 Device B 中优先级最高的 Device A 作为 Master 设备，承担网关的功能，Device B 作为 Backup 设备。配置 VRRP 通过 Track 和 NQA 进行联动，使用 NQA 监测 10.1.2.2 是否可达。当 10.1.2.2 不可达时，NQA 通过 Track 通知 VRRP，降低 Device A 在备份组中的优先级，从而使 Device B 成为 Master

设备，取代 Master 设备继续履行网关职责，从而保证局域网内的主机可不间断地与外部网络进行通信。当 Device A 故障恢复，NQA 检测到 Device A 路由可达后，能通过 Track 模块立即通知 VRRP。

图10 VRRP 与 NQA 联动组网图

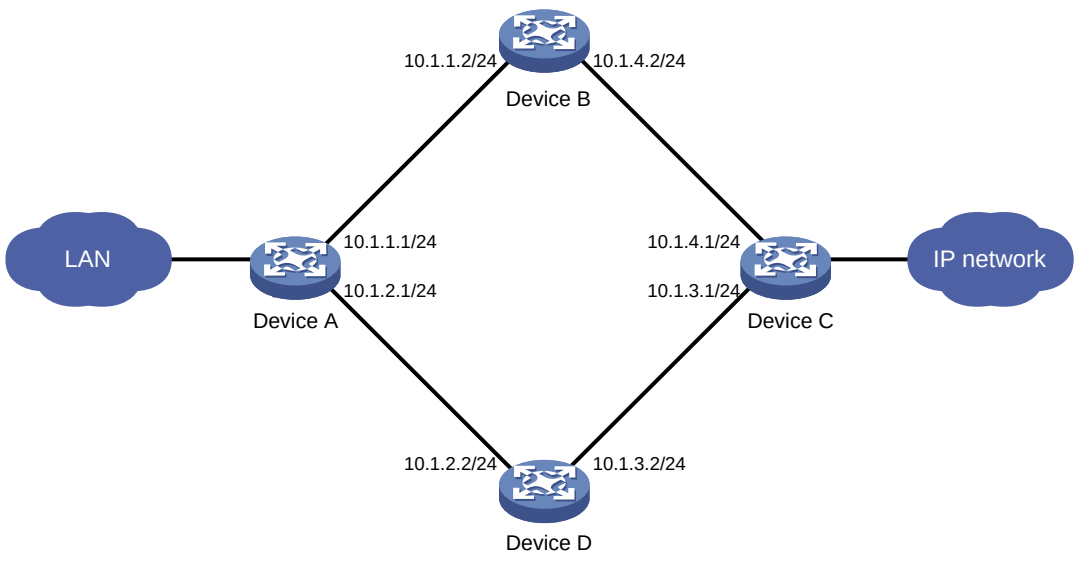


3.2 NQA与静态路由联动

通过在 NQA、Track 模块和静态路由模块之间建立联动，可以实现静态路由有效性的实时判断。利用 NQA 对静态路由的下一跳地址进行探测，如果 NQA 探测成功，则静态路由有效；否则，静态路由无效。

如图 11 所示，Device A 可以通过 Device B、Device D 两条路径达到 Device C，在这四台设备上均配置了动态路由协议 OSPF。Device A 希望通过 Device B 将数据发送给 Device C，于是，在 Device A 上配置到达 Device C 的静态路由下一跳地址为 10.1.1.2，通过 NQA 监测 10.1.1.2 是否可达，并配置静态路由通过 Track 模块与 NQA 实现联动。如果 NQA 发现 10.1.1.2 不可达，它将通过 Track 模块通知静态路由，将该静态路由项置为无效，Device A 将使用动态路由协议生成的路由通过 Device D 将数据发送给 Device C；如果 NQA 发现 10.1.1.2 可达，则通过 Track 模块通知静态路由，将该静态路由项恢复为有效。

图11 NQA 与静态路由联动组网图



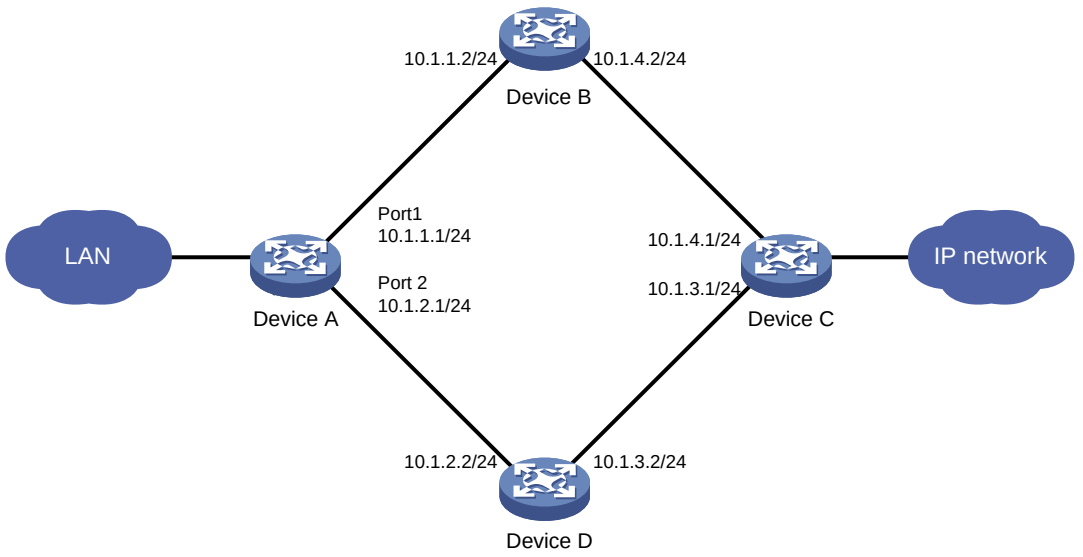
3.3 NQA与接口备份联动

NQA 与接口备份模块联动，用来实现接口根据网络状况动态改变备份状态。

利用 NQA 监测主接口的状态，如果 NQA 监测到主接口所在的链路出现故障，则通过 Track 模块通知接口备份模块，启动备份接口所在的链路进行通信；如果 NQA 监测到与主接口相连的链路恢复正常，则通过 Track 模块通知接口备份模块，仍然通过主接口所在的链路通信。

如图 12 所示，Device A 可以通过 Device B、Device D 两条路径达到 Device C。Device A 上配置配置接口备份功能，Port1 作为主接口，Port2 作为备份接口。正常情况下，主链路为 Device A－Device B－Device C，即数据通过 Device B 发送给 Device C。在 Device A 上配置接口备份与 Track、NQA 联动后，如果 NQA 监测到通过 Device B 到 Device C 的链路故障，导致主链路 Device A－Device B－Device C 不可达，则通过 Track 模块通知接口备份模块，主链路切换为 Device A－Device D－Device C，即数据将通过 Device D 发送给 Device C；如果 NQA 监测到 Device B 到 Device C 的链路恢复正常，则通过 Track 模块通知接口备份模块，主链路倒换为 Device A－Device B－Device C，数据重新通过 Device B 发送给 Device C。

图12 NQA 与接口备份联动组网图



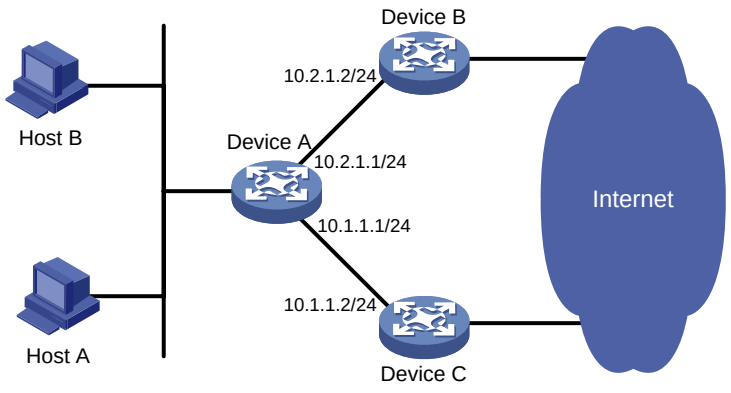
3.4 NQA与策略路由联动

IP 单播策略路由通过与 NQA、Track 联动，增加了应用的灵活性，增强了策略路由对网络环境的动态感知能力。

策略路由可以在配置报文的发送接口、缺省发送接口、下一跳、缺省下一跳时，通过 Track 与 NQA 关联。如果 NQA 探测成功，则该策略有效，可以指导转发；如果探测失败，则该策略无效，转发时忽略该策略。

如图 13 所示，Device A 可以通过 Device B 和 Device C 两个设备连入 Internet。在 Device A 上定义策略路由，实现 Device A 连接局域网接口接收到的所有 TCP 报文通过 Device B 转发（报文的下一跳地址为 10.2.1.2）。同时，配置策略路由与 NQA、Track 联动，利用 NQA 探测 Device B 的可达性。如果 Device B 可达，则该策略可以指导转发，接口接收到的 TCP 报文下一跳地址为 10.2.1.2；否则，该策略无效，接口接收到的 TCP 报文根据路由查找可用的下一跳。

图13 NQA 与策略路由联动组网图



NQA 配置

目 录

1 NQA

1.1 NQA配置任务简介

NQA 配置任务如下：

(1) 配置 NQA 服务器

在进行 TCP、UDP-echo、UDP-jitter 和 Voice 类型测试前，必须在目的端设备上进行本配置。进行其他类型测试时，不需要进行本配置。

(2) 开启 NQA 客户端功能

(3) 配置 NQA 测试组和模板

请至少选择以下一项任务进行配置：

- 在 NQA 客户端上配置 NQA 测试组
- 在 NQA 客户端上配置 NQA 模板

NQA 测试组配置完毕后，通过调度或启动测试组就可以进行测试操作；NQA 模板配置完毕后并不启动测试，需要从外部特性（如负载均衡）调用 NQA 模板后，设备自动创建 NQA 测试组并启动 NQA 测试。

1.2 配置NQA服务器

1. 配置限制和指导

对于 NQA 服务器的启动要求：

- TCP、UDP-echo、UDP-jitter 和 Voice 类型测试，测试前必须在目的端设备上开启 NQA 服务器，并配置对应的 TCP/UDP 监听服务。
- 路径服务质量和 Y.1564 类型测试，测试前必须在目的端设备上开启 NQA 服务器，并配置服务器的报文反射功能。
- 其他类型测试，无须在目的端设备上开启 NQA 服务器，只须在目的端设备开启相应服务即可。

UDP-jitter 测试的高性能模式下，NQA 服务器端不能处理大于 100 字节的 NQA 报文，若客户端发送的报文长度大于 100 字节，可能导致 NQA 测试失败。

在一个 NQA 服务器上可以配置多个 TCP（或 UDP）监听服务，每个监听服务对应一个监听的 IP 地址和一个端口号。

NQA 服务器上配置的监听 IP 地址、端口号、VPN 参数必须与 NQA 客户端上的配置一致，且不能与已有的 TCP（或 UDP）监听服务冲突。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) （可选）在 NQA 服务器上配置 TCP 监听服务。

nqa server tcp-connect { *ipv4-address* | **ipv6** *ipv6-address* } *port-number* [**vpn-instance** *vpn-instance-name*] [**tos** *tos*]

仅 TCP 和 DLSw 测试类型下必须进行本命令，且对于 DLSw 测试类型，*port-number* 值必须为 2065。否则，测试失败。

(3) （可选）在 NQA 服务器上配置 UDP 监听服务。

nqa server udp-echo { *ipv4-address* | **ipv6** *ipv6-address* } *port-number* [**vpn-instance** *vpn-instance-name*] [**high-performance-mode**] [**tos** *tos*]

仅 UDP-echo、UDP-jitter 和 Voice 测试类型下必须进行本配置。

(4) 在 NQA 服务器上配置路径服务质量和 Y.1564 测试的反射参数。

nqa reflector *reflector-id* **interface** *interface-type interface-number* [**service-instance** *instance-id*] { { **ip** | **ipv6** } { **destination** *address1* [**to** *address2*] | **source** *address1* [**to** *address2*] } * | **source-port**

port-number1 [**to** *port-number2*] | **destination-port** *port-number1* [**to** *port-number2*] | **destination-mac** *mac-address1* [**to** *mac-address2*] | **source-mac** *mac-address1* [**to** *mac-address2*] | **vlan** { *vlan-id1* [**to** *vlan-id2*] | **s-vid** *vlan-id1* [**to** *vlan-id2*] **c-vid** *vlan-id1* [**to** *vlan-id2*] } | **exchange-port** | **vpn-instance** *vpn-instance-name* } *

缺省情况下，未配置路径服务质量和 Y.1564 测试的反射参数。

(5) 开启 NQA 服务器功能。

nqa server enable

缺省情况下，NQA 服务器功能处于关闭状态。

1.3 开启NQA客户端功能

(1) 进入系统视图。

system-view

(2) 使能 NQA 客户端功能。

nqa agent enable

缺省情况下，NQA 客户端功能处于开启状态。

只有使能 NQA 客户端功能后，NQA 客户端的相关配置才会生效。

1.4 在NQA客户端上配置NQA测试组

1.4.1 NQA 测试组配置任务简介

管理员通过 NQA 测试组来实现对 NQA 测试的管理和调度。在一台设备上可以创建多个 NQA 测试组，可以同时启动多个 NQA 测试组进行测试。

NQA 测试组配置任务如下：

(1) 配置 NQA 测试组

- 配置 ICMP-echo 测试
- 配置 ICMP-jitter 测试
- 配置 DHCP 测试
- 配置 DNS 测试
- 配置 FTP 测试
- 配置 HTTP 测试
- 配置 UDP-jitter 测试
- 配置 SNMP 测试
- 配置 TCP 测试
- 配置 UDP-echo 测试
- 配置 UDP-tracert 测试
- 配置 Voice 测试
- 配置 DLSw 测试
- 配置 Path-jitter 测试
- 配置 Y.1564 测试
- 配置路径服务质量测试

(2) （可选）配置 NQA 测试组通用参数

(3) （可选）配置联动功能

(4) （可选）配置阈值告警功能

(5) （可选）配置 NQA 统计功能

(6) （可选）配置 NQA 历史记录功能

(7) 在 NQA 客户端上调度 NQA 测试组

1.4.2 配置 ICMP-echo 测试

1. 功能简介

ICMP-echo 测试利用 ICMP 协议，根据是否接收到应答报文判断目的主机的可达性。ICMP-echo 测试的功能与 **ping** 命令类似，但 ICMP-echo 测试中可以指定测试的下一跳设备。在源端和目的端设备之间存在多条路径时，通过配置下一跳设备可以指定测试的路径。并且，与 **ping** 命令相比，ICMP-echo 测试输出的信息更为丰富。

对于 ICMP-echo 测试，一次探测操作是指向目的端发送一个探测报文。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 NQA 测试组，并进入 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(3) 配置测试类型为 ICMP-echo，并进入测试类型视图。

type icmp-echo

(4) 配置探测报文的目的地址。

（IPv4 网络）

destination ip *ip-address*

缺省情况下，未配置探测报文的目的地址。

（IPv6 网络）

destination ipv6 *ipv6-address*

缺省情况下，未配置探测报文的目的地址。

(5) 配置探测报文的源地址。请选择其中一项进行配置。

- 使用指定接口的 IP 地址作为探测报文的源 IP 地址。

  source interface *interface-type interface-number*

  缺省情况下，以报文发送接口的主 IP 地址作为探测报文中的源 IP 地址。

  source interface 命令指定的接口必须为 up 状态。

- 配置探测报文的源 IPv4 地址。

  source ip *ip-address*

  缺省情况下，以报文发送接口的主 IPv4 地址作为探测报文中的源 IPv4 地址。

  该命令指定的源地址必须是设备上接口的 IP 地址，且接口为 up 状态，否则测试将会失败。

- 配置探测报文的源 IPv6 地址。

  source ipv6 *ipv6-address*

  缺省情况下，以报文发送接口的 IPv6 地址作为探测报文中的源 IPv6 地址。

  该命令指定的源地址必须是设备上接口的 IPv6 地址，且接口为 up 状态，否则测试将会失败。

(6) 配置探测报文出接口或下一跳 IP 地址。请选择其中一项进行配置。

- 配置探测报文出接口。

  out interface *interface-type interface-number*

  缺省情况下，设备通过查询路由表信息确认探测报文出接口。
- 配置探测报文的下一跳 IPv4 地址。

  next-hop ip *ip-address*

  缺省情况下，未配置探测报文的下一跳 IPv4 地址。
- 配置探测报文的下一跳 IPv6 地址。

  next-hop ipv6 *ipv6-address*

  缺省情况下，未配置探测报文的下一跳 IPv6 地址。

(7) （可选）配置探测报文中的填充内容大小。

data-size *size*

缺省情况下，探测报文中的填充内容大小为 100 字节。

(8) （可选）配置探测报文的填充字符串。

data-fill *string*

本命令的缺省情况与设备型号有关，请以设备的实际情况为准。

1.4.3 配置 ICMP-jitter 测试

1. 功能简介

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

ICMP-jitter 测试的过程如下：

(1) 源端以一定的时间间隔向目的端发送探测报文。

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

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

对于 ICMP-jitter 测试，一次探测操作是指向目的端连续发送多个探测报文，发送探测报文的个数由 **probe packet-number** 命令来设定。

2. 配置限制和指导

display nqa history 命令的显示信息无法反映 ICMP-jitter 测试的结果，如果想了解 ICMP-jitter 测试的结果，建议通过 **display nqa result** 命令查看最近一次 NQA 测试的当前结果，或通过 **display nqa statistics** 命令查看 NQA 测试的统计信息。

进行本测试前需保证网络时钟的 NTP 同步。有关 NTP 的详细介绍请参见“网络管理和监控配置指导”的“NTP”。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 NQA 测试组，进入 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(3) 配置测试类型为 ICMP-jitter，并进入测试类型视图。

type icmp-jitter

(4) 配置探测报文的目的 IP 地址。

destination ip *ip-address*

缺省情况下，未配置探测报文的目的 IP 地址。

(5) 配置一次 ICMP-jitter 探测中发送探测报文的个数。

probe packet-number *number*

缺省情况下，一次 ICMP-jitter 探测中发送 10 个探测报文。

(6) 配置 ICMP-jitter 测试中发送探测报文的时间间隔。

probe packet-interval *interval*

缺省情况下，ICMP-jitter 测试中发送探测报文的时间间隔为 20 毫秒。

(7) 配置 ICMP-jitter 测试中等待响应报文的超时时间。

probe packet-timeout *timeout*

缺省情况下，ICMP-jitter 测试中等待响应报文的超时时间为 3000 毫秒。

(8) 配置探测报文的源 IP 地址。

source ip *ip-address*

缺省情况下，以报文发送接口的主 IP 地址作为探测报文中的源 IP 地址。

该命令指定的源地址必须是设备上接口的 IP 地址，且接口为 up 状态，否则测试将会失败。

1.4.4 配置 DHCP 测试

1. 功能简介

DHCP 测试主要用来测试网络上的 DHCP 服务器能否响应客户端请求，以及为客户端分配 IP 地址所需的时间。

NQA 客户端模拟 DHCP 中继转发 DHCP 请求报文向 DHCP 服务器申请 IP 地址的过程，DHCP 服务器进行 DHCP 测试的接口 IP 地址不会改变。DHCP 测试完成后，NQA 客户端会主动发送报文释放申请到的 IP 地址。

对于 DHCP 测试，一次探测操作是指完成一次向 DHCP 服务器申请一个 IP 地址。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 NQA 测试组，并进入 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(3) 配置测试类型为 DHCP，并进入测试类型视图。

type dhcp

(4) 配置探测报文的目的 IP 地址。

destination ip *ip-address*

缺省情况下，未配置探测报文的目的 IP 地址。

(5) 配置探测报文出接口。

out interface *interface-type interface-number*

缺省情况下，设备通过查询路由表信息确认探测报文出接口。

(6) 配置探测报文的源 IP 地址。

source ip *ip-address*

缺省情况下，以报文发送接口的主 IP 地址作为探测报文中的源 IP 地址。

该命令指定的源地址必须是设备上接口的 IP 地址，且接口为 up 状态，否则测试将会失败。

1.4.5 配置 DNS 测试

1. 功能简介

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

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

对于 DNS 测试，一次探测操作是指完成一次将一个域名解析为 IP 地址。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 NQA 测试组，并进入 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(3) 配置测试类型为 DNS，并进入测试类型视图。

type dns

(4) 配置探测报文的目的 IP 地址。

destination ip *ip-address*

缺省情况下，未配置探测报文的目的 IP 地址。

(5) 配置要解析的域名。

resolve-target *domain-name*

缺省情况下，没有配置要解析的域名。

1.4.6 配置 FTP 测试

1. 功能简介

FTP 测试主要用来测试 NQA 客户端是否可以与指定的 FTP 服务器建立连接，以及与 FTP 服务器之间传送文件的时间，从而判断 FTP 服务器的连通性及性能。

在进行 FTP 测试之前，需要获取 FTP 用户的用户名和密码。

对于 FTP 测试，一次探测操作是指完成一次向 FTP 服务器上传或下载一个文件。

2. 配置限制和指导

进行 **put** 操作时，若配置了 **filename**，发送数据前判断 **filename** 指定的文件是否存在，如果存在则上传该文件，如果不存在则探测失败。

进行 **get** 操作时，如果 FTP 服务器上没有以 **url** 中所配置的文件名为名称的文件，则测试不会成功。进行 **get** 操作时，设备上不会保存从服务器获取的文件。

进行 **get**、**put** 操作时，请选用较小的文件进行测试，如果文件较大，可能会因为超时而导致测试失败，或由于占用较多的网络带宽而影响其他业务。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 NQA 测试组，并进入 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(3) 配置测试类型为 FTP，并进入测试类型视图。

type ftp

(4) 配置 FTP 登录用户名。

username *username*

缺省情况下，未配置 FTP 登录用户名。

(5) 配置 FTP 登录密码。

password { **cipher** | **simple** } *string*

缺省情况下，未配置 FTP 登录密码。

(6) 配置探测报文的源 IP 地址。

source ip *ip-address*

缺省情况下，以报文发送接口的主 IP 地址作为探测报文中的源 IP 地址。

该命令指定的源地址必须是设备上接口的 IP 地址，且接口为 up 状态，否则测试将会失败。

(7) 配置 FTP 测试的数据传输方式。

mode { **active** | **passive** }

缺省情况下，FTP 测试的数据传输方式为主动方式。

(8) 配置 FTP 测试的操作类型。

operation { **get** | **put** }

缺省情况下，FTP 操作方式为 **get** 操作，即从 FTP 服务器获取文件。

(9) 配置 FTP 测试访问的网址。

url *url*

缺省情况下，没有配置 FTP 测试访问的网址。

url 可以设置为 ftp://*host*/*filename* 或 ftp://*host*:*port*/*filename*。当 FTP 测试的操作类型为 **get** 方式时，必须在 *url* 中配置 *filename* 指定从 FTP 服务器获取的文件名。

(10) 配置 FTP 服务器和客户端传送文件的文件名。

filename *filename*

缺省情况下，未配置 FTP 服务器和客户端之间传送文件的文件名。

当 FTP 测试的操作类型为 **put** 方式时，必须配置本命令来指定向 FTP 服务器传送的文件。当 FTP 测试的操作类型为 **get** 方式时，不以此命令为准。

1.4.7 配置 HTTP 测试

1. 功能简介

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

HTTP 测试支持如下操作类型：

- **get**：从 HTTP 服务器获取数据。
- **post**：向 HTTP 服务器提交数据。
- **raw**：向 HTTP 服务器发送 RAW 请求报文。

对于 HTTP 测试，一次探测操作是指完成一次相应操作类型的功能。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 NQA 测试组，并进入 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(3) 配置测试类型为 HTTP，并进入测试类型视图。

type http

(4) 配置 HTTP 测试访问的网址。

url *url*

缺省情况下，没有配置 HTTP 测试访问的网址。

url 配置形式为 http://*host/resource* 或 http://*host:port/resource*。

(5) 配置 HTTP 登录用户名。

username *username*

缺省情况下，未配置 HTTP 登录用户名。

(6) 配置 HTTP 登录密码。

password { **cipher** | **simple** } *string*

缺省情况下，未配置 HTTP 登录密码。

(7) 配置 HTTP 测试所使用的协议版本。

version { v1.0 | v1.1 }

缺省情况下，HTTP 测试使用的版本为 1.0。

(8) 配置 HTTP 测试的操作类型。

operation { **get** | **post** | **raw** }

缺省情况下，HTTP 操作方式为 **get** 操作。如果 HTTP 操作方式为 **raw** 操作，则向服务器发送的探测报文的内容为 **raw-request** 视图中的内容。

(9) 配置 HTTP 测试请求报文。

a. 进入 raw-request 视图。

raw-request

输入 **raw-request** 命令进入 raw-request 视图，每次进入视图原有报文内容清除。

b. 配置 HTTP 测试请求报文内容。

逐个字符输入或拷贝粘贴请求报文内容。

缺省情况下，未配置 HTTP 测试请求报文内容。

要求报文内容中不能包含 **alias** 命令配置的别名，请用户自行确保报文的正确性，否则探测将失败。有关 **alias** 命令的详细介绍请参见“基础配置命令参考”中的“CLI”。

c. 保存输入内容并退回测试类型视图。

quit

当配置 HTTP 测试的操作类型为 **raw** 时，必须完成此操作且保证发送的测试报文正确有效。

(10) 配置探测报文的源 IP 地址。

source ip *ip-address*

缺省情况下，以报文发送接口的主 IP 地址作为探测报文中的源 IP 地址。

该命令指定的源地址必须是设备上接口的 IP 地址，且接口为 up 状态，否则测试将会失败。

1.4.8 配置 UDP-jitter 测试

1. 功能简介

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

UDP-jitter 测试的过程如下：

(1) 源端以一定的时间间隔向目的端发送探测报文。

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

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

对于 UDP-jitter 测试，一次探测操作是指连续发送多个探测报文，发送探测报文的个数由 **probe packet-number** 命令来设定。

UDP-jitter 测试需要 NQA 服务器和客户端配合才能完成。进行 UDP-jitter 测试之前，必须保证 NQA 服务器端配置了 UDP 监听功能，配置方法请参见“1.2 配置 NQA 服务器”。

2. 配置限制和指导

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

display nqa history 命令的显示信息无法反映 UDP-jitter 测试的结果，如果想了解 UDP-jitter 测试的结果，建议通过 **display nqa result** 命令查看最近一次 NQA 测试的当前结果，或通过 **display nqa statistics** 命令查看 NQA 测试的统计信息。

进行本测试前需保证网络时钟的 NTP 同步。有关 NTP 的详细介绍请参见“网络管理和监控配置指导”的“NTP”。

开启高性能模式后，命令 **route-option bypass-route**、**data-size**、**reaction checked-element** { **jitter-ds** | **jitter-sd** } **threshold-type accumulate**、**reaction checked-element rtt threshold-type accumulate** 将不再生效。

UDP-jitter 测试的高性能模式在客户端和服务器端都需要开启，且要求客户端发送的报文长度必须小于等于 100 字节，否则，可能导致 NQA 测试失败。使用 **data-size** 可配置探测报文中的填充内容的大小。

如需测试链路传输 MPLS 报文时的服务质量，必须先开启 UDP-jitter 测试的高性能模式，且只能测试直连链路上 MPLS 流量的服务质量。请在直连链路的两端配置 NQA 客户端和服务器，并使用 **mpls enable** 命令开启接口的 MPLS 功能。有关 **mpls enable** 命令的详细介绍，请参见“MPLS 命令参考”的“MPLS 基础”。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 NQA 测试组，并进入 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(3) 配置测试类型为 UDP-jitter，并进入测试类型视图。

type udp-jitter

(4) （可选）开启 UDP-jitter 测试的高性能模式。

high-performance-mode enable

缺省情况下，UDP-jitter 测试的高性能模式处于关闭状态。

(5) （可选）开启 UDP-jitter 测试的 MPLS 模拟测试功能。

mpls-simulation enable [**exp** *exp-value*]

缺省情况下，UDP-jitter 测试的 MPLS 模拟测试功能处于关闭状态。

(6) 配置探测报文的目的地址。

（IPv4 网络）

destination ip *ip-address*

缺省情况下，未配置探测报文的目的 IPv4 地址。

必须与 NQA 服务器上 **nqa server udp-echo** 命令配置的监听服务的 IPv4 地址一致。

（IPv6 网络）

destination ipv6 *ipv6-address*

缺省情况下，未配置探测报文的目的 IPv6 地址。

必须与 NQA 服务器上 **nqa server udp-echo** 命令配置的监听服务的 IPv6 地址一致。

MPLS 模拟测试功能暂不支持使用 IPv6 地址作为探测报文的目的地址。

(7) 配置测试操作的目的端口。

destination port *port-number*

缺省情况下，未配置测试操作的目的端口号。

必须与 NQA 服务器上 **nqa server udp-echo** 命令配置的监听服务的端口号一致。

(8) 配置探测报文的源地址。

（IPv4 网络）

source ip *ip-address*

缺省情况下，以报文发送接口的主 IPv4 地址作为探测报文中的源 IPv4 地址。

该命令指定的源地址必须是设备上接口的 IP 地址，且接口为 up 状态，否则测试将会失败。

（IPv6 网络）

source ipv6 *ipv6-address*

缺省情况下，以报文发送接口的 IPv6 地址作为探测报文中的源 IPv6 地址。

该命令指定的源地址必须是设备上接口的 IPv6 地址，且接口为 up 状态，否则测试将会失败。

(9) 配置探测报文的源端口。

source port *port-number*

缺省情况下，系统自动选择设备当前空闲的端口号。

(10) （可选）配置探测报文出接口。

out interface *interface-type interface-number*

缺省情况下，设备通过查询路由表信息确认探测报文出接口。

(11) 配置一次 UDP-jitter 探测中发送探测报文的个数。

probe packet-number *number*

缺省情况下，一次 UDP-jitter 探测中发送 10 个探测报文。

(12) 配置 UDP-jitter 测试中发送探测报文的时间间隔。

probe packet-interval *interval*

缺省情况下，UDP-jitter 测试中发送探测报文的时间间隔为 20 毫秒。

(13) 配置 UDP-jitter 测试中等待响应报文的超时时间。

probe packet-timeout *timeout*

缺省情况下，UDP-jitter 测试中等待响应报文的超时时间为 3000 毫秒。

(14) 配置探测报文中的填充内容的大小。

data-size *size*

缺省情况下，探测报文中的填充内容大小为 100 字节。

(15) （可选）配置探测报文的填充字符串。

data-fill *string*

本命令的缺省情况与设备型号有关，请以设备的实际情况为准。

1.4.9 配置 SNMP 测试

1. 功能简介

SNMP 测试主要测试从 NQA 客户端向 SNMP Agent 设备发出一个 SNMP 协议查询，根据能否收到应答报文判断 SNMP Agent 上提供的 SNMP 服务是否可用。

对于 SNMP 测试，一次探测操作是指发送三个 SNMP 协议报文，分别对应 SNMPv1、SNMPv2c 和 SNMPv3 三个版本。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 NQA 测试组，并进入 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(3) 配置测试类型为 SNMP，并进入测试类型视图。

type snmp

(4) 配置探测报文的目的地址。

destination ip *ip-address*

缺省情况下，未配置探测报文的目的 IP 地址。

(5) 配置测试操作的目的端口。

destination port *port-number*

缺省情况下，测试操作的目的端口号为 161。

(6) 配置探测报文的源 IP 地址。

source ip *ip-address*

缺省情况下，以报文发送接口的主 IP 地址作为探测报文中的源 IP 地址。

该命令指定的源地址必须是设备上接口的 IP 地址，且接口为 up 状态，否则测试将会失败。

(7) 配置探测报文的源端口。

source port *port-number*

缺省情况下，系统自动选择设备当前空闲的端口号。

(8) 配置用于 SNMPv1 或者 SNMPv2c 探测报文的团体名。

community read { **cipher** | **simple** } *community-name*

缺省情况下，SNMPv1 或者 SNMPv2c 探测报文使用的团体名为 public。

该命令配置的团体名必须为 SNMP Agent 上已配置具有读权限的团体名。

1.4.10 配置 TCP 测试

1. 功能简介

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

TCP 测试需要 NQA 服务器和客户端配合才能完成。在 TCP 测试之前，需要在 NQA 服务器端配置 TCP 监听功能，配置方法请参见“1.2 配置 NQA 服务器”。

对于 TCP 测试，一次探测操作是指建立一次 TCP 连接。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 NQA 测试组，并进入 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(3) 配置测试类型为 TCP，并进入测试类型视图。

type tcp

(4) 配置探测报文的目的地址。

（IPv4 网络）

destination ip *ip-address*

缺省情况下，未配置探测报文的目的 IPv4 地址。

必须与 NQA 服务器上 **nqa server tcp-connect** 命令配置的监听服务的 IPv4 地址一致。

（IPv6 网络）

destination ipv6 *ipv6-address*

缺省情况下，未配置探测报文的目的 IPv6 地址。

必须与 NQA 服务器上 **nqa server tcp-connect** 命令配置的监听服务的 IPv6 地址一致。

(5) 配置测试操作的目的端口。

destination port *port-number*

缺省情况下，未配置测试操作的目的端口号。

必须与 NQA 服务器上 **nqa server tcp-connect** 命令配置的监听服务的端口号一致。

(6) 配置探测报文的源地址。

（IPv4 网络）

source ip *ip-address*

缺省情况下，以报文发送接口的主 IPv4 地址作为探测报文中的源 IPv4 地址。

该命令指定的源地址必须是设备上接口的 IP 地址，且接口为 up 状态，否则测试将会失败。

（IPv6 网络）

source ipv6 *ipv6-address*

缺省情况下，以报文发送接口的 IPv6 地址作为探测报文中的源 IPv6 地址。

该命令指定的源地址必须是设备上接口的 IPv6 地址，且接口为 up 状态，否则测试将会失败。

1.4.11 配置 UDP-echo 测试

1. 功能简介

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

UDP-echo 测试需要 NQA 服务器和客户端配合才能完成。在进行 UDP-echo 测试之前，需要在 NQA 服务器端配置 UDP 监听功能，配置方法请参见“1.2 配置 NQA 服务器”。

对于 UDP-echo 测试，一次探测操作是指发送一个探测报文。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 NQA 测试组，并进入 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(3) 配置测试类型为 UDP-echo，并进入测试类型视图。

type udp-echo

(4) 配置探测报文的目的地址。

（IPv4 网络）

destination ip *ip-address*

缺省情况下，未配置探测报文的目的 IPv4 地址。

必须与 NQA 服务器上 **nqa server udp-echo** 命令配置的监听服务的 IPv4 地址一致。

（IPv6 网络）

destination ipv6 *ipv6-address*

缺省情况下，未配置探测报文的目的 IPv6 地址。

必须与 NQA 服务器上 **nqa server udp-echo** 命令配置的监听服务的 IPv6 地址一致。

(5) 配置测试操作的目的端口。

destination port *port-number*

缺省情况下，未配置测试操作的目的端口号。

必须与 NQA 服务器上 **nqa server udp-echo** 命令配置的监听服务的端口号一致。

(6) 配置探测报文的源地址。

（IPv4 网络）

source ip *ip-address*

缺省情况下，以报文发送接口的主 IPv4 地址作为探测报文中的源 IPv4 地址。

该命令指定的源地址必须是设备上接口的 IP 地址，且接口为 up 状态，否则测试将会失败。

（IPv6 网络）

source ipv6 *ipv6-address*

缺省情况下，以报文发送接口的 IPv6 地址作为探测报文中的源 IPv6 地址。

该命令指定的源地址必须是设备上接口的 IPv6 地址，且接口为 up 状态，否则测试将会失败。

(7) 配置探测报文的源端口。

source port *port-number*

缺省情况下，系统自动选择设备当前空闲的端口号。

(8) （可选）配置探测报文中的填充内容大小。

data-size *size*

缺省情况下，探测报文中的填充内容大小为 100 字节。

(9) （可选）配置探测报文的填充字符串。

data-fill *string*

本命令的缺省情况与设备型号有关，请以设备的实际情况为准。

1.4.12 配置 UDP-tracert 测试

1. 功能简介

UDP-tracert 测试可以用来发现源端到目的端之间的路径信息。UDP-tracert 测试和普通 Tracert 流程一致，由源端发送一个目的端口不可达的报文，当目的端收到该报文后，会回复源端一个端口不可达报文，以便使源端知道 Tracert 测试结束。

对于 UDP-tracert 测试，一次探测操作是指一个特定 TTL 值的节点发送一个探测报文。

2. 配置限制和指导

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

3. 配置准备

配置 UDP-tracert 测试需要在中间设备（源端与目的端之间的设备）上开启 ICMP 超时报文发送功能。如果中间设备是 H3C 设备，需要在设备上执行 **ip ttl-expires enable** 命令（该命令的详细介绍请参见“三层技术-IP 业务命令参考”中的“IP 性能优化”）。

需要在目的端开启 ICMP 目的不可达报文发送功能。如果目的端是 H3C 设备，需要在设备上执行 **ip unreachables enable** 命令（该命令的详细介绍请参见“三层技术-IP 业务命令参考”中的“IP 性能优化”）。

4. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 NQA 测试组，并进入 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(3) 配置测试类型为 UDP-tracert，并进入测试类型视图。

type udp-tracert

(4) 配置探测报文的目的主机名或目的 IP 地址。请选择其中一项进行配置。

- 配置探测报文的目的主机名。

  destination host *host-name*

  缺省情况下，未配置探测报文的目的主机名。

- 配置探测报文的目的 IP 地址。

  destination ip *ip-address*

  缺省情况下，未配置探测报文的目的 IP 地址。

(5) 配置测试操作的目的端口。

destination port *port-number*

缺省情况下，测试操作的目的端口号为 33434。

该端口必须是对端设备上未启用的端口，这样对端设备会回复目的端口不可达的 ICMP 差错报文。

(6) 配置探测报文的出接口。

out interface *interface-type interface-number*

缺省情况下，设备通过查询路由表信息确认探测报文出接口。

(7) 配置探测报文的源 IP 地址。请选择其中一项进行配置。

- 配置使用指定接口的 IP 地址作为探测报文的源 IP 地址。

  source interface *interface-type interface-number*

  缺省情况下，以报文发送接口的主 IP 地址作为探测报文中的源 IP 地址。

  该命令指定的接口必须为 up 状态，否则测试会失败。

- 配置探测报文的源 IP 地址。

  source ip *ip-address*

  缺省情况下，以报文发送接口的主 IP 地址作为探测报文中的源 IP 地址。

  该命令指定的源地址必须是设备上接口的 IP 地址，且接口为 up 状态，否则测试会失败。

(8) 配置探测报文的源端口。

source port *port-number*

缺省情况下，系统自动选择设备当前空闲的端口号。

(9) 配置测试最大连续失败次数。

max-failure *times*

缺省情况下，最大失败次数为 5。

(10) 配置发送的探测报文的初始跳数。

init-ttl *value*

缺省情况下，UDP-tracert 测试中探测报文初始跳数为 1。

(11) （可选）配置探测报文中的填充内容大小。

data-size *size*

缺省情况下，探测报文中的填充内容大小为 100 字节。

(12) （可选）配置探测的禁止报文分片功能。

no-fragment enable

缺省情况下，禁止报文分片功能处于关闭状态。

1.4.13 配置 Voice 测试

1. 功能简介

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

Voice 测试的过程如下：

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

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

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

对于 Voice 测试，一次探测操作是指连续发送多个探测报文，发送探测报文的个数由 probe packet-number 命令来设定。

除了抖动时间等参数，Voice 测试还可以计算出反映 VoIP 网络状况的语音参数值：

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

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

Voice 测试需要 NQA 服务器和客户端配合才能完成。进行 Voice 测试之前，必须保证 NQA 服务器端配置了 UDP 监听功能，配置方法请参见“1.2 配置 NQA 服务器”。

2. 配置限制和指导

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

display nqa history 命令的显示信息无法反映 Voice 测试的结果，如果想了解 Voice 测试的结果，建议通过 **display nqa result** 命令查看最近一次 NQA 测试的当前结果，或通过 **display nqa statistics** 命令查看 NQA 测试的统计信息。

进行本测试前需保证网络时钟的 NTP 同步。有关 NTP 的详细介绍请参见“网络管理和监控配置指导”的“NTP”。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 NQA 测试组，并进入 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(3) 配置测试类型为 Voice，并进入测试类型视图。

type voice

(4) 配置探测报文的目的 IP 地址。

destination ip *ip-address*

缺省情况下，未配置探测报文的目的 IP 地址。

必须与 NQA 服务器上 **nqa server udp-echo** 命令配置的监听服务的 IP 地址一致。

(5) 配置测试操作的目的端口。

destination port *port-number*

缺省情况下，未配置测试操作的目的端口号。

必须与 NQA 服务器上 **nqa server udp-echo** 命令配置的监听服务的端口号一致。

(6) 配置探测报文的源 IP 地址。

source ip *ip-address*

缺省情况下，以报文发送接口的主 IP 地址作为探测报文中的源 IP 地址。

该命令指定的源地址必须是设备上接口的 IP 地址，且接口为 up 状态，否则测试将会失败。

(7) 配置探测报文的源端口。

source port *port-number*

缺省情况下，系统自动选择设备当前空闲的端口号。

(8) 配置 Voice 测试的基本参数。

- 配置 Voice 测试的编码格式。

  codec-type { g711a | g711u | g729a }

  缺省情况下，语音编码格式为 G.711 A 律。

- 配置用于计算 MOS 值和 ICPIF 值的补偿因子。

  advantage-factor *factor*

  缺省情况下，补偿因子取值为 0。

(9) 配置 Voice 测试的探测参数。

- 配置一次 Voice 探测中发送探测报文的个数。

  probe packet-number *number*

  缺省情况下，一次 Voice 探测中发送 1000 个探测报文。

- 配置 Voice 探测中发送探测报文的时间间隔。

  probe packet-interval *interval*

  缺省情况下，Voice 探测中发送探测报文的时间间隔为 20 毫秒。

- 配置 Voice 测试中等待响应报文的超时时间。

  probe packet-timeout *timeout*

  缺省情况下，Voice 测试中等待响应报文的超时时间为 5000 毫秒。

(10) 配置探测报文中的填充内容。

a. 配置探测报文中的填充内容大小。

data-size *size*

缺省情况下，探测报文中的填充内容大小与配置的编码格式有关，编码格式为**g.711a**和**g.711u**时缺省报文大小为172字节，**g.729a**时为32字节。

b. （可选）配置探测报文中的填充字符串。

data-fill *string*

本命令的缺省情况与设备型号有关，请以设备的实际情况为准。

1.4.14 配置 DLSw 测试

1. 功能简介

DLSw 测试主要用来测试 DLSw 设备的响应时间。

对于 DLSw 测试，一次探测操作是指建立一次 DLSw 连接。

2. 配置限制和指导

请务必在 NQA 服务器上配置 **nqa server tcp-connect** 命令，且 *port-number* 值必须为 2065。否则，测试失败。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 NQA 测试组，并进入 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(3) 配置测试类型为 DLSw，并进入测试类型视图。

type dlsw

(4) 配置探测报文的目的 IP 地址。

destination ip *ip-address*

缺省情况下，未配置探测报文的目的 IP 地址。

(5) 配置探测报文的源 IP 地址。

source ip *ip-address*

缺省情况下，以报文发送接口的主 IP 地址作为探测报文中的源 IP 地址。

该命令指定的源地址必须是设备上接口的 IP 地址，且接口为 up 状态，否则测试将会失败。

1.4.15 配置 Path-jitter 测试

1. 功能简介

Path-jitter 测试可以作为 UDP-jitter 测试的一种补充，用于在抖动比较大的情况下，进一步探测中间路径的网络质量，以便查找出网络质量差的具体路段。Path-jitter 测试项对每一条路径记录结果，在路径上的每一跳均记录抖动值、正向抖动值和负向抖动值。

Path-jitter 测试的过程如下：

(1) NQA 客户端使用 tracert 机制发现到达目的地址的路径信息。

(2) NQA 客户端根据 tracert 结果，逐跳使用 ICMP 机制探测从本机至该跳设备的路径上报文是否有丢失，同时计算该跳路径的时延和抖动时间等信息。

对于 Path-jitter 测试，一次探测操作分为两个步骤：首先通过 tracert 探路获取到达目的地址的路径（最大为 64 跳）；再根据 tracert 结果，分别向路径上的每一跳发送多个 ICMP-echo 探测报文，发送探测报文的个数由 **probe packet-number** 命令来设定。

2. 配置准备

配置 Path-jitter 测试需要在中间设备（源端与目的端之间的设备）上开启 ICMP 超时报文发送功能。如果中间设备是 H3C 设备，需要在设备上执行 **ip ttl-expires enable** 命令（该命令的详细介绍请参见“三层技术-IP 业务命令参考”中的“IP 性能优化”）。需要在目的端开启 ICMP

目的不可达报文发送功能。如果目的端是 H3C 设备，需要在设备上执行 **ip unreachables enable** 命令（该命令的详细介绍请参见“三层技术-IP 业务命令参考”中的“IP 性能优化”）。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 NQA 测试组，并进入 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(3) 配置测试类型为 Path-jitter，并进入测试类型视图。

type path-jitter

(4) 配置探测报文的目的 IP 地址。

destination ip *ip-address*

缺省情况下，未配置探测报文的目的 IP 地址。

(5) 配置探测报文的源 IP 地址。

source ip *ip-address*

缺省情况下，以报文发送接口的主 IP 地址作为探测报文中的源 IP 地址。

该命令指定的源地址必须是设备上接口的 IP 地址，且接口为 up 状态，否则探测将会失败。

(6) 配置 Path-jitter 测试的探测参数。

- 配置一次 Path-jitter 探测中发送探测报文的个数。

  probe packet-number *number*

  缺省情况下，一次 Path-jitter 探测中发送 10 个 ICMP 探测报文。

- 配置 Path-jitter 测试中发送探测报文的时间间隔。

  probe packet-interval *interval*

  缺省情况下，Path-jitter 测试中发送探测报文的时间间隔为 20 毫秒。

- 配置 Path-jitter 测试中等待响应报文的超时时间。

  probe packet-timeout *timeout*

  缺省情况下，Path-jitter 测试中等待响应报文的超时时间为 3000 毫秒。

(7) （可选）配置松散路由。

lsr-path *ip-address*&<1-8>

缺省情况下，未配置松散路由。

通过本命令配置松散路由，在 tracert 过程使用该配置进行探路，NQA 客户端根据该松散路由计算时延和抖动时间。

(8) （可选）配置仅对目的地址探测。

target-only

缺省情况下，未配置仅对目的地址探测，Path-jitter 测试中会逐跳进行探测。

(9) （可选）配置探测报文中的填充内容大小。

data-size *size*

缺省情况下，探测报文中的填充内容大小为 100 字节。

(10) （可选）配置探测报文的填充字符串。

data-fill *string*

本命令的缺省情况与设备型号有关，请以设备的实际情况为准。

1.4.16 配置 Y.1564 测试

1. 功能简介

Y.1564 测试是用来测试网络中路径的质量，能较为精确的反映网络资源的性能。使用 Y.1564 测试能快速地检测网络质量是否满足服务等级规约 SLA（Service Level Agreement）。

