NQA 技术白皮书

Copyright © 2019 紫光恒越技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除紫光恒越技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。本文中的内容为通用性技术信息，某些信息可能不适用于您所购买的产品。

目 录

1 概述 1
1.1 产生背景 1
1.2 技术优点 1
2 NQA 技术实现 1
2.1 概念介绍 1
2.2 NQA 测试机制 2
2.2.1 UDP-echo 测试机制 2
2.2.2 UDP-tracert 测试机制 3
2.2.3 UDP-jitter 测试机制 4
2.2.4 Path-jitter 测试机制 6
2.2.5 ICMP-echo 测试机制 7
2.2.6 ICMP-jitter 测试机制 8
2.2.7 Voice 测试机制 8
2.2.8 TCP 测试机制 9
2.2.9 DHCP 测试机制 9
2.2.10 DLSw 测试机制 10
2.2.11 DNS 测试机制 10
2.2.12 FTP 测试机制 10
2.2.13 HTTP 测试机制 10
2.2.14 SNMP 测试机制 10
2.2.15 ARP 测试机制 11
2.3 联动功能机制 11
2.4 阈值告警功能机制 12
2.5 NQA 统计功能 12
2.6 NQA 历史记录功能 13
2.7 NQA server 处理机制 13
3 典型组网案例 13
3.1 NQA 与 VRRP 联动 13
3.2 NQA 与静态路由联动 14
3.3 NQA 与接口备份联动 15
3.4 NQA 与策略路由联动 16

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。

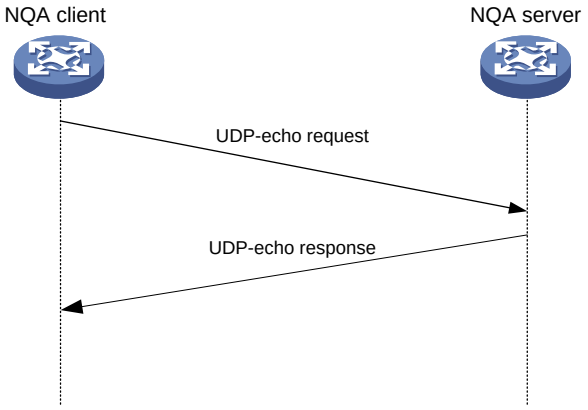
如图 1 所示，UDP-echo 测试机制如下：

(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）。

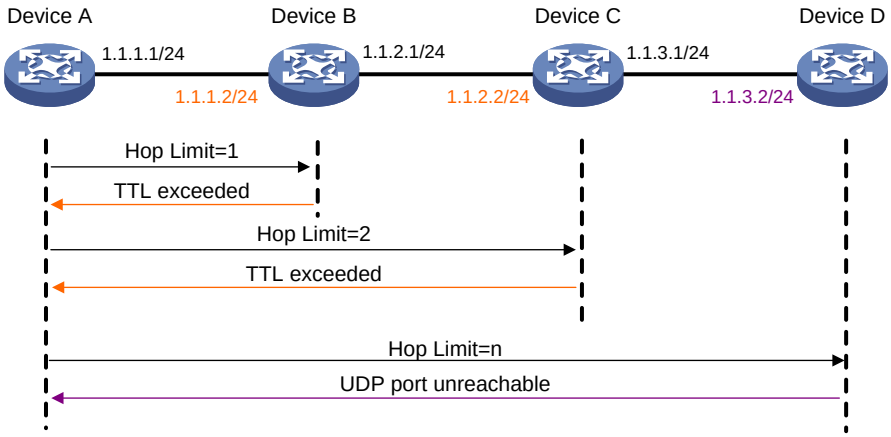
(3) 源端重新向目的端发送一个 IP 数据报文，TTL 值为 2。

(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UNIS 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。

