



SIN 389

Issue 1.3
June 2010

Suppliers' Information Note

For The BT Network

BT SurfPort and SurfPort24 Service Description

Each SIN is the copyright of British Telecommunications plc. Reproduction of the SIN is permitted only in its entirety, to disseminate information on the BT Network within your organisation. You must not edit or amend any SIN or reproduce extracts. You must not remove BT trademarks, notices, headings or copyright markings.

This document does not form a part of any contract with BT customers or suppliers.

Users of this document should not rely solely on the information in this document, but should carry out their own tests to satisfy themselves that terminal equipment will work with the BT network.

BT reserves the right to amend or replace any or all of the information in this document.

BT shall have no liability in contract, tort or otherwise for any loss or damage, howsoever arising from use of, or reliance upon, the information in this document by any person.

Due to technological limitations a very small percentage of customer interfaces may not comply with some of the individual characteristics which may be defined in this document.

Publication of this Suppliers' Information Note does not give or imply any licence to any intellectual property rights belonging to British Telecommunications plc or others. It is your sole responsibility to obtain any licences, permissions or consents which may be necessary if you choose to act on the information supplied in the SIN.

Those BT services marked ® indicates it is a registered trademark of British Telecommunications plc.

Those BT services marked ™ indicates it is a trademark of British Telecommunications plc.

This SIN is available in Portable Document Format (pdf) from: <http://www.sinet.bt.com/index.htm>

Enquiries relating to this document should be directed to: help@sinet.bt.com

CONTENTS

1	INTRODUCTION	3
1.1	DEFINITIONS.....	3
1.2	PRODUCT OUTLINE	3
1.2.1	<i>Standard IP</i>	3
1.2.2	<i>L2TP Passthrough</i>	5
2	TECHNICAL SPECIFICATION FOR END USER INTERFACE	6
3	TECHNICAL SPECIFICATION FOR CUSTOMER INTERFACE	10
3.1	PHYSICAL LAYER (STANDARD IP AND L2TP PASSTROUGH)	10
3.2	IP LAYER (STANDARD IP AND L2TP PASSTROUGH)	13
3.3	USER IP LAYER (STANDARD IP ONLY)	13
3.4	L2TP LAYER (L2TP PASSTROUGH ONLY).....	14
3.5	RADIUS PROTOCOL.....	14
3.5.1	<i>Standard IP</i>	16
3.5.2	<i>L2TP Passthrough</i>	20
3.6	NETWORK TERMINATING EQUIPMENT (NTE)	23
4	FURTHER INFORMATION CONTACT POINTS	23
5	IMPLEMENTATION OF RFC2661	23
6	REFERENCES	24
7	ACRONYMS	25
8	HISTORY	27
	Figure 1 Basic architecture of the SurfPort / SurfPort24 “Standard IP” option	4
	Figure 3 Basic architecture of the SurfPort / SurfPort24 “L2TP Passthrough” option.	5
	Table 1 Analogue Interface presentation (Standard IP and L2TP passthrough)	7
	Table 2 ISDN Interface presentation (Standard IP and L2TP passthrough)	7
	Table 3 PPP & IP RFCs (Standard IP)	8
	Table 4 PPP RFCs (L2TP Passthrough)	8
	Table 5 Fast Ethernet presentation.....	10
	Table 6 Gigabit Ethernet Presentation	11
	Table 7 Packet over SONET/Fibre Presentation (STM-1/4)	11
	Table 8 Packet over SONET default configuration	12
	Table 9 IP over ATM/Fibre Presentation (STM-1/4)	12
	Table 10 RADIUS packet types.....	15
	Table 11 Configurable RADIUS Client Parameters	16
	Table 12 Standard IP Access-Request Attributes	17
	Table 13 Standard IP Access-Accept Attributes.....	18
	Table 14 Standard IP Accounting-Request Attributes	19
	Table 15 L2TP Access-Request Attributes.....	20
	Table 16 L2TP Access-Accept Attributes	21
	Table 17 L2TP Accounting-Request Attributes.....	22

Note: This product was Withdrawn From New Supply in April 2009. It is no longer available for new customers

1. INTRODUCTION

This Suppliers' Information Note (SIN) describes the characteristics of the BT SurfPort and SurfPort24 products.

1.1 Definitions

Customer - The Providers of Electronic Communications Services (PECS) or Corporate Customer (CC) who purchases a BT Dial IP product from BT and sells or provides it to “End Users”.

End User - The person using their CPE (Customer Premises Equipment), to connect to a PECS/CC's IP network via the BT Dial IP product.

L2TP Tunnel Concentrator - Where a L2TP Tunnel Switch is used to concentrate, or reduce the number of tunnels presented.

L2TP Passthrough – Passing through the L2TP tunnels to the “Customer”.

For further definitions please refer to RFC2661^[10].

Formatted: Check grammar, Superscript

Deleted: ¹⁰

1.2 Product Outline

The BT SurfPort and SurfPort24 products are available in two main technical variants, ‘standard’ IP and L2TP passthrough. These are outlined in 1.2.1 and 1.2.2. A single delivery of the SurfPort / SurfPort24 product may include both variants on a common IP infrastructure.

1.2.1 Standard IP

The service handles end user originated dial-in sessions, terminating the PPP layer originating from the End User client and routes the user IP traffic to the Customer's network as shown in the architecture diagram, Figure 1.

This option includes a resilient connection between the Customer's premises and BT's high speed data network which hosts a number of routers, allocated to the Customer for any instance of the product.

The Customer Allocated Routers' main function is to de-couple, at the IP level, any given SurfPort / SurfPort24 product from the rest of the BT IP network, creating a virtual private IP network for each SurfPort / SurfPort24 instance.

The Customer Allocated Routers' provides a RADIUS interface allowing the Customer to accept or reject any given user's session request.

