Worldwide Headquarters

20400 Observation Drive
Germantown, Maryland
20876-4023 USA

Acterna is present in more than 80 countries. To find your local sales office go to:
www.acterna.com

Regional Sales Headquarters

North America
20400 Observation Drive
Germantown, Maryland
20876-4023 USA
Toll Free: +1 866 228 3762
Tel: +1 301 353 1550
Fax: +1 301 444 8468

Latin America
Av. Eng. Luis Carlos Berrini
936/8° e 9° andares
04571-000 São Paulo
SP-Brasil
Tel: +55 11 5503 3800
Fax: +55 11 5505 1598

Asia Pacific
42 Clarendon Street
PO Box 141
South Melbourne
Victoria 3205
Australia
Tel: +61 3 9690 6700
Fax: +61 3 9690 6750

Western Europe
Arbachtalstraße 6
72800. Eningen u.A.
Germany
Tel: +49 7121 86 2222
Fax: +49 7121 86 1222

Eastern Europe, Middle East & Africa
Elisabethstraße 36
PO Box 13
2500 Baden
Austria
Tel: +43 2252 85 521 0
Fax: +43 2252 80 727

1st Neopalimovskiy Per.
15/7 (4th floor)
RF 119121 Moscow
Russia
Tel: +7 095 248 2508
Fax: +7 095 248 4189

Note: Specifications, terms and conditions are subject to change without notice.

ACTERNA™
The Keepers of Communications

PoS/PG/OPT/01-02/AE/ACT00074

Packet over SONET/SDH Pocket Guide

PoS

ACTERNA™
The Keepers of Communications

Acterna is an active member of ITU-T

Publisher: Acterna Eningen GmbH
Postfach 12 62
72795 Eningen u. A.
Germany
e-mail: andreas.kaufmann@acterna.com
http://www.acterna.com

Author: Andreas Kaufmann

Content

Introduction

This Pocket guide is intended to provide an overview of transport traffic features and especially the transport below the Internet Protocol (IP) layer, known as **Packet over SONET/SDH (PoS)**.

Towards the end of the 1980s, Synchronous Digital Hierarchy (SDH) and Synchronous Optical NETwork (SONET) technology were introduced to overcome the problems with Plesiochronous Digital Hierarchy (PDH) technology. Both SDH and SONET are Time Division Multiplexing (TDM) transmission technologies. The SDH/SONET standard has evolved to 10 Gbit/s for today's new systems, which are mainly optimized for voice transmission. However the trend is not only towards higher bit rates like 40 Gbit/s and 80 Gbit/s, Wavelength Division Multiplexing (WDM) technology is also enjoying steady growth. Systems with up to 160 wavelength channels are now operating, each transmitting 10 Gbit/s on one fiber.

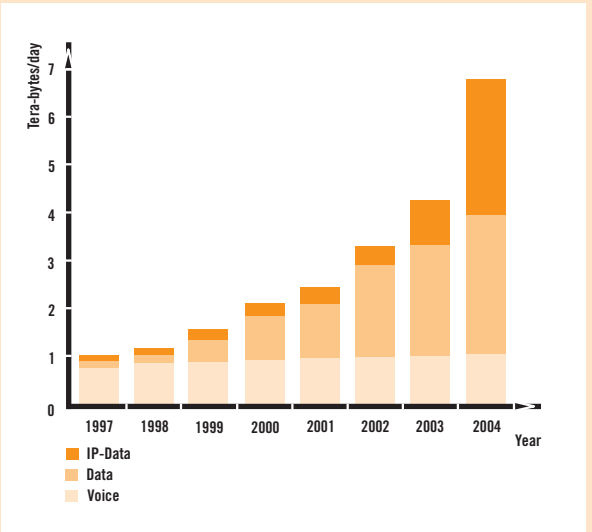
These trends are driven by market development towards more data oriented traffic as illustrated in Figure 1. IP in particular, continues to grow at an explosive pace. Leading Internet providers report that bandwidth doubling on their backbones approximately every six to nine months.

The adoption of Intranets and Extranets for networked commerce will bring further changes to the IP-service infrastructure, both through bandwidth demands and feature requirements. Service providers recognize this unprecedented explosion in packet-based traffic and are re-evaluating their network architectures in light of these changes.

Resourceful designers combine the benefits of Dense Wavelength Division Multiplexing (DWDM), TDM and the reliable SDH/SONET technologies. In doing so it is possible to transport data streams up into the terabit range.

The increased IP traffic requires a technology to transport the IP packets to the physical layer. This transport below IP is presented by Packet over SONET/SDH as one possible route.

figure 1 *Trend in traffic types*



Benefits of Packet over SONET/SDH

- Efficient point-to-point IP service at high speeds
- Future-proof technology
- IP offers simultaneous handling of voice, video and data traffic
- Utilizes advantages (reliability, scalability and manageability) of existing SDH/SONET infrastructure
- PoS offers significant advantages through efficient bandwidth utilization due to less overhead, see figure 2
- One layer less to manage than with ATM, see figure 3
- Reuse of familiar link-layer protocols

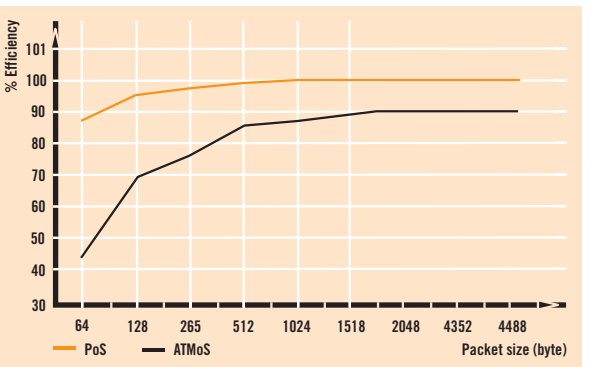
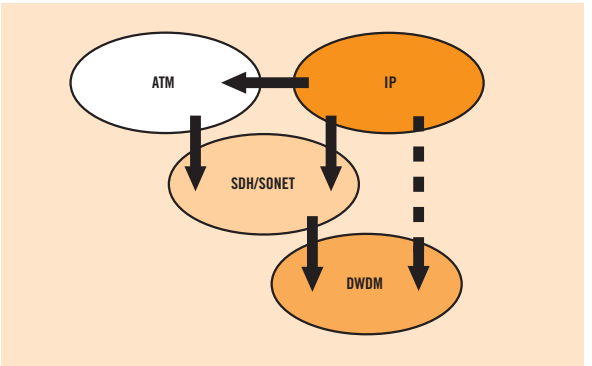


figure 2 *PoS and ATM bandwidth efficiency*

figure 3 *Possible scenario for IP traffic to the physical layer*



OSI Model and Internet Protocol

The Open System Interconnection (OSI) model is used to step through a typical transmission process leading to the description of the various layer protocols and finally on to that of Packet over SONET/SDH (PoS) description. As a result, the correlation between the different layers becomes clearer.

