



**Inter-operability  
Test Cases for a  
SIP-H.323 Interworking Proxy  
and the OSP Peering Protocol**

**7 June 2006**

<b>1. Introduction</b> .....	<b>4</b>
<b>2. SIP to H.323 Test Cases</b> .....	<b>5</b>
<b>2.1. non-OSP Source to non-OSP Destination</b> .....	<b>5</b>
2.1.1. Call Rejected or No Circuit and Retry.....	5
2.1.2. No Response or No Connection and Retry - Proxy Times Out.....	13
2.1.3. No Response or No Connection and Retry - Source Times Out.....	14
2.1.4. Call Duration Limit Exceeded.....	15
2.1.5. Call Rejected - Protocol Error and Retry.....	16
2.1.6. Number Translation.....	17
<b>2.2. non-OSP Source to OSP Destination</b> .....	<b>18</b>
2.2.1. Call Rejected or No Circuit and Retry.....	19
2.2.2. No Response or No Connection and Retry - Proxy Times Out.....	20
2.2.3. No Response or No Connection and Retry - Source Times Out.....	21
2.2.4. Call Duration Limit Exceeded.....	22
2.2.5. Number Translation.....	23
<b>2.3. OSP Source and non-OSP Destination</b> .....	<b>25</b>
2.3.0. Invalid Authorization Token.....	25
2.3.1. Call Rejected or No Circuit and Retry.....	26
2.3.2. No Response or No Connection and Retry - Proxy Times Out.....	30
2.3.3. No Response or No Connection and Retry - Source Times Out.....	32
2.3.4. Call Duration Limit Exceeded.....	33
2.3.5. Look Ahead Routing.....	34
2.3.6. Look Ahead Routing: Call Rejected or No Circuit.....	36
2.3.7. Look Ahead Routing: No Response or No Connection - Proxy Times Out.....	37
2.3.8. Look Ahead Routing: No Response or No Connection - Source Times Out.....	38
2.3.9. Look Ahead Routing: Call Duration Limit Exceeded.....	39
2.3.10. Look Ahead Routing: Protocol Error.....	40
<b>2.4. OSP Source to OSP Destination</b> .....	<b>41</b>
2.4.0. Invalid Authorization Token.....	41
2.4.1. Call Rejected or No Circuit and Retry.....	42
2.4.2. No Response or No Connection and Retry - Proxy Times Out.....	43
2.4.3. No Response or No Connection and Retry - Source Times Out.....	44
2.4.4. Call Duration Limit Exceeded.....	45
2.4.5. Look Ahead Routing.....	46
2.4.6. Look Ahead Routing: Call Rejected or No Circuit.....	47
2.4.7. Look Ahead Routing: No Response or No Connection - Proxy Times Out.....	48
2.4.8. Look Ahead Routing: No Response or No Connection - Source Times Out.....	49
2.4.9. Look Ahead Routing: Call Duration Limit Exceeded.....	50
<b>3. H.323 to SIP Test Cases</b> .....	<b>51</b>
<b>3.1. non-OSP Source to non-OSP Destination</b> .....	<b>51</b>
3.1.1. Call Rejected or No Circuit and Retry.....	51
3.1.2. No Response or No Connection and Retry - Proxy Times Out.....	59
3.1.3. No Response or No Connection and Retry - Source Times Out.....	60
3.1.4. Call Duration Limit Exceeded.....	61
3.1.5. Call Rejected - Protocol Error and Retry.....	62
3.1.6. Number Translation.....	63
<b>3.2. non-OSP Source to OSP Destination</b> .....	<b>64</b>
3.2.1. Call Rejected or No Circuit and Retry.....	65
3.2.2. No Response or No Connection and Retry - Proxy Times Out.....	66

3.2.3.	No Response or No Connection and Retry - Source Times Out.....	67
3.2.4.	Call Duration Limit Exceeded .....	68
3.2.5.	Number Translation.....	69
<b>3.3.</b>	<b>OSP Source and non-OSP Destination .....</b>	<b>71</b>
3.3.0.	Invalid Authorization Token.....	71
3.3.1.	Call Rejected or No Circuit and Retry .....	72
3.3.2.	No Response or No Connection and Retry - Proxy Times Out .....	76
3.3.3.	No Response or No Connection and Retry - Source Times Out.....	78
3.3.4.	Call Duration Limit Exceeded .....	79
3.3.5.	Look Ahead Routing .....	80
3.3.6.	Look Ahead Routing: Call Rejected or No Circuit.....	82
3.3.7.	Look Ahead Routing: No Response or No Connection - Proxy Times Out .....	83
3.3.8.	Look Ahead Routing: No Response or No Connection - Source Times Out.....	84
3.3.9.	Look Ahead Routing: Call Duration Limit Exceeded .....	85
3.3.10.	Look Ahead Routing: Protocol Error.....	86
<b>3.4.</b>	<b>OSP Source to OSP Destination .....</b>	<b>87</b>
3.4.0.	Invalid Authorization Token.....	87
3.4.1.	Call Rejected or No Circuit and Retry .....	88
3.4.2.	No Response or No Connection and Retry - Proxy Times Out .....	89
3.4.3.	No Response or No Connection and Retry - Source Times Out.....	90
3.4.4.	Call Duration Limit Exceeded .....	91
3.4.5.	Look Ahead Routing .....	92
3.4.6.	Look Ahead Routing: Call Rejected or No Circuit.....	93
3.4.7.	Look Ahead Routing: No Response or No Connection - Proxy Times Out .....	94
3.4.8.	Look Ahead Routing: No Response or No Connection - Source Times Out.....	95
3.4.9.	Look Ahead Routing: Call Duration Limit Exceeded .....	96

### 1. Introduction

The document defines test cases for a standard implementation of the European Telecommunications Standards Institute (ETSI) Technical Specification 101 321 V4.1.1 (also referred to as OSP) with a SIP/H.323 interworking proxy. The OSP protocol, designed for inter-domain authorization, routing and accounting, is well suited for secure management of peer to peer IP applications such as VoIP and video over IP. For more information on ETSI, please refer to [www.etsi.org](http://www.etsi.org).

The test cases in this document are divided into sub-sections based on whether or not the source and destination devices support the OSP peering protocol. The focus of these test cases is on the inter-working proxy which is presented as gray box in the middle of each test case illustration. Note, these test cases assume the interworking proxy being tested is capable of tracking the call state from beginning to end and then reporting call duration in a call detail record.

Included with the test cases is guidance on how to use OSP Toolkit functions to implement the OSP protocol for VoIP peering. The OSP Toolkit is an open source OSP client implementation available from [www.sipfoundry.org](http://www.sipfoundry.org). Each test case presents SIP messages in blue. H.323 messages are in plum (purple). OSP messages are presented in green. Application Program Interface (API) calls between the inter-working proxy and the OSP Toolkit are presented in red. A description of the messages and OSP Toolkit calls is provided with test case 2.1.1 and 3.1.1. Detailed information on the OSP Toolkit API function calls is provided in the OSP Toolkit Programming Interface document available on [www.sipfoundry.org](http://www.sipfoundry.org).

A basic requirement for these test cases is the ability of the inter-working proxy to enroll with the OSP server. The enrollment process is a two step process. First, the inter-working proxy requests the public key of the OSP server or certificate authority. Second, the inter-working proxy sends a certificate request to the OSP server which returns a signed certificate to the inter-working proxy. Secure inter-domain access control requires that the inter-working proxy must be able to validate an OSP peering authorization token digitally signed by the OSP server. The Enroll utility included with the OSP Toolkit provides the functionality required for the inter-working proxy to create a public/private key pair and to send a certificate request to a certificate authority such as an OSP server. For more information on the Enroll utility included with the OSP Toolkit, please see the Enrollment document available from [www.sipfoundry.org](http://www.sipfoundry.org).

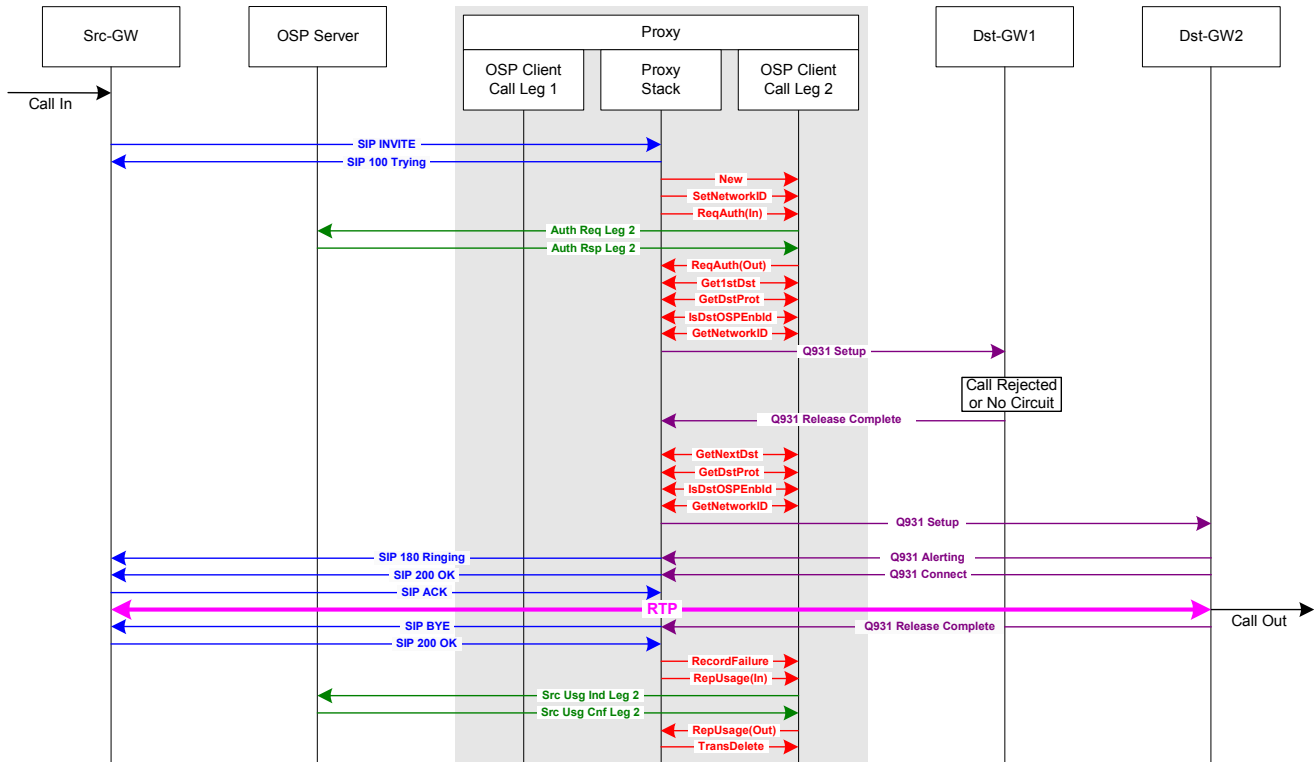
## 2. SIP to H.323 Test Cases

### 2.1. non-OSP Source to non-OSP Destination

This subsection defines test cases when both the source SIP and destination H.323 devices are not OSP enabled. In these test cases, the inter-working proxy sends OSP messages to an OSP server to determine routing and report call detail records. OSP interdomain peering authorization access tokens are not used in these test cases.

Configuration of VoIP devices on OSP server for test cases in section 2.1		
Device	Destination Protocol	OSP Version
Src-GW	SIP	0.0.0 (Not OSP Enabled)
Proxy	SIP or H323_Q931	2.1.1 or 4.1.1
Dst-GW1	H323_Q931	0.0.0 (Not OSP Enabled)
Dst-GW2	H323_Q931	0.0.0 (Not OSP Enabled)

#### 2.1.1. Call Rejected or No Circuit and Retry



**Test Case 2.1.1: non-OSP SIP Source to Proxy to non-OSP H.323 Destination: Call Rejected or No Circuit & Retry**  
**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Detailed Description of Test Case

The call scenario diagram above illustrates the SIP messages (in blue), H.323 messages (in plum), OSP messages (in green) and OSP Toolkit function calls (in red) for this test case. (Please see the OSP Toolkit Programming Interface V3.3.1 document for details on OSP Toolkit function calls.) The gray box in the middle of the illustration represents the inter-working proxy. These call scenarios for the proxy, have two call legs. One inbound call leg from the source SIP device to the proxy and a second outbound call leg from the

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

proxy to the destination H.323 device. Each of these call legs require a message transaction between the proxy and the OSP client. To illustrate different OSP Toolkit transactions for the inbound (call leg 1) and outbound (call leg 2) call legs, the OSP client is shown twice in the gray box representing the proxy. The test case is described in detail below.

1. **Call In.** The call begins at the source SIP device. The source of the SIP call could be from a variety of devices, such as a SIP phone registered to the Source SIP device which is acting as a proxy, or a PSTN trunk which is connected to SIP gateway which is acting as a user agent.
2. **SIP INVITE.** The source SIP device sends a SIP INVITE to the proxy.
3. **SIP 100 Trying.** The proxy receives the SIP INVITE and responds to the source SIP device.
4. **NEW.** The proxy does not have a route defined to complete the call to the dialed number. The proxy queries the OSP server for a route to an inter-domain destination to complete the call. The proxy establishes a new transaction with the OSP client using `OSPPTtransactionNew` function. Please see the OSP Toolkit Programming Interface V3.3.1 document for details on this and other function calls.
5. **SetNetworkID.** The `OSPPTtransactionSetNetworkIds` function call identifies the trunk group or partition in the source SIP device which originated the call. In this test case, the `ospvSrcNetworkId` (trunk group or partition of the source device) must be taken from the SIP INVITE from the source SIP device. The `SrcNetworkId` is included in the `AuthorizationRequest` to the OSP server and may be used by the OSP server operator for routing and billing of calls by source trunk group or partition.
6. **ReqAuth(In).** The proxy calls the `OSPPTtransactionRequestAuthorisation` OSP Toolkit function.
7. **Auth Req Leg 2.** The OSP client sends an OSP `AuthorizationRequest` to the OSP server requesting a list of devices which can complete the call. The OSP request includes the calling and called telephone numbers, and the IP address of the source SIP device.
8. **Auth Rsp Leg 2.** The OSP server sends an OSP `AuthorizationResponse` to the OSP client. The OSP `AuthorizationResponse` includes a list of one or more destinations enabling the proxy to retry the call setup multiple times to different destinations until the call is completed. In this test case, the response includes the IP addresses, signaling protocol and OSP version supported by two destination H.323 devices.
9. **ReqAuth(Out).** The OSP Toolkit responds to the proxy that the `OSPPTtransactionRequestAuthorisation` function is complete.
10. **Get1stDst.** The proxy calls the OSP Toolkit function `OSPPTtransactionGetFirstDestination` to get the IP address of the first destination gateway.
11. **GetDstProt.** The proxy calls the OSP Toolkit function `OSPPTtransactionGetDestProtocol` to get the signaling protocol required by the destination H.323 device. In this case, the `DestinationProtocol` is `H323_Q931`. If `DestinationProtocol` is not `H323_Q931` (i.e. `SIP`, `H323_LRQ` or `IAX`), the proxy should reject the call and report a `FailureReason` of 111. If `DestinationProtocol` is unknown or undefined, the proxy should assume the destination protocol is `H323_Q931` and complete the call.

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

12. **IsDstOSPEnabled.** The OSPPTTransactionDestOSPEnabled function tells the proxy whether or not the destination H.323 device is OSP enabled and capable of validating the OSP authorization token. In this case the destination H.323 device is not OSP enabled (OSPE\_OSP\_FALSE). The proxy should not include the OSP peering authorization token in the Q931 Setup to the destination H.323 device. (Note, to ensure backward compatibility with OSP V1.4.3, if OSPE\_OSP is unknown or undefined, the proxy should assume the destination is OSP enabled and include the OSP authorization token in the Q931 Setup to the destination.)
13. **GetNetworkID.** The proxy calls the OSP Toolkit function OSPGetDestNetworkID to get the destination trunk group if it is available. If the destination trunk group is available, it should be included in the Q931 Setup (H.323 parameter destinationCarrierID) to the destination.
14. **Q931 Setup.** The proxy sends a Q931 call setup message to the first destination H.323 device. An OSP authorization token is not included in the Q931 Setup since the destination gateway does not support OSP. The Q931 Setup should NOT include the source trunk group information from the source SIP device.
15. **Q931 Release Complete.** The first destination H.323 device does not accept the Q931 Setup and returns a 21 Call Rejected to the proxy. This test case applies for any case when the destination H.323 device rejects the Q931 Setup. The call may be rejected for a variety of reasons such as unauthorized access or no circuits available.
16. **GetNextDst.** The proxy retries the call to the second destination and calls OSP Toolkit function OSPPTTransactionGetNextDestination to obtain the IP address of the next destination H.323 device. The OSPPTTransactionGetNextDestination function call should include the FailureReason for the previous failed call attempt. In this test case the FailureReason should be the release cause reported by the destination or 21.
17. **GetDstProt.** The proxy gets the destination protocol of the second destination H.323 device. In this test case the destination protocol is H323\_Q931. If DestinationProtocol is not H323\_Q931 (i.e. SIP, H323\_LRQ or IAX), the proxy should reject the call and report a FailureReason of 111. If DestinationProtocol is unknown or undefined, the proxy should assume the destination protocol is H323\_Q931 and send a Q931 Setup to the destination.
18. **IsDstOSPEnabled.** The OSPPTTransactionDestOSPEnabled function tells the proxy whether or not the destination device is OSP enabled and capable of validating the OSP authorization token. In this case the destination H.323 device is not OSP enabled (OSPE\_OSP\_FALSE). The proxy should not include the OSP authorization token in the Q931 Setup to the destination device. (Note, to ensure backward compatibility with OSP V1.4.3, if OSPE\_OSP is unknown or undefined, the proxy should assume the destination is OSP enabled and include the OSP authorization token in the Q931 Setup to the destination.)
19. **GetNetworkID.** The proxy calls the OSP Toolkit function OSPGetDestNetworkID to get the destination trunk group if it is available. If the destination trunk group is available, it should be included in the Q931 Setup (H.323 parameter destinationCarrierID) to the destination.
20. – 30. Standard SIP to H.323 communications for the completing the call.