2. 业务验收标准

业务验收标准 SAC（Service Acceptance Criteria）用于定义网络性能目标的参数集合，这些参数确保运营商所提供的网络服务满足 SLA 要求的最小需求。

Y.1564 中所采用的 SAC 是在 ITU-T Y.1564 中定义的，包括：信息速率 IR（Information Rate）、丢包率 FLR（Frame Loss Ratio）、传输时延 FTD（Frame Transfer Delay）、时延抖动 FDV（Frame Delay Variation）。

3. Y.1564 测试的阶段

Y.1564 测试包含如下两个测试阶段：

(1) 服务配置测试（Service Configuration Test），用于验证网络部署是否正确，是否可以按照预期处理网络中的报文。

(2) 服务性能测试（Service Performance Test），用于测试网络持续提供业务流转发服务的质量。

4. 服务配置测试

服务配置测试阶段又分为三个测试：

(1) CIR 测试

CIR 测试表示以每次递增一个平均速率（平均速率=CIR/执行步数）的方式发送报文，直到发送速率达到承诺信息速率。

在每步 CIR 测试结束后，设备都会计算网络性能参数，若 FLR、FTD、FDV 都在 SAC 的配置范围内，表示该步测试通过；否则，终止 CIR 测试，整个测试过程也随之停止。

(2) PIR 测试

PIR 测试根据设备是否开启颜色标记模式分为两种情况：

- 开启颜色标记模式时，以承诺信息速率为绿色报文发送速率，以峰值速率为黄色报文发送速率，同时发送报文进行测试。测试结束后，若绿色报文的 FLR、FTD、FDV 都在 SAC 的配置范围之内，则表明 PIR 测试通过；否则，终止 PIR 测试，整个测试过程也随之停止。
- 未开启颜色标记模式时，以“承诺信息速率+峰值速率”开始测试。测试结束后，若 CIR * （1 – FLRSAC） ≤ IR ≤ CIR + PIR（其中，FLRSAC 为用户配置的 FLR，IR 为计算得到的平均 IR），则认为测试通过；否则，终止 PIR 测试，整个测试过程也随之停止。

PIR 测试用于测试当网络流量同时存在承诺信息速率和峰值速率或超过承诺信息速率时的丢包率是否符合标准。

(3) Traffic-policing 测试

Traffic policing（流量监管）测试根据设备是否开启颜色标记模式分为两种情况：

- 开启颜色标记模式时，以 CIR 为绿色报文发送速率，以 125%的 PIR 为黄色报文发送速率（若配置的 PIR<20%*CIR，则黄色报文发送速率=25%*CIR+PIR），同时发送报文进行测试。测试结束后，若计算出绿色报文的 FLR、FTD、FDV 都在 SAC 的配置范围之内，并且 CIR * (1 – FLRSAC) ≤ IR ≤ CIR + PIR + M（其中，FLRSAC 为用户配置的 FLR，M=（CIR + PIR） * 1%），则认为测试通过；反之，终止流量监管测试，整个测试过程也随之停止。
- 未开启颜色标记模式时，以 CIR+125%*PIR 作为报文发送速率（若配置的 PIR<20%*CIR，则发送报文速率=125%*CIR+PIR），发送报文进行测试。测试结束后，若 CIR * (1 – FLRSAC) ≤ IR ≤ CIR + PIR + M（其中，FLRSAC 为用户配置的 FLR，M=（CIR + PIR） * 1%），则认为测试通过；反之，终止流量监管测试，整个测试过程也随之停止。

5. 服务性能测试

服务性能测试阶段直接以 CIR 发送报文进行测试。测试结束后，若计算出的 FLR、FTD、FDV 都在 SAC 的配置范围之内，则表明该业务流通过测试。

6. 配置限制和指导

display nqa history、**display nqa statistics** 命令的显示信息无法反映 Y.1564 测试的结果，如果想了解 Y.1564 测试的结果，建议通过 **display nqa result** 命令查看最近一次 NQA 测试的当前结果。

对于 Y.1564 测试，请按照以下要求配置源地址和目的地址，否则，会导致 NQA 测试启动失败：

- 三层以太网和三层 VPN 环境下必须配置源地址和目的地址。
- 其他组网环境下，源地址和目的地址要么均配置要么均不配置，如果配置，要求均为 IPv4 类型或者均为 IPv6 类型。

7. 配置 Y.1564 测试组

(1) 进入系统视图。

system-view

(2) 创建 NQA 测试组，进入 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(3) 配置测试类型为 Y.1564，并进入测试类型视图。

type y1564

(4) 配置 Y.1564 测试的地址及端口。

a. 配置探测报文的源 IP 地址。

（IPv4 网络）

source ip *ipv4-address1* [**to** *ipv4-address2*]

缺省情况下，未配置探测报文的源 IPv4 地址。

（IPv6 网络）

source ipv6 *ipv6-address1* [**to** *ipv6-address2*]

缺省情况下，未配置探测报文的源 IPv6 地址。

b. 配置探测报文的目的 IP 地址。

（IPv4 网络）

destination ip *ipv4-address1* [**to** *ipv4-address2*]

缺省情况下，未配置探测报文的目的 IPv4 地址。

（IPv6 网络）

destination ipv6 *ipv6-address1* [**to** *ipv6-address2*]

缺省情况下，未配置探测报文的目的 IPv6 地址。

c. 配置探测报文的源 AC 或源接口。

source interface *interface-type interface-number* [**service-instance** *instance-id*]

二层 VPN 环境下必须配置 **service-instance** 参数。

缺省情况下，未配置探测报文的源 AC 或源接口。有关 AC 口的详细介绍，请参见“MPLS 配置指导”中的“VPLS”。

该命令指定的接口必须为 up 状态。

d. 配置探测报文的出接口。

out interface *interface-type interface-number*

客户端为三层以太网关和三层 VPN 网关时必须进行本配置。

缺省情况下，未配置探测报文的出接口。

e. 配置探测报文的源端口号。

source port *port-number1* [**to** *port-number2*]

缺省情况下，探测报文的源端口号为 49184。

f. 配置探测报文的目的端口号。

destination port *port-number1* [**to** *port-number2*]

缺省情况下，探测报文的目的端口号为 7。

g. 配置探测报文的源 MAC 地址。

source mac *mac-address1* [**to** *mac-address2*]

二层以太网和二层 VPN 环境下必须进行本配置。

缺省情况下，以报文发送接口的 MAC 作为探测报文的源 MAC。

h. 配置探测报文的目的 MAC 地址。

destination mac *mac-address1* [**to** *mac-address2*]

二层以太网和二层 VPN 环境下必须进行本配置。

缺省情况下，探测报文的目的 MAC 地址为 0023-8900-0001。

(5) 配置 Y.1564 测试的基本参数。

- （可选）配置测试组的描述信息。

  description *text*

  缺省情况下，未配置描述信息。

- 配置测试时的 CIR 与 PIR。

  bandwidth cir *cir-value* [**pir** *pir-value*]

  缺省情况下，未配置测试时的 CIR 与 PIR。

- 配置探测报文的长度。

  frame-size *size*&<1-7>

  缺省情况下，发送的探测报文的大小为 512 字节。

- 配置可接受的时延抖动上限。

  allowed-jitter *jitter*

  缺省情况下，未配置可接受的时延抖动上限。

- 配置 100000 个包中设备可接受的丢包数。

  allowed-frame-loss *count*

  缺省情况下，未配置可接受的丢包率上限。

- 配置可接受的时延上限。

  allowed-transfer-delay *delay*

  缺省情况下，未配置可接受的时延上限。

- 配置 NQA 探测报文 IP 报文头中服务类型域的值。

  tos *value*

  缺省情况下，NQA 探测报文 IP 报文头中服务类型域的值为 0。

(6) 开启 Y.1564 测试。请至少选择其中一项进行配置。

- 开启 CIR 测试。

  cir-test enable [**step-count** *count*] [**step-duration** *duration*]

  缺省情况下，CIR 测试处于开启状态。

- 开启 PIR 测试。

  pir-test enable [**duration** *duration*]

  缺省情况下，PIR 测试处于开启状态。

- 开启流量监管测试。

  traffic-policing-test enable [**duration** *duration*]

  缺省情况下，Traffic policing 测试处于关闭状态。

- 开启服务性能测试。

  performance-test enable [**duration** *duration*]

  缺省情况下，Service performance 测试处于开启状态。

(7) （可选）开启颜色标记模式。

color-aware-mode enable [**8021p green** *value1* [**to** *value2*] **yellow** *value1* [**to** *value2*] | **dscp green** *value1* [**to** *value2*] **yellow** *value1* [**to** *value2*]]

缺省情况下，颜色标记模式处于关闭状态。

(8) （可选）配置探测报文的 VLAN 标签。

vlan { *vlan-id1* [**to** *vlan-id2*] | **s-vid** *vlan-id1* [**to** *vlan-id2*] **c-vid** *vlan-id1* [**to** *vlan-id2*] }

缺省情况下，未配置探测报文的 VLAN 标签。

(9) 指定测试操作所属的 VPN 实例。

vpn-instance *vpn-instance-name*

三层 VPN 环境下必须进行本配置。

缺省情况下，未指定测试操作所属的 VPN 实例。

(10) （可选）开启源目的端口的交换功能。

exchange-port enable

缺省情况下，源目的端口的交换功能处于关闭状态。

(11) （可选）配置探测报文的 802.1p 优先级。

priority 8021p *value*

缺省情况下，探测报文的 802.1p 优先级为 0。

(12) 配置 NQA 探测超时时间。

probe timeout *timeout*

缺省情况下，探测的超时时间为 3000 毫秒。

8. 配置 Y.1564 操作组

NQA Y.1564 操作组用于关联 Y.1564 测试组，使用操作组可以同时启动多个 Y.1564 测试。

使用 Y.1564 操作组进行测试时，设备依次开始进行服务配置测试（即先完成一项服务配置测试之后，再开始下一项服务配置测试），待所有服务配置测试完成后，再并行启动服务性能测试。

(1) 进入系统视图。

system-view

(2) 创建 Y.1564 操作组，进入 Y.1564 操作组视图。

nqa y1564 group *group-name*

(3) 在 NQA Y.1564 操作组下关联 Y.1564 测试组。

bind nqa-entry *admin-name operation-tag*

缺省情况下，NQA Y.1564 操作组下没有关联任何 Y.1564 测试组。

9. 配置测试结果上传到 ftp 服务器

若需要存档测试结果，可以使用本功能将测试结果上传到 ftp 服务器上。

(1) 进入系统视图。

system-view

(2) 配置测试结果上传的 FTP 服务器信息。

nqa report-ftp url *url* [**username** *username*] [**password** { **cipher** | **simple** } *string*]

缺省情况下，未配置 FTP 服务器信息。

10. 启动 Y.1564 测试

Y.1564 测试进行时会占用测试的整个链路带宽，为确保测试的准确性，请在启动测试前暂停该链路上的所有流量。

Y.1564 测试与其它 NQA 测试组不可以同时运行。

当设备正在进行 Y.1564 测试时，不能再启动其它 Y.1564 测试。

(1) 进入系统视图。

system-view

(2) 进入 Y.1564 视图。请选择其中一项进行配置。

- 进入 Y.1564 操作组视图。

  nqa y1564 group *group-name*

- 进入 Y.1564 测试组视图。

  nqa entry *admin-name operation-tag*

(3) 启动 Y.1564 测试。

start

11. 停止 Y.1564 测试

(1) 进入系统视图。

system-view

(2) 进入 Y.1564 视图。请选择其中一项进行配置。

- 进入 Y.1564 操作组视图。

  nqa y1564 group *group-name*

- 进入 Y.1564 测试组视图。

  nqa entry *admin-name operation-tag*

(3) （可选）停止 Y.1564 测试。

stop

Y.1564 测试完成所有的测试项目后会自动停止，本命令可用于强行中断测试。若强行中断测试，则进行到一半的测试将不会有结果。

1.4.17 配置路径服务质量测试

1. 路径服务质量测试综述

路径服务质量测试是根据 RFC2544 协议开发的 NQA 测试。对于路径服务质量测试，一次探测操作是指在一段时间内以一定的速率连续发送并接收特定长度的探测报文。路径服务质量测试以二层数据帧作为测试的探测报文。

路径服务质量测试是用来测试网络中从源站点到目的站点之间路径的质量。路径服务质量测试可以测试的服务质量指标包括：丢包率、吞吐量、时延。如图 1-1 所示，在 MPLS L2VPN 中，路径服务质量测试用来测试 Device A 到 Device B 之间路径的质量。

图1-1 配置路径服务质量测试（以 L2VPN 为例）

1. 丢包率测试过程

丢包率测试的具体测试过程如下：

(1) 用户首先设定一种或多种探测报文的长度。测试开始后，NQA 客户端按用户设定的首个长度构造环回探测报文，以指定的速率发送，发送持续时间为一个探测周期。

(2) 目的端收到探测报文后，将探测报文返还给 NQA 客户端。

(3) NQA 客户端记录一个探测周期内发送和接收探测报文的总数量，计算出在传输过程中丢失的探测报文占总发送报文的比例，即丢包率。丢包率计算公式为：

丢包率=((发送报文数-接收报文数)* 100)/发送报文数

(4) NQA 客户端按用户设定的第二个长度构造探测报文，测试此类探测报文的丢包率，依此类推，直至完成所有长度的探测报文的测试。

2. 吞吐量测试过程

吞吐量测试的具体测试过程如下：

(1) 用户首先设定一种或多种探测报文的长度。测试开始后，NQA 客户端按用户设定的首个长度构造环回探测报文，以指定的速率发送，发送持续时间为一个探测周期。

(2) NQA 客户端根据接收到的目的端返回探测报文数目计算出路径上的丢包率，记录测试结果。

(3) NQA 客户端调整发送速率，重新发送探测报文，直到计算出的丢包率小于等于可接受的丢包率上限。所有发送速率中的最大速率，即为本次探测的吞吐量。

(4) NQA 客户端按用户设定的第二个长度构造探测报文，测试此类探测报文的吞吐量，依此类推，直至完成所有长度的探测报文的测试。

3. 时延测试过程

时延测试的具体测试过程如下：

(1) 用户首先设定一种或多种探测报文的长度。测试开始后，NQA 客户端按用户设定的首个长度构造环回探测报文，以指定的速率发送，发送持续时间为一个探测周期。

(2) 接收到对端返回的探测报文后，NQA 客户端将接收探测报文的时间减去探测报文中记录的发送时间，计算该探测报文在路径上往返所需的时间，即时延。

(3) 探测周期结束后，NQA 客户端通过公式计算出本周期内所有探测报文的时延平均值。平均时延计算公式为：

平均时延=探测报文时延之和/发送探测报文的数量

(4) NQA 客户端按用户设定的第二个长度构造探测报文，测试此类探测报文的时延平均值，依此类推，直至完成所有长度的探测报文的测试。

4. 配置限制和指导

display nqa history 命令的显示信息无法反映路径服务质量测试的结果，如果想了解路径服务质量测试的结果，建议通过 **display nqa result** 命令查看最近一次 NQA 测试的当前结果。

对于路径服务质量测试，请按照以下要求配置源地址和目的地址，否则，会导致 NQA 测试启动失败：

- 三层以太网和三层 VPN 环境下必须配置源地址和目的地址。
- 其他组网环境下，源地址和目的地址要么均配置要么均不配置，如果配置，要求均为 IPv4 类型或者均为 IPv6 类型。

5. 配置并启动测试

(1) 进入系统视图。

system-view

(2) （可选）配置测试结果上传的 FTP 服务器信息。

nqa report-ftp url *url* [**username** *username*] [**password** { **cipher** | **simple** } *string*]

缺省情况下，未配置 FTP 服务器信息。

仅路径服务质量测试支持上传测试结果到服务器。

(3) 创建 NQA 测试组，并进入 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(4) 配置路径服务质量测试类型。请至少选择其中一项进行配置。

- 配置测试类型为丢包率测试。

  type frame-loss

- 配置测试类型为吞吐量测试。

  type throughput

- 配置测试类型为时延测试。

  type latency

(5) 配置路径服务质量测试的地址及端口。

a. 配置探测报文的源 IP 地址。

（IPv4 网络）

source ip *ipv4-address*

缺省情况下，未配置探测报文的源 IPv4 地址。

（IPv6 网络）

source ipv6 *ipv6-address*

缺省情况下，未配置探测报文的源 IPv6 地址。

b. 配置探测报文的目的 IP 地址。

（IPv4 网络）

destination ip *ipv4-address*

缺省情况下，未配置探测报文的目的 IPv4 地址。

（IPv6 网络）

destination ipv6 *ipv6-address*

缺省情况下，未配置探测报文的目的 IPv6 地址。

c. 配置探测报文的源 AC 或源接口。

source interface *interface-type interface-number* [**service-instance** *instance-id*]

二层 VPN 环境下必须配置 **service-instance** 参数。

缺省情况下，未配置探测报文的源 AC 或源接口。有关 AC 口的详细介绍，请参见“MPLS 配置指导”中的“VPLS”。

该命令指定的接口必须为 up 状态。

d. 配置探测报文的出接口。

out interface *interface-type interface-number*

客户端为三层以太网关和三层 VPN 网关时必须进行本配置。

缺省情况下，未配置探测报文的出接口。

e. 配置探测报文的源端口号。

source port *port-number*

缺省情况下，探测报文的源端口号为 49184。

f. 配置探测报文的目的端口号。

destination port *port-number*

缺省情况下，探测报文的目的端口号为 7。

g. 配置探测报文的源 MAC 地址。

source mac *mac-address*

二层以太网和二层 VPN 环境下必须进行本配置。

缺省情况下，以报文发送接口的 MAC 地址作为探测报文的源 MAC。

h. 配置探测报文的目的 MAC 地址。

destination mac *mac-address*

二层以太网和二层 VPN 环境下必须进行本配置。

缺省情况下，探测报文的目的 MAC 地址为 0023-8900-0001。

(6) 配置路径服务质量测试的基本参数。

- （可选）配置测试组的描述信息。

  description *text*

  缺省情况下，未配置描述信息。

- 配置探测报文的长度。

  frame-size *size*&<1-7>

  缺省情况下，发送的探测报文的大小为 1518 字节。

  报文的长度可以指定一种或同时指定多种。

- 配置发送探测报文的初始速率。

  speed init *init-speed*

  本命令的缺省情况与设备型号有关，请以设备的实际情况为准。

  在进行丢包率和时延测试时，设备始终以设定的速率发送探测报文；在进行吞吐量测试时，每完成一个探测周期，设备将按照速率调整精度调整一次发送速率。

- 配置探测报文的速率调整精度。

  speed granularity *value*

  缺省情况下，速率调整精度为 1000Kbps。

  仅在进行吞吐量测试时支持配置该数值。

  在进行吞吐量测试时，设备由初始速率开始，以设定值为调整精度调整发送探测报文的速率。

- 配置可接受的丢包率上限。

  allowed-loss-ratio *ratio*

  缺省情况下，可接受的丢包率上限为 1/10000。

  仅在进行吞吐量测试时支持配置该数值。

- 配置 NQA 探测报文 IP 报文头中服务类型域的值。

  tos *value*

  缺省情况下，NQA 探测报文 IP 报文头中服务类型域的值为 0。

(7) 配置路径服务质量测试的探测参数。

- 配置探测的时间间隔。

  probe interval *interval*

  缺省情况下，探测的时间间隔为 4 秒。

- 配置探测周期的时长。

  probe duration *time*

  缺省情况下，探测周期的时长为 60 秒。

- 配置探测的超时时间。

  probe timeout *timeout*

  缺省情况下，探测的超时时间为 3000 毫秒。

(8) （可选）配置探测报文的 VLAN 标签。

vlan { *vlan-id* | **s-vid** *vlan-id* **c-vid** *vlan-id* }

缺省情况下，未配置探测报文的 VLAN 标签。

(9) 指定测试操作所属的 VPN 实例。

vpn-instance *vpn-instance-name*

三层 VPN 环境下必须进行本配置。

缺省情况下，未指定测试操作所属的 VPN 实例。

(10) 配置探测报文的 802.1p 优先级。

priority 8021p *value*

缺省情况下，探测报文的 802.1p 优先级为 0。

(11) （可选）开启源目的端口的交换功能。

exchange-port enable

缺省情况下，源目的端口的交换功能处于关闭状态。

(12) 启动路径服务质量测试。

start

路径服务质量测试既可以使用本命令启动，也可以使用调度 NQA 测试组功能启动。调度 NQA 测试组功能的配置方法请参见“1.4.23 在 NQA 客户端上调度 NQA 测试组”。

6. 停止测试

(1) 进入系统视图。

system-view

(2) 进入路径服务质量测试视图。

nqa entry *admin-name operation-tag*

请输入路径服务质量测试的管理员名称和标签。

(3) 停止路径服务质量测试。

stop

1.4.18 配置 NQA 测试组通用参数

1. 配置限制和指导

NQA 测试组的通用参数，只对当前测试组中的测试有效。

除特别说明外，所有测试类型都可以根据实际情况选择配置下列通用参数。

通用参数中路径服务质量和 Y.1564 测试目前仅支持 **description**、**tos** 及 **vpn-instance** 命令。请参见“1.4.16 配置 Y.1564 测试”和“1.4.17 配置路径服务质量测试”的配置。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入已配置测试类型的 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(3) 配置测试组的描述信息。

description *text*

缺省情况下，未配置描述信息。

(4) 配置测试组连续两次测试开始时间的时间间隔。

frequency *interval*

缺省情况下，Voice、Path-jitter 测试中连续两次测试开始时间的时间间隔为 60000 毫秒；其他类型的测试为 0 毫秒，即只进行一次测试。

到达本命令指定的时间间隔时，将开始下一个间隔的计时，但如果此时测试尚未完成或者测试未超时，则不启动新一轮测试，直到测试完成或者测试超时，才开始新一轮测试。

(5) 配置一次 NQA 测试中进行探测的次数。

probe count *times*

缺省情况下，对于 UDP-tracert 测试类型，对于一个 TTL 值的节点发送的探测报文次数为 3 次；其他类型的 NQA 测试一次测试中的探测次数为 1 次。

Voice 和 Path-jitter 测试中探测次数只能为 1，不支持该命令。

(6) 配置 NQA 探测超时时间。

probe timeout *timeout*

缺省情况下，探测的超时时间为 3000 毫秒。

ICMP-jitter、UDP-jitter、Voice 和 Path-jitter 测试不能配置该参数。

(7) 配置探测报文在网络中可以经过的最大跳数。

ttl *value*

缺省情况下，UDP-tracert 测试探测报文在网络中可以经过的最大跳数为 30 跳。其他类型的探测报文在网络中可以经过的最大跳数为 20 跳。

DHCP 和 Path-jitter 测试不能配置该参数。

(8) 配置 NQA 探测报文 IP 报文头中服务类型域的值。

tos *value*

缺省情况下，NQA 探测报文 IP 报文头中服务类型域的值为 0。

(9) 启动路由表旁路功能。

route-option bypass-route

缺省情况下，路由表旁路功能处于关闭状态。

DHCP 和 Path-jitter 测试不能配置该参数。

测试目的端使用 IPv6 地址时，本命令配置无效。

(10) 指定测试操作所属的 VPN 实例。

vpn-instance *vpn-instance-name*

缺省情况下，未指定测试操作所属的 VPN 实例。

本命令的支持情况与设备的型号有关，请以设备的实际情况为准。

1.4.19 配置联动功能

1. 功能简介

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

2. 配置限制和指导

ICMP-jitter、UDP-jitter、UDP-tracert、Voice、Path-jitter、路径服务质量和 Y.1564 测试不支持联动功能。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入已配置测试类型的 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(3) 建立联动项。

reaction *item-number* **checked-element probe-fail threshold-type consecutive** *consecutive-occurrences* **action-type trigger-only**

联动项创建后，不能再通过 **reaction** 命令修改该联动项的内容。

(4) 退回系统视图。

quit

(5) 配置 Track 与 NQA 联动。

配置方法请参见“可靠性配置指导”中的“Track”

(6) 配置 Track 与应用模块联动。

配置方法请参见“可靠性配置指导”中的“Track”

1.4.20 配置阈值告警功能

1. 功能简介

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

NQA 阈值告警功能支持的阈值类型包括：

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

NQA 阈值告警功能可以触发如下动作：

- **none**：只在本地记录监测结果，以便通过显示命令查看，不向网络管理系统发送 Trap 消息。
- **trap-only**：不仅在本地记录监测结果，当阈值告警项的状态改变时，还向网络管理系统发送 Trap 消息。采用本动作时，需要通过 **snmp-agent target-host** 命令配置 Trap 消息的目的地址。**snmp-agent target-host** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“SNMP”。
- **trigger-only**：在显示信息中记录监测结果的同时，触发其他模块联动。

阈值告警项包括 invalid、over-threshold 和 below-threshold 三种状态：

- NQA 测试组未启动时，阈值告警项的状态为 invalid。

- NQA 测试组启动后，每次测试或探测结束时，检查监测的对象是否超出指定类型的阈值。如果超出阈值，则阈值告警项的状态变为 over-threshold；如果未超出阈值，则状态变为 below-threshold。

2. 配置限制和指导

Path-jitter、路径服务质量和 Y.1564 测试不支持配置阈值告警功能。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入已配置测试类型的 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(3) 配置在指定条件下向网管服务器发送 Trap 消息。

reaction trap { **path-change** | **probe-failure** *consecutive-probe-failures* | **test-complete** | **test-failure** [*accumulate-probe-failures*] }

缺省情况下，不向网管服务器发送 Trap 消息。

ICMP-jitter、UDP-jitter、Voice 测试只支持 **reaction trap test-complete**。

UDP-tracert 测试不支持 **probe-failure** 和 *accumulate-probe-failures* 参数。

(4) 创建阈值告警组。请至少选择其中一项进行配置。

- 创建监测探测持续时间的阈值告警组。

  reaction *item-number* **checked-element probe-duration threshold-type** { **accumulate** *accumulate-occurrences* | **average** | **consecutive** *consecutive-occurrences* } **threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

  除 ICMP-jitter、UDP-jitter、UDP-tracert 和 Voice 测试外，均支持。

- 创建监测探测失败次数的阈值告警组。

  reaction *item-number* **checked-element probe-fail threshold-type** { **accumulate** *accumulate-occurrences* | **consecutive** *consecutive-occurrences* } [**action-type** { **none** | **trap-only** }]

  除 ICMP-jitter、UDP-jitter、UDP-tracert 和 Voice 测试外，均支持。

- 创建监测报文往返时延的阈值告警组。

  reaction *item-number* **checked-element rtt threshold-type** { **accumulate** *accumulate-occurrences* | **average** } **threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

  仅 ICMP-jitter、UDP-jitter 和 Voice 测试支持。

- 创建监测每次测试中丢包数的阈值告警组。

  reaction *item-number* **checked-element packet-loss threshold-type accumulate** *accumulate-occurrences* [**action-type** { **none** | **trap-only** }]

  仅 ICMP-jitter、UDP-jitter 和 Voice 测试支持。

- 创建监测单向抖动时间的阈值告警组。

  reaction *item-number* **checked-element** { **jitter-ds** | **jitter-sd** } **threshold-type** { **accumulate** *accumulate-occurrences* | **average** } **threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

  仅 ICMP-jitter、UDP-jitter 和 Voice 测试支持。

- 创建监测单向时延的阈值告警组。

  reaction *item-number* **checked-element** { **owd-ds** | **owd-sd** } **threshold-value** *upper-threshold lower-threshold*

仅 ICMP-jitter、UDP-jitter 和 Voice 测试支持。

- 创建监测 Voice 测试 ICPIF 值的阈值告警组。

  reaction *item-number* **checked-element icpif threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

  仅 Voice 测试支持。

- 创建监测 Voice 测试 MOS 值的阈值告警组。

  reaction *item-number* **checked-element mos threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

  仅 Voice 测试支持。

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

1.4.21 配置 NQA 统计功能

1. 功能简介

NQA 将在指定时间间隔内完成的 NQA 测试归为一组，计算该组测试结果的统计值，这些统计值构成一个统计组。通过 **display nqa statistics** 命令可以显示该统计组的信息。

当 NQA 设备上保留的统计组数目达到最大值时，如果形成新的统计组，保存时间最久的统计组将被删除。

统计组具有老化功能，即统计组保存一定时间后，将被删除。

2. 配置限制和指导

- UDP-tracert、路径服务质量和 Y.1564 测试不支持 NQA 统计功能。
- 如果通过 **frequency** 命令指定连续两次测试开始时间的时间间隔为 0，则不生成统计组信息。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入已配置测试类型的 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(3) 配置对测试结果进行统计的时间间隔。

statistics interval *interval*

缺省情况下，对测试结果进行统计的时间间隔为 60 分钟。

(4) 配置能够保留的最大统计组个数。

statistics max-group *number*

缺省情况下，能够保留的最大统计组数为 2。

最大统计组个数为 0 时，不进行统计。

(5) 配置统计组的保留时间。

statistics hold-time *hold-time*

缺省情况下，统计组的保留时间为 120 分钟。

1.4.22 配置 NQA 历史记录功能

1. 功能简介

开启 NQA 测试组的历史记录保存功能后，系统将记录 NQA 测试的历史信息，通过 **display nqa history** 命令可以查看该测试组的历史记录信息。

2. 配置限制和指导

ICMP-jitter、UDP-jitter、Voice、Path-jitter、路径服务质量和 Y.1564 测试不支持配置历史记录功能。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入已配置测试类型的 NQA 测试组视图。

nqa entry *admin-name operation-tag*

(3) 开启 NQA 测试组的历史记录保存功能。

history-record enable

缺省情况下，UDP-tracert 类型测试组的历史记录保存功能处于开启状态，其他类型的 NQA 测试组的历史记录保存功能处于关闭状态。

(4) 配置 NQA 测试组中历史记录的保存时间。

history-record keep-time *keep-time*

缺省情况下，NQA 测试组中历史记录的保存时间为 120 分钟。

历史记录保存时间达到配置的值后，该历史记录将被删除。

(5) 配置在一个测试组中能够保存的最大历史记录个数。

history-record number *number*

缺省情况下，一个测试组中能够保存的最大历史记录个数为 50。

如果历史记录个数超过设定的最大数目，则最早的历史记录将会被删除。

1.4.23 在 NQA 客户端上调度 NQA 测试组

1. 功能简介

通过本配置，可以设置测试组进行测试的启动时间和持续时间。

系统时间在<启动时间>到<启动时间＋持续时间>范围内时，测试组进行测试。执行 **nqa schedule** 命令时：

- 如果系统时间尚未到达启动时间，则到达启动时间后，启动测试；
- 如果系统时间在<启动时间>到<启动时间＋持续时间>之间，则立即启动测试；
- 如果系统时间已经超过<启动时间＋持续时间>，则不会启动测试。

通过 **display clock** 命令可以查看系统的当前时间。

2. 配置限制和指导

测试组被调度后就不能再进入该测试组视图和测试类型视图。

对于已启动的测试组或已经完成测试的测试组，不受系统时间调整的影响，只有等待测试的测试组受系统时间调整的影响。

路径服务质量测试和 Y.1564 测试不支持使用本配置调度测试。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 在 NQA 客户端上调度 NQA 测试组。

nqa schedule *admin-name operation-tag* **start-time** { *hh:mm:ss* [*yyyy/mm/dd* | *mm/dd/yyyy*] | **now** } **lifetime** { *lifetime* | **forever** } [**recurring**]

1.5 在NQA客户端上配置NQA模板

1.5.1 配置限制和指导

对于 NQA 各类型模板，某些测试参数既可以由外部特性提供（如负载均衡），也可以手工直接进行配置。若同时通过以上两种方式获取到测试参数，则以手工配置的测试信息为准。

1.5.2 NQA 模板配置任务简介

NQA 模板配置任务如下：

(1) 配置 NQA 模板

- 配置 ARP 类型的 NQA 模板
- 配置 ICMP 类型的 NQA 模板
- 配置 IMAP 类型的 NQA 模板
- 配置 DNS 类型的 NQA 模板
- 配置 POP3 类型的 NQA 模板
- 配置 SMTP 类型的 NQA 模板
- 配置 TCP 类型的 NQA 模板
- 配置 TCP Half Open 类型的 NQA 模板
- 配置 UDP 类型的 NQA 模板
- 配置 HTTP 类型的 NQA 模板
- 配置 HTTPS 类型的 NQA 模板
- 配置 FTP 类型的 NQA 模板
- 配置 RADIUS 类型的 NQA 模板
- 配置 SNMP 类型的 NQA 模板
- 配置 SSL 类型的 NQA 模板

(2) （可选）配置 NQA 模板通用参数

1.5.3 配置 ARP 类型的 NQA 模板

1. 功能简介

ARP 类型的 NQA 模板为外部特性提供 ARP 类型测试，外部特性通过引用该模板启动 ARP 测试。测试时 NQA 客户端向目的端设备发送 ARP 请求报文，根据能否收到应答报文判断目的端设备的 ARP 服务是否可用。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 ARP 类型的 NQA 模板，并进入模板视图。

nqa template arp *name*

(3) 配置测试操作的目的 IP 地址。

destination ip *ip-address*

缺省情况下，未配置测试操作中探测报文的目的 IP 地址。

(4) （可选）配置测试操作中探测报文的源 IP 地址。

source ip *ip-address*

缺省情况下，以报文发送接口的主 IP 地址作为探测报文中的源 IP 地址。

该命令指定的源地址必须是设备上接口的 IP 地址，且接口为 up 状态，否则探测将会失败。

1.5.4 配置 ICMP 类型的 NQA 模板

1. 功能简介

ICMP 类型的 NQA 模板为外部特性提供 ICMP 类型的测试，外部特性通过引用该模板来启动 ICMP 测试，并根据是否接收到 ICMP 应答报文判断目的主机的可达性。ICMP 类型的 NQA 模板支持 IPv4 和 IPv6 网络。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 ICMP 类型的 NQA 模板，并进入模板视图。

nqa template icmp *name*

(3) 配置测试操作的目的地址。

（IPv4 网络）

destination ip *ip-address*

（IPv6 网络）

destination ipv6 *ipv6-address*

缺省情况下，未配置探测报文的目的地址。

(4) 配置探测报文的源地址。请选择其中一项进行配置。

- 使用指定接口的 IP 地址作为探测报文的源 IP 地址。

  source interface *interface-type interface-number*

  缺省情况下，以报文发送接口的主 IP 地址作为探测报文中的源 IP 地址。

  source interface 命令指定的接口必须为 up 状态。

- 配置探测报文的源 IPv4 地址。

  source ip *ip-address*

  缺省情况下，以报文发送接口的主 IPv4 地址作为探测报文中的源 IPv4 地址。

  该命令指定的源地址必须是设备上接口的 IP 地址，且接口为 up 状态，否则测试将会失败。

- 配置探测报文的源 IPv6 地址。

  source ipv6 *ipv6-address*

  缺省情况下，以报文发送接口的 IPv6 地址作为探测报文中的源 IPv6 地址。

  该命令指定的源地址必须是设备上接口的 IPv6 地址，且接口为 up 状态，否则测试将会失败。

(5) 配置探测报文的下一跳地址。

（IPv4 网络）

next-hop ip *ip-address*

（IPv6 网络）

next-hop ipv6 *ipv6-address*

缺省情况下，未配置探测报文的下一跳地址。

(6) 配置每次探测结束时都将探测结果发送给外部特性。

reaction trigger per-probe

缺省情况下，连续探测成功或失败 3 次时，NQA 客户端会把探测成功或失败的消息发送给外部特性，使外部特性利用 NQA 测试的结果进行相应处理。

reaction trigger per-probe 命令与 **reaction trigger probe-pass** 命令作用相同，多次执行这两条命令时，最后一次执行的命令生效。

reaction trigger per-probe 命令与 **reaction trigger probe-fail** 命令作用相同，多次执行这两条命令时，最后一次执行的命令生效。

(7) （可选）配置探测报文中的填充内容大小。

data-size *size*

缺省情况下，探测报文中的填充内容大小为 100 字节。

(8) （可选）配置探测报文的填充字符串。

data-fill *string*

本命令的缺省情况与设备型号有关，请以设备的实际情况为准。

1.5.5 配置 IMAP 类型的 NQA 模板

1. 功能简介

IMAP（Internet Mail Access Protocol，Internet 邮件访问协议）类型的 NQA 模板为外部特性提供 IMAP 类型测试，外部特性通过引用该模板，与指定的 IMAP 服务器建立连接，并计算与 IMAP 服务器之间报文交互的时间，来判断服务器 IMAP 业务的可用性。

在进行 IMAP 测试之前，需要在服务器上开启 IMAP Server 服务，并进行相应的配置，包括测试时登录 IMAP 服务器的用户名、密码、邮箱名等。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 IMAP 类型的 NQA 模板，并进入模板视图。

nqa template imap *name*

(3) 配置测试操作的目的地址。

（IPv4 网络）

destination ip *ip-address*

（IPv6 网络）

destination ipv6 *ipv6-address*

缺省情况下，未配置测试操作中探测报文的目的地址。

(4) 配置测试操作的目的端口。

destination port *port-number*

缺省情况下，测试操作的目的端口号为 143。

(5) 配置探测报文的源地址。

（IPv4 网络）

source ip *ip-address*

缺省情况下，以报文发送接口的主 IPv4 地址作为探测报文中的源 IPv4 地址。

该命令指定的源地址必须是设备上接口的 IPv4 地址，且接口为 up 状态，否则测试将会失败。

（IPv6 网络）

source ipv6 *ipv6-address*

缺省情况下，以报文发送接口的 IPv6 地址作为探测报文中的源 IPv6 地址。

该命令指定的源地址必须是设备上接口的 IPv6 地址，且接口为 up 状态，否则测试将会失败。

(6) 配置 IMAP 登录用户名。

username *username*

缺省情况下，未配置 IMAP 登录用户名。

(7) 配置 IMAP 登录密码。

password { **cipher** | **simple** } *string*

缺省情况下，未配置 IMAP 登录密码。

(8) 配置 IMAP 登录的邮箱名。

mailbox *mailbox-name*

缺省情况下，IMAP 测试操作的邮箱名称为 INBOX。

1.5.6 配置 DNS 类型的 NQA 模板

1. 功能简介

DNS 类型的 NQA 模板为外部特性提供 DNS 类型的测试。外部特性通过引用该模板来启动 DNS 测试，NQA 客户端向指定的 DNS 服务器发送 DNS 请求报文，NQA 客户端通过是否收到应答及应答报文的合法性来确定服务器的状态。DNS 类型的 NQA 模板支持 IPv4 和 IPv6 网络。

在 DNS 类型的 NQA 模板视图下，用户可以配置期望返回的地址。如果 DNS 服务器返回的 IP 地址中包含了期望地址，则该 DNS 服务器为真实的服务器，测试成功；否则，测试失败。

2. 配置准备

在进行 DNS 测试之前，需要在 DNS 服务器上创建域名和地址的映射关系。DNS 服务器配置方法，请参见 DNS 服务器相关资料。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 DNS 类型的 NQA 模板，并进入模板视图。

nqa template dns *name*

(3) 配置测试操作的目的地址。

（IPv4 网络）

destination ip *ip-address*

（IPv6 网络）

destination ipv6 *ipv6-address*

缺省情况下，未配置探测报文的目的地址。

(4) 配置测试操作的目的端口。

destination port *port-number*

缺省情况下，测试操作的目的端口号为 53。

(5) 配置探测报文的源地址。

（IPv4 网络）

source ip *ip-address*

缺省情况下，以报文发送接口的主 IPv4 地址作为探测报文中的源 IPv4 地址。

该命令指定的源地址必须是设备上接口的 IPv4 地址，且接口为 up 状态，否则测试将会失败。

（IPv6 网络）

source ipv6 *ipv6-address*

缺省情况下，以报文发送接口的 IPv6 地址作为探测报文中的源 IPv6 地址。

该命令指定的源地址必须是设备上接口的 IPv6 地址，且接口为 up 状态，否则测试将会失败。

(6) 配置探测报文的源端口。

source port *port-number*

缺省情况下，未配置探测报文的源端口号。

(7) 配置要解析的域名。

resolve-target *domain-name*

缺省情况下，没有配置要解析的域名。

(8) 配置域名解析类型。

resolve-type { **A** | **AAAA** }

缺省情况下，域名解析类型为 A 类型。

其中 A 类型表示将域名解析为 IPv4 地址，AAAA 类型表示将域名解析为 IPv6 地址。

(9) （可选）配置用户期望返回的地址。

（IPv4 网络）

expect ip *ip-address*

（IPv6 网络）

expect ipv6 *ipv6-address*

缺省情况下，未设定期望返回的地址。

1.5.7 配置 POP3 类型的 NQA 模板

1. 功能简介

POP3 类型的 NQA 模板为外部特性提供 POP3 类型测试，外部特性通过引用该模板，与指定的 POP3 服务器建立连接，并计算与 POP3 服务器之间报文交互的时间，来判断服务器 POP3 业务的可用性。

在进行 POP3 测试之前，需要在 POP3 服务器上开启 POP3 Server 服务，并进行相应的配置，包括测试时登录 POP3 服务器的用户名、密码等。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 POP3 类型的 NQA 模板，并进入模板视图。

nqa template pop3 *name*

(3) 配置测试操作的目的地址。

（IPv4 网络）

destination ip *ip-address*

（IPv6 网络）

destination ipv6 *ipv6-address*

缺省情况下，未配置测试操作中探测报文的目的地址。

(4) 配置测试操作的目的端口。

destination port *port-number*

缺省情况下，测试操作的目的端口号为 110。

(5) 配置探测报文的源地址。

（IPv4 网络）

source ip *ip-address*

缺省情况下，以报文发送接口的主 IPv4 地址作为探测报文中的源 IPv4 地址。

该命令指定的源地址必须是设备上接口的 IPv4 地址，且接口为 up 状态，否则测试将会失败。

（IPv6 网络）

source ipv6 *ipv6-address*

缺省情况下，以报文发送接口的 IPv6 地址作为探测报文中的源 IPv6 地址。

该命令指定的源地址必须是设备上接口的 IPv6 地址，且接口为 up 状态，否则测试将会失败。

(6) 配置 POP3 登录用户名。

username *username*

缺省情况下，未配置 POP3 登录用户名。

(7) 配置 POP3 登录密码。

password { **cipher** | **simple** } *string*

缺省情况下，未配置 POP3 登录密码。

1.5.8 配置 SMTP 类型的 NQA 模板

1. 功能简介

SMTP 类型的 NQA 模板为外部特性提供 SMTP 类型测试，外部特性通过引用该模板，与指定的 SMTP 服务器建立连接，并计算与 SMTP 服务器之间报文交互的时间，来判断服务器 SMTP 业务的可用性。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 SMTP 类型的 NQA 模板，并进入模板视图。

nqa template smtp *name*

(3) 配置测试操作的目的地址。

（IPv4 网络）

destination ip *ip-address*

（IPv6 网络）

destination ipv6 *ipv6-address*

缺省情况下，未配置测试操作中探测报文的目的地址。

(4) 配置测试操作的目的端口。

destination port *port-number*

缺省情况下，测试操作的目的端口号为 25。

(5) 配置探测报文的源地址。

（IPv4 网络）

source ip *ip-address*

缺省情况下，以报文发送接口的主 IPv4 地址作为探测报文中的源 IPv4 地址。

该命令指定的源地址必须是设备上接口的 IPv4 地址，且接口为 up 状态，否则测试将会失败。

（IPv6 网络）

source ipv6 *ipv6-address*

缺省情况下，以报文发送接口的 IPv6 地址作为探测报文中的源 IPv6 地址。

该命令指定的源地址必须是设备上接口的 IPv6 地址，且接口为 up 状态，否则测试将会失败。

1.5.9 配置 TCP 类型的 NQA 模板

1. 功能简介

TCP 类型的 NQA 模板为外部特性提供 TCP 类型测试，外部特性通过引用该模板，测试客户端和服务器指定端口之间能否建立 TCP 连接。

在 TCP 类型的 NQA 模板视图下，用户可以配置期望的应答内容。如果用户未配置期望的应答内容，则 NQA 客户端与服务器间只建立 TCP 连接。

TCP 测试需要 NQA 服务器和客户端配合才能完成。在 TCP 测试之前，需要在 NQA 服务器端配置 TCP 监听功能。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 TCP 类型的 NQA 模板，并进入模板视图。

nqa template tcp *name*

(3) 配置测试操作的目的地址。

（IPv4 网络）

destination ip *ip-address*

（IPv6 网络）

destination ipv6 *ipv6-address*

缺省情况下，未配置探测报文的目的地址。

必须与 NQA 服务器上配置的监听服务的 IP 地址一致。

(4) 配置测试操作的目的端口。

destination port *port-number*

缺省情况下，未配置测试操作的目的端口号。

必须与 NQA 服务器上配置的监听服务的端口号一致。

(5) 配置探测报文的源地址。

（IPv4 网络）

source ip *ip-address*

缺省情况下，以报文发送接口的主 IPv4 地址作为探测报文中的源 IPv4 地址。

该命令指定的源地址必须是设备上接口的 IPv4 地址，且接口为 up 状态，否则测试将会失败。

（IPv6 网络）

source ipv6 *ipv6-address*

缺省情况下，以报文发送接口的 IPv6 地址作为探测报文中的源 IPv6 地址。

该命令指定的源地址必须是设备上接口的 IPv6 地址，且接口为 up 状态，否则测试将会失败。

(6) （可选）配置探测报文的填充字符串。

data-fill *string*

本命令的缺省情况与设备型号有关，请以设备的实际情况为准。

(7) （可选）配置用户期望的应答内容。

expect data *expression* [**offset** *number*]