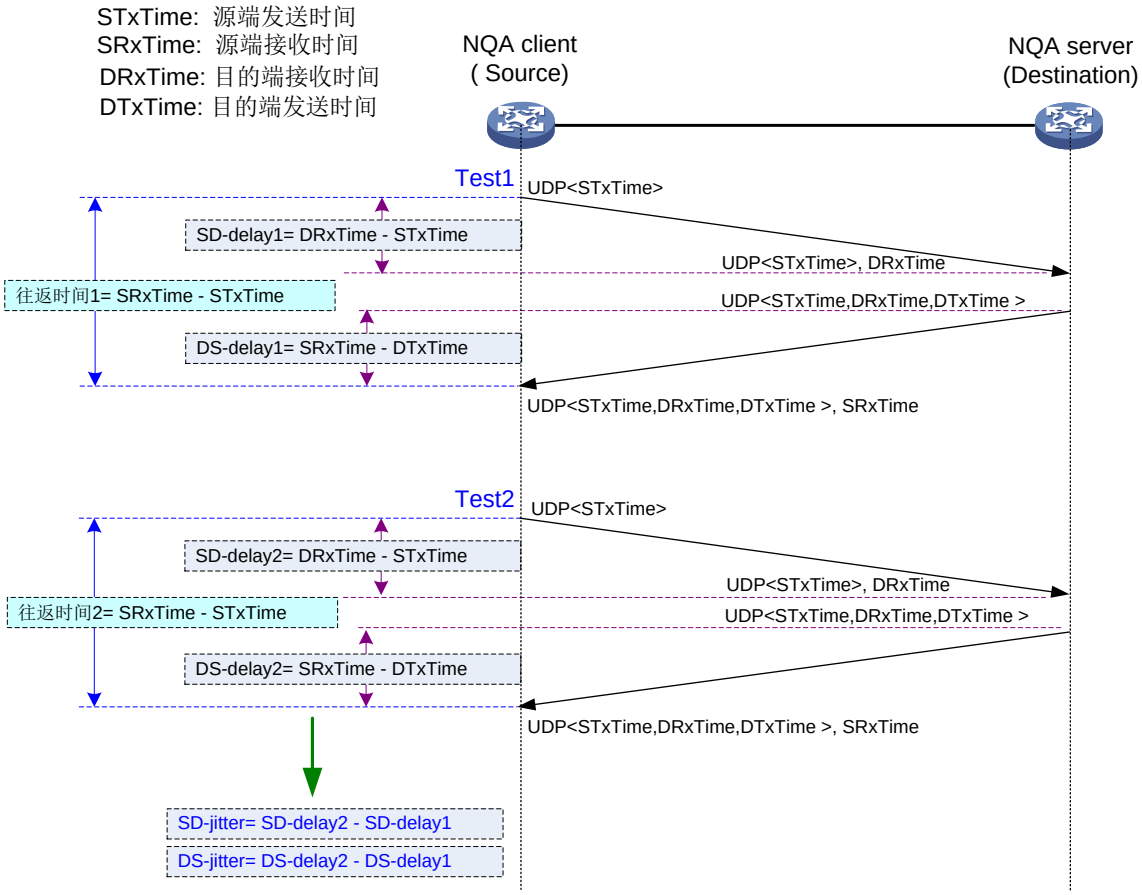
(1) UDP-jitter 报文到达 NQA server，NQA server 在报文中加上接收到该报文的时间 DRxTime。

