SIN 502

Issue 1.1
September 2014

Suppliers' Information Note

For The BT Network

BT IPstream Connect Session Steering

Service & Interface 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.btplc.com/sinet/
Enquiries relating to this document should be directed to: sinet.helpdesk@bt.com

CONTENTS

FIGURES

TABLES

1. Introduction

This Suppliers Information Note (SIN) provides service description information about the BT IPstream Connect Session Steering product enhancement.

2. Service Outline

2.1 Background

This SIN should be read in conjunction with SIN 482 which details BT's IPstream Connect product and SIN 496 which details IPstream Connect SID for Authentication.

2.2 Definitions

Customer: The Communications Provider (CP) or Business Customer (BC) who purchases the BT IPstream Connect service from BT and sells or provides it to End Users.

End User: The person using their PC to connect to a CP's/BC's IP network via the BT IPstream Connect service.

2.3 Service Availability

IPStream Connect Session Steering is available as an option to all customers of the IPStream Connect product who takes L2TP hand-off.

Note: At present this option is not supported for customers who take a mix of L2TP and PTA mode on the same domain.

3. Interface Descriptions

3.1 Basic BT IPstream Connect architecture

The basic architecture of the BT IPstream Connect product is as follows:

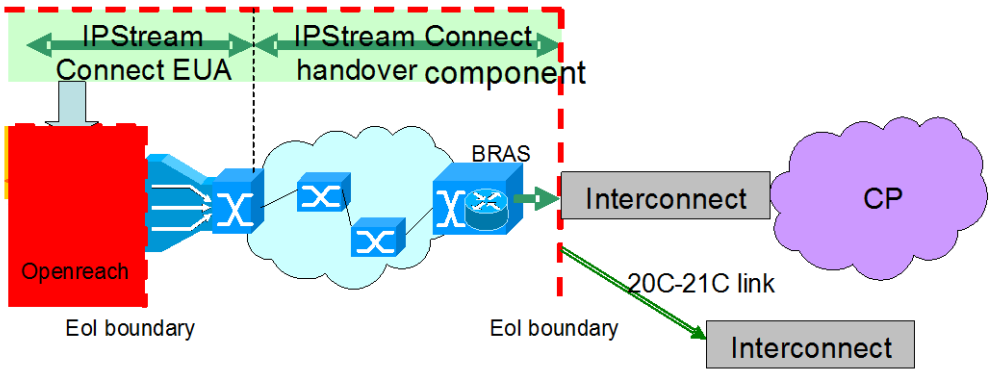

Figure 1. Basic architecture of the BT IPstream Connect product

The Session Steering capability allows a customer to control which LNS should be allocated to each end user that logs onto the service. This is achieved by sending a RADIUS authentication request from BT's RADIUS to the customer's RADIUS, allowing the

customer to respond with tunnelling parameters for the end user. These parameters are passed to the BT BRAS and used during tunnel set-up.

Session Steering is supported for L2TP Mode customers. It is not currently supported for Mixed PTA/L2TP domains.

Session Steering may be used in conjunction with SID for Authentication.

3.2 Interface specification for Session Steering

3.2.1 Background

This SIN (502) specifically addresses the BT to customer interface for Session Steering.

Session Steering requires an interface between the RADIUS servers in BT's broadband access network, and the customer's RADIUS servers. This SIN should be read in conjunction with SIN496 IPstream Connect SID for Authentication if customers are also taking that option.

Session Steering will be chosen by a CP as an optional configuration. If it is not chosen by a given customer, then the interface is not utilised by that customer. If it is chosen by a customer, then it is possible to define whether Session Steering is required for each domain for which they are responsible.

3.2.2 (Platform) Access Requests

Section 3.2.2 covers the expected format of RADIUS packets in this interface.

The attributes for Access Requests are as shown in Table 1 below. These are the same attributes as used for SID for authentication [2].

