PTC 229

Specification for Customer Equipment connecting to Spark New Zealand Voice Connect SIP Trunking network

Access Standards

Spark New Zealand Limited

Wellington

NEW ZEALAND

March 2018 issue 3

Table of contents

References

Standard	Description
RFC 791	Internet Protocol (IPv4)
RFC 2327	SDP: Session Description Protocol
RFC 2782	A DNS RR for specifying the location of services (DNS SRV)
RFC 2833	(Obsolete) RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals. RFC 2833 is Spark's preferred method for transporting DTMF tones. The customer endpoints should be able to handle in-band if RFC 2833 is not supported (by the PBX and/or the far end).
RFC 3261	SIP: Session Initiation Protocol The transport methods supported are UDP (RFC 768) and TCP (RFC 793). UDP is Spark's preferred transport method. The PBX-specific agreed transport method (i.e. UDP or TCP) shall apply in both directions between the PBX and the service.

RFC 3262	Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
RFC 3263	Session Initiation Protocol (SIP): Locating SIP Servers
RFC 3264	An Offer/Answer Model with Session Description Protocol (SDP)
RFC 3311	The Session Initiation Protocol (SIP) UPDATE Method
RFC 3515	The Session Initiation Protocol (SIP) Refer Method
RFC 3550	RTP: A Transport Protocol for Real-Time Applications
RFC 3891	"Replaces" Header.
RFC 3892	Referred-By Mechanism.
RFC 3960	Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)
RFC 4028	Session Timers in the Session Initiation Protocol (SIP)
RFC 4244	An Extension to the Session Initiation Protocol (SIP) for Request History Information
RFC 4566	SDP: Session Description Protocol (obsoletes RFC 2327)
RFC 4629	RTP Payload Format for ITU-T Rec. H.263 Video
RFC 4904	Representing Trunk Groups in tel/sip Uniform Resource Identifiers (URIs)
RFC 5806	Diversion Indication in SIP (network accepts does not send)
ITU G.168	Echo cancellation
SIPconnect 1.1	SIP-PBX/Service Provider Interoperability (SIP Forum)
PTC 220	Requirements for private network equipment for connection to Spark voice networks
Voice Connect PBX Interface Guide v2.5	Interface Guide for VC service

The grant of a Telepermit for any item of terminal equipment indicates only that Spark New Zealand has accepted that the item complies with minimum conditions for connection to its network. It indicates no endorsement of the product by Spark New Zealand, nor does it provide any sort of warranty. Above all, it provides no assurance that any item will work correctly in all respects with another item of Telepermitted equipment of a different make or model, nor does it imply that any product is compatible with all of Spark New Zealand's network services

1 Introduction

1.1 Document Purpose

The purpose of this document is to describe the Spark SIP Trunking "Voice Connect" service and to list the tests required for PTC purposes. As interfacing with this service is largely a matter of customer equipment configuration rather than physical or electrical characteristics, most of this specification is dedicated to describing the details of this particular implementation of the SIP protocol. It does not cover the requirements for transmission planning or interfaces to analogue telephones. These are covered by PTC 220.

1.2 Product Description

Voice Connect (VC) is a Session Initiated Protocol (SIP) enabled service also known as SIP Trunking that supports Voice over IP (VoIP) Telephony.
Voice Connect delivers high quality voice service over a single access circuit to an on premise IP-PBX systems.
Voice Connect is an alternative to traditional ISDN PRA access that provides features and benefits above and beyond what is delivered by ISDN.
The Voice Connect service consists of the following:

- Fibre or copper access delivered from the Spark Voice Connect Network using HSNS or UFB circuits provided by Chorus or other access provider
- VLAN bandwidth to meet the customer's channels requirement.
- CLNE, the client side Ethernet port being the demarcation point between Spark's network and the customer's network.
- IP addressing. The Voice Connect service supports both public and private customer IP addressing. NAT is enabled on the CLNE for standard VC implementation.
- Telephone numbers which can either be Migrated Telephone Numbers or number range of Greenfields Telephone Numbers. These may be:
  - Standard telephone numbers that can receive simultaneous calls
  - Telephone numbers capable of DDI.
- Network delivered features

1.3 Power Outages and Availability of Emergency Call Services

Emergency 111 calls will not be able to be made in the event of a service outage, power failure or disruption. The Client MUST maintain additional means to enable emergency service calling.

1.4 PTC Certification (Telepermit)

This specification covers the requirements which a PBX must meet to achieve basic compatibility with the Spark Voice Connect service.
In additions to this specification, the equipment must also comply with electrical safety (AS/NZS 60950) and EMC (AS/NZS CISPR 22) requirements, and the appropriate rf specifications for any wireless interfaces such as WiFi or DECT. Where the PBX has analogue extension phone ports these must also be tested against the appropriate clauses of PTC 220. This also applies to any other network interfaces such as analogue or IDSN trunks

- *See http://www.telepermit.co.nz/certification_process.html for details on the Telepermit Application process.*

2 Voice Connect Overview

The diagram below illustrates a high level network centric view of the Spark SIP Trunking solution.

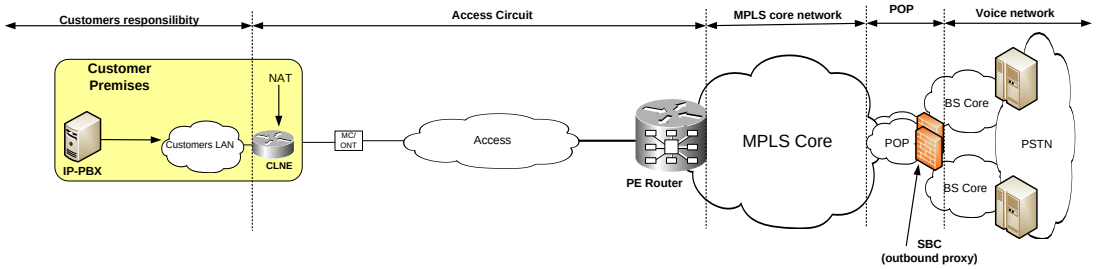


Fig.1 Voice Connect service boundaries

Media Converter (MC) or Optical Network Terminal (ONT) is provided by the Local Fibre Company (LFC) as a part of the access circuit and installed on the customer premises. For Copper High Speed Network Service (HSNS) the Media Converter is not required as it is included in the CLNE.

2.1 VC Service Interface Reference Architecture

The diagram below shows the functional elements required to support the interface described in this document.

The diagram shows two points of interconnect:

- SIP signalling messages to support voice services between the Enterprise Network SIP-PBX and the Spark network.
- The RTP and RTCP packets between the Spark and Enterprise Media Endpoints.

An Enterprise Media Endpoint could be contained within a physical SIP-PBX, an IWF, an IP-based user device (e.g., SIP phone) in the Enterprise, or a media-relay device in the Enterprise Network.

The Spark Media Endpoint is signalled using SIP and is typically a session border controller (SBC)

The two interfaces together comprise together Voice Connect service interface.

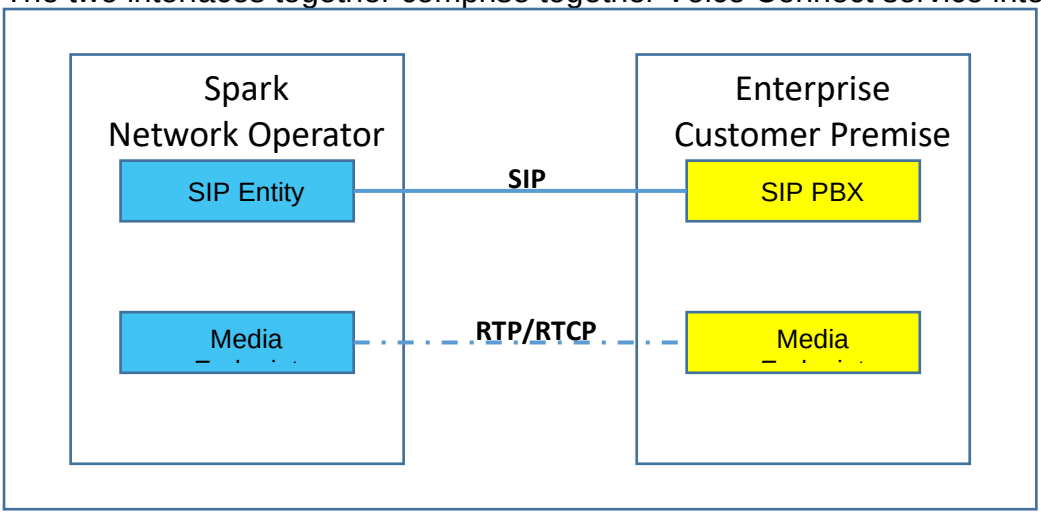


Fig.2 Voice Connect interfaces

2.2 Service Definitions

2.2.1 Trunk User

The Trunk User is the common type of user and refers to a user that has a public DDI assigned to their user profile.
The Trunk User cannot be the SIP AOR (Address-of-Record), it cannot REGISTER.

2.2.2 Pilot User

Each Trunk Group must have a single unique user that REGISTERs with the VC service; the Pilot User is used for Trunk Group Identification (TGI) and its AOR acts as the location information on where to send messages intended for the Trunk Group. The Pilot User is typically configured at the Trunk Group initiation time where one of the DDI's is selected to act as the Pilot User for the new Trunk Group.

2.2.3 Redirecting User

A redirection call must have a redirecting user which is a known subscriber to Voice Connect with its own service profile; it is the service profile of this user that will be applied to the redirected call where the redirection header URI is a match. A Redirecting User must be either a Pilot User or a Trunk User.

2.2.4 Caller ID Presentation User

Each call attempt received from a PBX is evaluated to consider the user identity that will be presented to the destination. If a call has no suitable identity then it will fall back to using the Pilot user identity. For redirecting calls if the identity in the from header is not a Trunk or Pilot User it may still be used as the Caller ID.
In the case of redirection:

- in-dialog - integrity checks will have been performed on the identity on the initial originating call leg and therefore for in-dialog A party pass through is available for all calls.
- out of dialog – where the initial call leg came from Voice Connect and the PBX is redirecting the call back to Voice Connect then the From header will be used as the caller ID if the user part of the URI matches exactly, the host part of the URI may be 'telecom.co.nz' or simply have the parameter 'user=phone' to effectively ignore the host part of the UURI matching logic. Other user identification headers such as PAI, PPI, RPID cannot be present for the A party to be passed through. Where the initial call came from a source other than the voice connect enterprise that the redirected call is presented, meaning that the integrity of the caller ID cannot be confirmed and to avoid upstream spoofing concerns the Trunk Group Pilot user identity will be used instead.

2.2.5 In-Dialog

The in-dialog PBX redirection scenario typically begins with Voice Connect sending an INVITE request to the PBX for a new call. The call processing on the PBX results in the PBX redirecting the call back through Voice Connect. In the specific case of an in-dialog PBX deflection, the PBX sends Voice Connect a SIP message in the same dialog as the original INVITE request.

The two in-dialog redirection types available can be thought as an update to the original INVITE request (REFER) or a response to the original INVITE (3xx).

Example 1: If the call is unanswered, which means the PBX has not yet sent a final response to the INVITE request, the PBX may send a 3xx response to indicate that Voice Connect should deflect the call based on the contact header.

Example 2: If the call is answered, then the PBX sends a REFER request – again, in the same dialog as the original INVITE request.

Note for the example use cases of a 302 response is a Call Forwarding scenario, while the REFER request is a Call Transfer.

An in-dialog deflection or recursion does not require Voice Connect to identify the trunk group being used as this was established on the original INVITE that created the dialog.

2.2.6 Out-of-Dialog

Definition: An out-of-dialog PBX redirection is defined as an initial INVITE coming from a PBX endpoint to Voice Connect with a Diversion or History-Info header.

In the out-of-dialog PBX redirection scenario, the PBX sends Voice Connect a new INVITE request to establish a new call leg for the redirection.
Usually, Voice Connect would interpret a new INVITE request from the PBX as a new originating call. In the PBX deflection scenario, however, Voice Connect interprets the new INVITE request as a redirection. To achieve this interpretation, the PBX must add the required redirection information to the INVITE request in a History-Info header (preferred) or a Diversion header.

An out-of-dialog redirection requires Voice Connect to successfully identify the Trunk Group using an AOR.

Voice Connect does not support an Out-of-Dialog REFER method.

2.3 PBX Types

The BroadSoft platform uses a concept of dividing PBX's into various types:
Type A – SIP Registering PBX
Type B – SIP Non-registering PBX
Type C - Registering PBX with modified Request-URI Header
Type D – Non-registering PBX with modified Request-URI Header
Type E - Device Addressing PBX
Type F – Subscriber Registering PBX
Only Type A PBX are supported natively with all other types requiring some interworking function (IWF) to present the PBX as Type A to the CLNE.

It is important to note that where a PBX Type A does not bridge the media through its IP address then it also will need to deploy an IWF. This is not seen as a concern as most small PBXes will bridge the media, while customers with larger PBXes will often deploy a security device between the Voice Connect CLNE and their local environment. In this case the IWF is in essence a SBC type device and therefore doubles up as inter-working and security border device.

The service demarcation stops at the client side Ethernet port of the CLNE and there is no SIP signalling phone interaction with the Voice Connect service instead the PBX or the IWF will be the originating/terminating point for l signalling streams. It is the PBX/IWF and where necessary the customer switching and routing devices responsibility to ensure that the signalling and media is correctly passed on to the SIP endpoint (handset).

2.4 Interworking Function (IWF)

The IWF is in essence a SBC type device and therefore doubles up as inter-working and security border device. The following diagram shows the location of the IWF within the solution.

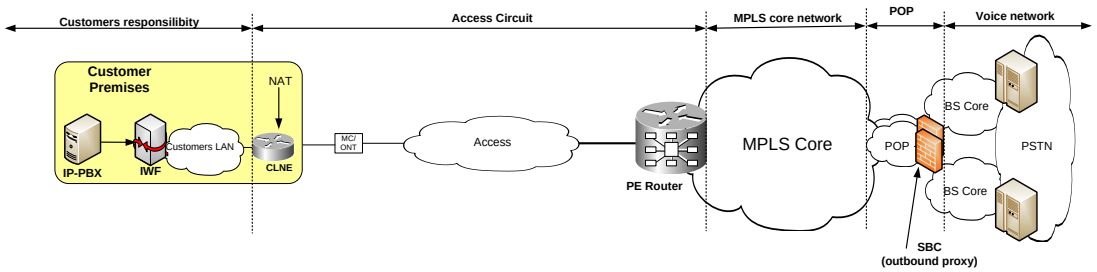


Fig.3 Voice Connect with IWF deployment

In some implementations the IWF can also be where a small PBX function is provided and PRA for use in different failure events.

2.5 IWF for MS Lync

Microsoft Lync cannot directly operate with Spark Voice Connect and requires an IWF device to provide interoperability. Spark provides Lync Trunk service by installing a Sonus gateway as an IWF device. This is beyond the scope of this specification, but Spark Digital can assist in the deployment of Microsoft Lync systems.

2.6 SIPConnect

The SIPconnect Technical Recommendation is an industry-wide, standards-based approach to direct IP peering between SIP-enabled IP PBXs and VoIP service provider networks.
Voice Connect is based upon the SIPconnect 1.1 standard. SIPconnect is a set of guidelines and recommendations that have come out of a multi vendor working party of the SIP Implementers forum.

2.7 Call Progress Tones

Call progress tones should be provided by the PBX in the first instance to the New Zealand standard. This includes tones as dial tone and busy tone. PSTN tones and announcements will still be delivered by the PSTN or BroadWorks as applicable.
On receipt of Session Description Protocol (SDP) information in 183 Session Progress SIP message the PBX must immediately disable any locally generated call progress tones and cut-through the early media to the end-user.
DTMF tones are supported by RFC 2833 and clear channel (RFC2833 is the preferred choice)
Echo Control is required. 64mS G.168 echo cancellers would be sufficient to eliminate any hybrid imbalance & handset conduction.

The mapping of SIP Status codes to NZ Standard Tones is given in the following table:

Incoming SIP Status Code	**Release Cause**	**Recommended Tone generated by CPE**
404 Note: **410, 484 & 604** mapped to 404:	USER_NOT_FOUND	Number Unobtainable Tone
413 Note: 413 is mapped to 404	TRANSLATION_FAILURE	Number Unobtainable Tone
486 Note: **600** is mapped to 486	BUSY	Busy Tone
480 Note: **401, 407 & 606** mapped to 480	TEMPORARILY_UNAVAILABLE	Disconnect Tone

403, 603 Note: these codes mapped to 480	FORBIDDEN	Disconnect Tone
408 Note This code mapped to 480	REQUEST_TIMEOUT	Disconnect Tone
400, 402,405, 406, 409, 411, 414, 415, 420, 422, 481, 482, 483,485, 487, 488 and all other 4XX codes not listed above. Note: These codes mapped to 480	REQUEST_FAILURE	Disconnect Tone
All 5xx	SERVER_FAILURE	Disconnect Tone
All other 6xx not listed above	GLOBAL_FAILURE	Disconnect Tone

The standard New Zealand tones are given in the table below:

Tone Name	Abbreviation	Frequency	Level(dBm0)	Cadence	Timeout
Dial Tone	DT	400 Hz	-9 dBm0	Continuous	-
Busy Tone	BT	400 Hz	-9 dBm0	500 ms ON 500 ms OFF Repeated	45 seconds
Disconnect Tone (also known as Congestion Tone)	DSCT	400 Hz	-9 dBm0	250 ms ON 250 ms OFF Repeated	45 seconds
Number Unobtainable Tone	NUT	400 Hz	-9 dBm0	75 ms ON 100 ms OFF 75 ms ON 100 ms OFF 75 ms ON 100 ms OFF 75 ms ON 400 ms OFF Repeated	45 seconds
Ring Back Tone (also known as Ringing Tone)	RBT	400 Hz + 450 Hz	-12 dBm0	400 ms ON 200 ms OFF 400 ms ON 2.0 sec OFF Repeated until timeout unless call answered, abandoned, or other timeout. Then Busy Tone	300 seconds followed by Busy Tone

The level of the tones is given in dBm0 which is the level at the Transmission Reference Point (TRP). In most cases this will be attenuated by attenuation PADs at an analogue interface. Details

of these PADs as part of the Transmission Plan are given in PTC 220 section 4 with specific requirements for an analogue port given in section 5. Typically for an analogue port intended for connection to a phone via a short line (< 2km), the PAD value will be 8.5 dB loss. For a long line (>2 km) the PAD value will be 6 dB loss. These loss PADs must be added to the values given in the table above to give the level as measured in dBm at the port.

2.9 Access Network Number Formats

In Voice Connect the CLNE is not configured as a SIP aware gateway and cannot reformat the SIP messages, thus the PBX must not present the leading digits as a prefix to the CLNE as the CLNE is not capable of removing it.
The PBX must send the number as dialled excluding any offnet access numbers. The BroadWorks core is configured to understand the national (0) and international (00, “+”) access codes and will correctly process 7 digit local, 0+AC + LMN and 00+CC + AC + LMN number formats.

Extension Digit String Limitations
The following digit strings are not permitted on BroadSoft as PBX extensions:

- 1X.
- 1XX
- 1XXX
- 1XXXX
- 1XXXXX
- 911
- 999.

Voice Connect sends numbers in national format only toward the PBX.

3 COMMON INTERWORKING SPECIFICATION

3.1 SIP Related

3.1.1 SIP Server Discovery

The Voice Connect service supports SRV RR and A RR DNS queries; it does not currently support NAPTR or AAAA RR queries.
The IWF or the PBX must be configured to direct SIP traffic to the BroadSoft trunk group domain or IP address.

3.1.2 DNS

DNS services for Voice Connect are provided from the following, although any public aware DNS server may be used for Voice Connect SRV and A record lookup:

- 122.56.237.1
- 210.55.111.1

3.1.3 Outbound Proxy

Voice Connect only supports PBXs and IWF that support the use of an Outbound Proxy.
Set the outbound proxy address to the address of the Spark edge SBC that provides the Voice Connect service. This is normally a FQDN but could be set to an IP address if no DNS involvement is required.

3.1.4 URI format

The Voice Connect service supports the SIP URI format as opposed to the Tel URI.
The Address of Record number format to be presented by the PBX to the network is national number without the leading zero, and no intermediary spaces or dashes.
For example an Auckland number of 09 123 4567 if used as an Address of Record would become 91234567

3.1.5 PBX Redirection Handling

An IP PBX may handle call redirections within the PBX in a variety of ways. For example, a call comes through the Voice Connect trunk group to a subscriber in the PBX. The PBX subscriber has the Call Forwarding service enabled in the PBX. The call is subsequently forwarded by the PBX back to the PSTN through the Voice Connect trunk group.