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

31. **RecordFailure**. At the completion of the call, the proxy reports the call disconnect reason for the successful retry, to the OSP Toolkit using the OSPPTtransactionRecordFailure function.
32. **RepUsage(In)**. The proxy calls the OSPPTtransactionReportUsage function to report the call duration.
33. **Src Usg Ind Leg 2**. The OSP client sends an OSP UsageIndication message (Call Detail Record) to the OSP server. The UsageIndication is a type 'source' call detail record since the proxy is the source device for the second leg of the call.
34. **Src Usg Cnf Leg 2**. The OSP server responds with an OSP UsageConfirmation message.
35. **RepUsage(Out)**. The OSP Toolkit closes the ReportUsage transaction.
36. **TransDelete**. The proxy deletes the OSP Toolkit transaction.

### Expected CDRs for Test Case 2.1.1

This test case should generate two OSP UsageIndication messages, or CDRs, from the proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the first call attempt should be the response from Dst-GW1. In this example, the response is 21, but other responses are also valid. For the successful retry call, the proxy should set the FailureReason to 16 or 1016.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW1	21	0
2	source	Src-GW	Dst-GW2	16 or 1016	greater than 0

### Expected OSP Messages for Test Case 2.1.1

This section presents the expected OSP messages for Test Case 2.1.1. After each OSP message is a table correlating each XML tag in the OSP message with a corresponding OSP Toolkit variable

#### AuthorizationRequest Leg 2 (generated by OSPPTtransactionRequestAuthorisation)

```
<?xml version="1.0"?>
<Message messageId="11703738491" random="1170373849">
<AuthorizationRequest componentId="11703738490">
<Timestamp>2005-05-12T17:32:57Z</Timestamp>
<CallId encoding="base64">Call ID</CallId>
<SourceInfo type="e164">Calling Number</SourceInfo>
<DeviceInfo type="transport">[Src-GW IP Address]</DeviceInfo>
<SourceAlternate type="transport">[Proxy IP address]</SourceAlternate>
<SourceAlternate type="network">Partition</SourceAlternate>
<DestinationInfo type="e164">Called Number</DestinationInfo>
<Service/>
<MaximumDestinations>Number of Destination</MaximumDestinations>
</AuthorizationRequest>
</Message>
```

OSP XML Tag	Toolkit Variable	Note
<CallId encoding="base64">	CallId	
<SourceInfo type="e164">	CallingNumber	
<DeviceInfo type="transport">	SourceDevice	Src-GW IP Address
<SourceAlternate	Source	Proxy IP Address

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

type="transport">		
<SourceAlternate type="network">	NetworkId	Partition or trunk group
<DestinationInfo type="e164">	CalledNumber	
<MaximumDestinations>	NumberOfDestinations	Maximum number of possible destinations requested.

### AuthorizationResponse Leg 2 (response from OSP server)

```

<?xml version='1.0'?>
<Message messageId='11703738491' random='21655'>
<AuthorizationResponse componentId='11703738490'>
<Timestamp>2005-05-12T18:32:59Z</Timestamp>
<Status>
<Description>SUCCESS</Description>
<Code>200</Code>
</Status>
<TransactionId>Transaction ID</TransactionId>
<Destination>
<CallId encoding='base64'>Call ID</CallId>
<DestinationInfo type='e164'>Called Number</DestinationInfo>
<DestinationSignalAddress>[Dst-GW1 IP Address]</DestinationSignalAddress>
<Token encoding='base64'>OSP Token</Token>
<UsageDetail>
<Amount>14400</Amount>
<Increment>1</Increment>
<Service/>
<Unit>s</Unit>
</UsageDetail>
<ValidAfter>2005-05-12T18:27:59Z</ValidAfter>
<ValidUntil>2005-05-12T18:37:59Z</ValidUntil>
<DestinationProtocol critical='False'>h323-Q931</DestinationProtocol>
<OSPVersion critical='False'>0.0.0</OSPVersion>
<SourceInfo type='e164' critical='False'>Calling Number</SourceInfo>
<DestinationAlternate type='network'
critical='False'></DestinationAlternate>
</Destination>
<Destination>
<CallId encoding='base64'>Call ID</CallId>
<DestinationInfo type='e164'>Called Number</DestinationInfo>
<DestinationSignalAddress>[Dst-GW2 IP Address]</DestinationSignalAddress>
<Token encoding='base64'>OSP Token</Token>
<UsageDetail>
<Amount>14400</Amount>
<Increment>1</Increment>
<Service/>
<Unit>s</Unit>
</UsageDetail>
<ValidAfter>2005-05-12T18:27:59Z</ValidAfter>
<ValidUntil>2005-05-12T18:37:59Z</ValidUntil>
<DestinationProtocol critical='False'>h323-Q931</DestinationProtocol>
<OSPVersion critical='False'>0.0.0</OSPVersion>
<SourceInfo type='e164' critical='False'>Calling Number</SourceInfo>
<DestinationAlternate type='network'
critical='False'></DestinationAlternate>
</Destination>
</AuthorizationResponse>

```

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

</Message>

OSP XML Tag	Toolkit Variable	Note
<TransactionId>		Transaction ID from OSP server
<CallId encoding="base64">	CallId	
<DestinationInfo type="e164">	CalledNumber	May be translated in AuthResponse
<DestinationSignalAddress>	Destination	Dst-GW1 IP Address
<Token encoding="base64">	Token	Authorization token
<Amount>	TimeLimit	Authorized call duration in seconds
<Increment>		Default is 1
<Service>		Default is voice
<Unit>		Default is seconds
<ValidAfter>	ValidAfter	Time after which call is authorized
<ValidUntil>	ValidUntil	Time until which call is authorized
<DestinationProtocol>	DestinationProtocol	VoIP signaling protocol expected by Dst-GW1
<OSPVersion>	DestinationOSPStatus	Version of OSP supported by Dst-GW1
<SourceInfo type="e164">	CallingNumber	May be translated in AuthResponse
<DestinationAlternate type="network">	DstNetworkID	Partition or trunk group of Dst-GW1
<CallId encoding="base64">	CallId	
<DestinationInfo type="e164">	CalledNumber	May be translated in AuthResponse
<DestinationSignalAddress>	Destination	Dst-GW2 IP Address
<Token encoding="base64">	Token	Authorization token
<Amount>	TimeLimit	Authorized call duration in seconds
<Increment>		Default is 2
<Service>		Default is voice
<Unit>		Default is seconds
<ValidAfter>	ValidAfter	Time after which call is authorized
<ValidUntil>	ValidUntil	Time until which call is authorized
<DestinationProtocol>	DestinationProtocol	VoIP signaling protocol expected by Dst-GW2
<OSPVersion>	DestinationOSPStatus	Version of OSP supported by Dst-GW2
<SourceInfo type="e164">	CallingNumber	May be translated in AuthResponse
<DestinationAlternate type="network">	DstNetworkID	Partition or trunk group of Dst-GW2

### Source UsageIndication Leg 2 (generated by OSPPTTransactionReportUsage)

```

<?xml version="1.0"?>
<Message messageId="47850982870685430173" random="1140717192">
<UsageIndication componentId="47850982870685430172">
<Timestamp>2005-05-12T17:33:33Z</Timestamp>
<Role>source</Role>
<TransactionId>Transaction ID</TransactionId>
<CallId encoding="base64">Call ID</CallId>
<SourceInfo type="e164">Calling Number</SourceInfo>
<DeviceInfo type="transport">[Src-GW IP Address]</DeviceInfo>
<SourceAlternate type="transport">[Proxy IP Address]</SourceAlternate>

```

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

```

<DestinationInfo type="e164">Called Number</DestinationInfo>
<DestinationAlternate type="transport">[Dst-GW1 IP address]</DestinationAlternate>
<FailureReason>21</FailureReason>
</UsageIndication>
<UsageIndication componentId="47850982870685430174">
<Timestamp>2005-05-12T17:33:33Z</Timestamp>
<Role>source</Role>
<TransactionId>Transaction ID</TransactionId>
<CallId encoding="base64">Call ID</CallId>
<SourceInfo type="e164">Calling Number</SourceInfo>
<DeviceInfo type="transport">[Src-GW IP Address]</DeviceInfo>
<SourceAlternate type="transport">[Proxy IP Address]</SourceAlternate>
<DestinationInfo type="e164">Called Number</DestinationInfo>
<DestinationAlternate type="transport">[Dst-GW2 IP address]</DestinationAlternate>
<UsageDetail>
<Amount>23</Amount>
<Increment>1</Increment>
<Unit>s</Unit>
<StartTime>2005-05-12T17:33:10Z</StartTime>
<AlertTime>2005-05-12T17:42:12Z</EndTime>
<EndTime>2005-05-12T17:42:27Z</EndTime>
<ConnectTime>2005-05-12T17:42:17Z</ConnectTime>
<ReleaseSource>0</ReleaseSource>
</UsageDetail>
<FailureReason>1016</FailureReason>
<Statistics critical="False">
<LossSent critical="False">
<Packets critical="False">0</Packets>
<Fraction critical="False">0</Fraction>
</LossSent>
<LossReceived critical="False">
<Packets critical="False">0</Packets>
<Fraction critical="False">0</Fraction>
</LossReceived>
</Statistics>
</UsageIndication>
</Message>

```

OSP XML Tag	Toolkit Variable	Note
<Role>		Source CDR for 1st try of call leg 2
<TransactionId>		Transaction ID from OSP server
<CallId encoding="base64">	CallId	
<SourceInfo type="e164">	CallingNumber	May be translated in AuthResponse
<DeviceInfo type="transport">	SourceDevice	Src-GW IP Address
<SourceAlternate type="transport">	Source	Proxy IP Address
<DestinationInfo type="e164">	CalledNumber	May be translated in AuthResponse
<DestinationAlternate>	Destination	Dst-GW1 IP Address
<FailureReason>	FailureReason	Call Release Code
<Role>		Source CDR for 2nd try of call leg 2
<TransactionId>		Transaction ID from OSP server
<CallId encoding="base64">	CallId	
<SourceInfo type="e164">	CallingNumber	May be translated in AuthResponse
<DeviceInfo type="transport">	SourceDevice	Src-GW IP Address

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

OSP XML Tag	Toolkit Variable	Note
<SourceAlternate type="transport">	Source	Proxy IP Address
<DestinationInfo type="e164">	CalledNumber	May be translated in AuthResponse
<DestinationAlternate>	Destination	Dst-GW2 IP Address
<Amount>	Duration	Call duration in seconds
<Increment>		Default is 1
<Unit>		Default is seconds
<StartTime>	StartTime	Time stamp when Q931 Setup is sent to the first destination device.
<AlertTime>	AlertTime	Time stamp when Q931 Alerting message is received.
<EndTime>	EndTime	Time stamp when Q931 Release Complete is received from source or destination.
<ConnectTime>	ConnectionTime	Time stamp when SIP ACK is received.
<ReleaseSource>	ReleaseSource	0 for source, 1 for destination
<FailureReason>	FailureReason	Call Release Code
<LossSent><Packets>	LossPacketSent	
<LossSent><Fraction>	LossFractionSent	
<LossReceived><Packets>	LossPacketReceived	
<LossReceived><Fraction>	LossFractionReceived	

### Source UsageConfirmation Leg 2 (confirmation from OSP server)

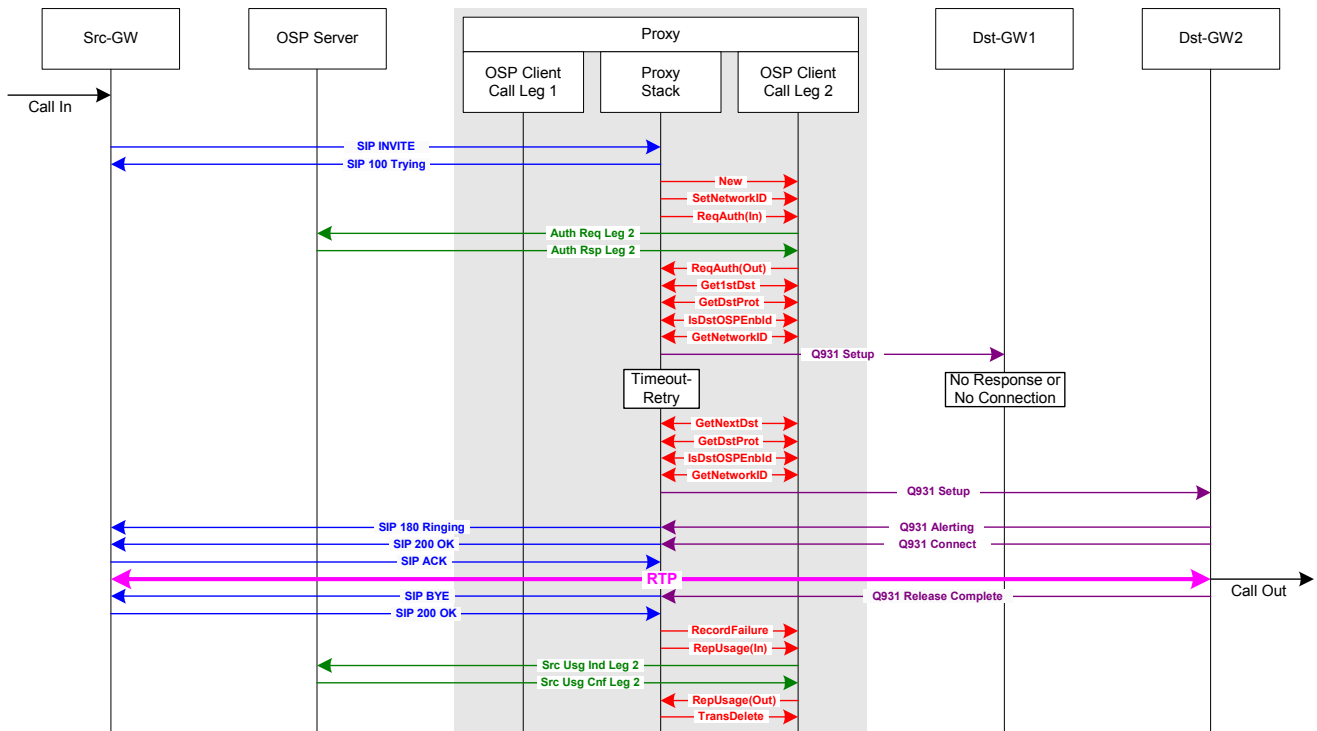
```

<?xml version='1.0'?>
<Message messageId='47850982870685430173' random='21172'>
<UsageConfirmation componentId='47850982870685430172'>
<Timestamp>2005-05-12T18:33:34Z</Timestamp>
<Status>
<Description>SUCCESS</Description>
<Code>200</Code>
</Status>
</UsageConfirmation>
<UsageConfirmation componentId='47850982870685430174'>
<Timestamp>2005-05-12T18:33:34Z</Timestamp>
<Status>
<Description>SUCCESS</Description>
<Code>200</Code>
</Status>
</UsageConfirmation>
</Message>

```

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

### 2.1.2. No Response or No Connection and Retry - Proxy Times Out



**Test Case 2.1.2: non-OSP SIP Source to Proxy to non-OSP H.323 Destination:  
No Response or No Connection & Retry - Proxy Times Out**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

This case tests the call scenarios when a destination H.323 device does not respond to the proxy. This test case requires that the OSP server return two or more destinations in the AuthorizationResponse to the proxy. After the first call attempt fails, the proxy must retry the call to second destination. This test case must be executed four times to test the following four different call scenarios.

1. The proxy cannot establish a TCP connection with Dst-GW1. After TCP time-out, the proxy should retry call to Dst-GW2. (When OSP Toolkit function OSPPTTransactionGetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 47 – resource unavailable, unspecified.)
2. No route to IP address of Dst-GW1 device. The proxy should retry call to Dst-GW2. (When OSP Toolkit function OSPPTTransactionGetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 2 – no route to specified transit network.)
3. TCP connection refused by destination, Dst-GW1. After TCP connection is refused, the proxy should retry the call to Dst-GW2. (When OSP Toolkit function OSPPTTransactionGetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 63 – service or option not available, unspecified.)
4. No response from Dst-GW1. The proxy establishes TCP connection with Dst-GW1, but Dst-GW1 never responds to Q931 Setup. The proxy should time-out and retry the call to Dst-GW2. (When OSP Toolkit function OSPPTTransactionGetNextDestination

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

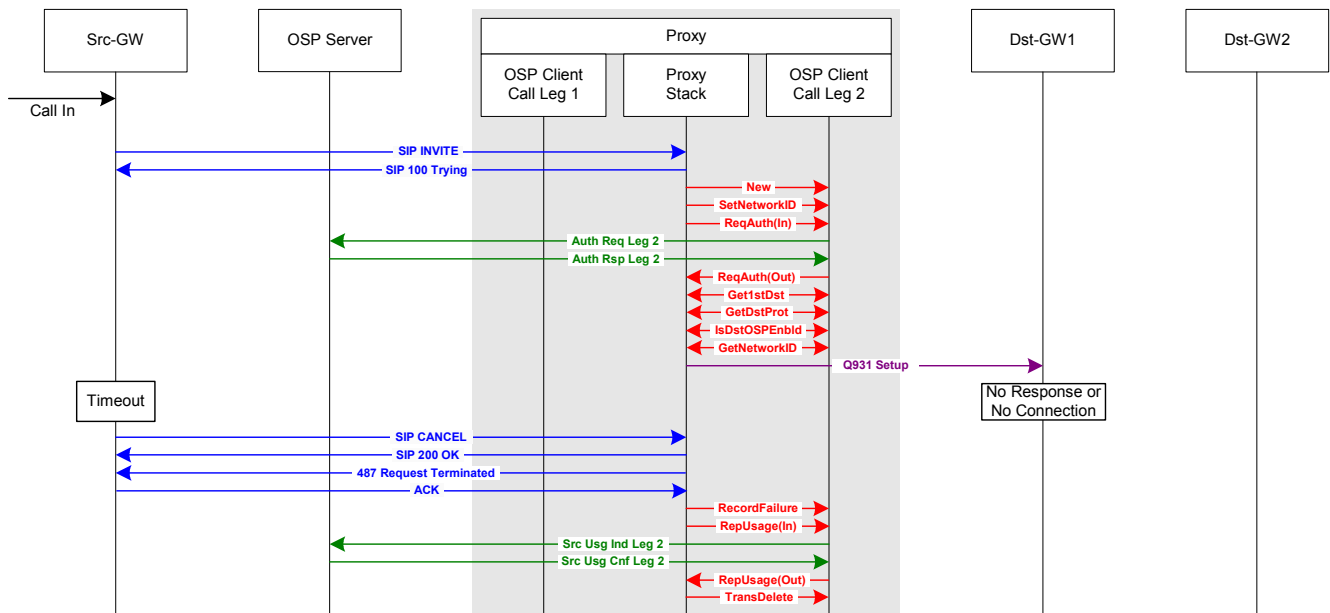
is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 27 – destination out of order.)