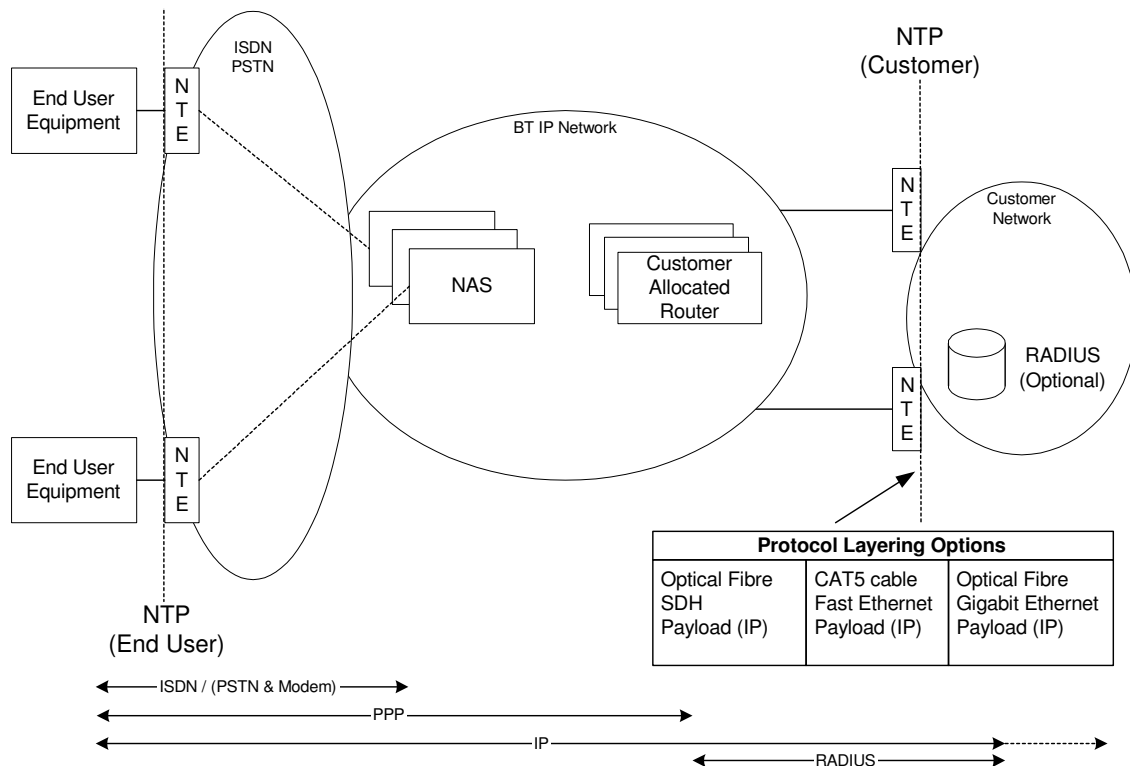


Figure 1 Basic architecture of the SurfPort / SurfPort24 “Standard IP” option

The “Customer” must provide the following information to BT in order for the service to function:

- IP addresses for either the LAN I/F on the Customer’s premises or sub-nets for the WAN I/Fs where SDH is used.
- A single host IP address for each of BT’s “Customer Allocated Routers” used to source the RADIUS packets.
- RADIUS host IP addresses, Authentication and Accounting server UDP ports and RADIUS shared secrets.
- IP addresses of Primary and Secondary DNS servers to be forwarded to dial-in users if required.
- The range of IP addresses to be allocated to dial-in users, which may be public or to RFC1918^[6].
- The preferred PPP authentication protocol or protocols.

IP routing information needs to be exchanged between BT and the Customer about the Customer Allocated Routers, the Customer RADIUS and networks. This can be provided using one of the dynamic routing protocols offered as part of the product, or pre-provisioned statically on BT’s equipment. If a dynamic routing protocol is used, BT will advertise only the IP addresses that the Customer equipment needs, via this protocol. In this case, the range of IP addresses assigned to dial-in users will be advertised permanently, regardless of the state of any individual connection.

Formatted: Super

Deleted: 6

Customers may opt not to use RADIUS and use instead a single username and password configured on the Customer Allocated Routers. This will restrict the availability of many of the SurfPort / SurfPort24 features, since these generally depend on parameters returned via RADIUS.

1.2.2 L2TP Passthrough

The BT SurfPort / SurfPort24 L2TP Passthrough option allows the Customer to have direct access to their End Users' PPP sessions. End User PPP sessions are presented to the Customer in L2TP tunnels.

The L2TP Tunnel Concentrators main function is to de-couple the Customer RADIUS from the rest of the BT network and isolate the Customer interface from the complexity of the network. L2TP Tunnels between the L2TP Tunnel Concentrator and Customer's LNS are established dynamically on demand.

A RADIUS interface is provided between the Customer and L2TP Tunnel Concentrator to allow the Customer control, on a per End User session basis, of the Customer side L2TP tunnel end points.

Figure 2 shows the basic L2TP Passthrough service architecture as described above.

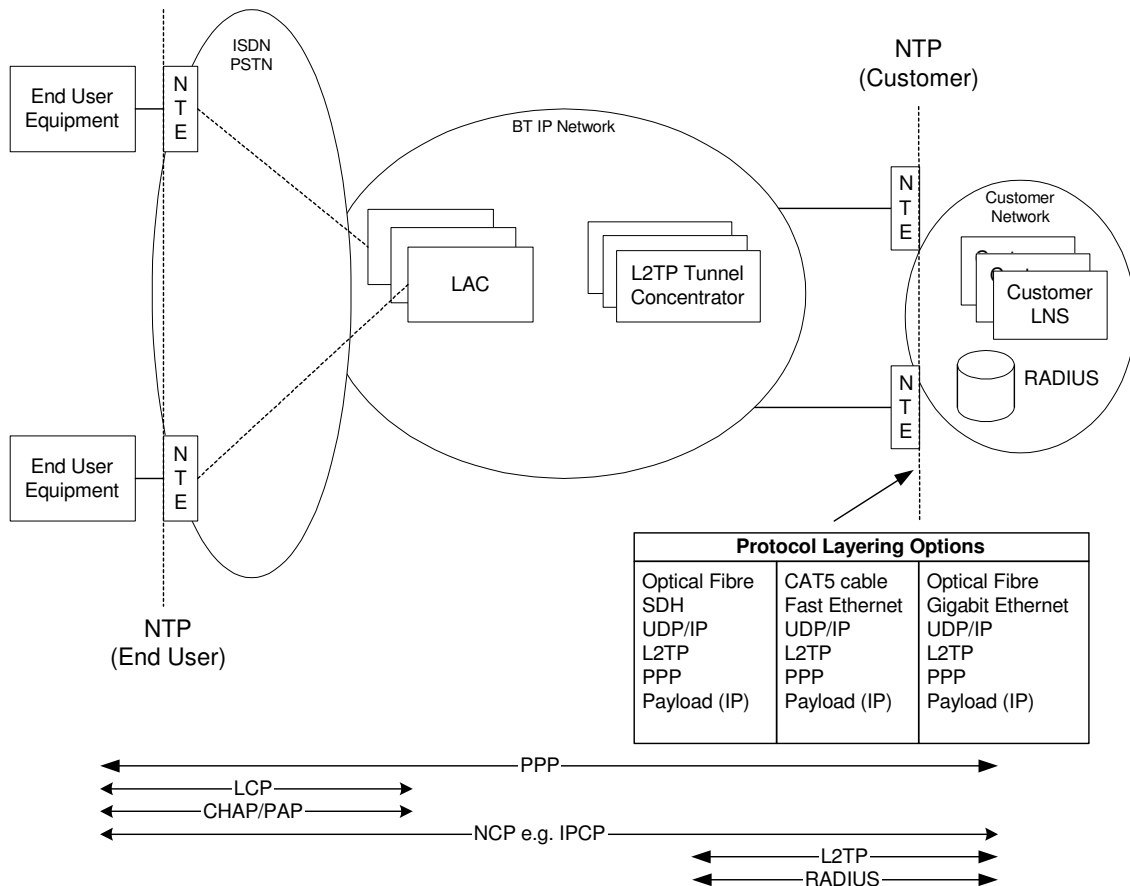


Figure 2 Basic architecture of the SurfPort / SurfPort24 "L2TP Passthrough" option.

