NQA技术白皮书

关键词：NQA、测试、探测、联动、调度

摘　要：随着Internet的高速发展，网络支持的业务和应用日渐增多，为了对网络进行更加精确和实时的监测，用户对网络性能的分析方法提出了更高的要求。H3C公司的NQA（Network Quality Analyzer，网络质量分析）是一种实时的网络性能探测和统计技术，可以对响应时间、网络抖动、丢包率等网络信息进行统计。同时，H3C的NQA结合Track联动，还能为用户的网络提供极佳的可靠性。本文首先介绍基本概念，然后重点介绍相关特性的原理、技术特点以及典型组网应用等。

缩略语：

缩略语	英文全名	中文解释
NQA	Network Quality Analyzer	网络质量分析

目 录

1 概述 3
2 特性介绍 3
2.1 相关术语 3
2.2 测试处理机制 4
2.2.1 ICMP-echo处理机制 4
2.2.2 UDP-echo处理机制 5
2.2.3 UDP-jitter处理机制 5
2.2.4 TCP处理机制 7
2.2.5 DLSw处理机制 8
2.2.6 SNMP处理机制 8
2.2.7 HTTP处理机制 8
2.2.8 FTP处理机制 8
2.2.9 DHCP处理机制 9
2.3 联动功能机制 9
2.4 NQA Server处理机制 10
3 典型组网案例 10
3.1 NQA与VRRP联动 10
3.2 NQA与静态路由联动 11
3.3 NQA与备份中心联动 12
3.4 NQA与策略路由联动 13

1 概述

NQA是H3C公司Network Quality Analyzer（网络质量分析）软件特性的简称。

目前H3C公司全线路由器设备以及部分中高端交换机设备均支持NQA特性。

H3C的NQA特性通过发送测试报文，对网络性能或服务质量进行分析，为用户提供准确的网络性能参数，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

H3C的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，它提供了更多的功能。

目前NQA支持九种测试类型：ICMP-echo、DHCP、FTP、HTTP、UDP-jitter、SNMP、TCP、UDP-echo和DLSw测试。

- 支持多测试组并发

NQA模块支持多个测试组并发，用户可以根据需求手工配置并发个数。但对于DHCP测试，同一时刻只允许有一个测试组进行测试。

- 支持联动功能

2 特性介绍

2.1 相关术语

- NQA agent：NQA 网络测试的客户端。
- NQA server：NQA 网络测试的服务器端。狭义上指 UDP-echo、TCP 和 UDP-jitter 三种测试的 NQA server 端。广义上指所有要被探测的对端设备，如 FTP server、HTTP server 等。

- 测试组：NQA 测试功能是以测试组的形式进行组织，测试组是 NQA 测试功能的最小单位。每一个测试组都具有和测试项目相关的一系列的属性，例如，测试类型，测试目的地址，测试目的端口，测试发包频率等。
- 测试组的标识：测试组由管理员名和操作标签来标识。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。测试组创建之后，可以在测试组视图下配置测试类型，然后进入测试类型视图配置其他参数。
- 探测：一个能够得到完整探测结果的独立过程。对于 TCP、DLSw 测试，一次探测是指一次连接；对于 UDP-jitter 测试，一次探测发送探测报文的个数由用户来设定；对于 FTP、HTTP、DHCP 测试，一次探测是指完成一次相应的功能；对于 ICMP-echo、UDP-echo 测试，一次探测发送一个探测报文；对于 SNMP 测试，一次探测发送三个探测报文。
- 测试：一次测试由若干次连续的探测组成。
- UDP-jitter 探测：每次 UDP-jitter 探测发送一组报文，根据各个回应报文中携带的信息计算探测的结果。
- SD：从源端到目的端。
- DS：从目的端到源端。
- frequency：测试组连续两次测试开始时间的时间间隔。
- 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。
- 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 测试处理机制