### Expected CDRs for Test Case 2.1.2

This test case should generate two OSP UsageIndication messages, or CDRs, from the proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the first call attempt should be determined by the proxy based on the reason for the failure. For the successful retry call, the proxy should set the FailureReason to 16 or 1016.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW1	47, 2, 63 or 27	0
2	source	Src-GW	Dst-GW2	16 or 1016	greater than 0

### 2.1.3. No Response or No Connection and Retry - Source Times Out



**Test Case 2.1.3: non-OSP SIP Source to Proxy to non-OSP H.323 Destination:  
No Response or No Connection & Retry - Source Times Out**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

### Test Case Notes

This case tests the call scenario when the source ends the call before the first destination Dst-GW1 responds to the Q931 Setup from the proxy. In these cases, the proxy should terminate the call and report usage to the OSP server. The OSP Toolkit parameter FailureReason reported with the OSPPTtransactionRecordFailure function should be set to the release cause reported in the SIP CANCEL message from the source device, Src-GW. If no release reason is reported in the SIP CANCEL message, the proxy should set the FailureReason 487.

### Expected CDRs for Test Case 2.1.3

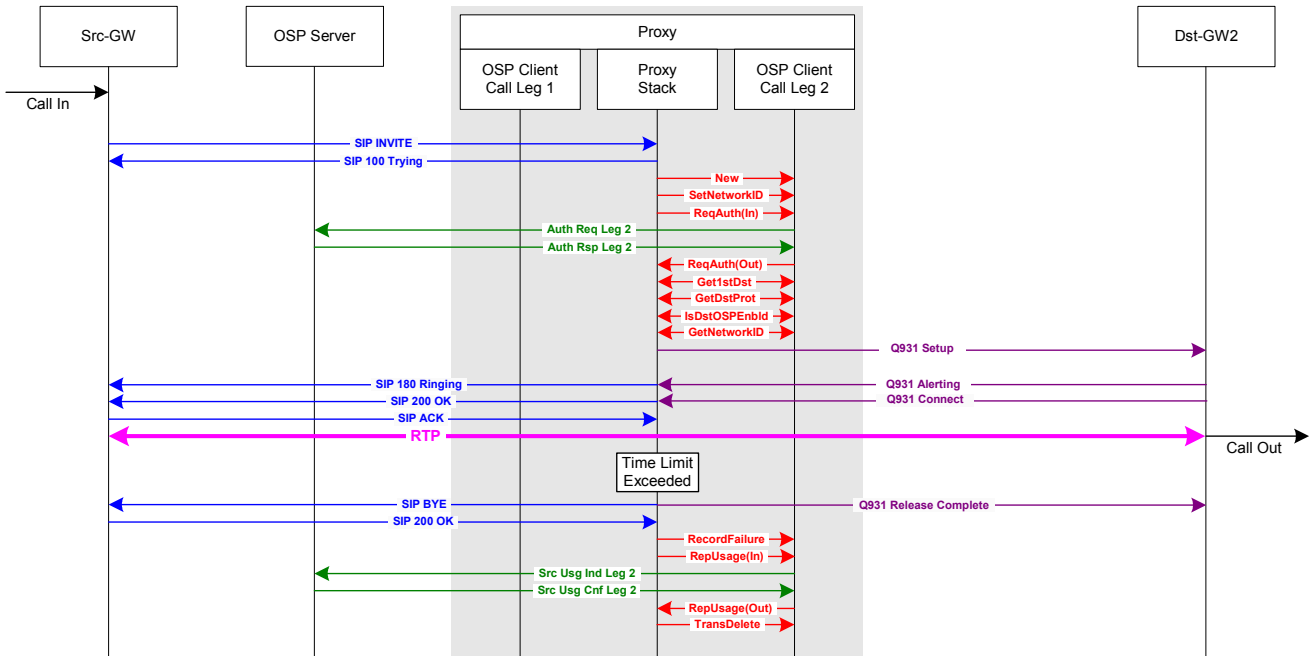
This test case should generate one OSP UsageIndication message, or CDR, from the proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

cause code, for the call should be determined from the release reason included in the SIP CANCEL message from Src-GW. If no release reason is included in the SIP CANCEL message, the proxy should report a FailureReason of 487.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW1	487	0

### 2.1.4. Call Duration Limit Exceeded



**Test Case 2.1.4: non-OSP SIP Source to Proxy to non-OSP H.323 Destination: Time Limit Exceeded**  
**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

This call scenario tests the proxy's ability to end a call when its authorized call duration has been exceeded. In the AuthorizationResponse, the OSP server includes the authorized call duration. The OSP Toolkit parameter TimeLimit, returned in the GetFirstDestination or GetNextDestination function calls, defines the maximum duration for each call. The proxy should terminate a call when the call duration exceeds the TimeLimit. In this case, when the proxy forcefully ends a call that has exceeded its maximum call duration, the proxy should use the RecordFailure OSP Toolkit function call to report a FailureReason of 8 (preemption) and then use the ReportUsage OSP Toolkit function call to send a UsageIndication call detail record to the OSP server.

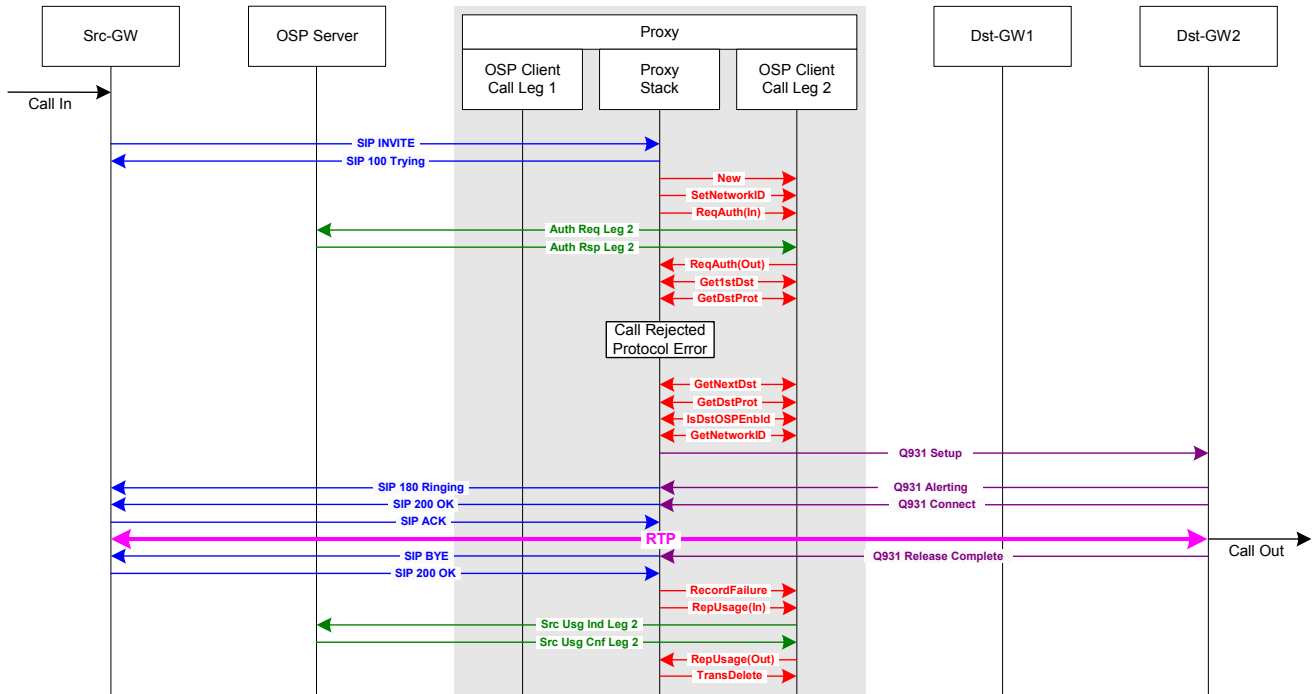
#### Expected CDRs for Test Case 2.1.4

This test case should generate one OSP UsageIndication message, or CDR, from the proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the call should be set by the proxy to 8 to indicate the call was forcefully shutdown by the proxy.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW2	8	greater than 0

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

### 2.1.5. Call Rejected - Protocol Error and Retry



**Test Case 2.1.5: non-OSP SIP Source to Proxy to non-OSP H.323 Destination: Protocol Error & Retry**  
**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

This case tests the error condition when the OSP server returns a DestinationProtocol that is not supported by the proxy, such as H323\_LRQ or IAX. When this occurs, the proxy should reject the destination, record FailureReason 111 (protocol error) and retry the call to the next destination if it is available.

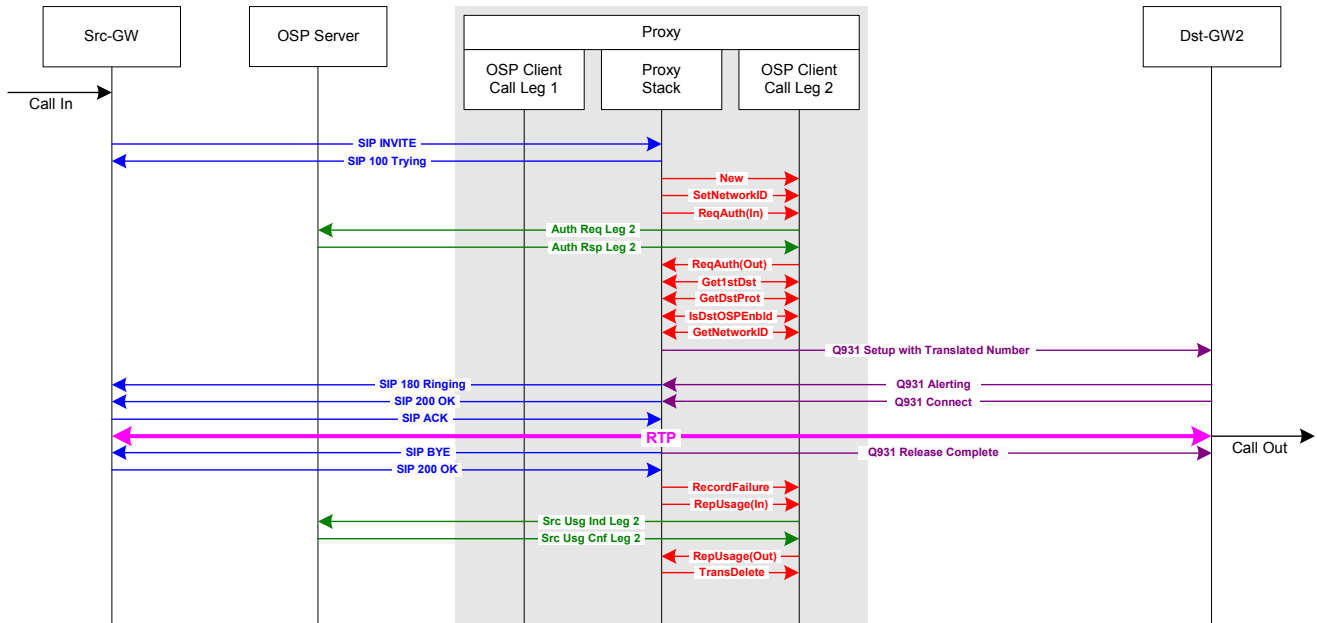
For this test case, the destination protocol for device Dst-GW1 is NOT configured as H323\_Q931 on the OSP server. The OSPPTTransactionGetDestProtocol function call returns a DestinationProtocol not supported by the inter-working proxy. The proxy should recognize the protocol error and reject the call attempt. Note, if the DestinationProtocol is unknown or undefined for a destination, the inter-working proxy may either ignore the destination and record FailureReason 111 or attempt a call setup to the destination using its default signaling protocol.

#### Expected CDRs for Test Case 2.1.5

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW1	111	0
2	source	Src-GW	Dst-GW2	16 or 1016	greater than 0

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

### 2.1.6. Number Translation



**Test Case 2.1.6: non-OSP SIP Source to Proxy to non-OSP H.323 Destination: Number Translation**  
**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

This case tests the call scenario when the OSP server returns translated called and calling numbers in the OSP AuthorizationResponse to the proxy. When this occurs, the called and calling numbers in the Q931 Setup from the proxy to the destination H.323 gateway should be the translated called and calling numbers from the OSP AuthorizationResponse.

For this test case, the called and calling number translation rules are configured on the OSP server. The OSPTransactionGetFirstDestination function call returns the translated called and calling numbers. The proxy should send a Q931 Setup with the translated numbers to the destination. The OSPTransactionReportUsage function should report the un-translated called and calling numbers.

#### Expected CDRs for Test Case 2.1.6

This test case should generate one OSP UsageIndication message, or CDR, from the proxy as the source of call leg 2. The called and calling numbers reported in the OSP UsageIndication message from the proxy, should be the called and calling numbers from the SIP INVITE received from the source SIP gateway in call leg 1. The translated called and calling numbers should not be reported in the OSP UsageIndication message.

Call Leg	Role	Source IP Address	Destination IP Address	Calling Number	Called Number	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW2	Not Translated	Not Translated	16 or 1016	greater than 0

**Note:** OSP Toolkit version 3.3.3 and earlier report translated numbers in the CDR. Version 3.3.4 reports translated calling number and not translated called number.

## 2.2. *non-OSP Source to OSP Destination*

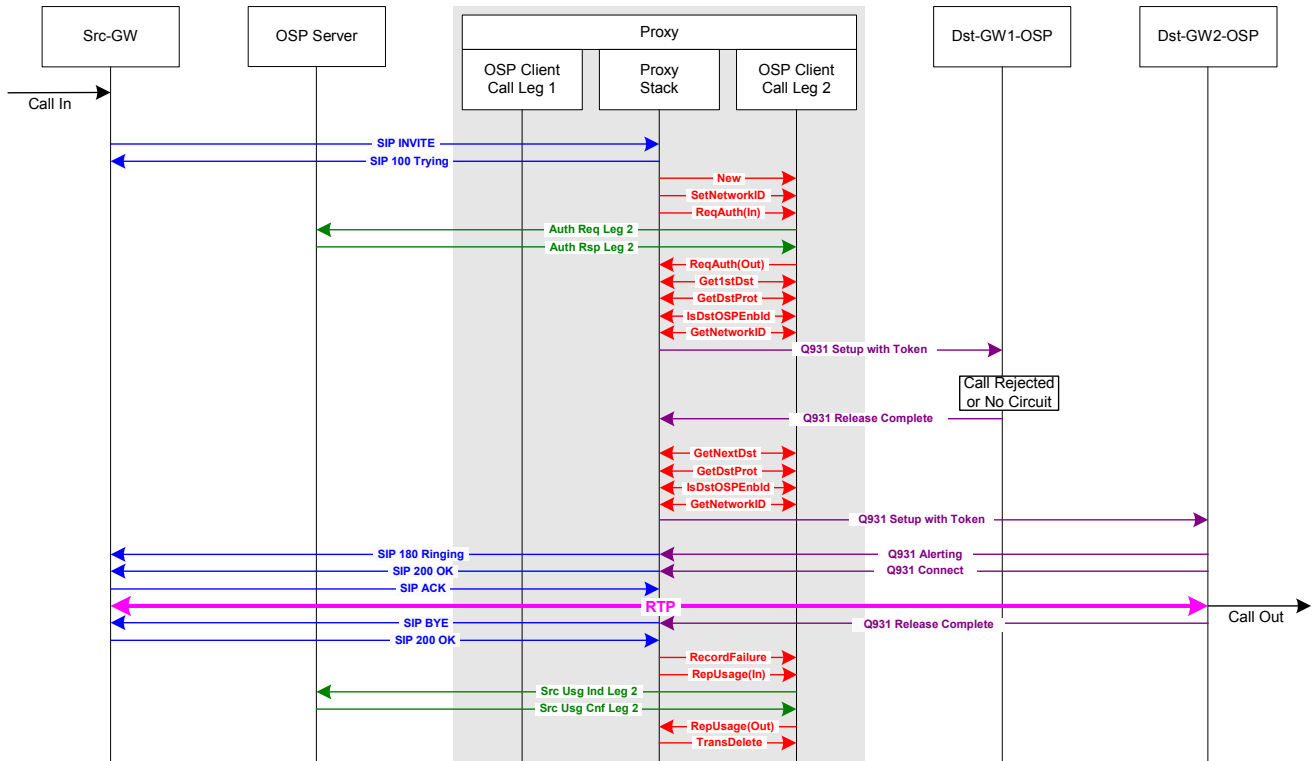
This subsection of cases tests call scenarios when the destination is an OSP enabled H.323 device. In these call scenarios, the proxy must include the OSP peering token, returned in the OSP AuthorizationResponse, in the Q931 call setup message to the destination H.323 device. The destination H.323 device, which must be enrolled with the OSP server, will extract the token from the Q931 Setup and validate the token was digitally signed by the OSP server. If the token is valid, the destination H.323 device will accept the call. If not, the Q931 Setup will be rejected by the destination H.323 device.

Subsection 2.1 presented failover (retry call attempt) test cases with non-OSP destination devices. This subsection presents failover test cases with OSP destination devices. The implementer should note that an OSP AuthorizationResponse can contain a list of multiple destination devices and that the list may contain OSP and non-OSP enabled destination devices. An OSP implementation with the inter-working proxy should allow for call attempt retries to multiple destination devices and the list of destination devices may be any combination of non-OSP and OSP enabled devices.

