



SIN 383

Issue 2.1
June 2010

Suppliers' Information Note

For The BT Network

BT WebPort 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.

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

1. INTRODUCTION	3
1.1 DEFINITIONS.....	3
2. SERVICE OUTLINE	3
3. TECHNICAL SPECIFICATION FOR END USER INTERFACE	5
3.1 MP TERMINATION.....	7
3.2 MP AND L2TP PASSTHROUGH.....	7
3.3 L2TP PASSTHROUGH.....	8
4. TECHNICAL SPECIFICATION FOR CUSTOMER INTERFACE	8
5. WEBPORT RADIUS ATTRIBUTE SUPPORT	9
5.1 RADIUS ATTRIBUTES DEFINITION.....	11
5.2 ADDITIONAL RADIUS ATTRIBUTES EXPLANATION.....	15
5.2.1 <i>Session-Timeout</i>	15
5.2.2 <i>Idle-Timeout</i>	15
5.2.3 <i>DNS</i>	15
5.2.4 <i>Filters</i>	16
5.2.5 <i>Filter Examples</i>	16
5.3 PERFORMANCE TECHNIQUES.....	16
5.4 BT PROXY AUTHENTICATION SERVERS.....	17
5.4.1 <i>RADIUS Timeout Settings</i>	17
5.5 MULTILINK PROTOCOL SUPPORT.....	17
6. FURTHER INFORMATION CONTACT POINTS	18
7. REFERENCES	18
8. ABBREVIATIONS	19
9. HISTORY	21
FIGURE 1 –WEBPORT SERVICE OVERVIEW.....	4
TABLE 1 ANALOGUE INTERFACE PRESENTATION.....	5
TABLE 2 ISDN INTERFACE PRESENTATION.....	6
TABLE 3 PPP & IP RFCs (PPP TERMINATION).....	6
TABLE 4 PPP & IP RFCs (L2TP PASSTHROUGH).....	6
TABLE 5 CUSTOMER INTERFACE PRESENTATION (PPP TERMINATION).....	8
TABLE 6 CUSTOMER INTERFACE PRESENTATION (L2TP PASSTHROUGH).....	9
TABLE 7 ACCESS-REQUEST ATTRIBUTES (PPP TERMINATION & L2TP PASSTHROUGH).....	11
TABLE 8 ACCESS-ACCEPT ATTRIBUTES (PPP TERMINATION).....	12
TABLE 9 ACCESS-ACCEPT ATTRIBUTES (L2TP PASSTHROUGH).....	12
TABLE 10 ACCOUNTING-REQUEST ATTRIBUTES (PPP TERMINATION & L2TP PASSTHROUGH).....	14

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 customer interface for the BT WebPort services, which are part of the BT IP Services Transport Portfolio, and it does not apply to any other BT Service.

The WebPort services are designed to provide Internet Access for use by Providers of Electronic Communications Services (PECS), and BT. The service provides PECS end users with dial-in access to the Internet. 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.

1.1 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 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.

NAS / LAC - Network Access Server / L2TP Access Concentrator. The device that contains the modems and terminates the End User telephony channels.

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

2. Service Outline

The WebPort service is offered to PECS and other customers requiring provision of end user dial access to the Internet.

The service supports two main technical variants:

1. PPP Termination

PPP based End User accesses terminated within the BT network on a shared router. These sessions are onward routed via the Internet.

2. L2TP Passthrough

where the End User PPP sessions are presented to the Customer in L2TP tunnels.

An optional RADIUS interface is provided to the Customer.

The service boundaries are as illustrated in Figure 1.

