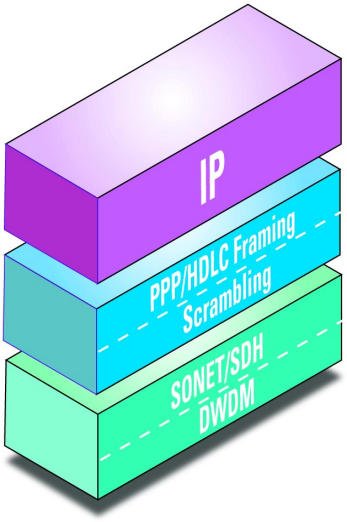
Packet over SONET/SDH (POS)

Technical paper



Packet over SONET/SDH (POS) was first deployed in 1996 at 155 Mb/s, and has since become a key protocol standard for building large internet protocol (IP) backbones. Networks worldwide now carry POS traffic at line rates of 622 Mb/s and 2.5 Gb/s to accomodate the explosion in internet traffic. This technology note examines the key features of POS, focusing on layers 1 and 2 where the hardware processing takes place.

Agilent Technologies
Innovating the HP Way

Packet over SONET/SDH (POS)

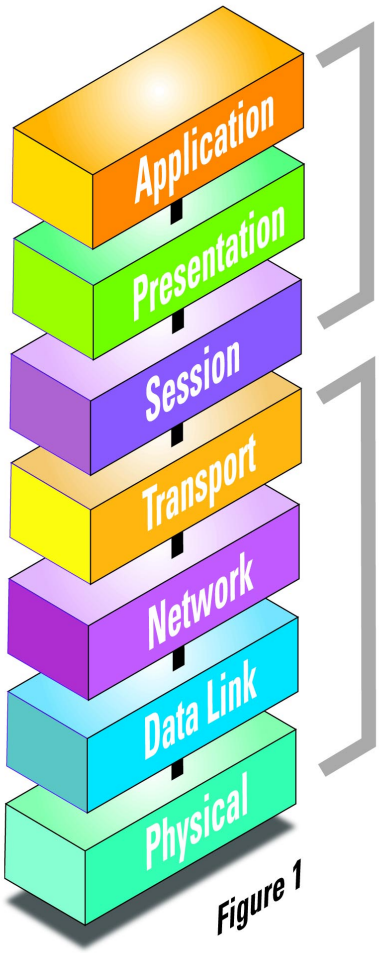


Figure 1

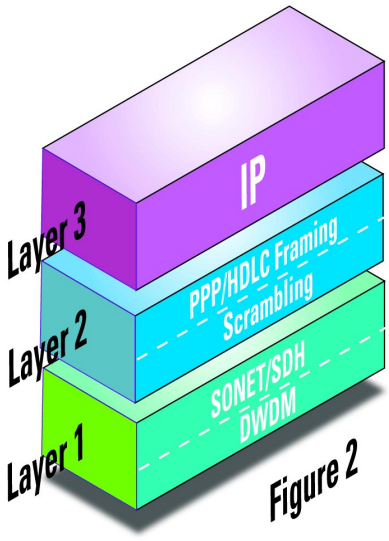


Figure 2

What is it?

OSI reference model

POS is often referred to as a 'Layer 2 protocol', in other words, a formal set of rules and conventions that governs how routers exchange information over a network medium. 'Layer 2' refers to the Open Systems Interconnects (OSI) conceptual 7-layer model (figure 1) that describes the process of transferring applications across a network.

POS hardware processing is mainly limited to the first three layers, (figure 2) beginning at layer 1, the physical layer. This is the media (usually fiber), physical connectors, as well as the signal characteristics carried on the medium – SONET or SDH for POS. Layer 2, the data link layer, is responsible for reliable transit of data across the physical network link. Finally, Layer 3, the network layer, looks after the topology of the network, that is, routing and related functions that enable multiple data links to be combined into an internetwork. Layer 3 and above accounts for the software component of POS.

