DRAFT

SCHEDULE 1

ANNEXURES

Disclaimer: The technical specification and security requirements presented in the following sections are supplementary to the IMDA Technical Specification and Security Requirements. In the event of any inconsistency or discrepancy, the original IMDA Technical Specification and Security Requirements (**Annex C** and **Annex D**) shall prevail.

ANNEX A

SECTION 1

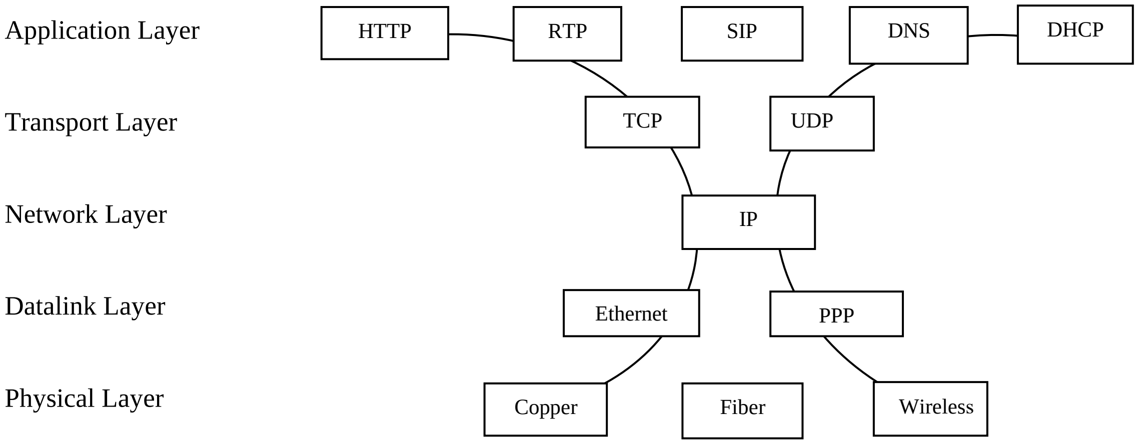
SECTION 1 – SESSION INITIATION PROTOCOL SPECIFICATION

1.1 OVERVIEW

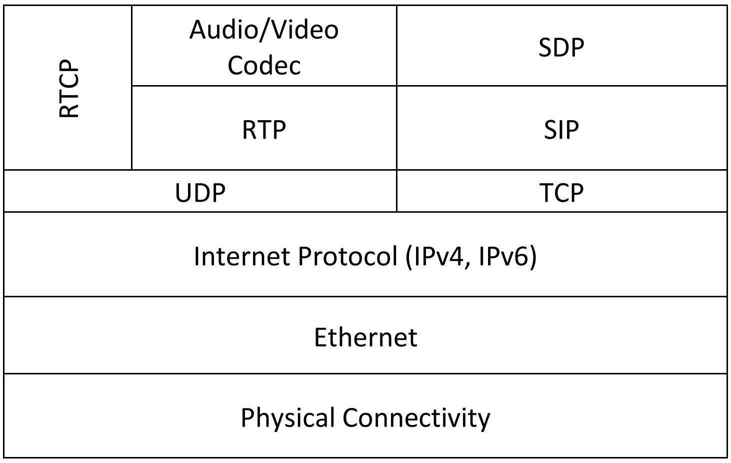
Session Initiation Protocol specification for Singtel is based on standard IETF RFCs from IMDA technical specification in **Annex C**.

1.2 STRUCTURE

Session Initiation Protocol works in application layer. Thus, network layer (IP)connectivity must be established before bringing up the SIP Interconnection link. SIP can work on either UDP or TCP. Interconnecting between telecom operators, UDP shall be adopted as it is best suited for Realtime communication (Voice).



SIP in the Application Layer



SIP Protocol Stack in Layer View

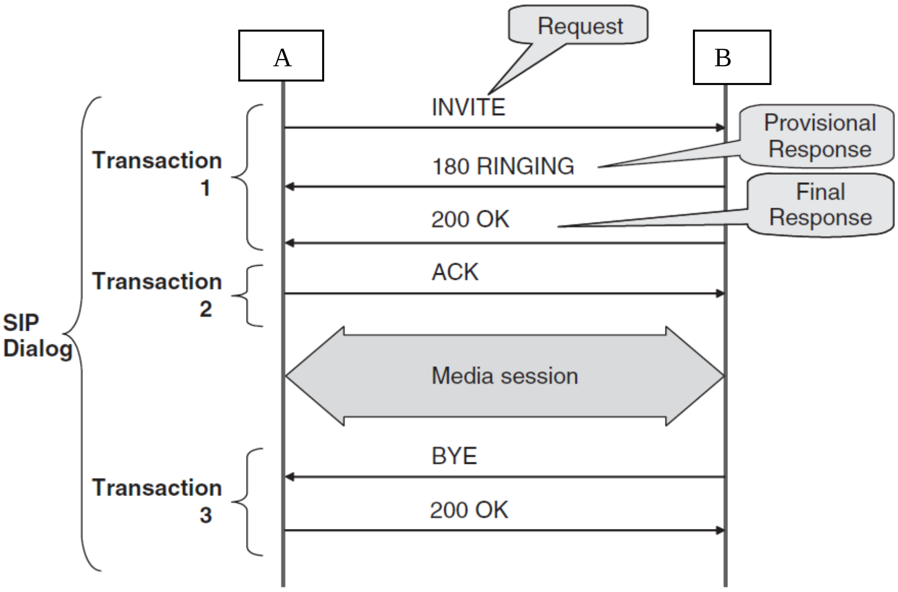
UDP is ideal for real-time services like voice over IP. Because TCP’s “reliable” nature can trigger the bad end user experience when packet loss occurs. The delays, which are caused by retransmitting broken packets and any following packets that may have already been sent, translate into an unacceptable level of jitter for the end user.

1.3 SESSION DEFINITION

1.3.1 Dialog and Transaction

Within a SIP session there contains transaction and dialogue. A dialog is a peer-to-peer SIP relationship between two UAs that persist for some time. A dialog is established by SIP messages, such as a 2xx response to an INVITE request. A dialog is identified by a call identifier, local tag, and a remote tag. A dialog was formerly known as a call leg in RFC 2543.

A transaction consists of a Request, any non-final (1xx) Responses received, and a final Response (2xx, 3xx, 4xx, 5xx, or 6xx), as well as the acknowledgements of the Responses (ACK or PRACK), except for ACKs to 2xx Responses.



2. SIP REQUEST MESSAGES

2.1 METHODS

The INVITE, REGISTER, BYE, ACK, CANCEL, and OPTIONS methods are the original six methods in SIP protocol. REGISTER method is not relevant for interconnection.

No.	SIP Messages	Inter-network interworking interface	
		send	receiving
1	ACK	Mandatory	Mandatory
2	BYE	Mandatory	Mandatory
3	CANCEL	Mandatory	Mandatory
4	INVITE	Mandatory	Mandatory
5	PRACK	Mandatory	Mandatory
6	UPDATE	Mandatory	Mandatory
7	OPTIONS	Mandatory	Mandatory

The following explains the methods that are required to establish SIP session between telecom providers.

2.1.1 INVITE

The INVITE method is used to establish media sessions between user agents. In telephony, it is equivalent of an initial address message (IAM) in ISUP.

2.1.2 BYE

The BYE method is used to terminate an established media session. In telephony, it is like a release (REL) message in ISUP. A session is considered established if an INVITE has received a success class response (2xx) (ANM) or an ACK has been sent.

A BYE cannot be used to cancel pending INVITEs because it will not be forked like an INVITE and may not reach the same set of UAs as the INVITE.

2.1.3 ACK

The ACK method is used to acknowledge final responses to INVITE requests. Final responses to all other requests are never acknowledged. Final responses are defined as 2xx, 3xx, 4xx, 5xx, or 6xx class responses.

2.1.4 CANCEL

The CANCEL method is used to terminate pending INVITEs or call attempts. It can be generated by either user agents or proxy servers provided that a 1xx response containing a tag has been received, but no final response has been received.

2.1.5 OPTIONS

The OPTIONS method is used to query a user agent or server about its capabilities and discover its current availability. The response to the request lists the capabilities of the user agent or server. In the case of SIP interconnection, OPTIONS message will be sent to detect the peer end availability. If no response from the peer end within a set of timers, the server will determine that the trunk is faulty and call traffic will not be sent to faulty link.

2.1.6 PRACK

The PRACK method is used to acknowledge receipt of reliably transported provisional responses (1xx). The reliability of 2xx, 3xx, 4xx, 5xx, and 6xx responses to INVITEs is achieved using the ACK method. However, in cases where a provisional response, such as 180 Ringing, is critical in determining the call state, it may be necessary for the receipt of a provisional response to be confirmed. The PRACK method applies to all provisional responses except the 100 Trying response, which is never reliably transported.

2.1.7 UPDATE

The UPDATE method is used to modify the state of a session without changing the state of the dialog. In an established session, a re-INVITE is used to update session parameters. In the case of codec re-negotiation during the call, update shall be sent.

2.2 URI

2.2.1 SIP URI

SIP URIs are used in several places including the To, From, and Contact headers, as well as in the Request-URI, which indicates the destination telephone number. The information in a SIP URI indicates the way in which the resource should be contacted.

2.2.2 TEL URI

The TEL URI can be used to represent a resource identified by a telephone number. Telephone numbers can be of two general forms, local or global. A local number is only valid in a particular geographic area or within an operator. A global telephone number, E.164 number, is one that is, in principle, valid anywhere and will represent in TEL URI e.g. tel:+6580XXXXXX.

2.3 SIP RESPONSE MESSAGE

2.3.1 INFORMATIONAL

2.3.2 100 Trying

This special case response is only a hop-by-hop request. It is never forwarded and may not contain a message body.

2.3.3 180 Ringing

This response is used to indicate that the INVITE has been received by the user agent and alerting is taking place. It's normally mapped to ACM in ISUP.

2.3.4 The 183 Session Progress

The 183 Session Progress response indicates that information about the progress of the session (call state) may be present in a message body or media stream. Unlike a 100 Trying response, a 183 is an end-to-end response and establishes a dialog (must contain a To tag and Contact).

2.4 SUCCESS

2.4.1 200 OK

The 200 OK response has two uses in SIP. When used to accept a session invitation, it will contain a message body containing the media properties of the UAS (called party). When used in response to other requests, it indicates a successful completion or receipt of the request.

2.5 CLIENT ERROR

2.5.1 403 Forbidden

This response is used to deny a request without giving the caller any recourse. It is sent when the server has understood the request, found the request to be correctly formulated, but will not service the request. This response is not used when authorization is required.

2.5.2 **404 Not Found**

This response indicates that the user identified by the sip or sips URI in the Request-URI cannot be located by the server, or that the user is a allocated number in the system.

2.5.3 **410 Gone**

This response is similar to the 404 Not Found response but contains the hint that the requested user will not be available at this location in the future. This response could be used by a service provider when a user cancels their service.

2.5.4 **415 Unsupported Media Type**

This response indicates that the media type contained in the INVITE request is not supported. For example, a request for a video conference on a SIP trunk that only handles telephone calls will result in this response.

2.5.5 **486 Busy Here**

This response is used to indicate that the UA cannot accept the call at this location. In general, a 486 Busy Here is sent by a UAS unless it knows definitively that the user cannot be contacted. This response is equivalent to the busy tone in the PSTN.

2.5.6 **487 Request Terminated**

This response can be sent by a UA that has received a CANCEL request for a pending INVITE request. A 200 OK is sent to acknowledge the CANCEL, and a 487 is sent in response to the INVITE.

2.6 SERVER ERROR

This class of responses is used to indicate that the request cannot be processed because of an error with the server.

2.6.1 500 Server Internal Error

This server error class response indicates that the server has experienced an error that is preventing it from processing the request. The reason phrase can be used to identify the type of failure. The client can retry the request again at this server after several seconds.

2.6.2 503 Service Unavailable

This response indicates that the requested service is temporarily unavailable. The request can be retried after a few seconds, or after the expiration of the Retry-After header field.

3. SESSION DESCRIPTION PROTOCOL

3.1 To negotiate the setup of sessions, SIP uses another protocol, Session Description Protocol that describe the actual parameters of the media session. This includes information such as media type, codec, bit rate, and the IP address and port numbers for the media session. So it is necessary to add a SDP payload format to declare which types of events a receiver can understand. SDP fields are below.

Field	Name	Mandatory/Optional
v=	Protocol version number	m
o=	Owner/creator and session identifier	m
s	Session name	m
i=	Session information	o
u=	Uniform Resource Identifier	o
e=	E-mail address	o
p=	Phone number	o
c=	Connection information	m
b=	Bandwidth information	o
t=	Timer session starts and stops	m
r=	Repeat times	o
z=	Time zone correction	o
a=	Attribute lines	o
m=	Media information	o
a=	Media attributes	o

An example SDP message containing many of the optional fields is shown here:

```
v=0
o=sbc@ 2890844526 2890844526 IN IP4 43.32.1.5
s=IETF Update
i=This broadcast will cover the latest from the IETF
u=http://www.sipstation.com
e=user@test.com
p=+1-314-555-3333 (Daytime Only)
c=IN IP4 225.45.3.56/236
b=CT:144
t=2877631875 2879633673
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
m=video 23422 RTP/AVP 31
a=rtpmap:31  H261/90000
```

3.2 **SDP Fields Description**

3.2.1 Protocol Version

The v= field contains the SDP version number. Because the current version of SDP is 0, a valid SDP message will always begin with v=0.

3.2.2 Origin

The o= field contains information about the originator of the session and session identifiers. This field is used to uniquely identify the session. The field contains:

3.2.3 Session Name and Information

The s= field contains a name for the session. It can contain any nonzero number of characters. The optional i= field contains information about the session. It can contain any number of characters.

3.2.4 URI

The optional u= field contains a uniform resource indicator (URI) with more information about the session.

3.2.5 Email address and phone number

The optional e= field contains an e-mail address of the host of the session.

3.2.6 Connection Data

The c= field contains information about the media connection. The field contains:

3.2.7 Time, Repeat Times, and Time Zones

The t= field contains the start time and stop time of the session.

