Packet over SONET/SDH (POS) functional testing

Product note

Testing the hardware components that enable efficient transport of data over SONET/SDH transmission networks

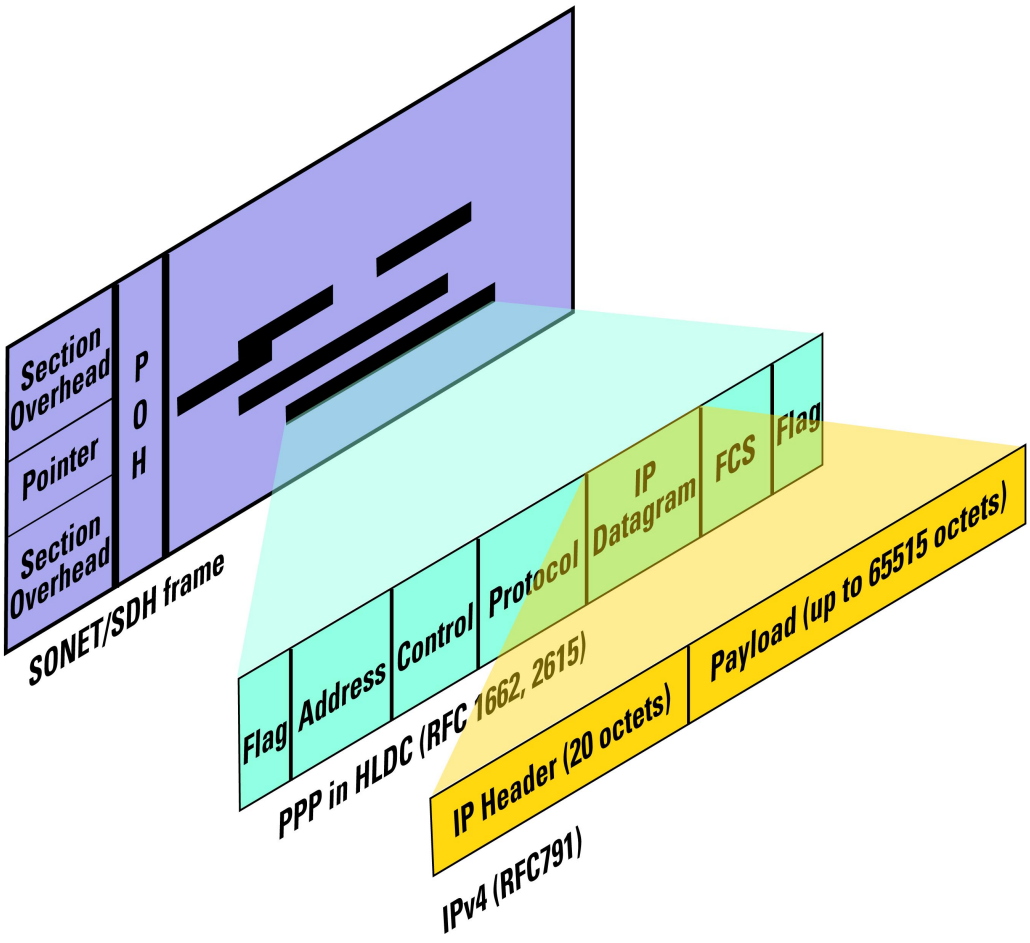
Agilent Technologies
Innovating the HP Way

Introduction

Packet over SONET/SDH (POS) has emerged as the technology of choice for high-speed routers as it enables efficient transmission of internet protocol (IP) packets directly over SONET/SDH fiber. POS is deployed in the line cards of Gigabit and Terabit routers and is implemented in hardware to handle wire speeds ranging from 51 Mb/s to 10 Gb/s.

Pinpointing problems at these line rates can be tricky, particularly as packets at OC-48 could arrive every 130 ns! The data could be captured, but would require analysis off-line to try and track down the problem. On the other hand, real-time POS testing with OmniBER highlights the problem on the spot.

This product note provides an overview of the generic architecture of a router, and the design challenges, and test requirements of POS line cards and chip-sets used in today's backbone and access network routers.



