Agilent N2X
Measuring IPTV/ MSTV QoE in Conjunction with IGMPoPPP and IGMPoDHCP

Application Note

Test Objective

This application note shows how to use N2X without the IPTV QoE Productivity Application (PA) to make MDI quality of experience measurements on simulated subscribers. This approach is suitable when dynamic subscriber behavior (e.g., channel changing) and channel zapping measurements are not required. This approach scales to higher levels and does not require the PA license. It is also somewhat simpler in that it only involves a single software product: the main N2X application.

The purpose of this test is to assess Quality of Experience for video subscribers connecting to the network using PPPoE or DHCP. The performance of these access protocols is not the focus of the test. MDI measurements are used to determine whether video Quality of Experience is adequate when the traffic is delivered over PPP or when DHCP-assigned addresses are used. This Application Note also shows how N2X can be used to make MDI measurements on traffic delivered from a third-party source, which could be a video server or a real Microsoft TV system.

Test Set-up

Network Diagram: Testing against a real DUT

Key Features

► Highly scalable per-subscriber video quality metrics
► IGMPoPPP/DHCP support
► Microsoft TV support (MDI and protocol decodes)
► 10 GbE video subscriber/server support
**Intended Audience:**

This test is relevant to engineers building and testing access network equipment, such as a B-RAS, Access Node (DSLAM or PON OLT), Edge Router, Layer 2 switch, BNG, or MSPP, which will be deployed in an IPTV infrastructure. This will be of interest to network equipment manufacturers (including IPTV development test, system test, and Proof-Of-Concept lab groups) and service providers (including service validation and pre-deployment test groups).

**Equipment Required**

**N2X Equipment**
- Two N5551A/B Tri-rate Ethernet ports
- E7881A/B Packets and Protocols License
  - N2X System Release 6.7 or later
- E7888A Access Protocols Software License (for PPP)
- E7887A DHCP Protocol Software License
- E7877A Video Generation and Analysis License
- E7828A IGMP License (for release 6.9 and later only)

**Device Under Test (DUT)**

This particular test assumes that the DUT is acting as an IPv4 multicast (IGMP) replicator. The device must have Ethernet interfaces (Ethernet, Fast Ethernet or GbE), either electrical or optical. Typical DUTs include B-RAS/BNGs, EARs and BSA/BSRs.

**DUT Configuration:**

Configure a single VLAN on DUTSubPort. Appendix 1 provides example N2X and DUT addresses. Each VLAN represents a single subscriber. Create a single VLAN on DUTVidPort.

**Test Instructions**

*This Application Note explains how to:*
- setup link-layer communication
- configure IGMP host emulation
- configure IGMPoDHCP emulation
- configure IGMPoPPP emulation
- create multicast address group pools
- setup multicast traffic
- setup bi-directional background traffic
- monitor MDI statistics by setting up field statistics

**General guidelines for simulating video subscribers:**

1. **Choose a Video Subscriber personality for a test port.**
   - Selecting a wrong personality for the test port will result in inability to get MDI statistics and capture video traffic.
2. **Simulate multiple IGMP hosts.**
   - This test introduces variations of IGMP hosts: IGMPoDHCP and IGMPoPPP.
3. **Define a multicast group pool.**
4. **Set up the IGMP hosts to join the multicast groups.**
   - Setting up subscribers to join the multicast groups represents the broadcast TV and Pay-Per-View channels.
5. **Start IGMP emulation.**
   - The test ports begin sending the IGMP messages to simulate subscribers switching to multicast channels.
6. **Optional: Leave and Join different multicast groups.**
   - This optional step simulates channel-changing subscribers by leaving and joining different multicast groups.
Selecting Ports

1. Click Ports from the main window top tool bar. In Port Selection dialog, select one test port, change its type to “Video Server”. Select another test port. Change its type to “Video Subscriber”. Click Ok.
   Note: These ports can send regular traffic as well, but will be limited due to the video load on them.

2. Click Physical Layer from the main window side tool bar.
3. Configure the ports selected
4. In the Physical Configuration dialog, change the Media Type to SPF if using optical connection, or RJ45 if using copper wire.
   Note: For SPF, Step 5 and 6 must be performed. For other media type, skip step 5 and 6.
5. Click Turn All Laser Off
6. Click Turn ALL Laser On
7. Close physical layer configuration
Resolving Link Layer

Note: To enable a test port to establish a communication link with its connected SUT interface, you must configure its link framing and addressing. There are two ways to do so. For non-GPF protocols like BGP-4, RSVP, IGMP*, and PPPoE*, the link layer configuration and address discovery is through the Link dialog box. You must manually initiate ARP/NDP to resolve addresses. For GPF protocols like DHCP (v4 and v6), MLD, LACP, and MPLS OAM, the link layer configuration is through the <Emulated Devices> Properties dialog box. See N2X Help for details on GPF protocols.

