Agilent N2X

# Packets Application Software

E7880B
Technical Data Sheet

**Highly scalable and flexible traffic generation and analysis software for verifying the performance of frame and packet-based networking devices.**

Agilent Technologies

## Key Features

- **Measure performance impact across 32,768 clients or aggregates by generating and measuring traffic on over 32,768 transmit/receive streams**
- **Flexibility to test at any layer in the protocol stack by using the versatile PDU builder to build PDUs with any encapsulation and contents**
- **Broad Test coverage via complete user control on any PDU field**
- **Powerful for negative, abnormal or yet to be defined test conditions**
- **N2X Fast Find measurement database allowing quick time to insight through sorting and filtering mechanisms for large quantities of post test results**
- **Comprehensive suite of traffic performance QuickTests including RFC2544 and RFC2889**

## Product Overview

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.

Agilent N2X delivers unparalleled test realism to verify the ultimate performance, scalability and resilience of carrier grade services and infrastructure.

The N2X Packets and Protocols Application enables N2X to verify the traffic forwarding performance, protocol scalability, services delivering capabilities and interoperability of switching and routing devices.

The E7880B Packets Application software enables the most advanced features for flexible multi-port traffic generation and analysis of the N2X . It provides a highly scalable and flexible PDU builder designed to address the specific test needs of a wide variety of Layer 2 and 3 data networking devices such as IP routers, Ethernet/ATM switches, DSL modems, firewalls, and multi-service provisioning devices.

Over 32,000 streams representing individual client transactions can be generated and measured on any port. Each stream can be individually configured down to the bit level. With the large array of predefined frame or packet formats you are able to create realistic traffic at each point in the network.

The traffic can be defined by multiple load profiles, which can be adjusted by a slider control on the GUI so you can observe dynamic changes without stopping a test. In addition, measurements can be made on thousands of streams of L2oMPLS, L2TP, GRE, VLAN, Frame Relay or PPP encapsulated traffic.

But - it's not just about traffic. By adding the E7881B Packets and Protocols Application software plus protocol licenses, support is provided for a range of signaling and routing protocols including:

IPv4, IPv6, BGP-4/BGP-4+/MP-BGP-4, IS-IS, OSPF/OSPF-TE, RIP, LDP/CR-LDP, RSVP-TE, MPLS, GMPLS, IGMP, PIM, PPPoX, L2TP, DHCP, DHCPv6, MLD, LACP, BFD, xSTP, E-OAM, CFM plus more.

These protocols can be used for advertising routes, or for building layer 2 & 3 VPNs. Traffic features of the Packets Application software can be used to send and measure traffic over the simulated network and routes.

# Product Features

## Stream Scalable

Users can generate up to 32,768 transmit and receive streams per port, making it easy to scale your tests beyond the maximum performance parameters of your network or device.

The E7880B Packets Application software provides users with the following key capabilities:

- Transmit and measure up to 32,768 streams per port, transmit billions of flows
- Use stream groups to rapidly define hundreds or thousands of streams
- All managed through an easy to use graphical user interface

## Rapidly Configure Thousands of Streams

The Packets Application software has a user interface specifically designed to easily and quickly set up and make measurements on thousands of streams. Driving this new functionality is a GUI specifically tailored to ease the setup and management of thousands of streams.

## Flexible PDU builder

The Packets Application software has the flexibility to transmit and make real-time measurements on any packet format, from Ethernet frames through to GRE encapsulated packets, plus any user-defined packet format:

- Define and transmit any L2 to 7 PDU
- Manipulate any protocol field - define the entire contents of every single field.
- Users can easily define their own PDU formats and then use the GUI to easily build, transmit then capture and decode custom PDUs
- The flexible PDU builder is a valuable tool that can be used for testing a variety of networking technologies, wireless protocols such as GTP and RTP - the possibilities are endless

## Built-in capture control

Users can capture data on a single port for detailed analysis. This in conjunction with ‘event triggering’ provides a unique ability to identify and isolate performance issues.

## Services, hardware and negative testing

Traffic Generation and Analysis software is used for both highly-scalable testing of service levels as well as precisely controlling the frames sent into networking hardware to validate hardware functionality.

## Services Testing

Services testing measures the ability of a router to deliver service level agreements for thousands of customers:

- Quickly create traffic representing individual customer traffic characteristics
- Individually control the bandwidth offered across 15 different service levels
- Scale the number of generated customer streams up to 32,768 traffic streams per port
- Define billions of traffic flows per traffic stream
- Individually measure packet performance (latency, throughput, packet loss, etc.) on up to 32,768 traffic streams

## Accelerate time to insight

N2X Fast Find provides measurement sorting and filtering mechanisms on 10s of millions of results, helping users find the "worst offending" streams with a single click.

# Hardware and Negative Testing

The Packets Application software has a rich set of features specifically for testing hardware interfaces and for performing negative testing:

- Send precise numbers of packets (i.e. send a single packet)
- Packet payload integrity check detects payload errors (plus PRBS-15 pattern in the payload)
- Specify transmit lengths at layer 2 or layer 3
- On demand traffic injection
- Easily copy/paste/duplicate stream groups
- Supports transmitting/receiving Frame Relay frames on POS interfaces
- Built in capture
- Built in Quickest launch pad
- Specify packet inter-departure times through the API
- Define packet transmit sequence.
- Randomize packet fields, packet payloads and packet lengths for truly randomized packet generation and measurement

This complete set of features makes the Traffic Generation and Analysis software ideally suited for the test needs of hardware test engineers.

## Powerful Analysis

The Packets Application software provides a comprehensive range of graphical and tabular measurement analysis tools to aid fault diagnosis and understand device performance.

