Testing Quality of Service

Application Note

Comprehensive QoS validation requires a large scale of mixed traffic of different classes and types. The Agilent N2X simplifies QoS testing with per field statistics and scalable traffic generation.
Introduction

In the context of networking, quality of service (QoS) refers to various technologies in which traffic flows are classified and given forwarding preference on the basis of assigned priority levels. QoS strategies create better utilization of network resources by giving delay-sensitive and mission critical applications precedence over lower-priority streams during periods of network congestion.

QoS priority information is carried at Layer-2 in the VLAN tag’s user priority field and at Layer-3 in the IP packet header’s IP Precedence or differentiated services Code Point (DSCP) field. Using six bits, the DSCP field is capable of defining 64 service levels. Each service level corresponds to a Per-Hop-Behavior (PHB) that defines the relative priority and QoS parameters that a packet should be given by each node in a Differentiated Services (DS) domain. As differentiated services marks each packet with specific service-level requirements, routing decisions can be made on per-packet rather than per-session basis. This application note describes how to use the N2X test system to test the SUT’s implementation of Layer-3 QoS based on different DSCP service levels.

QoS testing based on VLAN traffic with different priority levels is described in a separate application note “Testing Quality of Service with the RouterTester900 Application”.

Test Challenges

Since QoS agreements must be based on realistic guarantees, it is important to verify that routers supporting QoS must provide the following features:

- Appropriately mark different classes of traffic based on the QoS policy set.
- Allocate at least the minimum bandwidth guaranteed to each priority traffic stream.
- Limit the bandwidth allocated to certain traffic class to avoid starving other traffic classes of bandwidth.
- Keep latency and jitter within acceptable limits.

Testing if a router implements the above features correctly in real-life QoS situation requires that different traffic classes are injected into the router under test. N2X is capable of generating in large scale a rich mix of application-like traffic classes and types, and hence is able to fully satisfy this test requirement. In the context of this application note, traffic classes are based on different DSCP values and destination IP addresses. In addition, user may also assign traffic classification using the Real-time Transport Protocol (RTP) and defined UDP port range.

Testing with Agilent N2X

Agilent N2X is the industry’s most comprehensive test solution for testing the development and deployment of network services for converging network infrastructures. Service providers, network equipment manufacturers (NEMs), and component manufacturers can verify service attributes of entire networks end-to-end, while also isolating problems down to individual networking devices and subsystems.
N2X simplifies Layer 3 QoS testing through its scalable and flexible traffic generation and extensive measurement capability. N2X can generate wire-speed traffic streams of varying classes, types and service priorities simultaneously. Using a concept called a stream group, the N2X Flexible PDU Builder makes it easy to build streams of Layer-2 to Layer-7 Protocol Data Units (PDUs) containing multiple encapsulations and even proprietary formats. You can define a packet length distribution and common header type, then edit any field, including the payload. Different packet lengths and profiles can be applied to each of the generated streams so that the effects of these parameters on a router’s QoS performance can be determined.

N2X also delivers performance measurements in real time to help you identify the router’s QoS performance. Real-time statistics can be viewed on either a per-field, per-stream or per-port basis. Using the per-field statistics view, you can easily view statistics on packets that have a particular value in a field such as different DSCP field values. N2X also provides the Highlight Errored Streams measurement which detects and highlights any measured statistical values that are outside a user defined range (for example, throughput that falls below a guaranteed bandwidth, or latency that exceeds an expected QoS).

Agilent N2X provides this level of testing at full scale. The test can include 256 test ports per system, with 15 traffic profiles and up to 1023 – 4095 stream groups per port, depending on the port type. In total, N2X can generate and measure statistics on 32,768 streams per port, using either four separate measurements over 32,768 streams or twelve measurements over 4,096 streams.