*IGMP and PPPoE becomes part of GPF protocols in 6.9 releases. The link layer configuration is done through the <Emulated Devices> Properties dialog. Address discovery prior to 6.9 needs to be done in the Link dialog box.

For practice purpose, the following procedures describe the link layer setup through the Link dialog box.

8. From the Packets and Protocols window: Setup bar, click Link Layer. The Link dialog box is displayed.
9. Click the Ethernet tab.
10. Click LAN/VLAN Addresses. The LAN/VLAN IPv4 Addresses dialog box is displayed.
11. In the display area, select the LAN or VLAN address pool listed under a tester row. Click Edit.
12. Enable VLAN ID 1 with value being 1.
13. Configure SUT IP Address. (See the Appendix for example N2X and SUT IP addresses) Click OK.
15. On the LAN/VLAN IPv4 Addresses dialog box, click Send All ARP Requests.

Note: Green indicators suggest successful link layer resolution.

Figure 2. Link Layer Configuration
Setting up Multicast Traffic

16. From the Packets and Protocols window: Setup bar, click Video.

17. In the Setup – Video area, remove the default Video Source.

18. From the Setup – Video button bar, click New Video Source. A Video Source row is added. Note: If you have configured the link layer correctly, the IP address for the video source should be your assigned Tester IP Address for the Video Source Port.

19. Select the Video Source row and click on New Channel Pool from the Setup – Video button bar. A channel pool row is added. Double-click on the channel pool row to bring up the <Channel Pool Name> Properties dialog box.

20. Under the Channels tab, enter the Name, Channels, and Video Clip Name.

- Name: e.g. IPTV1
- Channels: 10
- Video Clip: Click Browse, and select Animals_VOD_NTSC_H264_2.1Mbps_06MB.ts

21. Click the Fields tab.

22. Check that VLAN tag is enabled with VLAN ID being 1.

23. In the Layer 3 > IPv4 Destination Address field, select Multicast to simulate a broadcast TV or Pay-Per-View channel sent to multiple TVs at the same time. Enter the first multicast address; see the Appendix for example addresses.

24. To generate 10 unique addresses for all channels in the pool, click Field Modifier > Increment. Change the Prefix length (bits) from 24 to 32.

Figure 3. Configuring Video Source Properties
**Defining a Multicast Group Pool**

A multicast group pool allows you to simulate many multicast groups so that you can send traffic to many different multicast groups at once. In this exercise, it is also used for the subscribers (IGMP hosts and their variations) to identify which multicast groups to join.

25. From the Packets and Protocols window: Setup bar, click Emulation.

26. From the Packets and Protocols window: Menu bar, click Actions > View Multicast Group Pools.

27. Select an IPv4 row and click Add to create a new multicast group pool.

28. Enter the Group Name, First Address, Num Addresses, and Modifier values.
   - Group Name: E.g. Group1_Multicast_Pool
   - First Address: Enter the first address of the multicast address range. See Appendix for examples.
   - Num Addresses: 10
   - Modifier: 1/32

![Figure 4. Multicast Group Pools Setup](image-url)
Creating IGMP Sessions

The IGMP Emulation Software simulates multicast subscribers in the lab, subjecting routers to real-world requests to join and leave multicast groups.

IGMP Host Emulation Setup

29. From the Packets and Protocols window: Setup bar, click Emulation.
30. In the Setup – Emulation area, select the Video Subscriber port row, and click New from the Setup – Emulation button bar.
31. Create a group of 100 IGMP host emulations. Click OK. The IGMP Host Properties dialog is displayed.
   Note: N2X supports sending IGMP over LACP Link Aggregation Groups (LAGs).
32. Click <Click to Add Item> under Ethernet > VLANs. Enter VLAN ID = 1.
   Note: You can configure stacked VLANs by clicking <Click to Add Item> again.
33. Configure the Tester IPv4 fields:
   • From: the first video subscriber tester IP address; for example, 101.1.1.2. See Appendix for other examples.
   • To: the first video subscriber tester IP address incremented by 100 with a prefix of 32. For example, group 1: 101.1.1.101
   • Prefix length: 32 bits
34. Configure the SUT IPv4 fields.
35. Enter the first SUT IP address; for example, 101.1.1.1.
   Note: In releases 6.7 onwards, GPF protocols provide automatic SUT address discovery: anytime N2X encounters a SUT IP address and VLAN combination that does not have an associated MAC address, N2X sends an ARP or NDP message to discover the SUT MAC address.