3.2.8 Media Announcements

The optional m= field contains information about the type of media session. The field contains:
m=media port transport format-list
The media parameter is either audio, video, text, application, message, image, or control. The port parameter contains the port number. The transport parameter contains the transport protocol or the RTP profile used. The format-list contains more information about the media. Usually, it contains media payload types defined in RTP audio video

profiles. More than one media payload type can be listed, allowing multiple alternative codecs for the media session. For example, the following media field lists three codecs:
m=audio 49430 RTP/AVP 0 6 8 99

3.2.9 Attributes

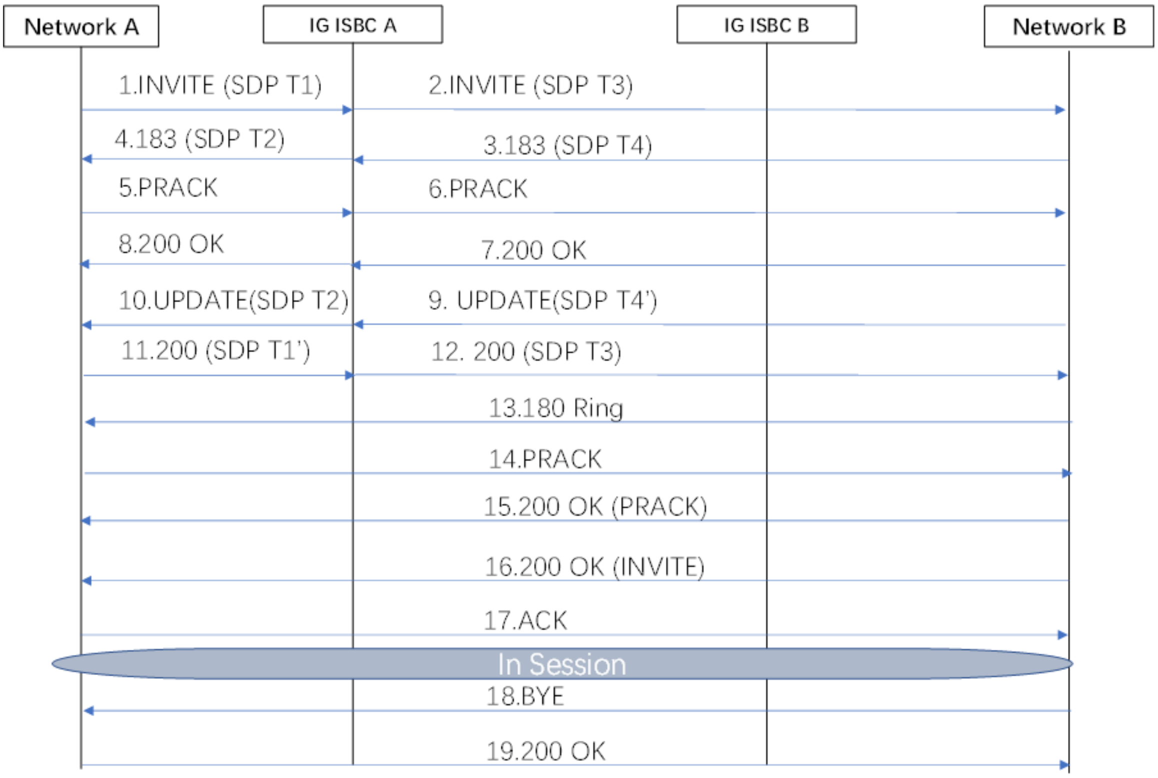
The optional a= field contains attributes of the preceding media session. This field can be used to extend SDP to provide more information about the media. The following three attribute fields could follow the media field:

a=rtpmap:0 PCMU/8000
a=rtpmap:6 DVI4/16000
a=rtpmap:8 PCMA/8000
a=rtpmap:99 iLBC

Some SDP Attribute Values Defined in RFC 4566

Attribute	Name
a=rtpmap:	RTP/AVP list.
a=fmtp:	Format transport.
a=ptime:	Length of time in milliseconds for each packet.
a=cat:	Category of the session.
a=keywds:	Keywords of session.
a=orient:	Orientation for whiteboard sessions.
a=type:	Type of conference.
a=lang:	Default language for the session.
a=quality:	Suggests quality of encoding.
a=direction:	Direction for symmetric media.
a=inactive:	Inactive mode.
a=recvonly:	Receive only mode.
a=sendrecv	Send and receive mode.
a=sendonly	Send only mode.

4. REFERENCE CALL FLOWS



4.1 Normal Call

1: Core network A sends an INVITE request to IBCF A. The INVITE request carries the SDP information about the originating UE or network A.

```
INVITE sip: 68593500@sip.ims.com;User=phone SIP/2.0
Via: SIP/2.0/UDP 192.168.2.10:5060;branch=z9hG4bK24becfdaef107dba
From: <sip: 63240104@sip.ims.com;User=phone>;tag=77f494f3f4cbabfd1b
To: <sip:68593500@ sip.ims.com;User=phone>
Call-ID: eea69e583b07a35fc59f3c5bddab96e9
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Contact: <sip:192.168.2.10:5060>
Supported: 100rel
P-Asserted-Identity: <sip: 63240104@sip.ims.com;cpc=ordinary>,<tel:
63240104;cpc=ordinary>
Max-Forwards: 30
Content-Length: 172
Content-Type:application/sdp

v=0
o=Spider-Phone 576772365 576772365 IN IP4 172.18.3.18
```

```
s=Spider-Phone
c=IN IP4 172.18.3.18
t=0 0
m=audio 30200 RTP/AVP 8
a=rtpmap:8 PCMA/8000
a=ptime:20
```

1. ISBC A sends an INVITE (SDP) request to core network B based on route configurations. The following is an example INVITE (SDP) request:

```
INVITE sip: 68593500 @sip.ims.com;user=phone SIP/2.0
Via: SIP/2.0/UDP
172.16.1.10:5060;branch=z9hG4bKp6dqidnajo0b9b69a8jbq6iq9;Hpt=75e2_16
Call-ID: isbceea69e583b07a35fc59f3c5bddab96e9
From: <sip:63240104@sip.ims.com;user=phone>;tag=77f494f3f4cbabfd1b
To: <sip:68593500@sip.ims.com;user=phone>
CSeq: 1 INVITE
Allow: INVITE,ACK,CANCEL,BYE,PRACK,UPDATE,REFER,MESSAGE
Contact: <sip:172.16.1.10:5060;Hpt=75e2_16;CxtId=4>
Record-Route: <sip:172.16.1.10:5060;Hpt=75e2_16;lr>
Supported: 100rel
P-Asserted-Identity: <sip: 63240104@sip.ims.com;cpc=ordinary>,<tel:
63240104;cpc=ordinary>
Max-Forwards: 29
Content-Length: 155
Content-Type: application/sdp

v=0
o=- 576772365 576772365 IN IP4 172.16.1.11
s=SBC call
c=IN IP4 172.16.1.11
t=0 0
m=audio 13538 RTP/AVP 8
a=rtpmap:8 PCMA/8000
a=ptime:20
```

3. Core network B returns a 183 response (INVITE) to ISBC A.
Example: 183 response (INVITE).

```
SIP/2.0 183 Session Progress
Via:SIP/2.0/UDP
172.16.1.10:5060;branch=z9hG4bKp6dqidnajo0b9b69a8jbq6iq9;Hpt=75e2_16
From: <sip: 63240104@sip.ims.com;user=phone>;tag=77f494f3f4cbabfd1b
To: <sip: 68593500@sip.ims.com;user=phone>;tag=27f307ae77cb20
Call-ID: isbceea69e583b07a35fc59f3c5bddab96e9
```

```
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Require: 100rel
Contact: <sip:172.16.1.30:10002>
RSeq:100
P-Asserted-Identity: <sip: 63240104@sip.ims.com;user=phone>
Record-Route: <sip:192.168.3.10:5060;lr>
Record-Route: <sip:172.16.1.10:5060;Hpt=75e2_16;lr>
Content-Length: 184
Content-Type:application/sdp

v=0
o=MRS 576773398 576773398 IN IP4 172.16.1.16
s=MRS
c=IN IP4 172.16.1.16
t=0 0
m=audio 30210 RTP/AVP 8
a=rtpmap:8 PCMA/8000
a=ptime:20
a=sendonly
```

4. ISBC A sends a 183 response (INVITE) to core network A. The 183 response (INVITE) contains the originating side SDP (SDP T2). The following is an example 183 response (INVITE):

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP 192.168.2.10:5060;branch=z9hG4bK24becfdaef107dba
Call-ID: eea69e583b07a35fc59f3c5bddab96e9
From: <sip: 63240104@sip.ims.com;user=phone>;tag=77f494f3f4cbabfd1b
To: <sip: 68593500@sip.ims.com;user=phone>;tag=27f307ae77cb20
CSeq: 1 INVITE
Allow: INVITE,ACK,CANCEL,BYE,PRACK,UPDATE,REFER,MESSAGE
Require: 100rel
Contact: <sip:172.17.2.1:5060;Hpt=75e2_16;CxtId=3>
Record-Route: <sip:172.17.2.1:5060;Hpt=75e2_16;lr>
RSeq: 100
P-Asserted-Identity: <sip: 63240104@sip.ims.com;user=phone>
Content-Length: 167
Content-Type: application/sdp

v=0
o=- 576773398 576773398 IN IP4 172.18.3.10
s=SBC call
c=IN IP4 172.18.3.10
```

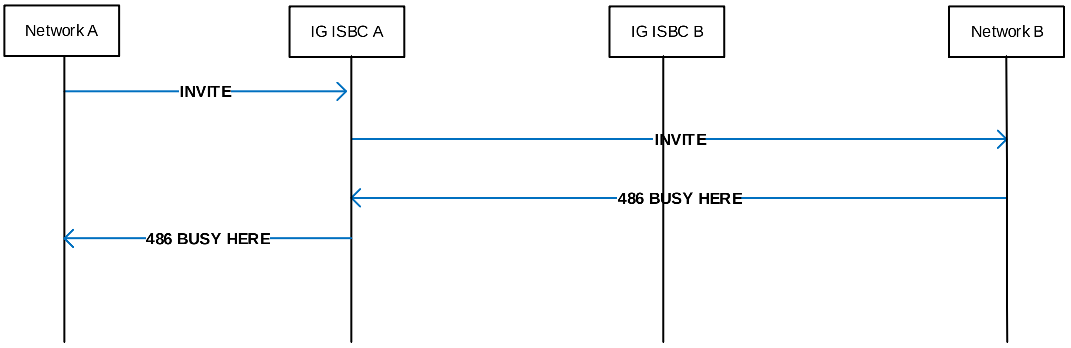
```
t=0 0
m=audio 13154 RTP/AVP 8
a=rtpmap:8 PCMA/8000
a=ptime:20
a=sendonly
```

5-8. Core network A sends a PRACK request to ISBC A, and ISBC A forwards the PRACK request to core network B. Core network B sends a 200 OK response (PRACK) to ISBC A, and ISBC A forwards the 200 OK response (PRACK) to core network A.

9-12. Core network B sends an UPDATE request to ISBC A for media renegotiation. The UPDATE request contains the terminating side media address, with the flow attribute changed to **sendrecv**. ISBC A forwards the UPDATE request to core network A. Core network A sends a 200 OK response (UPDATE) to ISBC A, and ISBC A forwards the 200 OK response (UPDATE) to core network B.

13. Core network B sends a 180 response (INVITE) to IBCF A, indicating that the called UE is ringing. ISBC A forwards the 180 response (INVITE) to core network A.
14-15. Core network A sends a PRACK request to IBCF A, and ISBC A forwards the PRACK request to core network B. Core network B sends a 200 OK response (PRACK) to ISBC A, and ISBC A forwards the 200 OK response (PRACK) to core network A.
16-17. The call is answered. Core network B returns a 200 OK(INVITE) response to ISBC A, and ISBC A forwards the 200 OK(INVITE) response to core network A. Core network A returns an ACK message specific to the 200 OK response to ISBC A, and ISBC A forwards the ACK message to core network B.
The call is established.
18. Core network B sends a BYE request to ISBC A to terminate the call, and ISBC A forwards the BYE request to core network A.
19. Core network A sends a 200 OK response (BYE) to ISBC A, and ISBC A forwards the 200 OK response (BYE) to core network B. At this point, the call is released.

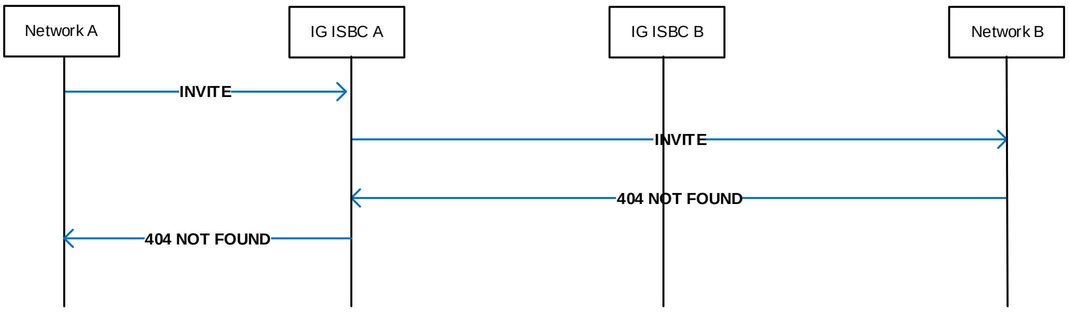
4.2 User busy



1: Core network A sends an INVITE request to ISBC A.

2. Core network B sends a 486 Busy Here message to ISBC A, and ISBC A forwards the request to core network A. The call is end due to called party is busy/user cannot be contacted.

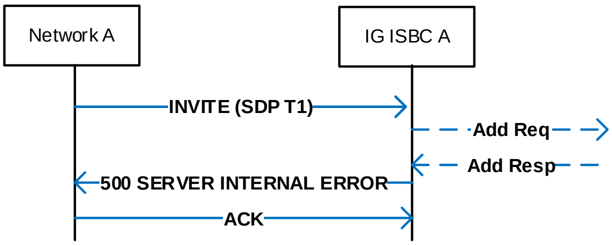
4.3 Unallocated



1: Core network A sends an INVITE request to ISBC A.

2. Core network B sends a 404 Not Found message to ISBC A, and ISBC A forwards the request to core network A. This response indicates that the user identified by the sip or sips URI in the Request-URI cannot be located by the server, or that the user is a unallocated number in the system.

4.4 Failed call



1. The core network sends an INVITE request to the IBCF. The INVITE request contains the SDP of the calling UE (SDP T1).

2. The IBCF sends an ADD Req message to the BGF, instructing the BGF to allocate a media address + port for the core-side termination. The ADD Req message contains the core-side media domain name.

3. The BGF returns an ADD Resp message to the IBCF, indicating a failure because of insufficient resources.

4. The IBCF returns a 500 (Server Internal Error) response to the core network. The 500 response contains the Warning header. An example 500 message is as follows:

SIP/2.0 500 Server Internal Error

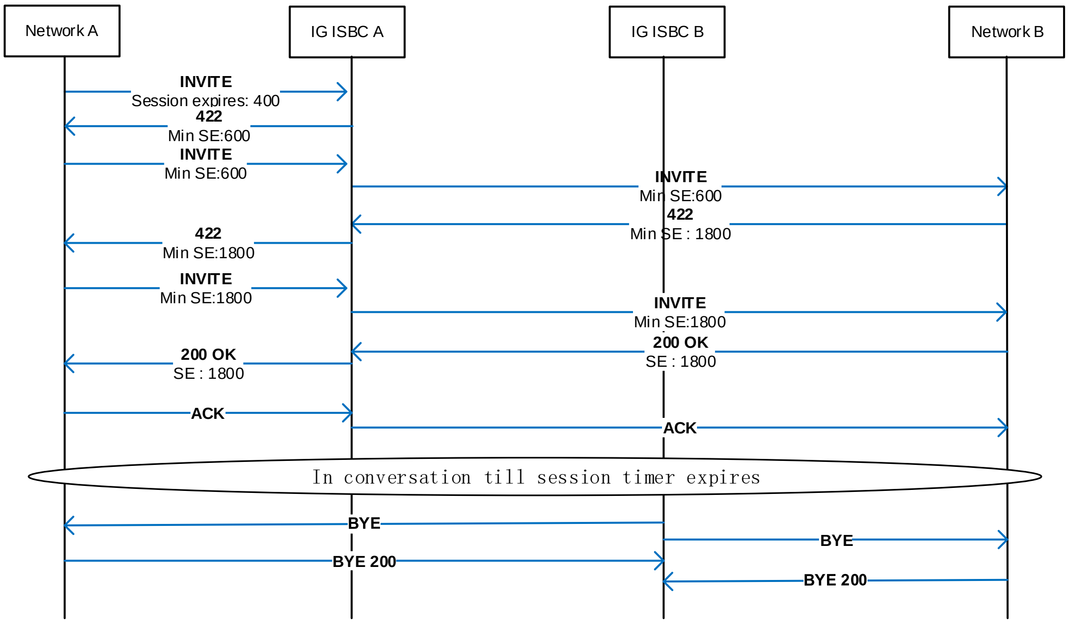
......

Warning: 399 35864.5433.A.228.90.11.0.16.21760.15386150.0. "Media Negotiation Failed"

......

5. The core network sends an ACK message to the IBCF. At this point, the call is disconnected.

4.5 Releasing resources in a failed session



1. Core network A initiates an INVITE request to the SBC. If the UE requires the session timer, the UE sets the value of the Supported header in the INVITE request to **timer** and the Session-Expires header to 400 seconds.

2. After receiving the INVITE request, the SBC checks the supported Min-SE value, which is 600 seconds by default and can be changed using MOD STMR. The value of the Session-Expires header in the INVITE request is less than that configured on the SBC. Therefore, the core network returns a 422 response. The 422 response contains the Min-SE header, informing the UE that the value of the Min-SE header supported by the IBCF is 600 seconds.

3. Core network A initiates an INVITE request again after receiving the 422 response. The INVITE request carries the Call-ID, From, and To headers, which are the same as those in the previous INVITE request and carries the new Session-Expires value and adds the Min-SE header. The value of the Min-SE header is the larger one between the local Min-SE value and the Min-SE value that is carried in the 422 response. After receiving the INVITE request, core network B checks the request based on session timer configurations. The value of the Session-Expires header in the INVITE request is smaller

than the Min-SE header value configured on core network B. Therefore, core network B returns a 422 response to the SBC. Then the SBC forwards the 422 response to the UE.

4. Core network A initiates an INVITE request again after receiving the 422 response. The INVITE request carries the Call-ID, From, and To headers, which are the same as those in the previous INVITE request and carries the new Session-Expires value and adds the Min-SE header. The SBC checks the request again. If the request meets configuration requirements, the SBC forwards the request to core network B. Core network B checks the request based on session timer configurations. If the request meets configuration requirements, core network B forwards the request to the called UE. After the called UE returns a 200 OK response, core network B sends the 200 OK response to the MO-side SBC. The 200 OK response carries the Session-Expires value and specifies the NE that refreshes the session.

5. After receiving a 200 OK response, core network A returns an ACK message to the SBC. The SBC forwards the ACK message to core network B. The call is successfully connected.

6. The call expires, and neither core network A or core network B initiates any re-INVITE or UPDATE request to update the session timer. The SBC sends BYE requests to both core networks. The BYE requests carry the Reason header, indicating that the session is released due to session timer timeout. Core network A and core network B return 200 OK responses (BYE) to the SBC. At this point, the session is released. The following is an example BYE message:

