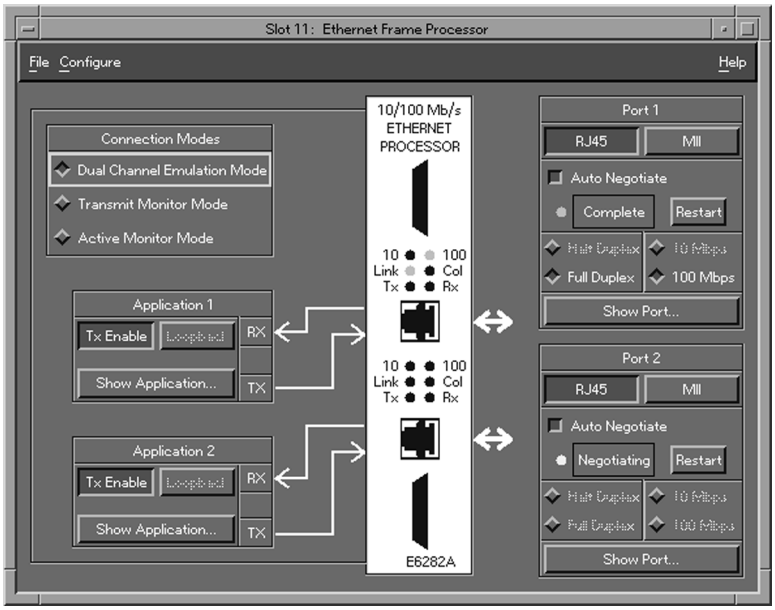
10/100 Mb/s Ethernet Frame Processor

Agilent Technologies Broadband Series Test System

E6282A



Main control dialog for the dual port E6282A Ethernet Frame Processor showing key operational modes and interface type, duplex and rate.

Product Features

- Dual port 10/100 Ethernet module for the BSTS
- Enables LAN-LAN, LAN-ATM and LAN-WAN interworking
- Comprehensive real-time analysis and filtering
- IP CoS stimulus/response testing
- Functional and performance IP testing
- More than 100 protocols supported
- Error injection and the ability to transmit non-conforming streams
- Over 200 real-time measurements
- Full and half duplex configuration support
- Network Services including RIP, Ping and full ARP implementation

The Agilent Technologies E6282A 10/100 Mb/s Ethernet Frame Processor brings LAN interworking and native Ethernet testing to the BSTS. As with all BSTS modules, the Ethernet Frame Processor has a rich set of test features tailored for equipment design and network test applications.

You can create LAN Protocol Data Units (PDUs) such as IP, send them individually or use the capabilities provided by the traffic generator to create complex traffic streams. On the receive side, you can filter out the LAN traffic of interest for further analysis. This analysis includes real-time statistical monitoring, multifunctioned triggers, and capture playback.

The playback viewer supports the decoding of over 100 LAN protocols.

This module works seamlessly with other BSTS ATM or frame relay modules to form the foundation of a functional interworking test.

Important test connection modes supported include:

- Dual Channel Emulation
- Transmit Monitor
- Active Monitor

Physical layer support includes a choice of RJ45 or Media Independent Interfaces (MII). Full or half duplex operation is available for either 10BaseT or 100BaseTX interface rates.

Key Benefits

Interworking with BSTS ATM and Frame Relay modules

The Ethernet Frame Processor is a fully integrated BSTS module. It can be used as a stimulus/response tester and debugging tool for native LAN, WAN and ATM when used in conjunction with E4209B Cell Protocol Processor, E4206A T1/E1 Frame Processor, or E4207A V-Interface Frame Processor modules. You can view PDUs from either of two networking domains (LAN or ATM) in one merged viewer. The power of the BSTS allows events in all domains to be synchronized to the same timebase.

Layer 3 Performance Testing

A comprehensive set of real-time full bandwidth statistics are available on the Ethernet module. Statistics are grouped into two major categories: aggregate and data stream specific statistics.

Aggregate statistics are available for all of the incoming frames and include information such as:

- total frames
- minimum, maximum or average frame length
- FCS errored frames
- collisions

Data stream statistics pertain only to the stream(s) of traffic identified by the user in the receiver setup dialog. They can be grouped into generic, service and performance categories and include:

- total PDUs
- PDU throughput
- minimum, maximum or average PDU length
- bits per second

The data stream statistics are based on the combination of the token bucket and leaky bucket models outlined in RFC2215. By defining the TS parameters, a user is able to verify the conformance of a stream against this model.

The data stream performance statistics leverage off the capabilities provided by the instrumented frame. Instrumented frames augment PDU payload with:

- timestamps
- sequence numbers
- payload cyclic redundancy checks.

This provides the capability to measure in real-time:

- duplicated or misordered frames
- minimum, maximum or average latency
- payload integrity errored PDUs.

Powerful Traffic Generator

The traffic generator has eight fully featured data streams. Load levels are specified in user friendly terms such as throughput (kb/s), frame rate (frames/s) or load (percentage of line rate). Supported traffic generator profiles include random, burst and constant. Profiles and load levels can be combined deterministically across the eight data streams to create a multitude of complex traffic profiles. Furthermore, users have the capability to modify the load levels and profiles while the traffic generator is operating.

Additionally, you can specify ranges of LAN addresses or PDU lengths over which the traffic generator will automatically increment.

