



N-Squared Software N2SIP  
SIP-SDP-RTP Protocol Conformance  
Statement

Version 2024-08.1

# 1 Document Information

## 1.1 Scope and Purpose

This document describes the implementation of the SIP, SDP, and RTP protocols for real-time flows for voice interaction control using the N-Squared family of SIP enabled products.

This includes the N-Squared Interactive Voice Response (N2IVR) product, as well as SIP-protocol deployments of the N-Squared Inter-Working Function (N2IWF), N-Squared Automated Call Distribution (N2ACD), and N-Squared Simple Number Services (N2SNS) products.

All of these products are built on a shared SIP framework named “N2SIP”. This document describes the overall features and behavior of that N-Squared SIP framework, noting that not all features will be applicable to all products.

This document should be read in conjunction with the respective Technical Guides [R-1], [R-2], [R-3], [R-4] as applicable. This document assumes a working knowledge of the relevant SIP, SDP, RTP and other telephony concepts.

## 1.2 Definitions, Acronyms, and Abbreviations

Term	Meaning
AMR[-NB]	Adaptive Multi-Rate Narrow Band
AMR-WB	Adaptive Mulit-Rate Wide Band
AVP	Audio Video Profile
B2BUA	Back-to-Back User Agent
DTMF	Dual Tone Multi-Frequency
ETSI	European Telecommunications Standards Institute
IETF	Internet Engineering Task Force
INAP	Intelligent Networking Application Part
IP	Intelligent Peripheral
MIME	Multipurpose Internet Mail Extensions
N2	N-Squared
N2ACD	N-Squared Advanced Call Distribution (supports SIP routing of toll-free call flows)
N2IVR	N-Squared Interactive Voice Response platform (SIP-trunked IVR with many control options)
N2IWF	N-Squared Inter-Working Function (supports SIP real-time call charging to an OCS)
N2SIP	N-Squared SIP common framework underlying all N-Squared SIP-capable products
N2SNS	N-Squared Simple Number Services (supports SIP-protocol number handling)
PCMA	Pulse Code Modulation a-law
PCMU	Pulse Code Modulation $\mu$ -law
PGP	Pretty Good Privacy
RFC	Request For Comments
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
SCP	Service Control Point
SCTP	Stream Control Transmission Protocol

Term	Meaning
SDP	Session Description Protocol
SIP	Session Initiation Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
SRF	Specialized Resource Function
SRTP	Secure RTP
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UAC	User Agent Client (SIP transaction role sending Request)
UAS	User Agent Server (SIP transaction role receiving Request)
UDP	User Datagram Protocol
URL	Uniform Resource Locator

### 1.3 References

The following documents are referenced within this document:

Ref.	Document
[R-1]	N2SIP Technical Guide (including N2IVR Technical Guide) <a href="https://www.nsquared.co.nz/files/n2sip/technical_guide/">https://www.nsquared.co.nz/files/n2sip/technical_guide/</a>
[R-2]	N2ACD Technical Guide <a href="https://www.nsquared.co.nz/files/n2acd/technical_guide/">https://www.nsquared.co.nz/files/n2acd/technical_guide/</a>
[R-3]	N2IWF Technical Guide <a href="https://www.nsquared.co.nz/files/n2iwf/technical_guide/">https://www.nsquared.co.nz/files/n2iwf/technical_guide/</a>
[R-4]	N2SNS Technical Guide <a href="https://www.nsquared.co.nz/files/n2sns/technical_guide/">https://www.nsquared.co.nz/files/n2sns/technical_guide/</a>
[R-10]	IETF RFC 3261 SIP: Session Initiation Protocol
[R-11]	IETF RFC 8866 SDP: Session Description Protocol
[R-12]	IETF RFC 3550 RTP: A Transport Protocol for Real-Time Applications
[R-13]	IETF RFC 3581 An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
[R-14]	IETF RFC 6086 The SIP INFO Method
[R-15]	IETF RFC 3262 Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
[R-16]	IETF RFC 4733 RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals
[R-17]	IETF RFC 3263 Session Initiation Protocol (SIP): Locating SIP Servers
[R-18]	IETF RFC 3326 The Reason Header Field for the Session Initiation Protocol (SIP)

Ref.	Document
[R-19]	draft-kaplan-dispatch-info-dtmf-package-00 A Session Initiation Protocol (SIP) INFO Package for Dual-Tone Multi-Frequency (DTMF) Events
[R-20]	IETF RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
[R-21]	IETF RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
[R-22]	IETF RFC 2616 Hypertext Transfer Protocol -- HTTP/1.1
[R-23]	IETF RFC 4867 RTP Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs
[R-24]	IETF RFC 6337 Session Initiation Protocol (SIP) Usage of the Offer/Answer Model
[R-25]	IETF RFC 7315 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3GPP
[R-26]	IETF RFC 3959 The Early Session Disposition Type for the Session Initiation Protocol (SIP)
[R-27]	IETF RFC 3960 Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)

#### 1.4 Ownership and Usage

This document, including the information contained herein, is proprietary to N-Squared Software (NZ) Limited but released for informational purposes only.

This document shall not be used or reproduced for any other purpose without the written approval of N-Squared Software (NZ) Limited.

**N-Squared Software (NZ) Limited**  
 PO Box 5035  
 Terrace End  
 Palmerston North 4410  
 New Zealand

## 2 Contents

1	Document Information .....	2
1.1	Scope and Purpose.....	2
1.2	Definitions, Acronyms, and Abbreviations.....	2
1.3	References .....	3
1.4	Ownership and Usage .....	4
2	Contents.....	5
3	SIP Compliance.....	11
3.1	SIP Overview .....	11
3.2	SIP Request Methods.....	11
3.3	Common SIP UAS Notes.....	11
3.3.1	Transport Layer .....	11
3.3.2	SIP Message Codec.....	12
3.3.3	Inbound SIP Requests .....	12
3.3.4	Malformed SIP Request Handling .....	13
3.3.5	Compact Form (Short) Headers .....	13
3.3.6	Outbound SIP Responses .....	14
3.4	Common SIP UAC Notes.....	14
3.4.1	Transport Layer .....	15
3.4.2	Outbound SIP Requests.....	16
3.4.3	Compact Form (Short) Headers .....	16
3.4.4	Inbound SIP Responses .....	17
3.5	Other Common SIP Notes .....	17
3.5.1	Multicast .....	17
3.5.2	SIP-I .....	17
3.5.3	SIP-T .....	17
3.5.4	Digest Authentication .....	18
3.6	REGISTER (Server/Inbound) .....	19
3.6.1	Message Flow.....	19
3.6.2	REGISTER Inbound Request .....	19
3.6.3	REGISTER Server Transaction.....	20
3.6.4	REGISTER Response (Declined) .....	20
3.6.5	REGISTER Response (Accepted) .....	20
3.7	REGISTER (Client/Outbound) .....	21
3.7.1	Message Flow.....	21

3.7.2	REGISTER Outbound Request .....	21
3.7.3	REGISTER Client Transaction .....	21
3.7.4	REGISTER Response.....	22
3.8	OPTIONS (Server/Inbound) .....	22
3.8.1	Message Flow.....	22
3.8.2	OPTIONS Inbound Request .....	22
3.8.3	OPTIONS Server Transaction.....	22
3.8.4	OPTIONS Response (Declined) .....	22
3.8.5	OPTIONS Response (Accepted) .....	23
3.9	INVITE & ACK & PRACK (Server/Inbound, A-Leg Only) .....	24
3.9.1	Message Flow.....	24
3.9.2	INVITE Inbound Request .....	25
3.9.3	INVITE Server Transaction.....	26
3.9.4	INVITE Response (Declined) .....	26
3.9.5	INVITE Response (Provisional, Trying) .....	27
3.9.6	INVITE Response (Provisional) .....	28
3.9.7	INVITE Response (Success).....	28
3.9.8	ACK Request (Inbound, A-Leg, for Declined 300-699 Status Code) .....	29
3.9.9	ACK Request (Inbound, A-Leg, for Success 200-299 Status Code).....	30
3.9.10	PRACK Request (Inbound, A-Leg).....	31
3.9.11	PRACK Response (Declined).....	31
3.9.12	PRACK Response (Accepted) .....	31
3.10	INVITE & ACK & PRACK (Client/Outbound, A-Leg).....	32
3.10.1	Message Flow.....	32
3.10.2	INVITE Outbound Request .....	33
3.10.3	INVITE Client Transaction.....	33
3.10.4	INVITE Response (Declined).....	34
3.10.5	INVITE Response (Provisional, Trying) .....	34
3.10.6	INVITE Response (Provisional) .....	34
3.10.7	INVITE Response (Success).....	35
3.10.8	ACK Request (Outbound, A-Leg, for Declined 300-699 Status Code) .....	36
3.10.9	ACK Request (Outbound, A-Leg, for Success 200 Status Code) .....	36
3.10.10	PRACK Request (Outbound, A-Leg).....	37
3.10.11	PRACK Response (Declined).....	37
3.10.12	PRACK Response (Accepted) .....	37
3.11	INVITE & ACK & PRACK (Client/Outbound, B-Leg).....	38

3.11.1	Message Flow.....	38
3.11.2	INVITE Outbound Request .....	39
3.11.3	INVITE Client Transaction.....	40
3.11.4	INVITE Response (Declined).....	40
3.11.5	INVITE Response (Provisional, Trying) .....	40
3.11.6	INVITE Response (Provisional) .....	40
3.11.7	INVITE Response (Success).....	42
3.11.8	ACK Request (Outbound, B-Leg, for Declined 300-699 Status Code) .....	43
3.11.9	ACK Request (Outbound, B-Leg, for Success 200-299 Status Code).....	43
3.11.10	PRACK Request (Outbound, B-Leg).....	44
3.11.11	PRACK Response (Declined).....	45
3.11.12	PRACK Response (Accepted).....	45
3.12	CANCEL (Server/Inbound).....	46
3.12.1	Message Flow.....	46
3.12.2	CANCEL Inbound Request .....	46
3.12.3	CANCEL Server Transaction.....	46
3.12.4	CANCEL Response (Declined).....	46
3.12.5	CANCEL Response (Accepted).....	47
3.13	CANCEL (Client/Outbound).....	48
3.13.1	Message Flow.....	48
3.13.2	CANCEL Outbound Request .....	48
3.13.3	CANCEL Client Transaction.....	48
3.13.4	CANCEL Response (Declined).....	48
3.13.5	CANCEL Response (Accepted).....	49
3.14	Re-INVITE (Server/Inbound).....	49
3.14.1	Message Flow.....	49
3.14.2	Re-INVITE Inbound Request.....	50
3.14.3	Re-INVITE Server Transaction .....	51
3.14.4	Re-INVITE Response (Declined).....	51
3.14.5	Re-INVITE Response (Provisional, Trying) .....	52
3.14.6	Re-INVITE Response (Provisional).....	52
3.14.7	Re-INVITE Response (OK).....	52
3.14.8	ACK Request (Inbound for Declined 300-99 Status Code) .....	53
3.14.9	ACK Request (Inbound for Success 200-299 Status Code).....	53
3.14.10	PRACK Request.....	53
3.15	Re-INVITE (Client/Outbound).....	54

3.15.1	Message Flow.....	54
3.15.2	Re-INVITE Outbound Request.....	55
3.15.3	Re-INVITE Client Transaction .....	55
3.15.4	Re-INVITE Response (Declined).....	55
3.15.5	Re-INVITE Response (Provisional, Trying) .....	56
3.15.6	Re-INVITE Response (Provisional).....	56
3.15.7	Re-INVITE Response (OK).....	56
3.15.8	ACK Request (Outbound for Declined 300-699 Status Code).....	57
3.15.9	ACK Request (Outbound for Success 200-299 Status Code).....	57
3.15.10	PRACK Request.....	57
3.16	BYE (Server/Inbound).....	59
3.16.1	Message Flow.....	59
3.16.2	BYE Inbound Request.....	59
3.16.3	BYE Server Transaction .....	59
3.16.4	BYE Response (Declined).....	60
3.16.5	BYE Response (Accepted).....	60
3.17	BYE (Client/Outbound).....	61
3.17.1	Message Flow.....	61
3.17.2	BYE Outbound Request.....	61
3.17.3	BYE Client Transaction .....	61
3.17.4	BYE Response .....	62
3.18	INFO (Server/Inbound).....	62
3.18.1	Message Flow.....	62
3.18.2	INFO Inbound Request.....	62
3.18.3	INFO Server Transaction .....	63
3.18.4	INFO Response (Declined).....	63
3.18.5	INFO Response (Accepted).....	63
3.19	NOTIFY.....	63
4	SIP-I Compliance (ISUP in SIP) .....	64
4.1	SIP-I Content Encoding (SDP and/or ISUP).....	64
4.1.1	Content Encoding.....	64
4.1.2	Inbound Content-Type.....	64
4.1.3	Inbound Content Headers (SDP) .....	64
4.1.4	Inbound Content Headers (ISUP).....	65
4.1.5	Outbound Content-Type.....	65
4.1.6	Outbound Content Headers (SDP).....	65



4.1.7	Outbound Content Headers (ISUP).....	65
4.2	Inbound A-Leg SIP-I INVITE Transaction .....	66
4.2.1	Inbound A-Leg SIP-I INVITE Request (IAM) .....	66
4.2.2	Inbound A-Leg SIP-I INVITE Responses .....	66
4.3	Outbound B-Leg SIP-I INVITE Transaction.....	70
4.3.1	Outbound B-Leg SIP-I INVITE Request (IAM) .....	70
4.3.2	Outbound B-Leg SIP-I INVITE Responses .....	71
4.4	Inbound SIP-I BYE Transaction .....	73
4.4.1	Inbound SIP-I BYE Request.....	73
4.4.2	Inbound SIP-I BYE Request (200 OK Response) .....	73
4.5	Outbound SIP-I BYE Transaction .....	74
4.5.1	Outbound SIP-I BYE Request.....	74
4.5.2	Outbound SIP-I BYE Request (Any Response) .....	74
5	SDP Compliance .....	75
5.1	SDP Overview.....	75
5.2	SDP Patterns (RFC 6337) .....	75
5.3	SDP Use-Case Details .....	76
5.3.1	B-Leg Termination (With SDP Offer after A-Leg Incall).....	76
5.3.2	B-Leg Termination (With SDP Offer after A-Leg Outcall).....	78
5.3.3	B-Leg Termination (without A-Leg SDP Offer) .....	78
5.4	SDP Normalisation (A-Leg).....	79
5.5	SDP Inactive/Suspended .....	79
5.5.1	Suspended (No Host) .....	79
5.5.2	Suspended (No Media) .....	80
5.5.3	Suspended (Inactive).....	80
5.6	SDP Security .....	80
5.7	SDP Fields.....	80
5.7.1	Base Fields.....	80
5.7.2	AMR and AMR-WB SDP Media Format Parameters .....	83
6	RTP Compliance .....	84
6.1	RTP Functional Scope.....	84
6.2	RTP Transport.....	84
6.3	RTP Security .....	84
6.4	RTP Endpoint Capabilities .....	85
6.4.1	Audio Payloads.....	85
6.4.2	Event Payloads .....	86

- 7 SIP Scenarios ..... 87
  - 7.1 Scenario: A-Leg Redirection ..... 87
  - 7.2 Scenario: A-Leg Screening ..... 88
  - 7.3 Scenario: Internal Announcement (Script, 200 OK) ..... 89
  - 7.4 Scenario: Internal Announcement (Script, 183 Session Progress) ..... 90
  - 7.5 Scenario: Internal Announcement (N2IVR INAP) ..... 91
  - 7.6 Scenario: External Announcement ..... 92
  - 7.7 Scenario: B-Leg Termination Attempt ..... 93
  - 7.8 Scenario: A-Leg Outcall with Internal Announcement ..... 95

## 3 SIP Compliance

### 3.1 SIP Overview

N2SIP communicates with a core network soft-switch to set-up and teardown SIP audio sessions, as well as for transferring audio signal (and out-of-band information such as DTMF telephony events) over RTP. The core network soft-switch will trunk these audio sessions to other network elements over circuit-switched, SIP/RTP, radio network or other channels, although this is not generally visible to N2SIP.

SIP compliance for N2SIP is based on RFC 3261 [R-10]. N2SIP is not compliant with prior versions of SIP such as RFC 2543.

### 3.2 SIP Request Methods

N2SIP supports the following SIP Request Methods for the various SIP interactions.

Request	Inbound (to N2SIP Server)	Outbound (from N2SIP Client)
REGISTER	Supported	Used
OPTIONS	Supported	Used
INVITE (new session)	Supported	Used
re-INVITE (existing session)	Supported	Used
CANCEL	Supported	Used
BYE	Supported	Used
ACK	Supported	Used
PRACK	Supported	Used
INFO	Supported	Not Used

*Table 1: SIP Request Methods*

### 3.3 Common SIP UAS Notes

The following compliance notes apply generally to the N2SIP framework when it is operating as a User Agent Server (UAS), i.e. when it is processing transactions initiated by an inbound SIP Request, and the associated subsequent outbound SIP Responses, and inbound ACK (if applicable).

#### 3.3.1 Transport Layer

N2SIP supports UDP and TCP transport for INVITE and non-INVITE UAS SIP transactions, specifically:

- Inbound (connectionless) UDP, and
- Inbound permanent TCP connections, and
- Inbound transient TCP connections.

The following are not supported:

- Outbound transient TCP connections, and
- SCTP connections.

N2SIP does not support any signalling encryption or signing/authentication mechanism at the connection level. Specifically, the TLS encryption mechanism is not supported.

N2SIP can be configured to challenge inbound requests using Digest Authentication, as described in 3.5.4 , Digest Authentication. No other signing/authentication is supported at the message level. Specifically:

- The "sips:" URI scheme is not supported.
- The PGP mechanism for encrypting or signing content body is not supported.
- The S/MIME signing or encrypting mechanism for content body is not supported.

### 3.3.2 SIP Message Codec

As noted in RFC 3261, SIP is “HTTP-like” in its encoding but it is not an extension of HTTP.

The N-Squared SIP Message encode/decode and transmit/receive functions are purpose-built for SIP, and do not include any HTTP functionality except as expressly required for SIP.

Specifically:

- Decoding of inbound SIP messages is not tolerant of LF-terminated lines, as optionally specified in section 19.3 of RFC 2616 [R-22]. All inbound messages must have their header lines terminated with the full CR LF sequence.

### 3.3.3 Inbound SIP Requests

All inbound SIP Requests must be well-formed according to section 27.1: *Option Tags* of [R-10] (including Method and URI). The following base headers apply to all requests:

Request Header	Type	Notes
Call-Id	String	Must be present.
Via	String	Must be present.
[sent-protocol]	String	"SIP/2.0/UDP" or "SIP/2.0/TCP"
[sent-by]	String	Must include host. May include port.
.branch=	String	Must be present.
.received	String	Supported.
.rport	Integer	Supported.
.*	Various	Unrecognised Via parameter tags are ignored.
From	String	Must be present.
.tag	String	Must be present.
To	String	Must be present.
CSeq	String	Must be present.
Max-Forwards	Integer	Must be present.
Content-Length	Integer	May be present for UDP. Must be present for TCP.
Require	String	May be present. Rejected except where indicated.
Supported	String	May be present. Ignored except where indicated.
P-Charging-Vector	String(s)	May be present.

Table 2: Common Inbound SIP Request Headers

As per section 20: *Header Fields* of [R-10], N2SIP will ignore all inbound header parameters (see [R-10] section 7.3: *Header Fields*) that are not understood. These may be used by site-specific service logic and/or configuration.

### 3.3.4 Malformed SIP Request Handling

An inbound SIP Request which is missing any of the mandatory SIP Request attributes or SIP Request headers will be considered misformatted, and a 500 Error Response will immediately be sent as follows without further processing:

Response Attribute	Type	Notes
Response Status Code	Integer	500
Response Status Message	String	"Internal Server Error"

Table 3: Common SIP Response Attributes for Malformed SIP Request

Request Header	Type	Notes
Call-Id	String	Copy of received Call-Id (if present).
Via	String	Copy of received Via (if present).
From	String	Copy of received From (if present).
To	String	Copy of received To (if present).
CSeq	String	Copy of received CSeq (if present).
Contact	String	Copy of received Contact (if present).
Content-Length	Integer	0

Table 4: Common SIP Response Headers for Misformatted SIP Request

Note that N2SIP handling for Misformatted Inbound SIP Requests does not create or correlate to any SIP transaction and does not create any Transaction state machine or associated retry timers. In case of failure, no attempt will be made to re-send this SIP Response.

### 3.3.5 Compact Form (Short) Headers

When processing inbound received SIP Requests, N2SIP will *accept* the compact form of the following inbound headers from RFC 3261.

Header	Short Form	Notes
Content-Type	c	-
From	f	-
Call-ID	i	-
Supported	k	-
Content-Length	l	-
Contact	m	-
To	t	-
Via	v	-

Table 5: Compact Form (Short) Headers

Additionally, custom SIP INVITE headers may be configured, with long and compact form names, either of which will be accepted for inbound SIP INVITE Requests. Depending on configuration, these SIP headers may also be replicated into:

- a. Specific SIP INVITE Response messages, and/or
- b. The corresponding B-Leg outbound SIP INVITE Request when N2SIP acts as a B2BUA.

Note that when processing compact form headers for SIP Requests and Responses:

- It is supported that one header use compact form, and another header use long form within a single Request or Response. E.g. it is permitted that the From header be represented as compact form “f: ...” while the Contact header be specified in full as “Contact: ...”.
- It is not supported to mix compact and long forms for a single repeated header. E.g. it is not permitted that a repeated Via header be present as both “Via: ...” and “v: ...” forms within a single Request or Response. In any such case, only the long form header will be used.

N2SIP does not transmit compact form headers in any outbound SIP Requests or Responses. When replicating inbound SIP INVITE Request headers outbound in a SIP Request or Response, N2SIP will always use the long form header name.

### 3.3.6 Outbound SIP Responses

All SIP Responses sent by N2SIP to well-formatted Inbound SIP Requests will be well-formed SIP Responses according to section 7.2: *Responses* of [R-10] (including Status Code and Status Message), and will include at least the following mandatory Headers:

Response Header	Type	Notes
Call-Id	String	Always present.
Via	String	Always present.
[sent-protocol]	String	"SIP/2.0/UDP" or "SIP/2.0/TCP".
[sent-by]	String	Will include host. Include port from Request if present.
.received=	String	Present if requested by inbound "rport" or if inbound Via Sent By host was not numeric.
.branch=	String	Always present.
.rport=	String	Present if requested by inbound "rport".
From	String	Always present.
.tag	String	Always present.
To	String	Always present.
.tag	String	Present if dialog is being formed.
CSeq	String	Always present.
Content-Length	Integer	Always present.
User-Agent	String	Set to configurable value.
P-Charging-Vector	String	Copied from the topmost “P-Charging-Vector” header in the corresponding Request, if present.

Table 6: Common Outbound SIP Response Headers

Note that custom site-specific service logic and/or configuration may implement (add or accept) additional Response headers not listed in this document.

### 3.4 Common SIP UAC Notes

The following compliance notes apply generally to the N2SIP framework when it is operating as a User Agent Client (UAC). I.e. when it is creating transactions initiated by an outbound SIP Request, and the associated subsequent inbound SIP Responses, and outbound ACK (if applicable).

### 3.4.1 Transport Layer

N2SIP supports UDP and TCP transport for INVITE and non-INVITE UAC SIP Transactions. Specifically, N2SIP supports:

- Outbound (connectionless) UDP, and
- Outbound permanent TCP connections, and
- Re-use of inbound transient TCP connections.

SCTP transport is not supported.

Note specifically that the current version of N2SIP has limited support for transient TCP connections when sending outbound SIP Responses. It will re-use the inbound transient TCP connection on which the corresponding inbound SIP Request arrived. However, it will never create an outbound transient TCP connection.

N2SIP does not support any signalling encryption or signing/authentication mechanism at the connection level. Specifically, the TLS encryption mechanism is not supported.