Configuration of VoIP devices on OSP server for test cases in section 2.2		
Device	Destination Protocol	OSP Version
Src-GW	SIP	0.0.0 (Not OSP Enabled)
Proxy	SIP or H323_Q931	2.1.1 or 4.1.1
Dst-GW1	H323_Q931	1.4.3, 2.1.1 or 4.1.1
Dst-GW2	H323_Q931	1.4.3, 2.1.1 or 4.1.1

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

### 2.2.1. Call Rejected or No Circuit and Retry



**Test Case 2.2.1: non-OSP SIP Source to Proxy to OSP H.323 Destination: Call Rejected or No Circuit & Retry**  
**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

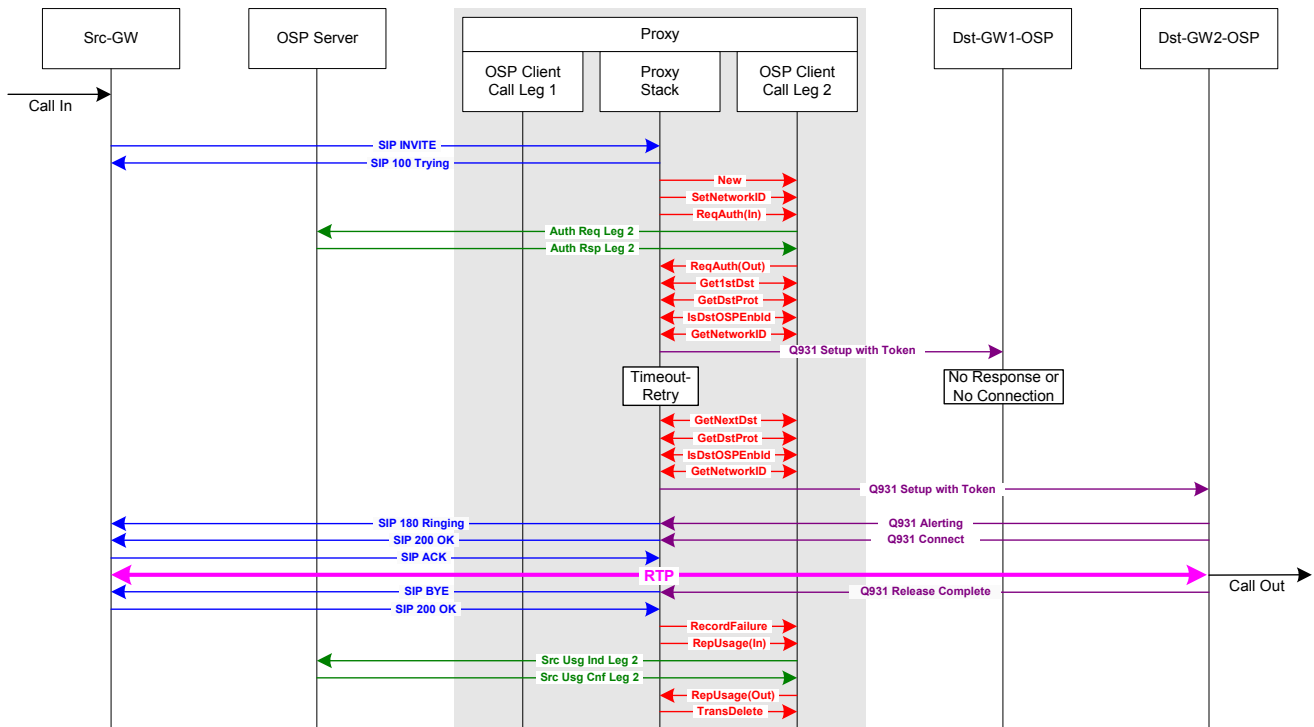
This test case is identical to test case 2.1.1 except that the OSP token returned in OSPPTTransactionRequestAuthorization function should be included in the Q931 Setup to the destination.

#### Expected CDRs for Test Case 2.2.1

This test case should generate two OSP UsageIndication messages, or CDRs, from the proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the first call attempt should be the response from Dst-GW1-OSP. In this example, the response is 21, but other responses are also valid. For the successful retry call, the proxy should set the FailureReason to 16 or 1016.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW1-OSP	21	0
2	source	Src-GW	Dst-GW2-OSP	16 or 1016	greater than 0

### 2.2.2. No Response or No Connection and Retry - Proxy Times Out



**Test Case 2.2.2: non-OSP SIP Source to Proxy to OSP H.323 Destination:  
No Response or No Connection & Retry - Proxy Times Out**

**Legend:** SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green

#### Test Case Notes

This test case is identical to test case 2.1.2 except that the OSP peering token returned in OSPPTtransactionRequestAuthorization function should be included in the Q931 call setup message to the destination.

This case tests the call scenarios when a destination H.323 device does not respond to the proxy. This test case requires that the OSP server return two or more destinations in the AuthorizationResponse to the proxy. After the first call attempt fails, the proxy must retry the call to second destination. This test case must be executed four times to test the following four different call scenarios.

1. The proxy cannot establish a TCP connection with Dst-GW1-OSP. After TCP time-out, the proxy should retry call to Dst-GW2-OSP. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 47 – resource unavailable, unspecified.)
2. No route to IP address of Dst-GW1-OSP device. The proxy should retry the call to Dst-GW2-OSP. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 2 – no route to specified transit network.)
3. TCP connection refused by destination. After TCP connection is refused, the proxy should retry the call to Dst-GW2-OSP. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

FailureReason for the first call attempt should be set to 63 – service or option not available, unspecified.)

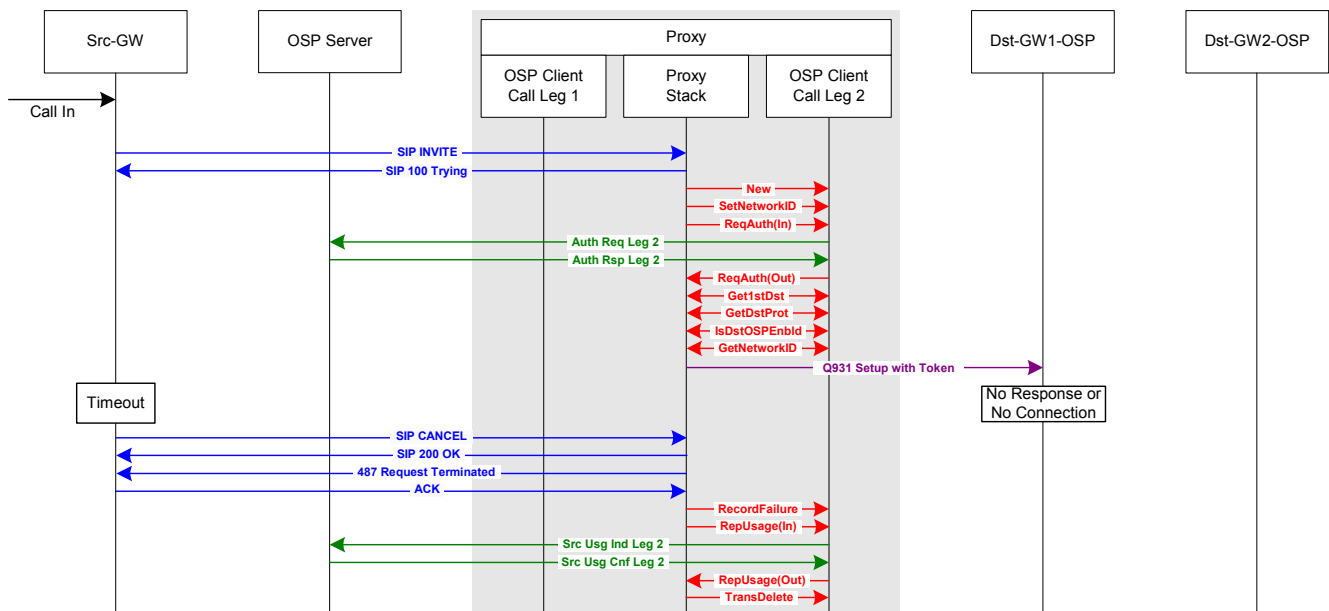
- No response from Dst-GW1-OSP device. the proxy establishes TCP connection with Dst-GW1-OSP, but Dst-GW1-OSP never responds to Q931 Setup. The proxy should time-out and retry the call to Dst-GW2-OSP. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 27 – destination out of order.)

### Expected CDRs for Test Case 2.2.2

This test case should generate two OSP UsageIndication messages, or CDRs, from the proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the first call attempt should be determined by the proxy based on the reason for the failure. For the successful retry of call leg 2, the proxy should set the FailureReason to 16 or 1016.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW1-OSP	47, 2, 63 or 27	0
2	source	Src-GW	Dst-GW2-OSP	16 or 1016	greater than 0

### 2.2.3. No Response or No Connection and Retry - Source Times Out



**Test Case 2.2.3: non-OSP SIP Source to Proxy to OSP H.323 Destination:  
No Response or No Connection & Retry - Source Times Out**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

### Test Case Notes

This test case identical to test case 2.1.3 except that the OSP peering token returned in OSPPTTransactionRequestAuthorization function should be included in the Q931 Setup to the destination. This case tests the call scenario when the source ends the call before the first destination Dst-GW1-OSP responds to the Q931 call setup from the proxy. In these cases, the proxy should terminate the call and report usage to the OSP. The OSP

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

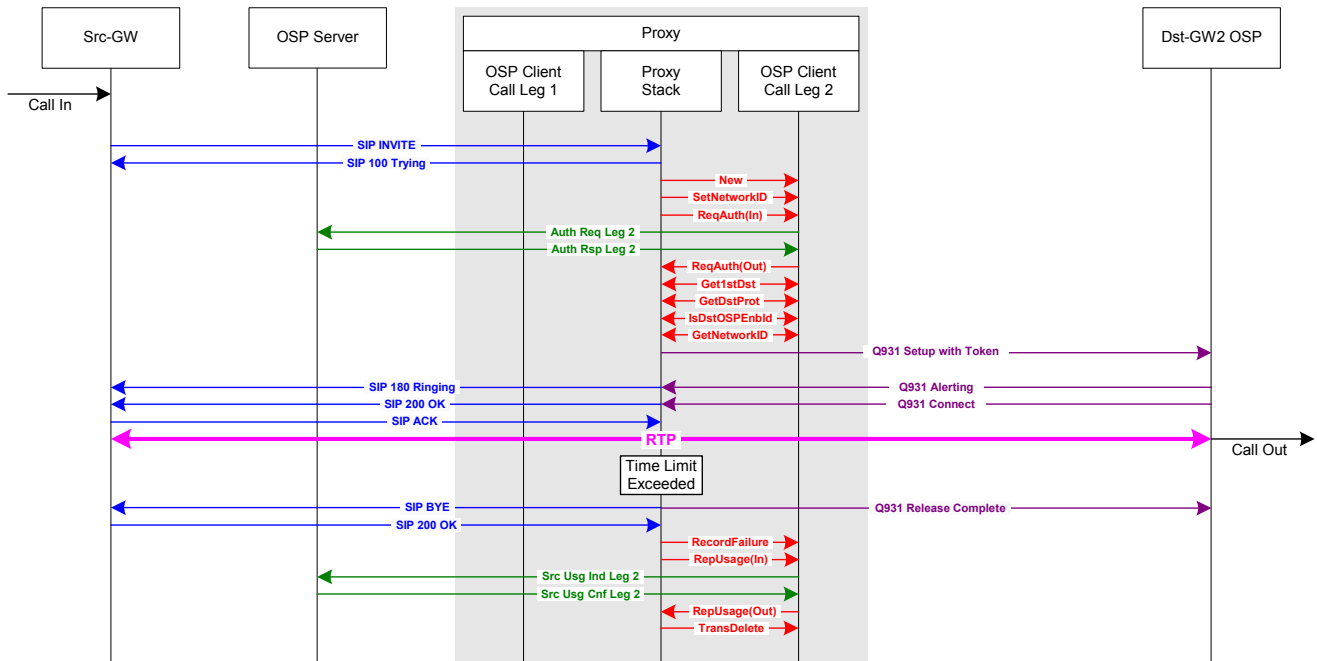
Toolkit parameter FailureReason reported with the OSPTransactionRecordFailure function should be set to the release cause reported in the SIP CANCEL message from the source device, Src-GW. If no release reason is reported in the SIP CANCEL message, the proxy should set the FailureReason to 487.

### Expected CDRs for Test Case 2.2.3

This test case should generate one OSP UsageIndication message, or CDR, from the proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the call attempt should be determined by the release reason included in the SIP CANCEL message from Src-GW. If no release reason is included in the SIP CANCEL message, the proxy should report a FailureReason of 487.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW1-OSP	487	0

### 2.2.4. Call Duration Limit Exceeded



**Test Case 2.2.4: non-OSP SIP Source to Proxy to OSP H.323 Destination: Time Limit Exceeded**  
**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

### Test Case Notes

This test case identical to test case 2.1.4 except that the OSP peering token returned in OSPTransactionRequestAuthorization function should be included in the Q931 Setup to the destination. This call scenario tests the proxy's ability to end a call when its authorized call duration has been exceeded. In the AuthorizationResponse, the OSP server includes the authorized call duration. The OSP Toolkit parameter ospvTimeLimit, returned in the GetFirstDestination or GetNextDestination function calls, defines the maximum duration for each call. The proxy should terminate a call when the call duration exceeds the TimeLimit. In this case, when the proxy forcefully ends a call that has exceeded its maximum call duration, the proxy should use the RecordFailure OSP

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

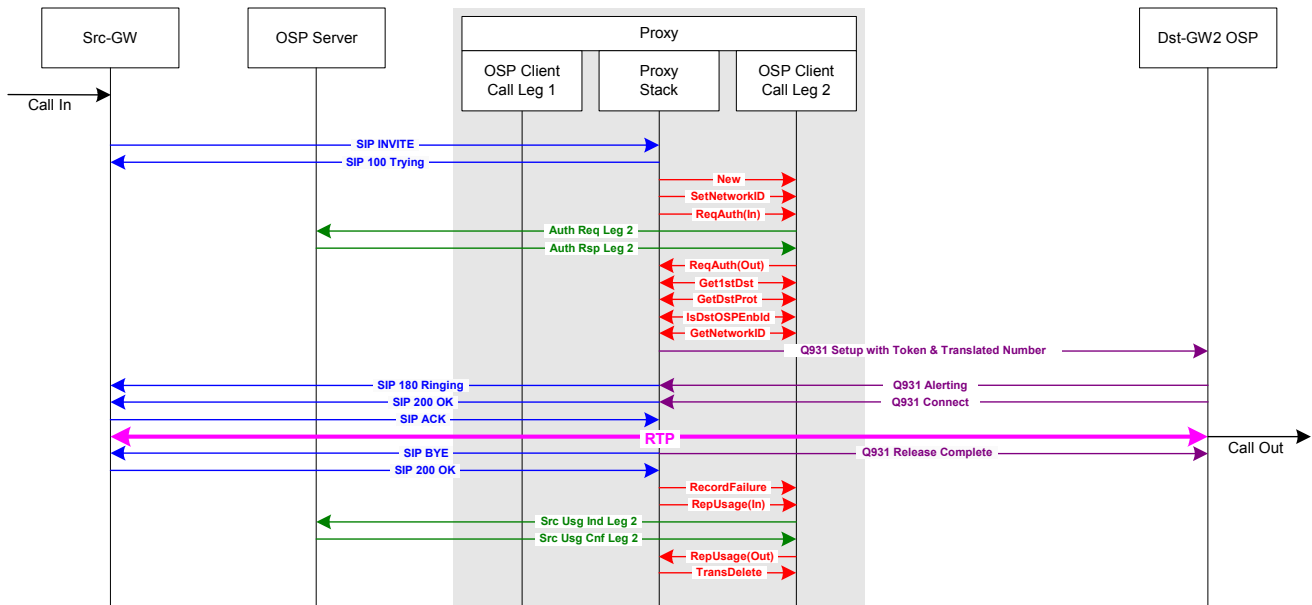
Toolkit function call to report a FailureReason of 8 (preemption) and then use the ReportUsage OSP Toolkit function call to send a UsageIndication call detail record to the OSP server.

### Expected CDRs for Test Case 2.2.4

This test case should generate one OSP UsageIndication message, or CDR, from the proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the call should be set by the proxy to 8 to indicate the call was forcefully shutdown by the proxy.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW2-OSP	8	greater than 0

### 2.2.5. Number Translation



Test Case 2.2.5: non-OSP SIP Source to Proxy to OSP H.323 Destination: Number Translation

Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green

### Test Case Notes

This test case identical to test case 2.1.6 except that the OSP peering token returned in OSPPTtransactionRequestAuthorization function should be included in the Q931 call setup message to the destination. This case tests the call scenario when the OSP server returns translated called and calling numbers in the OSP AuthorizationResponse to the proxy. When this occurs, the called and calling numbers in the Q931 call setup from the proxy to the destination gateway should be the translated called and calling numbers from the OSP AuthorizationResponse.

For this test case, the called and calling number translation rules are configured on the OSP server. The OSPPTtransactionGetFirstDestination function call returns the translated called and calling numbers. The OSPPTtransactionReportUsage function should report the un-translated called and calling numbers.

### Expected CDRs for Test Case 2.2.5

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

This test case should generate one OSP UsageIndication message, or CDR, from the proxy as the source of call leg 2. The called and calling numbers reported in the OSP UsageIndication message from the proxy, should be the called and calling numbers from the SIP INVITE received from the source gateway in call leg 1. The translated called and calling numbers should not be reported in the OSP UsageIndication message.

<b>Call Leg</b>	<b>Role</b>	<b>Source IP Address</b>	<b>Destination IP Address</b>	<b>Calling Number</b>	<b>Called Number</b>	<b>Release Reason or TC Code</b>	<b>Call Duration</b>
2	source	Src-GW	Dst-GW2-OSP	Not Translated	Not Translated	16 or 1016	greater than 0

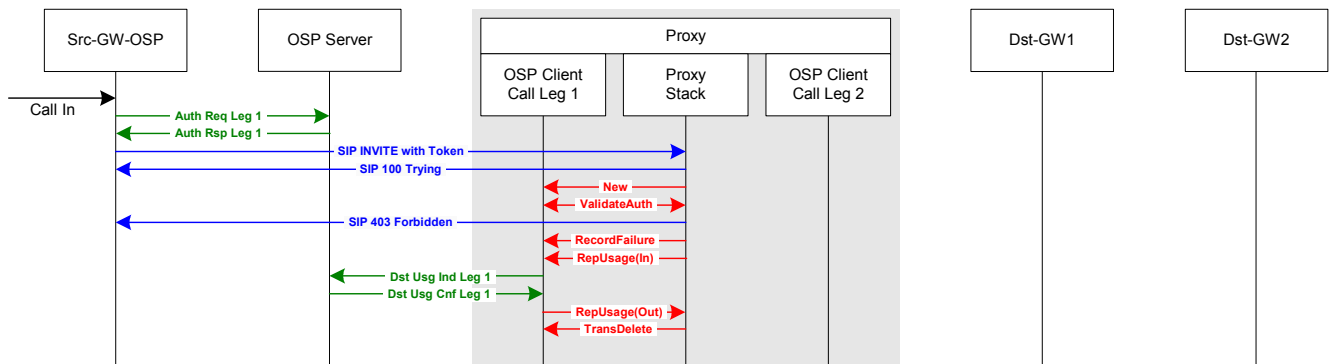
**Note:** OSP Toolkit version 3.3.3 and earlier report translated numbers in the CDR. Version 3.3.4 reports translated calling number and not translated called number.