Network Services Support

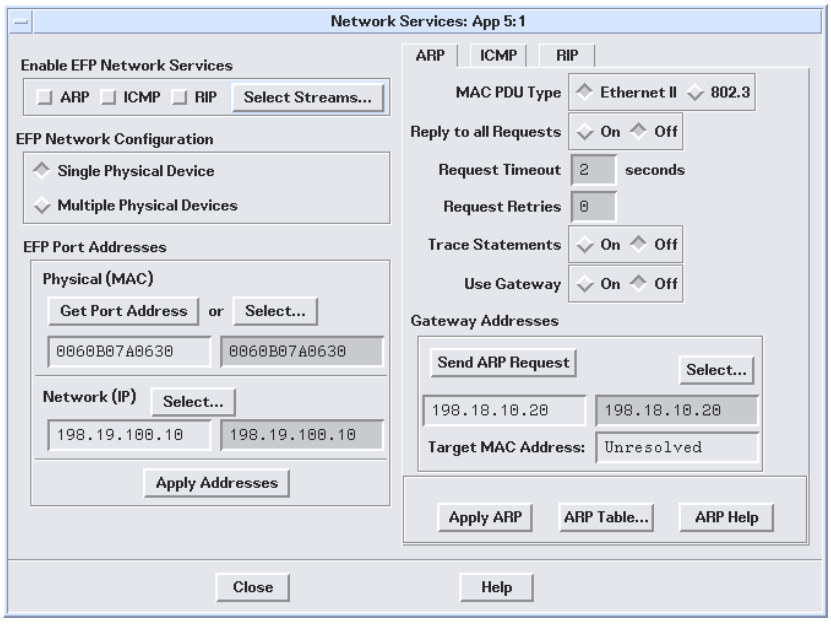
Each Ethernet Port provides network services tools to easily establish IP network connectivity. These tools simplify test setup by automatically configuring the Ethernet module and DUT.

RIP update messages allow the router under test to configure its routing tables with the EFP IP addresses. If the EFP is configured as multiple devices, then a RIP update message will contain messages for each device that the EFP is emulating.

ICMP Ping provides the ability to test for network connectivity and is a required part of every IP implementation. Ping requests from the EFP can be sent a user definable number of times or continuously. Ping also provides a summary of statistics including number of packets sent and received, minimum, maximum, and average times to receive a response.

A full ARP implementation provides:

- Real Time address resolution for each traffic stream
- Emulation of multiple physical source devices
- Emulation of multiple IP destinations
- Flexible gateway support to modify ARP load on the DUT



Network Services dialog provides access to a full ARP implementation

Multiple Ports per System

Each Ethernet Frame Processor module has 2 fully featured 10/100 Ethernet ports. Multiple Ethernet Frame Processor modules can be installed in a single BSTS test rack, providing:

- up to 10 Ethernet ports (5 modules) in a Form 7 chassis
- up to 20 Ethernet ports in a Form 13 chassis

Each port is a fully featured Ethernet analyzer, allowing you to efficently diagnose system problems.

Native LAN Support

The Ethernet module provides full support for the classic LAN protocols including: MAC, IP, TCP, UDP and ICMP. An extensive PDU editor is available for each of these protocols which gives access to all protocol fields and automatically highlights protocol errors. In addition, full decode support is provided for over 100 LAN protocols from the following protocol suites:

- TCP/IP
- Microsoft LAN Manager
- Appletalk
- Banyan/VINES
- DECnet
- IBM/SNA
- Xerox/XNS
- Novell/IPX
- ISO
- Sun
- X Windows

Configuration and Use With Other BSTS Modules and Applications

The Agilent E6282A 10/100 Mb/s Ethernet Frame Processor is fully functional as a stand alone module. It can be combined with an E4209B Cell Protocol Processor and line interface or an E4206A T1/E1 Frame Processor to build the foundation for interworking testing.

The Agilent E6282A requires the following system configuration:

- 1 x V743 HP-UX controller running at 64 MHz or 100 MHz
  - a minimum of 32 MB RAM (not recommended)
  - 64 MB RAM (recommended) or 128 MB RAM
- minimum 2 GB SCSI hard drive

Since the Agilent BSTS is a flexible and modular ATM/B-ISDN test platform, you can maximize the return on your test equipment investment by selecting a chassis, line interfaces, dedicated hardware modules, and test software that suit your specific needs. Remember that you can always add extra software or modules at any time.

Warranty & Support Options

Hardware

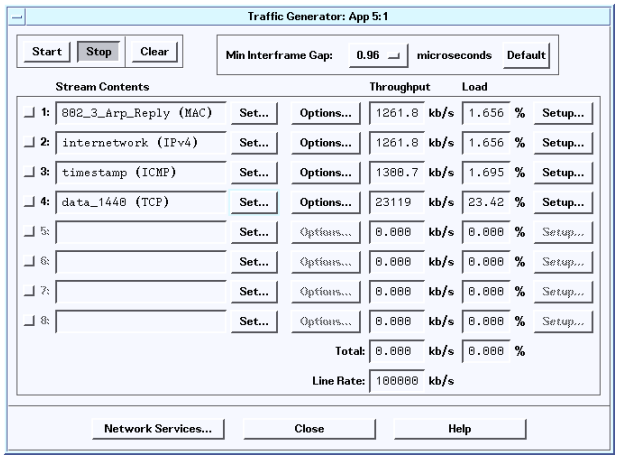
All BSTS hardware components are warranted for a period of 3 years. Products must be returned to an authorized Agilent service center for service.