(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。

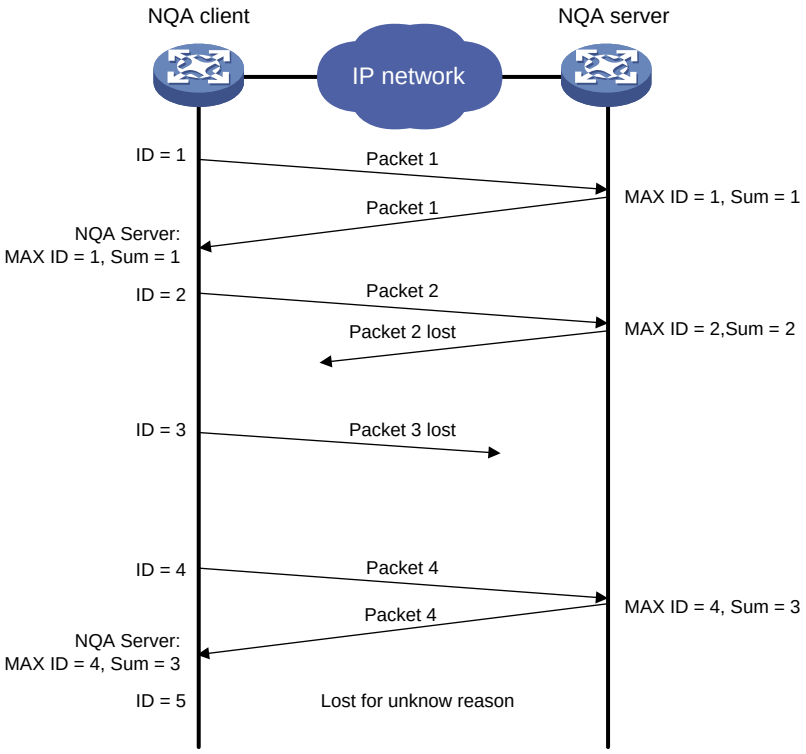
NQA client 可以获取的信息有：

- 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

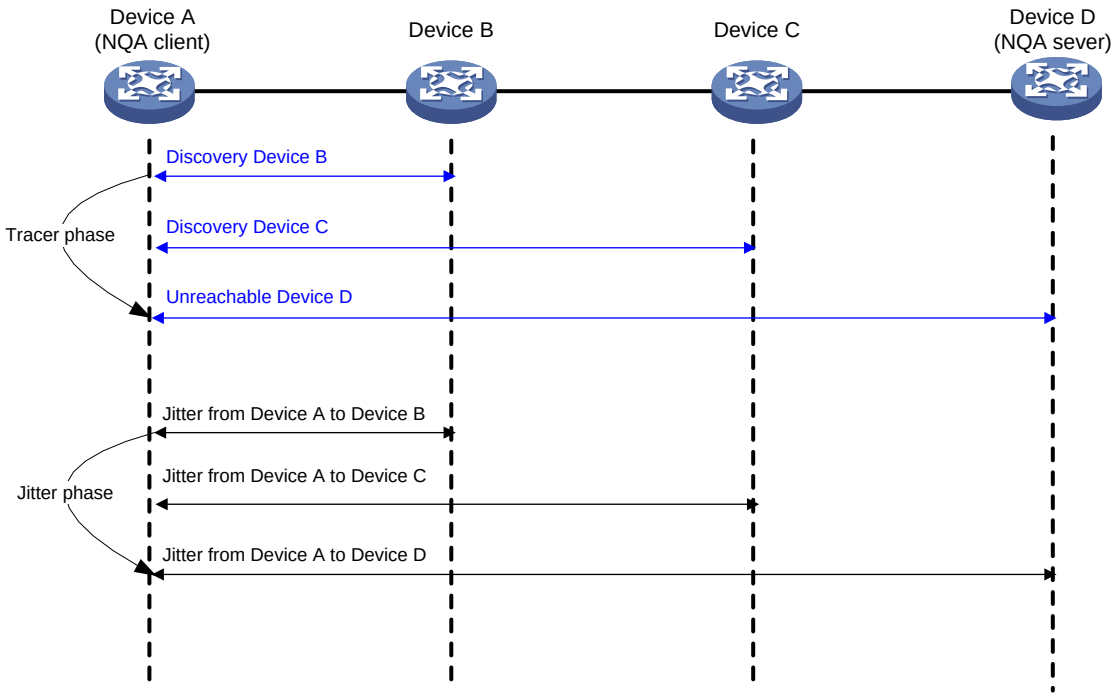
Path-jitter 测试可以作为 UDP-jitter 测试的一种补充，用于在抖动比较大的情况下，进一步探测中间路径的网络质量，以便查找出网络质量差的具体路段。