Figure 5. Creating IGMP Hosts

Figure 6. IGMP Host Properties – VLAN and IP Addresses Configuration
36. Click IGMP Host tab.
37. IGMP version fields: IGMPv2
38. From the button bar, click Group Membership. The Group Membership Profiles dialog box is displayed.
   Note: This dialog box is used to define the multicast groups to be joined and simulate subscribers joining and leaving multicast groups. For IGMPv3 sessions, you can also use it to define the sources that are (not) allowed to send traffic to multicast groups.
39. Under the Group Membership Profiles tab, click Add. Add Multicast Group Pools dialog box is displayed.
40. Enable the multicast group pool that you created from step 28. Click OK.

B **IGMPoDHCP Emulation Setup**

41. Repeat step 29 and 30 to create emulations.
42. Create a group of 100 IGMP Host with DHCP Client emulations. Click OK. The IGMP Host with DHCP Client Properties dialog is displayed.
43. Click <Click to Add Item> under Ethernet > VLANs. Enter VLAN ID = 1.
44. (Optional) Click DHCP Client tab. Configure the properties of DHCP client.
45. Repeat step 36 to 40 to configure IGMP host fields and multicast group membership.

C **IGMPoPPP Emulation Setup**

Note: In 6.9 we support IGMPoPPPoE only. In 6.10, we’ll add IGMPoPPPoEoA and IGMPoPPPoA.

46. Repeat step 29 and 30 to create emulations.
47. Create a group of 100 IGMP Host over PPP Client emulations. Click OK. The IGMP Host with PPP Client Properties dialog is displayed.
48. Click <Click to Add Item> under Ethernet > VLANs. Enter VLAN ID = 1.
49. Click PPPoE tab.
50. Configure IPCP fields.
   • From: the first video subscriber tester IP address; for example, 101.1.1.2
   • To: the first video subscriber tester IP address incremented by 100 with a prefix of 32. For example, 101.1.1.101
   • Prefix length: 32 bits
51. Repeat step 36 to 40 to configure IGMP host fields and multicast group membership.
Creating Background Traffic

You can create some traffic stream groups to simulate a real-world scenario in which video traffic is sent alongside Internet traffic like voice and data. The following procedures describe setup for bi-directional traffic.

52. From the Packets and Protocol windows: Setup bar, click Traffic.
53. In the Setup – Traffic area, select the Video Server port row.
54. Click on New > IPv4 Mesh to create traffic mesh. The TrafficMesh Properties dialog box is displayed.
Note: A traffic mesh controls the distribution and orientation of the traffic across multiple stream groups. It also defines how traffic is routed from sources, through the SUT, to destinations.

55. Distribution: Partial mesh. (This sends traffic from each source to all destinations.)

56. Orientation: Bidirectional. (This sends traffic sources to destinations, and also from destinations to sources.)

57. Click Sources and Destination tab.

58. Select Video Server Port > Add Source.

59. Select Video Subscriber > Add Destination.
60. Observe that a stream group is added to your Video Server port.

<table>
<thead>
<tr>
<th>Name</th>
<th>Packet</th>
<th>L3 Source</th>
<th>L3 Destination</th>
<th>Streams</th>
<th>Connections</th>
<th>Lengths</th>
<th>Destination Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 101/2 (10.0%)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AGT_CONSTANT_PROFILE2 (1480.0 Fps)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TrafficMesh 1/2 IPv4/Ethernet</td>
<td>101.1.1.2</td>
<td>100.1.1.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 12. A Traffic Stream Group Added to the Video Server Port

61. Observe that a stream group is added to your Video Subscriber port.

<table>
<thead>
<tr>
<th>Name</th>
<th>Packet</th>
<th>L3 Source</th>
<th>L3 Destination</th>
<th>Streams</th>
<th>Connections</th>
<th>Lengths</th>
<th>Destination Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 101/1 (10.0%)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AGT_CONSTANT_PROFILE1 (1480.0 Fps)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TrafficMesh 1/1 IPv4/Ethernet</td>
<td>101.1.1.2</td>
<td>101.1.1.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 13. A Traffic Stream Group Added to the Video Subscriber Port


63. Check the VLAN configuration is correct. (VLAN ID is 1 in this lab exercise)

64. Check the Source and Destination addresses are correct. (The source address should be the first Tester IP address for your Video Server port. The destination address should be the first Tester IP address for your Video Subscriber port.)

