SIP Trunk Technical Description

Version	Date	Description
1.0	1st February 2014	Document creation
1.1	1St August 2014	Branding and name changes
1.2	1st November 2014	Addition of the Active – Standby Resilience+ option

Contents

1.0 Introduction

This document provides the technical specification of our SIP Trunking service, also known as IP Direct Connect and is written for Network Engineers, System Administrators, Field Engineers, and Technical Consultants who have been tasked with setting up, managing, troubleshooting our SIP Trunking service. It has been assumed that those who use it will have a basic knowledge of VoIP services and protocols.

The document should be read in conjunction with the SIP Trunk Service Description.

2. Service Overview

IP Direct Connect (IPDC) is the product name for our SIP Trunking service which provides VoIP connectivity for certified PBXs, allowing inbound and outbound telephony through Gamma's network for termination with both national and international destinations.

Our SIP Trunking service uses SIP (Session Initiation Protocol) as the signalling method and offers both Public and Private Access to the service depending on the specific customer needs.

Please note – This technical description relates to the core SIP Trunking service and excludes the IP access to the Gamma network (whether supplied by Gamma or not) and any Customer Premises Equipment (CPE).

Our SIP Trunking service includes the following:

- CLIP (Calling Line Identity Presentation);
- CLIR (Calling Line Identity Restriction);
- Call Park, Transfer & Conferencing
- Emergency Call Divert
- CallGuard
- CLI presentation flexibility
- Call Admission Control
- Call barring
- Fax and DTMF support

The features listed above are supported in the Gamma network, however it should be noted that the features are not guaranteed to be supported on every Customer Premises Equipment (CPE) platform connected to our SIP Trunking Service because of vendor interoperability issues.

Our SIP Trunking provides SIP signalling as a method for Communication Providers to inter-connect with Gamma's VoIP network, supporting calls to/from the PSTN as well as VoIP to VoIP calling between SIP accounts created within our SIP Trunking service.

The following types of calls will be supported across this interface:

- Voice calls to/from PSTN or geographic destinations (01,02)
- Voice calls to/from non-geographical, corporate or VoIP numbers (03, 05, 08)
- Voice calls to/from Premium numbers (09),UK, International)
- Voice calls to/from Mobile destinations (07)

- Voice calls to/from International destinations (00..)
- Operator, Emergency and non-Emergency calls (100, 101,111,112, 116xxx, 118, 123 1800x, 195, 999)

Our SIP Trunking service can be accessed via public internet or private interconnects and these connectivity options include the following:

- Gamma provided Private and Public connections such as Gamma IP Assured or Ethernet
- Public internet via third party Internet Service Providers (ISPs)
- Private Interconnect – Public IP Addressing – Layer 3 routing
- Private Interconnect – Private IP Addressing – Layer 2 VLAN

We offer three design options as standard for the configuration of the customer's SIP Trunking service.

- A single site working off a single Gamma SBC HA cluster.
- Dual sites in active / standby mode working off different Gamma SBC HA clusters.
- Dual sites in load-balanced mode working off different Gamma SBC HA clusters.

3. Service Features

3.1. Calling Line Presentation (CLIP)

Calling Line Identification Presentation (CLIP) is a service that transmits a caller's number to the called party's telephone equipment during the ringing signal.

If the CPE connected to the Gamma network presents a geographic number in the UK National format, the Gamma Network will pass these details as the A-Number CLI into the PSTN or Mobile network. This outbound presentation will be supported by default if the number presented is as follows:

- A number in the UK national format without a leading zero presented by the Customer Premises equipment (CPE) as the A-number.
- A Gamma provided Geographic Number that is allocated to the Endpoint at order creation
- A Gamma provided Geographic Number that is allocated to the Endpoint at a later date via a Customer Change Request
- A Geographic number that is ported from another Carrier to the Gamma Network

The A-number is checked against a database on the Gamma network of geographic numbers that are allocated to the SIP Trunking Endpoint. If the number presented does not meet the above criteria, the A-Number CLI presented will be a default CLI, which is the first number in the Gamma allocated Geographic DDI range. If the presented number meets these criteria, the A-Number CLI is presented to the called party.

When CLIP is requested by the calling party on an inbound call towards the CPE, we will ensure that all CLI information is passed to the SIP trunk endpoints; those headers being From, Contact and Privacy header (PAID/RPID)

For example:

Headers contained within Invite towards SIP trunk endpoint

From: <sip:+441625827748@83.245.6.117>;tag=3541226335-339769

Contact: <sip:+441625827748@83.245.6.117>

P-Asserted-Identity: <sip:+441625827748@83.245.6.117>

NOTE: With CLIP, no modifications are performed for SIP trunk untrusted requirements.

3.2. Calling Line Restriction (CLIR)

When the calling (A-Party) has requested privacy (CLIR), we will enforce privacy in accordance with RFC3325. Calling party information, including From Address, Contact and associated Privacy Header (PAID) are withheld from an endpoint.

For calls from the customer to Gamma, the customer must indicate that CLI is to be withheld by the following mechanism:

- RFC3261 Section 8.1.1.3 and 20.20 which describes the use of an "Anonymous" display field to the From: header to indicate that the client is requesting privacy
- SIP Privacy which is described by RFC 3323 and RFC 3325

For calls from Gamma to the customer CPE:

- the From address is set to - “Anonymous”<sip: anonymous@anonymous.invalid> as per RFC 3323, the contact header is set to Anonymous and the Privacy header (P-Asserted-Identity RFC 3325) is removed from the outbound INVITE to the SIP trunk endpoint to provide true CLI restriction.
- If the Privacy header contains only "id," or only "id" and "critical" values, we remove the Privacy header completely.
- The Contact user part is changed to “anonymous.”

For example:

Public Side Invite; (Going out to SIP trunk endpoint)

From: Anonymous <sip:anonymous@anonymous.invalid>;tag=3541226365-699915

Contact: <sip:anonymous@83.245.6.117:5060>

NOTE: NO PAID Header, it has been removed to provide the calling party full anonymity.

3.3. Call Park, Transfer & Conferencing

This service provides the features listed below in the majority of cases but are not guaranteed on every platform connected to SIP trunks because of vendor interoperability issues:

- Call Parking
- Call Transfer
- Conferencing

These features are supported via the SIP re-invite mechanism

3.4. Emergency Call Divert

This service provides the facility to pre-configure call diverts for both individual numbers and DDI number ranges from the portal. Under failure conditions, the customer can contact us and request activation either of all pre-configured numbers with a single action, or activation of individual diverts as necessary. .

Deactivation is performed in the same manner by contacting us and requesting deactivation.

The diverted destinations are subject to the same call barring option as the main SIP trunk, e.g. if the user does not allow calls to mobiles, then the divert destination options will also exclude mobile numbers. The customer will be billed for the diverted leg for all diverted calls.

We do not support emergency diverts to international or other numbers which exceed 11 digits in length. In addition, customers are constrained to a total maximum of 100 emergency call diverts configured per endpoint at any point in time.

Please note that the emergency diverts are enabled within the Gamma core network. The range of standard SIP trunk endpoint features (e.g. CallGuard alerts, CLI flexibility, call admission control) do not apply to CLIs with emergency diverts enabled.

3.5. CallGuard Alerts

SIP Trunking endpoints are potentially vulnerable to fraudulent spend, particularly if the customer were to adopt weak access security to their PBX. The CallGuard alert function allows customers to set pre-arranged spend limits on individual SIP trunks.

These spend limits can be set to monitor both 24hr and 7 day periods with individual figures associated with both. On reaching 85% of the maximum spend in any period, an email and SMS alert will be sent to the customer. If the spend reaches 100% of the agreed limit a further email and SMS will be sent to the customer and all subsequent calls from that end-point will be barred.

Service can be restored by the customer contacting us to discuss the barring of the service.

Note:

- Calls to the emergency services 999, 112 and 18000 will be unaffected.
- Inbound Calls are not affected
- Calls set-up via the emergency divert function are excluded in the CallGuard fraud calculation.

3.6. CLI Flexibility

As an optional service, customers can enable the ability to present non Gamma registered CLIs as the Presentation A-Number CLI.

The service supports the presentation of the following A-Number CLI types:

- National Significant (1NNNNNNNNN, 2NNNNNNNNN, 3NNNNNNNNN, 7NNNNNNNNN, 8NNNNNNNNN) for UK numbers.
- National Significant with leading zero (01NNNNNNNNN, 02NNNNNNNNN, 03NNNNNNNNN, 07NNNNNNNNN, 08NNNNNNNNN) for UK numbers.
- E.164 (441NNNNNNNNN, 442NNNNNNNNN, 443NNNNNNNNN, 447NNNNNNNNN, 448NNNNNNNNN) for UK numbers.
- SIP E.164 - with leading plus - (+441NNNNNNNNN, +442NNNNNNNNN, +443NNNNNNNNN, +447NNNNNNNNN, +448NNNNNNNNN) for UK numbers.
- UK International (00441NNNNNNNNN, 00442NNNNNNNNN, 00443NNNNNNNNN, 00447NNNNNNNNN, 00448NNNNNNNNN) for UK numbers.
- SIP E.164 - with leading plus - (+CCNNNNNNNNN) for non-UK numbers.