Software

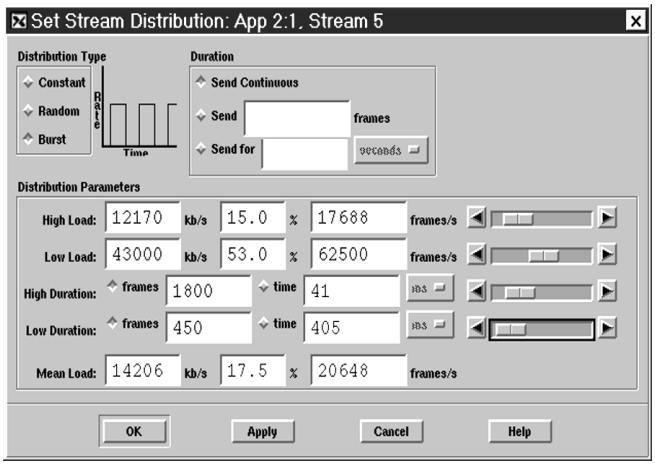
Agilent Broadband Series Test System software and firmware products are supplied on transportable media such as disk, CD-ROM or integrated circuits. The warranty covers physical defects in the media, and defective media is replaced at no charge during the warranty period. When installed in an Agilent Broadband Series Test System, the software/firmware media has the same warranty period as the product.

Product Numbers

- **E6282A** 10/100 Mb/s Ethernet Frame Processor
- **E4215B** LAN Protocols Test Software
- **E4200B** BSTS Form-7 Transportable Chassis
- **E4210B** BSTS Form-13 Mainframe Chassis
- **E4209B** Cell Protocol Processor
- **E6283A** Packet Performance Application
- **E6282A #UK6** Calibration and test report



Main traffic generator provides for 8 independent, fully-featured data streams.

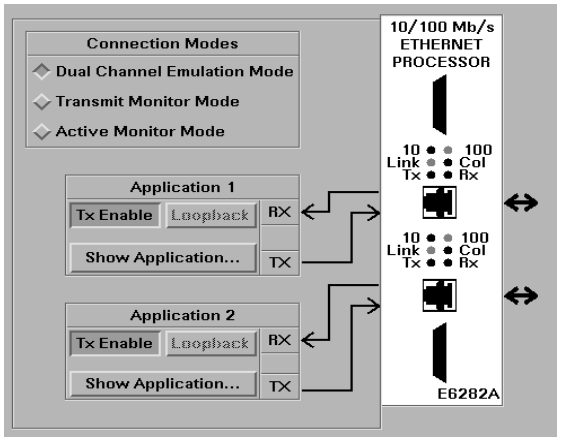


The traffic generator setup dialog gives access to traffic profile parameters.

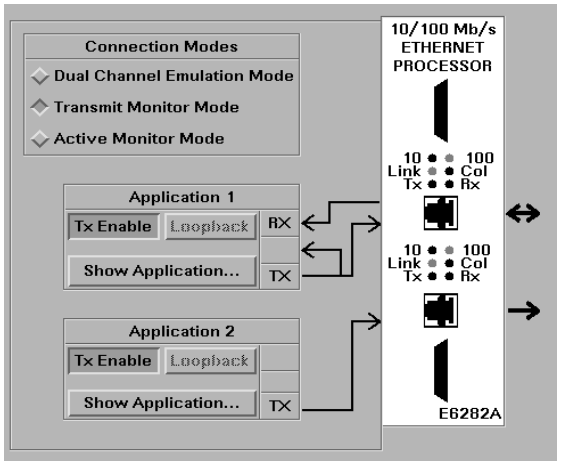
Technical Specifications

10/100 Mb/s Ethernet Test Ports

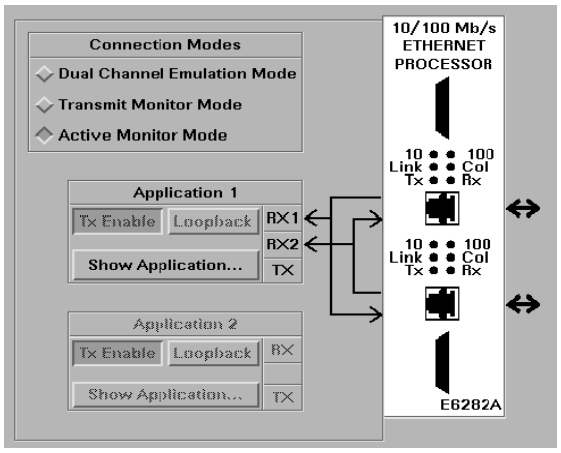
Dual-port Ethernet test access • Two Tx/Rx ports	Configurable parameters for each Tx/Rx port • RJ45 or MII media connection • 10 Mb/s or100 Mb/s Ethernet • Full-duplex or half-duplex operation • Auto-negotiation on or off
Auto-negotiation capabilities of each Ethernet port	Each port can advertise the following local capabilities: • 10BaseT half-duplex • 10BaseT full-duplex • 100BaseTx half-duplex • 100BaseTx full-duplex Each port can detect the following remote capabilities: • Auto-negotiation capable • 10BaseT half-duplex • 10BaseT full-duplex • 100BaseTx half-duplex • 100BaseTx full-duplex • 100BaseT4
Two independent test applications • Application 1 and 2	Each test application provides: • Building of layer 2, 3, 4 PDUs • Traffic generation on 8 streams • Real-time control of layer 2, 3, 4 PDU fields • Data capture and real-time measurements on 8 streams • TSPEC (token bucket) conformance statistics on 8 streams • Receive streams can be defined in terms of layer 2, 3, 4 PDU fields • Capture buffer with protocol reassembly, > 1 sec of minimum-sized frames at maximum line rate • Graphical display, numeric display, and logging of real-time statistics
Connection Modes • Application 1/2 to Port 1/2 mapping	• **Dual-channel emulation**: Application 1 sends/receives on Port 1 Tx/Rx; Application 2 sends/ receives on Port 2 Tx/Rx: use this mode for independent testing on two ports • **Transmit monitor**: Application 1 sends/receives on Port 1 Tx/Rx; Application 1 also monitors its own send traffic: use this mode to correlate send and receive traffic • **Active monitor**: EFP module acts as an in-line repeater between Port 1 Rx/Tx and Port 2 Tx/Rx; Application 1 monitors Port 1 and 2 traffic: use this mode for bi-directional in-line monitoring between two network elements
Tx Loopback capability • For Application1 or2	For Dual-channel emulation mode only: • Internally loop send to receive for Application 1; disable Port 1 Tx/Rx • Internally loop send to receive for Application 2; disable Port 2 Tx/Rx