N2SIP can be configured to retry outbound SIP Requests that were challenged with Digest Authentication, as described in 3.5.4 , Digest Authentication. No other signing/authentication is supported at the message level. Specifically:

- The "sips:" URI scheme is not supported.
- The PGP mechanism for encrypting or signing content body is not supported.
- The S/MIME signing or encrypting mechanism for content body is not supported.

### 3.4.2 Outbound SIP Requests

The N2SIP framework will generate well-formed outbound SIP Requests according to section 27.1: *Option Tags* of [R-10] (including Method and URI). The following base headers apply to all requests:

Request Header	Type	Notes
Call-Id	String	Always present.
Via	String	Always present.
[sent-protocol]	String	"SIP/2.0/UDP" or "SIP/2.0/TCP"
[sent-by]	String	Must include host. May include port.
.branch=	String	Always present.
.received	String	Not Used.
.rport	Integer	Not Used.
From	String	Always present.
.tag	String	Always present.
To	String	Always present.
CSeq	String	Always present.
Max-Forwards	Integer	Always present.
Content-Length	Integer	Always present.
Require	String	May be present.
Supported	String	May be present.
User-Agent	String	Set to configurable value.

*Table 7: Common Outbound SIP Request Headers*

### 3.4.3 Compact Form (Short) Headers

N2SIP does not transmit compact form headers in any outbound SIP Requests or Responses. When replicating inbound SIP INVITE Request headers outbound in a SIP Request or Response, N2SIP will always use the long form header name.

Note that custom site-specific service logic and/or configuration may always implement (add or accept) additional custom Request headers not listed in this document.



### 3.4.4 Inbound SIP Responses

All inbound SIP Responses must be well-formed according to section 27.1: *Option Tags* of [R-10] (including Method and URI). The following base headers apply to all inbound SIP Responses:

Request Header	Type	Notes
Call-Id	String	Must be present.
Via	String	Must be present.
[sent-protocol]	String	"SIP/2.0/UDP" or "SIP/2.0/TCP"
[sent-by]	String	Must include host. May include port.
.branch=	String	Must be present.
.received	String	Supported.
.rport	Integer	Supported.
.*	Various	Unrecognised Via parameter tags are ignored.
From	String	Must be present.
To	String	Must be present.
CSeq	String	Must be present.
Max-Forwards	Integer	Must be present.
Content-Length	Integer	May be present for UDP. Must be present for TCP.
Require	String	May be present. Rejected except where indicated.
Supported	String	May be present. Ignored except where indicated.

Table 8: Common Inbound SIP Response Headers

As per section 20: *Header Fields* of [R-10], N2SIP will ignore all inbound header parameters (see [R-10] section 7.3: *Header Fields*) that are not understood. These may be used by site-specific service logic and/or configuration.

## 3.5 Other Common SIP Notes

### 3.5.1 Multicast

The N2SIP framework has no support for multicast.

The “maddr” parameter is silently ignored if it appears in any URI parameter.

The “ttl” parameter is silently ignored if it appears in any URI parameter.

### 3.5.2 SIP-I

N2SIP Offers support for basic SIP-I encapsulation of ISUP messages, as described subsequently in section 4, SIP-I Compliance (ISUP in SIP).

This includes the use of Content-Type = multipart/mixed as required.

### 3.5.3 SIP-T

The current release of N2SIP does not support SIP-T.

### 3.5.4 Digest Authentication

The N2SIP supports Digest Authentication for both inbound and outbound Requests and Responses using the standard mechanisms defined in RFC 3261 [R-10]. Standard headers are used in both directions.

For Requests:

Request Header	Type	Notes
<b>Content of Table 2: Common Inbound SIP Request Headers, plus...</b>		
Authorization	String	Present when using Digest authentication.

Table 9: Digest Authentication Request Headers

Response Header	Type	Notes
<b>Content of Table 6: Common Outbound SIP Response Headers, plus...</b>		
WWW-Authenticate	String	Present when using Digest authentication.

Table 10: Digest Authentication Response Headers

Within N2SIP, Digest Authentication can be applicable to the following method types.

Request	Inbound (to N2SIP UAS)	Outbound (from N2SIP UAC)
REGISTER	Applicable	Applicable
OPTIONS	Applicable	Not Used
INVITE (new session)	Applicable	Applicable
re-INVITE (existing session)	Applicable	Applicable
CANCEL	Not Applicable	Not Applicable
BYE	Applicable	Applicable
ACK	Not Applied	Not Applied
PRACK	Not Applied	Not Used
INFO	Applicable	Not Used

Table 11: SIP Requests Applicable to Digest Authentication

The following SIP Response codes and strings are specific to Digest Authorization and can be present in the Response to any Inbound method SIP Request listed as “Applicable” in the preceding table.

Status Code	Error-Info
401	<none> (Used to indicate that authorization is required).
403	Authorization Failure (Nonce).
403	Authorization Failure (Username).
403	Authorization Failure (Password).
404	Subscriber domain not known here.
404	Subscriber not known at this domain.
500	<various>

Table 12: Digest Authorization Common Response Codes

### 3.6 REGISTER (Server/Inbound)

#### 3.6.1 Message Flow

N2SIP supports inbound SIP REGISTER Requests for pre-configured subscriptions. If the registration is accepted, N2SIP will retain the registered Contact information and will use it for initiating subsequent outbound INVITE requests to that address.

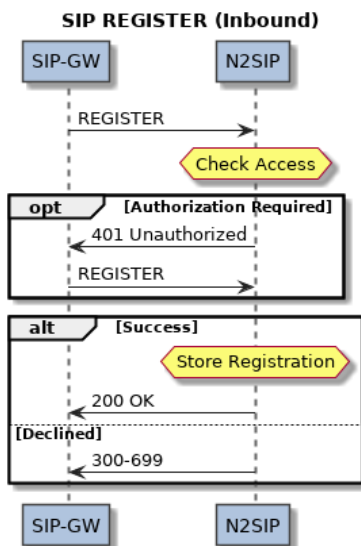


Figure A - Inbound SIP REGISTER

Note that in addition to dynamically registered Contact addresses, N2SIP also supports static configuration of Contacts for outbound INVITE requests.

#### 3.6.2 REGISTER Inbound Request

N2SIP supports receiving the following attributes and headers in inbound REGISTER.

Request Attribute	Type	Notes
Request Method	String	REGISTER
Request Header	Type	Notes
<b>Content of Table 2: Common Inbound SIP Request Headers, plus...</b>		
<b>Content of Table 9: Digest Authentication Request Headers, plus...</b>		
From		Must be present.
.URI	URI	Must be present and set to To URI.
To		Must be present.
.URI	URI	Must be present and set to From URI.
Contact	String(s)	Must be present. Only the first Contact header will be registered (no multi-home). Only one Contact per header line is supported. The "*" form of the Contact header from RFC 3261 [R-10] 10.2.2 Removing Bindings is not supported.
.Address	String	Must be present.
.expires	Integer	Optional. Default value 3600 seconds.

Table 13: Inbound SIP REGISTER Request

Any content body for the REGISTER Request is ignored.

### 3.6.3 REGISTER Server Transaction

The client may re-use the REGISTER Via "branch" for subsequent registrations, however N2SIP will not retain an open transaction in this case and will discard REGISTER transaction context at the expiry of Timer J as per [R-10] *Figure 8*. The re-REGISTER will be treated as a new transaction.

N2SIP will create a SIP Server non-INVITE Transaction for the SIP REGISTER Request as described by [R-10] section 17.2.2: *Non-INVITE Server Transaction* and [R-10] *Figure 8* and will obey the timers and retransmission rules defined by this state machine.

### 3.6.4 REGISTER Response (Declined)

If a well-formed REGISTER Request is declined, then N2SIP will send a SIP Response with Status Code that is not 2xx and constructed according to the rules defined in section 3.3.6: Outbound SIP Response.

The following is a list of the possible Status Codes, along with the most common Error-Info strings used, when declining a well-formatted REGISTER Request. The list of strings is only indicative, and other Error-Info strings may be returned. The spelling and formatting of these strings may change without notice.

Status Code	Error-Info
<b>Any Response from Table 12: Digest Authorization Common Response Codes, plus...</b>	
420	A Require option is not supported.
500	Received REGISTER with From URI that is not To URI.
500	Received REGISTER with no 'Contact'.
500	<Any other exception string generated internally during processing>

*Table 14: Indicative List of REGISTER Codes and Error-Info Strings*

### 3.6.5 REGISTER Response (Accepted)

If the REGISTER Request is accepted, N2SIP will generate a SIP Response with Status Code 200 OK.

Response Header	Type	Notes
<b>Content of Table 6: Common Outbound SIP Response Headers, plus...</b>		
Allow	String	Configured value or "INVITE,ACK,BYE,CANCEL,OPTIONS,REGISTER,INFO,PRACK"
Accept	String	"application/sdp"
Contact Address	String	Copy of received Contact Address.
Contact "expires"	Integer	Always present.

*Table 15: Outbound SIP REGISTER Response Headers*

### 3.7 REGISTER (Client/Outbound)

#### 3.7.1 Message Flow

N2SIP Server supports sending outbound SIP REGISTER to a configured SIP peer. This will be done for any local “endpoint” addresses which the N2SIP is configured to manage. Refer to the Technical Guide for information on configuring managed endpoints.

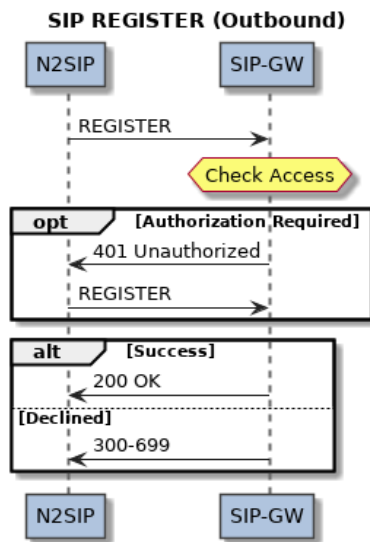


Figure B - Outbound SIP REGISTER

#### 3.7.2 REGISTER Outbound Request

The N2SIP supports sending the following attributes and headers in outbound REGISTER.

Request Attribute	Type	Notes
Request Method	String	REGISTER
Request Header	Type	Notes
<b>Content of Table 7: , plus...</b>		
<b>Content of Table 10: Digest Authentication Response Headers, plus...</b>		
From URI	String	sip:<pstn-digits>@<sip-peer-domain>
To URI	String	sip:<pstn-digits>@<sip-peer-domain>
Contact URI	String	sip:<pstn-digits>@<sip-public-host>[:<port>]
Expires	Integer	Configured value, or 0 when we de-REGISTER.

Table 16: Outbound SIP REGISTER Request

No content body is created for the REGISTER Request.

#### 3.7.3 REGISTER Client Transaction

N2SIP does not re-use the REGISTER Via "branch" for subsequent registrations. Each outbound REGISTER request is a new transaction.

N2SIP will create a SIP Client non-INVITE Transaction for the SIP REGISTER Request as described in [R-10] section 17.1.2: Non-INVITE Client Transaction and [R-10] Figure 6 and will obey the timers and retransmission rules defined by this state machine.

### 3.7.4 REGISTER Response

N2SIP accepts well-formatted SIP Responses to the REGISTER Request and expects a 200 OK Response.

A 401 response will cause a retry using Digest Authentication. This requires that a username and password be configured within the N2SIP for the far-end SIP Peer associated with the endpoint.

## 3.8 OPTIONS (Server/Inbound)

### 3.8.1 Message Flow

N2SIP SIP Server supports inbound SIP OPTIONS Requests.

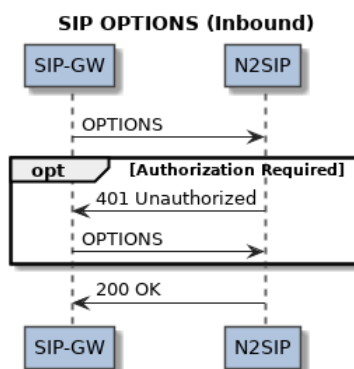


Figure C - Inbound SIP OPTIONS

### 3.8.2 OPTIONS Inbound Request

N2SIP supports receiving the following attributes and headers in inbound OPTIONS.

Request Attribute	Type	Notes
Request Method	String	OPTIONS
Request Header	Type	Notes
<b>Content of Table 2: Common Inbound SIP Request Headers, plus...</b>		
<b>Content of Table 9: Digest Authentication Request Headers, plus...</b>		

Table 17: Inbound SIP OPTIONS Request

Any content body for the OPTIONS Request is ignored.

### 3.8.3 OPTIONS Server Transaction

N2SIP will create a SIP Server non-INVITE Transaction for the SIP OPTIONS Request as described by [R-10] section 17.2.2: Non-INVITE Server Transaction and [R-10] Figure 8 and will obey the timers and retransmission rules defined by this state machine.

### 3.8.4 OPTIONS Response (Declined)

If a well-formed OPTIONS Request is declined, then N2SIP will send a SIP Response with a Status Code that is not 2xx and constructed according to the rules defined in section 3.3.6: Outbound SIP Response.

The following is a list of the possible Status Codes, along with the most common Error-Info strings used, when declining a well-formatted OPTIONS Request. The list of strings is only indicative, and

other Error-Info strings may be returned. The spelling and formatting of these strings may change without notice.

Status Code	Error-Info
<b>Any Response from Table 12: Digest Authorization Common Response Codes, plus...</b>	
420	A Require option is not supported.
500	<Any other exception string generated internally during processing>

*Table 18: Indicative List of OPTIONS Codes and Error-Info Strings*

### 3.8.5 OPTIONS Response (Accepted)

All well-formed OPTIONS requests are accepted, assuming they pass any applicable authorization checks. N2SIP will generate a SIP Response with Status Code 200 OK.

Response Header	Type	Notes
<b>Content of Table 6: Common Outbound SIP Response Headers, plus...</b>		
<b>Content of Table 10: Digest Authentication Response Headers, plus...</b>		
Allow	String	Configured value, or "INVITE,ACK,BYE,CANCEL,OPTIONS,REGISTER,INFO,PRACK".
Accept	String	"application/sdp"

*Table 19: Outbound SIP OPTIONS Response Headers*

### 3.9 INVITE & ACK & PRACK (Server/Inbound, A-Leg Only)

This section 3.9 relates to scenarios where N2SIP acting as a UAS receives a SIP INVITE Request which initiates a new Dialog, a new Call-ID and a new call-control service logic instance. It does not relate to re-INVITE within an existing SIP Dialog. For re-INVITE refer to section 3.14: *Re-INVITE (Server/Inbound)*.

#### 3.9.1 Message Flow

N2SIP supports inbound A-Leg SIP INVITE Requests for establishing the A-Leg for the purpose of call control, where the subsequent call treatment may be one (or more) of:

- Connecting to an internal RTP stream generator for A-Leg audio interaction, and/or
- Attempting an A-Leg to B-Leg termination, operating as a back-to-back user agent
- Declining the request with a 300-699, potentially with address redirection.

The SIP message flow associated with an incall A-Leg SIP INVITE Request is:

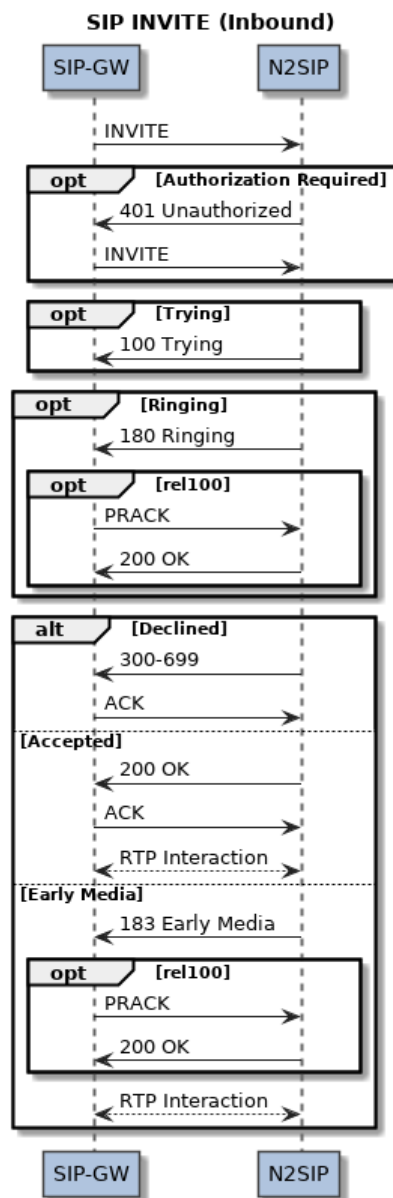


Figure D - Inbound SIP INVITE



The subsequent handling may involve:

- PRACK for reliable provisional responses.
- Re-INVITE for change of SDP parameters.
- Setup of SDP/RTP audio stream using provisional 1xx INVITE Responses.

Note: Inbound SIP INVITE Request is applicable to A-Leg establishment only. N2SIP does not support any scenarios where any B-Leg can be established via inbound SIP INVITE Request.

### 3.9.2 INVITE Inbound Request

N2SIP supports receiving the following attributes and headers in inbound INVITE for A-Leg.

Request Attribute	Type	Notes
Request Method	String	INVITE
Request Header	Type	Notes
<b>Content of Table 2: Common Inbound SIP Request Headers, plus...</b>		
<b>Content of Table 9: Digest Authentication Request Headers, plus...</b>		
Record-Route	String(s)	Copied into the first INVITE Response that establishes a Dialog.
From		Must be present.
.URI	String	Must be "sip:" URI scheme. May be used by service logic as the "Calling Party Address" to determine what interactions to perform during the session. When operating as an independent (internal logic), N2SIP service logic may use this From URI in processing.
.tag	String	Must be present as the remote Dialog tag.
To		Must be present.
.URI	String	Must be "sip:" URI scheme. May be used by service logic as the "Called Party Address" to determine what interactions to perform during the session. For example, when N2IVR is deployed as an INAP-controlled SRF then this field typically contains the SCP ID and Correlation ID which uniquely identifies the controlling INAP SCP session.
.tag	String	Must not be present.
Contact	String(s)	Must be present. Only the first Contact header will be used (no multi-home). Only one Contact per header line is supported.
Content-Type	String	Either "application/sdp", "application/ISUP" or "multipart/mixed" containing both SDP and ISUP. SDP will be present for RFC 6337 [R-24] patterns 1 or 3 only.
Require	String	"100rel" is accepted. Other entries are rejected.
Supported	String	"100rel" is accepted. Other entries are ignored.
P-Asserted-Identity	String	The topmost "P-Asserted-Identity" header is accepted and parsed according to RFC 3323 [R-20] and RFC 3325 [R-21], with details made available to service logic.

P-Preferred-Identity	String	The topmost “P-Preferred-Identity” header is accepted and parsed according to RFC 3323 [R-20] and RFC 3325 [R-21], with details made available to service logic.
Privacy	String	The topmost “Privacy” header is accepted and parsed according to RFC 3323 [R-20] and RFC 3325 [R-21], with details made available to service logic.
<b>Request Content</b>	<b>Type</b>	<b>Notes</b>
<b>May include an SDP Session "Offer" (RFC 6337 [R-24] pattern 1 or 3), as per section 5: SDP Compliance. May include ISUP, as per section 4: SIP-I Compliance (ISUP in SIP).</b>		

Table 20: Inbound SIP INVITE Request (A-Leg)

### 3.9.3 INVITE Server Transaction

If the INVITE Transaction is accepted, N2SIP will create a SIP Server INVITE Transaction for the SIP INVITE Request as described by [R-10] section 17.2.1: INVITE Server Transaction and [R-10] Figure 7 and will obey the timers and retransmission rules defined by this state machine.

### 3.9.4 INVITE Response (Declined)

If a well-formed INVITE Request is declined, then N2SIP will send a SIP Response with non-2xx Status Code and constructed according to the rules defined in section 3.3.6: Outbound SIP Response.

Note that the use of a 300-699 Response Code is a valid processing scenario and does not necessarily indicate that a processing “error” has occurred. Many “normal” business-cases use this mechanism in SIP, including:

- Subscriber not available (Did Not Answer, Busy).
- Subscriber has moved (Number Ported).
- Call deliberately declined (Missed Call Attempt).
- Insufficient Funds or Call Black-Listed.
- Natural End of IVR Interaction using Early Media.

The following Response content may be present.

Response Attribute	Type	Notes
Response Status Code	Integer	300-699
Response Status Message	String	<Associated Status Message>
Response Header	Type	Notes
<b>Content of Table 6: Common Outbound SIP Response Headers, plus...</b>		
Contact	String	Optional. Redirection Contact, e.g. for 302 Response.
Reason	String	Optional. Reason as per RFC 3326 [R-18].
.protocol	String	“SIP”, “Q.850” or other value.
.cause	Integer	16 or other value.
.text	String	“Terminated” or other value.

Table 21: Outbound SIP INVITE 300-699 Response Headers

The following is a list of the standard “declined” Status Codes, along with common Error-Info strings (if applicable) used when declining a well-formatted INVITE Request. The list of strings is only

indicative, and other Error-Info strings may be returned. The spelling and formatting of these strings may change without notice.

Status Code	Error-Info
<b>Any Response from Table 12: Digest Authorization Common Response Codes, plus...</b>	
ANY	Any Status Code in the range 300-699 chosen by custom service logic.
480	<none> (Natural conclusion of an IVR interaction with clean call teardown).
481	Invite has 'To' (local) tag but does not match a known Dialog. (Will occur if re-INVITE is used. N2SIP does not support re-INVITE.)
487	<none> (Used when INVITE is terminated by CANCEL)
500	Missing Content-Type header for INVITE.
500	Unsupported Content-Type header '<content-type>' for INVITE.
500	Missing 'application/sdp' Content on INVITE.
500	Missing remote tag on From header for initial INVITE.
500	Failure on A-Leg Invite Handler: <extended-reason>
500	<Any other exception string generated internally during processing>
603	Server forced clean shutdown at end of INVITE processing.

Table 22: Indicative List of INVITE Codes and Error-Info Strings

Note that an error SIP Response on initial processing may occur before or after the sending of the 100 Trying Response - see section 3.9.5: INVITE Response (Provisional, Trying).

### 3.9.5 INVITE Response (Provisional, Trying)

If the INVITE Request is accepted, then N2SIP will (if configured to do so) immediately generate a provisional SIP Response with Status Code 100 Trying to indicate that the Request has been accepted and service logic will now be performed to determine the appropriate call handling.

Response Attribute	Type	Notes
Response Status Code	Integer	100
Response Status Message	String	"Trying"
Response Header	Type	Notes
<b>Content of Table 6: Common Outbound SIP Response Headers, plus...</b>		
Record-Route	String(s)	Copied from the SIP INVITE Request if the Response establishes a Dialog.

Table 23: Outbound SIP INVITE 100 Trying Response Headers

Note that according to RFC 3262 [R-15], Reliable Provisional Response is not applicable to 100 "Trying" Responses.

### 3.9.6 INVITE Response (Provisional)

N2SIP may use a provisional SIP INVITE Responses (101-199) either when:

- Relaying a provisional response received from the outbound B-Leg, or
- Sending an internally generated RTP media stream using “Early Media”.

The response may include:

Response Attribute	Type	Notes
Status Code	Integer	180 or other 101-199 status code
Status Message	String	"Ringing" or other message corresponding to code
Response Header	Type	Notes
<b>Content of Table 6: Common Outbound SIP Response Headers, plus...</b>		
Require	String	"100rel" if PRACK is required.
RSeq	Integer	Response sequence number if PRACK is required
Contact	String	May be present to indicate Contact for PRACK.
Content-Type	String	Either “application/sdp”, “application/ISUP” or “multipart/mixed” containing both SDP and ISUP. SDP will be present for RFC 6337 [R-24] pattern 3 only.
Record-Route	String(s)	Copied from the SIP INVITE Request if the Response establishes a Dialog.
Response Content	Type	Notes
<b>May include an SDP Session "Answer" (RFC 6337 [R-24] pattern 3), as per section 5: SDP Compliance. SDP Session "Offer" (RFC 6337 [R-24] pattern 4) is not supported. May include ISUP, as per section 4: SIP-I Compliance (ISUP in SIP).</b>		

Table 24: Outbound SIP INVITE Provisional Response Headers

Contact information is provided (if configured) for PRACK routing as per RFC 3263 [R-17].

