SIN 399

Issue 1.3
June 2010

Suppliers' Information Note

For The BT Network

BT BusinessPort
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/index.htm

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

CONTENTS

FIGURES

TABLES

Note: This product was Withdrawn From New Supply in April 2009.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 BusinessPort product.

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.

1.2 Product Outline

The BusinessPort service handles end user originated dial-in sessions, terminating the PPP layer originating from the End User client and routing 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 BusinessPort product from the rest of the BT IP network, creating a virtual private IP network for each BusinessPort instance.

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

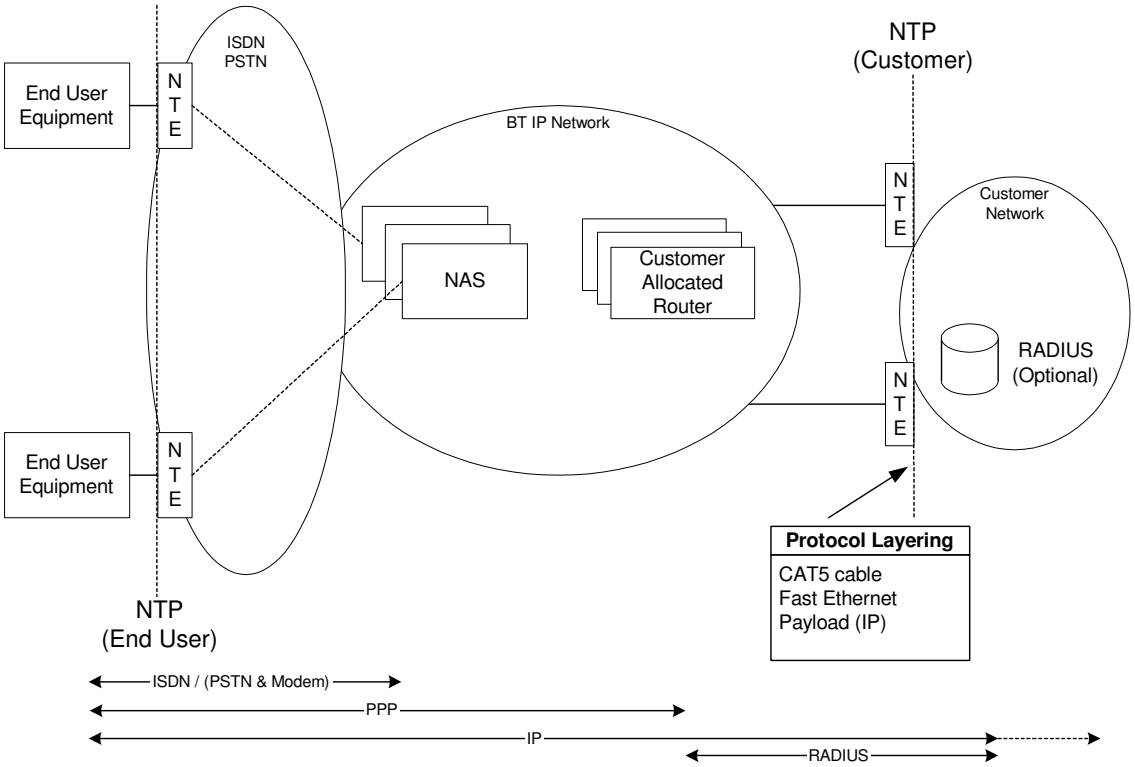

Figure 1 Basic BusinessPort architecture.

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

- IP addresses for the LAN I/F on the Customer's premises.
- 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[5].
- 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.

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 some of the BusinessPort features, since these generally depend on parameters returned via RADIUS.

2. TECHINCAL SPECIFICATION FOR END USER INTERFACE

Physical layer standards applicable to the PSTN & Modem interfaces 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
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 are contained in Table 3.

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

The BT NAS/LAC 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

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[6] an MRRU and End Point Discriminator may be negotiated. This capability will always be present for ISDN connections using RFC1618[2].

If the capability for two channel MP is not ordered as part of Customers service, where these parameters are negotiated with the client the BusinessPort service 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 BusinessPort service will implement the MP protocol and will allow 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.

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.

Once authenticated IPCP will commence.

3. TECHNICAL SPECIFICATION FOR CUSTOMER INTERFACE

This section specifies the interface options for the connection to the customer's site.

3.1 Physical Layer

There is one option for the physical layer and IP encapsulation:-

- IP over Ethernet using 100BaseT

The LAN interface 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 4 Fast Ethernet presentation

3.2 IP Layer

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]

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 considered as a suitable routing protocol option for this service.

When static routes are used, where both interfaces terminate on the same LAN, BT can provide some additional resilience using HSRP to RFC 2281[8] (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.

3.3 User IP Layer

A number of Customer Allocated Routers are dedicated to each BusinessPort 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[5]. 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,

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 service offering.