- Real-time stream and port statistics
- Real-time histograms for latency and latency variation
- N2X Fast Find for post-test measurement analysis

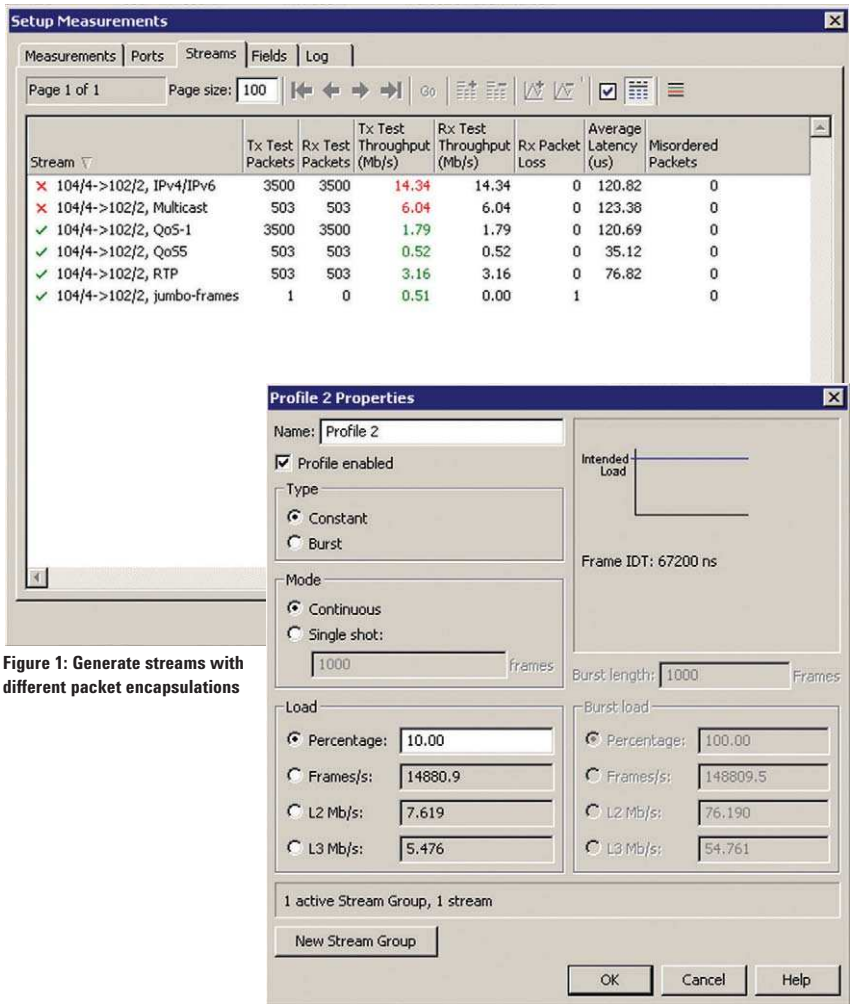


**Figure 1: Generate streams with different packet encapsulations**

**Figure 2: Defining traffic profiles**

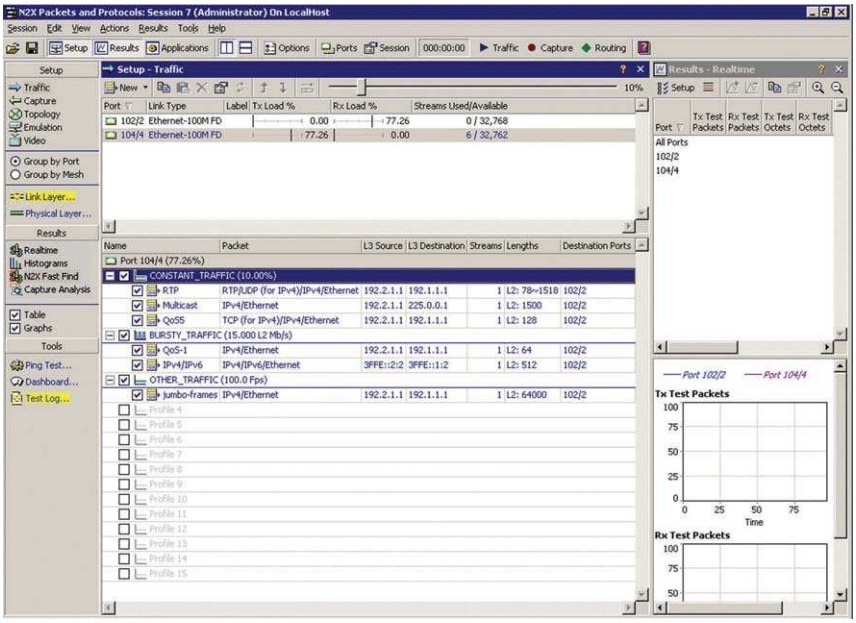


**Figure 3: Applying defined traffic profiles to various traffic streams**

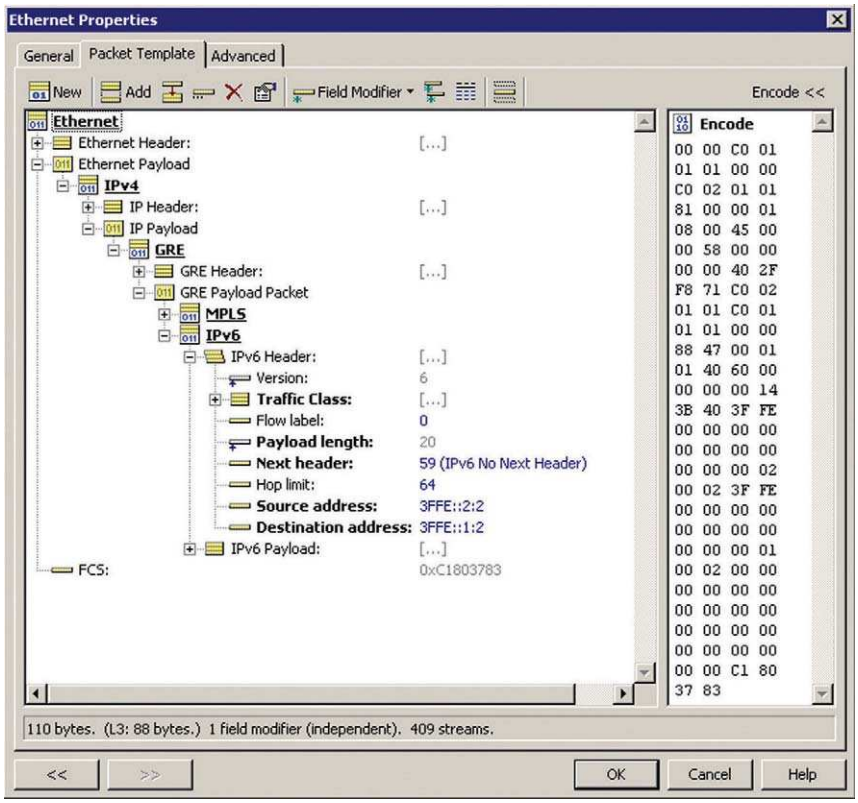


**Figure 4: PDU Builder rapidly builds multi layer encapsulated packets - This is an example of an IPv6 over MPLS over GRE over IPv4 over Ethernet**

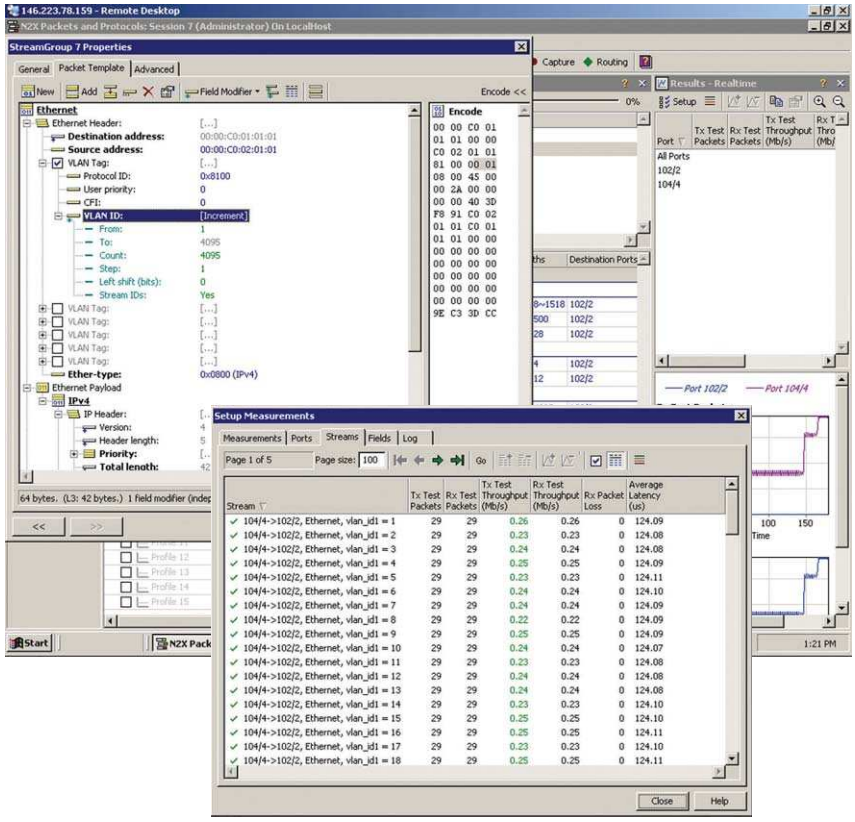


**Figure 5: Make accurate measurements of 32,768 individual streams.**

# Test Scenarios

The Packets Application software was designed specifically for highly scalable packet performance testing. It is uniquely capable of:

- Measuring the throughput of mixed traffic types through a device;
- Ensuring and measuring traffic encapsulation through a router;
- Performing negative testing of networking equipment; and
- Making measurements across thousands of clients.

The following examples detail these unique features of the Packet application.

## Mixed Traffic Throughput

Using the Packets Application Software, you can generate streams with different packet encapsulations. In figure 1 below, six different packet streams are shown: IPv4/IPv6 packets, Multicast, QoS-1, QoS-5, RTP and jumbo-frames.

Agilent's Packets Application software places a test payload into each packet. This test payload carries a timestamp (indicating the time the packet was transmitted), a sequence number, and a packet payload integrity check. Unlike some other test equipment, the receiver automatically finds the test payload, and reports statistics for each stream. You do not have to configure the receiver to tell it where it should find the test payload.

Traffic profiles can be defined using the GUI shown in figure 2 and applied to various traffic streams as shown in figure 3. The traffic load slider control is set at 10%, but can be adjusted for dynamic changes without stopping the test.

## Traffic Encapsulation Testing

Agilent's Packets Application software can be used to quickly create packets with any type of protocol encapsulation, even custom encapsulations.

In Figure 4, a PDU containing an IPv6 packet in MPLS is tunneled through IPv4 using GRE encapsulation. This PDU takes seconds to build, and has proven valuable at verifying the proper handling of tunneled IPv6 packets through a router.