The “Customer” must provide the following information to BT in order for the service to function:

- IP addresses for either the LAN I/F on the Customer’s premises or sub-nets for the WAN I/Fs where SDH is used.
- A single host IP address for each of BT’s “L2TP Tunnel Concentrators" used to source L2TP and RADIUS packets.
- RADIUS host IP addresses, Authentication and Accounting server UDP ports and RADIUS shared secrets.
- The preferred initial PPP authentication protocol or protocols.

IP routing information needs to be exchanged between BT and the Customer about the L2TP Tunnel Concentrators, the Customer RADIUS and LNS. This can be provided using one of the dynamic routing protocols offered as part of the product, or pre-provisioned statically on BT’s equipment. If a dynamic routing protocol is used, BT will advertise only the IP addresses that the Customer equipment needs, via this protocol.

2 TECHNICAL SPECIFICATION FOR END USER INTERFACE

The End User interface for both the 'standard' IP and L2TP passthrough is common at the physical level, i.e. a connection via ISDN or PSTN and Modem. PPP is used above this physical layer. In the case of the L2TP passthrough variant the specification of the higher layers above PPP is open to the Customer in addition to certain aspects of PPP itself. The Standard IP variant uses PPP to transport only IP.

Standards applicable to the PSTN & Modem interface for both variants are listed in Table 1.

SIN 350	BT Public Switched Telephone Network (PSTN): Network Tones and Announcements
SIN 351	BT Public Switched Telephone Network (PSTN): Technical Characteristics Of The Single Analogue Line Interface
SIN 352	BT Public Switched Telephone Network (PSTN): Technical Characteristics Of The Multi-Line Analogue Line Interface.
SIN 367	Characteristics of the BT Network: Electrical Safety and EMC
MNP5	Microcom Network Protocol 5. A data compression protocol for analogue modems
ITU-T V.21	300 bits per second duplex modem standardized for use in the general switched telephone network (11/88)
ITU-T V.22	1200 bits per second duplex modem standardized for use in the general switched telephone network and on point-to-point 2-wire leased telephone-type circuits (11/88)
ITU-T V.23	600/1200-baud modem standardized for use in the general switched telephone network (11/88)

ITU-T V.22bis	2400 bits per second duplex modem using the frequency division technique standardized for use on the general switched telephone network and on point-to-point 2-wire leased telephone-type circuits (11/88)
ITU-T V.32bis	A duplex modem operating at data signalling rates of up to 14 400 bit/s for use on the general switched telephone network and on leased point-to-point 2-wire telephone-type circuits (02/91)
ITU-T V.34	A modem operating at data signalling rates of up to 33 600 bit/s for use on the general switched telephone network and on leased point-to-point 2-wire telephone-type circuits (02/98)
ITU-T V.42	Error-correcting procedures for DCEs using asynchronous-to-synchronous conversion (10/96)
ITU-T V.42bis	Data compression procedures for data circuit-terminating equipment (DCE) using error correction procedures (01/90)
ITU-T V.90	A digital modem and analogue modem pair for use on the Public Switched Telephone Network (PSTN) at data signalling rates of up to 56 000 bit/s downstream and up to 33 600 bit/s upstream (09/98)

Table 1 Analogue Interface presentation (Standard IP and L2TP passthrough)

The corresponding standards for ISDN connections are contained in Table 2

SIN 171	ISDN 2 Service (I.420) - Description
SIN 232	BT ISDN 30 (I.421) Service - Service Description
SIN 261	BT ISDN 2e and ISDN 30e (ISDN30 (I.421) using full ETSI Call Control - Service Description
SIN 312	BT ISDN Services Overview
SIN 367	Characteristics of the BT Network: Electrical Safety and EMC
RFC 1618	PPP over ISDN
V.110	Support by an ISDN of data terminal equipment with V-Series type interfaces. (02/2000) (For a digital mobile network)

Table 2 ISDN Interface presentation (Standard IP and L2TP passthrough)

The IETF RFCs applicable to the PPP and IP layers of the SurfPort / SurfPort24 'standard' IP variant are contained in Table 3 below and the sub-set applicable to the L2TP passthrough variant in Table 4.

STD 5	IP Standard comprising:- RFC0791 Internet Protocol RFC0792 Internet Control Message Protocol RFC0919 Broadcasting Internet Datagrams RFC0922 Broadcasting Internet Datagrams in the presence of Subnets RFC0950 Internet Standard Subnetting Procedure RFC1112 Host Extensions for IP Multicasting
STD 51	PPP Standard comprising:- RFC1661 The Point-to-Point Protocol (PPP) RFC1662 PPP in HDLC-like Framing
RFC 1332	The PPP Internet Protocol Control Protocol (IPCP)
RFC 1877	PPP IPCP Extensions (Primary and Secondary DNS address options only)
RFC 1990	The PPP Multilink Protocol (MP)
RFC 1994	PPP Challenge Handshake Authentication Protocol

Table 3 PPP & IP RFCs (Standard IP)

STD 51	PPP Standard comprising:- RFC1661 The Point-to-Point Protocol (PPP) RFC1662 PPP in HDLC-like Framing
RFC 1994	PPP Challenge Handshake Authentication Protocol

Table 4 PPP RFCs (L2TP Passthrough)

The BT NAS/LAC will request the following LCP options appropriate to a narrow-band PPP link for both 'standard' IP and L2TP passthrough variants:-

- PFC PPP Protocol Field Compression
- ACFC PPP Address and Control Field Compression
- ACCM Async Control Character Map: 0x000A0000
- CHAP Challenge Handshake Authentication Protocol OR
- PAP Password Authentication Protocol

Customers may choose one of two LCP authentication protocol negotiation strategies for each dialled number,

- CHAP followed by PAP
- PAP only

The more flexible CHAP option is preferred to PAP.

If the client is configured for MP^[2] an MRRU and End Point Discriminator may be negotiated. This capability will always be present for ISDN connections using RFC1618^[2].

Formatted: Check grammar, Superscript

Deleted: 7

Deleted: 2

Formatted: Superscript

If the capability for two channel MP is not ordered as part of the Customers service, where these parameters are negotiated with the client the 'standard' IP variant may implement the MP protocol but will only support a single link. Clients will be limited to a single link by configuration. Attempts to negotiate a 2nd link may appear successful to the client but in practice, it is unlikely that an MP 'bundle' interface will be established. In this case the performance of the service will be indeterminate.

If the capability for two channel MP is ordered as part of the Customers service, then where these parameters are negotiated with the client and both links are authenticated, then the 'standard' IP variant will implement the MP protocol and will bundle a maximum of two MP links into a single session. The bundle interface created for this session will use the client username, hence this username should be unique. Optionally an additional end point discriminator can be negotiated with the client CPE that can also be used to uniquely define this bundle. This session will be assigned a single IP address.

In the case of the L2TP Passthrough variant, MP frames are carried transparently by PPP.

After LCP negotiation completes the negotiated authentication protocol will commence. In the case of CHAP the hostname of the device issuing the challenge will be 'BTMDIP' for ISDN connections to RFC1618^[2]. In all other cases, the hostname is unspecified.