Early Media with late offer (Pattern 4) is not supported. The INVITE Request must have contained an SDP session offer for Early Media to be successfully negotiated via N2SIP.

### 3.9.7 INVITE Response (Success)

N2SIP may use a final success SIP INVITE Responses (200-299) either when:

- Relaying a final success response received from the outbound B-Leg, or
- Sending an internally generated RTP media stream using full stream establishment.

The response may include:

Response Attribute	Type	Notes
Response Status Code	Integer	200 or 201-299
Response Status Message	String	"OK" or other associated status message
Response Header	Type	Notes
<b>Content of Table 6: Common Outbound SIP Response Headers, plus...</b>		
Record-Route	String(s)	Copied from the SIP INVITE Request if the Response establishes a Dialog.

Allow	String	Configured value, or "INVITE,ACK,BYE,CANCEL,OPTIONS,REGISTER,INFO,PRACK".
Content-Type	String	Either "application/sdp", "application/ISUP" or "multipart/mixed" containing both SDP and ISUP. SDP will be present for RFC 6337 [R-24] patterns 1 and 2.
Contact	String(s)	Specifies contact address for other dialog transactions.
Response Content	Type	Notes
<p><b>May include an SDP Session "Offer" (RFC 6337 [R-24] pattern 2) or "Answer" (RFC 6337 [R-24] pattern 1), as per section 5: SDP Compliance.</b></p> <p><b>May include ISUP, as per section 4: SIP-I Compliance (ISUP in SIP).</b></p>		

Table 25: Outbound SIP INVITE Acceptance Response Headers

N2SIP expects ACK on this response and implements the transport layer re-transmission for INVITE 200 OK as described in [R-10] section 17.2.1: INVITE Server Transaction.

Contact information is provided for ACK, BYE routing as per RFC 3263 [R-17].

### 3.9.8 ACK Request (Inbound, A-Leg, for Declined 300-699 Status Code)

N2SIP supports receiving the following attributes and headers in inbound ACK in the context of an inbound A-Leg SIP INVITE for which N2SIP responded with Status Code 300-699.

Request Attribute	Type	Notes
Request Method	String	ACK
Request Header	Type	Notes
<b>Content of Table 2: Common Inbound SIP Request Headers, plus...</b>		
CSeq		Present
.Method	String	INVITE
.Number	Integer	INVITE CSeq Number
Via	<b>Content of Table 2: Common Inbound SIP Request Headers "Via" Header, plus...</b>	
.via-branch	String	Must match existing INVITE Transaction.

Table 26: Inbound SIP ACK Request for INVITE and Re-INVITE Response 300-699

Any content body for the ACK Request for a Declined INVITE Result is ignored.

### 3.9.9 ACK Request (Inbound, A-Leg, for Success 200-299 Status Code)

N2SIP supports receiving the following attributes and headers in inbound ACK as a new pseudo-Transaction in the context of an existing INVITE Inbound A-Leg dialog for which N2SIP responded to the INVITE Transaction with a success Status Code 2xx.

Request Attribute	Type	Notes
Request Method	String	ACK
Request Header	Type	Notes
<b>Content of Table 2: Common Inbound SIP Request Headers, plus...</b>		
CSeq		Present
.Method	String	ACK
.Number	Integer	ACK CSeq Number
From	<b>Content of Table 2: Common Inbound SIP Request Headers "From" Header, plus...</b>	
.tag	String	Must be present as the remote Dialog tag.
To	<b>Content of Table 2: Common Inbound SIP Request Headers "To" Header, plus...</b>	
.tag	String	Must be present as the local Dialog tag.
Content-Type	String	Either "application/sdp", "application/ISUP" or "multipart/mixed" containing both SDP and ISUP. SDP will be present for RFC 6337 [R-24] pattern 2 only.
Request Content	Type	Notes
<b>May include an SDP Session "Answer" (RFC 6337 [R-24] pattern 2), as per section 5: SDP Compliance. May include ISUP, as per section 4: SIP-I Compliance (ISUP in SIP).</b>		

*Table 27: Inbound SIP ACK Request for INVITE Response 200-299*

No response is generated for this ACK Request and no Transaction state model is created.

### 3.9.10 PRACK Request (Inbound, A-Leg)

N2SIP supports receiving the following attributes and headers in inbound PRACK as a new Transaction in the context of an existing INVITE Inbound A-Leg dialog for which N2SIP responded to the initial INVITE Transaction with Status Code 101-199 and where N2SIP offered or required “100rel” support.

The received PRACK Request fields are:

Request Attribute	Type	Notes
Request Method	String	PRACK
Request Header	Type	Notes
<b>Content of Table 2: Common Inbound SIP Request Headers, plus...</b>		
CSeq		Present
.Method	String	PRACK
.Number	Integer	PRACK Cseq Number
From	<b>Content of Table 2: Common Inbound SIP Request Headers “From” Header, plus...</b>	
.tag	String	Must be present as the remote Dialog tag.
To	<b>Content of Table 2: Common Inbound SIP Request Headers “To” Header, plus...</b>	
.tag	String	Must be present as the local Dialog tag.
Rack	String	Formed as per RFC 3262 [R-15].

Table 28: Inbound SIP PRACK Request for INVITE Response 101-199

Any content for the PRACK Request is ignored. RFC 6337 [R-24] patterns 4 and 5 are not supported.

Note that in the case of back-to-back treatment of a Provisional INVITE Response from the B-Leg to the A-Leg, the state machines of the PRACK handling for the two call legs are entirely independent from each other. No information is passed between the two separate PRACK transactions.

### 3.9.11 PRACK Response (Declined)

If a well-formed PRACK Request is declined, then N2SIP will send a SIP Response with Status Code that is not 2xx and constructed according to the rules defined in section 3.3.6: Outbound SIP Response.

The following is a list of the supported Status Codes, along with the most common Error-Info strings used when declining a well-formatted PRACK Request. The list of strings is only indicative, and other Error-Info strings may be returned. Spelling and format of these strings may change without notice.

Status Code	Error-Info
481	<none – used when PRACK does not match an unacknowledged reliable provisional Response>
500	<Any other exception string generated internally during processing>

Table 29: Indicative List of PRACK Codes and Error-Info Strings

### 3.9.12 PRACK Response (Accepted)

If the PRACK Request is accepted, N2SIP will generate a SIP Response with status 200 OK.

Response Header	Type	Notes
<b>Content of Table 6: Common Outbound SIP Response Headers only</b>		

Table 30: Outbound SIP PRACK Response Headers

### 3.10 INVITE & ACK & PRACK (Client/Outbound, A-Leg)

#### 3.10.1 Message Flow

This section 3.10 relates to the scenario where N2SIP acting as a UAC performs a SIP INVITE Request to initiate a new Dialog, a new Call-ID for the purpose of establishing a new standalone “outcall” A-Leg.

This section does not relate to re-INVITE within an existing dialog, see section 3.15: *Re-INVITE (Client/Outbound)*. It does not relate to the attempt to terminate a B-Leg in the context of an existing A-Leg, see section 3.11: *INVITE & ACK & PRACK (Client/Outbound, B-Leg)*.

In either case, N2SIP will initiate an outbound SIP INVITE with the following message flow:

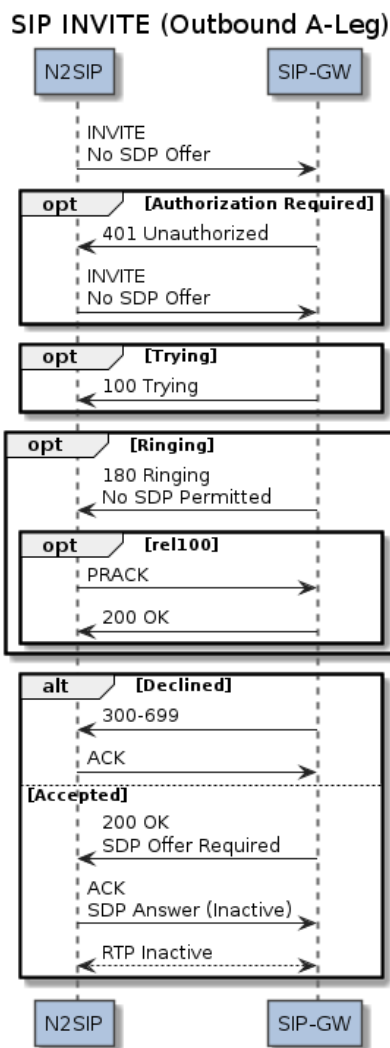


Figure E – Outbound SIP INVITE to establish A-Leg

SDP negotiation in the outbound A-Leg SIP INVITE is limited to Pattern 2.

- N2SIP will not send any SDP Offer.
- The A-Party must provide an SDP Offer in the 2xx INVITE Response.
- N2SIP will provide a placeholder “inactive” SDP Answer in the ACK.

No RTP stream is active at this time. The RTP will start once the B-Leg or internal RTP stream is active.



### 3.10.2 INVITE Outbound Request

N2SIP supports sending the following attributes and headers in outbound INVITE to A-Leg.

	Type	Notes
Request Method	String	INVITE
Request Header	Type	Notes
<b>Content of Table 7: , plus...</b>		
<b>Content of Table 9: Digest Authentication Request Headers, plus...</b>		
From		Always present.
.URI	String	Always "sip:" URI scheme. Determined from service logic-provided "Calling Party Address" with configured public host/domain.
.tag	String	Always present as the local Dialog tag.
To		Always present.
.URI	String	Always "sip:" URI scheme. Determined from service logic-provided "Called Party Address" with configured public host/domain.
.tag	String	Never present.
Contact	String	Must be present. May be repeated. Only one Contact per header line is supported.
Content-Type	String	Never present.
Require	String	"100rel" may be used, depending on configuration.
Supported	String	"100rel" may be used, depending on configuration.
P-Asserted-Identity	String	The topmost inbound A-Leg INVITE "P-Asserted-Identity" header according to RFC 3323 [R-20] and RFC 3325 [R-21] may be copied to the B-Leg outbound INVITE, depending on configuration.
P-Charging-Vector	String	The topmost inbound A-Leg INVITE "P-Charging-Vector" header may be copied to the B-Leg outbound INVITE, depending on configuration.
P-Preferred-Identity	String	The topmost inbound A-Leg INVITE "P-Preferred-Identity" header according to RFC 3323 [R-20] and RFC 3325 [R-21] may be copied to the B-Leg outbound INVITE, depending on configuration.
Privacy	String	The topmost inbound A-Leg INVITE "Privacy" header according to RFC 3323 [R-20] and RFC 3325 [R-21] may be copied to the B-Leg outbound INVITE, depending on configuration.

Table 31: Outbound SIP INVITE Request to A-Leg

No Content is present in the SIP INVITE Request. ISUP is never included in an outbound A-Leg. SDP is not present since only Pattern 2 is supported.

### 3.10.3 INVITE Client Transaction

N2SIP will create a SIP Client INVITE Transaction for the SIP INVITE Request as described in [R-10] section 17.1.1: *INVITE Client Transaction* and [R-10] *Figure 5* and will obey the timers and retransmission rules defined by this state machine.

### 3.10.4 INVITE Response (Declined)

N2SIP will accept a well-formatted SIP Response with Status Code 300-699.

A 401 response will cause a re-try using Digest Authentication. This requires that a username and password be configured within the N2SIP for the far-end SIP Peer associated with the endpoint.

Any other value will be returned to the service logic to allow it to decide how to proceed.

The following Response content may be present.

Response Attribute	Type	Notes
Response Status Code	Integer	300-699
Response Status Message	String	<Associated Status Message>
Response Header	Type	Notes
<b>Content of Table 8: , plus...</b>		
Contact	String	Optional. Redirection Contact, e.g. for 302 Response.
Reason	String	Optional. Reason as per RFC 3326 [R-18].
.protocol	String	"SIP", "Q.850" or other value.
.cause	Integer	16 or other value.
.text	String	"Terminated" or other value.
<Any>	String	Used for passthrough or custom service logic.

Table 32: Inbound SIP INVITE 300-699 Response Headers

### 3.10.5 INVITE Response (Provisional, Trying)

N2SIP will accept a provisional 100 Trying response, which will stop the retransmission of the SIP INVITE Request. It is not passed to the controlling service logic.

Note that according to RFC 3262 [R-15], Reliable Provisional Response is not applicable to 100 "Trying" Responses.

### 3.10.6 INVITE Response (Provisional)

The N2SIP platform accepts 180 as an indication of Ringing, as well as other 101-199 INVITE Responses.

No Content is permitted:

- This Provisional response may not contain any SDP content, since only Pattern 2 is supported.
- No ISUP content is supported for this A-Leg outcall scenario.

A PRACK will be performed if required.

Response Attribute	Type	Notes
Status Code	Integer	180 or other 101-199 status code
Status Message	String	"Ringing" or other status message
Response Header	Type	Notes
<b>Content of Table 8: , plus...</b>		
Require	String	"100rel" indicates if PRACK is required.
RSeq	Integer	Response sequence number if PRACK is required

Contact	String	May be present to indicate Contact for PRACK.
Content-Type	String	Never present.
Record-Route	String(s)	May be present if the Response establishes a Dialog and a Dialog-specific Route applies.
<Any>	String	Used for passthrough or custom service logic.

Table 33: Inbound SIP INVITE Ringing Response Headers

Contact information (if provided) is used for PRACK routing as per RFC 3263 [R-17].

### 3.10.7 INVITE Response (Success)

The N2SIP platform accepts 200 status code INVITE Response to confirm the A-Leg outcall INVITE dialog.

This must contain an SDP Offer from the A-Party.

Response Attribute	Type	Notes
Response Status Code	Integer	Must be 200. Other codes are not accepted.
Response Status Message	String	"OK" or other associated status message
Response Header	Type	Notes
<b>Content of Table 8: , plus...</b>		
Allow	String	"INVITE,ACK,BYE,CANCEL,OPTIONS,REGISTER,INFO,PRACK".
Content-Type	String	Must be "application/sdp". Only RFC 6337 [R-24] pattern 2 is supported.
Contact	String	Specifies contact address for other dialog transactions.
Record-Route	String(s)	May be present if the Response establishes a Dialog and a Dialog-specific Route applies.
<Any>	String	Used for passthrough or custom service logic.
Response Content	Type	Notes
<b>Must be an SDP Session "Offer" (RFC 6337 [R-24] pattern 2) as per section 5: SDP Compliance.</b>		

Table 34: Inbound SIP INVITE Acceptance Response Headers

Contact information (if provided) is used for ACK, BYE routing as per RFC 3263 [R-17].

### 3.10.8 ACK Request (Outbound, A-Leg, for Declined 300-699 Status Code)

N2SIP sends the following attributes and headers in outbound ACK in the context of an INVITE Outbound A-Leg Client Transaction for which N2SIP received a Response with Status Code 300-699.

Request Attribute	Type	Notes
Request Method	String	ACK
Request Header	Type	Notes
<b>Content of Table 7: , plus...</b>		
CSeq		Present
.Method	String	INVITE
.Number	Integer	INVITE CSeq Number
Via	<b>Content of Table 7: "Via" Header, plus...</b>	
.via-branch	String	Must match existing INVITE Transaction.

Table 35: Outbound SIP ACK Request for INVITE and Re-INVITE Response 300-699

No content body is created for the ACK Request to a Declined Status Code.

### 3.10.9 ACK Request (Outbound, A-Leg, for Success 200 Status Code)

N2SIP sends ACK as a new pseudo-Transaction in the context of an existing INVITE A-Leg Outbound Client dialog for which N2SIP received an INVITE Response with Status Code 200.

Request Attribute	Type	Notes
Request Method	String	ACK
Request Header	Type	Notes
<b>Content of Table 7: , plus...</b>		
CSeq		Present
.Method	String	ACK
.Number	Integer	ACK CSeq Number
From	<b>Content of Table 7: "From" Header, plus...</b>	
.tag	String	Always present as the local Dialog tag.
To	<b>Content of Table 7: "To" Header, plus...</b>	
.tag	String	Always present as the remote Dialog tag.
Content-Type	String	Will be "application/sdp". Only RFC 6337 [R-24] pattern 2 is supported.
Route	String(s)	Will be present if a Dialog-specific route applies.
Request Content	Type	Notes
<b>This will be a placeholder "inactive" SDP Session "Answer" (RFC 6337 [R-24] pattern 2), as per section 5: SDP Compliance.</b>		

Table 36: Outbound SIP ACK Request for INVITE and Re-INVITE Response 200

No response is expected for this ACK Request and no Transaction state model is created.

### 3.10.10 PRACK Request (Outbound, A-Leg)

Where PRACK is applicable, N2SIP sends the following attributes and headers in outbound PRACK as a new Transaction in the context of an existing INVITE Outbound Client dialog for which a Response with Status Code 101-199 has been received.

Request Attribute	Type	Notes
Request Method	String	PRACK
Request Header	Type	Notes
<b>Content of Table 7: , plus...</b>		
CSeq		Present
.Method	String	PRACK
.Number	Integer	PRACK CSeq Number
From	<b>Content of Table 7: "From" Header, plus...</b>	
.tag	String	Always present as the local Dialog tag.
To	<b>Content of Table 7: "To" Header, plus...</b>	
.tag	String	Always present as the remote Dialog tag.
RAck	String	Formed as per RFC 3262 [R-15].

Table 37: Outbound SIP PRACK Request for INVITE Response 101-199

No content body is created for the PRACK Request.

### 3.10.11 PRACK Response (Declined)

N2SIP accepts a SIP Response with Status Code that is not 2xx. This is an error case and will result in forced teardown of the outbound A-Leg INVITE transaction.

Response Header	Type	Notes
<b>Content of Table 6: Common Outbound SIP Response Headers only</b>		

Table 38: Inbound SIP PRACK Response Headers

### 3.10.12 PRACK Response (Accepted)

N2SIP accepts a SIP Response with status 200 OK as successful transmission and reception of the associated Provisional Response.

Response Header	Type	Notes
<b>Content of Table 6: Common Outbound SIP Response Headers only</b>		

Table 39: Inbound SIP PRACK Response Headers

### 3.11 INVITE & ACK & PRACK (Client/Outbound, B-Leg)

#### 3.11.1 Message Flow

This section 3.10 relates to the scenario where N2SIP acting as a UAC performs a SIP INVITE Request to initiate a new Dialog, a new Call-ID for the purpose of creating a B-Leg which will be connected with an existing A-Leg, with N2SIP performing the role of a back-to-back SIP User Agent.

This section does not relate to re-INVITE within an existing dialog, see 3.15 *Re-INVITE (Client/Outbound)*.

N2SIP will initiate an outbound SIP INVITE with the following message flow:

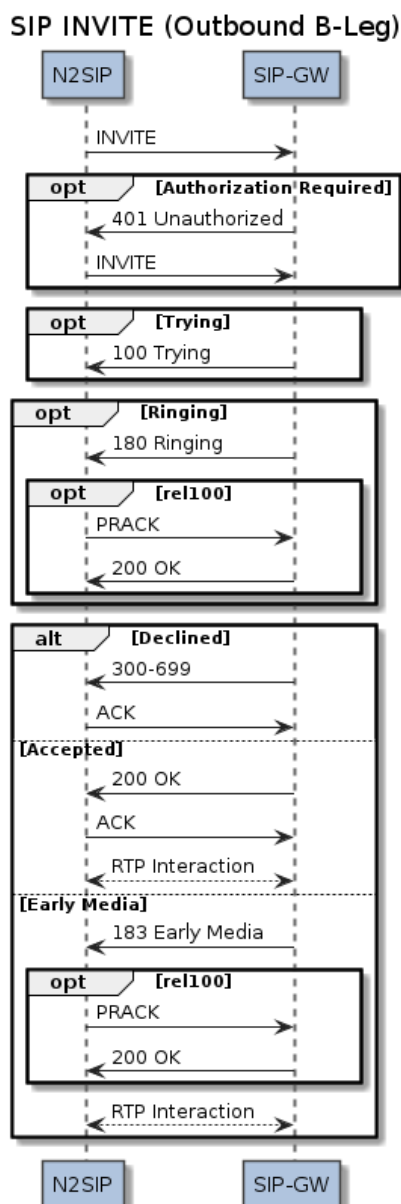


Figure F – Outbound SIP INVITE

When using RFC 6337 Pattern 1 or Pattern 3, then the SIP INVITE Request will contain an SDP Offer which is the SDP Offer provided by the A-Leg.

The SIP INVITE Request may contain ISUP, if this call is using ISUP.

### 3.11.2 INVITE Outbound Request

N2SIP supports sending the following attributes and headers in outbound INVITE to a B-Leg.

	Type	Notes
Request Method	String	INVITE
Request Header	Type	Notes
<b>Content of Table 7: , plus...</b>		
<b>Content of Table 9: Digest Authentication Request Headers, plus...</b>		
From		Always present.
.URI	String	Always “sip:” URI scheme. Determined from service logic-provided “Calling Party Address” with configured public host/domain.
.tag	String	Always present as the local Dialog tag.
To		Always present.
.URI	String	Always “sip:” URI scheme. Determined from service logic-provided “Called Party Address” with configured public host/domain.
.tag	String	Never present.
Contact	String	Must be present. May be repeated. Only one Contact per header line is supported.
Content-Type	String	Either “application/sdp”, “application/ISUP” or “multipart/mixed” containing both SDP and ISUP. SDP will be present for RFC 6337 [R-24] patterns 1 and 3 only.
Require	String	“100rel” may be used, depending on configuration.
Supported	String	“100rel” may be used, depending on configuration.
P-Asserted-Identity	String	The topmost inbound A-Leg INVITE “P-Asserted-Identity” header according to RFC 3323 [R-20] and RFC 3325 [R-21] may be copied to the B-Leg outbound INVITE, depending on configuration.
P-Charging-Vector	String	The topmost inbound A-Leg INVITE “P-Charging-Vector” header may be copied to the B-Leg outbound INVITE, depending on configuration.
P-Preferred-Identity	String	The topmost inbound A-Leg INVITE “P-Preferred-Identity” header according to RFC 3323 [R-20] and RFC 3325 [R-21] may be copied to the B-Leg outbound INVITE, depending on configuration.
Privacy	String	The topmost inbound A-Leg INVITE “Privacy” header according to RFC 3323 [R-20] and RFC 3325 [R-21] may be copied to the B-Leg outbound INVITE, depending on configuration.
Request Content	Type	Notes
<b>May include an SDP Session “Offer” (RFC 6337 patterns 1 or 3) copied from the inbound A-Leg INVITE Request Content, as per section 5: SDP Compliance.</b> <b>May include ISUP, as per section 4: SIP-I Compliance (ISUP in SIP).</b>		

Table 40: Outbound SIP INVITE Request to B-Leg

### 3.11.3 INVITE Client Transaction

N2SIP will create a SIP Client INVITE Transaction for the SIP INVITE Request as described in [R-10] section 17.1.1: *INVITE Client Transaction* and [R-10] *Figure 5* and will obey the timers and retransmission rules defined by this state machine.

### 3.11.4 INVITE Response (Declined)

N2SIP will accept a well-formatted SIP Response with Status Code 300-699.

A 401 response will cause a re-try using Digest Authentication. This requires that a username and password be configured within the N2SIP for the far-end SIP Peer associated with the endpoint.

For other values, the Status Code will be passed through to the controlling service logic. The service logic may decide to return this value back to the A-Leg (if possible), or it may decide to attempt other call control actions.

The following Response content may be present.

Response Attribute	Type	Notes
Response Status Code	Integer	300-699
Response Status Message	String	<Associated Status Message>
Response Header	Type	Notes
<b>Content of Table 8: , plus...</b>		
Contact	String	Optional. Redirection Contact, e.g. for 302 Response.
Reason	String	Optional. Reason as per RFC 3326 [R-18].
.protocol	String	"SIP", "Q.850" or other value.
.cause	Integer	16 or other value.
.text	String	"Terminated" or other value.
<Any>	String	Used for passthrough or custom service logic.

Table 41: Inbound SIP INVITE 300-699 Response Headers

### 3.11.5 INVITE Response (Provisional, Trying)

N2SIP will accept a provisional 100 Trying response, which will stop the retransmission of the SIP INVITE Request. It is not passed to the controlling service logic.