```
BYE sip:192.168.10.1:5060 SIP/2.0
......
Reason: Q.850;cause=31,SIP;text="A.080.011.228.0.0.00084.00000000 Released the session because of session timer expiration"
Content-Length: 0
```

5. MEDIA NEGOTIATION

When an interworking session sets up, the two peer ISBC negotiate the media code through SIP/SDP. The ISBC can add common voice codecs to user negotiation to ensure successful interworking sessions. In this process, the SBC can control codec on the media layer.

During interworking, the SDP should support the offer/answer model specified in IETF RFC 3264 [RFC 3264: An Offer/Answer Model with SDP].If media messages are transmitted over TCP, the SDP must comply with IETF RFC 4145. RTP/RTCP protocol (specified in IETF RFC 3550) should be supported for audio calls.

5.1 Voice

Table 4 recommended codecs. All other codecs are optional and subject to bilateral agreements. Apart from Codec, the recommended Packetization Period for all Codecs is 20ms.

Table 4 Recommended Codecs Fixed Networks

Narrowband
G.711a/u
G.729

5.2 Fax

Fax is a telecommunications service in which data is transmitted between two fax machines. It provides a complete set of service functions, including fax data bearer and fax service management, for fax machines on both sides of the network.

ISBC is deployed between two IMS networks or between one IMS network and another type of network and forwards fax data between the networks.

On IP interconnects where fax transmissions are a mandatory supported service this SHOULD be done according to the methods described below.

ISBC MUST use the default values in ITU-T Recommendation T.38 (09/2010) Annex H table H.1 and H.2. Following attributes MUST be included in SDP offer and SDP answer with the T.38 image:

```
m=image <portnumber> udpt | t38
a=T38FaxVersion:0
a=T38FaxRateManagement:transferredTCF
a=T38FaxUdpEC:t38UDPRedundancy
a=T38MaxBitRate:14400
a=T38FaxMaxBuffer:200
a=T38FaxMaxDatagram:200
```

The I-SBC must support fax transmission through audio (e.g., ITU-T G.711over RTP) including fax and modem service. Following attributes MUST be included in SDP offer and SDP answer with fax type:

```
m=audio 156 RTP/AVP 8 0
a=X-fax
```

Modem type is following:

```
m=audio 156 RTP/AVP 8 0
a=X-modem
```

5.3 DTMF detection

ISBC shall support DTMF digits generated during a SIP session. DTMF can be carried by inbound or outbound signalling via SIP INFO.

The DTMF dialling number is carried in the MIME subtype telephone-event of the SDP message as the payload. For the encoding requirements, see IETF RFC 4733.

When sending an SDP offer, it should indicate support of events 0 to 15 (0-9, A-D, *, #) which are encoded with event codes 0-9, 10, 11 and 12-15 respectively.) in the fmtp attribute. If the SDP offer includes a single codec then the RTP clock rate used for DTMF shall be the same as for the offered codec. If the SDP offer includes codecs with different RTP clock rates then it shall include one RTP payload type representing telephone events per each of these RTP clock rates.

Here's an example：

```
a=rtpmap:98 AMR-WB/16000/1
a=rtpmap:99 telephone-event/16000
a=fmtp:99 0-15
a=rtpmap:100 AMR/8000/1
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

If audio codecs with two clock rates, 8000 and 16000, are transmitted over audio channels, I-SBC should also contain two telephone-event codecs, one with the clock rate 8000 and the other with the clock rate 16000. The order in which the two telephone-event codecs are arranged in the message is determined by the order in which the clock rates of the audio codecs are presented.

If audio codecs with only the clock rate 8000 or clock rate 16000 is transmitted over audio channels, I-SBC should also contain only one telephone-event codec with the same clock rate as that of the audio codecs.

6. NP (NUMBER PORTABILITY)

The I-SBC shall be able to support following SIP headers in NP service.

- P-Additional-Calling-Party:
  P-Additional-Calling-Party is used to carry the N2 number of the number portability subscriber.

SIP header	Receive	Send
P-Additional-Calling-Party	Y	Y

Example:
P-Additional-Calling-Party: tel:+6569689560

- Reason:
  Reason header is used to present the Q.850 cause information in a SIP error response message. subscriber.

SIP header	Receive	Send
Reason	Y	Y

Example:
Reason: Q.850;cause=14;text="Number ported out",SIP;cause=410;text="Gone"
Reason: Q.850;cause=14;text="unknown"

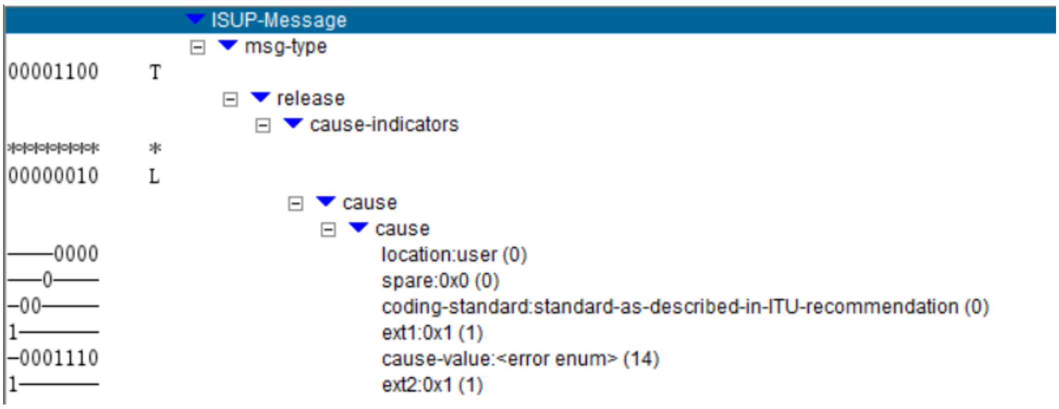
Note: ISBC shall keep the cause value not changed

Sample Message:
vIG receive:

```
SIP/2.0 410 Gone
Via: SIP/2.0/UDP 10.161.224.67:5065;branch=z9hG4bKwxijp8788dw78iovd7p64xvij
Call-ID: u4du467vixxoi7ounnfj4tifppi8j448@UAC
From: <sip:84577342@10.161.180.5;user=phone;cpc=ordinary;srvattri=national>;tag=vxjdoouv-CC-1004
To: <sip:+6569689060@10.161.224.139:5059;user=phone>;tag=3mq0kq3d
CSeq: 1 INVITE
Warning: 399 5244.683.B.261.5.65.0.19.41728.0.0.vims.singtel.com "Server Internal Error"
Reason: Q.850;cause=14;text="Number ported out",SIP;cause=410;text="Gone"
Content-Length: 0
```

vIG send:

```
 SIP/2.0 410 Gone
Via: SIP/2.0/UDP 10.161.180.5:5061;branch=z9hG4bKmbyvyywopnpmvy33eooyn2eny
Call-ID: ygwvlowm3wexoznwbygg2vllwptewpll@UAC3000
From: <sip:84577342@10.161.180.5;user=phone>;tag=g2xxvnel-CC-24
To: <sip:69689060@10.161.224.139:5059;user=phone>;tag=4unfuiju
CSeq: 1 INVITE
Reason: Q.850;cause=14;text="unknown"
Warning: 399 - "UAC3000 R001-ACU Rel POS:[14015] Release from CCB PP[0x1f5] CS[0x7] AS[0x4] FR[0x8] TR[0x9] TYPE[0x2]"
Content-Length: 6
Content-Type: application/isup;version=sin
0C 02 00 02 80 8E
```



```
                    ISUP-Message
                      msg-type
00001100     T
                        release
                          cause-indicators
********     *
00000010     L
                            cause
                              cause
——0000                          location:user (0)
——0———                          spare:0x0 (0)
–00———                          coding-standard:standard-as-described-in-ITU-recommendation (0)
1————                           ext1:0x1 (1)
–0001110                        cause-value:<error enum> (14)
1————                           ext2:0x1 (1)
```

```
INVITE sip:10.161.224.14:5091;transport=udp;Hpt=8f22_16;suid=5BMRBA7goQoAAAAAAAAAAAAAAABAAAA;srti=d0_1024 SIP/2.0
Via: SIP/2.0/UDP 10.161.224.36:5060;branch=z9hG4bKmcppoadaptleomedwcqbll5pq;Role=3;Dpt=7a44_16;TRC=ffffffff-31f49,SIP/2.0/UDP 10.161.224.2:5060;branch=z9hG4bKpqw0yxrrjrxaqr9po89qpyyp0;Role=3;Dsp=ed4a__2e_5f8ef9da_2_18;TRC=ffffffff-22c59
Route: <sip:term@10.161.224.219:5060;transport=udp;lr;ssn;hwnos;Hpt=8f22_86;TRC=365-
```

```
ffffffff;suid=5BMRBA7goQoAAAAAAAAAAAAAAAAABAAAA;srti=d0_1024>,<sip:term@10.161.224.14;lr>;IMS-END-TYPE=IMS-BRA;MID-NUM=1000;USN=80001
Record-Route: <sip:10.161.224.36;lr;Dpt=7a44_116;Role=3;CxtId=4;X-UaSKv=51_5f8ef9da_5;spln=S;X-HwB2bUaCookie=1;TRC=ffffffff-31f49>,<sip:10.161.224.2:5060;lr;Dsp=ed4a__2e_5f8ef9da_2_18;Role=3;CxtId=4;TRC=ffffffff-22c59;X-HwB2bUaCookie=0>
Call-ID: oa33psrjaptpuqwaorrsr9xpsur9wj8j@10.161.224.2
From: <tel:98810971;noa=subscriber;phone-context=+65>;tag=auxqjwyy
To: <tel:69689061;phone-context=+65>
CSeq: 1 INVITE
Allow:
INVITE,ACK,OPTIONS,BYE,CANCEL,REGISTER,INFO,PRACK,SUBSCRIBE,NOTIFY,UPDATE,MESSAGE,REFER
Contact: <sip:10.161.224.2:5060;TRC=ffffffff-22c59;Dsp=ed4a-200>
Max-Forwards: 62
Supported: timer,100rel
User-Agent: Huawei UAC3000 V500R019
Session-Expires: 1800
Min-SE: 600
P-Asserted-Identity:
<sip:+6598810971@vims.singtel.com;cpc=ordinary>,<tel:+6598810971;cpc=ordinary>
P-Visited-Network-ID: "jeagcf1.vims.singtel.com"
P-Access-Network-Info: ANI_10.166.215.50
P-Charging-Vector: icid-value=agcf--20201020145313-100103696;orig-ioi=plscscf1.vims.singtel.com
Request-Disposition: fork
P-Early-Media: gated
P-Called-Party-ID: <sip:+6569689061@vims.singtel.com>
X-Trace: 262134;relative=0
P-Additional-Calling-Party: tel:+6569689560
Content-Length: 1427
Content-Length: 359
Content-Type: application/sdp

v=0
o=HuaweiATS9900 1 1 IN IP4 10.161.224.2
s=SBC call
c=IN IP4 10.161.244.67
t=0 0
m=audio 11252 RTP/AVP 8 0 18 4 2 98 99 101
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:18 G729/8000
a=rtpmap:4 G723/8000
a=rtpmap:2 G726-32/8000
a=rtpmap:98 G726-40/8000
a=rtpmap:99 G726-32/8000
a=rtpmap:101 G726-24/8000
a=ptime:20
a=fmtp:18 annexb=no

--ssboundary-1_--
```

7. SECURITY

In this session we highlight the security related to interconnection scenario.
The security control between interconnect links, IMDA security requirements in **Annex D** shall be applied mutually.