figure 4 *ISO-OSI model*

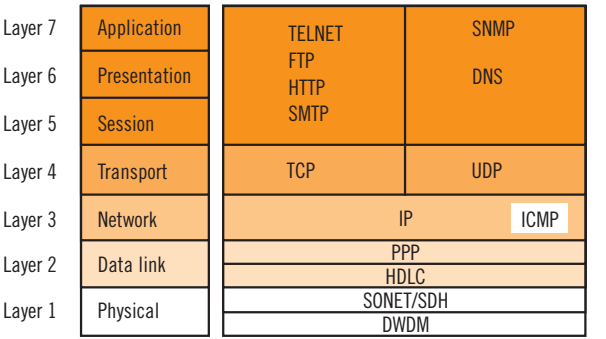


Figure 4 shows the seven layers of the OSI model. From top to bottom, the OSI model starts with the Application layer which is directly accessible to the user. The signal is then transmitted through several layers to the physical layer.

Application Layer

The Application, Presentation, and Session layers (7, 6, and 5) are merged and in the following section will be referred to as the “Application Layer”.

The applications can be divided into two groups, one using the **Transmission Control Protocol (TCP)** for additional transport, the other utilizing **User Datagram Protocol (UDP)** protocol. (The difference between these two protocols will be addressed later.)
Table 1 provides an overview of the most commonly used applications to the reader because they are regularly used in daily life. Some are mentioned briefly below:

User application	Protocol	Request For Comments (RFC)
E-mail	Simple mail Transfer Protocol **SMTP**	RFC821
For copying files File transfer	File Transfer Protocol **FTP**	RFC959
Remote terminal login	**Telnet**	RFC854
Exchange of WWW information	Hyper Text Transfer Protocol **HTTP**	RFC1945
For Simple Network Management applications	Simple Network Management Protocol **SNMP**	RFC1157
Identification of host with IP address	Domain Name System **DNS**	RFC2929, RFC1591

table 1 *Application protocols and their use*

Transport Layer

Due to the more general nature of this booklet, detailed descriptions of the protocols running in the application layers will not be covered.

The Transport layer contains two major protocols – TCP and UDP – distinguishable by their reliability and low transport overhead.

User Datagram Protocol (UDP) – The User Datagram Protocol is the simpler of the two and is typically used when reliability and security are are of secondary importance to the speed and size of the overhead. It is an end-to-end protocol which adds port addresses, checksum error control and length information to data from the upper layer. Figure 5 illustrates the UDP header format.

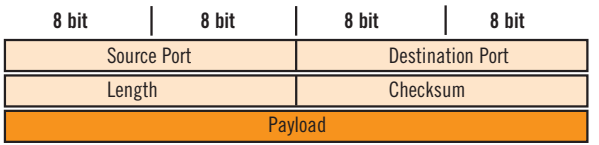


figure 5 *UDP datagram*

Table 2 provides a brief description of these header fields:

table 2 *Definitions of UDP header fields*

Source port	Specifies the port address of the application program which created the message
Destination port	Specifies the address of the application program which will receive the message
Length (16 bit)	Specifies the total length of the user datagram in bytes
Checksum	This is a 16-bit field used in error detection

When paired with the Internet **Control Message Protocol (ICMP)**, UDP can inform the transmitter when a user datagram has been damaged and discarded. Neither protocol is able to specify which packet has been damaged when repairing an error. UDP can only signal that an error has occurred.

Transmission Control Protocol (TCP)– TCP provides full transport layer services to applications. It is **connection-oriented**, meaning that a connection must be established between two peers before either can transmit data. In doing so, TCP establishes a **virtual connection** between sender and receiver which remains active for the duration of the transmission.

Each transmission via TCP starts with a message to the receiver, alerting it that more IP packets are on their way. Each transmission is terminated by a termination message. When sending data, TCP divides long data packets into smaller data units and packages them into “segments”. Each segment includes a sequencing number for reordering after receipt, as well as an acknowledgement ID number. These segments are transported across the network inside the IP datagrams. The receiver collects each datagram as it comes in and re-orders the transmission based on the sequence numbers. TCP is a reliable protocol, as each data transmission is acknowledged by the receiver with TCP, data is transmitted in both directions. If the sender does not receive acknowledgement within a specified time, it retransmits the data.

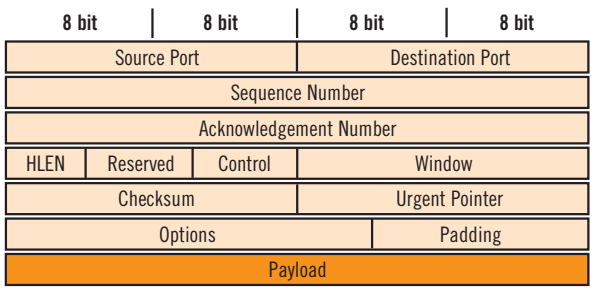


figure 6 *TCP datagram*

To provide secure delivery for the TCP an extensive segment header is required (see figure 6).

Table 3 contains a description of the TCP segment fields:

Source port	Defines application program in the source computer
Destination port	Defines the application program in the destination computer
Sequence number	The Sequence number shows the position of the data in the original data stream
Acknowledgement number	32-bit acknowledgement number is used to acknowledge receipt of data
Header length (HLEN)	Indicates the number of 32-bit words in the TCP header
Reserved	6-bit field reserved for future use
Control	6-bit field providing control functions
Window size	16-bit field defines the size of the sliding window
Checksum	16-bit checksum used in error detection
Urgent pointer	Valid only when the URG bit in the control field is active.
Options and padding	Defines optional fields and are used to convey additional information to the receiver or for alignment purposes.

table 3 *Definitions of TCP header fields*

Comparison of UDP and TCP protocols

UDP features:
- Connectionless protocol
- No error recovery
- Unreliable
- Fast speed
- Small overhead

TCP features:
- Connection-oriented protocol
- Error detection and recovery
- Reliable
- Slower than UDP
- Large overhead

UDP applications:
- Voice
- Broadcasting
- Etc.

TCP applications:
- HTTP
- FTP
- Etc.

Network Layer – Internet Protocol version 4

The History of the Internet Protocol – The Internet Protocol (IP) was developed by the **A**dvanced **R**esearch **P**roject **A**gency (ARPA), an arm of the U.S. Department of Defense and was first tested in 1968/69 with computer-to-computer connections. The objective was to ensure that the military could maintain communications in the event of a nuclear war.
The protocols and conventions developed by the ARPA evolved to become TCP/IP. Due to the growth of TCP/IP traffic the ARPANET became the backbone of a network known today as the Internet.