Note that according to RFC 3262 [R-15], Reliable Provisional Response is not applicable to 100 "Trying" Responses.

### 3.11.6 INVITE Response (Provisional)

N2SIP platform will accept provisional 1xx INVITE Response from the B-Leg, with or without SDP. E.g. 180 Ringing with no SDP. 180 Ringing with SDP for custom ring tone, 183 Session Progress with SDP for early media using Pattern 3, etc.

If the B-Leg provisional response contains SDP then that SDP will be passed back to the A-Leg as described in section 5: *SDP Compliance*. The B-Leg SDP may be normalised towards the A-Leg as described in section 5.4: *SDP Normalisation (A-Leg)*.

- a) If the A-Leg is an inbound SIP INVITE Request and N2SIP has not yet sent a final INVITE Response, then the SDP provided by the B-Leg provisional response (using Pattern 3) will be



sent in a corresponding provisional 1xx response to the A-Leg using the same provisional status code.

- b) If the A-Leg is an outbound SIP INVITE Request, or the A-Leg was inbound, but a final INVITE Response has been sent, then the SDP provided by the B-Leg provisional response will be sent in an outbound SIP re-INVITE request to the A-Leg.

If the B-Leg provisional response does not contain SDP, then a wider range of processing options exist.

If the A-Leg is inbound and incomplete, then the provisional response is typically passed-through.

- 1) If the A-Leg is an inbound SIP INVITE Request and N2SIP has not yet sent a final INVITE Response, then N2SIP will send a corresponding provisional response to the A-Leg using the same status code, with no SDP.
- 2) **Exception to (1) for “compact ringing”.** If the “compact ringing” option is enabled, and the B-Leg provisional status code is 180 Ringing, and the most recent provisional status code sent to the A-Leg was also 180 Ringing without SDP, then the just-received B-Leg provisional response is considered redundant and is *not* passed on to the A-Leg.

If the A-Leg is outbound, or inbound complete, then the provisional response is typically not passed-through.

- 3) If the A-Leg is an outbound SIP INVITE Request, or the A-Leg was inbound but a final INVITE Response has been sent, then the B-Leg provisional response will be discarded and will not be sent to the A-Leg.
- 4) **Exception to (3) for “internal ring tone generation”.** If the “internal ring tone generation” is enabled and configured, and the B-Leg provisional status code is 180 Ringing but without SDP, then N2SIP will initiate Internal Ring Tone Generation.

Internal Ring Tone Generation is an N2SIP feature which will detect the indicated specific scenario from (3) and will establish a local RTP stream endpoint to play a “Ring Tone” audio stream in the case where the received B-Party 180 Ringing cannot be passed back to the A-Party.

The following INVITE Response structure is accepted for this purpose.

Response Attribute	Type	Notes
Status Code	Integer	180 or other 101-199 status code
Status Message	String	"Ringing" or other status message
Response Header	Type	Notes
<b>Content of Table 8: , plus...</b>		
Require	String	"100rel" indicates if PRACK is required.
RSeq	Integer	Response sequence number if PRACK is required
Contact	String	May be present to indicate Contact for PRACK.
Content-Type	String	Either "application/sdp", "application/ISUP" or "multipart/mixed" containing both SDP and ISUP. SDP will be present for RFC 6337 [R-24] pattern 3.
Record-Route	String(s)	May be present if the Response establishes a Dialog and a Dialog-specific Route applies.
<Any>	String	Used for passthrough or custom service logic.
Response Content	Type	Notes
<b>May include an SDP Session "Answer" (RFC 6337 [R-24] pattern 3), as per section 5: SDP Compliance. May include ISUP, as per section 4: SIP-I Compliance (ISUP in SIP).</b>		

Table 42: Inbound SIP INVITE Provisional Response Headers

Contact information (if provided) is used for PRACK routing as per RFC 3263 [R-17].

### 3.11.7 INVITE Response (Success)

The N2SIP platform accepts 200 or other successful response to confirm the INVITE dialog to the B-Party.

When using Pattern 1, this must contain the SDP Answer to the Offer provided in the B-Leg SIP INVITE Request. When using Pattern 2, this must contain the SDP Offer that we will pass to the A-Leg.

The SDP will be passed back to the A-Leg as described in section 5: SDP Compliance. The B-Leg SDP may be normalised towards the A-Leg as described in 5.4: SDP Normalisation (A-Leg).

- a) If the A-Leg is an inbound SIP INVITE Request and N2SIP has not yet sent a final INVITE Response, then any SDP provided by the B-Leg final response will be sent in the corresponding successful final 2xx response to the A-Leg using the same success status code.
- b) If the A-Leg is an outbound SIP INVITE Request, or the A-Leg was inbound but a final INVITE Response has been sent, then the SDP provided by the B-Leg final response will be sent in an outbound SIP re-INVITE request to the A-Leg.

The supported 2xx INVITE Response attributes are:

Response Attribute	Type	Notes
Response Status Code	Integer	200 or 201-299
Response Status Message	String	"OK" or other associated status message
Response Header	Type	Notes

Content of Table 8: , plus...		
Allow	String	"INVITE,ACK,BYE,CANCEL,OPTIONS,REGISTER,INFO,PRACK".
Content-Type	String	Either "application/sdp", "application/ISUP" or "multipart/mixed" containing both SDP and ISUP. SDP will be present for RFC 6337 [R-24] patterns 1 or 2.
Contact	String	Specifies contact address for other dialog transactions.
Record-Route	String(s)	May be present if the Response establishes a Dialog and a Dialog-specific Route applies.
<Any>	String	Used for passthrough or custom service logic.
Response Content	Type	Notes
<p><b>May include an SDP Session "Offer" (RFC 6337 [R-24] pattern 2) or "Answer" (RFC 6337 [R-24] pattern 1), as per section 5: SDP Compliance.</b></p> <p><b>May include ISUP, as per section 4: SIP-I Compliance (ISUP in SIP).</b></p>		

Table 43: Inbound SIP INVITE Acceptance Response Headers

Contact information (if provided) is used for ACK, BYE routing as per RFC 3263 [R-17].

### 3.11.8 ACK Request (Outbound, B-Leg, for Declined 300-699 Status Code)

N2SIP sends the following attributes and headers in outbound ACK in the context of an INVITE Outbound B-Leg Client Transaction for which N2SIP received a Response with Status Code 300-699.

Request Attribute	Type	Notes
Request Method	String	ACK
Request Header	Type	Notes
Content of Table 7: , plus...		
CSeq		Present
.Method	String	INVITE
.Number	Integer	INVITE CSeq Number
Via	Content of Table 7: "Via" Header, plus...	
.via-branch	String	Must match existing INVITE Transaction.

Table 44: Outbound SIP ACK Request for INVITE and Re-INVITE Response 300-699

No content body is created for the ACK Request.

### 3.11.9 ACK Request (Outbound, B-Leg, for Success 200-299 Status Code)

N2SIP sends ACK as a new pseudo-Transaction in the context of an existing INVITE Outbound Client dialog for which N2SIP received an INVITE Response with Status Code 2xx.

Request Attribute	Type	Notes
Request Method	String	ACK
Request Header	Type	Notes
Content of Table 7: , plus...		
CSeq		Present
.Method	String	ACK
.Number	Integer	ACK CSeq Number

From	<b>Content of Table 7: "From" Header, plus...</b>	
.tag	String	Always present as the local Dialog tag.
To	<b>Content of Table 7: "To" Header, plus...</b>	
.tag	String	Always present as the remote Dialog tag.
Content-Type	String	Either "application/sdp", "application/ISUP" or "multipart/mixed" containing both SDP and ISUP. SDP will be present for RFC 6337 [R-24] pattern 2.
Route	String(s)	Will be present if a Dialog-specific route applies.
<b>Request Content</b>	<b>Type</b>	<b>Notes</b>
<p><b>May include an SDP Session "Answer" (RFC 6337 [R-24] pattern 2) copied from the A-Leg, as per section 5: SDP Compliance.</b></p> <p><b>May include ISUP, as per section 4: SIP-I Compliance (ISUP in SIP).</b></p>		

Table 45: Outbound SIP ACK Request for INVITE and Re-INVITE Response 200-299

No response is expected for this ACK Request and no Transaction state model is created.

### 3.11.10 PRACK Request (Outbound, B-Leg)

Where PRACK is applicable, N2SIP sends the following attributes and headers in outbound PRACK as a new Transaction in the context of an existing INVITE Outbound Client dialog for which a Response with Status Code 101-199 has been received.

Request Attribute	Type	Notes
Request Method	String	PRACK
Request Header	Type	Notes
<b>Content of Table 7: , plus...</b>		
CSeq		Present
.Method	String	PRACK
.Number	Integer	PRACK CSeq Number
From	<b>Content of Table 7: "From" Header, plus...</b>	
.tag	String	Always present as the local Dialog tag.
To	<b>Content of Table 7: "To" Header, plus...</b>	
.tag	String	Always present as the remote Dialog tag.
RAck	String	Formed as per RFC 3262 [R-15].

Table 46: Outbound SIP PRACK Request for INVITE Response 101-199

No content body is created for the PRACK Request.

Note that because N2SIP does not support any SDP Patterns which involve PRACK, then the PRACK handling on the A-Leg and B-Leg is not synchronized. When PRACK is used on both legs, the PRACK Request/Response timing is entirely independent for each leg.

### 3.11.11 PRACK Response (Declined)

N2SIP accepts a SIP Response with Status Code that is not 2xx. This is an error case and will result in forced teardown of the INVITE transaction.

Response Header	Type	Notes
<b>Content of Table 6: Common Outbound SIP Response Headers only</b>		

*Table 47: Inbound SIP PRACK Response Headers*

### 3.11.12 PRACK Response (Accepted)

N2SIP accepts a SIP Response with status 200 OK as successful transmission and reception of the associated Provisional Response.

Response Header	Type	Notes
<b>Content of Table 6: Common Outbound SIP Response Headers only</b>		

Inbound SIP PRACK Response Headers

### 3.12 CANCEL (Server/Inbound)

#### 3.12.1 Message Flow

N2SIP supports inbound SIP CANCEL Requests as part of inbound INVITE and re-INVITE Transactions.

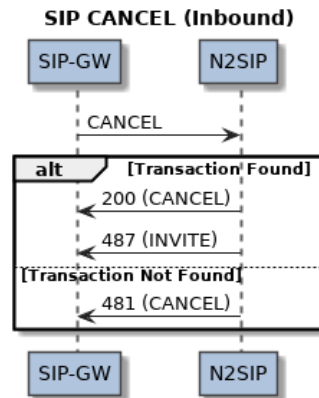


Figure G – Inbound SIP CANCEL

#### 3.12.2 CANCEL Inbound Request

N2SIP supports receiving the following attributes and headers in inbound CANCEL.

Request Attribute	Type	Notes
Request Method	String	CANCEL
Request Header	Type	Notes
<b>Content of Table 2: Common Inbound SIP Request Headers, plus...</b>		
Cseq		Present
.Method	String	CANCEL
.Number	Integer	INVITE or re-INVITE Cseq Number
Via	<b>“Via” Header from Table 2: Common Inbound SIP Request Headers, plus...</b>	
.via-branch	String	Must match existing INVITE or re-INVITE Transaction.

Table 48: Inbound SIP CANCEL Request for INVITE and Re-INVITE

Any content body for the CANCEL Request is ignored.

Note that as per RFC 3261 [R-10], Digest Authentication is not applicable to CANCEL Requests.

#### 3.12.3 CANCEL Server Transaction

N2SIP will create a SIP Server non-INVITE Transaction for the SIP CANCEL Request as described by [R-10] section 17.2.2: Non-INVITE Server Transaction and [R-10] Figure 8 and will obey the timers and retransmission rules defined by this state machine.

#### 3.12.4 CANCEL Response (Declined)

If a well-formed CANCEL Request is declined, then N2SIP will send a SIP Response with Status Code that is not 2xx and constructed according to the rules defined in section 3.3.6: Outbound SIP Response.

The following is a list of the supported Status Codes, along with the most common Error-Info strings used when declining a well-formatted CANCEL Request. The list of strings is only indicative, and other Error-Info strings may be returned. The spelling and formatting of these strings may change without notice.

Status Code	Error-Info
481	<none – used when CANCEL does not match a known INVITE or re-INVITE transaction>
500	<Any other exception string generated internally during processing>

*Table 49: Indicative List of CANCEL Codes and Error-Info Strings*

### 3.12.5 CANCEL Response (Accepted)

If the CANCEL Request is accepted, N2SIP will generate a SIP Response with status 200 OK.

Response Header	Type	Notes
<b>Content of Table 6: Common Outbound SIP Response Headers only</b>		

*Table 50: Outbound SIP CANCEL Response Headers*

The corresponding INVITE or re-INVITE transaction will be terminated with a 487 Status Code.

### 3.13 CANCEL (Client/Outbound)

#### 3.13.1 Message Flow

N2SIP supports outbound SIP CANCEL Requests as part of outbound INVITE and re-INVITE Transactions.

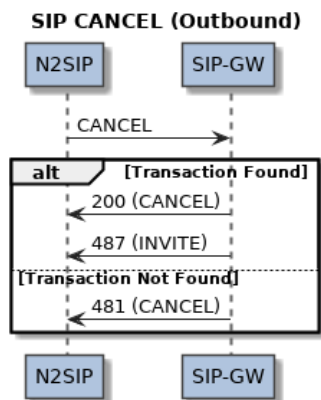


Figure H - Outbound SIP CANCEL

#### 3.13.2 CANCEL Outbound Request

N2SIP uses the following attributes and headers in outbound CANCEL.

Request Attribute	Type	Notes
Request Method	String	CANCEL
Request Header	Type	Notes
<b>Content of Table 7: , plus...</b>		
CSeq		Present
.Method	String	CANCEL
.Number	Integer	INVITE CSeq Number
Via	<b>"Via" Header from Table 7: , plus...</b>	
.via-branch	String	Must match existing INVITE or re-INVITE Transaction.

Table 51: Outbound SIP CANCEL Request for INVITE and Re-INVITE

No content body is created for the CANCEL Request.

Note that as per RFC 3261 [R-10], Digest Authentication is not applicable to CANCEL Requests.

#### 3.13.3 CANCEL Client Transaction

N2SIP will create a SIP Client non-INVITE Transaction for the SIP CANCEL Request as described in [R-10] section 17.1.2: *Non-INVITE Client Transaction* and [R-10] Figure 6 and will obey the timers and retransmission rules defined by this state machine.

#### 3.13.4 CANCEL Response (Declined)

N2SIP accepts a SIP Response with Status Code that is not 2xx. This is an error case and will result in forced teardown of the INVITE or re-INVITE transaction.



Response Header	Type	Notes
<b>Content of Table 8: only</b>		

*Table 52: Inbound SIP CANCEL Response Headers*

### 3.13.5 CANCEL Response (Accepted)

N2SIP accepts a SIP Response with status 200 OK as clean teardown of the INVITE or re-INVITE transaction.

Response Header	Type	Notes
<b>Content of Table 8: only</b>		

*Table 53: Inbound SIP CANCEL Response Headers*

The corresponding INVITE or re-INVITE transaction is expected to be terminated with a received 487 Status Code Response.

## 3.14 Re-INVITE (Server/Inbound)

### 3.14.1 Message Flow

N2SIP accepts inbound SIP re-INVITE Requests for the purpose of:

- Client-initiated SDP changes as part of back-to-back user agent INVITE call control.
- Client-initiated activity testing (ping).

N2SIP will accept re-INVITE with SDP changes when acting as a back-to-back user agent between two external legs and will pass-through the SDP to the “other” leg.

N2SIP does not accept re-INVITE with SDP changes when it is generating the RTP stream packets as an audio endpoint.

The “Target Refresh” functionality described in R-10 is never supported.

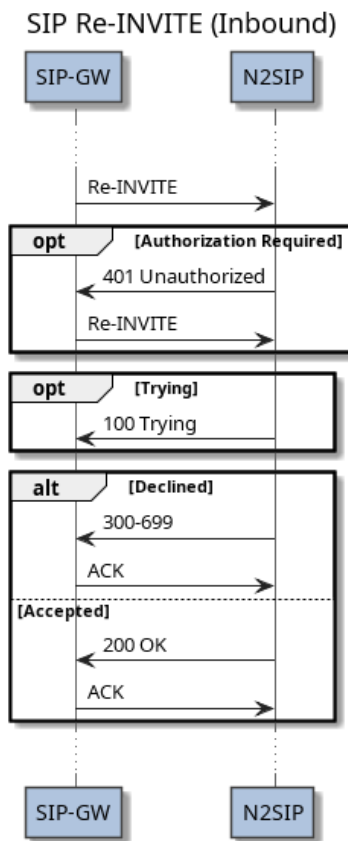


Figure 1 - Inbound SIP Re-INVITE

### 3.14.2 Re-INVITE Inbound Request

N2SIP supports receiving the following attributes and headers in inbound re-INVITE.

Request Attribute	Type	Notes
Request Method	String	INVITE
Request Header	Type	Notes
<b>Content of Table 2: Common Inbound SIP Request Headers, plus...</b>		
<b>Content of Table 9: Digest Authentication Request Headers, plus...</b>		
From	<b>Content of Table 2: Common Inbound SIP Request Headers "From" Header, plus...</b>	
.tag	String	Must be present as the remote Dialog tag.
To	<b>Content of Table 2: Common Inbound SIP Request Headers "To" Header, plus...</b>	
.tag	String	Must be present as the local Dialog tag.
Contact	String(s)	Must be present.
Content-Type	String	Must be "application/sdp" if present. SDP will be present for RFC 6337 [R-24] pattern 1.
Request Content	Type	Notes
<b>For Client-initiated SDP changes, must be an SDP Session "Offer" (RFC 6337 [R-24] pattern 1), as per section 5: SDP Compliance.</b>		

Table 54: Inbound SIP Re-INVITE Request

### 3.14.3 Re-INVITE Server Transaction

If the re-INVITE Transaction is accepted, N2SIP will create a SIP Server INVITE Transaction for the SIP re-INVITE Request as described by [R-10] section 17.2.1: *INVITE Server Transaction* and [R-10] Figure 7 and will obey the timers and retransmission rules defined by this state machine.

### 3.14.4 Re-INVITE Response (Declined)

If a well-formed re-INVITE Request is declined, then N2SIP will send a SIP Final Response with a 300-699 Status Code, constructed according to the rules defined in section 3.3.6: Outbound SIP Response.

The following Response content may be present.

Response Attribute	Type	Notes
Response Status Code	Integer	300-699
Response Status Message	String	<Associated Status Message>
Response Header	Type	Notes
<b>Content of Table 6: Common Outbound SIP Response Headers, plus...</b>		
Contact	String	Optional. Redirection Contact, e.g. for 302 Response.
Reason	String	Optional. Reason as per RFC 3326 [R-18].
.protocol	String	"SIP", "Q.850" or other value.
.cause	Integer	16 or other value.
.text	String	"Terminated" or other value.

Table 55: Outbound SIP Re-INVITE 300-699 Response Headers

The following is a list of the standard "declined" Status Codes, along with common Error-Info strings (if applicable) used when declining a well-formatted re-INVITE Request. The list of strings is only indicative, and other Error-Info strings may be returned. The spelling and formatting of these strings may change without notice.

Status Code	Error-Info
<b>Any Response from Table 12: Digest Authorization Common Response Codes, plus...</b>	
ANY	Upstream re-INVITE was declined.
488	Upstream re-INVITE was lost.

Table 56: Indicative List of Re-INVITE Codes and Error-Info Strings

Note that an error SIP Response on initial processing may occur before or after the sending of the 100 Trying Response - see section 3.14.5: *Re-INVITE Response (Provisional, Trying)*.

### 3.14.5 Re-INVITE Response (Provisional, Trying)

For Client-initiated SDP change re-INVITES, N2SIP will (if configured to do so) immediately generate a provisional SIP Response with Status Code 100 Trying to indicate that the Request has been accepted for passthrough.

Response Attribute	Type	Notes
Response Status Code	Integer	100
Response Status Message	String	"Trying"
Response Header	Type	Notes
<b>Content of Table 6: Common Outbound SIP Response Headers, only</b>		

Table 57: Outbound SIP Re-INVITE 100 Trying Response Headers

Note that according to RFC 3262 [R-15], Reliable Provisional Response is not applicable to 100 "Trying" Responses.

### 3.14.6 Re-INVITE Response (Provisional)

Provisional Responses with Status Code 101-199 are not sent for inbound re-INVITE Requests.

### 3.14.7 Re-INVITE Response (OK)

The following Response structure is used for inbound re-INVITE if the re-INVITE is accepted.

Response Attribute	Type	Notes
Response Status Code	Integer	200 or 201-299
Response Status Message	String	"OK" or other associated status message
Response Header	Type	Notes
<b>Content of Table 6: Common Outbound SIP Response Headers, plus...</b>		
Allow	String	Configured value, or "INVITE,ACK,BYE,CANCEL,OPTIONS,REGISTER,INFO,PRACK".
Content-Type	String	Must be "application/sdp" if present. SDP will be present for RFC 6337 [R-24] pattern 1.
Response Content	Type	Notes
<b>For Client-initiated SDP changes, will be an SDP Session "Answer" (RFC 6337 [R-24] pattern 1) copied from the other Leg's Response, as per section 5: SDP Compliance.</b>		

Table 58: Outbound SIP Re-INVITE Acceptance Response Headers

For Client-initiated SDP changes this Response is passed through from the other Leg.

N2SIP waits for the ACK on this response and implements the transport layer re-transmission for re-INVITE 200 OK as described in [R-10] section 17.2.1: INVITE Server Transaction.

### 3.14.8 ACK Request (Inbound for Declined 300-99 Status Code)

N2SIP supports receiving the following attributes and headers in inbound ACK in the context of an inbound re-INVITE within an existing INVITE Dialog where N2SIP responded to the re-INVITE with Status Code 300-699.

Request Attribute	Type	Notes
Request Method	String	ACK
Request Header	Type	Notes
<b>Content of Table 2: Common Inbound SIP Request Headers, plus...</b>		
CSeq		Present
.Method	String	INVITE
.Number	Integer	re-INVITE CSeq Number
Via	<b>Content of Table 2: Common Inbound SIP Request Headers "Via" Header, plus...</b>	
.via-branch	String	Must match existing re-INVITE Transaction.

Table 59: Inbound SIP ACK Request for Re-INVITE Response 300-699

Any content body for the ACK Request is ignored.

### 3.14.9 ACK Request (Inbound for Success 200-299 Status Code)

N2SIP supports receiving the following attributes and headers in inbound ACK as a new pseudo-Transaction in the context of an inbound re-INVITE within an existing INVITE Dialog where N2SIP responded to the re-INVITE with Status Code 2xx.

Request Attribute	Type	Notes
Request Method	String	ACK
Request Header	Type	Notes
<b>Content of Table 2: Common Inbound SIP Request Headers, plus...</b>		
CSeq		Present
.Method	String	ACK
.Number	Integer	ACK CSeq Number
From	<b>Content of Table 2: Common Inbound SIP Request Headers "From" Header, plus...</b>	
.tag	String	Must be present as the remote Dialog tag.
To	<b>Content of Table 2: Common Inbound SIP Request Headers "To" Header, plus...</b>	
.tag	String	Must be present as the local Dialog tag.
Content-Type	String	Never Present

Table 60: Inbound SIP ACK Request for Re-INVITE Response 200-299

No response is generated for this ACK Request and no Transaction state model is created.

### 3.14.10 PRACK Request

Receiving PRACK Requests is not applicable for re-INVITE as N2SIP does not send Responses with Status Code 101-199 for inbound re-INVITES.

### 3.15 Re-INVITE (Client/Outbound)

#### 3.15.1 Message Flow

N2SIP uses outbound SIP re-INVITE Requests for the purpose of:

- Suspending and reconnecting RTP for the A-Leg when changing the B-Leg as part of passthrough INVITE call control.
- Passing through Client-initiated SDP changes as part of passthrough INVITE call control.
- Activity testing (ping).