2.2.1 ICMP-echo处理机制

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报文来计算网络响应时间及丢包率。

ICMP-echo测试成功的前提条件是目的设备要能够正确响应ICMP echo request报文。NQA客户端会根据设置的探测时间及频率向探测的目的IP地址发ICMP echo request报文，目的地址收到ICMP echo request报文后，回复ICMP echo reply报文。NQA客户端根据ICMP echo reply报文的接收情况，如接收时戳以及报文个数，可以计算出到目的IP地址的响应时间及丢包率，从而反映出当前的网络性能及网络情况。

2.2.2 UDP-echo处理机制

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，需要NQA server端打开对应的UDP端口。RFC 2925中规定7号端口用于UDP-echo，但是一般厂商都未实现。所以当前的UDP-echo测试已经没有端口号这个限制了。

NQA客户端会根据设置的探测时间及频率向探测的目的IP地址发送UDP报文，目的地址收到UDP探测报文后，直接利用该报文进行回复。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。

UDP-echo功能的测试结果和历史记录将记录在测试组中，可以通过命令行来查看探测结果和历史记录。

2.2.3 UDP-jitter处理机制

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。

UDP-jitter测试的报文是H3C与华为公司共同定义的，探测时对端也需要支持NQA并配置NQA server相关参数；目前暂时无法与其他厂商设备互通。

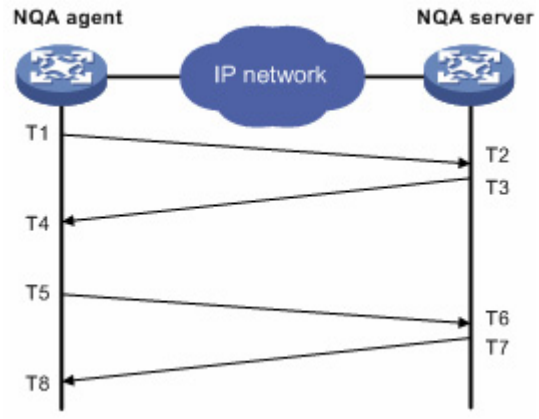

图1 UDP-jitter实现原理

UDP-jitter测试的工作过程如图1所示：

(1) NQA Agent 发送一个 UDP-jitter 报文给 NQA server，并在报文中记录报文离开时间 T1。

(2) 当此 UDP-jitter 报文到达 NQA server 时，NQA server 在报文中加上接收到该报文的时间 T2。

(3) 当此 UDP-jitter 报文离开 NQA server 时，NQA server 再加上报文离开时的时间 T3。

(4) 当 NQA Agent 接收到该响应报文时，记录接收到响应报文的时间 T4。

(5) NQA Agent 以固定发包间隔（T5-T1）发送多个探测报文，重复上述过程。

(6) NQA Agent根据成功收到回应的相邻两个报文的往返时间，分别计算从源端到目的端和从目的端到源端的抖动。以 图 1中所示的两个报文为例：

SD jitter＝（T6－T5）－（T2－T1）＝（T6－T2）－（T5－T1）

DS jitter＝（T8－T7）－（T4－T3）＝（T8－T4）－（T7－T3）

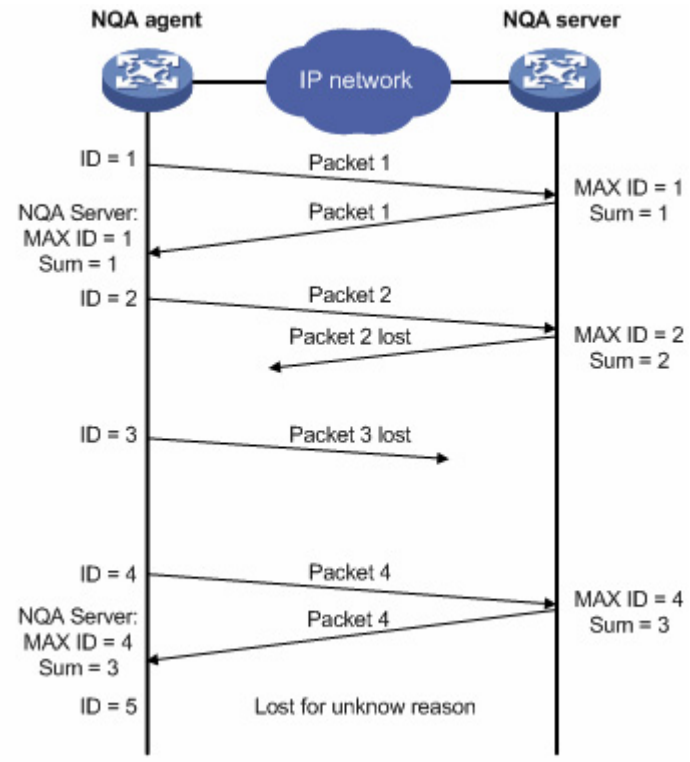

图2 UDP-jitter单向丢包统计原理

如图2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 agent发送的每个报文中都包含报文ID。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 agent；NQA agent