- UK International (00CCNNNNNNNNN) for non-UK numbers.

The presentation of any other A-Number CLI types, badly formatted CLI A-Numbers or UK revenue sharing numbers (9NNNNNNNNN, 09NNNNNNNNN, 449NNNNNNNNN, +449NNNNNNNNN and 00449NNNNNNNNN) is not supported by Gamma and such numbers will be replaced by the default CLI, which is the first number in the Gamma allocated DDI range. The presentation number must not be a number that connects to a revenue sharing number which will generate excessive or unexpected call charges; the use of such numbers may result in the suspension and/or withdrawal of the Presentation CLI Flexible Service

Presentation of Mobile A-Number CLI types (7NNNNNNNNN, 07NNNNNNNNN, 447NNNNNNNNN, +447NNNNNNNNN and 00447NNNNNNNNN) excludes Personal numbers.

For calls made to the Emergency, Non-emergency & Operator Services (100, 101,111,112,116, 118,123,1800 and 999), only Gamma A-Number CLIs are accepted and must be in the National Significant (with or without a leading zero) or the SIP E.164 - with leading plus - format, any other A-Number CLI or A-Number CLI format will be overwritten by the default CLI, which is the first number in the Gamma allocated DDI range.

All A-Number CLIs will be "normalised" within the Gamma network to the SIP E.164 format for external presentation but we are not responsible for subsequent carriers changing the presented A-Number CLI or its format.

We will populate column/field 4 of the Gamma SIP Trunking Daily/Monthly CDRs with the Presentation A-Number CLI presented in the SIP FROM Header field.

3.7. Call Admission Control

Through a process known as Call Admission Control (CAC), the maximum call limit of an endpoint defines its capacity for routing calls in the network. SIP Trunking customers pay a fixed monthly charge for the number of concurrent calls allowed on their endpoint. As each customer endpoint will have 2 ports - one for outgoing and one for incoming - the CAC limit will be allocated to both ports to allow maximum flexibility.

Thus we will support any combination of incoming or outgoing calls provided the total number of calls does not exceed the total channel allocation (i.e. CAC limit).

- Maximum Total Calls – specifies the overall number of calls the endpoint will support, both ingress and egress.
- Maximum Ingress Calls – specifies the maximum calls that may be placed from that endpoint to the Gamma network.
- Maximum Egress Calls – specifies the maximum number of calls that may be placed to that endpoint by us

For example, if the channel limits is 100 concurrent calls, and there are 70 ingress calls, the maximum number of egress calls allowed will be 30.

In the case that the call control constraints are exceeded at a Session Border Control (SBC), the invites will be rejected with either a SIP Response 486 or 503.

3.8. Call Barring

By default, calls to international and premium numbers will be barred. Customers are able to modify their profiles to allow or restrict access to:

- International Numbers.

- Mobile Number
- Premium rate numbers (i.e. 09….).

Similarly, customers can modify their barring profile to allow or restrict all outbound and/or inbound calls. Calls to the emergency services 999, 112 remain unaffected irrespective of the barring applied.

3.9. Fax and DTMF support

The SIP Trunking service will support fax and modem transmission subject to the following constraints:

- FAX and Modem transport in band using G.711 a-law codec is supported.
- Renegotiation to T.38 is supported. (subject to interoperability testing)

The use of G729 for in-band faxes is not recommended as its compressed nature may cause tones and messages to be lost.

If the fax option for an endpoint is set to T.38 enabled then:

- The Gamma network will attempt to re-negotiate [re-INVITE] to T.38 for fax calls for ingress (Customer to Gamma) calls on detection of a fax tone.
- The Gamma network will accept a re-negotiation [re-INVITE] to T.38 for fax calls for egress (Gamma to Customer) calls.
- The re-negotiation must be done using the re-INVITE mechanism after answer.
- Due to different vendor implementations Gamma cannot guarantee T.38 interoperability with all vendors and will not accept responsibility if T.38 interoperability cannot be achieved with a specific vendors implementation.

If the fax option for an endpoint is set to T.38 disabled then:

- All fax calls will be handled as G.711 pass through providing the customer has a G.711 codec available in his media profile.

If calls are made to another partner that does not support the method of transport for the tones, we will not perform any form of inter-working between the two different methods.

The following methods will be supported to transport DTMF tones:

The Gamma core network will support the generation of ‘In-band’ or ‘RFC2833’ DTMF transport based on end to end negotiation.

- RFC2833 is the preferred method for the transport of DTMF tones. Support of RFC 2833 is dependent on successful codec negotiation and requires the payload type 101 to be assigned. RFC2833 will be used with both G.711.and G.729 codecs.
- In band over G.711 codec only

If a G729 codec is being used then DTMF tones should not be sent in-band, we will not guarantee the delivery of in-band DTMF over a G729 codec.

3.10. Emergency, Non-Emergency and other short code Calls

Important Note: This is a VoIP service as defined by Ofcom and can be used to support Emergency Services calls. Once the service is fully operational, 999/112 public emergency call services can be accessed and will be routed to the national emergency call handling agents. The CLI presented will always be the site CLI, indicated as

a VoIP service type from Gamma, so that the emergency services operator will check the address details. It is the Operators responsibility to ensure this address associated with the default site CLI is always up to date.

As a VoIP service, SIP trunks may not be possible, in the following circumstances:

- During a service outage where the customer loses connectivity for example, owing to a power outage or the failure of DSL routing equipment
- If a customer's account has been suspended

In such circumstances the customer should use their PSTN line to make the emergency call.

In addition, the customer should also be made aware that the emergency personnel would need to confirm the identity and the actual location of the caller when they dial 999/112.

The SIP trunking service supports routing the following dialled short codes:

- 999 (Access to the Emergency services)
- 100 (Access to Operator Assistance)
- 101 (The national single non-emergency number for the Police Force)
- 111 (The national single non-emergency number for the NHS)
- 112 (Access to the Emergency services)
- 116 xxx (Harmonised Services of Social value)
- 118 (UK Directory enquiries)
- 123 (Access to Speaking Clock)
- 18000* to *18009 (Access to Voice Text Services for the Deaf)
- 195 (Access to Blind & Disabled Directory Enquiry Facilities)

4. Service Characteristics

4.1. Endpoints

An endpoint represents the unique IP address used by the customer's on-site signalling proxy for Customer Premises Equipment (CPE). This signalling proxy supports SIP protocol, transferring VoIP calls to and from the CP site. Each SIP Trunking customer will have one or more endpoints configured on the Gamma SBC. CPE equipment may connect via a single endpoint or multiple endpoints for added resilience.

Endpoint Naming

The following naming convention is used for identifying endpoints on the Gamma network:

Unique Endpoint Name + suffix e.g. **DC2NYYABC1234_L1** where

- The Unique Endpoint Name (DC2NYYABC1234) is an identifier to Gamma SIP Trunking service and helps ensure all IP interconnects are easily identified for reporting and fault resolution purposes.

Resilient endpoints can be easily identified by virtue of the fact that the naming convention has been extended to append an ‘A’ (active), ‘S’ (standby), ‘R’ (Resilience+) or ‘L’ (load share) to the endpoint name. There will typically be 2 endpoints per design though may be more for larger Load share deployments

The Suffix differentiates the endpoint design type i.e.

- _L1: A Loadshare endpoint
- _A1: An Active endpoint in an Active /Standby design
- _S1: A Standby endpoint in an Active/Standby design
- _R1: A Resilience+ endpoint in an Active/Standby design

The suffix will simply increment in the case of multiple loadshare or standby endpoints associated with the same design.

4.2. Calling Plans and Number formats

Two calling plans are allocated to each endpoint: one for incoming calls from the customer to Gamma (ingress), and one for outgoing calls from Gamma to the customer (egress). It is a requirement of the SIP trunk product that the calling party (A-number) be validated to confirm the format and ensure that the number is owned by Gamma, so that the emergency services have an accurate record of the calling customer.

Presentation CLI (A-Number)

A-numbers (SIP FROM, P-Asserted-ID) should be presented in E.164 format, i.e. +441611234567. The A-number is validated by the SBC and if it is not in the Gamma range it is overwritten with an agreed network CLI from the customer’s Gamma-allocated range. It is a requirement of the SIP Trunking service that the calling party (A-number) be validated to confirm the format and ensure that the number is owned by Gamma, so that the emergency services have an accurate record of the calling customer.