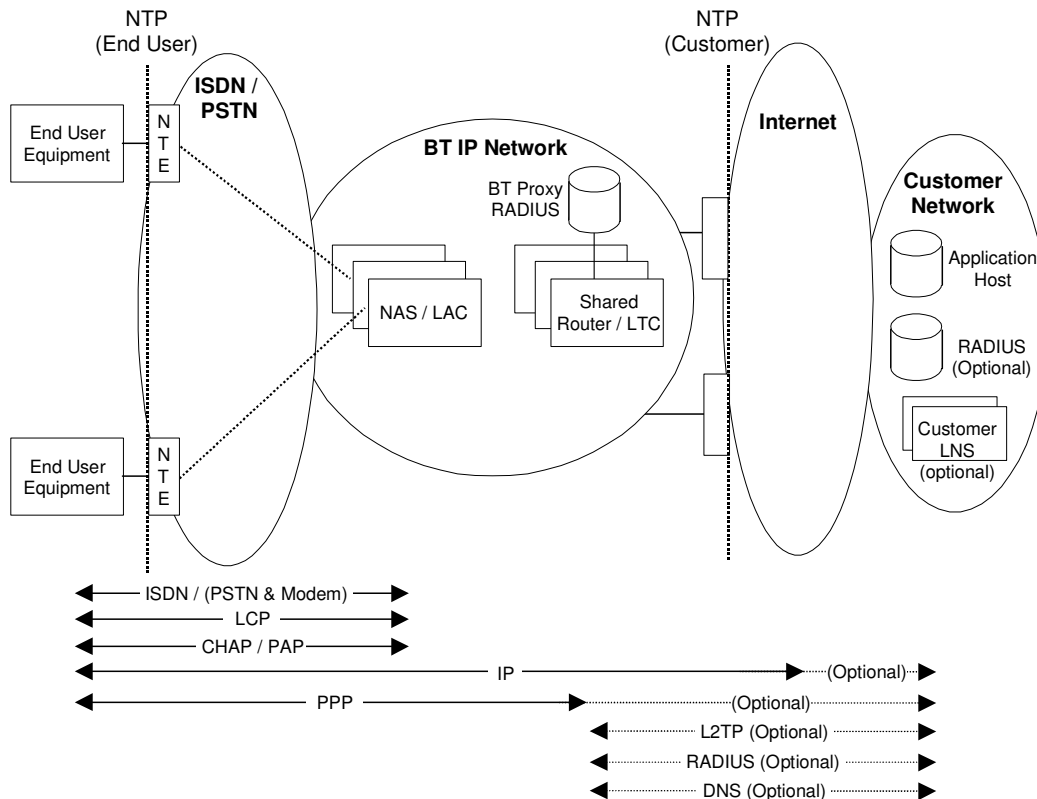


Figure 1 –WebPort Service Overview

The Customer will need to provide the following information to BT in order for the service to function if they wish to run their own RADIUS:-

- RADIUS parameters including IP address(s), shared secret and UDP ports for Authentication and Accounting.
- Choice of End User authentication protocol

Customers may opt not to use their own RADIUS and use instead the BT provided proxy RADIUS configured on the shared Routers. This will require definition of the service features at the time of order, since these generally depend on parameters returned via RADIUS.

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. PPP is used above this physical layer and only transports IP. 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.

Standards applicable to the PSTN & Modem interface are listed in [Table 1](#).

Deleted: 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 standardised for use in the general switched telephone network (11/88)
ITU-T V.22	1200 bits per second duplex modem standardised 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 standardised 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 standardised 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](#).

Deleted: 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)
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

The IETF RFCs applicable to the PPP and IP layers for the PPP Terminated variant are contained in [Table 3](#).

Deleted: Table 3

STD 5	Internet Protocol: DARPA Internet Program Protocol, 1981
STD 51	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 (PPP Termination)

The IETF RFCs applicable to the PPP and IP layers for the L2TP Passthrough variant are contained in [Table 4](#).

Deleted: Table 4

STD 51	PPP Standard
RFC 1994	PPP Challenge Handshake Authentication Protocol (CHAP)

Table 4 PPP & IP RFCs (L2TP Passthrough)

The BT NAS will request the following LCP options appropriate to a narrow-band PPP link:-

- 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 MP4^[4] an MRRU and End Point Discriminator may be negotiated. This capability will always^v be present for ISDN connections using RFC 1618^[2].

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 RFC 1618^[2]. In all other cases the hostname is unspecified.

If the PPP session is to be terminated by BT, IPCP will commence at this point, and the End-User will be assigned an IP address from a common BT pool of addresses. If the Customer has opted for L2TP Passthrough, the PPP session will be extended to a nominated Customer LNS. The Customer may use the RADIUS protocol to determine the terminating LNS and associated optional L2TP parameters.

