SIN 392

Issue 1.4
June 2010

Suppliers' Information Note

For The BT Network

BT Dial IP SurfNet
Service Description

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.

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

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

CONTENTS

Note: This product was Withdrawn From New Supply in April 2009.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

INTRODUCTION

This Suppliers' Information Note (SIN) describes the network interfaces for the BT SurfNet service, which is part of the BT IP Services Transport Portfolio. It does not apply to any other BT Service.

This version updates the previous version (1.2) with some minor changes as a result of a migration to an alternative equipment vendor. During the course of migration both variants are relevant. Issue 1.2 is therefore appended to this document for reference. It is not anticipated that equipment currently working with the interface described in issue 1.2 would need to be modified to work with the interface described in this document.

Reference is made to specific interfaces within this document that will be supported by the BT SurfNet service. This document will define these interfaces, however where reference is made to external interface definitions e.g. other BT SINs, this is to provide additional information on how these interfaces will be supported. It should be noted that these external definitions may contain details of interface types that are not supported as part of the BT SurfNet service.

Note the L2TP Interface described in Annex A is consistent with the definition as ratified by the industry task group.

The BT SurfNet service is designed to provide a dedicated network infrastructure to enable Providers of Electronic Communications Services (PECS) to give their end users dial-in access to the PECS own network. The service has been designed for PECS operating their own Service Desk capability offering their own front-end installation, maintenance and billing support to their dial-in users.

1 DEFINITIONS

Customer - The PECS or Corporate Customer (CC) who purchases a Dial IP product from BT and sells or provides this to their own 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.

LAC - L2TP Access Concentrator. The device that originates L2TP tunnels.

L2TP Pass-through – Passing through the L2TP tunnels to the "Customer".

For details of L2TP, please refer to RFC 2661[12], and NICC Document ND1009 (PNO-ISC/SPEC/009) Layer 2 Tunnelling Protocol[16], for the UK implementation of L2TP.

NAS – Network Access Server. The device that contains the modems and terminates the End User telephony channels. In the BT Dial IP products, the NAS can also act as a LAC.

RADIUS - A suite of protocols used for Authentication, Authorisation and Accounting of dial-in sessions.

TCP Clear – A method of transporting un-framed serial data from a network based modem to a remote host.

Formatted: Ch
grammar, Super
Deleted: 12
Deleted: 16
Formatted: Su

2 SERVICE OUTLINE

The BT SurfNet service is offered to Service Providers and other customers requiring dial access into their IP networks. Dial access will be available only on the BT FRIACO number range.

The service supports PPP based End User accesses which can be either terminated locally within the BT network on the NAS, or forwarded in L2TP tunnels to the Customer's network and TCP Clear connections. A RADIUS interface is provided between the NAS/LAC and the Customer.
RADIUS must be used by the Customer to deliver sufficient data to enable the LAC to build an L2TP tunnel into the Customer's network. RADIUS is not used with TCP Clear or locally terminated PPP sessions.

The service is packaged according to the number of dedicated 2 Mbps links that the customer wishes their service to support (as specified on the Customer's order). These are provided from the BT DLEs to BT Dial POPs hosting the NASs as part of the service.

Additionally the service includes a resilient connection between the Customer's premises and BT's high speed data network.