If the CPE connected to the Gamma network presents a geographic number, the Gamma Network will pass these details as the A-Number CLI into the PSTN or Mobile networks. This outbound presentation will be supported by default if the number presented is as follows:

- A-numbers are presented by the Customer Premises Equipment (CPE) in the SIP FROM and P-Asserted-ID fields as E.164 format
- It is a Gamma provided Geographic Number that is allocated to the Endpoint at order creation
- A Gamma provided Geographic Number that is allocated to the Endpoint at a later date via a Customer Change Request
- A Geographic number that is ported from another Carrier to the Gamma Network

If the presented number meets these criteria the A-Number CLI will be sent to the PSTN/next hop network. The delivery of the Presentation Number is dependent on the terminating network and is not under the control of Gamma.

The A-number is checked against a database on the Gamma network of geographic numbers that are allocated to the SIP Trunking endpoint.

If the number presented does not meet the above criteria, the A-Number CLI that will be presented will be a default CLI , which is the first number in the Gamma allocated Geographic DDI range.

For ingress calls, A-numbers are sent to customers as received by Gamma from other network operators.

Network CLI (A-Number)

Every endpoint must have at least one CLI from the Gamma-allocated range i.e. a non-ported in number. This default number is known as the Network CLI and will be presented in the case of emergency calls and other call scenarios where the presented is invalid. Physical address information must be associated with a network CLI and it is the customer responsibility to ensure this address information remains current.

Gamma supports both Network and Presentation CLIs. For calls from the customer to Gamma where the call terminates on the PSTN, the SIP FROM field is mapped to the presentation CLI and the SIP P-Asserted-ID is mapped to the network CLI. The behaviour is based on NICC document ND1017 (Table 2), which specifies the mapping from SIP (FROM field) to ISUP (Presentation Number).

To ensure the correct Network CLI is passed into the Gamma network and then forwarded to the PSTN Gamma will insert the customer Network CLI Number in E.164 format into the PA-ID, replacing any value received from the customer CPE.

For calls from the PSTN to the Gamma SIP Trunking endpoint, the SIP FROM field will contain the Presentation Number when available and the P-Asserted-ID field will contain the Network Number when available. If only the Network Number is available then this will be mapped to both the SIP FROM field and the P-Asserted-ID field.

B-Numbers

B-numbers should be sent to Gamma in the following format:

- UK National 0 NSN (National Significant Number) 44 NSN, +44 NSN and 0044 NSN.
- International 00 CC NSN and +CC NSN (+CC NSN format is offered on limited connections currently, check with support).
- Service and emergency calls no leading 0(s), + or CC (Country Code) to be used.

As a default configuration B-numbers will be presented to the customer including a leading 0, (0 NSN); however this is flexible, customers can request that a prefix be inserted, or that their number range includes a country code.

Number Portability

Number portability for the SIP Trunking service is fully supported and tested. Number Porting changes are currently carried out manually, and it should be noted that BT will only port to a ‘live’ number; hence the Gamma SIP Trunking endpoints must be configured before the porting can take place.

4.3. Maximum Calls per Second (CPS)

For security reasons, we will also set limits for the maximum calls per second (CPS). The limits dependent on the endpoint design type.

Allocated Channels i.e. CAC limit	Calls/second limit
Single endpoint design	2
Resilient endpoint design	5

If this constraint is reached, we will log and reject calls with a SIP response 486 or 503.

4.4. Channel bandwidth

The table below gives an estimate of the bandwidth requirements for VoIP calls using G.711, and G.729,

The maximum number of concurrent channels equals the available bandwidth/total bandwidth, so if for example a customer has a 512 kbps upload line-speed, assuming no contention, using G.729 with a sample period of 20 ms, there will be 512/39.2 10 usable concurrent channels available. The figures for VoIP using ADSL access are similar.

Table 1 -- Suggested MINIMUM VOIP Bandwidth Consumption over Ethernet, Per Channel

Codec	Sample period	Encoded sound bandwidth	IP/UDP/RTP overhead	Ethernet overhead	Total bandwidth
G.711	10 ms	64 kbps	32 kbps	30.4 kbps	126.4 kbps
	20 ms	64 kbps	16 kbps	15.2 kbps	95.2 kbps
G.729	10 ms	8 kbps	32 kbps	30.4 kbps	70.4 kbps
	20 ms	8 kbps	16 kbps	15.2 kbps	39.2 kbps

Please note that the above represents the best case, un-contended scenario. Use of other transport protocols (e.g. IPSec), coding mechanisms or contended 'pipes' will further increase the minimum bandwidth required.

Generally G.729 is the preferred VoIP codec (the algorithm that encodes and decodes analogue voice to and from digital) when access is via ADSL, owing to its efficient use of bandwidth whilst still providing good audio quality.

4.5. Long Duration Calls

We have a policy of terminating any call that exceeds eight hours.

4.6. IP Addressing and DNS

IP version 4.0 is supported. IP Version 6.0 is not supported.

In terms of the CP interaction with Gamma's network, DNS capability, including SRV and A record look up, is not supported.

4.7. Codecs

Voice encoding can be G.711 A-law or G.729A. Currently the most common sample period is 20ms, although customers may opt for 10ms, which introduces less latency, but at the expense of greater bandwidth. It is important to note that Gamma can only control the sample period in the egress direction of calls made by its customers.

It is recommended that all customers offer G.711 a-law (20ms) as a common denominator when negotiating calls, although there is no requirement for this to be the first choice of codec.

We police the media-stream bandwidth based on the negotiated codec. If a customer exceeds the bandwidth for a specific codec, RTP packets will be discarded and this will result in poor voice quality.

Ptime:- We do not support the negotiation of codec Ptime.

4.8. Session Failover and Endpoint resilience

The following scenarios will result in an endpoint as being tagged as 'out of service'. In the case of resilient designs these scenarios initiate failover to alternative sites.

- Destination Unreachable (ICMP unreachable response)
- SIP Ping failure
- SIP failure response code

Destination unreachable

This happens in two ways:

- We receive an ICMP unreachable message in response to the INVITE message that it sends out to the endpoint. This could indicate that there is no network route to that destination (i.e. the access method has failed) or the destination is temporarily out of service.
- Outgoing INVITEs are retransmitted from us three times. If that limit is reached, we will stop trying that endpoint and initiate failover to another endpoint.

In the case of resilient designs, failover is initiated when we conclude that a SIP Trunking endpoint cannot be reached.

SIP Ping failure

If SIP Ping is enabled at both Gamma and the endpoint and SIP Ping fails to respond favourably. We will send a SIP Ping every 60 seconds. The customers CPE should reply with a 200 OK.

If Gamma does not receive a response within 3 pings, the endpoint is removed from service after the 3rd unsuccessful response. SIP Pings will continue to be sent out every 60 seconds and as soon as 3 responses are received the endpoint will be brought back into service.

SIP Response Codes

When we receive a SIP Final Response, code as detailed in Table 9, in reply to one of its own initial INVITE messages a failover will be initiated in the case of a resilient design. If a SIP response code is received which is not detailed in Table 9 then no failover will occur.

If the SIP response includes a Q.850 reason header then this will take precedence over the SIP response code.

Prevention of Session loss

In order to minimise the impact of failure of network components, it is recommended that within the customer's network (Proxies and CPE) session timers, as specified by RFC 4028 are implemented. The preferred method for CP to request a change of the refresh time is by means of a SIP error response 422 or a Re-INVITE.

To avoid a high volume of Invite-422-ReInvite iterations at the start of the call, where the Session-Expires value in the originating Invite is less than 1800 seconds (as per RFC 4028), it is recommended this value should not be less than 600 seconds. This will not prevent Session Interval Too Small responses entirely and it is highly recommended that the CPs that advertise support of the 'timer' feature enable their call-servers to resend the Invite request with the new Session-Expires value upon receipt of a 422 response.

The session refresh time cannot be negotiated by means of UPDATE. The session can be refreshed by means of a Re-INVITE or an UPDATE.

4.9. Customer Premises Equipment

The supply, provisioning and support of all hardware at the customer's site are the responsibility of the customer. To ensure compatibility of equipment and ease of installation, we are continually undertaking conformance testing with equipment vendors.

For the CPE devices that have been tested, we suggest customers contact their equipment vendor for assistance with the installation of this equipment.

Important Note: if connection is required for a device that has not previously been connected to Gamma, the customer can request Gamma's cooperation with conformance testing to ensure that the device is fully compatible with the Gamma network prior to live provisioning with a customer.

4.10. Network Security

Access to the Service from the customers CPE is via IP Authentication and as such, the service will only accept traffic from genuine SIP Trunking endpoints that have been registered on the service.

It is the customer's responsibility to ensure that calls emanating from their endpoint are legitimate and that all practical steps have been taken to avoid fraudulent activity. This would include secure access to their network by means of a Firewall or a Session Border Controller (SBC).