65. (Optional) Configure the PDU builder to create data-like or voice-like contents.

66. Repeat step 62 to 65 for the Video Subscriber port.

Figure 13B. Source and Destination address
Setting up Field Statistics

Note: In this lab, we would want to monitor MDI statistics based on the channels (multicast addresses).

67. From N2X Packets and Protocols main window: Results - Realtime, click Setup from the button bar. Setup Measurements dialog box is displayed.

68. Under the Measurements tab: Predefined selection combo box > MDI.

69. Click Ports tab.

70. Select the Video Subscriber port row. Click <Port> Measurement Properties dialog box is displayed.

71. Collect measurements based on Field values.

72. From the Field dropdown list, select ipv4_destination.

73. Enter 225.1.0.0 as the Base value. Click OK.

Figure 14. Selecting MDI Statistics
74. Click Fields tab.

75. Highlight multicast addresses that you are interested in monitoring. Right click > Add to Measurements Table.

76. Click Fields tab.

77. Highlight multicast addresses that you are interested in monitoring. Right click > Add to Measurements Table.
Enabling Emulations and Running the Test

To Enable IGMP Host Emulation

78. Enable IGMP Host Emulation.

79. In the Setup – Emulation area, click Actions-IGMP Host from the button bar. Click Join All. 
   Note: You must join the multicast groups in order to receive the multicast traffic. Join and Leave can be done while the traffic is running.

80. Click to start traffic.

81. Observe measurements in the Results – Realtime area. All the MDI statistics are collected. 
   Note: *very important* The MDI statistics MUST be in the cumulative mode. Make sure you enable from the button bar.

82. Stop traffic.

83. Go back to the Setup – Emulation area, click Actions-IGMP Host from the button bar. Click Leave All.

84. Disable IGMP Host Emulation.
To Enable IGMP Host with DHCP Client Emulation

85. Enable IGMP Host with DHCP Client Emulation.
86. In the Setup – Emulation area, click Actions > DHCP Client > Start.

*Note: The state of the emulations will change from Init to Bounded. A bounded state indicates successful IP addresses allocation.*

87. In the Setup – Emulation area, click Actions > IGMP Host > Join All.
88. Repeat step 80 to 82 to start traffic and observe measurements.
89. Go back to the Setup – Emulation area, click Actions > IGMP Host > Leave All.
90. Click Actions > DHCP Client > Release.
91. Disable IGMP Host with DHCP Client Emulation.
To Enable IGMP Host with PPPoE Client Emulation

92. Enable IGMP Host with PPPoE Client Emulation.

93. In the Setup – Emulation area, click Actions > PPPoE Client > Open Connections.

   Note: The state of the emulations will change from Discovery to Established. A Established state indicates successful IP addresses allocation.

94. In the Setup – Emulation area, click Actions > IGMP Host > Join All.

95. Repeat step 80 to 82 to start traffic and observe measurements.

96. Go back to the Setup – Emulation area, click Actions > IGMP Host > Leave All.

97. Click Actions > PPPoE Client > Close Connections.

98. Disable IGMP Host with PPPoE Client Emulation.
Microsoft TV uses a proprietary protocol encapsulation to transmit video traffic over RTP. It uses a form of RFC2250 with Microsoft-specific RTP extensions. N2X can decode this traffic by capturing the data and then using the Flexible Decoder to examine the packets. A XML file is required in order to decode the traffic, and it is important that this XML file is only given to customers who are valid MSTV licensees (i.e. they are customers or partners of Microsoft’s for MSTV). We sell this XML decode file as N5572A.

This section of the lab shows how to use the N5572A to decode this MSTV traffic.

99. Capture some MSTV traffic. In case you do not have an MSTV server in your lab or any source of real MSTV traffic, Agilent can provide a sample capture file.

100. Click Capture. In the Capture window, select the Video Subscriber port.

101. Open a capture file. Select mstv-a-server.cap. This is a file we captured from a real MSTV network at Alcatel.

   a. Click “Decode”.