"Packet over SONET/SDH"

Inside a router

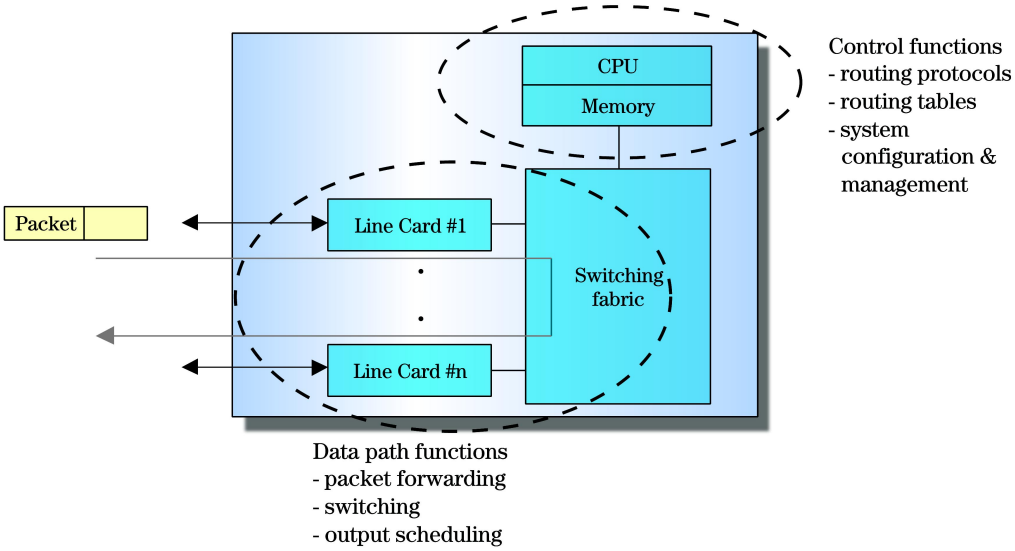


Figure 1 Generic architecture of a router.

Router functions can be separated into control functions and datapath functions.

Control functions

Control functions include routing protocols, the creation and maintenance of forwarding tables used in packet forwarding, and centralized system configuration and management. These functions are performed in software and therefore will not be examined in this product note.

Datapath functions

These are operations that are performed on every IP datagram that passes through the router. They are most often implemented in special purpose hardware and, in terms of packet processing performance of a router, they are crucial. For example, ports may implement sophisticated queuing algorithms to support differentiated services. The hardware elements involved in datapath functions include input ports, switching fabric, and output ports:

- **Input ports:** These ports provide the physical link and are the point of entry for incoming packets. Multiple ports can be supported on a single line card. The input port performs layer 2 encapsulation, and route lookup to determine the incoming packet's destination port.

- **Switching fabric:** Once the route lookup is done, the packet is sent to the output port via the switching fabric. The switching fabric interconnects input ports with output ports, and is a critical component in delivering wire-speed throughput.

- **Output ports:** These ports store packets before they are transmitted on the output link. Like input ports, they also support layer 2 encapsulation.

Having described the generic architecture of a router, the next section looks at the design challenges and functional test requirements of POS line cards and chip-sets.

Design challenges

The port speeds of high-end routers range from 155 Mb/s (OC-3) to 10 Gb/s (OC-192).

To achieve clock speeds that can be processed within hardware, the line-rate needs to be divided down into very wide parallel electrical busses. For example, a 2.5 Gb/s line may be transformed into a 32-bit wide bus operating at 80 MHz. As port speeds increase, the clock speed and/or bus width need to increase as shown below:

Typical POS line card architecture speeds

SONET/SDH rate	OC-3/STM-1	OC-12/STM-4	OC-48/STM-16	OC-192/STM-64
Rate	155 Mb/s	622 Mb/s	2.5 Gb/s	10 Gb/s
Clock speed	20 MHz	40 MHz	80 MHz	80 MHz
Bus width	8 bits	16 bits	32 bits	128 bits

At these line rates, High-level Data Link Control (HDLC) framing must be performed by hardware. Frame Check Sequence (FCS) calculation, octet stuffing and de-stuffing, and payload scrambling are the major sources of complexity in implementing POS, particularly in high-speed wide-bus architectures.

This paper outlines a series of test requirements that have been established to address corner cases of traffic patterns that the line card has to deal with. This helps to highlight the design challenges faced by today's engineers.

POS functional test

The following sections describe the key POS functional test categories. Agilent's OmniBER 718 and 719 analyzers are designed to address each application, and references to specific product features are used to demonstrate how the tests are performed.

Channelized testing

The edge of the network is associated with traffic aggregation or distribution. It is also the point of convergence of regional traffic housed in facilities referred to as network Points of Presence (PoPs). Channelized payloads could be very important in such applications, as the POS payload may only be a part of the full bandwidth signal (Figure 2).