N2SIP will accept inbound re-INVITE with SDP changes when acting as a back-to-back user agent between two external legs and will use outbound re-INVITE pass-through the SDP to the “other” leg, acting as a back-to-back user agent.

The “Target Refresh” functionality described in R-10 is never supported.

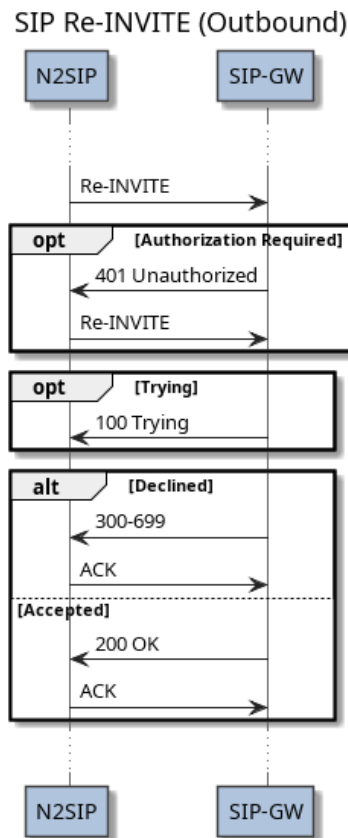


Figure J - Outbound SIP Re-INVITE

### 3.15.2 Re-INVITE Outbound Request

N2SIP supports sending the following attributes and headers in outbound re-INVITE.

Request Attribute	Type	Notes
Request Method	String	INVITE
Request Header	Type	Notes
<b>Content of Table 7: , plus...</b>		
<b>Content of Table 9: Digest Authentication Request Headers, plus...</b>		
From	<b>Content of Table 7: "From" Header, plus...</b>	
.tag	String	Always present as the local Dialog tag.
To	<b>Content of Table 7: "To" Header, plus...</b>	
.tag	String	Always present as the remote Dialog tag.
Contact	String(s)	Will be present.
Content-Type	String	Will be "application/sdp" if present. SDP will be present for RFC 6337 [R-24] pattern 1.
P-Charging-Vector	String	May be a copy of the topmost inbound A-Leg INVITE "P-Charging-Vector" header, depending on configuration.
Request Content	Type	Notes
<p><b>When suspending A-Leg RTP, will be an SDP Session "Offer" (RFC 6337 pattern 1), as per section 5: SDP Compliance.</b></p> <p><b>When reconnecting A-Leg RTP, will be an SDP Session "Offer" (RFC 6337 pattern 1) copied from the B-Leg, as per section 5: SDP Compliance.</b></p> <p><b>For Client-initiated SDP changes, will be an SDP Session "Offer" (RFC 6337 pattern 1) copied from the other Leg, as per section 5: SDP Compliance.</b></p>		

Table 61: Outbound SIP Re-INVITE Request

### 3.15.3 Re-INVITE Client Transaction

N2SIP will create a SIP Client INVITE Transaction for the SIP re-INVITE Request as described in [R-10] section 17.1.1: *INVITE Client Transaction* and [R-10] *Figure 5* and will obey the timers and retransmission rules defined by this state machine.

### 3.15.4 Re-INVITE Response (Declined)

N2SIP will accept a well-formatted SIP Response with Status Code 300-699.

A 401 response will cause a re-try using Digest Authentication. This requires that a username and password be configured within the N2SIP for the far-end SIP Peer associated with the endpoint.

For other values:

- When attempting to suspend an A-Leg, the A-Leg will be disconnected.
- When attempting to reconnect an A-Leg to a new B-Leg, the Status Code will be returned to the service logic.
- When passing through Client-initiated SDP changes, the Status Code will be passed through to the originating Client.
- When performing an activity test, the call will be disconnected.

The following Response content may be present.

Response Attribute	Type	Notes
Response Status Code	Integer	300-699
Response Status Message	String	<Associated Status Message>
Response Header	Type	Notes
<b>Content of Table 8: , plus...</b>		
Reason	String	Optional. Reason as per RFC 3326 [R-18].
.protocol	String	"SIP", "Q.850" or other value.
.cause	Integer	16 or other value.
.text	String	"Terminated" or other value.

Table 62: Inbound SIP Re-INVITE 300-699 Response Headers

### 3.15.5 Re-INVITE Response (Provisional, Trying)

N2SIP will accept a provisional 100 Trying response. It is not processed. In the case of passthrough re-INVITE, it is not relayed to the originating Client because N2SIP sends its own provisional 100 Trying response on reception of the re-INVITE as per section 3.14.5: *Re-INVITE Response (Provisional, Trying)*.

Note that according to RFC 3262 [R-15], Reliable Provisional Response is not applicable to 100 "Trying" Responses.

### 3.15.6 Re-INVITE Response (Provisional)

Provisional Responses with Status Code 101-199 are not accepted for outbound re-INVITE Requests.

### 3.15.7 Re-INVITE Response (OK)

The N2SIP platform accepts 200 or other successful response for outbound re-INVITE.

- When attempting to suspend an A-Leg, processing will continue.
- When attempting to reconnect an A-Leg to a new B-Leg, the Status Code will be passed through to the B-Leg. The originating and terminating endpoints will initiate an RTP stream. N2SIP remains in the call control path but is not part of the RTP stream.
- When passing through Client-initiated SDP changes, the Status Code will be passed through to the originating Client.
- When performing an activity test, the call will continue.



### 3.15.8 ACK Request (Outbound for Declined 300-699 Status Code)

N2SIP sends the following attributes and headers in outbound ACK in the context of an outbound re-INVITE Client Transaction (on any leg) for which N2SIP received a Response with Status Code 300-699.

Request Attribute	Type	Notes
Request Method	String	ACK
Request Header	Type	Notes
<b>Content of Table 7: , plus...</b>		
CSeq		Present
.Method	String	INVITE
.Number	Integer	re-INVITE CSeq Number
Via	<b>Content of Table 7: "Via" Header, plus...</b>	
.via-branch	String	Must match existing re-INVITE Transaction.

Table 63: Outbound SIP ACK Request for Re-INVITE Response 300-699

No content body is created for the ACK Request.

### 3.15.9 ACK Request (Outbound for Success 200-299 Status Code)

N2SIP sends ACK as a new pseudo-Transaction in the context of an existing re-INVITE Outbound Client dialog for which N2SIP received a re-INVITE Response with Status Code 2xx.

Request Attribute	Type	Notes
Request Method	String	ACK
Request Header	Type	Notes
<b>Content of Table 7: , plus...</b>		
CSeq		Present
.Method	String	ACK
.Number	Integer	ACK CSeq Number
From	<b>Content of Table 7: "From" Header, plus...</b>	
.tag	String	Always present as the local Dialog tag.
To	<b>Content of Table 7: "To" Header, plus...</b>	
.tag	String	Always present as the remote Dialog tag.
Content-Type	String	Never Present
Route	String(s)	Will be present if a Dialog-specific route applies.

Table 64: Outbound SIP ACK Request for Re-INVITE Response 200-299

No content body is created for the ACK Request.

No response is expected for this ACK Request and no Transaction state model is created.

### 3.15.10 PRACK Request

N2SIP will never send PRACK Requests as N2SIP does not accept Responses with Status Code 101-199 for outbound re-INVITES.

Response Attribute	Type	Notes
Response Status Code	Integer	200 or 201-299
Response Status Message	String	"OK" or other associated status message
Response Header	Type	Notes
<b>Content of Table 8: , plus...</b>		
Content-Type	String	Must be "application/sdp" if present. SDP will be present for RFC 6337 [R-24] pattern 1.
<Any>	String	Used for passthrough or custom service logic.
Response Content	Type	Notes
<b>When suspending or reconnecting A-Leg RTP, and for Client-initiated SDP changes, must be an an SDP Session "Answer" (RFC 6337 pattern 1), as per section 5: SDP Compliance.</b>		

*Table 65: Inbound SIP Re-INVITE Acceptance Response Headers*

### 3.16 BYE (Server/Inbound)

#### 3.16.1 Message Flow

N2SIP supports inbound SIP BYE Requests in the context of an existing, confirmed SIP Dialog, which may have arisen from either incall or outcall scenarios.

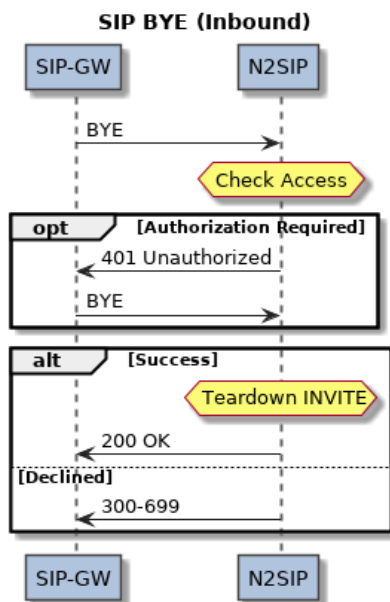


Figure K - Inbound SIP BYE

#### 3.16.2 BYE Inbound Request

N2SIP supports receiving the following attributes and headers in inbound BYE.

Request Attribute	Type	Notes
Request Method	String	BYE
Request Header	Type	Notes
<b>Content of Table 2: Common Inbound SIP Request Headers, plus...</b>		
From	<b>Content of Table 2: Common Inbound SIP Request Headers "From" Header, plus...</b>	
.tag	String	Must be present as the remote Dialog tag.
To	<b>Content of Table 2: Common Inbound SIP Request Headers "To" Header, plus...</b>	
.tag	String	Must be present as the local Dialog tag.

Table 66: Inbound SIP BYE Request

Any content body for the BYE Request is ignored.

#### 3.16.3 BYE Server Transaction

N2SIP will create a SIP Server non-INVITE Transaction for the SIP BYE Request as described in [R-10] section 17.2.2: Non-INVITE Server Transaction and [R-10] Figure 8 and will obey the timers and retransmission rules defined by this state machine.

### 3.16.4 BYE Response (Declined)

If a well-formed BYE Request is declined, N2SIP will send a SIP Response with Status Code that is not 2xx and constructed according to the rules defined in section 3.3.6: Outbound SIP Response.

The following is a list of the supported Status Codes, along with the most common Error-Info strings used when declining a well-formatted BYE Request. The list of strings is only indicative, and other Error-Info strings may be returned. The spelling and formatting of these strings may change without notice.

Status Code	Error-Info
<b>Any Response from Table 12: Digest Authorization Common Response Codes, plus...</b>	
481	<none – used when BYE does not match a known INVITE transaction>
500	<Any other exception string generated internally during processing>

Table 67: Indicative List of BYE Codes and Error-Info Strings

### 3.16.5 BYE Response (Accepted)

If the BYE Request is accepted, then N2SIP will generate a SIP Response with status 200 OK.

Response Attribute	Type	Notes
Status Code	Integer	200
Status Message	String	OK
Response Header	Type	Notes
<b>Content of Table 6: Common Outbound SIP Response Headers, plus...</b>		
Content-Type	String	May be “application/ISUP” if ISUP is present.
Response Content	Type	Notes
<b>May include ISUP, as per section 4: SIP-I Compliance (ISUP in SIP).</b>		

Table 68: Outbound SIP BYE Response Headers

### 3.17 BYE (Client/Outbound)

#### 3.17.1 Message Flow

N2SIP may initiate an outbound SIP BYE Request in the context of an existing, confirmed SIP Dialog, which may have arisen from either incall or outcall scenarios.

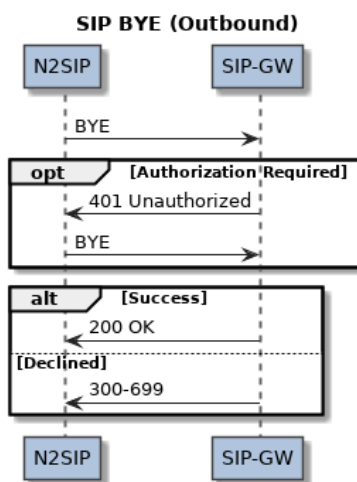


Figure L - Outbound SIP BYE

#### 3.17.2 BYE Outbound Request

N2SIP supports sending the following attributes and headers in outbound BYE.

Request Attribute	Type	Notes
Request Method	String	BYE
Request Header	Type	Notes
<b>Content of Table 7: , plus...</b>		
From		Present.
.URI	URI	Present and set to To URI from the INVITE.
.tag	String	Present as the remote Dialog tag.
To		Present.
.URI	URI	Present and set to From URI from the INVITE.
.tag	String	Present as the local Dialog tag.
Route	String(s)	Will be present if a Dialog-specific route applies.
P-Charging-Vector	String	May be a copy of the topmost inbound A-Leg INVITE "P-Charging-Vector" header, depending on configuration.

Table 69: Outbound SIP BYE Request

No content body is created for the BYE Request.

#### 3.17.3 BYE Client Transaction

N2SIP will create a SIP Client non-INVITE Transaction for the SIP BYE Request as described in [R-10] section 17.1.2: Non-INVITE Client Transaction and [R-10] Figure 6 and will obey the timers and retransmission rules defined by this state machine.

### 3.17.4 BYE Response

N2SIP accepts well-formatted SIP Responses to the BYE Request and expects a 200 OK Response.

## 3.18 INFO (Server/Inbound)

### 3.18.1 Message Flow

N2SIP supports inbound SIP INFO Requests as a new transaction within an existing INVITE dialog, for the purpose of receiving DTMF digit information when RTP telephony-event as per RFC 4733 [R-16] is not available.

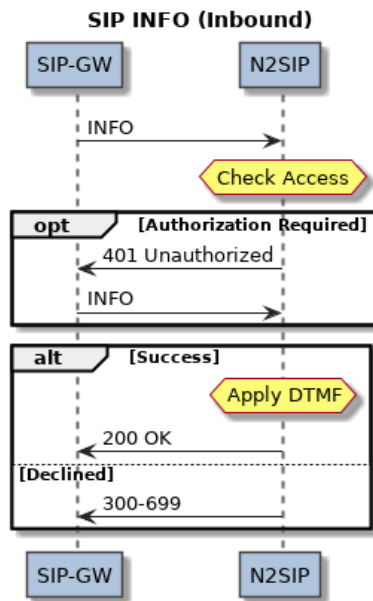


Figure M - Inbound SIP INFO

### 3.18.2 INFO Inbound Request

N2SIP supports receiving the following attributes and headers in inbound INFO.

Request Attribute	Type	Notes
Request Method	String	INFO
Request Header	Type	Notes
<b>Content of Table 2: Common Inbound SIP Request Headers, plus...</b>		
<b>Content of Table 9: Digest Authentication Request Headers, plus...</b>		
From	<b>Content of Table 2: Common Inbound SIP Request Headers "From" Header, plus...</b>	
.tag	String	Must be present as the remote Dialog tag.
To	<b>Content of Table 2: Common Inbound SIP Request Headers "To" Header, plus...</b>	
.tag	String	Must be present as the local Dialog tag.
Content-Type	String	Must be "application/dtmf-relay".

Table 70: Inbound SIP INFO Request

The following attributes of the content body are accepted as per Draft RFC [R-19].

Body Attribute	Type	Notes
Signal	Character	DTMF input type.
Duration	Integer	Ignored.

*Table 71: Inbound SIP INFO Request Body*

All other event lines are ignored in the body of the Content.

### 3.18.3 INFO Server Transaction

N2SIP will create a SIP Server non-INVITE Transaction for the SIP INFO Request as described by [R-10] section 17.2.2: *Non-INVITE Server Transaction* and [R-10] *Figure 8* and will obey the timers and retransmission rules defined by this state machine.

### 3.18.4 INFO Response (Declined)

If a well-formed INFO Request is declined, then N2SIP will send a SIP Response with Status Code that is not 2xx and constructed according to the rules defined in section 3.3.6: *Outbound SIP Response*.

The following is a list of the possible Status Codes, along with the most common Error-Info strings used, when declining a well-formatted INFO Request. The list of strings is only indicative, and other Error-Info strings may be returned. The spelling and formatting of these strings may change without notice.

Status Code	Error-Info
<b>Any Response from Table 12: Digest Authorization Common Response Codes, plus...</b>	
420	A Require option is not supported.
481	<none – used when INFO does not match a known INVITE transaction>
500	<Any other exception string generated internally during processing>

*Table 72: Indicative List of INFO Codes and Error-Info Strings*

### 3.18.5 INFO Response (Accepted)

If the INFO Request is accepted, then N2SIP will generate a SIP Response with Status Code 200 OK.

Response Header	Type	Notes
<b>Content of Table 6: Common Outbound SIP Response Headers, plus...</b>		

*Table 73: Outbound SIP INFO Response Headers*

## 3.19 NOTIFY

N2SIP does not provide any support for SIP NOTIFY.

## 4 SIP-I Compliance (ISUP in SIP)

The N2SIP framework offers support for most basic SIP-I scenarios, using binary-encoded ISUP message parts in the SIP Request/Response body for certain INVITE and BYE interactions.

The framework support is limited to the functionality described in this section. It is intended to offer a minimum SIP-I implementation compatible with the specific set scenarios described herein. The solution does not claim “full”, “complete”, nor “general” SIP-I compliance.

### 4.1 SIP-I Content Encoding (SDP and/or ISUP)

The N2SIP framework supports the inclusion of ISUP for sent and received SIP Request and/or Response content for the specific set of scenarios and associated SIP messages as described in this chapter.

#### 4.1.1 Content Encoding

All ISUP messages sent and received by N2SIP expect to use the “binary” encoding mechanism for the ISUP message octets. I.e. the actual binary octets (which will include 0x00 NULL octets) are expected to be placed in-line as the content or multi-part content part.

Other encodings such as base64 are not supported at this time.

#### 4.1.2 Inbound Content-Type

These Content-Type values are supported for receiving inbound content in a SIP Request or Response.

Content-Type	Notes
application/sdp	The content contains SDP only. Tags are ignored. Case- sensitive match.
application/ISUP	The content contains ISUP only. Tags are ignored. Case-sensitive match.
multipart/mixed	The content may contain SDP and/or ISUP. The “boundary” tag is respected. All other tags are ignored.

*Table 74: Supported inbound Content-Type values.*

The following notes on content type are relevant to both SDP and ISUP content as indicated.

#### 4.1.3 Inbound Content Headers (SDP)

For SDP the following Content header notes apply.

Location	Header	Notes
Top-Level	Content-Length	Required for TCP transport. Optional for UDP.
Top-Level or Multipart	Content-Transfer-Encoding	Ignored.
Top-Level or Multipart	Content-Disposition	If present, must be “session” Gateway Model from RFC 3959 [R-26], RFC 3960 [R-27]. The “early-session” Application Server model is not supported.

*Table 75: Relevant inbound Content headers (SDP).*



#### 4.1.4 Inbound Content Headers (ISUP)

For ISUP the following Content header notes apply.

Location	Header	Notes
Top-Level	Content-Length	Required for TCP transport. Optional for UDP.
Top-Level or Multipart	Content-Transfer-Encoding	Ignored. Only "binary" encoding is supported.
Top-Level or Multipart	Content-Disposition	Ignored.

*Table 76: Relevant inbound Content headers (ISUP).*

#### 4.1.5 Outbound Content-Type

These Content-Type values are used for sending outbound content in a SIP Request or Response.

Content-Type	Notes
application/sdp	The content contains SDP only. No tags will be set.
application/ISUP;base=itu-t92+;version=itu-t92+	The content contains ISUP only. The "base" and "version" tags are present. The tags set on this content type may vary according to site configuration.
multipart/mixed	The content contains SDP and/or ISUP. The "boundary" tag is set. No other tags will be set.

*Table 77: Supported outbound Content-Type values.*

#### 4.1.6 Outbound Content Headers (SDP)

For outbound SDP sent by N2SIP the following Content header notes apply.

Location	Header	Notes
Top-Level	Content-Length	Set for TCP and UDP transport.
Top-Level	Content-Disposition	This header is not set at the top level. It is used only for multipart.
Multipart	Content-Disposition	Set to "session;handling=required" when both SDP and ISUP are present (i.e. when using multipart/mixed MIME encoding).

*Table 78: Relevant outbound Content headers (SDP).*

#### 4.1.7 Outbound Content Headers (ISUP)

For ISUP the following Content header notes apply.

Location	Header	Notes
Top-Level	Content-Length	Required for TCP transport. Optional for UDP.
Top-Level or Multipart	Content-Transfer-Encoding	Set to "binary".
Top-Level	Content-Disposition	This header is not set at the top level.
Multipart	Content-Disposition	Set to "signal;handling=required" when both SDP and ISUP are present (i.e. when using multipart/mixed MIME encoding).

*Table 79: Relevant outbound Content headers (ISUP).*

## 4.2 Inbound A-Leg SIP-I INVITE Transaction

The N2SIP framework will accept inbound A-Leg SIP INVITE Requests for Server Transactions which contain an “application/ISUP” content subject to the content encoding limitations described above.

The presence of the ISUP part in the initial A-Leg INVITE Request means that N2SIP will treat this A-Leg INVITE call/dialog as a SIP-I dialog, with consequential behavior as described here (e.g. sending of REL message in the associated SIP BYE). This will affect the INVITE transaction and the associated BYE transaction.

In addition, any B-Leg outbound SIP INVITE Requests performed as a back-to-back user agent on behalf of this A-Leg will also be treated as SIP-I dialogs.

### 4.2.1 Inbound A-Leg SIP-I INVITE Request (IAM)

The following limitations apply to any inbound SIP-I A-Leg INVITE Request.

- a) Only a single “application/ISUP” content part may be present.
- b) The ISUP part must be an ISUP Initial Address (IAM) Message.
- c) Presence of any other ISUP message in the content is an error.
- d) A malformed ISUP message is an error.

The IAM Message will be decoded as per Q.763 [R-26] Table 32, with the following notes.

Field	Encoding	Notes
Message Type	Fixed 1 Octet	1 = Indicates IAM
Nature of Connection Indicators	Fixed 1 Octet	Provided to service logic and used for pass-through.
Forward Call Indicators	Fixed 2 Octets	Provided to service logic and used for pass-through.
Calling Party's Category	Fixed 1 Octet	Provided to service logic and used for pass-through.
Transmission Medium Requirement	Fixed 1 Octet	Provided to service logic and used for pass-through.
Called Party Number	Mandatory Variable	Decoded according to Q.763 Figure 10. Provided to service logic.
Calling Party Number	Optional Variable Tag = 10	Decoded according to Q.763 Figure 11. Provided to service logic and used for pass-through.
<other>	Other Tags	Accepted, available to service logic, and used for pass-through.

*Table 80: Inbound A-Leg SIP INVITE Request ISUP IAM Message*

### 4.2.2 Inbound A-Leg SIP-I INVITE Responses

The following possible SIP INVITE Response cases apply for any inbound SIP-I A-Leg.

#### 4.2.2.1 Immediate 200 OK Response (CON)

This section describes the ISUP content for a 200 OK response (or other 200-299 success response code if applicable) generated by the N2SIP framework in the case where there is no provisional INVITE Response (i.e. no SIP 101-199 Response code) has yet been sent on that A-Leg.

Note that 100 Trying does not count as a provisional response for this purpose.

In practice, this is only likely to occur in the case where the N2SIP framework itself is acting as the RTP audio endpoint, i.e. it is acting as an IVR and accepting the call for the purpose of performing IVR interactions by emitting and accepting RTP packets.

By contrast, in the back-to-back user agent case, it is most likely that the B-Leg will send a provisional response, and that will be passed back to the A-Leg prior to the call being confirmed with 200 OK, which is a separate sub-case.

In the case when the N2SIP framework sends a 200 OK SIP INVITE Response on the A-Leg as the first response (without preceding provisional response), then:

- This Response may contain SDP content as described in the SDP Compliance section.
- This Response will contain ISUP Connect (CON) message in the content.

The CON message will be encoded as per Q.763 [R-26] Table 27, with the following notes.