### 2.3. OSP Source and non-OSP Destination

This subsection tests call scenarios when the source is an OSP enabled SIP device and the destination H.323 device is not OSP enabled. In these test cases, the proxy will receive a SIP INVITE message which includes an OSP peering token. The proxy must validate the digitally signed token to determine whether or not to accept the call. On the second call leg, the proxy must not include an OSP token in the Q931 Setup to the destination H.323 device since the destination H.323 device is not OSP enabled and cannot validate an OSP token.

Configuration of VoIP devices on OSP server for test cases in section 2.3		
Device	Destination Protocol	OSP Version
Src-GW-OSP	SIP	1.4.3, 2.1.1 or 4.1.1
Proxy	SIP or H323_Q931	2.1.1 or 4.1.1
Dst-GW1	H323_Q931	0.0.0 (OSP not enabled)
Dst-GW2	H323_Q931	0.0.0 (OSP not enabled)

#### 2.3.0. Invalid Authorization Token



**Test Case 2.3.0: OSP SIP Source to Proxy to non-OSP H.323 Destination: Invalid Authorization Token**  
**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

In this test case, the peering authorization token included in the SIP INVITE message cannot be validated by the proxy. The token could be invalid for different reasons such as: the token contents or digital signature has been corrupted, the token has expired, the token is not signed or the proxy does not have the public key of the OSP server that signed the authorization token (the public key is used to validate the digital signature).

The proxy responds to the source that the call is forbidden and then performs the OSP Toolkit function calls OSPPTTransactionRecordFailure and OSPPTTransactionReportUsage to create an OSP destination UsageIndication Call Detail Record which is sent to the OSP server. The FailureReason for this call should be 403.

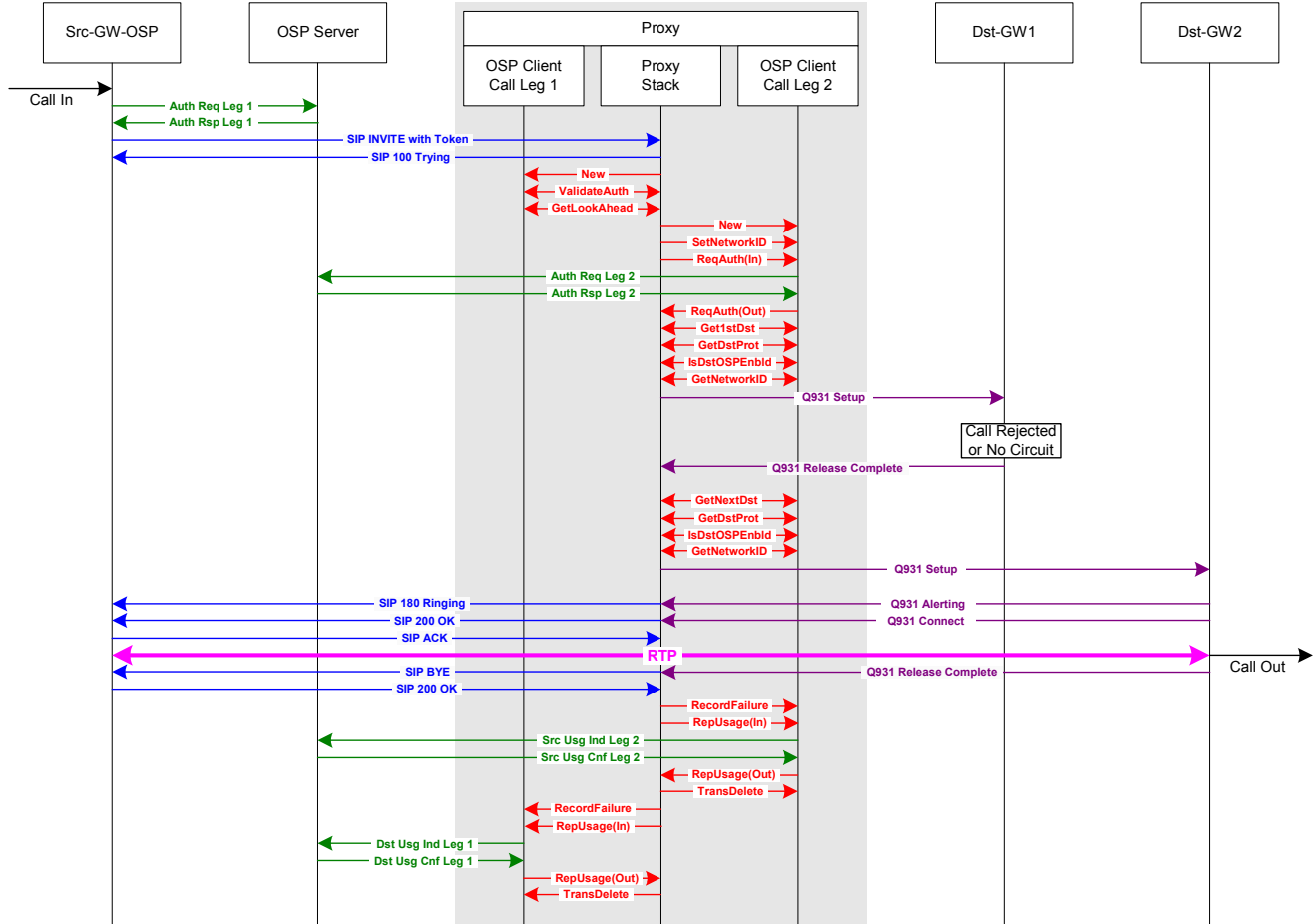
#### Expected CDR for Test Case 2.3.0

This test case should generate one OSP UsageIndication message, or CDR, from the proxy as the destination of call leg 1. The release reason (ospvFailureReason), or termination cause code, for the call should be set by the proxy to 403 to indicate the authorization token was invalid.

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1	destination	Src-GW-OSP	Proxy	403	0

### 2.3.1. Call Rejected or No Circuit and Retry



**Test Case 2.3.1: OSP SIP Source to Proxy to non-OSP H.323 Destination: Call Rejected or No Circuit & Retry**  
**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Detailed Description of Test Case

1. **Call In.** The call begins at the source SIP device.
2. **Auth Req Leg 1.** The source SIP device sends an OSP AuthorizationRequest to the OSP server.
3. **Auth Rsp Leg 1.** The OSP server returns the IP address, DestinationProtocol, and OSPVersion of the proxy, plus a signed authorization token, to the source SIP device.
4. **SIP INVITE with Token.** The source SIP device sends a SIP INVITE message to the proxy. The SIP INVITE message header includes an OSP authorization token.
5. **SIP 100 Trying.** The proxy receives the SIP INVITE message and responds.
6. **NEW.** The proxy recognizes the presence of an OSP authorization token in the SIP INVITE message and establishes a transaction with the OSP client to validate the token.

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

7. **ValidateAuth.** The proxy calls the OSP Toolkit function `OSPPTTransactionValidateAuthorisation` and passes the OSP peering token to the OSP client for validation. The OSP client determines if the token signature is valid and responds to the proxy. In this call scenario, the token is valid and the call processing continues. If the token was not valid, the proxy would end the transaction with the OSP client and reject the call (test case 2.3.0). An important variable passed in this function call is `ospvTimeLimit` – which is the maximum call duration authorized by the OSP server. If the call duration exceeds the authorized time limit, the proxy should end the call (test case 2.3.4).
8. **GetLookAhead.** The proxy calls the OSP Toolkit function `OSPPTTransactionGetLookAhead` to determine if routing information for the second call leg was embedded in the OSP token. In this test case, no Look Ahead Routing information is included in the token and the inter-working proxy must query the OSP server for a destination gateway to complete the second call leg. (test case 2.3.5 provides an explanation of Look Ahead Routing.)
9. **NEW.** The proxy does not have a route defined to complete the call to the dialed number. The proxy will query an OSP server for a route to an inter-domain destination to complete the call. The proxy establishes a new transaction with the OSP client using `OSPPTTransactionNew` function.
10. **SetNetworkID.** The `OSPPTTransactionSetNetworkIds` function call identifies the trunk group or partition in the source device which originated the call. In this test case, where the proxy is acting as a proxy, the `ospvSrcNetworkId` (trunk group or partition of the source device) must be taken from the SIP INVITE from the source device. The `SrcNetworkId` is included in the `AuthorizationRequest` to the OSP server and may be used by the OSP server operator for routing and billing of calls by source trunk group or partition.
11. **ReqAuth(In).** The proxy calls the OSP client function `OSPPTTransactionRequestAuthorisation`.
12. **Auth Req Leg 2.** The OSP client sends an `OSP AuthorizationRequest` to the OSP server requesting a list of devices which can complete the call. The OSP request includes the calling and called telephone numbers, and the IP address of the source SIP device.
13. **Auth Rsp Leg 2.** The OSP server sends an `OSP AuthorizationResponse` to the OSP client. The response includes the IP addresses of two destination devices, the signaling protocol required by the destination devices and the version of OSP supported.
14. **ReqAuth(Out).** The OSP Toolkit responds to the proxy that the `OSPPTTransactionRequestAuthorisation` function is complete.
15. **Get1stDst.** The proxy calls the OSP Toolkit function `OSPPTTransactionGetFirstDestination` to get the IP address of the first destination gateway.
16. **GetDstProt.** The proxy calls the OSP Toolkit function `OSPPTTransactionGetDestProtocol` to get the signaling protocol required by the destination H.323 device. In this case, the `DestinationProtocol` is `H323_Q931`. If `DestinationProtocol` is not supported by the proxy (i.e. `H323_LRQ` or `IAX`), the proxy

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

should reject the call and report a FailureReason of 111 (test case 2.1.5). If DestinationProtocol is unknown or undefined, the proxy may reject the destination and report a FailureReason of 111 or attempt the call to the destination using the proxy's default signaling protocol.

17. **IsDstOSPEnabled.** The OSPPTTransactionDestOSPEnabled function tells the proxy whether or not the destination device is OSP enabled and capable of validating the OSP authorization token. In this case the destination H.323 device is not OSP enabled (OSPE\_OSP\_FALSE). The proxy should not include the OSP authorization token in the Q931 Setup to the destination device. (Note, to ensure backward compatibility with OSP V1.4.3, if OSPE\_OSP is unknown or undefined, the proxy should assume the destination is OSP enabled and include the OSP authorization token in the Q931 Setup to the destination.)
18. **GetNetworkID.** The proxy calls the OSP Toolkit function OSPPTTransactionGetDestNetworkID to get the destination trunk group if it is available. If the destination trunk group is available, it should be included in the Q931 call setup message to the destination.
19. **Q931 Setup.** The proxy sends a Q931 call setup message to the first destination H.323 device. An OSP authorization token is not included in the Q931 Setup since the destination gateway does not support OSP. Note: If source trunk group was included in the SIP INVITE from the source device, it should NOT be included in the Q931 Setup to the destination.
20. **Q931 Release Complete.** The destination H.323 device does not accept the call setup and returns a 21 Call Rejected to the proxy. This test case applies for any case when the destination H.323 device rejects the Q931 Setup. The call may be rejected for a variety of reasons such as unauthorized access or no circuits available.
21. **GetNextDst.** The proxy retries the call to the second destination and calls OSP Toolkit function OSPPTTransactionGetNextDestination to obtain the IP address of the next destination H.323 device. The GetNextDestination function call should include the FailureReason for the previous failed call attempt. In this case the FailureReason should be the release cause reported by the destination or 21.
22. **GetDstProt.** The proxy calls the OSP Toolkit function OSPPTTransactionGetDestProtocol to get the signaling protocol required by the destination H.323 device. In this case, the DestinationProtocol is H323\_Q931. If DestinationProtocol is not supported by the proxy (i.e. SIP, H323\_LRQ or IAX), the proxy should reject the destination and report a FailureReason of 111 (test case 2.1.5). If DestinationProtocol is unknown or undefined, the proxy may either reject the destination and report a FailureReason of 111 or attempt a call setup to the destination using the default signaling protocol of the proxy.
23. **IsDstOSPEnabled.** The OSPPTTransactionDestOSPEnabled function tells the proxy whether or not the destination device is OSP enabled and capable of validating the OSP authorization token. In this case the destination H.323 device is not OSP enabled (OSPE\_OSP\_FALSE). The proxy should not include the OSP peering authorization token in the Q931 call setup message to the destination device. (Note, to ensure backward compatibility with OSP V1.4.3, if OSPE\_OSP is unknown or

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

undefined, the proxy should assume the destination is OSP enabled and include the OSP authorization token in the Q931 Setup to the destination.)

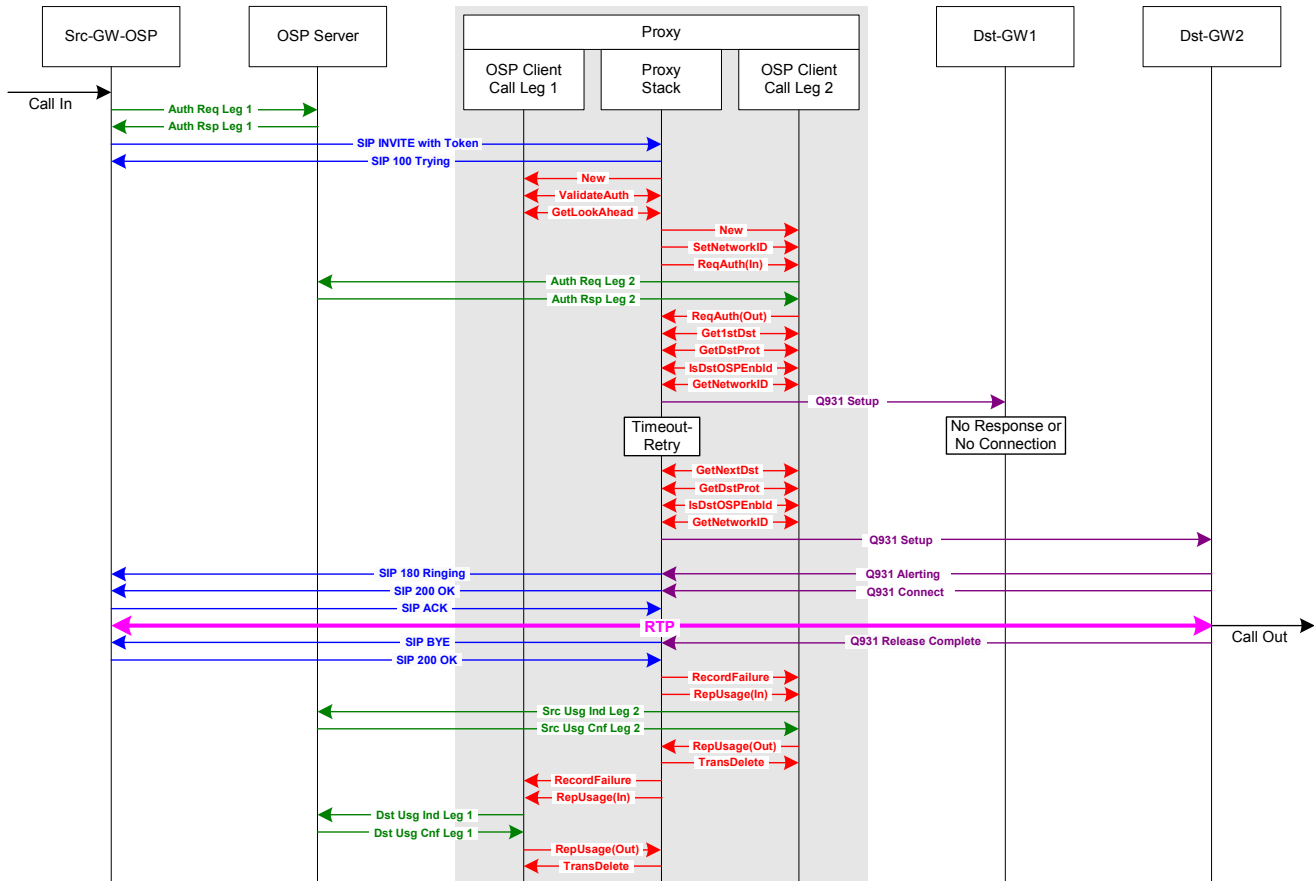
24. **GetNetworkID**. The proxy calls the OSP Toolkit function OSPPGetDestNetworkID to get the destination trunk group if it is available. If the destination trunk group is available, it should be included in the Q931 call setup message to the destination.
25. – 35. Standard SIP to H.323 communications for the completing the call.
36. **RecordFailure**. At the completion of the call, the proxy reports the call disconnect reason for the successful retry of the second call leg, to the OSP Toolkit using the OSPPTTransactionRecordFailure function.
37. **RepUsage(In)**. The proxy calls the OSPPTTransactionReportUsage function to report the call duration for the second call leg.
38. **Src Usg Ind Leg 2**. The OSP client sends an OSP UsageIndication message (Call Detail Record) to the OSP server. The UsageIndication is a type ‘source’ call detail record since the proxy is the source device for the second leg of the call.
39. **Src Usg Cnf Leg 2**. The OSP server responds with an OSP UsageConfirmation message.
40. **RepUsage(Out)**. The OSP Toolkit closes the ReportUsage transaction.
41. **TransDelete**. The proxy deletes the OSP Toolkit transaction for the second call leg.
42. **RecordFailure**. The proxy reports the call disconnect reason, for the first call leg, to the OSP Toolkit using the OSPPTTransactionRecordFailure function.
43. **RepUsage(In)**. The proxy calls the OSPPTTransactionReportUsage function to report the call duration for the first call leg.
44. **Src Usg Ind Leg 1**. The OSP client sends an OSP UsageIndication message (Call Detail Record) to the OSP server. The UsageIndication is a type ‘destination’ call detail record since the proxy is the destination device for the first leg of the call.
45. **Src Usg Cnf Leg 1**. The OSP server responds with an OSP UsageConfirmation message.
46. **RepUsage(Out)**. The OSP Toolkit closes the ReportUsage transaction.
47. **TransDelete**. The proxy deletes the OSP Toolkit transaction for the first call leg.