An overview of the service is illustrated below:-

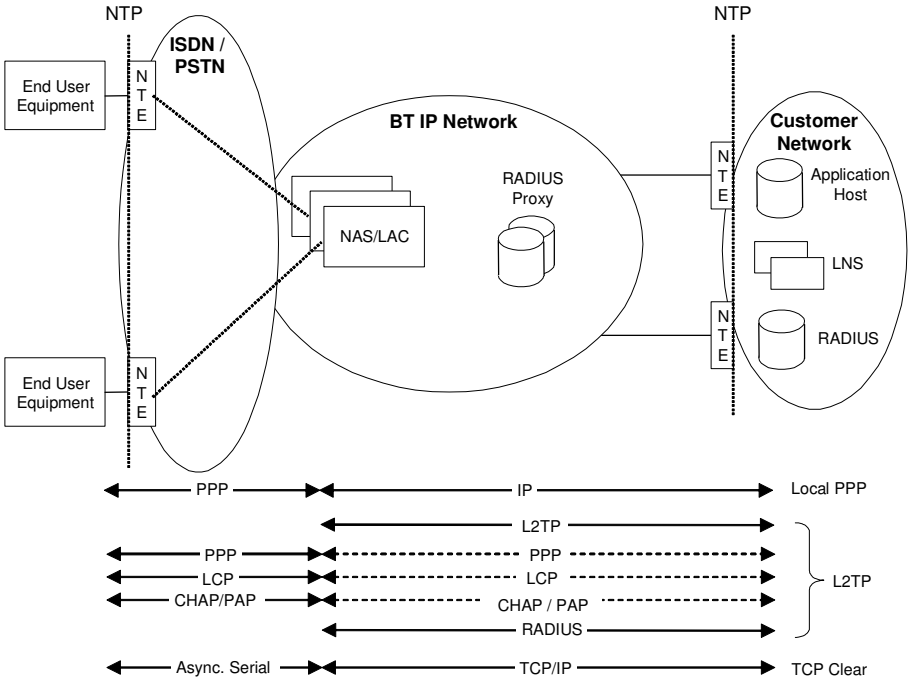

Figure 1 – BT SurfNet Service Overview

IP routing information needs to be exchanged between BT and the Customer about the NASs. This will be provided by 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.

The Customer needs to 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 subnets for the WAN I/Fs where SDH is used.
- Choice of routing protocol for host link (as defined in section 3.1.)
- RADIUS parameters including IP address(s), shared secret and UDP port for Authentication.
- Generic local username/password if BT is to perform End User network authentication
- Choice of End User authentication protocol
- IP addresses for locally terminated PPP sessions
- Idle timeout value for PPP sessions locally terminated on BT NASs.
- DNS Server addresses.
- End station name and port for TCP Clear connections.

Deleted: 4.1

3 TECHNICAL SPECIFICATION FOR END USER INTERFACE

The End User interface is connected at a physical level using PSTN or ISDN as defined in Tables 1 & 2 respectively. In summary, BT SurfNet will support:

- Modem access at 14.4, 28.8, 33.6 and 56Kbps
- Synchronous ISDN access at 64Kbps
- Access within the UK via the BT FRIACO number range 0808 9944

Standards applicable to the PSTN & Modem interface 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

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 (May-94)
RFC 1990	The PPP Multilink Protocol (MP)

Table 2 ISDN Interface presentation

The IETF RFCs applicable to the PPP and IP layers are contained in Table 3 below.

STD 5[31]	Internet Protocol: DARPA Internet Program Protocol, 1981
STD 51[34]	PPP Standard
RFC 1332	The PPP Internet Protocol Control Protocol (IPCP)
RFC 1877	PPP IPCP Extensions (Primary and Secondary DNS address options only)
RFC 1994	PPP Challenge Handshake Authentication Protocol (CHAP)

Table 3 PPP & IP RFCs

The BT NAS/LAC will request the following LCP options appropriate to a narrow-band PPP link for both the locally terminated PPP 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

In addition if the client is configured for MP[7], an MRRU and End Point Discriminator may be negotiated. This capability will always be present for ISDN connections using RFC 1618[2].

Where these parameters are negotiated the locally terminated PPP variant will implement the MP protocol but will only support a single link. 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 the network and the performance of the return path will be severely degraded. Should an MP 'bundle' be established, the number of links is limited to one by configuration.

Deleted: 31
Formatted: Su
Deleted: 34
Formatted: Su
Formatted: Su
Deleted: 7
Deleted: 2
Formatted: Su

3.1 TCP Clear

TCP Clear as a protocol is transparent to dial-in users. It is a method of transporting the serial data transparently from the user to the Customer, allowing the Customer to apply any framed protocol without intervention by the NAS.

Following a successful modem connection, the NAS will present a login banner followed by a login prompt, if the user does not send a PPP frame after a pre-determined timeout period. The user can pre-empt this by sending a Carriage Return character (0x0D) after the modem has connected. The Customer may specify the banner, username and password, which will be common to all TCP Clear connections.

If the user presents the correct username and password, the NAS will establish a TCP Clear connection. Once established, the NAS will send user bytes transparently over the TCP connection to the customer's TCP server and send bytes received from the connection transparently to the user.

4 TECHNICAL SPECIFICATION FOR CUSTOMER INTERFACE

Dual fixed connections to the customer's host site will be delivered via the following physical layer and IP encapsulation option:-

- IP encapsulated directly in SDH (i.e. Packet over SONET), delivered on single mode optical fibre at STM-4 rates.