3.1 MP Termination

Where BT terminate the PPP session, MP is supported. If the capability for two channel MP is not ordered as part of the Customers WebPort service, where these parameters are negotiated with the client WebPort will implement the MP protocol but will only support a single link. Clients will be limited to a single link by configuration. If a Customer adjusts this limit using the RADIUS attribute Port-Limit then attempts to negotiate a 2nd link by the client may appear successful but in practice it is highly unlikely that a 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 WebPort service then where these parameters are negotiated with the client WebPort will implement the MP protocol and will allow a maximum of two PPP links. Customers may set the number of links per user; using the RADIUS attribute Port-Limit (only values of 1 or 2 are valid).

3.2 MP and L2TP Passthrough

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

The nature of the WebPort service and its geographic distribution means 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 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).

Deleted: 4

Formatted: Super

Deleted: 2

Formatted: Super

Formatted: Check grammar, Superscript

Deleted: 2

3.3 L2TP Passthrough

With the L2TP Passthrough variant, no IP layer is specified and consequently no IP related NCP is required. In this case the End User PPP session will be available at the Customer's LNS after the End-User authentication data has been captured, and consequently the specification and implementation of these protocols is open to the Customer.

Although RFC 2661^[6] 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 BT prior to implementation.

The 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. The authentication data will be forwarded as part of the L2TP tunnel request to the Customer.

L2TP tunnels will be sourced from a BT defined public IP address on each LTC, present in the RADIUS NAS-IP-Address attribute value pair.

If the Customer chooses not to run their own RADIUS server then specific L2TP tunnel details will need to be captured at the time of order and configured on the BT network. For each service instance, BT will require a single L2TP Host Name, Tunnel Password and list of one or more LNS IP addresses, which will be configured on a per service limit basis as defined on the Customer order. Calls to each service instance will be randomly distributed across the list of LNS IP addresses supplied.

4. Technical Specification for Customer Interface

Note this is not a formal BT interface, but a connection to the Internet. In summary BT WebPort will support:

- End User access to Internet provided directly from BT network
- Customer RADIUS support

The industry standards for normal connection apply, and reference should be made to the following RFCs:

RFC 2865	Remote Authentication Dial In User Service (RADIUS)
RFC 2866	RADIUS Accounting
STD 5	Internet Protocol: DARPA Internet Program Protocol, 1981
STD 13	Domain Implementation and Specification

Table 5 Customer Interface presentation (PPP Termination)

RFC 2865	Remote Authentication Dial In User Service (RADIUS)
RFC 2866	RADIUS Accounting
RFC 2867	RADIUS Accounting Modifications for Tunnel Protocol Support
RFC 2868	RADIUS Attributes for Tunnel Protocol Support
RFC 2869	RADIUS Extensions
STD 5	Internet Protocol: DARPA Internet Program Protocol, 1981
RFC 2661	Layer 2 Tunneling Protocol L2TP

Table 6 Customer Interface presentation (L2TP Passthrough)

You should be aware that transparent port 80 caching could be active on your service.

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, either in the RADIUS Access-Accept in response to a RADIUS Access-Request, or pre-configured on BTs equipment. 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^[6].

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.

5. WebPort RADIUS Attribute Support

The BT Dial Access Platform supports a number of attributes from RFC 2865^[7] and RFC 2866^[8]. Additionally RFC 2867^[9], RFC 2868^[10] and RFC 2869^[11] for L2TP Passthrough support. These are described in more detail in the following sections. Returning attributes other than those described may cause unexpected operation, including service denial, as BT may discard the unrecognised attributes from the RADIUS packets.

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

Formatted: Super

Deleted: 6

Deleted: 7

Formatted: Super

Deleted: 9

Deleted: 10

Formatted: Super

Deleted: 8

Deleted: 11

Formatted: Super

Formatted: Super

Formatted: Super

RADIUS interoperation requires a shared secret to be configured on the Customer RADIUS servers associated with the BT Proxy RADIUS servers, acting as a RADIUS client. The RADIUS server knows the client by its IP address. The RADIUS response must be returned from the same address as the request was sent to. The customer RADIUS must also reverse the UDP ports in the response. The BT platform, by default, uses UDP port 1645 for authentication and 1646 for accounting. Although this is not strictly RFC 2865 / 2866 compliant it is the accepted norm. This service is configurable and customers may request the use of port 1812 for authentication and 1813 for accounting, if they require.