**Test Description**

This application note describes how to use the N2X test system to test a device’s ability to mark and remark packets; guarantee minimum per-flow bandwidth to priority streams; and limit bandwidth allocated to real-time voice and video traffic. It also describes how latency and jitter measurements can be collected for performance evaluation purposes.

**Test Configuration**

As shown in figure 1, a source test port sends IP traffic with different DSCP service levels to a destination test port through the system under test (SUT). A second source port sends traffic to oversubscribe the SUT’s output port to test its ability to apply the correct quality of service during network congestion.
Test Steps

This note does not illustrate the following preamble steps:

i. Select the source and destination ports.
Select three Ethernet ports to act as source and destination ports.

ii. Bring up the physical layer.

iii. Resolve the Link Layer.

iv. Add IPv4 address pools to the test ports.
On each test port, add one address pool on network 162.x.70.x and another one on network 162.x.90.x.

v. Setup traffic on the first source port (test port 1).

a. Generate voice traffic
A sample frame format of voice traffic that uses codec G.711 is shown in table 1.

<table>
<thead>
<tr>
<th>Ethernet header</th>
<th>IP header</th>
<th>UDP header</th>
<th>RTP header</th>
<th>RTP Payload</th>
<th>FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 bytes</td>
<td>20 bytes</td>
<td>8 bytes</td>
<td>12 bytes</td>
<td>160 bytes</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 1

Add a StreamGroup. Build the above frame format to emulate voice traffic. Using the field modifier feature, create 100 flows of the voice traffic. Set the traffic profile load to 5000 frames/s to correspond to a voice flow rate of 1 packet every 20ms. Name the StreamGroup and profile “voice” and “Profile_Voice” respectively.

(Tip: To emulate voice traffic that uses a different codec, change the RTP payload size and the profile load accordingly.)
b. Generate video traffic
A sample frame format using MPEG2 TS is shown in table 2.

<table>
<thead>
<tr>
<th>Ethernet header</th>
<th>IP header</th>
<th>UDP header</th>
<th>RTP header</th>
<th>RTP Payload</th>
<th>FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 bytes</td>
<td>20 bytes</td>
<td>8 bytes</td>
<td>12 bytes</td>
<td>1316 bytes total (188 bytes each)</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 2

On a new traffic profile, add a StreamGroup. Build the above frame format to emulate MPEG2 TS video traffic.

Using the field modifier feature, create 10 flows of the video traffic. Set the traffic profile load to 2 Mbps. Name the StreamGroup and profile “video “Profile_Video” respectively.

c. Generate priority data traffic
On a new profile, add a StreamGroup with DSCP service level set to CS1 to emulate priority data flows. Create 30 flows of the priority data traffic. Set the traffic load to 9 Mbps. Name the StreamGroup and profile “priority data” and “Profile_Priority_data” respectively.

d. Generate regular data
On a new profile, add a StreamGroup with DSCP service level set to Default to emulate regular data flows. Name the StreamGroup and profile “data” and “Profile_Data” respectively.

This note assumes that the user has completed the above preamble steps prior to executing the test steps hereafter illustrated:
**Step 1: Check Packet Marking and Remarking**

Send traffic and verify using per-field statistics view that some packets coming back from the SUT are marked with DSCP value CS3 and no packet is marked with DSCP values EF and AF41.

Change the IP destination address of the voice and video traffic to 162.x.90.x and 162.x.70.x respectively. Check that voice and video packets are now marked with DSCP values EF and AF41 respectively.

Using per-stream statistics view, verify that all voice and video streams are correctly marked by the SUT.

**Step 2: Check the Per-Flow Bandwidth Allocation**

Using the Highlight Errored Streams feature, verify that each priority data stream is provided with the minimum bandwidth guaranteed. Over-subscribe the destination port by sending regular data traffic from the second source port and verify that minimum bandwidth is guaranteed to priority data during traffic congestion.