- The IP PBX may handle the forward by sending an INVITE on a new dialog with the request-URI containing the forward destination and a Diversion or History-Info header containing the PBX subscriber identity.
- The IP PBX or IWF may look to the Network to handle the redirection by sending a REFER with the refer-to header containing the forward destination and the referred-by header containing the PBX subscriber identity.

3.1.6 Network Redirection Handling

The network supports both the History-info and the Diversion header as information headers for calls where they are forwarded to the PBX to inform the PBX that the call has been previously diverted.
Call forwards and Transfer features can be statically configured in the network (as opposed to dynamically upon a call request) and will be triggered typically by a specific event occurring, as this reduces the access bandwidth from being consumed this may be useful for customers that wish to forward calls to alternative destinations that are reached via the network service.

3.1.7 Pilot Number Registration

The IWF device or PBX must be configured to direct SIP registrations to the BroadSoft trunk group domain. Only the trunk pilot number is configured to register.
The username must match the pilot user that has been agreed at both the customer and the network end for each Trunk Group.
The inclusion of a P-Asserted identity (PAI) header is ignored and is not required for a successful registration.
Voice Connect uses the contact from the Trunk Pilot (aka parent) registration for all terminations through the Trunk Group to the IP PBX or IWF.

3.1.8 Authentication

The Pilot user registration from the customer is authenticated for each Trunk Group provisioned.
The INVITE messages presented to the network by the customer will be challenged and authenticated
The REFER messages presented to the network by the customer will be challenged and authenticated.
The INVITE messages presented to the customer by the network MUST not be challenged for authentication.
The UPDATE messages presented to the network by the customer that have either a contact change or a session change will be challenged and need to be authenticated.
The authentication settings for the gateway must match the BroadWorks trunk group authentication settings.
Other SIP methods in both directions will not be authenticated.

The voice connect service does not authenticate responses and does not generate the Authentication-Info: header to allow responses to be authenticated.

In the event that the voice connect service receives a request with an expected Authorization realm and rejects the request because of an authentication failure, then the network sends a 403 response instead of a 401 response.

A series of authentication failures can cause the network to “lock out” a trunk group. When the device endpoint is locked out, the network immediately sends a 403 response, without attempting to authenticate the request. Because the 403 response may be sent for numerous reasons, the network sets the status-line reason-phrase to provide additional information about the authentication failure and the lockout status of the device endpoint:

- “403 Authentication Failure” indicates that the request failed authentication.
- “403 Authentication Failure Lockout” indicates that the request failed authentication and caused a lockout of the trunk group.
- “403 Locked Out” indicates that the request failed because the device endpoint or trunk group is locked out.
- “403 Authentication Loop” indicates that the request failed because the network considered it part of an authentication loop.

NOTE: The username/password for ‘authentication’ and PBX pilot user/ number ‘credentials’ will normally be the same.

3.1.9 Call Failure Treatment

SIP responses specify a three-digit integer response code, which is one of a number of defined codes that detail the status of the request. The Spark network sends the appropriate status code back to the PBX for local processing (see tables on pages 10-11).

Spark recommend that customers follow the common practise of PBX call processing and map the SIP status calls within the PBX to suit their users.

3.1.10 Child INVITE to Network

A PBX or Trunking device will REGISTER a pilot user for each trunk provisioned to the network.
A child is a subscriber of the PBX that is not registered directly with the network and instead utilises the Parent (Trunk Group Pilot) registration.
An unscreened call is one where the trunk group has been successfully identified but the user identity in the FROM header is unknown to the network in this case the network will use the services and Caller-ID assigned to the pilot user.

In both the child and the unscreened case if a PAI of a Pilot User is not provided the call will fail due to the trunk Group identity not being established. See section 5.2 for details.
The network tries to find an originating trunk and an originating user for every call presented.
An example cut down INVITE message from a child subscriber is shown below:

```
INVITE sip: 041231234@outbound.proxy.example.co.nz:5060;user=phone
SIP/2.0
From: "Joe Soap"<sip:1020@example.co.nz;user=phone>;tag=123456789-
9876543210-
To: "Fred Blogs"<sip:041231234@200.200.200.200:5060>
CSeq: 3 INVITE
Contact: <sip: 1020@10.65.1.100:5060;transport=udp>
P-Asserted-Identity: sip:412310005@example.co.nz
```

The user “Joe Soap” with extension 1020 is calling “Fred Blogs” on 041231234
The Trunk Group in this example is identified by the PAI (P-Asserted-Identity) header as a SIP URI of sip:412310005@example.co.nz
The network will check for the directory number 1020 if this is not known on this Enterprise then the call will be treated as an unscreened call.

3.2 SIP Methods & Headers

3.2.1 OPTIONS Method

The SIP method OPTIONS is often used for a device to ascertain reachability of an upstream element. Voice Connect supports the ability to respond to devices that send a SIP OPTIONS ping request and this will be responded to by the SBC's acting as outbound proxies for the Voice Connect service.

It is recommended the frequency of the SIP OPTIONS ping requests are kept to a sensible level as these messages are counted towards the total messages from a customer.
As part of DOS protection thresholds are set which prevents a malicious or misbehaving device from denying service to all customers, this works by dropping SIP messages when an entity has exceeded a preset threshold and can result in requests for calls (INVITES) being dropped until the number of messages has stabilised under the DOS thresholds.
A single SIP OPTIONS ping every minute or so would be a sensible approach. A SIP OPTIONS ping more frequently would not be considered sensible nor would one for every call presented.

Customers must support receiving the OPTIONS method. The PBX/IWF must provide a SIP response to the OPTIONS method.

Note that Voice Connect does not include SDP capabilities in the OPTIONS request sent to devices.

3.2.2 REFER Method

Voice Connect never sends a REFER request to a PBX.
Voice Connect accepts receiving a REFER request for unattended transfer and a REFER request with Replaces header encapsulated into Refer-to header for attended transfer.
Voice Connect does not support receiving a REFER request outside of a dialog.

Voice Connect will not send NOTIFY messages updating the transferred call progress but will instead send a BYE after the 202 Accepted response.

3.2.3 UPDATE Method

A device according to the recommendations of RFC 3311 should not send the UPDATE method with SDP on confirmed dialogs. However, Voice Connect will process received UPDATE requests with SDP on confirmed dialogs if presented.

Also, if Voice Connect receives an UPDATE request with SDP for a confirmed dialog, Voice Connect will forward the request as-is to the other party as long as the other party advertised support of the UPDATE method. If the other party did not advertise support of the UPDATE method, then Voice Connect will change the UPDATE request into a re-INVITE.

The UPDATE method may be used to update the SDP of a dialog or the dialog itself. The following are some of the SIP headers that Voice Connect allows to be updated by a received UPDATE request:

- Allow:
- Contact:
- Min-SE:
- Session-Expires:
- Supported:

Voice Connect assumes that the UPDATE method is not supported within a dialog until explicitly informed otherwise by a received Allow: header.

The UPDATE method may also be sent by Voice Connect for a session-timer refresh or a session audit refresh if the dialog indicates that the remote party supports the UDPATE method.

3.2.4 Contact: Header

The Contact: header field provides a single SIP URI that can be used to contact the sender of the INVITE for subsequent requests. The Contact: header field MUST be present and contain exactly one SIP URI in any request that can result in the establishment of a dialog.
The contact header should be presented to the network in the form of
<user-part>@<host-IPv4-address:port>
The contact header may have other parameters added to the line to provide details such as supported transport.

An example of a complete header with a user-part (optional) is shown below:

```
Contact: <sip:42295102@103.111.112.244:5060;transport=udp>
```

The host-part should be in the form of an IPv4 address, and must be routable by the customer in their network or belong to the outbound proxy being used for registration of the Trunk Group.
An exception is where a 3xx response is provided in answer to a network originated INVITE, in this case the user part is mandatory and should be in the form as if dialled by a user as this is the number that the call will be redirected to, and the SIP domain should be used, there is no requirement in this deflection scenario to have a port number specified. e.g.

```
Contact: sip:042295102@telecom.co.nz
```

In the case where the calls Trunk Group association is to be identified using the contact header see section 4.2 for details.

3.2.5 Privacy: Header

Calls from the PBX to Voice Connect.
It is recommended that the Privacy: header is used whenever possible to request privacy from the network. The Privacy header is specified in RFC 3323 and is used to request “Network-Provided Privacy” between the User agent and the network privacy service; it is recommended that “User Provided Privacy” guidelines in the RFC are followed whenever a customer seeks not to divulge unnecessary identifying information.

VC supports the following <priv-values> for the Privacy header:
id
user
history

- *The <priv-value> of history will set privacy for the redirecting number in calls classified as redirections not originating calls.*

The Privacy: header is not supported by voice connect for call forwards using the 3xx response or for REFER method messages. In both these cases the use of facility access codes (FAC) are recommended instead.

Calls from Voice Connect to the PBX.
Voice Connect may send a Privacy: header that contains a priv-value of either ‘id’ or ‘none’. The PBX should support receiving either of these values.

3.2.6 P-Asserted-Identity: Header

Calls from the PBX to Voice Connect.
The use of the P-ASSERTED-IDENTY: header is supported and for new dialog call attempts the INVITE must contain a Pilot AOR (Address of Record) if it is being used for Trunk Group Identification (TGI)
If the P-Asserted-Identity: header is not being used for TGI then it is recommended that the PAI is not passed to Voice Connect as it may inadvertently cause issues in call redirection scenarios.
Calls from Voice Connect to the PBX.
If the caller requested privacy, Voice Connect will remove all P-Asserted-Identity: header fields in the INVITE request before sending the request to the PBX.

If the caller did not request privacy, and the caller identity is asserted, then voice connect will include a P-Asserted-Identity: header field containing a URI identifying the calling user in the INVITE request before sending the request to the PBX.

3.2.7 P-Preferred-Identity: Header

The use of the PPI header is supported and must contain a Pilot URI when used for Trunk Group Identification, otherwise a Child DDI may be used typically in the case where a call has been anonymised when presented to the network.

If the P-Preferred-Identity: header is not being used for TGI then it is recommended that the PPI is not passed to Voice connect as it may inadvertently cause issues in call redirection scenarios.

3.2.8 Replaces Header

Voice Connect supports receiving the Replaces header in a REFER request, but never sends any request with a Replaces header.
Voice Connect does not support receiving a Replaces header in an INVITE, in the event one is received, VC ignores the Replaces header field and processes the INVITE as if the Replaces header is not present.

3.3 Call Forwarding

Although the main focus of this section and the subsequent sub-sections are for calls that are redirected using Voice Connect, it should be noted that calls that flow from Voice Connect and terminate on the PBX may also be forwarded onwards using other service providers, it is recommended to avoid 'dead air' and false positive failure treatment that the PBX send a '181 Call is being Forwarded' response so that voice connect is aware of session progress.

3.3.1 3xx Response

SIP PBX that operate as a proxy server can use a 3xx response to deflect a call back to Voice Connect.
The 3xx response is acted upon by Voice Connect not as a redirect server "contact advance" but instead as a call deflection. The service profile of the redirecting party will be applied to the deflected call including call barring restrictions.

The 3xx response can support Call Forward Always, Call Forward Busy, Call Forward No Answer and Call Forward Unreachable for devices that are located through the PBX via the Enterprise.

The first URI provided in the contact header is used as the forward-to target address of the original INVITE.
Addition of feature access codes (FAC) as prefixes to the forward-to URI such as for privacy is supported and will implement the feature on behalf of the redirecting party.
As the 3xx response is in-dialog to the initial INVITE there is no Trunk Group Identification check performed.

The Privacy:, Diversion:, and History-Info: headers in a 3xx response are ignored by Voice Connect.

3.3.2 INVITE

In order to forward a call, the PBX may send an INVITE request to Voice Connect, with the Request-URI: identifying the forwarded-to target destination.
Note that the following have particular relevance for forwarded calls:

- The To: header field URI can identify the originally targeted destination, in which case it will not match the Request-URI;
- The P-Asserted-Identity: header field is not used to identify the Trunk Group for a redirected call.
- The From: header field URI can contain an identity that is not an Enterprise Public Identity.

A redirecting header (Diversion / History-Info) MUST be present and populated with a known Voice Connect user with a service profile, this identity will be used as the redirecting party (the redirecting party can also be the Pilot User).

If a P-Asserted-Identity: header is present as well as the redirecting header, the INVITE will be treated as an initial INVITE for a new originating call and NOT as a redirection.

Out-of-dialog redirections support passing of the original calling party through to the destination when integrity checks by the network have been met; if the URI in the From: header is unable to meet the integrity checks then the Pilot User caller ID will be presented and any Redirecting Party service profile restrictions will be applied.

3.4 Call Transfer

Call transfer can be accomplished by the use of a REFER requests ("proxy model") or by the use of one or more INVITE/re-INVITE requests (a "third party call control model"), the latter is better suited to B2BUA PBX types..

There are three types of Call Transfer; they sometime can be given alternative names.
The document may use alternative names to fit in with a particular source (i.e. Vendor, RFC, and SIPconnect).

Name	Alt Name(s)	Definition used by this document
Unattended	Blind	In an unattended transfer (also known as a blind transfer), the PBX completes the transfer and terminates the call between the transferor and transferee immediately after it receives notification that the transfer request has been accepted.
Semi-attended		"Semi-attended transfer", is effectively a hybrid between a fully attended transfer and an unattended transfer. Typically the PBX finishes the transfer after receiving a notification of progress.
Attended	Consultation Or Consulted	In an attended transfer, the PBX monitors the progress of the transfer and finishes the transfer after it receives a notification of success.

Voice Connect supports the use of INVITE or REFER by the PBX for initiating call transfers.

Voice Connect also supports the Replaces: header see section 4.2.2 for more details.
The technique for target-refresh is supported using re-INVITE/UDATE method and also supports the SIP and SDP next connection advice (Contact: header & c= line) which will determine if the PBX is to remain in the signalling path for the call or not.

3.5 Common Failures

3.5.1 Registration Failure

If the PBX or (Trunking device in the case of Third Party Registrations) hereafter referred to as the "registering device" fails to receive any response to a REGISTER request in Timer_F time (typically 32 seconds) or encounters a transport error when sending a REGISTER request, the registering device MUST consider the Outbound Proxy unreachable and try to register through an alternate Outbound Proxy address if it has one. If the registering device has an established connection-based transport (e.g., TCP) to the Outbound Proxy, and Timer_F expires or a transport error is encountered as above, it MUST try to re-establish a connection to the same Outbound proxy before considering it unreachable, by resetting Timer_F and sending a new REGISTER request. The registering device MUST NOT attempt to re-establish the connection to the same Outbound Proxy address more than once before considering the Outbound Proxy unreachable. This allows for cases where the Outbound Proxy lost previous transport connection state but is otherwise reachable, such that the registering device will try a second time and only consider the Outbound Proxy unreachable if that second attempt fails.
If no Outbound Proxy is reachable, or no alternates are available, the registering device MUST delay reattempting Registration for 30 seconds, and increasing this delay value by doubling it for each successive delivery failure until delivery succeeds, up to a maximum value of 960 seconds. Note that receiving an explicit non-2xx final response from the Outbound Proxy does not constitute a delivery failure.

3.5.2 Registration Unknown Identity

The Outbound Proxy will issue a 404 Not Found response to a REGISTER request, if the Registration AOR of the registering device is not found in the networks database.
A registering device receiving such a response to a REGISTER request MUST consider the Registration attempt to have failed, and notify the registering device administrator if possible through some means. The registering device SHOULD follow the backoff procedures defined previously in Section 3.5.1 Registration Failure

3.5.3 Incorrect SIP-PBX Password

The statements offered in this section are in line with the SIP Forums SIPConnect v1.1 recommendation.
In the event of a digest challenge response of the PBX in its request is stale or invalid; the network will issue one of the following response codes:

- a 401 Unauthorized,
- a 407 Proxy Authentication Required or
- a 403 Forbidden

unless the network has entered a state of silently discarding these requests based on policy.
If a PBX receives more than three responses of 401, 407 or 403 in aggregate, without a different response other than one of those in between, then the PBX MUST consider the request attempt to have failed, and notify the PBX administrator if possible through some means. The PBX SHOULD follow the backoff procedures defined previously in Section 3.5.1 Registration Failure.

3.5.4 DOS & Reachability

Voice Connect utilises various levels of DOS and DDOS protection that enables our customers to carry on making and receiving calls in times of service attacks.
To ensure customers are not demoted or even denied access there are some simple guidelines to be followed.

Every message to voice connect is checked for correctness of syntax as many attacks exploit issues with syntax parsing, any header manipulations performed by integrators should be carefully checked as although a small number of these "suspicious" messages may be passed once a threshold is triggered the customer site will receive degraded or no service for a period of time.

In a similar vein the volume of messages is monitored and when thresholds are breached restrictions are imposed resulting in the customer site receiving degraded or no service for a period of time. Customer should note that increasing the frequency of REGISTER and OPTIONS transactions may result in a higher probability of degraded service activation in the busy hour and not in a higher reliability with faster failover that was desired.

The frequency and volume of ICMP (Ping) messages can also cause a site to be demoted and receive degraded or denied service entirely. Pinging is a good troubleshooting tool it is not an assure tool.

Voice Connect is highly reliable and doing frequent checks will only result in your site reliability being jeopardised. When calls are active and successfully being processed there is little to be gained by sending OPTIONS and ICMP messages to check if voice connect is available.

3.5.5 Customer Firewalls

The Voice Connect service supports an IWF and sees that this role could be performed by a Session Border Controller (SBC), the use of a regular data firewall with SIP ALG (Application Layer Gateway) is not recommended due to the bad experiences of these devices with keeping up with complex call scenarios and RFC evolution.
If basic firewalling at a transport level is desired then setting the following port forward rules through the firewall is recommended

Assuming all traffic towards Voice Connect sourced from the customer network is permitted then the following rules may be used to constrain the traffic coming from the voice connect service.

Source	Transport	Destination Port(s)	Description
<Outbound-Proxy IP Address>	UDP/TCP	5060	Well Known SIP Port
	UDP	1024:65535	RTP and RTCP ports

It is recommended that during the installation and future troubleshooting of the voice connect service is performed without firewall constraints in place and then once service has been established the customer may activate their security policy for production traffic use.

If the Spark NTP and DNS servers are being accessed through the Voice Connect service then ensure additional rules are added to include them through the firewall.

Note that the rules provided above do not permit ICMP through as ICMP is considered a troubleshooting tool and not necessary for production service.

3.6 PSTN Related

3.6.1 PSTN Identity

This specification considers a single E.164 address equivalent to a single “PSTN identity.” Accordingly, a PBX with 100 assigned telephone numbers would have 100 associated PSTN identities.
The customers’ PBX MUST choose which of its valid PSTN identities to use on a per-call basis. For example, on a call from a user without a dedicated telephone number (i.e. DDI number) the

PBX might choose to assert its trunk group “pilot” identity (e.g. the company’s main business number), while a call from a user with a dedicated DDI number may wish to use the identity of that user’s specific telephone number.

3.6.2 Caller Identity

A PBX can use P-Asserted-Identity: and P-Preferred-Identity: headers in addition to the From: header to identify the originating number, as they take precedence over the From: header. PBX calls can still use only the From: header to identify the caller.
As the P-Asserted-Identity: and P-Preferred-Identity: headers are also possibilities for Trunk Group identification customers should take care on how these headers are used.
In redirecting scenarios the use of a P-Asserted-Identity: or a P-Preferred-Identity: header will simply prevent the call from being treated as a redirected call (falls back to originating call processing) unless Trunk Group Identification is performed using a modified Contact: header (tgrp, tgrp-context) in which case the presence of a PAI header may hinder the A party pass through capabilities based on the From: header.

3.6.3 Dial Plan

It is the customers’ responsibility to ensure that the PBX and any IWF support the correct dial plan to enable calls to be made to the desired services both within New Zealand and the rest of the world.
The customer may choose to strip the leading zero from incoming calls before passing the call in to the endpoint as this may be preferable in the customers’ environment. However any SIP messages offered back to the Spark network must be returned to the original format.

3.6.4 DTMF

Voice Connect support RFC 2833 events 0 to 15 (not flash-hook) for DTMF, however all device should be able support inband DTMF to allow for devices that may not support RFC 2833.
The support of RFC 4733 will be included when devices within the market become easily available. Designers should note that RFC 4733 depreciates the support of the flash-hook event (event 16 of RFC 2833).
For wide scale compatibility reasons any Media Endpoint MUST be prepared to receive telephone-event packets for all events in the range 0-15 and MUST be prepared to accept SDP with a payload type mapped to telephone-event, even if it does not have an associated "a=fmtp" line.

3.6.5 Hold

The Voice Connect service supports RFC 3264 for placing a call on hold:
RFC 3264 mechanism uses the a= line in the SDP, setting a=inactive or a=sendonly will place the call in progress into a hold state.

3.6.6 VAD

Voice Connect service is dimensioned with sufficient bandwidth for the media for the duration of the call. As the use of VAD (Voice Activity Detection) is to conserve IP bandwidth there is no reason for this feature to be enabled on the Voice Connect service. Some devices with poor implementations of VAD have been known to introduce pops and other quality degradation artefacts.