The CHAP-Challenge attribute (60) is not used. Instead, the CHAP challenge is inserted into the Access-Request field in the RADIUS packet header.

The NAS-IP-Address (4) should not be used to validate the call. It is used by BT to identify the internal BT platform RADIUS client and the values it contains can change over time. Additionally BT does not use the NAS-Identifier (32). The IP addresses of the BT Proxy RADIUS servers should be used to validate the call, which will be the source address of the RADIUS packets.

The Proxy-State attribute will be present on all requests; Customers MUST include this AVP in the Access-Accept, Access-Reject, and Accounting-Response. If this is not present the message will be ignored.

There are only 2 AVPs which can be returned in an Access-Reject message, these are Proxy-State and Reply-Message.

Note: Attributes that do not appear in the following tables will be ignored.

5.1 RADIUS Attributes definition

This section describes the RFC 2865 and 2866 attributes that are used by the BT platform to communicate with the customer's RADIUS server.

Most attributes have a variable (session dependant) value.

ID	Name	Value	Comment
1	User-name	CHAP/PAP username	User ID, typically "name@domain" (Note 1)
2	User-Password	user's PAP password	As entered by End User and hidden as RFC 2865 (Note 2)
3	CHAP-Password	user's CHAP password	Optional. PPP MD5 encrypted password (Notes 2 & 3)
4	NAS-IP-Address		IP address of NAS (RADIUS client)
5	NAS-Port		Virtual port number
6	Service-Type	(2) Framed	Framed service
7	Framed-Protocol	(1) PPP	PPP framing
30	Called-Station-Id		Dialled number (DNIS)
31	Calling-Station-Id		Originators number (CLID). No leading zero. End Users may withhold.
33	Proxy-State		Indicates the request has been forwarded by a Proxy Server.
61	NAS-Port-Type	(0) Async (2) ISDN Sync (4) ISDN Async V.110	Port type (Note 4)

Table 7 Access-Request Attributes (PPP Termination & L2TP Passthrough)

ID	Name	Value	Comment
6	Service-Type	(2) Framed	Framed service (Note 5)
7	Framed-Protocol	(1) PPP	PPP framing (Note 5)
8	Framed-IP-Address		(Note 5 & 6)
11	Filter-Id		Optional (Note 7). See section 5.2.4 for guidance.
25	Class		Optional (Note 7).
27	Session-Timeout		Optional (Note 7). Maximum time in seconds before session is terminated. See section 5.2.1 for guidance.
28	Idle-Timeout		Optional (Note 7). See section 5.2.2 for guidance.
33	Proxy-State		Indicates the request has been forwarded by a Proxy Server.
62	Port-Limit	1 or 2	Optional (Note 7). Maximum number of ports that can be bundled (Note 11)

Table 8 Access-Accept Attributes (PPP Termination)

ID	Name	Value	Comment
6	Service-Type	(2) Framed	Optional (Note 7)
7	Framed-Protocol	(1) PPP	Optional (Note 7)
25	Class		Optional (Note 7)
33	Proxy-State		Indicates the request has been forwarded by a Proxy Server.
64	Tunnel-Type	(3) L2TP	
65	Tunnel-Medium-Type	(1) IPv4	
67	Tunnel-Server-Endpoint	LNS IP address	(Note 12).
69	Tunnel-Password	password	Mandatory (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 9 Access-Accept Attributes (L2TP Passthrough)