IP is the transmission method used by TCP/IP.
IP transport is sent in packets called “datagrams”, each of which are transported separately. The individual packets may travel by different routes, as IP has no tracking capabilities or facility for reordering lost datagrams.

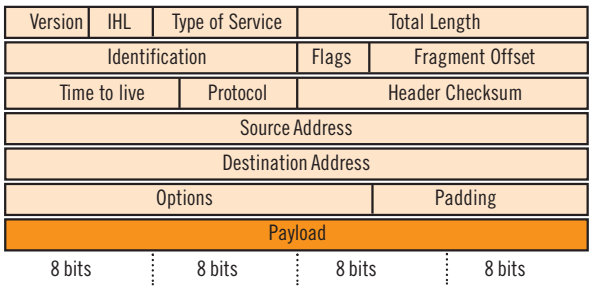


figure 7 *The format of an IP datagram*

An IP datagram is a variable-length packet of up to 65,536 bytes consisting of two parts; the header (made up of 20 to 60 bytes) and the data (20 to 65,536 bytes). The header contains essential information about routing and delivery service of the IP packets. The structure of the IP header is illustrated in figure 7.

table 4 *Definitions of IP header fields*

Version	This field defines the version number. IPv4 corresponds to bin. 0100
Internet Header Length (IHL)	This field defines the length of the header in multiples of four bytes.
Type of Service	This field defines how the datagram should be handled (priority of transport, reliability and delay) and contains information on the Type of Service (ToS)
Total Length	This field defines the total length of the IP datagram. It is a two-byte field (16 bits) and can define up to 65,536 bytes (this includes the header and the data).
Identification	This field is used in fragmentation. When packets are moving independently through the network, they are identified by a number in this field.
Flag	The bits in this field handle fragmentation
Fragmentation offset	This field provides a pointer which shows the offset of the data in the original datagram

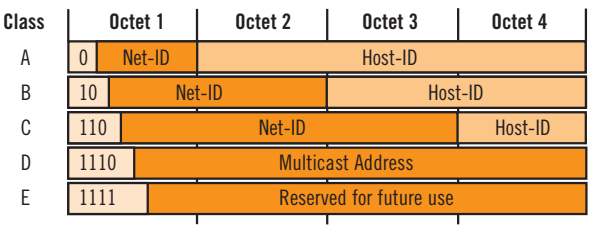
Time to Live	This field defines the number of hops a packet can travel before it is discarded. The source host sets this field to an initial value (max. 256). Each router decrements this value by “1”. Should this value reach “0” before the datagram reaches its destination, it is discarded.
Protocol	This field defines which upper-layer protocol data are encapsulated in the packet (e.g. TCP, UDP, ICMP, etc.)
Header Checksum	Field of 16 bit length, calculates the checksum of the header only.
Source Address	This field contains a four-byte (32-bit) with IPv4 Internet address and identifies the original source of the packets.
Destination Address	This field contains a four-byte (32-bit) with IPv4 Internet address and identifies the final destination of the packets.
Options	This field can carry information which controls the routing, timing, management and alignment of the data.

Internet Addressing – The source and destination address identify the connection of the host to its network. Each internet address consists of four bytes (32 bits) which define 3 fields: class type, Net-ID and Host-ID. These fields have varying lengths depending on the class of the address. The general structure of the IP address is illustrated in figure 8.

figure 8 *IP address structure*

Currently five different classes exist from A to E. They each are different pattern lengths and are designed to cover the needs of different types of organization. The Internet classes and their byte distribution are shown in figure 9.

figure 9 *Existing Internet address formats*



Class A only uses one byte to identify the class type and Net-ID, leaving three bytes available for Host-ID numbers. This results in Class A networks accommodating far more hosts than **Class B** or **C** networks. At present Classes A and B are full. Addresses are only available in Class C.
An overview of how many networks and hosts can be supplied by different types of class is shown in table 5.

table 5 *Internet Class addresses and their potential use*

Class A	– 127 possible network IDs – 16,777,214 host IDs per network ID
Class B	– 16,384 possible network Ids – 65,534 host IDs per network ID
Class C	– 2,097,152 possible network IDs – 254 host IDs per network ID

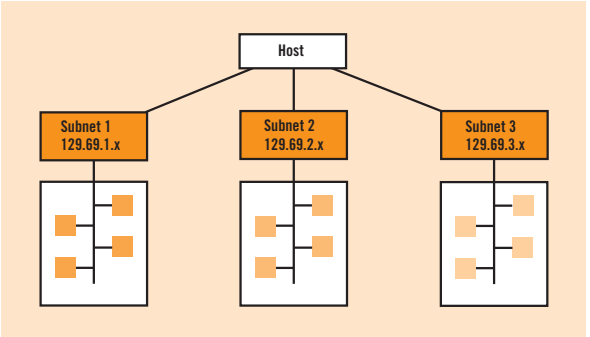
Class D is reserved for **multicast** addresses. This means that IP datagrams are allowed to be delivered to a selected *group* of hosts only, rather than to an *individual*.
Class E is reserved for future use. Internet addresses are usually written in decimal form, points separating the bytes (for example 137.23.145.23).

Subnetting – To circumvent some of the limitations of the addressing conventions of IPv4, it is possible to introduce *subnet* structures. The addressing convention (RFC950) used results in the following division of the classes (see figure 10).

figure 10 *IP addressing in case of subnetting*

The network administrator is able to divide the host address space into groups (subnets) mainly to mirror topological or organizational structures. At a university, for example, the various faculties might be groups under the host name.
This procedure simplifies routing in a network and allows a clearer structure of the network to be seen.
Figure 11 illustrates how a subnetting structure might look.

figure 11 *Example of subnetting for a Class A type IP address.*



Internet Control Message Protocol (ICMP) – The Internet Control Message Protocol (ICMP) is used by hosts and gateways to inform the sender of datagram problems and to exchange control messages. The Internet Control Message Protocol (Recommendation RFC792) uses IP to deliver these messages. Although IP is an unreliable and connectionless protocol, ICMP uses IP to inform the sender if a datagram is undeliverable. ICMP only reports problems, it does not correct errors. The following examples show the types of messages which could be sent:

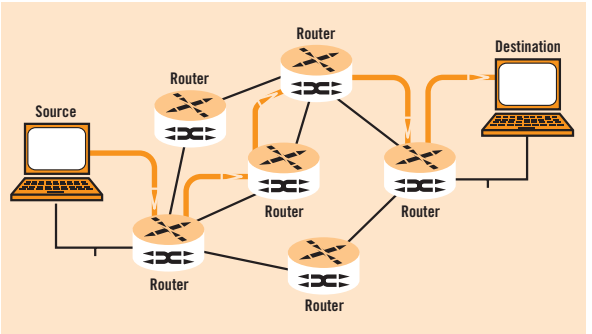
Error messages:
- Destination unreachable
- Redirect packet
- Time exceeded

Information messages:
- Echo request, echo response
- Time stamp (Ping)

If a user were to type an incorrect HTTP address in the Web browser, it would be sent to the DNS server which in turn would return an IP address to be sent to the respective server. If the server were down, the message: "Destination unreachable" would be sent to the user.