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：

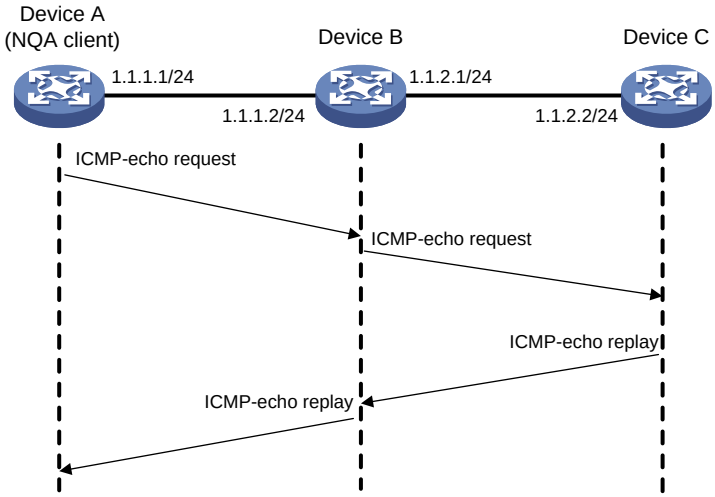
(1) NQA 客户端根据设置的探测时间及频率向探测的目的 IP 地址发送 ICMP echo request 报文。

(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。

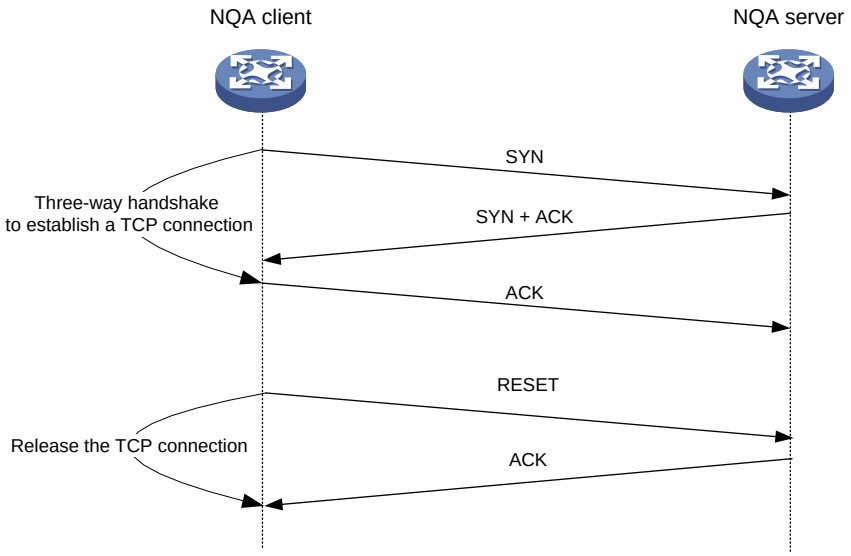
需要注意的是，不能太频繁地发起 TCP 探测，以免占用过多资源，影响目的设备上的正常服务。

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。

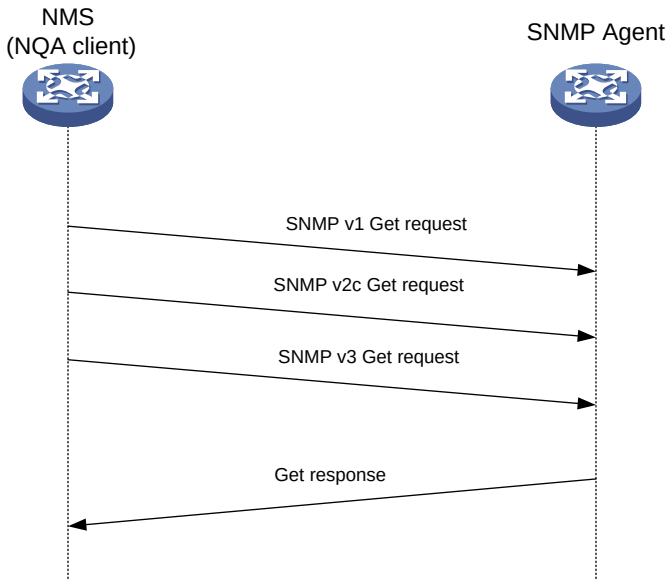
HTTP 测试时，NQA 客户端会向指定地址的 HTTP 服务器发送 GET 请求或者 POST 请求，在接收到回应信息以后，计算整个测试的时间。整个过程只是和 HTTP 服务器建立连接，如果建立连接成功即认为测试成功。