7.1 Threats

Denial of service is an attack by a third party who tries to interrupt service of a protocol or a service. For example, a simple denial of service attack is a packet flood, where an attacker sends a flood of IP packets, which overloads the target. This type of DOS attack is not specific to SIP or Internet communication. When launched from multiple hosts, the attack is called a distributed denial of service attack (DDOS).

Eavesdropping is an attack that involves monitoring or listening in to a session. This could be the signaling, indicating who is communicating with whom, or it could be the actual conversation itself. As such, this can be a signaling (SIP) or media (RTP) attack. Impersonation is pretending to be someone else in a communication. An attacker could pretend to be either a SIP user or a server, depending on the attack.

7.2 Security Protocols

IPSec or IP security is a protocol that operates at the IP layer of the protocol stack. As a result, it works with any transport protocol above it in the protocol stack, such as TCP and UDP, and protocols such as SIP and RTP run over it without any changes. In general, an IPSec session needs to be established between hosts on the Internet.

7.3 SIP Security Model

This section will introduce the security model for SIP. Security begins with authentication, and there are a number of ways a SIP message can be authenticated. One way is if it is received over an IPSec or VPN tunnel that has previously been authenticated. Another method is if it is received over a TLS connection that has been properly authenticated.

7.4 Security Measures on SIP Interconnect

This session defines security measure from the perspective of SIP interconnection.

7.4.1 Signaling Firewall Function

- The ISBC should provide the signaling protection function. The ISBC shall be able to comply with the 5-tuple (source IP address, destination IP address, transmission protocol, source port, and destination port).
- The ISBC should provide the application-level signaling protection function. That is, the ISBC should be able to analyze the syntax of SIP messages and discard abnormal messages.

- The ISBC should be able to provide signaling overload protection. The ISBC preferentially processes SIP messages related to ongoing sessions and rejects new INVITE messages when the load is heavy.
- The ISBC should be able to configure the size of a single SIP signaling message to be received and forwarded.
- The ISBC must be able to check SIP messages and detect malicious attacks. When detecting a malicious attack, the ISBC can automatically block the attack, blocklist the attack source, and record information in logs.
- The ISBC should be able to enable or disable tools such as ICMP, SNMP, and DNS or administrative services. When these tools or managed services are open, traffic should be limited. In addition, the ARP traffic rate can be limited to prevent ISBC exceptions caused by misconfiguration or local ARP storms caused by faulty engines.

7.5 Anti-Dos Attack

- The ISBC should be able to detect DoS attacks and automatically intercept DoS attacks without manual intervention. In addition, the ISBC should provide the load protection function. When the system load exceeds the threshold, the ISBC can automatically reject some calls to ensure that the system does not lose service capability due to overload.

7.6 Media Stream Filtering

- The ISBC should be able to provide user plane protection. The ISBC should be able to receive media packets from authorized media terminations and discard media packets from unauthorized media terminations based on signaling negotiation results. In addition, the ISBC should be able to limit the media rate.
- The ISBC should be able to use the filtering mechanism to ensure that only valid media stream packets pass through.

7.7 Blacklist and Whitelist Function

- ISBC should provide the blacklist and whitelist function to enable block or allow the incoming call from specified trunk.
- ISBC shall be able to configure the blacklist and whitelist based the calling number and called number prefix.

ABBRIVIATION

IETF	Internet Engineering Task Force
ITU-T	International Telecommunication Union-Telecommunications Sector
RFC	Request for comments
ICMP	The Internet Control Message Protocol
SNMP	Simple Network Management Protocol
SIP	Session Initiation Protocol
IP	Internet Protocol
SDP	Session Description
DNS	Domain Name System
ARP	Address Resolution Protocol
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
RTP	Realtime Transport Protocol
RTCP	Realtime Transport Control Protocol
IBCF	Interconnection Border Control Function
ISBC	Interconnect Session Border Controller
VPN	Virtual Private Network
IPSec	IP Security
DoS	Denial of Service

ANNEX A

SECTION 1A

SECTION 1A: INTERCONNECT TESTING

1. TESTING PRINCIPLES

a. The purpose of the Interconnect Testing is to provide reassurance that each Party's Network can inter-work correctly with the other Party's Network and that the Interconnection will not adversely affect the existing services provided by each Party to their respective customers.

b. Interconnection to SingTel's Network shall be carried out and provision of Services under this RIO Agreement provided only after the satisfactory completion of the Interconnect Testing under this Annex and after SingTel is satisfied with the Interconnect Testing results in accordance with this Schedule.

2 PRE-REQUISITES FOR INTERCONNECT TESTING

a. Prior to the conduct of Interconnect Testing, the Requesting Licensee shall fully test its Network to ensure that it conforms to the Interface Specification as specified in Section 1 of Annex A. Any defects in hardware or software of the Requesting Licensee's Network so discovered must be corrected before the commencement of Interconnect Testing.

3 TESTING ITEMS

a. Interconnect Testing shall be carried out in accordance with SingTel's testing manuals. The Requesting Licensee shall perform Interconnect Testing in accordance with this Annex or as otherwise agreed by SingTel:

    a. where initial Interconnection, whether Physical Interconnection or Virtual (Distant) Interconnection, is to occur; or

    b. where a new POI is to be established; or

    c. where the Parties have agreed to implement a Network Change; or

    d. prior to the reinstatement of a Service that has been suspended under clause 12 of the RIO Agreement; or

e. where either Party has implemented new software or updated existing software that affects or is likely to affect Interconnection between the SingTel Network and the Requesting Licensee's Network.

4 TIMELINE FOR TESTING

a. The Requesting Licensee shall book the required test date and the testing duration at least one (1) month prior to the requested testing date. The Requesting Licensee shall submit the test order form as contained in the Attachment to SingTel to request Interconnect Testing. The test order form shall contain the necessary details for the testing setup, including the proposed test schedule and the requested test date.

b. SingTel shall advise the Requesting Licensee of the test date in writing within ten (10) Business Days of receipt of the test order form. If SingTel is not able to perform the testing on the requested test dates, SingTel shall counter-propose an alternative test schedule with the response and negotiate in good faith with the Requesting Licensee to arrange an alternative schedule.

c. The Parties shall act in good faith and make reasonable endeavours to complete all test items within the estimated testing period.

d. The requested testing duration is subject to mutual agreement by the Parties.

e. Any request for extension to the testing duration beyond the agreed time frame by the Requesting Licensee is subject to mutual agreement by both Parties. The Requesting Licensee shall make its request for extension at least two (2) Business Days prior to the end of the testing duration.

f. SingTel shall not be liable to the Requesting Licensee for any delay in completing all the test items unless such delay is directly attributable to the neglect or fault of SingTel.

5 DAILY TIME TABLE FOR INTERCONNECT TESTING

a. All Interconnect Testing shall be carried out during Business Days between 0900 hours and 1700 hours, with one (1) hour lunch break in between.

6 TESTING RESULTS

A. Connection of the Requesting Licensee's Network to SingTel's designated IGS/SGS shall be carried out only upon satisfactory completion of the Interconnect Testing in accordance with SingTel's interconnect manuals and after SingTel is satisfied with the Interconnect Testing results.

b. In the event that SingTel identifies a Critical Problem(s), the Requesting Licensee shall ensure that such problems are resolved within the testing period. Otherwise, the Requesting Licensee shall make booking for a new testing date to verify these Critical Problem(s) when solutions are available. Critical Problem refers to a problem affecting the conveyance of Interconnected Calls between SingTel's Network and the Requesting Licensee's Network including, but not limited to, problems that result from deviations by the Requesting Licensee from the specifications that it provided to SingTel.

7 CHARGES FOR INTERCONNECT TESTING

a. The Requesting Licensee shall pay SingTel the Charges specified in Schedule 9 for Interconnect Testing.

b. All Calls made during the Interconnect Testing shall be chargeable to the Requesting Licensee.

8 CANCELLATION AND DELAY IN TESTING

a. The Requesting Licensee shall adhere to the testing date and testing duration as approved by SingTel.

b. Any request for cancellation of Interconnect Testing shall be made in writing to SingTel and the Requesting Licensee shall pay SingTel the cancellation Charges in accordance with Schedule 9.

c. In the event that Interconnect Testing is completed or is terminated by the Requesting Licensee before the last day of the testing duration, the Requesting Licensee shall pay SingTel the Charges for the testing duration up to and including the day on which testing was completed or terminated and such other reasonable costs as may be incurred by SingTel as a result of early termination of the Interconnect Testing.

d. SingTel may unilaterally delay or postpone the testing date or duration due to matters outside SingTel's reasonable control. SingTel shall allocate a corresponding extension of the testing period for the number of days so delayed or allocate a new testing date for Interconnect Testing on a non-discriminatory basis. The Requesting Licensee shall not be liable to pay additional Charges for such extension period granted.

APPLICATION FORM FOR INTERCONNECT TESTING

Page 1 of 2

OPERATOR	
Name of Operator	Licence Type/Class
Business Address Postal Code:	
I wish to apply for SIP Interworking Test For the period from _________________ to _______________ . (____ Days)	
In support of my application, I provide the following Technical Information for the Setting up of Interconnect Testing **For SIP Trunk Testing**	

I confirm that we have a valid License from the Authority to operate telecommunication services. I agree that approval of this application is subject to SingTel's discretion and that SingTel reserves the right to decline the application or to make variation to the requested testing period without giving any reason.

I understand and agree that I shall execute the RIO Agreement prior to the conduct of the Interconnect Testing. I am liable for all charges that may arise from any delay or cancellation of Interconnect Testing should the RIO Agreement not be executed prior to the test.

I understand and agree that in addition to the charges for Interconnect Testing, all Calls made during the Interconnect Testing shall be chargeable to me.

I understand and agree that any request for cancellation of Interconnect Testing shall be made in writing to SingTel and I shall pay SingTel the cancellation charges as follows:

No. of calendar days (from the receipt of cancellation notice to the date of commencement of testing):

<7	100%
7-13	80%
14-20	35%
>21	20%

I acknowledge that the interconnect testing may only be carried out subject to the Terms and Conditions of the RIO Agreement, and the Terms and Conditions of this Application. I agree to be bound by the said terms and conditions and in consideration of my application being approved. Upon approval, I agree to pay the charges as required.

I confirm that all the information given in making this application is true, correct and complete.

Signature Designation

Name Date

FOR SINGTEL USE

The application is □ Approved
□ Rejected
Reason for rejection: ____________________________

Agreed Schedule for Interconnect Testing

from _________________ to _______________ . (____ Days)

SingTel SIP Signalling information

Signalling IP

Media IP

Signature Designation

Name Date

ANNEX A

SECTION 2

SECTION 2 - SIP INTERWORKING TESTING MANUAL

1 INTRODUCTION

1.1 GENERAL

This manual describes the test items for the SIP testing, the testing principles, and the criteria for successful testing.

2. TESTING ACTIVITIES

2.1 TRANSMISSION POWER TEST

2.1.1 Fibre connectivity shall be set up. Acceptable Tx/Rx power must be received at both ends. If it’s Metro-E, bandwidth testing will be done.

2.2 NETWORK REACHABILITY TEST

2.2.1 IP connectivity shall be set up with IPv4 address space. Public IP addressing shall be used. Static or Dynamic routing shall be configured at both ends.

2.2.2 Ping test shall be performed, and ping reply shall be received within acceptable milliseconds.

2.3 SIP REACHABILITY TEST

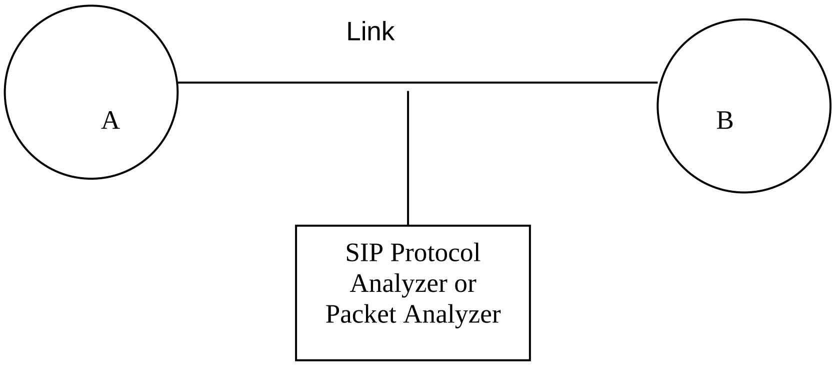
2.3.1 Both ends shall be configured to use OPTIONS message to detect SIP Heartbeat. Both ends shall receive 200 OK after it sends OPTIONS message to peer end.

2.4 SIP SECURITY TEST

2.4.1 Perform the available security tests according to Chapter 7 security setting and definitions.

2.5 TEST CONFIGURATION

SIP Signaling links are required to be connected as shown below. An SIP Protocol Analyzer or Packet Analyzer shall be used to monitor and capture the SIP messages exchanged between the two end points.



TEST ITEM	SIP TEST ITEM	TITLE	RESULT	DATE	TESTED BY	REMARK
1	2.1	Transmission Power Test				
2	2.2	Network Reachability Test				
3	2.3	SIP Reachability Test				
4	2.4	Security Test				

ANNEX A

SECTION 2A

SECTION 2A – SIP PEERING TEST SPECIFICATION

1 SIP HEARTBEAT (OPTION) MANAGEMENT

1.1 SIP Option Message activation

Enable the SIP Option method in SIP peering configuration. Confirm that the SIP peers become available after Option and 200 OK messages are exchanged.

2. LOAD SHARING BETWEEN SIP PEERING GROUP

2.1 All SIP peers are available.

To check the load sharing between SIP PEER. Make Test calls to same destination by using same route. The call must go in round robin manner between available SIP peering group.

3 Failover

3.1 Failover as with one peer unavailable

To check the failover between SIP peering groups when a SIP peer is unavailable. Confirm that Calls with must go to secondary peer in the group.

SECTION 2A : SIP INTERCONNECTION TEST SPECIFICATION

TEST ITEM	TEST ITEM	TITLE	RESULT	DATE	TESTED BY	REMARK
1	1.1	SIP Option message activation				
2	2.1	Load sharing between SIP peering group				
3	3.1	Failover				

ANNEX A

SECTION 2B

SECTION 2B - SIP BASIC CALL TEST

1 SUCCESSFUL CALL SETUP

1.1 Ordinary Call (with INVITE, 180 and 200OK)

To verify that a Call can be successfully completed using address complete message, Call progress message and answer message.