5. Customer Network Design Options

We offer three design options as standard for the Gamma SIP Trunking Service.

- Single Site – A single site working off a single Gamma SBC High Availability (HA) Cluster. This option provides a service availability of 99.95%.
- Active Standby – Dual sites in active / standby mode working off different Gamma SBC HA Clusters. This enhanced Service offers multiple Customer IP addresses and the Gamma network is Geo Resilient. This option provides a service availability of 99.99% when installed in conjunction with a private interconnect.
- Load-share – Dual sites in load share mode working off different Gamma SBC HA Clusters. This enhanced Service offers multiple Customer IP addresses and the Gamma network is Geo Resilient. This option provides a service availability of 99.99% when installed in conjunction with a private interconnect.

In the case of resilient designs (Active Standby or Load-share) one SBC pair is usually located in London and the other in Manchester to provide geographic diversity.

5.1. Single Site

This design offers a single site connected to a single Gamma SBC HA Cluster. The connection to the Gamma network may be DSL, Ethernet or a Private connection. There is no site resilience available in this set up.

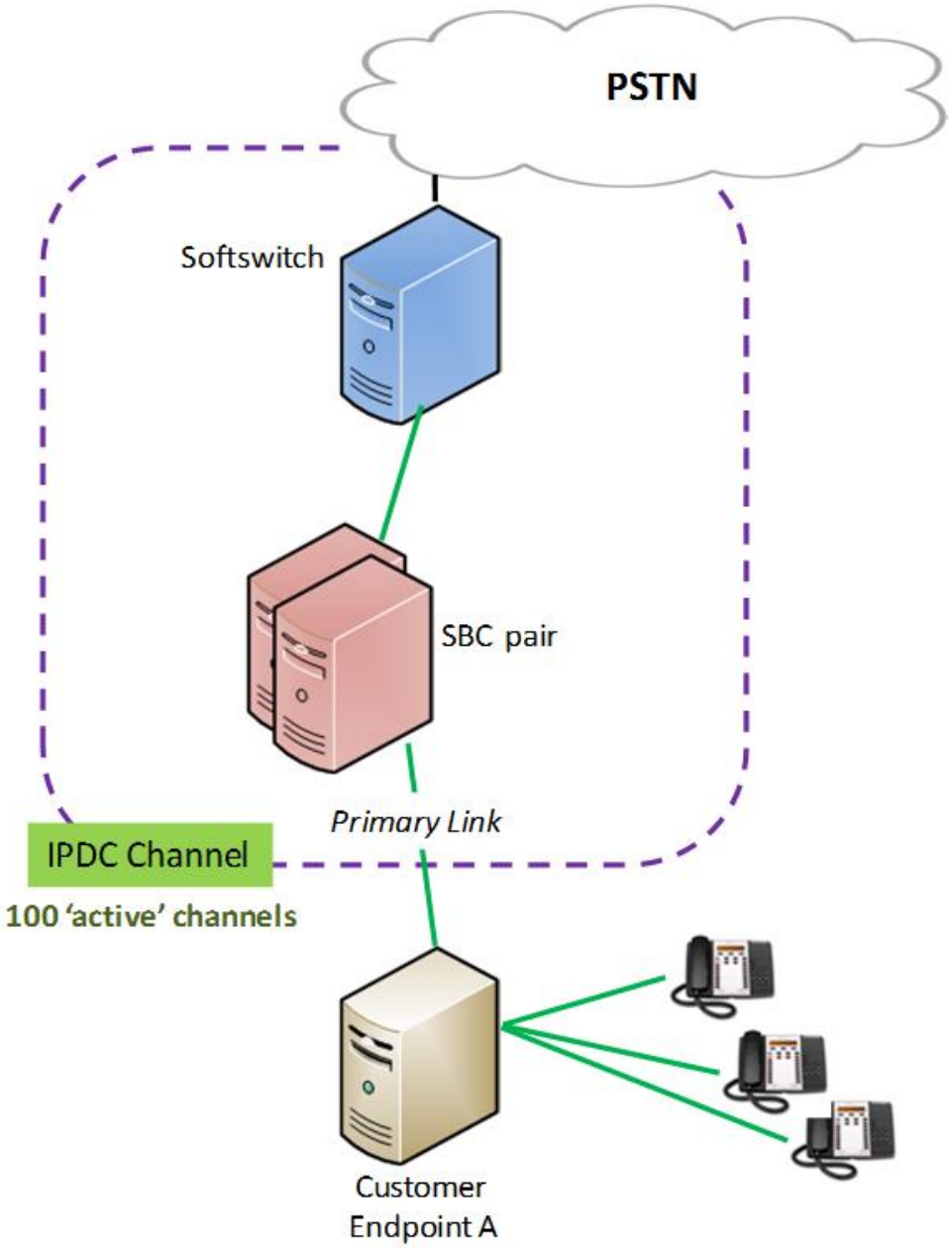


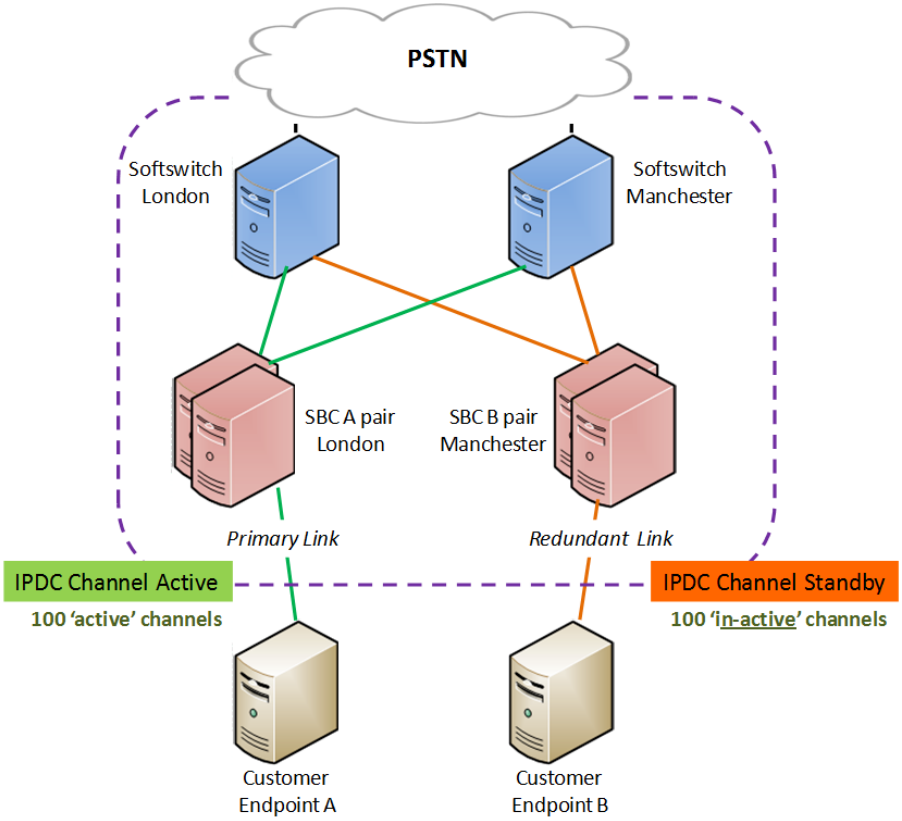
Table 3 -- Single Site Configuration Summary

Parameter	Description
Customer Endpoint	Single customer IP address
Channel Limit	Minimum 2 channels , No upper Limit
Call Admission control	Channel limit shared between incoming and outgoing calls
Access	Public or Private
CPS	Limit 2 CPS

SBC Gateway	Single Gamma SBC HA Cluster
DDI's	Multiple ranges
Codecs & Packetisation	G.711 a-law or G729 at 10 ms or 20ms
Provisioning SLA	Automatic and immediate
Availability	SLA 99.95%

5.2. Active Standby

This design offers dual endpoints in active / standby mode working off geographically diverse Gamma SBC HA Clusters i.e. SBC pairs A & B. For this configuration, all traffic will route to the primary endpoint A. In the event of failure all calls will route to the secondary endpoint.



Call Admission Control (CAC)

The Gamma soft switches are configured to route via the SBC A pair as the first choice, and via the SBC B pair as the second choice. Both SIP endpoints are configured with a CAC limit which is equivalent to the total channel allocation (e.g. 100 channels). Each channel allocation is shared between incoming and outgoing calls.

It is the customer's responsibility to keep within subscribed bandwidth and the maximum number of concurrent calls allowed. These constraints apply to all calls associated with the customer, regardless of whether they were incoming or outgoing.

In the event that Endpoint A is in service but sends back a hunt-able SIP response (e.g. 408, 503, 504) then calls will be presented to Endpoint B and those calls will not be accounted for in further CAC restriction at Endpoint A. For example; If endpoint A fails and 'x' number of calls are setup to endpoint B and then Endpoint A recovers for the duration of the 'x' calls then the total CAC possible would be 'x' + 100 calls.