Deleted: 2

Formatted: Super

Once authenticated IPCP will commence with the 'standard' IP variant. With the L2TP variant there is no IP layer specified and consequently no IP related NCP is required. The End User PPP session will be available at the Customers LNS at this point and consequently the specification and implementation of these protocols is open to the Customer.

Although RFC2661^[10] provides the mechanisms to allow the LNS to arbitrarily re-negotiate LCP with the client, this mode of operation is not generally recommended. LCP re-negotiation will increase the connection time and some PPP clients may not reliably support LCP re-negotiation at all.

Deleted: 10

Formatted: Super

If the use of LCP re-negotiation is required, Customers should discuss the technical implications with a BT Technical Support Engineer prior to implementation.

The BT Dial IP L2TP passthrough service is primarily aimed at the transport of IP datagrams encapsulated by PPP, however PPP is capable of encapsulating other protocols and associated NCPs (Network Control Protocols). These aspects of the product are not defined in this document since their transport is transparent. The only PPP constraints are that LCP must be negotiated with the BT network and either CHAP or PAP must be used as an authentication protocol initially as described above. The authentication data will be captured by the BT LAC and forwarded as part of L2TP to the Customer.

The BT Dial IP L2TP passthrough variant will transport MP^[7] (Multilink Protocol) frames within the L2TP tunnels. The PPP LCP protocol is initiated between the End User client software and the BT network and as such some compromises, common to all PPP services that BT supports on its Dial IP platform, have to be made. Negotiation of MP is supported at this point on ISDN connections to RFC1618^[2].

Formatted: Check grammar, Superscript

Deleted: 7

The Customer LNS is the first point in the connection that individual MP links can be re-combined. BT will not attempt to re-combine any MP links before forwarding the PPP session to the Customer LNS.

Deleted: 2

Formatted: Super

The nature of the BT Dial IP service and its geographic distribution mean that there can be far more packet delay variation than would be seen in a simple point to point MP configuration, where variable delay in the ISDN/PSTN is the only consideration. Due to the scale of the BT

Dial IP network calls are quite likely to be terminated on different BT LACs. The IP based transport used to forward these packets from the BT LACs to the L2TP tunnel concentrators cannot therefore control the order MP frames will arrive at the Customer LNS. Typically, the differential packet delay for such a connection within the BT network for a 64 byte packet will be less than 200ms. (Note: In the case of analogue modems additional delay variation will be introduced as a result of the modulation, compression and error correction protocols used.)

3 TECHNICAL SPECIFICATION FOR CUSTOMER INTERFACE

The Customer interface is either End User IP or End User PPP over L2TP over UDP/IP.

The technical interface specifications for these options are described in the following sections as appropriate:

3.1 Physical Layer (Standard IP and L2TP Passthrough)

There are a number of options for the physical layer and IP encapsulation:-

- IP over Ethernet using 100BaseT
- IP over Ethernet using 1000BaseSX.
- IP encapsulated directly in SDH (i.e. Packet over SONET), delivered on single mode optical fibre at either STM-1 or STM-4 rates.

The Customer may opt for either a LAN or SDH WAN interface. The specific interface type deployed will depend on the aggregate bandwidth requirement for any given product instance.

LAN interfaces will require an IP address from the Customer's LAN sub-net for each interface. If HSRP is used one or two additional IP addresses in the same sub-net will be required.

RJ45	Fast Ethernet LAN physical connection
IEEE 802.3	IEEE standards for Local Area Networks: CSMA/CD Access Method.
STD 37	ARP: An Ethernet Address Resolution Protocol
STD 43	A standard for the transmission of IP Datagrams over IEEE 802 networks
STD 5	IP Standard comprising:- RFC0791 Internet Protocol RFC0792 Internet Control Message Protocol RFC0919 Broadcasting Internet Datagrams RFC0922 Broadcasting Internet Datagrams in the presence of Subnets RFC0950 Internet Standard Subnetting Procedure RFC1112 Host Extensions for IP Multicasting

Table 5 Fast Ethernet presentation

SIN 360	Gigabit Ethernet for the BT Network – Interface Characteristics
IEEE 802.3z	Gigabit Ethernet Standard (1000BaseSX multimode)
RFC 1042	A standard for the transmission of IP Datagrams over IEEE 802 networks
STD 37	ARP: An Ethernet Address Resolution Protocol
STD 5	IP Standard comprising:- RFC0791 Internet Protocol RFC0792 Internet Control Message Protocol RFC0919 Broadcasting Internet Datagrams RFC0922 Broadcasting Internet Datagrams in the presence of Subnets RFC0950 Internet Standard Subnetting Procedure RFC1112 Host Extensions for IP Multicasting

Table 6 Gigabit Ethernet Presentation

SIN 289	"BT MegaStream 155 and BT MegaStream Aggregate Service Description" (MegaStream155 section – optical only) Certain aspects apply: <ul style="list-style-type: none"> • ITU-T G.957 – Optical Interfaces for Equipment's and Systems relating to the Synchronous Digital Hierarchy – 1995 • BS EN 60825-1 Safety of Laser Products Part 1 Equipment Classification – 1995 • BS EN 60825-2 Safety of Laser Products Part 2 Safety of Optical Fibre Communications Systems – 1995 • BS EN 1186110 Sectional Specification. Connector sets for optical fibre and cables type FC – 1994
SIN 333	SDH Customer Interfaces at the STM-N level (where N=1,4,16) Interface Characteristics – certain aspects only
SIN 337	BT MegaStream 622 and BT MegaStream Aggregate (STM-4) Service Description – certain aspects only
STD 5	IP Standard comprising:- RFC0791 Internet Protocol RFC0792 Internet Control Message Protocol RFC0919 Broadcasting Internet Datagrams RFC0922 Broadcasting Internet Datagrams in the presence of Subnets RFC0950 Internet Standard Subnetting Procedure RFC1112 Host Extensions for IP Multicasting
RFC 2615	PPP over SONET/SDH, A Malis, June 1999

Table 7 Packet over SONET/Fibre Presentation (STM-1/4)

POS interfaces are numbered using a /30 sub-net with IP addresses supplied by the Customer. These can be public or to RFC 1918^[6].

Formatted: Super
Deleted: 6

The following default configuration is configured on the BT POS interfaces.

Parameter	BT Default
Maximum Transmission Unit	4470 bytes
SDH overhead bits	c2 = 0xcf (PPP or HDLC) j0 = 0xcc (SDH default) s1s0 = 2 (SDH)
Scrambling	Enabled as RFC2615
Cyclic Redundancy Check	32 bit
Clock	External (Network supplied).

Table 8 Packet over SONET default configuration

The option of IP encapsulated in ATM over SDH, delivered on single mode optical fibre at either STM-1 or STM-4 rates described in Table 9 below is not available for new sales. This is superseded by the generally more bandwidth efficient POS interface option.