2 NORMAL CALL RELEASE

2.1 Calling party clears before answer

To verify that the Calling Party can successfully release a Call prior to receipt of answer.

2.2 Calling Party clears after answer

To verify that the Calling Party can successfully release a Call after answer.

2.3 Called Party clears after answer

To verify that a Call can be successfully released in the backward direction.

2.4 Suspend and resume initiated by a Calling Party

To verify that the Calling subscriber can successfully suspend and resume a Call.

2.5 Suspend and resume initiated by a Called Party

To verify that the Called subscriber can successfully suspend and resume a Call.

3 UNSUCCESSFUL CALL SETUP

Validate a set of known causes for release

To verify that the Call will be immediately released if a release message with a given cause is received and the correct indication is given to the Calling Party.

3.1 Called subscriber busy : # 486 user busy

3.2 Destination links are busy : # 503 service unavailable

3.3 Call rejected or not accepted #486 Call rejected

3.4 Calling to an unallocated number : #404 unallocated number

3.5 All outgoing routes/trunk busy : #503 Service unavailable

3.6 Q.118 timer; no answer from Called Party : # Cancel

4. BEARER SERVICES (MEDIA NEGOTIATION)

G.711 a/u

4.1 Successful Call setup (G.711 a/u)

To verify that a 64 kb/s audio Call can be successfully completed using appropriate transmission medium requirement and user service information parameters.

4.2 Unsuccessful Call setup

To verify that the Call will be immediately released when the unsupported media type is used to establish the session.

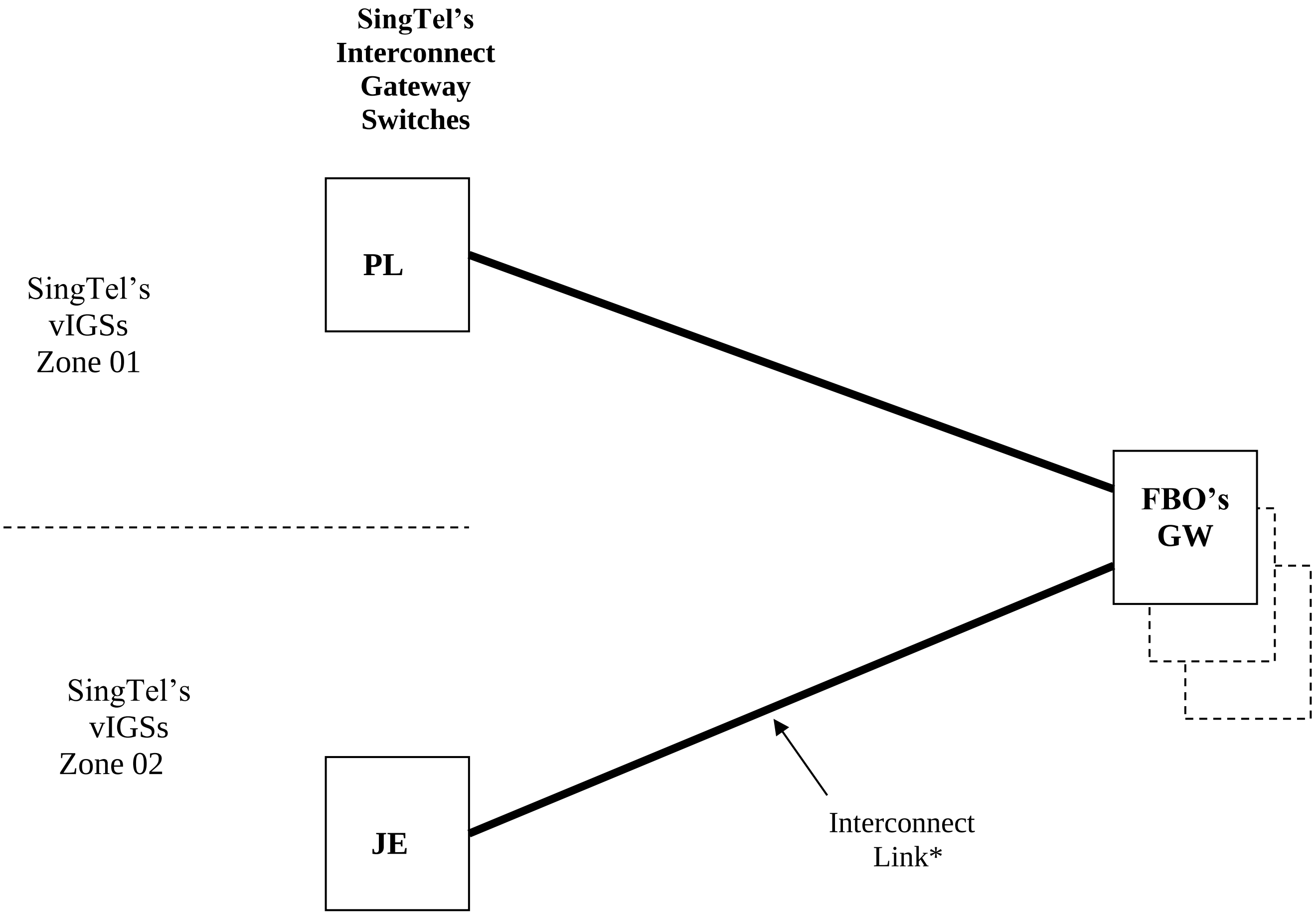
SECTION 2B : SIP BASIC CALL CONTROL TEST SPECIFICATION

TEST ITEM	SIP TEST ITEM	TITLE	RESULT	DATE	TESTED BY	REMARK
1	1.1	Ordinary Call (with Invite and 180, 200 OK)				
2	2.1	Calling party clears before answer				
3	2.2	Calling party clears after answer				
4	2.3	Called party clears before answer				
5	2.4	Suspend and resume initiated by a Calling Party				
6	2.5	Suspend and resume initiated by a Called Party				
7	3.1	Called subscriber busy: #486 Busy Here				
8	3.2	Destination links are busy: #503 Service Unavailable				
9	3.3	Call rejected or not accepted #486 Busy Here				
10	3.4	Calling to an unallocated number: #404 Not Found				
11	3.5	All outgoing routes/trunks busy : #503 Service Unavailable				
12	3.6	No answer from Called Party: #Cancel				
13	4.1	Successful Call setup (G.711 a/u)				
14	4.2	Unsuccessful Call setup				

ANNEX A

SECTION 2C

SECTION 2C - INTERCONNECT LINKS AND INTERCONNECT CONFIGURATION BETWEEN SINGTEL AND FBO



Legend:

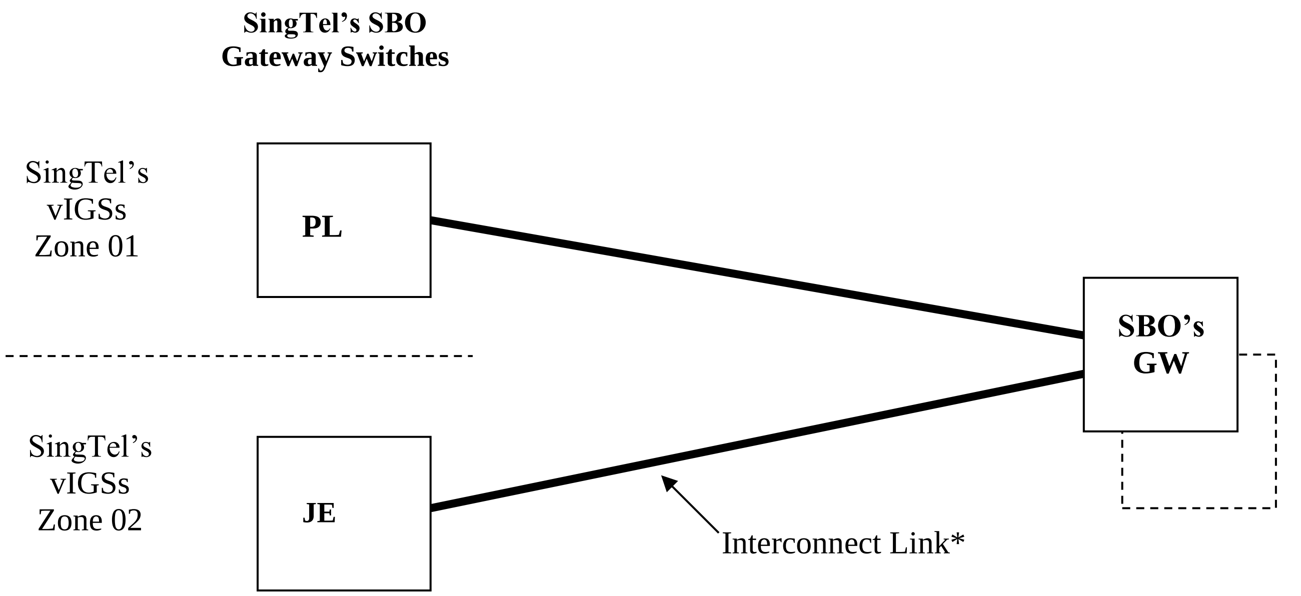
PL – Paya Lebar
JE - Jurong East
GW – Gateway Switch

* Minimum Interconnection Link Capacity 1 Gbps per IGS

ANNEX A

SECTION 2D

SECTION 2D - INTERCONNECT LINKS AND INTERCONNECT CONFIGURATION BETWEEN SINGTEL AND SBO



Legend:

PL – Paya Lebar
JE - Jurong East
GW – Gateway Switch

* Minimum Interconnection Capacity of 1 Gbps per SGS

ANNEX B

OPERATIONAL PROCEDURES

ANNEX B – OPERATIONAL PROCEDURES

1. INTRODUCTION

1.1 This Annex provides the operations and maintenance procedures to be carried out by the Parties to maintain satisfactory connection to each other's Network. It generally provides the fault handling procedures related to the Network. Procedures for carrying out planned engineering works, testing and monitoring are also described in this Section.

2 FAULT HANDLING PROCEDURES

2.1 General

2.1.1 Prior to activating the fault handling procedures, the Party reporting the fault (**reporting Party**) must reasonably establish that a genuine fault exists and also that every effort has been made to prove that the fault is not within the reporting Party's side of the POI.

2.1.2 Faults related to the Interconnect Links from SingTel are not covered in this RIO Agreement and its Annexes. The Requesting Licensee is responsible for the Interconnect Links. It is the Requesting Licensee's responsibility to ensure that the fault does not lie on its side of the POI, including a fault relating to the Interconnect Link before reporting the fault to SingTel under this RIO Agreement.

2.1.3 Each Party shall maintain its own fault reporting centre which shall be responsible for handling the faults between Networks, coordinating the fault clearance (including escalations) within its own Network and subsequently reporting the clearance of the fault to the other Party. Appendices 1 and 2 contain details of both Parties' fault reporting centres.

2.1.4 Both Parties shall co-operate in any investigation and follow up actions and keep each other informed on the status of the progress of the fault clearance in a timely manner.

2.1.5 Each Party shall establish twenty-four (24) hour contact points for fault reporting at its nominated fault reporting centre. Appendices 1 & 2 contain information on the contact points of the Parties for such purpose.

2.2 Type Of Faults

2.2.1 Faults reported may be classified as follows:

2.2.1.1 Signalling Link faults; and

2.2.1.2 Gateway Switch Network faults.

2.2.2 Signalling Link Faults

2.2.2.1 All Signalling Links provided by SingTel shall be supervised closely by the Requesting Licensee and any fault shall be reported to the reporting centre of SingTel as soon as possible.

2.2.3 Gateway Switch Network Faults

2.2.3.1 Faults related to the IGS/SGS or Requesting Licensee’s system shall be referred to the related IGS/SGS Switch during office hours, or NMC during After Office Hours.

2.3 Interconnect Fault Status

2.3.1 When a Party reports a fault to the other Party, they shall agree on the classification of the fault reported, i.e. whether it is service affecting or non-service affecting. They will also exercise their judgement and discretion and agree upon whether a non-service affecting fault could eventually develop into a service affecting fault.

2.3.2 Service affecting fault(s) may cause service interruption to the Customers when Interconnected Calls conveyed between the Networks encounter great difficulty in completion. Failure of more than one-third of the Interconnect Links, breakdown of major cable plant, loss of SIP Signalling, one-way voice, distorted voice, mute calls etc, which are all likely to result in various degrees of service interruption shall be included in the classification of service affecting fault(s).

2.3.3 Non-service affecting fault(s) are those that do not adversely affect the Call handling capability of the Network to complete the Interconnected Calls. Failure of less than one-third of the Interconnect Links or the loss of SIP Signalling Links shall be included in the classification of non-service affecting fault(s) unless otherwise agreed by both Parties to upgrade it to service affecting fault(s).

2.3.4 Table 3.1 below shows the target response time for service affecting and non-service affecting fault(s).

2.4 Handling Of Faults

2.4.1 Interconnect Link faults (Network Level/IP Reachability)

2.4.1.1 Faults due to optical fibre breakdown, IP Core equipment failure or other related equipment in the IGS/SGS which causes the unavailability of an Interconnect Link shall constitute an Interconnect Link fault.

2.4.1.2 Interconnect Link faults that affect less than one-third of the working capacity of the relevant Interconnect Link shall be included in the classification of non-service affecting fault(s). Interconnect Link faults that affect one-third or more of the working capacity of the relevant Interconnect Link shall be included in the classification of service affecting fault(s).

2.4.2 SIP Signalling Link Faults

All SIP Signalling Links shall be supervised closely by both Parties and any fault shall be reported to the reporting centre of the concerned Party as soon as possible. SIP Signalling Link failures that affect the operation of the call signalling shall be considered as service affecting.

2.4.3 IGS/SGS Network Faults

Faults related to the IGS/SGS equipment may have an effect on the conveyance of Interconnected Calls between the Networks. If such IGS/SGS fault cannot be cleared by normal fault clearance procedures by the Party/Parties concerned, then it will be reported to the higher level following the fault escalation procedure.

3 TARGET RESPONSE TIMES

3.1 The target response time for attendance to an alarm or reported fault will depend on the time of its occurrence as contained in Table 3.1 below. "Office Hours" is defined as 8am to 5pm for Mondays to Fridays (except Public Holidays). The whole of Saturday, Sunday and any Public Holiday and the hours outside the Office Hours are referred to as “After Office Hours”.