A standardized way for mapping IP Packets into SONET/SDH payloads

How does it work?

The layer 2 protocol used by POS technology offers a standarized way for mapping IP packets into SONET/SDH payloads. Data is first segmented into an IP datagram that includes a 20-byte IP header. This datagram is encapsulated via Point-to-Point Protocol (PPP) packets and framing information is added with High-level Data Link Control (HDLC) – framing. Gaps between frames are filled with flags, set to value 7E. Octet stuffing occurs if any flags or resultant escape characters (of value 7D) are found in the data. The resulting data is scrambled, and mapped synchronously by octet into the SONET/SDH frame.

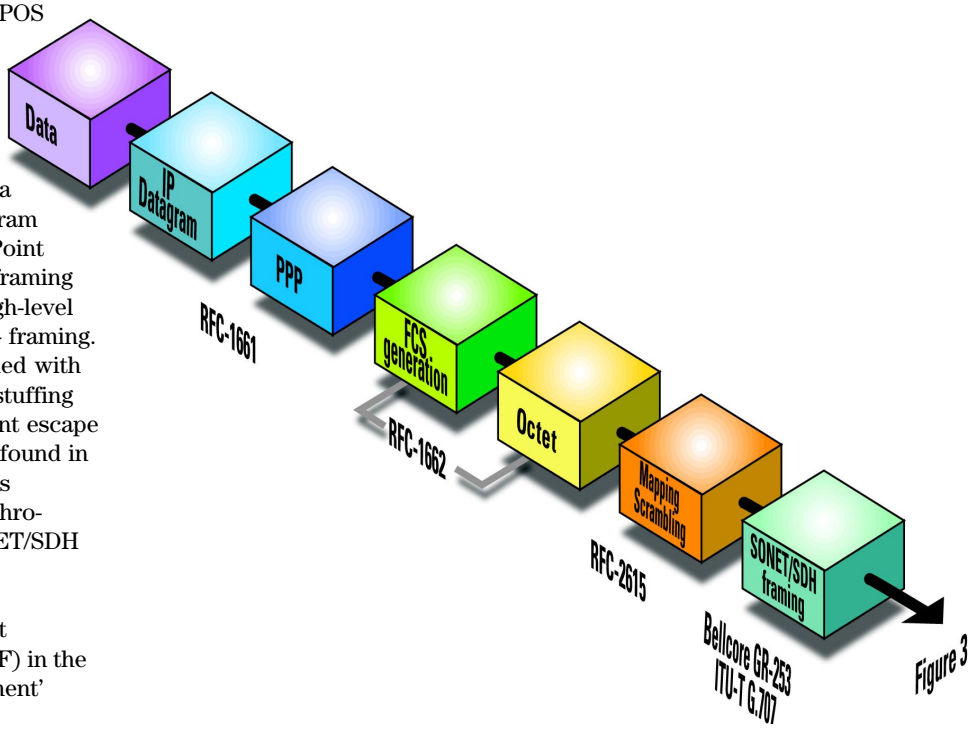


Figure 3

POS is defined by the Internet Engineering Task Force (IETF) in the following 'Request For Comment' (RFC) documents:

RFC-1661	The Point-to-Point Protocol (PPP)
RFC-1662	PPP in HDLC framing
RFC-2615	PPP over SONET/SDH

The main components

IP datagram

The internet protocol is a network-layer (layer 3) protocol that contains addressing information and some control information that enables datagrams to be routed through a network to their destination. The role of POS is to package these IP datagrams efficiently. It is important to note that IP datagrams are not POS specific and can be transported by other means such as ATM or Ethernet. POS, therefore, can be thought of as a 'high-speed WAN transport that leaves LAN traffic in its native format'.