SIN 289	"BT MegaStream 155 and BT MegaStream Aggregate Service Description" (MegaStream155 section – optical only) Certain aspects apply: <ul style="list-style-type: none"> • ITU-T G.957 – Optical Interfaces for Equipment's and Systems relating to the Synchronous Digital Hierarchy – 1995 • BS EN 60825-1 Safety of Laser Products Part 1 Equipment Classification – 1995 • BS EN 60825-2 Safety of Laser Products Part 2 Safety of Optical Fibre Communications Systems – 1995 • BS EN 1186110 Sectional Specification. Connector sets for optical fibre and cables type FC – 1994
SIN 333	SDH Customer Interfaces at the STM-N level (where N=1,4,16) Interface Characteristics – certain aspects only
SIN 337	BT MegaStream 622 and BT MegaStream Aggregate (STM-4) Service Description – certain aspects only
STD 5	IP Standard comprising:- <ul style="list-style-type: none"> RFC0791 Internet Protocol RFC0792 Internet Control Message Protocol RFC0919 Broadcasting Internet Datagrams RFC0922 Broadcasting Internet Datagrams in the presence of Subnets RFC0950 Internet Standard Subnetting Procedure RFC1112 Host Extensions for IP Multicasting
RFC 2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5 (Note 1)

Table 9 IP over ATM/Fibre Presentation (STM-1/4)

Note 1: Only IP encapsulation is required therefore the VC multiplexing option is used. (i.e. there is no LLC field).

A single ATM VC is configured on each link. The VPI/VCI of the VC is by default VP=16, VCI = 32. The Customer may nominate any valid alternatives. At the IP level each VC is numbered using a /30 sub-net with IP addresses supplied by the Customer. These can be public or to RFC 1918^[6].

The ATM VC Service Class is VBR-nrt (Variable Bit Rate - non real-time) with the peak and sustained cell rates set to the line rate of 155000k bit/s.

3.2 IP Layer (Standard IP and L2TP Passthrough)

This layer must conform to RFC 791^[1]. Source routing is not supported.

Two connections between the Customer and the BT network are provided. There are a number of routing protocol options for managing this resilience:-

- Static routes
- RIP version 2 as RFC 1723^[4]
- BGP version 4 as RFC 1771^[5] and RFC 2796^[11]

Since the connection between BT and the Customer is a reliable stable network, with very few sub-nets to be advertised in either direction, RIP version 2 is preferred.

When static routes are used with either of the LAN interface options, where both interfaces terminate on the same LAN, BT can provide some additional resilience using HSRP to RFC 2281^[9] (Cisco Hot Standby Router Protocol). This requires the Customer to allocate either one or two additional virtual IP addresses on the LAN and transport the Ethernet encapsulated HSRP protocol messages between the two BT NTEs on that LAN. There is no need for any Customer equipment to implement any other aspects of this protocol. It should be noted however that there are still some failure modes using this approach which can be avoided by not terminating both interfaces on the same equipment and using a dynamic routing protocol.

The network comprising the BT-provided and maintained routers and any other support infrastructure used to provide connectivity up to the NTP on the Customer's premises is effectively a VPN (Virtual Private Network) using a combination of RFC1918^[6] addresses and public IP addresses supplied by the Customer as they so require. For this reason the iBGP form of BGP is the most appropriate. In the event that the Customer network consists of a number of BGP speakers, BT would not expect to participate in a full mesh of these and only peer with route reflectors as RFC 2796^[11].

3.3 User IP Layer (Standard IP only)

A number of Customer Allocated Routers are dedicated to each SurfPort / SurfPort24 instance. End User sessions at the IP layer are logically directly connected to these routers.

The set of IP addresses from which End User IP addresses are assigned is provided by the Customer and may be public or to RFC1918^[6]. This set of IP addresses is summarised and advertised permanently, regardless of the state of any individual End User connection.

There are three methods of assigning an IP address to an End User available from this set,

Deleted: 6

Formatted: Super

Deleted: 1

Formatted: Check grammar, Supersc

Formatted: Check grammar, Supersc

Deleted: 4

Deleted: 5

Formatted: Check grammar, Supersc

Deleted: 11

Formatted: Check grammar, Supersc

Formatted: Check grammar, Supersc

Deleted: 9

Formatted: Check grammar, Supersc

Deleted: 6

Deleted: 11

Formatted: Check grammar, Supersc

Formatted: Super

Deleted: 6

- Dynamic** The IP address is assigned from a pool of IP addresses configured on the Customer Allocated Router terminating the session. A given End User session may generally terminate on any of the Customer Allocated Routers. This supports the PPP MP Standard IP service offering.
- Static** The IP address pre-configured on the End User CPE is used. All calls from this End User must terminate on the same Customer Allocated Router. This requires a separate telephone number for each Customer Allocated Router so configured, when more than two such routers are required to deliver the service.
- Leased** The IP address is assigned by the Customer RADIUS. If the same IP address is always used for this user the same restrictions apply as the static case above. Alternatively the Customer RADIUS can maintain a pool of IP addresses for each router using the RADIUS NAS-IP-Address attribute to determine the router making the request. BT must be notified of the IP address ranges of these remote pools to correctly configure the IP routing within the VPN.

In addition, the Customer may use RADIUS to inject a route to a sub-net via the IP address assigned to the End User. In this case, since the sub-net address is not dynamic the same restrictions as the static case above apply.

BT will provide sufficient Customer Allocated Routers to support the number of SurfPort / SurfPort24 ports ordered, with an additional margin for resilience. This resilient capacity is usable only with dynamic IP address assignment when more than two Customer Allocated Routers are required.

3.4 L2TP Layer (L2TP Passthrough only)

The L2TP Tunnel Concentrators can deliver dynamic L2TP tunnels to an unrestricted number of end points in the Customer's network. The end points are defined by the Customer in the RADIUS Access-Accept in response to a RADIUS Access-Request. The Customer's equipment terminating the L2TP tunnels, either one or more LNSs or the Customer's own L2TP Tunnel Concentrators, must conform to RFC 2661^[10].

A maximum concurrent session count will be enforced across all the tunnels leaving any one BT L2TP Tunnel Concentrator in order to limit the load of any one concentrator. BT will provide sufficient L2TP Tunnel Concentrators for any given service instance to meet the number of ports ordered and arrange for a reasonably uniform distribution of traffic across these. As the technology improves it is anticipated that the number of sessions supported by a single L2TP Tunnel Concentrator will increase.

L2TP packets are encapsulated in UDP/IP. The use of UDP header checksums on L2TP data channel packets is not recommended. The BT L2TP Concentrators will use UDP header checksums only on L2TP control channel packets.

A default retry timer of 1 second is used. Sequence numbers are not used by default on the L2TP data channel.

3.5 RADIUS protocol

RADIUS is key to successful operation of this product.

There are two services provided by RADIUS, authentication and accounting. Authentication is essential for the normal operation of this product. The use of RADIUS accounting is optional.

Formatted: Check grammar, Superscript

Deleted: 10

The BT platform supports the following RADIUS packet types:-

ID	Packet Type
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response

Table 10 RADIUS packet types

RADIUS interoperation requires a shared secret to be configured on the Customer's RADIUS servers associated with each router, acting as a RADIUS client. The RADIUS server knows the client by its IP address, in this case a logical IP address configured on each Customer Allocated Router or L2TP Tunnel Concentrator that will source RADIUS packets. This can be either a public IP address or one from a sub-net identified in RFC1918^[6].