WAN interfaces are numbered using a /30 sub-net with IP addresses supplied by the Customer. These can be public or to RFC 1918[6]. BT provides a DNS service for customers wishing to support their own DNS service conformant to STD 13[33].

Formatted: Su
Deleted: 6
Deleted: 33
Formatted: Su

This interface is defined by the following:-

SIN 286	BT LAN Extension Service 155 - Service Description
SIN 289	"BT Megastream 155 and BT Megastream Aggregate Service Description" (MegaStream155 section – optical only) Certain aspects apply: • ITU-T G.957 – Optical Interfaces for Equipments 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 293	BT Local Area Network (LAN) Extension Service 622
SIN 333	SDH Customer Interfaces at the STM-4 level Interface Characteristics – certain aspects only relevant to the interface
SIN 337	BT MegaStream 622 and BT MegaStream Aggregate (STM-4) Service Description – certain aspects only relevant to the interface
RFC 2615	PPP over SONET/SDH, A Malis, June 1999
STD 5	Internet Protocol: DARPA Internet Program Protocol, 1981
STD 7[32]	Transmission Control Protocol: DARPA Internet Program Protocol

Formatted: Su

Deleted: 32

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

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 RFC 2615
Cyclic Redundancy Check	32 bit
Clock source	Internal

Table 5 Packet over SONET default configuration

4.1 Network Terminating Equipment (NTE)

In the case of the SDH based WAN interfaces, BT will use a Short Haul Data Service LES 155 & LES 622 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 as in Table 4.

BT will require rack space and power for the terminating transmission equipment and additional NTE routers, if necessary. The specific requirements will be dependent upon the particular delivery method- LES 155, LES 622, SDH, MegaStream 155.

4.2 IP Transport Layer

This layer must conform to STD 5[31]. 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[3]
- BGP version 4 as RFC 1771[4] and RFC 2796[13]

4.3 L2TP Layer

The L2TP Interface, as in Annex A, is consistent with the definition as published in NICC Document ND1009 (PNO-ISC/SPEC/009 Layer 2 Tunnelling Protocol). The NASs, acting as Layer 2 Tunnel Protocol Access Concentrators (LACs), 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 an access-request from the LAC. The RADIUS interface for the control of L2TP sessions is as specified in Annex B. In the case where the customer does not return a Tunnel-Password attribute, the value provided by the Customer will be configured identically on all LACs within the BT SurfNet implementation. It should be noted that in BT SurfNet, the NAS acts as the LAC and is the tunnel origination point into the customers network, and as such exhibits those aspects of the behaviour of the L2TP Tunnel Concentrator (LTC) as described in SIN 389[30] which are particular to the interface into the customers network. The Customer's equipment terminating tunnels, either one or more L2TP Network Servers (LNSs) or the Customer's own L2TP Tunnel Concentrators must conform to RFC 2661 and take account of NICC Document ND1009.

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

Sequence numbers are not used by default on the L2TP data channel.

4.4 PPP Layer

The End User's terminating equipment must support the Point-to-Point Protocol (PPP) for dial services[34].

LCP must be negotiated with the BT network and either CHAP[8] or PAP must be used as an authentication protocol initially. The PPP authentication protocol(s) to be used is defined by the customer and will be applied to all NASs within the BT SurfNet implementation. The PPP LCP protocol is initiated between the End User client software and the BT network. Negotiation of Multi-link PPP (MP[7]) is supported, if requested by the Customer, for ISDN and/or analogue connections. Multi-chassis MP is not supported by the NAS/LAC. A fuller description of the network constraints associated with MP in the L2TP pass-through environment can be found in Annex A. Customers may configure their LNS to re-negotiate LCP in the event that the BT default parameters are not suitable.

End User authentication is the responsibility of the Customer. BT can provide network access authentication against a single (generic) local account for PPP sessions that are terminated on the NAS. In the L2TP Pass-through environment BT can forward End User authentication details to a Customer provided RADIUS server. If RADIUS authentication of End Users is required, requests will be directed to the same set of RADIUS servers that handle L2TP pass-through LNS requests. In the L2TP Pass-through environment, End User authentication is handled by the Customer's equipment terminating the tunnels. The RADIUS interface for L2TP forwarded PPP sessions is as specified in Annex B.