**Step 3: Check Per Traffic Class Bandwidth Allocation**

Increase the amount of video and priority data traffic and vary the regular data traffic from the second source port in incrementing steps. Verify that video traffic is bandwidth limited and priority data traffic has guaranteed minimum bandwidth.

**Step 4: Measure Latency and Jitter**

Measure average and maximum latency statistics on voice and video traffic. Capture the voice and video packets and generate their capture analysis results.

**SUT Setup**

Configure the router with the following QoS policy:

<table>
<thead>
<tr>
<th>Traffic Class</th>
<th>Policy</th>
</tr>
</thead>
</table>
| Voice         | • 80k each call.  
  • Maximum 20% of total available bandwidth in the link.  
  • Lowest latency possible.  
  • Packets marked as EF. |
| Video         | • 2 Mbps per user.  
  • Maximum 40% of total available bandwidth in the link.  
  • Lowest latency possible.  
  • Packets marked as AF41. |
| Priority Data | • Max 300k per flow.  
  • Oversubscribed data will be remarked to normal data.  
  • Minimum 10% of available bandwidth in the link.  
  • Packets marked as CS3. |
| Data          | • Remaining bandwidth. |
Addressing Scheme

Map destination addresses to different classes of traffic according to the following addressing scheme. Configure the router to mark different classes of traffic based on their destination IP address.

162.1.1.1 - 162.255.1.255 – Priority data (IP DSCP = CS3)
162.1.1.1 - 162.255.1.255 – Data (IP DSCP = Default)
162.1.70.1 - 162.255.1.255 – Video (IP DSCP = AF1)
162.1.90.1 - 162.255.1.255 – Voice (IP DSCP = EF)
Step 1: Check Packet Marking and Remarking

1. In the Results – Realtime area, double click on the third test port (destination port) to display its Measurement Properties dialog.
2. Choose to collect measurements based on Field values and select `ipv4_diffserv_codepoint` from the Field dropdown list.

   ![Figure 2: Selecting ipv4_diffserv_codepoint from the Field dropdown list](image)

3. In the Main View’s toolbar area, click the Traffic button to start traffic.
4. Click the Setup button in the Results- Realtime area to display the Setup Measurement dialog.
5. Select the Fields tab to view per-field statistics. Verify that no packet is coming back marked as EF (Expedited Forwarding, DSCP decimal value = 46) and AF41 (Assured Forwarding 41, DSCP decimal value = 34). Also verify that some packets are coming back marked as CS3 (DSCP decimal value = 24) by the router.

   ![Figure 3: Selecting the Fields tab to view per-fields statistics](image)
6. Stop traffic and change the destination IP addresses of the voice traffic to be on network 162.x.90.x.
7. Start traffic again. Verify in per-field statistics view that some packets are coming back marked as AF41 and EF by the router. Stop traffic.
8. From the N2X Packets and Protocols main window, click **Tools>Frame Matcher Library Editor** to open the Frame Matcher Library dialog.

![Frame Matcher Library dialog](image)

**Figure 4: Opening the Frame Matcher Library dialog**

9. In the **Frame Matcher Properties** area, select the check box next to **Pattern** and click **Edit Patterns** to open the Pattern Library Editor dialog.

![Pattern Library Editor dialog](image)

**Figure 5: Open the Pattern Library Editor dialog**

10. In the **Pattern details** area, select the Protocol type as **ipv4** and name the pattern as “AGT_PATTERN_dscp46”.
11. In the **Field Details** area, select ds_codepoint and set its decimal value to 46. Click **Exact** to match exactly.
12. Click **Done** to apply the settings and click Close to exit the dialog.

![Figure 6: Pattern Library Editor dialog](image)

13. Back in the Frame Matcher Library Editor dialog, select **AGT_PATTERN_dscp46** from the Pattern dropdown list.
14. Click **Apply** and close the dialog.