Although a full discussion of the IP datagram is outwith the scope of this document, it is worth mentioning that the IP datagram contains a header and an information (data) field. The IP header contains the addressing and control information. The datagram can vary in length up to 65,535 octets, and although all values are possible, it is more common to have many packet sizes with few variations. For example, it is not uncommon for minimum length (40 octets) IP packets containing Transmision Control Protocol (TCP) acknowledgements to represent 40% of the traffic. Processing these small packets at wireline speeds is a serious challenge for POS hardware as it maximizes the rate of frame check sequence (FCS) calculations and stresses the HDLC framing.

IP is described in RFC-791 for further reference.

Point-to-point protocol (RFC-1661)

PPP is the encapsulation protocol used by POS to transfer multi-protocol datagrams over point-to-point communication links. It carries the network layer in its information field and uses a 16-bit protocol field to identify which network layer protocol is being carried.

It is important to note that this protocol field could contain different values relating to different protocols, for example, Xerox, Appletalk, DECnet. POS uses only a small subset of these values to identify whether it is an IP packet or a PPP control protocol. Some common values are shown below.

PPP ID field	Protocol in PPP information field
0021	IP v 4
0800	Cisco HDLC
0281	MPLS unicast
0283	MPLS multicast
8021	Internet Protocol Control Protocol (IPCP)*
c021	Link Control Protocol (LCP)*

* A link between two routers must be established and set up before any data is passed. This is often referred to as 'link negotiation'. There must also be the means to identify which network layer packets are to be transferred, keep the link active and the means to close the link. LCP is a protocol used for negotiating link parameters and facilities and IPCP enables the exchange of IP addresses across the link.

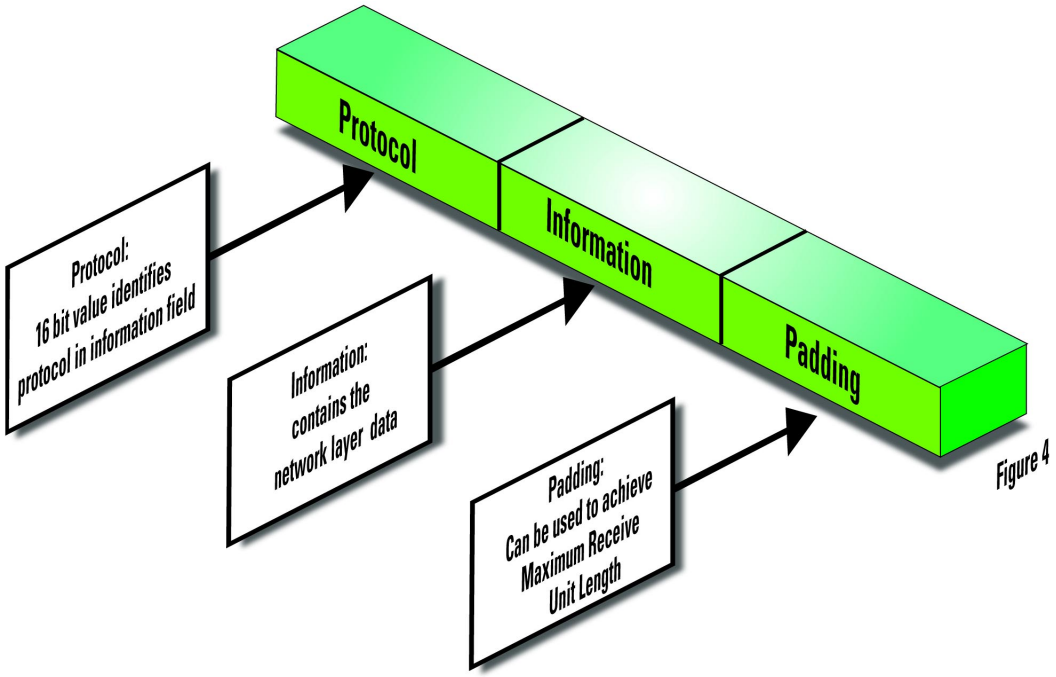

Protocol
Information
Padding
Protocol:
16 bit value identifies
protocol in information field
Information:
contains the
network layer data
Padding:
Can be used to achieve
Maximum Receive
Unit Length

Figure 4

PPP in HDLC framing

PPP encapsulated packets are mapped into frames. HDLC framing is used to delineate the packet boundaries so that the receiver can extract them from the SONET/SDH frame. Gaps between packets are filled with standard HDLC flags of value 7E.