## Negative Testing

The Packets Application software allows you to change any field in any packet. For example, a common negative test is to ensure that an Ethernet interface recognizes the VLAN tag type field.

The PDU Builder is used to create a packet with an invalid VLAN tag type. This packet can be sent once, or repeatedly, to examine how a hardware interface handles packets with invalid values.

## Verify VLAN Performance

The Packets Application software allows you to use the stream scalability to measure the flow of every VLAN user priority (8 levels) for every VLAN ID (4096 values) through an Ethernet switch.

Agilent's Packets Application software is configured to use 8 traffic profiles. Under each traffic profile, 4096 streams are assigned - one stream for every VLAN ID.

In Figure 5 we demonstrate how you can quickly configure up to 32,768 VLAN streams per port.

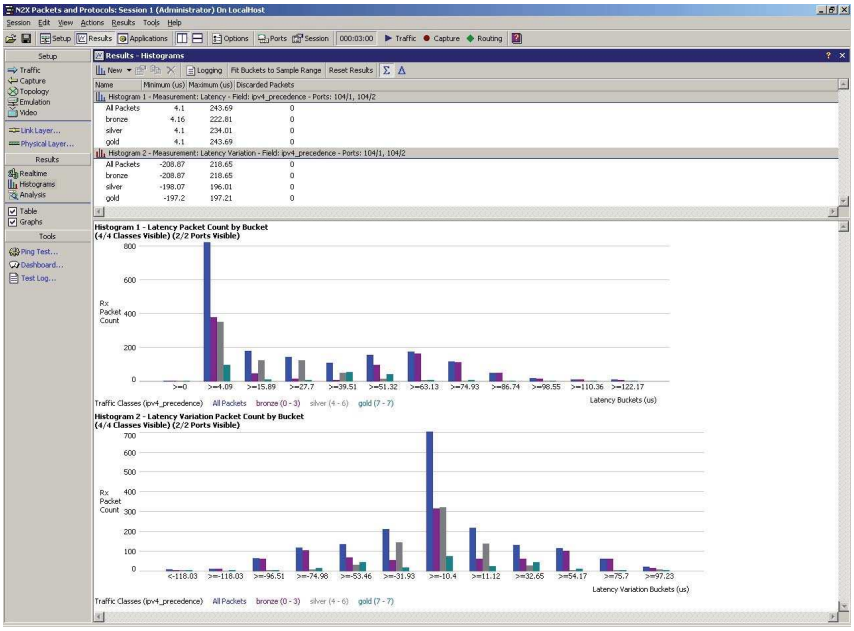


**Figure 6: Analyze latency and latency variation in real-time using auto-calibrated histograms.**

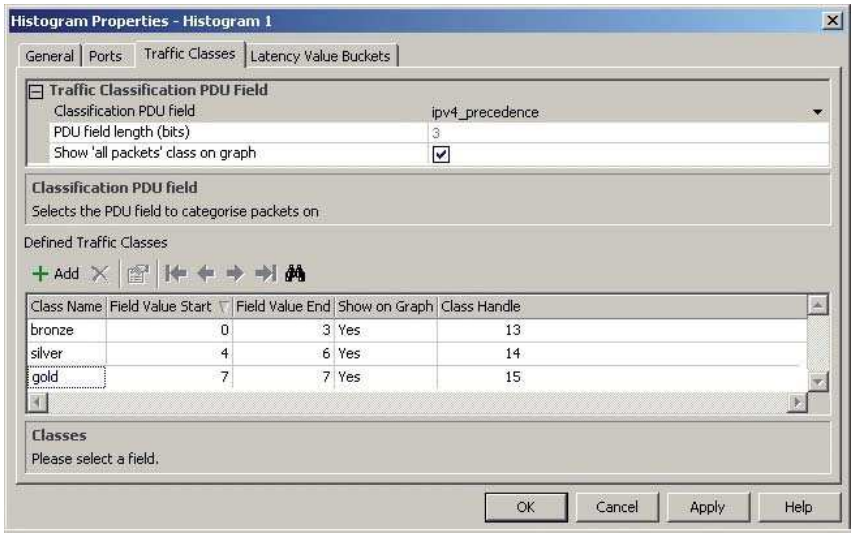


**Figure 7: Define histogram classes to group traffic of different priority for quick analysis using specified Field of Interest values.**