For total CAC exhaustion (i.e. both across Endpoint A & B) a network failure message / announcement is returned e.g. SIP response 503.

Fail over and resiliency

Gamma network nodes are configured to route via SBC A as the first choice with second choice routing to SBC B. Failover scenarios are only invoked in the event that a recognized and supported hunt message is received at the Gamma SBC from the end user voice platform.

The following scenarios will invoke failover to the secondary endpoint:

- CAC exhaustion at the Active Endpoint
- Destination Unreachable (ICMP unreachable response)
- SIP failure response code which invokes the hunt procedure (Please refer to Table 9)
- SIP Options Ping failure (if configured)

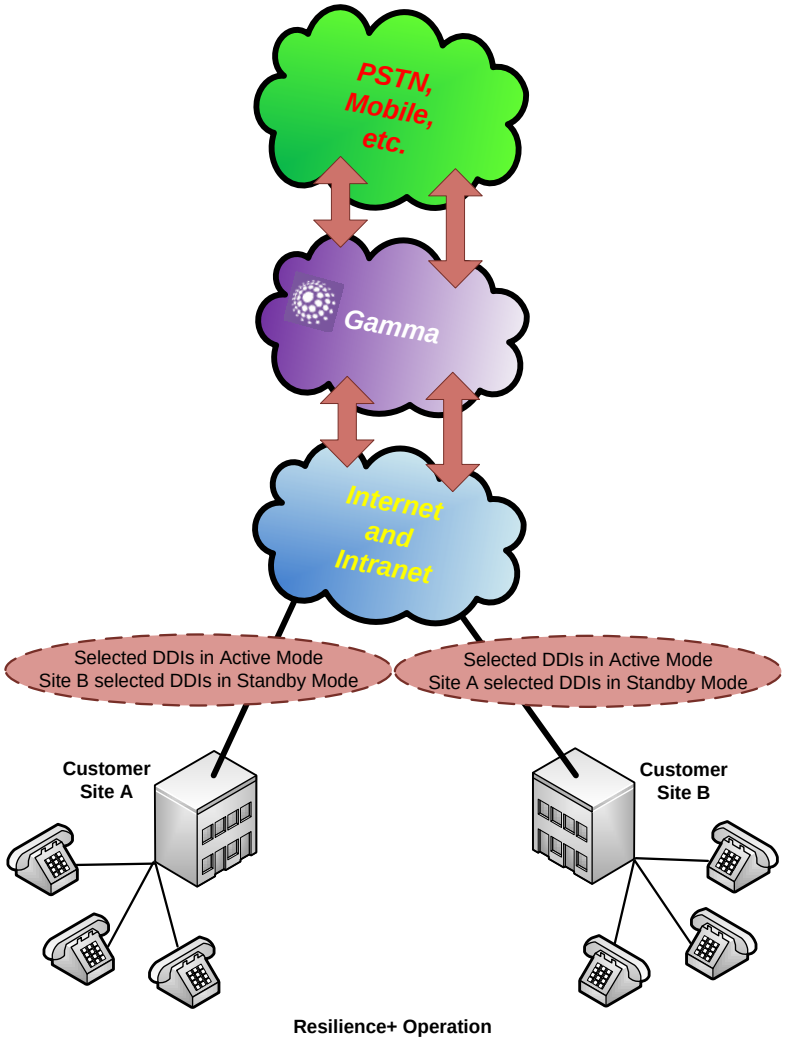
Please note that a failure condition at endpoint A can increase Post Dial Delay (PDD) by up to 1.5 seconds.

Table 4 -- Active Standby Configuration Summary

Parameter	Description
Customer Endpoint	2x customer IP addresses on same site or different sites
Channel Limit	Minimum 2 channels , No upper Limit
Call Admission control	Channel limit shared between incoming and outgoing calls Theoretical channel maximum = 200% of channel allocation
Fail over	100% of channel allocation in fail over scenario
Access	Public or Private
CPS	Limit 5 CPS
SBC Gateway	2 Geographically diverse HA Clusters
DDI's	Same DDI ranges shared across both endpoints
Codecs & Packetisation	G.711 a-law or G729 at 10 ms or 20ms
Provisioning SLA	10 day lead time
Availability	SLA 99.99%

5.3 Active Standby Resilience+

The Resilience+ option is designed to offer two SIP endpoint connections where each endpoint is active to selected DDIs whilst standby resilience is provided by the other endpoint. The Resilience+ option offers dual live sites with dual failover options.



Resilience+ Operation

The Resilience+ design offers dual endpoints both in active-standby mode working off geographically diverse Gamma SBC HA Clusters. For this configuration, individual DDIs or DDI ranges can be allocated to the desired endpoint and traffic route accordingly. In the event of connection or site failure all calls will route to the alternate endpoint.

Benefits of the Resilience+ option include the ability to define both the DDI ranges and channel allocations at each site. In the event that communication to either site is unavailable, then the remaining site will receive all related traffic. Resilience+ services do not have to be symmetric e.g. in a 100 channel deployment, channels can be allocated in a 60/40, 70/30, etc. configuration if desired.

Call Admission Control (CAC)

The Gamma soft switches are configured to route via the Session Border Controller (SBC) A pair as the first choice, and via the SBC B pair as the second choice.

Both SIP endpoints are configured with a CAC limit which is equivalent to the total channel allocation (e.g. 100 channels). Each channel allocation is shared between incoming and outgoing calls.

In the event that Endpoint A is in service but sends back a hunt-able SIP response (e.g. 408, 503, 504) then calls will be presented to Endpoint B and those calls will not be accounted for in further CAC restriction at Endpoint A.

For example; If endpoint A fails and 'x' number of calls are setup to endpoint B and then Endpoint A recovers for the duration of the 'x' calls then the total CAC possible would be 'x' + 100 calls.

For total CAC exhaustion (i.e. both across Endpoint A & B) a network failure message / announcement is returned e.g. SIP response 503.

Fail over and resiliency

Gamma network nodes are configured to route via SBC A as the first choice with second choice routing to SBC B. Failover scenarios are only invoked in the event that a recognised and supported hunt message is received at the Gamma node from the customer voice platform. The following scenarios will invoke failover and force traffic to the alternative endpoint:

- CAC exhaustion
- Destination Unreachable (ICMP unreachable response)
- SIP failure response code which invokes the hunt procedure (Please refer to **Table 9**)
- SIP Options Ping failure (if configured)

In the event of a Gamma SBC, connectivity or customer site failure, traffic will route to the alternative site and channel allocation will revert to the total call allowance.

Parameter	Description
Customer Endpoint	2x customer IP addresses on same site or different sites
Channel Limit	Minimum 2 channels , No upper Limit
Call Admission control	Channel limit shared between incoming and outgoing calls Theoretical channel maximum = 200% of channel allocation
Fail over	100% of channel allocation in fail over scenario
Access	Public or Private
CPS	Limit 5 CPS
SBC Gateway	2 Geographically diverse HA Clusters
DDI's	Same DDI ranges shared across both endpoints
Codecs & Packetisation	G.711 a-law or G729 at 10 ms or 20ms
Provisioning SLA	10 day lead time
Availability	SLA 99.99%

Resilience+ Restrictions

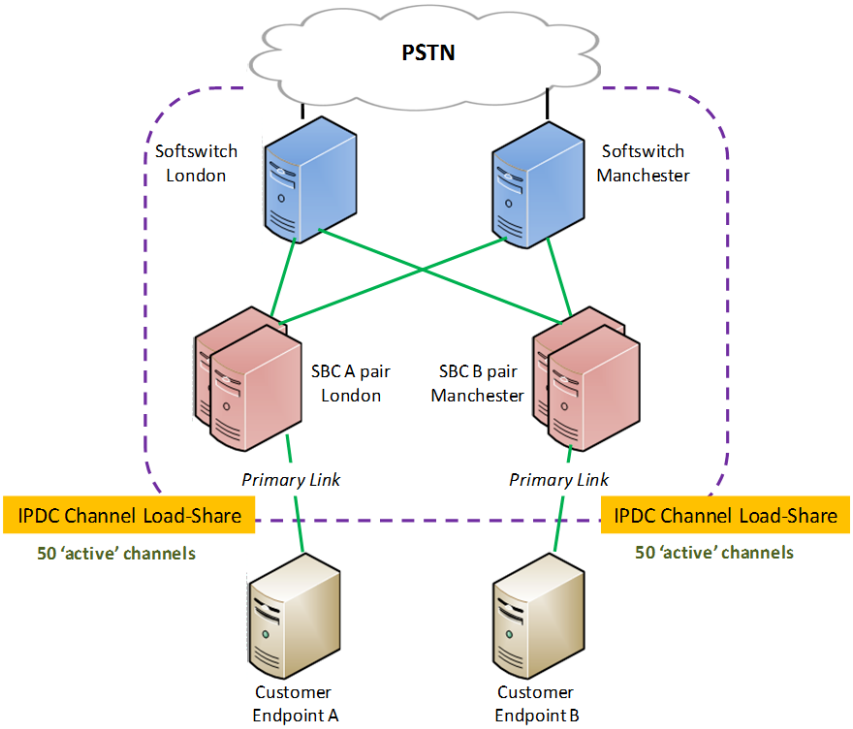
Resilience+ is limited to dual endpoint implementations and if there are more than two sites, please involve the IPT Pre-sales team.