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



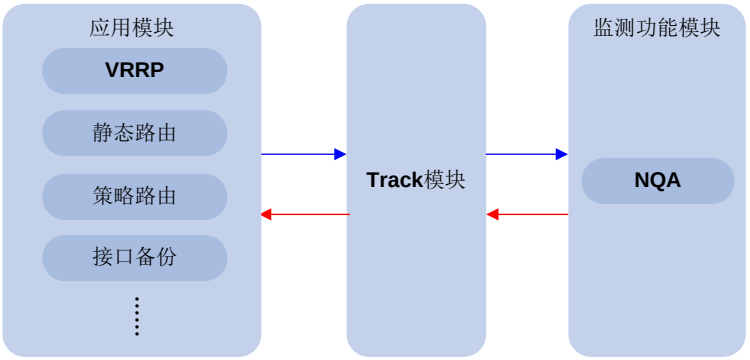
2.2.15 ARP 测试机制

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。UNIS 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

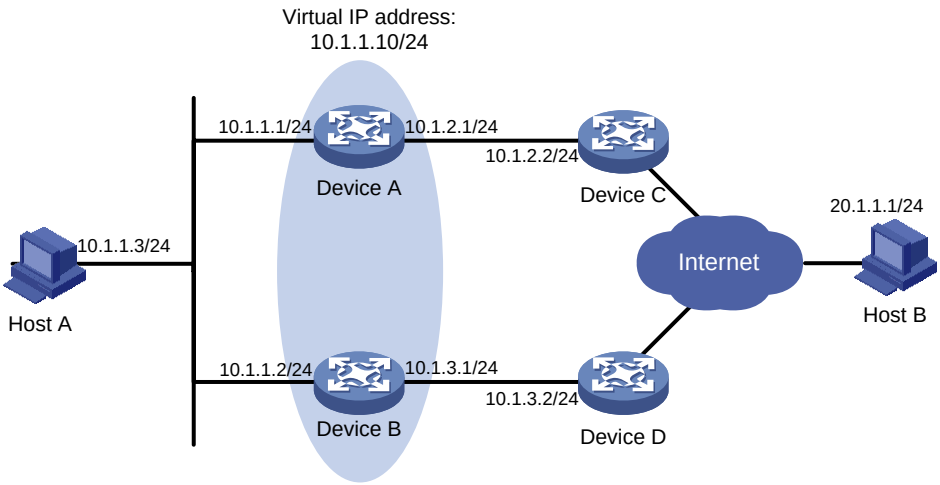
NQA 通常应用在联动功能中。NQA 可以通过 Track 模块，实现与 VRRP、静态路由、备份中心、策略路由联动，以便及时发现网络中的故障，避免通信中断或服务质量降低。