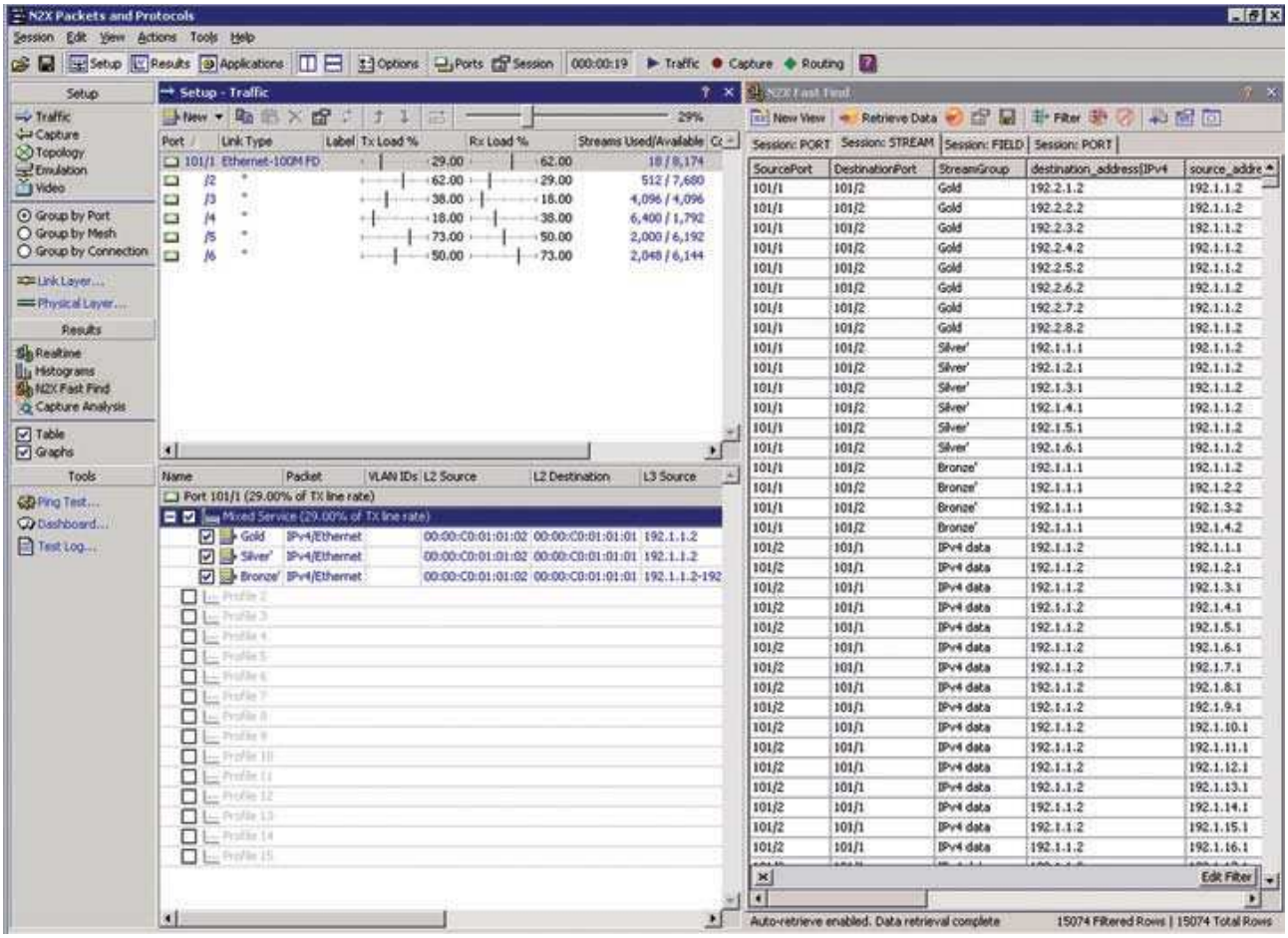


**Figure 8: N2X Fast Find for post-test measurement analysis and accelerated time to insight.**

# Technical Specifications

## Traffic Generation

Agilent's Traffic Generation and Analysis software is designed to make it easy to set up and make measurements on thousands of traffic streams. The traffic generator works as follows.

- Streams are created by defining stream groups. Within each stream group, you use the PDU builder to create a packet template. You can vary the fields in the PDU by assigning a field modifier to cycle through or randomize field values and quickly create 10,000s of streams and millions of flows with ease. Then, you can generate unique stream IDs with one of these modified fields to generate individual streams on which you can make measurements.
- Stream groups can be assigned to traffic profiles. Each traffic profile defines the rate and traffic distribution of the underlying stream groups.

**Streams**

You can define up to 32,768 per interface port

**Stream Groups**

A stream group is a mechanism for quickly defining many traffic streams.

- Up to 4095 stream groups are available per port
- Each stream group consists of a template and a packet length distribution
- A template can define up to 32,768 streams per test port
- Up to 3 field modifiers can be inserted per packet template
- A field modifier can be applied to any field in a frame or packet
- A field modifier can be set to increment or decrement or be random within a range or a user defined list of values
- Unique stream ID can be enabled up to 32,768 distinct streams

A packet length distribution can be:

- Fixed - all frames belonging to the packet template are sent with the same frame length
- Incrementing/decrementing - frames are sent with frame lengths from a specified minimum and maximum length. The length of each successive frame is a specified increment/decrement from the previous frame.
- Random - frames are sent with lengths randomly selected between a specified minimum and maximum length.

**Traffic Profiles**

Each N2X port has 15 traffic profiles.
A traffic profile specifies the mode and distribution of transmitted frames.

**Mode**

- Continuous
- Single shot:
  A single shot mode can be sent at any time

**Distributions**

- Constant and burst distributions are available.
- All loads can be specified in percentage of line rate, frames/s, or Mb/s

**Constant distribution**

Specified by:

- intended load
- frame rate (frames/s)
- throughput (Mb/s)

**Burst parameters**

Specified by:

- average load
- burst load
- burst length (frames)

Traffic loads can be manipulated "on the fly", via the traffic slider bar.

### Real-time Bandwidth Control

The Agilent N2X is the only multi-port traffic generator available that allows the offered bandwidth to be changed in real-time. The immediate effect of bandwidth changes on a device under test are seen by changing the offered load per traffic profile, while observing the real-time statistics.

### Randomness Features

The Traffic Generation and Analysis software can generate purely random traffic.
Up to three 32 bit fields per stream group template are used to randomize any three fields in any packet. For example, you can randomize the Ethernet MAC source address, destination addresses and VLAN tag ID simultaneously.
The length of packets transmitted per stream group can also be randomized, creating multiple random streams of packet lengths.
The payload of transmitted packets can also be randomized.