If the RADIUS client does not receive a response within a configurable period, it will re-try. If no response is received after a configurable number of retries and the Customer has nominated a back-up RADIUS server, this will be tried. If this is successful, all future requests will be sent to that server for a dead-time period, by default 10 minutes. After this period, the next request will be sent to the primary server.

If no response is received from the back-up RADIUS server, the End User's PPP session will not authenticate and the associated incoming ISDN/PSTN call is disconnected as a result. This should not be used as a mechanism for denying access.

A RADIUS server should always respond to a request from a valid RADIUS client. A silent discard is not appropriate, as the platform will attempt a retry. The only occasion where a silent discard is warranted is where the authenticator fails to match. Otherwise a response should always be made to prevent the RADIUS client from re-transmitting. In the case of an Access-Request the response should be Access-Reject whilst for an Accounting-Request the response should be Accounting-Response.

If an Access-Reject is returned, the End User session is terminated. No accounting data will be generated. No Access-Reject attributes are supported.

The RADIUS client parameters required by the above are contained in Table 11.

Formatted: Check grammar, Superscript

Deleted: 6

Parameter	Default Value	Comment
Primary RADIUS authentication server IP address	none	Required for L2TP Passthrough - Customer supplied Optional for Standard IP.
Secondary RADIUS authentication server IP address	none	Optional
Primary RADIUS accounting server IP address	As authentication server	Optional
Secondary RADIUS accounting server IP address	As authentication server	Optional
RADIUS authentication UDP port	1645	Any port in the range 1 – 65535. Only required if RADIUS authentication used.
RADIUS accounting UDP port	1646	Any port in the range 1 - 65535. Only required if RADIUS accounting used.
Shared Secret	Customer supplied	Random 1- 16 characters. A 16-character secret is recommended.
Retry timer	5 seconds	Customer defined, not less than one second, in whole seconds. Only relevant if a secondary RADIUS is defined.
Retry count	3	Customer defined - in whole number of retries. Value can be zero for no retries.
Dead time	10 minutes	Customer defined. Value in whole minutes, not less than 1 min.
Interim accounting period	none	Customer defined, not less than 10 minutes, in whole minutes. Only relevant if interim accounting is required.

Table 11 Configurable RADIUS Client Parameters

There are differences in the use of RADIUS attribute value pairs between the Standard IP and L2TP Passthrough options, the details of each are described in separate sections that follow.

3.5.1 Standard IP

The BT SurfPort and SurfPort24 products support a number of attributes for authentication and accounting according to RFC2865^[12] and RFC2866^[13]. Returning attributes other than those described in Table 12 may cause unexpected operation.

Deleted: ¹²

Deleted: ¹³

Formatted: Super

Formatted: Super

No	Attribute	Value	Comment
1	User-Name	CHAP/PAP username	As entered by End User
2	User-Password	user's PAP password	As entered by End User and hidden as RFC2865 (Note 2)
3	CHAP-Password	user's CHAP password	MD5 encrypted password (Note 3)
4	NAS-IP-Address	Customer Allocated Router - logical source address	
5	NAS-Port	Customer Allocated Router - logical port	
6	Service-Type	(2) Framed	
7	Framed-Protocol	(1) PPP	
30	Called-Station-Id	DNIS	Full dialled number less leading zero
31	Calling-Station-Id	End User's CLI	Presentation CLI with no leading zero. End Users may withhold their CLI in which case this attribute will not be present.
61	NAS-Port-Type	(0) Async (2) ISDN Sync (4) ISDN Async V.110	Port Type (Note 4)

Table 12 Standard IP Access-Request Attributes

Note 2: The End-User may negotiate either PAP or CHAP as an authentication protocol. If PAP is negotiated this attribute will be present.

Note 3: The End-User may negotiate either PAP or CHAP as an authentication protocol. If CHAP is negotiated this attribute will be present. The option specified in RFC2865^[12] where the CHAP challenge is a 16 bit value is used. i.e. the Access-Request authenticator contains the CHAP challenge and the CHAP-Password attribute contains the CHAP identity and response string.

Note 4: This attribute indicates the type of the physical port of the NAS. For the two channel MP Standard IP service, End Users that attempt to connect with a value of Async (0) should be rejected. Additionally if the two channel MP Standard IP service is being used NAS-Port-Type is indeterminate for the second channel connected and a value of Virtual (5) may be sent.

The range of Access-Accept attributes supported is shown in Table 13. These attributes are necessary for the product to work unless shown as optional in the comment column.

Formatted: Check grammar, Superscript

Deleted: ¹²

No	Attribute	Value	Comment
6	Service-Type	Framed	
7	Framed-Protocol	PPP	
8	Framed-IP-Address	0xFFFFFFFF	(Note 5)
11	Filter-Id	string	Optional (Note 6) (Note 7)
22	Framed-Route	string	Optional (Note 8)
25	Class	string	Optional
27	Session-Timeout	integer	Optional (Note 7)
28	Idle-Timeout	integer	Optional Note (Note 7) (Note 9)

Table 13 Standard IP Access-Accept Attributes

Note 5: The Framed-IP-Address value may also be either a specific IP address or 0xFFFFFFFF to allow the client to negotiate its pre-configured (static) IP address. In this case, there are restrictions requiring the mapping of any given dialled number to a specific Customer Allocated Router.

Note 6: Customers requiring the use of RADIUS attribute 11 will need to supply an agreed named filter beforehand. The format of the Filter-Id value is then 'filtername.in'

Note 7: It should be noted that MP supports RADIUS attributes on the bundled interface i.e. per IP address. Specifically RADIUS attributes returned for the first channel will be supported and anything returned for the second channel will be ignored. This applies to Filters and Session and Idle Timeouts.

Note 8: The Framed-Route Attribute is used to inject a route to a network available via the Framed-IP-Address. Similar restrictions apply to the use of this attribute as that for the Framed-IP-Address attribute above. In addition, BT will need to be informed of the super-net used to correctly configure the SurfPort24 internal routing protocol.

Note 9: A default Idle-Timeout of 20 minutes is applied. This will be replaced by the contents of the RADIUS Idle-Timeout value if used.

No	Attribute	Value	Comment
1	User-Name	username	
4	NAS-IP-Address	Tunnel Concentrator logical source address	
5	NAS-Port	Tunnel Concentrator logical port	
6	Service-Type	(2) Framed	
7	Framed-Protocol	(1) PPP	
8	Framed-IP-Address	integer IP address	IP Address assigned to end-user

No	Attribute	Value	Comment
25	Class	string	Present if returned in corresponding Access-Accept.
30	Called-Station-Id	DNIS	Full dialled number less leading zero
31	Calling-Station-Id	End User's CLI	Presentation CLI with no leading zero. End Users may withhold their CLI in which case this attribute will not be present.
40	Acct-Status-Type	(1) Start (2) Stop (3) Interim-Update	
41	Acct-Delay-Time	integer	Always zero unless RADIUS retries enabled. May not be present if value is zero.
42	<i>Acct-Input-Octets</i>	<i>integer</i>	
43	<i>Acct-Output-Octets</i>	<i>integer</i>	
44	Acct-Session-Id	unique string	
45	Acct-Authentic	RADIUS	
46	<i>Acct-Session-Time</i>	<i>integer</i>	
47	<i>Acct-Input-Packets</i>	<i>integer</i>	
48	<i>Acct-Output-Packets</i>	<i>integer</i>	
49	<i>Acct-Terminate-Cause</i>	<i>integer</i>	
50	Acct-Multi-Session-Id	string	Present if End-User negotiates MP
51	Acct-Link-Count	1	Present if End-User negotiates MP
61	NAS-Port-Type	(0) Async (2) ISDN Sync (4) ISDN Async V.110	(Note 4)

Table 14 Standard IP Accounting-Request Attributes

Attributes in Italics are only present in Stop or Interim update packets.