记录回应报文个数，并从回应报文中获取NQA server端信息。

NQA agent可以获取的信息有：

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

根据这些信息可以计算：

SD（源到目的）丢包个数＝NQA server收到的最大报文ID－NQA server端收到报文个数

DS（目的到源）丢包个数＝NQA server端收到报文个数－NQA agent收到报文个数

未知方向上丢包个数＝NQA agent发包个数－NQA agent收包个数－SD丢包个数－DS丢报个数

UDP-jitter可以统计如下信息：报文响应时间、丢包率、报文探测失败原因统计、agent端到server端抖动时延统计、server端到agent端抖动时延统计以及单向丢包统计。

UDP-jitter功能的测试结果和历史记录将记录在测试组中，可以通过命令行来查看探测结果。

📖 **说明：**

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。

2.2.4 TCP处理机制

TCP测试主要是测试客户端和指定的服务器之间是否能够建立TCP连接，以及建立TCP连接所需的时间。

由TCP协议本身的机制完成TCP连接，不能太频繁的发起TCP探测，以免占用过多资源，影响到目的设备上的正常服务。

TCP功能的测试结果和历史记录将记录在测试组中，可以通过命令行来查看探测结果和历史记录。

2.2.5 DLSw处理机制

NQA DLSw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，确认对端设备是否使能DLSw功能。由于NQA的DLSw测试只是测试DLSw是否配置，在实现上和TCP基本一样，可以看作固定目的端口号的TCP测试。

DISw功能的测试结果和历史记录将记录在测试组中，可以通过命令行来查看探测结果和历史记录。

2.2.6 SNMP处理机制

SNMP测试发送SNMP协议报文到指定端口，根据回应确认对端SNMP功能是否开启。在客户端无法指定SNMP服务的版本号。每次测试时会对SNMP v1/v2c/v3三个版本都进行测试，收到任何一个版本的回复，即认为探测成功。不管后续是否还有回应报文，都会同时关闭连接端口。因此SNMP测试无法测出SNMP Server支持哪个版本。

SNMP功能的测试结果和历史记录将记录在测试组中，可以通过命令行来查看探测结果和历史记录。

2.2.7 HTTP处理机制

HTTP测试主要是测试是否可以与指定的HTTP服务器建立连接，从而判断该设备是否提供了HTTP服务以及建立连接的时间。

HTTP测试支持GET和POST操作，即向指定地址的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成功。

HTTP功能的测试结果和历史记录将记录在测试组中，可以通过命令行来查看探测结果和历史记录。

2.2.8 FTP处理机制

FTP测试主要是测试是否可以与指定的FTP服务器建立连接，以及与FTP服务器之间传送文件的时间，可以使用该功能探测任何FTP服务器。

FTP测试支持GET和PUT操作。GET操作并不会把文件放到本地的文件系统，只是计算下载该文件所需要的时间，取得数据后随即自动释放占用的内存；PUT操作并不是将本地文件放到服务器上，而是上传固定大小及内容的文件（文件名由用户配置，数据为系统内部指定的固定数据；如果配置的文件名和服务器上已有的文件重