IP Routing and Switching – In the Internet, packets are dynamically routed from the source to the destination by a hop-by-hop movement. Routers and switches are used to ensure the packet is delivered correctly.
Routers are "intelligent" network elements operating in the Network layer of the OSI model. Routers have access to Network layer addresses and contain software enabling them to determine which of several possible paths between addresses is appropriate for a particular transmission. Routers relay packets among multiple interconnected networks and can route packets from one network to any number of destination networks on an internet (see figure 12).

figure 12 *Possible routing scenario*



The IP networks are usually designed in a mesh structure so that if an interruption in the transmission occurs, an alternative path can be found quickly. The routing process is a **dynamic procedure** which allows the system to forward a packet via its most efficient path from source to destination address. The "decision" as to how packets are routed through a network follows multiple routing algorithms. The description of these algorithms would, however, be beyond the scope of this booklet.

Switches are layer 2 network elements responsible for establishing temporary **static connections** between two or more devices linked to the switch, but not to each other.

figure 13 *Switched network*

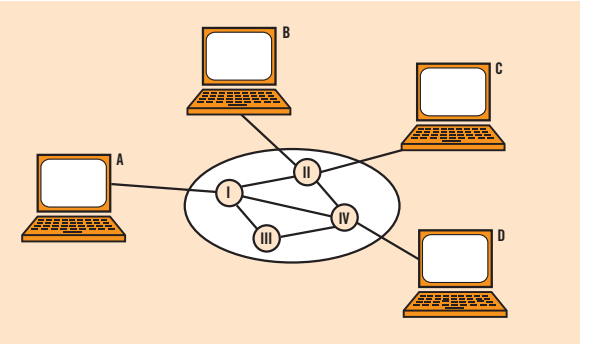
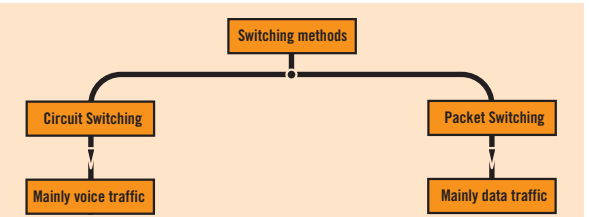


Figure 13 illustrates a switched network. The communicating devices are labeled A, B, C, D, the switches I, II, III, IV. Each switch is connected to multiple links and is used to complete the connections between the communicating peers. As soon as the switches are set, they are static for one specific transmission process and can then be reconfigured. Figure 14 shows two principal switching methods available.

figure 14 *Network switching methods*

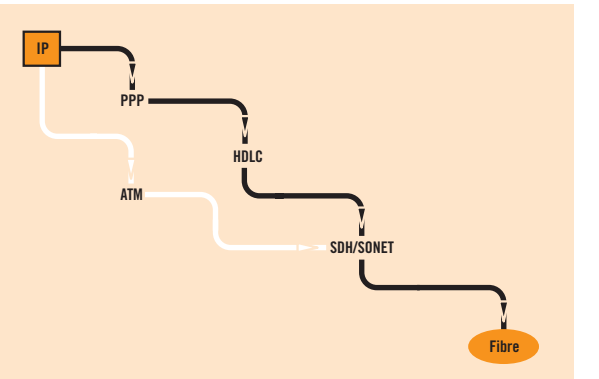


Circuit switching was designed primarily for voice communication. In a telephone conversation for example, once a circuit is established it remains connected for the duration of the session. Circuit switching is not suitable for data or other non-conversational transmissions. Non-voice transmissions tend to come in bursts therefore in a circuit switched circuit, the line is often idle and its facilities wasted. In a **packet switched** network, data is transmitted in discrete units of potentially variable length packets. The maximum length of a packet is established by the network and long transmissions are broken into multiple packets. Each packet contains not only the data but also a header containing the control information. The packets are sent over the network hop-by-hop and routed through the network according to the information in the packet header with the address information.
Message switching, with a network node receives a message, stores it until the appropriate route is free, then sends it.

Packet over SONET/SDH (PoS)

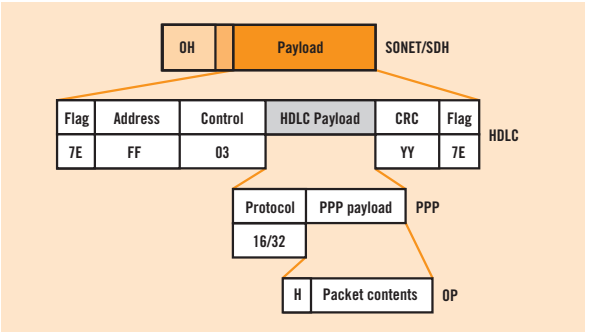
From the Network layer, the IP packets need to be delivered to underlying layers. The actual transmission below the transport layer is called Packet over SONET/SDH (PoS). This transmission can be achieved via alternative routes, two of which are illustrated in figure 15.

figure 15 *Alternative routes for transmitting IP packets to the fiber*



The route (solid line) described in this booklet is recommended by the Internet Engineering Task Force (IETF) and is illustrated in figure 16.

figure 16 *Mapping of IP packets into SONET/SDH frames*



The IP packets are encapsulated in a Point-to-Point Protocol which in turn is mapped into a HDLC-like frame. This frame is then mapped into the SONET/SDH frame.

Point-to-Point Protocol

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams (e.g. IP packets) over point-to-point links. Initially, PPP was used over Plain Old Telephone Services (POTS). However, since the SONET/SDH technology is by definition a point-to-point circuit, PPP/HDLC is well suited for use over these lines. PPP is designed to transport packets between two peers across a simple link.

Features of the PPP link:

- Allows for full-duplex and simultaneous operation
- No restrictions regarding transmission rates imposed
- Operates across most Data Terminating Equipment/Data Circuit-terminating Equipment (DTE/DCE) interfaces (e.g. RS232, RS422, V.35, etc.)
- Does not require any hardware control signals (e.g. Request to Send, Clear To Send, etc.)

PPP is intended to provide a common solution for the easy connection of a wide variety of hosts, bridges and routers. The encapsulation of PPP into HDLC-like frames allows for the multiplexing of different network-layer protocols (IP, IPX, AppleTalk, etc.) simultaneously over the same link.