Field	Encoding	Notes
Message Type	Fixed 1 Octet	7 = Indicates CON
Backward Call Indicators	Fixed 2 Octets	Constructed as follows.
.End-to-End Method	2 bits	Constant = 0 (None)
.Called Party Status	2 bits	Constant = 1 (Ordinary Subscriber)
.Called Party Category	2 bits	Constant = 0 (None)
.Charge	2 bits	Globally Configured, Default = 2 (Charge)
.SCCP Method	2 bits	Constant = 0 (None)
.Echo Control Device	1 bit	Constant = 0 (None)
.ISDN Access	1 bit	Constant = 0 (non-ISDN)
.Holding	1 bit	Constant = 0 (Not Requested)
.ISDN User Part	1 bit	Constant = 1 (Used All The Way)
.End-to-End Information	1 bit	Constant = 0 (None)
.Interworking	1 bit	Constant = 0 (None)
[Optional Parameters]	[Various]	None. No optional parameters will be present.

*Table 81: Inbound A-Leg SIP INVITE Transaction (Immediate 200 OK Response) ISUP CON Message*

Note that this CON is constructed from scratch by the N2SIP stack and is not a pass-through of the ISUP CON (if any) which may have been received on the B-Leg.

#### 4.2.2.2 First 1XX Provisional Response (ACM)

This is the case where the N2SIP stack receives an inbound A-Leg SIP INVITE Request with ISUP IAM, and determines that it will send a provisional (101-199) response to that A-Leg INVITE, being either:

- A provisional response initiated by the local resident service logic, or
- A pass-through provisional response from the B-Leg in a back-to-back user agent role.

Note that 100 Trying does not count as a provisional response for this purpose.

In this case:

- This Response may contain SDP content as described in the SDP Compliance section.
- This Response will contain an ISUP Address Complete (ACM) message in the content.

The ACM message will be encoded as per Q.763 [R-26] Table 21, with the following notes.

Field	Encoding	Notes
Message Type	Fixed 1 Octet	6 = Indicates ACM
Backward Call Indicators	Fixed 2 Octets	Constructed as follows.
.End-to-End Method	2 bits	Constant = 0 (None)
.Called Party Status	2 bits	Constant = 1 (Ordinary Subscriber)
.Called Party Category	2 bits	Constant = 0 (None)
.Charge	2 bits	Globally Configured, Default = 2 (Charge)
.SCCP Method	2 bits	Constant = 0 (None)
.Echo Control Device	1 bit	Constant = 0 (None)
.ISDN Access	1 bit	Constant = 0 (non-ISDN)
.Holding	1 bit	Constant = 0 (Not Requested)
.ISDN User Part	1 bit	Constant = 1 (Used All The Way)
.End-to-End Information	1 bit	Constant = 0 (None)
.Interworking	1 bit	Constant = 0 (None)
[Optional Parameters]	[Various]	None. No optional parameters will be present.

*Table 82: Inbound A-Leg SIP INVITE Transaction (First Provisional Response) ISUP ACM Message*

Note that this ACM is constructed from scratch by the N2SIP stack and is not a pass-through of the ISUP ACM (if any) which may have been received on the B-Leg.

#### 4.2.2.3 Inbound A-Leg SIP-I INVITE Transaction (Subsequent 1XX Provisional Response, CPG)

This is the case where the N2SIP stack receives an inbound A-Leg SIP INVITE Request with ISUP IAM, and determines that it will send a second or subsequent provisional (101-199) response to that A-Leg INVITE, being either:

- A subsequent provisional response initiated by the local resident service logic, or
- A pass-through subsequent provisional response from the B-Leg in a back-to-back user agent role.

Note that 100 Trying does not count as a provisional response for this purpose.

In this case:

- This Response may contain SDP content as described in the SDP Compliance section.
- This Response will contain an ISUP Call Progress (CPG) message in the content.

The CPG message will be encoded as per Q.763 [R-26] Table 23, with the following notes.

Field	Encoding	Notes
Message Type	Fixed 1 Octet	44 = Indicates CPG
Event Information	Fixed 1 Octet	Constructed as follows.
.Event Presentation Restricted Indicator	1 bit	Constant = 0 (No Indication)
.Event Indicator	7 bits	Set to either: 1 (Alerting) if the SIP Provisional Response Code = 180 2 (Progress) for any other SIP Provisional Response Code
[Optional Parameters]	[Various]	None. No optional parameters will be present.

*Table 83: Inbound A-Leg SIP INVITE Transaction (Subsequent Provisional Response) ISUP CPG Message*

Note that this CPG is constructed from scratch by the N2SIP stack and is not a pass-through of any ISUP CPG (if any) which may have been received on the B-Leg.

#### 4.2.2.4 Inbound A-Leg SIP-I INVITE Transaction (200 OK Response after Provisional, ANM)

This section describes the ISUP content for a 200 OK response (or other 200-299 success response code if applicable) generated by the N2SIP framework in the case where N2SIP has already sent a preceding provisional INVITE Response (i.e. SIP 101-199 Response code) on that A-Leg.

Note that 100 Trying does not count as a provisional response for this purpose.

In this case when the N2SIP framework sends a 200 OK SIP INVITE Response on the A-Leg not as the first response (i.e. is sent after one or more preceding provisional responses), then:

- This Response may contain SDP content as described in the SDP Compliance section.
- This Response will contain ISUP Answer (ANM) message in the content.

The ANM message will be encoded as per Q.763 [R-26] Table 27, with the following notes.

Field	Encoding	Notes
Message Type	Fixed 1 Octet	9 = Indicates ANM
[Optional Parameters]	[Various]	None. No optional parameters will be present.

*Table 84: Inbound A-Leg SIP INVITE Transaction (200 OK Response after Provisional) ISUP ANM Message*

Note that this ANM is constructed from scratch by the N2SIP stack and is not a pass-through of the ISUP ANM (if any) which may have been received on the B-Leg.

### 4.3 Outbound B-Leg SIP-I INVITE Transaction

The N2SIP framework will also use SIP-I for some outbound B-Leg SIP INVITE Requests.

This will be done when performing an outbound back-to-back user agent B-Leg on behalf of an inbound A-Leg which itself used SIP-I, i.e. where the A-Leg inbound SIP INVITE Request contained an ISUP Initial Address Message (IAM).

#### 4.3.1 Outbound B-Leg SIP-I INVITE Request (IAM)

In the case where N2SIP performs an outbound B-Leg SIP INVITE Request as a back-to-back B-Leg related to an inbound SIP-I Call/Dialog, then that B-Leg Call/Dialog will also be performed as SIP-I for the INVITE Transaction and the associated BYE transaction.

Specifically:

- e) The outbound B-Leg SIP-I INVITE Request will contain a single ISUP part.
- f) The ISUP part will be an ISUP Initial Address (IAM) Message.

The IAM Message will be encoded as per Q.763 [R-26] Table 32, with the following notes.

Field	Encoding	Notes
Message Type	Fixed 1 Octet	1 = Indicates IAM
Nature of Connection Indicators	Fixed 1 Octet	Copied from the inbound A-Leg IAM.
Forward Call Indicators	Fixed 2 Octets	Copied from the inbound A-Leg IAM.
Calling Party's Category	Fixed 1 Octet	Copied from the inbound A-Leg IAM.
Transmission Medium Requirement	Fixed 1 Octet	Copied from the inbound A-Leg IAM.
Called Party Number	Mandatory Variable	Encoded according to Q.763 Figure 10. Digits will be the new called party as per the SIP "To" URI user. NoA will be derived from digits using denormalization rules. NPI will be set to 1 (E.164). INN will be set to 0 (allowed).
Calling Party Number	Optional Variable Tag = 10	Copied from the inbound A-Leg IAM.
<other>	Other Tags	Copied from the inbound A-Leg IAM.

*Table 85: Outbound B-Leg SIP INVITE Request ISUP IAM Message*

### 4.3.2 Outbound B-Leg SIP-I INVITE Responses

The following possible SIP INVITE Response cases are supported when receiving INVITE responses for any outbound SIP-I B-Leg.

#### 4.3.2.1 Immediate 200 OK Response (CON)

This section describes the ISUP content for a 200 OK response (or other 200-299 success response code if applicable) received by the N2SIP framework in the case where no provisional INVITE Response (i.e. no SIP 101-199 Response code) is received on that B-Leg.

Note that 100 Trying does not count as a provisional response for this purpose.

In this case when the N2SIP framework receives a 200 OK SIP INVITE Response on the B-Leg as the first response (without preceding provisional response), then:

- This Response may contain SDP content as described in the SDP Compliance section.
- This Response may contain ISUP Connect (CON) message in the content.
- Presence of any other ISUP message in the content is an error.
- A malformed ISUP message is an error.

The CON message will be decoded as per Q.763 [R-26] Table 27.

Field	Encoding	Notes
Message Type	Fixed 1 Octet	7 = Indicates CON
Backward Call Indicators	Fixed 2 Octets	Ignored.
[Optional Parameters]	[Various]	Accepted but ignored.

*Table 86: Outbound B-Leg SIP INVITE Transaction (Immediate 200 OK Response) ISUP CON Message*

#### 4.3.2.2 First 1XX Provisional Response (ACM)

This is the case where the N2SIP stack receives the first provisional (101-199) response to an outgoing B-Leg INVITE for which the original SIP INVITE Request sent by N2SIP included an ISUP IAM.

Note that 100 Trying does not count as a provisional response for this purpose.

In this case:

- This Response may contain SDP content as described in the SDP Compliance section.
- This Response may contain an ISUP Address Complete (ACM) message in the content.
- Presence of any other ISUP message in the content is an error.
- A malformed ISUP message is an error.

The ACM message will be decoded as per Q.763 [R-26] Table 21, with the following notes.

Field	Encoding	Notes
Message Type	Fixed 1 Octet	6 = Indicates ACM
Backward Call Indicators	Fixed 2 Octets	Ignored.
[Optional Parameters]	[Various]	Accepted but ignored.

*Table 87: Outbound B-Leg SIP INVITE Transaction (First Provisional Response) ISUP ACM Message*

#### 4.3.2.3 Subsequent 1XX Provisional Response (CPG)

This is the case where the N2SIP stack receives a provisional (101-199) response to an outgoing B-Leg INVITE for which the original SIP INVITE Request sent by N2SIP included an ISUP IAM, and where a previous provisional (101-199) response for that B-Leg INVITE with ISUP ACM in the content has already been received.

Note that 100 Trying does not count as a provisional response for this purpose.

In this case:

- This Response may contain SDP content as described in the SDP Compliance section.
- This Response may contain an ISUP Call Progress (CPG) message in the content.
- Presence of any other ISUP message in the content is an error.
- A malformed ISUP message is an error.

The CPG message will be decoded as per Q.763 [R-26] Table 23, with the following notes.

Field	Encoding	Notes
Message Type	Fixed 1 Octet	44 = Indicates CPG
Event Information	Fixed 1 Octet	Ignored
[Optional Parameters]	[Various]	Accepted but ignored.

*Table 88: Outbound B-Leg SIP INVITE Transaction (Subsequent Provisional Response) ISUP CPG Message*

#### 4.3.2.4 200 OK Response after Provisional (ANM)

This section describes the ISUP content for a 200 OK response (or other 200-299 success response code if applicable) received by the N2SIP framework in the case where one or more preceding provisional INVITE Responses (i.e. SIP 101-199 Response code) were received on that B-Leg.

Note that 100 Trying does not count as a provisional response for this purpose.

In this case when the N2SIP framework receives a 200 OK SIP INVITE Response on the A-Leg not as the first SIP-I response (i.e. is sent after one or more preceding provisional responses containing ISUP content), then:

- This Response may contain SDP content as described in the SDP Compliance section.
- This Response will contain ISUP Answer (ANM) message in the content.
- Presence of any other ISUP message in the content is an error.
- A malformed ISUP message is an error.

The ANM message will be decoded as per Q.763 [R-26] Table 27, with the following notes.

Field	Encoding	Notes
Message Type	Fixed 1 Octet	9 = Indicates ANM
[Optional Parameters]	[Various]	Accepted but ignored.

*Table 89: Outbound B-Leg SIP INVITE Transaction (200 OK Response after Provisional) ISUP ANM Message*



#### 4.4 Inbound SIP-I BYE Transaction

The N2SIP framework will accept inbound SIP BYE Requests (on any leg) which contain an “application/ISUP” content subject to the content encoding limitations described in section 4.1: *SIP-I Content Encoding (SDP and/or ISUP)*. The presence of the ISUP part in the BYE Request is treated as follows.

##### 4.4.1 Inbound SIP-I BYE Request

The following limitations apply.

- Only a single “application/ISUP” content part may be present.
- The ISUP part must be an ISUP Release (REL) message.

Any other ISUP message type present in the inbound SIP BYE Request may generate a warning. Failure to decode the REL message will mean that the RLC Message will not be sent in the 200 OK BYE Response.

The REL message will be decoded as per Q.763 [R-26] Table 33, with the following notes.

Field	Encoding	Notes
Message Type	Fixed 1 Octet	12 = Indicates REL
Cause Indicators	Mandatory Variable	Ignored.
<other>	Optional Tags	Accepted but ignored.

Table 90: Inbound SIP BYE Request ISUP REL Message

##### 4.4.2 Inbound SIP-I BYE Request (200 OK Response)

This section describes the ISUP content for a 200 OK Response generated by the N2SIP framework in the following case:

- The inbound SIP BYE Request contained an acceptable ISUP REL message.

In this case, when the N2SIP framework sends a 200 OK SIP BYE Response.

- This will contain an ISUP Release Complete (RLC) message in the SIP BYE Response content.

Note that the decision to send an RLC message in the SIP BYE Response is activated by the presence of the REL message in the received SIP BYE Request. In practice, this will always occur in relation to a call/dialog which contained ISUP in the original INVITE Request/Response.

The RLC message will be encoded as per Q.763 [R-26] Table 34, with the following notes.

Field	Encoding	Notes
Message Type	Fixed 1 Octet	16 = Indicates RLC

Table 91: Inbound SIP BYE Request (200 OK Response) ISUP RLC Message

## 4.5 Outbound SIP-I BYE Transaction

When initiating end-of-dialog for a call/dialog which is being treated as “SIP-I” (i.e. any call where the initial SIP INVITE contained ISUP message/s) then the SIP BYE Request sent by N2SIP will contain an ISUP Release (REL) message.

### 4.5.1 Outbound SIP-I BYE Request

When N2SIP sends SIP BYE Request for a call being treated as SIP-I, then:

- This will contain an ISUP Release (REL) message in the SIP BYE Request content.

The REL message will be encoded as per Q.763 [R-26] Table 33.

Field	Encoding	Notes
Message Type	Fixed 1 Octet	12 = Indicates REL
Cause Indicators	Fixed 2 Octets	Constructed with a static value.
.Last Octet	1 bit	Flag 1 = Last Bit
.Coding Standard	2 bits	Constant = 0 (ITU-T Coding)
.Cause Location	4 bits	Constant = 10 (Network beyond interworking point BI)
.Last Octet	1 bit	Flag 1 = Last Bit
.Cause Indicator	7 bits	Constant = 16 (Normal call clearing)

*Table 92: Outbound SIP BYE Request ISUP REL Message*

### 4.5.2 Outbound SIP-I BYE Request (Any Response)

After sending an outbound SIP BYE Request with an ISUP REL message, the N2SIP framework will accept an ISUP RLC message in the response.

- Only a single “application/ISUP” content part may be present.
- The ISUP part must be an ISUP Release Complete (RLC) message.

Any other ISUP message type present in the received Response to the Outbound SIP BYE Request may generate a warning.

The RLC message will be decoded as per Q.763 [R-26] Table 33.

Field	Encoding	Notes
Message Type	Fixed 1 Octet	16 = Indicates RLC
<other>	Optional Tags	Accepted but ignored.

*Table 93: Outbound SIP BYE Request (Any Response)*

## 5 SDP Compliance

### 5.1 SDP Overview

The N2SIP framework uses SDP for three distinct purposes.

- a) Passthrough of SDP between A-Leg and B-Leg, operating as a back-to-back user agent.
- b) Negotiation of SDP for local RTP generated by N2SIP and sent to the A-Leg only.
- c) Negotiation of SDP to suspend RTP during periods where no stream is available.

In case (a) then N2SIP will examine the passed-through SDP for the purpose of recording the “preferred” media codec, but does not apply any modification to the SDP other than A-Leg SDP Normalisation described in section 5.4: SDP Normalisation (A-Leg). In this case N2SIP does not sit within the RTP path and will never proxy or transcode any RTP packets. The IP addresses contained in the SDP Offer/Answer will always be the A-Leg and B-Leg IP addresses.

In case (b) where N2SIP is the endpoint generating an RTP stream to the A-Leg then the SDP scope will be limited to the RTP endpoint capabilities of N2SIP as described in section 6.4: RTP Endpoint Capabilities. N2SIP will provide its own IP address and will generate and accept RTP packets subject to the specified limitations.

In case (c) when N2SIP is not generating RTP and there is no B-Leg endpoint, then N2SIP will construct an “suspended” SDP Offer for the purpose of notifying the A-Leg that RTP is not currently active. This occurs when changing from one B-Leg to another, or when changing from a B-Leg to or from a locally generated RTP stream. N2 will provide a configured IP address (which may be “0.0.0.0”) but will not generate or accept any RTP packets while the RTP stream is suspended.

### 5.2 SDP Patterns (RFC 6337)

N2SIP supports only a subset of the RFC 6337 [R-24] patterns (Table 1). The term “INVITE” here refers only to the SIP INVITE which initiates a dialog, except where re-INVITE is specifically stated.

#### A-Leg Incall (N2SIP receives SIP INVITE Request)

Pattern	Offer	Answer
1	INVITE Request	2xx INVITE Response
2	2xx INVITE Response	ACK Request
3	INVITE Request	1xx-rel INVITE Response (Early Media)
1	Re-INVITE Request	2xx re-INVITE Response.

Table 94: Supported SDP Patterns (A-Leg Incall)

#### A-Leg Outcall (N2SIP sends SIP INVITE Request)

Pattern	Offer	Answer
2	2xx INVITE Response	ACK Request
1	Re-INVITE Request	2xx re-INVITE Response.

Table 95: Supported SDP Patterns (A-Leg Outcall)

**B-Leg Outcall (N2SIP sends SIP INVITE Request)**

Pattern	Offer	Answer
1	INVITE Request	2xx INVITE Response
2	2xx INVITE Response	ACK Request
3	INVITE Request	1xx-rel INVITE Response (Early Media)
1	Re-INVITE Request	2xx re-INVITE Response.

*Table 96: Supported SDP Patterns (B-Leg Outcall)*

Whenever SDP is included in the Content of any SIP Request or Response, either:

- a) The top-level Content-Type header must be present as “application/sdp”, or
- b) The top-level Content-Type must be “multipart/mixed” and the content must contain a content part with Content-Type “application/sdp”.

**5.3 SDP Use-Case Details**

Within the above theoretical capabilities of the SDP codec, there exists a specific sub-set of use-case scenarios where the N2SIP framework will create, process, or pass-through SDP session definitions.

For SDP Pattern definitions, see RFC 6337 [R-24].

Note: N2SIP does not currently offer any support for Pattern 4 (offer in 1xx INVITE Response), or Pattern 5 (offer in PRACK Request), nor Pattern 6 (offer in UPDATE Request) scenarios.

**5.3.1 B-Leg Termination (With SDP Offer after A-Leg Incall)**

The N2SIP framework will perform termination attempts to establish an outgoing B-Leg using an outbound SIP INVITE Request. This includes the case where a temporary B-Leg is being established for the purpose of bridging to an external IVR platform for audio interaction.

Where an A-Leg SDP Offer has been provided prior to the attempt to the new B-Leg, then:

- N2SIP will use Pattern 1 or 3 to the B-Leg.
- N2SIP will use Pattern 1 or 3 to the A-Leg if possible, or Pattern 1 re-INVITE otherwise.

The following tables provide a full breakdown of this behavior.

Firstly, when the A-Leg provided an SDP Offer according to Pattern 1 (or Pattern 3), i.e. where the A-Leg SDP Offer was provided in original SIP INVITE Request:

A-Leg Set-up	B-Leg Behavior	A-Leg Follow-up
Incall A-Leg sent SDP Offer to N2SIP in SIP INVITE Request. A-Leg Pattern 1 or 3 <i>Case: No final A-Leg INVITE Response has been sent.</i>	N2SIP relays A-Leg SDP Offer to B-Leg in SIP INVITE Request. <i>Case: B-Leg returns SDP Answer in 2xx INVITE Response.</i> B-Leg Pattern 1	N2SIP relays B-Leg SDP Answer in 2xx INVITE Response to A-Leg. A-Leg Pattern 1

(as above)	N2SIP relays A-Leg SDP Offer to B-Leg in SIP INVITE Request. <i>Case: B-Leg returns SDP Answer in 1xx INVITE Response.</i> B-Leg Pattern 3	N2SIP relays B-Leg SDP Answer in 1xx INVITE Response to A-Leg. A-Leg Pattern 3
(as above, except...) <i>Case: Final A-Leg INVITE Response has been sent due to previous activity.</i>	N2SIP relays A-Leg SDP Offer to B-Leg in SIP INVITE Request. <i>Case: B-Leg returns SDP Answer in 2xx INVITE Response.</i> B-Leg Pattern 1	N2SIP uses A-Leg re-INVITE to relay B-Leg SDP Answer to A-Leg [†Note]. A-Leg Pattern 1 (re-INVITE)
(as above)	N2SIP relays A-Leg SDP Offer to B-Leg in SIP INVITE Request. <i>Case: B-Leg returns SDP Answer in 1xx INVITE Response.</i> B-Leg Pattern 3	N2SIP uses A-Leg re-INVITE to relay B-Leg SDP Answer to A-Leg [†Note]. A-Leg Pattern 1 (re-INVITE)

Table 97: B-Leg Termination SDP Cases (Incall A-Leg with SDP Offer in INVITE Request)

†Note: In these scenarios, the B-Leg has provided an SDP Answer to N2SIP. However, the SIP User Agent state machine on the A-Leg is no longer able to accept an SDP Answer. Instead, N2SIP must use a re-INVITE to the A-Leg to provide the B-Leg SDP Answer to the A-Leg as an SDP Offer.

In such cases then:

- The B-Leg SDP Answer from the INVITE (provisional or final) Response is provided to the A-Leg as an SDP Offer in a re-INVITE Request.
- The A-Leg must accept this re-INVITE Request with a re-INVITE 200 Response. If the A-Leg rejects the re-INVITE Request, then this is treated as an unrecoverable error on the call.
- The A-Leg will provide an SDP Answer in the re-INVITE 200 Response. There is no available supported mechanism for providing this A-Leg SDP Answer content back to the B-Leg.

Because there is no mechanism for returning this A-Leg SDP Answer back to the B-Leg in this scenario, it is necessary to make some assumptions that this will not cause problems in the SDP negotiation. Specifically N2SIP must assume that:

- The A-Leg returning a re-INVITE 200 Response means that it has fully accepted the SDP Answer (presented as Offer), and
- the content of the SDP Answer contained in the re-INVITE 200 Response is a simple confirmation of the Offer, and
- the SDP Answer provided by the A-Leg does not modify the RTP port number, IP address, or any codec parameters in such a way that the RTP stream becomes inoperable.

### 5.3.2 B-Leg Termination (With SDP Offer after A-Leg Outcall)

A-Leg Outcall has the following approach:

A-Leg Set-up	B-Leg Behavior	A-Leg Follow-up
<p>N2SIP outcall (never supplies SDP Offer) to A-Leg using SIP INVITE Request.</p> <p>A-Leg must provide SDP Offer in 2xx INVITE Response. No other behavior is supported by N2SIP.</p> <p>N2SIP provides placeholder (inactive) SDP Answer in 2xx ACK Request.</p> <p>A-Leg Pattern 2</p>	<p>N2SIP relays A-Leg SDP Offer to B-Leg in SIP INVITE Request.</p> <p><i>Case: B-Leg returns SDP Answer in 2xx INVITE Response.</i></p> <p>B-Leg Pattern 1</p>	<p>N2SIP uses A-Leg re-INVITE to relay B-Leg SDP Answer to A-Leg [†Note].</p> <p>A-Leg Pattern 1 (re-INVITE)</p>
	<p>N2SIP relays A-Leg SDP Offer to B-Leg in SIP INVITE Request.</p> <p><i>Case: B-Leg returns SDP Answer in 1xx INVITE Response.</i></p> <p>B-Leg Pattern 3</p>	<p>N2SIP uses A-Leg re-INVITE to relay B-Leg SDP Answer to A-Leg [†Note].</p> <p>A-Leg Pattern 1 (re-INVITE)</p>

Table 98: B-Leg Termination SDP Cases (Outcall A-Leg)

[†Note] See the corresponding [†Note] in section 5.3.1: B-Leg Termination (With SDP Offer after A-Leg Incall).