---

1. This format is documented in a Microsoft Confidential document titled “Microsoft IPTV carriage of MPEG transport: RFC 2250, IPTV extensions, Applications for Ad Splicing”, Geoffrey Smith, March 24, 2006.
102. In the Packet Decode window, select the Flexible Decoder mode.
103. Examine the UDP header in the captured data, and determine which UDP Destination Port number contains the MSTV traffic. Make a note of this number.
104. Go to the directory C:\Program Files\Agilent\N2X\RouterTester900\UserData\Protocols.
105. Edit the file AgtPdu_RTPMSTV.xml.
106. In the first line of XML code: <enum value="7523" name="N2X: RTP for MSTV"…, change this value to the one noted in step 102.
107. Save the file.
108. Exit and restart N2X Packets and Protocols (this reloads the XML file).
109. Repeat steps 100-102.
110. Examine packet #7. Note the RTP MSTV header, and the Extension Bit which signifies the presence of this MSTV extension.
111. Examine the 20-byte MSTV IPTV Header Extension.
112. Notice the NTP (Network Time Protocol) timestamps. These are used in MSTV for timing and synchronization.
113. Examine packet #32. Notice the field “PUSI contained in datagram”. PUSI means “Payload Unit Start Indicator”. This indicates that this packet contains the first packet of a full frame of video. If the Random Access Point (RAP) bit were set, it would indicate that this packet contained an I-frame, or the start of a video sequence!
**Advanced information.**

**PUSI bit**
When DVR systems are generating index files, efficiency can be gained from indicating how long the I-frame for each random-access point is so that reads of data from the disk system can be optimized. The Acquisition Server/repacketizer indicates in the RTP header whether the given RTP packet contains an MPEG transport packet with the PUSI bit set for the pid which is carrying the master stream. This allows client-side DVR to be performed without examining the transport stream at all.

**Random Access Point**
Random access points are signaled using a single bit in the main IPTV extension. This is used by two components downstream from the Acquisition Server. First, the DServer uses this indicator to determine which points are valid ICC start locations without needing to parse the stream and examine the ECMs. Second, the client DVR subsystem uses this indicator to be able to detect random-access points for its index file creation without needing to parse the stream. When this bit is set, the MPEG transport packets starting from the first one contained within the RTP packet are assumed to be acceptable both as an instant channel change start location and as a frame to be displayed during trick modes.

While the Acquisition Server is processing the incoming stream, if it detects that the next MPEG transport packet in the stream indicates the beginning of a random-access point, it will close out the previous RTP packet and begin a new packet, as well as creating the required PAT, PMT, and ECM packets to enable immediate use of the packets upon reception.

114. Now look under MP2T Header in the same packet. You should see 7 MPEG-2 packets contained in this one RTP/UDP packet. Most IPTV networks, including MSTV, pack 7 MPEG-2 TS packets (188 bytes each) into a single UDP or RTP packet.

115. Close the Packet Decode Window.

116. Select the mstv-a-server.cap file again. Click on “View Video”.

117. Watch the video clip! We can demultiplex and view captured MSTV video traffic too. Of course, the encryption has to be turned off.
## Appendix — Example N2X and SUT Addresses

The following table shows example N2X and SUT addresses that allow up to five users to run the test scenario independently at the same time using a single N2X controller.