Fault Type	Response Time	
	During Office Hours	After Office Hours
Service Affecting	within one (1) hour of receipt of notification	within two (2) hours of receipt of notification
Non-Service Affecting	within two (2) hours of receipt of notification	within next Working Day of receipt of notification

Table 3.1 - Target Response Time

4 FAULT ESCALATION

4.1 Procedure

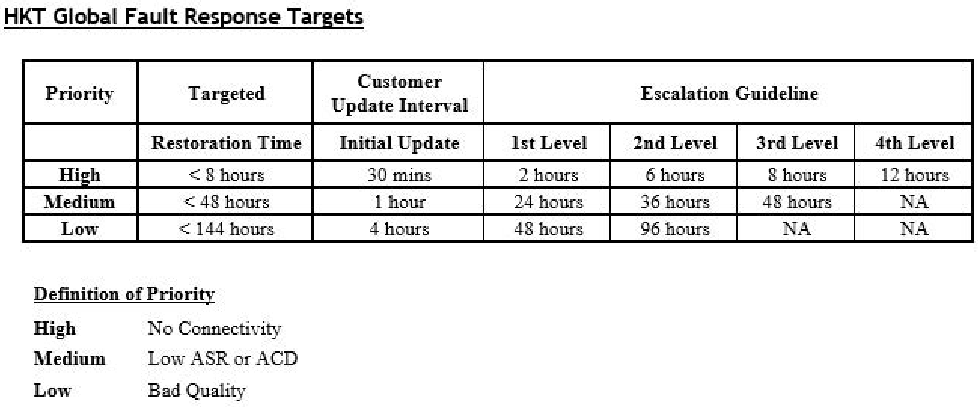
4.1.1 Where a fault persists and the Parties agree that progress of the remedy is not satisfactory, the fault may be escalated according to the fault escalation timescales and escalation reporting levels as outlined in clauses 11b and 11c herein respectively.

4.1.2 The Parties shall immediately inform the first level of escalation within the respective Party's organisation at the same time when the Party which detected the fault notifies the fault reporting point of the Party for action.

4.1.3 The Parties shall maintain the communication links at the affected site(s) and report on the progress of the restoration work.

4.2 Fault Escalation Timescales

4.2.1 The Parties shall use the following timescales as guidelines for the fault escalation process. The timescales shall be used in deciding whether the restoration of a fault is being progressed satisfactorily. If the escalation time has expired and both Parties are satisfied with the progress of the fault restoration, no immediate escalation is necessary.



HKT Global Fault Response Targets

Priority	Targeted	Customer Update Interval	Escalation Guideline			
	Restoration Time	Initial Update	1st Level	2nd Level	3rd Level	4th Level
High	< 8 hours	30 mins	2 hours	6 hours	8 hours	12 hours
Medium	< 48 hours	1 hour	24 hours	36 hours	48 hours	NA
Low	< 144 hours	4 hours	48 hours	96 hours	NA	NA

Definition of Priority

High	No Connectivity
Medium	Low ASR or ACD
Low	Bad Quality

Fault Type	Maximum Time For Escalation (Commencing after the Response Time)		
	First Level	Second Level	Third Level
Service Affecting	Immediate	two (2) hours	four (4) hours
Non-Service Affecting	Immediate	eight (8) hours	twenty-four (24) hours

Table 4.2 – Fault Escalation Timescales

4.3 Escalation Reporting Levels

4.3.1 All requests for escalation shall be notified through each Party's fault reporting point. The reporting levels are :

Operator Escalation Level	SingTel	Requesting Licensee
First	Switch Engineer	to be advised by Requesting Licensee
Second	Interconnect Operations Manager	to be advised by Requesting Licensee
Third	Operations Director	to be advised by Requesting Licensee

Table 4.3 - Escalation Reporting Levels

4.4 Persistent or Repeated Faults

4.4.1 Persistent or repeated faults or issues which cannot be resolved satisfactorily through the normal channels of the Parties shall be escalated to the Second Level to expedite the fault clearance process.

4.5 Escalation Problems

4.5.1 The Parties shall notify their respective and appropriate officers stated in Table 4.3 above for problems encountered in the implementation or execution of the fault escalation procedures.

5 MAJOR SERVICE INTERRUPTION (MSI)

5.1 General

5.1.1 Major service interruption (MSI) is defined as a fault or problem which results in the inability of the available links on an interconnect route and has a major impact on the service offered to either Party's Customers. MSI is therefore classified as service affecting. Examples of MSI are as follows:

5.1.1.1 An extensive line plant failure.

5.1.1.2 A major failure of IP Core system terminating at the Interconnect Links.

5.1.1.3 Total loss of the IP or SIP signalling of the Interconnect Links.

5.2 Procedures

5.2.1 The Party encountering an MSI shall notify the other Party through email, phone Call or other means providing real-time communication between the Parties. This should take place within thirty (30) minutes of the MSI becoming known to the Party.

5.2.2 Direct communications links shall be established between the Parties' interconnect fault reporting centres (set up as per clause 5.1.3 above). The communication links shall facilitate the effective exchange of information and progress reports. Communication liaison officers shall be appointed to maintain and man the communication links.

5.2.3 The Party responsible for clearing the MSI shall provide to the other Party regular updates of the progress through the communication links established according to clause 8.2.2 above.

5.2.4 The Party responsible for clearing the MSI fault shall inform the other Party through the communication links within thirty (30) minutes upon clearance of the MSI fault.

6 PLANNED ENGINEERING WORKS

6.1 For any planned engineering works within the Requesting Licensee's Network, which will result in momentary outage of service of the, SIP Signalling Links, or Gateway

Exchange, the Requesting Licensee shall inform SingTel by email through the contact points as given in Appendices 1 & 2.

6.2 The details of the works to be carried out shall be recorded on an "Advice of Planned Engineering Work" form (**Advice form**). The Advice form as provided in Appendix 3 shall state the date, time and duration of such works, the impact to the conveyance of Calls between the Parties' Network, any Network management procedures required, and any contingency measures to be taken by either Party or both Parties. The schedule and duration of the planned work proposed by the Requesting Licensee shall be agreed to by SingTel before the commencement of such works.

6.3 The Requesting Licensee, prior to performing the planned engineering works, shall give advance notice of at least five (5) Business Days to the other Party.

6.4 The preferred times and duration allowed for carrying out various planned engineering works shall be between 0100 through 0500 hrs, applicable on everyday, including public holidays.

6.5 The Requesting Licensee shall notify SingTel that the works have been completed by completing and emailing to SingTel the last section of the Advice form.

7 TESTING AND MONITORING

7.1 The Requesting Licensee shall be responsible for testing and monitoring the performance of its own Network. Testing of the Interconnection Link and Signalling Links shall be kept to a minimum and shall be avoided during the busy hour periods. No testing shall be carried out before SingTel has agreed to the conduct of such tests, including any routine tests.

7.2 For handling problems which can only be localised through a series of test Calls (eg difficulty in reaching certain number groups), both Parties shall agree upon the details of the testing required. Test numbers and contact points shall be exchanged to facilitate the testing.

APPENDIX 1

Notification Contact Points for SingTel:-

(a) SingTel Network Operations Centre (NOC) (after office hours)

Location :

Telephone :

Email :

Supervisor :

(b) SingTel IGS/SGS

Location :

Telephone :

Email :

Supervisor :

APPENDIX 2

Notification Contact Points for Requesting Licensee

(a) Requesting Licensee’s Network Management Centre (NMC) - 24 hours

Location :

Telephone :

Email :

Supervisor :

(b) Name of Requesting Licensee’s Network Location:

Location :

Telephone :

Email :

Supervisor :

APPENDIX 3

Advice of Planned Engineering Works

Subject:	*Title of the planned works*
Switch/ Location:	*Indicate the Switch or location of the planned work*
Type of planned works:	*Signalling Link /Interconnect Link/Exchange*
Outage Date:	*Indicate the date of the planned work*
Outage Time:	*Indicate the start time of the planned work.*
Service Interruption Duration:	*Provide an estimated duration on the service interruption*
Number of Interconnect Links/ Signalling Links affected:	*Indicate the number and system ID of the Interconnect Links or Signalling Links affected by the planned work*
Effect of planned work:	*Describe the effect of the planned works on Calls and in which direction*
Reason of planned work:	*Describe the reason for the planned works eg due to routine/urgent maintenance or software upgrade etc*
Remarks:	*To include additional comments or remarks eg Preparation work will commence at around "time" on "date"*
Issuing Officer:	*Indicate the name and designation of the officer issuing the advice of planned work.*

ANNEX C - IMDA SIP TECHNICAL SPECIFICATIONS

Telecommunications Standards Advisory Committee (TSAC)

Technical Specification

SIP standards for Voice Interconnection

IMDA TS SIP-INTC
Issue 1 Rev 1, Feb 2025

Info-communications Media Development Authority
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

Acknowledgement

The Info-communications Media Development Authority (IMDA) and the Telecommunications Standards Advisory Committee (TSAC) would like to acknowledge the following members of the TSAC Task Force (TF) for SIP standards for Voice Interconnection for their invaluable contributions to the preparation of this Technical Specification:

List of TSAC TF Members (2022-2024)

S/N	Organisation	Name
1	IMDA	Lim Wai Yean
2	IMDA	Sim Bak Chor
3	M1	Goh Bee Guat Emily
4	M1	Goh Lay Teng Christina
5	MyRepublic	Sia Chiew Shin
6	MyRepublic	Walter Klomp
7	Orange	Loris Guilbaud
8	Orange	Patrick Chu
9	Simba	Benjamin Tan
10	Singtel	Tan Wee Tiong
11	Singtel	Tay Wee Chin
12	StarHub	Aw Lay Kuan Janet
13	StarHub	Chern Kok Wai
14	StarHub	Ng Wee Peng Jason
15	SuperInternet	Wing-yan Louey
16	SuperInternet	Chee Peng Kwan
17	Verizon	Au Yeong Pak Wai
18	Verizon	Dong Jae Kum
19	Verizon	Priya Mahajan

Telecommunications Standards Advisory Committee (TSAC)

The TSAC advises IMDA on the setting of ICT standards as well as on the development and recommendation of specifications, standards, information notes, guidelines and other forms of documentation for adoption and advancement of the standardisation effort of the Singapore ICT industry (hereafter termed "IMDA Standards").

Telecommunications standards-setting in Singapore is achieved with the assistance of TSAC, where professional, trade and consumer interest in telecommunications standards is represented on the TSAC with representatives from network and service operators, equipment suppliers and manufacturers, academia and researchers, professional bodies and other government agencies.

List of TSAC Members (2024-2027)

TSAC Chairman:

Dr Chin Woon Hau Director (Standards Development and Regulatory Technology) Infocomm Media Development Authority (IMDA) **TSAC Members:**

Mr George Choo	President Association of Telecommunications Industry of Singapore (ATIS)
Mr Andy Phang	Assistant Director, Standards Development and Regulatory Technology Infocomm Media Development Authority (IMDA)
Mr Marcus Tan Cheng Lin	Head of Cybersecurity Department Institute for Infocomm Research (I2R)
Mr Denis Seek	CTO M1 Limited
Mr Ng Thian Khoon	Head, Broadcast Engineering/ Broadcast Engineering (Technology) Mediacorp Pte Ltd
Associate Professor Chau Yuen	Associate Professor, School of Electrical & Electronic Engineering Provost's Chair in Wireless Communications Nanyang Technological University (NTU)
Dr Biplab Sikdar	Head of Department, Electrical and Computer Engineering, & Area Director (Communications & Networks) National University of Singapore (NUS)
Mr Gao Peng	Head of Radio Planning Simba Telecom Pte. Ltd.
Professor Susanto Rahardja	Professor, Engineering Cluster Singapore Institute of Technology (SIT)
Mr Lim Yu Leong	Vice President, Group Strategy, Engineering & Innovation Singapore Telecommunications Ltd (Singtel)
Professor Tony Quek	Head of Information Systems and Technology Design Pillar; Cheng Tsang Man Chair Professor Singapore University of Technology and Design (SUTD)
Mr Lin Ming Yee	Vice President, Mobile Core StarHub Ltd

Contents

NOTICE

THE INFO-COMMUNICATIONS MEDIA DEVELOPMENT AUTHORITY ("IMDA") MAKES NO REPRESENTATION OR WARRANTY OF ANY KIND WITH REGARD TO THE MATERIAL PROVIDED HEREIN AND EXCLUDES ANY EXPRESS OR

IMPLIED WARRANTIES OR CONDITIONS OF NON-INFRINGEMENT, MERCHANTABILITY, SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE. SUBJECT TO THE MAXIMUM EXTENT PERMITTED UNDER LAW, IMDA SHALL NOT BE RESPONSIBLE OR LIABLE TO YOU OR ANY THIRD PARTY FOR ANY ERRORS AND/OR OMISSIONS CONTAINED HEREIN OR FOR ANY LOSSES OR DAMAGES (INCLUDING ANY LOSS OF PROFITS, BUSINESS, GOODWILL OR REPUTATION, AND/OR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES) IN CONNECTION WITH THE USE OF THIS MATERIAL.

IMDA RESERVES THE RIGHT TO CHANGE, MODIFY OR ADD TO ANY PART OF THIS DOCUMENT. NOTHING HEREIN IS INTENDED TO CREATE OR IMPOSE ANY BINDING LEGAL OBLIGATIONS OR LIABILITY WHATSOEVER ON IMDA, WHETHER EXPRESSED OR IMPLIED, AND WHETHER CONTRACTUAL OR OTHERWISE. WITHOUT PREJUDICE TO THE FOREGOING, NOTHING IN THIS DOCUMENT SHALL BIND IMDA TO ADOPT ANY PARTICULAR COURSE OF ACTION. CONSEQUENTLY, NOTHING HEREIN SHALL BE CONSTRUED AS GRANTING ANY EXPECTATION, WHETHER PROCEDURAL OR SUBSTANTIVE IN NATURE, THAT IMDA WILL TAKE OR NOT TAKE ANY PARTICULAR COURSE OF ACTION IN THE FUTURE, ARISING FROM OR DUE TO ANYTHING IN THIS DOCUMENT OR IN THE EXERCISE OF ITS DISCRETION AS A PUBLIC AUTHORITY.

IMDA DRAWS ATTENTION TO THE POSSIBILITY THAT ANY PRACTICE OR IMPLEMENTATION OF THIS STANDARD/SPECIFICATION MAY INVOLVE THE USE OF INTELLECTUAL PROPERTY RIGHTS AND TAKES NO POSITION CONCERNING THE EXISTENCE, VALIDITY AND/OR APPLICABILITY OF ANY SUCH INTELLECTUAL PROPERTY RIGHTS, WHETHER ASSERTED BY TSAC MEMBERS OR ANY THIRD PARTY.

AS OF THE DATE OF ISSUANCE OF THIS STANDARD/SPECIFICATION, IMDA HAS NOT RECEIVED WRITTEN NOTICE OF ANY PATENT RIGHTS WHICH MAY BE RELEVANT IN RELATION TO THE IMPLEMENTATION OF THIS STANDARD/SPECIFICATION.