Deleted: 31
Formatted: Sup
Deleted: 3
Formatted: Ch grammar, Super
Deleted: 13
Formatted: Ch grammar, Super
Deleted: 4
Formatted: Ch grammar, Super
Formatted: For Superscript
Deleted: 30
Formatted: Sup
Deleted: 34
Formatted: Sup
Deleted: 8
Deleted: 7
Formatted: Sup

4.5 TCP Clear

A separate TCP[32] connection is established by the NAS to a nominated TCP port on a specific TCP host for each locally authenticated user, The host may be defined using a fully qualified domain name in which case this will be resolved using DNS[33]. The IP address of a primary and secondary DNS server used for this purpose can be defined by the Customer.

Formatted: Re
spelling and gra
Deleted: 32
Deleted: 33
Formatted: Su

5 FURTHER INFORMATION CONTACT POINTS

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

1. Your Company's BT account manager
2. 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

6 REFERENCES

1	RFC 1332	The PPP Internet Protocol Control Protocol (IPCP)	May-92
2	RFC 1618	PPP over ISDN	May-94
3	RFC 1723	RIP V2: Routing Information Protocol – Version 2	Nov-94
4	RFC 1771	A Border gateway Protocol 4 (BGP4)	Mar-95
5	RFC 1877	PPP IPCP Extensions (Primary and Secondary DNS address options only)	Dec-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 2132	DHCP Options and BOOTP Vendor Extension	Mar-97
10	RFC 2151	A Primer On Internet and TCP/IP Tools and Utilities	Jun-97
11	RFC 2615	PPP over SONET/SDH, A Malis, June 1999	Jun-99
12	RFC 2661	Layer Two Tunnelling Protocol "L2TP"	Aug-99
13	RFC 2796	BGP Route Reflection – an alternative to full mesh iBGP	Apr-00
14	RFC 2865	Remote Authentication Dial In User Service (RADIUS)	Jun-00
15	RFC 2868	RADIUS Attributes for Tunnel Protocol Support	Jun-00
16	NICC Document ND1009 (PNO-ISC/SPEC/009) Layer 2 Tunnelling Protocol		
17	SIN 171	ISDN 2 Service (I.420) - Description	
18	SIN 232	BT ISDN 30 (I.421) Service - Service Description	
19	SIN 261	BT ISDN 2e and ISDN 30e (ISDN30 (I.421) using full ETSI Call Control - Service Description	
20	SIN 286	BT LAN Extension Service 155 - Service Description (1.1)	
21	SIN 289	BT Megastream 155 and BT Megastream Aggregate Service Description	
22	SIN 293	BT Local Area Network (LAN) Extension Service 622 (1.1)	
23	SIN 312	BT ISDN Services Overview	
24	SIN 333	SDH Customer Interfaces at the STM-4 level Interface Characteristics	
25	SIN 337	BT MegaStream 622 and BT MegaStream Aggregate (STM-4) Service Description	

26	SIN 350	BT Public Switched Telephone Network (PSTN): Network Tones and Announcements	
27	SIN 351	BT Public Switched Telephone Network (PSTN): Technical Characteristics Of The Single Analogue Line Interface	
28	SIN 352	BT Public Switched Telephone Network (PSTN): Technical Characteristics Of The Multi-Line Analogue Line Interface	
29	SIN 367	Characteristics of the BT Network: Electrical Safety and EMC	
30	SIN 389	L2TP Interface For BT Dial IP	
31	STD 5	Internet Protocol: DARPA Internet Program Protocol comprising: RFC 791 Internet Protocol RFC 792 Internet Control Message Protocol RFC 919 Broadcasting Internet Datagrams RFC 922 Broadcasting Internet datagrams in the presence of subnets RFC 950 Internet Standard Subnetting Procedure RFC 1112 Host extensions for IP multicasting	Sep-81
32	STD 7	Transmission Control Protocol: DARPA Internet Program Protocol comprising: RFC 793 Transmission Control Protocol	Sep-81
33	STD 13	Domain Implementation and Specification comprising: RFC 1034 Domain names - concepts and facilities RFC 1035 Domain names - implementation and specification	Nov-87
34	STD 51	The Point-to-Point Protocol (PPP) comprising: RFC 1661 The Point-to-Point Protocol (PPP) RFC 1662 PPP in HDLC-like Framing	Jul-94

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/docsources.htm.