![Figure 7: Selecting AGT_PATTERN_dscp46 from the Pattern dropdown list](image)

15. Bring up the Measurement Properties dialog on the destination port. Select measurements to be collected based on **Stream IDs**.
Click the **Setup** button in the Results – Realtime area to open the Setup Measurement dialog box.

On the **Measurements** tab, select the check box next to **Rx Expected Stream Field Mismatches #0**.
18. Start traffic.
19. View per-stream statistics on the Streams tab and verify that the **Rx Expected Stream Field Mismatches #0** statistics is zero for all voice streams.

![Figure 10: Viewing per-stream statistics](image)

20. Repeat as per sub-steps 8 to 19 described above to verify that all video streams coming back from the router are marked correctly with DSCP value AF41 (or decimal value 34). Set the destination address of the video streams to be on network 1622.x.70.x in the StreamGroup Properties dialog. Set the decimal DSCP value to match 34 in the Pattern Library Editor dialog.
Step 2: Check the Per-Flow Bandwidth Allocation

1. Stop traffic.
2. On the Streams tab of the Setup Measurements dialog, multi-select all 30 priority data streams. Right click on the highlighted streams and select Add to Measurements Table. All 30 priority data streams are added to the measurement table in the Results – Realtime area.

3. On the Measurements tab, select the check box next to Rx Test Throughput (Mb/s)

4. Click the Highlight Errored Streams icon to open the Highlight Errored Streams dialog.
5. From the Measurement dropdown list, select **Rx Test Throughput (Mb/s)**. Set the minimum and maximum values to 0.3 Mb/s and 100 Mb/s respectively.

![Figure 13: Measurement dropdown list](image)

6. Start traffic and verify that each stream is getting the minimum bandwidth. A stream that is not getting a bandwidth within the range specified is marked with a red “x”.

![Figure 14: Starting traffic](image)

7. Stop traffic.
8. In the Setup-Traffic area, select test port 2 to act as the second source port.
9. Add a new StreamGroup on Profile 1 and double click on it to open its StreamGroup Properties dialog.
10. Name the StreamGroup “over_Sub”. Define the packet length in terms of Layer 3 packet and set the third test port as the destination port.

![Image](image1.png)

Figure 15: Starting traffic

11. On the Packet Template tab of the StreamGroup Properties dialog, expand the Priority field and select Diff-serv. Expand the PHB field under the Diff-serv tree, and select Default to set the DSCP value to Default.

![Image](image2.png)

Figure 16: Packet Template tab of the StreamGroup Properties dialog

12. Start traffic to inject more data traffic from the second source port to the same destination port.

13. Verify that the allocated bandwidth for the priority data traffic is maintained above the minimum 300k.
Step 3: Check Per Traffic Class Bandwidth Allocation

1. Stop traffic.
2. In the Setup – Traffic area, select test port 1.
3. Double click on **StreamGroup video** to open its StreamGroup Properties dialog.
4. Select the Packet Template tab. Under the Destination address field, change the value of Count to 25 to increase the number of video streams to 25.

![Figure 17: Increasing the number of video streams](image)

5. Double click on **Profile Video** to open its Profile dialog and change the Layer 3 Load to 50 Mb/s.

![Figure 18: Changing the Layer 3 Load](image)
6. Repeat as per sub-steps 3 to 5 described above, increase the number of priority data streams to 50 and increase the Layer 3 profile load to 15Mb/s.
7. In the Results – Realtime area, double click on the third test port (destination port) to display its Measurement Properties dialog.
8. In the Measurement index area, choose to collect measurements based on Field values and select `ipv4_diffserv_codepoint` from the Field dropdown list.

![Figure 19: Changing the measurement properties](image1.png)

9. Click the **Setup** button in the Results- Realtime area to display the Setup Measurement dialog.
10. Select the **Measurements** tab and check the box next to **Rx Throughput (Mb/s)**.

![Figure 20: Setup Measurement dialog box](image2.png)

17
11. In the Main View’s toolbar area, click the Traffic button to start traffic.