3.6.7 Ring Timeout

The standard Ring timeout in New Zealand is 4 minutes it is recommended that the customer follows this guideline where ringing tone is provided by a device within the customers’ network to a caller.

3.6.8 Call Duration

The maximum duration of a call is restricted to 86400 seconds which is 24 hours.

3.6.9 Fax
For the first release of the Voice Connect service T.38 fax is not supported. For the first release of the Voice Connect service clear channel fax is not recommended.

3.6.10 Echo Cancellation
Any media endpoint that can introduce echo MUST support G.168 echo cancellers.

3.7 IP Transport and NAT Related
3.7.1 Internet Protocol
The service only supports IPv4; there is no support at this time for IPv6.
Support is provided for Public IP addressing owned by the customer.
Support is also offered for RFC 1918 addressing with the following exemptions:
172.18.0.0/16 when VC is installed on HSNS access.

The address block 198.18.0.0/15 as specified in RFC 59735 is not supported for use by PBX's or other customer equipment connecting through this service.

3.7.2 Interface Presentation
A dedicated physical 10/100/1000 Mbps which by default will be configured to support auto speed and duplex negotiation is provided by the CLNE.

This physical port can optionally support IEEE802.1Q Encapsulation if required.

3.7.3 IEEE 802.1p COS Markings
The Traffic presented over the CLNE LAN interface that has IEEE 802.Q encapsulation configured will mark using 802.1p the VC service traffic as follows:
* Audio Stream: 5
* Video Stream: 4
* SIP Signalling: 3
* Image (T.38): 5
* DNS: 0

Note: classification for CLNE scheduling and queuing is performed based on the DSCP markings of a packet not the 802.1p value.

3.7.4 Transport Type
Voice Connect supports
- SIP over UDP and TCP.
- T.38 is only supported using UDPTL (not supported in first release of service)
- RTP is only supported over UDP

When TCP is used for SIP, Voice Connect includes the transport=tcp parameter in the Contact entry. Explicitly specifying the transport provides better interoperability with devices unable to perform NAPTR or SRV queries to recognize that Voice Connect prefers the continued use of TCP for the dialog.
Voice Connect does not support draft-ietf-sip-connect-reuse-06.txt.

SIPconnect have stated within version 1.1 of the technical recommendations that they currently recommend customers to consider using TCP and in the next version of the recommendation the option for using UDP will be removed.
Spark is looking at future support of TLS as the way to move to TCP as this offers clear advantages over UDP
- *dTLS (TLS over UDP) is not widely supported.*

3.7.5 Maximum Transmission Unit
The Maximum Transmission Unit (MTU) size is set as 1500 bytes for this service.

3.7.6 IP QoS Markings
Spark expects and strongly recommends for call quality reasons that all multimedia packets are marked with the following DSCP (DiffServ Code Point).

Packet Type	DSCP class	Binary value
Audio Stream	EF	101110
Video Stream	AF41	100010
SIP Signalling	CS3 (or AF31)	011000 (or 011010)
Image (T.38)	EF	101110

- *T.38 is not supported in first release of service*
- *The SIP signalling will be presented from the Network using CS3, however customers that mark signalling traffic as AF31 will still be treated as though it was marked as CS3.*

These markings are for Voice Connect services that provide real-time quality, if the service is only offered as a best effort service then all media types above should be marked as BE.
If packets are incorrectly marked they may be discarded or the call quality may suffer as the incorrect treatment may be applied. This is especially important when MSSA (Multiple Services Single Access) functionality is used with Voice Connect.

Any call quality issues reported that are found to be as a result of incorrectly customer marked packets will mean the customer is held responsible for the call quality degradation.

3.7.7 Symmetric Signalling
Voice Connect service requires that the PBX or IWF function supports symmetric signalling; meaning that the same port is used for both sending and receiving of the SIP traffic (bi-directional)

3.7.8 RPID Support
The Voice Connect service supports the use of the remote-party-id header, although for customers that elect to use the Cisco CUBE to perform the IWF role it is worth noting that if RPID is enabled it can cause interoperability issues with the BroadSoft platform. Therefore for CUBE users it is best to disable the RPID header.

3.7.9 Media path
The Voice Connect service supports RTP media path that is symmetric.
All calls to the Voice Connect service will have the media transit the network SBC's. This will be achieved by the SDP c= address being returned by the SBC set to the SBC own IP address.
The c= line in the SDP offered by a customer must equal the IP address that is routable from the Spark SBC which is in the progress of setting up or holds the established session.
It is the networks responsibility to ensure that the media is delivered to the correct endpoint as it is the customers' responsibility that the media is delivered to the correct endpoint within their environment.

3.7.10 Codec Support
Any customer device that passes audio RTP to the CLNE must use a packetisation of 20 milli-seconds. Only the 64k variants of the audio codec's stipulated below are supported.
Voice Connect currently supports the following audio codec's:
G.711 A-law
G.722

3.7.11 RTCP

The Voice Connect service supports the use of RTCP and recommends that it is used particularly for video conferencing. The use of RTCP allows end devices and inline call quality monitoring devices to get an IP transport end to end view of the call quality.
The absence of RTCP can also be used as a way of clearing down stale resources this is not recommended as there is no guarantee that the far end device will support RTCP.
RTCP should be marked with the same IP QoS markings as the audio stream.

4 Multiple Trunks

4.1 Overview

The Voice Connect service has a powerful feature that enables customers to have multiple Trunk Groups; they can even be carried across the same access bearer.
Each Trunk Group has:
- A unique pilot number
- Call Capacity controls
- Fast failover for entire Trunk Group – Trunk Group re-routing (Future release feature)

The high availability and multiple tenant features are based on the ability of multiple trunk groups. The use of multiple trunks is also useful for customers that only have a single access but would like to offer different grades of services (GoS), for example a customer that has two groups of users (could be departments), group 1 has a large number of users but for normal operations would not be expected to be heavy public call users.
A call capacity that reflects group 1 usage pattern can be set that is independent of group 2 call controls. The group 2 users are few in number but deal heavily with external parties and the call usage reflects this with a large number of channels required to support this user group.

4.2 Trunk Group Identification

Trunk Group Identification is mandatory for Voice Connect.
Each call initiated is required to pass checks to establish which Trunk Group the dialog will belong to.

4.2.1 Order of Precedence

The methods of Trunk Group identification for an originating call are placed in the order of priority:

1. tgrp parameter in the Contact header
2. URI in P-Asserted-Identity matches identity of trunk group pilot user
3. URI in P-Preferred-Identity matches identity of trunk group pilot user
4. URI in From header matches identity of trunk group pilot user

There is currently no support offered for methods that involve network device addressing information.

Redirecting out-of-dialog calls rely on the identity presented in the tgrp parameter of the contact header. Alternatively the redirecting header can contain a URI of a Trunk Group pilot user. AOR using the redirection header for the Trunk Group Identification will limit out-of-dialog redirections to only be possible using the Pilot User.

4.2.2 P-Asserted-Identifier

The customer may set the PAI (P-Assured-Identifier) for all new originating INVITE messages to the Trunk pilot user identifier (used for registration) this associates the dialog to the Trunk Group.

An example cut down INVITE message from a child subscriber is shown below and the PAI is highlighted:

```
INVITE sip: 0441231234@outbound.proxy.telecom.co.nz:5060;user=phone
SIP/2.0
From: "Joe Soap"<sip:1020@telecom.co.nz;user=phone>;tag=123456789-
9876543210-
To: "Fred Blogs"<sip:041231234@200.200.200.200:5060>
CSeq: 3 INVITE
Contact: <sip: 1020@10.65.1.100:5060;transport=udp>
P-Asserted-Identity: sip:412310005@telecom.co.nz
```

Using this TGI mechanism call redirection initiated with an out of Dialog INVITE will only be able to redirect using the Pilot user of the trunk group, an additional constraint is that the caller ID of the A party may only pass through to the target when using an in-dialog redirection type.

4.2.3 Contact Header with tgrp parameter

The contact header may have the tgrp and trunk-context parameters set to provide the necessary identification of the Trunk Group the call is to be associated with.

An example cut down INVITE message from a child subscriber is shown below and the contact header is highlighted:

```
INVITE sip: 041231234@outbound.proxy.telecom.co.nz:5060;user=phone
SIP/2.0
From: "Joe Soap"<sip:1020@telecom.co.nz;user=phone>;tag=123456789-
9876543210-
To: "Fred Blogs"<sip:041231234@200.200.200.200:5060>
CSeq: 3 INVITE
Contact: <sip: 1020;tgrp=<TG-ID>;trunk-
context=telecom.co.nz@10.65.1.100:5060;transport=udp>
```

The syntax of the Contact: header with the tgrp and trunk-context parameters is aligned with RFC4904.

The <TGID> is normally set to the Trunk Group Pilot User AOR at provisioning time, for customers that were provisioned prior to the capability becoming available and wishing to use this RFC 4904 based method of Trunk Group identification should contact Spark to have this retrospective provisioned.

Using this TGI mechanism call redirection initiated with an out of Dialog INVITE will be able to redirect using any DDI assigned to the enterprise including the Pilot user of a trunk group.

For out-of-dialog redirection use cases the original A party caller ID will be provided to the redirected target if the original call came from Voice Connect using the same enterprise that redirects it, in this case the PAI header should not be sent to Voice connect as it will simply cause unexpected behaviour..
These advantages listed above are the reason why Spark recommends the use of the tgrp method over the use of PAI for Trunk Group Identification.

4.3 Advanced Routing (Enterpise Trunking)

Various routing options and policies can be applied for PBX inbound calls on Voice Connect service with multiple trunk groups. This includes failover, overflow or/and load balancing between

the Trunk Groups. The multiple Trunk Groups being used can be registered to the same or different Outbound Proxy depending on the customer diversity design.
Whilst the Enterprise Trunking routing policies will be allied to the PBX inbound calls, it is a customer responsibility to configure the PBX outbound routing policy
Failover
Failover between Trunk Groups will occur when a Trunk Groups is considered unreachable i.e. when
- Trunk Group is not registered

- Trunk Group failed to response to the network, and the invitation timer is expired.
- Failure SIP response other than busy or challenge is received form the PBX before any non-100 provisional response

Stateful failover feature allows to exclude the failed Trunk group from the routing policy until it is back to service.
A failover timer (1 to 15 seconds) can be configured. Note that for a short failover period, it is recommended that the PBX sends a provisional response to the network (e.g. SIP 181) while forwarding the incoming call to another destination to prevent the timer expiration and a false failure detection.

It is a customer responsibility to detect the failure on the PBX side and re-route the outbound calls to an alternative Trunk Group. The preferred method of detection for when calls are not being processed and as a recovery mechanism for failback is via SIP OPTION ping to the Outbound Proxy address. The minimum interval between SIP OPTION ping requests should 60 seconds

4.2.4 Load Balancing
The Enterprise Trunk can be configured to load share any calls destined to the DDI's between two or more Trunk Groups.

4.2.5 Overflow
The Enterprise Trunk can be configured to use one Trunk Group in preference to the others and only use the other Trunk Groups if the first Trunk Group call capacity limit is reached.

4.2.6 Limitations
Currently, load sharing and failover across Incoming Trunk Groups is available using Weighted Overflow policy only – each trunk group is provisioned with a priority and a weight. This mechanism provides a percentage-like split of incoming calls, starting with the trunk groups that have the highest priority, according to a weighted random pick.
Additional routing mechanisms (round-robin, least used, most used, etc.) will be implemented in FY16

4.2.7 Delivery
Enterprise Trunking can be deployed on a customer basis at this stage. Please contact Product Manager for the customised deployment.

4.4 Access Diversity
Access Diversity is an option that offers protection from the failure of the following main components:
- CLNE
- Access circuit
- PE Router
- Outbound proxy (core SBC)

The term Access Diversity refers to a customer that connects their PBX or Trunking device on a single site or multiple sites via two “Standard Access” each Standard Access is completely diverse of the other with no single point of failure from the CLNE customer LAN Ethernet connection to the PE router; a customer is provided with a single CLNE over a single HSNS pipe to a single Provider Edge router (PE).
Two FQDN’s /IP addresses are provided to the customer for the Outbound Proxy that is suitable for their geographic location. These addresses permit Outbound Proxy redundancy configuration or discovery on the customers PBX or Trunking device.

The number of calls across a single access circuit is the maximum number of calls that can be provided to the customer, if the access circuits have different capacities the lowest capacity will be used.

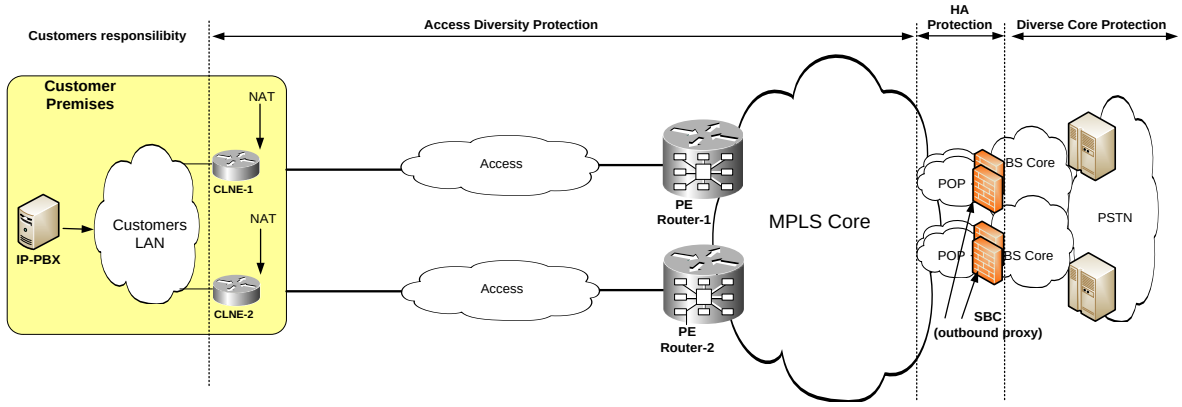


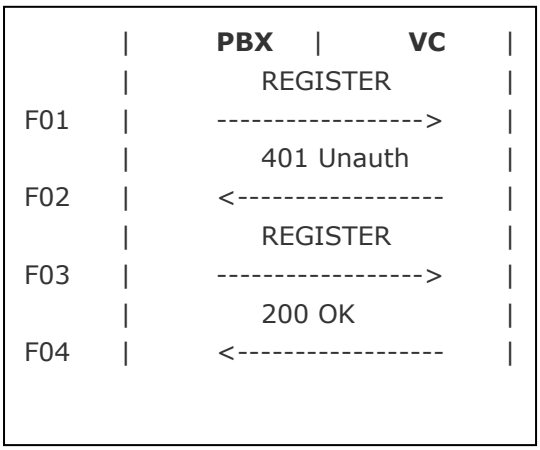
Fig. 4 Access Diversity

5 Example Call flows

These call flows were in the main using SIPp (http://sipp.sourceforge.net) these flows were not as a result of an actual PBX.
They do however offer benefit as a reference model for a working flow and a corresponding breakdown of the messages within the flow.

5.1 Pilot User Registration

Directory Numbers
Pilot User AOR: 42295135



F01

```
REGISTER sip:telecom.co.nz SIP/2.0
Via: SIP/2.0/UDP 192.168.1.4:5060;branch=z9hG4bK-3740-1-0
From: <sip:42295135@telecom.co.nz>;tag=1
To: <sip:42295135@telecom.co.nz>
Call-ID: 1-3740@192.168.1.4
CSeq: 1 REGISTER
Contact: sip:42295135@192.168.1.4:5060
Max-Forwards: 70
Expires: 60
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE,
SUBSCRIBE, INFO
User-Agent: SIPp/Win32
Content-Length: 0
```

F02

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 192.168.1.4:5060;received=172.18.250.37;branch=z9hG4bK-
3740-1-0;rport=54656
From: <sip:42295135@telecom.co.nz>;tag=1
To: <sip:42295135@telecom.co.nz>;tag=SDgp92499-141197423-1323209925246
Call-ID: 1-3740@192.168.1.4
CSeq: 1 REGISTER
WWW-Authenticate: DIGEST
qop="auth",nonce="BroadWorksXgvvh0wouTaim14uBW",realm="telecom.co.nz",al
gorithm=MD5
Content-Length: 0
```

F03

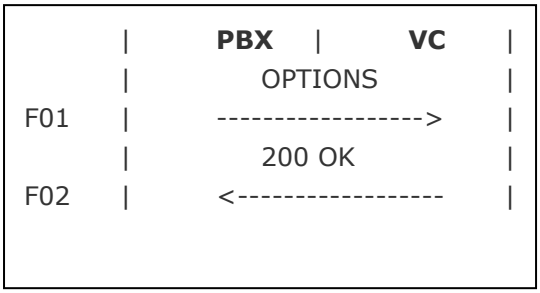
```
REGISTER sip:telecom.co.nz SIP/2.0
Via: SIP/2.0/UDP 192.168.1.4:5060;branch=z9hG4bK-3740-1-4
From: <sip:42295135@telecom.co.nz>;tag=1
To: <sip:42295135@telecom.co.nz>
Call-ID: 1-3740@192.168.1.4
CSeq: 2 REGISTER
Contact: sip:42295135@192.168.1.4:5060
Max-Forwards: 70
Expires: 60
User-Agent: SIPp/Win32
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE,
SUBSCRIBE, INFO
Content-Length: 0
Authorization: Digest
username="42295135",realm="telecom.co.nz",cnonce="5851f42d",nc=00000001,
qop=auth,uri="sip:10.111.111.245:5060",nonce="BroadWorksXgvvh0wouTaim14u
BW",response="0842554e6a8042317664508f7be3f7bc",algorithm=MD5
```

F04

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.1.4:5060;received=172.18.250.37;branch=z9hG4bK-
3740-1-4;rport=54656
From: <sip:42295135@telecom.co.nz>;tag=1
To: <sip:42295135@telecom.co.nz>;tag=SDgp92499-908249492-1323209925285
Call-ID: 1-3740@192.168.1.4
CSeq: 2 REGISTER
Contact: <sip:42295135@192.168.1.4:5060>;expires=55;q=0.5
Allow-Events: call-info,line-seize,dialog,message-summary,as-feature-
event,x-broadworks-hoteling,x-broadworks-call-center-status
Content-Length: 0
```

5.2 Pilot User OPTION Ping

Directory Numbers
Not Applicable



F01

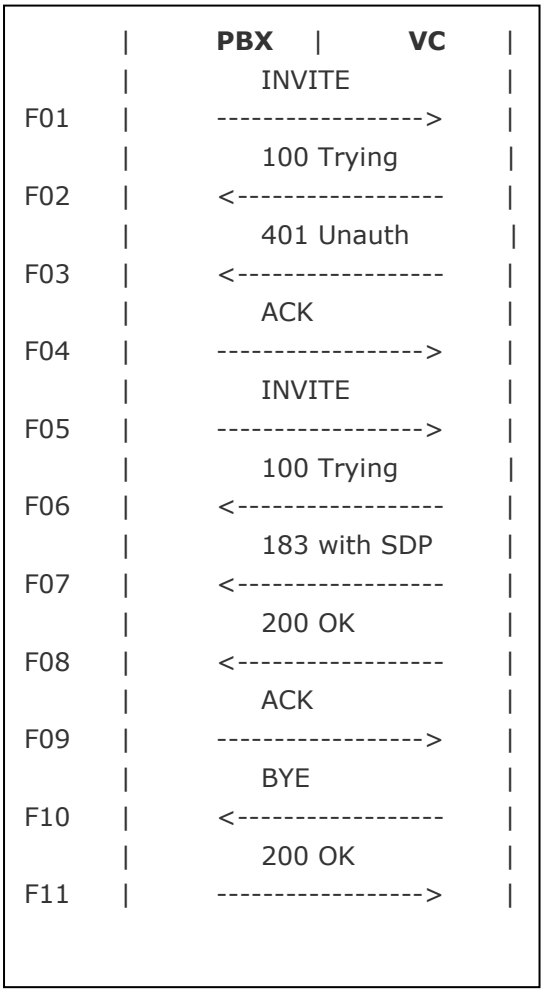
```
OPTIONS sip:10.207.44.88:5060 SIP/2.0
Via: SIP/2.0/UDP 10.10.1.62:5060;branch=z9hG4bK55E708D
From: <sip:10.10.1.62>;tag=AB6D28CC-18BE
To: <sip:10.207.44.88>
Call-ID: 2C407E1C-E65211E1-86A3AB3C-61AB6047@10.10.1.62
Max-Forwards: 70
CSeq: 101 OPTIONS
Contact: <sip:10.10.1.62:5060>
Content-Length: 0
```