PPP consists of three main components:

- A method for encapsulating multi-protocol datagrams (PPP encapsulation).
- A Link Control Protocol (LCP) for establishing, configuring and testing of the data link connection.
- A family of Network Control Protocols (NCPs) for establishing and configuring different network layer protocols.

PPP Encapsulation and PPP Emulation

PPP Encapsulation – To allow multi-protocol datagrams to be transmitted across a link, a method must be used to enable unambiguous decisions to be made between the various protocols. The PPP encapsulation of the IP packets is illustrated in figure 17.

figure 17 *PPP encapsulation according to RFC1661*

The fields are transmitted from left to right and have the following names and functions:

Protocol Field – Consists of 1 or 2 octets, with values identifying the encapsulated datagram.
Data Field – This field is zero or more octets long and it contains the datagram for the protocol specified in the Protocol field. The maximum length, including padding (but not the protocol field) defaults to 1500 octets. This means, for example, that if an IP datagram with a larger payload were transported it would be fragmented into several packets to fit the size of the data field.
Padding Field – At the beginning of the transmission this field may be padded with an arbitrary number of octets (up to 1500 octets). It is the responsibility of the protocol to distinguish padding from real information.

PPP Emulation – The **PPP emulation** describes:
- The Link Control Protocol and
- The Network Control Protocol

Link Control Protocol (LCP)

The LCP is responsible for correctly establishing, configuring and testing the Point-to-Point Protocol. Before IP datagrams can be transported across a PPP link, each of the connected PPP interfaces must send out a series of LCP packets.

figure 18 *Illustration of LCP procedure*

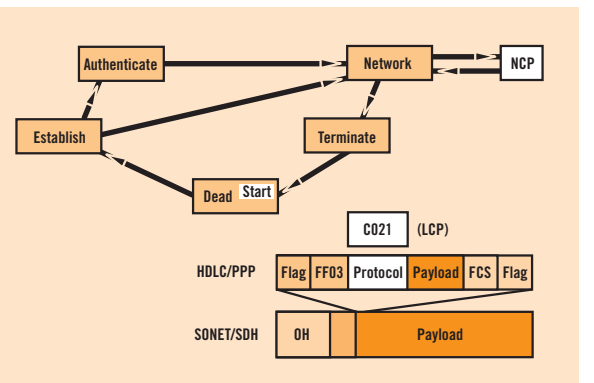


Figure 18 illustrates the four key phases the LCP steps through.

Step: Link dead – Each PPP connection starts and ends in this state. In this state there is either no connection to the modem or the connection has been interrupted. When an external event (control signal or network administrator) indicates that the Physical layer is ready to be used, PPP proceeds to the establishment phase.

Step: Link Establishment – Before data from an upper layer (e.g. IP) can be transported across a connection, the link is prepared via configuration packets. This exchange is completed, and the Open state achieved after a "Configure" packet has been sent and received. The entire configuration options are set to default values, unless altered. Any non-LCP packets received during the establishment phase are discarded.

Step: Authentication – This is an optional step, allowing the PPP peers to identify each other via authentication protocols. These are called **Password Authentication Protocol** (PAP) and **Challenge Handshake Authentication Protocol** (CHAP).

The **Password Authentication Protocol** sends a password across the link, so that the circumstances in which it can operate are negotiated.

The **Challenge Handshake Authentication Protocol** has the ability to provide reliable and secure authentication. As the authenticator and authenticatee share a common password. The authenticator sends the connected peer a challenge in the form of a random number. The authenticatee uses this random number to derive a secret code. This code is then transmitted to the authenticator and if the results match, the next connection stage can proceed.

Step: Network Layer Protocol Configuration – This is necessary for the configuration of the Network Control Protocols (NCP) used on this connection. Each network layer protocol (e.g. IP, Appletalk, etc.) must be separately configured by the appropriate NCP. It is possible with PPP to run several NCPs over one connection.
After an NCP has reached the Opened state, PPP will carry the corresponding network layer protocol packets. Any network layer protocol packets received when the corresponding Opened state has not been reached are discarded. During this phase, link traffic consists of any possible combination of LCP, NCP and network layer protocol packets.

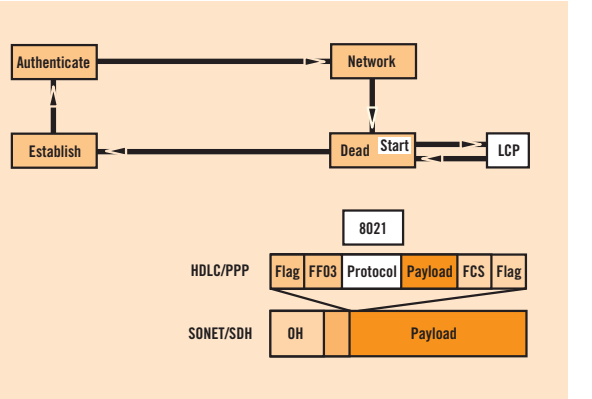
Step: Link Termination – With the LCP it is possible to close a connection at any time. This can be done by a user event, set timer or missing interface signal. Between step 3 and step 4, Link Quality Monitoring (LQM) can take place and the data connection tested for quality of transmission. The **Link Control Protocol information** is sent in the form of PPP datagrams, which fall into the following three major classes:

- **Link Configuration packets** used to establish and configure a link (RFC1661)
- **Link Termination packets** used to terminate a link (RFC1661)
- **Link Maintenance packets** used to manage and debug a link (RFC1661)

Network Control Protocol (NCP)

A family of **Network Control Protocols** allow for the preparation and configuration of different protocols to run in the various network layers. One of these protocols, the IPCP, is described below as an example and is illustrated in figure 19.

figure 19 *Illustration of a common NCP procedure*



This protocol allows for the activation, configuration and deactivation of the IP protocol modules on both sides of the point-to-point connection. Like the LCP, these functions are achieved through the exchange of special data packets, for IPCP, this packet is hex8021 (protocol identifier). The exchange of IPCP packets starts after completion of step 4 of the LCP protocols. The NCP then runs through steps equivalent to those of the LCP procedure once the LCP protocol is in the network state (see figure 21).

When the LCP and the NCP protocols are fulfilled the data can be transmitted across the point-to-point connection.

High-Level Data Link Control (HDLC)

The Point-to-Point Protocol provides a standard method for transporting multi-protocol datagrams over point-to-point links. The PPP packets are encapsulated in a HDLC-like frame which is then mapped into the SONET frame. The format of this HDLC frame is illustrated in figure 20.

figure 20 *Format of HDLC-like frame according to RFC1662*

Flag Sequence – Each frame begins and ends with a Flag Sequence, which is the binary sequence 01111110 (hex 0x7e). All implementations check for this flag which is used for frame synchronization. Only one Flag Sequence is required between two frames. Two consecutive Flag Sequences constitute an empty frame which is then discarded silently.