缺省情况下，未配置期望的应答内容。

仅当 **data-fill** 和 **expect data** 命令都配置时，进行期望应答内容的检查，否则不做检查。

1.5.10 配置 TCP Half Open 类型的 NQA 模板

1. 功能简介

TCP Half Open 类型的 NQA 模板为外部特性提供 TCP Half Open 类型测试。作为 TCP 测试的补充，TCP Half Open 测试不需要指定目的端端口。当外部特性的现有 TCP 连接无法得到对端应答时，可以引用 TCP Half Open 模板进行测试。开启测试后，NQA 客户端将主动向对端发出 TCP ACK 报文，以是否能收到对端返回的 RST 报文来判断对端的 TCP 服务是否可用。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 TCP Half Open 类型的 NQA 模板，并进入模板视图。

nqa template tcphalfopen *name*

(3) 配置测试操作的目的地址。

（IPv4 网络）

destination ip *ip-address*

（IPv6 网络）

destination ipv6 *ipv6-address*

缺省情况下，未配置探测报文的目的地址。

必须与 NQA 服务器上配置的监听服务的 IP 地址一致。

(4) 配置探测报文的源地址。

（IPv4 网络）

source ip *ip-address*

缺省情况下，以报文发送接口的主 IPv4 地址作为探测报文中的源 IPv4 地址。

该命令指定的源地址必须是设备上接口的 IPv4 地址，且接口为 up 状态，否则测试将会失败。

（IPv6 网络）

source ipv6 *ipv6-address*

缺省情况下，以报文发送接口的 IPv6 地址作为探测报文中的源 IPv6 地址。

该命令指定的源地址必须是设备上接口的 IPv6 地址，且接口为 up 状态，否则测试将会失败。

(5) 配置探测报文的下一跳地址。

（IPv4 网络）

next-hop ip *ip-address*

（IPv6 网络）

next-hop ipv6 *ipv6-address*

缺省情况下，未配置探测报文的下一跳地址。

(6) 配置每次探测结束时都将探测结果发送给外部特性。

reaction trigger per-probe

缺省情况下，连续探测成功或失败 3 次时，NQA 客户端会把探测成功或失败的消息发送给外部特性，使外部特性利用 NQA 测试的结果进行相应处理。

reaction trigger per-probe 命令与 **reaction trigger probe-pass** 命令作用相同，多次执行这两条命令时，最后一次执行的命令生效。

reaction trigger per-probe 命令与 **reaction trigger probe-fail** 命令作用相同，多次执行这两条命令时，最后一次执行的命令生效。

1.5.11 配置 UDP 类型的 NQA 模板

1. 功能简介

UDP 类型的 NQA 模板为外部特性提供 UDP 类型测试，外部特性通过引用该模板，测试客户端和服务器指定端口之间 UDP 传输的联通性。NQA 客户端通过处理服务器端的应答报文，判断服务器指定端口上提供的服务是否可用。

在 UDP 类型的 NQA 模板视图下，用户可以配置期望的应答内容。如果用户未配置期望的应答内容，则 NQA 客户端只要收到合法的回应报文就认为探测成功。

UDP 测试需要 NQA 服务器和客户端配合才能完成。在进行 UDP 测试前，需要在 NQA 服务器端配置 UDP 监听服务。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 UDP 类型的 NQA 模板，并进入模板视图。

nqa template udp *name*

(3) 配置测试操作的目的地址。

（IPv4 网络）

destination ip *ip-address*

（IPv6 网络）

destination ipv6 *ipv6-address*

缺省情况下，未配置探测报文的目的地址。

必须与 NQA 服务器上配置的监听服务的 IP 地址一致。

(4) 配置测试操作的目的端口。

destination port *port-number*

缺省情况下，未配置测试操作的目的端口号。

必须与 NQA 服务器上配置的监听服务的端口号一致。

(5) 配置探测报文的源地址。

（IPv4 网络）

source ip *ip-address*

缺省情况下，以报文发送接口的主 IPv4 地址作为探测报文中的源 IPv4 地址。

该命令指定的源地址必须是设备上接口的 IPv4 地址，且接口为 up 状态，否则测试将会失败。

（IPv6 网络）

source ipv6 *ipv6-address*

缺省情况下，以报文发送接口的 IPv6 地址作为探测报文中的源 IPv6 地址。

该命令指定的源地址必须是设备上接口的 IPv6 地址，且接口为 up 状态，否则测试将会失败。

(6) （可选）配置探测报文的填充字符串。

data-fill *string*

本命令的缺省情况与设备型号有关，请以设备的实际情况为准。

在未配置此命令情况下配置 **expect data** 命令则会探测失败。

(7) （可选）配置探测报文中的填充内容大小。

data-size *size*

缺省情况下，探测报文中的填充内容大小为 100 字节。

(8) （可选）配置用户期望的应答内容。

expect data *expression* [**offset** *number*]

缺省情况下，未配置期望的应答内容。

仅当 **data-fill** 和 **expect data** 命令都配置时，进行期望应答内容的检查，否则不做检查。

1.5.12 配置 HTTP 类型的 NQA 模板

1. 功能简介

HTTP 类型的 NQA 模板为外部特性提供 HTTP 类型测试，外部特性通过引用该模板，测试 NQA 客户端是否可以与指定的 HTTP 服务器建立连接，以及从 HTTP 服务器获取数据所需的时间，从而判断 HTTP 服务器的连通性及性能。

在 HTTP 类型的 NQA 模板中，用户可以配置期望返回的数据。通过该功能用户可以判断 HTTP 服务器应答报文的合法性。当应答报文中存在“Content-Length”字段，且配置了 **expect data** 命令时，设备将进行期望应答内容的检查。

在 HTTP 类型的 NQA 模板中，用户可以配置应答状态码。应答状态码是由 3 位十进制数组成的字段，它包含 HTTP 服务器的状态信息，用户可以根据该状态码了解 HTTP 服务器的状态。状态码的第一位表示状态码的类型。

2. 配置准备

在进行 HTTP 测试之前，需要完成 HTTP 服务器的配置。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 HTTP 类型的 NQA 模板，并进入模板视图。

nqa template http *name*

(3) 配置 HTTP 测试访问的目的网址。

url *url*

缺省情况下，没有配置 HTTP 测试访问的网址。

url 配置形式为 http://*host/resource* 或 http://*host:port/resource*。

(4) 配置 HTTP 登录用户名。

username *username*

缺省情况下，未配置 HTTP 登录用户名。

(5) 配置 HTTP 登录密码。

password { **cipher** | **simple** } *string*

缺省情况下，未配置 HTTP 登录密码。

(6) 配置 HTTP 所使用的协议版本。

version { **v1.0** | **v1.1** }

缺省情况下，HTTP 使用的版本为 v1.0。

(7) 配置 HTTP 的操作方式。

operation { **get** | **post** | **raw** }

缺省情况下，HTTP 操作方式为 **get** 操作。

如果 HTTP 操作方式为 **raw** 操作，则向服务器发送的探测报文的内容为 **raw-request** 视图中的内容。

(8) 配置 HTTP 测试请求报文。

a. 进入 raw-request 视图。

raw-request

输入 **raw-request** 命令进入 raw-request 视图，每次进入视图原有报文内容清除。

b. 配置 HTTP 测试请求报文内容。

逐个字符输入或拷贝粘贴请求报文内容。

缺省情况下，未配置 HTTP 测试请求报文内容。

要求报文内容中不能包含 **alias** 命令配置的别名，请用户自行确保报文的正确性，否则探测将失败。有关 **alias** 命令的详细介绍请参见“基础配置命令参考”中的“CLI”。

c. 保存输入内容并退回测试类型视图。

quit

当配置 HTTP 测试的操作类型为 **raw** 时，必须完成此操作且保证发送的测试报文正确有效。

(9) 配置探测报文的源地址。

（IPv4 网络）

source ip *ip-address*

缺省情况下，以报文发送接口的主 IPv4 地址作为探测报文中的源 IPv4 地址。

该命令指定的源地址必须是设备上接口的 IPv4 地址，且接口为 up 状态，否则测试将会失败。

（IPv6 网络）

source ipv6 *ipv6-address*

缺省情况下，以报文发送接口的 IPv6 地址作为探测报文中的源 IPv6 地址。

该命令指定的源地址必须是设备上接口的 IPv6 地址，且接口为 up 状态，否则测试将会失败。

(10) （可选）配置期望的应答状态码。

expect status *status-list*

缺省情况下，未配置期望的应答状态码。

(11) （可选）配置期望的应答内容。

expect data *expression* [**offset** *number*]

缺省情况下，未配置期望的应答内容。

1.5.13 配置 HTTPS 类型的 NQA 模板

1. 功能简介

HTTPS（Hypertext Transfer Protocol Secure，超文本传输协议的安全版本）是支持 SSL（Secure Sockets Layer，安全套接字层）协议的 HTTP 协议，通过 SSL 为 HTTP 协议提供安全保证。HTTPS 类型的 NQA 模板为外部特性提供 HTTPS 类型测试，外部特性通过引用该模板，测试 NQA 客户端是否可以与指定的 HTTPS 服务器建立连接，以及从 HTTPS 服务器获取数据所需的时间，从而判断 HTTPS 服务器的连通性及性能。

在 HTTPS 类型的 NQA 模板中，用户可以配置期望返回的数据。通过该功能用户可以判断 HTTPS 服务器应答报文的合法性。当应答报文中存在“Content-Length”字段，且配置了 **expect data** 命令时，设备将进行期望应答内容的检查。

在 HTTPS 类型的 NQA 模板中，用户可以配置应答状态码。应答状态码是由 3 位十进制数组成的字段，它包含 HTTPS 服务器的状态信息，用户可以根据该状态码了解 HTTPS 服务器的状态。状态码的第一位表示状态码的类型。

2. 配置准备

在进行 HTTPS 测试之前，需要在测试客户端完成 SSL 客户端策略配置，以及在目的端完成 HTTPS 服务器的配置。SSL 客户端策略的配置方法请参见“安全配置指导”中的“SSL”。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 HTTPS 类型的 NQA 模板，并进入模板视图。

nqa template https *name*

(3) 配置 HTTPS 测试访问的目的网址。

url *url*

缺省情况下，没有配置 HTTPS 测试访问的网址。

url 参数的格式为 https://*host/resource* 或 https://*host:port/resource*。

(4) 配置 HTTPS 登录用户名。

username *username*

缺省情况下，未配置 HTTPS 登录用户名。

(5) 配置 HTTPS 登录密码。

password { **cipher** | **simple** } *string*

缺省情况下，未配置 HTTPS 登录密码。

(6) 绑定 SSL 客户端策略。

ssl-client-policy *policy-name*

缺省情况下，未绑定 SSL 客户端策略。

(7) 配置 HTTPS 所使用的协议版本。

version { **v1.0** | **v1.1** }

缺省情况下，HTTPS 使用的版本为 v1.0。

(8) 配置 HTTPS 的操作方式。

operation { **get** | **post** | **raw** }

缺省情况下，HTTPS 操作方式为 **get** 操作。

如果 HTTP 操作方式为 **raw** 操作，则向服务器发送的探测报文的内容为 **raw-request** 视图中的内容。

(9) 配置 HTTPS 测试请求报文。

a. 进入 raw-request 视图。

raw-request

输入 **raw-request** 命令进入 raw-request 视图，每次进入视图原有报文内容清除。

b. 配置 HTTPS 测试请求报文内容。

逐个字符输入或拷贝粘贴请求报文内容。

缺省情况下，未配置 HTTPS 测试请求报文内容。

要求报文内容中不能包含 **alias** 命令配置的别名，请用户自行确保报文的正确性，否则探测将失败。有关 **alias** 命令的详细介绍请参见“基础配置命令参考”中的“CLI”。

c. 保存输入内容并退回测试类型视图。

quit

当配置 HTTPS 测试的操作类型为 **raw** 时，必须完成此操作且保证发送的测试报文正确有效。

(10) 配置探测报文的源地址。

（IPv4 网络）

source ip *ip-address*

缺省情况下，以报文发送接口的主 IPv4 地址作为探测报文中的源 IPv4 地址。

该命令指定的源地址必须是设备上接口的 IPv4 地址，且接口为 up 状态，否则测试将会失败。

（IPv6 网络）

source ipv6 *ipv6-address*

缺省情况下，以报文发送接口的 IPv6 地址作为探测报文中的源 IPv6 地址。

该命令指定的源地址必须是设备上接口的 IPv6 地址，且接口为 up 状态，否则测试将会失败。

(11) （可选）配置期望的应答内容。

expect data *expression* [**offset** *number*]

缺省情况下，未配置期望的应答内容。

(12) （可选）配置期望的应答状态码。

expect status *status-list*

缺省情况下，未配置期望的应答状态码。

1.5.14 配置 FTP 类型的 NQA 模板

1. 功能简介

FTP 类型的 NQA 模板为外部特性提供 FTP 类型测试，外部特性通过引用该模板，与指定的 FTP 服务器建立连接，以及与 FTP 服务器之间传送文件的时间，从而判断 FTP 服务器的连通性及性能。

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

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 FTP 类型的 NQA 模板，并进入模板视图。

nqa template ftp *name*

(3) 配置 FTP 登录用户名。

username *username*

缺省情况下，未配置 FTP 登录用户名。

(4) 配置 FTP 登录密码。

password { **cipher** | **simple** } *string*

缺省情况下，未配置 FTP 登录密码。

(5) 配置探测报文的源地址。

（IPv4 网络）

source ip *ip-address*

缺省情况下，以报文发送接口的主 IPv4 地址作为探测报文中的源 IPv4 地址。

该命令指定的源地址必须是设备上接口的 IPv4 地址，且接口为 up 状态，否则测试将会失败。

（IPv6 网络）

source ipv6 *ipv6-address*

缺省情况下，以报文发送接口的 IPv6 地址作为探测报文中的源 IPv6 地址。

该命令指定的源地址必须是设备上接口的 IPv6 地址，且接口为 up 状态，否则测试将会失败。

(6) 配置 FTP 的数据传输方式。

mode { **active** | **passive** }

缺省情况下，FTP 数据传输方式为主动方式。

(7) 配置 FTP 的操作类型。

operation { **get** | **put** }

缺省情况下，FTP 操作方式为 **get** 操作，即从 FTP 服务器获取文件。

(8) 配置 FTP 测试访问的目的网址。

url *url*

缺省情况下，没有配置 FTP 测试访问的网址。

url 可以设置为 ftp://*host*/*filename* 或 ftp://*host*:*port*/*filename*。当 FTP 测试的操作类型为 **get** 方式时，必须在 *url* 中配置 *filename* 指定从 FTP 服务器获取的文件名。

(9) 配置 FTP 服务器和客户端传送文件的文件名。

filename *filename*

缺省情况下，未配置 FTP 服务器和客户端之间传送文件的文件名。

当 FTP 测试的操作类型为 **put** 方式时，必须配置本命令来指定向 FTP 服务器传送的文件。

当 FTP 测试的操作类型为 **get** 方式时，不以此命令为准。

1.5.15 配置 RADIUS 类型的 NQA 模板

1. 功能简介

RADIUS 类型的 NQA 模板为外部特性提供 RADIUS 类型测试，外部特性通过引用该模板来启动 RADIUS 测试，来检测 RADIUS 服务器的业务可用性。

RADIUS 服务器是一种提供认证、授权和计费功能的服务器，RADIUS 类型的 NQA 模板检测过程选择了最基本的 RADIUS 认证过程：

(1) NQA 客户端根据配置的用户名和密码，向 RADIUS 服务器发送认证请求包（Access-Request），其中的密码在共享密钥 Key 的参与下利用 MD5 算法进行加密处理。

(2) RADIUS 服务器对用户名和密码进行认证，如果认证成功，RADIUS 服务器向 NQA 客户端发送认证接受包（Access-Accept）；如果认证失败，则返回认证拒绝包（Access-Reject）。

(3) 当 NQA 客户端收到 RADIUS 服务器发出的认证接受包后，则表示 RADIUS 服务器是健康的；否则，该 RADIUS 服务器被认为无法成功提供服务。

2. 配置准备

RADIUS 测试需要 RADIUS 服务器和 NQA 客户端配合才能完成。进行 RADIUS 探测时，要求 RADIUS 服务器存在探测使用的用户信息，并配置与 NQA 客户端相同的密钥（Key）。RADIUS 服务器配置方法，请参见“安全配置指导”中的“AAA”。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 RADIUS 类型的 NQA 模板，并进入模板视图。

nqa template radius *name*

(3) 配置测试操作的目的地址。

（IPv4 网络）

destination ip *ip-address*

（IPv6 网络）

destination ipv6 *ipv6-address*

缺省情况下，未配置探测报文的目的地址。

(4) 配置测试操作的目的端口。

destination port *port-number*

缺省情况下，测试操作的目的端口号为 1812。

(5) 配置 RADIUS 用户名。

username *username*

缺省情况下，未配置 RADIUS 用户名。

(6) 配置 RADIUS 密码。

password { **cipher** | **simple** } *string*

缺省情况下，未配置 RADIUS 密码。

(7) 配置 RADIUS 认证使用的共享密钥。

key { **cipher** | **simple** } *string*

缺省情况下，未配置 RADIUS 认证使用的共享密钥。

(8) 配置探测报文的源地址。

（IPv4 网络）

source ip *ip-address*

缺省情况下，以报文发送接口的主 IPv4 地址作为探测报文中的源 IPv4 地址。

该命令指定的源地址必须是设备上接口的 IPv4 地址，且接口为 up 状态，否则测试将会失败。

（IPv6 网络）

source ipv6 *ipv6-address*

缺省情况下，以报文发送接口的 IPv6 地址作为探测报文中的源 IPv6 地址。

该命令指定的源地址必须是设备上接口的 IPv6 地址，且接口为 up 状态，否则测试将会失败。

1.5.16 配置 SNMP 类型的 NQA 模板

1. 功能简介

SNMP 类型的 NQA 模板为外部特性提供 SNMP 类型测试，外部特性通过引用该模板来启动 SNMP 测试。测试时 NQA 客户端向 SNMP Agent 设备发送一个协议查询报文，根据能否收到应答报文判断 SNMP Agent 上提供的 SNMP 服务是否可用。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 SNMP 类型的 NQA 模板，并进入模板视图。

nqa template snmp *name*

(3) 配置测试操作的目的地址。

（IPv4 网络）

destination ip *ip-address*

（IPv6 网络）

destination ipv6 *ipv6-address*

缺省情况下，未配置探测报文的目的地址。

(4) 配置测试操作的目的端口。

destination port *port-number*

缺省情况下，测试操作的目的端口号为 161。

(5) 配置探测报文的源地址。

（IPv4 网络）

source ip *ip-address*

缺省情况下，以报文发送接口的主 IPv4 地址作为探测报文中的源 IPv4 地址。

该命令指定的源地址必须是设备上接口的 IPv4 地址，且接口为 up 状态，否则测试将会失败。

（IPv6 网络）

source ipv6 *ipv6-address*

缺省情况下，以报文发送接口的 IPv6 地址作为探测报文中的源 IPv6 地址。

该命令指定的源地址必须是设备上接口的 IPv6 地址，且接口为 up 状态，否则测试将会失败。

(6) 配置用于 SNMPv1 或者 SNMPv2c 探测报文的团体名。

community read { **cipher** | **simple** } *community-name*

缺省情况下，SNMPv1 或者 SNMPv2c 探测报文使用的团体名为 public。

该命令配置的团体名必须为 SNMP Agent 上已配置具有读权限的团体名。

1.5.17 配置 SSL 类型的 NQA 模板

1. 功能简介

SSL 类型的 NQA 模板为外部特性提供 SSL 类型测试，外部特性通过引用该模板，测试 NQA 客户端是否可以与指定的 SSL 服务器建立 SSL 连接，从而通过 SSL 连接建立的时间判断服务器的连通性及性能。

2. 配置准备

在进行 SSL 测试之前，需要在测试客户端完成 SSL 客户端策略配置。SSL 客户端策略配置方法请参见“安全配置指导”中的“SSL”。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 SSL 类型的 NQA 模板，并进入模板视图。

nqa template ssl *name*

(3) 配置测试操作的目的地址。

（IPv4 网络）

destination ip *ip-address*

（IPv6 网络）

destination ipv6 *ipv6-address*

缺省情况下，未配置探测报文的目的地址。

(4) 配置测试操作的目的端口。

destination port *port-number*

缺省情况下，未配置测试操作的目的端口号。

(5) 绑定 SSL 客户端策略。

ssl-client-policy *policy-name*

缺省情况下，未绑定 SSL 客户端策略。

(6) 配置探测报文的源地址。

（IPv4 网络）

source ip *ip-address*

缺省情况下，以报文发送接口的主 IPv4 地址作为探测报文中的源 IPv4 地址。

该命令指定的源地址必须是设备上接口的 IPv4 地址，且接口为 up 状态，否则测试将会失败。

（IPv6 网络）

source ipv6 *ipv6-address*

缺省情况下，以报文发送接口的 IPv6 地址作为探测报文中的源 IPv6 地址。

该命令指定的源地址必须是设备上接口的 IPv6 地址，且接口为 up 状态，否则测试将会失败。

1.5.18 配置 NQA 模板通用参数

1. 配置限制和指导

NQA 模板的通用参数，只对当前模板的测试有效。

除特别说明外，所有类型 NQA 模板都可以根据实际情况选择配置下列通用参数。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入已存在的 NQA 模板视图。

nqa template { **arp** | **dns** | **ftp** | **http** | **https** | **icmp** | **imap** | **pop3** | **smtp** | **snmp** | **ssl** | **tcp** | **tcphalfopen** | **udp** } *name*

(3) 配置 NQA 模板的描述信息。

description *text*

缺省情况下，未配置模板的信息。

(4) 配置连续两次探测开始时间的时间间隔。

frequency *interval*

缺省情况下，连续两次探测开始时间的时间间隔为 5000 毫秒。

如果到达 **frequency** 指定的时间间隔时，上次探测尚未完成，则不启动新一轮探测。

(5) 配置每次探测超时时间。

probe timeout *timeout*

缺省情况下，探测的超时时间为 3000 毫秒。

(6) 配置探测报文在网络中可以经过的最大跳数。

ttl *value*

缺省情况下，探测报文在网络中可以经过的最大跳数为 20 跳。

ARP 类型的 NQA 模板不支持配置本命令。

(7) 配置 NQA 探测报文 IP 报文头中服务类型域的值。

tos *value*

缺省情况下，NQA 探测报文 IP 报文头中服务类型域的值为 0。

ARP 类型的 NQA 模板不支持配置本命令。

(8) 指定操作所属的 VPN 实例。

vpn-instance *vpn-instance-name*

缺省情况下，未指定操作所属的 VPN 实例。

(9) 配置连续探测成功的次数，当连续探测成功次数达到命令配置的数值时，NQA 客户端会把探测成功的消息发送给外部特性，使外部特性利用 NQA 测试的结果进行相应处理。

reaction trigger probe-pass *count*

缺省情况下，连续探测成功 3 次时，NQA 客户端会把探测成功的消息发送给外部特性，使外部特性利用 NQA 测试的结果进行相应处理。

(10) 配置连续探测失败的次数，当连续探测失败次数达到命令配置的数值时，NQA 客户端会把探测失败的消息发送给外部特性，使外部特性利用 NQA 测试的结果进行相应处理。

reaction trigger probe-fail *count*

缺省情况下，连续探测失败 3 次时，NQA 客户端会把探测失败的消息发送给外部特性，是外部特性利用 NQA 测试的结果进行相应处理。

1.6 NQA显示和维护

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

表1-1 NQA 显示和维护（NQA 客户端）

操作	命令
显示NQA测试组的历史记录	**display nqa history** [*admin-name operation-tag*]
显示NQA阈值告警功能的当前监测结果	**display nqa reaction counters** [*admin-name operation-tag* [*item-number*]]
显示最近一次NQA测试的当前结果	**display nqa result** [*admin-name operation-tag*]
显示NQA测试的统计信息	**display nqa statistics** [*admin-name operation-tag*]

表1-2 NQA 显示和维护（NQA 服务器）

操作	命令
显示路径服务质量测试和Y.1564测试反射端的会话信息	**display nqa reflector** [*reflector-id*]
显示服务器的状态信息	**display nqa server**

1.7 NQA测试典型配置举例

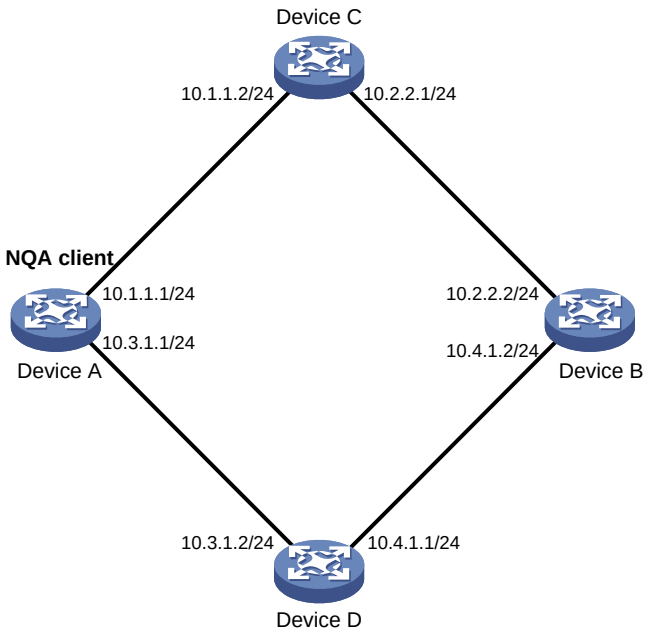
1.7.1 ICMP-echo 测试配置举例

1. 组网需求

使用 NQA 的 ICMP-echo 测试功能，测试本端（Device A）发送的报文是否可以经过指定的下一跳设备（Device C）到达指定的目的端（Device B），以及报文的往返时间。

2. 组网图

图1-2 ICMP-echo 测试组网图



3. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

创建 ICMP-echo 类型的 NQA 测试组（管理员为 admin，操作标签为 test1），并配置探测报文的目的地址为 10.2.2.2。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type icmp-echo
[DeviceA-nqa-admin-test1-icmp-echo] destination ip 10.2.2.2
```

配置下一跳地址为 10.1.1.2，以便测试报文经过指定的下一跳设备（Device C）到达目的端，而不是通过 Device D 到达目的端。

```
[DeviceA-nqa-admin-test1-icmp-echo] next-hop ip 10.1.1.2
```

配置可选参数：一次 NQA 测试中探测的次数为 10，探测的超时时间为 500 毫秒，测试组连续两次测试开始时间的时间间隔为 5000 毫秒。

```
[DeviceA-nqa-admin-test1-icmp-echo] probe count 10
[DeviceA-nqa-admin-test1-icmp-echo] probe timeout 500
[DeviceA-nqa-admin-test1-icmp-echo] frequency 5000
```

开启 NQA 历史记录保存功能，并配置一个测试组中能够保存的最大历史记录个数为 10。

```
[DeviceA-nqa-admin-test1-icmp-echo] history-record enable
[DeviceA-nqa-admin-test1-icmp-echo] history-record number 10
[DeviceA-nqa-admin-test1-icmp-echo] quit
```

启动 ICMP-echo 测试操作，并一直进行测试。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

测试执行一段时间后，停止 ICMP-echo 测试操作。

```
[DeviceA] undo nqa schedule admin test1
```

4. 验证配置

显示 ICMP-echo 测试中最后一次测试的当前结果。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
```

```
    Send operation times: 10             Receive response times: 10
    Min/Max/Average round trip time: 2/5/3
    Square-Sum of round trip time: 96
    Last succeeded probe time: 2011-08-23 15:00:01.2
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

显示 ICMP-echo 测试的历史记录。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  370        3            Succeeded        2011-08-23 15:00:01.2
  369        3            Succeeded        2011-08-23 15:00:01.2
  368        3            Succeeded        2011-08-23 15:00:01.2
  367        5            Succeeded        2011-08-23 15:00:01.2
  366        3            Succeeded        2011-08-23 15:00:01.2
  365        3            Succeeded        2011-08-23 15:00:01.2
  364        3            Succeeded        2011-08-23 15:00:01.1
  363        2            Succeeded        2011-08-23 15:00:01.1
  362        3            Succeeded        2011-08-23 15:00:01.1
  361        2            Succeeded        2011-08-23 15:00:01.1
```

以上显示信息表示，Device A 发送的报文可以通过 Device C 到达 Device B；测试过程中未发生丢包；报文的最小、最大、平均往返时间分别为 2 毫秒、5 毫秒和 3 毫秒。

1.7.2 ICMP-jitter 测试配置举例

1. 组网需求

使用 NQA 的 ICMP-jitter 测试功能，测试本端（Device A）和指定目的端（Device B）之间传送报文的时延抖动。

2. 组网图

图1-3 ICMP-jitter 测试组网图

3. 配置步骤

(1) 配置各接口的 IP 地址。（配置过程略）

(2) 配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

(3) 配置 Device A

创建 ICMP-jitter 类型的 NQA 测试组（管理员为 admin，操作标签为 test1）。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type icmp-jitter
```

配置测试操作的探测报文的目的地址为 10.2.2.2。

```
[DeviceA-nqa-admin-test1-icmp-jitter] destination ip 10.2.2.2
```

配置可选参数：测试组连续两次测试开始的时间间隔为 1000 毫秒。

```
[DeviceA-nqa-admin-test1-icmp-jitter] frequency 1000
[DeviceA-nqa-admin-test1-icmp-jitter] quit
```

启动 ICMP-jitter 测试操作，并一直进行测试。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

测试执行一段时间后，停止 ICMP-jitter 测试操作。

```
[DeviceA] undo nqa schedule admin test1
```

4. 验证配置

显示 ICMP-jitter 测试中最后一次测试的当前结果。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 10             Receive response times: 10
    Min/Max/Average round trip time: 1/2/1
    Square-Sum of round trip time: 13
    Last packet received time: 2015-03-09 17:40:29.8
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  ICMP-jitter results:
   RTT number: 10
    Min positive SD: 0                   Min positive DS: 0
    Max positive SD: 0                   Max positive DS: 0
    Positive SD number: 0                Positive DS number: 0
    Positive SD sum: 0                   Positive DS sum: 0
    Positive SD average: 0               Positive DS average: 0
    Positive SD square-sum: 0            Positive DS square-sum: 0
    Min negative SD: 1                   Min negative DS: 2
    Max negative SD: 1                   Max negative DS: 2
    Negative SD number: 1                Negative DS number: 1
    Negative SD sum: 1                   Negative DS sum: 2
    Negative SD average: 1               Negative DS average: 2
    Negative SD square-sum: 1            Negative DS square-sum: 4
    SD average: 1                        DS average: 2
  One way results:
    Max SD delay: 1                      Max DS delay: 2
    Min SD delay: 1                      Min DS delay: 2
    Number of SD delay: 1                Number of DS delay: 1
    Sum of SD delay: 1                   Sum of DS delay: 2
    Square-Sum of SD delay: 1            Square-Sum of DS delay: 4
    Lost packets for unknown reason: 0
```

显示 ICMP-jitter 测试的统计结果。

```
[DeviceA] display nqa statistics admin test1
NQA entry (admin admin, tag test1) test statistics:
  NO. : 1
    Start time: 2015-03-09 17:42:10.7
    Life time: 156 seconds
```

```
  Send operation times: 1560           Receive response times: 1560
  Min/Max/Average round trip time: 1/2/1
  Square-Sum of round trip time: 1563
Extended results:
  Packet loss ratio: 0%
  Failures due to timeout: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packets out of sequence: 0
  Packets arrived late: 0
ICMP-jitter results:
 RTT number: 1560
  Min positive SD: 1                   Min positive DS: 1
  Max positive SD: 1                   Max positive DS: 2
  Positive SD number: 18               Positive DS number: 46
  Positive SD sum: 18                  Positive DS sum: 49
  Positive SD average: 1               Positive DS average: 1
  Positive SD square-sum: 18           Positive DS square-sum: 55
  Min negative SD: 1                   Min negative DS: 1
  Max negative SD: 1                   Max negative DS: 2
  Negative SD number: 24               Negative DS number: 57
  Negative SD sum: 24                  Negative DS sum: 58
  Negative SD average: 1               Negative DS average: 1
  Negative SD square-sum: 24           Negative DS square-sum: 60
  SD average: 1                        DS average: 1
One way results:
  Max SD delay: 1                      Max DS delay: 2
  Min SD delay: 1                      Min DS delay: 1
  Number of SD delay: 4                Number of DS delay: 4
  Sum of SD delay: 4                   Sum of DS delay: 5
  Square-Sum of SD delay: 4            Square-Sum of DS delay: 7
  Lost packets for unknown reason: 0
```

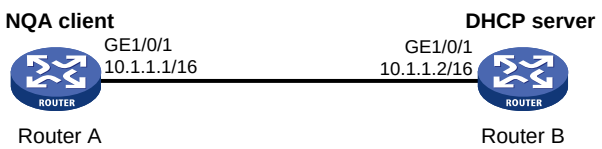
1.7.3 DHCP 测试配置举例（路由应用）

1. 组网需求

使用 NQA 的 DHCP 测试功能，测试 Router A 从 DHCP 服务器 Router B 申请到 IP 地址所需的时间。

2. 组网图

图1-4 配置 DHCP 测试组网图



3. 配置步骤

创建 DHCP 类型的 NQA 测试组（管理员为 admin，操作标签为 test1），并指定进行 DHCP 测试中探测报文的目的地址为 10.1.1.2。

```
<RouterA> system-view
[RouterA] nqa entry admin test1
```

```
[RouterA-nqa-admin-test1] type dhcp
[RouterA-nqa-admin-test1-dhcp] destination ip 10.1.1.2
```

开启 NQA 测试组的历史记录保存功能。

```
[RouterA-nqa-admin-test1-dhcp] history-record enable
[RouterA-nqa-admin-test1-dhcp] quit
```

启动 DHCP 测试操作，并一直进行测试。

```
[RouterA] nqa schedule admin test1 start-time now lifetime forever
```

测试执行一段时间后，停止 DHCP 测试操作。

```
[RouterA] undo nqa schedule admin test1
```

4. 验证配置

显示 DHCP 测试中最后一次测试的当前结果。

```
[RouterA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 512/512/512
    Square-Sum of round trip time: 262144
    Last succeeded probe time: 2011-11-22 09:54:03.8
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

显示 DHCP 测试的历史记录。

```
[RouterA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          512          Succeeded        2011-11-22 09:54:03.8
```

以上显示信息表示，Router A 可以从 DHCP 服务器获取 IP 地址，获取 IP 地址所需的时间为 512 毫秒。

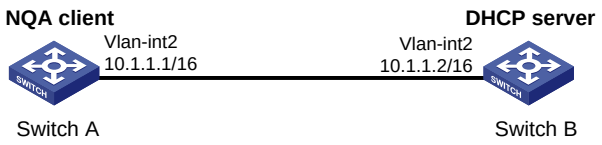
1.7.4 DHCP 测试配置举例（交换应用）

1. 组网需求

使用 NQA 的 DHCP 测试功能，测试 Switch A 从 DHCP 服务器 Switch B 申请到 IP 地址所需的时间。

2. 组网图

图1-5 配置 DHCP 测试组网图



3. 配置步骤

创建 DHCP 类型的 NQA 测试组（管理员为 admin，操作标签为 test1），并指定进行 DHCP 测试中探测报文的目的地址为 10.1.1.2。

```
<SwitchA> system-view
[SwitchA] nqa entry admin test1
[SwitchA-nqa-admin-test1] type dhcp
[SwitchA-nqa-admin-test1-dhcp] destination ip 10.1.1.2
```

开启 NQA 测试组的历史记录保存功能。

```
[SwitchA-nqa-admin-test1-dhcp] history-record enable
[SwitchA-nqa-admin-test1-dhcp] quit
```

启动 DHCP 测试操作，并一直进行测试。

```
[SwitchA] nqa schedule admin test1 start-time now lifetime forever
```

测试执行一段时间后，停止 DHCP 测试操作。

```
[SwitchA] undo nqa schedule admin test1
```

4. 验证配置

显示 DHCP 测试中最后一次测试的当前结果。

```
[SwitchA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 512/512/512
    Square-Sum of round trip time: 262144
    Last succeeded probe time: 2011-11-22 09:56:03.2
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

显示 DHCP 测试的历史记录。

```
[SwitchA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          512          Succeeded        2011-11-22 09:56:03.2
```

以上显示信息表示，Switch A 可以从 DHCP 服务器获取 IP 地址，获取 IP 地址所需的时间为 512 毫秒。

1.7.5 DNS 测试配置举例

1. 组网需求

使用 NQA 的 DNS 测试功能，测试 Device A 是否可以通过指定的 DNS 服务器将域名 host.com 解析为 IP 地址，并测试域名解析所需的时间。

2. 组网图

图1-6 配置 DNS 组网图

3. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

创建 DNS 类型的 NQA 测试组（管理员为 admin，操作标签为 test1）。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type dns
```

配置探测报文的目的地址为 DNS 服务器的 IP 地址 10.2.2.2，要解析的域名为 host.com。

```
[DeviceA-nqa-admin-test1-dns] destination ip 10.2.2.2
[DeviceA-nqa-admin-test1-dns] resolve-target host.com
```

开启 NQA 测试组的历史记录保存功能。

```
[DeviceA-nqa-admin-test1-dns] history-record enable
[DeviceA-nqa-admin-test1-dns] quit
```

启动 DNS 测试操作，并一直进行测试。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

测试执行一段时间后，停止 DNS 测试操作。

```
[DeviceA] undo nqa schedule admin test1
```

4. 验证配置

显示 DNS 测试中最后一次测试的当前结果。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 62/62/62
    Square-Sum of round trip time: 3844
    Last succeeded probe time: 2011-11-10 10:49:37.3
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

显示 DNS 测试的历史记录。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          62           Succeeded        2011-11-10 10:49:37.3
```

以上显示信息表示，Device A 可以通过指定的 DNS 服务器将域名 host.com 解析为 IP 地址，域名解析所需的时间为 62 毫秒。

1.7.6 FTP 测试配置举例

1. 组网需求

使用 NQA 的 FTP 测试功能，测试 Device A 是否可以和指定的 FTP 服务器 Device B 建立连接，以及往 FTP 服务器上传一个文件的时间。登录 FTP 服务器的用户名为 admin，密码为 systemtest，要传送到服务器的文件名为 config.txt。

2. 组网图

图1-7 配置 FTP 组网图

3. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

创建 FTP 类型的 NQA 测试组（管理员为 admin，操作标签为 test1）。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type ftp
```

配置测试操作的目的地址为 FTP 服务器的 IP 地址 10.2.2.2。

```
[DeviceA-nqa-admin-test1-ftp] url ftp://10.2.2.2
```

配置探测报文的源 IP 地址为 10.1.1.1。

```
[DeviceA-nqa-admin-test1-ftp] source ip 10.1.1.1
```

配置测试执行的操作为向 FTP 服务器上传文件 config.txt。

```
[DeviceA-nqa-admin-test1-ftp] operation put
[DeviceA-nqa-admin-test1-ftp] filename config.txt
```

配置 FTP 操作的登录用户名为 admin。

```
[DeviceA-nqa-admin-test1-ftp] username admin
```

配置 FTP 操作的登录密码为 systemtest。

```
[DeviceA-nqa-admin-test1-ftp] password simple systemtest
```

开启 NQA 测试组的历史记录保存功能。

```
[DeviceA-nqa-admin-test1-ftp] history-record enable
[DeviceA-nqa-admin-test1-ftp] quit
```

启动 FTP 测试操作，并一直进行测试。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

测试执行一段时间后，停止 FTP 测试操作。

```
[DeviceA] undo nqa schedule admin test1
```

4. 验证配置

显示 FTP 测试中最后一次测试的当前结果。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 173/173/173
    Square-Sum of round trip time: 29929
    Last succeeded probe time: 2011-11-22 10:07:28.6
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

显示 FTP 测试的历史记录。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          173          Succeeded        2011-11-22 10:07:28.6
```

以上显示信息表示，Device A 可以和指定的 FTP 服务器 Device B 建立连接，向 FTP 服务器上传一个文件的时间是 173 毫秒。

1.7.7 HTTP 测试配置举例

1. 组网需求

使用 NQA 的 HTTP 测试功能，测试是否可以和指定的 HTTP 服务器之间建立连接，以及从 HTTP 服务器获取数据的时间。

2. 组网图

图1-8 HTTP 测试组网图

3. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

创建 HTTP 类型的 NQA 测试组（管理员为 admin，操作标签为 test1）。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type http
```

配置 HTTP 测试服务器的 IP 地址为 10.2.2.2，访问的网址为/index.html。

```
[DeviceA-nqa-admin-test1-http] url http://10.2.2.2/index.html
```

配置 HTTP 测试的操作方式为 get 操作。（get 操作为缺省操作方式，因此，可以不执行本配置）

```
[DeviceA-nqa-admin-test1-http] operation get
```

配置 HTTP 测试使用的版本为 1.0。（缺省情况下使用的版本为 1.0，因此，可以不执行本配置）

```
[DeviceA-nqa-admin-test1-http] version v1.0
```

开启 NQA 测试组的历史记录保存功能。

```
[DeviceA-nqa-admin-test1-http] history-record enable
[DeviceA-nqa-admin-test1-http] quit
```

启动 HTTP 测试操作，并一直进行测试。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

测试执行一段时间后，停止 HTTP 测试操作。

```
[DeviceA] undo nqa schedule admin test1
```

4. 验证配置

显示 HTTP 测试中最后一次测试的当前结果。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 64/64/64
    Square-Sum of round trip time: 4096
    Last succeeded probe time: 2011-11-22 10:12:47.9
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
```

```
    Failures due to other errors: 0
```

显示 HTTP 测试的历史记录。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          64           Succeeded        2011-11-22 10:12:47.9
```

以上显示信息表示，Device A 可以和指定的 HTTP 服务器 Device B 建立连接，从 HTTP 服务器获取数据的时间为 64 毫秒。

1.7.8 UDP-jitter 测试配置举例

1. 组网需求

使用 NQA 的 UDP-jitter 测试功能，测试本端（Device A）和指定目的端（Device B）的端口 9000 之间传送报文的抖动时间。

2. 组网图

图1-9 UDP-jitter 测试组网图

3. 配置步骤

(1) 配置各接口的 IP 地址。（配置过程略）

(2) 配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

(3) 配置 Device B

使能 NQA 服务器，配置监听的 IP 地址为 10.2.2.2，UDP 端口号为 9000。

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server udp-echo 10.2.2.2 9000
```

(4) 配置 Device A

创建 UDP-jitter 类型的 NQA 测试组（管理员为 admin，操作标签为 test1）。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type udp-jitter
```

配置测试操作的探测报文的目的地址为 10.2.2.2，目的端口号为 9000。

```
[DeviceA-nqa-admin-test1-udp-jitter] destination ip 10.2.2.2
[DeviceA-nqa-admin-test1-udp-jitter] destination port 9000
```

配置可选参数：测试组连续两次测试开始时间的时间间隔为 1000 毫秒。

```
[DeviceA-nqa-admin-test1-udp-jitter] frequency 1000
[DeviceA-nqa-admin-test1-udp-jitter] quit
```

启动 UDP-jitter 测试操作，并一直进行测试。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

测试执行一段时间后，停止 UDP-jitter 测试操作。

```
[DeviceA] undo nqa schedule admin test1
```

4. 验证配置

显示 UDP-jitter 测试中最后一次测试的当前结果。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 10             Receive response times: 10
    Min/Max/Average round trip time: 15/32/17
    Square-Sum of round trip time: 3235
    Last packet received time: 2011-05-29 13:56:17.6
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  UDP-jitter results:
    RTT number: 10
    Min positive SD: 4                   Min positive DS: 1
    Max positive SD: 21                  Max positive DS: 28
    Positive SD number: 5                Positive DS number: 4
    Positive SD sum: 52                  Positive DS sum: 38
    Positive SD average: 10              Positive DS average: 10
    Positive SD square-sum: 754          Positive DS square-sum: 460
    Min negative SD: 1                   Min negative DS: 6
    Max negative SD: 13                  Max negative DS: 22
    Negative SD number: 4                Negative DS number: 5
    Negative SD sum: 38                  Negative DS sum: 52
    Negative SD average: 10              Negative DS average: 10
    Negative SD square-sum: 460          Negative DS square-sum: 754
    SD average: 10                       DS average: 10
  One way results:
    Max SD delay: 15                     Max DS delay: 16
    Min SD delay: 7                      Min DS delay: 7
    Number of SD delay: 10               Number of DS delay: 10
    Sum of SD delay: 78                  Sum of DS delay: 85
    Square-Sum of SD delay: 666          Square-Sum of DS delay: 787
    SD lost packets: 0                   DS lost packets: 0
    Lost packets for unknown reason: 0
```

显示 UDP-jitter 测试的统计结果。

```
[DeviceA] display nqa statistics admin test1
NQA entry (admin admin, tag test1) test statistics:
  NO. : 1
    Start time: 2011-05-29 13:56:14.0
    Life time: 47 seconds
    Send operation times: 410            Receive response times: 410
    Min/Max/Average round trip time: 1/93/19
    Square-Sum of round trip time: 206176
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
```

```
  Packets arrived late: 0
UDP-jitter results:
 RTT number: 410
  Min positive SD: 3                  Min positive DS: 1
  Max positive SD: 30                 Max positive DS: 79
  Positive SD number: 186             Positive DS number: 158
  Positive SD sum: 2602               Positive DS sum: 1928
  Positive SD average: 13             Positive DS average: 12
  Positive SD square-sum: 45304       Positive DS square-sum: 31682
  Min negative SD: 1                  Min negative DS: 1
  Max negative SD: 30                 Max negative DS: 78
  Negative SD number: 181             Negative DS number: 209
  Negative SD sum: 181                Negative DS sum: 209
  Negative SD average: 13             Negative DS average: 14
  Negative SD square-sum: 46994       Negative DS square-sum: 3030
  SD average: 10                      DS average: 7
One way results:
  Max SD delay: 46                    Max DS delay: 46
  Min SD delay: 7                     Min DS delay: 7
  Number of SD delay: 410             Number of DS delay: 410
  Sum of SD delay: 3705               Sum of DS delay: 3891
  Square-Sum of SD delay: 45987       Square-Sum of DS delay: 49393
  SD lost packets: 0                  DS lost packets: 0
  Lost packets for unknown reason: 0
```