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

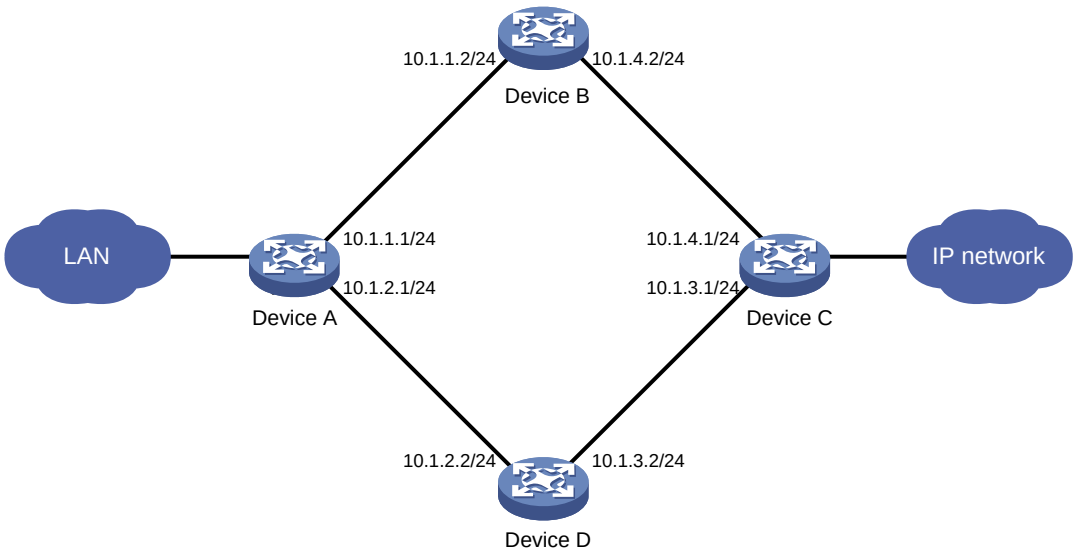


3.2 NQA与静态路由联动

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



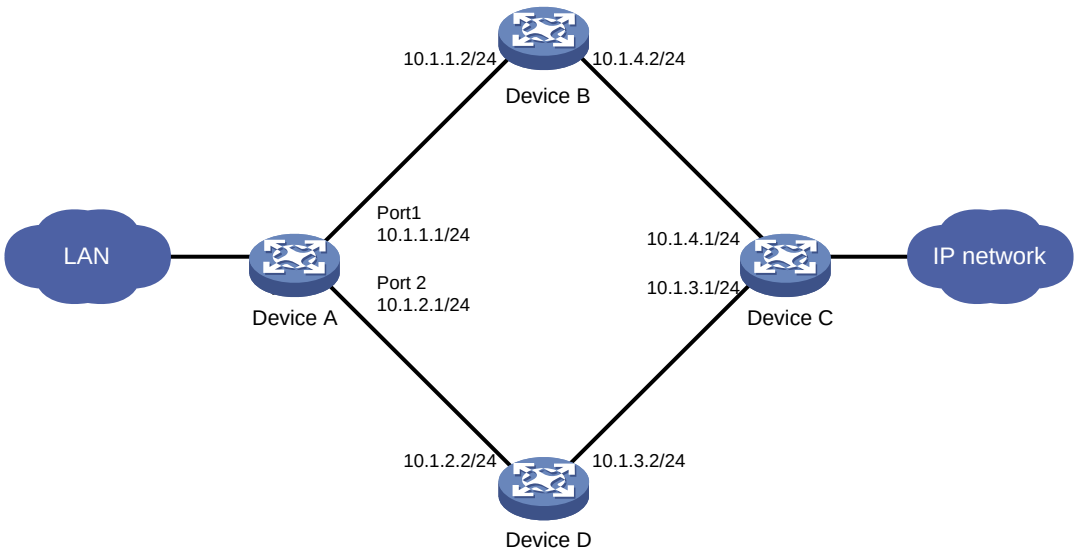
3.3 NQA与接口备份联动

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。

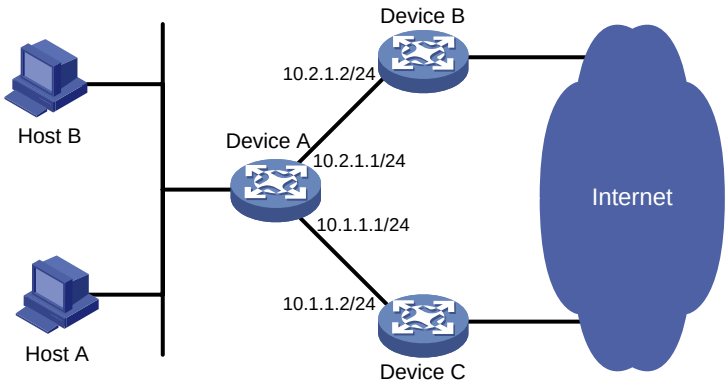



图13 NQA 与策略路由联动组网图