3.2.2.1 Attributes

Attribute Number	Attribute Name	Mandatory / Optional
1	User-Name	M
2[7]	User-Password	M
3[7]	CHAP-Password	M
4[1]	NAS-IP-Address	M
5[1]	NAS-Port	M
6	Service-Type	M
7	Framed-Protocol	M
26[2]	Vendor-Specific	M
32[3]	NAS-Identifier	M
33	Proxy-State	M
61	NAS-Port-Type	M
87[4]	NAS-Port-Id	M

31[5]	Calling-Station-Id	O
60[6]	CHAP-Challenge	O

Table 1. Access Request

Notes:

1. NAS-IP-Address and NAS-Port are maintained but amended for security reasons.
2. The BT RADIUS will include vendor-specific attribute 26 with Enterprise Code 594, Enterprise Tag 1 (containing '594:1:"Platform Authentication"'). The Customer RADIUS servers should recognise IPstream Connect authentication requests by checking for the specified format and values in Attribute 26.
3. According to IETF RFC2865 [3] an access request MUST contain a NAS-IP-Address (4) or a NAS-Identifier (32) or both.
4. According to IETF RFC2869 [5] an access request should contain either a NAS-Port (5) or a NAS-Port-Id (87).
5. Attribute 31, Calling-Station-Id, will be used for populating the Service ID (SID) if required. This field will take the form "FTIP<numeric>" or "BBIP<numeric>". The SID is the end user identifier used in the IPStream Connect provision, reporting and Advanced Services interfaces.
6. Attribute 60, CHAP-Challenge may be populated for requests depending on the source equipment within BT Wholesales platform.
7. Either User-Password or CHAP-Password will be supplied in the request, not both

3.2.3 Access Accept

In reply to the Access Request, the following Access Accept message attributes need to be supported by customers taking Session Steering and returned from the customer RADIUS server to the BT RADIUS server.

The session steering functionality supports multiple Tunnel-Server-Endpoints for each Access-Accept. However in order to avoid performance issues, it is strongly recommended that no more than 3 tunnel end points are returned per end user access accept.

The customer RADIUS must support tagging. All tunnelling parameters associated with a given Tunnel Server Endpoint must be tagged with the same tag number. If a CP only returns one Tunnel Server Endpoint, it must still be tagged.

3.2.3.1 Attributes for Access Accepts

Attribute Number	Attribute Name	Attribute Content	Mandatory / Optional/ Alternate
6	Service-Type	Framed	M
7	Framed-Protocol	PPP	M
25	Class	<string> to appear in all Accounting-Requests associated with the session	O
33	Proxy-State	<determined by RADIUS>	O
26	Vendor Specific Attribute	Juniper Context-Name VSA. Required for all End User Session Steering Requests. Normally set to 4874:1:"central"	M
67	Tunnel-Server-Endpoint[1]	CP LNS IP address	M
64	Tunnel-Type	L2TP	M
65	Tunnel-Medium-Type	IPv4	M
69	Tunnel-Password[2]	Password	M
82	Tunnel-Assignment-ID	String	O
83	Tunnel-Preference[3]	Preference for the associated Tunnel-End-Point	M
90	Tunnel-Client-Auth-ID[4]	String	M

Table 2. Access Accept

Notes:

1. The Tunnel-Server-Endpoint is the IP address of an LNS within the CP's network. This must be a Public IP address. IP Addresses must be in dotted decimal format as specified in RFC 2868[4].
2. Tunnel-Password must be formatted to RFC2868
3. Tunnel-Preference is mandatory. If a CP has a preference, the Tunnel Server Endpoint with the lowest preference value (e.g. 1) will be given first preference. If a CP doesn't wish to specify a preference, the same value should be used for all Tunnel Server Endpoints.
4. The Tunnel-Client-Auth-ID's returned by a CP may be different for each response; however they must be the same for all tunnels that are destined for a given Tunnel Server Endpoint IP Address.

5. Any tunnelling parameters received other than those listed in the table above will be filtered out by BT RADIUS.
6. For SID for Authentication, without sessions steering, Framed-Route or Framed-IP-Address must be returned. For Session Steering, these parameters need not be sent to drive tunnelling of the session. If they are sent, they will be ignored by BT RADIUS.