Each implementation will need to have the correct number of channels to handle automatic failover, for example, in a 100 channel deployment (say 70/30) you would need to actually have 200 channels (split 100/100) to handle

the full 100 channel capacity requirements in the event of an emergency. Otherwise the customer might see some impact on voice quality when the Call Admission Control (CAC) limit is reached.

5.4. Load-Share

This design offers dual endpoints in load-share mode working off geographically diverse Gamma SBC HA Clusters i.e. SBC pairs A & B. For this configuration, traffic will be delivered in a round robin fashion to ensure equal distribution between endpoints.



Call Admission Control (CAC)

Each SIP endpoints is configured with half the total channel allocation (e.g. 50 out of 100 channels). Each channel allocation is shared between incoming and outgoing calls.

In cases where the call control constraint (CAC limit) is exceeded at an SBC, excess traffic will overflow/re-route to the alternative SBC if additional capacity is available. To ensure this operation, CAC exhaustion on both SBC A and SBC B will send a 503 SIP response back to the Gamma network to ensure it hunts between the two SBC clusters. This configuration ensures 100% of the channel allocation is available at any time, except in outage cases when only 50% of channel allocation would be available.

Fail over and resiliency

Gamma network nodes are configured to load share traffic across both SBC nodes. Failover scenarios are only invoked in the event that a recognized and supported hunt message is received at the Gamma SBC from the end user voice platform. The following scenarios will invoke failover and force traffic to the alternative endpoint:

- CAC exhaustion
- Destination Unreachable (ICMP unreachable response)

- SIP failure response code which invokes the hunt procedure (Please refer to Table 9)
- SIP Options Ping failure (if configured)

In the event of SBC or customer connectivity failure, traffic will route to the alternative site. Channel allocation will remain at ½ the total call allowance.

Table 5 - Load Share Configuration Summary

Parameter	Description
Customer Endpoint	2x customer IP addresses on same site or different sites
Channel Limit	Minimum 2 channels , No upper Limit
Call Admission control	Channel limit shared between incoming and outgoing calls Theoretical channel maximum = 100% of channel allocation
Fail over	50% of channel allocation in fail over scenario
Access	Public or Private
CPS	Limit 5 CPS
SBC Gateway	2 Geographically diverse HA Clusters
DDI's	Same DDI ranges shared across both endpoints
Codecs & Packetisation	G.711 a-law or G729 at 10 ms or 20ms
Provisioning SLA	10 day lead time
Availability	SLA 99.99%

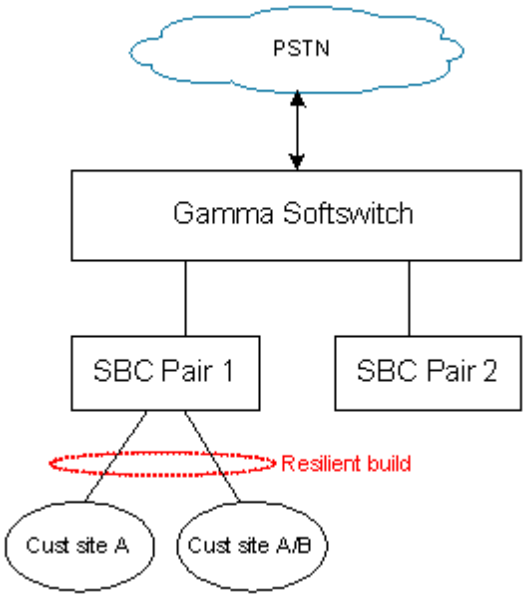
5.5. Failover examples

Gamma resilient SIP trunk solutions rely on customer CPE response codes in order to trigger a hunt action i.e. an attempt to deliver an inbound call to the customer's secondary endpoint in a failure scenario. Gamma will also trigger a hunt action if no response is received from the customer CPE due to circumstances such as a total loss of IP connectivity.

In order that the customer is able to configure their CPE to interoperate correctly with Gamma, the following response codes are required by Gamma in order to trigger an inbound hunt action. This also outlines what Gamma suggests the customer CPE reacts to in the event that Gamma has reason to deliver a SIP failure response code to the customer platform.

Scenario 1

The end user has a resilient SIP trunk build, Active/Standby or Load-balanced over 2+ SIP trunk end points. Gamma's policy for building and deploying resilient designs is that each endpoint is built back to a geographically diverse SBC HA pair, situated in Manchester and London. It can be the case though that in order to support end user requirements Gamma builds more than one endpoint back to the same SBC HA pair.



If resiliency is setup between 2+ endpoints built back to the same Gamma SBC pair, we will force a hunt response (inbound calls – Gamma to end user) if it receives one of the following SIP response codes from the CPE:

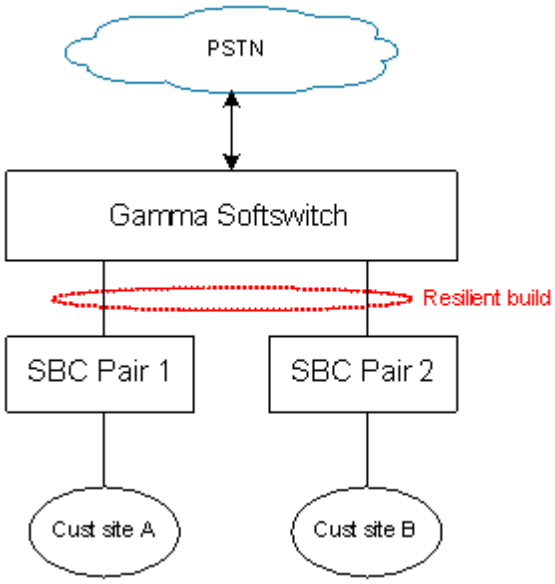
SBC Hunt response codes (Grid 1):

400	402	405	406	408	409	411	413
414	415	420	480	482	483	485	487
488	500	502	503	504	505	580	606

Example MSG flow and response:

Scenario 2

The customer has a resilient SIP trunk build, Active/Standby or Load-balanced over 2+ SIP trunk end points. The solution uses the standard Gamma implementation method whereby each endpoint is configured on a separate Gamma SBC HA pair.

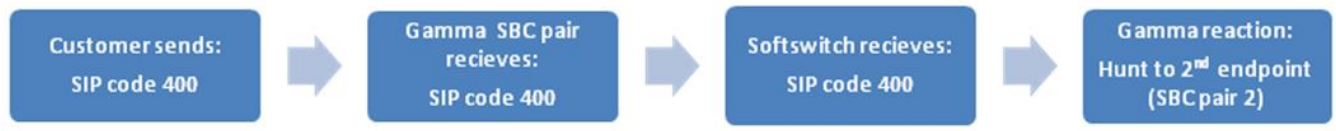


In this instance the Gamma SBC HA pair will pass back the SIP error response it receives from the end user CPE. The response is then handled by the top layer of the Gamma SIP trunk resilient mechanism. The Gamma Soft switch layer will force a hunt response if it receives one of the following SIP response codes:

Soft switch Hunt response codes (Grid 2):

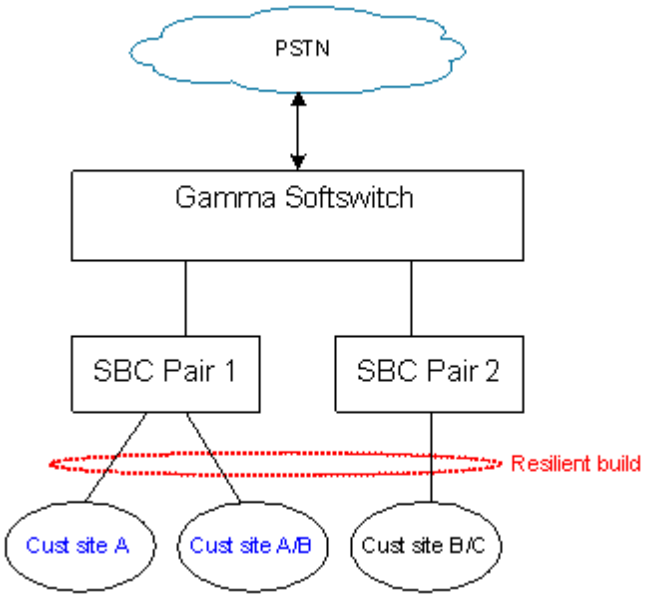
400	408	480	481	500	502	503	504

Example SBC flow and response:



Scenario 3

The End user has a resilient SIP trunk build, Active/Standby or Load-balanced over 3+ SIP trunk end points which form a mixture of scenario 1 and 2 above. As an example the end user has 2 SIP trunk end points built back to Gamma SBC HA pair 1 and a 3rd end point built back to Gamma SBC HA pair 2.