Static The IP address pre-configured on the End User CPE is used. In this case, there are some constraints with using the service to ensure that these IP Addresses can be summarised on BT's network. BT must be notified of the IP address ranges of these remote users to correctly configure the IP routing within the VPN.

Leased The IP address is assigned by the Customer RADIUS. If the same IP address is always used for this user, the same constraints apply as the static case. 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 constraints as the static case apply.

BT will provide sufficient Customer Allocated Routers to support the number of BusinessPort 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 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.

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 5 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[5].

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 disconnected. No accounting data will be generated. No Access-Reject attributes are supported.

The RADIUS client parameters required by the above are contained in Table 6.

Parameter	Default Value	Comment
Primary RADIUS authentication server IP address	None	Optional - Customer supplied
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 6 Configurable RADIUS Client Parameters

The BT BusinessPort product supports a number of attributes for authentication and accounting according to RFC2865[9] and RFC2866[10]. Returning attributes other than those described in Table 7 may cause unexpected operation.

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 1)
3	CHAP-Password	user's CHAP password	MD5 encrypted password (Note 2)
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 3)

Table 7 Access-Request Attributes

Note 1: The End-User may negotiate either PAP or CHAP as an authentication protocol. If PAP is negotiated, this attribute will be present.

Note 2: 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[9] 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 3: This attribute indicates the type of the physical port of the NAS. For the two channel MP service, End Users that attempt to connect with a value of Async (0) should be rejected. Additionally if the two channel MP 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 7. These attributes are necessary for the product to work unless shown as optional in the comment column.

No	Attribute	Value	Comment
6	Service-Type	Framed	
7	Framed-Protocol	PPP	
8	Framed-IP-Address	0xFFFFFFFE	(Note 4)
11	Filter-Id	String	Optional (Note 5) (Note 6)
22	Framed-Route	String	Optional (Note 7)
25	Class	String	Optional
27	Session-Timeout	Integer	Optional (Note 6) (Note 8)
28	Idle-Timeout	Integer	Optional (Note 6) (Note 8) (Note 9)

Table 8 Access-Accept Attributes

Note 4: 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 5: 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 6: 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 7: 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 BusinessPort internal routing protocol.

Note 8: The Integer value is the timeout in minutes.

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
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	*Acct-Input-Octets*	*integer*	
43	*Acct-Output-Octets*	*integer*	
44	Acct-Session-Id	unique string	
45	Acct-Authentic	RADIUS	
46	*Acct-Session-Time*	*integer*	
47	*Acct-Input-Packets*	*integer*	
48	*Acct-Output-Packets*	*integer*	
49	*Acct-Terminate-Cause*	*integer*	
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 3)

Table 9 Accounting-Request Attributes

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

3.5 Network Terminating Equipment (NTE)

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

For the Ethernet LAN interfaces, BT will generally use a LAN Extension Service[12][13] to provide the connection from the Customer's premises to the nearest convenient BT Point of presence.

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

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 1918	Address Allocation for Private Internets	Feb-96
6	RFC 1990	The PPP Multilink Protocol (MP)	Aug-96
7	RFC 1994	PPP Challenge Handshake Authentication Protocol (CHAP)	Aug-96
8	RFC 2281	Cisco Hot Standby Router Protocol (HSRP)	Mar-98
9	RFC 2865	Remote Authentication Dial In User Service (RADIUS)	June-00
10	RFC 2866	RADIUS Accounting	June-00
11	SIN 286	BT LAN Extension Service 155 - Service Description	
12	SIN 311	BT LAN Extension Service 100 Enhanced, Service Description.	
13	SIN 338	BT LAN Extension Service 1000 - Service Description	

7. ACRONYMS

ADM	Add-drop Multiplexer [SDH]
ARP	Address Resolution Protocol
AVP	Attribute Value Pair
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
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
LAN	Local Area Network
LCP	Link Control Protocol
LLC	Link Layer Control
MP	Multilink Protocol
MRRU	Maximum Received Reconstructed Unit
NAS	Network Access Server
NCP	Network Control Protocols
NTE	Network Termination Equipment
NTP	Network Terminating Point
PAP	Password Authentication Protocol
PC	Personal/Portable Computer
PECS	Providers of Electronic Communications Services
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]
STD	Standard (IETF)
STM-1	Synchronous Transport Module Level 1 (155 Mbit/s)
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

8. HISTORY

Issue	Date	Change History
SIN 399 1.0	13 August 2002	First Issue – new SIN for BusinessPort. The BusinessPort service was previously documented in SIN 321
SIN 399 1.1	6 November 2003	Terminal Equipment approval clause removed, information available via www.sinet.bt.com Useful Contacts page. Editorial changes.
SIN 399 1.2	18 May 2004	MP option added.
Issue 1.3	June 2010	Inserted notification of 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.