### IMIX Traffic Generation

The Traffic Generation and Analysis software can be used to easily generate IMIX (Internet Mix) traffic.
A separate stream group can be created for each point in an IMIX distribution. For example, for an IMIX distribution with 40, 552, 576 and 1500 byte packet lengths, a stream group with the packet length fixed to each stream group can be easily created. For individual bandwidth control on each packet length, the stream group can be easily moved to a different traffic profile.

## Frame/Packet Builder

The Traffic Generation and Analysis software includes the industry's most flexible packet creation mechanism.
Packet templates are defined in XML files. Customers can easily create their own packet templates in XML. The XML files are loaded at run-time into the Traffic Generation and Analysis software.
An intuitive GUI gives access to any field in a packet. Any field can be errored or set to any value. Counters can be placed into any field.
Packets with many layers of encapsulation can be quickly and rapidly created in the packet builder. For example, IPv6 packets encapsulated in GRE and tunneled over a martini (layer 2 over MPLS) tunnel can be created in seconds.

**Packet Templates available**

New packet templates are added continuously. Packet templates currently supported include:

- AAL5
- ARP
- ATM Cell
- ATM Payload
- ATP
- BFD
- BGP-4
- Bridge PDUs (spanning tree)
- CDP
- CGMP
- CLNP
- Cisco (Frame Relay)
- Cisco HDLC
- Cisco-NLPID
- DDP
- DHCP
- DHCPv6
- Decnet Phase IV
- Distance Vector Multicast
- EAP
- EAPOL
- EIGRP
- ELAP Encapsulated PPP
- Ethernet
- Ethernet LLC/SNAP
- Ethernet MAC Control
- Ethernet SAP
- Ethernet Slow Control
- Frame Relay
- GMRP
- GRE
- GTP-U
- GVRP
- HSRP
- ICMP
- IETF NLPID
- IETF SNAP
- IGAP
- IGMP
- IGRP
- IPX
- IPv4

**Packet Templates available (continued)**

- IPv6 protocols, including:
  - ICMPv6
  - IPv6 data packets
  - UDPv6
  - TCPv6
- IS-IS
- ISL (Cisco InterSwitch Link)
- L2TP v2 and v3
- LDP
- L2 MPLS (martini) control word
- MDT
- MPLS
- MSDP
- NLPID
- NLPID_PPP
- OAM
- OSPFv2
- OSPFv3
- PAgP
- PIM
- POP3
- PPP-MP
- PPPoE Discovery
- PPPoE Session
- PPPoHDLC
- PWE AAL5 PDU
- PWE AAL5 SDU Data
- PWE ATM 1:1 Cell
- PWE ATM N:1 Cell
- PWE Control Word
- PWE FR Data
- Q.993
- RGMP
- RIP
- RIPng
- RSVP
- RTMP
- RTP
- Raw Data shim
- Raw IPv4 socket
- Raw Layer 2
- Raw payload
- SNAP
- SNAP-Bridged
- SNAP-Bridged-PPPoE
- TCP (IPv4/IPv6)
- UDP (IPv4/IPv6)
- VC-Mux-Bridged
- VC-Mux-Bridged-PPPoE
- VC-Mux-PPP
- VRRP

**Packet lengths**

- Packet lengths are defined as part of the stream group
- Length fields within packet templates (for example, the IP header length) are automatically calculated. Automatically calculated fields can be overridden.

| | |
|---|---|
| **Counters per template (increment capabilities)** | • Three counters can be inserted per packet template.<br>• A counter can be placed into any packet template field<br>• A custom counter can be placed into any place in the packet template, including across packet template field boundaries. |
| **Payload** | The payload in a packet template can be:<br>• Completely specified by the user<br>• Randomized with a PRBS-15 pattern<br>• Autofilled with a user-specified pattern<br>• An incrementing 8 or 16 bit pattern, starting at a specified location in the payload.<br>A packet payload integrity check is placed into the test payload to provide errors on the test payload only |
| **Test payload** | A proprietary test payload can optionally be placed into packets. Including the test payload allows the test system to provide per stream latency, packet loss, misdirected packet, out of sequence packets and packet header and packet payload protection. |
| **Errored packets** | Any field in a packet template can be set to an invalid value for negative testing |
| **Checksum calculations** | • FCS and CRC values in packet templates can be automatically calculated or set to errored values.<br>• Checksums associated with the hardware interface (for example, the CRC-16 for Packet over SONET/SDH interfaces) can be errored. See the appropriate hardware interface data sheet for details. |

## Traffic Analysis

The Traffic Generation and Analysis software provides per-port statistics and per-stream statistics on up to 32,768 streams per port using 64-bit counters.

### Port Statistics

Statistics are displayed for the entire port, including all streams received on that port.

### Stream Statistics

Stream statistics are automatically displayed on the basis of the stream-enabled counter per stream group. For example, if a stream-enabled counter is placed into a VLAN tag ID field, and the counter goes through the range of valid VLAN IDs (0 to 4095), then a stream statistic will be automatically reported for each VLAN ID value. To report stream statistics, a stream group must carry a test payload.
Stream statistics can be reported in summary or detailed mode. Summary mode reports any 12 statistics on up to 4096 streams. Detailed mode reports any 4 statistics on up to 32,768 streams.

### Agilent N2X automatically finds the test payload

The user does not have to specify the location of the test payload. Thus, N2X will report statistics on streams, even if the packet encapsulation changes through a device under test, or if it receives packets with different encapsulations or modified header fields.