In this instance customer site A and A/B in the diagram above (Blue) will have CPE DR message requirements as per Scenario A. Customer site B/C will have Inbound DR message requirements as per Scenario B

Example SBC flow and response:

Customer site A is the primary inbound delivery trunk for a particular call. Customer site A fails and sends a 408 SIP response code.

Customer site A is the primary inbound delivery trunk for a particular call. Customer site A fails and send a 408 SIP response code. Customer site A/B also fails returning a 503 SIP response code.

6. Network Access and Connectivity Options

SIP trunk endpoints can be configured as both public and private IP addresses allowing access to Gamma SIP Trunking services via public internet or private interconnect. This access can be provided by Gamma or Third Parties with the following options:

6.1. Public Internet

The customer's CPE (typically an IPBX supporting SIP) is defined as an 'endpoint' within the Gamma SBC, with each endpoint capable of having a number of devices connected to it.

A static public IP address assigned by the customer's ISP will be configured and used to authenticate the endpoint, providing duplex interconnection to the PSTN.

6.2. Private Interconnect

In order to assuage perceived security and quality concerns, Gamma offers improved access options:

- Private interconnection via the Gamma IP Assured service
- Private interconnection via Ethernet
- Private interconnection to Gamma into POP (Layer 2 VLAN)

Access via Private interconnection is possible at the following Gamma peering points:

- Telecity 2, 8/9 Harbour Exchange Square, E14 9GE - Rack 3V20
- Telehouse East, E14 2AA - TFM51 Rack E18
- Redbus, 6/7 Harbour Exchange Square, E14 9HE - Rack 1624 Floor 8
- Telehouse North, E14 2AA - TFM15 Cab C13
- Eplison Global Hubs, Paul St, 2nd Floor, 69-77 Paul St, London, EC2A 4NW - Meet Me Room (MMR
- City Lifeline, 80 Clifton St, London, EC2A 4HB - Citrus Suite, 2nd Floor, Rack B4
- Telecity Powergate, Unit 1, Powergate Business Park, Volt Avenue, London, NW10 6PW - Meet Me Room (MMR)
- Kilburn House at Telecity, Manchester, M15 6SE - Rack AH4

Network Demarcation

For Private interconnection the Gamma Telecom demarcation point resides at the internal fibre cross connect presentation at the customer rack location with the Data centre. It is the customers responsibility to identify (localise) and resolve problems affecting IPT services caused by the customer premises equipment (CPE) and local infrastructure beyond this demarcation.

Quality of service

It is not necessary for the customer to mark traffic on the egress to their network before it enters the Gamma device terminating the internal cross connect and Gamma will not deliver marked voice traffic (Signalling or Media) to the customer.

Resilient Connectivity

For maximum resilience, it is required that customers interconnect at two diverse peering points. All peering point combinations are diverse with the exception of the following combinations:

- Telecity 8/9 and Telecity Powergate

Connection Types

Connection types include copper, single or multi-mode fibre and bandwidths ranging from 10Mbps to 1Gbps. Interconnect port types include Layer 3 BGP, Layer 2 VLAN or Layer2 801q VLAN. For improved connectivity resilience at each peering point, CP's should consider diverse connections as opposed to single connections.

IP Addressing and Gamma Ethernet connectivity

For SIP trunk customers connecting via Gamma Ethernet, Gamma allocated a private /29 subnet for use on the customer side of the Gamma router. This /29 subnet includes:

- 1 IP out of the range for the customer to configure their CPE
- 1 IP out of the range as the Customer Default Gateway

Please note: The Gamma SIP trunk Signalling and Media Gateway address is in a different range. Customer will therefore need to configure their CPE to use the Customer Default Gateway as the route to the Gamma signalling address.

7. Protocol and Signalling support

Gamma can offer SIP signalling transport over UDP. The standard is UDP. In cases where PBXs use TCP signalling, SIP Proxy servers/IP gateways are required to convert to UDP on the customer's premises.

7.1. RFC Support

The Gamma SIP Trunking service supports the following RFC's. Full compliance is subject to differences in interpretation, interoperability constraints and the exceptions noted below.

Table 2 -- Gamma SIP Trunking reference RFCs and other Standards

RFC	Supported
RFC 2327 Session Description Protocol	Yes
RFC2543 SIP: Session Initiation Protocol	Yes, Putting Media streams on Hold, Indicate the IP in SDP message when "call-hold" mechanism is used according RFC 2543: Gamma will support receiving either the actual IP or 0.0.0.0 if interworking to TDM. If the incoming/outgoing route is via a SIP interconnect partner this may not be the case.
RFC 2833 - RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals	Yes
SIP RFC 3261- SIP Messages, Headers & Protocol	Yes
RFC 3262 - Reliability of Provisional Responses in SIP:	Yes
RFC 3264 - An offer/answer model with SDP:	Yes
SIP RFC 3311 - SIP Update Method	Yes (only during unconfirmed dialogue). Re-INVITE should be used when dialogue is in confirmed state.

SIP RFC 3323 - Privacy Mechanism for SIP	Yes
SIP RFC 3325 - Privacy extensions to SIP for Asserted Identity within trusted networks	Yes
SIP RFC 3326 - Reason-Header Field for SIP	Yes
RFC 3398 - ISDN to SIP Mapping:	Yes
RFC 3551 - RTP Profile for audio:	Partial, Gamma will only support G711, G729 and G729A codecs
RFC 4028 Session Timers in the Session Initiation Protocol	Yes
NICC ND1017:2006/07. TSG/SPEC/017. Interworking between Session Initiation Protocol (SIP) and UK ISDN User Part (UK ISUP)	Yes

7.2. Signalling and Encoding

Gamma SIP Trunking provides SIP signalling as a method for Communication Providers to inter-connect with Gamma's VoIP network, supporting VoIP to VoIP calling as well as calls to/from the PSTN.

Gamma SIP Trunking supports the transport of SIP signalling messages using UDP. SIP messages sent using TCP(except for MS Lync), TLS, SCTP and IPSEC are not supported at present.

SIP V2 is supported between the SBC and the customer CPE. The SIP standard is documented in the Internet Engineering Task Force (IETF) RFC 3261.

Please note that this service does not support H.323, SIP-I, SIP-D and SIP-T.

Format of the SIP INVITE Field

The SIP header requirements in the INVITE packets originated from the CPE should be set as follows:

- Request URI must contain the B-number followed by the assigned Gamma SIP gateway IP address:
- INVITE sip:01618700000@"IP Address";user=phone SIP/2.0
- The FROM header must contain your public facing IP address and originating CLI:
- FROM: <sip:+441618777148@"IP Address">; tag=3528194925-554920
- The TO header must contain the assigned Gamma SIP gateway IP address and the B-number*:*
- To: <sip:01618700000@"IP Address";user=phone>
- SDP payload must be present, and must contain your public IP address. See section 4.7 for supported codecs.

Traffic on the following ports must be forwarded through relevant routers and firewalls on the customer premises to allow access to the Gamma SIP Trunking Network:

- UDP Port 5060 egress/ingress
- UDP all ports between 6000 - 40000 egress/ingress

For ingress calls the INVITE Request Line must contain a SIP URI.

For egress calls from Gamma to the customer the INVITE Request Line will contain a SIP URI.

Example of the initial SIP INVITE

The SIP gateway here is 88.215.61.195 – this will be stated in the SIP trunk order confirmation.

The CPE IP address is 88.215.25.5 – the public IP address with which Gamma's SBC communicates. This address is defined in the SIP trunk order, and can be updated via the Gamma Portal. The fields highlighted below must contain the CPE IP address. If the PBX is operating behind a NAT these addresses will need to be NAT'ed by a SIP aware device e.g. an SBC, a router with an ALG, the PBX itself via STUN.