1.7.9 SNMP 测试配置举例

1. 组网需求

使用 NQA 的 SNMP 测试功能，测试从 Device A 发出 SNMP 协议查询报文到收到 SNMP Agent（Device B）响应报文所用的时间。

2. 组网图

图1-10 SNMP 配置测试组网图

3. 配置步骤

(1) 配置各接口的 IP 地址。（配置过程略）

(2) 配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

(3) 配置 SNMP Agent（Device B）

启动 SNMP Agent 服务，设置 SNMP 版本为 all、只读团体名为 public、读写团体名为 private。

```
<DeviceB> system-view
[DeviceB] snmp-agent sys-info version all
[DeviceB] snmp-agent community read public
[DeviceB] snmp-agent community write private
```

(4) 配置 Device A

创建 SNMP 类型的测试组（管理员为 admin，操作标签为 test1），并配置测试操作的探测报文的目的地址为 SNMP Agent 的 IP 地址 10.2.2.2。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type snmp
[DeviceA-nqa-admin-test1-snmp] destination ip 10.2.2.2
```

开启 NQA 测试组的历史记录保存功能。

```
[DeviceA-nqa-admin-test1-snmp] history-record enable
[DeviceA-nqa-admin-test1-snmp] quit
```

启动测试操作，并一直进行测试。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

测试执行一段时间后，停止 SNMP 测试操作。

```
[DeviceA] undo nqa schedule admin test1
```

4. 验证配置

显示 SNMP 测试中最后一次测试的当前结果。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 50/50/50
    Square-Sum of round trip time: 2500
    Last succeeded probe time: 2011-11-22 10:24:41.1
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

显示 SNMP 测试的历史记录。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          50           Succeeded        2011-11-22 10:24:41.1
```

以上显示信息表示，Device A 可以和 SNMP Agent（Device B）建立连接，从 Device A 发出一个 SNMP 协议查询报文到收到 SNMP Agent 响应报文所用的时间为 50 毫秒。

1.7.10 TCP 测试配置举例

1. 组网需求

使用 NQA 的 TCP 测试功能，测试本端（Device A）和指定目的端（Device B）的端口 9000 之间建立 TCP 连接所需的时间。

2. 组网图

图1-11 TCP 测试组网图

3. 配置步骤

(1) 配置各接口的 IP 地址。（配置过程略）

(2) 配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

(3) 配置 Device B

使能 NQA 服务器，配置监听的 IP 地址为 10.2.2.2，TCP 端口号为 9000。

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server tcp-connect 10.2.2.2 9000
```

(4) 配置 Device A

创建 TCP 类型的测试组（管理员为 admin，操作标签为 test1）。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type tcp
```

配置探测报文的目的地址为 10.2.2.2，目的端口号为 9000。

```
[DeviceA-nqa-admin-test1-tcp] destination ip 10.2.2.2
[DeviceA-nqa-admin-test1-tcp] destination port 9000
```

开启 NQA 测试组的历史记录保存功能。

```
[DeviceA-nqa-admin-test1-tcp] history-record enable
[DeviceA-nqa-admin-test1-tcp] quit
```

启动测试操作，并一直进行测试。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

测试执行一段时间后，停止 TCP 测试操作。

```
[DeviceA] undo nqa schedule admin test1
```

4. 验证配置

显示 TCP 测试中最后一次测试的当前结果。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 13/13/13
    Square-Sum of round trip time: 169
    Last succeeded probe time: 2011-11-22 10:27:25.1
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

显示 TCP 测试的历史记录。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          13           Succeeded        2011-11-22 10:27:25.1
```

以上显示信息表示，Device A 可以与 Device B 的端口 9000 建立 TCP 连接，建立连接所需的时间为 13 毫秒。

1.7.11 UDP-echo 测试配置举例

1. 组网需求

使用 NQA 的 UDP-echo 测试功能，测试本端（Device A）和指定目的端（Device B）的端口 8000 之间 UDP 协议报文的往返时间。

2. 组网图

图1-12 UDP-echo 测试组网图

3. 配置步骤

(1) 配置各接口的 IP 地址。（配置过程略）

(2) 配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

(3) 配置 Device B

使能 NQA 服务器，配置监听的 IP 地址为 10.2.2.2，UDP 端口号为 8000。

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server udp-echo 10.2.2.2 8000
```

(4) 配置 Device A

创建 UDP-echo 类型的测试组（管理员为 admin，操作标签为 test1）。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type udp-echo
```

配置探测报文的目的地址为 10.2.2.2，目的端口号为 8000。

```
[DeviceA-nqa-admin-test1-udp-echo] destination ip 10.2.2.2
[DeviceA-nqa-admin-test1-udp-echo] destination port 8000
```

开启 NQA 测试组的历史记录保存功能。

```
[DeviceA-nqa-admin-test1-udp-echo] history-record enable
[DeviceA-nqa-admin-test1-udp-echo] quit
```

启动测试操作，并一直进行测试。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

测试执行一段时间后，停止 UDP-echo 测试操作。

```
[DeviceA] undo nqa schedule admin test1
```

4. 验证配置

显示 UDP-echo 测试中最后一次测试的当前结果。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 25/25/25
    Square-Sum of round trip time: 625
    Last succeeded probe time: 2011-11-22 10:36:17.9
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
```

```
    Failures due to internal error: 0
    Failures due to other errors: 0
```

显示 UDP-echo 测试的历史记录。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          25           Succeeded        2011-11-22 10:36:17.9
```

以上显示信息表示，Device A 和 Device B 的端口 8000 之间 UDP 协议报文的往返时间为 25 毫秒。

1.7.12 UDP-tracert 测试配置举例

1. 组网需求

使用 NQA 的 UDP-tracert 测试功能，探测本端（Device A）到指定目的端（Device B）之间经过的路径信息。

2. 组网图

图1-13 UDP-tracert 测试组网图

3. 配置步骤

(1) 配置各接口的 IP 地址。（配置过程略）

(2) 配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

(3) 在中间设备上配置 **ip ttl-expires enable** 命令，在 Device B 上配置 **ip unreachables enable** 命令。

(4) 配置 Device A

创建 UDP-tracert 类型的测试组（管理员为 admin，操作标签为 test1）。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type udp-tracert
```

配置测试操作的目的地址为 10.2.2.2，目的端口号为 33434。（目的端口号为 33434 是缺省操作方式，因此，可以不执行本配置）

```
[DeviceA-nqa-admin-test1-udp-tracert] destination ip 10.2.2.2
[DeviceA-nqa-admin-test1-udp-tracert] destination port 33434
```

配置可选参数：对一个 TTL 值的节点的探测次数为 3（探测次数为 3 是缺省操作方式，因此，可以不执行本配置），探测的超时时间为 500 毫秒，测试组连续两次测试开始时间的时间间隔为 5000 毫秒。

```
[DeviceA-nqa-admin-test1-udp-tracert] probe count 3
[DeviceA-nqa-admin-test1-udp-tracert] probe timeout 500
[DeviceA-nqa-admin-test1-udp-tracert] frequency 5000
```

配置 UDP-tracert 测试的出接口为 GigabitEthernet1/0/1。

```
[DeviceA-nqa-admin-test1-udp-tracert] out interface gigabitethernet 1/0/1
```

开启 UDP-tracert 测试的禁止报文分片功能。

```
[DeviceA-nqa-admin-test1-udp-tracert] no-fragment enable
```

配置最大连续失败次数为 6 次，配置初始 TTL 为 1

```
[DeviceA-nqa-admin-test1-udp-tracert] max-failure 6
[DeviceA-nqa-admin-test1-udp-tracert] init-ttl 1
```

启动测试操作，并一直进行测试。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

测试执行一段时间后，停止 UDP-tracert 测试操作。

```
[DeviceA] undo nqa schedule admin test1
```

4. 验证配置

显示 UDP-tracert 测试中最后一次测试的当前结果。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 6              Receive response times: 6
    Min/Max/Average round trip time: 1/1/1
    Square-Sum of round trip time: 1
    Last succeeded probe time: 2013-09-09 14:46:06.2
  Extended results:
    Packet loss in test: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
Failures due to other errors: 0
  UDP-tracert results:
    TTL    Hop IP             Time
    1      3.1.1.1            2013-09-09 14:46:03.2
    2      10.2.2.2           2013-09-09 14:46:06.2
```

显示 UDP-tracert 测试的历史记录。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
Index      TTL  Response  Hop IP           Status          Time
1          2    2         10.2.2.2         Succeeded       2013-09-09 14:46:06.2
1          2    1         10.2.2.2         Succeeded       2013-09-09 14:46:05.2
1          2    2         10.2.2.2         Succeeded       2013-09-09 14:46:04.2
1          1    1         3.1.1.1          Succeeded       2013-09-09 14:46:03.2
1          1    2         3.1.1.1          Succeeded       2013-09-09 14:46:02.2
1          1    1         3.1.1.1          Succeeded       2013-09-09 14:46:01.2
```

1.7.13 Voice 测试配置举例

1. 组网需求

使用 NQA 的 Voice 测试功能，测试本端（Device A）和指定的目的端（Device B）之间传送语音报文的抖动时间和网络语音质量参数。

2. 组网图

图1-14 Voice 测试组网图

3. 配置步骤

(1) 配置各接口的 IP 地址。（配置过程略）

(2) 配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

(3) 配置 Device B

使能 NQA 服务器，配置监听的 IP 地址为 10.2.2.2，UDP 端口号为 9000。

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server udp-echo 10.2.2.2 9000
```

(4) 配置 Device A

创建 Voice 类型的 NQA 测试组（管理员为 admin，操作标签为 test1）。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type voice
```

配置探测报文的目的地址为 10.2.2.2，目的端口号为 9000。

```
[DeviceA-nqa-admin-test1-voice] destination ip 10.2.2.2
[DeviceA-nqa-admin-test1-voice] destination port 9000
[DeviceA-nqa-admin-test1-voice] quit
```

启动 Voice 测试操作，并一直进行测试。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

测试执行一段时间后，停止 Voice 测试操作。

```
[DeviceA] undo nqa schedule admin test1
```

4. 验证配置

显示 Voice 测试中最后一次测试的当前结果。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1000          Receive response times: 1000
    Min/Max/Average round trip time: 31/1328/33
    Square-Sum of round trip time: 2844813
    Last packet received time: 2011-06-13 09:49:31.1
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
Packets out of sequence: 0
    Packets arrived late: 0
  Voice results:
   RTT number: 1000
    Min positive SD: 1                  Min positive DS: 1
    Max positive SD: 204                Max positive DS: 1297
    Positive SD number: 257             Positive DS number: 259
    Positive SD sum: 759                Positive DS sum: 1797
    Positive SD average: 2              Positive DS average: 6
    Positive SD square-sum: 54127       Positive DS square-sum: 1691967
    Min negative SD: 1                  Min negative DS: 1
    Max negative SD: 203                Max negative DS: 1297
    Negative SD number: 255             Negative DS number: 259
    Negative SD sum: 759                Negative DS sum: 1796
    Negative SD average: 2              Negative DS average: 6
    Negative SD square-sum: 53655       Negative DS square-sum: 1691776
    SD average: 2                       DS average: 6
  One way results:
    Max SD delay: 343                   Max DS delay: 985
```

```
    Min SD delay: 343                     Min DS delay: 985
    Number of SD delay: 1                 Number of DS delay: 1
    Sum of SD delay: 343                  Sum of DS delay: 985
    Square-Sum of SD delay: 117649        Square-Sum of DS delay: 970225
    SD lost packets: 0                  DS lost packets: 0
    Lost packets for unknown reason: 0
  Voice scores:
    MOS value: 4.38                       ICPIF value: 0
```

显示 Voice 测试的统计结果。

```
[DeviceA] display nqa statistics admin test1
NQA entry (admin admin, tag test1) test statistics:
  NO. : 1

    Start time: 2011-06-13 09:45:37.8
    Life time: 331 seconds
    Send operation times: 4000          Receive response times: 4000
    Min/Max/Average round trip time: 15/1328/32
    Square-Sum of round trip time: 7160528
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
Packets out of sequence: 0
    Packets arrived late: 0
  Voice results:
   RTT number: 4000
    Min positive SD: 1                    Min positive DS: 1
    Max positive SD: 360                  Max positive DS: 1297
    Positive SD number: 1030              Positive DS number: 1024
    Positive SD sum: 4363                 Positive DS sum: 5423
    Positive SD average: 4                Positive DS average: 5
    Positive SD square-sum: 497725        Positive DS square-sum: 2254957
    Min negative SD: 1                    Min negative DS: 1
    Max negative SD: 360                  Max negative DS: 1297
    Negative SD number: 1028              Negative DS number: 1022
    Negative SD sum: 1028                 Negative DS sum: 1022
    Negative SD average: 4                Negative DS average: 5
    Negative SD square-sum: 495901        Negative DS square-sum: 5419
    SD average: 2                         DS average: 3
  One way results:
    Max SD delay: 359                     Max DS delay: 985
    Min SD delay: 0                       Min DS delay: 0
    Number of SD delay: 4                 Number of DS delay: 4
    Sum of SD delay: 1390                 Sum of DS delay: 1079
    Square-Sum of SD delay: 483202        Square-Sum of DS delay: 973651
    SD lost packets: 0                  DS lost packets: 0
    Lost packets for unknown reason: 0
  Voice scores:
    Max MOS value: 4.38                   Min MOS value: 4.38
    Max ICPIF value: 0                    Min ICPIF value: 0
```

1.7.14 DLSw 测试配置举例

1. 组网需求

使用 NQA 的 DLSw 测试功能，测试 DLSw 设备的响应时间。

2. 组网图

图1-15 DLSw 测试组网图

3. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

创建 DLSw 类型的测试组（管理员为 admin，操作标签为 test1），并配置探测报文的目的地址为 10.2.2.2。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type dlsw
[DeviceA-nqa-admin-test1-dlsw] destination ip 10.2.2.2
```

开启 NQA 测试组的历史记录保存功能。

```
[DeviceA-nqa-admin-test1-dlsw] history-record enable
[DeviceA-nqa-admin-test1-dlsw] quit
```

启动测试操作，并一直进行测试。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

测试执行一段时间后，停止 DLSw 测试操作。

```
[DeviceA] undo nqa schedule admin test1
```

4. 验证配置

显示 DLSw 测试中最后一次测试的当前结果。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 19/19/19
    Square-Sum of round trip time: 361
    Last succeeded probe time: 2011-11-22 10:40:27.7
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

显示 DLSw 测试的历史记录。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          19           Succeeded        2011-11-22 10:40:27.7
```

以上显示信息表示，DLSw 设备的响应时间为 19 毫秒。

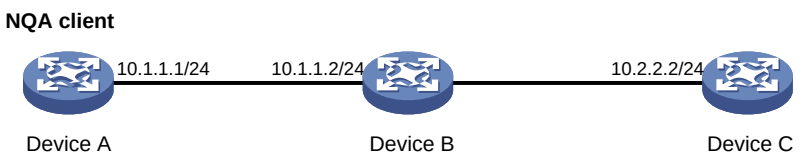
1.7.15 Path-jitter 测试配置举例

1. 组网需求

使用 NQA 的 Path-jitter 测试功能，测试本端（Device A）到指定目的端（Device C）间的网络质量情况。

2. 组网图

图1-16 Path-jitter 测试组网图



3. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

在 Device B 上配置 **ip ttl-expires enable** 命令，在设备 C 上配置 **ip unreachables enable** 命令。

创建 Path-jitter 类型的 NQA 测试组（管理员为 admin，操作标签为 test1），并配置探测报文的目的地址为 10.2.2.2。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type path-jitter
[DeviceA-nqa-admin-test1-path-jitter] destination ip 10.2.2.2
```

配置可选参数：测试组连续两次测试开始时间的时间间隔为 10000 毫秒。

```
[DeviceA-nqa-admin-test1-path-jitter] frequency 10000
[DeviceA-nqa-admin-test1-path-jitter] quit
```

启动 Path-jitter 测试操作，并一直进行测试。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

测试执行一段时间后，停止 Path-jitter 测试操作。

```
[DeviceA] undo nqa schedule admin test1
```

4. 验证配置

显示 Path-jitter 测试中最后一次测试的当前结果。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
  Hop IP 10.1.1.2
    Basic Results
      Send operation times: 10             Receive response times: 10
      Min/Max/Average round trip time: 9/21/14
      Square-Sum of round trip time: 2419
    Extended Results
      Failures due to timeout: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packets out of sequence: 0
      Packets arrived late: 0
    Path-Jitter Results
      Jitter number: 9
```

```
      Min/Max/Average jitter: 1/10/4
    Positive jitter number: 6
      Min/Max/Average positive jitter: 1/9/4
      Sum/Square-Sum positive jitter: 25/173
    Negative jitter number: 3
      Min/Max/Average negative jitter: 2/10/6
      Sum/Square-Sum positive jitter: 19/153

Hop IP 10.2.2.2
  Basic Results
    Send operation times: 10             Receive response times: 10
    Min/Max/Average round trip time: 15/40/28
    Square-Sum of round trip time: 4493
  Extended Results
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  Path-Jitter Results
    Jitter number: 9
      Min/Max/Average jitter: 1/10/4
    Positive jitter number: 6
      Min/Max/Average positive jitter: 1/9/4
      Sum/Square-Sum positive jitter: 25/173
    Negative jitter number: 3
      Min/Max/Average negative jitter: 2/10/6
      Sum/Square-Sum positive jitter: 19/153
```

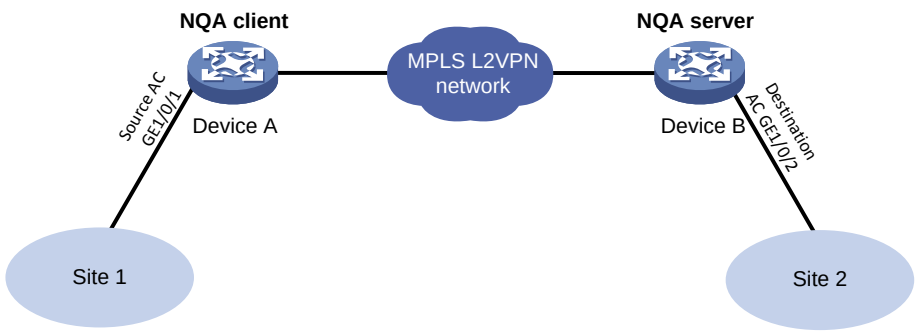
1.7.16 路径服务质量测试配置举例

1. 组网需求

使用 NQA 的 Frame-loss/Throughput/Latency 测试功能，测试本端（Device A）到指定目的端（Device B）间的网络质量。Frame-loss/Throughput/Latency 三个测试配置相似，本举例以 MPLS L2VPN 网络中进行 Throughput 测试为例。

2. 组网图

图1-17 路径服务质量测试组网图



3. 配置步骤

完成 MPLS L2VPN 网络的搭建及相关配置。（配置过程略）

(1) 配置 Device B

开启 NQA 服务器路径服务质量测试的报文反射功能。

```
[DeviceB] nqa reflector 1 interface gigabitethernet 1/0/2 service-instance 1 destination-mac 2-2-2 source-mac 1-1-1
```

开启 NQA 服务器功能。

```
[DeviceB] nqa server enable
```

(2) 配置 Device A

创建 throughput 类型的 NQA 测试组（管理员为 admin，操作标签为 test1），并配置其地址及端口。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type throughput
[DeviceA-nqa-admin-test1-throughput] source mac 1-1-1
[DeviceA-nqa-admin-test1-throughput] destination mac 2-2-2
[DeviceA-nqa-admin-test1-throughput] source interface gigabitethernet 1/0/1 service-instance 1
```

配置探测报文的长度。

```
[DeviceA-nqa-admin-test1-throughput] frame-size 64 512 1024 1280
```

启动路径服务质量测试操作，并一直进行测试。

```
[DeviceA-nqa-admin-test1-throughput] start
```

测试执行一段时间后，停止路径服务质量测试操作。

```
[DeviceA-nqa-admin-test1-throughput] stop
[DeviceA-nqa-admin-test1-throughput] quit
```

4. 验证配置

显示路径服务质量测试的当前结果。

```
[DeviceA] display nqa result
NQA entry (admin admin, tag test1) test results:
  Basic results     :
    Initial speed(Kbps)    : 100000
    Speed granularity(Kbps): 1000
    Probe duration(s)      : 60
    Probe interval(s)      : 4
    Allowed-loss-ratio     : 1/10000

  Throughput results:
    Frame size(Byte): 64
      Current speed(Kbps): -
      Frame-loss(Loss/Tx): -
      Status             : Failed
      Time               : 2015-03-17 07:20:40.8
    Frame size(Byte): 512
      Current speed(Kbps): 4000
      Frame-loss(Loss/Tx): 0/10000
      Status             : Succeeded
      Time               : 2015-03-17 07:21:40.8
    Frame size(Byte): 1024
      Current speed(Kbps): 8000
      Frame-loss(Loss/Tx): 0/10000
      Status             : Succeeded
```

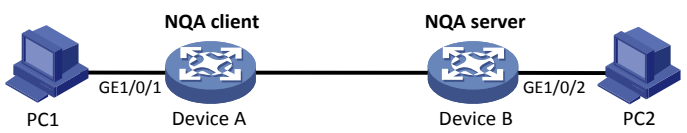
```
  Time               : 2015-03-17 07:22:52.8
Frame size(Byte): 1280
  Current speed(Kbps): 10000
  Frame-loss(Loss/Tx): 0/10000
  Status             : Succeeded
  Time               : 2015-03-17 07:23:45.8
Frame size(Byte): 1518
  Current speed(Kbps): 10000
  Frame-loss(Loss/Tx): 0/10000
  Status             : Succeeded
  Time               : 2015-03-17 07:24:45.8
```

1.7.17 Y.1564 测试普通二层以太网场景配置举例

1. 组网需求

在普通二层以太网环境下，PC1 和 PC2 通过接入二层网络进行互联。使用 NQA 的 Y.1564 测试功能，测试 PC 的二层接入网络本端（Device A）到指定目的端（Device B）间的网络质量。

2. 组网图



3. 配置步骤

(1) 配置 Device B

配置 NQA 服务器 Y.1564 测试的报文反射参数。

```
<DeviceB> system-view
[DeviceB] nqa reflector 1 interface gigabitethernet 1/0/2 destination-port 20000 source-port 10000 destination-mac 2-2-2
source-mac 1-1-1 vlan 100
```

开启 NQA 服务器功能。

```
[DeviceB] nqa server enable
```

(2) 配置 Device A

创建 Y.1564 类型的 NQA 测试组（管理员为 admin，操作标签为 test1），并配置其地址及端口。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type y1564
[DeviceA-nqa-admin-test1-y1564] source port 10000
[DeviceA-nqa-admin-test1-y1564] destination port 20000
[DeviceA-nqa-admin-test1-y1564] source mac 1-1-1
[DeviceA-nqa-admin-test1-y1564] destination mac 2-2-2
[DeviceA-nqa-admin-test1-y1564] source interface gigabitethernet 1/0/1
```

配置 Y.1564 测试的基本参数。

```
[DeviceA-nqa-admin-test1-y1564] bandwidth cir 1000 pir 600
[DeviceA-nqa-admin-test1-y1564] allowed-jitter 1000
[DeviceA-nqa-admin-test1-y1564] allowed-frame-loss 1000
[DeviceA-nqa-admin-test1-y1564] allowed-transfer-delay 1000
```

开启流量监管测试。

```
[DeviceA-nqa-admin-test1-y1564] traffic-policing-test enable
```

配置 Y.1564 测试探测报文的 VLAN 标签。

```
[DeviceA-nqa-admin-test1-y1564] vlan 100
```

启动 Y.1564 测试操作，测试持续时间与配置的测试项目以及每个项目的时间有关。

```
[DeviceA-nqa-admin-test1-y1564] start
[DeviceA-nqa-admin-test1-y1564] quit
```

4. 验证配置

显示 Y.1564 测试的当前结果。

```
[DeviceA] display nqa result
NQA entry (admin admin, tag test1) test results:
  Status                    : Succeeded
  Last test                 : Service performance test
  Estimated total time (s)  : 909
  Actual test time used (s) : 909
  Detailed test results:
    CIR test (with the step of 1):
      Start time               : 2018-11-03 11:51:38.1
      End time                 : 2018-11-03 11:51:41.3
      Status                   : Succeeded
      Min/Max/Average IR (kbps) : 998/1002/1000
      Min/Max/Average FTD (us)  : 232/236/234
      Min/Max/Average FDV (us)  : 32/36/34
      FL count/FLR              : 2/0.002%
      Packets out of order      : 0
      Severely Err Secs/AVAIL   : 0/100.000%
    PIR test (color-blind):
      Start time               : 2018-11-03 11:51:41.1
      End time                 : 2018-11-03 11:51:44.3
      Status                   : Succeeded
      Min/Max/Average IR (kbps) : 1598/1602/1600
      Min/Max/Average FTD (us)  : 373/377/375
      Min/Max/Average FDV (us)  : 73/77/75
      FL count/FLR              : 2/0.002%
      Packets out of order      : 0
      Severely Err Secs/AVAIL   : 0/100.000%
    Traffic policing test (color-blind):
      Start time               : 2018-11-03 11:51:44.3
      End time                 : 2018-11-03 11:51:47.5
      Status                   : Succeeded
      Min/Max/Average IR (kbps) : 1310/1314/1312
      Min/Max/Average FTD (us)  : 409/413/411
      Min/Max/Average FDV (us)  : 9/13/11
      FL count/FLR              : 5/0.005%
      Packets out of order      : 0
      Severely Err Secs/AVAIL   : 0/100.000%
    Service performance test:
      Start time               : 2018-11-03 11:51:47.5
      End time                 : 2018-11-03 12:06:47.7
      Status                   : Succeeded
      Min/Max/Average IR (kbps) : 998/1002/1000
```

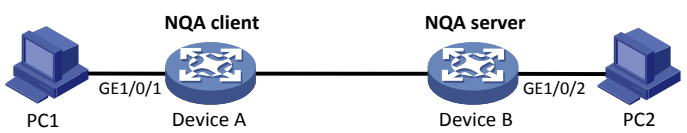
```
Min/Max/Average FTD (us)  : 232/236/234
Min/Max/Average FDV (us)  : 32/36/34
FL count/FLR              : 2/0.002%
Packets out of order      : 0
Severely Err Secs/AVAIL   : 0/100.000%
```

1.7.18 Y.1564 测试普通三层以太网场景配置举例

1. 组网需求

在普通三层以太网环境下，PC1 和 PC2 通过接入三层网络进行互联。使用 NQA 的 Y.1564 测试功能，测试 PC 的三层接入网络本端（Device A）到指定目的端（Device B）间的网络质量。

2. 组网图



3. 配置步骤

(1) 配置各接口的 IP 地址。（配置过程略）

(2) 配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

(3) 配置 Device B

配置 NQA 服务器 Y.1564 测试的报文反射参数。

```
<DeviceB> system-view
[DeviceB] nqa reflector 1 interface gigabitethernet 1/0/2 ip destination 10.2.2.2 source 10.1.1.1 destination-port 20000 source-port 10000
```

开启 NQA 服务器功能。

```
[DeviceB] nqa server enable
```

(4) 配置 Device A

创建 Y.1564 类型的 NQA 测试组（管理员为 admin，操作标签为 test1），并配置其地址及端口。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type y1564
[DeviceA-nqa-admin-test1-y1564] source ip 10.1.1.1
[DeviceA-nqa-admin-test1-y1564] destination ip 10.2.2.2
[DeviceA-nqa-admin-test1-y1564] source port 10000
[DeviceA-nqa-admin-test1-y1564] destination port 20000
[DeviceA-nqa-admin-test1-y1564] source interface gigabitethernet 1/0/1
```

配置 Y.1564 测试的基本参数。

```
[DeviceA-nqa-admin-test1-y1564] bandwidth cir 10000 pir 1000
[DeviceA-nqa-admin-test1-y1564] allowed-jitter 1000
[DeviceA-nqa-admin-test1-y1564] allowed-frame-loss 20
[DeviceA-nqa-admin-test1-y1564] allowed-transfer-delay 10000
```

开启流量监管测试。

```
[DeviceA-nqa-admin-test1-y1564] traffic-policing-test enable
```

启动 Y.1564 测试操作，测试持续时间与配置的测试项目以及每个项目的时间有关。

```
[DeviceA-nqa-admin-test1-y1564] start
```

```
    [DeviceA-nqa-admin-test1-y1564] quit
```

4. 验证配置

显示 Y.1564 测试的当前结果。

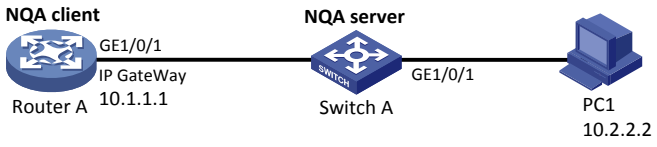
```
[DeviceA] display nqa result
NQA entry (admin admin, tag test1) test results:
  Status                    : In progress
  Last test                 : Traffic policing test
  Estimated total time (s)  : 909
  Actual test time used (s) : 24
  Detailed test results:
    CIR test (with the step of 1):
      Start time                : 2018-11-03 13:39:10.3
      End time                  : 2018-11-03 13:39:13.5
      Status                    : Succeeded
      Min/Max/Average IR (kbps) : 9998/10002/10000
      Min/Max/Average FTD (us)  : 347/351/349
      Min/Max/Average FDV (us)  : 47/51/49
      FL count/FLR              : 2/0.002%
      Packets out of order      : 0
      Severely Err Secs/AVAIL   : 0/100.000%
    PIR test (color-blind):
      Start time                : 2018-11-03 13:39:13.5
      End time                  : 2018-11-03 13:39:16.7
      Status                    : Succeeded
      Min/Max/Average IR (kbps) : 10998/11002/11000
      Min/Max/Average FTD (us)  : 582/586/584
      Min/Max/Average FDV (us)  : 82/86/84
      FL count/FLR              : 2/0.002%0
      Packets out of order      : 0
      Severely Err Secs/AVAIL   : 0/100.000%
  Traffic policing test (color-blind):
    Start time                : 2018-11-03 13:39:16.7
    End time                  : 2018-11-03 13:39:19.9
    Status                    : Succeeded
    Min/Max/Average IR (kbps) : 10123/10127/10125
    Min/Max/Average FTD (us)  : 169/173/171
    Min/Max/Average FDV (us)  : 69/73/71
    FL count/FLR              : 6/0.006%
    Packets out of order      : 0
    Severely Err Secs/AVAIL   : 0/100.000%
```

1.7.19 Y.1564 测试普通以太网三层网关场景配置举例（路由应用）

1. 组网需求

在普通以太网三层网关环境下，PC1 通过交换机 Switch A 连接到网关 Router A。使用 NQA 的 Y.1564 测试功能，测试网关路径本端（Router A）到指定目的端（Switch A）间的网络质量。

2. 组网图



3. 配置步骤

(1) 配置各接口的 IP 地址。（配置过程略）

(2) 配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

(3) 配置 Switch A

配置 NQA 服务器 Y.1564 测试的报文反射参数。

```
<SwitchA> system-view
[SwitchA] nqa reflector 1 interface gigabitethernet 1/0/1 ip destination 10.2.2.2 source 10.1.1.1 destination-port 20000
source-port 10000
```

开启 NQA 服务器功能。

```
[SwitchA] nqa server enable
```

(4) 配置 Router A

创建 Y.1564 类型的 NQA 测试组（管理员为 admin，操作标签为 test1），并配置其地址及端口。

```
<RouterA> system-view
[RouterA] nqa entry admin test1
[RouterA-nqa-admin-test1] type y1564
```

配置源 IP 为网关口 IP。

```
[RouterA-nqa-admin-test1-y1564] source ip 10.1.1.1
```

配置目的 IP 为用户 IP。

```
[RouterA-nqa-admin-test1-y1564] destination ip 10.2.2.2
```

配置源端口和目的端口。

```
[RouterA-nqa-admin-test1-y1564] source port 10000
[RouterA-nqa-admin-test1-y1564] destination port 20000
```

配置报文出接口。

```
[RouterA-nqa-admin-test1-y1564] out interface gigabitethernet 1/0/1
```

配置 Y.1564 测试的基本参数。

```
[RouterA-nqa-admin-test1-y1564] bandwidth cir 100 pir 10000
[RouterA-nqa-admin-test1-y1564] allowed-jitter 1000
[RouterA-nqa-admin-test1-y1564] allowed-frame-loss 1000
[RouterA-nqa-admin-test1-y1564] allowed-transfer-delay 1000
```

开启流量监管测试。

```
[RouterA-nqa-admin-test1-y1564] traffic-policing-test enable
```

启动 Y.1564 测试操作，测试持续时间与配置的测试项目以及每个项目的时间有关。

```
[RouterA-nqa-admin-test1-y1564] start
[RouterA-nqa-admin-test1-y1564] quit
```

4. 验证配置

显示 Y.1564 测试的当前结果。

```
[RouterA] display nqa result
NQA entry (admin admin, tag test1) test results:
  Status                    : In progress
```

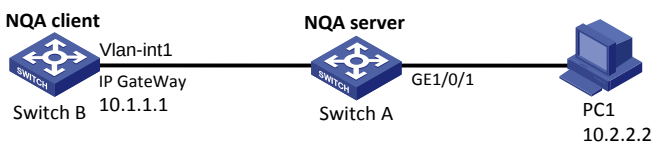
```
Last test                 : Traffic policing test
Estimated total time (s)  : 909
Actual test time used (s) : 24
Detailed test results:
  CIR test (with the step of 1):
    Start time               : 2018-11-03 13:44:16.1
    End time                 : 2018-11-03 13:44:19.3
    Status                   : Succeeded
    Min/Max/Average IR (kbps) : 97/103/100
    Min/Max/Average FTD (us)  : 22/28/23
    Min/Max/Average FDV (us)  : 23/29/25
    FL count/FLR             : 6/0.006%
    Packets out of order     : 0
    Severely Err Secs/AVAIL   : 0/100.000%
  PIR test (color-blind):
    Start time               : 2018-11-03 13:44:19.3
    End time                 : 2018-11-03 13:44:22.5
    Status                   : Succeeded
    Min/Max/Average IR (kbps) : 10098/10102/10100
    Min/Max/Average FTD (us)  : 371/375/373
    Min/Max/Average FDV (us)  : 71/75/73
    FL count/FLR             : 7/0.007%
    Packets out of order     : 0
    Severely Err Secs/AVAIL   : 0/100.000%
  Traffic policing test (color-blind):
    Start time               : 2018-11-03 13:44:22.5
    End time                 : 2018-11-03 13:44:25.7
    Status                   : Succeeded
    Min/Max/Average IR (kbps) : 9455/9458/9456
    Min/Max/Average FTD (us)  : 958/972/960
    Min/Max/Average FDV (us)  : 78/79/78
    FL count/FLR             : 11/0.01%
    Packets out of order     : 0
    Severely Err Secs/AVAIL   : 0/100.000%
```

1.7.20 Y.1564 测试普通以太网三层网关场景配置举例（交换应用）

1. 组网需求

在普通以太网三层网关环境下，PC1 通过交换机 Switch A 连接到网关 Switch B。使用 NQA 的 Y.1564 测试功能，测试网关路径本端（Switch B）到指定目的端（Switch A）间的网络质量。

2. 组网图



3. 配置步骤

(1) 配置各接口的 IP 地址。（配置过程略）

(2) 配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

(3) 配置 Switch A

配置 NQA 服务器 Y.1564 测试的报文反射参数。

```
<SwitchA> system-view
[SwitchA] nqa reflector 1 interface gigabitethernet 1/0/1 ip destination 10.2.2.2 source 10.1.1.1 destination-port 20000
source-port 10000
```

开启 NQA 服务器功能。

```
[SwitchA] nqa server enable
```

(4) 配置 Switch B

创建 Y.1564 类型的 NQA 测试组（管理员为 admin，操作标签为 test1），并配置其地址及端口。

```
<SwitchB> system-view
[SwitchB] nqa entry admin test1
[SwitchB-nqa-admin-test1] type y1564
```

配置源 IP 为网关口 IP。

```
[SwitchB-nqa-admin-test1-y1564] source ip 10.1.1.1
```

配置目的 IP 为用户 IP。

```
[SwitchB-nqa-admin-test1-y1564] destination ip 10.2.2.2
```

配置源端口和目的端口。

```
[SwitchB-nqa-admin-test1-y1564] source port 10000
[SwitchB-nqa-admin-test1-y1564] destination port 20000
```

配置报文出接口。

```
[SwitchB-nqa-admin-test1-y1564] out interface vlan-interface 1
```

配置 Y.1564 测试的基本参数。

```
[SwitchB-nqa-admin-test1-y1564] bandwidth cir 100 pir 10000
[SwitchB-nqa-admin-test1-y1564] allowed-jitter 1000
[SwitchB-nqa-admin-test1-y1564] allowed-frame-loss 1000
[SwitchB-nqa-admin-test1-y1564] allowed-transfer-delay 1000
```

开启流量监管测试。

```
[SwitchB-nqa-admin-test1-y1564] traffic-policing-test enable
```

启动 Y.1564 测试操作，测试持续时间与配置的测试项目以及每个项目的时间有关。

```
[SwitchB-nqa-admin-test1-y1564] start
[SwitchB-nqa-admin-test1-y1564] quit
```

4. 验证配置

显示 Y.1564 测试的当前结果。

```
[SwitchB] display nqa result
NQA entry (admin admin, tag test1) test results:
  Status                    : In progress
  Last test                 : Traffic policing test
  Estimated total time (s)  : 909
  Actual test time used (s) : 24
  Detailed test results:
    CIR test (with the step of 1):
      Start time               : 2018-11-03 13:44:16.1
      End time                 : 2018-11-03 13:44:19.3
      Status                   : Succeeded
      Min/Max/Average IR (kbps) : 97/103/100
      Min/Max/Average FTD (us)  : 22/28/23
```

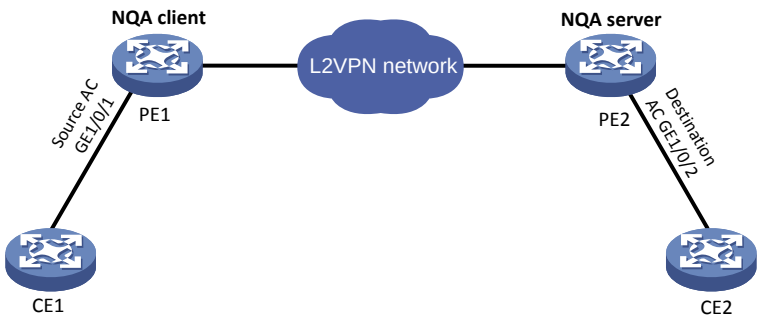
```
  Min/Max/Average FDV (us)  : 23/29/25
  FL count/FLR              : 6/0.006%
  Packets out of order      : 0
  Severely Err Secs/AVAIL   : 0/100.000%
PIR test (color-blind):
  Start time                : 2018-11-03 13:44:19.3
  End time                  : 2018-11-03 13:44:22.5
  Status                    : Succeeded
  Min/Max/Average IR (kbps) : 10098/10102/10100
  Min/Max/Average FTD (us)  : 371/375/373
  Min/Max/Average FDV (us)  : 71/75/73
  FL count/FLR              : 7/0.007%
  Packets out of order      : 0
  Severely Err Secs/AVAIL   : 0/100.000%
Traffic policing test (color-blind):
  Start time                : 2018-11-03 13:44:22.5
  End time                  : 2018-11-03 13:44:25.7
  Status                    : Succeeded
  Min/Max/Average IR (kbps) : 9455/9458/9456
  Min/Max/Average FTD (us)  : 958/972/960
  Min/Max/Average FDV (us)  : 78/79/78
  FL count/FLR              : 11/0.01%
  Packets out of order      : 0
  Severely Err Secs/AVAIL   : 0/100.000%
```

1.7.21 Y.1564 测试 L2VPN 场景配置举例

1. 组网场景

在 L2VPN 环境下，CE1 和 CE2 通过二层 VPN 网络进行互联。使用 NQA 的 Y.1564 测试功能，测试二层 VPN 网络本端（PE1）到指定目的端（PE2）间的网络质量。

2. 组网图



3. 配置步骤

(1) L2VPN 组网的基本配置过程略。

(2) 配置 PE2

配置 NQA 服务器 Y.1564 测试的报文反射参数。

```
<PE2> system-view
[PE2] nqa reflector 1 interface gigabitethernet 1/0/2 service-instance 100 destination-port 20000 source-port 10000
destination-mac 2-2-2 source-mac 1-1-1
```

开启 NQA 服务器功能。

```
[PE2] nqa server enable
```

(3) 配置 PE1

创建 Y.1564 类型的 NQA 测试组（管理员为 admin，操作标签为 test1），并配置其地址及端口。

```
<PE1> system-view
[PE1] nqa entry admin test1
[PE1-nqa-admin-test1] type y1564
[PE1-nqa-admin-test1-y1564] source port 10000
[PE1-nqa-admin-test1-y1564] destination port 20000
[PE1-nqa-admin-test1-y1564] source mac 1-1-1
[PE1-nqa-admin-test1-y1564] destination mac 2-2-2
[PE1-nqa-admin-test1-y1564] source interface gigabitethernet 1/0/1 service-instance 100
```

配置 Y.1564 测试的基本参数。

```
[PE1-nqa-admin-test1-y1564] bandwidth cir 1000 pir 10
[PE1-nqa-admin-test1-y1564] allowed-jitter 1000
[PE1-nqa-admin-test1-y1564] allowed-frame-loss 10
[PE1-nqa-admin-test1-y1564] allowed-transfer-delay 1000
```

开启流量监管测试。

```
[PE1-nqa-admin-test1-y1564] traffic-policing-test enable
```

启动 Y.1564 测试操作，测试持续时间与配置的测试项目以及每个项目的时间有关。

```
[PE1-nqa-admin-test1-y1564] start
[PE1-nqa-admin-test1-y1564] quit
```

4. 验证配置

显示 Y.1564 测试的当前结果。

```
[PE1] display nqa result
NQA entry (admin 1, tag 1) test results:
  Status                    : Failed
  Last test                 : Traffic policing test
  Estimated total time (s)  : 909
  Actual test time used (s) : 9
  Detailed test results:
    CIR test (with the step of 1):
      Start time               : 2018-11-03 13:47:09.1
      End time                 : 2018-11-03 13:47:12.1
      Status                   : Succeeded
      Min/Max/Average IR (kbps) : 998/1002/1000
      Min/Max/Average FTD (us)  : 232/236/234
      Min/Max/Average FDV (us)  : 32/36/34
      FL count/FLR              : 2/0.002%
      Packets out of order      : 0
      Severely Err Secs/AVAIL   : 0/100.000%
    PIR test (color-blind):
      Start time               : 2018-11-03 13:47:12.1
      End time                 : 2018-11-03 13:47:15.1
      Status                   : Succeeded
      Min/Max/Average IR (kbps) : 1008/1012/1010
      Min/Max/Average FTD (us)  : 235/239/237
      Min/Max/Average FDV (us)  : 35/39/37
      FL count/FLR              : 2/0.002%
```

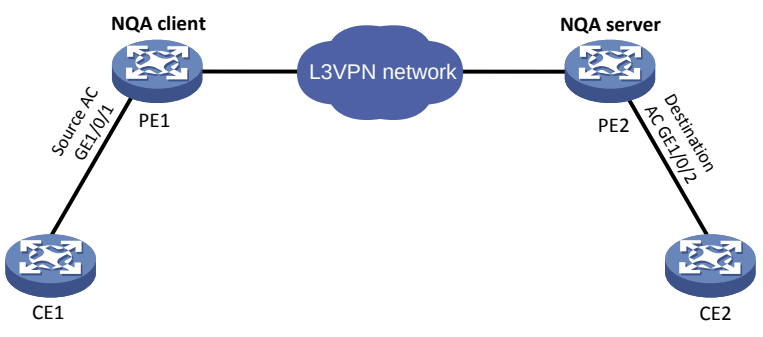
```
  Packets out of order      : 0
  Severely Err Secs/AVAIL   : 0/100.000%
Traffic policing test (color-blind):
  Start time                : 2018-11-03 13:47:15.1
  End time                  : 2018-11-03 13:47:18.1
  Status                    : Failed
  Min/Max/Average IR (kbps) : 943/947/945
  Min/Max/Average FTD (us)  : 294/298/296
  Min/Max/Average FDV (us)  : 94/98/96
  FL count/FLR              : 4/0.004%
  Packets out of order      : 0
  Severely Err Secs/AVAIL   : 0/100.000%
```

1.7.22 Y.1564 测试 L3VPN 场景配置举例

1. 组网需求

在 L3VPN 环境下，CE1 和 CE2 通过三层 VPN 网络进行互联。使用 NQA 的 Y.1564 测试功能，测试三层 VPN 网络本端（PE1）到指定目的端（PE2）间的网络质量。

2. 组网图



3. 配置步骤

(1) L3VPN 组网的基本配置过程略。

(2) 配置 PE2

配置 NQA 服务器 Y.1564 测试的报文反射参数。

```
<PE2> system-view
[PE2] nqa reflector 1 interface gigabitethernet 1/0/2 ip destination 10.2.2.2 source 10.1.1.1 destination-port 20000 source-port 10000 vpn-instance vpn1
```

开启 NQA 服务器功能。

```
[PE2] nqa server enable
```

(3) 配置 PE1

创建 Y.1564 类型的 NQA 测试组（管理员为 admin，操作标签为 test1），并配置其地址及端口。

```
<PE1> system-view
[PE1] nqa entry admin test1
[PE1-nqa-admin-test1] type y1564
[PE1-nqa-admin-test1-y1564] source ip 10.1.1.1
[PE1-nqa-admin-test1-y1564] destination ip 10.2.2.2
[PE1-nqa-admin-test1-y1564] source port 10000
[PE1-nqa-admin-test1-y1564] destination port 20000
[PE1-nqa-admin-test1-y1564] source interface gigabitethernet 1/0/1
```

配置 Y.1564 测试的基本参数。

```
[PE1-nqa-admin-test1-y1564] bandwidth cir 100 pir 10000
[PE1-nqa-admin-test1-y1564] allowed-jitter 1000
[PE1-nqa-admin-test1-y1564] allowed-frame-loss 1000
[PE1-nqa-admin-test1-y1564] allowed-transfer-delay 1000
```