### 5.3.3 B-Leg Termination (without A-Leg SDP Offer)

N2SIP may also be requested to perform an outbound B-Leg termination attempt without having yet received an SDP Offer from the A-Leg. I.e. when an incall A-Leg to N2SIP has initiated Pattern 2 (late offer) SIP INVITE Request without SDP but not yet completed the pattern.

In these cases, Pattern 2 will also be used on the B-Leg.

N2SIP does not support Pattern 4 (or Pattern 5) on either leg.

A-Leg Set-up	B-Leg Behavior	A-Leg Follow-up
<p>Incall A-Leg sent SIP INVITE Request to N2SIP without SDP Offer content.</p> <p>A-Leg Pattern 2</p> <p><i>Case: No final A-Leg INVITE Response has been sent.</i></p>	<p>N2SIP sends SIP INVITE Request to B-Leg without SDP Offer.</p> <p>B-Leg Pattern 2</p> <p>B-Leg must provide SDP Offer in 2xx INVITE Response. No other behavior is supported by N2SIP.</p>	<p>N2SIP provides SDP Offer in 2xx INVITE Response to A-Leg.</p> <p>A-Leg Pattern 2</p>

<p>Incall A-Leg sent SIP INVITE Request to N2SIP without SDP Offer content.</p> <p>A-Leg Pattern 2</p> <p><i>Case: Final A-Leg INVITE Response has been sent due to previous activity.</i></p>	<p>N2SIP sends SIP INVITE Request to B-Leg without SDP Offer.</p> <p>B-Leg Pattern 2</p> <p>B-Leg must provide SDP Offer in 2xx INVITE Response. No other behavior is supported by N2SIP.</p>	<p>N2SIP uses A-Leg re-INVITE to relay B-Leg SDP Offer to A-Leg.</p> <p>A-Leg Pattern 1 (re-INVITE)</p>
--	---	---

Table 99: B-Leg Termination SDP Cases (Incall A-Leg SIP INVITE Request without SDP)

## 5.4 SDP Normalisation (A-Leg)

When performing passthrough INVITE call control, SDP is “copied” from a Request or Response on one Leg into a Request or Response on the other Leg.

One single A-Leg session may receive SDP copied from more than one distinct B-Leg session or internally generated RTP stream, each of which is a standalone SDP session.

The SDP session towards the A-Leg must be presented as a single logical session, with consistent identifiers.

Hence:

1. Each B-Leg also has its own independent SDP Session.
2. The A-Leg SDP Session ID and Version are normalised – i.e. a single, coherent SDP Session is represented to the A-Leg which will conceal any B-Leg session ID changes.

## 5.5 SDP Inactive/Suspended

After first using SDP to negotiate the initial RTP audio stream between the A-Leg and the first connected B-Leg or local RTP audio stream, any follow-on call control (i.e. any change to a new B-Leg or local RTP stream) will require notifying the A-Party that the previous SDP session is no longer valid, and that momentarily there is no current stream active.

The SIP/SDP standards do not appear to explicitly define how this should be done in an interoperable manner.

N2SIP supports three different mechanisms for instructing the A-Party that there is currently no RTP stream during any period of leg control, follow-on hunting, etc. when no far-end RTP stream is applicable. The “suspend mechanism” to use is a set by a global configuration parameter in N2SIP. The mechanism cannot be controlled on a per-call basis.

The mechanisms are:

### 5.5.1 Suspended (No Host)

The “No Host” mechanism uses the following approach to construct a “suspended stream” SDP session description for the A-Party when no far-end RTP stream is applicable.

- The IP address is “0.0.0.0”.
- The RTP port number is a configured “suspended stream” port number (may be zero).

- The audio media payload type is the first (only) payload type from the most recently seen SDP Answer session description, or “PCMU/8000” if no SDP Answer has yet been seen.
- No telephony-event payload type will be present.

### 5.5.2 Suspended (No Media)

The “No Media” mechanism uses the following approach to construct a “suspended stream” SDP session description for the A-Party when no far-end RTP stream is applicable.

- The IP address is a configured “suspended stream host IP” (may be “0.0.0.0”).
- The RTP port number is a configured “suspended stream port number” (may be zero).
- No audio media payload type will be present.
- No telephony-event payload type will be present.

### 5.5.3 Suspended (Inactive)

The “Inactive” mechanism uses the following approach to construct a “suspended stream” SDP session description for the A-Party when no far-end RTP stream is applicable.

- The IP address is a configured “suspended stream host IP” (may be “0.0.0.0”).
- The RTP port number is a configured “suspended stream port number” (may be zero).
- The audio media payload type is the first (only) payload type from the most recently seen SDP Answer session description, or “PCMU/8000” if no SDP Answer has yet been seen.
- This audio media stream will have the “inactive” attribute specified.
- No telephony-event payload type will be present.

## 5.6 SDP Security

N2SIP does not support encryption or signing of the SDP content in any form. Specifically:

- SRTP is not supported.
- Encryption Keys (k=) are not supported.
- SIP S/MIME encapsulation of SDP is not supported.
- SIP TLS is not supported.

## 5.7 SDP Fields

### 5.7.1 Base Fields

The following compliance is implemented for SDP Fields.

Field	Inbound Offer/Answer	Outbound Answer/Offer	Passthrough
v (Version)	Must be 0	0	Yes
o (Origin)	Must be Present	Present	Yes
.Username	Ignored	Configured value of “sdp_owner_username”	Yes
.Session ID	Ignored	Auto-Generated Value	Replaced
.Session Version	Ignored	Auto-Generated Value	Replaced
.Net Type	Must be "IN"	"IN"	"IN"
.Address Type	Must be "IP4"	"IP4"	"IP4"



Field	Inbound Offer/Answer	Outbound Answer/Offer	Passthrough
.Unicast Address	Ignored	Configured value of "sdp_owner_host" or "sdp_suspend_host".	Yes
s (Session Name)	Ignored	""	Yes
i (Session Info)	Ignored	Not Present	Yes
u (URI)	Ignored	Not Present	No
e (Email Address)	Ignored	Not Present	No
p (Phone Number)	Ignored	Not Present	No
c (Connection Data)	Must be Present	Present	Yes
.Net Type	Must be "IN"	"IN"	"IN"
.Address Type	Must be "IP4"	"IP4"	"IP4"
.Connection Address	Far-End URL for RTP Multicast Not Supported TTL Not Supported	Local URL for RTP May be "0.0.0.0" or configured value of "sdp_suspend_host" when suspending the A-Leg. Multicast Not Present TTL Not Present	Yes
b (Bandwidth)	Ignored	Not Present	Yes
t (Start Time)	Ignored	0	0
t (End Time)	Ignored	0	0
r (Repeat Times)	Ignored	Not Present	No
z (Time Zones)	Ignored	Not Present	No
k (Encryption)	Ignored	Not Present	No
m (Media Descriptions)	A media description must exist for media "audio". Other media descriptions are ignored.	A single media description is usually present, as below. May only be absent when suspending the A-Leg.	Yes
.Media	Ignore all except "audio".	"audio"	Yes
.Port	Far-End UDP Port for RTP	Local UDP Port for RTP. Will be the configured "sdp_suspend_inactive_port" when suspending the A-Leg.	Yes
.Proto	Must be "RTP/AVP"	"RTP/AVP"	"RTP/AVP"
.Format	Ignore all except: <ul style="list-style-type: none"> <li>• 0 (PCMU/8000),</li> <li>• 8 (PCMA/8000)</li> <li>• "AMR/8000"</li> <li>• "AMR-WB/16000"</li> <li>• "telephone-event"</li> </ul>	For Answer, depends on offered format compatibility and configuration. For Offer, depends on configuration. In both cases may include: <ul style="list-style-type: none"> <li>• 0 ("PCMU/8000")</li> <li>• 8 ("PCMA/8000")</li> <li>• "AMR/8000"</li> <li>• "AMR-WB/16000"</li> <li>• "telephone-event"</li> </ul>	Yes

Field	Inbound Offer/Answer	Outbound Answer/Offer	Passthrough
a (SDP Attributes)	Ignore all except: <ul style="list-style-type: none"> <li>• 0 (PCMU/8000),</li> <li>• 8 (PCMA/8000)</li> <li>• "AMR/8000"</li> <li>• "AMR-WB/16000"</li> <li>• "telephone-event"</li> </ul>		Yes
.rtptime	May be present for 0 (PCMU/8000) and 8 (PCMA/8000). Must be present for: <ul style="list-style-type: none"> <li>• "AMR/8000"</li> <li>• "AMR-WB/16000"</li> <li>• "telephone-event"</li> </ul>	Present for all Offered or Accepted formats. Not Present for all others.	Yes
.fmtp	"telephone-event": Event codes 0-15 are accepted and usable. Events 16+ are accepted but silently discarded. "PCMU/8000" and "PCMA/8000": Offered attributes are silently discarded. "AMR/8000" and "AMR-WB/16000": As per <i>Table 101</i> .	"telephone-event": For Answer the inbound attribute will be returned unchanged if the format is Accepted. "AMR/8000" and "AMR-WB/16000": As per <i>Table 101</i> . Not Present for all others.	Yes
.ptime	May be present.	Not Present	Yes
.maxptime	May be present.	Not Present	Yes
.inactive	Ignored	May be present when suspending the A-Leg.	Yes
.recvonly	May be present.	Not present.	Yes
.sendonly	Ignored	Configurable option when using DTMF in out-of-band RTP for PCMU/8000 or PCMA/8000.	Yes
.sendrecv	May be present.	Present when not using "inactive" or "sendonly".	Yes

Table 100: SDP Field Compliance

All other non-recognised fields or SDP Attributes are ignored.

## 5.7.2 AMR and AMR-WB SDP Media Format Parameters

RFC 4867 [R-23] defines AMR and AMR-WB format parameters. Compliance is described in the following table.

Parameter Name	Inbound Offer/Answer	Outbound Offer	Outbound Answer	Comments
octet-align	May be present with value "0" or "1".	Two format parameter ("fmt") attributes are offered. The first contains "octet-align=1"; the second contains "octet-align=0".	Copied from Inbound Offer.	Both octet-aligned mode and bandwidth-efficient mode are accepted and supported for either inbound or outbound audio streams.
mode-set	May be present with any combination of valid modes.	Not present	Copied from Inbound Offer.	Mode restrictions are accepted for inbound audio streams, and applied to outbound audio streams.
mode-change-period	May be present with value "1" or "2".	"1"	Not present	Mode change restrictions are accepted for outbound audio streams. Mode change restrictions are not required for inbound audio streams.
mode-change-capability	May be present with value "1" or "2".	"2"	"2"	
mode-change-neighbor	"May be present with value "0" or "1".	"0"	Not present	
crc	May be present with value "0".	"0"	Copied from inbound offer.	Frame CRCs, robust payload sorting, and frame interleaving are not accepted or supported for either inbound or outbound audio streams.
robust-sorting	May be present with value "0".	"0"	Copied from inbound offer.	
interleaving	Must not be present.	Not present	Not present	
max-red	May be present with any valid value.	"0"	"0"	Frame redundancy is accepted for inbound audio streams, however redundant frames are discarded unused. Frame redundancy is not supported for outbound audio streams.
channels	May be present with value "1".	"1"	Copied from inbound offer.	Only mono (single channel) audio is supported for both inbound and outbound audio streams.

Table 101: AMR and AMR-WB Format Parameters

All other non-recognised parameters are ignored.

## 6 RTP Compliance

### 6.1 RTP Functional Scope

In any case N2SIP will never transcode or transit RTP packets.

N2SIP will only ever perform one of the following:

- Act as a SIP Back-to-back User Agent and pass-through SDP Offer and Answer between two third-party endpoints who will then exchange RTP media independently between themselves, without transiting N2SIP, or
- Act as an endpoint for a media stream in which N2SIP exchanges RTP directly with the A-Party for the purposes of playing an announcement and collecting input from the A-Party.

When acting as a back-to-back user agent, N2SIP does not place any limitations on the SDP negotiation of media codecs and capabilities which are negotiated between the A-Leg and the B-Leg.

When acting as an RTP endpoint, N2SIP supports a limited set of media codecs as described in the following section *6.4: RTP Endpoint Capabilities*.

### 6.2 RTP Transport

The RTP stream is negotiated in the Offer/Answer SDP interaction described above.

N2SIP supports:

- RTP over UDP
- RTP a=sendonly (mono-directional: N2SIP to soft-switch) or a=sendrecv (bi-directional).
- RTP audio payloads.
- RTP telephony event payloads.

N2SIP does not support encryption or signing of the RTP content in any form and does not support underlying transports other than UDP. Specifically:

- SRTP is not supported.
- RTP over TLS is not supported.
- RTP over TCP or SCTP is not supported.

N2SIP does not support monitoring of call quality:

- RTCP is not supported.

RTCP functionality may be disabled on the soft-switch to save resources.

### 6.3 RTP Security

N2SIP uses uncompressed, unencrypted, unsigned RTP for Audio Streaming.

## 6.4 RTP Endpoint Capabilities

This chapter outlines the supported capability of the N2SIP framework when it is acting as an RTP endpoint. I.e. when an N-Squared product such as N2IVR is constructing and emitting an RTP audio stream.

The following compliance is implemented for RTP packets:

RTP Field	Receive	Send
Version	Must be 2.	2
Padding	Supported	0 (Not Used)
Extension	Not Supported	0 (Not Used)
# CSRC	Ignored	0 (Not Used)
Marker	Ignored	1 if the payload contains AMR/8000 or AMR-WB/16000 audio, and the first frame in the payload is the first audio frame in a talkspurt (as per RFC 4867 [R-23]). Otherwise 0.
Payload Type	Must be one of: <ul style="list-style-type: none"> <li>• 0 (ITU-T REC G.711 PCMU/8000),</li> <li>• (ITU-T REC G.711 PCMA/8000), or</li> <li>• Dynamically mapped payload type for: <ul style="list-style-type: none"> <li>○ AMR/8000 (3GPP TS 26.073)</li> <li>○ AMR-WB/16000 (ITU-T REC G.722.2)</li> <li>○ Telephony Event (IETF RFC 4733)</li> </ul> </li> </ul>	One of: <ul style="list-style-type: none"> <li>• 0 (ITU-T REC G.711 PCMU/8000),</li> <li>• (ITU-T REC G.711 PCMA/8000), or</li> <li>• Dynamically mapped payload type for: <ul style="list-style-type: none"> <li>○ AMR/8000 (3GPP TS 26.073)</li> <li>○ AMR-WB/16000 (ITU-T REC G.722.2)</li> <li>○ Telephony Event (IETF RFC 4733)</li> </ul> </li> </ul>
Telephony Event Code	0-15 (Digits) – accepted and processed. 16 (Flash) – accepted and ignored. Other values – accepted and ignored.	Not Present

Table 102: RTP Packet Compliance

These RTP limitations will be represented in the SDP Offer or Answer which N2SIP generates to the A-Leg.

### 6.4.1 Audio Payloads

Audio packets are sent out when playing announcements.

Received audio packets are either:

- Discarded, or
- Partially decoded to detect AMR mode change requests, or
- Decoded and analyzed in real-time for DTMF audio events.

		Audio Format	
		AMR/8000 or AMR-WB/16000	Other
DTMF Detection	Inactive	Partial Decode	Discard
	Inband	Decode	Decode
	Telephony Event	Partial Decode	Discard
	SIP INFO	Partial Decode	Discard

Table 103: RTP Audio Payloads

Supported audio payload types are:

- PCMU/8000 (ITU-T REC G.711 uLaw 8kHz Mono)
- PCMA/8000 (ITU-T REC G.711 aLaw 8kHz Mono)
- AMR/8000 (3GPP TS 26.073 8kHz Mono)
- AMR-WB/16000 (ITU-T REC G.722.2 16kHz Mono)

Inband DTMF detection is supported for all supported payload types except AMR/8000.

#### 6.4.2 Event Payloads

Inbound event payloads are supported as per RFC 4733 [R-16].

- Event volume is ignored.

Outbound event payloads are not used.

## 7 SIP Scenarios

This chapter provides example call flows for some of the most common scenarios implemented by N-Squared products built on the N2SIP framework.

Not all scenarios are applicable to all products. This set of scenarios is far from exhaustive, since the products are highly configurable and in most cases the features can be customized using service scripts written in the Lua scripting language.

Note that for simplicity most of these the Message Flow diagrams in the following subsections indicate early SDP offer (RFC 6337 [R-24] pattern 1). Patterns 2 and 3 are also supported as specified in section 5: *SDP Compliance*.

### 7.1 Scenario: A-Leg Redirection

In this case, the service logic executing on N2SIP determines that the called party should be simply “translated” to another number – e.g. in the number portability lookup case. It sends a SIP Invite Response with status code 302.

The Response Contact header indicates the new (translated or prefixed) called party address.

The call is no longer under control of the N2SIP application. The SSP will perform call redirection.

N2SIP Script: Call Redirect (302 Moved Temporarily)

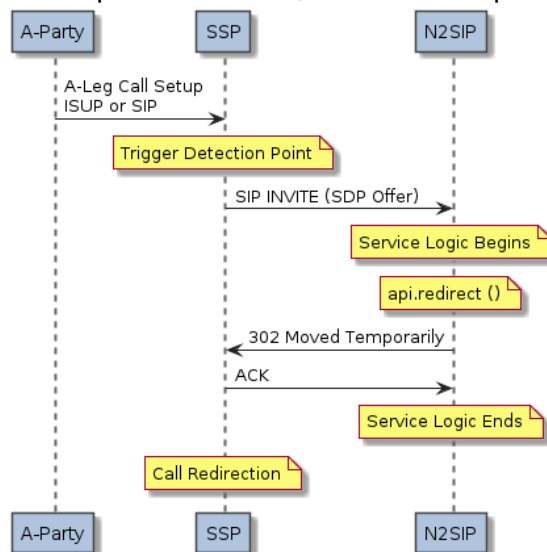


Figure N – N2SIP Flow: A-Leg Redirection

The service logic may not perform any further telephony actions.

## 7.2 Scenario: A-Leg Screening

In this case, the service logic executing on the N2SIP determines that the call is not permitted and should be dropped. It sends a SIP Invite Response with status code 470, or any other appropriate status code as may be desired.

The call is no longer under control of N2SIP. The SSP will perform call release, or other follow-on treatment.

**N2SIP Script: Call Screening (470 Consent Needed)**

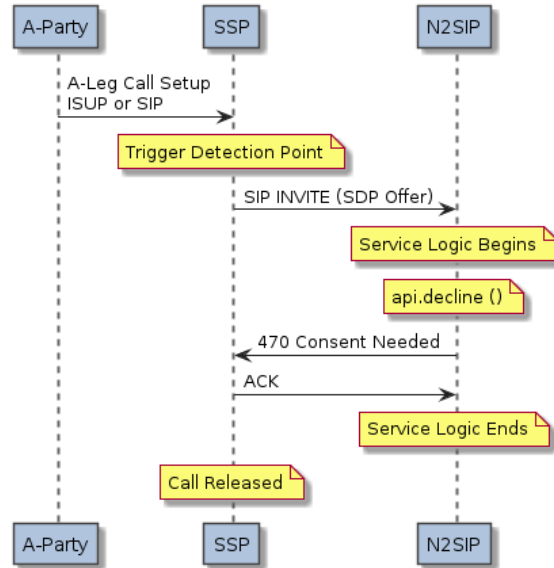


Figure O – N2SIP Flow: A-Leg Screening

The service logic may not perform any further telephony actions.



### 7.3 Scenario: Internal Announcement (Script, 200 OK)

This example shows an N2SIP service making use of the built-in “internal” media server capability to interact with the A-Leg. DTMF collection may be performed.

The flow shows the use of the internal media service from a local script, rather than INAP or VXML control. It uses a 200 OK INVITE Response to complete the speech path for the RTP stream.

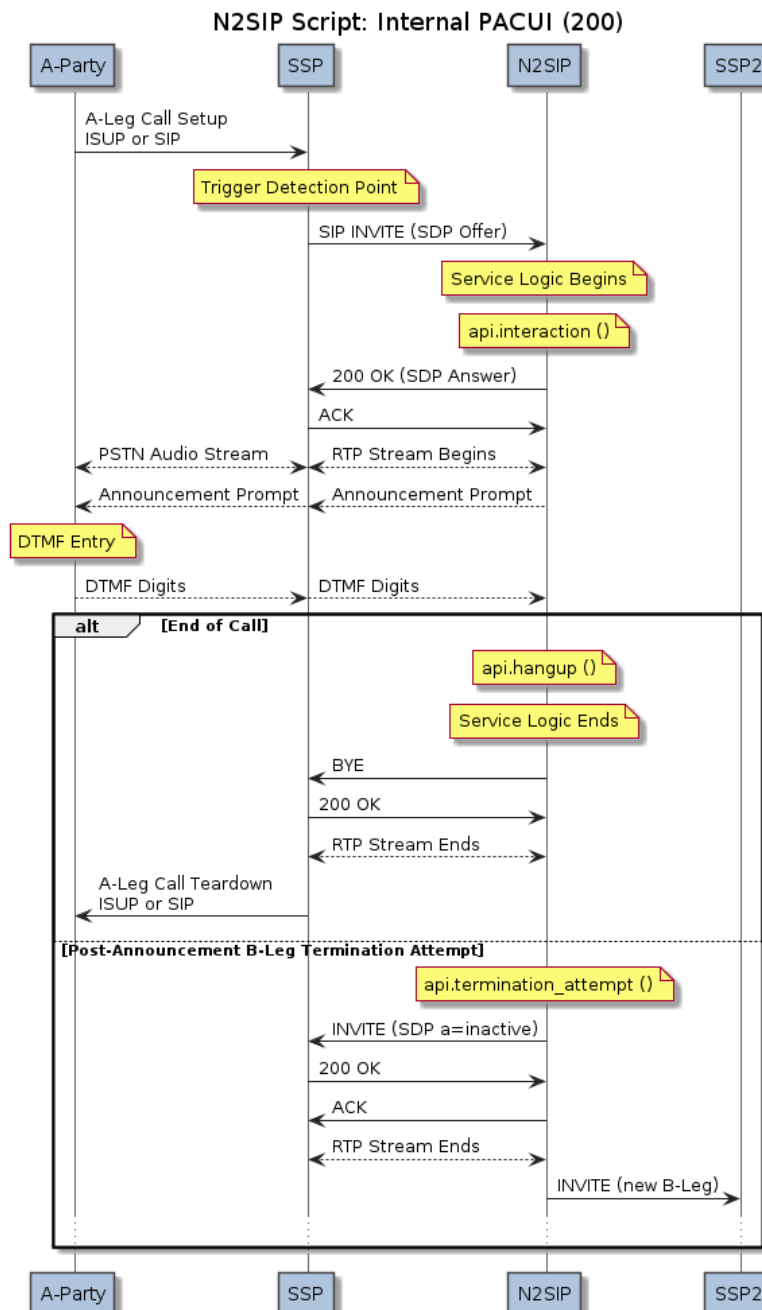


Figure P – N2SIP Flow: Internal Announcement (Script, 200 OK)

The service logic may subsequently perform any other valid SIP call control action, e.g.

- Hangup with BYE
- Internal Announcements
- B-Leg Termination Attempt or External Announcement

### 7.4 Scenario: Internal Announcement (Script, 183 Session Progress)

The example is like the proceeding, except that it uses the N2SIP capability to use Pattern 3 for the SDP Offer response, e.g. 183 Session Progress (early media) for the media setup.