To conduct independent testing on two ports, use the **dual-channel emulation** mode.



To correlate, send and receive traffic, use the **transmit monitor** mode.



For bi-directional in-line monitoring between two network elements, use the **active monitor** mode.

Multi-stream Traffic Generation (per Ethernet Port)

Traffic Generation	Burst mode • Send a burst of PDUs or sequences Continuous mode • Configure up to 8 continuous traffic streams
Global Traffic Generation Parameter	• Transmit interframe gap (23, 24, 25, or 26 nibbles; default = 24)
Configuration of the 8 Continuous Traffic Streams	Configurable parameters for each stream: • Payload (PDU or sequence) • Distribution modified by the user in real time (Constant, Random, or Burst) • Protocol parameters (MAC, IPv4, TCP, UDP, ICMP)
Specification of Traffic Stream Payload	PDU builders for the following protocols: • MAC (Ethernet-II or 802.3) • IPv4 • TCP • UDP • ICMP Sequence Builder • Concatenates PDUs into sequences
Specification of Traffic Stream Distribution	**Constant** distribution; specify: • Constant Load (kb/s,%, or frames/s) **Random** distribution; specify: • Maximum Load (kb/s,%, or frames/s) • Minimum Load (kb/s,%, or frames/s) **Burst** distribution; specify: • High Load (kb/s,%, or frames/s) • Low Load (kb/s,%, or frames/s) • High Duration (frames or time [ms or s]) • Low Duration (frames or time [ms or s]) For each of the above distributions, the traffic duration can be specified as: • Continuous, or • Send for n frames, or • Send for m [seconds or minutes]
Specification of Traffic Stream Protocol Parameters (All incrementing range parameters are incremented in real time)	**MAC** parameters • Header type (Ethernet II or 802.3) • Destination address (single value or incrementing range) • Source address (single value or incrementing range) • Data length (single value or incrementing range) • Link layer type (LLC, LLC/SNAP, or None) • Error Options (dribble frame, alignment error, or FCS error) **IPv4** parameters • Source address (single value or incrementing range) • Destination address (single value or incrementing range) • Time to Live (single value) • Type of Service (delay, throughput, reliability, cost, and precedence) • Data length (single value or incrementing range) • Error Options (header checksum errors) **TCP** parameters • Source port (single value or incrementing range) • Destination port (single value or incrementing range) • Sequence number (single value) • Acknowledgment number (single value) • Window (single value) • Data length (single value or incrementing range) • Error Options (checksum errors) **UDP** parameters • Source port (single value or incrementing range) • Destination port (single value or incrementing range) • Data length (single value or incrementing range) • Error Options (checksum errors) **ICMP** parameters • Error Options (checksum errors)
Instrumented Payload	Inserted into MAC, IP, UDP, or TCP layer • Timestamp • Sequence number • Payload integrity check Used in conjunction with receive streams and statistics allows users to: • measure latency (LIFO and FIFO), payload integrity and frame sequencing, lost, misordered, severely misordered, or correctly sequenced frames

Network Services (per Ethernet Port)

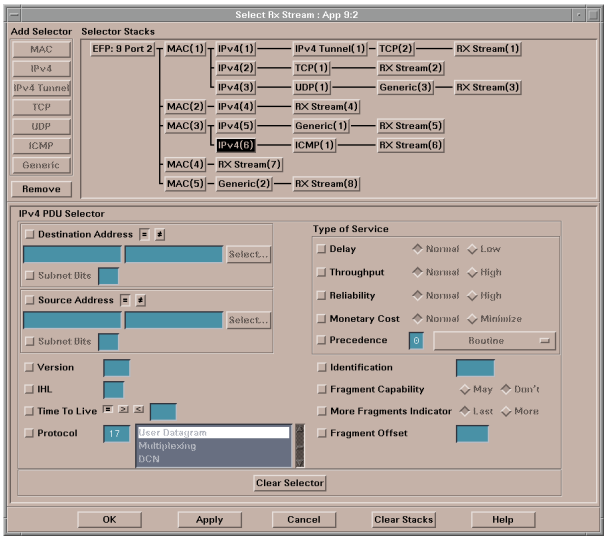
Network Configuration

- Single or multiple physical device emulation

ARP Services	Automatic ARP emulation for enabled streams **MAC Encapsulation** • Ethernet II or 802.3 **Configuration** • Reply to all requests • Request timeout (sec) • Request retries • ARP Trace Statements Logging **Gateway Configuration** • Automatic gateway support
ICMP Ping	• Enable/disable Echo requests, replies or both • The interval between echo requests is also the timeout value for receiving replies **MAC Encapsulation** • Ethernet II or 802.3 **Statistics** • Number of packets sent • Number of replies received • % packet loss • Average time for reply • Maximum time for reply • Minimum time for reply
RIP	**MAC Encapsulation** • Ethernet II or 802.3 **Configuration** • Update messages sent out at user-defined intervals (default of 30 seconds) • Metric (hop count) can be set between 1-16, with a default of 1 • User can add the default route to RIP update message