12. Click on Fields tab to view per-field statistics. Check how much video and priority data is forwarded by reading the Rx test Throughput value beside DSCP value 34 and 24 respectively.

13. Increment the traffic load on the second source port to observe the effect of over-subscription on the video and priority data forwarding performance.
   (Tip: To disable a traffic stream, disable its profile. Otherwise, traffic has to be re-started to re-enable the stream.)

14. Verify that the video traffic has a fixed bandwidth indifferent of other traffic and priority data traffic has a minimum bandwidth of at least 10 Mb/s.
Step 4: Measure Latency and Jitter

1. Stop traffic.
2. In the Results – Realtime area, double click on the destination port to bring up its Measurement Properties dialog. Select measurements to be collected based on Stream IDs.
3. Click the Setup button to open the Setup Measurement dialog box.
4. On the Measurements tab, select the check box next to Maximum Latency and Average Latency.

```
Figure 22: Select Maximum Latency and Average Latency in the Setup Measurement dialog box
```

5. Start traffic.
6. On the Streams tab, view the per-stream real-time statistics results. Click on the show measurement icon if statistics are not displayed.

```
Figure 23: Viewing the per-stream real-time statistics results in the Streams tab
```
7. From the N2X Packets and Protocols window: Setup bar, click the **Capture** button to display the Setup - Capture area.

![Figure 24: Click the Capture button to display the Setup - Capture area](image)

8. Right click on the destination port (test port 3) and select **Properties** to open the Capture Properties dialog.

![Figure 25: Capture Properties dialog](image)
9. On the Triggers and Filters tab, click the **Edit Frame Matches** button to open the Frame Matcher Library Editor dialog.

Figure 26: Click the Edit Frame Matches button to open the Frame Matcher Library Editor dialog

10. Click the **Edit Pattern** button to open the Pattern Library Editor dialog.

Figure 27: Pattern Library Editor dialog
11. Click the Add button to add a new pattern matcher. In the Field details area, set the source and destination addresses to match that of the first voice stream exactly. Click Done to apply the changes.

![Figure 28: Set the source and destination addresses to match the first voice stream](image)

12. Repeat sub-step 11 to add a new pattern to match the source and destination address of the first video stream.

![Figure 29: Add a new pattern to match the source and destination](image)
13. Go back to the Frame Matcher Library Editor dialog and click **Add** to add both frame matchers to the destination port.

![Figure 30: Add both frame matchers to the destination port](image)

14. In the Capture Properties dialog, uncheck **Store Frames** on any frame and check **Store Frames** on the frame matcher for the first voice stream. Click **OK** to exit the Capture Properties dialog.

![Figure 31: Uncheck Store Frames](image)

15. Start capture.

16. Stop capture after about 1000 packets are received. Wait for the capture state to become “stopped”.

---

**Figure 30: Add both frame matchers to the destination port**

**Figure 31: Uncheck Store Frames**
17. Double click on the **capture** on the destination port to bring up its packet decode. Click on the **test** icon to show test payload field of the packet. Scroll down the packets to verify they are all from the same stream by checking the **Stream ID** field.

![Figure 32: Verify packets are all from the same stream](image)

18. Click the **Save** icon to save the captured packets.
19. Repeat as per the sub-steps 14 to 17 described above to capture the packets from the first video stream.

![Figure 33: Capture packets from the first video stream](image)

20. From the N2X Packets and Protocols window: **Results** bar, click **Analysis** to switch from real-time statistics view to analysis results view.
21. Click **Capture>Open File** to open the Capture file saved in sub-step 18.
22. In the Setup – Capture area, select both the destination port and the opened capture file by holding down the “Ctrl” key.
23. Click the **Analyze** button to begin analysis.
24. Wait for analysis to finish and the results to show up in the analysis results area.