ID	Name	Value	Comment
1	User-name		User ID, typically "name@domain"
4	NAS-IP-Address		IP address of NAS (RADIUS client)
5	NAS-Port		Virtual port number
6	Service-Type	(2) Framed	Framed service
7	Framed-Protocol	(1) PPP	PPP framing
8	Framed-IP-Address		IP Address assigned to end-user. (Note 8)
25	Class		Optional. (Note 9)
30	Called-Station-Id		Dialled number (DNIS)
31	Calling-Station-Id		Originators number (CLID)
33	Proxy-State		Indicates the request has been forwarded by a Proxy Server.
40	Acct-Status-Type	(1) Start (2) Stop	Start or Stop record
41	Acct-Delay-Time		Number of seconds the HG tried to send the record.
42	<i>Acct-Input-Octets</i>		<i>Number of bytes received from user</i>
43	<i>Acct-Output-Octets</i>		<i>Number of bytes sent to user</i>
44	Acct-Session-Id		Session identifier
45	Acct-Authentic	(1) RADIUS	Authentication method
46	<i>Acct-Session-Time</i>		<i>Session duration</i>
47	<i>Acct-Input-Packets</i>		<i>Number of packets received from user</i>
48	<i>Acct-Output-Packets</i>		<i>Number of packets sent to user</i>
49	<i>Acct-Terminate-Cause</i>		<i>Optional. Session completion code. (Note 10)</i>
50	Acct-Multi-Session-Id		Optional. MP Session Identifier. (Note 11)
51	Acct-Link-Count		Optional. The number of links that have been in the bundle at this time. (Note 11)
55	Event-Timestamp		L2TP only.
61	NAS-Port-Type	(0) Async (2) ISDN Sync (4) ISDN Async V.110	Port type (Note 4)

64	Tunnel-Type	L2TP	L2TP only.
66	Tunnel-Client-Endpoint	IP address	L2TP only.
67	Tunnel-Server-Endpoint	IP address	L2TP only.
68	Acct-Tunnel-Connection	String	L2TP only.
90	Tunnel-Client-Auth-ID	Name	L2TP only.
91	Tunnel-Server-Auth-ID	Name	L2TP only.

Table 10 Accounting-Request Attributes (PPP Termination & L2TP Passthrough)

Attributes in Italics above are only present in Accounting-Request Stop packets.

Notes:

Note 1 RFC 2865 Mandatory attribute.

Note 2 RFC 2865 Mandates that either User-Password (2) or CHAP-Password (3) must be present.

Note 3 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.

Note 4 This attribute indicates the type of the physical port of the NAS. For the two channel MP WebPort service End Users that attempt to connect with a value of Async (0) should be rejected. Additionally if the two channel MP WebPort service is being used NAS-Port-Type is indeterminate for the second channel connected and a value of Virtual (5) may be sent (also see note 11).

Note 5 BT Platform required attribute - customer must return these attributes.

Note 6 Some RADIUS implementations are capable of managing IP address pools and could return a real address to be assigned to the end-user. This would require a complementary routing table in use within the BT network. Note:- BT does not support this, and service denial will result. The Access-Accept message should have the following value to support Dynamic Addressing: 255.255.255.254 to allow the NAS to select from local IP address pool.

Note 7 Optional attribute returned by customer.

Note 8 End-user assigned IP address will be present in the Accounting-Request (START) packet.

Note 9 Optional attribute, only present if associated attribute defined in the customer Access-Accept message. The BT platform will return this attribute unmodified as described in RFC 2865.

Note 10 Indicator of how the session was terminated.

Note 11 The MP protocol is supported on the WebPort platform for a single link only (this is because certain clients use this by default). For the two channel MP WebPort service either 1 or 2 links is supported.

Note 12 Only the dotted decimal notation format required in RFC 2868 is supported.

Note 13 The tunnel password is mandatory if returned via a Customer RADIUS. In the case where no Customer RADIUS is required it needs to be defined on the initial order and will be configured on the LTC.

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 RFC 2868. 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.

5.2 Additional RADIUS Attributes explanation

Further explanation is given for the following attributes to support customer defined features.

5.2.1 Session-Timeout

The BT platform is not configured with a default session timeout value. This is used to disconnect a session after a pre-set interval. Support for Session-Timeout (27) is being undertaken to allow the customer to define this on a per client basis.

For example, definition of a Session-Timeout is provided for the support of Premium Rate numbers to enable compliance to the ICSTISⁱ recommendations.

5.2.2 Idle-Timeout

The BT platform is currently configured with a default idle timeout of 20 minutes. This is used to disconnect a session if there is no traffic over the PPP link in a pre-set interval. Support for Idle-Timeout (28) is being undertaken to allow the customer to define this on a per client basis, and will override the default value.

5.2.3 DNS

There is no RFC attribute for defining a DNS server. BT provides a DNS service for customers connected to the Internet. These server addresses are delivered to the end-user as part of the IPCP negotiation.