7 ACRONYMS

ACCM	Async Control Character Map
ACFC	Address and Control Field Compression
AVP	Attribute Value Pair
BGP4	Border Gateway Protocol version 4
CHAP	Challenge Handshake Authentication Protocol
CLI	Calling Line Identity
CPE	Customers' Premises Equipment
DARPA	Defense Advanced Research Project Agency [USA]
DCE	Data Circuit-terminating Equipment
DLE	Digital Local Exchange
DNIS	Dialled Number Information String
DNS	Domain Name System
EMC	Electro-Magnetic Compatibility
ETSI	European Telecommunications Standards Institute
FRIACO	Flat Rate Internet Access Call Origination
HDLC	High-level Data-Link Control
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union - Telecommunications Standardisation Sector
L2TP	Layer 2 Tunnelling Protocol
LAC	L2TP Access Concentrator
LAN	Local Area Network
LCP	Link Control Protocol
LES	LAN Extension Service
LNS	L2TP Network Server
LTC	L2TP Tunnel Concentrator
MNP	Microcom Network Protocol
MP	Multi-link PPP Protocol
MRRU	Maximum Received Reconstructed Unit
NAS	Network Access Server
NCP	Network Control Protocol
NICC	Network Interoperability Consultative Committee (Ofcom)
NTE	Network Termination Equipment
NTP	Network Terminating Point
Ofcom	Office of communications
OLO	Other Licensed Operator
ONO	Other Network Operator
PAP	Password Authentication Protocol
PECS	Providers of Electronic Communications Services
PNO-ISC	Public Network Operators Interconnect Standards Committee
POP	Point Of Presence
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
SDH	Synchronous Digital Hierarchy
SIN	Supplier Information Note [BT]
SONET	Synchronous Optical Network
STIN	Suppliers' Trial Information Note
STM-4	Synchronous Transport Module Level 4 (622 Mbit/s)
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WAN	Wide Area Network

8 HISTORY

Issue 1	March 2002	First Issue
Issue 1.1	13th August 2002	Updated to provide a single standalone SIN for BT SurfNet. Plus additional help text added.
Issue 1.2	May 2004	Clause on terminal equipment approval requirements removed. Editorial changes.
Issue 1.3	March 2006	Modified for alternative NAS vendor and RADIUS proxy servers. TCP Clear feature further described
Issue 1.4	June 2010	Text inserted to reflect service is not available for new customers

ANNEX A – L2TP PASSTHROUGH

This annex contains details of the L2TP Pass-through offering.

A. 1 Interface Outline

BT Dial IP L2TP Passthrough offering 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 End User access remains the same as that currently used by BT Dial IP products.

The BT Dial IP L2TP passthrough interface provides connection between the Customer's premises and BT's high speed data network, which hosts a number of NASs allocated to the Customer for any instance of the BT SurfNet product.

The NASs 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 NAS and Customer's LNS are established dynamically on demand.

A RADIUS interface is provided between the Customer and the NAS to allow the Customer full control, on a per End User session basis, of the Customer side L2TP tunnel end points. The RADIUS interface is described in Annex B to accommodate the necessary L2TP RADIUS extension attribute/value pairs.

Figure 1 shows the basic service architecture as described above.

A. 2 L2TP Layer

The NASs, acting as LACs, 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 reply string in response to an access-request from the LAC. The Customer's equipment terminating tunnels (one or more LNSs) must conform to RFC 2661.

A. 3 PPP Layer

After LCP negotiation completes the negotiated authentication protocol will commence.

Once authenticated, IPCP will commence for locally terminated PPP sessions. BT will configure customer specific DNS server IP addresses to be assigned via IPCP to the dial-in client, if required.

With the L2TP variant there is no IP layer specified and consequently no IP related NCP (Network Control Protocol) 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 RFC 2661[12] 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. If the use of LCP re-negotiation is required, Customers should discuss the technical implications with a BT Technical Support Engineer prior to implementation.

Formatted: Su

Deleted: [12]

The L2TP pass-through capability is primarily aimed at the transport of IP datagrams encapsulated by PPP, however PPP is capable of encapsulating other protocols and associated NCPs. 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 pass-through interface will transport Multi-link PPP frames within the L2TP tunnels. The PPP LCP protocol is initiated between the End User client software and the BT network. Negotiation of MP is supported at this point on ISDN connections to RFC 1618[2].
The customer LNS is the first point in the connection that individual MP connections can be re-combined. BT will not attempt to re-combine any MP connections before forwarding the PPP session to the Customer LNS.
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 LACs. The IP based transport used to forward these packets from the LACs 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.)