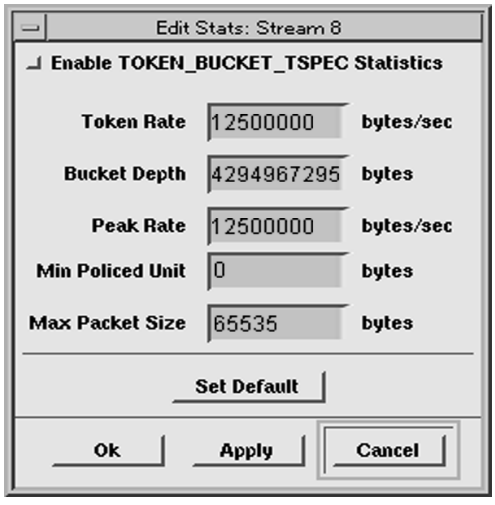
Real-Time Measurements (per Ethernet Port)

Real-time Analysis on up to 8 Streams	Real-time analysis on each stream • Rx aggregate statistics • Tx aggregate statistics • Rx stream 1..8 statistics (including TSPEC conformance) • Tx stream 1..8 statistics (including TSPEC conformance)
Specification of the 8 Receive Streams	Stream filters can be specified in terms of the following protocol layer pattern matches: • MAC • IPv4 • TCP • UDP • ICMP • Generic (HEX pattern match, maximum length 64 octets) Each stream filter provides flexible combinations of the above protocol pattern matches using logical AND operations. • The filter can be specified in terms of logical AND combinations of any of the above pattern matches e.g.stream(1) = MAC(1) AND IP(1) AND TCP(1)



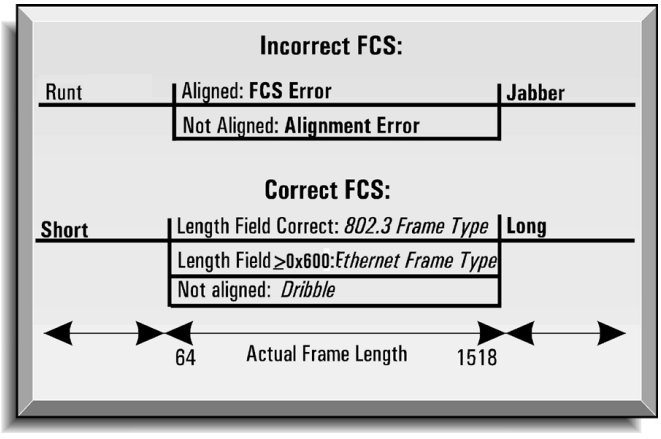
Specify 8 user definable receive streams for real time statistics monitoring , triggering and capture playback.

Specification of real-time **TSPEC** (token bucket) conformance	Traffic conformance in accordance with RFC2215 traffic specification. Configurable parameters for each stream • Token rate (bytes/s) • Bucket depth (bytes) • Peak rate (bytes/s) • Minimum policed unit (bytes) • Maximum packet size (bytes)
Rx aggregate statistics	• % utilization • total bits/s • total frames • total frames/s • average frame length (bytes) • maximum frame length (bytes) • minimum frame length (bytes) • unerrored frame bits/s • unerrored frame/s • unerrored frames **Errors** (see chart for error definitions) • dribble frames • FCS errors (error count) • jabber frames (error count) • long frames (error count) • non-octet aligned frames (error count) • runt frames (error count) • short frames (error count)
Tx aggregate statistics	All statistics listed under **Rx aggregate**, plus: • single collisions (error count) • excessive collisions (error count)



Each traffic stream entering the network can be monitored for network behavior under conforming and non-conforming traffic conditions.

Rx stream 1..8 statistics	For each stream: • % utilization • frame bits/s • frames • frames/s • average PDU length (bytes) • maximum PDU length (bytes) • minimum PDU length (bytes) • PDU bit/s Refer to real-time measurements for specification of TSPEC parameters • conforming (TSPEC) IP packet bits/s • conforming (TSPEC) IP packet/s • conforming (TSPEC) IP packets • non-conforming (TSPEC) IP packet bits/s • non-conforming (TSPEC) IP packet/s • non-conforming (TSPEC) IP packets Use instrumented payload: • FIFO average latency (s) • FIFO maximum latency (s) • FIFO minimum latency (s) • LIFO average latency (s) • LIFO maximum latency (s) • LIFO minimum latency (s) • sequenced frames • duplicated frames (error count: repeated frames) • lost frames (error count: frames missing from an ordered sequence) • payload errored frames (error count: in-band payload integrity check) • misordered (error count: frames misordered in an ordered sequence)
Tx stream 1..8 statistics	For each stream, all statistics listed under **Rx stream 1..8**



Event/Action Triggers (per Ethernet Port)