开启流量监管测试。

```
[PE1-nqa-admin-test1-y1564] traffic-policing-test enable
```

启动 Y.1564 测试操作，测试持续时间与配置的测试项目以及每个项目的时间有关。

```
[PE1-nqa-admin-test1-y1564] start
[PE1-nqa-admin-test1-y1564] quit
```

4. 验证配置

显示 Y.1564 测试的当前结果。

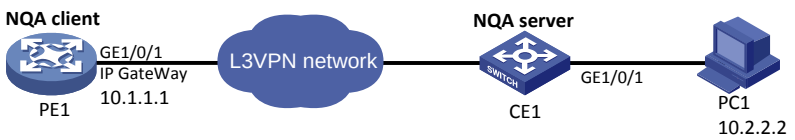
```
[PE1] display nqa result
NQA entry (admin admin, tag test1) test results:
  Status                    : In progress
  Last test                 : Traffic policing test
  Estimated total time (s)  : 909
  Actual test time used (s) : 24
  Detailed test results:
    CIR test (with the step of 1):
      Start time               : 2018-11-03 13:44:16.1
      End time                 : 2018-11-03 13:44:19.3
      Status                   : Succeeded
      Min/Max/Average IR (kbps) : 98/102/100
      Min/Max/Average FTD (us)  : 21/25/23
      Min/Max/Average FDV (us)  : 21/25/23
      FL count/FLR              : 2/0.002%
      Packets out of order      : 0
      Severely Err Secs/AVAIL   : 0/100.000%
    PIR test (color-blind):
      Start time               : 2018-11-03 13:44:19.3
      End time                 : 2018-11-03 13:44:22.5
      Status                   : Succeeded
      Min/Max/Average IR (kbps) : 10098/10102/10100
      Min/Max/Average FTD (us)  : 371/375/373
      Min/Max/Average FDV (us)  : 71/75/73
      FL count/FLR              : 7/0.007%
      Packets out of order      : 0
      Severely Err Secs/AVAIL   : 0/100.000%
    Traffic policing test (color-blind):
      Start time               : 2018-11-03 13:44:22.5
      End time                 : 2018-11-03 13:44:25.7
      Status                   : Succeeded
      Min/Max/Average IR (kbps) : 9448/9452/9450
      Min/Max/Average FTD (us)  : 958/962/960
      Min/Max/Average FDV (us)  : 58/62/60
      FL count/FLR              : 10/0.01%
      Packets out of order      : 0
      Severely Err Secs/AVAIL   : 0/100.000%
```

1.7.23 Y.1564 测试 L3VPN 网关场景配置举例

1. 组网需求

在 L3VPN 网关环境下，PC1 通过 CE1 接入三层 VPN 网关。使用 NQA 的 Y.1564 测试功能，测试三层 VPN 网关路径本端（PE1）到指定目的端（CE1）间的网络质量。

2. 组网图



3. 配置步骤

(1) L3VPN 组网的基本配置过程略。

(2) 配置 CE1

配置 NQA 服务器 Y.1564 测试的报文反射参数。

```
<CE1> system-view
[CE1] nqa reflector 1 interface gigabitethernet 1/0/1 ip destination 10.2.2.2 source 10.1.1.1 destination-port 20000 source-port 10000
```

开启 NQA 服务器功能。

```
[CE1] nqa server enable
```

(3) 配置 PE1

创建 Y.1564 类型的 NQA 测试组（管理员为 admin，操作标签为 test1），并配置其地址及端口。

```
<PE1> system-view
[PE1] nqa entry admin test1
[PE1-nqa-admin-test1] type y1564
```

配置源 IP 为网关口 IP。

```
[PE1-nqa-admin-test1-y1564] source ip 10.1.1.1
```

配置目的 IP 为用户 IP。

```
[PE1-nqa-admin-test1-y1564] destination ip 10.2.2.2
```

配置源端口和目的端口。

```
[PE1-nqa-admin-test1-y1564] source port 10000
[PE1-nqa-admin-test1-y1564] destination port 20000
```

配置报文出接口。

```
[PE1-nqa-admin-test1-y1564] out interface gigabitethernet 1/0/1
```

配置 Y.1564 测试的基本参数。

```
[PE1-nqa-admin-test1-y1564] bandwidth cir 100 pir 10000
[PE1-nqa-admin-test1-y1564] allowed-jitter 1000
[PE1-nqa-admin-test1-y1564] allowed-frame-loss 1000
[PE1-nqa-admin-test1-y1564] allowed-transfer-delay 1000
```

开启流量监管测试。

```
[PE1-nqa-admin-test1-y1564] traffic-policing-test enable
```

启动 Y.1564 测试操作，测试持续时间与配置的测试项目以及每个项目的时间有关。

```
[PE1-nqa-admin-test1-y1564] start
[PE1-nqa-admin-test1-y1564] quit
```

4. 验证配置

显示 Y.1564 测试的当前结果。

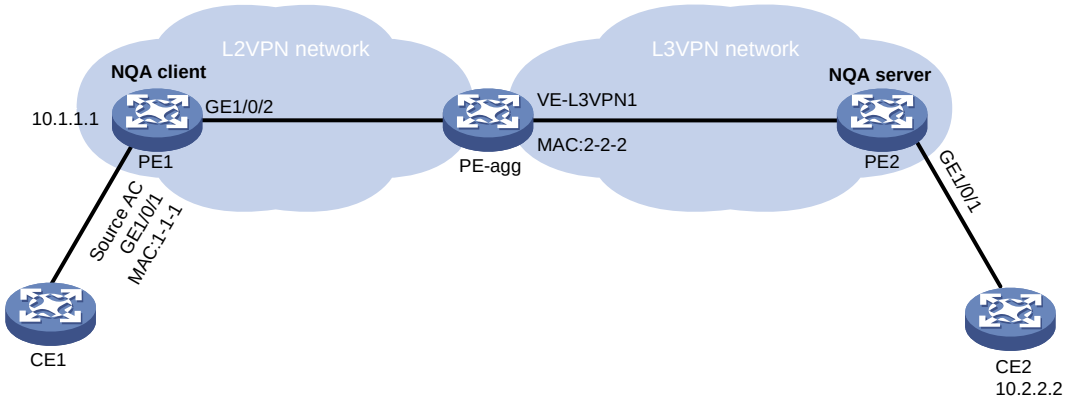
```
[PE1] display nqa result
NQA entry (admin admin, tag test1) test results:
  Status                    : In progress
  Last test                 : Traffic policing test
  Estimated total time (s)  : 909
  Actual test time used (s) : 24
  Detailed test results:
    CIR test (with the step of 1):
      Start time               : 2018-11-03 14:44:16.1
      End time                 : 2018-11-03 14:44:19.3
      Status                   : Succeeded
      Min/Max/Average IR (kbps) : 98/102/100
      Min/Max/Average FTD (us)  : 31/35/33
      Min/Max/Average FDV (us)  : 31/35/33
      FL count/FLR             : 5/0.005%
      Packets out of order     : 0
      Severely Err Secs/AVAIL   : 0/100.000%
    PIR test (color-blind):
      Start time               : 2018-11-03 14:44:19.3
      End time                 : 2018-11-03 14:44:22.5
      Status                   : Succeeded
      Min/Max/Average IR (kbps) : 10198/10202/10200
      Min/Max/Average FTD (us)  : 383/386/384
      Min/Max/Average FDV (us)  : 71/75/73
      FL count/FLR             : 7/0.007%
      Packets out of order     : 0
      Severely Err Secs/AVAIL   : 0/100.000%
  Traffic policing test (color-blind):
    Start time               : 2018-11-03 14:44:22.5
    End time                 : 2018-11-03 14:44:25.7
    Status                   : Succeeded
    Min/Max/Average IR (kbps) : 9563/9568/9566
    Min/Max/Average FTD (us)  : 876/985/980
    Min/Max/Average FDV (us)  : 58/62/60
    FL count/FLR             : 10/0.01%
    Packets out of order     : 0
    Severely Err Secs/AVAIL   : 0/100.000%
```

1.7.24 Y.1564 测试 L2VPN 接入 L3VPN 场景配置举例

1. 组网需求

在 L2VPN 接入 L3VPN 环境下，CE1 和 CE2 通过 L2VPN 接入 L3VPN 网络进行互联。使用 NQA 的 Y.1564 测试功能，测试 L2VPN 接入 L3VPN 网络本端（PE1）到指定目的端（PE2）间的网络质量。

2. 组网图



3. 配置步骤

(1) L2VPN、L3VPN 组网的基本配置过程略。

(2) 配置 PE2

配置 NQA 服务器 Y.1564 测试的报文反射参数。

```
<PE2> system-view
[PE2] nqa reflector 1 interface gigabitethernet 1/0/1 service-instance 100 ip destination 10.2.2.2 source 10.1.1.1
destination-port 20000 source-port 10000
```

开启 NQA 服务器功能。

```
[PE2] nqa server enable
```

(3) 配置 PE1

创建 Y.1564 类型的 NQA 测试组（管理员为 admin，操作标签为 test1），并配置其地址及端口。

```
<PE1> system-view
[PE1] nqa entry admin test1
[PE1-nqa-admin-test1] type y1564
[PE1-nqa-admin-test1-y1564] source ip 10.1.1.1
[PE1-nqa-admin-test1-y1564] destination ip 10.2.2.2
[PE1-nqa-admin-test1-y1564] source port 10000
[PE1-nqa-admin-test1-y1564] destination port 20000
```

配置源 MAC。

```
[PE1-nqa-admin-test1-y1564] source mac 1-1-1
```

配置目的 MAC 为 PE-agg 的 VE-L3VPN1 虚接口 MAC。

```
[PE1-nqa-admin-test1-y1564] destination mac 2-2-2
```

配置 AC 源接口。

```
[PE1-nqa-admin-test1-y1564] source interface gigabitethernet 1/0/1 service-instance 100
```

配置 Y.1564 测试的基本参数。

```
[PE1-nqa-admin-test1-y1564] bandwidth cir 100 pir 10000
[PE1-nqa-admin-test1-y1564] allowed-jitter 1000
[PE1-nqa-admin-test1-y1564] allowed-frame-loss 1000
[PE1-nqa-admin-test1-y1564] allowed-transfer-delay 1000
```

开启流量监管测试。

```
[PE1-nqa-admin-test1-y1564] traffic-policing-test enable
```

启动 Y.1564 测试操作，测试持续时间与配置的测试项目以及每个项目的时间有关。

```
[PE1-nqa-admin-test1-y1564] start
[PE1-nqa-admin-test1-y1564] quit
```

4. 验证配置

显示 Y.1564 测试的当前结果。

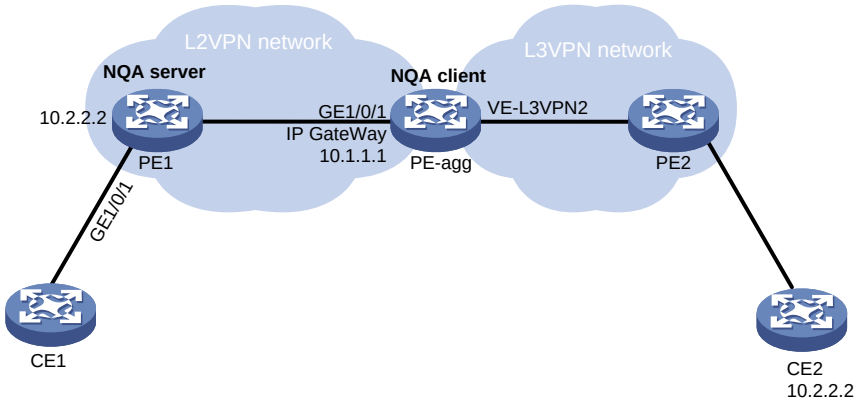
```
[PE1] display nqa result
NQA entry (admin admin, tag test1) test results:
  Status                    : In progress
  Last test                 : Traffic policing test
  Estimated total time (s)  : 909
  Actual test time used (s) : 24
  Detailed test results:
    CIR test (with the step of 1):
      Start time               : 2018-11-03 15:10:16.1
      End time                 : 2018-11-03 15:10:19.3
      Status                   : Succeeded
      Min/Max/Average IR (kbps) : 87/132/105
      Min/Max/Average FTD (us)  : 31/35/33
      Min/Max/Average FDV (us)  : 41/45/43
      FL count/FLR             : 3/0.003%
      Packets out of order     : 0
      Severely Err Secs/AVAIL   : 0/100.000%
    PIR test (color-blind):
      Start time               : 2018-11-03 15:10:19.3
      End time                 : 2018-11-03 15:10:22.5
      Status                   : Succeeded
      Min/Max/Average IR (kbps) : 10098/10102/10100
      Min/Max/Average FTD (us)  : 321/384/353
      Min/Max/Average FDV (us)  : 81/85/83
      FL count/FLR             : 7/0.007%
      Packets out of order     : 0
      Severely Err Secs/AVAIL   : 0/100.000%
  Traffic policing test (color-blind):
    Start time               : 2018-11-03 15:10:22.5
    End time                 : 2018-11-03 15:10:25.7
    Status                   : Succeeded
    Min/Max/Average IR (kbps) : 6338/7563/6980
    Min/Max/Average FTD (us)  : 945/987/960
    Min/Max/Average FDV (us)  : 58/62/60
    FL count/FLR             : 10/0.01%
    Packets out of order     : 0
    Severely Err Secs/AVAIL   : 0/100.000%
```

1.7.25 Y.1564 测试 L2VPN 接入 L3VPN 网关场景配置举例

1. 组网需求

在 L2VPN 接入 L3VPN 环境下，CE1 和 CE2 通过 L2VPN 接入 L3VPN 网络进行互联。使用 NQA 的 Y.1564 测试功能，测试 CE1 到 PE-agg 网关的网关路径本端（PE-agg）到指定目的端（PE1）间的网络质量。

2. 组网图



3. 配置步骤

(1) L2VPN、L3VPN 组网的基本配置过程略。

(2) 配置 PE1

配置 NQA 服务器 Y.1564 测试的报文反射参数。

```
<PE1> system-view
[PE1] nqa reflector 1 interface gigabitethernet 1/0/1 ip destination 10.2.2.2 source 10.1.1.1 destination-port 20000 source-port 10000
```

开启 NQA 服务器功能。

```
[PE1] nqa server enable
```

(3) 配置 PE-agg

创建 Y.1564 类型的 NQA 测试组（管理员为 admin，操作标签为 test1）。

```
<PE-agg> system-view
[PE-agg] nqa entry admin test1
[PE-agg-nqa-admin-test1] type y1564
```

配置源 IP 为网关口 IP。

```
[PE-agg-nqa-admin-test1-y1564] source ip 10.1.1.1
```

配置目的 IP 为用户 IP。

```
[PE-agg-nqa-admin-test1-y1564] destination ip 10.2.2.2
```

配置源端口和目的端口。

```
[PE-agg-nqa-admin-test1-y1564] source port 10000
[PE-agg-nqa-admin-test1-y1564] destination port 20000
```

配置报文出接口。

```
[PE-agg-nqa-admin-test1-y1564] out interface VE-L3VPN2
```

配置 Y.1564 测试的基本参数。

```
[PE-agg-nqa-admin-test1-y1564] bandwidth cir 100 pir 10000
[PE-agg-nqa-admin-test1-y1564] allowed-jitter 1000
[PE-agg-nqa-admin-test1-y1564] allowed-frame-loss 1000
[PE-agg-nqa-admin-test1-y1564] allowed-transfer-delay 1000
```

开启流量监管测试。

```
[PE-nqa-admin-test1-y1564] traffic-policing-test enable
```

启动 Y.1564 测试操作，测试持续时间与配置的测试项目以及每个项目的时间有关。

```
[PE-agg-nqa-admin-test1-y1564] start
[PE-agg-nqa-admin-test1-y1564] quit
```

4. 验证配置

显示 Y.1564 测试的当前结果。

```
[PE-agg] display nqa result
NQA entry (admin admin, tag test1) test results:
  Status                    : In progress
  Last test                 : Traffic policing test
  Estimated total time (s)  : 909
  Actual test time used (s) : 24
  Detailed test results:
    CIR test (with the step of 1):
      Start time               : 2018-11-03 15:44:16.1
      End time                 : 2018-11-03 15:44:19.3
      Status                   : Succeeded
      Min/Max/Average IR (kbps) : 58/82/68
      Min/Max/Average FTD (us)  : 21/25/23
      Min/Max/Average FDV (us)  : 21/25/23
      FL count/FLR             : 2/0.002%
      Packets out of order     : 0
      Severely Err Secs/AVAIL   : 0/100.000%
    PIR test (color-blind):
      Start time               : 2018-11-03 15:44:19.3
      End time                 : 2018-11-03 15:44:22.5
      Status                   : Succeeded
      Min/Max/Average IR (kbps) : 10123/10234/10187
      Min/Max/Average FTD (us)  : 371/375/373
      Min/Max/Average FDV (us)  : 71/75/73
      FL count/FLR             : 7/0.007%
      Packets out of order     : 0
      Severely Err Secs/AVAIL   : 0/100.000%
  Traffic policing test (color-blind):
    Start time               : 2018-11-03 15:44:22.5
    End time                 : 2018-11-03 15:44:25.7
    Status                   : Succeeded
    Min/Max/Average IR (kbps) : 8328/8769/8654
    Min/Max/Average FTD (us)  : 738/762/740
    Min/Max/Average FDV (us)  : 58/62/60
    FL count/FLR             : 10/0.01%
    Packets out of order     : 0
    Severely Err Secs/AVAIL   : 0/100.000%
```

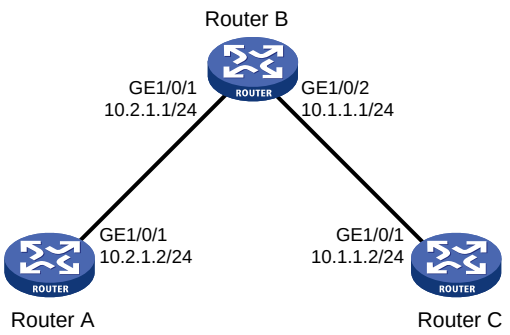
1.7.26 NQA 联动配置举例（路由应用）

1. 组网需求

- Router A 到达 Router C 的静态路由下一跳为 Router B。
- 在 Router A 上通过静态路由、Track 与 NQA 联动，对到达 Router C 的静态路由有效性进行实时判断。

2. 组网图

图1-18 NQA 联动配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址。（配置过程略）

(2) 在 Router A 上配置静态路由，并与 Track 项关联。

配置到达 Router C 的静态路由下一跳地址为 10.2.1.1，并配置静态路由与 Track 项 1 关联。

```
<RouterA> system-view
[RouterA] ip route-static 10.1.1.2 24 10.2.1.1 track 1
```

(3) 在 Router A 上配置 NQA 测试组

创建管理员名为 admin、操作标签为 test1 的 NQA 测试组。

```
[RouterA] nqa entry admin test1
```

配置测试类型为 ICMP-echo。

```
[RouterA-nqa-admin-test1] type icmp-echo
```

配置目的地址为 10.2.1.1。

```
[RouterA-nqa-admin-test1-icmp-echo] destination ip 10.2.1.1
```

测试频率为 100ms。

```
[RouterA-nqa-admin-test1-icmp-echo] frequency 100
```

配置联动项 1（连续失败 5 次触发联动）。

```
[RouterA-nqa-admin-test1-icmp-echo] reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type
trigger-only
[RouterA-nqa-admin-test1-icmp-echo] quit
```

启动 ICMP-echo 探测操作，并一直进行测试。

```
[RouterA] nqa schedule admin test1 start-time now lifetime forever
```

(4) 在 Router A 上配置 Track 项

配置 Track 项 1，关联 NQA 测试组（管理员为 admin，操作标签为 test1）的联动项 1。

```
[RouterA] track 1 nqa entry admin test1 reaction 1
```

4. 验证配置

显示 Router A 上 Track 项的信息。

```
[RouterA] display track all
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 0 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test1
    Reaction: 1
```

显示 Router A 的路由表。

```
[RouterA] display ip routing-table

Destinations : 11        Routes : 11

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
10.1.1.0/24         Static 60   0            10.2.1.1        GE1/0/1
10.2.1.0/24         Direct 0    0            10.2.1.2        GE1/0/1
10.2.1.0/32         Direct 0    0            10.2.1.2        GE1/0/1
10.2.1.2/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.255/32       Direct 0    0            10.2.1.2        GE1/0/1
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

以上显示信息表示，NQA 测试的结果为下一跳地址 10.2.1.1 可达（Track 项状态为 Positive），配置的静态路由生效。

在 Router B 上删除接口 GigabitEthernet1/0/1 的 IP 地址。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] undo ip address
```

显示 Router A 上 Track 项的信息。

```
[RouterA] display track all
Track ID: 1
  State: Negative
  Duration: 0 days 0 hours 0 minutes 0 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test1
    Reaction: 1
```

显示 Router A 的路由表。

```
[RouterA] display ip routing-table

Destinations : 10        Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
10.2.1.0/24         Direct 0    0            10.2.1.2        GE1/0/1
10.2.1.0/32         Direct 0    0            10.2.1.2        GE1/0/1
10.2.1.2/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.255/32       Direct 0    0            10.2.1.2        GE1/0/1
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

以上显示信息表示，NQA 测试的结果为下一跳地址 10.2.1.1 不可达（Track 项状态为 Negative），配置的静态路由无效。

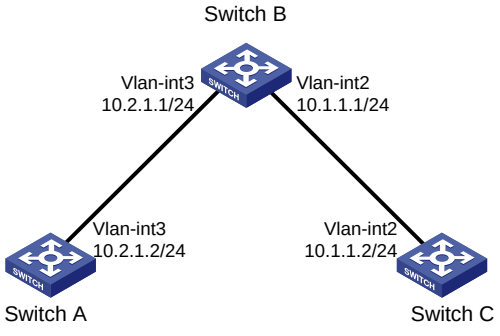
1.7.27 NQA 联动配置举例（交换应用）

1. 组网需求

- Switch A 到达 Switch C 的静态路由下一跳为 Switch B。
- 在 Switch A 上通过静态路由、Track 与 NQA 联动，对到达 Switch C 的静态路由有效性进行实时判断。

2. 组网图

图1-19 NQA 联动配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址。（配置过程略）

(2) 在 Switch A 上配置静态路由，并与 Track 项关联。

配置到达 Switch C 的静态路由下一跳地址为 10.2.1.1，并配置静态路由与 Track 项 1 关联。

```
<SwitchA> system-view
[SwitchA] ip route-static 10.1.1.2 24 10.2.1.1 track 1
```

(3) 在 Switch A 上配置 NQA 测试组

创建管理员名为 admin、操作标签为 test1 的 NQA 测试组。

```
[SwitchA] nqa entry admin test1
```

配置测试类型为 ICMP-echo。

```
[SwitchA-nqa-admin-test1] type icmp-echo
```

配置目的地址为 10.2.1.1。

```
[SwitchA-nqa-admin-test1-icmp-echo] destination ip 10.2.1.1
```

测试频率为 100ms。

```
[SwitchA-nqa-admin-test1-icmp-echo] frequency 100
```

配置联动项 1（连续失败 5 次触发联动）。

```
[SwitchA-nqa-admin-test1-icmp-echo] reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type
trigger-only
[SwitchA-nqa-admin-test1-icmp-echo] quit
```

启动 ICMP-echo 探测操作，并一直进行测试。

```
[SwitchA] nqa schedule admin test1 start-time now lifetime forever
```

(4) 在 Switch A 上配置 Track 项

配置 Track 项 1，关联 NQA 测试组（管理员为 admin，操作标签为 test1）的联动项 1。

```
[SwitchA] track 1 nqa entry admin test1 reaction 1
```

4. 验证配置

显示 Switch A 上 Track 项的信息。

```
[SwitchA] display track all
Track ID: 1
```

```
  State: Positive
  Duration: 0 days 0 hours 0 minutes 0 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test1
    Reaction: 1
```

显示 Switch A 的路由表。

```
[SwitchA] display ip routing-table

Destinations : 11        Routes : 11

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
10.1.1.0/24         Static 60   0            10.2.1.1        Vlan3
10.2.1.0/24         Direct 0    0            10.2.1.2        Vlan3
10.2.1.0/32         Direct 0    0            10.2.1.2        Vlan3
10.2.1.2/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.255/32       Direct 0    0            10.2.1.2        Vlan3
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

以上显示信息表示，NQA 测试的结果为下一跳地址 10.2.1.1 可达（Track 项状态为 Positive），配置的静态路由生效。

在 Switch B 上删除 VLAN 接口 3 的 IP 地址。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] undo ip address
```

显示 Switch A 上 Track 项的信息。

```
[SwitchA] display track all
Track ID: 1
  State: Negative
  Duration: 0 days 0 hours 0 minutes 0 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test1
    Reaction: 1
```

显示 Switch A 的路由表。

```
[SwitchA] display ip routing-table

Destinations : 10        Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
10.2.1.0/24         Direct 0    0            10.2.1.2        Vlan3
10.2.1.0/32         Direct 0    0            10.2.1.2        Vlan3
10.2.1.2/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.255/32       Direct 0    0            10.2.1.2        Vlan3
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
```

```
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
255.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
```

以上显示信息表示，NQA 测试的结果为下一跳地址 10.2.1.1 不可达（Track 项状态为 Negative），配置的静态路由无效。

1.8 NQA模板典型配置举例

说明

NQA 模板典型配置举例中只描述如何配置 NQA 模板，关于如何引用 NQA 模板的配置举例请参见“可靠性配置指导”中的“负载均衡”。

1.8.1 ARP 类型的 NQA 模板配置举例

1. 组网需求

外部特性通过引用 ARP 类型的 NQA 模板，测试 Device B 上的 ARP 功能是否可用。

2. 组网图

图1-20 ARP 类型的 NQA 模板配置组网图

3. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

创建 ARP 类型的 NQA 模板，模板名为 arp。

```
<DeviceA> system-view
[DeviceA] nqa template arp arp
```

配置 ARP 测试操作中探测报文的目的地址为 10.1.1.2。

```
[DeviceA-nqatplt-arp-arp] destination ip 10.1.1.2
```

配置确定节点有效前需要连续探测成功的次数为 2。当连续探测成功次数达到 2 次时，NQA 客户端把探测成功的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-arp-arp] reaction trigger probe-pass 2
```

配置确定节点失效需要连续探测失败的次数为 2。当连续探测失败次数达到 2 次时，NQA 客户端把探测失败的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-arp-arp] reaction trigger probe-fail 2
[DeviceA-nqatplt-arp-arp] quit
```

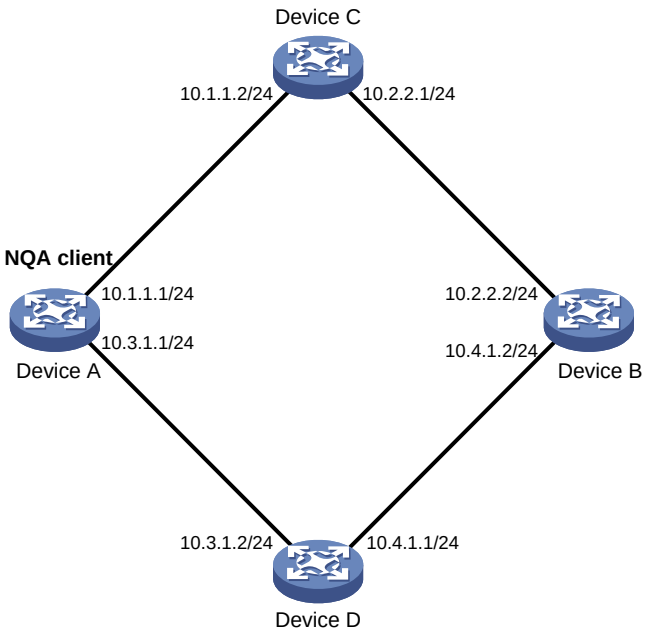
1.8.2 ICMP 类型的 NQA 模板配置举例

1. 组网需求

外部特性通过引用 ICMP 类型的 NQA 模板，测试本端（Device A）发送的报文是否可以到达指定的目的端（Device B）。

2. 组网图

图1-21 ICMP 类型的 NQA 模板配置组网图



3. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

创建 ICMP 类型的 NQA 模板，模板名为 icmp，并配置操作中探测报文的目的地址为 10.2.2.2。

```
<DeviceA> system-view
[DeviceA] nqa template icmp icmp
[DeviceA-nqatplt-icmp-icmp] destination ip 10.2.2.2
```

配置 ICMP 一次探测的超时时间为 500 毫秒，连续两次探测开始时间的时间间隔为 3000 毫秒。

```
[DeviceA-nqatplt-icmp-icmp] probe timeout 500
[DeviceA-nqatplt-icmp-icmp] frequency 3000
```

配置确定节点有效前需要连续探测成功的次数为 2。当连续探测成功次数达到 2 次时，NQA 客户端把探测成功的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-icmp-icmp] reaction trigger probe-pass 2
```

配置确定节点失效需要连续探测失败的次数为 2。当连续探测失败次数达到 2 次时，NQA 客户端把探测失败的消息发送给外部特性，是外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-icmp-icmp] reaction trigger probe-fail 2
[DeviceA-nqatplt-icmp-icmp] quit
```

1.8.3 IMAP 类型的 NQA 模板配置举例

1. 组网需求

外部特性通过引用 IMAP 类型的 NQA 模板，测试 Device A 是否可以和指定的 IMAP 服务器 Device B 建立连接，以及能否登录服务器邮箱。登录 IMAP 服务器的用户名为 admin，密码为 123456，要登录的邮箱名为 test。

组网图

图1-22 IMAP 类型的 NQA 模板配置组网图

2. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

创建 IMAP 类型的 NQA 模板，模板名为 imap。

```
<DeviceA> system-view
[DeviceA] nqa template imap imap
```

配置 IMAP 测试操作中探测报文的目的地址为 10.2.2.2。

```
[DeviceA-nqatplt-imap-imap] destination ip 10.2.2.2
```

配置登录 IMAP 服务器的用户名为 admin。

```
[DeviceA-nqatplt-imap-imap] username admin
```

配置登录 IMAP 服务器的密码为 123456。

```
[DeviceA-nqatplt-imap-imap] password simple 123456
```

配置登录 IMAP 服务器的邮箱名为 test。

```
[DeviceA-nqatplt-imap-imap] mailbox test
```

配置确定节点有效前需要连续探测成功的次数为 2。当连续探测成功次数达到 2 次时，NQA 客户端把探测成功的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-imap-imap] reaction trigger probe-pass 2
```

配置确定节点失效需要连续探测失败的次数为 2。当连续探测失败次数达到 2 次时，NQA 客户端把探测失败的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-imap-imap] reaction trigger probe-fail 2
[DeviceA-nqatplt-imap-imap] quit
```

1.8.4 DNS 类型的 NQA 模板配置举例

1. 组网需求

外部特性通过引用 DNS 类型的 NQA 模板，测试 Device A 是否可以通过指定的 DNS 服务器将域名 host.com 解析为 IP 地址。

2. 组网图

图1-23 DNS 类型的 NQA 模板配置组网图

3. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

创建 DNS 类型的 NQA 模板，模板名为 dns。

```
<DeviceA> system-view
[DeviceA] nqa template dns dns
```
配置操作中探测报文的目的地址为 DNS 服务器的 IP 地址 10.2.2.2，要解析的域名为 host.com，解析类型为 A，用户期望返回的 IP 地址为 3.3.3.3。
```
[DeviceA-nqatplt-dns-dns] destination ip 10.2.2.2
[DeviceA-nqatplt-dns-dns] resolve-target host.com
[DeviceA-nqatplt-dns-dns] resolve-type A
[DeviceA-nqatplt-dns-dns] expect ip 3.3.3.3
```
配置确定节点有效前需要连续探测成功的次数为 2。当连续探测成功次数达到 2 次时，NQA 客户端把探测成功的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。
```
[DeviceA-nqatplt-dns-dns] reaction trigger probe-pass 2
```
配置确定节点失效需要连续探测失败的次数为 2。当连续探测失败次数达到 2 次时，NQA 客户端把探测失败的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。
```
[DeviceA-nqatplt-dns-dns] reaction trigger probe-fail 2
[DeviceA-nqatplt-dns-dns] quit
```

1.8.5 POP3 类型的 NQA 模板配置举例

1. 组网需求

外部特性通过引用 POP3 类型的 NQA 模板，测试 Device A 是否可以和指定的 POP3 服务器（Device B）建立连接，以及能否登录服务器。登录 POP3 服务器的用户名为 admin，密码为 123456。

2. 组网图

图1-24 POP3 类型的 NQA 模板配置组网图

3. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

#创建 POP3 类型的 NQA 模板，模板名为 pop3。
```
<DeviceA> system-view
[DeviceA] nqa template pop3 pop3
```
配置 POP3 测试操作中探测报文的目的地址为 10.2.2.2。
```
[DeviceA-nqatplt-pop3-pop3] destination ip 10.2.2.2
```
配置登录 POP3 服务器的用户名为 admin。
```
[DeviceA-nqatplt-pop3-pop3] username admin
```
配置登录 POP3 服务器的密码为 123456。
```
[DeviceA-nqatplt-pop3-pop3] password simple 123456
```
配置确定节点有效前需要连续探测成功的次数为 2。当连续探测成功次数达到 2 次时，NQA 客户端把探测成功的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。
```
[DeviceA-nqatplt-pop3-pop3] reaction trigger probe-pass 2
```

配置确定节点失效需要连续探测失败的次数为 2。当连续探测失败次数达到 2 次时，NQA 客户端把探测失败的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-pop3-pop3] reaction trigger probe-fail 2
[DeviceA-nqatplt-pop3-pop3] quit
```

1.8.6 SMTP 类型的 NQA 模板配置举例

1. 组网需求

外部特性通过引用 SMTP 类型的 NQA 模板，测试 Device A 是否可以和指定的 SMTP 服务器（Device B）建立连接，以及能否登录服务器邮箱。

2. 组网图

图1-25 SMTP 类型的 NQA 模板配置组网图

3. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

#创建 SMTP 类型的 NQA 模板，模板名为 smtp。

```
<DeviceA>system-view
[DeviceA] nqa template smtp smtp
```

配置 SMTP 测试操作中探测报文的目的地址为 10.2.2.2。

```
[DeviceA-nqatplt-smtp-smtp] destination ip 10.2.2.2
```

配置确定节点有效前需要连续探测成功的次数为 2。当连续探测成功次数达到 2 次时，NQA 客户端把探测成功的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-smtp-smtp] reaction trigger probe-pass 2
```

配置确定节点失效需要连续探测失败的次数为 2。当连续探测失败次数达到 2 次时，NQA 客户端把探测失败的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-smtp-smtp] reaction trigger probe-fail 2
[DeviceA-nqatplt-smtp-smtp] quit
```

1.8.7 TCP 类型的 NQA 模板配置举例

1. 组网需求

外部特性通过引用 TCP 类型的 NQA 模板，测试本端（Device A）和服务器（Device B）的端口之间能否建立 TCP 连接，并处理服务器端的应答数据。

2. 组网图

图1-26 TCP 类型的 NQA 模板配置组网图

3. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

(1) 配置 Device B

使能 NQA 服务器，配置监听的 IP 地址为 10.2.2.2，TCP 端口号为 9000。

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server tcp-connect 10.2.2.2 9000
```

(2) 配置 Device A

创建 TCP 类型的 NQA 模板，模板名为 tcp。

```
<DeviceA> system-view
[DeviceA] nqa template tcp tcp
```

配置 TCP 探测报文的目的地址为 10.2.2.2，目的端口号为 9000。

```
[DeviceA-nqatplt-tcp-tcp] destination ip 10.2.2.2
[DeviceA-nqatplt-tcp-tcp] destination port 9000
```

配置确定节点有效前需要连续探测成功的次数为 2。当连续探测成功次数达到 2 次时，NQA 客户端把探测成功的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-tcp-tcp] reaction trigger probe-pass 2
```

配置确定节点失效需要连续探测失败的次数为 2。当连续探测失败次数达到 2 次时，NQA 客户端把探测失败的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-tcp-tcp] reaction trigger probe-fail 2
[DeviceA-nqatplt-tcp-tcp] quit
```

1.8.8 TCP Half Open 类型的 NQA 模板配置举例

1. 组网需求

外部特性通过引用 TCP Half Open 类型的 NQA 模板，测试本端（Device A）和服务器（Device B）的 TCP 服务是否可用。

2. 组网图

图1-27 TCP Half Open 类型的 NQA 模板配置组网图

3. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

创建 TCP Half Open 类型的 NQA 模板，模板名为 test。

```
<DeviceA> system-view
[DeviceA] nqa template tcphalfopen test
```

配置 TCP Half Open 探测报文的目的地址为 10.2.2.2。

```
[DeviceA-nqatplt-tcphalfopen-test] destination ip 10.2.2.2
```

配置连续探测成功的次数为 2。当连续探测成功次数达到 2 次时，NQA 客户端把探测成功的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-tcphalfopen-test] reaction trigger probe-pass 2
```

配置连续探测失败的次数为 2。当连续探测失败次数达到 2 次时，NQA 客户端把探测失败的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-tcphalfopen-test] reaction trigger probe-fail 2
[DeviceA-nqatplt-tcphalfopen-test] quit
```

1.8.9 UDP 类型的 NQA 模板配置举例

1. 组网需求

外部特性通过引用 UDP 类型的 NQA 模板，测试本端（Device A）和服务器（Device B）的端口之间的 UDP 报文交互，并处理服务器端的应答数据。

2. 组网图

图1-28 UDP 类型的 NQA 模板配置组网图

3. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

(1) 配置 Device B

使能 NQA 服务器，配置监听的 IP 地址为 10.2.2.2，UDP 端口号为 9000。

```
<DeviceB> system-view
[DeviceB] nqa server enable
[DeviceB] nqa server udp-echo 10.2.2.2 9000
```

(2) 配置 Device A

创建 UDP 类型的 NQA 模板，模板名为 udp。

```
<DeviceA> system-view
[DeviceA] nqa template udp udp
```

配置 UDP 探测报文的目的地址为 10.2.2.2，目的端口号为 9000。

```
[DeviceA-nqatplt-udp-udp] destination ip 10.2.2.2
[DeviceA-nqatplt-udp-udp] destination port 9000
```

配置确定节点有效前需要连续探测成功的次数为 2。当连续探测成功次数达到 2 次时，NQA 客户端把探测成功的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-udp-udp] reaction trigger probe-pass 2
```

配置确定节点失效需要连续探测失败的次数为 2。当连续探测失败次数达到 2 次时，NQA 客户端把探测失败的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-udp-udp] reaction trigger probe-fail 2
[DeviceA-nqatplt-udp-udp] quit
```

1.8.10 HTTP 类型的 NQA 模板配置举例

1. 组网需求

外部特性通过引用 HTTP 类型的 NQA 模板，测试是否可以和指定的 HTTP 服务器之间建立连接，以及能否从 HTTP 服务器获取数据。

2. 组网图

图1-29 HTTP 类型的 NQA 模板配置组网图

3. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

创建 HTTP 类型的 NQA 模板，模板名为 http。

```
<DeviceA> system-view
[DeviceA] nqa template http http
```

配置 HTTP 测试的网址为 https://10.2.2.2/index.html。

```
[DeviceA-nqatplt-http-http] url http://10.2.2.2/index.html
```

配置 HTTP 测试的操作方式为 get 操作。（get 操作为缺省操作方式，因此，可以不执行本配置）

```
[DeviceA-nqatplt-http-http] operation get
```

配置确定节点有效前需要连续探测成功的次数为 2。当连续探测成功次数达到 2 次时，NQA 客户端把探测成功的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-http-http] reaction trigger probe-pass 2
[DeviceA-nqatplt-http-http] quit
```

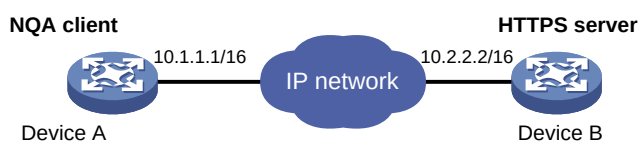
1.8.11 HTTPS 类型的 NQA 模板配置举例

1. 组网需求

外部特性通过引用 HTTPS 类型的 NQA 模板，测试是否可以和指定的 HTTPS 服务器之间建立连接，以及能否从 HTTPS 服务器获取数据。

2. 组网图

图1-30 HTTPS 类型的 NQA 模板配置组网图



3. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

在 Device A 上配置 SSL 客户端策略，确保客户端与服务器端可以建立 SSL 安全连接。（配置过程略）

创建 HTTPS 类型的 NQA 模板，模板名为 test。

```
<DeviceA> system-view
[DeviceA] nqa template https https
```

配置 HTTPS 测试的网址为 https://10.2.2.2/index.html。

```
[DeviceA-nqatplt-https-https] url https://10.2.2.2/index.html
```

配置 HTTPS 绑定的 SSL 客户端策略为 abc。

```
[DeviceA-nqatplt-https-https] ssl-client-policy abc
```

配置 HTTPS 测试的操作方式为 get 操作。（get 操作为缺省操作方式，可不执行本配置）

```
[DeviceA-nqatplt-https-https] operation get
```

配置 HTTPS 测试使用的版本为 1.0。（缺省情况下使用的版本为 1.0，可不执行本配置）

```
[DeviceA-nqatplt-https-https] version v1.0
```

配置连续探测成功的次数为 2。当连续探测成功次数达到 2 次时，NQA 客户端把探测成功的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-https-https] reaction trigger probe-pass 2
```

配置确定节点失效需要连续探测失败的次数为 2。当连续探测失败次数达到 2 次时，NQA 客户端把探测失败的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-https-https] reaction trigger probe-fail 2
[DeviceA-nqatplt-https-https] quit
```

1.8.12 FTP 类型的 NQA 模板配置举例

1. 组网需求

外部特性通过引用 FTP 类型的 NQA 模板，测试 Device A 是否可以和指定的 FTP 服务器 Device B 建立连接，以及能否往 FTP 服务器上传文件。登录 FTP 服务器的用户名为 admin，密码为 systemtest，要传送到服务器的文件名为 config.txt。

2. 组网图

图1-31 FTP 类型的 NQA 模板配置组网图

3. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

创建 FTP 类型的 NQA 模板，模板名为 ftp。

```
<DeviceA> system-view
[DeviceA] nqa template ftp ftp
```

配置操作的目的地址为 FTP 服务器的 IP 地址 10.2.2.2。

```
[DeviceA-nqatplt-ftp-ftp] url ftp://10.2.2.2
```

配置探测报文的源 IP 地址为 10.1.1.1。

```
[DeviceA-nqatplt-ftp-ftp] source ip 10.1.1.1
```
配置执行的操作为向 FTP 服务器上传文件 config.txt。
```
[DeviceA-nqatplt-ftp-ftp] operation put
[DeviceA-nqatplt-ftp-ftp] filename config.txt
```
配置登录 FTP 服务器的用户名为 admin。
```
[DeviceA-nqatplt-ftp-ftp] username admin
```
配置登录 FTP 服务器的密码为 systemtest。
```
[DeviceA-nqatplt-ftp-ftp] password simple systemtest
```
配置确定节点有效前需要连续探测成功的次数为 2。当连续探测成功次数达到 2 次时，NQA 客户端把探测成功的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。
```
[DeviceA-nqatplt-ftp-ftp] reaction trigger probe-pass 2
```
配置确定节点失效需要连续探测失败的次数为 2。当连续探测失败次数达到 2 次时，NQA 客户端把探测失败的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。
```
[DeviceA-nqatplt-ftp-ftp] reaction trigger probe-fail 2
[DeviceA-nqatplt-ftp-ftp] quit
```

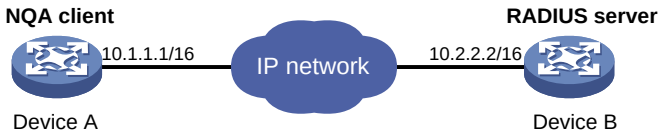
1.8.13 RADIUS 类型的 NQA 模板配置举例

1. 组网需求

外部特性通过引用 RADIUS 类型的 NQA 模板，测试 Device A 是否可以和指定的 RADIUS 服务器 Device B 建立连接，并检测 Device B 是否提供服务。RADIUS 用户名为 admin，RADIUS 密码为 systemtest，RADIUS 认证使用的共享密钥为 123456。

2. 组网图

图1-32 RADIUS 类型的 NQA 模板配置组网图



3. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

配置 RADIUS 服务器 Device B。（配置步骤略）

创建 RADIUS 类型的 NQA 模板，模板名为 radius。
```
<DeviceA> system-view
[DeviceA] nqa template radius radius
```
配置 RADIUS 探测报文的目的地址为 10.2.2.2。
```
[DeviceA-nqatplt-radius-radius] destination ip 10.2.2.2
```
配置 RADIUS RADIUS 用户名为 admin，RADIUS 密码为明文 systemtest。
```
[DeviceA-nqatplt-radius-radius] username admin
[DeviceA-nqatplt-radius-radius] password simple systemtest
```
配置 RADIUS 用于 RADIUS 认证的共享密钥为明文 123456。
```
[DeviceA-nqatplt-radius-radius] key simple 123456
```
配置确定节点有效前需要连续探测成功的次数为 2。当连续探测成功次数达到 2 次时，NQA 客户端把探测成功的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。
```
[DeviceA-nqatplt-radius-radius] reaction trigger probe-pass 2
```

配置确定节点失效需要连续探测失败的次数为 2。当连续探测失败次数达到 2 次时，NQA 客户端把探测失败的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-radius-radius] reaction trigger probe-fail 2
[DeviceA-nqatplt-radius-radius] quit
```

1.8.14 SNMP 类型的 NQA 模板配置举例

1. 组网需求

外部特性通过引用 SNMP 类型的 NQA 模板，测试 Device B 上的 SNMP 功能是否可用。

2. 组网图

图1-33 SNMP 类型的 NQA 模板配置组网图

3. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

(1) 配置 SNMP Agent（Device B）

启动 SNMP Agent 服务，设置 SNMP 版本为 all、只读团体名为 public、读写团体名为 private。

```
<DeviceB> system-view
[DeviceB] snmp-agent sys-info version all
[DeviceB] snmp-agent community read public
[DeviceB] snmp-agent community write private
```

(2) 配置 Device A

创建 SNMP 类型的 NQA 模板，模板名为 snmp。