<table>
<thead>
<tr>
<th>Video Source Port</th>
<th>User 1</th>
<th>User 2</th>
<th>3</th>
<th>User 4</th>
<th>User 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connector</td>
<td>RJ45</td>
<td>RJ45</td>
<td>RJ45</td>
<td>RJ45</td>
<td>RJ45</td>
</tr>
<tr>
<td>Tester IP Addr</td>
<td>100.1.1.2</td>
<td>102.1.1.2</td>
<td>104.1.1.2</td>
<td>106.1.1.2</td>
<td>201.1.1.2</td>
</tr>
<tr>
<td>SUT IP Addr</td>
<td>100.1.1.1</td>
<td>102.1.1.1</td>
<td>104.1.1.1</td>
<td>106.1.1.1</td>
<td>201.1.1.1</td>
</tr>
<tr>
<td>Router Interface</td>
<td>FE 1/0</td>
<td>FE 1/2</td>
<td>FE 1/4</td>
<td>FE 1/6</td>
<td>FE 2/1</td>
</tr>
<tr>
<td>Multicast Addr Range</td>
<td>From 225.1.0.10</td>
<td>225.1.0.20</td>
<td>225.1.0.30</td>
<td>225.1.0.40</td>
<td>225.1.0.50</td>
</tr>
<tr>
<td></td>
<td>To</td>
<td>225.1.0.19</td>
<td>225.1.0.29</td>
<td>225.1.0.39</td>
<td>225.1.0.49</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subscriber Port</th>
<th>User 1</th>
<th>User 2</th>
<th>3</th>
<th>User 4</th>
<th>User 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connector</td>
<td>RJ45</td>
<td>RJ45</td>
<td>RJ45</td>
<td>RJ45</td>
<td>RJ45</td>
</tr>
<tr>
<td>Tester IP Addr</td>
<td>101.1.1.2</td>
<td>103.1.1.2</td>
<td>105.1.1.2</td>
<td>107.1.1.2</td>
<td>202.1.1.2</td>
</tr>
<tr>
<td>SUT IP Addr</td>
<td>101.1.100.2</td>
<td>103.1.100.2</td>
<td>105.1.100.2</td>
<td>107.1.100.2</td>
<td>202.1.100.2</td>
</tr>
<tr>
<td>Router Interface</td>
<td>FE 1/1</td>
<td>FE 1/3</td>
<td>FE 1/5</td>
<td>FE 1/7</td>
<td>FE 2/2</td>
</tr>
<tr>
<td></td>
<td>From</td>
<td>101.1.1.1</td>
<td>103.1.1.1</td>
<td>105.1.1.1</td>
<td>107.1.1.1</td>
</tr>
<tr>
<td></td>
<td>To</td>
<td>101.1.100.1</td>
<td>103.1.100.1</td>
<td>105.1.100.1</td>
<td>107.1.100.1</td>
</tr>
</tbody>
</table>
Remove all doubt

Our repair and calibration services will get your equipment back to you, performing like new, when promised. You will get full value out of your Agilent equipment throughout its lifetime. Your equipment will be serviced by Agilent-trained technicians using the latest factory calibration procedures, automated repair diagnostics and genuine parts. You will always have the utmost confidence in your measurements.

Agilent offers a wide range of additional expert test and measurement services for your equipment, including initial start-up assistance onsite education and training, as well as design, system integration, and project management.

For more information on repair and calibration services, go to www.agilent.com/find/removealldoubt

www.agilent.com

For more information on Agilent Technologies’ products, applications or services, please contact your local Agilent office. The complete list is available at:
www.agilent.com/find/contactus

Americas
Canada (877) 894-4414
Latin America 305 269 7500
United States (800) 829-4444

Asia Pacific
Australia 1 800 629 485
China 800 810 0189
Hong Kong 800 938 693
India 1 800 112 929
Japan 0120 (421) 345
Korea 080 769 0800
Malaysia 1 800 888 848
Singapore 1 800 375 8100
Taiwan 0800 047 866
Thailand 1 800 226 008

Europe & Middle East
Austria 01 36027 71571
Belgium 32 (0) 2 404 93 40
Denmark 45 70 13 15 15
Finland 358 (0) 10 855 2100
France 0825 010 700*
  *0.125 €/minute
Germany 07031 464 6333**
  **0.14€/minute
Ireland 1890 924 204
Israel 972-3-9288-504/544
Italy 39 02 92 60 8484
Netherlands 31 (0) 20 547 2111
Spain 34 (91) 631 3300
Sweden 0200-88 22 55
Switzerland 0800 80 53 53
United Kingdom 44 (0) 118 9276201
Other European Countries: www.agilent.com/find/contactus
Revised: July 17, 2008

Product specifications and descriptions in this document subject to change without notice.

© Agilent Technologies, Inc. 2008
Printed in USA, July 30, 2008
5989-8866EN

Agilent Email Updates
www.agilent.com/find/emailupdates
Get the latest information on the products and applications you select.

Agilent Direct
www.agilent.com/find/agilentdirect
Quickly choose and use your test equipment solutions with confidence.

Agilent Open
www.agilent.com/find/open
Agilent Open simplifies the process of connecting and programming test systems to help engineers design, validate and manufacture electronic products. Agilent offers open connectivity for a broad range of system-ready instruments, open industry software, PC-standard I/O and global support, which are combined to more easily integrate test system development.

LXI
www.lxistandard.org
LXI is the LAN-based successor to GPIB, providing faster, more efficient connectivity. Agilent is a founding member of the LXI consortium.