Trigger Events	**Stream 1..8 pattern** • Match or Not match • Direction: Tx, Rx, or Both • Event to Action delay: n [frames or ms] **MAC frame errors** • Runt frame • Jabber frame • Short frame • Long frame • Alignment error • FCS error • Payload integrity check • Dribble frame • Direction: Tx, Rx, or Both • Event to Action delay: n [frames or ms] **Capture full** • Immediate trigger condition **Rx overflow** • Receive buffer overflow • Immediate trigger condition **Tx underrun** • Transmit buffer empty • Immediate trigger condition **Excessive collisions** • 16 attempts to send a frame • Immediate trigger condition **External trigger input** • Input level: SMB connector, TTL rising edge, 50 ohms terminated to 0 V • Immediate trigger condition **Time of day 1** and **Time of day 2** • Specify hour, minute • Immediate trigger condition
Trigger Actions	Each of the above events can cause any combination of the following actions: • Disarm trigger after firing • Capture start or stop • Statistics start or stop; for statistics start action, specify integration period from 1 s to 72 h • Traffic generator start or stop • Generate trace; specify the text message to display in the capture playback viewer • Display message; specify the text message to display on screen • External trigger output (SMB connector, output level: TTL source, output impedance: 50 ohms, pulse width: 30 ns active high level)
Event/Action Configuration	• A set of actions can be configured independently for each trigger event • Each trigger event (and associated actions) can be independently armed or disarmed; any combination of events can be armed at one time

Capture and Decode Capability (per Ethernet Port)

Capture Buffer Size	• 12 Mbytes capture buffer per port.
Timestamp Resolution	• 100 ns
Capture Modes	• Manual (on/off) • One-time (fill capture buffer then stop) • Wrap-around (fill buffer, then wrap around to the start of the buffer) • Triggered (on stream filter or frame error)
Capture Filter Controls	Stream 1..8 filters • As specified under **Real-Time Measurements** Global active streams action • Pass or Block Each stream filter can be selected with the following direction: • Direction: Tx, Rx, or Both MAC Frame errors • Runt frame • Jabber frame • Short frame • Long frame • Alignment error • FCS error • Payload integrity check (if instrumented frames are activated) • Dribble frame Any of the above frame error conditions can be selected with the following criteria/direction applied to the logical AND combination. • Action: Pass or Block • Direction: Tx, Rx, or Both

Specified Decode Options	MAC layer • MAC type (Ethernet II, 802.3, 802.3-LLC, or auto-detect) • Use MAC address names (see **User-definable Names**) • Ignore dribble errors • Decode up to specified LAN layer (Application, Presentation, Session, Transport, Network, Datalink, or None) IPv4 layer • Use user-defined IP address names (see **User-definable Names**) • Decode up to specified LAN layer (Application, Presentation, Session, Transport, or None)
Specified Protocol Stack for Decoding	Manual or automatic decode method specification • Manually specify the protocol stack, by selecting from: MAC, IPv4, TCP, UDP, ICMP • Capture traffic, then automatically determine the protocol stack above MAC or IPv4

Decoded Protocols

Datalink	**MAC** - IEEE 802.3; CSMA/CD **LLC** - ISO 8802; Logical Link Control **SNAP** - RFC-1042; 802.1 (RFC1904), RFC1356, RFC1294 Sub Network Access Protocol **BPDU** - IEEE 802.1D; Bridge Protocol Data Unit
DARPA/IETF	**ARP** - RFC826; An Ethernet Address Resolution Protocol; IETF; November 1982 **BGP** - RFC1105; Border Gateway Protocol; June 1989 **BGP-4** - RFC1771; A Border Gateway Protocol 4; March 1995 **BOOTP** - RFC951; Bootstrap Protocol; September 1985 **DHCP** - RFC2131; Dynamic Host Configuration Protocol; March 1997 **DLSW** - RFC1795; Data Link Switching Protocol v1.0 **EGP** - RFC904; Exterior Gateway Protocol; April 1984 **GARP, GMRP**- IEEE 802.1p **GGP** - RFC 823; Gateway Gateway Protocol; September 1982 **HTTP 1.1** - RFC1945; Hypertext Transfer Protocol; May 1996 **ICMP** - RFC792; Internet Control Message Protocol; September 1981 **IGP** - RFC823; Internet Gateway Protocol; DARPA; September 1982 **IGMP** - RFC1112; Internet Group Management Protocol; August 1989 **IGRP** - Charles L. Hedrick Rutgers University NJ; August 1991 **IP** - RFC791; Internet Protocol; September 1981 **IPNP** - Inter Paging Network Protocol **IPNPPLI** - IPNP Packet Layer Interface **IPV6** - RFC1883; Internet Protocol Version 6; December 1995 **L2F** - Layer 2 Forwarding, May 1998 **L2TP** - draft-ietf-pptext-12tp-14.txt **MDLP** - CDPD, MDLP Release 1.1, January 1995 **NTP** - RFC1119; Network Time Protocol (version 2); September 1989 **OSPF** - RFC2328; OSPF Version 2; July 1991 **RARP** - RFC903; An Ethernet Reverse Address Resolution Protocol; IETF; June 1984 **RIP** - RFC 1993; Route Daemon Protocol; March 1993 **RTP** - RFC1889; A Transport Protocol for Real-Time Applications; January 1996 **RTCP** - RFC1889; Real-Time Control Protocol; January 1996 **SNDCP** - CDCP, SNDCP Release 1.1, January 1995 **SMTP** - RFC821; Simple Mail Transfer Protocol; August 1982 **TCP** - RFC793; Transmission Control Protocol; September 1981 **TFTP** - RFC783; Trivial File Transfer Protocol (revision 2); June 1981 **TIMED** - Timed Daemon Protocol; Sun **UDP** - RFC768; User Datagram Protocol; August 1980 **X11** - X Open; X Window Protocol, X 11 R4