F02

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP
10.10.1.62:5060;received=172.18.250.57;branch=z9hG4bK55E708D;rport=1024
From: <sip:10.10.1.62>;tag=AB6D28CC-18BE
To: <sip:10.207.44.88>;tag=SDfhfs599-
Call-ID: 2C407E1C-E65211E1-86A3AB3C-61AB6047@10.10.1.62
CSeq: 101 OPTIONS
Content-Length: 0
```

5.3 Pilot User Originating Call

Directory Numbers
Pilot User AoR: 42295120
Originator: 042295120
Destination: 077701246 (Dialled)



F01

```
INVITE sip:077701245@telecom.co.nz SIP/2.0
Via: SIP/2.0/UDP 192.168.1.12:5060
From: <sip:042295120@telecom.co.nz:5060>;tag=null3
To: <sip:077701245@telecom.co.nz>
Call-ID: 3@telecom.co.nz
CSeq: 3 INVITE
Max-Forwards: 70
Contact: <sip:042295120@192.168.1.12:5060;transport=UDP>
User-Agent: SIP Test
P-Asserted-Identity: <sip:42295120@telecom.co.nz>
Content-Type: application/sdp
Content-Length: 207

v=0
o=DUT 843670094 1 IN IP4 192.168.1.12
s=-
c=IN IP4 192.168.1.12
```

```
t=0 0
a=sendrecv
m=audio 6000 RTP/AVP 8 101
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
```

F02

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.1.12:5060;received=172.18.30.36;rport=1027
From: <sip:042295120@telecom.co.nz:5060>;tag=null3
To: <sip:077701245@telecom.co.nz>
Call-ID: 3@telecom.co.nz
CSeq: 3 INVITE
```

F03

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 192.168.1.12:5060;received=172.18.30.36;rport=1027
From: <sip:042295120@telecom.co.nz:5060>;tag=null3
To: <sip:077701245@telecom.co.nz>;tag=SDg9rf599-1351706373-1382640988179
Call-ID: 3@telecom.co.nz
CSeq: 3 INVITE
WWW-Authenticate: DIGEST
qop="auth",nonce="BroadWorksXhn6cquc3TsrazkiBW",realm="telecom.co.nz",al
gorithm=MD5
Content-Length: 0
```

F04

```
ACK sip:077701245@telecom.co.nz SIP/2.0
Via: SIP/2.0/UDP 192.168.1.12:5060
From: <sip:042295120@telecom.co.nz:5060>;tag=null3
To: <sip:077701245@telecom.co.nz>;tag=SDg9rf599-1351706373-1382640988179
Call-ID: 3@telecom.co.nz
CSeq: 3 ACK
Max-Forwards: 70
Contact: <sip:042295120@192.168.1.12:5060;transport=UDP>
User-Agent: SIP Test
Content-Length: 0
```

F05

```
INVITE sip:077701245@telecom.co.nz SIP/2.0
Via: SIP/2.0/UDP 192.168.1.12:5060
From: <sip:042295120@telecom.co.nz:5060>;tag=null3
To: <sip:077701245@telecom.co.nz>
Call-ID: 3@192.168.1.12
CSeq: 4 INVITE
Max-Forwards: 70
Contact: <sip:042295120@192.168.1.12:5060;transport=UDP>
User-Agent: SIP Test
P-Asserted-Identity: <sip:42295120@telecom.co.nz>
Authorization: Digest
username="42295120",realm="telecom.co.nz",nonce="BroadWorksXhn6cquc3Tsra
zkiBW",uri="sip:077701245@telecom.co.nz",response="153a51905033971ae9bfe
```

```
8d9c3b099d6",qop=auth,cnonce="4863492f8c3d50f7",nc=00000001,algorithm=MD
5
Content-Type: application/sdp
Content-Length: 207

v=0
o=DUT 843670094 1 IN IP4 192.168.1.12
s=-
c=IN IP4 192.168.1.12
t=0 0
a=sendrecv
m=audio 6000 RTP/AVP 8 101
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20

F06
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.1.12:5060;received=172.18.30.36;rport=1027
From: <sip:042295120@telecom.co.nz:5060>;tag=null3
To: <sip:077701245@telecom.co.nz>
Call-ID: 3@192.168.1.12
CSeq: 4 INVITE
```

F07

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP 192.168.1.12:5060;received=172.18.30.36;rport=1027
From: <sip:042295120@telecom.co.nz:5060>;tag=null3
To: <sip:077701245@telecom.co.nz>;tag=SD6u2of99-81622971-1382640989071
Call-ID: 3@192.168.1.12
CSeq: 4 INVITE
Supported:
Contact: <sip:077701245@122.56.255.168:5060;transport=udp>
Session: Media
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Content-Type: application/sdp
Content-Length: 177

v=0
o=BroadWorks 13997282 1 IN IP4 122.56.255.168
s=-
c=IN IP4 122.56.255.168
t=0 0
m=audio 12042 RTP/AVP 8 101
a=rtpmap:101 telephone-event/8000
a=ptime:20
a=sendrecv
```

F08

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.1.12:5060;received=172.18.30.36;rport=1027
From: <sip:042295120@telecom.co.nz:5060>;tag=null3
To: <sip:077701245@telecom.co.nz>;tag=SD6u2of99-81622971-1382640989071
```

```
Call-ID: 3@192.168.1.12
CSeq: 4 INVITE
Supported:
Contact: <sip:077701245@122.56.255.168:5060;transport=udp>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: application/media_control+xml,application/sdp
Content-Type: application/sdp
Content-Length: 165

v=0
o=BroadWorks 13997282 1 IN IP4 122.56.255.168
s=-
c=IN IP4 122.56.255.168
t=0 0
m=audio 12042 RTP/AVP 8 101
a=rtpmap:101 telephone-event/8000
a=ptime:20
```

F09

```
ACK sip:077701245@telecom.co.nz SIP/2.0
Via: SIP/2.0/UDP 192.168.1.12:5060
From: <sip:042295120@telecom.co.nz:5060>;tag=null3
To: <sip:077701245@telecom.co.nz>;tag=SD6u2of99-81622971-1382640989071
Call-ID: 3@192.168.1.12
CSeq: 4 ACK
Max-Forwards: 70
Contact: <sip:042295120@192.168.1.12:5060;transport=UDP>
P-Asserted-Identity: <sip:42295120@telecom.co.nz>
Authorization: [authentication username=42295120;
password=xxxxxxxxxxxx;]
User-Agent: SIP Test
Content-Length: 0
```

F10

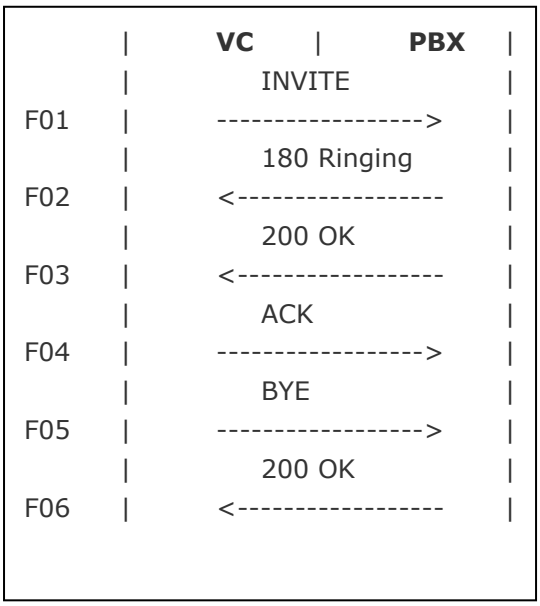
```
BYE sip:042295120@192.168.1.12:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bKou2tdf206001hhcql331sdl9qh9v0.1
From: <sip:077701245@telecom.co.nz>;tag=SD6u2of99-81622971-1382640989071
To: <sip:042295120@telecom.co.nz:5060>;tag=null3
Call-ID: 3@192.168.1.12
CSeq: 904501310 BYE
Max-Forwards: 69
Content-Length: 0
```

F11

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bKou2tdf206001hhcql331sdl9qh9v0.1
From: <sip:077701245@telecom.co.nz>;tag=SD6u2of99-81622971-1382640989071
To: <sip:042295120@telecom.co.nz:5060>;tag=null3
Call-ID: 3@192.168.1.12
CSeq: 904501310 BYE
Contact: <sip:042295120@192.168.1.12:5060>
Content-Length: 0
```

5.4
Pilot User Terminating call

Directory Numbers
Pilot User AoR: 42295120
Originator: 077701246
Destination: 042295120 (Dialled)



F01

```
INVITE sip:42295120@10.10.1.201:5061 SIP/2.0
Via: SIP/2.0/UDP
10.111.111.245:5060;branch=z9hG4bK5p42h93018801foh5341.1
From: <sip:077701246@10.207.44.132;user=phone>;tag=SDbkplf01-1166560318-
1326846641998-
To: "Pauls Pizza"<sip:42295120@telecom.co.nz;user=phone>
Call-ID: SDbkplf01-b4cdc93bee3d0bbb8c135ab4bb57c98a-v3000i1
CSeq: 924615592 INVITE
Contact: <sip:077701246@10.111.111.245:5060;transport=udp>
Supported: 100rel
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: application/media_control+xml,application/sdp,multipart/mixed
Max-Forwards: 69
Content-Type: application/sdp
Content-Length: 162

v=0
o=BroadWorks 44135 1 IN IP4 10.111.111.245
s=-
c=IN IP4 10.111.111.245
t=0 0
m=audio 13392 RTP/AVP 8 101
a=rtpmap:101 telephone-event/8000
a=ptime:20
```

F02

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP
10.111.111.245:5060;branch=z9hG4bK5p42h93018801foh5341.1
```

```
From: <sip:077701246@10.207.44.132;user=phone>;tag=SDbkplf01-1166560318-
1326846641998-
To: "Pauls Pizza"<sip:42295120@telecom.co.nz;user=phone>;tag=5
Call-ID: SDbkplf01-b4cdc93bee3d0bbb8c135ab4bb57c98a-v3000i1
CSeq: 924615592 INVITE
Contact: <sip:10.10.1.201:5061;transport=UDP>
Content-Length: 0
```

F03

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP
10.111.111.245:5060;branch=z9hG4bK5p42h93018801foh5341.1
From: <sip:077701246@10.207.44.132;user=phone>;tag=SDbkplf01-1166560318-
1326846641998-
To: "Pauls Pizza"<sip:42295120@telecom.co.nz;user=phone>;tag=5
Call-ID: SDbkplf01-b4cdc93bee3d0bbb8c135ab4bb57c98a-v3000i1
CSeq: 924615592 INVITE
Contact: <sip:10.10.1.201:5061;transport=UDP>
Content-Type: application/sdp
Content-Length:   193

v=0
o=user1 53655765 2353687637 IN IP4 10.10.1.201
s=-
c=IN IP4 10.10.1.201
t=0 0
m=audio 6016 RTP/AVP 8
a=rtpmap:8 PCMA/8000/1
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16,32,36
```

F04

```
ACK sip:10.10.1.201:5061;transport=UDP SIP/2.0
Via: SIP/2.0/UDP
10.111.111.245:5060;branch=z9hG4bK59b5ji3028jgtesqv3k0.1
From: <sip:077701246@10.207.44.132;user=phone>;tag=SDbkplf01-1166560318-
1326846641998-
To: "Pauls Pizza"<sip:42295120@telecom.co.nz;user=phone>;tag=5
Call-ID: SDbkplf01-b4cdc93bee3d0bbb8c135ab4bb57c98a-v3000i1
CSeq: 924615592 ACK
Contact: <sip:077701246@10.111.111.245:5060;transport=udp>
Max-Forwards: 69
Content-Length: 0
```

F05

```
BYE sip:10.10.1.201:5061;transport=UDP SIP/2.0
Via: SIP/2.0/UDP
10.111.111.245:5060;branch=z9hG4bK8pbhd1108gg13fgho3k1.1
From: <sip:077701246@10.207.44.132;user=phone>;tag=SDbkplf01-1166560318-
1326846641998-
To: "Pauls Pizza"<sip:42295120@telecom.co.nz;user=phone>;tag=5
Call-ID: SDbkplf01-b4cdc93bee3d0bbb8c135ab4bb57c98a-v3000i1
CSeq: 924615593 BYE
Max-Forwards: 69
```

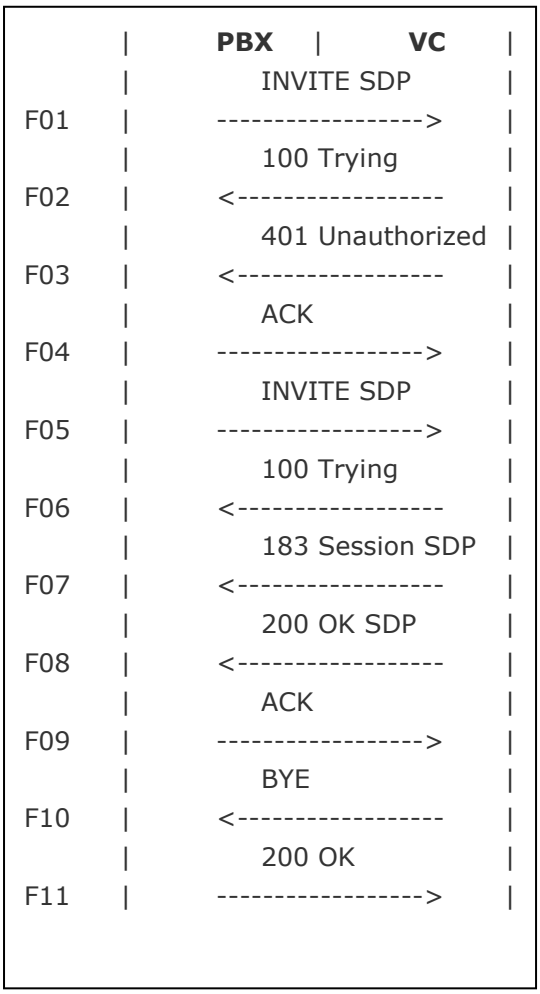
```
Content-Length: 0
```

F06

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP
10.111.111.245:5060;branch=z9hG4bK8pbhd1108gg13fgho3k1.1
From: <sip:077701246@10.207.44.132;user=phone>;tag=SDbkplf01-1166560318-
1326846641998-
To: "Pauls Pizza"<sip:42295120@telecom.co.nz;user=phone>;tag=5
Call-ID: SDbkplf01-b4cdc93bee3d0bbb8c135ab4bb57c98a-v3000i1
CSeq: 924615593 BYE
Contact: <sip:10.10.1.201:5061;transport=UDP>
Content-Length: 0
```

5.5 Child Subscriber Originating Call

Directory Numbers
Pilot User AoR: 42295120
Originator: 042295121
Destination: 077701245 (Dialled)



F01

```
INVITE sip:077701245@10.207.44.87:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.47:5060
From: "A.Party" <sip:42295121@telecom.co.nz>;tag=2
To: "B.Party" <sip:077701245@telecom.co.nz>
Call-ID: 2-3760@192.168.1.47
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:42295121@192.168.1.47:5060;transport=UDP>
P-Asserted-Identity: <sip:42295120@telecom.co.nz>
Expires: 240
Content-Length:   209
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER
Content-Type: application/sdp

v=0
o=user1 10000 20000 IN IP4 192.168.1.47
s=-
c=IN IP4 192.168.1.47
```

```
t=0 0
m=audio 6000 RTP/AVP 8 101
a=rtpmap:8 PCMA/8000/1
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=sendrecv
```

F02

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.1.47:5060;received=172.18.250.33;rport=1541
From: "A.Party" <sip:42295121@telecom.co.nz>;tag=2
To: "B.Party" <sip:077701245@telecom.co.nz>
Call-ID: 2-3760@192.168.1.47
CSeq: 1 INVITE
```

F03

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 192.168.1.47:5060;received=172.18.250.33;rport=1541
From: "A.Party" <sip:42295121@telecom.co.nz>;tag=2
To: "B.Party" <sip:077701245@telecom.co.nz>;tag=SDg9ai799-1735684993-
1345063302527
Call-ID: 2-3760@192.168.1.47
CSeq: 1 INVITE
WWW-Authenticate: DIGEST
qop="auth",nonce="BroadWorksXh5wvyminTglp22rBW",realm="telecom.co.nz",al
gorithm=MD5
Content-Length: 0
```

F04

```
SIP/2.0/UDP 192.168.1.47:5060
From: "A.Party" <sip:42295121@telecom.co.nz>;tag=2
To: "B.Party" <sip:077701245@telecom.co.nz>;tag=SDg9ai799-1735684993-
1345063302527
Call-ID: 2-3760@192.168.1.47
CSeq: 1 ACK
Contact: <sip:42295121@192.168.1.47:5060;transport=UDP>
Max-Forwards: 70
Content-Length: 0
```

F05

```
INVITE sip:077701245@10.207.44.87:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.47:5060
From: "A.Party" <sip:42295121@telecom.co.nz>;tag=2
To: "B.Party" <sip:077701245@telecom.co.nz>
Call-ID: 2-3760@192.168.1.47
CSeq: 2 INVITE
Max-Forwards: 70
Contact: <sip:42295121@192.168.1.47:5060;transport=UDP>
Authorization: Digest
username="42295120",realm="telecom.co.nz",cnonce="40b18ccf",nc=00000001,
qop=auth,uri="sip:10.207.44.87:5060",nonce="BroadWorksXh5wvyminTglp22rBW
",response="c9def2e9c3ddd83e34b485046aef3256",algorithm=MD5
P-Asserted-Identity: <sip:42295120@telecom.co.nz>
```

```
Expires: 240
Content-Length:   209
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER
Content-Type: application/sdp

v=0
o=user1 10000 20000 IN IP4 192.168.1.47
s=-
c=IN IP4 192.168.1.47
t=0 0
m=audio 6000 RTP/AVP 8 101
a=rtpmap:8 PCMA/8000/1
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=sendrecv
```

F06

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.1.47:5060;received=172.18.250.33;rport=1541
From: "A.Party" <sip:42295121@telecom.co.nz>;tag=2
To: "B.Party" <sip:077701245@telecom.co.nz>
Call-ID: 2-3760@192.168.1.47
CSeq: 2 INVITE
```

F07

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP 192.168.1.47:5060;received=172.18.250.33;rport=1541
From: "A.Party" <sip:42295121@telecom.co.nz>;tag=2
To: "B.Party" <sip:077701245@telecom.co.nz>;tag=SDg9ai799-2030702463-
1345063303224
Call-ID: 2-3760@192.168.1.47
CSeq: 2 INVITE
Supported:
Contact: <sip:07770245@10.207.44.87:5060;transport=udp>
Session: Media
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Content-Type: application/sdp
Content-Length: 169

v=0
o=BroadWorks 3488 1 IN IP4 10.207.44.87
s=-
c=IN IP4 10.207.44.87
t=0 0
m=audio 13152 RTP/AVP 8 101
a=rtpmap:101 telephone-event/8000
a=ptime:20
a=sendrecv
```

F08

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.1.47:5060;received=172.18.250.33;rport=1541
From: "A.Party" <sip:42295121@telecom.co.nz>;tag=2
```

```
To: "B.Party" <sip:077701245@telecom.co.nz>;tag=SDg9ai799-2030702463-
1345063303224
Call-ID: 2-3760@192.168.1.47
CSeq: 2 INVITE
Supported:
Contact: <sip:077701245@10.207.44.87:5060;transport=udp>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: application/media_control+xml,application/sdp
Content-Type: application/sdp
Content-Length: 157

v=0
o=BroadWorks 3488 1 IN IP4 10.207.44.87
s=-
c=IN IP4 10.207.44.87
t=0 0
m=audio 13152 RTP/AVP 8 101
a=rtpmap:101 telephone-event/8000
a=ptime:20
```

F09

```
ACK sip:077701245@10.207.44.87:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.47:5060
From: "A.Party" <sip:42295121@telecom.co.nz>;tag=2
To: "B.Party" <sip:077701245@telecom.co.nz>;tag=SDg9ai799-2030702463-
1345063303224
Call-ID: 2-3760@192.168.1.47
CSeq: 2 ACK
Contact: <sip:42295121@192.168.1.47:5060;transport=UDP>
Max-Forwards: 70
Content-Length: 0
```

F10

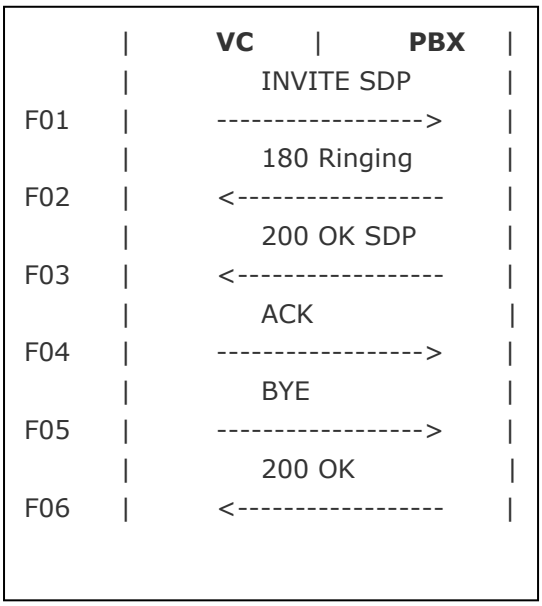
```
BYE sip:42295121@192.168.1.47:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP
10.207.44.87:5060;branch=z9hG4bK98jucc007010ehg16040sdmg0kp23.1
From: "B.Party" <sip:077701245@telecom.co.nz>;tag=SDg9ai799-2030702463-
1345063303224
To: "A.Party" <sip:42295121@telecom.co.nz>;tag=2
Call-ID: 2-3760@192.168.1.47
CSeq: 369269445 BYE
Max-Forwards: 69
Content-Length: 0
```