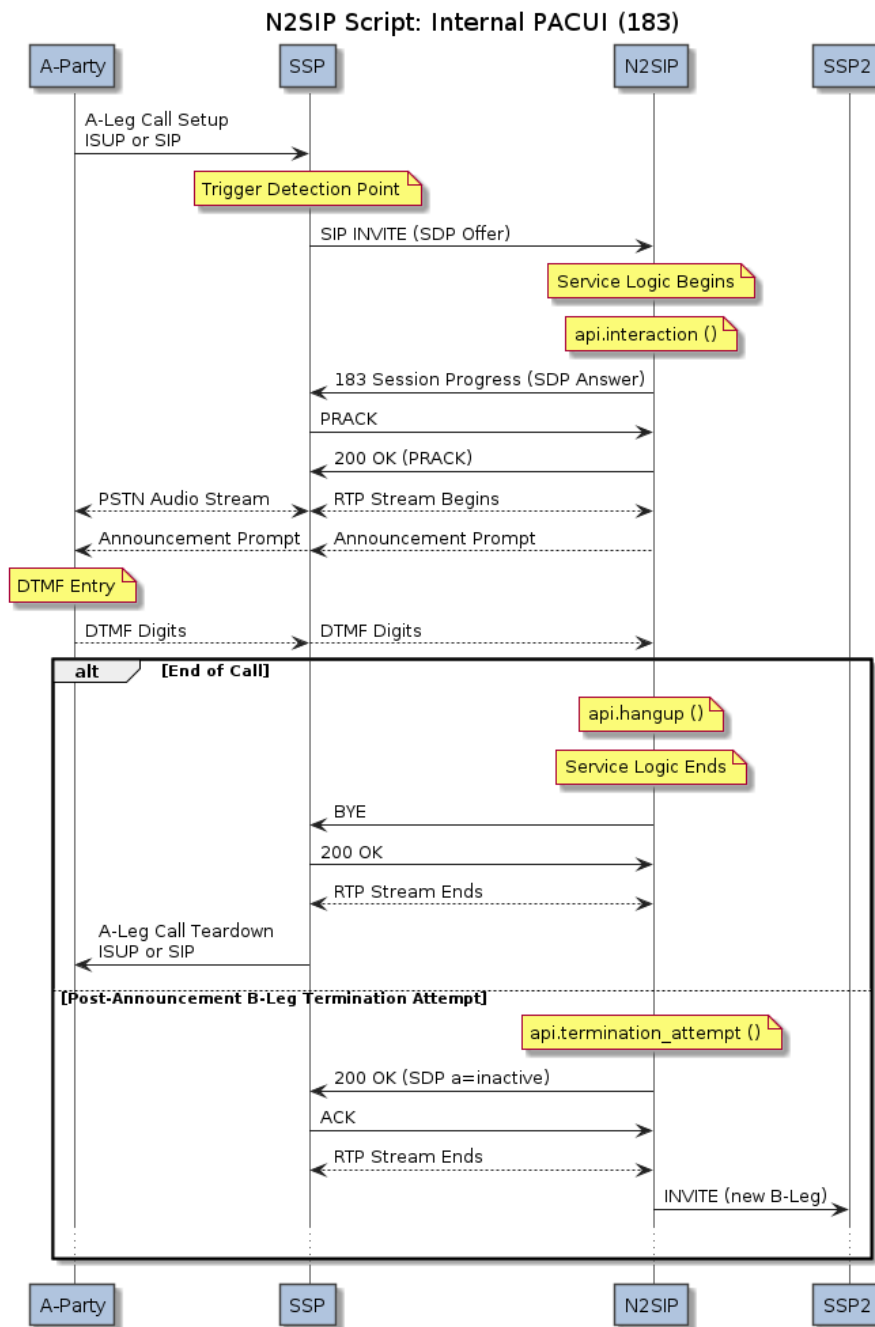


Figure Q – N2SIP Flow: Internal Announcement (Script, 183 Session Progress)

The service logic may subsequently perform any other valid SIP call control action, e.g.

- Final SIP INVITE Response with status code 300-699.
- Hangup with BYE
- Internal Announcements
- B-Leg Termination Attempt or External Announcement

### 7.5 Scenario: Internal Announcement (N2IVR INAP)

This flow is essentially identical to the “Internal Announcement (Script, 200 OK)” scenario, however it shows additional INAP messaging for an N2IVR scenario where the N2IVR is operating as an INAP Controlled IVR.

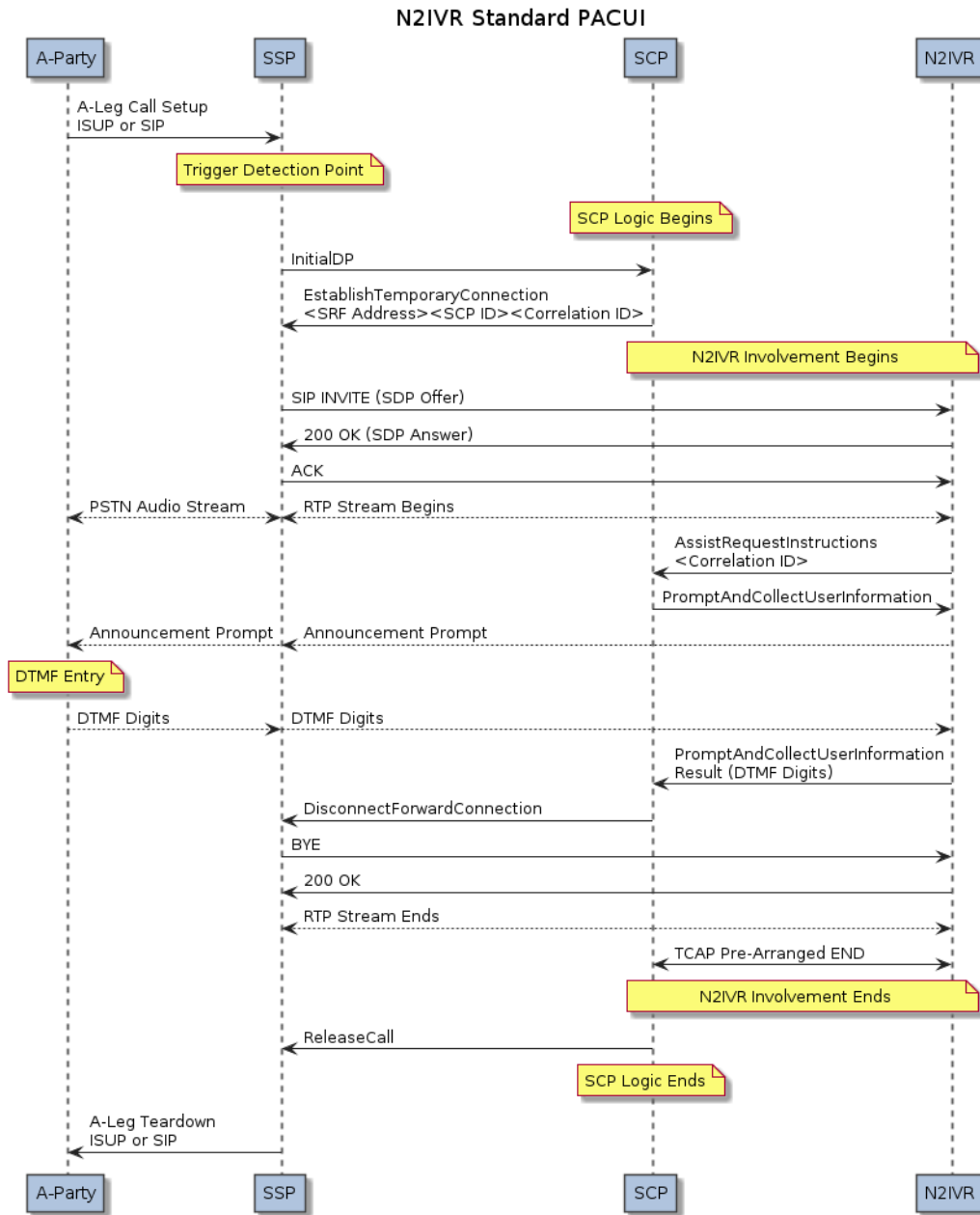


Figure R – N2SIP Flow: Internal Announcement (N2IVR INAP)

### 7.6 Scenario: External Announcement

Service logic in N2SIP may play announcements using an external INAP-controlled SRF. The temporary SRF B-Leg is established with an outbound SIP INVITE.

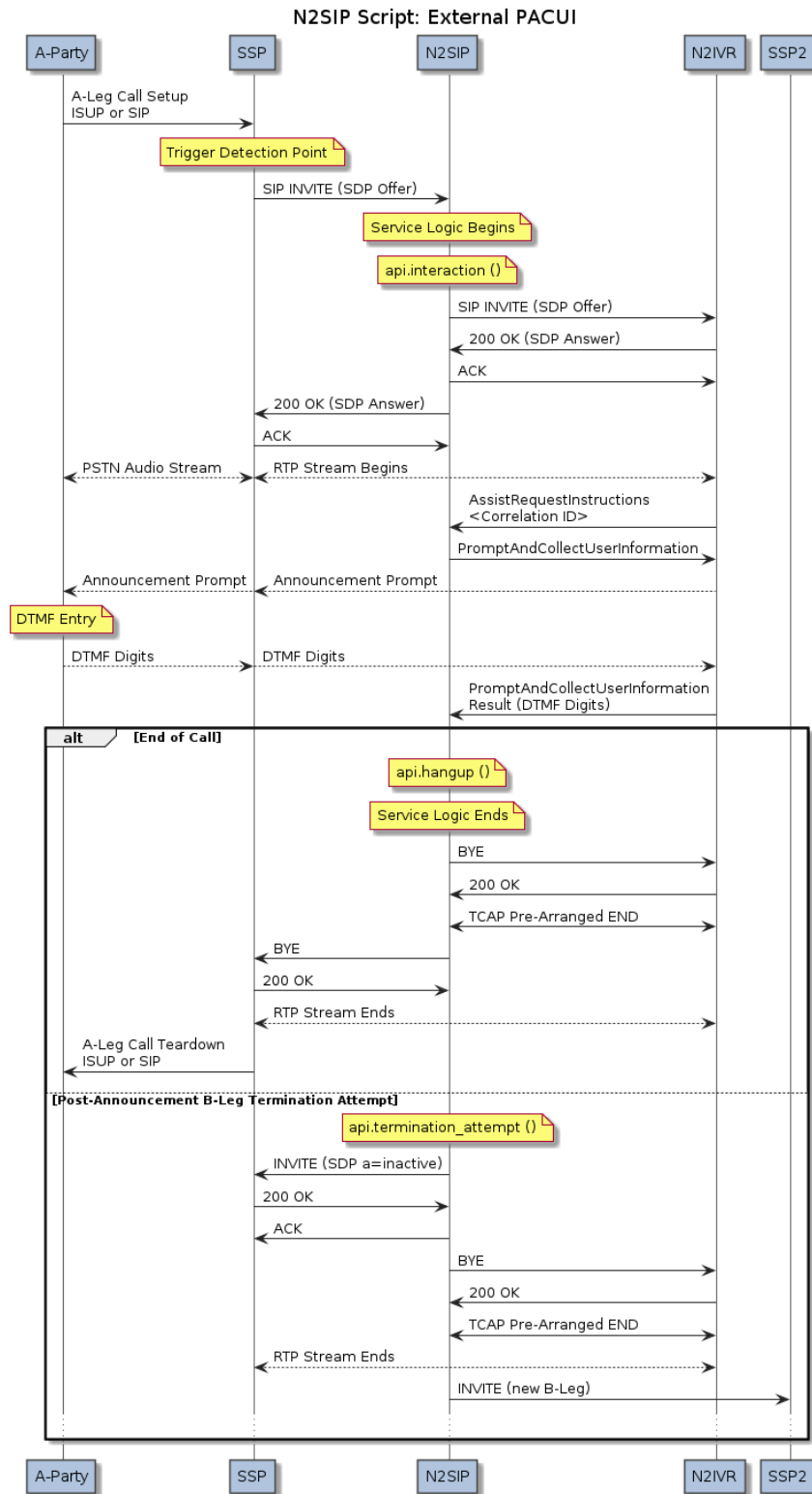


Figure S – N2SIP Flow: External Announcement

### 7.7 Scenario: B-Leg Termination Attempt

Service logic in N2SIP framework may attempt termination to external endpoints. The B-Leg is established with SIP INVITE. The A-Leg and B-Legs are joined with re-INVITE.

This flow shows a B-Leg hunting sequence with three attempts to terminate the B-Leg.

This Part 1 shows (a) a Busy result, and then (b) a No Answer where the N2SIP-controlled no-answer timer expires before the B-Leg returns a final response. The B-Leg is cancelled.

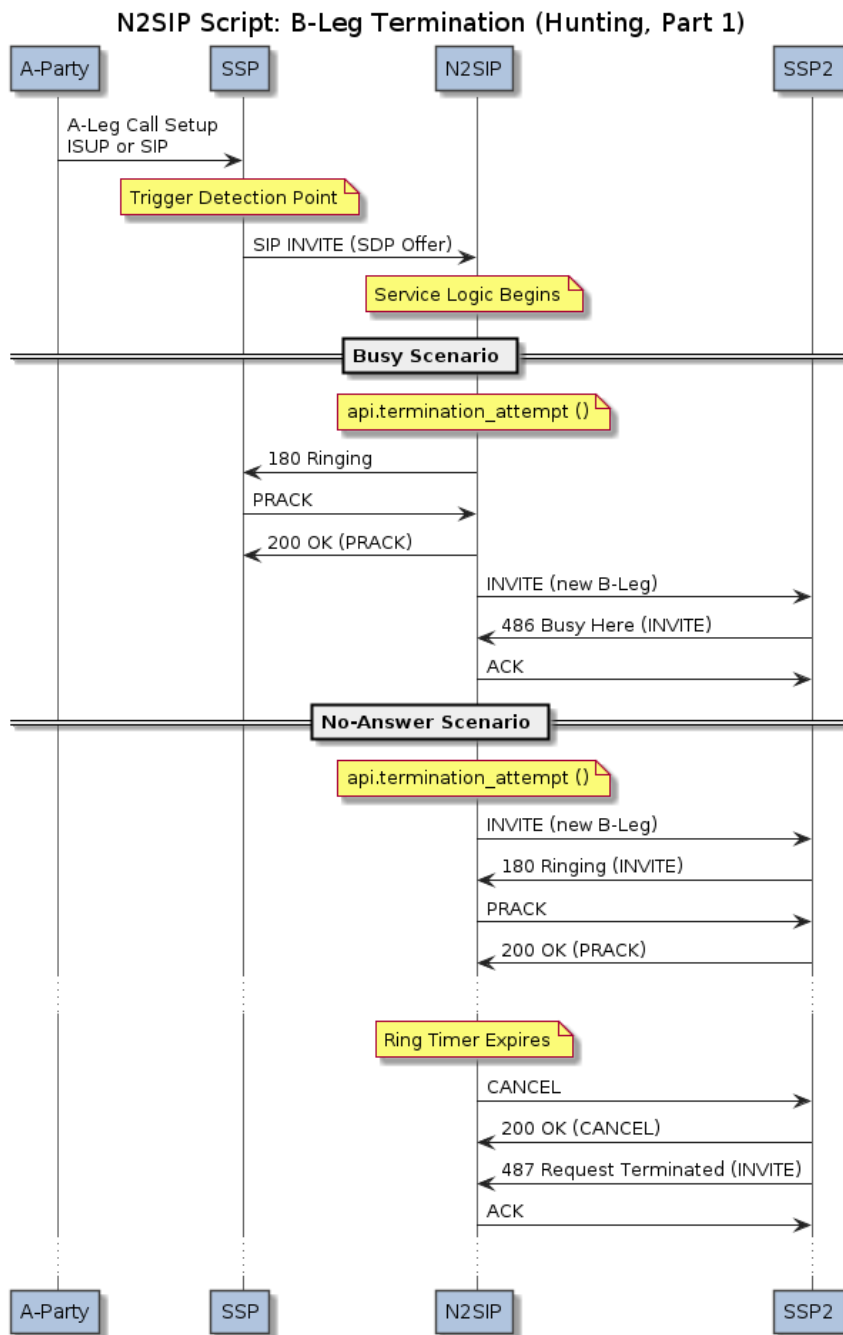


Figure T – N2SIP Flow: B-Leg Termination Attempt, Part 1

This final Part 2 shows the successful B-Leg termination attempt and the end-of-call cleanup.

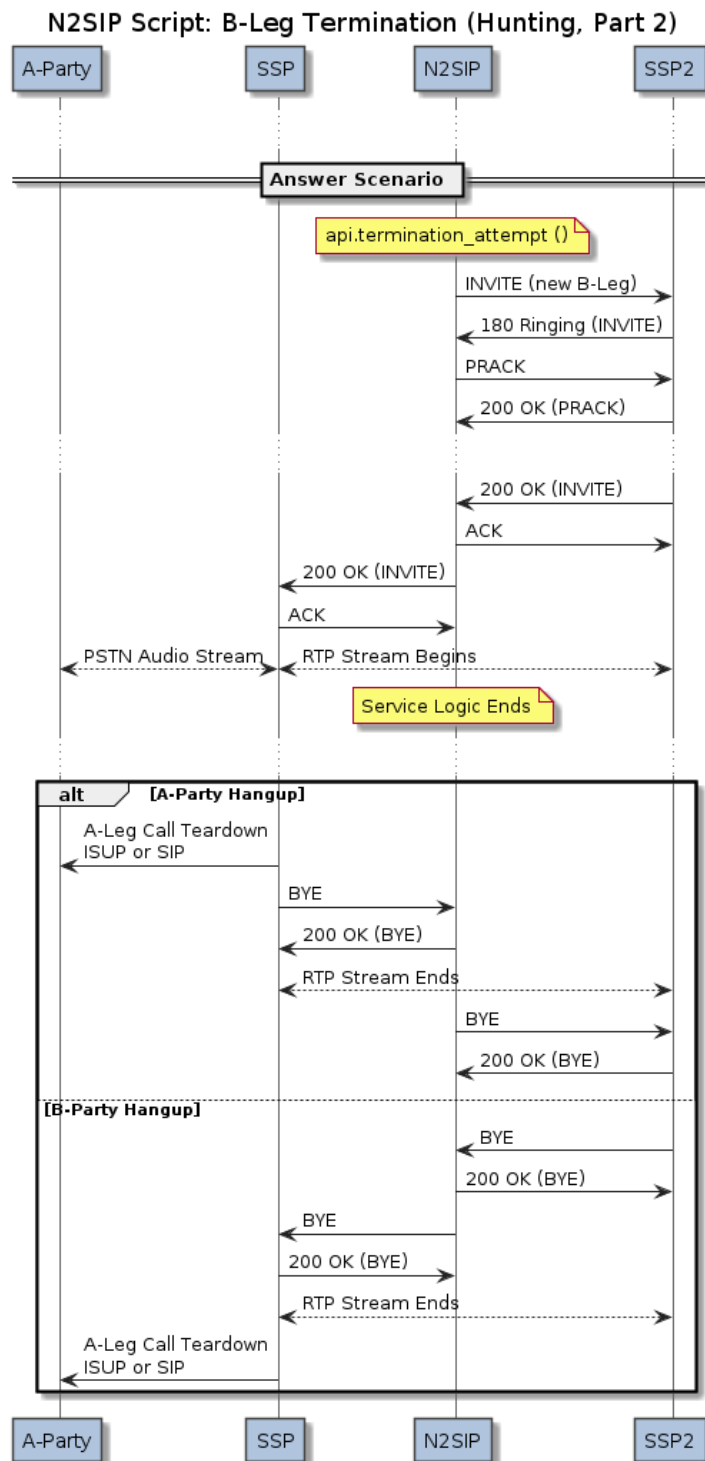


Figure U – N2SIP Flow: B-Leg Termination Attempt, Part 2

The N2SIP framework supports three different B-Leg Termination call control models when answered.

- 1) Service logic control is over. Stay in the SIP path to perform back-to-back on BYE.
- 2) Service logic will “monitor” the call, sending periodic re-INVITE “ping” to both legs.
- 3) Service logic will “charge” the call, performing “grants”, and force-end when balance expires.

Follow-on calls and announcements are permitted if the service logic uses “monitored” or “charged”.

### 7.8 Scenario: A-Leg Outcall with Internal Announcement

N2SIP can also perform an outcall to establish the A-Leg. The A-Leg is established using a provisional, inactive SDP. Once the A-Leg is established then the service logic can proceed with interactions or B-Leg termination attempts using the standard service logic API methods.

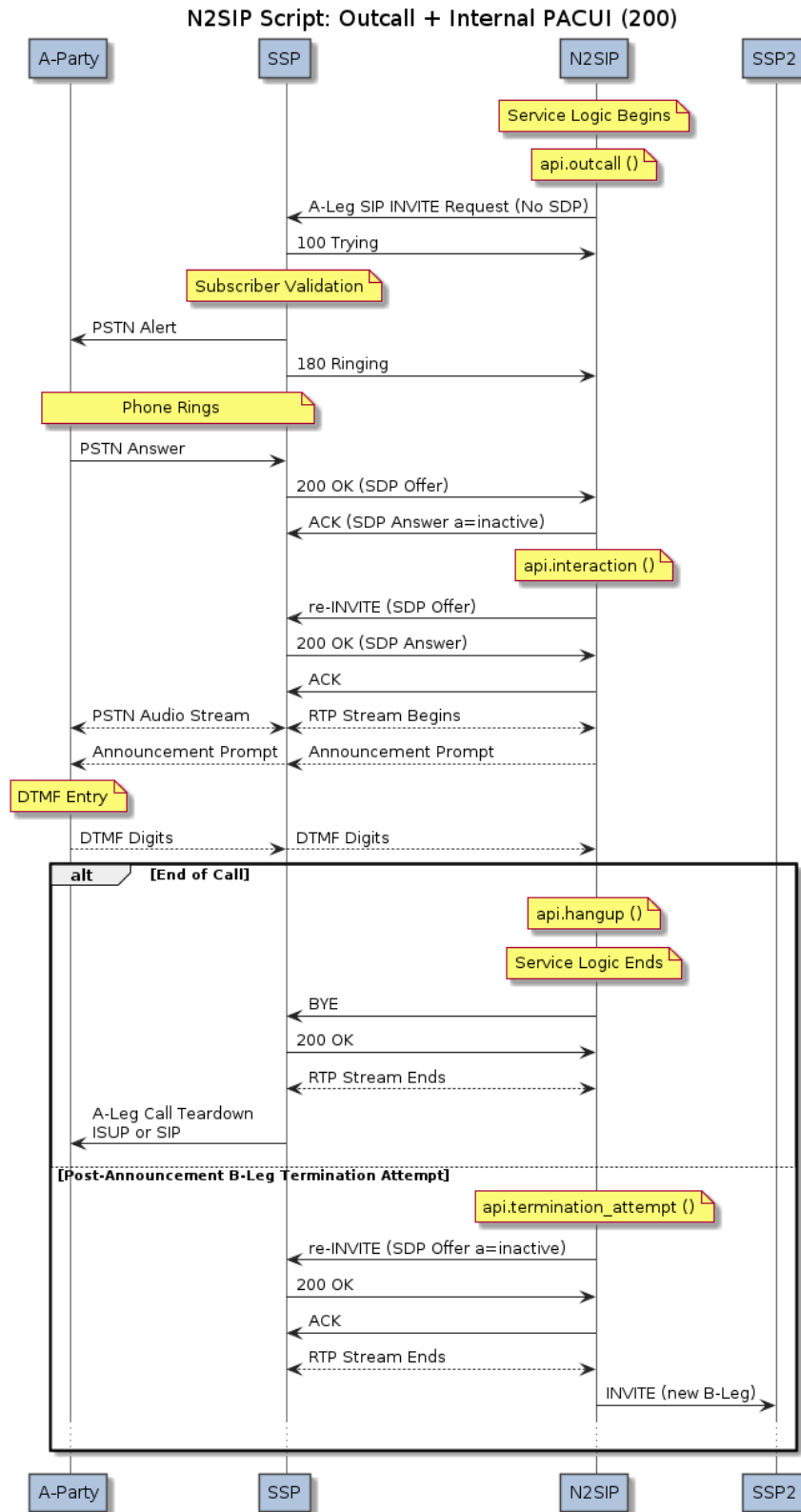


Figure V – N2SIP Flow: Outcall A-Leg followed by Internal Announcement using 200 OK