Address Field – The Address Field is a single octet containing the binary sequence 11111111 (hex 0xff). Individual station addresses are not assigned.

Control Field – The Control Field contains the binary sequence 00000011 (hex 0x03). Frames with unrecognized Control field values are discarded silently.

Protocol Field – The Protocol Field is one or two octets, with a value identifying the datagram encapsulated within the Information field of the packet. The identifiers for the most frequently used protocols are:

table 6 *Identifiers used in the protocol field in the HDLC frame*

Hex value	Protocol used
0021	IP
C021	LCP
8021	NCP (IPCP)

Information – The Information field is zero or more octets and contains the datagram for the protocol specified in the Protocol field. The Information field, including Padding but not including the Protocol field, is called the Maximum Receive Unit (MRU) and has a maximum length of 1500 octets.

Padding – The Information field may be padded with an arbitrary number of octets up to the MRU.

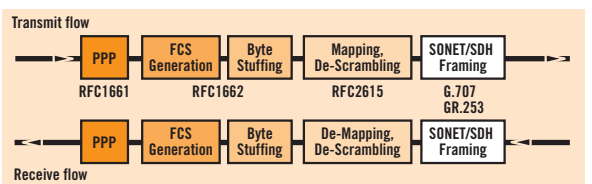
Frame Check Sequence Field – The Frame Check Sequence (FCS) defaults to 16 bits for OC-3/STM-1 although other speeds use 32 bits as well. Its use is described in PPP LCP Extensions of RFC2615.

The FCS field is calculated over all bits of the Address, Control, Protocol, Information and Padding fields and is illustrated by the grey fields in Figure 21. It **does not include** the Flag Sequences or the FCS field itself.

figure 21 *Fields of the HDLC-like frame used to perform the FCS*

PPP uses the FCS for error detection and is commonly available in hardware implementations. The end of the Information and Padding fields is found by locating the closing Flag Sequence and removing the Frame Check Sequence field. The **HDLC process** and related recommendations are illustrated in figure 22.

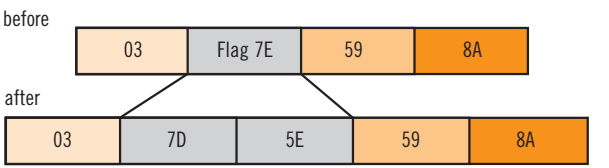
figure 22 *How an IP packet is transmitted to and received by the SONET/SDH frame*



FCS generation/detection – See page 38.

Byte stuffing/de-stuffing – The PPP protocol **must not** place any restrictions on the use of certain bit patterns in the network layer packet and must be **transparent** to any type of data. Because the PPP protocol uses specific patterns, e.g. the flag **field 0x7e** which indicates the beginning and end of a frame, a method is required to avoid restrictions. This is achieved through **byte stuffing** where the PPP defines a special **control escape byte, 0x7d**. The byte stuffing procedure also acts for the Control Field and the Control Escape byte.
The process of byte stuffing is illustrated in Figure 23 where the Flag 7E is replaced by 7D,5E.

figure 23 *Illustration of the Byte-stuffing procedure*



If the Control Flag 7D is within the payload, it is replaced by 7D,5D.

Scrambling/Descrambling procedure – Described in RFC2615, a data scrambler with the $1+x^{43}$ polynomial is used in this procedure. While the HDLC FCS is calculated, the scrambler operates continuously through the bytes of the payload bypassing SONET Path Overhead bytes and any fixed information. This type of scrambling is performed during insertion into the SONET/SDH payload.
The **Path Signal Label C2** is used so that the SONET/SDH can recognize the payload content.

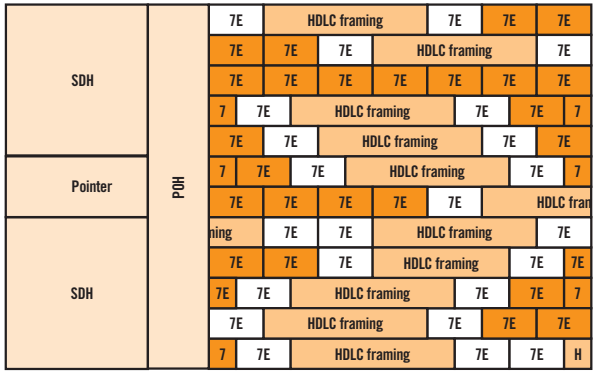
table 7 *Path Signal label C2 identifier*

Value signal label C2	Scrambler state
0x16	PPP with $1+x^{43}$ scrambling
0xCF	PPP with scrambler off

Mapping into the SONET/SDH frame

The PPP frames are inserted into the SONET/SDH payload sequentially row by row and sit in the payload envelope as octet streams aligned to octet boundaries.

figure 24 *Mapping of HDLC/PPP/IP packets into the SONET/SDH payload*



Because the frames can be of variable length they are allowed to cross the SONET/SDH boundaries. The HDLC frames are mapped into the SONET/SDH frame dynamically meaning that when there is no traffic, the SONET/SDH frame is filled with **idle frames** 7E, see figure 24.

PoS Measurement Tasks

With the increase in IP traffic transported across SDH/SONET/DWDM networks, it is necessary to measure the quality parameters with genuine IP traffic. Thus, the payload is filled with HDLC/PPP/IP packets instead of a traditional Pseudo Random Bit Sequence (PRBS). This corresponds to a more realistic representation of the real traffic to be transmitted on these networks.
The user is provided with information on how many packets were lost in a specified period (for example 24 hours), instead of an error rate of 10^{-14} for example. This is more informative than the traditional error rate when sending packets.
Using packets instead of PRBS to fill the payload provides a more realistic traffic profile. Due to the increased transport data and IP traffic in our networks, the payload being filled with IP packets will become more widely accepted in the future.
The following applications are suitable for measuring the quality parameters of individual Network Elements (NE) as well as entire SDH/SONET/DWDM networks during installation.

Frame errors – This error message gives information on the number of HDLC frames lost over a predefined period of time. The customers benefit from receiving a performance measurement based on packet and not byte parameters.

Frame rate – This is the rate of frames which are sent over the link and are calculated from the HDLC frame size and the bandwidth.

Transfer delay – The transfer delay is the amount of time it takes for IP packets to travel a set path through the network.

HDLC bandwidth – This corresponds with the user set bandwidth of the link. The allowable bandwidth depends on the interface used and the container size chosen.