```
<DeviceA> system-view
[DeviceA] nqa template snmp snmp
```

配置 SNMP 测试操作中探测报文的目的地址为 10.2.2.2，目的端口号为 161。

```
[DeviceA-nqatplt-snmp-snmp] destination ip 10.2.2.2
[DeviceA-nqatplt-snmp-snmp] destination port 161
```

配置 SNMP 测试操作中 SNMP 团体名称为 public。

```
[DeviceA-nqatplt-snmp-snmp] community read simple public
```

配置确定节点有效前需要连续探测成功的次数为 2。当连续探测成功次数达到 2 次时，NQA 客户端把探测成功的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-snmp-snmp] reaction trigger probe-pass 2
```

配置确定节点失效需要连续探测失败的次数为 2。当连续探测失败次数达到 2 次时，NQA 客户端把探测失败的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-snmp-snmp] reaction trigger probe-fail 2
[DeviceA-nqatplt-snmp-snmp] quit
```

1.8.15 SSL 类型的 NQA 模板配置举例

1. 组网需求

外部特性通过引用 SSL 类型的 NQA 模板，本端（Device A）通过引用指定的 SSL 客户端策略与 SSL 服务器（Device B）建立 SSL 连接，从而测试 SSL 客户端和服务器端的连通性和性能。

2. 组网图

图1-34 SSL 类型的 NQA 模板配置组网图

3. 配置步骤

配置各接口的 IP 地址。（配置过程略）

配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

在 Device A 上配置 SSL 客户端策略，确保客户端与服务器端可以建立 SSL 安全连接。（配置过程略）

创建 SSL 类型的 NQA 模板，模板名为 ssl。

```
<DeviceA> system-view
[DeviceA] nqa template ssl ssl
```

配置 SSL 探测报文的目的地址为 10.2.2.2，目的端口号为 9000。

```
[DeviceA-nqatplt-ssl-ssl] destination ip 10.2.2.2
[DeviceA-nqatplt-ssl-ssl] destination port 9000
```

配置 SSL 绑定的 SSL 客户端策略为 abc。

```
[DeviceA-nqatplt-ssl-ssl] ssl-client-policy abc
```

配置连续探测成功的次数为 2。当连续探测成功次数达到 2 次时，NQA 客户端把探测成功的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-ssl-ssl] reaction trigger probe-pass 2
```

配置连续探测失败的次数为 2。当连续探测失败次数达到 2 次时，NQA 客户端把探测失败的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
[DeviceA-nqatplt-ssl-ssl] reaction trigger probe-fail 2
[DeviceA-nqatplt-ssl-ssl] quit
```

技术介绍

iNQA
智能网络质量分析

简介

iNQA（Intelligent Network Quality Analyzer，智能网络质量分析）是一种适用于大规模IP网络、可快速测量网络丢包性能的机制，可测量单向和双向丢包信息（包括报文丢失数、报文丢失率、字节丢失数、字节丢失率）。网络管理员利用iNQA的测量结果可快速定位丢包时间、丢包位置、丢包严重程度。

技术优势

测量范围广

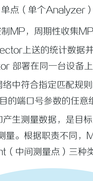
iNQA支持对二层和三层网络中的丢包信息进行测量

支持场景多样

支持点到点、点到多点、多点到多点等多种场景

定位速度快

iNQA按周期自动测量目标流转发路径上各段的丢包信息。与发现丢包后再逐点检测、逐步排查故障点的测量方法相比，iNQA定位故障的速度更快



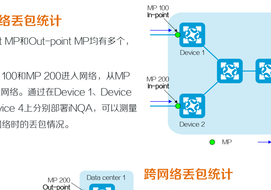
测量精度高

相比NQA等通过模拟业务报文进行测量的技术，iNQA通过标识业务报文，直接对业务报文进行丢包测量，测量数据可以真实反映网络质量，丢包计算更精准

网络模型

iNQA使用多点（多个Collector）收集、单点（单个Analyzer）计算的网络模型，其模型中包含以下元素：

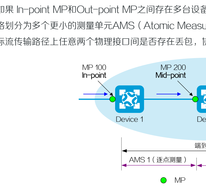
- **Collector**（采集器）：负责管理和控制MP，周期性收集MP产生的统计数据并上报给Analyzer。
- **Analyzer**（分析器）：负责收集Collector上送的统计数据并完成数据的汇总和计算。Analyzer可以独立部署在一台设备上，也可以和Collector 部署在同一台设备上。
- **目标流**：iNQA统计的目标对象，是网络中符合指定匹配规则的业务报文流。可以通过源IP地址/网段、目的IP地址/网段、协议类型、源端口号、目的端口号参数的任意组合来定义一条目标流。
- **MP**（测量点）：负责执行测量动作和产生测量数据，是目标流的实际测量点。MP和Collector上的接口绑定，完成对接口收发报文丢包情况的测量。根据职责不同，MP分为in-point（流量入口测量点）、Out-point（流量出口测量点）和Mid-point（中间测量点）三种类型。



应用场景

端到端丢包统计

端到端丢包统计用于测量流量从In-point MP进入网络、Out-point MP离开网络过程中的丢包信息。



点到点网络丢包统计

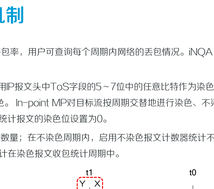
该场景下，In-point MP和Out-point MP均只有一个，且均在同一个网络（如均在广域网）内。

例如，目标流从MP 100进入网络，从MP 300离开网络，通过在Device 1和Device 3上部署iNQA，可以测量报文穿越该网络时的丢包情况。

多点到多点网络丢包统计

该场景下，In-point MP和Out-point MP均有多个，且均在同一个网络。

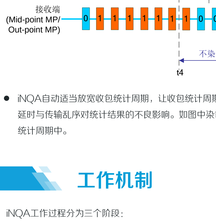
例如，目标流从MP 100和MP 200进入网络，从MP 300和MP 400离开网络。通过在Device 1、Device 2、Device 3和Device 4上分别部署iNQA，可以测量报文多路径穿越该网络时的丢包情况。



跨网络丢包统计

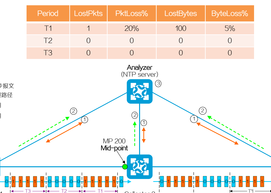
该场景下，In-point MP和Out-point MP不在同一个网络内，中间跨越了其它网络。

例如，用户通过Internet访问数据中心，业务流量在互为备份的数据中心1和数据中心2之间进行负载分担。在用户网络和数据中心网络边缘设备上部署iNQA，可以统计流量穿越Internet时是否存在丢包。



逐点丢包统计

如果In-point MP和Out-point MP之间存在多台设备、多段线路，可以使用Mid-point MP将端到端测量网络划分为多个更小的测量单元AMS（Atomic Measurement Span，原子测量段）。使用AMS可以测量目标流传输路径上任意两个物理接口间是否存在丢包，协助进一步定位丢包位置，这就是逐点丢包统计。



报文染色和计数机制

为方便用户及时了解网络丢包情况，iNQA按周期测量丢包率，用户可查询每个周期内网络的丢包情况。iNQA通过以下技术实现按周期测量并确保测量的准确性：

- 通过染色技术区别相邻统计周期内的报文。iNQA使用IP报文头中ToS字段的5～7位中的任意比特作为染色位。将染色位设置为1表示染色，设置为0表示不染色。In-point MP对目标流按周期交替地进行染色、不染色处理；Out-point MP进行去染色处理，即将所有统计报文的染色位设置为0。
- 在染色周期内，启用染色报文计数器统计染色报文的数量；在不染色周期内，启用不染色报文计数器统计不染色报文的数量。例如，图中的不染色报文Y不会统计在染色报文收包统计周期中。

- iNQA自动适当放宽收包统计周期，让收包统计周期比发包统计周期长一点，这样可以最大程度地避免网络延时与传输乱序对统计结果的不良影响。如图中染色报文X延时到达，接收端仍会将其统计到染色报文收包统计周期中。

工作机制

iNQA工作过程分为三个阶段：

1. 所有参与测量的设备通过NTP或者PTP功能达到时间同步。在测量开始前，为确保各Collector能够基于相同的周期进行报文染色、上报、统计，所有Collector必须时间同步。如果时间不同步，会导致iNQA计算结果不准确。同时，为便于管理维护，建议Analyzer和所有Collector 之间时间同步。
2. Collector周期性收集MP产生的统计数据并上报给Analyzer。
3. Analyzer对相同周期内相同目标流的报文进行丢包分析，计算报文丢失数（LostPkts）、报文丢失率（PktLoss%）、字节丢失数（LostBytes）、字节丢失率（ByteLoss%）。

LostPkts = PktsIngress - PktsEgress　　PktLoss% = LostPkts/PktsIngress

LostBytes = BytesIngress - BytesEgress　　ByteLoss% = LostBytes/BytesIngress

Period	LostPkts	PktLoss%	LostBytes	ByteLoss%
T1	1	20%	100	5%
T2	0	0	0	0
T3	0	0	0	0

In-point MP上的处理：

a. 根据匹配规则筛选出目标流

b. 对目标流报文按周期交替进行染色、不染色

c. 按周期对目标流报文计数，并上报给Analyzer

Mid-point MP上的处理：

a. 根据匹配规则筛选出目标流

b. 按周期对目标流报文计数，并上报给Analyzer

Out-point MP上的处理：

a. 根据匹配规则筛选出目标流

b. 按周期对目标流报文计数，并上报给Analyzer

c. 对染色报文进行去染色操作

新华三资料开发部出品

iNQA 技术白皮书

目 录

1 概述

1.1 产生背景

随着网络的普及和通信技术的发展，各种网络业务层出不穷，新业务对网路性能提出了更高的要求。其中，语音和视频业务是众多网络业务中应用最广泛的，它们对网络丢包、时延和时延抖动非常敏感。丢包率高、时延大会导致语音卡顿、视频马赛克，影响用户体验，严重时无法正常通信。当语音和视频业务质量下降时，用户希望能够快速定位并排除网络故障。

目前，IP 网络丢包、时延测量方法分为两大类：

- 间接测量：通过模拟真实业务报文发包的情况，计算模拟报文的丢包率、时延，间接得到业务报文的丢包率和时延。
- 直接测量：通过直接检测真实业务报文的收发情况，得到业务报文丢包率和时延。

表 1 描述了常见的传统丢包、时延测量技术。这些技术应用于小规模网络环境时，定位丢包、时延问题速度较快，但应用于大规模网络环境时，存在定位速度慢、定位消耗大、定位困难等问题。

表1 传统丢包、时延测量技术描述表

测量方法	传统测量技术	说明
间接测量	• Ping • NQA • TWAMP Light（Two-Way Active Measurement Protocol，双向主动测量协议）	• 仅支持三层网络 • 通过不断尝试与可能出现故障的设备建立连接的方式，逐步缩小故障检测范围，定位时间长 • 仅支持点到点场景 • 模拟发包，检测结果不够真实
直接测量	Y.1731，即CFD（Connectivity Fault Detection，连通错误检测）	• 仅支持二层网络 • 通过不断尝试与可能出现故障的设备建立连接的方式，逐步缩小故障检测范围，定位时间长 • 支持点到点、点到多点、多点到多点场景 • 对真实报文进行丢包检测，检测结果真实
	RFC 6374/6375（MPLS网络的丢包和时延测量）	• 仅支持 MPLS 网络 • 通过检测每一段的丢包情况，逐步缩小丢包范围，定位时间长 • 仅支持点到点场景 • 对真实报文进行丢包检测，检测结果真实

iNQA（Intelligent Network Quality Analyzer，智能网络质量分析）是一种适用于大规模 IP 网络、可快速测量网络丢包性能的检测机制。iNQA 可测量正向、反向以及双向的丢包情况，包括丢失的报文数、报文的丢失率、丢失的字节数、字节的丢失率。网络管理员利用测量结果可快速定位丢包时间、丢包位置、丢包严重程度。

1.2 技术优点

相较于传统丢包测量技术，iNQA 具有以下优势：

- 丢包检测结果真实。iNQA 是一种直接测量技术。它直接对业务报文进行测量，测量数据可以真实反映网络质量状况，丢包计算更精准。
- 丢包检测范围广，可测量二层网络和三层网络的丢包参数。
- 定位速度快，iNQA 会自动按周期测量丢包参数。相比发现丢包后，再不断尝试与可能出现故障的设备建立连接进行测量的方式，定位速度更快。
- 支持点到点、点到多点、多点到多点等多种场景。

2 iNQA 技术实现

2.1 基本概念

1. 目标流

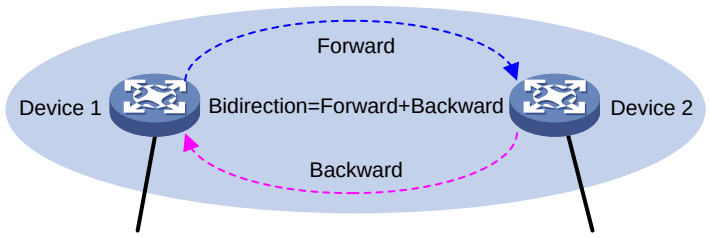
目标流指的是 iNQA 统计的目标对象，是网络中符合指定匹配规则的业务报文流。用户可通过表 2 中所示参数来定义一条目标流。这些参数可以任意组合来匹配业务报文。指定的参数越多，目标流就越精准，统计起来也越有针对性。

表2 目标流匹配参数

字段	描述
源IP地址/网段	根据业务报文的源IP地址或者源IP地址所属网段来匹配目标流
目的IP地址/网段	根据业务报文的目的IP地址或者目的IP地址所属网段来匹配目标流
协议类型	根据业务报文承载了何种协议（例如TCP、UDP等）来匹配目标流
源端口号	根据业务报文的源端口号来匹配目标流
目的端口号	根据业务报文的目的端口号来匹配目标流
DSCP	根据业务报文的DSCP（Differentiated Services Code Point，差分服务编码点）值来匹配目标流

iNQA 还支持按照目标流的方向进行测量。目标流的正向和反向是一个相对的概念，用户根据实际测量需要确定流的正向之后，则反方向的流即为反向流，正向流加反向流即为双向流。如图 1 所示，当用户将 Device 1 到 Device 2 的目标流定义为正向流时，则 Device 2 到 Device 1 的流量则为反向流，需要同时测量正向流和反向流的丢包情况时，可以使用双向流。双向流中正向报文和反向报文途途经的设备可以相同也可以不同。

图1 目标流方向示意图



2. 染色位

染色位又叫特征标识位，它能够对目标流进行周期性地标识，以达到对目标流进行周期性采样、统计的目的。iNQA 使用 IPv4 报文头中 ToS（Type of Service，服务类型）字段的 5～7 位作为染色位。

提示

ToS 字段包含 8 位，0～5 为 DSCP（Differentiated Services Code Point，差分服务编码点）位，用于提供差分服务，6～7 为保留位。当使用第 5 位作为染色位时，建议不要将 ToS 字段中的第 5 位用于 DSCP，以免造成丢包统计不准确。

3. 实例

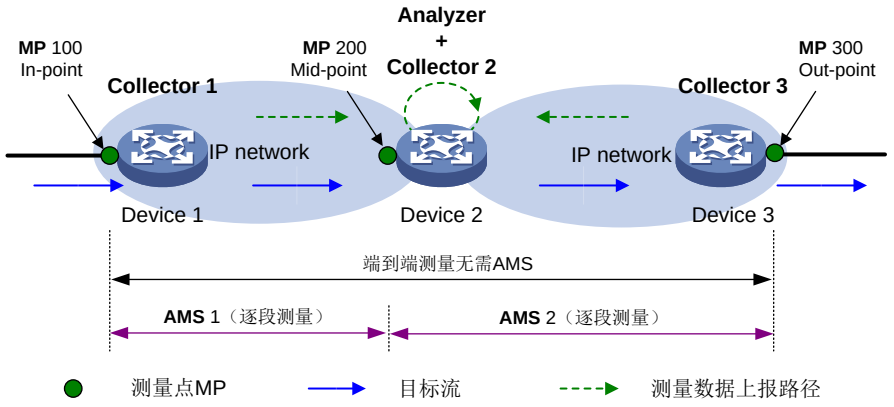
在实际网络中，经常需要在同一台设备上测量多条目标流的丢包率。iNQA 通过实例来实现不同目标流丢包率的独立测量和统计。

实例是一个逻辑概念，是 iNQA 的最小配置单元。实例中可以指定目标流、测量方向、测量位置、测量周期等参数，用于实现对指定目标流丢包情况的测量和统计。一个实例下绑定一条目标流。通过配置多个实例，绑定不同的目标流，可以同时测量和统计多种目标流的丢包情况。

2.2 网络模型

如图 2 所示，iNQA 网络模型中包含以下重要元素：MP（Measurement Point，测量点）、Collector（采集器）、Analyzer（分析器）和 AMS（Atomic Measurement Span，原子测量段）。

图2 iNQA 网络模型示意图



1. MP

MP 是一个逻辑的概念，在 iNQA 统计系统中负责测量动作的执行和测量数据的产生，是目标流的实际测量点。MP 需要和 Collector 上的接口绑定，完成对接口收发报文丢包情况的测量。MP 包含以下三种类型：

- In-point：表示目标流进入某一网络区域时的入口测量点。在该测量点上，系统对正向流进行染色操作，对反向流进行去染色操作，并对报文进行计数。
- Out-point：表示目标流离开网络区域时的出口测量点。在该测量点上，系统对正向流进行去染色操作，对反向流进行染色操作，并对报文进行计数。
- Mid-point：表示目标流传输路径的中间测量点，在该测量点上只统计报文的计数，不进行染色、去染色操作。当 In-point 和 Out-point 之间有丢包，需要进一步确认它们之间的更小的网络区段是否存在丢包时，才需要用到 Mid-point。

2. Collector

Collector 负责管理和控制 MP，周期性收集 MP 产生的统计数据并上报给 Analyzer。

3. Analyzer

Analyzer 负责以实例为单位收集 Collector 上送的统计数据并完成数据的汇总和计算。

说明

为了保护用户的投资，提高设备的利用率，设备同时支持作为 Collector 和 Analyzer。您可以将 Collector 和 Analyzer 分开部署，也可以部署在同一台设备上。

---

4. AMS

AMS 配置在 Analyzer 上，用于定义一个测量区段。通过 AMS 可以实现逐段排查丢包位置。一个实例下配置多个 AMS，每个 AMS 和这个实例下的任意 Collector 上的 MP 绑定，可以实现任意一段网络区间正向、反向或者双向流的数据的汇总和计算。

如图 2 所示：

- 如果仅需测量 MP 100 到 MP 300 之间的丢包情况，则无需使用 AMS。
- 当检测到 MP 100 到 MP 300 之间有丢包，在 Analyzer 上创建 AMS 1 和 AMS 2，可分段进一步定位 MP 100 到 MP 200、MP 200 到 MP 300 之间的丢包情况。其中，

- AMS 1 绑定 Collector 1 MP 100 和 Collector 2 MP 200。
- AMS 2 绑定 Collector 2 MP 200 和 Collector 3 MP 300。

2.3 工作机制

2.3.1 时间同步

iNQA 是一个多点收集、单点计算的模型，Collector（多个）按周期收集和上报报文计数，Analyzer（单个）按周期汇总和计算测量数据。iNQA 丢包计算依据报文守恒原理，即一段时间（多个周期）内、一个网络的入报文数量和出报文数量应该相等。如果不相等，则说明网络内存在丢包现象。所以，在测量开始前，要求所有 Collector 时间已经同步，从而确保各个 Collector 能够基于相同的周期进行报文染色、上报、统计。如果时间不同步，会导致 iNQA 计算结果不准确。Analyzer 和 Collector 的时间同步与否不影响计算结果，但为了便于管理和维护，建议 Analyzer 和所有 Collector 的时间均保持同步。

iNQA 支持使用 NTP（Network Time Protocol，网络时间协议）和 PTP（Precision Time Protocol，精确时间协议）协议进行时间同步，使用 NTP 还是 PTP 对 iNQA 测量结果无影响。NTP 和 PTP 功能的具体原理请参见 NTP、PTP 相关资料。

2.3.2 报文染色和计数机制

在 iNQA 的工作流程中，染色和计数是非常关键的步骤。染色和计数的准确性直接影响 iNQA 统计的准确性。

开启 iNQA 测量后，iNQA 会持续测量网络的丢包率。为方便用户随时了解网络丢包情况，iNQA 按周期测量丢包率，用户可查询每个周期内网络的丢包情况。同时为了实现按周期测量以及确保测量的准确性，iNQA 采用交替染色技术，即将染色位按周期交替设置为 1（染色）和 0（去染色），在染色周期只统计目标流中染色报文的数量；在不染色周期，只统计目标流中不染色报文的数量。

iNQA 报文染色和计数机制大体为：

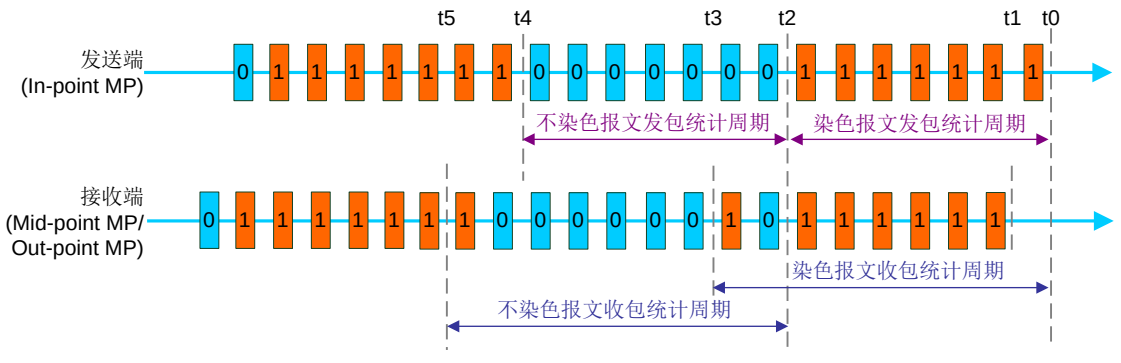
- 发送端（In-point MP）接收到报文后，会按照配置的 iNQA 匹配规则，筛选出目标流，对目标流按周期进行交替染色、周期计数，并将每个周期的报文计数上报给 Analyzer。
- 如果接收端为 Mid-point MP，Mid-point MP 收到报文后，会按照同样的 iNQA 匹配规则，筛选出目标流，对目标流周期计数并按周期将报文计数上报给 Analyzer，然后转发给下一跳。
- 如果接收端为 Out-point MP，Out-point MP 收到报文后，会和 Mid-point MP 一样对目标流周期计数并按周期将报文计数上报给 Analyzer，然后对目标流去染色后转发给下一跳。

为了确保计数的准确性，所有 MP 会同时用到两个计数器：

- 染色报文计数器用于统计染色报文的个数和字节数。
- 不染色报文计数器用于统计不染色报文的个数和字节数。

染色与不染色周期性交替，以及适当放宽接收端的统计周期，使得 iNQA 测量结果更加准确。

图3 iNQA 报文染色和计数示意图



如图 3 所示，iNQA 报文染色和计数过程如下：

(1) t0 时刻：发送端开始染色，并开始统计染色报文；接收端开启染色报文计数器，也开始统计染色报文。

(2) t1 时刻：发送端的首个染色报文到达接收端，接收端统计到第一个染色报文。

(3) t2 时刻：发送端结束一个周期的报文染色，并将统计到的染色报文的个数以及字节数上报给 Analyzer。同时开始不染色报文的计数。接收端开启不染色报文计数器，也开始统计不染色报文。

(4) t3 时刻：接收端结束对染色报文的统计，并将统计到的染色报文的个数以及字节数上报给 Analyzer。

由于网络存在延时，为了最大程度地避免网络延时与乱序对统计结果的不良影响，接收端结束一个统计周期的时间要比发送端 t2 晚一点。t0～t3 为染色报文收包统计周期，在该时间段内，接收端的染色计数器只统计染色报文，以确保延迟到达的染色报文能被统计。

(5) t4 时刻：发送端结束一个周期的报文不染色，并将统计到的不染色报文的个数以及字节数上报给 Analyzer。同时开始染色报文的计数。接收端也开始统计染色报文。

(6) t5 时刻：接收端结束不染色报文的统计，并将统计到的不染色报文的个数以及字节数上报给 Analyzer。

t2～t5 为不染色报文收包统计周期，在该时间段内，接收端的不染色计数器只统计不染色报文，不会统计染色报文的数量。

2.3.3 工作流程

以图 4 所示组网为例，目标流经过网络中的三台设备，在这三台设备上部署 Collector 和 NTP 客户端，在汇聚设备上部署 Analyzer 和 NTP 服务器，测量流量从 MP 100 进入、途经 MP 200 的时候是否存在丢包，以及从 MP 300 流出时是否存在丢包。

iNQA 的工作流程如下：

(1) Analyzer 和所有 Collector 之间通过 NTP 或者 PTP 协议完成时间的同步，本文中以 NTP 为例。

(2) Collector 1 在报文入 MP 上根据匹配规则，从业务流中筛选出目标流，对报文进行一个周期染色一个周期不染色的交替动作，同时按周期对报文计数并上报给 Analyzer。

(3) Collector 2 在中间 MP 上根据匹配规则，从业务流中筛选出目标流，按周期对报文计数并上报给 Analyzer。

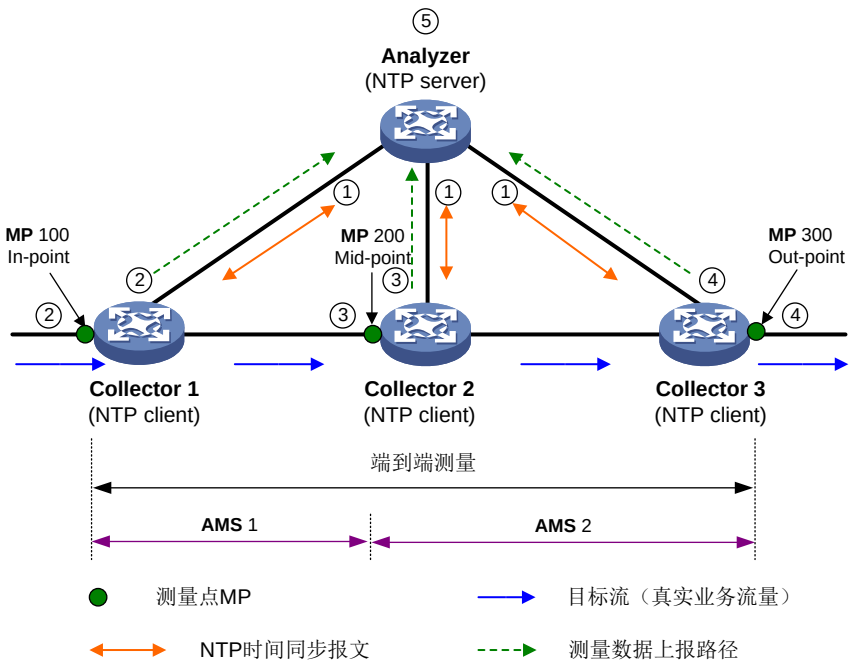
(4) Collector 3 在报文出 MP 上根据匹配规则，从业务流中筛选出目标流，对染色报文进行去染色操作，按周期对报文计数并上报给 Analyzer。

(5) Analyzer 对相同周期、相同实例、相同流量进行丢包分析，计算丢失的报文数、报文的丢失率、丢失的字节数、字节的丢失率。

丢失的报文数＝入口总报文个数－出口总报文个数，报文的丢失率＝丢失的报文数/入口总报文个数；丢失的字节数＝入口总字节数－出口总字节数，字节的丢失率＝丢失的字节数/入口总字节数。

- MP 100 收到的报文计数减去 MP 300 收到的报文计数为网络入口到出口的丢包情况。
- MP 100 收到的报文计数减去 MP 200 收到的报文计数为 AMS 1 的丢包情况。
- MP 200 收到的报文计数减去 MP 300 收到的报文计数为 AMS 2 的丢包情况。

图4 iNQA 工作流程示意图



2.4 应用限制

iNQA 依赖于时间同步功能，只有时间同步完成了，Analyzer 以及所有 Collector 才能进行同一个周期内报文的染色和测量。如果时间未同步，会导致 iNQA 计算结果不准确。可使用 NTP 或 PTP 进行时间同步。

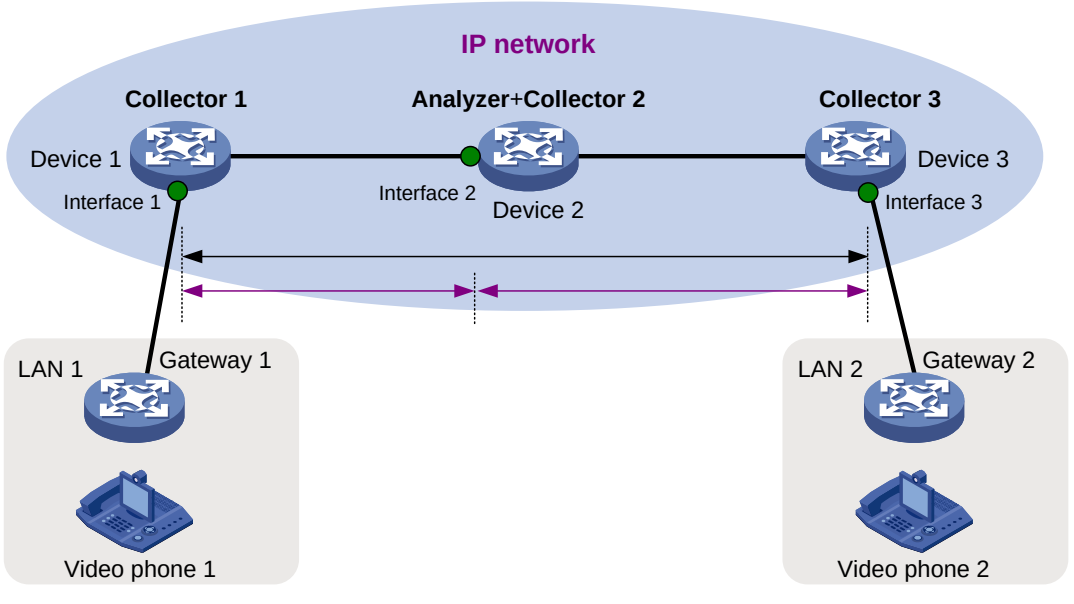
3 典型组网应用

3.1 iNQA点到点丢包测量

如图 5 所示，当 Video phone 1 和 Video phone 2 在进行视频通话时发现视频有马赛克现象，可使用 iNQA 来测试 IP 网络的丢包率，确认视频流量在穿越 IP 承载网络时，是否存在严重丢包，协助用户定位网络问题。

- 用户可先测试整个 IP 网络的丢包率，即 Interface 1 和 Interface 3 之间的丢包率。
- 如果 Interface 1 和 Interface 3 之间的丢包率较高，可进一步测量 Interface 1 和 Interface 2、Interface 2 和 Interface 3 之间的丢包率，从而确定故障发生的网络区段。

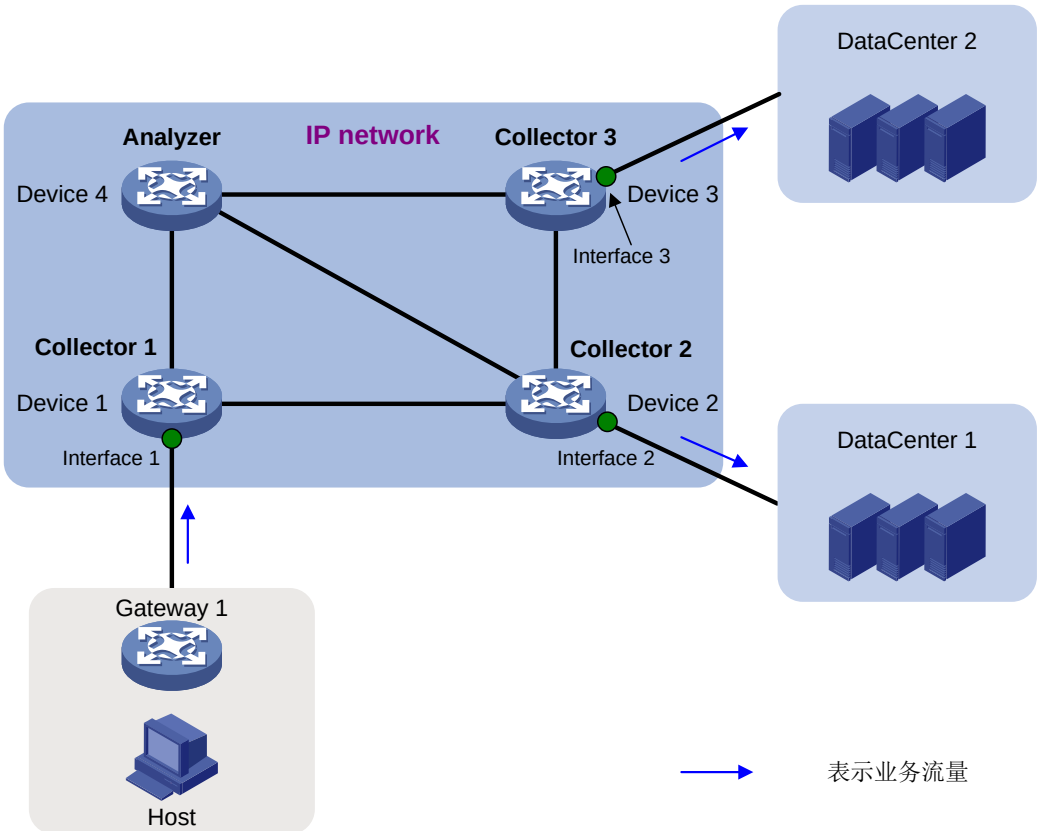
图5 iNQA 点到点丢包测量组网图



3.2 iNQA点到多点丢包测量

如图 6 所示，数据中心使用负载分担技术将数据存储在 DataCenter1 和 DataCenter2，Host 将数据保存到数据中心后发现部分信息丢失。通过部署 iNQA 功能，可测量数据从 Interface 1 进入 IP 网络，从 Interface 2、Interface 3 出 IP 网络时是否有丢包，协助用户定位网络问题。

图6 iNQA 点到多点丢包测量组网图



iNQA 配置

目 录

1 iNQA

1.1 iNQA配置限制和指导

1.1.1 iNQA 对配置的要求和限制

Analyzer 是根据 Collector 上报的统计数据进行汇总和计算的，如果 Analyzer 实例未正确关联 Collector 或关联的 Collector 未按时上报统计数据，那么 Analyzer 会将其统计数据按 0 计算。例如：只配置了 In-point MP，没有配置 Out-point MP，那么在 Analyzer 统计的时候，Out-point MP 的值就是 0，此时丢包率为 100%。

iNQA 使用 Collector ID 标识 Collector。对于同一台 Collector，Collector 上定义的 ID 和 Analyzer 上绑定的 Collector ID 必须一致。该标识为 Collector 上已经配置的 IPv4 地址，该地址和 Analyzer 之间必须路由可达。Collector 标识必须全网唯一，建议配置为 Collector 的 Router ID。

iNQA 使用 Analyzer ID 标识 Analyzer。对于同一台 Analyzer，Analyzer 上定义的 ID 和 Collector 上绑定的 Analyzer ID 必须一致。该标识为 Analyzer 上已经配置的 IPv4 地址，该地址和 Collector 之间必须路由可达。Analyzer 标识必须全网唯一，建议配置为 Analyzer 的 Router ID。

请使用同一实例对同一目标流进行统计，即用于统计同一目标流的 Analyzer 和 Collector 上的实例编号必须相同，目标流的匹配规则和统计周期必须相同。

1.1.2 iNQA 对网络的要求和限制

参与同一目标流测量的所有 MP 绑定的物理接口所属网络类型必须相同，例如均为 IP 网络或者均为 VXLAN 网络等。因为：

- iNQA 统计的是目标流报文的个数和整个报文的字节数（包括报文头和数据部分）。如果报文头在传输过程中被修改了，例如添加或删除了 VLAN tag，可能会导致 iNQA 统计结果不准确。
- iNQA 根据报文头中指定字段的取值匹配目标流。如果报文在传输过程中被封装或者解封装了，例如入 MP 在 IP 网络、出 MP 在 VXLAN 网络，可能会使得 iNQA 无法准确匹配到目标流，从而导致 iNQA 统计结果不准确。

iNQA 支持对已知 IPv4 单播报文进行丢包统计。对于未知 IP 单播、广播和组播报文，可能会因为设备将一份入报文复制成了多份出报文，导致统计结果错误。

1.1.3 iNQA 与其它软件特性的兼容性与限制

当在聚合口上应用 iNQA 功能时，在成员接口加入聚合组后，可能会因设备 ACL 资源不足导致聚合口上的 iNQA 功能异常，此时可适当减少聚合口的成员接口数，或等其他功能模块释放 ACL 资源后再按需加入新的成员接口。设备 ACL 资源使用情况可通过 **display qos-acl resource** 命令查看。有关 **display qos-acl resource** 命令的介绍，请参见“ACL 和 QoS 命令参考”中的“ACL”。

当在二层聚合接口上应用 iNQA 功能时，为确保 iNQA 功能正常，不建议通过 **port s-mlag group** 命令将该聚合接口加入 S-MLAG 组。有关 **port s-mlag group** 命令的介绍，请参见“二层技术-以太网交换命令参考”中的“以太网链路聚合”。

当设备上开启了 ECN（Explicit Congestion Notification，显示拥塞通知）功能时，请勿使用 ToS 字段的第 6 和 7 比特位作为 iNQA 染色位；反之，使用 ToS 字段的第 6 和 7 比特位作为 iNQA 染色位时，请不要开启 ECN 功能。有关 ECN 的详细介绍，请参见“ACL 和 QoS 配置指导”中的“拥塞避免”。

1.2 iNQA配置任务简介

iNQA 配置任务如下：

- 配置 Collector
  - 配置 Collector 全局参数
  - 配置 Collector 实例
  - 配置 MP

1.3 配置准备

在配置 iNQA 前，请完成 NTP 或者 PTP 的配置，使得 Analyzer 和所有 Collector 时间同步。关于 NTP 功能的具体配置请参见“网络管理和监控配置指导”中的“NTP”，关于 PTP 功能的具体配置请参见“网络管理和监控配置指导”中的“PTP”。

1.4 配置Collector

1.4.1 配置 Collector 全局参数

1. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启 Collector 功能并进入 Collector 视图。

inqa collector

缺省情况下，Collector 功能处于关闭状态。

(3) 配置 Collector 的标识。

collector id *collector-id*

缺省情况下，未配置 Collector 标识。

(4) 配置 iNQA 染色位。

flag loss-measure tos-bit *tos-bit*

缺省情况下，未配置 iNQA 染色位。

(5) 将 Collector 实例和全局 Analyzer 关联。

analyzer *analyzer-id* [**udp-port** *port-number*] [**vpn-instance** *vpn-instance-name*]

缺省情况下，Collector 实例未关联 Analyzer。

Collector 视图下关联的 Analyzer 对该 Collector 的所有实例生效；Collector 实例视图下关联的 Analyzer 仅对当前实例生效。Collector 实例视图下的配置优先。每个视图下只能关联一个 Analyzer，同一视图下，多次执行本命令，最后一次执行的命令生效。

1.4.2 配置 Collector 实例

1. 配置限制和指导

Analyzer 对多个 Collector 上的同一条目标流进行丢包统计时，Analyzer 和 Collector 上都需要创建实例，且统计实例的标识必须相同。

一个 Collector 实例下只能包含一条正向目标流、或者一条双向流、或者一条正向流加一条反向流。

- 如果目标流是一条流，用户只能通过指定 **forward** 配置成正向流。
- 如果目标流是两条流，且这两条流的两端设备相同，只是流向相反，一个流是从源 IP 到目的 IP，一条流的方向是目的 IP 到源 IP 时，用户需要指定 **bidirection** 配置成双向流，同时需要指定源 IP 和目的 IP。

- 如果目标流是两条流，且这两条流的两端设备不完全相同，则用户需要首先通过 **forward** 配置一条正向流，然后通过 **backward** 配置一条反向流。或者创建两个实例，每个实例下面配置一条正向流。

不同 Collector 实例中配置的目标流的流特征不能相同。

同一 Collector 实例中包含的正向流和反向流的流特征也不能相同，如果正向流和反向流除了方向，其他流特征相同，请配置为双向流。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 Collector 视图。

inqa collector

(3) 创建 Collector 实例并进入实例视图。如果实例已经创建，则直接进入该实例视图。

instance *instance-id*

(4) 将 Collector 实例和 Analyzer 关联。

analyzer *analyzer-id* [**udp-port** *port-number*] [**vpn-instance** *vpn-instance-name*]

缺省情况下，未配置 Collector 实例关联的 Analyzer。

Collector 视图下关联的 Analyzer 对该 Collector 的所有实例生效；Collector 实例视图下关联的 Analyzer 仅对当前实例生效。Collector 实例视图下的配置优先。每个视图下只能关联一个 Analyzer，同一视图下，多次执行本命令，最后一次执行的命令生效。

(5) 指定 Collector 实例统计的目标流。

flow { **backward** | **bidirection** | **forward** } { **destination-ip** *dest-ip-address* [*dest-mask-length*] | **dscp** *dscp-value* | **protocol** { { **tcp** | **udp** } { **destination-port** *dest-port-number1* [**to** *dest-port-number2*] | **source-port** *src-port-number1* [**to** *src-port-number2*] } * | *protocol-number* } | **source-ip** *src-ip-address* [*src-mask-length*] } *

缺省情况下，未配置 Collector 实例中的目标流。

(6) 配置 Collector 实例的统计周期。

interval *interval*

缺省情况下，Collector 实例的统计周期为 10 秒。

同一个统计系统中的所有 Collector 上的统计周期要保持一致。

统计周期在 Collector 实例开启时不允许修改，此时如果需要修改统计周期，必须先在该实例视图下关闭统计功能，且必须同步修改相同统计系统包含的所有 Collector 的统计周期。

(7) （可选）配置 Collector 实例的描述信息。

description *text*

缺省情况下，没有配置 Collector 实例的描述信息。

1.4.3 配置 MP

(1) 进入系统视图。

system-view

(2) 进入 Collector 视图。

inqa collector

(3) 进入实例视图。

instance *instance-id*

(4) 创建 MP。

mp *mp-id* { **in-point** | **mid-point** | **out-point** } **port-direction** { **inbound** | **outbound** }

缺省情况下，不存在 MP。

(5) 退回 Collector 视图。

quit

(6) 退回系统视图。

quit

(7) 进入接口视图。

interface *interface-type interface-number*

(8) 配置 MP 和接口的绑定关系。

inqa mp *mp-id*

缺省情况下，接口未绑定 MP。

1.4.4 开启 Collector 实例的丢包统计功能

1. 功能简介

按照丢包统计时间的长短，Collector 实例的丢包统计功能可以分为：

- 按需丢包统计功能

  当用户需要统计特定时间段的网络性能时，或者已知网络有丢包，想准确定位网络故障点时，可以开启按需丢包统计功能。iNQA 会统计指定时间段的丢包信息。

- 持续丢包统计功能

  为了防止出现网络丢包而用户无法感知的情况，可以开启持续丢包统计功能。iNQA 会一直统计丢包信息，直到关闭丢包统计功能为止。

2. 配置限制和指导

不能同时开启按需丢包统计功能和持续丢包统计功能，请根据业务需要，选择一种进行配置。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 Collector 视图。

inqa collector

(3) 进入实例视图。

instance *instance-id*

(4) 开启 Collector 实例的按需丢包统计功能。

非中间节点上的配置：

loss-measure enable duration [*duration*]

中间节点上的配置：

loss-measure enable mid-point duration [*duration*]

缺省情况下，Collector 实例的按需丢包统计功能处于关闭状态。

只有逐点丢包统计场景中才需要配置中间节点。

(5) 开启 Collector 实例的续丢包统计功能。

loss-measure enable continual

缺省情况下，Collector 实例的持续丢包统计功能处于关闭状态。

1.5 配置Analyzer

1.5.1 配置 Analyzer 全局参数

(1) 进入系统视图。

system-view

(2) 开启 Analyzer 功能并进入 Analyzer 视图。

inqa analyzer

缺省情况下，Analyzer 功能处于关闭状态。

(3) 在 Analyzer 设备上配置 Analyzer 的标识。

analyzer id *analyzer-id*

缺省情况下，没有配置 Analyzer 标识。

(4) （可选）配置 Analyzer 和 Collector 之间通信时使用的 UDP 端口号。

protocol udp-port *port-number*

缺省情况下，Analyzer 和 Collector 之间通信时使用的 UDP 端口号是 53312。

1.5.2 配置 Analyzer 实例

(1) 进入系统视图。

system-view

(2) 进入 Analyzer 视图。

inqa analyzer

(3) 创建 Analyzer 实例，并进入 Analyzer 实例视图。

instance *instance-id*

(4) （可选）配置 Analyzer 实例的描述信息。

description *text*

缺省情况下，未配置 Analyzer 实例的描述信息。

(5) 在 Analyzer 上将 Analyzer 实例和 Collector 关联。

collector *collector-id*

缺省情况下，Analyzer 实例未关联 Collector。

1.5.3 配置 AMS

1. 功能简介

端到端丢包统计场景无需配置 AMS，逐点丢包统计场景中必须配置 AMS。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 Analyzer 视图。

inqa analyzer

(3) 进入 Analyzer 实例视图。

instance *instance-id*

(4) 创建 AMS，并进入 AMS 视图。

ams *ams-id*

(5) 配置逐点丢包统计的目标流方向。

flow { **backward** | **bidirection** | **forward** }

缺省情况下，未配置 Analyzer 要统计的目标流的方向。

(6) 配置 AMS 的入 MP 组。

in-group collector *collector-id* **mp** *mp-id*

缺省情况下，未配置 AMS 的入 MP 组。

(7) 配置 AMS 的出 MP 组。

out-group collector *collector-id* **mp** *mp-id*

缺省情况下，未配置 AMS 的出 MP 组。

1.5.4 开启 Analyzer 实例的丢包统计功能

(1) 进入系统视图。

system-view

(2) 进入 Analyzer 视图。

inqa analyzer

(3) 进入 Analyzer 实例视图。

instance *instance-id*

(4) 开启 Analyzer 实例的统计功能。

measure enable

缺省情况下，Analyzer 实例的统计功能处于关闭状态。

1.6 配置iNQA日志功能

1. 功能简介

开启丢包统计，并配置本功能后，iNQA 会按周期统计丢包率：

- 如果连续五个周期的丢包率都大于等于丢包超限阈值，表示该实例中丢包过多，Analyzer 会生成丢包超限日志。
- 如果连续五个周期的丢包率都小于丢包超限恢复阈值，表示该实例中丢包率已经恢复到正常范围，Analyzer 会生成丢包恢复日志。

iNQA 日志将被发送到设备的信息中心，并通过信息中心配置的参数，最终决定 iNQA 日志的输出规则（即是否允许输出以及输出方向）。有关信息中心的详细介绍请参见“网络管理和监控配置指导”中的“信息中心”。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 Analyzer 视图。

inqa analyzer

(3) 进入 Analyzer 实例视图。

instance *instance-id*

(4) 配置 Analyzer 实例的丢包日志参数。

loss-measure alarm upper-limit *upper-limit* **lower-limit** *lower-limit*

缺省情况下，未配置 Analyzer 实例的丢包日志参数，Analyzer 不会自动发送丢包超限日志及其恢复日志。

1.7 Collector显示和维护

在 Collector 上完成 Collector 的配置后，在任意视图下执行 **display** 命令，均可以显示配置后 Collector 的运行情况，通过查看显示信息，来验证配置的效果。

表1-1 Collector 显示和维护

操作	命令
显示Collector的配置信息	**display inqa collector**
显示Collector实例的配置信息	**display inqa collector instance** { *instance-id* | **all** }

1.8 Analyzer显示和维护

在 Analyzer 上完成 Analyzer 的配置后，在任意视图下执行 **display** 命令，均可以显示配置后 Analyzer 的运行情况，通过查看显示信息，来验证配置的效果。

表1-2 Analyzer 显示和维护

操作	命令
显示Analyzer的配置信息	**display inqa analyzer**
显示Analyzer实例的配置信息	**display inqa analyzer instance** { *instance-id* | **all** }
显示Analyzer实例下AMS的配置信息	**display inqa analyzer instance** *instance-id* **ams** { *ams-id* | **all** }
显示iNQA丢包统计信息	**display inqa statistics loss instance** *instance-id* [**ams** *ams-id*]

1.9 iNQA典型配置举例

1.9.1 iNQA 端到端丢包统计配置举例

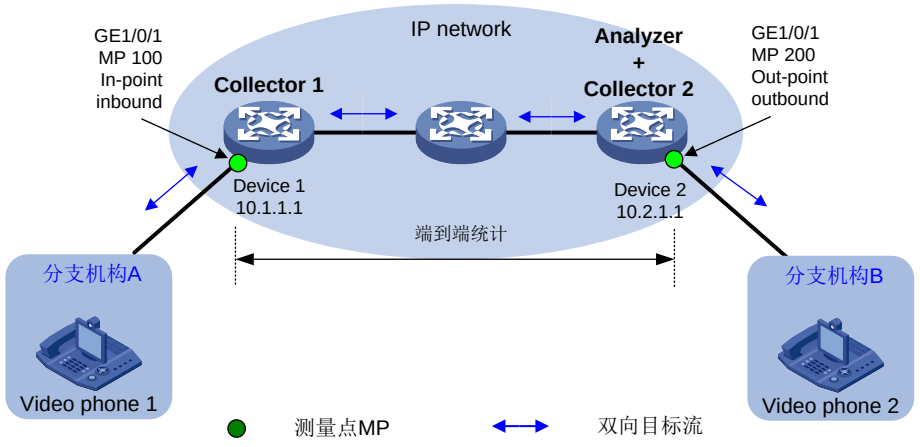
1. 组网需求

如图 1-1 所示，Video phone 1 和 Video phone 2 在进行视频通话时发现视频有马赛克现象，需要确认视频流量在穿越 IP 承载网络时，是否存在严重丢包现象，协助用户定位网络问题：

- 在 IP 网络的入口设备 Device 1 和出口设备 Device 2 上部署 iNQA 功能。Device 1 为 Collector 1；Device 2 同时作为 Collector 2 和 Analyzer。Device 1 到 Device 2 的方向为正向。测量 MP 100 到 MP 200 之间的双向丢包率。
- 为了方便用户及时感知网络故障的发生，配置丢包超限阈值为 6%，丢包超限恢复阈值为 4%。当丢包率到达阈值时，设备自动生成对应的日志。

2. 组网图

图1-1 iNQA 端到端丢包统计组网图



3. 配置准备

(1) 配置 IP 地址和单播路由协议

在 Collector 1 上配置地址 10.1.1.1，在 Collector 2 上配置地址 10.2.1.1。

在 IP 网络内配置 OSPF 协议，使 Collector 1（IP 地址 10.1.1.1）和 Analyzer（IP 地址 10.2.1.1）之间路由可达，具体配置过程略。

(2) 配置 NTP 或者 PTP

在 Collector 1 和 Collector 2 上配置 NTP 或者 PTP 功能，使得 Collector 1 和 Collector 2 之间的时间达到同步，具体配置过程略。

4. 配置 Collector 1

(1) 配置 Collector 1 全局参数：Collector 标识为 10.1.1.1，和 Analyzer 10.2.1.1 绑定，将 ToS 字段的第 6 比特位作为 iNQA 染色位。