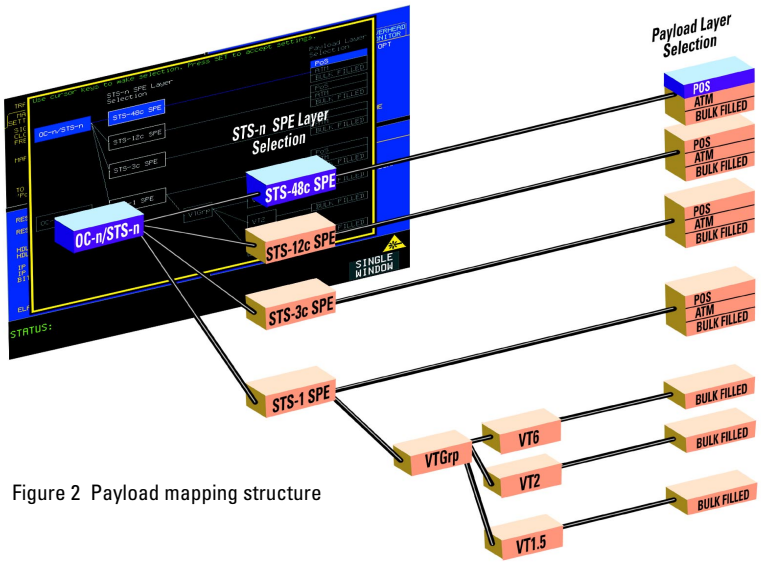


Figure 2 Payload mapping structure

Many layer 1 and layer 2 chip-sets and line cards support SONET/SDH channelization.

Typical configurations are:
3 × STS-1c → OC-3
4 × STS-3c → OC-12
4 × STS-12c → OC-48
16 × STS-3c → OC-48

Any of the POS tests described in this section can be performed either in a single channel, for example, test STS-12c #2 in an OC-48, with the other channels filled with either a 'background' payload (channelized mode), or over the full SONET/SDH bandwidth (concatenated mode).

Continuity check

A simple and effective check of continuity over a packet stream can be made by running a PRBS through the payload part of all the packets (Figure 3) and checking that the PRBS arrives at the receiver intact with no bit errors. A lost or corrupted packet will result in a burst of errors at the OmniBER 718's or 719's receiver.

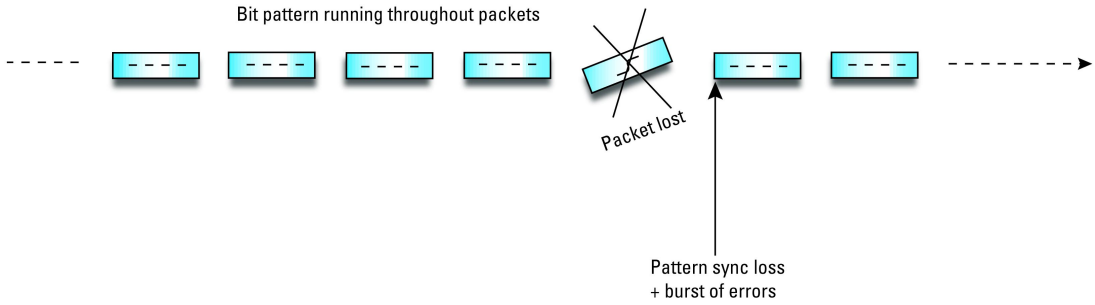


Figure 3 Continuity check

Throughput testing

Throughput refers to the rate at which packets transit a network device. POS line cards and chip-sets will have performance limits imposed by the hardware architecture and by the size and management of buffers. It will be necessary to check that packets can be passed at:
a) minimum packet size, and/or
b) maximum packet rate

The OmniBER 718 and 719 can generate a continuous stream of packets with any size, and with any inter-packet gap.

Achieving the desired throughput:

There are four factors that determine the packet rate:

1. Channel bandwidth (STS-1, STS-3c, STS-12c or STS-48c)
2. Packet size
3. HDLC byte stuffing
4. Inter-packet gap

The available bandwidth (in bytes/second) for packet transmission for each channel type is:

STS-1	6,048,000
STS-3c	18,720,000
STS-12c	74,880,000
STS-48c	299,520,000

For IP, the packet size is specified in terms of the IP datagram size including the 20-byte IP header. The actual packet size transmitted includes four bytes of PPP/HDLC overhead (Address, Control, and Protocol fields) plus the FCS which is two bytes for FCS-16, or four bytes for FCS-32.