HDLC utilization – This is a percentage measure of how much of the link is actually in use.These parameters are usually measured by the following applications:

- Transparency testing
- Connectivity testing and
- Performance testing

Check for PoS Transparency

This measurement is mainly performed by carriers and fiber installers. It is needed to qualify the line for data transport, thereby guaranteeing that the transmission between two points (A and B) does not exhibit any errors. A typical setup is illustrated in figure 25.

It is also possible to send and receive using the same instrument (see Figure 25, dotted line) so that a specific line segment can be tested for transparency.

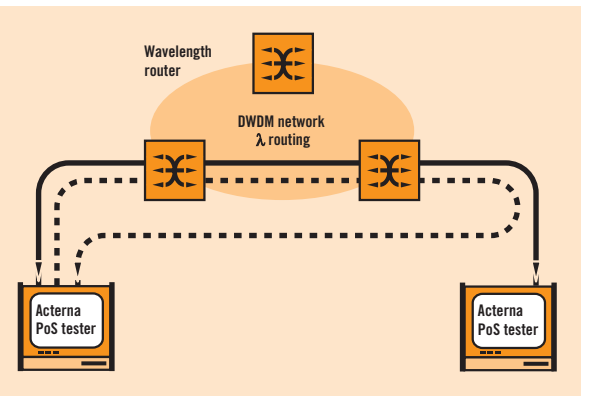


figure 25 *Typical setup for a transparency check*

To guarantee the proper setup of the transmission line, the measuring equipment sends HCLC/PPP/IP frames and receives them again when the transmitter and the receiver are looped back to each other.

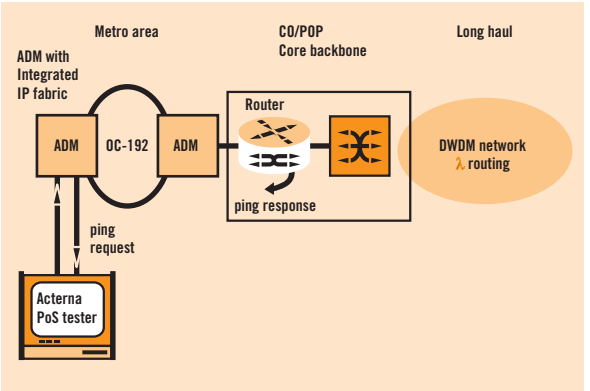
The parameters which can change are the frame size (in bytes) and the bandwidth of the transmission. It is also possible to introduce errors and check the resulting degradations on the receiver. The result of this measurement provides the following parameters: frame error, frame rate, transfer delay, link bandwidth and link utilization.

Verify IP Connectivity of new Network Elements

Usually, this test is performed when a new NE or a new user is connected to the network. It checks whether the NE or user is properly connected to the network and if it is able to communicate. A typical test setup is shown in figure 26.

The test equipment sends out a “ping” and waits for the response.
Thus measuring the round trip delay of the “ping”.
The “ping” parameter provides definite information about the state of connection of the NE and the time delay indicates if the line to and from the NE is OK. The customer benefits by receiving information about the connection of a new NE.

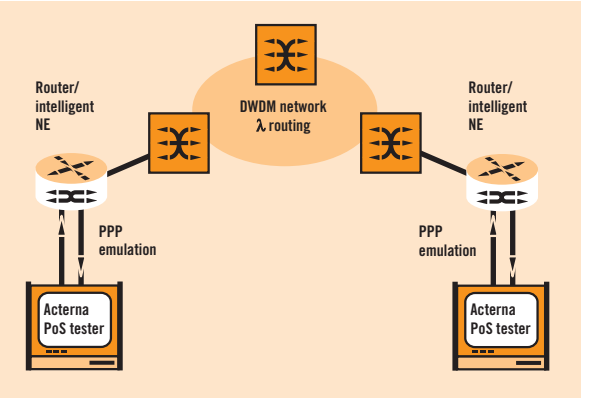
figure 26 *Typical measurement arrangement to check connectivity of NE*



Check of PoS Performance

This is a test of particular Network Elements and the entire network under load and checks the interfaces of Network Elements.
Figure 27 illustrates a typical arrangement for such a measurement test.

figure 27 *Measurement arrangement to check performance of PoS Network Elements*



This test is performed when the customer is connected to the network or when new connections between NEs are installed. The measuring instrument sends a signal and checks if the NE is connected and can pass the signals through to the next network element. To perform the PoS performance test, the equipment must be capable of performing the entire PPP emulation. This measurement delivers the same parameters as the transparency check.

Summary of applications

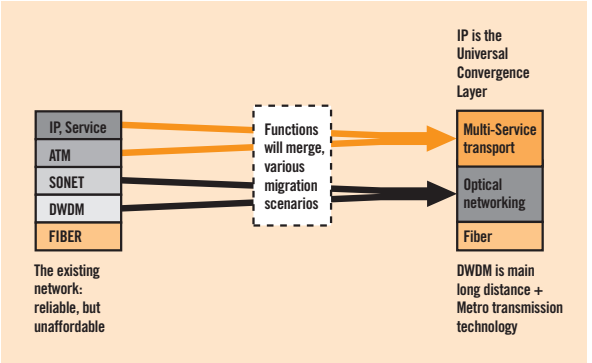
	Challenge	Solution	Parameters
PoS Transparency	Is the line between two users properly setup and transparent for IP traffic?	Send IP traffic and check the return traffic.	Frame error, frame rate etc.
Connectivity	Is a NE or user properly connected to the network?	Send ping request and wait for answers from NE or user. A full PPP emulation is required.	Ping and delay time.
PoS Performance	How does the system behave under stress?	Perform test under load with full PPP emulation.	Frame error, frame rate etc.

table 8 *Summary of possible applications for PoS systems*

Outlook

Future networks will need to cope with the ever-increasing bandwidth requirements mentioned in the introduction of this booklet.
TDM transmission rates are increasing to 40 Gbit/s while simultaneously the number of channels in DWDM systems are increasing to 128 and more. Total capacity rates of approximately 320 Gbit/s, 1 Tbit/s and higher are therefore quite possible. This challenge will be met by some of the technologies described in the following pages.
When discussing possible future networks the expression **converging networks** is often used.

figure 28 *Possible convergence scenario in the telecommunication world*



Converging networks lead to a decrease in the number of network elements and potentially less trouble for network operators. One platform used in this process is the so called Multi-Service Provision Platform. In addition, techniques like Multi-Protocol Label Switching and Multi-Protocol λ Switching will help to establish this trend. Figure 28 illustrates the possible convergence of functions with various layers.