```
<Collector1> system-view
[Collector1] inqa collector
[Collector1-inqa-collector] collector id 10.1.1.1
[Collector1-inqa-collector] analyzer 10.2.1.1
[Collector1-inqa-collector] flag loss-measure tos-bit 6
```

(2) 配置 Collector 实例 1：该实例用于统计 10.1.1.0/24 到 10.2.1.0/24 的双向丢包率，流量入接口为 GigabitEthernet1/0/1，并开启持续丢包统计功能。

```
[Collector1-inqa-collector] instance 1
[Collector1-inqa-collector-instance-1] flow bidirection source-ip 10.1.1.0 24 destination-ip 10.2.1.0 24
[Collector1-inqa-collector-instance-1] mp 100 in-point port-direction inbound
[Collector1-inqa-collector-instance-1] quit
[Collector1-inqa-collector] quit
[Collector1] interface gigabitethernet 1/0/1
[Collector1-GigabitEthernet1/0/1] inqa mp 100
[Collector1-GigabitEthernet1/0/1] quit
[Collector1] inqa collector
[Collector1-inqa-collector] instance 1
[Collector1-inqa-collector-instance-1] loss-measure enable continual
[Collector1-inqa-collector-instance-1] quit
[Collector1-inqa-collector] quit
```

5. 配置 Collector 2+Analyzer

(1) 配置 Collector 2 全局参数：Collector 标识为 10.2.1.1，和 Analyzer 10.2.1.1 绑定，将 ToS 字段的第 6 比特位作为 iNQA 染色位。

```
<AnalyzerColl2> system-view
```

```
[AnalyzerColl2] inqa collector
[AnalyzerColl2-inqa-collector] collector id 10.2.1.1
[AnalyzerColl2-inqa-collector] analyzer 10.2.1.1
[AnalyzerColl2-inqa-collector] flag loss-measure tos-bit 6
```

(2) 配置 Collector 实例 1：该实例用于统计 10.1.1.0/24 到 10.2.1.0/24 的双向丢包率，流量入接口为 GigabitEthernet1/0/1，并开启持续丢包统计功能。

```
[AnalyzerColl2-inqa-collector] instance 1
[AnalyzerColl2-inqa-collector-instance-1] flow bidirection source-ip 10.1.1.0 24 destination-ip 10.2.1.0 24
[AnalyzerColl2-inqa-collector-instance-1] mp 200 out-point port-direction outbound
[AnalyzerColl2-inqa-collector-instance-1] quit
[AnalyzerColl2-inqa-collector] quit
[AnalyzerColl2] interface gigabitethernet 1/0/1
[AnalyzerColl2-GigabitEthernet1/0/1] inqa mp 200
[AnalyzerColl2-GigabitEthernet1/0/1] quit
[AnalyzerColl2] inqa collector
[AnalyzerColl2-inqa-collector] instance 1
[AnalyzerColl2-inqa-collector-instance-1] loss-measure enable continual
[AnalyzerColl2-inqa-collector-instance-1] quit
[AnalyzerColl2-inqa-collector] quit
```

(3) 配置 Analyzer 全局参数：Analyzer 标识为 10.2.1.1。

```
[AnalyzerColl2] inqa analyzer
[AnalyzerColl2-inqa-analyzer] analyzer id 10.2.1.1
```

(4) 配置 Analyzer 实例 1：和 Collector 1 10.1.1.1、Collector 2 10.2.1.1 绑定；丢包超限阈值为 6%，丢包超限恢复阈值为 4%；开启统计功能。

```
[AnalyzerColl2-inqa-analyzer] instance 1
[AnalyzerColl2-inqa-analyzer-instance-1] collector 10.1.1.1
[AnalyzerColl2-inqa-analyzer-instance-1] collector 10.2.1.1
[AnalyzerColl2-inqa-analyzer-instance-1] loss-measure alarm upper-limit 6 lower-limit 4
[AnalyzerColl2-inqa-analyzer-instance-1] measure enable
[AnalyzerColl2-inqa-analyzer-instance-1] quit
[AnalyzerColl2-inqa-analyzer] quit
```

6. 验证配置

(1) 在 Collector 1 上验证配置

查看 Collector 的配置。

```
[Collector1] display inqa collector
Collector ID             : 10.1.1.1
Loss-measure flag        : 6
Analyzer ID              : 10.2.1.1
Analyzer UDP-port        : 53312
VPN-instance-name        : --
Current instance count   : 1
```

查看 Collector 实例 1 的配置。

```
[Collector1] display inqa collector instance 1
Instance ID              : 1
Status                   : Enabled
Duration                 : --
Description              : --
Analyzer ID              : --
Analyzer UDP-port        : --
```

```
VPN-instance-name       : --
Interval                : 10 sec
Flow configuration:
  flow bidirection source-ip 10.1.1.0 24 destination-ip 10.2.1.0 24
MP configuration:
  mp 100 in-point inbound, GE1/0/1
```

(2) 在 Collector 2+Analyzer 上验证配置

查看 Collector 的配置。

```
[AnalyzerColl2] display inqa collector
Collector ID            : 10.2.1.1
Loss-measure flag       : 6
Analyzer ID             : 10.2.1.1
Analyzer UDP-port       : 53312
VPN-instance-name       : --
Current instance count  : 1
```

查看 Collector 实例 1 的配置。

```
[AnalyzerColl2] display inqa collector instance 1
Instance ID             : 1
Status                  : Enabled
Duration                : --
Description             : --
Analyzer ID             : --
Analyzer UDP-port       : --
VPN-instance-name       : --
Interval                : 10 sec
Flow configuration:
  flow bidirection source-ip 10.1.1.0 24 destination-ip 10.2.1.0 24
MP configuration:
  mp 200 out-point outbound, GE1/0/1
```

查看 Analyzer 的配置。

```
[AnalyzerColl2] display inqa analyzer
Analyzer ID             : 10.2.1.1
Protocol UDP-port       : 53312
Current instance count  : 1
```

查看 Analyzer 实例 1 的配置。

```
<AnalyzerColl2] display inqa analyzer instance 1
Instance ID             : 1
Status                  : Enable
Description             : --
Alarm upper-limit       : 6.000000%
Alarm lower-limit       : 4.000000%
Current AMS count       : 0
Collectors              : 10.1.1.1
                          10.2.1.1
```

查看 Analyzer 实例 1 的丢包统计结果。

```
[AnalyzerColl2] display inqa statistics loss instance 1
Latest packet loss statistics for forward flow:
 Period     LostPkts             PktLoss%     LostBytes            ByteLoss%
 19122483   15                   15.000000%   1500                 15.000000%
 19122482   15                   15.000000%   1500                 15.000000%
```

19122481	15	15.000000%	1500	15.000000%
19122480	15	15.000000%	1500	15.000000%
19122479	15	15.000000%	1500	15.000000%
19122478	15	15.000000%	1500	15.000000%

Latest packet loss statistics for backward flow:

Period	LostPkts	PktLoss%	LostBytes	ByteLoss%
19122483	15	15.000000%	1500	15.000000%
19122482	15	15.000000%	1500	15.000000%
19122481	15	15.000000%	1500	15.000000%
19122480	15	15.000000%	1500	15.000000%
19122479	15	15.000000%	1500	15.000000%
19122478	15	15.000000%	1500	15.000000%

1.9.2 iNQA 逐点丢包统计配置举例

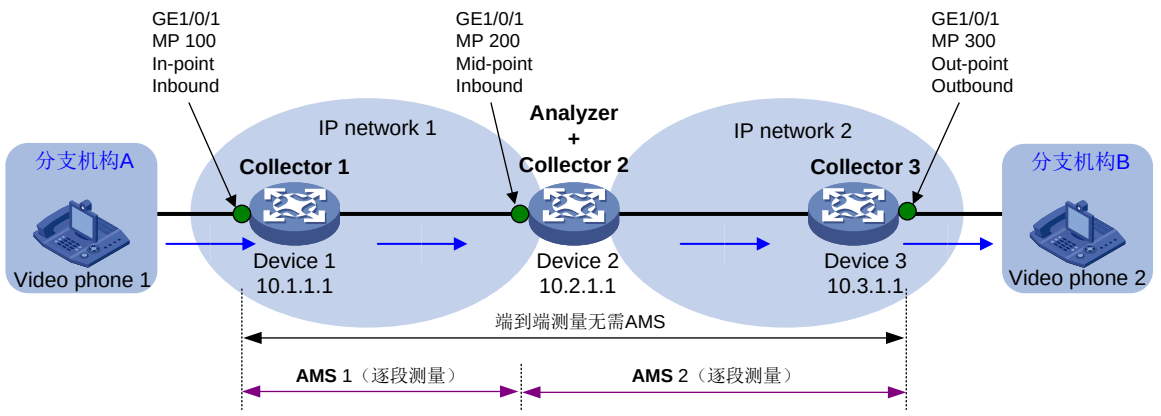
1. 组网需求

如图 1-2 所示，Video phone 1 和 Video phone 2 在进行视频通话时发现视频有马赛克现象，需要确认视频流量在穿越 IP 承载网络时，是否存在严重丢包现象，协助用户定位网络问题：

- 在 IP 网络的入口设备 Device 1 和出口设备 Device 3 上部署 iNQA 功能。Device 1 为 Collector 1；Device 2 同时作为 Collector 2 和 Analyzer；Device 3 为 Collector 3。Device 1 到 Device 3 的方向为正向。测量 MP 100 到 MP 300 之间的正向丢包率，以及 MP 100 到 MP 200、MP 200 到 MP 300 之间区间的正向丢包率。
- 持续测量 15 分钟。为了方便用户及时感知网络故障的发生，配置丢包超限阈值为 6%，丢包超限恢复阈值为 4%。当丢包率到达阈值时，设备自动生成对应的日志。

2. 组网图

图1-2 iNQA 逐点丢包统计组网图



3. 配置准备

(1) 配置 IP 地址和单播路由协议

在 Collector 1 上配置地址 10.1.1.1，在 Collector 2 上配置地址 10.2.1.1，在 Collector 3 上配置地址 10.3.1.1。

在 IP 网络内配置 OSPF 协议，使 Collector 1（IP 地址 10.1.1.1）、Collector 3（IP 地址 10.3.1.1）和 Analyzer（IP 地址 10.2.1.1）之间路由可达，具体配置过程略。

(2) 配置 NTP 或者 PTP

在 Collector 1、Collector 2 和 Collector 3 上配置 NTP 或者 PTP 功能，使得 Collector 1、Collector 2 和 Collector 3 之间的时间达到同步，具体配置过程略。

4. 配置 Collector 1

(1) 配置 Collector 1 全局参数：Collector 标识为 10.1.1.1，和 Analyzer 10.2.1.1 绑定，将 ToS 字段的第 6 比特位作为 iNQA 染色位。

```
<Collector1> system-view
[Collector1] inqa collector
[Collector1-inqa-collector] collector id 10.1.1.1
[Collector1-inqa-collector] analyzer 10.2.1.1
[Collector1-inqa-collector] flag loss-measure tos-bit 6
```

(2) 配置 Collector 实例 1：该实例用于统计 10.1.1.0/24 到 10.3.1.0/24 的正向丢包率，流量入接口为 GigabitEthernet1/0/1，并开启按需丢包统计功能 15 分钟。

```
[Collector1-inqa-collector] instance 1
[Collector1-inqa-collector-instance-1] flow forward source-ip 10.1.1.0 24 destination-ip 10.3.1.0 24
[Collector1-inqa-collector-instance-1] mp 100 in-point port-direction inbound
[Collector1-inqa-collector-instance-1] quit
[Collector1-inqa-collector] quit
[Collector1] interface gigabitethernet 1/0/1
[Collector1-GigabitEthernet1/0/1] inqa mp 100
[Collector1-GigabitEthernet1/0/1] quit
[Collector1] inqa collector
[Collector1-inqa-collector] instance 1
[Collector1-inqa-collector-instance-1] loss-measure enable duration 15
[Collector1-inqa-collector-instance-1] quit
[Collector1-inqa-collector] quit
```

5. 配置 Collector 2+Analyzer

(1) 配置 Collector 2 全局参数：Collector 标识为 10.2.1.1，和 Analyzer 10.2.1.1 绑定，将 ToS 字段的第 6 比特位作为 iNQA 染色位。

```
<AnalyzerColl2> system-view
[AnalyzerColl2] inqa collector
[AnalyzerColl2-inqa-collector] collector id 10.2.1.1
[AnalyzerColl2-inqa-collector] analyzer 10.2.1.1
[AnalyzerColl2-inqa-collector] flag loss-measure tos-bit 6
```

(2) 配置 Collector 实例 1：该实例用于统计 10.1.1.0/24 到 10.3.1.0/24 的正向丢包率，流量入接口为 GigabitEthernet1/0/1，并开启按需丢包统计功能 15 分钟。

```
[AnalyzerColl2-inqa-collector] instance 1
[AnalyzerColl2-inqa-collector-instance-1] flow forward source-ip 10.1.1.0 24 destination-ip 10.3.1.0 24
[AnalyzerColl2-inqa-collector-instance-1] mp 200 mid-point port-direction inbound
[AnalyzerColl2-inqa-collector-instance-1] quit
[AnalyzerColl2-inqa-collector] quit
[AnalyzerColl2] interface gigabitethernet 1/0/1
[AnalyzerColl2-GigabitEthernet1/0/1] inqa mp 200
[AnalyzerColl2-GigabitEthernet1/0/1] quit
[AnalyzerColl2] inqa collector
[AnalyzerColl2-inqa-collector] instance 1
[AnalyzerColl2-inqa-collector-instance-1] loss-measure enable mid-point duration 15
[AnalyzerColl2-inqa-collector-instance-1] quit
[AnalyzerColl2-inqa-collector] quit
```

(3) 配置 Analyzer 全局参数：Analyzer 标识为 10.2.1.1。

```
[AnalyzerColl2] inqa analyzer
[AnalyzerColl2-inqa-analyzer] analyzer id 10.2.1.1
```

(4) 配置 Analyzer 实例 1：和 Collector 1 10.1.1.1、Collector 2 10.2.1.1、Collector 3 10.3.1.1 绑定。

```
[AnalyzerColl2-inqa-analyzer] instance 1
```

```
[AnalyzerColl2-inqa-analyzer-instance-1] collector 10.1.1.1
[AnalyzerColl2-inqa-analyzer-instance-1] collector 10.2.1.1
[AnalyzerColl2-inqa-analyzer-instance-1] collector 10.3.1.1
```

(5) 配置 AMS 1，用于测量 MP 100 到 MP 200 之间的正向丢包率。

```
[AnalyzerColl2-inqa-analyzer-instance-1] ams 1
[AnalyzerColl2-inqa-analyzer-instance-1-ams-1] flow forward
[AnalyzerColl2-inqa-analyzer-instance-1-ams-1] in-group collector 10.1.1.1 mp 100
[AnalyzerColl2-inqa-analyzer-instance-1-ams-1] out-group collector 10.2.1.1 mp 200
[AnalyzerColl2-inqa-analyzer-instance-1-ams-1] quit
```

(6) 配置 AMS 2，用于测量 MP 200 到 MP 300 之间的正向丢包率。

```
[AnalyzerColl2-inqa-analyzer-instance-1] ams 2
[AnalyzerColl2-inqa-analyzer-instance-1-ams-2] flow forward
[AnalyzerColl2-inqa-analyzer-instance-1-ams-2] in-group collector 10.2.1.1 mp 200
[AnalyzerColl2-inqa-analyzer-instance-1-ams-2] out-group collector 10.3.1.1 mp 300
[AnalyzerColl2-inqa-analyzer-instance-1-ams-2] quit
```

(7) 配置 Analyzer 实例 1：丢包超限阈值为 6%，丢包超限恢复阈值为 4%；并开启按需丢包统计功能 15 分钟。

```
[AnalyzerColl2-inqa-analyzer-instance-1] loss-measure alarm upper-limit 6 lower-limit 4
[AnalyzerColl2-inqa-analyzer-instance-1] measure enable
[AnalyzerColl2-inqa-analyzer-instance-1] quit
[AnalyzerColl2-inqa-analyzer] quit
```

6. 配置 Collector 3

(1) 配置 Collector 3 全局参数：Collector 标识为 10.3.1.1，和 Analyzer 10.2.1.1 绑定，将 ToS 字段的第 6 比特位作为 iNQA 染色位。

```
<Collector3> system-view
[Collector3] inqa collector
[Collector3-inqa-collector] collector id 10.3.1.1
[Collector3-inqa-collector] analyzer 10.2.1.1
[Collector3-inqa-collector] flag loss-measure tos-bit 6
```

(2) 配置 Collector 实例 1：该实例用于统计 10.1.1.0/24 到 10.3.1.0/24 的正向丢包率，流量出接口为 GigabitEthernet1/0/1，并开启按需丢包统计功能 15 分钟。

```
[Collector3-inqa-collector] instance 1
[Collector3-inqa-collector-instance-1] flow forward source-ip 10.1.1.0 24 destination-ip 10.3.1.0 24
[Collector3-inqa-collector-instance-1] mp 300 out-point port-direction outbound
[Collector3-inqa-collector-instance-1] quit
[Collector3-inqa-collector] quit
[Collector3] interface gigabitethernet 1/0/1
[Collector3-GigabitEthernet1/0/1] inqa mp 300
[Collector3-GigabitEthernet1/0/1] quit
[Collector3] inqa collector
[Collector3-inqa-collector] instance 1
[Collector3-inqa-collector-instance-1] loss-measure enable duration 15
[Collector3-inqa-collector-instance-1] quit
[Collector3-inqa-collector] quit
```

7. 验证配置。

(1) 在 Collector 1 上验证配置

查看 Collector 的配置。

```
[Collector1] display inqa collector
Collector ID             : 10.1.1.1
Loss-measure flag        : 6
```

```
Analyzer ID              : 10.2.1.1
Analyzer UDP-port        : 53312
VPN-instance-name        : --
Current instance count   : 1
```

查看 Collector 实例 1 的配置。

```
[Collector1] display inqa collector instance 1
Instance ID              : 1
Status                   : Enabled
Duration                 : 15 min (Non mid-point)
Remaining time           : 14 min 52 sec
Description              : --
Analyzer ID              : --
Analyzer UDP-port        : --
VPN-instance-name        : --
Interval                 : 10 sec
Flow configuration:
  flow forward source-ip 10.1.1.0 24 destination-ip 10.3.1.0 24
MP configuration:
  mp 100 in-point inbound, GE1/0/1
```

(2) 在 Collector 2+Analyzer 上验证配置

查看 Collector 的配置。

```
[AnalyzerColl2] display inqa collector
Collector ID             : 10.2.1.1
Loss-measure flag        : 6
Analyzer ID              : 10.2.1.1
Analyzer UDP-port        : 53312
VPN-instance-name        : --
Current instance count   : 1
```

查看 Collector 实例 1 的配置。

```
[AnalyzerColl2>  display inqa collector instance 1
Instance ID              : 1
Status                   : Enabled
Duration                 : 15 min (Mid-point)
Remaining time           : 14 min 50 sec
Description              : --
Analyzer ID              : --
Analyzer UDP-port        : --
VPN-instance-name        : --
Interval                 : 10 sec
Flow configuration:
  flow forward source-ip 10.1.1.0 24 destination-ip 10.3.1.0 24
MP configuration:
  mp 200 mid-point inbound, GE1/0/1
```

查看 Analyzer 的配置。

```
[AnalyzerColl2] display inqa analyzer
Analyzer ID              : 10.2.1.1
Protocol UDP-port        : 53312
Current instance count   : 1
```

查看 Analyzer 实例 1 的配置。

```
<AnalyzerColl2] display inqa analyzer instance 1
```

```
Instance ID              : 1
Status                   : Enabled
Description              : --
Alarm upper-limit        : 6.000000%
Alarm lower-limit        : 4.000000%
Current AMS count        : 2
Collectors               : 10.1.1.1
                           10.2.1.1
                           10.3.1.1
```

查看 Analyzer 实例 1 下的 AMS 的配置。

```
[AnalyzerColl2] display inqa analyzer instance 1 ams all
AMS ID                   : 1
Flow direction           : forward
In-group                 : collector 10.1.1.1 mp 100
Out-group                : collector 10.2.1.1 mp 200

AMS ID                   : 2
Flow direction           : forward
In-group                 : collector 10.2.1.1 mp 200
Out-group                : collector 10.3.1.1 mp 300
```

查看 Analyzer 实例 1 AMS 1 的丢包统计结果。

```
[AnalyzerColl2] display inqa statistics loss instance 1 ams 1
Latest packet loss statistics for forward flow:
```

Period	LostPkts	PktLoss%	LostBytes	ByteLoss%
19122483	15	15.000000%	1500	15.000000%
19122482	15	15.000000%	1500	15.000000%
19122481	15	15.000000%	1500	15.000000%
19122480	15	15.000000%	1500	15.000000%
19122479	15	15.000000%	1500	15.000000%
19122478	15	15.000000%	1500	15.000000%

(3) 在 Collector 3 上验证配置

查看 Collector 的配置。

```
[Collector3] display inqa collector
Collector ID             : 10.3.1.1
Loss-measure flag        : 6
Analyzer ID              : 10.2.1.1
Analyzer UDP-port        : 53312
VPN-instance-name        : --
Current instance count   : 1
```

查看 Collector 实例 1 的配置。

```
[Collector3] display inqa collector instance 1
Instance ID              : 1
Status                   : Enabled
Duration                 : 15 min (Non mid-point)
Remaining time           : 14 min 51 sec
Description              : --
Analyzer ID              : --
Analyzer UDP-port        : --
VPN-instance-name        : --
Interval                 : 10 sec
```

```
Flow configuration:
  flow forward source-ip 10.1.1.0 24 destination-ip 10.3.1.0 24
MP configuration:
  mp 300 out-point outbound, GE1/0/1
```

TWAMP Light 技术白皮书

目 录

1 概述

1.1 产生背景

随着网络技术的飞速发展，网络中承载的业务越来越多，语音、视频、游戏等业务对网络丢包和时延要求越来越高。网络管理者需要一种测量工具来及时了解网络的丢包和时延情况，以便根据测试结果进行网络调整和优化，满足业务需求。

TWAMP（Two-Way Active Measurement Protocol，双向主动测量协议）用来测量网络中任意两台设备之间报文的双向时延、时延抖动、丢包率等性能参数，为网络质量分析提供依据。

TWAMP 协议定义了两种架构：标准框架和轻量级架构。TWAMP Light 是 TWAMP 协议的轻量级架构，简化了建立性能测量会话的控制协议，提高了测试性能，越来越多的厂家青睐并支持 TWAMP Light 技术。

1.2 技术优点

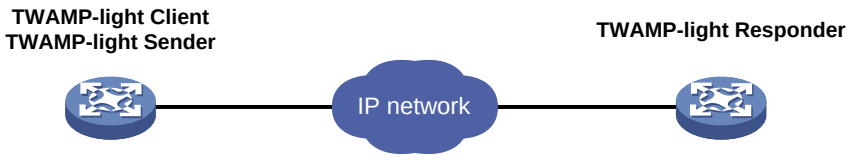
常见的丢包、时延测量技术包括 NQA（Network Quality Analyzer，网络质量分析）和 RFC 6374/6375（MPLS 网络的丢包和时延测量）等。与这些技术相比，TWAMP Light 技术具有以下优点：

- TWAMP Light 是 IPPM（IP performance monitoring，IP 性能监控）工作组定义的 IP 网络性能统计协议，具有统一的检测模型、统一的报文格式，不同厂商的设备之间可以互通。
- TWAMP Light 能够部署在 IP、MPLS、L3VPN（Layer 3 Virtual Private Network，三层虚拟专用网）等网络，满足不同类型网络的测量需求。
- TWAMP Light 测试包含客户端（测试源端）和服务器端（测试目的端），只需在客户端生成和维护性能测量数据，服务器端无需生成和维护性能测量数据，方便网管设备快速获取测量数据。
- 与 TWAMP 标准架构相比，TWAMP Light 将服务器端的部分功能移到客户端实现，简化了建立性能测量会话的控制协议，大大降低了对服务器端的能力要求，有助于服务器端的快速部署。

2 TWAMP Light 技术实现

2.1 网络架构

图1 TWAMP Light 网络架构示意图



如图 1 所示，TWAMP Light 网络模型中包含了以下角色：

- TWAMP Light 在测试源端设备上定义了两个角色：
  - TWAMP-light Client：负责配置 TWAMP-light 测试会话。
  - TWAMP-light Sender：负责启动、停止 TWAMP-light 测试会话，是 TWAMP-light 测试的源端设备。
- TWAMP Light 在测试目的端设备上定义了 TWAMP-light Responder。

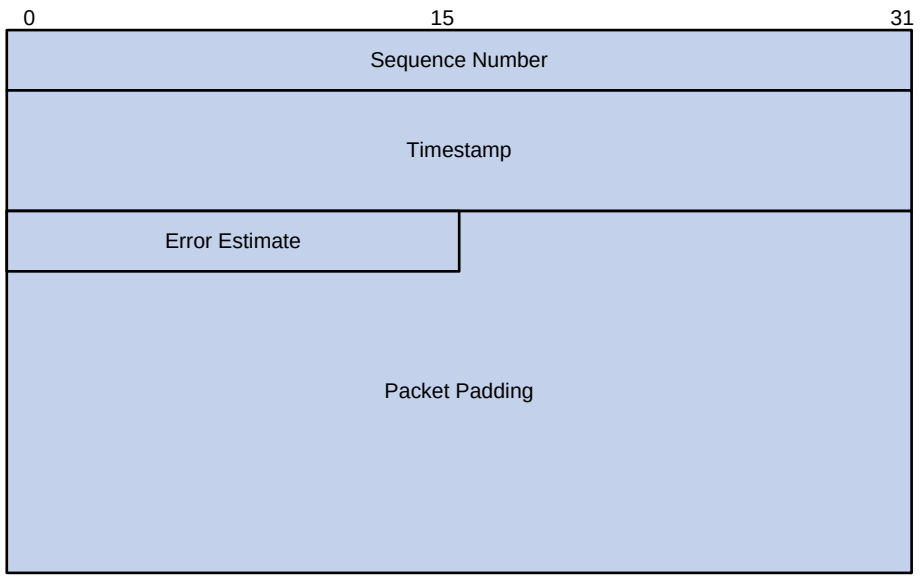
  Responder 是 TWAMP-light 测试的目的端设备，负责将会话测试报文反射回去。

2.2 报文格式

TWAMP-light 测试定义了 Test-request 和 Test-response 两种报文。

1. Test-request 报文格式

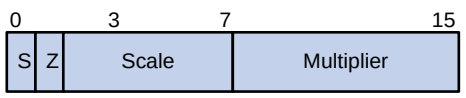
图2 Test-request 报文格式示意图



TWAMP-light Sender 发送 Test-request 报文，报文中各字段含义如下：

- Sequence Number：报文发送序列号。
- Timestamp：发送报文的时间戳，支持 PTP 和 NTP 两种时间戳格式，具体采用哪种格式由 Error Estimate 字段中“Z”区域的取值决定。
- Error Estimate：误差估计，单位为秒。如图 3 所示，误差估计由以下几个部分组成：
  - S：取值为 0，表示没有外接时钟。
  - Z：时间戳的格式，0 表示 NTP 格式，1 表示 PTP 格式。
  - Scale：取值为 0x3F。
  - Multiplier：取值为 0xFF。

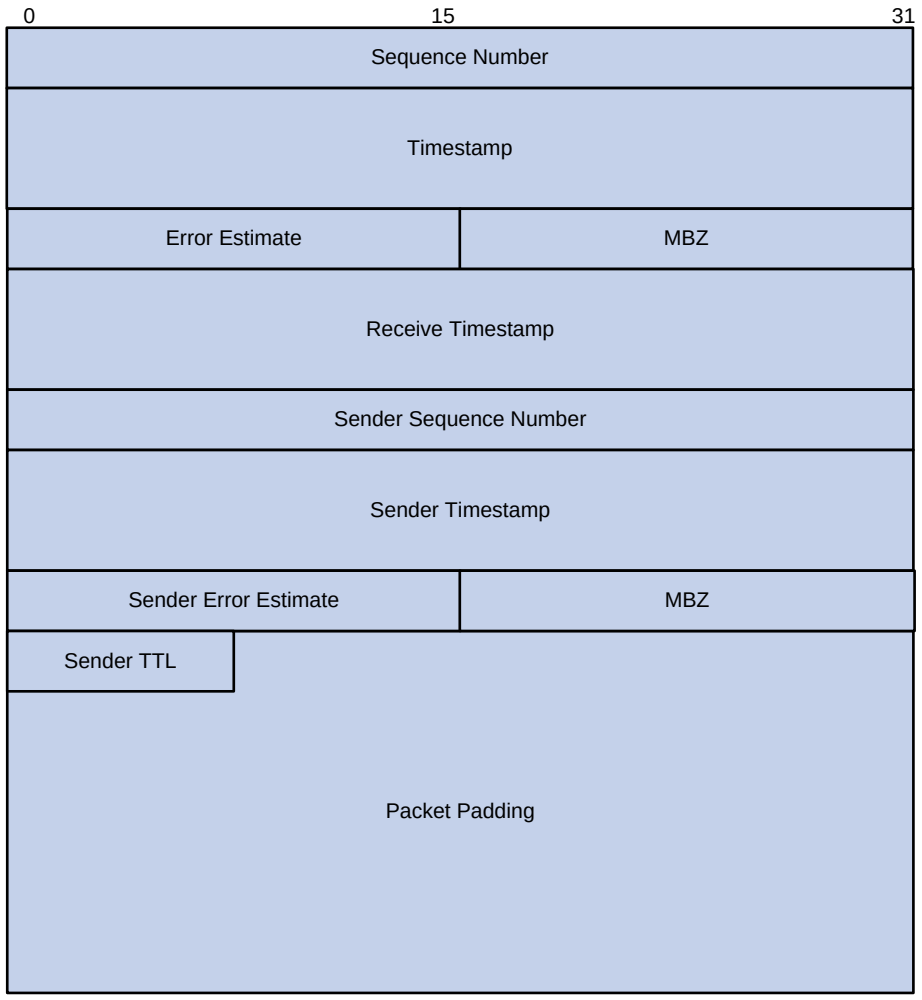
  图3 Error Estimate 字段结构示意图

- Packet Padding：报文的填充字段，随机填充数据。

2. Test-response 报文格式

图4 Test-response 报文格式示意图



TWAMP-light Responder 收到 Test-request 报文后，回应 Test-response 报文。报文中各字段含义如下：

- Sequence Number：报文发送序列号，取值为 Responder 实际发送报文的序列号。
- Timestamp：发送报文时的时间戳，支持 PTP 和 NTP 两种时间戳格式，具体采用哪种格式由 Error Estimate 字段中“Z”区域的取值决定。
- Error Estimate：误差估计，单位为秒，填充方法同 Test-request 报文。
- MBZ：Must be zero，取值必须为 0。
- Receive Timestamp：接收报文时的时间戳，支持 PTP 和 NTP 两种时间戳格式，具体采用哪种格式由 Error Estimate 字段中“Z”区域的取值决定。
- Sender Sequence Number：请求报文的序列号，该值拷贝自对应 Test-request 报文中的 Sequence Number 字段。
- Sender Timestamp：请求报文中的时间戳，该值拷贝自对应 Test-request 报文中的 Timestamp 字段。
- Sender Error Estimate：请求报文中的误差估计，单位为秒，该值拷贝自对应 Test-request 报文中的 Error Estimate 字段。
- Sender TTL：请求报文中的 TTL，该值拷贝自对应 Test-request 报文中的 TTL 字段。
- Packet Padding：报文的填充字段，随机填充数据。

2.3 测量机制

2.3.1 TWAMP Light 测量机制概述

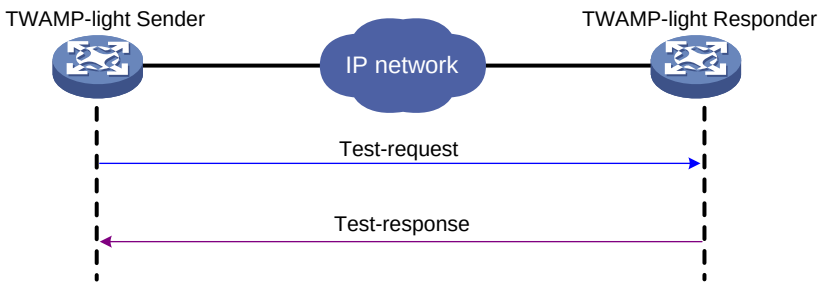
如图 5 所示，TWAMP-light 测量机制大致如下：

(1) Sender 使用预先设置好的 IP 地址、UDP 端口号等参数，构造测试报文（Test-request），每隔一段时间进行一次测试，每次测试发送一个 Test-request 报文给 Responder。

(2) Responder 收到探测报文后，构造反射报文（Test-response），填充时间戳和 TTL 等信息，将报文反射回 Sender。

(3) Sender 根据收到 Test-response 报文的个数，以及接收 Test-response 的时间，计算 Test-request 报文的丢失率、往返时延和时延抖动，从而判断源端到目的端、目的端到源端链路质量的好坏。

图5 TWAMP Light 测量机制示意图



2.3.2 丢包测量机制

如图 6 所示，TWAMP Light 丢包测量过程如下：

(1) t0 时刻：Sender 开始第一个发包统计周期的发包（以指定的发包间隔持续发送测试报文 Test-request）和计数，并开始第一个收包统计周期的收包（接收 Responder 反射回来的 Test-response 报文）和计数。

(2) t1 时刻：Sender 收到 Responder 反射回来的首个 Test-response 报文。

(3) t2 时刻：第一个发包统计周期（t0～t2）结束，Sender 统计第一个发包周期内发送 Test-request 报文的个数。同时开始第二个发包统计周期的发包和计数，以及第二个收包统计周期的收包和计数。

(4) t3 时刻：第一个收包统计周期（t0～t3）结束，Sender 统计第一个收包周期内收到 Test-response 报文的个数，并计算第一个发包周期的丢包率。

丢包率计算公式为：

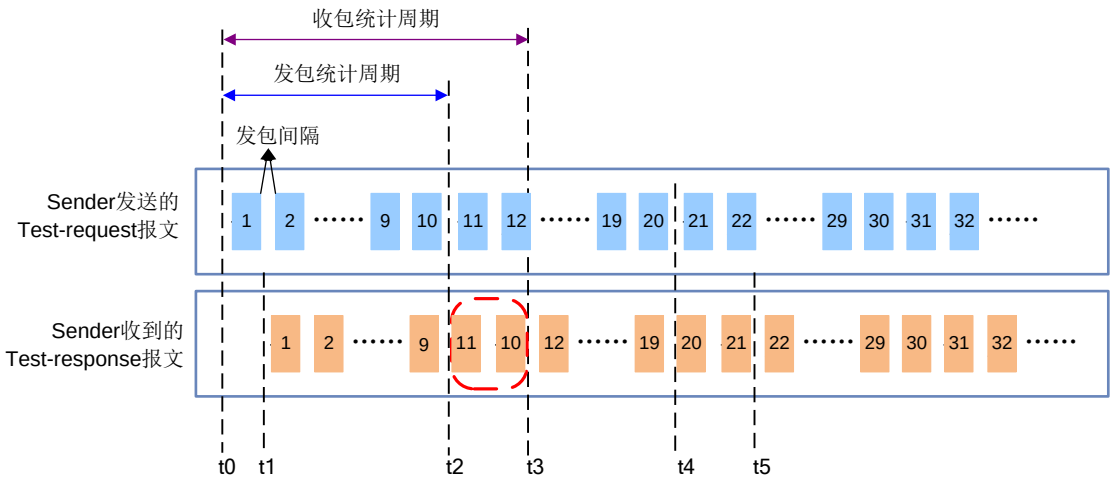
丢包率 = (第 n 个周期内发送报文数 – 第 n 个周期内接收报文数) / 第 n 个周期内发送报文数

(5) t4 时刻：第二个发包统计周期（t2～t4）结束，Sender 统计第二个发包周期内发送 Test-request 报文的个数。同时开始下一个发包统计周期的发包和计数，以及下一个收包统计周期的收包和计数。

(6) t5 时刻：第二个收包统计周期（t2～t5）结束，Sender 统计第二个收包周期内收到 Test-response 报文的个数，并计算第二个发包周期的丢包率。

如此反复，计算每一个周期的丢包率，直到测量结束。

图6 TWAMP Light 丢包测量机制示意图



TWAMP Light 通过以下两个重要技术使得测量结果更加准确：

- 适当放宽收包统计周期，即收包统计周期比发包统计周期长一点，这样可以最大程度地避免由于网络延时与传输乱序对统计结果的不良影响。

  如图 6 中的第 10 号报文，它在第一个发包统计周期结束后、第一个收包统计周期结束前到达，Sender 仍会将其统计到第一个收包统计周期中。

- 通过序列号（Sequence Number）来识别该报文所属的发送统计周期。
  - Sender 会自动为 Test-request 报文分配序列号；
  - Responder 构造 Test-response 报文时，会将 Test-request 报文的序列号拷贝到 Test-response 报文的 Sender Sequence Number 字段；
  - Sender 收到 Test-response 报文后，根据报文中的 Sender Sequence Number 字段，判断 Test-response 所属的周期。

  如图 6 中，第一个收包统计周期只统计序列号为 1～10 的报文，不会统计第 11 号报文；第二个收包统计周期只统计序列号为 11～20 的报文，不会统计其他序列号的报文，从而保证了统计的准确性。

2.3.3 时延、时延抖动测量机制

如图 7 所示，TWAMP Light 按周期发送测试报文，并在测试报文中携带时间戳，基于相邻两个报文的时间戳来计算时延和时延抖动。测量过程如下：

(1) Sender 发送一个 Test-request 报文给 Responder，并在报文中携带报文离开时间 STxTime。

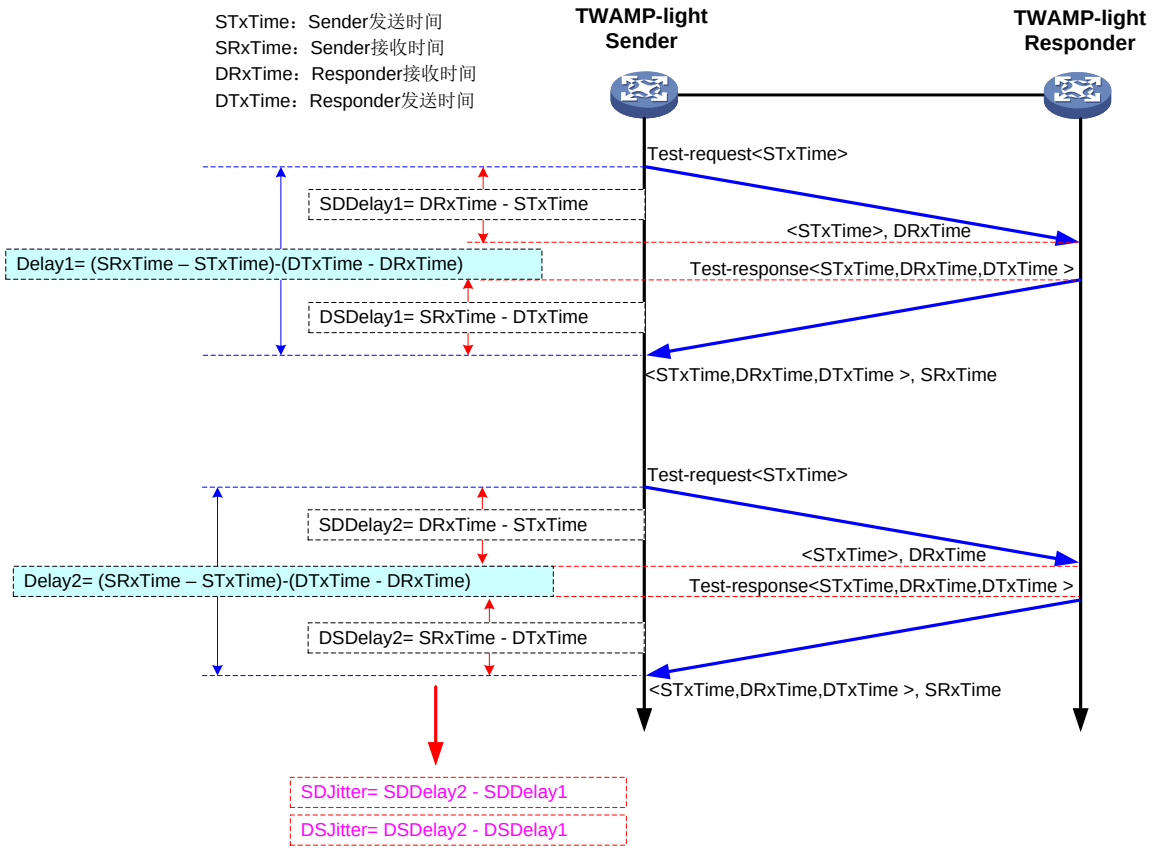
(2) Test-request 报文到达 Responder，Responder 记录接收 Test-request 报文的时间 DRxTime。

(3) Responder 根据 Test-request 报文中的字段构造 Test-response 报文，并将时间戳 STxTime、DRxTime 以及预估的 Test-response 报文离开时间 DTxTime 等信息记录在 Test-response 报文中反射回 Sender。

(4) Test-response 报文到达 Sender，Sender 记录接收 Test-response 报文的时间 SRxTime，并根据 STxTime、DRxTime、DTxTime 和 SRxTime 四个时间戳，计算出 Sender 到 Responder 之间的双向链路时延 Delay1。

Sender 以固定周期发送多个探测报文，重复上述过程，从而计算出 Sender 到 Responder 之间的双向链路时延 Delay2、Delay3 等，以及源端到目的端的时延抖动 SD-jitter、目的端到源端的时延抖动 DS-jitter。

图7 TWAMP Light 时延、时延抖动测量机制示意图

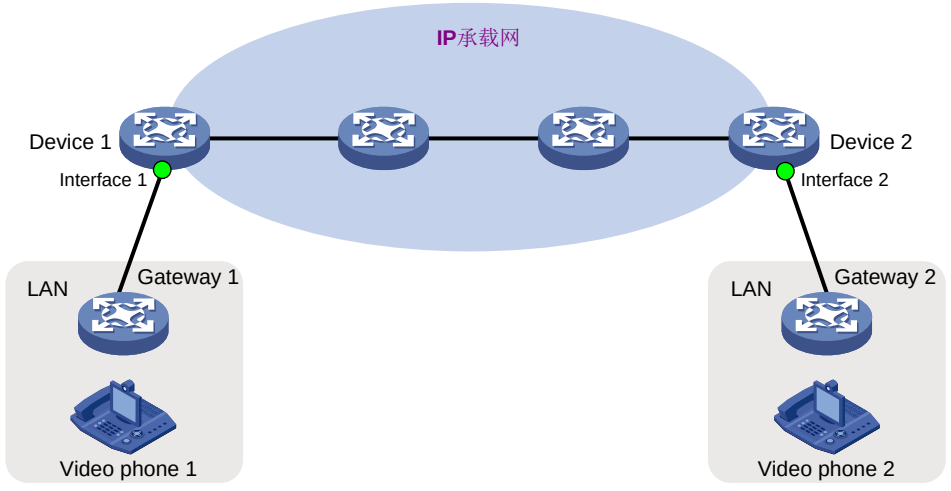


3 典型组网应用

3.1 使用TWAMP Light测试IP网络性能

如图 8所示，Video phone 1 和 Video phone 2 在进行视频通话时发现语音有卡顿、视频有马赛克现象，需要测试 IP 承载网络的性能，确认语音和视频流量在穿越 IP 承载网络时，是否存在严重丢包和延时现象。在 Device 1 和 Device 2 上使用 TWAMP Light 功能，可以测试业务流在穿越 IP 承载网络时，Interface 1 到 Interface 2 的双向路径时延、抖动及丢包率参数，协助用户定位网络问题。

图8 使用 TWAMP Light 测试 IP 网络性能组网图

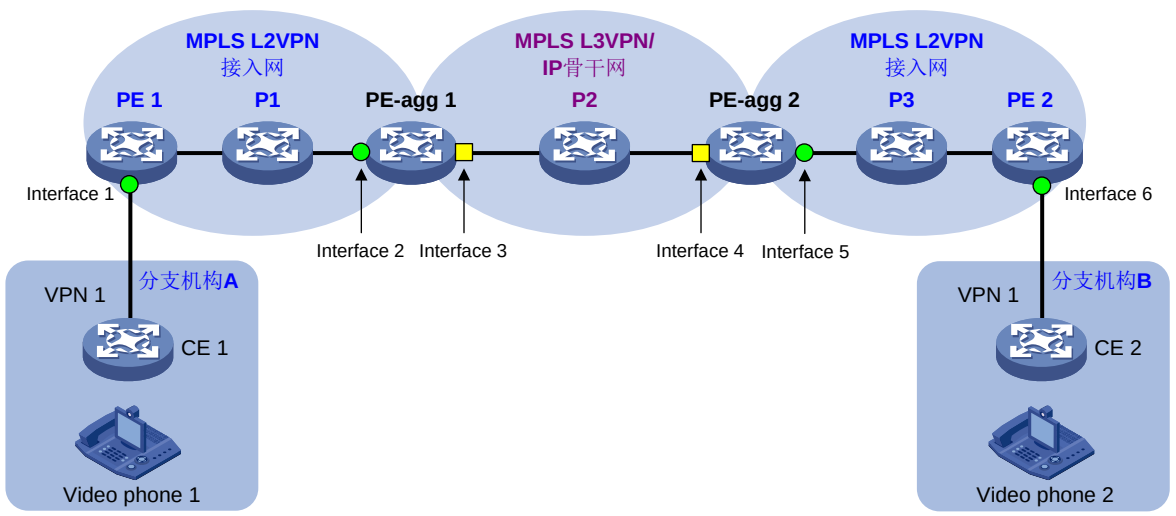


3.2 使用TWAMP Light测试VPN网络性能

如图 9 所示，某企业的两个分支机构分别在 A 地和 B 地办公，使用 VPN 通道连接两地网络。Video phone 1 和 Video phone 2 在进行视频通话时发现语音有卡顿、视频有马赛克现象，需要测试 VPN 网络的性能，确认哪部分网络丢包和延时比较严重。使用 TWAMP Light 功能，可以测试业务流在穿越 VPN 网络时，路径的双向路径时延、抖动及丢包率参数，协助用户定位网络问题：

- 在 PE 1 和 PE 2 上部署 TWAMP Light 功能，测试整个运营商网络（Interface 1 到 Interface 6）的性能。如果存在严重时延和丢包，可以继续执行下面测试定位问题网络。
- 在 PE 1 和 PE-agg 1 上部署 TWAMP Light 功能，可以测试 MPLS L2VPN 网络（Interface 1 到 Interface 2）的性能。
- 在 PE-agg 1 和 PE-agg 2 上部署 TWAMP Light 功能，可以测试 MPLS L3VPN 网络（Interface 3 到 Interface 4）的性能。
- 在 PE 1 和 PE-agg 2 上部署 TWAMP Light 功能，可以测试 MPLS L2VPN 接入 MPLS L3VPN 网络（Interface 1 到 Interface 5）的性能。

图9 使用 TWAMP Light 测试 VPN 网络性能组网图



NQA TWAMP-light 配置

目 录

1 NQA TWAMP-light

1.1 NQA TWAMP-light配置任务简介

NQA TWAMP-light 配置任务如下：

(1) 配置 NQA TWAMP-light 服务器

(2) 在 NQA 客户端上配置 TWAMP-light client

(3) （可选）在 NQA 客户端上配置 TWAMP-light 测试告警功能

(4) 在 NQA 客户端上启动 NQA TWAMP-light 测试

(5) （可选）在 NQA 客户端上停止 NQA TWAMP-light 测试

1.2 配置NQA TWAMP-light服务器

(1) 进入系统视图。

system-view

(2) 在 NQA 服务器上创建 TWAMP-light responder，并进入 TWAMP-light responder 视图。

nqa twamp-light responder

(3) 在 NQA 服务器上创建 TWAMP-light Responder 端的测试会话。

test-session *session-id* [**interface** *interface-type interface-number* [**service-instance** *instance-id*]] { { **ip** | **ipv6** } **destination** *address* **source** *address* **destination-port** *port-number* **source-port** *port-number* [**vpn-instance** *vpn-instance-name*] | **destination-mac** *mac-address* **source-mac** *mac-address* } * [**vlan** { *vlan-id* | **s-vid** *vlan-id* **c-vid** *vlan-id* } | **timestamp-format** { **ntp** | **ptp** } | **description** *text*] *

(4) 退回系统视图。

quit

(5) 开启 NQA 服务器功能。

nqa server enable

缺省情况下，NQA 服务器功能处于关闭状态。

1.3 在NQA客户端上配置TWAMP-light client

1. 配置限制和指导

如果同时启动多个 TWAMP-light 测试，那么每个测试会话指定的地址及端口号不能完全相同，否则多个测试匹配同一条流将影响测试结果。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 使能 NQA 客户端功能。

nqa agent enable

缺省情况下，NQA 客户端功能处于开启状态。

只有使能 NQA 客户端功能后，NQA 客户端的相关配置才会生效。

(3) 创建 TWAMP-light client 并进入 Twamp-light-client 视图。

nqa twamp-light client

(4) 创建 TWAMP-light Client 的测试会话，并进入 Client-session 视图。

test-session *session-id*

(5) 配置 TWAMP-light 测试的地址及端口号。

a. 配置探测报文的源 IP 地址。

（IPv4 网络）

source ip *ip-address*

缺省情况下，未配置探测报文的源 IP 地址。

（IPv6 网络）

source ipv6 *ipv6-address*

缺省情况下，未配置探测报文的源 IPv6 地址。

b. 配置探测报文的目的 IP 地址。

（IPv4 网络）

destination ip *ipv4-address*

缺省情况下，未配置探测报文的目的 IPv4 地址。

（IPv6 网络）

destination ipv6 *ipv6-address*

缺省情况下，未配置探测报文的目的 IPv6 地址。

c. 配置探测报文的源接口。

source interface *interface-type interface-number* [**service-instance** *instance-id*]

缺省情况下，未配置探测报文的源接口。

该命令指定的接口必须为 up 状态。

d. 配置探测报文的源端口号。

source port *port-number*

缺省情况下，未配置测试操作的源端口号。

e. 配置探测报文的目的端口号。

destination port *port-number*

缺省情况下，未配置测试操作的目的端口号。

f. 配置探测报文的源 MAC 地址。

source mac *mac-address*

缺省情况下，未配置探测报文的源 MAC 地址。

g. 配置探测报文的目的 MAC 地址。

destination mac *mac-address*

缺省情况下，未配置探测报文的目的 MAC 地址。

(6) 配置 TWAMP-light 测试的时间戳格式

timestamp-format { **ntp** | **ptp** }

缺省情况下，TWAMP-light 测试的时间戳格式为 PTP。

(7) 配置 TWAMP-light 测试的基本参数。

- 配置探测报文中的填充内容大小。

data-size *size*

缺省情况下，探测报文中的填充内容大小为 142 字节。

- 配置探测报文的填充字符串。请选择其中一项进行配置。

  （十进制）

  data-fill *string*

  （十六进制）

  hex-data-fill *hex*

  两条命令的作用相同，多次执行这两条命令时，最后一次执行的命令生效。

  本命令的缺省情况与设备的型号有关，请以设备的实际情况为准。

- （可选）配置探测报文的描述信息。

  description *text*

  缺省情况下，未配置描述信息。

- 配置探测报文中 IP 报文头中服务类型域的值。

  tos *value*

  缺省情况下，NQA 探测报文中 IP 报文头中服务类型域的值为 0。

- （可选）配置探测报文所属的 VPN 实例。

  vpn-instance *vpn-instance-name*

  缺省情况下，未指定探测报文所属的 VPN 实例，NQA 用来测试公网的连通性。

(8) （可选）配置探测报文的 VLAN 标签。

vlan { *vlan-id* | **s-vid** *vlan-id* **c-vid** *vlan-id* }

缺省情况下，未配置探测报文的 VLAN 标签。

(9) （可选）配置 TWAMP-light 测试会话的绑定出接口。

test-session *session-id* **bind interface** *interface-type interface-number*

缺省情况下，未配置 TWAMP-light 测试会话的绑定出接口。

1.4 在NQA客户端上配置TWAMP-light测试告警功能

(1) 进入系统视图。

system-view

(2) 创建 TWAMP-light client 并进入 Twamp-light-client 视图。

nqa twamp-light client

(3) 创建 TWAMP-light Client 的测试会话，并进入 Client-session 视图。

test-session *session-id*

(4) 创建 TWAMP-light 测试的阈值告警组，请至少选择其中一项进行配置。

- 创建监测双向时延的阈值告警组。

  reaction *item-number* **checked-element two-way-delay threshold-value** *upper-threshold lower-threshold* **[action-type { none | trap-only }]**

  缺省情况下，不存在监测双向时延的阈值告警组。

- 创建监测双向丢包率的阈值告警组。

  reaction *item-number* **checked-element two-way-loss threshold-value** *upper-threshold lower-threshold* **[action-type { none | trap-only }]**

  缺省情况下，不存在监测双向丢包率的阈值告警组。

- 创建监测双向抖动的阈值告警组。

  reaction *item-number* **checked-element two-way-jitter threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]

  缺省情况下，不存在监测双向抖动的阈值告警组。

1.5 在NQA客户端上启动NQA TWAMP-light测试

1. 配置限制和指导

如果同时启动多个 TWAMP-light 测试，那么每个测试会话指定的源 IP、源端口、目的 IP 和目的端口四个参数不能均相同，否则多个测试匹配同一条流将影响测试结果。

如果配置了 **data-fill** 命令，则启动 TWAMP-light 测试时报文发送周期不允许配置为 10ms 和 100ms。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 TWAMP-light sender，并进入 TWAMP-light sender 视图。

nqa twamp-light sender

(3) 启动 TWAMP-light 测试。

start test-session *session-id* { **permanent** | **duration** *duration* | **packet-count** *count* } [**tx-interval** { **10** | **100** | **1000** | **10000** | **30000** }] [**timeout** *timeout*] [[**statistics-interval** *statistics-interval*] **monitor-time** *time*]

1.6 在NQA客户端上停止NQA TWAMP-light测试

(1) 进入系统视图。

system-view

(2) 进入 TWAMP-light sender 视图。

nqa twamp-light sender

缺省情况下，不存在 TWAMP-light sender。

(3) 停止 TWAMP-light 测试。

stop { **all** | **test-session** *session-id* }

1.7 NQA TWAMP-light显示和维护

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

表1-1 NQA 显示和维护（NQA 客户端）

操作	命令
显示TWAMP-light client会话的统计信息，包括双向时延、双向抖动和双向丢包信息	**display nqa twamp-light client statistics** { **two-way-delay**	**two-way-loss** } **test-session** *session-id*
显示TWAMP-light client阈值告警组的当前监测结果	**display nqa twamp-light client test-session reaction counters** [*session-id* [*item-number*]]
显示TWAMP-light client会话的信息	**display nqa twamp-light client** [**test-session** *session-id*	**verbose**]

表1-2 NQA 显示和维护（NQA 服务器）

操作	命令
显示TWAMP-light responder会话的信息	**display nqa twamp-light responder** [**test-session** *session-id*]

1.8 NQA TWAMP-light典型配置举例

1.8.1 NQA TWAMP-light 测试基本组网配置举例

1. 组网需求

使用 NQA TWAMP-light 功能，测试本端（Device A）到指定目的端（Device B）间的网络质量。

2. 组网图

图1-1 NQA TWAMP-light 基本配置组网图

3. 配置步骤

(1) 配置各接口的 IP 地址。（配置过程略）

(2) 配置静态路由或动态路由协议，确保各设备之间路由可达。（配置过程略）

(3) 配置 Device B

开启 NQA 服务器。