### Statistics system details

Statistics are accumulated on the N2X hardware, and are sampled every sampling interval for a total measurement interval period. Statistics can be reported for the last sampling interval, or can be accumulated from the start of the test.
Statistics can be displayed in a table, in bar line charts, histograms or can be logged to a data file.

| | |
|---|---|
| **Measurement Interval** | Measurements can be accumulated over a period from one second to 7 days |
| **Sampling interval** | Measurements are reported every sampling interval. The sampling interval can range from one second to one hour |
| **Statistics reporting** | • Statistics can be reported instantaneously or cumulatively<br>• Instantaneous statistics are reported for the sampling interval (for example, the number of test packets received over the last second)<br>• Cumulative statistics are computed over the entire measurement interval, and reported every sampling interval (for example, the total number of test packets received since statistics were started, updated every second) |
| **Statistics logging** | Statistics can be displayed in a table, displayed on a graph, or logged to a file<br>Table:<br>• Up to 12 statistics can be selected and displayed numerically in a table.<br>Graph:<br>• Results on up to 10 streams or ports can be shown on up to 9 line or bar charts<br>File:<br>• Statistics can be logged to a comma separated values (CSV) file |

### Per Port Transmit Statistics

| Statistic | Description | Resolution |
|---|---|---|
| IPv4 packets transmitted | Count of IPv4 packets transmitted | 1 packet |
| IPv4 octets transmitted | Count of IPv4 octets transmitted | 1 octet |

| | | |
|---|---|---|
| IPv6 packets transmitted | Count of IPv6 packets transmitted | 1 packet |
| IPv6 octets transmitted | Count of IPv6 octets transmitted | 1 octet |
| MPLS packets transmitted | Count of MPLS packets transmitted | 1 packet |
| MPLS octets transmitted | Count of MPLS octets transmitted | 1 octet |
| Test packets transmitted | Count of packets transmitted containing a test payload. | 1 packet |
| Test octets transmitted | Count of octets belonging to packets transmitted containing a test payload. | 1 octet |

## Per Port Receive Statistics

| Statistic | Description | Resolution |
|---|---|---|
| IPv4 packets received | Count of IPv4 packets received | 1 packet |
| IPv4 octets received | Count of IPv4 octets received | 1 octet |
| IPv4 header checksum errors received | Count of IPv4 header checksum errors received | 1 packet |
| IPv4 fragmented packets received | Count of IPv4 packets received with the "more fragments" bit set and a fragment offset of zero. | 1 packet |
| IPv6 packets received | Count of IPv6 packets received | 1 packet |
| IPv6 octets received | Count of IPv6 octets received | 1 octet |
| MPLS packets received | Count of MPLS packets received | 1 packet |
| MPLS octets received | Count of MPLS octets received | 1 octet |
| Test packets received | Count of packets received containing a test payload | 1 packet |
| Test octets received | Count of octets belonging to packets received containing a test payload. | 1 octet |
| Payload integrity error | Count of packets received with a packet payload integrity check error. | 1 packet |
| Packet Error Rate | Ratio of payload integrity errored packets received divided by the number of test packets received. | ratio |
| Minimum latency | The minimum latency measured during the measurement or sampling interval for all packets received with a valid test payload. | 10 ns |
| Average latency | The average latency measured during the measurement or sampling interval for all packets received with a valid test payload. | 10 ns |
| Maximum latency | The maximum latency measured during the measurement or sampling interval for all packets received with a valid test payload. | 10 ns |
| Misdirected packets received | Count of packets misdirected and received on the selected port. | 1 packet |

## Per Stream Transmit Statistics

Packets must contain a test payload for transmit and receive statistics to be reported.

| Statistic | Description | Resolution |
|---|---|---|
| Test packets transmitted | Count of packets transmitted with a test payload. | 1 packet |
| Test octets transmitted | Count of octets belonging to packets transmitted containing a test payload. | 1 octet |

## Per Stream Receive Statistics

Packets must contain a test payload for transmit and receive statistics to be reported.

| Statistic | Description | Resolution |
|---|---|---|
| Test packets received | Count of packets received with a test payload | 1 packet |
| Test octets received | Count of octets belonging to packets received containing a test payload. | 1 octet |
| Min latency received | The Minimum latency measured during the measurement or sampling interval for all packets received with a valid test payload. | 10 ns |
| Average latency received | The average latency measured during the measurement or sampling interval for all packets received with a valid test payload. | 10 ns |
| Max latency received | The Maximum latency measured during the measurement or sampling interval for all packets received with a valid test payload. | 10 ns |

| | | |
|---|---|---|
| Sequence errors received | Count of packets where the sequence number in the test payload is not exactly one more than the previous packet | 1 packet |
| Misordered packets received | Count of packets where the sequence number in the test payload of the currently received packet is less than the previously received packet. | 1 packet |
| Packets with payload integrity errors received | Count of packets received with a packet payload integrity check error. | 1 packet |
| Packet Error Rate | Ratio of payload integrity errored packets received divided by the number of test packets received. | 1 packet |

## Frame/Packet Capture

The Traffic Generation and Analysis software also includes packet capture. Triggers and filters can be set up to trigger on specific events, and capture packets meeting particular criteria. Packet decodes are provided for over 400 protocols.

### Triggers & filter conditions

| Condition | Action |
|---|---|
| Valid IP frame received | Capture is stopped or started, and packet is stored or discarded |
| Any frame received | Capture is stopped or started, and packet is stored or discarded |
| Emulation frame received | Capture is stopped or started, and packet is stored or discarded |
| MPLS frame received | Capture is stopped or started, and packet is stored or discarded |
| Frame Matchers | 2 frame matchers are provided.<br>Capture is stopped or started, or packets are stored or discarded on any user-specified pattern AND of the following conditions:<br>• Valid IP packet received<br>• Valid IPv4 packet received<br>• Valid IPv6 packet received<br>• Fragmented IPv4 packet received<br>• Packet with an IPv4 header checksum error received<br>• MPLS frame received<br>• Emulation packet received<br>• Misdirected packet received<br>• Packet with a sequence number error received<br>• Mis-ordered packet received<br>• Packet with a payload integrity check error received<br>• Packet with a layer 2 frame error received |

### Capture Size

For details on the capture size, please see the appropriate hardware interface data sheet.