### Expected CDRs for Test Case 2.3.1

This test case should generate three OSP UsageIndication messages, or CDRs, from the proxy. Two CDRs as the source of call leg 2 and one CDR as the destination of call leg 1. The release reason (ospvFailureReason) in the source CDR for call leg 2 for the first call attempt should be the response from Dst-GW1. In this example, the response is 21, but other responses are also valid. For the successful retry for call leg 2, the proxy should set the FailureReason to 16 or 1016 in the source CDR. For the destination CDR for call leg 1, the FailureReason should also be set to 16 or 1016 by the proxy.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	Source	Src-GW-OSP	Dst-GW1	21	0
2	Source	Src-GW-OSP	Dst-GW2	16 or 1016	greater than 0
1	destination	Src-GW-OSP	Proxy	16 or 1016	greater than 0

2.3.2. No Response or No Connection and Retry - Proxy Times Out



Test Case 2.3.2: OSP SIP Source to Proxy to non-OSP H.323 Destination:  
No Response or No Connection & Retry - Proxy Times Out

Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

This case tests the call scenarios when a destination H.323 device does not respond to the proxy. This test case requires that the OSP server return two or more destinations in the AuthorizationResponse to the proxy. After the first call attempt fails, the proxy must retry the call to second destination. This test case must be executed four times to test the following four different call scenarios.

1. The proxy cannot establish a TCP connection with Dst-GW1. After TCP time-out, the proxy should retry call to Dst-GW2. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 47 – resource unavailable, unspecified.)
2. No route to IP address of Dst-GW1 IP device. The proxy should retry call to Dst-GW2. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 2 – no route to specified transit network.)
3. TCP connection refused by destination Dst-GW1. After TCP connection is refused, the proxy should retry the call to Dst-GW2. (When OSP Toolkit function

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

GetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 63 – service or option not available, unspecified.)

4. No response from Dst-GW1. The proxy establishes TCP connection with Dst-GW1, but Dst-GW1 never responds to Q931 Setup. The proxy should time-out and retry the call to Dst-GW2. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 27 – destination out of order.)

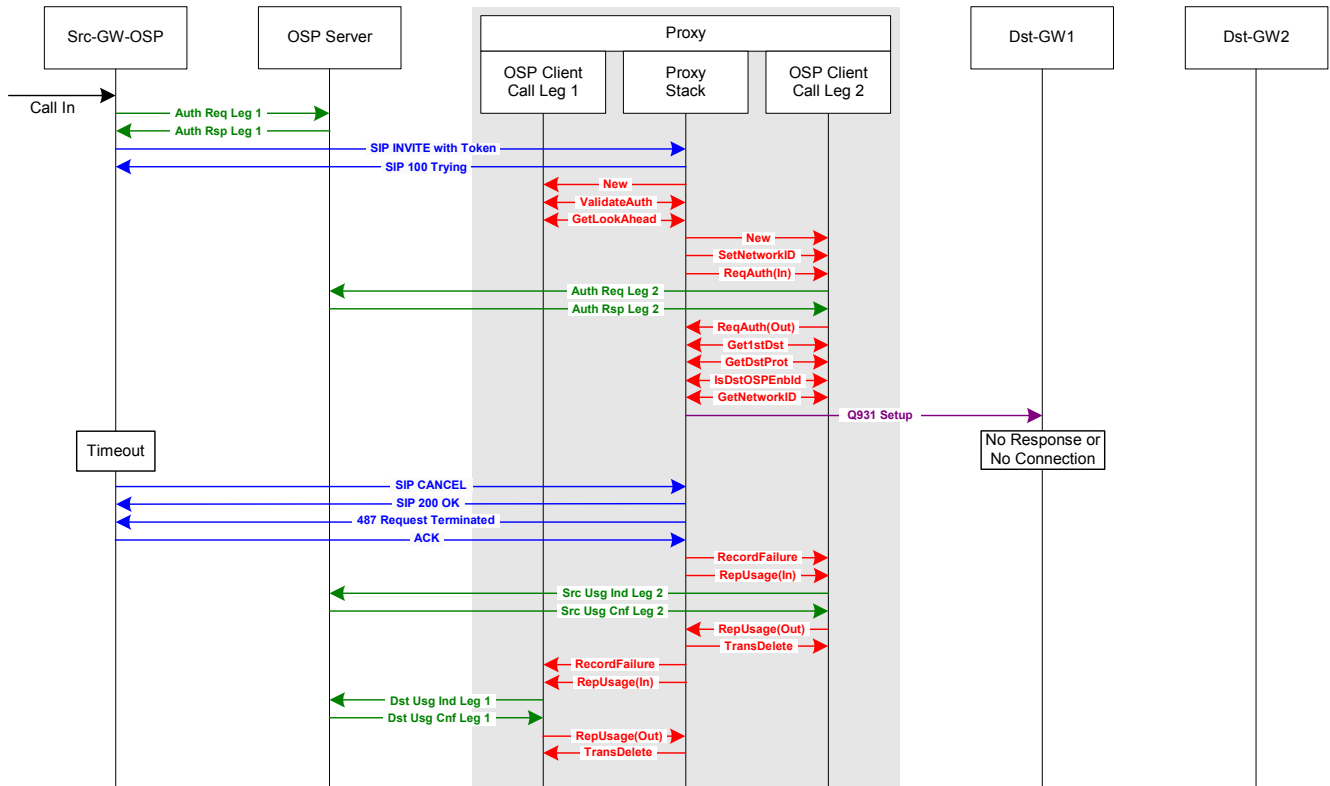
**Note:** The destination UsageIndication call detail record for call leg one, should have FailureReason set to the release code for the last call attempt.

### Expected CDRs for Test Case 2.3.3

This test case should generate three OSP UsageIndication messages, or CDRs, from the proxy. Two CDRs created as the source of call leg 2 and one CDR as the destination of call leg 1. The release reason (ospvFailureReason), or termination cause code, for the first attempt of call leg 2 should be determined by the proxy based on the reason for the failure. For the successful retry of call leg 2, the proxy should set the FailureReason to 16 or 1016. The FailureReason for the destination CDR of call leg 1 should be 16 or 1016.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW-OSP	Dst-GW1	47, 2, 63 or 27	0
2	source	Src-GW-OSP	Dst-GW2	16 or 1016	greater than 0
1	destination	Src-GW-OSP	Proxy	16 or 1016	greater than 0

2.3.3. No Response or No Connection and Retry - Source Times Out



Test Case 2.3.3: OSP SIP Source to Proxy to non-OSP H.323 Destination: No Response or No Connection & Retry - Source Times Out

Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

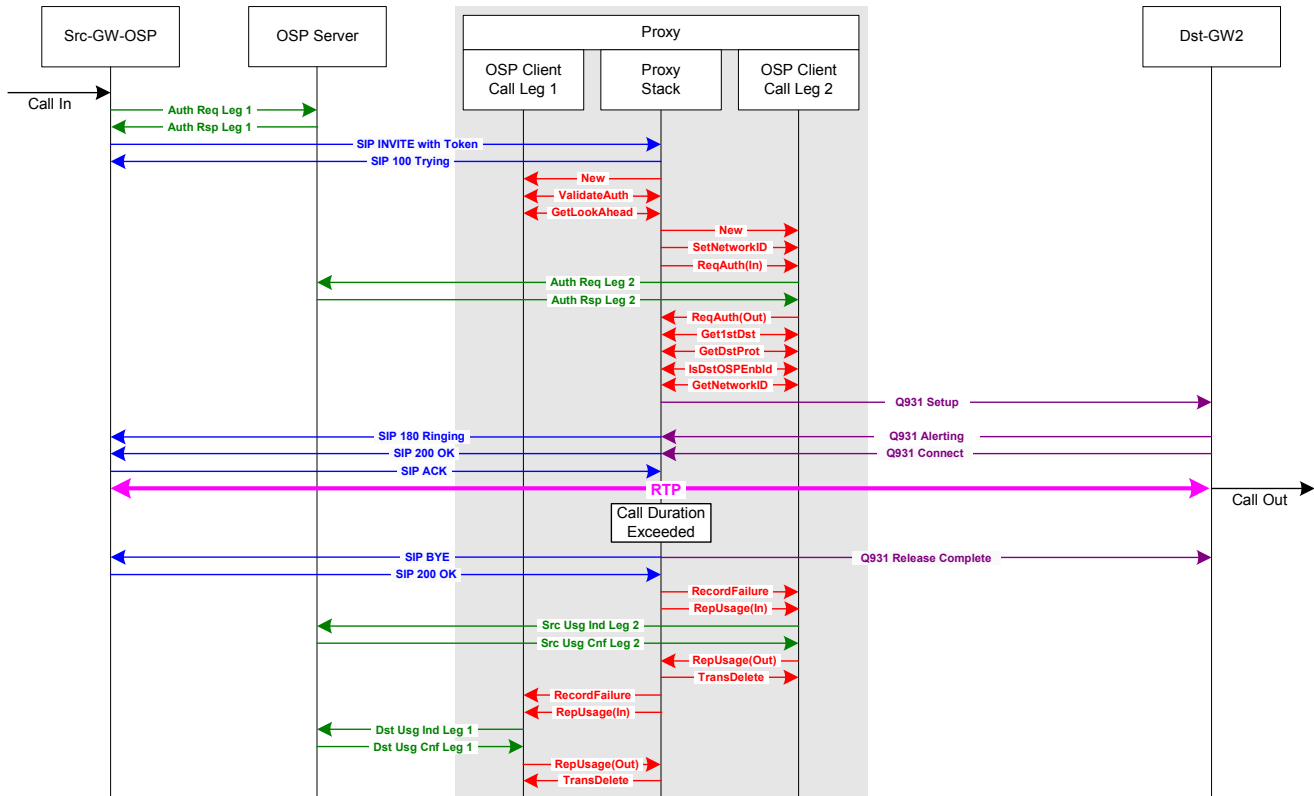
This case tests the call scenario when the source ends the call before the first destination Dst-GW1 responds to the Q931 Setup from the proxy. In these cases, the proxy should terminate the call and report usage to the OSP server. The OSP Toolkit parameter FailureReason reported with the OSPPTtransactionRecordFailure function should be set to the release cause reported in the SIP CANCEL message from the source device, Src-GW. If no release reason is reported in the SIP CANCEL message, the proxy should set the FailureReason to 487. The FailureReason should be the same and included in the RecordFailure function for both the source UsageIndication call detail record for call leg two and the destination UsageIndication call detail record for call leg one.

Expected CDRs for Test Case 2.3.3

This test case should generate two OSP UsageIndication messages, or CDRs, from the proxy. One CDR as the source of call leg 2 and another as the destination of call leg 1. The release reason (ospvFailureReason), or TC code, for the CDRs is determined by the release reason in the SIP CANCEL message from Src-GW-OSP. If no release reason is included in the SIP CANCEL message, the proxy should report a FailureReason of 487.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW-OSP	Dst-GW1	487	0
1	destination	Src-GW-OSP	Proxy	487	0

### 2.3.4. Call Duration Limit Exceeded



**Test Case 2.3.4: OSP SIP Source to Proxy to non-OSP H.323 Destination: Call Duration Limit Exceeded**  
**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

This call scenario tests the proxy’s ability to end a call when its authorized call duration has been exceeded. In the AuthorizationResponse, the OSP server includes the authorized call duration. The OSP Toolkit parameter `ospvTimeLimit`, returned in the `GetFirstDestination` or `GetNextDestination` function calls, defines the maximum duration for each call. The proxy should terminate a call when the call duration exceeds the `TimeLimit`. In this case, when the proxy forcefully ends a call that has exceeded its maximum call duration, the proxy should use the `RecordFailure` OSP Toolkit function call to report a `FailureReason` of 8 (preemption) and then use the `ReportUsage` OSP Toolkit function call to send a `UsageIndication` call detail record to the OSP server.

**Note:** In this call scenario, there are two authorized call durations. The authorized call duration for call leg one is defined by the `ospvTimeLimit` variable returned by the `OSPPTtransactionValidateAuthorization` function. The authorized call duration for call leg two is defined by the `ospvTimeLimit` variable returned by the `OSPPTtransactionGetFirstDestination` or `OSPPTtransactionGetNextDestination` functions. When the `ospvTimeLimit` for call leg one and two are different, the shorter `TimeLimit` takes priority and should be used by the proxy to determine when to forcefully end a call.

#### Expected CDRs for Test Case 2.3.4

This test case should generate two OSP `UsageIndication` messages, or CDRs. One from the proxy as the source of call leg 2 and another as the destination for call leg 1. The

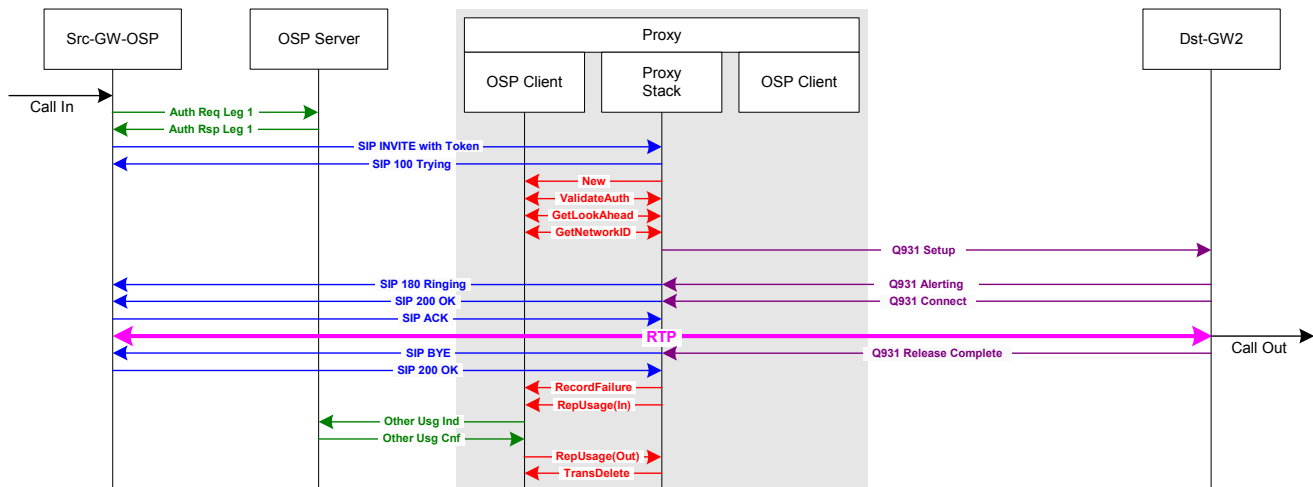
## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

release reason (ospvFailureReason), or termination cause code, for the call should be set by the proxy to 8 to indicate the call was forcefully shutdown by the proxy.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW-OSP	Dst-GW2	8	greater than 0
1	destination	Src-GW-OSP	Proxy	8	greater than 0

### 2.3.5. Look Ahead Routing

Look Ahead Routing is a unique application OSP peering for proxies. In this test case for Look Ahead Routing the IP address, destination protocol, OSP version and destination trunk group of the destination device are embedded in the OSP authorization token sent from the source device to the proxy. When the proxy validates the OSP token, the proxy calls the function OSPTransactionGetLookAheadInfoIfPresent. If Look Ahead Routing information is available, it is passed from the OSP client to the proxy and eliminates the need for a second lookup to the OSP server. Note that only one OSP Toolkit transaction between the proxy and the OSP Toolkit is required when Look Ahead Routing is used.



Test Case 2.3.5: OSP SIP Source to Proxy to non-OSP H.323 Destination: Look Ahead Routing

Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green

#### Test Case Notes

V3.3.6, and earlier versions, of the OSP Toolkit support only a single Look Ahead route embedded in an OSP authorization token. Future releases of the OSP Toolkit will support multiple destinations in a Look Ahead token so the proxy can retry the call to other destinations if the call attempt to the first destination fails.

#### Detailed Description of Test Case

1. **Call In.** The call begins at the source SIP device.
2. **Auth Req Leg 1.** The source SIP device sends an OSP AuthorizationRequest to the OSP server.
3. **Auth Rsp Leg 1.** The OSP server returns the IP address, DestinationProtocol, and OSPVersion of the proxy, plus a signed authorization token, to the source SIP device.
4. **SIP INVITE with Token.** The source SIP device sends a SIP INVITE message to the proxy. The SIP INVITE message header includes an OSP authorization token.

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

5. **SIP 100 Trying.** The proxy receives the SIP INVITE message and responds.
6. **NEW.** The proxy recognizes the presence of an OSP peering authorization token in the SIP INVITE message and establishes a transaction with the OSP Toolkit to validate the token.
7. **ValidateAuth.** The proxy calls the OSP Toolkit function `OSPPTTransactionValidateAuthorisation` and passes the OSP peering token to the OSP Toolkit for validation. The OSP Toolkit determines if the token signature is valid and responds to the proxy. In this call scenario, the token is valid and the call processing continues. If the token was not valid, the proxy would end the transaction with the OSP Toolkit and reject the call (test case 2.3.0). An important variable passed in this function call is `ospvTimeLimit` – which is the maximum call duration authorized by the OSP server. When the call duration exceeds the authorized time limit, the proxy should end the call (test case 2.3.4).
8. **GetLookAhead.** The proxy calls the OSP Toolkit function `OSPPTTransactionGetLookAheadInfoIfPresent` to determine if routing information for the second call leg was embedded in the OSP token. In this test case, Look Ahead Routing information is present and the function call returns the destination IP address, the destination protocol (`OSPE_DEST_PROT`) and the destination OSP enabled status (`OSPE_OSP`). For this test case, the expected value for `OSPE_DEST_PROT` is `H323_Q931`.

**Note:** If `OSPE_DEST_PROT` is a protocol not supported by the proxy, such as `H323_LRQ` or `IAX`, the proxy should reject the call and report a `FailureReason` of 111 (protocol error). If `OSPE_DEST_PROT` is `UNDEFINED` or `UNKNOWN`, the proxy may either reject the destination and record `FailureReason` 111 or attempt the call to the destination using the proxy's default signaling protocol.

**Note:** For this test case, the expected value for `OSPE_OSP` is `FALSE`. The Look Ahead destination is not OSP enabled, therefore no token should be included in the Q931 call setup message to the destination. A value of `OSPE_OSP_TRUE` indicates that the Look Ahead destination is OSP enabled and that the LookAhead token should be included, as is, in the Q931 call setup message to the destination. If `OSPE_OSP` is `UNKNOWN` or `UNDEFINED`, the proxy should assume the Look Ahead destination is OSP enabled and include the Look Ahead token in the Q931 Setup to the destination.
9. **GetNetworkID.** The proxy calls the OSP client Toolkit function `OSPPTTransactionGetDestNetworkID` to get the destination trunk group if it is available. The Look Ahead token may also include the destination trunk group of the destination device. If the destination trunk group is available, it should be included in the Q931 call setup message to the destination.
10. **Q931 Setup.** The proxy sends a Q931 call setup message to the H.323 destination device. An OSP peering authorization token is not included in the Q931 Setup since the destination gateway does not support OSP. Note: If source trunk group was included in the SIP INVITE from the source device, it should NOT be included in the Q931 Setup from the proxy to the destination.
11. – 20. Standard SIP to H.323 communications for the completing the call.