F11

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP
10.207.44.87:5060;branch=z9hG4bK98jucc007010ehg16040sdmg0kp23.1
From: "B.Party" <sip:077701245@telecom.co.nz>;tag=SDg9ai799-2030702463-
1345063303224
To: "A.Party" <sip:42295121@telecom.co.nz>;tag=2
Call-ID: 2-3760@192.168.1.47
CSeq: 369269445 BYE
Contact: <sip:42295121@192.168.1.47:5060;transport=UDP>
Content-Length: 0
```

5.6 Child Subscriber Terminating call

Directory Numbers
Pilot User AoR: 42295120
Originator: 042291814
Destination: 042295121 (Dialled)



F01

```
INVITE sip:42295121@192.168.1.47:5060 SIP/2.0
Via: SIP/2.0/UDP 10.207.44.87:5060;branch=z9hG4bKl2hh3510e0uh0hkng1k0.1
From: <sip:042291814@10.207.44.132;user=phone>;tag=SDbeu9d01-1478764079-
1345063630734-
To: "Paul B"<sip:42295121@telecom.co.nz;user=phone>
Call-ID: SDbeu9d01-7738abc4bbf03a800adde2e0ae8c5d57-v300g00
CSeq: 369433544 INVITE
Contact: <sip:042291814@10.207.44.87:5060;transport=udp>
Supported: 100rel
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: application/media_control+xml,application/sdp,multipart/mixed
Max-Forwards: 69
Content-Type: application/sdp
Content-Length: 232

v=0
o=BroadWorks 3499 1 IN IP4 10.207.44.87
s=-
c=IN IP4 10.207.44.87
t=0 0
m=audio 13156 RTP/AVP 9 8 101
a=rtpmap:9 G722/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=sendrecv
```

F02

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 10.207.44.87:5060;branch=z9hG4bKl2hh3510e0uh0hkng1k0.1
From: <sip:042291814@10.207.44.132;user=phone>;tag=SDbeu9d01-1478764079-
1345063630734-
To: "Paul B"<sip:42295121@telecom.co.nz;user=phone>
Call-ID: SDbeu9d01-7738abc4bbf03a800adde2e0ae8c5d57-v300g00
CSeq: 369433544 INVITE
Contact: <sip:42295120@192.168.1.47:5060;transport=UDP>
Content-Length: 0
```

F03

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.207.44.87:5060;branch=z9hG4bKl2hh3510e0uh0hkng1k0.1
From: <sip:042291814@10.207.44.132;user=phone>;tag=SDbeu9d01-1478764079-
1345063630734-
To: "Paul B"<sip:42295121@telecom.co.nz;user=phone>;tag=3
Call-ID: SDbeu9d01-7738abc4bbf03a800adde2e0ae8c5d57-v300g00
CSeq: 369433544 INVITE
Contact: <sip:42295120@192.168.1.47:5060;transport=UDP>
Content-Type: application/sdp
Content-Length:   191

v=0
o=user1 10000 20000 IN IP4 192.168.1.47
s=-
c=IN IP4 192.168.1.47
t=0 0
m=audio 6008 RTP/AVP 8 101
a=rtpmap:8 PCMA/8000/1
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16,32,36
```

F04

```
ACK sip:42295120@192.168.1.47:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 10.207.44.87:5060;branch=z9hG4bKm2ulnn100071kg8oo-3.1
From: <sip:042291814@10.207.44.132;user=phone>;tag=SDbeu9d01-1478764079-
1345063630734-
To: "Paul B"<sip:42295121@telecom.co.nz;user=phone>;tag=3
Call-ID: SDbeu9d01-7738abc4bbf03a800adde2e0ae8c5d57-v300g00
CSeq: 369433544 ACK
Contact: <sip:042291814@10.207.44.87:5060;transport=udp>
Max-Forwards: 69
Content-Length: 0
```

F05

```
BYE sip:42295120@192.168.1.47:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 10.207.44.87:5060;branch=z9hG4bKm2ulnn100071kg8oo-
3cdm81mh43.1
From: <sip:042291814@10.207.44.132;user=phone>;tag=SDbeu9d01-1478764079-
1345063630734-
To: "Paul B"<sip:42295121@telecom.co.nz;user=phone>;tag=3
Call-ID: SDbeu9d01-7738abc4bbf03a800adde2e0ae8c5d57-v300g00
CSeq: 369433545 BYE
```

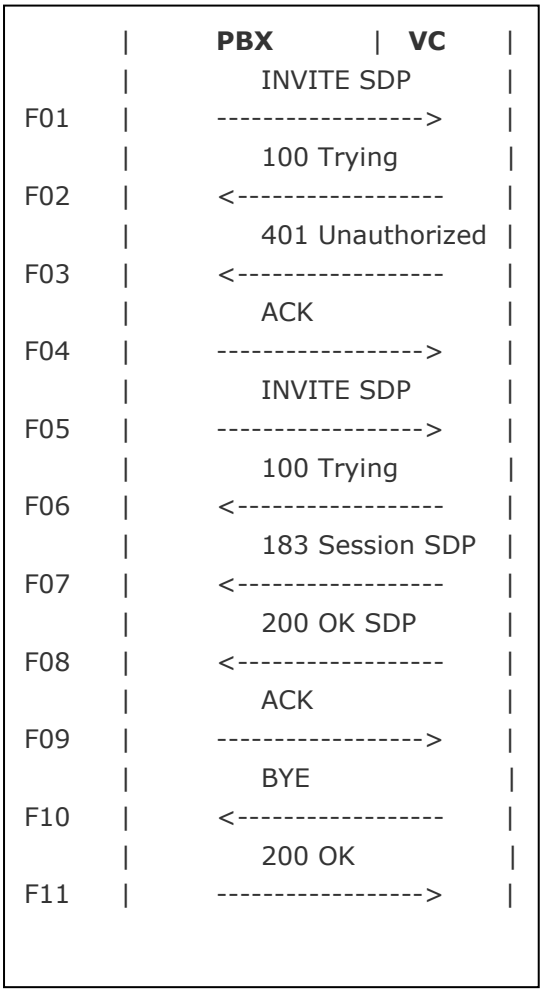
```
Max-Forwards: 69
Content-Length: 0
```

F06

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.207.44.87:5060;branch=z9hG4bKm2ulnn100071kg8oo-
3cdm81mh43.1
From: <sip:04229181 4@10.207.44.132;user=phone>;tag=SDbeu9d01-1478764079-
1345063630734-
To: "Paul B"<sip:42295121@telecom.co.nz;user=phone>;tag=3
Call-ID: SDbeu9d01-7738abc4bbf03a800adde2e0ae8c5d57-v300g00
CSeq: 369433545 BYE
Contact: <sip:42295120@192.168.1.47:5060;transport=UDP>
Content-Length: 0
```

5.7 Unscreened Originating Call

Directory Numbers
Pilot User AoR: 42295120
Originator: 0278263130 (unknown)
Destination: 077701245 (Dialled)



F01

```
INVITE sip:077701245@10.207.44.87:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.47:5060
From: "A.Party" <sip:0278263130@telecom.co.nz>;tag=2
To: "B.Party" <sip:077701245@telecom.co.nz>
Call-ID: 2-3276@192.168.1.47
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:0278263130@192.168.1.47:5060;transport=UDP>
P-Asserted-Identity: <sip:42295120@telecom.co.nz>
Expires: 240
Content-Length:   209
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER
Content-Type: application/sdp

v=0
o=user1 10000 20000 IN IP4 192.168.1.47
s=-
```

```
c=IN IP4 192.168.1.47
t=0 0
m=audio 6000 RTP/AVP 8 101
a=rtpmap:8 PCMA/8000/1
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=sendrecv
```

F02

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.1.47:5060;received=172.18.250.33;rport=1541
From: "A.Party" <sip:0278263130@telecom.co.nz>;tag=2
To: "B.Party" <sip:077701245@telecom.co.nz>
Call-ID: 2-3276@192.168.1.47
CSeq: 1 INVITE
```

F03

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 192.168.1.47:5060;received=172.18.250.33;rport=1541
From: "A.Party" <sip:0278263130@telecom.co.nz>;tag=2
To: "B.Party" <sip:077701245@telecom.co.nz>;tag=SDmha8799-1411885216-
1345063738740
Call-ID: 2-3276@192.168.1.47
CSeq: 1 INVITE
WWW-Authenticate: DIGEST
qop="auth",nonce="BroadWorksXh5ww7z3oTtgrw9BW",realm="telecom.co.nz",alg
orithm=MD5
Content-Length: 0
```

F04

```
ACK sip:077701245@10.207.44.87:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.47:5060
From: "A.Party" <sip:0278263130@telecom.co.nz>;tag=2
To: "B.Party" <sip:077701245@telecom.co.nz>;tag=SDmha8799-1411885216-
1345063738740
Call-ID: 2-3276@192.168.1.47
CSeq: 1 ACK
Contact: <sip:0278263130@192.168.1.47:5060;transport=UDP>
Max-Forwards: 70
Content-Length: 0
```

F05

```
INVITE sip:077701245@10.207.44.87:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.47:5060
From: "A.Party" <sip:0278263130@telecom.co.nz>;tag=2
To: "B.Party" <sip:077701245@telecom.co.nz>
Call-ID: 2-3276@192.168.1.47
CSeq: 2 INVITE
Max-Forwards: 70
Contact: <sip:0278263130@192.168.1.47:5060;transport=UDP>
Authorization: Digest
username="42295120",realm="telecom.co.nz",cnonce="40b18ccf",nc=00000001,
```

```
qop=auth,uri="sip:10.207.44.87:5060",nonce="BroadWorksXh5ww7z3oTtgrw9BW"
,response="368b63e426ebe91f97c1da3571c0f273",algorithm=MD5
P-Asserted-Identity: <sip:42295120@telecom.co.nz>
Expires: 240
Content-Length:   209
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER
Content-Type: application/sdp

v=0
o=user1 10000 20000 IN IP4 192.168.1.47
s=-
c=IN IP4 192.168.1.47
t=0 0
m=audio 6000 RTP/AVP 8 101
a=rtpmap:8 PCMA/8000/1
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=sendrecv
```

F06

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.1.47:5060;received=172.18.250.33;rport=1541
From: "A.Party" <sip:0278263130@telecom.co.nz>;tag=2
To: "B.Party" <sip:077701245@telecom.co.nz>
Call-ID: 2-3276@192.168.1.47
CSeq: 2 INVITE
```

F07

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP 192.168.1.47:5060;received=172.18.250.33;rport=1541
From: "A.Party" <sip:0278263130@telecom.co.nz>;tag=2
To: "B.Party" <sip:077701245@telecom.co.nz>;tag=SDmha8799-1689011624-
1345063739072
Call-ID: 2-3276@192.168.1.47
CSeq: 2 INVITE
Supported:
Contact: <sip:077701245@10.207.44.87:5060;transport=udp>
Session: Media
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Content-Type: application/sdp
Content-Length: 169

v=0
o=BroadWorks 3506 1 IN IP4 10.207.44.87
s=-
c=IN IP4 10.207.44.87
t=0 0
m=audio 13158 RTP/AVP 8 101
a=rtpmap:101 telephone-event/8000
a=ptime:20
a=sendrecv
```

F08

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.1.47:5060;received=172.18.250.33;rport=1541
From: "A.Party" <sip:0278263130@telecom.co.nz>;tag=2
To: "B.Party" <sip:077701245@telecom.co.nz>;tag=SDmha8799-1689011624-
1345063739072
Call-ID: 2-3276@192.168.1.47
CSeq: 2 INVITE
Supported:
Contact: <sip:077701245@10.207.44.87:5060;transport=udp>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: application/media_control+xml,application/sdp
Content-Type: application/sdp
Content-Length: 157

v=0
o=BroadWorks 3506 1 IN IP4 10.207.44.87
s=-
c=IN IP4 10.207.44.87
t=0 0
m=audio 13158 RTP/AVP 8 101
a=rtpmap:101 telephone-event/8000
a=ptime:20
```

F09

```
ACK sip:077701245@10.207.44.87:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.47:5060
From: "A.Party" <sip:0278263130@telecom.co.nz>;tag=2
To: "B.Party" <sip:077701245@telecom.co.nz>;tag=SDmha8799-1689011624-
1345063739072
Call-ID: 2-3276@192.168.1.47
CSeq: 2 ACK
Contact: <sip:0278263130@192.168.1.47:5060;transport=UDP>
Max-Forwards: 70
Content-Length: 0
```

F10

```
BYE sip:0278263130@192.168.1.47:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP
10.207.44.87:5060;branch=z9hG4bKgbgeea302gfg3hgkt4k0sdm81se03.1
From: "B.Party" <sip:077701245@telecom.co.nz>;tag=SDmha8799-1689011624-
1345063739072
To: "A.Party" <sip:0278263130@telecom.co.nz>;tag=2
Call-ID: 2-3276@192.168.1.47
CSeq: 369487552 BYE
Max-Forwards: 69
Content-Length: 0
```

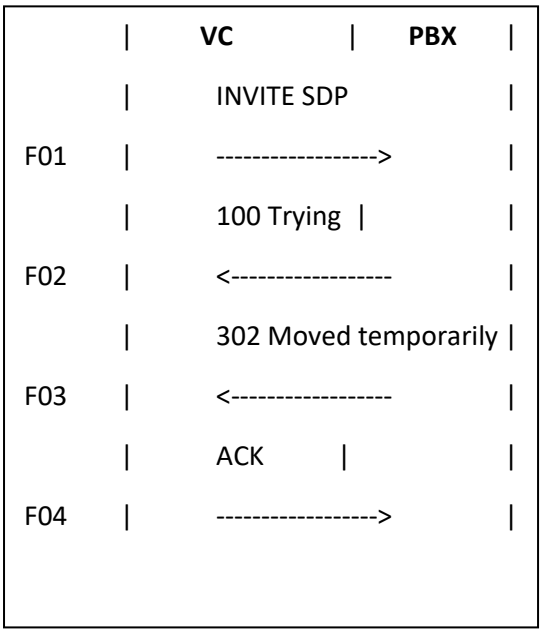
F11

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP
10.207.44.87:5060;branch=z9hG4bKgbgeea302gfg3hgkt4k0sdm81se03.1
From: "B.Party" <sip:077701245@telecom.co.nz>;tag=SDmha8799-1689011624-
1345063739072
```

```
To: "A.Party" <sip:0278263130@telecom.co.nz>;tag=2
Call-ID: 2-3276@192.168.1.47
CSeq: 369487552 BYE
Contact: <sip:0278263130@192.168.1.47:5060;transport=UDP>
Content-Length: 0
```

5.8 Call Forward - 3xx Deflection

Directory Numbers
Pilot User AoR: 44718607
Originator: 048010550
forwarder: 044718607
forward-to 044718601



F01

```
INVITE sip:44718607@192.168.1.12:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bKoni004200o704hcjb770.1
From: <sip:048010550@122.56.252.6;user=phone>;tag=SD9s12e01-1985613251-
1382297842680-
To: "Martin Reid"<sip:44718607@telecom.co.nz;user=phone>
Call-ID: SD9s12e01-44d1acacaeaaf071f80d232f5db5df78-v300g00
CSeq: 732928509 INVITE
Contact: <sip:048010550@122.56.255.168:5060;transport=udp>
Supported: 100rel
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: application/media_control+xml,application/sdp,multipart/mixed
Max-Forwards: 69
Content-Type: application/sdp
Content-Length: 165

v=0
o=BroadWorks 12434894 1 IN IP4 122.56.255.168
s=-
c=IN IP4 122.56.255.168
t=0 0
m=audio 12008 RTP/AVP 8 101
a=rtpmap:101 telephone-event/8000
a=ptime:20
```

F02

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bKoni004200o704hcjb770.1
From: <sip:048010550@122.56.252.6;user=phone>;tag=SD9s12e01-1985613251-
1382297842680-
To: "Martin Reid"<sip:44718607@telecom.co.nz;user=phone>
Call-ID: SD9s12e01-44d1acacaeaaf071f80d232f5db5df78-v300g00
CSeq: 732928509 INVITE
User-Agent: SIP-Test
Content-Length: 0
```

F03

```
SIP/2.0 302 Moved temporarily
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bKoni004200o704hcjb770.1
From: <sip:048010550@122.56.252.6;user=phone>;tag=SD9s12e01-1985613251-
1382297842680-
To: "Martin Reid"<sip:44718607@telecom.co.nz;user=phone>;tag=SD9s12e01-
44d1acacaeaaf071f80d232f5db5df78-v300g00
Call-ID: SD9s12e01-44d1acacaeaaf071f80d232f5db5df78-v300g00
CSeq: 732928509 INVITE
Contact: <sip:044718601@telecom.co.nz>
User-Agent: SIP-Test
Content-Length: 0
```

F04

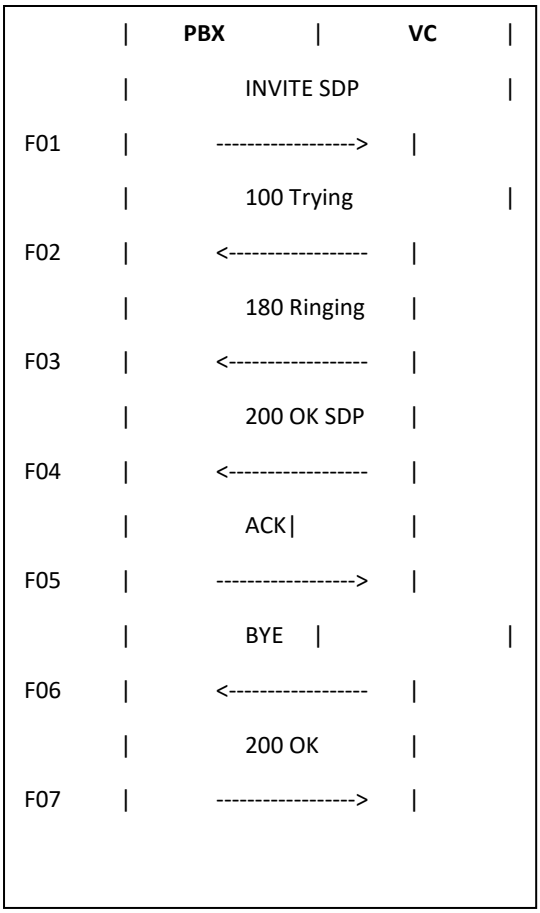
```
ACK sip:44718607@192.168.1.12:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bKoni004200o704hcjb770.1
CSeq: 732928509 ACK
From: <sip:048010550@122.56.252.6;user=phone>;tag=SD9s12e01-1985613251-
1382297842680-
To: "Martin Reid"<sip:44718607@telecom.co.nz;user=phone>;tag=SD9s12e01-
44d1acacaeaaf071f80d232f5db5df78-v300g00
Call-ID: SD9s12e01-44d1acacaeaaf071f80d232f5db5df78-v300g00
Max-Forwards: 69
Content-Length: 0
```

In this example, VC sends an INVITE to the PBX. The PBX wants to forward the call to another location, so it responds with a 302 Moved Temporarily message with the URI of the other location in the contact header field. VC then sends an ACK to the PBX to acknowledge receipt of the 302 and ends that transaction. VC then sends a new INVITE to the other location using the URI that it learned from the contact header field of the 302 response.

5.9 Call Forward - INVITE

This example shows an out of dialog call forward using an INVITE request with a Diversion: header as the redirecting information. The initial INVITE request and the subsequent change has been left off this example flow.

Directory Numbers
Pilot User AoR: 44718607
Originator: 044718608
forwarder: 044718607
forward-to 044718601



F01

```
INVITE sip:044718601@telecom.co.nz SIP/2.0
Via: SIP/2.0/UDP 192.168.1.12:5060
From: "A Party"
<sip:044718608@telecom.co.nz:5060>;tag=24417923471779367133
To: <sip:044718601@telecom.co.nz>
Call-ID: 10@192.168.1.12
CSeq: 3 INVITE
Max-Forwards: 70
Contact: <sip:044718608@192.168.1.12:5060;transport=UDP>
Diversion:
<sip:44718607@telecom.co.nz>;privacy=off;reason=unconditional;screen=yes
Authorization: Digest
username="44718607",realm="telecom.co.nz",nonce="BroadWorksXhn0v1kj8T5xu
cf3BW",uri="sip:044718601@telecom.co.nz",response="86842525800e4363d4f95
```