HOWEVER, IMPLEMENTERS ARE CAUTIONED THAT THIS MAY NOT REPRESENT THE LATEST INFORMATION AND ARE

THEREFORE STRONGLY URGED TO CHECK WITH THE RELEVANT DATABASE IN ITU, ISO, IEC OR THE RELEVANT STANDARDS DEVELOPMENT ORGANISATION FOR INFORMATION OF INTELLECTUAL PROPERTY RIGHTS. IMPLEMENTERS ARE ADVISED TO OBTAIN THEIR OWN PROFESSIONAL, TECHNICAL AND/OR LEGAL ADVICE AND CONDUCT ALL NECESSARY DUE DILIGENCE, INCLUDING BUT NOT LIMITED TO MAKING SUCH INVESTIGATIONS OR SEEKING CLARIFICATIONS AS MAY BE

APPROPRIATE, IN REGARD TO ANY DECISION OR ACTION THAT THEY INTEND TO TAKE, OR PRIOR TO THE IMPLEMENTATION OF ANY STANDARD/SPECIFICATION AS MAY BE REQUIRED.

Technical Specification for SIP standards for Voice Interconnection

1. SCOPE

This Specification defines the minimum technical requirements for SIP standards for Voice Interconnection at the Point of Interconnection (POI). While SIP is used for the setting up, modification and tearing down of multimedia sessions consisting of audio, video and/or data applications, the protocol and its extensions described in this document are being considered in the context of voice communications.

In addition to the standards that are used to define the signalling protocol at the POI, this document also provides the basic standards that governs communication over the media plane.

2. REFERENCES

For the technical requirements captured in this Specification, reference has been made to the following standards. Where versions are not indicated, implementation of this Specification shall be based on current and valid versions of these standards published by the respective Standards Development Organisations.

1. IETF RFC 2119: “Key words for use in RFCs to Indicate Requirement Levels”
2. IETF RFC 2822: “Internet Message Format”
3. IETF RFC 3261: “SIP: Session Initiation Protocol”
4. IETF RFC 3262: “Reliability of Provisional Responses in the Session Initiation Protocol (SIP)”
5. IETF RFC 3264: “An Offer/Answer Model with the Session Description Protocol (SDP)”
6. IETF RFC 3311: “The Session Initiation Protocol (SIP) UPDATE Method”
7. IETF RFC 3323: “A Privacy Mechanism for the Session Initiation Protocol (SIP)”

8. IETF RFC 3324: "Short Term Requirements for Network Asserted identity"
9. IEFT RFC 3325: "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks"
10. IETF RFC 3326: "The Reason Header Field for the Session Initiation Protocol (SIP)"
11. IETF RFC 3550: "RTP: A Transport Protocol for Real-Time Applications"
12. IETF RFC 4028: "Session Timers in the Session Initiation Protocol (SIP)"
13. IETF RFC 4566: "SDP: Session Description Protocol"
14. IETF RFC 4733: "RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals"
15. IETF RFC 5009: "Private Header (P-Header) Extension to the Session Initiation Protocol (SIP) for Authorization of Early Media"
16. IETF RFC 5806: "Diversion Indication in SIP"
17. ITU-T T.38: "Procedures for real-time Group 3 facsimile communication over IP networks"
18. ITU-T G.711: "Pulse code modulation (PCM) of voice frequencies"
19. GSMA IR.92: "IMS Profile for Voice and SMS"
20. 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3"
21. 3GPP TS 24.628: "Common Basic Communication procedures using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification"

3. ABBREVIATIONS

IETF	Internet Engineering Task Force
POI	Point of Interconnection
PoP	Point of Presence
PRACK	Provisional Response Acknowledgement
RFC	Request for Comments
SDP	Session Description Protocol
SIP	Session Initiated Protocol
UA	User Agent which is either a UAC or UAS
UAC	User Agent Client which sends request and receives responses
UAS	User Agent Server which receives requests and sends responses

4. TECHNICAL REQUIREMENTS

4.1 The POI is the physical interface that is used to connect between the gateways of two networks. In order for the smooth connection of the two networks, the operators of the networks have to agree on the signalling protocol(s) to be used at the POI.

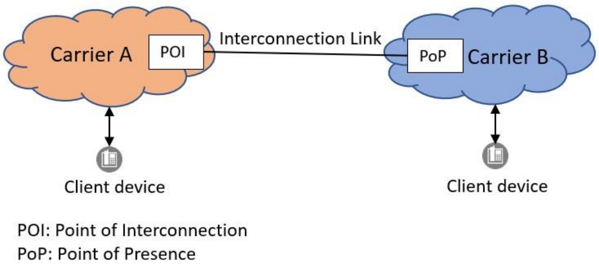


Figure 1. Interconnection between two networks

4.2 The signalling protocol to be used at the POI is the Session Initiation Protocol (SIP) defined by the Internet Engineering Task Force (IETF), a standards development organisation. The IETF produced a set of documents known as the “Request for Comments” (RFC) which have been used to define many internet protocols. SIP is an application layer signalling protocol for establishing, modifying and termination multimedia sessions between participants over an IP network. It is independent of the underlying transport layer protocol and can be used with User Datagram Protocol (UDP), the Transmission Control Protocol (TCP) and the Stream Control Transmission Protocol (SCTP).

4.3 Operators wishing to interconnect their networks using SIP need to agree on the set of RFCs used, so that the networks can communicate seamlessly with one another. The absolute requirements and prohibitions in the agreed RFCs listed in this document form the baseline specifications that the interconnecting networks must comply to. Additional specifications that need to be implemented are be negotiated and agreed to by the operators of the interconnecting networks. Similarly, RFC versions that are not stated in this document could be separately used by operators of the interconnecting networks, subject to agreements by the operators.

4.4 The following is the basic set of standards used for the signalling plane at the POI:

S/N	Standard	Description	Mandatory
1	RFC 3261	Session Initiation Protocol	Mandatory
2	RFC 4566	SDP: Session Description Protocol	Mandatory
3	RFC 3262	Reliability of Provisional Responses in Session Initiation Protocol	Mandatory
4	RFC 3264	An Offer/Answer Model with the Session Description Protocol	Mandatory
5	RFC 3311	The Session Initiation Protocol UPDATE Method	Mandatory
6	RFC 3323	A Privacy Mechanism for the Session Initiation Protocol	Privacy header to be supported in reception

7	RFC 3325	Private Extensions to the Session Initiation Protocol for Network Asserted Identity within Trusted Networks	P-Asserted-Identity header to be supported in reception
8	RFC 3326	The Reason Header Field for the Session Initiation Protocol	Mandatory
9	RFC 5806	Diversion Indication in SIP	Diversion header to be supported in reception
10	RFC 4028	Session Timers in the Session Initiation Protocol	Mandatory
11	RFC 5009	Private Header (P-Header) Extension to the Session Initiation Protocol for Authorization of Early Media	P-Early-Media header to be supported in reception; for Mobile Network Operators only
Note: "Supported" means that if the header is present, then it must be handled according to the stated standard			

Table 1. List of IETF RFCs for compliance at the POI

Descriptions of the RFCs are provided in section 5.

4.5 Besides the signalling plane standards, there are media plane standards used to ensure the seamless transmission of media streams between networks at the POI. The primary standards for the media plane are as follows:

S/N	Standard	Description
1	ITU-T T.38	Procedures for real-time Group 3 facsimile communication over IP networks
2	ITU-T G.711	Pulse code modulation (PCM) of voice frequencies
3	RFC 4733	RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals
4	RFC 3550	RTP: A Transport Protocol for Real-Time Applications
Note: Carriers that are not providing facsimile services are not required to comply to ITU-T T.38. This does not include carriers which are providing the POI in their networks.		

Table 2. List of standards to be used for the media plane

4.6 Cybersecurity requirements

The cybersecurity requirements for operators interconnecting their IP-based networks for voice services can be found in the document IMDA SEC-INTC. This document may be downloaded from the IMDA website at http://www.imda.gov.sg and shall not be distributed without written permission from IMDA. Operators must comply to these requirements.

5. DESCRIPTION OF RFCS FOR THE SIGNALLING PLANE

This section provides a brief description of the functionalities given in the list of RFCs in Table 1. The keywords used in the RFCs, "MUST" and "SHALL" are to be interpreted as absolute requirements of the specifications while "MUST" and "MUST NOT" are absolute prohibition of the specification, in accordance to RFC 2119.

It is to be noted that not all the absolute requirements or absolute prohibitions are mentioned in this section. Please refer to the official standards documents for the full details.

5.1 RFC 3261 – SIP: Session Initiation Protocol

A SIP message is either a request from a client to a server, or a response from a server to a client. Both Request and Response messages use the basic format of RFC 2822. Both types of messages consist of a start-line, one or more header fields, an empty line indicating the end of the header fields, and an optional message-body. The request message is also known as a method.

```
Generic-message          =         start-line
                                     *message-header
                                   CRLF
                         [message-body]
Start-line               =          Request-Line / Status-Line
```

The start-line, each message-header line, and the empty line must be terminated by a carriage-return line-feed sequence (CRLF). Note that the empty line must be present even if the message-body is not.

5.1.1 Request

SIP requests are distinguished by having a Request-Line for a start-line. A Request-Line contains a method name, a Request-URI, and the protocol version separated by a single space (SP) character. SIP responses are distinguished from requests by having a Status-Line as their start-line. There are fourteen SIP Request methods and the six below are the most basic:

SIP Method	Purpose	Remarks
INVITE	Invites a call by inviting user to participate in session. A media session is established when the INVITE, 200 OK and ACK messages have been exchanged between the UAC and UAS	Mandatory to support
ACK	Confirms that the client has received a final response to an INVITE request	Mandatory to support
BYE	Indicates termination of the call; A BYE is sent only by UAs participating in the session, never by proxies or other third parties	Mandatory to support
CANCEL	Cancels a pending request	Mandatory to support
OPTIONS	Used to query the capabilities of a server	Mandatory to support
REGISTER	Registers the user agent	Not needed for messages between operators

Table 3. Basic Request methods to support

A SIP request must, at a minimum, contain the following header fields.

SIP header	Description
To	The To header specifies the recipient of the call. The To header field may contain a SIP or SIPS URI, but it may also make use of other URI such as the tel URL (RFC 2806) when appropriate. All SIP implementations must support the SIP URI scheme, while implementation that supports TLS must support the SIPS URI scheme.
From	The From header specifies who the call is coming from.
CSeq	The CSeq header specifies the number of requests of each type that have been sent. It consists of a sequence number and a method. The method must match that of the request.
Call-ID	The Call-ID SIP header creates a globally unique identifier for the call. CallIDs are case-sensitive.
Max-Forwards	The Max-Forwards header sets the limit of the number of hops a request can transit on the way to its destination.
Via	The Via header identifies the call’s path. When UAC creates a request, it must insert a Via into that request together with the protocol name and protocol version, which are SIP and 2.0, respectively. The Via header field values must contain a branch parameter, which is a unique token and must start with the value z9hG4bK. It is used to identify the transaction created by that request and helps to ensure route back to originator.

Table 4. Minimum headers to be supported in a SIP request

5.1.2 Response and Status/Response codes

As opposed to requests, a SIP response has Status-Line as their start-line. A Status-Line consists of the protocol version followed by a numeric Status-Code and its associated textual phrase.

The response codes that are used in SIP are given in the below table, where “1xx” refers to any response with a status code between 100 and 199, “2xx” refers to a status code between 200 and 299, and so on.

Response codes	Description
1xx	Provisional
2xx	Success
3xx	Redirection
4xx	Client Error
5xx	Server Error
6xx	Global failures

Table 5. List of response codes

5.2 RFC 4566 – SDP: Session Description Protocol

This RFC defines the Session Description Protocol which is used to describe multimedia sessions for the purposes of session announcement, session invitation and other forms of multimedia session initiation.

An SDP session description is denoted by the media type “application/sdp”. SDP session descriptions are text-based and consists of a number of lines of text of the form:

Type=value

The type field is always one lower case character and the format of the value field depends on which type it applies. Whitespace must not be used on either side of the “=” sign.

An SDP session description starts with the session-level section followed by zero or more media-level sections. The session-level section contains information for the whole session, while media-level section contains information that applies to specific media stream. Session-level values are the default for all media unless overridden by an equivalent media-level value.

The descriptions contain REQUIRED and OPTIONAL lines, and all must appear in the order as given below:

Field	**Name**	**Mandatory/Optional**
Session description		
v	Protocol version	Mandatory
o	Originator and session identifier	Mandatory
s	Session name	Mandatory
i	Session information	Optional
u	URI of description	Optional
e	Email address	Optional
p	Phone number	Optional
c	Connection information	Mandatory (Not required if included in all media)
b	Bandwidth information	Optional
Time description		
t	Time session start and stop	Mandatory
r	Repeat times	Optional
Session description		
z	Time zone corrections	Optional
k	Encryption key	Optional
a	Attribute lines	Optional
Media description, if present		
m	Media information	Optional
i	Media title	Optional
c	Connection information	Optional
b	Bandwidth information	Optional

k	Encryption key	Optional
a	Media attributes	Optional

Table 6. List of SDP session descriptions

5.3 RFC 3262 – Reliability of Provisional Responses in the Session Initiation Protocol (SIP)

This document specifies an extension to the Session Initiation Protocol (SIP) providing reliable provisional response messages. SIP defines two types of responses, provisional and final. A final response is defined as a response that terminates a SIP transaction and is sent reliably. All 2xx, 3xx, 4xx, 5xx and 6xx responses are final.

A provisional response is one that does not terminate a SIP transaction and is not sent reliably. However, there are cases where reliable provision responses need to be sent. That capability is provided in this specification.

The UAS must send any non-100 provisional response reliably if the initial request contained a Require header with the option tag 100rel. UAS could also reject the initial request with a 420 (bad Extension) by including an Unsupported header field containing the option tag 100rel.

When using reliable provisional responses, responses are retransmitted by the UAS in response to an INVITE until a Provisional Response Acknowledgement (PRACK) is received from the UAC.

5.4 RFC 3264 – An Offer/Answer Model with the Session Description Protocol

This RFC defines a mechanism by which two entities can make use of the Session Description Protocol (SDP) to arrive at a common view of a multimedia session between them. While SDP describes multimedia sessions, it lacks the semantics and operational details on how it is actually done. RFC 3264 defines a simple offer/answer model based on SDP. In this model, one participant in the session, known as the offerer, generates an SDP message that lists the set of media streams and codecs, along with the IP addresses and ports, which the offerer would like to use to receive the media. Another participant in the session, known as the answerer, will generate an answer which has a matching media stream for each stream in the offer, indicating whether the stream is accepted or not, along with the codecs that will be used and the IP addresses and ports that the answerer wants to use to receive media.