The HDLC frame includes address, control, and protocol fields, followed by the encapsulated IP datagram. The address field is set to 0xFF for standard HDLC and 0x0F for Cisco HDLC. The control bits are set to 0x03 for standard HDLC and 0x00 for Cisco HDLC.

A 16-bit or 32-bit FCS, acting as a CRC checksum, protects the entire frame and gives an idea of traffic integrity. The preference is for 32-bit FCS, however, 16-bit FCS may be used at the lowest speeds in the SONET/SDH hierarchy. The FCS field is calculated over all bits of the address, control, protocol and information fields. It does not include the flag fields or the FCS field itself.

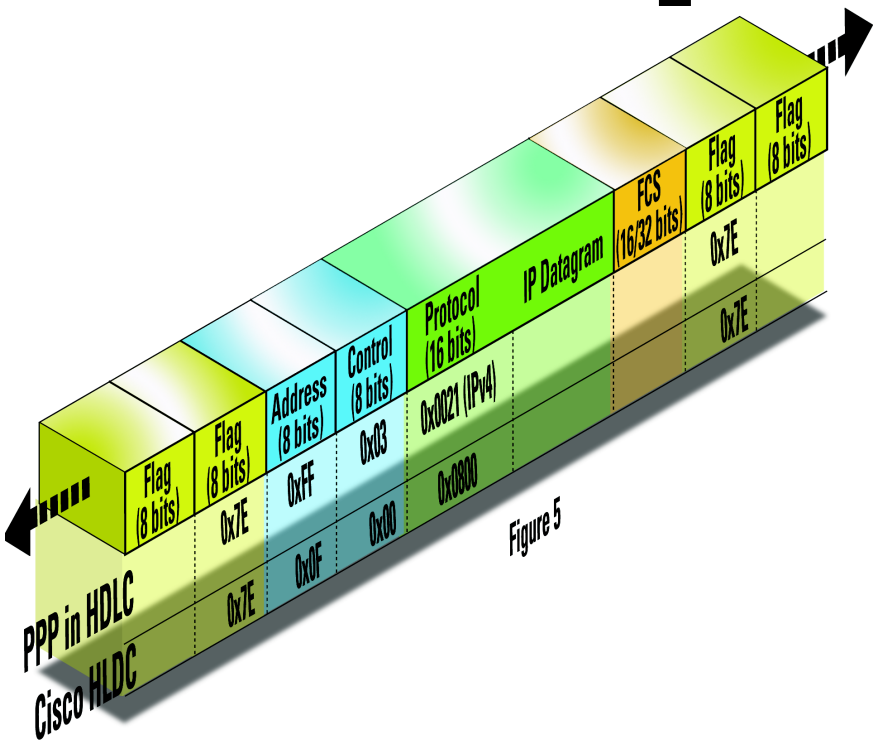


Figure 5

HDLC and stuffing

Octet stuffing and de-stuffing

Packets do not necessarily arrive at a router at fixed intervals. Indeed, the interval between packets varies depending on the volume and distribution of traffic between routers. A mechanism is therefore required to indicate the start and end of a frame. The octet value 7E is used for this. 7E is known as a 'flag' and is used whenever there are no packets occurring between frames. Clearly, 7E must not occur in the data, so an escape sequence is used to replace any 7E-octet value with 7D-5E. The 7D character is considered to be the 'escape' character so it too needs to be replaced. 7D is converted to 7D-5D. The entire process is reversed at the receiver. The example below shows how the bandwidth could increase dramatically if many replacements occurred.