SIP Message

INVITE sip:01412485779@88.215.61.195 SIP/2.0

Via: SIP/2.0/UDP 88.215.25.5:5080;branch=z9hG4bK-a8b33135

From: "+441414040025" <sip:+441414040025@88.215.61.195>;tag=9fa8f5c74acc1965o0

To: <sip:01412485779@88.215.61.195>

Call-ID: 9899ceef-2d38d25d@192.168.1.8

CSeq: 101 INVITE

Max-Forwards: 70

Contact: "+441414040025" <sip:+441414040025@88.215.25.5:5080>

Expires: 240

User-Agent: Linksys/SPA942-6.1.5(a)

Content-Length: 250

Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, PRACK, REFER

Supported: 100rel, replaces

Content-Type: application/sdp

SDP

v=0

o=- 14849 14849 IN IP4 192.168.1.8

s=-

c=IN IP4 88.215.25.5

t=0 0

m=audio 7776 RTP/AVP 8 18 101

a=rtpmap:8 PCMA/8000

a=rtpmap:18 G729a/8000

a=fmtp:18 annexb=yes

a=rtpmap:101 telephone-event/8000

a=fmtp:101 0-15

a=ptime:20

a=sendrecv

Explanation:

The Via header (the topmost via if there are multiple) is used in conjunction with the layer 3 IP address for authentication. If the address is unknown to our SBC (e.g. LAN address) it will respond 403: Forbidden.

The Contact header advises our SBC where to respond to. If this is a LAN address, or some other address which you're not expecting traffic on, the 2-way dialog will be disrupted and calls will not setup correctly.

The c= parameter in the SDP (connection address) is the address to which your user agent is requesting media (RTP) is sent. Again, this needs to be reachable by Gamma's SBC. If this is not NAT'ed, and you send a LAN IP address, the call may setup OK but you will get one way speech (with the remote party not heard by the SIP trunk user)

7.3. Supported SIP methods and responses

The list of supported SIP methods is detailed below.

Supported SIP methods

Table 6 -- Supported SIP methods

Method	Extent of Support	Notes
ACK	Full, receive and transmit	
BYE	Full, receive and transmit	The "Reason-Header" field in BYE or CANCEL message is preferred but not essential
CANCEL	Full, receive and transmit	The "Reason-Header" field in BYE or CANCEL message is preferred but not essential
INVITE	Full, receive and transmit	
OPTIONS	Full, receive and transmit	
PRACK	Full, receive and transmit	
UPDATE	Full, receive and transmit	UPDATE supported only during an unconfirmed dialogue

Supported SIP Responses

Table 7 -- Supported Responses

Response	Extent of Support	Notes
100 TRYING	Full, receive and transmit	

180 RINGING	Full, receive and transmit	
181 Forwarded	Minimal receive only	
183 Session Progress	Full, receive and transmit	In cases of TDM interworking then a 183 session progress will be sent when the outgoing MGW is seized regardless of the subscriber state. In cases where the outgoing route is towards a SIP interconnect partner this may not be the case.
200 OK	Full, receive and transmit	Gamma will include SDP in 200-Ok answer message which will be the same as any SDP previously sent in a 18x message
400 Bad Request	Full, receive and transmit	
403 Forbidden	Full, receive and transmit	
404 Not found	Full, receive and transmit	
405 Method Not Allowed	Minimal, receive only	
406 Not Acceptable	Minimal, receive only	
408 Request Timeout	Minimal, receive only	
415 Unsupported Media Type	Full, receive and transmit	
422 Session Timer Interval Too Small	Full	
480 Temporarily Unavailable	Full, receive and transmit	
481 Call Leg/Transaction Does Not Exist	Full, receive and transmit	
482 Loop Detected	Full, receive and transmit	
483 Too Many Hops	Full, receive and transmit	
484 Address Incomplete	Full, receive and transmit	
486 Busy Here	Full, receive and transmit	
487 Request Terminated	Full, receive and transmit	
488 Not Acceptable Here	Full, receive and transmit	
491 Request Pending	Full, receive and transmit	
500 Internal Error	Full, receive and transmit	
501 Not Implemented	Full, receive and transmit	
502 Bad Gateway	Minimal, receive only	
503 Service Unavailable	Full, receive and transmit	
504 Server Time-out	Full, receive and transmit	
600 Busy Everywhere	Minimal, receive only	

603 Decline	Minimal, receive only	
604 Does Not Exist	Minimal, receive only	
606 Not Acceptable	Minimal, receive only	

7.4. Hunt-able SIP Responses

The following SIP responses when sent back from SITE A (Active/Standby) or either SITE (Load Balanced), will cause the network to hunt to the next available customer endpoint.

Table 9 -- Hunt-able SIP responses

SIP Status Code received	Cause/CAN/Q850	Hunt-able SIP response
400 (Bad Request)	NONE	Yes
401 (Unauthorised)	NONE	
402 (Payment Required)	NONE	
403 (Forbidden)	NONE	
404 (Not found)	NONE	
404 (Not found)	1 (Unallocated Number)	
405 (Method Not Allowed)	NONE	
406 (Not Accepted)	NONE	
407 (Proxy Auth. Required)	NONE	
408 (Request Timeout)	NONE	Yes
410 (Gone)	NONE	
413 (Req.Entity Too Long)	NONE	
414 (Req. URI Too Long)	NONE	
415 (Unsupported Media Type)	NONE	
416 (Unsupported URI Scheme)	NONE	
420 (Bad Extension)	NONE	
421 (Extension required)	NONE	
423 (Interval Too Brief)	NONE	
480 (Temporarily Unavailable)	NONE	
480 (Temporarily Unavailable)	34 (No Channel Available)	
480 (Temporarily Unavailable)	41 (Temporary Failure)	Yes (with q.850 Reason Header containing reason 41)
480 (Temporarily Unavailable)	42 (Switching Equip. Cong)	
481 (Call / Transaction Not Exist)	NONE	Yes
482 (Loop Detected)	NONE	
483 (Too many Hops)	NONE	

484 (Address Incomplete)	NONE	
484 (Address Incomplete)	28 (Address Incomplete)	
485 (Ambiguous)	NONE	
486 (User Busy)	17 (User busy)	
486 (User Busy)	NONE	
487 (Request Terminated)	NONE	
488 (Not acceptable Here)	NONE	
491 (Request Pending)	NONE	
493 (Undecipherable)	NONE	
500 (Server Int. Error)	NONE	Yes (with q.850 Reason Header containing reason 41)
500 (Server Int. Error)	34 (No Channel Available)	
500 (Server Int. Error)	41 (Temporary Failure)	Yes (with q.850 Reason Header containing reason 41)
500 (Server Int. Error)	42 (Switching Equip. Cong)	
502 (Bad Gateway)	NONE	Yes
503 (Service Unavailable)	NONE	Yes (with q.850 Reason Header containing reason 41)
503 (Service Unavailable)	41 (Temp fail)	Yes (with q.850 Reason Header containing reason 41)
504 (Server Timeout)	NONE	Yes
600 (Busy Everywhere)	NONE	
603 (Decline)	NONE	
604 (Does Not exist Anywhere)	NONE	
606 (Not Acceptable)	NONE	

GLOSSARY

This appendix provides a basic glossary for some of the terms, acronyms, and abbreviations used in this document.

Term Definition	Description
ADSL	Asymmetric Digital Subscriber Line
ANI	Automatic Number Identification
ASR	Answer Seizure Ratio
ATM	Asynchronous Transfer Mode
CAC	Call Admission Control
CLI	Calling Line Identity
CLIP	CLI Presentation
CLIR	CLI Restriction
CP	Communications Provider
CPE	Customer Premise Equipment
CPS	Calls per Second. The maximum number of new call attempts per second.
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DTMF	Dual Tone Multi-Frequency
EDD	Ethernet Demarcation Device
G.711	ITU Recommendation for companding digital audio
G.729	Audio data compression algorithm
GSP	Global Services Platform – Nortel TDM switch
GUI	Graphical User Interface
H.323 ITU-T	VoIP Protocol
HA	High Availability
ISP	Internet Service Provider
IP	Internet Protocol (shorthand for TCP/IP)
IP DC	IP Direct Connect – Product name of the SIP Trunking service
IP PBX	IP Private Branch Exchange
IPT	Internet Telephony
L2TP	Layer 2 Tunnelling Protocol
LAN	Local Area Network
LLU	Local Loop Unbundling
MOS	Mean Opinion Score
MSX	NexTone Multi Protocol Session Exchange

NSN	National Significant Number
OSS	Operational Support Systems
PABX	Private Automatic Branch Exchange
PDD	Post-Dial Delay
POP	Point of Presence
PSTN	Public Switched Telephone Network
Q931	PABX signalling protocol (ITU definition)
RFC	Request For Comments
RTP	Real-Time Transport Protocol
SBC	Session Border Controller
SDH	Synchronous Digital Hierarchy
SIP	Session Initiation Protocol. A signalling protocol for Internet conferencing, telephony, presence, events notification and instant messaging.
SLA	Service Level Agreement
SME	Small/Medium Enterprise
SoHo	Small Office/Home Office
SQL	Structured Query Language
TSC	Gamma Technical Service Centre
TDM	Time Division Multiplexing (traditional digital telephony)
UDP	User Datagram Protocol
VoIP	Voice over IP
VPN	Virtual Private Network