```
<DeviceB> system-view
[DeviceB] nqa server enable
```

创建 TWAMP-light Responder 端的测试会话 1，配置报文的目的 IP 地址为 10.2.2.2，源 IP 地址为 10.1.1.1，配置报文的目的端口为 20000，源端口为 10000。

```
[DeviceB] nqa twamp-light responder
[DeviceB-twamp-light-responder] test-session 1 ip destination 10.2.2.2 source 10.1.1.1 destination-port 20000 source-port 10000
[DeviceB-twamp-light-responder] quit
```

(4) 配置 Device A

创建 TWAMP-light client 端的测试会话 1。

```
<DeviceA> system-view
[DeviceA] nqa twamp-light client
[DeviceA-nqa-twamp-light-client] test-session 1
```

配置报文的源 IP 地址为 10.1.1.1，目的 IP 地址为 10.2.2.2，配置报文的源端口为 10000，目的端口为 20000。

```
[DeviceA-nqa-twamp-light-client-session1] source ip 10.1.1.1
[DeviceA-nqa-twamp-light-client-session1] destination ip 10.2.2.2
[DeviceA-nqa-twamp-light-client-session1] source port 10000
[DeviceA-nqa-twamp-light-client-session1] destination port 20000
[DeviceA-nqa-twamp-light-client-session1] quit
[DeviceA-nqa-twamp-light-client] quit
```

创建并进入 TWAMP-light sender 视图，启动 TWAMP-light 测试，启动参数：发送报文的周期为 100ms，统计周期为 10000ms，监控时间为 20000ms。

```
[DeviceA] nqa twamp-light sender
[DeviceA-nqa-twamp-light-sender] start test-session 1 permanent tx-interval 100 statistics-interval 10000 monitor-time 20000
[DeviceA-nqa-twamp-light-sender] quit
```

4. 验证配置

显示指定测试会话 1 的信息。

```
[DeviceA] display nqa twamp-light client
Brief information about all test sessions:
Total sessions: 1
Active sessions: 1
--------------------------------------------------------------------------------
ID    Status     Source IP/Port         Destination IP/Port
1     Active     10.1.1.1/10000         10.2.2.2/20000
```

显示指定测试会话 1 的双向丢包统计信息。

```
[DeviceA] display nqa twamp-light client statistics two-way-loss test-session 1
Latest two-way loss statistics:
    Index      Loss count      Loss ratio      Error count  Error ratio
    11006      5               50.0000%        0            0.0000%
    11007      3               30.0000%        0            0.0000%
    11008      4               40.0000%        0            0.0000%
    11009      8               80.0000%        0            0.0000%
------------------------------------------------------------------------
Average loss count :          5      Average loss ratio :  55.3333%
Maximum loss count :         10      Maximum loss ratio : 100.0000%
Minimum loss count :          1      Minimum loss ratio :  10.0000%
Average error count:          0      Average error ratio:   0.0000%
Maximum error count:          0      Maximum error ratio:   0.0000%
Minimum error count:          0      Minimum error ratio:   0.0000%
```

eMDI
技术介绍

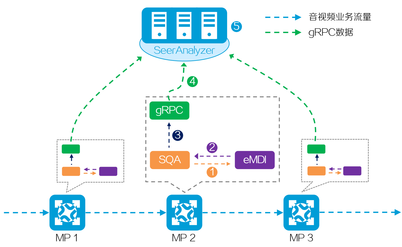
1
简介

eMDI（Enhanced Media Delivery Index，增强型媒体传输质量指标）是一种专门为音视频业务（例如VoIP和IPTV）设计的故障界定和健康诊断技术。通过在音视频业务流量途径的网络节点上部署eMDI，可以对音视频业务流量进行实时监控，提取所需数据并计算监控指标。之后，网络管理员结合多个网络节点计算出的监控指标，可以了解网络状况、界定网络故障发生的位置、优化网络部署，以满足用户的音视频业务质量要求。

2
工作机制

通常，eMDI与SQA（Service Quality Analysis，服务质量分析）、gRPC（Google Remote Procedure Call，Google远程过程调用）和SeerAnalyzer配合使用，形成智能化的音视频质量分析方案。方案部署后，其具体工作机制如下：

1. 在启用eMDI功能的网络设备MP（Measurement Point，测量点）上，SQA功能识别音视频业务流量，并将流量特征通知给eMDI。
2. eMDI基于SQA功能通知的流量特征对目标流进行监控，并将监控指标（例如速率、丢包率）发送给SQA。
3. SQA将监控指标发送给gRPC模块。
4. gRPC模块将监控指标封装在gRPC协议报文中上送给SeerAnalyzer。
5. SeerAnalyzer根据收到的监控指标进行故障界定和健康状况分析，并通过图形化界面呈现给网络管理员。



说明

eMDI也可以单独使用。网络管理员直接在MP上通过命令行手工配置eMDI功能，通过显示信息查看监控指标，结合多个MP上显示的监控指标进行流量的故障界定和健康状况分析。

3
技术特色

实时监控
实时提取目标流中eMDI所需的数据，用以计算监控指标

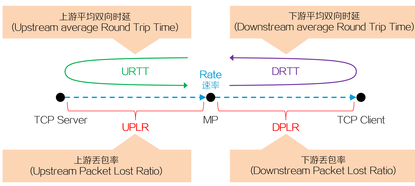
准确检测
监控指标多样，可以准确反映出目标流的健康状况

自动部署
SQA识别出流量特征后，为其自动部署eMDI功能

快速上报
周期性计算出的监控指标可通过gRPC快速上报

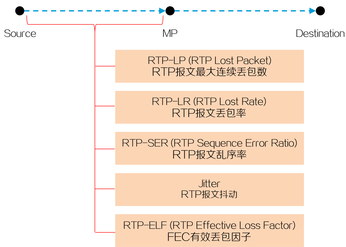
4
TCP流监控指标

对于采用TCP协议传输的音视频业务流（TCP流），eMDI支持的监控指标有Rate、UPLR、DPLR、URTT和DRTT。不同网络位置、报文路径上可获取的监控指标如下图所示：



5
RTP流监控指标

对于采用RTP协议传输的音视频业务流（RTP流），eMDI支持的监控指标有RTP-LP、RTP-SER、Jitter、RTP-LR和RTP-ELF。RTP监控指标反映的均是上游网络状况，如下图所示：

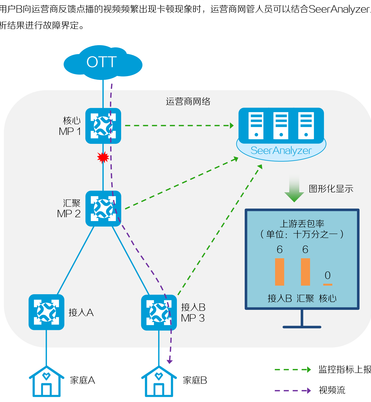


说明

RTP（Real-time Transport Protocol，实时传输协议）主要用来为音视频等需要实时传送的多媒体数据提供端到端的传输服务，由RFC 3550定义。

6
典型应用

如下图所示组网中，OTT（Over The Top，互联网内容提供商）经运营商网络向家庭用户提供IPTV业务。在运营商网络中的核心、汇聚和接入设备上部署eMDI、SQA、gRPC，并将监控指标上送给SeerAnalyzer，当家庭用户因向运营商反馈点播的视频频繁出现卡顿现象时，运营商网管人员可以结合SeerAnalyzer上的服务质量分析结果进行故障界定。



eMDI 配置

目 录

1 eMDI

1.1 eMDI配置限制和指导

一个 eMDI 实例只能监控一条目标数据流，不同 eMDI 实例不能监控相同的目标数据流或者存在冲突的数据流。存在包含关系（**clock-rate** 除外）的流即视为存在冲突。例如：

- 如下两条流，系统将视为存在冲突（存在包含关系，第一条流包含第二条流）：
  - **flow ipv4 tcp source 1.1.1.1 destination 2.2.2.2**
  - **flow ipv4 tcp source 1.1.1.1 destination 2.2.2.2 destination-port 20**
- 如下两条流，系统不会视为冲突（不存在包含关系）：
  - **flow ipv4 tcp source 1.1.1.1 destination 2.2.2.2 destination-port 10**
  - **flow ipv4 tcp source 1.1.1.1 destination 2.2.2.2 destination-port 20**

实例启动后，实例中的所有参数均不支持修改，如需修改请先使用 **stop** 命令停止实例；如果设备发生主备倒换或 eMDI 进程重启，实例会自动停止，如需启动请重新执行 **start** 命令。

在如下两种情况中，由于 eMDI 功能监控到的数据不是完整的，所以监控结果将会存在偏差：

- 被监控的数据流中，有部分流量在网络中传输时未经过本设备；
- 被监控的数据流中，虽然所有流量都经由本设备转发，但并不是经由本设备中的同一个单板转发。

1.2 eMDI配置准备

获取目标数据流的特征，才能根据特征为实例配置目标数据流。

1.3 配置eMDI

1.3.1 配置监控参数

(1) 进入系统视图。

system-view

(2) 开启 eMDI 功能并进入 eMDI 视图。

emdi

缺省情况下，eMDI 功能处于关闭状态。

(3) 创建 eMDI 实例并进入实例视图。

instance *instance-name*

(4) （可选）配置 eMDI 实例的描述信息。

description *text*

缺省情况下，未配置 eMDI 实例的描述信息。

(5) 配置目标数据流。请选择其中一项进行配置。

- 配置目标 TCP 数据流

  flow ipv4 tcp source *source-ip-address* **destination** *destination-ip-address* [**destination-port** *destination-port-number* | **source-port** *source-port-number* | **vlan** *vlan-id* | **vni** *vxlan-id*] *

- 配置目标 UDP 数据流

flow ipv4 udp source *source-ip-address* **destination** *destination-ip-address* [**destination-port** *destination-port-number* | **source-port** *source-port-number* | **vlan** *vlan-id* | **vni** *vxlan-id* | **pt** *pt-value* | **clock-rate** *clock-rate-value*] *

缺省情况下，未配置 eMDI 实例的目标数据流。

在进行模糊匹配（即未指定命令中除 **clock-rate** 之外的某些可选参数）时，实例仅会以设备收到的首包所属的流为基础进行指标计算。以目的端口号为例，假设配置的目标 TCP 数据流为 **flow ipv4 tcp source 10.0.0.1 destination 10.0.1.1**，此时设备收到了属于该规则的首包的目的端口号为 100，则后续该实例将仅基于源 IP 地址为 10.0.0.1、目的 IP 地址为 10.0.1.1、目的端口号为 100 这条流进行指标计算，而源 IP 地址为 10.0.0.1、目的 IP 地址为 10.0.1.1、目的端口号为非 100 的报文，将不会纳入计算范围。

上述模糊匹配的实现机制可能会导致最终的监控结果存在偏差，所以为了保证监控结果的精确性，建议将目标数据流的粒度配置得越精细越好。

(6) （可选）配置 eMDI 实例的告警阈值。

alarm { **dplr** | **rtp-lr** | **rtp-ser** | **uplr** } **threshold** *threshold-value*

缺省情况下，eMDI 实例的告警阈值为 100。

对于 TCP 数据流，仅支持配置 **dplr** 和 **uplr**；对于 UDP 数据流，仅支持配置 **rtp-lr** 和 **rtp-ser**。

(7) （可选）配置 eMDI 实例的告警抑制次数。

alarm suppression times *times-value*

缺省情况下，eMDI 实例的告警抑制次数为 3。

(8) （可选）配置目标 UDP 数据流的视频质量监控的滑动窗口和阈值。

fec { **window** *window-size* | **threshold** *threshold-value* } *

缺省情况下，UDP 数据流的视频质量监控的滑动窗口为 100，阈值为 5。

(9) （可选）配置 eMDI 实例的监控时间。

lifetime { **seconds** *seconds* | **minutes** *minutes* | **hours** *hours* | **days** *days* }

缺省情况下，eMDI 实例的监控时间为 1 小时。

(10) （可选）配置 eMDI 实例的监控周期。

monitor-period *period-value*

缺省情况下，eMDI 实例的监控周期为 60 秒。

1.3.2 启动 eMDI 实例

(1) 进入系统视图。

system-view

(2) 进入 eMDI 视图。

emdi

(3) 进入 eMDI 实例视图。

instance *instance-name*

(4) 启动 eMDI 实例。

start

1.3.3 停止 eMDI 实例

请选择其中一项进行配置。

- 停止 eMDI 实例。

  a. 进入系统视图。

system-view

b. 进入 eMDI 视图。

emdi

c. 进入 eMDI 实例视图。

instance *instance-name*

d. 停止 eMDI 实例。

stop

- 停止所有 eMDI 实例。

a. 进入系统视图。

system-view

b. 进入 eMDI 视图。

emdi

c. 停止所有 eMDI 实例。

stop all

1.4 eMDI显示和维护

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

在用户视图下执行 **reset** 命令可以清除 eMDI 的统计信息。

表1-1 eMDI 显示和维护

配置	命令
显示eMDI实例的信息	**display emdi instance** [**name** *instance-name* | **id** *instance-id*] [**verbose**]
显示设备的eMDI实例资源信息	**display emdi resource**
显示eMDI实例的监控统计信息	**display emdi statistics** { **instance-name** *instance-name* | **instance-id** *instance-id* } [**number** *number*] [**abnormal** | **verbose**]
清除eMDI实例的统计信息	**reset emdi statistics** [**instance-name** *instance-name* | **instance-id** *instance-id-value*]

1.5 eMDI典型配置举例

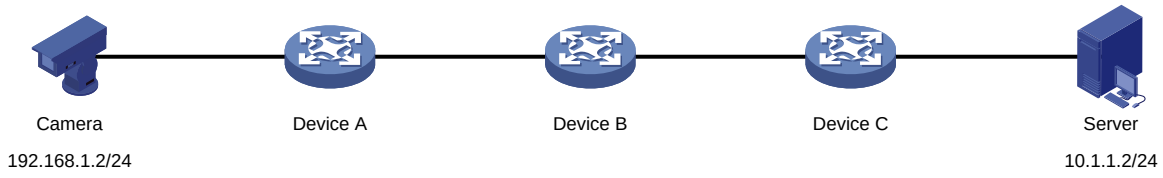
1.5.1 目标 UDP 数据流配置举例

1. 组网需求

如图 1-1 所示，Camera 通过 Device A、Device B 和 Device C 将 RTP 视频数据流回传给 Server。现发现 Server 端收到的画面有花屏，需在 Device A、Device B 和 Device C 配置 eMDI 功能，进行故障定界，以快速发现故障链路或设备。

2. 组网图

图1-1 eMDI 典型配置组网图



3. 配置准备

配置各设备的 IP 地址，并确保它们之间路由可达。

4. 配置步骤

(1) 配置 Device A

开启 eMDI 功能。

```
<DeviceA> system-view
[DeviceA] emdi
```

创建 eMDI 实例 test。

```
[DeviceA-emdi] instance test
```

配置目标 UDP 数据流：源 IP 为 192.168.1.2，目的 IP 为 10.1.1.2。

```
[DeviceA-emdi-instance-test] flow ipv4 udp source 192.168.1.2 destination 10.1.1.2
```

配置 eMDI 实例的监控周期为 10 秒。

```
[DeviceA-emdi-instance-test] monitor-period 10
```

配置 eMDI 实例的监控时间为 30 分钟。

```
[DeviceA-emdi-instance-test] lifetime minutes 30
```

启动 eMDI 实例。

```
[DeviceA-emdi-instance-test] start
```

(2) 配置 Device B 和 Device C

与 Device A 的配置相同，配置步骤略。

5. 验证配置

实例运行一段时间后，查看 Device A、Device B 和 Device C 上实例 test 的简要监控统计信息，结合三个设备上的数据，判断故障位置。下面以 Device A 的统计信息为例。

```
<DeviceA> display emdi statistics instance-name test
Instance name    : test
Instance ID      : 1
Monitoring period: 10 sec
Protocol         : UDP

Unit for RTP-LR, RTP-SER and RTP-ELF is 1/100000
Timestamp            Status   RTP-LR  RTP-SER  Jitter(us)  RTP-LP      RTP-ELF
2019/09/17 16:17:20  Normal   0       0        2560        0           0
2019/09/17 16:17:10  Abnormal 50000   0        2459        1           100000
2019/09/17 16:17:00  Abnormal 12634   33333    5236        3           23356
```

音视频质量分析技术介绍

1 音视频质量分析简介

多媒体音视频业务在日常生活中应用广泛，包括音视频会议、视频监控、视频播放等，用户对多媒体服务体验的要求也日益增高。通过部署音视频质量分析方案，设备可以实时监控基于SIP和H.323协议的音视频流量，并优先转发音视频流量。音视频质量分析方案还可以通过可视化方式展示音视频流量的质量分析结果，以便管理员快速发现和排除网络故障，改善并解决音视频质量问题，为用户提供良好的多媒体服务体验。

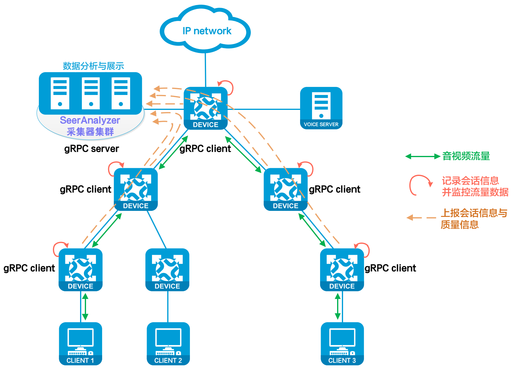
2 网络构成

- Client：使用音视频应用的终端。
- Device：音视频流量途经的设备，需要监控音视频流量、记录音视频会话信息并上报流量质量信息和会话信息。
- Voice server：语音服务器，用于管理语音用户的注册和呼叫。
- SeerAnalyzer（先知分析器）：SNA（SeerNetwork Architecture，先知网络架构）上的核心组件，可以实时采集网络业务流量数据，并通过大数据分析技术和人工智能算法可视化展示网络的运行情况。

3 工作机制

音视频质量分析方案中，音视频流途经的设备会通过SQA和eMDI功能监控音视频流量、记录音视频会话信息，并使用gRPC功能将会话和质量信息上报给SeerAnalyzer，由SeerAnalyzer进行数据分析与可视化展示。

SQA	Service quality analysis，服务质量分析
eMDI	Enhanced Media Delivery Index，增强型媒体传输质量指标
gRPC	Google Remote Procedure Call，Google远程过程调用



① 音视频流量途经的设备通过SQA功能识别基于SIP或H.323协议的音视频流量，获取报文的五元组信息（源/目的IP地址、源/目的端口号和协议号），并提高音视频流量的转发优先级，以便优先转发音视频流量。

② 设备上的SQA模块将获取到的五元组信息通知给eMDI模块，eMDI根据五元组信息对音视频流量的丢包、乱序和抖动数据进行监控。

③ 设备作为gRPC客户端，通过gRPC协议报文将eMDI监控到的丢包、乱序、抖动等质量信息以及SQA记录的SIP、H.323会话信息上送给SeerAnalyzer。

④ SeerAnalyzer根据上报的质量信息，对所有SIP和H.323流量的质量进行分析，并以可视化的方式展示音视频质量分析结果。网络管理员通过查看SeerAnalyzer展示的音视频质量分析数据和会话信息，了解网络状况，定位并解决网络中的问题，从而改善音视频业务的质量。

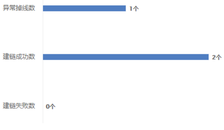
除了在SeerAnalyzer上查看音视频质量信息和会话信息，还可以在每台设备上通过eMDI的显示命令查看音视频流量的丢包率、时延、抖动、乱序率等信息，以及通过SQA的显示命令查看通话的详细信息，其中包含MOS（Mean Opinion Score，服务质量评估值）信息。MOS是音视频会话的质量指标，值越低表示质量越差。

4 可视化展示

SeerAnalyzer的音视频质量分析页面上，可以显示音视频流量的会话和质量信息，包括SIP和H.323的会话统计、流量趋势、路径描述、MOS等信息。

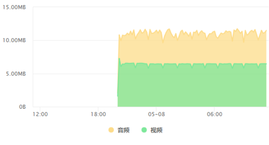
会话统计

统计SIP或H.323的会话数据。



流量趋势

汇总各时间段的音视频流量数据。



路径描述

在会话详情页，可查看流量路径。流量路径中显示了音视频流途经各个设备时的相关信息。

MOS

显示所选时间段内音视频会话的质量指标。

新华三资料开发部出品

服务质量分析配置

目 录

1 服务质量分析

1.1 服务质量分析配置限制和指导

服务质量分析功能不支持分析加密的 SIP 协议报文和加密的 H.323 协议报文。

1.2 配置基于SIP协议的服务质量分析功能

1. 配置限制和指导

侦听不同 VoIP 协议报文的端口必须不同。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入服务质量分析视图。

sqa

(3) 开启基于 SIP 协议的服务质量分析功能。

sqa-sip enable

缺省情况下，基于 SIP 协议的服务质量分析功能处于关闭状态。

(4) 配置设备侦听 SIP 报文的端口号。

sqa-sip port *port-number*

缺省情况下，设备侦听 SIP 报文的端口号为 5060。

设备侦听 SIP 报文的端口号必需与语音服务器上设置的 SIP 协议端口号保持一致。

(5) （可选）配置对指定 IP 地址范围的 SIP 通话进行服务质量分析。

sqa-sip filter address *start-address end-address*

缺省情况下，设备对所有 SIP 报文进行服务质量分析。

设备仅对呼叫方或应答方的 IP 地址在本命令配置的地址范围内的 SIP 通话进行服务质量分析。

多次执行本命令，最后一次执行的命令生效。

1.3 配置基于H.323协议的服务质量分析功能

1. 配置限制和指导

侦听不同 VoIP 协议报文的端口须配置不同的端口号。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入服务质量分析视图。

sqa

(3) 开启基于 H.323 协议的服务质量分析功能。

sqa-h323 enable

缺省情况下，基于 H.323 协议的服务质量分析功能处于关闭状态。

(4) 配置设备侦听 H.225 报文的端口号。

sqa-h225 port *port-number*

缺省情况下，设备侦听 H.225 报文的端口号是 1720。

设备侦听 H.225 报文的端口号必需与语音服务器上设置的 H.225 协议端口号保持一致。

(5) （可选）配置对指定 IP 地址范围的 H.323 通话进行服务质量分析。

sqa-h323 filter address *start-address end-address*

缺省情况下，设备对所有 H.323 报文进行服务质量分析。

设备仅对呼叫方或应答方的 IP 地址在本命令配置的地址范围内的 H.323 通话进行服务质量分析。

多次执行本命令，最后一次执行的命令生效。

1.4 服务质量分析显示和维护

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

表1-1 服务质量分析显示和维护

操作	命令
显示H.323或SIP通话的信息	**display sqa { h323 | sip } call [[call-id** *call-id* **] verbose]**
显示H.323或SIP通话的统计信息	**display sqa { h323 | sip } call-statistics**

1.5 服务质量分析典型配置举例

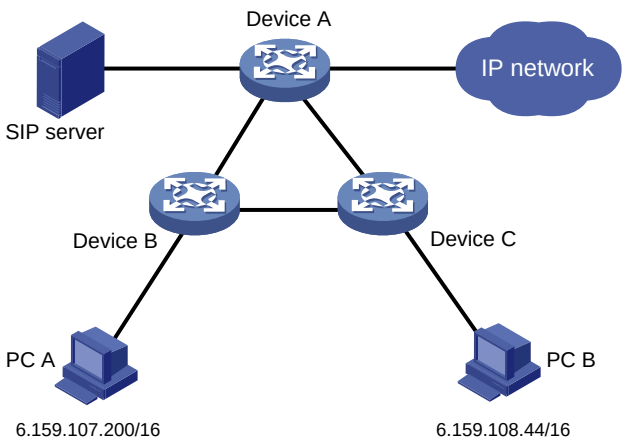
1.5.1 基于 SIP 协议的服务质量分析基本组网配置举例

1. 组网需求

如图 1-1 所示的组网中，SIP server 上安装了第三方 VoIP 软件电话系统，该设备同时作为 SIP 代理服务器和 SIP 注册服务器，管理 SIP 用户的注册并响应呼叫。PC A 和 PC B 可通过安装客户端实现相互呼叫。现在希望通过使用基于 SIP 协议的服务质量分析功能对流经各个设备的多媒体流量进行优化，满足优质的视听要求。

2. 组网图

图1-1 基于 SIP 协议的服务质量分析典型配置组网图



3. 配置准备

确保完成设备的接口配置并确保设备之间连通性。

4. 配置步骤

(1) 配置 SIP 代理服务器

安装第三方 VoIP 软件电话系统的服务器端，为客户端配置用户名（电话号码）和密码。

(2) 配置 PC A 与 PC B

安装第三方 VoIP 软件电话系统的客户端，配置 SIP 服务器的 IP 地址，以及用户名（电话号码）、密码及其它参数。

(3) 配置 Device A

开启基于 SIP 协议的服务质量分析功能。

```
<DeviceA> system-view
[DeviceA] sqa
[DeviceA-sqa] sqa-sip enable
```

配置设备侦听 SIP 报文的端口号为 5066。（该端口号需与 SIP server 上设置的端口号保持一致）

```
[DeviceA-sqa] sqa-sip port 5066
```

配置对 PC A 的 SIP 通话进行服务质量分析。

```
[DeviceA-sqa] sqa-sip filter address 6.159.107.200 6.159.107.210
[DeviceA-sqa] quit
[DeviceA] quit
```

(4) 配置 Device B 与 Device C

Device B 与 Device C 的配置过程同 Device A，此处略。

5. 验证配置

上述配置完成后，在 Device A 上执行以下命令，可以看到用户的 SIP 音、视频流量的简要信息。

```
<DeviceA> display sqa sip call
Caller                 Callee                 CallId
6.159.107.207:49172    6.159.108.51:52410     3101326658
6.159.107.203:49172    6.159.108.47:52410     4530332933
6.159.107.208:49172    6.159.108.52:52410     4445702693
6.159.107.206:49172    6.159.108.50:52410     8263542841
6.159.107.201:49172    6.159.108.45:52410     4752123310
6.159.107.200:49172    6.159.108.44:52410     99462146
```

在 Device A 上执行以下命令，可以看到当前用户多媒体业务服务质量评估值 MOS 等详细信息，正向流量与反向流量的 MOS 值越高表示服务质量越好。

```
<DeviceA> display sqa sip call call-id 99462146 verbose
Call ID: 99462146
  Caller information:
    IP: 6.159.107.200      Port: 49172    MAC: a036-9fd4-b5bd
    Tag: 1111@6.159.1.10
  Callee information:
    IP: 6.159.108.44       Port: 52410    MAC: a036-9fd4-b5bc
    Tag: 2222@6.159.1.10
  Type: Audio     VLAN: 0              StartTime: 2019-7-14 15:40:39
  MOS(F): 4       MOS(R): 4
  Forward flow (octet): 4793344        Forward flow (packet): 4681
  Reverse flow (octet): 3810304        Reverse flow (packet): 3721
```

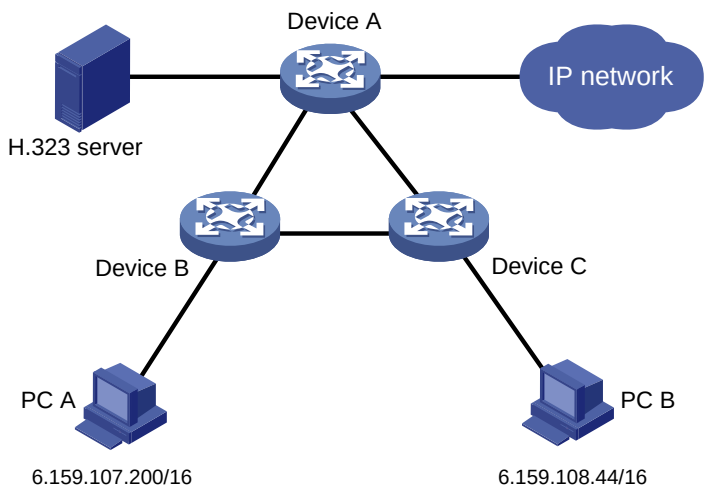
1.5.2 基于 H.323 协议的服务质量分析基本组网配置举例

1. 组网需求

如图 1-2 所示的组网中，H.323 server 上安装了第三方 VoIP 软件电话系统，该设备同时作为 H.323 代理服务器和 H.323 注册服务器，管理 H.323 用户的注册并响应呼叫。PC A 和 PC B 可通过安装客户端实现相互呼叫。现在希望通过使用基于 H.323 协议的服务质量分析功能对流经各个设备的多媒体流量进行优化，满足优质的视听要求。

2. 组网图

图1-2 基于 H.323 协议的服务质量分析典型配置组网图



3. 配置准备

确保完成设备的接口配置并确保设备之间连通性。

4. 配置步骤

(1) 配置 H.323 代理服务器

安装第三方 VoIP 软件电话系统的服务器端，为客户端配置用户名（电话号码）和密码。

(2) 配置 PC A 与 PC B

安装第三方 VoIP 软件电话系统的客户端，配置 H.323 服务器的 IP 地址，以及用户名（电话号码）、密码及其它参数。

(3) 配置 Device A

开启基于 H.323 协议的服务质量分析功能。

```
<DeviceA> system-view
[DeviceA] sqa
[DeviceA-sqa] sqa-h323 enable
```

配置设备侦听 H225 报文的端口号为 1720。（该端口号需与 H.323 server 上设置的端口号保持一致）

```
[DeviceA-sqa] sqa-h225 port 1720
```

配置对 PC A 的 H.323 通话进行服务质量分析。

```
[DeviceA-sqa] sqa-h323 filter address 6.159.107.200 6.159.107.210
[DeviceA-sqa] quit
[DeviceA] quit
```

(4) 配置 Device B 与 Device C

Device B 与 Device C 的配置过程同 Device A，此处略。

5. 验证配置

上述配置完成后，在 Device A 上执行以下命令，可以看到用户的 H.323 音、视频流量的简要信息。

```
<DeviceA> display sqa h323 call
Caller                 Callee                 CallId
6.159.107.207:49172    6.159.108.51:52410     42910c03-e31c-1910-9a63-000c29209aa9
6.159.107.203:49172    6.159.108.47:52410     3e33ecbd-6f1d-1910-8b52-6805ca5d1208
6.159.107.208:49172    6.159.108.52:52410     01a788fe-e21c-1910-8ee7-000c29209aa9
6.159.107.206:49172    6.159.108.50:52410     4e9516ff-e21c-1910-8f98-000c29209aa9
6.159.107.200:49172    6.159.108.44:52410     703b6fff-e21c-1910-9f51-000c29209aa9
```

在 Device A 上执行以下命令，可以看到当前用户多媒体业务服务质量评估值 MOS 等详细信息，正向流量与反向流量的 MOS 值越高表示服务质量越好。

```
<DeviceA> display sqa h323 call call-id 703b6fff-e21c-1910-9f51-000c29209aa9 verbose
Call ID: 703b6fff-e21c-1910-9f51-000c29209aa9
  Caller information:
    IP: 6.159.107.200      Port: 49172    MAC: a036-9fd4-b5bd
  Callee information:
    IP: 6.159.108.44       Port: 52410    MAC: a036-9fd4-b5bc
  GUID: 703b6fff-e21c-1910-9f61-000c29209aa9
  Protocol: TCP(6)
  Session ID: 2
  Type: Audio          Vlan: 1          StartTime: 2019-7-14 15:40:39
  MOS(F): 4            MOS(R): 4
  Forward flow (octet): 4793344         Forward flow (packet): 4681
  Reverse flow (octet): 3810304         Reverse flow (packet): 3721
```