The offer/answer assumes the existence of a higher-layer protocol (such as SIP) which is capable of exchanging SDP for the purposes of session establishment between agents. Protocol operation begins when one agent sends an initial offer to another agent. The agent receiving the offer may generate an answer, or it may reject the offer. Either agent may generate a new offer that updates the session but it must not generate a new offer if it has received an offer which it has not yet answered or rejected. It must also not generate a new offer if it has generated a prior offer for which it has not yet received an answer or a rejection.

5.4.1 Generating an Offer

The offer (and answer) must be a valid SDP message, and the SDP message used in the offer/answer model must contain exactly one session description.

The offer will contain zero or more streams (each media stream is described by an “m=” line and its associated attributes). Zero media streams implies that the offerer wishes to communicate, but that the streams for the session will be added at a later time through a modified offer.

If the offerer wishes to only send media on a stream to its peer, it must mark the stream as send-only with the “a=sendonly” attribute. If the offerer wishes to only receive media from its peers, it must mark the stream with the “a=recvonly” attribute. If the offerer wishes to communicate, but wishes to neither send nor receive media at this time, it must mark the stream with the “a=inactive” attribute.

If the offer has a port number of zero, it indicates that the stream is offered but must not be used.

5.4.2 Generating an Answer

For each “m=” line in the offer, there must be a corresponding “m=” line in the answer. The answer must contain exactly the same number of “m=” lines as the offer.

If the answer contains a zero port then it indicates that the stream is rejected, or if the stream is accepted then it contains a nonzero port number.

5.4.3 Modifying a Session

The “o=” line of the new SDP must be identical to that in the previous SDP, except that the version in the origin field must increment by one from the previous SDP. If the version in the origin line does not increment, the SDP must be identical to the SDP with that version number.

If an SDP is offered, which is different from the previous SDP, the new SDP must have a matching media stream for each media stream in the previous SDP. Deleted media streams from a previous SDP must not be removed in a new SDP; however, attributes for these streams need not be present.

Additional media streams can be added below the existing ones. Existing streams can also be terminated by setting the port number to zero.

5.5 RFC 3311 – The Session Initiation Protocol UPDATE Method

This specification defines the new UPDATE method for the SIP. UPDATE allows a client to update parameters of a session (such as the set of media streams and their codecs) but does not impact the state of a dialog. In this respect, it is different from RE-INVITE, which changes the state of a dialog. Also, as opposed to RE-INVITE, an UPDATE needs to be answered immediately. Another aspect which UPDATE is different from RE-INVITE is that it can be sent prior to session establishment. RE-INVITE is sent after a session has been established.

5.6 RFC 3323 – A Privacy Mechanism for the Session Initiation Protocol

This RFC provides privacy requirements and mechanisms for the Session Initiation Protocol. Privacy is defined in this RFC as the withholding of the identity of a person (and related personal information) from one or more parties in an exchange of communications.

RFC 3323 describes three degrees of privacy – one level of user-provided privacy and two levels of network-provided privacy (header privacy and session privacy).

This document defines a new SIP header, Privacy, that can be used to specify privacy handling for requests and responses. The syntax of the header field is as follows:

```
Privacy-hdr        =        “Privacy” HCOLON priv-value *(“;” priv-value)
priv-value         =           “header” / “session” / “user” / “none” / “critical” / token
```

When a Privacy header is constructed, it must consist of either the value “none”, or one or more of the values ‘user’, ‘header’, and ‘session’ (each of which must appear at most once which may in turn be followed by the ‘critical’ indicator.

When Privacy: none, it means that privacy services must not perform any privacy function, and intermediaries must not remove or alter the Privacy header.

5.7 RFC 3325 – Private Extensions to the Session Initiation Protocol for Asserted Identity within

5.8 Trusted Networks

This RFC describes private extensions to SIP that enable a network of trusted SIP servers to assert the identity of end users or end systems, and to convey indications of end-user requested privacy. The use of these extensions is only applicable inside a 'Trust Domain' as defined in RFC 3324.

The behaviour of a proxy could be summarised as follows:

Proxy behaviour when it receives a message

1. If proxy receives a message from a node that it trusts, it will use the information in the PAsserted-Identity header field as though it had authenticated the user itself. If there is no PAsserted-Identity header field, it may add at most one SIP/SIPS URI or at most one tel URI.
2. If proxy receives a message from a node that it does not trust, it must authenticate the originator of the message, and use the identity which results from this authentication to insert a P-Asserted-Identity header field into the message. If there is already a P-Asserted-Identity that contains a SIP/SIPS or tel URI then it must replace or remove the header field.

Proxy behaviour when it forwards a message

1. If proxy forwards a message to a node that it trusts, it does not remove any P-Asserted-Identity header fields that it generated, or that it received from a trusted source.
2. If proxy forwards a message to a node that it does not trust, it must examine the Privacy header (if present). If Privacy header field value is set to “id” then all the P-Asserted-Identity header fields must be removed. If Privacy header field value is set to “none” then P-Asserted-Identity header fields must not be removed. If there is no Privacy header field, then the proxy may include the P-Asserted-Identity header field or it may remove it.

On dealing with multiple identities

If proxy receives a P-Preferred-Identity header field from a node that it does not trust, it may use this information as a hint suggesting which of multiple valid identities for the authenticated user should be inserted. If such a hint is not possible, then the proxy can add a P-Asserted-Identity header of its own construction, or it can reject the request. The proxy must remove the user-provided P-PreferredIdentity header from any message it forwards.

The syntax of the P-Asserted-Identity header field is as follows:

```
PAssertedID              =          “P-Asserted-Identity” HCOLON PAssertedID-value
                                    *(COMMA PAssertedID-value)
PAssertedID-value        =          name-addr / addr-spec
```

The syntax of the P-Preferred-Identity header field is as follows:

```
PPreferredID          =     “P-Preferred-Identity” HCOLON PPreferredID-value
                            *(COMMA PPreferredID-value)
PPreferredID-value    =     name-addr / addr-spec
```

The syntax of the Privacy header field is as follows:

priv-value = “id”

5.9 RFC 3326 – The Reason Header Field for the Session Initiation Protocol

This RFC defines a header field, Reason, that provides the reason to why a particular SIP request is being issued.

One example of such a use could be when a SIP CANCEL request is being issued. Such a request can be issued when the call has been completed on another branch or it was abandoned before answer. Providing a reason for the CANCEL request will provide context to the recipient about the nature of the cancellation and this could be used for diagnostic and logging purposes.

The syntax of the header field is as follows:

```
Reason                =     “Reason” HCOLON reason-value *(COMMA reason-value)
reason-value          =     protocol *(SEMI reason-params)
protocol              =     “SIP” / “Q.850” / token
reason-params         =       protocol-cause / reason-text / reason-extension
protocol-cause        =     “cause” EQUAL cause
cause                 =     1*DIGIT
reason-text           =     “text” EQUAL quoted-string reason-
extension       =     generic-param
```

5.10 RFC 5806 – Diversion Indication in SIP

This RFC proposes an extension to SIP that provides the ability for the called SIP user agent to identify from whom the call was diverted and why the call was diverted. A header field, Diversion, is used to convey the diversion information.

The Diversion header should be added when a call is redirected or forwarded. It should not be added for normal call routing changes to the Request-URI. Prior to a diversion, the Diversion header must contain the Request-URI of the request. The Diversion header should also contain a reason that the diversion occurred.

Existing Diversion headers received in an incoming request must not be removed or changed in forwarded requests.

Existing Diversion headers received in an incoming response must not be removed or changed in the forwarded response.

The syntax of the Diversion header field is as follows:

```
Diversion             =     “Diversion” “:” 1# (name-addr *( “;”
diversion_params)) diversion-params        =      diversion-reason | diversion-
counter | diversion-limit | diversion-privacy |
                                  diversion-screen | diversion-extension
```

diversion-reason = "reason" "="
("unknown" | "user-busy" | "no-answer" |
"unavailable" | "unconditional" |
"time-of-day" | "do-not-disturb" |
"deflection" | "follow-me" |
"out-of-service" | "away" |
Token | quoted-string)
diversion-counter = "counter" "=" 1*2DIGIT
diversion-limit = "limit" "=" 1*2DIGIT diversion-privacy
= "privacy" "=" ("full" | "name" |
"uri" | "off" | token | quoted-string)
diversion-screen = "screen" "=" ("yes" | "no" | token | quoted-string) diversion-extension =
token ["=" (token | quoted-string)]

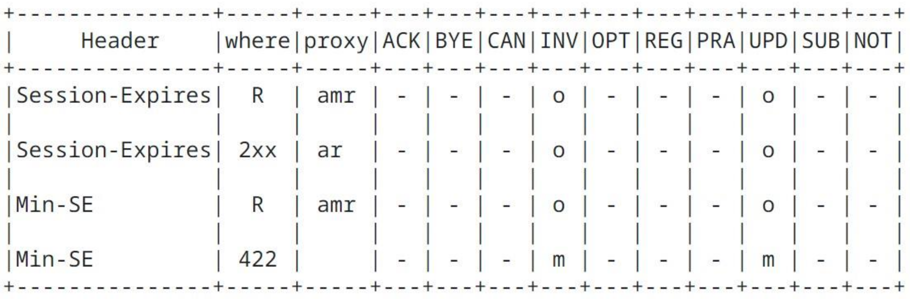
5.11 RFC 4028 – Session Timers in the Session Initiation Protocol

The Session-Expires header field conveys the session interval for a SIP session. It is placed only in INVITE or UPDATE requests, as well as in any 2xx response to an INVITE or UPDATE. Like the SIP Expires header field, it contains a delta-time. The absolute minimum for the Session-Expires header field is 90 seconds.

The syntax of the Session-Expires header field is as follows:

Session-Expires = ("Session-Expires" / "x") HCOLON delta-seconds *(SEMI se-params)
se-params = refresher-param / generic-param refresher-
param= "refresher" EQUAL ("uas" / "uac")

Note that a compact form, the letter x, has been reserved for Session-Expires.



Header	where	proxy	ACK	BYE	CAN	INV	OPT	REG	PRA	UPD	SUB	NOT
Session-Expires	R	amr	-	-	-	o	-	-	-	o	-	-
Session-Expires	2xx	ar	-	-	-	o	-	-	-	o	-	-
Min-SE	R	amr	-	-	-	o	-	-	-	o	-	-
Min-SE	422		-	-	-	m	-	-	-	m	-	-

Table 7: Session-Expires and Min-SE Header Fields

The Min-SE header field indicates the minimum value for the session interval, in units of delta-seconds.
When used in an INVITE or UPDATE request, it indicates the smallest value of the session interval that can be used for that session. When present in a request or response, its value must not be less than 90 seconds.

5.12 RFC 5009 – Private Header (P-Header) Extension to the Session Initiation Protocol for

5.13 Authorization of Early Media

It is a GSMA requirement that mobile UE need to support this. In the GSMA document, IR. 92, it is stated that:

> The UE must behave as specified in section 4.7.2.1 of 3GPP Release 13 TS 24.628.
>
> In addition, the UE must support the P-Early-Media header field with the “supported” parameter to initial INVITE requests it originates as specified in section 5.1.3.1 of 3GPP TS 24.229.
>
> The UE must also maintain an early media authorization state per dialog as described in RFC 5009.
>
> As stated in 3GPP TS 24.628, the UE must render locally generated communication progress information, if:
>
> - an early dialog exists where a SIP 180 response to the SIP INVITE was received;
> - no early dialog exists where the last received P-Early-Media header field as described in IETF RFC 5009 contained “sendrecv” or “sendonly”; and
> - in-band information is not received from the network.

6. EXAMPLE SHOWING RFC EXTRACTS THAT ARE BEING USED IN A TYPICAL SIP INVITE MESSAGE

Below is a typical SIP INVITE message showing the different headers and message body with their RFC references.

Sample INVITE message

```
Session Initiation Protocol (INVITE)  //IETF RFC 3261
   Request-Line: INVITE sip:69741234@domain.org;user=phone SIP/2.0
   Message Header //IETF RFC 3261
      Content-Length:430
      From:<sip:90920000@domain.org;user=phone>;tag=i484WbAA93745Ug5
To:<sip:69741234@domain.org;user=phone>
      Via:SIP/2.0/UDP
172.27.X.X:5080;branch=z9hG4bK7YDc0D979b3C8Z26;yop=00.00.CCEA4CC2.0000.7003
      Call-ID:0369F14BDD2BC156877D4397@0370ffffffff
      CSeq:1 INVITE
      Max-Forwards: 64
      P-Asserted-Identity:sip:90920000@domain.org;user=phone;cpc=ordinary //IETF RFC 3325
      Session-Expires:1800;refresher=uac    //IETF RFC 4028
      Contact:<sip:172.27.X.X:5080;yop=00.00.CCEA4CC2.0000.7003>
Require:precondition
      Supported:100rel    //IETF RFC 3262
      Allow:ACK,BYE,CANCEL,INFO,INVITE,NOTIFY,OPTIONS,PRACK,REFER,UPDATE       Content-
Type:application/sdp  //IETF RFC 4566

     Message Body
       Session Description Protocol    //IETF RFC 4566
          Media Description, name and address (m): audio 43078 RTP/AVP 96 97 3 8 98 //IETF RFC
3264
          Media Attribute (a): rtpmap:96 AMR/8000
          Media Attribute (a): rtpmap:97 GSM-EFR/8000
          Media Attribute (a): rtpmap:8 PCMA/8000
```

Media Attribute (a): rtpmap:98 telephone-event/8000 //**IETF RFC 4733**

Example provided by M1

ANNEX D - IMDA SECURITY REQUIREMENTS FOR IP INTERCONNECT

Security Requirements for IP Interconnection

IMDA SEC-INTC ISSUE 1 REV 1, FEB 2025

Info-communications Media Development Authority of Singapore
Infocomm Resource & Technology
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

1 SCOPE

Interconnection refers to the linking of communications networks to ensure that users of one communications network can access the communications networks and services of other telecommunications operators.

This IMDA document defines the security requirements to secure IP-based Interconnections for voice services between network operators, thus minimising the associated cybersecurity risks from the internet.

2 ABBREVIATIONS

CII	Critical Information Infrastructure
DDoS	Distributed Denial of Service
IPSEC	Internet Protocol Security
SBC	Session Border Controller
SIP	Session Initiation Protocol
SIRT	Security Incident Response Team

3 SECURITY REQUIREMENTS

3.1 The operator shall implement the following set of baseline network security requirements on the SBC infrastructure at any points of interconnection with another domestic network operator:

(a) Monitoring and analysis of SIP messages to detect malicious traffic (i.e., any SIP message used with the intent of causing harm, including messages used to perform unauthorised interceptions, service disruptions, spoofing, etc.);

(b) Filtering of malicious traffic on the SBC;

(c) Hardening of the SBC in accordance with industry standards or guidelines; and

(d) Performing of network security assessments and penetration tests at least once every 2 years on the portion of the network that is (i) external from the SBC; and (ii) facing external entities or connections at the points of interconnection.

3.2 NOT USED

3.3 NOT USED

3.4 NOT USED