3.2.4 Access Reject

In the event that the end user is denied service, an Access Reject message is returned by the customer RADIUS. The proxy-state attribute may be returned in the Access Reject message. No other attributes are required. This is the same mechanism as used for SID for Authentication.

3.3 Turning on/off Session Steering

Provision has been made within the BT systems for configuring Session Steering on/off on a domain basis. To turn on/off Session Steering for a domain, a CRF will be submitted by the CP. These changes become operational when the BT RADIUS servers next perform a reload of configuration data. Changes to Session Steering may therefore not become operational until the next day due to the frequency of data updates on the Broadband platform.

3.4 Routing options

The customer will specify the authentication routes (Primary/Secondary/Tertiary) to the customer's RADIUS on the CRF when ordering IPstream Connect. The customer will include data such as the IP address of the customer RADIUS, the shared secret to be used to authenticate the communications between the customer RADIUS and the BT RADIUS and the ports to be used for authentication traffic (normally port 1645; alternatively 1812). If the customer takes both Session Steering and SID for Authentication, the RADIUS details will be common for the 2 product elements.

The BT RADIUS will allow 7 seconds for the customer RADIUS to respond before timing out. This time limit also applies to multiple destinations. Re-tries must be within this overall limit which if not met will result in the access server timing out and authentication failing.

For RADIUS traffic between the BT RADIUS and customer RADIUS servers, both the destination and source address will be translated, using NAT capabilities, within the IPstream Connect handover network. RADIUS NAT IP addresses are allocated to each IPstream Connect handover site by BT.

The BT RADIUS will use the translated IP addresses

1) for the customer RADIUS traffic to achieve load balancing of external RADIUS traffic across a number of IPstream Connect Handover Nodes. The BT RADIUS will use an algorithm to balance RADIUS traffic across a number of handover nodes that have been chosen by the CP.

2) As the source address to ensure that packets are routed back from the customer to BT via the chosen IPstream Connect handover node which will assist BT in tracing potential faults. BT will provide the NAT IP addresses to the customer once an order has been submitted. BT will advertise the BT RADIUS Source Addresses via BGP at the CP's chosen sites for receiving RADIUS traffic.

3.5 CP RADIUS failure

If the CP RADIUS cannot be reached by the BT RADIUS, it will not be possible to receive the session steering information. In this scenario, the BT RADIUS will revert to standard allocation of sessions to tunnel end points and continue to allow End Users to access the service. For this scenario the CP must provide L2TP-Client-Auth-Id and Tunnel-Password, along with a valid list of Tunnel-End-Points, and they will be used in the event of a CP RADIUS failure.

Note: Session Steering is not compatible with the SID for Authentication option of rejecting end user sessions if the CP RADIUS cannot be reached.

4. References

[1]	SIN 482	BT IPstream Connect
[2]	SIN 496	BT IPstream Connect SID for Authentication
[3]	RFC2865	Remote Authentication Dial In User Service (RADIUS)
[4]	RFC2868	RADIUS attributes for Tunnel Protocol Support
[5]	RFC2869	RADIUS Extensions

BT Suppliers' Information Notes may be obtained from our www site at:

http://www.btplc.com/sinet/

5. Abbreviations

Acronym	Expansions
BC	Business Customer
BGP	Border Gateway Protocol
BRAS	Broadband Remote Access Server
BT	British Telecommunications plc
BTW	BT Wholesale
CHAP	Challenge Handshake Authentication Protocol
CRF	Customer Requirements Form
CP	Communications Provider
IETF	Internet Engineering Task Force
IP	Internet Protocol
L2TP	Layer 2 Tunnelling Protocol
NAS	Network Access Server
NAT	Network Address Translation

Acronym	Expansions
OSS	Operation Support System
PC	Personal Computer
PPP	Point-to-Point Protocol
PTA	PPP Termination and Aggregation
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comment
SID	Service Identifier
SIN	Suppliers' Information Note
VSA	Vendor Specific Attribute

6. History

Issue	Date	Changes
Issue 1.0	May 2011	First published as a SIN, and replaces STIN 502.
Issue 1.1	September 2014	Change SINet site references from http://www.sinet.bt.com to http://www.btplc.com/sinet/

-END-