ⁱ Independent Committee for the Supervision of Standards of Telephone Information Services

5.2.4 Filters

Cross-platform support for Filter-Id (11) is available for customers to return filters to be applied for the duration of the authenticated user's dial-in session. The RFC 2865 specification for attribute 11 is a string, used to identify a filter name. To make this feature more usable, BT has defined a structure for this attribute to allow the customer to return either:

The actual filter information (i.e. an IP Address or a range of IP Addresses to which access is permitted) is referred to below as a Dynamic Filter.

The filter structure is defined below, which details how the filter information should be defined in the customer's RADIUS server:

```
<BT-Dynamic-Filter> ::= "dyn:" <dynamic-filter>
<dynamic-filter>    ::= <ip-address> "/" <bit-mask>
<ip-address>       ::= <num256> "." <num256> "." <num256> "." <num256>
<bit-mask>        ::= <num32>
<num256>          ::= <digit> { <digit> } with range 0 to 255
<num32>           ::= <digit> { <digit> } with range 0 to 32
```

Note that "dyn:" is case insensitive.

5.2.5 Filter Examples

This section shows examples of valid filters.

Filter	Comment
Filter-Id = "dyn:1.2.3.4/32"	Legal dynamic filter
Filter-Id = "dyn:132.146.76.120/24", Filter-Id = "dyn:196.180.9.51/32"	Legal dynamic filters

5.3 Performance Techniques

RADIUS is a critical component within the overall dial service and a degree of co-operation is required to maximise efficiency. The BT platform is a shared resource supporting a number of customers simultaneously. The platform differentiates customers by dialled number. It is possible that a customer will receive authentication requests from unknown users resulting from a wrong number being dialled or a platform configuration error. Under such circumstances the server should return an Access-Reject. A silent discard is not appropriate, as the platform will attempt a retry. As the data hasn't changed nothing has been achieved except that additional processing time and data packets have been consumed. The only occasion where a silent discard is warranted is where the authenticator (shared secret) fails to match, as this may indicate an attempted hack. 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. 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 accounting data will be generated.

5.4 BT Proxy Authentication servers

BT maintains their own Proxy authentication servers, providing protection by reducing the impact of any one customer RADIUS affecting any other customers.

It is possible for a customer to choose a default action if their RADIUS is unreachable for any reason. This will be applied to an end user in response to an authentication request, and can Accept or Reject the call. A Default Accept action will only be applied if the end user has presented their CLI as part of the authentication request. This is to give additional security in any case of reported Internet abuse.

5.4.1 RADIUS Timeout Settings

For RADIUS authentication a timeout is set on the BT Proxy RADIUS when it communicates with the customer RADIUS, so that it can still perform a default action within a reasonable time even if connectivity is not possible for any reason e.g. any internet issues.

If a single customer RADIUS is supported then an initial request to the customer RADIUS will be performed, and if this times-out a single re-try will be performed. If both of these requests are unsuccessful the default action will be applied. In the case of PPP termination this can be either an access-reject or access-accept provided the dial-in user presented a CLI. In the case of L2TP Passthrough this will always be an access-reject.

If support for two customer RADIUSs is requested then an initial request to the primary customer RADIUS will be performed, and if this times-out a second request to the secondary customer RADIUS will be performed. If both of these requests are unsuccessful the customer defined default action will be applied.

5.5 Multilink Protocol Support

Where BT terminates the PPP session, if the capability for two channel MP is ordered as part of the Customers WebPort service then both channels from an End User can be bundled together as part of the PPP Multilink Protocol (MP) into a single session. The bundle interface is created using 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.

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 Session and Idle Timeouts and Filters.

MP is transparent to the BT network if L2TP Passthrough is used, as discussed in section 3.2.