The packet size may be further modified by HDLC stuffing. This will add one extra byte every time the flag (7E) or escape (7D) octet appears in the packet. The actual transmitted packet rate (in packets/second) is:

channel bandwidth / (packet size (including overhead and stuffing) + inter-packet gap size)

For example, setting up a packet stream of IP datagrams of size 75 bytes, with a 17 byte gap between packets for an IP datagram with FCS-32 the actual packet size is 75 + 4 + 4 = 83 bytes. Ignoring the effect of HDLC byte stuffing, at 2.5 Gb/s we would expect a packet rate of 299,520,000 / (83 + 17) = 2,995,200 pkts/sec. However, due to the effects of HDLC stuffing, this figure may be slightly reduced. To eliminate the uncertainty due to stuffing, it is possible to choose the IP header and payload carefully so that no stuffing takes place. This can be done by selecting a fixed word pattern as the payload and/or the IP datagram header bytes, until the expected packet rate is detected.

Stress testing (using traffic profiles)

Generating traffic with varying packet and gap sizes, including sizes rarely encountered in live networks, can be used to test all the 'corner cases' of a wide-bus architecture (such as packet sizes that are not rounded to 4-byte boundaries).

The OmniBER 718 and 719 can generate the following traffic profiles to facilitate POS hardware stress testing:

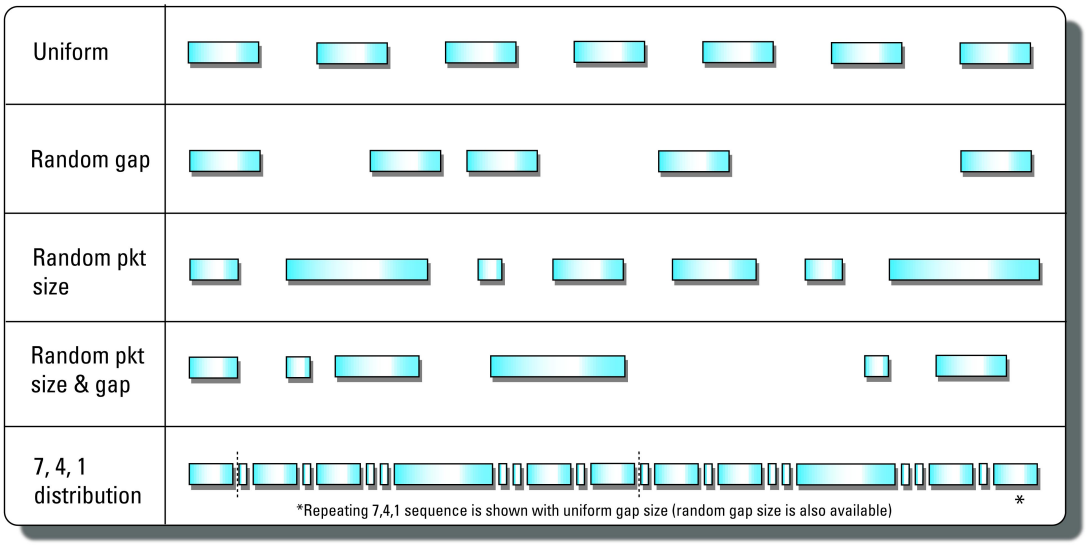


Figure 4 Traffic profiles

Uniform distribution
With uniform packet size and gap, the user can try out different 'phases' of the wide-bus architecture, for example selecting gap sizes of 1, 2, 3 and 4 will test all four byte phases of a 4-byte architecture. The datagram size can be set between 20 and 65,535 octets.

Random distribution
To check for corner case problems in POS hardware, a 'random' distribution can be used. Here, the IP datagram size and/or inter-packet gap is varied between minimum and maximum limits.

For more control over the test, the minimum and maximum values are settable. Minimum sizes are particularly important for stress testing hardware. All architectures have a minimum packet size they can process, so the OmniBER 718/719 tests down to the exact minimum. The probability of a packet with a particular size (between minimum and maximum) is roughly equal for all packet sizes (Figure 5).

