SIN 496

Issue 1.2

September 2015

Suppliers' Information Note

For The BT Network

BT IPstream Connect SID for Authentication

Service & Interface Description

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 Supplier's Information Note (SIN) 496 provides technical information on the BT IPstream Connect 'SID for Authentication' enhancement.

IPstream Connect SID for Accounting technical information is contained in SIN497.

2. Service Outline

2.1 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.

2.2 Background

This SIN should be read in conjunction with SIN 482 which details BT's IPstream Connect product and SIN 497 which details IPstream Connect SID for Accounting.

2.3 Service Availability and Tariffs

IPStream Connect SID for Authentication is available as an option to all customers of the IPStream Connect product.

3. Interface Descriptions

3.1 Basic BT IPstream Connect architecture

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

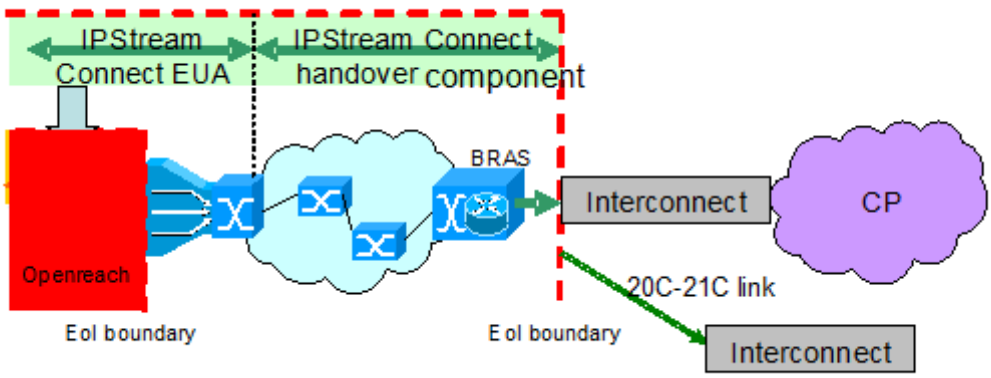

Figure 1. Basic architecture of the BT IPstream Connect product

The 'SID for Authentication' capability allows a customer to verify that an end user access request has originated from the same connection that was configured during service provision. This is achieved by supplying the SID in the authentication request sent to the customer's RADIUS, allowing the customer to compare this with the SID they were provided during end user provision.

The format of the SID is currently the prefix 'BBIP' or 'FTIP' followed respectively by an 8 or 9 digit string i.e. BBIPnnnnnnnn or FTIPnnnnnnnnn.

SID for Authentication is supported for PTA Mode, L2TP Mode and Mixed PTA/L2TP domains.

3.2 Interface specification for 'SID for Authentication'

3.2.1 Background

This SIN (496) specifically addresses the BT to customer interface for authentication data.

'SID for Authentication' requires an interface between the Platform RADIUS servers in BT's broadband access network, and the customer's RADIUS servers. To be read in conjunction with SIN497 IPstream Connect SID for Accounting if customers have taken this option.

Customers may wish to compare the end user SID, username and password from the SID authentication with the username and password from their own Home Gateway authentication.

SID notification in Authentication requests will be an optional configuration. If it is not chosen by a given customer, then the interface is not utilised by that customer. Depending

on which service option a given customer has chosen (L2TP or PTA), different attributes will pertain in authentication requests and accepts.

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

Note: The IPstream Connect SID service does not allow the use of both types of delimiter at the same time for the Domain, i.e. the @ or the / delimiter. The delimiter is the separator between the username and Domain. If you are using both types of delimiter for the Domain, you will not be able to have the SID service. When requesting the SID service, BT will assume you are using the @ delimiter, if you are using the / delimiter please add this to the notes.

3.2.2 (Platform) Access Requests

The attributes for Access Requests are as shown in Table 1 below.

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 Platform 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 an access request MUST contain a NAS-IP-Address (4) or a NAS-Identifier (32) or both.
4. According to IETF RFC2869 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). 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, having authenticated the end-user details, the following Access Accept message attributes need to be supported by customers for tunnelled/non-tunnelled users and returned from the customer RADIUS server to the BT platform RADIUS server.

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
8[1]	Framed-IP-Address	IP address to be used by the end-user	A
11	Filter-Id	Static or Dynamic	O
22[1]	Framed-Route	Used for No_NAT routing updates	A
25	Class	<string> to appear in all Accounting-Requests associated with the session	O
27	Session-Timeout	Minimum supported 7200 seconds	O
28	Idle-Timeout	Minimum Supported 7200 seconds	O
33	Proxy-State	<determined by RADIUS>	O

Table 2. Access Accept for normal traffic

1. If the response is for L2TP termination, the customer needs to return either a Framed-IP-Address or a Framed-Route in the Access Accept in response to the BT Platform RADIUS authentication request. The value of the attribute is not used - the end users PPP session will be tunnelled to a pre-defined tunnel end point associated with the service selection name presented by the end user during the PPP session setup attempt. If the response is for PTA Mode termination, the Framed-Route and Framed-IP-Address must not be populated – the end user's PPP session will be terminated within BTW's network and assigned an IP address at random from the pool of IP addresses provided by the CP to BTW for this purpose.

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.

3.3 Turning on/off SID Authentication

Provision has been made within the BT OSS for configuring SID Authentication on/off on a domain basis. To turn on/off SID Authentication for a domain, a CRF will be submitted by the CP. These changes become operational when the BT platform RADIUS servers next perform a reload of configuration data. Changes to SID Authentication 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 platform RADIUS and the ports to be used for authentication traffic (normally port 1645; alternatively 1812).

The time that the BT platform RADIUS will allow the customer RADIUS to respond before timing out is 7 seconds. Multiple destinations and re-tries must be within this overall limit otherwise the access server will timeout and authentication will fail.

For RADIUS traffic between the BT Platform and customer RADIUS servers, both the destination and source address will be NAT'd within the IPstream Connect handover network.

The BT RADIUS will use NAT'ed IP addresses for the customer RADIUS to achieve load balancing of external RADIUS traffic across a number of IPstream Connect Handover Nodes. The platform BT RADIUS will use a round-robin algorithm to balance RADIUS traffic across a number of handover nodes.

For Authentication, NAT'ing of the source address ensures that packets are routed back from the customer to BT via the chosen IPstream Connect handover node which assists BT in tracing potential faults. RADIUS NAT addresses are allocated to each IPstream Connect handover site by BT. BT will provide the 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.

4. References

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
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

6. History

Issue	Date	Changes
Issue 1.0	August 2009	New document providing detail on IPstream Connect SID for Authentication to supplement SIN482
Issue 1.1	November 2009	Section 3.2.4 - Modified to reflect that the proxy-state attribute may be included in the access reject.
Issue 1.2	September 2015	TAP2 Performacne Tester information removed from section 3.3 as TAP2 test on Performance Tester is no longer available Change SINet site references from http://www.sinet.bt.com to http://www.btplc.com/sinet/

-END-