```
11f87232885",qop=auth,cnonce="9f648ca0031819b8",nc=00000001,algorithm=MD
5
Content-Type: application/sdp
Content-Length: 213

v=0
o=044718608 843670094 1 IN IP4 192.168.1.12
s=-
c=IN IP4 192.168.1.12
t=0 0
a=sendrecv
m=audio 6000 RTP/AVP 8 101
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
```

F02

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.1.12:5060;received=172.18.30.36;rport=1026
From: "A Party"
<sip:044718608@telecom.co.nz:5060>;tag=24417923471779367133
To: <sip:044718601@telecom.co.nz>
Call-ID: 10@192.168.1.12
CSeq: 3 INVITE
```

F03

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.168.1.12:5060;received=172.18.30.36;rport=1026
From: "A Party"
<sip:044718608@telecom.co.nz:5060>;tag=24417923471779367133
To: <sip:044718601@telecom.co.nz>;tag=SDb8udf99-219992790-1382308924906
Call-ID: 10@192.168.1.12
CSeq: 3 INVITE
Supported:
Contact: <sip:044718601@122.56.255.168:5060;transport=udp>
P-Asserted-Identity: "Paul Miller"<sip:44718601@122.56.252.6;user=phone>
Privacy: none
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
Content-Length: 0
```

F04

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.1.12:5060;received=172.18.30.36;rport=1026
From: "A Party"
<sip:044718608@telecom.co.nz:5060>;tag=24417923471779367133
To: <sip:044718601@telecom.co.nz>;tag=SDb8udf99-219992790-1382308924906
Call-ID: 10@192.168.1.12
CSeq: 3 INVITE
Supported:
Contact: <sip:044718601@122.56.255.168:5060;transport=udp>
P-Asserted-Identity: "Paul Miller"<sip:44718601@122.56.252.6;user=phone>
Privacy: none
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
```

```
Accept: application/media_control+xml,application/sdp
Content-Type: application/sdp
Content-Length: 240

v=0
o=BroadWorks 12537989 1 IN IP4 122.56.255.168
s=-
c=IN IP4 122.56.255.168
t=0 0
m=audio 12022 RTP/AVP 9 8 101
a=rtpmap:9 G722/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=sendrecv
```

F05

```
ACK sip:044718601@telecom.co.nz SIP/2.0
Via: SIP/2.0/UDP 192.168.1.12:5060
From: "A Party"
<sip:044718608@telecom.co.nz:5060>;tag=24417923471779367133
To: <sip:044718601@telecom.co.nz>;tag=SDb8udf99-219992790-1382308924906
Call-ID: 10@192.168.1.12
CSeq: 3 ACK
Max-Forwards: 70
Contact: <sip:044718608@192.168.1.12:5060;transport=UDP>
Authorization: [authentication username=44718607;
password=xxxxxxxxxxxx;]
Content-Length: 0
```

F06

```
BYE sip:044718608@192.168.1.12:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bK94njfs0080p07hcj6730sdc11c293.1
From: <sip:044718601@telecom.co.nz>;tag=SDb8udf99-219992790-
1382308924906
To: "A Party"
<sip:044718608@telecom.co.nz:5060>;tag=24417923471779367133
Call-ID: 10@192.168.1.12
CSeq: 738469586 BYE
Max-Forwards: 69
Content-Length: 0
```

F07

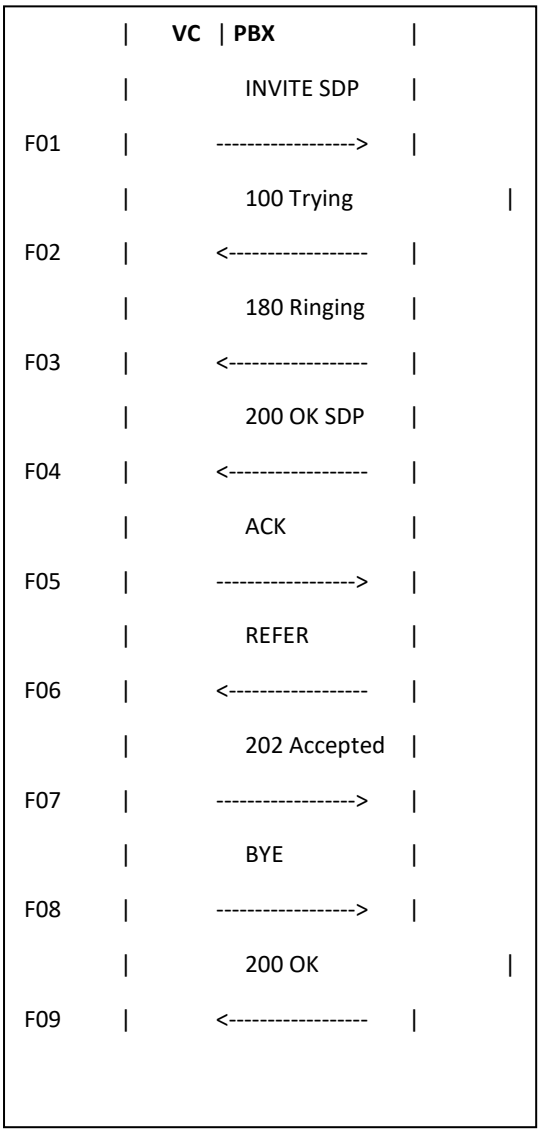
```
SIP/2.0 200 OK
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bK94njfs0080p07hcj6730sdc11c293.1
From: <sip:044718601@telecom.co.nz>;tag=SDb8udf99-219992790-
1382308924906
To: "A Party"
<sip:044718608@telecom.co.nz:5060>;tag=24417923471779367133
Call-ID: 10@192.168.1.12
CSeq: 738469586 BYE
```

```
Contact: <sip:044718608@192.168.1.12:5060>
Content-Length: 0
```

5.10 Call Transfer Unattended using REFER

The authentication of the REFER has been omitted.

Directory Numbers
Pilot User AoR: 44718607
transferee: 048010550
transferor: 044718608
transfer-target 044718601



F01

```
INVITE sip:44718607@192.168.1.12:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bKcmd6kt00cgbh1hcj6730.1
From: <sip:048010550@122.56.252.6;user=phone>;tag=SDlcb5f01-1163938444-
1382307689253-
To: "Martin Reid"<sip:44718607@telecom.co.nz;user=phone>
Call-ID: SDlcb5f01-dcfda485e8f1a584c97f43e6db9adb3e-v300g00
CSeq: 737851795 INVITE
Contact: <sip:048010550@122.56.255.168:5060;transport=udp>
Supported: 100rel
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
```

```
Accept: application/media_control+xml,application/sdp,multipart/mixed
Max-Forwards: 69
Content-Type: application/sdp
Content-Length: 165

v=0
o=BroadWorks 12526149 1 IN IP4 122.56.255.168
s=-
c=IN IP4 122.56.255.168
t=0 0
m=audio 12018 RTP/AVP 8 101
a=rtpmap:101 telephone-event/8000
a=ptime:20
```

F02

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bKcmd6kt00cgbh1hcj6730.1
From: <sip:048010550@122.56.252.6;user=phone>;tag=SDlcb5f01-1163938444-
1382307689253-
To: "Martin Reid"<sip:44718607@telecom.co.nz;user=phone>
Call-ID: SDlcb5f01-dcfda485e8f1a584c97f43e6db9adb3e-v300g00
CSeq: 737851795 INVITE
User-Agent: SIP Test
Content-Length: 0
```

F03

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bKcmd6kt00cgbh1hcj6730.1
From: <sip:048010550@122.56.252.6;user=phone>;tag=SDlcb5f01-1163938444-
1382307689253-
To: "Martin Reid"<sip:44718607@telecom.co.nz;user=phone>;tag=234567891-
s1234
Call-ID: SDlcb5f01-dcfda485e8f1a584c97f43e6db9adb3e-v300g00
CSeq: 737851795 INVITE
Contact: <sip:044718608@192.168.1.12:5060;transport=UDP>
User-Agent: SIP Test
Content-Length: 0
```

F04

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bKcmd6kt00cgbh1hcj6730.1
From: <sip:048010550@122.56.252.6;user=phone>;tag=SDlcb5f01-1163938444-
1382307689253-
To: "Martin Reid"<sip:44718607@telecom.co.nz;user=phone>;tag=234567891-
s1234
Call-ID: SDlcb5f01-dcfda485e8f1a584c97f43e6db9adb3e-v300g00
CSeq: 737851795 INVITE
Contact: <sip:044718608@192.168.1.12:5060;transport=UDP>
User-Agent: SIP Test
Supported: replaces
Content-Type: application/sdp
```

```
Content-Length:207

v=0
o=DUT 843670094 1 IN IP4 192.168.1.12
s=-
c=IN IP4 192.168.1.12
t=0 0
a=sendrecv
m=audio 6000 RTP/AVP 8 101
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
```

F05

```
ACK sip:044718608@192.168.1.12:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bKe61car107861lhcql331.1
From: <sip:048010550@122.56.252.6;user=phone>;tag=SDlcb5f01-1163938444-
1382307689253-
To: "Martin Reid"<sip:44718607@telecom.co.nz;user=phone>;tag=234567891-
s1234
Call-ID: SDlcb5f01-dcfda485e8f1a584c97f43e6db9adb3e-v300g00
CSeq: 737851795 ACK
Contact: <sip:048010550@122.56.255.168:5060;transport=udp>
Max-Forwards: 69
Content-Length: 0
```

F06

```
REFER sip:048010550@122.56.255.168:5060;transport=udp SIP/2.0
Via: SIP/2.0/UDP 192.168.1.12:5060;branch=z9hG4bK5112
From: <sip:044718608@telecom.co.nz;tag=234567891-s1234
To: <sip:044718601@telecom.co.nz;user=phone>;tag=SDlcb5f01-1163938444-
1382307689253-
Referred-By: <044718608@telecom.co.nz>
Call-ID: SDlcb5f01-dcfda485e8f1a584c97f43e6db9adb3e-v300g00
CSeq: 889345011 REFER
Max-Forwards: 70
Contact: <sip:044718608@192.168.1.12:5060;transport=UDP>
Refer-To: <sip:044718601@telecom.co.nz>
User-Agent: SIP Test
Supported: replaces
Content-Length: 0
```

F07

```
SIP/2.0 202 Accepted
Via: SIP/2.0/UDP
192.168.1.12:5060;received=172.18.30.36;branch=z9hG4bK5112;rport=1026
From: <sip:044718608@telecom.co.nz;tag=234567891-s1234
To: <sip:044718601@telecom.co.nz;user=phone>;tag=SDlcb5f01-1163938444-
1382307689253-
Call-ID: SDlcb5f01-dcfda485e8f1a584c97f43e6db9adb3e-v300g00
CSeq: 889345011 REFER
Contact: <sip:048010550@122.56.255.168:5060;transport=udp>
```

```
Content-Length: 0
```

F08

```
BYE sip:044718608@192.168.1.12:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bKe61car107861lhcql331cdbhujba2.1
From: <sip:048010550@122.56.252.6;user=phone>;tag=SDlcb5f01-1163938444-
1382307689253-
To: "Martin Reid"<sip:44718607@telecom.co.nz;user=phone>;tag=234567891-
s1234
Call-ID: SDlcb5f01-dcfda485e8f1a584c97f43e6db9adb3e-v300g00
CSeq: 737851796 BYE
Max-Forwards: 69
Content-Length: 0
```

F09

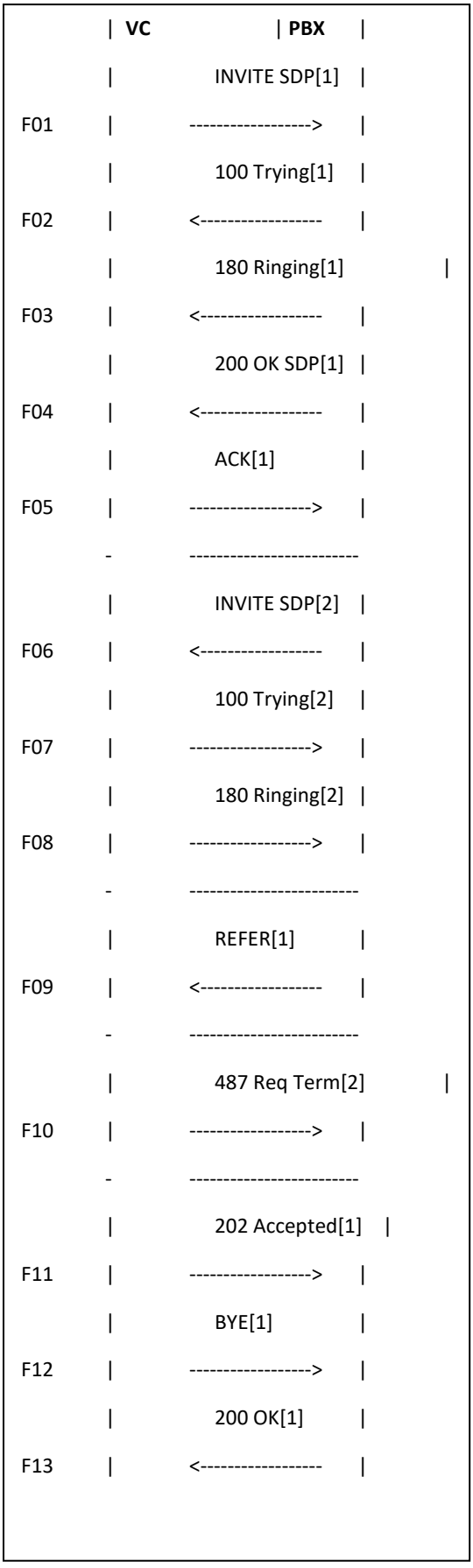
```
SIP/2.0 200 OK
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bKe61car107861lhcql331cdbhujba2.1
From: <sip:048010550@122.56.252.6;user=phone>;tag=SDlcb5f01-1163938444-
1382307689253-
To: "Martin Reid"<sip:44718607@telecom.co.nz;user=phone>;tag=234567891-
s1234
Call-ID: SDlcb5f01-dcfda485e8f1a584c97f43e6db9adb3e-v300g00
CSeq: 737851796 BYE
User-Agent: SIP Test
Contact: <sip:044718608@192.168.1.12:5060;transport=UDP>
Content-Length: 0
```

5.11
Call Transfer Semi-Attended using REFER with Replaces

This call transfer has two dialogs. Alice calls Bob on dialog[1] and they chat, Bob initiates a new call to Carol on dialog [2] and while listening to ringing decides to transfer Alice, using this type of Call Transfer Alice will receive the call treatment Carol has configured for Call Forward No Answer if Carol doe not answer the call.
This type of Call Transfer is popular with service desks.
The authentication of the INVITE & the REFER has been omitted.

Directory Numbers

Pilot User AoR:	44718607
transferee:	048010550
transferor:	044718608
transfer-target	044718601



F01

```
INVITE sip:44718607@192.168.1.12:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bKbevu0c20982hmh8qb630.1
```

```
From: <sip:048010550@122.56.252.6;user=phone>;tag=SDfkeje01-1771243513-
1382309365834-
To: "Martin Reid"<sip:44718607@telecom.co.nz;user=phone>
Call-ID: SDfkeje01-5091d980228be03994770cbd2dce4cfb-v300g00
CSeq: 738690086 INVITE
Contact: <sip:048010550@122.56.255.168:5060;transport=udp>
Supported: 100rel
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: application/media_control+xml,application/sdp,multipart/mixed
Max-Forwards: 69
Content-Type: application/sdp
Content-Length: 165

v=0
o=BroadWorks 12542169 1 IN IP4 122.56.255.168
s=-
c=IN IP4 122.56.255.168
t=0 0
m=audio 12024 RTP/AVP 8 101
a=rtpmap:101 telephone-event/8000
a=ptime:20
```

F02

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bKbevu0c20982hmh8qb630.1
From: <sip:048010550@122.56.252.6;user=phone>;tag=SDfkeje01-1771243513-
1382309365834-
To: "Martin Reid"<sip:44718607@telecom.co.nz;user=phone>
Call-ID: SDfkeje01-5091d980228be03994770cbd2dce4cfb-v300g00
CSeq: 738690086 INVITE
User-Agent: SIP Test
Content-Length: 0
```

F03

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bKbevu0c20982hmh8qb630.1
From: <sip:048010550@122.56.252.6;user=phone>;tag=SDfkeje01-1771243513-
1382309365834-
To: "Martin Reid"<sip:44718607@telecom.co.nz;user=phone>;tag=atobcall-
12345678
Call-ID: SDfkeje01-5091d980228be03994770cbd2dce4cfb-v300g00
CSeq: 738690086 INVITE
Contact: <sip:044718608@192.168.1.12:5060;transport=UDP>
User-Agent: SIP Test
Content-Length: 0
```

F04

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bKbevu0c20982hmh8qb630.1
From: <sip:048010550@122.56.252.6;user=phone>;tag=SDfkeje01-1771243513-
1382309365834-
```

```
To: "Martin Reid"<sip:44718607@telecom.co.nz;user=phone>;tag=atobcall-
12345678
Call-ID: SDfkeje01-5091d980228be03994770cbd2dce4cfb-v300g00
CSeq: 738690086 INVITE
Contact: <sip:044718608@192.168.1.12:5060;transport=UDP>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
User-Agent: SIP Test
Supported: replaces
Content-Type: application/sdp
Content-Length:215

v=0
o=111 843670094 843670094 IN IP4 192.168.1.12
s=-
c=IN IP4 192.168.1.12
t=0 0
a=inactive
m=audio 6000 RTP/AVP 8 101
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
```

F05

```
ACK sip:044718608@192.168.1.12:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bKcec3lv20e820shcql331.1
From: <sip:048010550@122.56.252.6;user=phone>;tag=SDfkeje01-1771243513-
1382309365834-
To: "Martin Reid"<sip:44718607@telecom.co.nz;user=phone>;tag=atobcall-
12345678
Call-ID: SDfkeje01-5091d980228be03994770cbd2dce4cfb-v300g00
CSeq: 738690086 ACK
Contact: <sip:048010550@122.56.255.168:5060;transport=udp>
Max-Forwards: 69
Content-Length: 0
```

F06

```
INVITE sip:044718601@telecom.co.nz SIP/2.0
Via: SIP/2.0/UDP 192.168.1.12:5060;branch=z9hG4bK-v2
From: <sip:044718608@telecom.co.nz>;tag=btoccall-12345678
To: <sip:044718601@telecom.co.nz>
Call-ID: sptest-123456789-orig
CSeq: 2 INVITE
P-Asserted-Identity: <sip:44718607@telecom.co.nz>
Max-Forwards: 69
Contact: <sip:044718608@192.168.1.12:5060>
Authorization: Digest
username="44718607",realm="telecom.co.nz",nonce="BroadWorksXhn0vb9eiTxsb
8vvBW",uri="sip:044718601@telecom.co.nz",response="9335f51f190033eec8099
8986dd17cad",qop=auth,cnonce="7dce978aea759406",nc=00000001,algorithm=MD
5
Content-Type: application/sdp
Content-Length: 207
```

```
v=0
o=AJT 843670094 1 IN IP4 192.168.1.12
s=-
c=IN IP4 192.168.1.12
t=0 0
a=sendrecv
m=audio 6002 RTP/AVP 8 101
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
```

F07

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.1.12:5060;received=172.18.30.36;branch=z9hG4bK-
v2;rport=1026
From: <sip:044718608@telecom.co.nz>;tag=btoccall-12345678
To: <sip:044718601@telecom.co.nz>
Call-ID: sptest-123456789-orig
CSeq: 2 INVITE
```

F08

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.168.1.12:5060;received=172.18.30.36;branch=z9hG4bK-
v2;rport=1026
From: <sip:044718608@telecom.co.nz>;tag=btoccall-12345678
To: <sip:044718601@telecom.co.nz>;tag=SDvq5i199-773864525-1382309377025
Call-ID: sptest-123456789-orig
CSeq: 2 INVITE
Supported:
Contact: <sip:044718601@122.56.255.168:5060;transport=udp>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
Content-Length: 0
```

F09

```
REFER sip:048010550@122.56.255.168:5060;transport=udp SIP/2.0
Via: SIP/2.0/UDP 192.168.1.12:5060
From: <sip:044718608@telecom.co.nz;user=phone>;tag=atobcall-12345678
To: <sip:048010550@122.56.252.6;user=phone>;tag=SDfkeje01-1771243513-
1382309365834-
Call-ID: SDfkeje01-5091d980228be03994770cbd2dce4cfb-v300g00
CSeq: 3 REFER
Max-Forwards: 70
Expires: 240
Contact: <sip:044718608@192.168.1.12:5060;transport=UDP>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Refer-To: <sip:044718601@telecom.co.nz?Replaces=sptest-123456789-
orig%3bfrom-tag%3dbtoccall-12345678%3bto-tag%3dSDvq5i199-773864525-
1382309377025>
User-Agent: SIP Test
Supported: replaces
Content-Length: 0
```