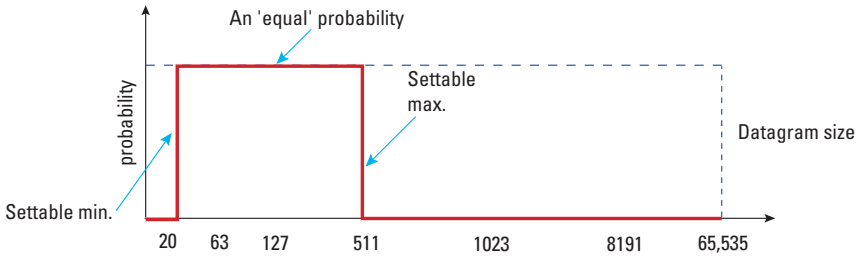


Figure 5 Random datagram sizes

Similarly, random gaps can be generated with roughly equal probability between one octet and maximum (Figure 6). Setting a lower maximum value will make the average packet rate higher.

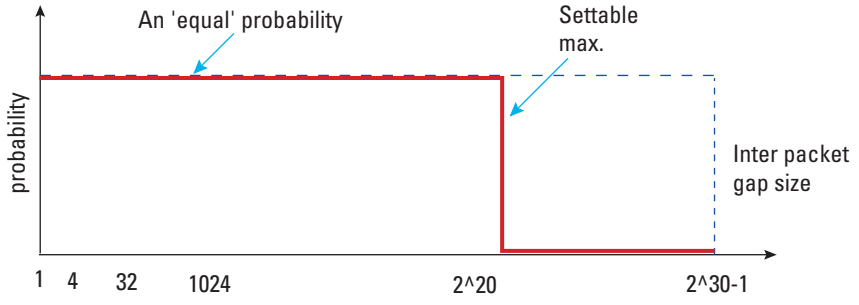


Figure 6 Random inter-packet gap size

Note that random distribution is not realistic traffic but it does exercise all packet sizes, that is, corner cases in the range specified. The stress on the POS hardware is increased if the packets and the gaps between them are not of a consistent size. Changing these parameters in a 'random' way will give a true indication of the performance of the POS hardware.

7,4,1 distribution

While all packet sizes (and gaps) between the hardware minimum and 65,535 octets are possible, studies show that real internet traffic exhibits a packet size distribution which is almost trimodal (Figure 7).

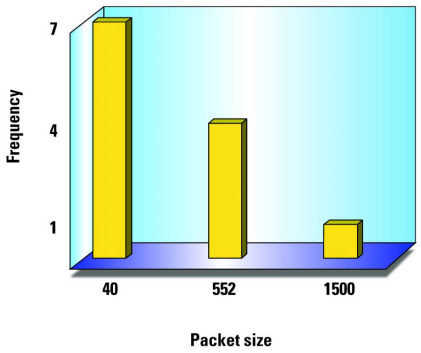


Figure 7 7,4,1,distribution

For example, between 30% and 40% of the packets fall into the 40-byte category. These 'small' packets are typically transmission control protocol (TCP) acknowledgement messages and appropriately considered to be an important corner case in the design of high performance routers. Other modes occur at 552 octets (TCP applications not performing maximum transmission unit discovery) and 1500 octets (maximum segment size for Ethernet). As a consequence, for a more 'realistic' traffic profile, the OmniBER 718 /719 offers a packet length which can be set to a "7,4,1" sequence. The "7,4,1" sequence emulates internet backbone traffic patterns by sending a repeating sequence of twelve packets in which, on average, seven are size 40 octets, four are size 552 octets, and one has size 1500 octets. With this traffic sequence, the gap between packets can be chosen by the user to be either fixed or random.

HDLC stuffing

To fully exercise the HDLC byte stuffing, patterns can be generated which deliberately contain many stuff bytes. The IP payload can be set to a repeating 16-bit or 32-bit word pattern. Any byte of this word can be set to 7E (to emulate the flag sequence) or 7D (to emulate the escape sequence). The OmniBER 718/719 will 'escape' these bytes wherever they occur by changing one bit and then prefixing them with an extra byte (that is the escape byte; 7D). For example, setting the user word pattern to 7E FF 7D FF will result in two extra escape bytes being stuffed into every 4-byte sequence during the payload. A pattern such as 7E 7D 7D 7E will exercise the worst case stuffing rate. Note how the transmit packet rate drops when such a pattern is set. This payload pattern also fully exercises the transmit-direction flow-control mechanism between the POS line card and the router's output buffer.

Service disruption

A common feature of secure networks is the ability to switch the user traffic to a backup path when the main path fails, or under administrative control. This can happen at the SONET/SDH layer, or even at higher protocol layers (for example MPLS). This will usually disrupt the traffic briefly, and the OmniBER 718/719 can measure this disruption by passing a pseudo random binary sequence (PRBS) through the IP payload and then timing the disruption to the PRBS (Figure 8).