![Figure 34: Results shown in the analysis results area](image)

25. Click the **+ graph** icon to add both analysis results to the line graph.
26. Click the **D** icon to request a distribution analysis. Click on the bar graph to see the distribution graphs.

![Figure 35: Distribution graphs](image)
Conclusion

The introduction of new IP-based standards coupled with improvements in router architectures is paving the way for end-to-end IP QoS. Testing these emerging technologies before network deployment is essential to ensure their ability to deliver QoS guarantees for new IP-based services.

Powered with its scalable and flexible traffic generation and extensive and versatile measurement capabilities, N2X provides a simple but effective solution to QoS testing so that QoS delivery can be continually improved.

A summary of N2X’s QoS features include:

- Support measurements on many individual subscribers.
- Generate and measure traffic throughput, latency and loss per subscriber.
- Generate and make measurements on stacked VLANs.
- Flexibly measure QoS per service, per subscriber or per customer group.
- Easily switch between loss per subscriber, per service, or per customer group measurements
- Identify lost or remarked packets per stream.
- Highlight non-compliant traffic streams.
This page intentionally left blank.
Agilent N2X

Agilent’s N2X multi-service tester combines leading-edge services with carrier grade infrastructure testing and emulation. The N2X solution set allows network equipment manufacturers and service providers to more comprehensively test new services end-to-end, resulting in higher quality of service and lower network operating costs.

Warranty and Support

Hardware Warranty
All N2X hardware is warranted against defects in materials and workmanship for a period of 1 year from the date of shipment.

Software Warranty
All N2X software is warranted for a period of 90 days. The applications are warranted to execute and install properly from the media provided. This warranty only covers physical defects in the media, whereby the media is replaced at no charge during the warranty period.

Software Updates
With the purchase of any new system controller Agilent will provide 1 year of complimentary software updates. At the end of the first year you can enroll into the Software and Support Agreement (SSA) contract for continuing software product enhancements.

Support
Technical support is available throughout the support life of the product. Support is available to verify that the equipment works properly, to help with product operation, and to provide basic measurement assistance for the use of the specified capabilities, at no extra cost, upon request.

Ordering Information
To order and configure the test system consult your local Agilent field engineer.

Sales, Service and Support

United States:
Agilent Technologies
Test and Measurement Call Center
P.O. Box 4026
Englewood, CO 80155-4026
1-800-452-4844

Canada:
Agilent Technologies Canada Inc.
2660 Matheson Blvd. E
Mississauga, Ontario
L4W 5M2
1-877-894-4414

Europe:
Agilent Technologies
European Marketing Organisation
P.O. Box 999
1180 AZ Amstelveen
The Netherlands
(31 20) 547-2323

United Kingdom
07004 666666

Japan:
Agilent Technologies Japan Ltd.
Measurement Assistance Center
9-1, Takakura Cho, Hachioji-Shi,
Tokyo 192-8510, Japan
Tel: (81) 426-56-7832
Fax: (81) 426-56-7840

Latin America:
Agilent Technologies
Latin American Region Headquarters
5200 Blue Lagoon Drive, Suite #850
Miami, Florida 33126
U.S.A.
Tel: (305) 269-7500
Fax: (305) 267-4286

Asia Pacific:
Agilent Technologies
18/F, Cityplaza One, 1111 King’s Road,
TaiKoo Shing, Hong Kong, SAR
Tel: (852) 3197-7777
Fax: (852) 2506-9233

Australia/New Zealand:
Agilent Technologies Australia Pty Ltd
347 Bunwood Highway
Forest Hill, Victoria 3131
Tel: 1-800-629-485 (Australia)
Fax: (61-3) 9272-0740
Tel: 0-800-738-378 (New Zealand)
Fax: (64-4) 802-6881

This information is subject to change without notice.
Printed on recycled paper
© Agilent Technologies, Inc. 2006
Printed in USA April 19, 2006
5989-4241EN

www.agilent.com/comms/n2x