Transmit	
Data (between flag sequences):	DE 45 **7E** 79 B7 D2 41
Octet stuffing*:	DE 45 **7D 5E** 79 B7 D2 41 (bandwidth increased)
Receive	
Data:	DE 45 **7D 5E** 79 B7 D2 41
Octet de-stuffing*:	DE 45 **7E** 79 B7 D2 41

** Octet stuffing only occurs on byte boundaries*

Scrambling

Scrambling

Payload scrambling is implemented in hardware. It is transparent to the user and adds to network stability. The addition of payload scrambling occurs when the HDLC framed PPP packets are inserted into the SONET/SDH frame.

POS scrambling ensures that a malicious user cannot bring the network down by sending patterns which result in SONET/SDH layer low-transition-density synchronization problems, emulating the SONET/SDH frame synchronous scrambler pattern, or replicating the SONET/SDH frame alignment word. POS uses the $x^{43}+1$ self-synchronous scrambler (also used by ATM) to alleviate these potential security problems. But how secure is it?

Predicting the output of the $x^{43}+1$ scrambler requires knowledge of the 43-bit state of the transmitter as the scrambling of a known input is begun. This requires knowledge of both the initial 43-bit state of the scrambler when it started, and every byte of data scrambled by the device since it was started. The odds of guessing correctly are 0.5^{43}, with the additional probability of 1 in 127 (due to the x^7+1 SONET/SDH scrambler) that a correct guess will leave the frame properly aligned in the SONET/SDH payload. This results in a probability of $9e^{-16}$ against being able to deliberately cause SONET/SDH-layer problems. With internet traffic, this level of security is crucial.