FDDI SMT	**SMT** - Station Management Protocol Rev 7.2; ANSI; June 1992
ISO	**ACSE** - ISO 8650; Association Control Service Element; CCITT, December 1988 **APPL** - ISO Application Protocol **CLNP** - ISO 8473; Connectionless Network Service; December 1988 **COTP** - ISO 8073; Connection Oriented Session Protocol; October 1992 **DAP** - ISO 9594; X.500; CCITT; December 1990 **ESIS** - ISO 9542; End System to Intermediate System **ISIS** - ISO 10589; Intermediate System to Intermediate System; June 1996 **MTS** - ISO 10021; Message Tranfer Service X.400; CCITT; December 1990 **PRES** - X.226; Presentation Protocol; ITU-T; July 1994 **ROSE** - ISO 9072; Remote Operations Service Element; November 1989 **RTSE** - ISO 9066; Reliable Transfer Element; ITU-T; March 1993 **SESS** - ISO 8327; Connection Oriented Session Protocol; August 1987
ITU-T	**H245** - H.245 Version 3; Multimedia Comm. Protocol **H450** - H.450 .1 -.3; Supplementary Services **MGCP** - Media Gateway Contorl Protocol, February 1999 **RAS** - ITU-T H.225.0 Version 2 **SDP** - Session Description Protocol **SGCP** - Simple Gateway Control Protocol, July 1998 **SIP** - Session Initiation Protocol **Q931** - ITU-T H.225.0 Version 2
Berkeley Services	**LPR** - RFC1179; Remote Line Printing Protocol; August 1990 **REXEC** - Remote Execution Protocol; University of California, Berkeley **RLOGIN** - RFC1282 Remote Login Protocol; December 1991 **RSHELL** - Remote Shell Protocol; University of California, Berkeley **RWHO** - RFC954; Remote Whois Protocol; October 1985
Sun	**BOOTPAMD** - Boot Parameter Daemon Protocol **LOCKD** - Lock Daemon Protocol; Sun **MOUNT** - Mount Protocol; Sun **NFS** - RFC1094; Network File System Protocol; Sun; March 1989 **PCNFSD** - PC Network File System Daemon; Sun **PMAP** - Port Mapper Protocol; Sun **RPC** - RFC1057; Remote Procedure Call Protocol; Sun; June 1988 **STATD** - Status Daemon Protocol; Sun **YP** - Yellow Pages Protocol; Sun **YPBIND** - Yellow Pages Binding Protocol; Sun
Xerox /XNS	**ECHO** Echo Protocol; Xerox **ERROR** - Error Protocol; Xerox **IDP** - Internetwork Datagram Protocol; Xerox **IPX** Internet Packet Exchange Protocol; Novell **PEP** - Packet Exchange Protocol; Xerox **RIP** - RFC1058; Routing Information Protocol; Xerox; June 1988 **SPP** - Sequence Packet Protocol; Xerox **SPX** - Sequence Packet Exchange Protocol; Novell
Novell Netware	**IPXDIAG** - Diagnostics Protocol; Novell **NCP** - NetWare Version 3.x and 4.x; Novell **NLSP** - Netware Link Services Protocol; Novell **SAP** - Service Access Point Protocol; Novell
AppleTalk	**AARP** - AppleTalk Address Resolution Protocol; AppleTalk Phase 2; June 1989 **ADSP** - AppleTalk Data Stream Protocol; AppleTalk Phase 2; June 1989 **AEP** - AppleTalk Echo Protocol; AppleTalk Phase 2; June 1989 **AFP** - AppleTalk Filing Protocol; AppleTalk Phase 2; June 1989 **ASP** - AppleTalk Session Protocol; AppleTalk Phase 2; June 1989 **ATP** - AppleTalk Transaction Protocol; AppleTalk Phase 2; June 1989 **DDP** - Datagram Delivery Protocol; AppleTalk Phase 1; June 1989 **DDPL** - Datagram Delivery Protocol; AppleTalk Phase 2; June 1989 **ELAP** - EtherTalk Link Access Protocol; AppleTalk Phase 2; June 1989 **NBP** - Name Binding Protocol; AppleTalk Phase 2; June 1989 **PAP** - Printer Access Protocol; AppleTalk Phase 2; June 1989 **RTMP** - Routing Table Maintenance Protocol; AppleTalk Phase 2; June 1989 **ZIP** - Zone Information Protocol; AppleTalk Phase 2; June 1989