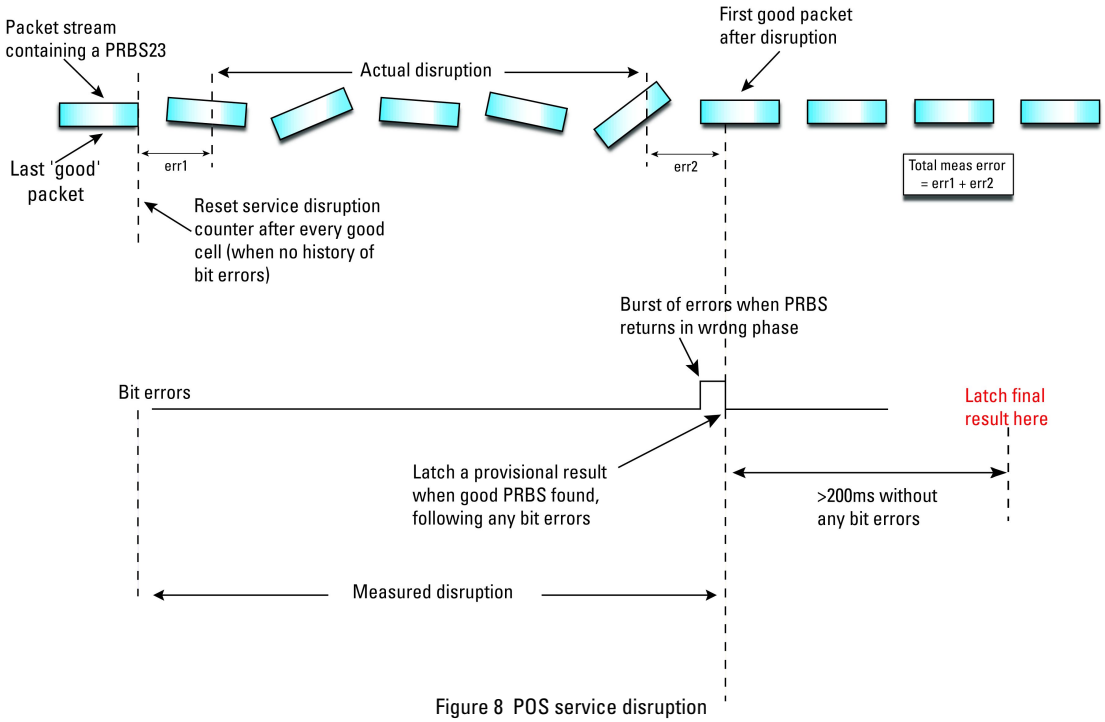


Figure 8 POS service disruption

The measurement is made by sending and receiving a PRBS pattern at the IP layer. The detection of a service disruption is based on the detection of bit errors on the received PRBS. The disruption period is the time from the end of a received error-free packet to the occurrence of the next error-free word (32 bits) after any bit errors have been detected. The measurement is recorded only if 200 ms of no bit errors occur after the disruption period.

Measurement accuracy is proportional to the packet rate. The packet rate in turn is dependent on four factors: channel bandwidth, packet size, inter-packet gap, and stuffing ratio. Hence, it is only practical to approximate the accuracy. To maximize the accuracy of this measurement, the inter-packet gap should be kept to a minimum and the packets should be kept small. However, the resulting packet rate must not exceed the specification of the system-under-test. The accuracy of the measurement is roughly +/- 2*(1/packet_rate). For example, a packet rate of 10,000 packets/sec gives an accuracy of roughly +/- 0.2 milliseconds which is probably accurate enough to measure typical disruptions of many milliseconds.

The network survivability schemes used at the SONET/SDH layer are known as Automatic Protection Switching (APS) for SONET and Multiplexing Switching Protection (MSP) for SDH. APS and MSP are fundamentally similar and depend on protection signaling via the K1/K2 line overhead bytes.

Conclusion

Functional test of the POS processing hardware found in the line cards of high speed routers has an important role to play. It instills confidence that the router hardware will perform to specification — no surprises can be afforded in the backbone infrastructure or data aggregation/distributions at the network edges.

The OmniBER 718/719 provide comprehensive SONET/SDH testing, as well as jitter and optional POS and/or ATM payloads. The POS capability has been specifically designed for fast verification of POS line cards and chip-sets. The focus is on layer 1 and 2 and as such the OmniBER 718/719 offers a very economical and easy to use approach to POS hardware test.

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
5980-2376E

Agilent Technologies
Innovating the HP Way