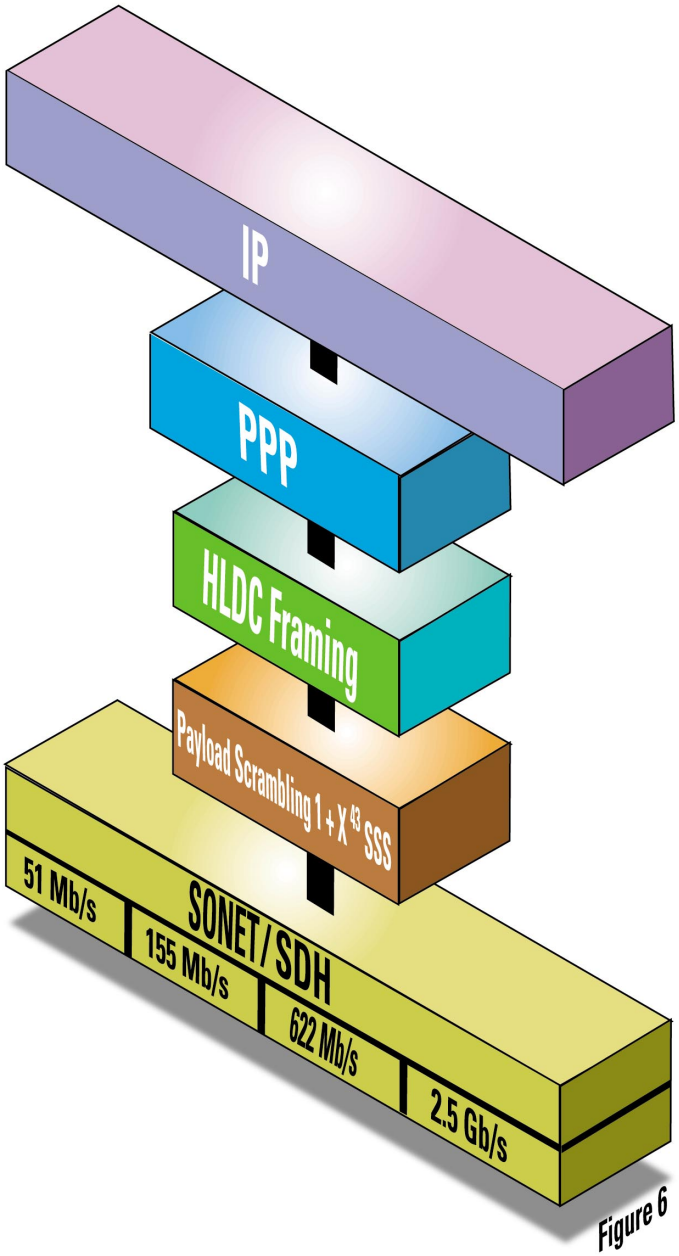
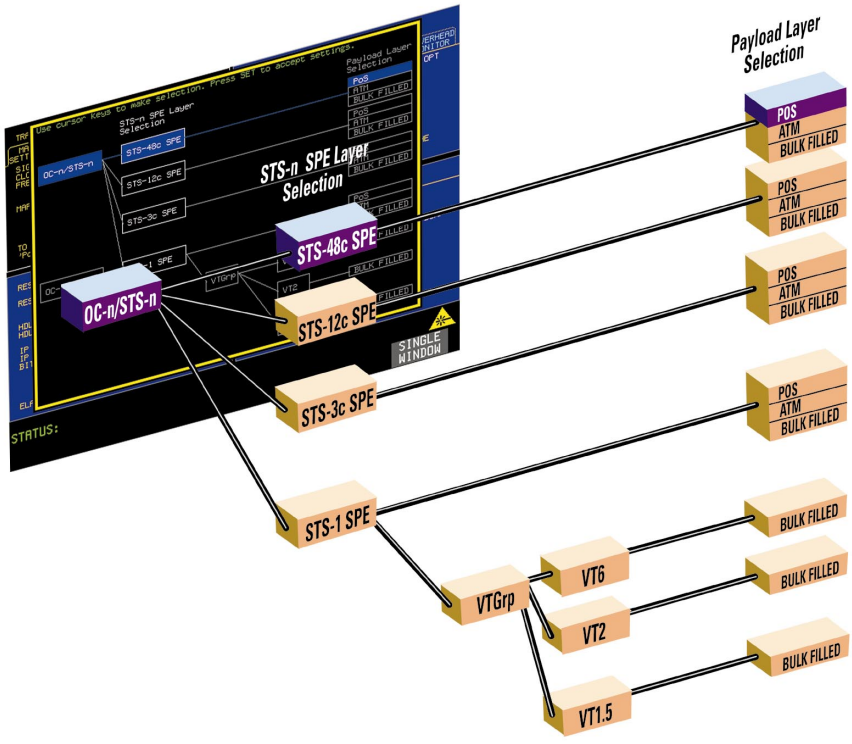

IP
PPP
HLDC Framing
Payload Scrambling 1 + X^43 SSS
SONET/SDH
51 Mb/s
155 Mb/s
622 Mb/s
2.5 Gb/s