6. 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/en/>

If you have enquiries relating to this document then please contact:

help@sinet.bt.com

7. References

1	RFC 1332	The PPP Internet Protocol Control Protocol (IPCP)	May-92
2	RFC 1618	PPP over ISDN	May-94
3	RFC 1877	PPP IPCP Extensions (Primary and Secondary DNS address options only)	Dec-95
4	RFC 1990	The PPP Multilink Protocol (MP)	Aug-96
5	RFC 1994	PPP Challenge Handshake Authentication Protocol (CHAP)	Aug-96
6	RFC 2661	Layer Two Tunnelling Protocol L2TP	Aug-99
7	RFC 2865	Remote Authentication Dial In User Service (RADIUS)	Jun-00
8	RFC 2866	RADIUS Accounting	Jun-00
9	RFC 2867	RADIUS Accounting Modifications for Tunnel Protocol Support	Jun-00
10	RFC 2868	RADIUS Attributes for Tunnel Protocol Support	Jun-00
11	RFC 2869	RADIUS Extensions	Jun-00
12	SIN 171	ISDN 2 Service (I.420) - Description	
13	SIN 232	BT ISDN 30 (I.421) Service - Service Description	
14	SIN 261	BT ISDN 2e and ISDN 30e (ISDN30 (I.421) using full ETSI Call Control - Service Description	
15	SIN 312	BT ISDN Services Overview	
16	SIN 350	BT Public Switched Telephone Network (PSTN): Network Tones and Announcements	
17	SIN 351	BT Public Switched Telephone Network (PSTN): Technical Characteristics Of The Single Analogue Line Interface	
18	SIN 352	BT Public Switched Telephone Network (PSTN): Technical Characteristics Of The Multi-Line Analogue Line Interface	
19	SIN 367	Characteristics of the BT Network: Electrical Safety and EMC	

20	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
21	STD 13	Domain Implementation and Specification comprising: RFC 1034 Domain names - concepts and facilities RFC 1035 Domain names - implementation and specification	Nov-87
22	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

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

8. Abbreviations

The following abbreviations have not been expanded elsewhere in this document.

Acronym	Expansion
ACCM	Async Control Character Map
ACFC	Address and Control Field Compression
ARP	Address Resolution Protocol [IETF]
AVP	Attribute Value Pair
BOOTP	Bootstrap Protocol [IETF]
CC	Corporate Customer
CHAP	Challenge Handshake Authentication Protocol [IETF]
CLID	Calling Station ID
CPE	Customer Premises Equipment
DARPA	Defence Advanced Research Project Agency [USA]
DCE	Data Circuit-terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DNIS	Dialled Number Information String
DNS	Domain Name System/Server [IETF]
DTMF	Dual Tone Multiple Frequency
EMC	Electro-Magnetic Compatibility

Acronym	Expansion
ETSI	European Telecommunications Standards Institute
HDLC	High-level Data-Link Control
HG	Home Gateway
ICSTIS	Independent Committee for the Supervision of Standards of Telephone Information Services
ID	Identity
IETF	Internet Engineering Task Force
IP	Internet Protocol [IETF]
IPCP	Internet Protocol Control Protocol [IETF]
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union - Telecommunications Standardisation Sector
Kbps	Kilo bit per second
L2TP	Layer 2 Tunneling Protocol
LAC	L2TP Access Concentrator
LCP	Link Control Protocol
LNS	L2TP Network Server
LTC	L2TP Tunnel Concentrator
MD5	Message Digest Authentication
MNP	Microcom Network Protocol
MP	Multilink Protocol
MRRU	Maximum Received Reconstructed Unit
NAS	Network Access Server
OS	Operating System
PAP	Password Authentication Protocol
PECS	Providers of Electronic Communications Services
PFC	Protocol Field Compression
PPP	Point-to-Point Protocol [IETF]
PSTN	Public Switched Telephone Network
RADIUS	Remote Authentication Dial In User Service [IETF]
RFC	Request for Comment [IETF]
SIN	Suppliers' Information Note [BT]
TCP	Transmission Control Protocol [IETF]
UDP	User Datagram Protocol [IETF]

9. History

Issue 1	3 May 2001	First Issue.
Issue 1.1	2 December 2001	Additional Premium Rate number ranges added. Inclusion of the DNS capability to enable customers to look up the DNIS used by an end user.
Issue 1.2	8 August 2002	Updated to align references as a single standalone SIN for BT WebPort.
Issue 1.3	15 October 2002	Expansion of MP single channel to include a second channel.
Issue 1.4	27 June 2003	Inclusion of L2TP tunnel passthrough option. Terminal approval requirements section removed.
Issue 1.5	13 May 2004	Tighten up definition on RADIUS port use. Editorial changes.
Issue 2.0	25 August 2005	DNIS Id feature removed.
Issue 2.1	June 2010	Text amended to reflect 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)