Formatted: Su

Deleted: 2

A. 4 RADIUS protocol

RADIUS Authentication is essential for the normal operation of the L2TP aspects of this product. RADIUS Accounting is not provided.

The BT platform supports the following RADIUS packet types:-

ID	Packet Type
1	Access-Request
2	Access-Accept
3	Access-Reject

RADIUS interoperation requires a shared secret to be configured on the Customer RADIUS servers associated with each NAS, acting as a RADIUS client. The RADIUS server knows the client by its IP address.
If the NAS 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 a number of subsequent requests will be sent to that server after which the next request will be sent again 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 A sensible server implementation would log an error to enable further diagnostic investigation if required.

If an Access-Reject is returned the End User session is terminated. No Access-Reject attributes are supported.

Parameter	Default Value	Comment
Primary RADIUS authentication IP address	Customer supplied	Required
Secondary RADIUS authentication IP address	Customer supplied	Optional
Primary RADIUS accounting IP address	Customer supplied	Optional
Secondary RADIUS accounting IP address	Customer supplied	Optional
RADIUS authentication UDP port	1645	Any port in the range 1 – 65535
Shared Secret	Customer supplied	Random 1- 16 characters. A 16 character secret is recommended.

Table 6 RADIUS Parameters

An incoming session to an NAS will trigger a RADIUS Access-Request using attributes shown in Table 7. The Customer's RADIUS should respond with attributes from Table 8.

ANNEX B – RADIUS PARAMETERS

This annex contains a summary of the RADIUS parameters used in the support of the BT SurfNet service.

Table 7 shows the key set of attributes presented by the BT LAC sent via the BT proxy RADIUS servers. In addition to the attributes shown here a number of Vendor-Specific (Attribute 26) RADIUS attributes may be present. These should be ignored by the Customer's RADIUS servers.

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 RFC 2865[14] (Note 1)
3	CHAP-Password	user's CHAP password	As captured by BT LAC. (Notes 1 & 2)
4	NAS-IP-Address	LAC source IP address	
5	NAS-Port	LAC local port	
6	Service-Type	Framed	
7	Framed-Protocol	PPP	
26	Vendor-Specific	Unspecified	
30	Called-Station-Id	DNIS	Full dialled number less leading zero
31	Calling-Station-Id	End User's CLI	No leading zero. End Users may withhold
32	NAS-Identifier	NAS host name	
33	Proxy-State	unique string	
44	Acct-Session-Id	unique string	
61	NAS-Port-Type	(0) Async (2) ISDN Sync (3) V.120	

Table 7 Access-Request Attributes

Note 1: RFC2865 Mandates that either User-Password (Attribute 2) or CHAP-Password (Attribute 3) must be present.

Note 2:The option specified in RFC 2865 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 8. These include some from RFC 2865 and the L2TP tunnel specific from RFC 2868[15]. These attributes are necessary for the product to work unless shown as optional in the comment column.

Formatted: Su
Deleted: 14
Deleted: 15
Formatted: Su

No	Attribute	Value	Comment
33	Proxy-State	unique string	Exact copy of Proxy-State from corresponding Access-Request.
64	Tunnel-Type	L2TP	
65	Tunnel-Medium-Type	IPv4	
67	Tunnel-Server-Endpoint	LNS IP address	(Note 3)
69	Tunnel-Password	password	Optional (Note 4)
82	Tunnel-Assignment-ID	string	Optional (Note 5)
83	Tunnel-Preference	integer	Optional (Note 6)
90	Tunnel-Client-Auth-ID	string	Optional (Note 7)

Table 8 Access-Accept Attributes

Note 3:Only the dotted decimal notation format required in RFC 2868 is supported.

Note 4: This attribute is used to populate the L2TP Challenge AVP as described in RFC 2661. Reference should be made to the security considerations for the Tunnel-Password attribute described in RFC 2868.

Note 5: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 NAS performance, so should be used with caution.

Note 6:This attribute is used to group tagged attributes as described in RFC 2868. Tagging is only required if more than one Tunnel-Server-Endpoint is used.

Note 7:The Tunnel-Client-Auth-ID is used to populate the L2TP Host Name AVP as described in RFC 2661. If the Tunnel-Client-Auth-ID attribute is not used, the default host name from the NAS will be used. The format of this host name is unspecified but will be unique for any given NAS.

< 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.