3.5.2 L2TP Passthrough

If the PPP session in the L2TP tunnel towards the Customer LNS is successfully established, an accounting start is sent. This does not indicate that the End User was necessarily successfully authenticated. When the End User's PPP session is terminated an accounting stop will be sent. The Customer may optional request interim updates.

An incoming session to an L2TP Tunnel Concentrator will trigger a RADIUS Access-Request using attributes shown in Table 15. The Customer's RADIUS server should respond with attributes from Table 16.

No	Attribute	Value	Comment
1	User-Name	CHAP/PAP username	As entered by End User
2	User-Password	user's PAP password	As entered by End User and hidden as RFC2865 (Note 10)
3	CHAP-Password	user's CHAP password	As captured by BT LAC. (Note 11)
4	NAS-IP-Address	Tunnel Concentrator logical source address	
5	NAS-Port	Tunnel Concentrator local logical port	
6	Service-Type	(2) Framed	
7	Framed-Protocol	(1) PPP	
30	Called-Station-Id	DNIS	Full dialled number less leading zero
31	Calling-Station-Id	End User's CLI	Presentation CLI with no leading zero. End Users may withhold their CLI in which case this attribute will not be present.
61	NAS-Port-Type	(0) Async (2) ISDN Sync (4) ISDN Async V.110	

Table 15 L2TP Access-Request Attributes

Note 10: The End-User may negotiate either PAP or CHAP as an authentication protocol. If PAP is negotiated, this attribute will be present.

Note 11: The End-User may negotiate either PAP or CHAP as an authentication protocol. If CHAP is negotiated, this attribute will be present. The option specified in RFC2865^[12] where the CHAP challenge is a 16 bit value is used. i.e. the Access-Request authenticator contains the CHAP challenge and the CHAP-Password attribute contains the CHAP identity and response string.

The range of Access-Accept attributes supported is shown in Table 16. These attributes are necessary for the product to work unless shown as optional in the comment column.

Formatted: Check grammar, Superscript

Deleted: ¹²

No	Attribute	Value	Comment
6	Service-Type	(2) Framed	Optional
7	Framed-Protocol	(1) PPP	Optional
25	Class	string	Optional
64	Tunnel-Type	(3) L2TP	
65	Tunnel-Medium-Type	(1) IPv4	
67	Tunnel-Server-Endpoint	LNS IP address	Note 12
69	Tunnel-Password	password	Note 13
82	Tunnel-Assignment-ID	string	Optional (Note 14)
83	Tunnel-Preference	integer	Optional (Note 15)
90	Tunnel-Client-Auth-ID	name	Optional (Note 16)

Table 16 L2TP Access-Accept Attributes

Note 12: Only the dotted decimal notation format required in RFC2868^[15] is supported.

Note 13: The tunnel password should normally be returned via RADIUS. However if an intermediate un-trusted RADIUS proxy is being used, where the tunnel password will be decrypted and re-encrypted, this may not be desirable. In such cases, BT can configure a tunnel password on the Tunnel Concentrator. This adds the restriction that only one unique tunnel password can be used with each L2TP Tunnel Concentrator.

Note 14: This attribute allows sessions to be grouped in separate tunnels between the same endpoints. Creating a large number of tunnels between the same end points can be detrimental to both LNS and L2TP Tunnel Concentrator performance so should be used with caution.

Note 15: This attribute is used to group tagged attributes as described in RFC2868^[15]. Tagging is only required if more than one Tunnel-Server-Endpoint is used.

Note 16: The Tunnel-Client-Auth-ID is used to populate the L2TP Host Name AVP. If this attribute is not used, the default host name from the L2TP Tunnel Concentrator will be used. The format of this host name is unspecified but will be unique for any given L2TP Tunnel Concentrator.

Attributes other than those shown in Table 16 are not supported. If other attributes are returned the product may work successfully but consistent operation on the same or other L2TP Tunnel Concentrators cannot be guaranteed.

RADIUS accounting is optional and is provided on request. Table 17 lists the set of RADIUS accounting attributes the product will present, from RFC2865^[12], RFC2866^[13], RFC2867^[14], RFC2868^[15] and RFC2869^[16]. Three accounting packet types are supported, Start, Stop and Interim update. Attributes in Italics are only present in Stop or Interim update packets.

Formatted: Check grammar, Superscript

Deleted: ¹⁵

Deleted: ¹⁵

Formatted: Check grammar, Superscript

Deleted: ¹³

Deleted: ¹⁴

Formatted: Check grammar, Superscript

Deleted: ¹²

Formatted: Check grammar, Superscript

Formatted: Check grammar, Superscript

Formatted: Check grammar, Superscript

Deleted: ¹⁵

Formatted: Superscript

Deleted: ¹⁶

No	Attribute	Value	Comment
1	User-Name	username	
4	NAS-IP-Address	Tunnel Concentrator logical source address	
5	NAS-Port	Tunnel Concentrator logical port	
6	Service-Type	(2) Framed	
7	Framed-Protocol	(1) PPP	
25	Class	string	Present if returned in corresponding Access-Accept.
30	Called-Station-Id	DNIS	Full dialled number less leading zero
31	Calling-Station-Id	End User's CLI	Presentation CLI with no leading zero. End Users may withhold their CLI in which case this attribute will not be present.
40	Acct-Status-Type	(1) Start (2) Stop (3) Interim-Update	
41	Acct-Delay-Time	integer	Only present if value is not zero.
42	<i>Acct-Input-Octets</i>	<i>integer</i>	
43	<i>Acct-Output-Octets</i>	<i>integer</i>	
44	Acct-Session-Id	unique string	
45	Acct-Authentic	(1) RADIUS	
46	<i>Acct-Session-Time</i>	<i>integer</i>	
47	<i>Acct-Input-Packets</i>	<i>integer</i>	
48	<i>Acct-Output-Packets</i>	<i>integer</i>	
49	<i>Acct-Terminate-Cause</i>	<i>integer</i>	
55	Event-Timestamp	integer	
61	NAS-Port-Type	(0) Async (2) ISDN Sync (4) ISDN Async V.110	
64	Tunnel-Type	L2TP	
66	Tunnel-Client-Endpoint	IP address	
67	Tunnel-Server-Endpoint	IP address	
68	Acct-Tunnel-Connection	string	
90	Tunnel-Client-Auth-ID	name	
91	Tunnel-Server-Auth-ID	name	

Table 17 L2TP Accounting-Request Attributes

Attributes in Italics are only present in Stop or Interim update packets.