Figure 6

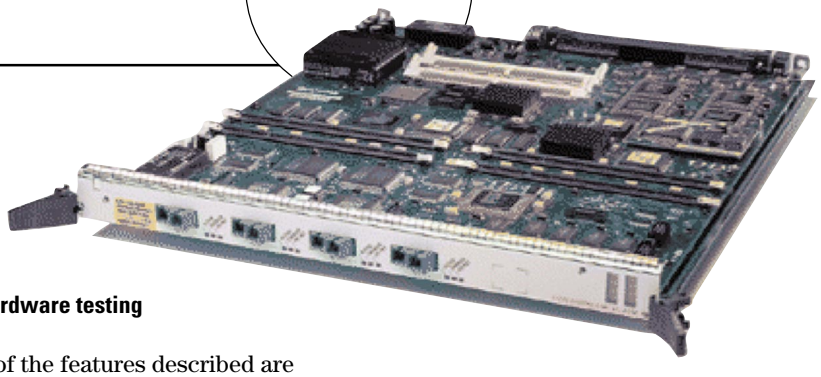
SONET/SDH

Since the mid ‘80s, SONET/SDH has clearly established itself as the primary layer 1 transport mechanism for broadband carrier networks. POS offers a new backbone architecture but preserves the significant investment in this transport infrastructure. SONET/SDH has many benefits including performance monitoring, alarm reporting and protection switching. The signal label byte C2, in the path overhead of the SONET/SDH frame indicates POS payloads. C2 has the value 0x16 when scrambling is ON, and 0xCF when scrambling is OFF. POS is mapped into STS-1/VC-3, STS-3c/VC-4, STS-12c/VC-4-4c or STS-48c/VC-4-16c containers, as shown.

SONET is described in Bellcore GR-253-core, SDH by G.707, for further reference.



POS hardware testing



POS hardware testing

Many of the features described are implemented via hardware. The objective for POS line cards is to process at wireline speeds, and as the rates increase, faster clock speeds and wide bus architectures need to be used. These components also need to be tolerant to any jitter present in the data network.

To ensure correct operation, the hardware has to be fully exercised. This can be done by generating traffic with varying packet sizes, verifying the scrambling, and by exercising the octet stuffing and de-stuffing process and HDLC framing.

Agilent Technologies OmniBER 718 and 719 communications performance analyzers offer extensive layer 1 and 2 POS test capability, including jitter test, channelized POS payloads and measurement of POS service disruption times. They also address the ATM, SDH and SONET technologies.

You'll find further details of the OmniBER 718 analyzer's test capability in the product specifications publications no. 5968-8335E and configuration guide publication no. 5968-8012E

Agilent Technologies' Test and Measurement Support, Services, and Assistance

Agilent Technologies aims to maximize the value you receive, while minimizing your risk and problems. We strive to ensure that you get the test and measurement capabilities you paid for and obtain the support you need. Our extensive support resources and services can help you choose the right Agilent products for your applications and apply them successfully. Every instrument and system we sell has a global warranty. Support is available for at least five years beyond the production life of the product. Two concepts underlie Agilent's overall support policy: "Our Promise" and "Your Advantage."

Our Promise

Our Promise means your Agilent test and measurement equipment will meet its advertised performance and functionality. When you are choosing new equipment, we will help you with product information, including realistic performance specifications and practical recommendations from experienced test engineers. When you use Agilent equipment, we can verify that it works properly, help with product operation, and provide basic measurement assistance for the use of specified capabilities, at no extra cost upon request. Many self-help tools are available.

Your Advantage

Your Advantage means that Agilent offers a wide range of additional expert test and measurement services, which you can purchase according to your unique technical and business needs. Solve problems efficiently and gain a competitive edge by contracting with us for calibration, extra-cost upgrades, out-of-warranty repairs, and on-site education and training, as well as design, system integration, project management, and other professional engineering services. Experienced Agilent engineers and technicians worldwide can help you maximize your productivity, optimize the return on investment of your Agilent instruments and systems, and obtain dependable measurement accuracy for the life of those products.

By internet, phone, or fax, get assistance with all your test & measurement needs

Online assistance:
www.agilent.com/find/assist

Phone or Fax

United States:
(tel) 1 800 452 4844

Canada:
(tel) 1 877 894 4414
(fax) (905) 206 4120

Europe:
(tel) (31 20) 547 2323
(fax) (31 20) 547 2390

Japan:
(tel) (81) 426 56 7832
(fax) (81) 426 56 7840

Latin America:
(tel) (305) 267 4245
(fax) (305) 267 4286

Australia:
(tel) 1 800 629 485
(fax) (61 3) 9272 0749

New Zealand:
(tel) 0 800 738 378
(fax) 64 4 495 8950

Asia Pacific:
(tel) (852) 3197 7777
(fax) (852) 2506 9284

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

Printed in USA 09/00
5980-2027E

Agilent Technologies
Innovating the HP Way