名，则覆盖原来的文件，测试完成后该文件并不被删除）。因此，FTP测试与本地文件系统无关。

FTP功能的测试结果和历史记录将记录在测试组中，可以通过命令行来查看探测结果和历史记录。

2.2.9 DHCP处理机制

DHCP测试模拟DHCP Client在指定的接口上发起DHCP请求，根据是否申请到地址，确定接口所在的网络中是否有DHCP Server服务以及测试申请到地址的时间。

DHCP测试只是借用操作接口发送DHCP报文，申请到地址后立即释放DCHP租约，不会为接口真正申请地址，因此不会占用DHCP Server的地址资源。进行DHCP测试的操作接口必须处于UP状态。

DHCP功能的测试结果和历史记录将记录在测试组中，可以通过命令行来查看探测结果和历史记录。

2.3 联动功能机制

联动功能是指通过建立联动项，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一定数目时，就触发其他模块联动（UDP-jitter测试不支持联动功能）。联动功能的实现如图3所示。

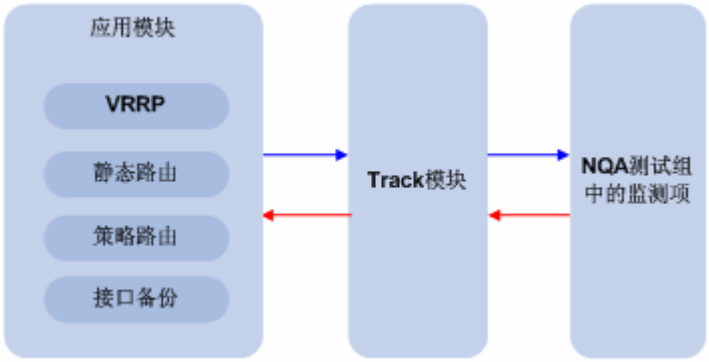

图3 联动功能的实现

联动功能由应用模块、Track模块和监测功能模块三部分组成。Track模块位于应用模块和NQA之间，当监测项的状态发生变化时，监测功能模块通知Track模块，再由Track模块通知应用模块进行相应的处理，从而实现联动。

以静态路由为例，用户配置了一条静态路由，下一跳为192.168.0.88，如果

192.168.0.88可达，那么该静态路由有效；如果192.168.0.88不可达，则该静态路由无效。通过在NQA、Track模块和应用模块之间建立联动，可以实现静态路由有效性的实时判断。如果NQA发现192.168.0.88不可达，NQA将通过Track模块通知静态路由模块，静态路由模块可以据此判断该静态路由项无效。

2.4 NQA Server处理机制

进行UDP-jitter、UDP-echo和TCP测试，需要配置NQA Server进行配合测试。对于UDP-echo测试，NQA server只是简单的把接收的报文直接传回客户端；对于TCP测试，NQA server只是建立监听端口，和客户端建立连接；对于UDP-jitter测试，NQA Server需要在报文中打上时间戳，并且记录当前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

目前H3C的NQA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、策略路由的联动，为用户的网络应用提供较高的可靠性。

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一个指定的数额。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路由器，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。