3.6 Network Terminating Equipment (NTE)

The NTE will vary depending on the interface option selected by the Customer and the bandwidth required.

In the case of the LAN interfaces BT will generally use a LAN Extension Service^{[19][21]} to provide the connection from the Customer's premises to the nearest convenient BT Point of presence. In this case, no additional terminating equipment will be required. If due to reach or other limitations a LAN extension service cannot be used, BT will use SDH transmission and additional NTE equipment to convert the SDH delivery to Ethernet.

In the case of the SDH based WAN interfaces BT will use a Short Haul Data Service^{[17][18]} wherever practical to provide the connection from the Customer's premises to the nearest convenient BT Point of presence. Where this is not practical, SDH transmission will be used.

BT will require rack space and power for the terminating transmission equipment and additional NTE routers if necessary.

4 FURTHER INFORMATION CONTACT POINTS

For further information about services provided over BT Dial IP please contact either:

- Your Company's BT account manager
- See the BT web site at <http://www.btglobalservices.com/>

If you have enquiries relating to this document then please contact: help@sinet.bt.com

5 IMPLEMENTATION OF RFC2661

BT participated in an Oftel NICC industry group that developed a UK understanding of how to implement the options within the RFC2661^[10]. This document has been published as NICC Document ND1009 (PNO-ISC/SPEC/009) Layer 2 Tunnelling Protocol^[20].

Deleted: 19

Formatted: Check grammar, Superscript

Deleted: 21

Formatted: Check grammar, Superscript

Deleted: 18

Formatted: Check grammar, Superscript

Deleted: 17

Formatted: Check grammar, Superscript

Formatted: Check grammar, Superscript

Deleted: 10

Formatted: Superscript

Deleted: 20

6 REFERENCES

1	RFC 791	Internet Protocol: DARPA Internet Program Protocol	Sep-81
2	RFC 1618	PPP over ISDN	May-94
3	RFC 1661	The Point-to-Point Protocol (PPP)	Jul-94
4	RFC 1723	RIP V2: Routing Information Protocol - Version 2	Nov-94
5	RFC 1771	A Border gateway Protocol 4 (BGP4)	Mar-95
6	RFC 1918	Address Allocation for Private Internets	Feb-96
7	RFC 1990	The PPP Multilink Protocol (MP)	Aug-96
8	RFC 1994	PPP Challenge Handshake Authentication Protocol (CHAP)	Aug-96
9	RFC 2281	Cisco Hot Standby Router Protocol (HSRP)	Mar-98
10	RFC 2661	Layer Two Tunnelling Protocol "L2TP"	Aug-99
11	RFC 2796	BGP Route Reflection – an alternative to full mesh iBGP	Apr-00
12	RFC 2865	Remote Authentication Dial In User Service (RADIUS)	June-00
13	RFC 2866	RADIUS Accounting	June-00
14	RFC 2867	RADIUS Accounting Modifications for Tunnel Protocol Support	June-00
15	RFC 2868	RADIUS Attributes for Tunnel Protocol Support	Jun-00
16	RFC 2869	RADIUS Extensions	Jun-00
17	SIN 286	BT LAN Extension Service 155 - Service Description	
18	SIN 293	BT Local Area Network (LAN) Extension Service 622	
19	SIN 311	BT LAN Extension Service 100 Enhanced, Service Description.	
20	ND1009	NICC Document ND1009 (PNO-ISC/SPEC/009), Layer 2 Tunnelling Protocol	
21	SIN 338	BT LAN Extension Service 1000 - Service Description	

The SIN/STINs are BT documents and are available from <http://www.sinet.bt.com/>.

For information on where to obtain other referenced documents, please see the document sources list at <http://www.sinet.bt.com/>.

7 ACRONYMS

ADM	Add-drop Multiplexer [SDH]
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
AVP	Attribute Value Pair
BGP4	Border Gateway Protocol version 4
BTNR	BT Network Requirement
CHAP	Challenge Handshake Authentication Protocol
CLI	Calling Line Identity
CPE	Customers' Premises Equipment
CSMA	Carrier Sense Multiple Access
DARPA	Defence Advanced Research Project Agency [USA]
DNIS	Dialled Number Information String
DNS	Domain Name System/Server
EMC	Electro-Magnetic Compatibility
HSRP	Hot Standby Router Protocol
iBGP	internal Border Gateway Protocol
IPCP	Internet Protocol Control Protocol
IEEE	Institute of Electronic and Electrical Engineers [USA]
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol Version 4
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union - Telecommunications Standardization Sector
L2TP	Layer 2 Tunnelling Protocol
LAC	L2TP Access Concentrator
LAN	Local Area Network
LCP	Link Control Protocol
LNS	L2TP Network Server
LLC	Link Layer Control
LTC	Layer 2 Tunnelling Protocol (L2TP) Tunnel Concentrator

MP	Multilink Protocol
MRRU	Maximum Received Reconstructed Unit
NAS	Network Access Server
NCP	Network Control Protocols
NICC	Network Interoperability Consultative Committee (Ofel)
NTE	Network Termination Equipment
NTP	Network Terminating Point
PAP	Password Authentication Protocol
PC	Personal/Portable Computer
PECS	Providers of Electronic Communications Services
POS	Packet Over SONET
PPP	Point-to-Point Protocol
PSTN	Public Switched Telephone Network
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comment
RIP	Routing Information Protocol
RJ45	Registered Jack 45
SDH	Synchronous Digital Hierarchy
SIN	Supplier Information Note [BT]
SONET	Synchronous Optical Network
STD	Standard (IETF)
STM-1	Synchronous Transport Module Level 1 (155 Mbit/s)
STM-4	Synchronous Transport Module Level 4 (622 Mbit/s)
UDP	User Datagram Protocol
VC	Virtual Circuit
VCI	Virtual Circuit Identifier
VP	Virtual Path
VPI	Virtual Path Identifier
VPN	Virtual Private Network
WAN	Wide Area Network

8 HISTORY

Issue	Date	Change History
STIN 389 1.0	01 November 2001	First Issue
SIN 389 1.0	26 April 2002	Updated STIN to SIN. Table 6 attributes 6 & 7 become "optional". Section 2.3 clarification on the recommended use of "LCP re-negotiation".
SIN 389 1.1	13 th August 2002	Addition of Standard IP operation as well as L2TP Passthrough to provide a single, up to date SIN for SurfPort and SurfPort24. RADIUS accounting on LT2P available.
SIN 389 1.2	14 May 2004	Terminal Equipment Approval information removed. MP option added. Editorial changes.
Issue 1.3	June 2010	Updated to reflect that service is not available to new customers

-END-

WE WOULD BE GRATEFUL IF YOU WOULD SPEND A FEW MINUTES TO COMPLETE AN ONLINE CUSTOMER SATISFACTION FORM AT [HTTP://WWW.SINET.BT.COM/HAPPY.HTM](http://www.sinet.bt.com/happy.htm).