Multi-Service Provisioning Platform (MSPP)

Since the majority of new telecommunication services are data-oriented, the transmission on these networks should be "data optimized". This is achieved with Multi-Service Provisioning Platforms (MSPP) which allow for the aggregation and switching of data packets by one network element. MSPPs can switch voice and video as well as different types of data traffic. The following three main features are necessary to perform the above tasks:

- Use DWDM technology to increase capacity of fibers
- Use of SONET/SDH to ensure QoS for time sensitive applications
- Use of layer 2 and layer 3 data intelligence (switches and routers) thus allowing products to switch and route data traffic

Combining these features into one instrument enables service providers to simplify their networks. Instead of installing a DWDM multiplexer, ADM and an IP router, just one device can be used. The number of devices and potential problems are reduced as a result.

Multi-Protocol Label Switching and Multi-Protocol λ Switching (MPLS and MPλS)

Multi-Protocol Label Switching (MPLS) is a high performance method of forwarding packets through a network. It is used by routers at the edge of the network to apply simple labels (or identifiers) to packets. These labels allow routers to switch packets according to their label with a minimal lookup overhead.
MPLS integrates the performance and traffic management capabilities of layer 2 with the scalability and flexibility of layer 3.
The label summarizes essential information about routing the packet including:

- Destination of packet
- Precedence of packet
- QoS information
- The route for the packet, as chosen by Traffic Engineering (TE)

At each router throughout the network, only the label of the incoming packet need be examined in order for it to be sent on to the next router across the network.
Advantages of this are that only one table lookup list from a fixed length label is required and switching and routing functions can be combined.

As with a router, an Optical Cross Connect (OXC), can intelligently route a wavelength through an OXC. The so called Multi-Protocol λSwitching signaling allows an OXC to convey a signal to the next OXC.
These devices exhibit similar advantages to the MPLS, by reducing the number of elements and potential problems in the network.

Appendix

IP version 6 (IPv6)

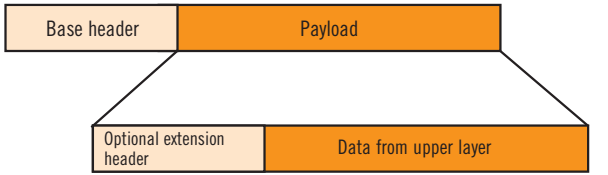
With the increasing number of Internet users, the pool of available addresses defined by IPv4 is decreasing fast. IP version 6 (IPv6) is addressing this and several other issues such as:
Quality of Service (QoS). The header is simpler and more flexible than for IPv4 due to the optional extension header. IP version 6 has already been standardized and test trials are running. It is still not widely used yet despite the fact that many large routers have already implemented IPv6. IPv6 is 128 bits long and consists of 16 bytes (octets). The protocol specifies hexadecimal colon notation. Whereby 128 bits are divided into eight sections, each of which are two bytes in length. An example of a principal IPv6 address appears in figure 29.

figure 29 *Possible IP address with IPv6*

FEEA:7648:CD33:9854:7654:FEDC:CE3E:0020

As with IPv4, the IP datagram for IPv6 consists of a mandatory base header followed by the payload. The payload consists of two parts an optional extension header and data from an upper layer (see figure 30).

figure 30 *IP header for IPv6*



Changes in the way IP header options are encoded enable more efficient forwarding, less stringent limits on the length of options and greater flexibility in introducing new options.
A new capability has been added to facilitate the labeling of packets belonging to a particular traffic “flow” for which the sender must request special handling. The simpler header offers faster processing by routers.

Terminology

The following definitions are taken from RFC recommendations.

Frame – The unit of transmission at the data link layer. A frame may include a header and/or a trailer, along with some number of units of data.

Packets – The basic unit of encapsulation, which is passed across the interface between the network layer and the data link layer. A packet is usually mapped to a frame; the exceptions are when data link layer fragmentation is being performed, or when multiple packets are incorporated into a single frame.

Datagram – The unit of transmission in the network layer (such as IP). A datagram may be encapsulated in one or more packets passed to the data link layer.

Peer – The other end of the point-to-point link.

Silently discarded – The implementation discards the packet without further processing. The implementation should provide the capability of logging the error, including the contents of the silently discarded packet, and should record the event in a statistics counter.

Abbreviations

A

ADM Add-Drop Multiplexer
ARPA Advanced Research Project Agency
ATM Asynchronous Transfer Mode

C

CHAP Challenge Handshake Authentication Protocol
CLEC Competitive Local Exchange Carrier

D

DCE Data Circuit-terminating Equipment
DNS Domain Name System
DTE Data Terminating Equipment
DWDM Dense Wavelength Division Multiplexing

F

FCS Frame Check Sequence
FTP File Transfer Protocol

H

HDLC High-Level Data Link Control
HTTP Hyper Text Transfer Protocol

I
ICMP Internet Control Message Protocol
IP Internetwork Protocol

L
LCP Link Control Protocol
LQM Link Quality Monitoring

M
MPLS Multi-Protocol Label Switching
MPλS Multi-Protocol λ Switching
MSPP Multi-Service Provisioning Platform

N
NCP Network Control Protocol
NE Network Element

O
OSI Open System Interconnection
OXC Optical Cross Connect

P
PAP Password Authentication Protocol
PDH Plesiochronous Digital Hierarchy
PoS Packet over Sonet/SDH
PPP Point-to-Point Protocol

R
RFC 'Request for Comment' documents, used to develop standards, procedures and specifications for TCP/IP, under the control of IETF

S
SDH Synchronous Digital Hierarchy
SONET Synchronous Optical Network
SMTP Simple Mail Transfer Protocol
SNMP Simple Network Management Protocol

T
TCP Transfer Control Protocol
TDM Time Division Multiplexing
TE Traffic Engineering
ToS Type of Service

U

UDP User Datagram Protocol

W

WDM Wavelength Division Multiplexing

References

RFC 1662	PPP in HDLC-like Framing
RFC 2615	PPP over SONET/SDH
RFC 1661	Point-to-Point Protocol (PPP)
RFC 950	Internet Standard Subnetting Procedure
RFC 821	Simple Mail Transfer Protocol
RFC 959	File Transfer Protocol (FTP)
RFC 854	Telnet Protocol Specification
RFC 1945	Hypertext Transfer Protocol - HTTP/1.0
RFC 1157	Simple Network Management Protocol (SNMP)
RFC 2929	Domain Name System (DNS) IANA Considerations
RFC 1332	PPP Internet Protocol Control Protocol (IPCP)
RFC 1333	PPP Link Quality Monitoring
RFC 2153	PPP Vendor Extensions
RFC 791	Internet Protocol
RFC 792	Internet Control Message Protocol
RFC 793	Transmission Control Protocol
G.707	Network Node Interface for the synchronous digital hierarchy (SDH)
GR.253	SONET Transport system: Common Generic Criteria