DECnet	**CTERM** - Network Command Terminal; DECnet Phase IV; Digital **DAP** - Data Access Protocol; DECnet Phase IV - Version 4; Digital **DNAR** - DNA Routing Protocol; Phase IV; Digital **LAT** - Local Area Transport Protocol; Digital **MOP** - Maintenance Operation Protocol; Digita **NICE** - Network Information and Command Exchange Protocol; DECnet Phase IV; Digital **NSP** - DNA Network Service Protocol; Phase IV; Digital **SCA** - DECnet Phase IV; Digital DECnet **SCP** - DNA Session Control Protocol; Phase IV - Version 1.0; Digital
IBM/SNA	**NETB** - Netbios Protocol; IBM **SMB** -Server Message Block, MS, Intel; November 1990 **SNADF** - Data Flow Control; SNA; IBM **SNAFMD** - Functional Management Protocol; SNA; IBM **SNAMS** - Management Services Protocol; SNA; IBM IBM Net BIOS **SNARH** - Transmission Control; SNA; IBM **SNASC** - Session Control Protocol; SNA; IBM **SNATH** - Path Control; SNA; IBM **SNAXID** - Transaction Id Protocol; SNA; IBM **SNANW** -Network Control Protocol; SNA; IBM
Banyan Vines	**VINES** - Banyan Vines Protocol; Banyan **VIPC** - Internet Control Protocol; Banyan **VSPP** - Sequence Packet Control; Banyan **VRPC** - Vine RPC; Banyan
Microsoft LAN Manager/X	**LMX_DG** - RFC1001; Microsoft LAN Manager Datagram Service; March 1987 **LMX_NS** - RFC1001; Microsoft LAN Manager Name Service; March 1987 **LMX_SS** - RFC1001; Microsoft LAN Manager Session Service; March 1987
Cisco	**CDP** - Cisco Discovery Protocol; Cisco **DISL** - Dynamic InterSwitch Link; Cisco **EIGRP** - Enhanced IGRP; Cisco **VTP** - VLAN Trunk Protocol; Cisco

User-definable Names

MAC IPv4	• user can associate names with MAC or IP addresses. • these names persist throughout the traffic generator, PDU builders, receive filters and playback viewer

Mechanical Specifications

Size, Weight & Power Dissipation

Size	• 1 slot C-size VXI card
Weight	• 1 kg (2.2 lb) nominal
Power Dissipation	• 25 Watts (max)

Front Panel LED Indicators (Per Port)

10	• 10 BaseTx
100	• 100 BaseTx
Link	• Link status
Col	• Collisions
Tx	• Transmitter frame
Rx	• Receive frame

Environmental Operation Conditions

Operating Temperature	• 0^0C to 45^0C
Storage Temperature	• -40^0C to 70^0C
Humidity	• 0% to 95% relative humidity from 25^0C to 40^0C

Applicable Standards

Physical Layer& Datalink Layer	• DIX Ethernet II • IEEE 802.3 - MAC • IEEE 802.2 - LLC
Network Layer & Transport Layer	• RFC791 - IPv4 • RFC793 - TCP • RFC768 - UDP • RFC792 - ICMP
Performance & Traffic Conformance	• RFC2215 - General Characterization Parameters for IntServ Network Elements (TSpec token bucket policing algorithm) • RFC1242/2285 - Terminology for LAN Switching Devices

Acronyms

ATM	Asynchronous Transfer Mode
ARP	Address Resolution Protocol
BSTS	Agilent Technologies Broadband Series Test System
DIX	Digital Intel Xerox (Ethernet II)
FIFO	First-(bit)-In, First-(bit)-Out (latency parameter)
FCS	Frame Check Sequence
ICMP	Internet Control Message Protocol (IETF)
IEEE	Institute of Electrical and Electronic Engineers (Ethernet standards
IETF	Internet Engineering Task Force (IP protocol suite)
IP	Internet Protocol (layer 3 LAN protocol)
IPv4	Internet Protocol version 4 (IETF)
IPv6	Internet Protocol version 6 (IETF)
LAN	Local Area Network
LIFO	Last-(bit)-In, First-(bit)-Out (latency parameter)
LLC	Logical Link Control
MAC	Media Access (layer 2 LAN protocol, for example Ethernet)
MII	Media Independent Interfaces
MPLS	Multi-Protocol Label Switching (IETF)
MPOA	ATM Forum Multi-Protocol Over ATM
PDU	Protocol Data Unit
Ping	Packet Internet Groper
RIP	Routing Information Protocol
SNAP	Sub Network Access Protocol
TCP	Transmission Control Protocol (IETF)
TSpec	Traffic Specification (RFC2215, token bucket algorithm)
UDP	User Datagram Protocol (IETF)
WAN	Wide Area Network

This page intentionally left blank.

This page intentionally left blank.

Agilent Technologies Broadband Series Test System

The Agilent Technologies BSTS is the industry-standard ATM/BISDN test system for R&D engineering, product development, field trials and QA testing. The latest leading edge, innovative solutions help you lead the fast-packet revolution and reshape tomorrow's networks. It offers a wide range of applications:

- ATM traffic management and signalling
- Packet over SONET/SDH (POS)
- switch/router interworking and performance
- third generation wireless tesing
- complete, automated conformance testing

The BSTS is modular to grow with your testing needs. Because we build all BSTS products without shortcuts according to full specifications, you'll catch problems other test equipment may not detect.

www.Agilent.com/comms/BSTS

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.
5150 Spectrum Way
Mississauga, Ontario
L4W 5G1
1-877-894-4414

Europe:
Agilent Technologies
European Marketing Organisation
P.O. Box 999
1180 AZ Amstelveen
The Netherlands
(31 20) 547-9999

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) 267-4245
Fax: (305) 267-4286

Asia Pacific:
Agilent Technologies
19/F, Cityplaza One, 1111 King's Road,
Taikoo Shing, Hong Kong, SAR
Tel: (852) 2599-7889
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

Specifications subject to change.

5965-8902E April 20, 2001 Rev G

Agilent Technologies
Innovating the HP Way