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

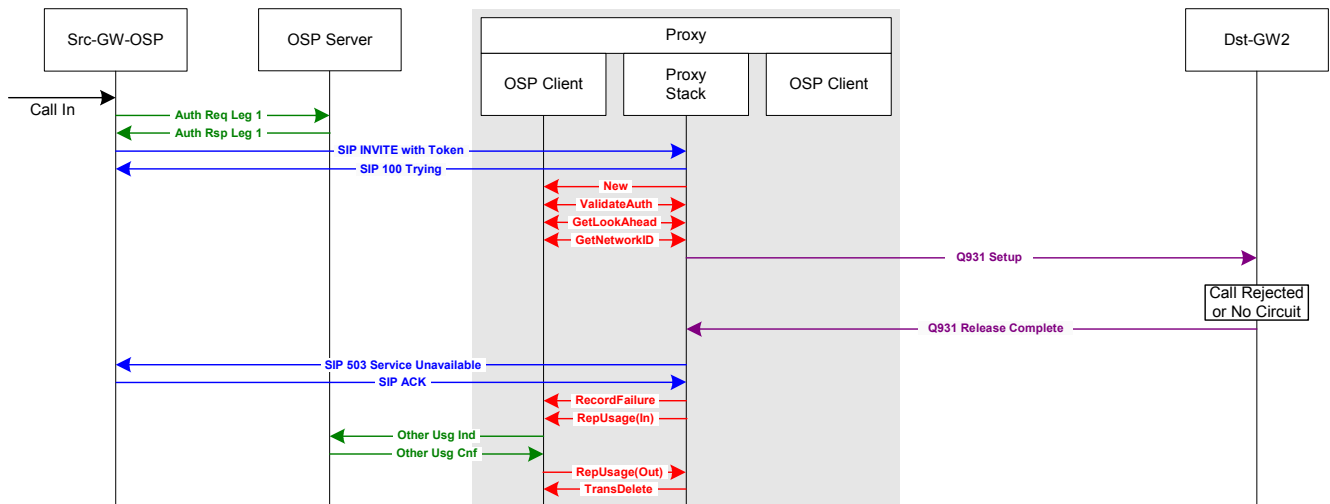
21. **RecordFailure**. At the completion of the call, the proxy reports the call disconnect reason for the call to the OSP Toolkit using the OSPTransactionRecordFailure function.
22. **RepUsage(In)**. The proxy calls the OSPTransactionReportUsage function to report the call duration for the second call leg.
23. **Other Usg Ind**. The OSP client sends an OSP UsageIndication message (Call Detail Record) to the OSP server. The UsageIndication is a type 'other' call detail record. In a Look Ahead call scenario, the proxy is the destination device for the first call leg and the source device for the second call leg.
24. **Other Usg Cnf**. The OSP server responds with an OSP UsageConfirmation message.
25. **RepUsage(Out)**. The OSP Toolkit closes the ReportUsage transaction.
26. **TransDelete**. The proxy deletes the OSP Toolkit transaction for the call.

### Expected CDR for Test Case 2.3.5

This test case should generate one OSP UsageIndication message, or CDR, from the proxy. Look Ahead Routing is a unique case when one OSP Toolkit transaction validates inbound call leg 1 and routes outbound call leg 2. Since one CDR is used to report usage for both the destination of call leg 1 and the source of call leg 2, the role is defined as other. As with other call scenarios, the FailureReason should be determined by the release code included in a SIP BYE header from the source SIP device, or by the H.323 response from destination H.323 device. If the call is successful and there is no release code reported, the proxy should report the FailureReason as 16 or 1016 to the OSP Toolkit ReportUsage function.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2	16 or 1016	greater than 0

### 2.3.6. Look Ahead Routing: Call Rejected or No Circuit



**Test Case 2.3.6: OSP SIP Source to Proxy to non-OSP H.323 Destination:  
Look Ahead Routing - Call Rejected or No Circuit & Retry**

Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

### Test Case Notes

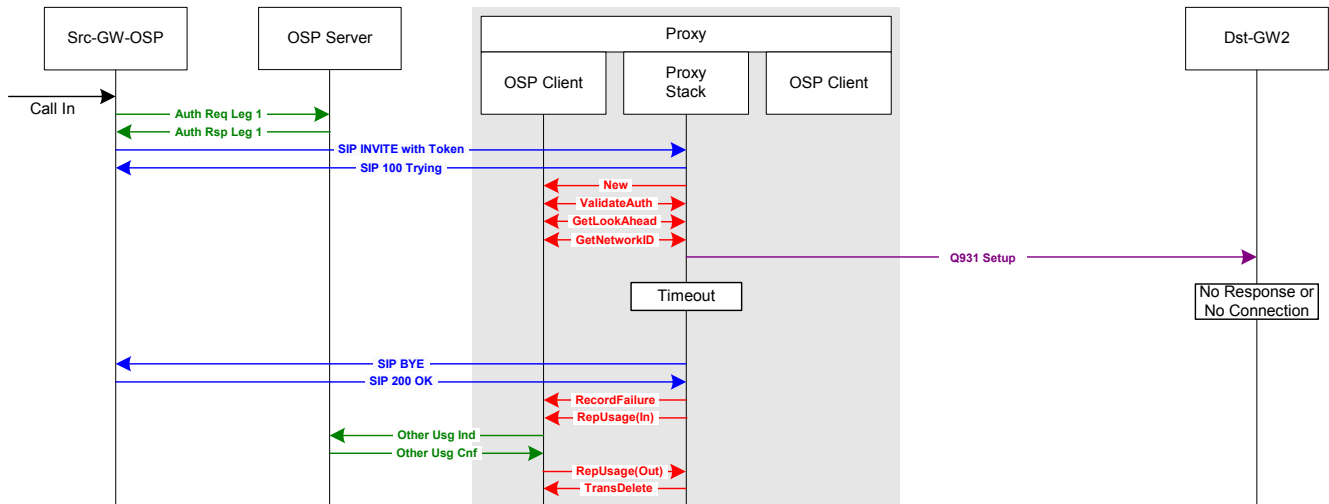
This case is similar to test case 2.3.1 and tests a Look Ahead call scenario when the destination H.323 device rejects the call.

### Expected CDR for Test Case 2.3.6

This test case should generate one OSP UsageIndication message, or CDR, from the proxy. The role should be 'other' and the FailureReason should be determined by the response from the destination H.323 device. In this example, the response is 21, but other responses are also valid.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2	21	0

### 2.3.7. Look Ahead Routing: No Response or No Connection - Proxy Times Out



**Test Case 2.3.7: OSP SIP Source to Proxy to non-OSP H.323 Destination: Look Ahead Routing - No Response or No Connection - Proxy Times Out**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

### Test Case Notes

This case is similar to test case 2.3.2 and tests a Look Ahead call scenario when the destination H.323 device does not respond to the proxy. This test case must be executed four times to test the following four different call scenarios.

1. The proxy cannot establish a TCP connection with Dst-GW1. After TCP time-out, the proxy should retry call to Dst-GW2. (When OSP Toolkit function RecordFailure is called, the FailureReason for the call attempt should be set to 47 – resource unavailable, unspecified.)
2. No route to IP address of Dst-GW1. The proxy should retry call to Dst-GW2. (When OSP Toolkit function RecordFailure is called, the FailureReason for the call attempt should be set to 2 – no route to specified transit network.)
3. TCP connection refused by destination. After TCP connection is refused, the proxy should retry the call to Dst-GW2. (When OSP Toolkit function RecordFailure is

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

called, the FailureReason for the call attempt should be set to 63 – service or option not available, unspecified.)

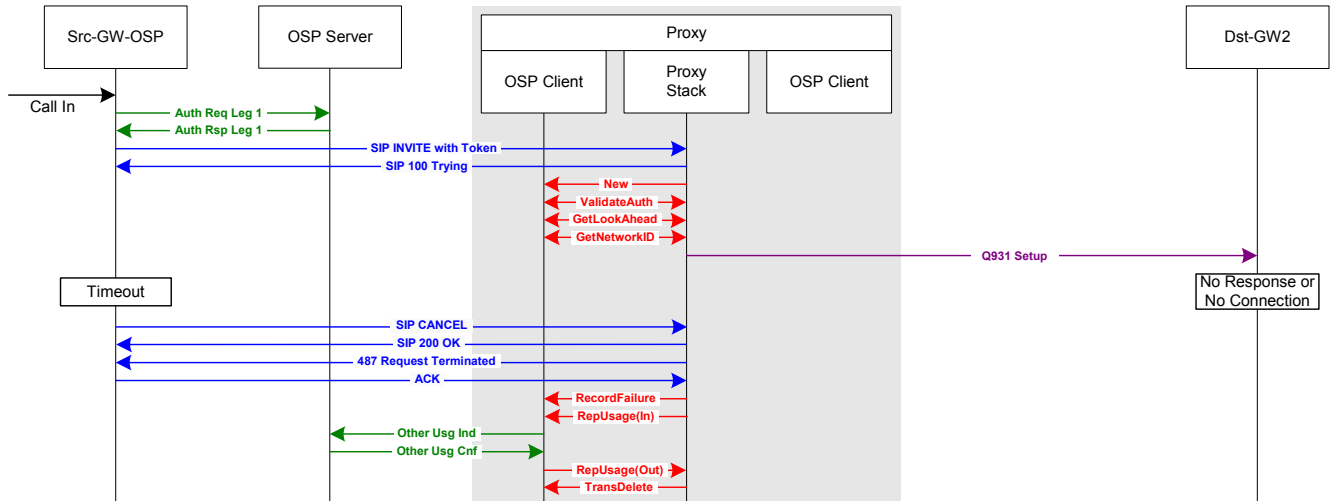
- No response from Dst-GW1. The proxy establishes TCP connection with Dst-GW1, but Dst-GW1 never responds to Q931 Setup. The proxy should time-out and retry the call to Dst-GW2. (When OSP Toolkit function RecordFailure is called, the FailureReason for the call attempt should be set to 27 – destination out of order.)

### Expected CDR for Test Case 2.3.7

This test case should generate one OSP UsageIndication message, or CDR, from the proxy. The role should be ‘other’ and the FailureReason should be determined by the proxy based on the failure reasons described above.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2	47, 2, 63 or 27	0

### 2.3.8. Look Ahead Routing: No Response or No Connection - Source Times Out



**Test Case 2.3.8: OSP SIP Source to Proxy to non-OSP H.323 Destination: Look Ahead Routing - No Response or No Connection - Source Times Out**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

### Test Case Notes

This test case is similar to test case 2.3.3 and tests the Look Ahead call scenario when the source ends the call before the destination Dst-GW2 responds to the Q931 Setup from the proxy. In this case, the proxy should terminate the call and report usage to the OSP server. The OSP Toolkit parameter FailureReason reported with the OSPTransactionRecordFailure function should be set to the release cause reported in the SIP CANCEL message from the source device, Src-GW. If no release reason is reported in the SIP CANCEL message, the proxy should set the FailureReason to 487.

### Expected CDR for Test Case 2.3.8

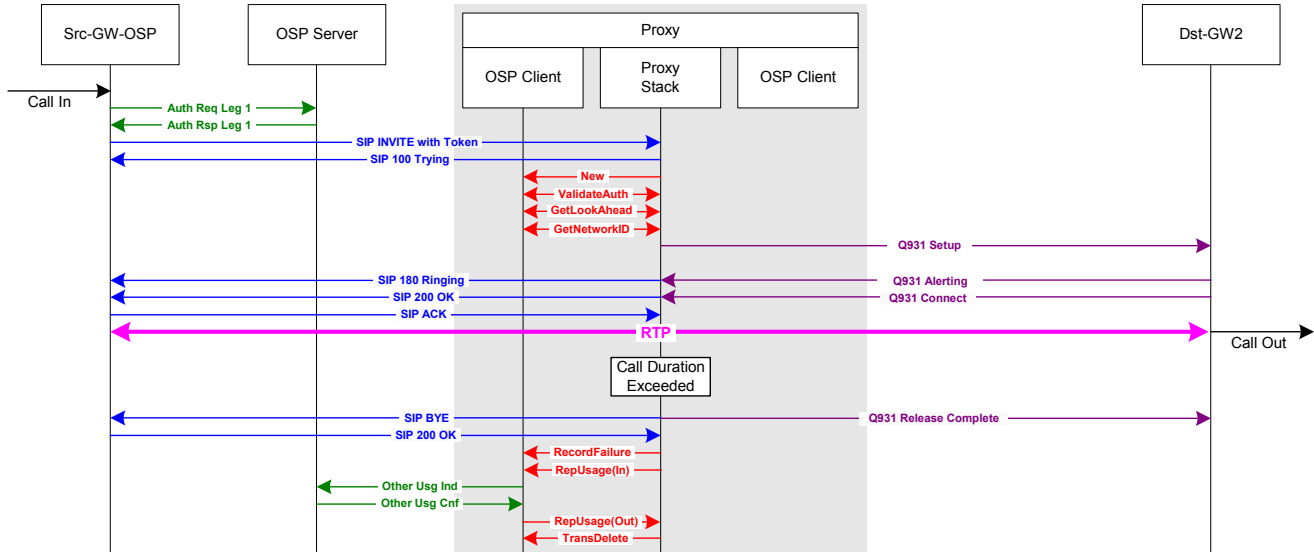
This test case should generate one OSP UsageIndication message, or CDR, from the proxy. The role should be ‘other’ and the FailureReason should be determined by the

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

release reason in the SIP CANCEL message from Src-GW. If no release reason is provided in the SIP CANCEL message, the proxy should set the FailureReason to 487.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2	487	0

### 2.3.9. Look Ahead Routing: Call Duration Limit Exceeded



**Test Case 2.3.9: OSP SIP Source to Proxy to non-OSP H.323 Destination:  
Look Ahead Routing - Call Duration Limit Exceeded**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

If the call duration exceeds the authorized call duration set by `ospvTimeLimit` value returned from the `OSPTransactionValidateAuthorisation` function, the proxy should forcefully end the call. When the proxy forcefully ends the call because the call duration exceeded the authorized time limit, the `FailureReason` parameter reported in the `RecordFailure` function should be set to 8 (preemption).

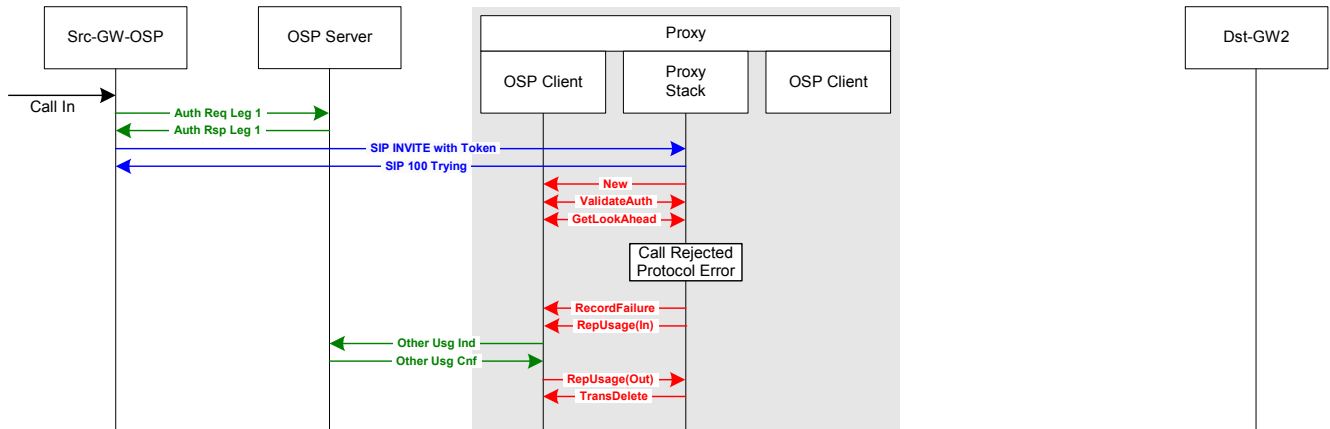
#### Expected CDR for Test Case 2.3.9

This test case should generate one OSP UsageIndication message, or CDR, from the proxy. The role should be 'other' and the FailureReason should be 8 to indicate the call was forcefully shutdown by the proxy.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2	8	0

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

### 2.3.10. Look Ahead Routing: Protocol Error



**Test Case 2.3.10: OSP SIP Source to Proxy to non-OSP H.323 Destination: Look Ahead Routing**  
**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

This case tests the error condition when the OSP server returns a DestinationProtocol in the Look Ahead token that is not supported by the proxy, such as H323\_LRQ or IAX. When this occurs, the proxy should reject the destination, record FailureReason 111 (protocol error) and report usage.

For this test case, the destination protocol for device Dst-GW2 is NOT configured as H323\_Q931 on the OSP server. The OSPPTtransactionGetLookAheadInfoIfPresent function call returns a DestinationProtocol not supported by the proxy. The proxy should recognize the protocol error and reject the call attempt. Note, if the DestinationProtocol is unknown or undefined, the proxy may either reject the destination and record FailureReason 111 or attempt a call setup to the destination using the proxy's default signaling protocol.

Expected CDRs for Test Case 2.3.10

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2	111	0

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

### 2.4. OSP Source to OSP Destination

This subsection of test cases describes call scenarios where both the source SIP and destination H.323 devices are OSP enabled. The source SIP device will include an OSP authorization token in the SIP INVITE message sent to the proxy. Based on the test case, the OSP peering token may or may not include Look Ahead Routing information. To complete the call, the proxy must include an OSP peering authorization token in the Q931 call setup message to the destination H.323 device. The destination H.323 device will extract the token from the call setup and validate the token signature to determine if the call from the proxy should be accepted.