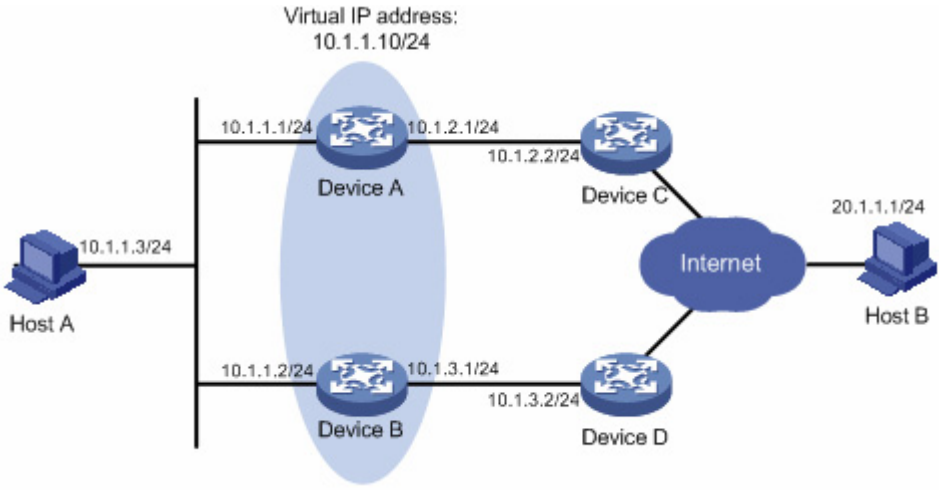

图4 VRRP与NQA联动

如图4所示，在Device A上通过NQA监测10.1.2.2是否可达，配置VRRP通过Track和NQA进行联动。当NQA监测到10.1.2.2不可达时，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路由器，取代Device A转发报文。

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。

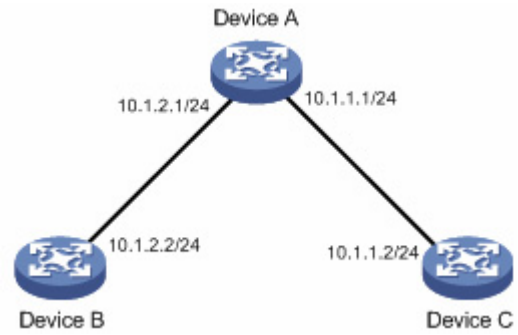

图5 NQA与静态路由联动

如图5所示，在Device B上配置到达Device C的静态路由下一跳地址为10.1.2.1，通过NQA监测10.1.2.1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10.1.2.1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；如果NQA发现10.1.2.1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。

3.3 NQA与备份中心联动

NQA与备份中心联动，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模块通知备份中心，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模块通知备份中心，仍然通过主接口所在的链路通信。

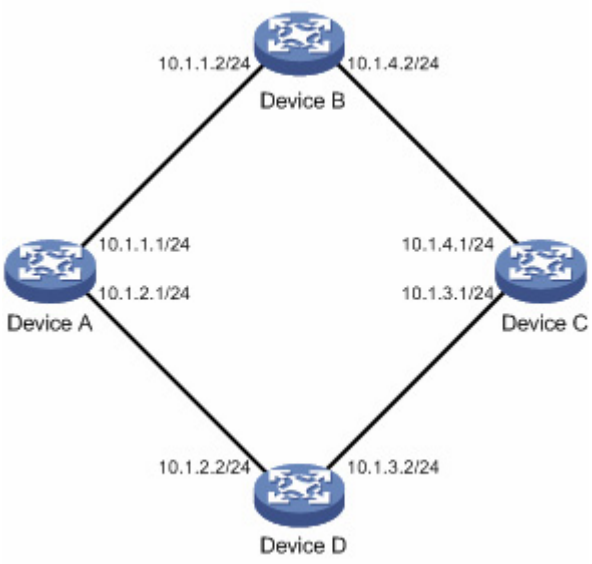

图6 NQA与备份中心联动

如图6所示，Device A可以通过Device B、Device D两条路径达到Device C。正常情况下，数据通过Device B发送给Device C。在Device A上配置备份中心与Track、NQA联动，备份中心配置到Device B的链路为主链路。之后如果NQA监测到通过Device B到Device C的链路不可达，则通过Track模块通知备份中心，主链路切换为A、D之间的链路，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模块通知备份中心，主链路倒换成A、B之间的链路，数据重新通过Device B发送给Device C。

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。