F10

```
SIP/2.0 487 Request terminated
Via: SIP/2.0/UDP 192.168.1.12:5060;received=172.18.30.36;branch=z9hG4bK-
v2;rport=1026
From: <sip:044718608@telecom.co.nz>;tag=btoccall-12345678
To: <sip:044718601@telecom.co.nz>;tag=SDvq5i199-773864525-1382309377025
Call-ID: sptest-123456789-orig
CSeq: 2 INVITE
Content-Length: 0
```

F11

```
SIP/2.0 202 Accepted
Via: SIP/2.0/UDP 192.168.1.12:5060;received=172.18.30.36;rport=1026
From: <sip:044718608@telecom.co.nz;user=phone>;tag=atobcall-12345678
To: <sip:048010550@122.56.252.6;user=phone>;tag=SDfkeje01-1771243513-
1382309365834-
Call-ID: SDfkeje01-5091d980228be03994770cbd2dce4cfb-v300g00
CSeq: 3 REFER
Contact: <sip:048010550@122.56.255.168:5060;transport=udp>
Content-Length: 0
```

F12

```
BYE sip:044718608@192.168.1.12:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bKcec3lv20e820shcql331cdcp18oj0.1
From: <sip:048010550@122.56.252.6;user=phone>;tag=SDfkeje01-1771243513-
1382309365834-
To: "Martin Reid"<sip:44718607@telecom.co.nz;user=phone>;tag=atobcall-
12345678
Call-ID: SDfkeje01-5091d980228be03994770cbd2dce4cfb-v300g00
CSeq: 738690087 BYE
Max-Forwards: 69
Content-Length: 0
```

F13

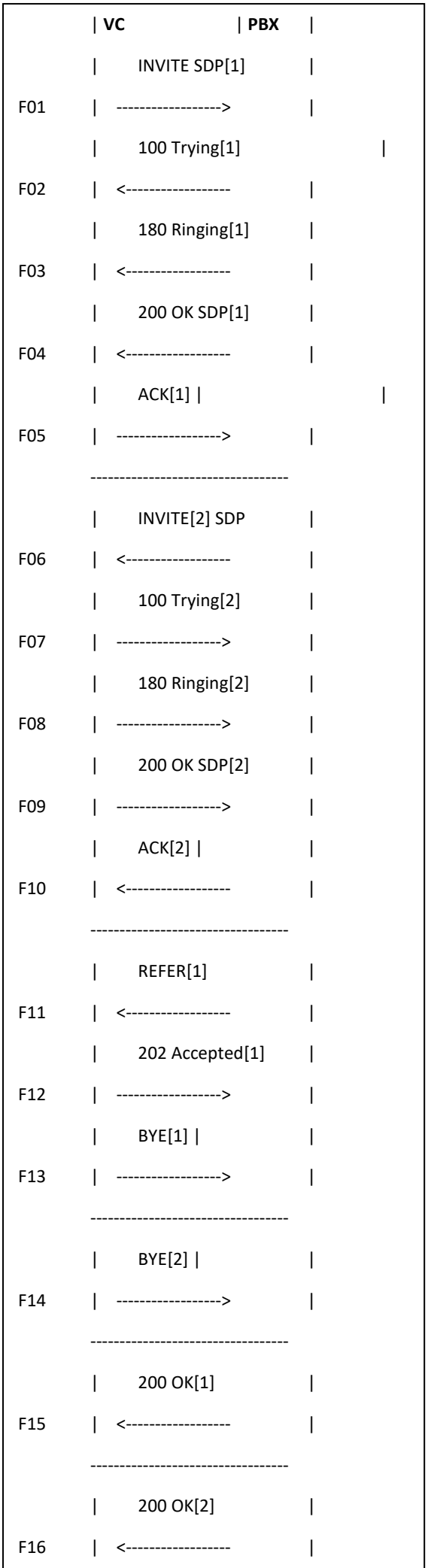
```
SIP/2.0 200 OK
Via: SIP/2.0/UDP
122.56.255.168:5060;branch=z9hG4bKcec3lv20e820shcql331cdcp18oj0.1
From: <sip:048010550@122.56.252.6;user=phone>;tag=SDfkeje01-1771243513-
1382309365834-
To: "Martin Reid"<sip:44718607@telecom.co.nz;user=phone>;tag=atobcall-
12345678
Call-ID: SDfkeje01-5091d980228be03994770cbd2dce4cfb-v300g00
CSeq: 738690087 BYE
User-Agent: SIP Test
Content-Length: 0
```

5.12 Call Transfer Attended using REFER with Replaces

This call transfer has two dialogs. Alice calls Bob on dialog[1] and they chat, Bob initiates a new call to Carol on dialog [2] and they chat; Bob decides to transfer Alice. The transfer uses dialog[1] and replaces Bob so that Alice and Carol are joined.
The authentication of the INVITE & the REFER has been omitted.
This use case is typically seen with call hold being initiated this has been omitted to simply reduce the message count of the example.

Directory Numbers

Pilot User AoR:	42291860
transferee:	042201050
transferor:	042291861
transfer-target	042295101


| VC | PBX |
| INVITE SDP[1] |
F01 | ----------> |
| 100 Trying[1] |
F02 | <---------- |
| 180 Ringing[1] |
F03 | <---------- |
| 200 OK SDP[1] |
F04 | <---------- |
| ACK[1] | |
F05 | ----------> |
| INVITE[2] SDP |
F06 | <---------- |
| 100 Trying[2] |
F07 | ----------> |
| 180 Ringing[2] |
F08 | ----------> |
| 200 OK SDP[2] |
F09 | ----------> |
| ACK[2] | |
F10 | <---------- |
| REFER[1] |
F11 | <---------- |
| 202 Accepted[1] |
F12 | ----------> |
| BYE[1] | |
F13 | ----------> |
| BYE[2] | |
F14 | ----------> |
| 200 OK[1] |
F15 | <---------- |
| 200 OK[2] |
F16 | <----------

F01

```
INVITE sip:42291861@192.168.1.32:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP
10.111.111.245:5060;branch=z9hG4bKihl9mh301g317h0im5c0.1
From: <sip:042201050@10.207.44.132;user=phone>;tag=SDrd1ed01-1531164018-
1381462287561-
To: "SIPI Child 1"<sip:42291861@telecom.co.nz;user=phone>
Call-ID: SDrd1ed01-9e013c6cd4858e18cababa4acfb62c23-v3000i1
CSeq: 315150949 INVITE
Contact: <sip:042201050@10.111.111.245:5060;transport=udp>
Supported: 100rel
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: application/media_control+xml,application/sdp,multipart/mixed
Max-Forwards: 69
Content-Type: application/sdp
Content-Length: 161

v=0
o=BroadWorks 4023 1 IN IP4 10.111.111.245
s=-
c=IN IP4 10.111.111.245
t=0 0
m=audio 13650 RTP/AVP 8 101
a=rtpmap:101 telephone-event/8000
a=ptime:20
```

F02

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP
10.111.111.245:5060;branch=z9hG4bKihl9mh301g317h0im5c0.1
From: <sip:042201050@10.207.44.132;user=phone>;tag=SDrd1ed01-1531164018-
1381462287561-
To: "SIPI Child 1"<sip:42291861@telecom.co.nz;user=phone>
Call-ID: SDrd1ed01-9e013c6cd4858e18cababa4acfb62c23-v3000i1
CSeq: 315150949 INVITE
User-Agent: SIPInspector_v_1.50
Content-Length: 0
```

F03

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP
10.111.111.245:5060;branch=z9hG4bKihl9mh301g317h0im5c0.1
From: <sip:042201050@10.207.44.132;user=phone>;tag=SDrd1ed01-1531164018-
1381462287561-
To: "SIPI Child 1"<sip:42291861@telecom.co.nz;user=phone>;tag=atobcall-
12345678
Call-ID: SDrd1ed01-9e013c6cd4858e18cababa4acfb62c23-v3000i1
CSeq: 315150949 INVITE
Contact: <sip:42291861@192.168.1.32:5060;transport=UDP>
User-Agent: SIPInspector_v_1.50
Content-Length: 0
```

F04

```
SIP/2.0 200 OK
```

```
Via: SIP/2.0/UDP
10.111.111.245:5060;branch=z9hG4bKihl9mh301g317h0im5c0.1
From: <sip:042201050@10.207.44.132;user=phone>;tag=SDrd1ed01-1531164018-
1381462287561-
To: "SIPI Child 1"<sip:42291861@telecom.co.nz;user=phone>;tag=atobcall-
12345678
Call-ID: SDrd1ed01-9e013c6cd4858e18cababa4acfb62c23-v3000i1
CSeq: 315150949 INVITE
Contact: <sip:42291861@192.168.1.32:5060;transport=UDP>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
User-Agent: SIPInspector_v_1.50
Supported: replaces
Content-Type: application/sdp
Content-Length:203

v=0
o=111 843670094 843670094 IN IP4 192.168.1.32
s=-
c=IN IP4 192.168.1.32
t=0 0
m=audio 6000 RTP/AVP 8 101
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
```

F05

```
ACK sip:42291861@192.168.1.32:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP
10.111.111.245:5060;branch=z9hG4bKl9mlgv00a89gah8he4g1.1
From: <sip:042201050@10.207.44.132;user=phone>;tag=SDrd1ed01-1531164018-
1381462287561-
To: "SIPI Child 1"<sip:42291861@telecom.co.nz;user=phone>;tag=atobcall-
12345678
Call-ID: SDrd1ed01-9e013c6cd4858e18cababa4acfb62c23-v3000i1
CSeq: 315150949 ACK
Contact: <sip:042201050@10.111.111.245:5060;transport=udp>
Max-Forwards: 69
Content-Length: 0
```

F06

```
INVITE sip:042295101@telecom.co.nz SIP/2.0
Via: SIP/2.0/UDP 192.168.1.32:5060;branch=z9hG4bK-v1
From: <sip:42291861@telecom.co.nz>;tag=btoccall-12345678
To: <sip:042295101@telecom.co.nz>
Call-ID: sptest-123456789-orig
CSeq: 1 INVITE
P-Asserted-Identity: <sip:42291860@telecom.co.nz:5060>
Max-Forwards: 70
Contact: <sip:42291861@192.168.1.32:5060>
User-Agent: Cisco/Sipi
Content-Type: application/sdp
Content-Length: 207
```

```
v=0
o=AJT 843670094 1 IN IP4 192.168.1.32
s=-
c=IN IP4 192.168.1.32
t=0 0
a=sendrecv
m=audio 6001 RTP/AVP 8 101
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
```

F07

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.1.32:5060;received=172.18.10.90;branch=z9hG4bK-
v1;rport=1094
From: <sip:42291861@telecom.co.nz>;tag=btoccall-12345678
To: <sip:042295101@telecom.co.nz>
Call-ID: sptest-123456789-orig
CSeq: 1 INVITE
```

F08

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.168.1.32:5060;received=172.18.10.90;branch=z9hG4bK-
v2;rport=1094
From: <sip:42291861@telecom.co.nz>;tag=btoccall-12345678
To: <sip:042295101@telecom.co.nz>;tag=SDvq5i199-2101189040-1381462297347
Call-ID: sptest-123456789-orig
CSeq: 2 INVITE
Supported:
Contact: <sip:042295101@10.111.111.245:5060; transport=udp>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
Content-Length: 0
```

F09

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.1.32:5060;received=172.18.10.90;branch=z9hG4bK-
v2;rport=1094
From: <sip:42291861@telecom.co.nz>;tag=btoccall-12345678
To: <sip:042295101@telecom.co.nz>;tag=SDvq5i199-2101189040-1381462297347
Call-ID: sptest-123456789-orig
CSeq: 2 INVITE
Supported:
Contact: <sip:042295101@10.111.111.245:5060;transport=udp>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: application/media_control+xml,application/sdp
Content-Type: application/sdp
Content-Length: 236

v=0
o=BroadWorks 4028 1 IN IP4 10.111.111.245
s=-
c=IN IP4 10.111.111.245
t=0 0
```

```
m=audio 13652 RTP/AVP 8 0 101
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=sendrecv
```

F10

```
ACK sip:042295101@10.111.111.245:5060;transport=udp SIP/2.0
Via: SIP/2.0/UDP 192.168.1.32:5060;branch=z9hG4bK-v2
From: <sip:42291861@telecom.co.nz>;tag=btoccall-12345678
To: <sip:042295101@telecom.co.nz>;tag=SDvq5i199-2101189040-1381462297347
Call-ID: sptest-123456789-orig
CSeq: 2 ACK
Max-Forwards: 70
Contact: <sip:42291861@192.168.1.32:5060>
Content-Length: 0
```

F11

```
REFER sip:042201050@10.111.111.245:5060;transport=udp SIP/2.0
Via: SIP/2.0/UDP 192.168.1.32:5060
From: <sip:42291861@telecom.co.nz;user=phone>;tag=atobcall-12345678
To: <sip:042201050@10.207.44.132;user=phone>;tag=SDrd1ed01-1531164018-
1381462287561-
Referred-By: <sip:42291861@telecom.co.nz>
Call-ID: SDrd1ed01-9e013c6cd4858e18cababa4acfb62c23-v3000i1
CSeq: 100 REFER
Max-Forwards: 70
Expires: 240
Contact: <sip:42291861@192.168.1.32:5060;transport=UDP>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Refer-To: <sip:042295101@telecom.co.nz?Replaces=sptest-123456789-
orig%3bfrom-tag%3dbtoccall-12345678%3bto-tag%3dSDvq5i199-2101189040-
1381462297347>
User-Agent: SIPInspector_v_1.50
Supported: replaces
Content-Length: 0
```

F12

```
SIP/2.0 202 Accepted
Via: SIP/2.0/UDP 192.168.1.32:5060;received=172.18.10.90;rport=1094
From: <sip:42291861@telecom.co.nz;user=phone>;tag=atobcall-12345678
To: <sip:042201050@10.207.44.132;user=phone>;tag=SDrd1ed01-1531164018-
1381462287561-
Call-ID: SDrd1ed01-9e013c6cd4858e18cababa4acfb62c23-v3000i1
CSeq: 100 REFER
Contact: <sip:042201050@10.111.111.245:5060;transport=udp>
Content-Length: 0
```

F13

```
BYE sip:42291861@192.168.1.32:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP
10.111.111.245:5060;branch=z9hG4bKt1bhbs00dgf0ahkpq6c0.1
```

```
From: <sip:042201050@10.207.44.132;user=phone>;tag=SDrd1ed01-1531164018-
1381462287561-
To: "SIPI Child 1"<sip:42291861@telecom.co.nz;user=phone >;tag=atobcall-
12345678
Call-ID: SDrd1ed01-9e013c6cd4858e18cababa4acfb62c23-v3000i1
CSeq: 315150950 BYE
Max-Forwards: 69
Content-Length: 0
```

F14

```
BYE sip:42291861@192.168.1.32:5060 SIP/2.0
Via: SIP/2.0/UDP
10.111.111.245:5060;branch=z9hG4bKuhhid510dggg8hkpe7s0.1
From: <sip:042295101@telecom.co.nz>;tag=SDvq5i199-2101189040-
1381462297347
To: <sip:42291861@telecom.co.nz>;tag=btoccall-12345678
Call-ID: sptest-123456789-orig
CSeq: 315155773 BYE
Max-Forwards: 69
Content-Length: 0
```

F15

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP
10.111.111.245:5060;branch=z9hG4bKt1bhbs00dgf0ahkpq6c0.1
From: <sip:042201050@10.207.44.132;user=phone>;tag=SDrd1ed01-1531164018-
1381462287561-
To: "SIPI Child 1"<sip:42291861@telecom.co.nz;user=phone>;tag=atobcall-
12345678
Call-ID: SDrd1ed01-9e013c6cd4858e18cababa4acfb62c23-v3000i1
CSeq: 315150950 BYE
User-Agent: SIPInspector_v_1.50
Content-Length:0
```