## Application Programming Interface

An Application Programming Interface (API) is provided through the Tool command Language (Tcl). The API is intended to automate configuration tasks, create repeatable test sequences, or to integrate the test system into a larger test system. The scripting language is Tcl/Tk. Tcl/Tk comes bundled with the Traffic Generation and Analysis software.

An API client may run directly on the N2X System Controller, or may run on any other PC or UNIX workstation connected to the System Controller via a TCP/IP connection. API clients communicate with the System Controller via an included package of Tcl commands.

All functions available through the GUI are available via the API. Any changes made through the API are automatically reflected on the GUI.

## Real-time Histograms

The Traffic Generation and Analysis software provides real-time latency and latency variation histograms. This allows a real-time graphical visualization of device or network performance.

### Latency

| Statistic | Description | Resolution |
|---|---|---|
| Minimum latency | The minimum latency measured since start of test or last reset for all packets received with a valid test payload and matching selected field of interest | 10 ns |
| Maximum latency | The maximum latency measured since start of test or last reset for all packets received with a valid test payload and matching selected field of interest. | 10 ns |

## Latency Variation

| Statistic | Description | Resolution |
|---|---|---|
| Minimum latency variation | The minimum latency variation measured since start of test or last reset for all packets received with a valid test payload and matching selected field of interest. | 10 ns |
| Maximum latency | The maximum latency variation measured since start of test or last reset for all packets received with a valid test payload and matching selected field of interest. | 10 ns |
| Discarded packet count | Count of packets received where latency variation could not be determined due to a sequence error. | 1 packet |
| System latency tolerance | The accuracy levels achievable for latency variation measurements. | +/-30ns |

## Histogram system details

| | |
|---|---|
| Number of time buckets | 3 to 64 |
| Time bucket distribution | Auto-calibrated<br>User-defined |
| Number of traffic classes | • 0 to 15. Measuring latency or latency variation on a single port.<br>• 0 to 7. Measuring both latency and latency variation on a single port (XR & XS cards only). |
| Histogram variants | • Count by traffic class (cluster or stack)<br>• Count by bucket (cluster or stack) |
| Statistics logging | Statistics can be displayed in a table, displayed on a graph, or logged to a file.<br>• Table: Minimum, maximum and discarded packet counts for each traffic class.<br>• Graph: Results on up to 8 histograms can be shown simultaneously.<br>• File: Statistics can be logged to a comma separated values (CSV) file. |
| Supported hardware | Not all test cards support real-time histograms. The following test cards are currently supported.<br>**N2X XP Cards – Packet Test Cards**<br>• N5553A/B N2X 4-port Ethernet 10/100/1000 XP-2 Test Card<br>**N2X XR Cards – Packet and Protocol Test Cards**<br>• N5550A/B: 4-port Ethernet 10/100 XR-2 Test Card<br>• N5551A/B: 4-port Ethernet 10/100/1000 XR-2 Test Card<br>• N5552A/B 2-port Ethernet 10/100/1000 XR-2 Test Card<br>• N5602A: 1-port 10Gb XR-2 Test Card (POS & Ethernet LAN/WAN XFP)<br>• N5603A: 1-port 10Gb XR-2 Test Card (Ethernet LAN/WAN XFP)<br>• N5604A: 4-port 10/100/1000 EPON XR Test Card<br>• N5605A: 10-port Ethernet SFP XR-2 Test Card<br>• E7317A/E7318A: 10Gb UniPHY XR Test Card<br>**N2X XS Cards – High Performance Packet and Protocol Test Cards**<br>• N5630A/B: 2-port Ethernet 10/100/1000<br>• XS-2 Test Card<br>• N5632A: 1-port 10Gb XS-2 Test Card (POS & Ethernet LAN/WAN XFP)<br>• E7317B/E7318B: 10Gb UniPHY XS Test Card<br>**Other Supported Test Cards**<br>• E7316B: 1-port 10Gb VSR4-1 Test Card |

## Online Help

An extensive online help system provides complete descriptions and detailed usage instructions for every component of N2X. Dialog-level, context-sensitive help provides rapid access to the relevant sections of the online help.

## Supports N2X XP and XP-2 Test Cards

Agilent's packet only cards such as the XP/XP-2 are limited to the E7880B Packets Application Software. The remaining cards such as the XR/XR-2 and XS will support the E7881B Packets and Protocols Application software.

## Configuration and Ordering Details

To use the E7880B Packets Application Software, N2X hardware is required.

**Hardware**
A N2X system is required, with:

- System controller
- Chassis
- Interface cards

Your local Agilent field engineer can provide more details on how to order and configure a test system.

This page intentionally left blank.

www.agilent.com/find/n2x

## 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 #950
Miami, Florida 33126
U.S.A.
Tel: (305) 269-7500
Fax: (305) 267-4286

**Asia Pacific:**
Agilent Technologies
19/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 Burwood Highway
Forest Hill, Victoria 3131
Tel: 1-800-629-485 (Australia)
Fax: (61-3) 9272-0749
Tel: 0-800-738-378 (New Zealand)
Fax: (64-4) 802-6881


Printed in USA July 16, 2008
5988-9860EN

Agilent Technologies