F16

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP
10.111.111.245:5060;branch=z9hG4bKuhhid510dggg8hkpe7s0.1
From: <sip:042295101@telecom.co.nz>;tag=SDvq5i199-2101189040-
1381462297347
To: <sip:42291861@telecom.co.nz>;tag=btoccall-12345678
Call-ID: sptest-123456789-orig
CSeq: 315155773 BYE
User-Agent: SIPInspector_v_1.50
Content-Length:0
```

6 Customer Premises Environment

The customer network contains the customer's SIP-enabled VoIP equipment i.e., an IP-PBX with Plain Old Telephone Service (POTS), digital or H.323/Skinny Call Control Protocol (SCCP) handsets, or a fully integrated SIP VoIP solution containing SIP enabled PBX and handsets. The customer network provides connectivity from the Spark demarcation point (CLNE LAN interface) and those devices.

Design of the customer's network is outside the scope of this document however, below are general guidelines for interconnection and information on IP-PBX/endpoint support.

6.1 Endpoint connection models

The CLNE supports two connection models. The customer is free to chose the method that most suits their needs.

6.1.1 CLNE directly connected to the Customer PBX

This solution is used when the only SIP-enabled device is the customer's PBX.

The CLNE LAN interface is on the same subnet as the PBX's IP interface. This connection can be done physically, with the use of a crossover cable, or via an Ethernet switch. Neither the CLNE nor the PBX need routing information as there are no routers between them.

In this scenario all signalling and media traffic passes between the CLNE and the customer's PBX.

6.1.2 CLNE connects to Customer LAN/WAN

This solution is used when there are many, distributed endpoints within the customer network which support SIP such as SIP handsets, media gateways etc.

The CLNE is connected to the customer LAN/WAN (possibly via the customer's firewall). The CLNE has a default static route configured if required, to a customer's next hop firewall or router. This default static route will allow the CLNE to reach the customer SIP endpoints.

6.1.3 CPE IVR

The customer may have their own IVR system within their own enterprise network. Integration of this for Voice Connect calls to/from the customer's IVR is the responsibility of the customer. As IVRs commonly use DTMF, customers are advised to support both RFC2833 and clear channel to ensure maximum support for remote endpoints.

6.1.4 Switches & Routers

The customer may implement switches and routers infrastructure between the Voice Connect CLNE and the PBX. As outlined in section 2.1.1, some PBXs provide a distributed architecture and some utilise a centralised model. The use of a customer-owned switching/routing fabric allows either to function. A limitation is that the CLNE can only interface to one routing point. Any other customer routers must interface to this router.

6.1.5 Firewall

The customer may decide to provide their own firewall between the Voice Connect CLNE and PBX. If included, the customer or their integrator assumes the responsibility for ensuring the Voice Connect service operates correctly through it and that it does not impact end to end call quality. The following ports must be opened on the customer firewall to allow Voice Connect calls to work by permitting them to pass through it.

SIP Signalling Port=5060

RTP/RTCP Media Port = 1024 --> 65535

The firewall may be a routing firewall, which may be a specific firewall dedicated/tailored to voice calls.

6.2 Customer IP Addressing

The diagram below describes a situation where the Customer has a switched LAN environment that connects IP PBX and CLNE.

IP Addressing:

IP-An Customers provided Private or Public IP addressing
IP-B Spark managed, NATTed IP address in range 172.18.0.0/16
IP-Cn Spark managed, provided to customer, Public IP addressed service components such as DNS servers and Outbound Proxy Server addresses.

6.3 PBX Configuration

6.3.1 Common Settings for all PBXs

These settings also need to be applied to any layer 5 device installed by the customer between the PBX SIP Trunking CLNE and PBX, e.g. their own Cisco CUBE, SBC 3800, voice firewall, etc.

	Information	**Apply to or Exceptions**
DHCP	Set in PBX	All
SIP Trunk IP Address	SIP trunk or SIP	IP address of Outbound Proxy (SBC)
Transport Protocol – SIP Signalling (SIP)	UDP/TCP	All PBXs
Codec (Media Stream)	Set in PBX	All G.711 A-law or G.722 with 20 ms packetisation
Early media (Media Stream)	Yes	All PBXs
VAD/CNG also silence suppression (Media Stream)	Off	All PBXs
DTMF (Media Stream)	RFC2833 Clear Channel	RFC2833 - All PBXs must have PTI set to “101”. Clear Channel – All PBXs
Transport Protocol – Media (RTP/RTCP) (Media Stream)	UDP	All PBXs The use of TCP for the media stream is not supported.
Calling Number - Outgoing	0+NN	All PBXs
Called Number - Outgoing	dialled number (no preceding 1)	All PBXs
Calling Number - Incoming	0+NN	All PBXs
Dial Plan	Set in PBX	All PBXs Note: Refer to section 4.6 Feature Access Codes for network-based feature access codes
Invite Expires Timer	30 sec	All PBXs
End of Dialling Digit	#	All PBXs

7 Service Features

Feature	Description
Direct Dial In (DDI)	The ability for PBX extensions to be associated with a public Directory Number that can be dialled by external parties to route directly to an PBX extension without having to go through an operator/IVR.
Direct Outgoing Dialling (DOD)	The ability for PBX extensions to dial out of the PBX to the public telephony network and be identified to the destination with that identity (Directory Number).
Pilot Numbers	The Voice Connect solution can be configured to insert a Pilot number as the CLI on outgoing calls if: • For extensions that do not have a DDI, • There is no CLI, • The CLI is not recognised. • Pilot numbers have multiple simultaneous calls (incoming and outgoing). • Features assigned to Pilot numbers are inherited by non-DDI extensions.
Extension Dialling	Allows extension dialling between members within the same Group, or other groups within the enterprise.
Voice VPN	Allows extension dialling outside of a Group (to other Groups or other networks, e.g. PSTN).
Caller Display (Calling Line ID Presentation (CLIP))	Caller Display is a terminating feature that allows a user to receive calling line ID information (Calling Number and Calling Name). Redirecting Line information (number and name) are also provided by assigning this feature.
Number Withhold (Calling Line ID Restriction (CLIR)) – permanent	Number Withhold is an originating service that blocks calling party address information from being presented to the called user for every call.
Number Withhold (Calling Line ID Restriction (CLIR)) – per call	Number Withhold per call service is an originating service that allows the caller to decide, on a call-by-call basis, whether to restrict visibility of the calling party number to the called party.
Calling Line ID Delivery per call	Calling Line ID Delivery per call service is an originating service that allows the caller to decide, on a call-by-call basis, whether to override the permanent CLIR

	assigned to their number and allow visibility of the calling party number to the called party.
Calling Line ID Restriction Override (CLIRO)	Calling Line ID Restriction Override is a terminating service that allows the called party to override any CLIR setting on the calling party and thus identify who originated the call to them.
Selective Call Acceptance (optional service)	Enables a user to define criteria that causes certain incoming calls to be allowed. If an incoming call meets user-specified criteria, the call is allowed to complete to the user. All other calls are blocked and the caller is informed that the user does not wish to receive the call. The user controls the service via a web interface, which provides the ability to establish the criteria sets for determining which calls are allowed to complete. A criteria set is based on incoming calling line identity, time of day, and day of week. Multiple criteria sets can be defined.
Selective Call Rejection (optional service)	Enables a user to define criteria that cause certain incoming calls to be blocked. If an incoming call meets user-specified criteria, the call is blocked and the caller is informed that the user is not accepting calls. The user controls the service via a web interface, which provides the ability to establish the criteria sets for determining which calls require blocking. A criteria set is based on incoming calling line identity, time of day, and day of week. Multiple criteria sets can be defined.
Call Barring (Outgoing Calls)	The Call Barring feature prevents a subscriber from making certain types of outgoing calls.
Call Forward Always (optional service)	When Call Forward Always is active, all incoming calls are forwarded to the specified forward-to number.
Call Forward on Busy (optional service)	When Call Forward on Busy is active, incoming calls are forwarded if the endpoint is busy, either because Voice Connect has determined that the maximum number of simultaneous dialogues has been reached or because the endpoint returned a busy response.
Call Forward No Answer (CFNA) (optional service)	When Call Forward No Answer is active, an incoming call is forwarded if it is not

	answered by the endpoint before the “no-answer timer” expires.
Call Transfer	Call transfer is a call re-arrangement of an existing call in which one party is replaced with another party. Initially, the transferor is in an active call with the transferee. Then the transferor initiates a call transfer to the transfer target. Finally the transfer target gets connected to the transferee. Transferor, transferee and transfer target may be within the PBX system or behind the PSTN (VC).
Multiple Codec Support	G.711 A-Law and G.722 are supported. G.722 is preferred.
Emergency Service	Originate emergency calls – even if their service has been temporarily restricted due to non-payment of their telephone bill.
Directory Service	Allows customers to place calls to the directory services
Local Number Portability	In-port their local telephone number from a competing Local Service Provider to the Voice Connect service if they are not moving from their Local Calling Area (LCA). Telephone numbers assigned to a clients Voice Connect service can be out-ported to another carrier.
Intelligent Network (IN) Services	The PSTN IN is used by Voice Connect customers to provide the following services or to dial the following services. e.g. - 0800 - 0900 - Televoting -- The PSTN DDI Voicemail (using the existing PSTN DDI service, with the same limitations)

7.1
Feature Access Codes
The following table of codes can be used from handsets to activate/deactivate network delivered features of Voice Connect.

Feature	Code	Alternative
Call Forwarding Always Activation	*17	1417

Call Forwarding Always Deactivation	#17	1517
Call Forwarding Always Interrogate	*21	1521
Call Forwarding Busy Activation	*15	1415
Call Forwarding Busy Deactivation	#15	1515
Call Forwarding Busy Interrogate	*67	1567
Call Forwarding No Answer Activation	*16	1416
Call Forwarding No Answer Deactivation	#16	1516
Call Forwarding No Answer Interrogate	*61	1561
Calling Line ID Delivery Blocking per Call	197	0197
Calling Line ID Delivery per Call	196	0196
No Answer Timer	*39xx	1439xx

•

The alternative column provides codes to be used by handsets that do not support the '#' or '' keys.*

8 Glossary

Term	Definition
A RR DNS Query	Type A DNS request for an IPV4 Address
Access	For the Voice Connect service this means a service over either fibre 10 megabits per second (Mbps) or 100 Mbps speeds; or copper using 1, 2, 3, 5, 7Mbps speeds. Capacity for the maximum number of channels, or maximum simultaneous conversations, required by the customer is assigned as VLAN bandwidth.
AC	Area Code
B2BUA	Back to back User Agent
BroadSoft Core (BC)	The cluster of servers that comprise the BroadSoft platform.
BroadWorks (BW)	Applications that sit on the BroadSoft core platform
CAC	Call Admission Control
CC	Country Code
CDR	Call Detail Record
CLI	Calling Line Identification

CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CLNE	Customer Located Network Equipment is the Voice Connect network end-point router located on the customer's premises. The CLNE is the physical demarcation point for the Voice Connect service.
CPE	Customer Premises Equipment
CUBE	Cisco Unified Border Element. Provides IWF like functionality.
DDI	Direct Dial In.
Delay	End to End delay from Speaker to listener (Codec, packet size, packet conversion, etc)
DHCP	Dynamic Host Configuration Protocol
DN	Directory Number
DNS	Domain Name System
DSCP	Differentiated Services Code Point (the first 6 bits of the TOS octet. See TOS and ECN.)
E.164	ITU standard public telephone numbers.
EAN	Ethernet Access Node – elements of the access network provided by Chorus
EAS	Ethernet Aggregation Switch - elements of the access network provided by Chorus
ECN	Explicit Congestion Notification (last 2 bits of TOS octet. See TOS and DSCP). Always set to 00.
FQDN	Fully Qualified Domain Name
G.711 Codec	Audio Codec that allows 3.1 kHz analogue bandwidth from 64Kbit of data
G.722 Codec	Audio Codec that allows 7 kHz analogue bandwidth from 64Kbit of data
GIS	Spark Digital Internet Services
GWS	Spark Digital WAN Services
HA	High Availability
HSNS	High Speed Network Service – access delivered by Chorus
IP	Internet Protocol is the method or protocol used for communicating data across a packet switched network.
IP Address	A numerical identification and logical address assigned to devices participating in a computer network utilizing the Internet Protocol for communication between nodes.
IP PBX	IP Private Branch Exchange.
ISDN	Integrated Services Digital Network as provided by NEAX and MGC-12 exchanges

IWF	Inter Working Function. A piece of hardware or software that is situated between a client PBX and the CLNE. It may be required in some situations to modify the interface presented by the PBX to the CLNE.
Jitter	The variation in latency or delay for IP packet flows across the Voice Connect service.
LAN	Local Area Network.
Latency	The overall latency or delay for IP packet flows across the Voice Connect service.
LCA	Local Calling Area
LICA	Local Interconnect Calling Area
LMN	An acronym for Local and Mobile Number
LNP	Local Number Portability
MACs	Moves, Adds and Changes.
Media Converter	Is the termination point for fibre delivery. It provides a physical interface between the glass fibre and the Ethernet cabling
MGC	Media Gateway Controller
Migrated Telephone Numbers	Telephone numbers originally working on the PSTN but now being used on the NGN with the Voice Connect service.
MOS	Mean Opinion Score
MPLS	Multiprotocol Label Switching – Spark's internal transport network
MSSA	Multi Service Single Access
NAT	Network Address Translation
NEAX	NEC Automatic Exchange Spark's Circuit switch telephone exchanges.
NGN	Next Generation Network is Spark's new IP network.
Packet Loss	The overall percentage of IP packets lost between the source and destination Voice Connect service terminating equipment.
PAI	P-Assured-Identity header. A SIP header field used to identify a specific trunk group.
PBX	Private Branch Exchange
PE	Provider Edge – large routers that sit at the edge of the Spark network
POP	Point of Presence – access points to the BroadSoft core network
POTS	Plain Old Telephone System
PPI	P-Preferred Identity
PSTN	Public Switched Telephone Network.
PTC	Permit to Connect, is the authorisation to connect external devices to the Spark Network.

QoS	Quality of Service.
RTP	Real Time Protocol
SBC	Session Border Controller – provides signalling and access control over the calls entering the network
SIP	Session Initiation Protocol, which is an open signalling protocol for establishing any kind of real time communication session. The communication session can involve voice or multimedia communications and can be used on many different communication devices.
SLA	Service Level Agreement
Spark Provider Edge	The entry point to the edge of the Spark network.
SRV RR DNS Query	Type SRV DNS request
ToS	Type of Service (now replaces by DSCP (6 bits) and ECN (2 bits))
URI	Uniform Resource Identifier
VoIP	Voice over Internet Protocol.
VLAN	Virtual Local Area Network.
VPN	Virtual Private Network.
WAN	Wide Area Network.

Appendix 1
Test Cases for PTC229 Connection to Spark Voice connect service.

1. Registration

1.1 Test method

Initiate a registration sequence from the PBX.

- *This could be initiated by turning on the PBX power, initiating a physical reset, or issuing a software command.*

Collect Trace from Wireshark

- *First attempt will be challenged by the network with a request for authentication. The second attempt will provide the authentication details. The authentication process requires the PBX to respond with the SIP password encrypted by a once only key from the server (nonce) and the MD5 algorithm.*

Registration Successful …Y/N

Expires value (>60) ……..Y/N

- *Could be zero if PBX wanted to cancel registration*

2. Password

2.1 Test Method

Set an incorrect password and initiate the registration process. The network will respond with a "403 Authentication Failure". The PBX may attempt to re-register.

Collect Wireshark Traces

Retry Interval

1st retry……s

2nd retry……s

3rd retry……s

4th retry……s

5th retry……s

Number of retries with less than one minute intervals…….no or retries.

Is there back off to retry intervals being greater than 1 minute……..Y/N

3. Outgoing Call from Pilot Extension

3.1 Make Call from Pilot extension to network PSTN number, Answer call, check speech and press several dial keys (in band DTMF) from PSTN phone and also PBX phone while speech path open. Terminate call from firstly PBX and then PSTN (two calls required). Take Wireshark traces of both calls.

3.2 Calls set up satisfactorily …….Y/N

- *Note that VC requests authentication from PBX, so first INVITE will receive the response "401 Unauthorized". A second INVITE will provide the authentication details.*

3.3 Is caller ID correctly displayed on PSTN phone? …….Y/N

3.4 Post dial delay before PSTN phone rings (<5 secs) ……s P/F

3.5 Speech path established with in 100 ms of answering ……..ms P/F

3.6 Are RTP Events observed and tones heard when DTMF keys pushed: PBX to PSTN……..Y/N

3.7 Are RTP Events observed and tones heard when DTMF keys pushed: PSTN to PBX……..Y/N

3.8 Call cleared down from PBX satisfactorily……Y/N

3.9 Call cleared down form PSTN satisfactorily ……Y/N

3.10 During SIP messages IP DSCP QoS marking (CS3= 011000 or AF31=011010) …… Y/N

3.11 During RTP IP DSCP QoS marking (EF=101110)……Y/N

3.12 Additional tests to other networks (mobile), national toll calls, international toll calls, service numbers (111, 911) etc

- *This tests the PBX's outgoing routing tables, and the ability to allow/bar some calls, and deal with different number lengths. As potential new destinations are always becoming available, testing would normally involve showing that the PBX can be programmed to call numbers and block with different lengths e.g. 3 digit service numbers, international numbers with up to 16 digits (including 00 escape digits).*

4. Outgoing call with CLIR

4.1 Make a call to a PSTN number from PBX extension (Pilot or other)and prefix the number with 0197. Collect Wireshark Trace.

4.2 Check that Caller ID is not presented at PSTN phone

5. Incoming Call to Pilot Extension

5.1 Make Call from PSTN number to Pilot extension, Answer call, check speech and terminate call from firstly PBX and then PSTN (two calls required). Take Wireshark traces of both calls.

5.2 Calls set up satisfactorily? …….Y/N

5.3 Is caller ID correctly displayed on PBX phone? …….Y/N

5.4 Post dial delay before PBX phone rings (<5 secs) ……s P/F

5.5 Speech path established with in 100 ms of answering ……..ms P/F

5.6 Call cleared down from PBX satisfactorily……Y/N

5.7 Call cleared down form PSTN satisfactorily ……Y/N

5.8 During SIP messages IP DSCP QoS marking (CS3= 011000 or AF31=011010) …… Y/N

5.9 During RTP IP DSCP QoS marking (EF=101110)……Y/N

6. Outgoing Call from DID extension

6.1 Make outgoing call from DID extension to PSTN number and collect Wireshark trace

6.2 Call set-up satisfactorily? ……..Y/N

6.3 Caller ID of extension phone received at PSTN phone? ……Y/N

6.4 P-Asserted Identity included in SIP INVITE message:- “P-Asserted-Identity:<sip:pilot number@telecom.co.nz>”……Y/N

- *The P-Asserted-Identity informs the network (VC) that the unknown extension number in the “From” field is associated with the (registered) pilot number*.

7. Incoming Call to DID extension

7.1 Make incoming call from PSTN to DID extension and collect Wireshark traces.

7.2 Call set-up satisfactorily……Y/N

7.3 Caller ID from PSTN received correctly…….....Y/N

7.4 Call cleared down satisfactorily from PSTN……Y/N

7.5 Call cleared down satisfactorily from PBX extension……Y/N

8. Outgoing Call from non-DDI extension

8.1 Make call from non-DDI extension and collect Wireshark traces.

8.2 Call set up and cleared down Satisfactorily?.....Y/N

8.3 Is Caller ID received by the PSTN Phone?.....Y/N

The additional tests required by sections 3 and 5 shall be spot checked for other call scenarios and tested comprehensively if there is any doubt of full compliance.

9. Call Diversion/Call forward and Call Transfer

There are a number of ways of implementing Call Diversion/Call Forward and Call Transfer. It is not mandatory for a PBX to implement these functions, but if they are implemented they shall comply with the following requirements.

9.1 Call Diversion or Call Forward

9.1.1 Make a call from the PSTN to the PBX with a call diversion set on the called party number, and collect Wireshark traces. Where conditional call diversion can be set, for example call forward always, call forward on busy, Call forward on no answer etc, each scenario shall be tested.

9.1.2 Call diverted to the correct destination……..Y/N

9.1.3 Call cleared satisfactorily from PSTN……Y/N

9.1.4 Call cleared satisfactorily from PBX……Y/N

9.2 Call Transfer

9.2.1 Make a call from the PSTN to the PBX then transfer to another number:

a) within the PBX …. Correct destination……Y/N

b) back to the PSTN …. Correct destination……Y/N

and collect Wireshark traces.

9.2.2 For each of the above categories:

a) the transferor shall hang up while ringing tone is still present, that is, before the transfer target has answered the phone. Transfer completed satisfactorily ……..Y/N

b) the transferor shall wait for and establish a call with the transfer target before hanging up. Transfer completed satisfactorily ……..Y/N

9.2.3 For each scenario, check that the correct Caller ID is presented at the transfer target.

Correct Caller ID: ……. Y/N

9.2.4 Call cleared satisfactorily from PBX (transfer target)…….Y/N

9.2.5 Call cleared satisfactorily from PSTN ……Y/N

Appendix 2

PTC 229 Test Schedule

Test Report to PTC 229

Report No:…….

Laboratory:……

Date of issue:…….

Client:……..

Manufacturer:…….

Product name:……..

Product Serial Number:……..

Hardware version:……..

Firmware Version:……..

Configuration details: Document as appropriate. Enough detail shall be captured to enable system to meet all the compliance requirements.

Product Description:

SIP trunks:……

FXS ports:……..

FXO trunks:……

ISDN trunks:……..

SIP Phone ports:…….

Proprietary phone ports:……

Product functional details:

……
……
……
……
……
……
……
……

Overall Compliance:…….Yes/No

Comments:

……
……
.....

Test no.	Test Description	Limit for compliance	Result + traces	Configuration for compliance	Comply Y/N	Comment
1	**Registration**	Registration successful	……Y/N			
	Expires Value	> 60	…..sec			
2	**Password**					
	Intervals between retries of unsuccessful registrations	< 3 retries at <60 sec interval, then >60 sec	1st …..s 2nd…..s 3rd……s 4th……s etc			
3	**Outgoing Call from Pilot to PSTN**					
3.2	Call setup satisfactorily		……Y/N			
3.3	Caller ID correctly displayed on far end phone		……Y/N			
3.4	Post dial delay before PSTN phone rings	<5 sec	……s			
3.5	Speech path established	<100 ms	……ms			
3.6	RTP “events” observed and tones heard on PSTN phone		……..Y/N			
3.7	RTP “events” observed and tones heard on PBX phone		……..Y/N			
3.8	Call cleared down from PBX		……Y/N			
3.9	Call cleared down from PSTN		…….Y/N			
3.10	DSCP during SIP signalling	CS3 or AF31	……DSCP marking			
3.11	DSCP during RTP	EF	……DSCP marking			
3.12	Other outgoing call scenarios as necessary					

4	**Outgoing call with CLIR**	No calling party number displayed on PSTN phone	……Displayed/not displayed			
5	**Incoming Call to Pilot Extension**					
5.2	Call established satisfactorily		…..Y/N			
5.3	Caller ID displayed		…..Y/N			
5.4	Post dial delay before PX phone rings	<5 s	……s			
5.5	Speech path established after phone answered	< 100 ms	……..ms			
5.6	Call cleared from PBX		……..Y/N			
5.7	Call cleared from PSTN		……..Y/N			
5.8	DSCP during SIP signalling	CS3 or AF31	……DSCP marking			
5.9	DSCP during RTP	EF	……DSCP marking			
6	**Outgoing Call from DID extension**					
6.2	Call set up satisfactorily		…….Y/N			
6.3	Caller ID of extension phone received at PSTN phone		……Y/N			
6.4	PAI included in INVITE message		…….Y/N			
7	**Incoming Call to DID extension**					
7.2	Call set up satisfactorily		……..Y/N			
	Caller ID from PSTN receiver correctly		……..Y/N			
	Call cleared from PSTN		……..Y/N			
	Call cleared from PBX?		……..Y/N			

8	**Outgoing Call from DID extension**					
8.2	Call set up and cleared down satisfactorily		…….Y/N			
8.3	Is correct Caller ID received by PSTN Phone		…….Y/N			
9.1	**Call Diversion/Call Forward**					
9.1.2	Call diverted to correct destination? Caller ID correct?		…….Y/N …….Y/N			
9.1.3	Call cleared from PSTN		…….Y/N			
9.1.4	Call cleared from PBX		…….Y/N			
9.2	**Call Transfer**					
9.2.1(a) 9.2.2(a)	Call transferred to correct destination within PBX without waiting for transfer target to answer? Caller ID correct?		…….Y/N …….Y/N			
9.2.3	Call Cleared from PBX?		…….Y/N			
9.2.4	Call Cleared from PSTN?		…….Y/N			
9.2.1(b) 9.2.2(a)	Call transferred to correct destination in PSTN without waiting for transfer target to answer? Caller ID correct?		…….Y/N …….Y/N			
9.2.3	Call cleared from PBX?		…….Y/N			

9.2.4	Call cleared from PSTN		…….Y/N			
9.2.1(a) 9.2.2(b)	Call transferred to correct destination within PBX after transfer target has answered and established a speech path? Caller ID correct?		…….Y/N …….Y/N			
9.2.3	Call cleared from PBX		…….Y/N			
9.2.4	Call cleared from PSTN		…….Y/N			
9.2.1(b) 9.2.2(b)	Call transferred to correct destination in PSTN after transfer target has answered and established a speech path? Caller ID correct?		…….Y/N …….Y/N			
9.2.3	Call cleared from PBX		…….Y/N			
9.2.4	Call cleared from PSTN		…….Y/N			