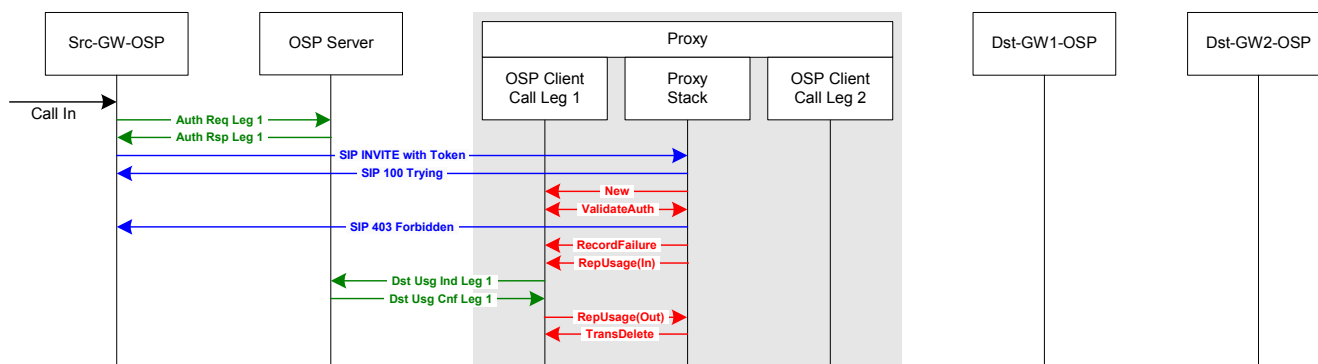
Configuration of VoIP devices on OSP server for test cases in section 2.4		
Device	Destination Protocol	OSP Version
Src-GW-OSP	SIP	1.4.3, 2.1.1 or 4.1.1
Proxy	SIP or H323_Q931	2.1.1 or 4.1.1
Dst-GW1-OSP	H323_Q931	1.4.3, 2.1.1 or 4.1.1
Dst-GW2-OSP	H323_Q931	1.4.3, 2.1.1 or 4.1.1

Configuration of destination devices in OSP server for these test cases:

DestinationProtocol = H323\_Q931

OSPVersion = 1.4.3, 2.1.1 or 2.1.1-P (OSP Enabled)

#### 2.4.0. Invalid Authorization Token



**Test Case 2.4.0: OSP SIP Source to Proxy to OSP H.323 Destination: Invalid Authorization Token**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

This test case is identical to 2.3.0.

#### Expected CDR for Test Case 2.4.0

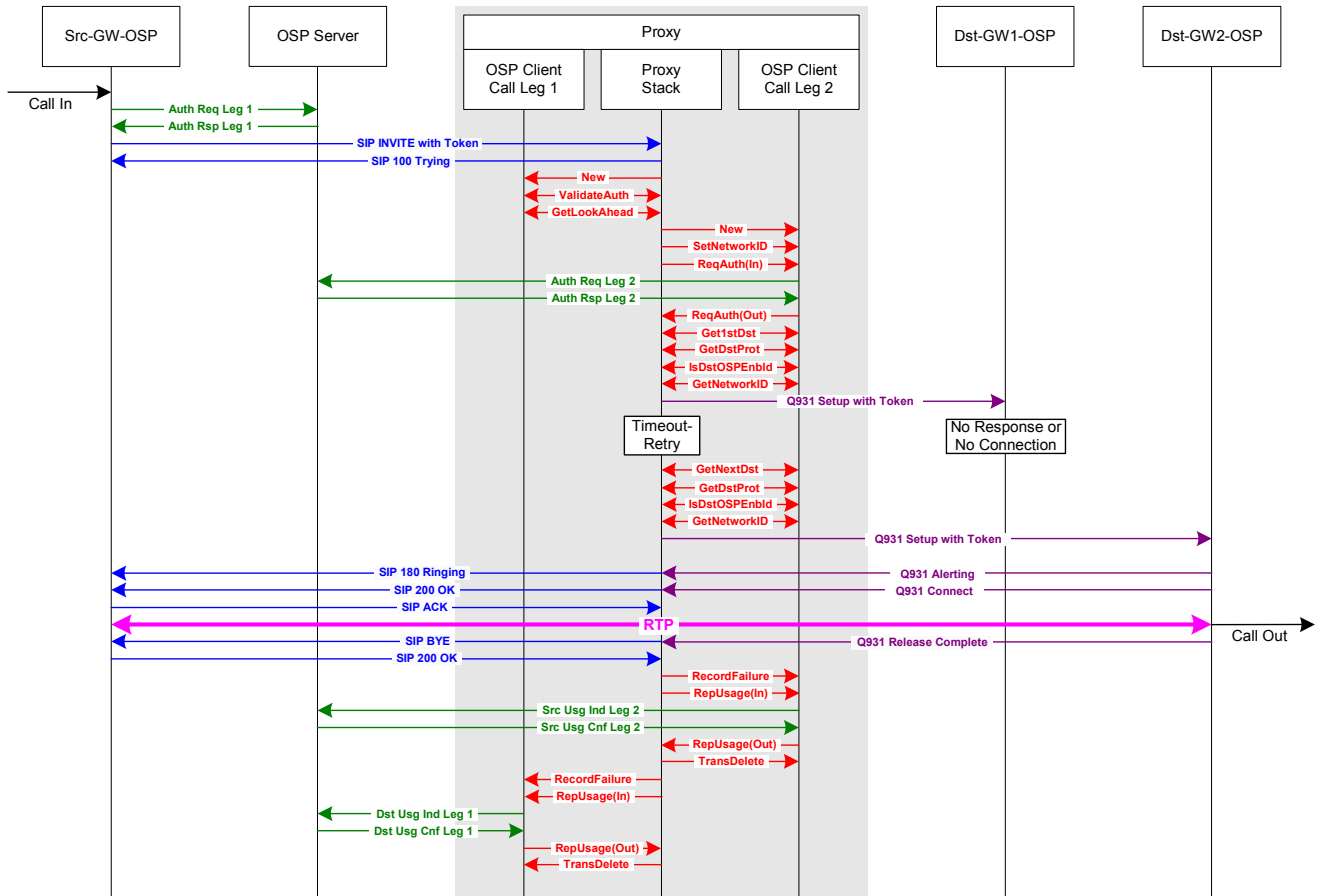
This test case should generate one OSP UsageIndication message, or CDR, from the proxy as the destination of call leg 1. The release reason (ospvFailureReason), or termination cause code, for the call should be set by the proxy to 403 to indicate the authorization token was invalid.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1	destination	Src-GW-OSP	Proxy	403	0



## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

### 2.4.2. No Response or No Connection and Retry - Proxy Times Out



**Test Case 2.4.2: OSP SIP Source to Proxy to OSP H.323 Destination:  
No Response or No Connection & Retry - Proxy Times Out**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

See test case 2.3.2.

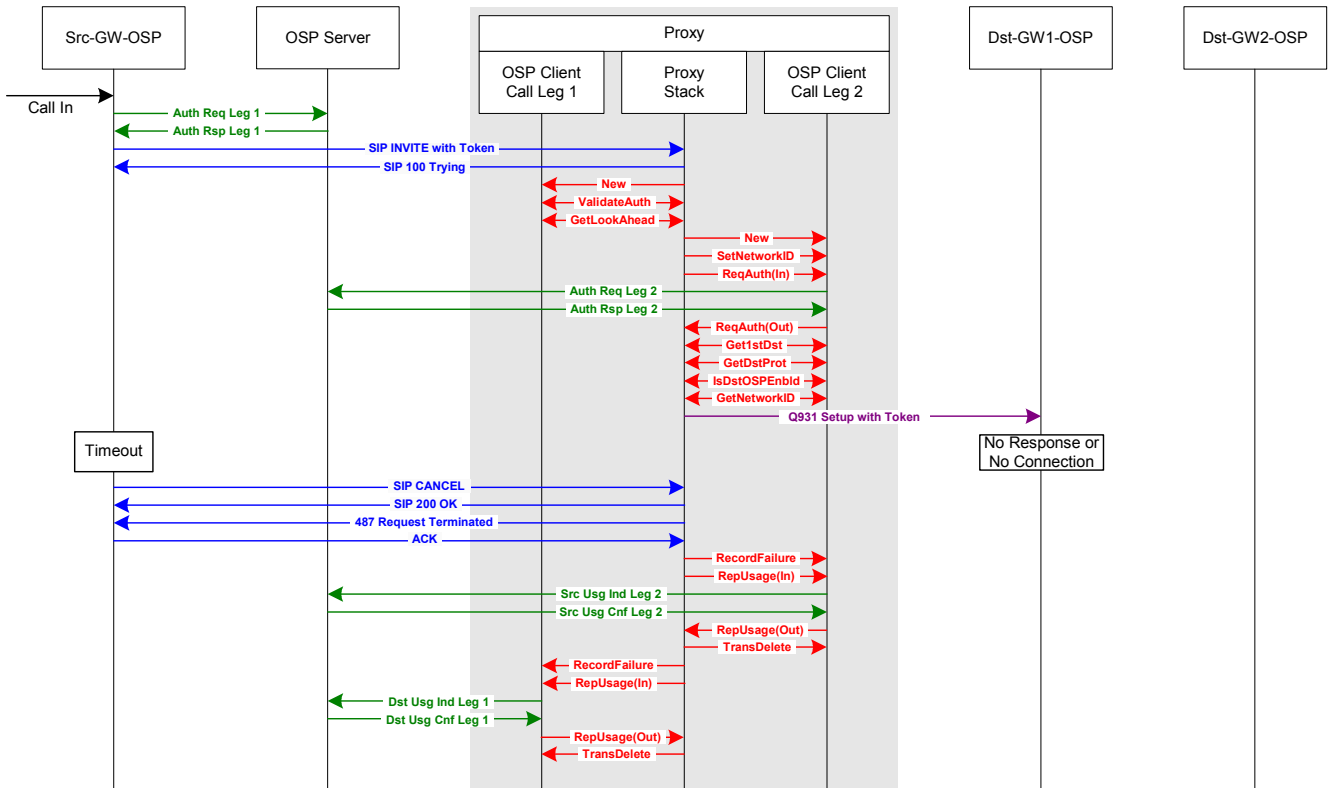
#### Expected CDRs for Test Case 2.4.2

This test case should generate three OSP UsageIndication messages, or CDRs, from the proxy. Two CDRs created as the source of call leg 2 and one CDR as the destination of call leg 1. The release reason (ospvFailureReason), or termination cause code, for the first attempt of call leg 2 should be determined by the proxy based on the call release reason for the failure. For the successful retry of call leg 2, the proxy should set the FailureReason to 16 or 1016. The FailureReason for the destination CDR of call leg 1 should be 16 or 1016.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW-OSP	Dst-GW1-OSP	47, 2, 63 or 27	0
2	source	Src-GW-OSP	Dst-GW2-OSP	16 or 1016	greater than 0
1	destination	Src-GW-OSP	Proxy	16 or 1016	greater than 0

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

### 2.4.3. No Response or No Connection and Retry - Source Times Out



**Test Case 2.4.3: OSP SIP Source to Proxy to OSP H.323 Destination:  
No Response or No Connection & Retry - Source Times Out**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

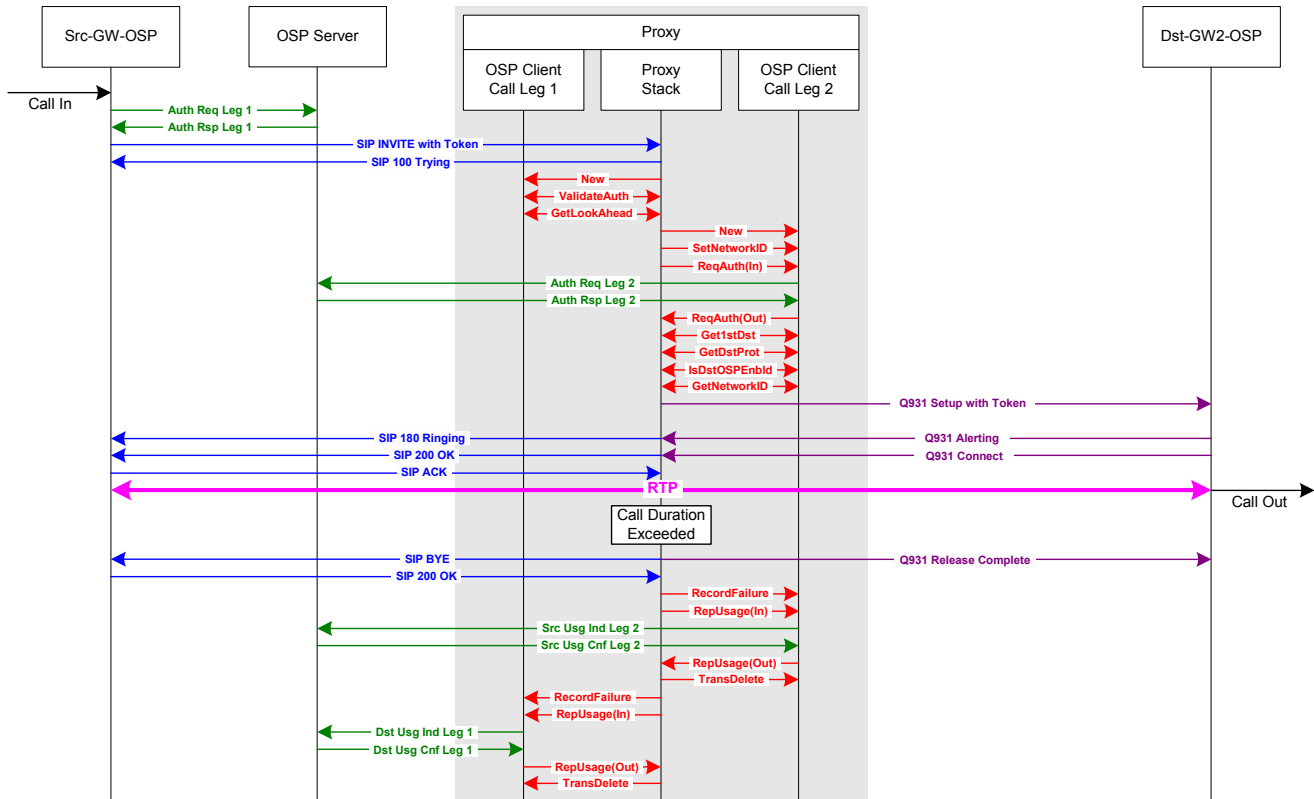
See test case 2.3.3.

#### Expected CDRs for Test Case 2.4.3

This test case should generate two OSP UsageIndication messages, or CDRs, from the proxy. One CDR as the source of call leg 2 and another as the destination of call leg 1. The release reason (ospvFailureReason), or termination cause code, for the CDRs should be determined by the release reason included in the SIP CANCEL message from Src-GW-OSP. If no release reason is included in the SIP CANCEL message, the proxy should report a FailureReason of 487.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW-OSP	Dst-GW1-OSP	487	0
1	destination	Src-GW-OSP	Proxy	487	0

### 2.4.4. Call Duration Limit Exceeded



Test Case 2.4.4: OSP SIP Source to Proxy to OSP H.323 Destination: Time Limit Exceeded

Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green

#### Test Case Notes

This call scenario tests the proxy’s ability to end a call when its authorized call duration has been exceeded. In the AuthorizationResponse, the OSP server includes the authorized call duration. The OSP Toolkit parameter TimeLimit, returned in the GetFirstDestination or GetNextDestination function calls, defines the maximum duration for each call. The proxy should terminate a call when the call duration exceeds the TimeLimit. In this case, when the proxy forcefully ends a call that has exceeded its maximum call duration, the proxy should use the RecordFailure OSP Toolkit function call to report a FailureReason of 8 (preemption) and then use the ReportUsage OSP Toolkit function call to send a UsageIndication call detail record to the OSP server.

**Note:** In this call scenario, there are two authorized call durations. The authorized call duration for call leg one is defined by the ospvTimeLimit variable returned by the OSPPTtransactionValidateAuthorization function. The authorized call duration for call leg two is defined by the ospvTimeLimit variable returned by the OSPPTtransactionGetFirstDestination or OSPPTtransactionGetNextDestination functions. When the ospvTimeLimit for call leg one and two are different, the shorter TimeLimit takes priority and should be used by the proxy to determine when to forcefully end a call.

#### Expected CDRs for Test Case 2.4.4

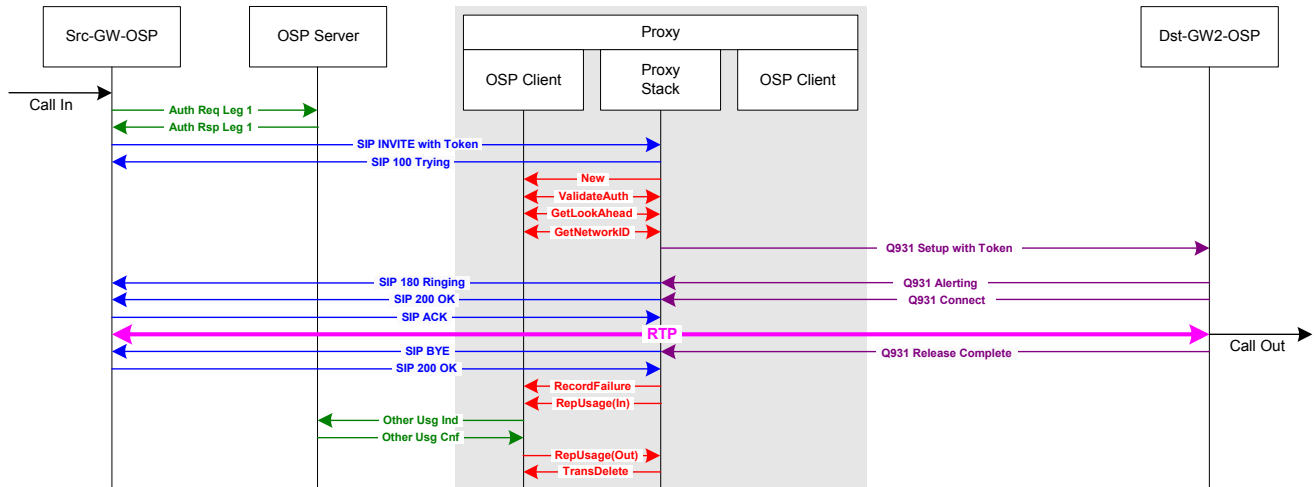
This test case should generate two OSP UsageIndication messages, or CDRs. One from the proxy as the source of call leg 2 and another as the destination for call leg 1. The

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

release reason (ospvFailureReason), or termination cause code, for the call should be set by the proxy to 8 to indicate the call was forcefully shutdown by the proxy.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW-OSP	Dst-GW2-OSP	8	greater than 0
1	destination	Src-GW-OSP	Proxy	8	greater than 0

### 2.4.5. Look Ahead Routing



Test Case 2.4.5: OSP SIP Source to Proxy to OSP H.323 Destination: Look Ahead Routing

Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green

#### Test Case Notes

See test case 2.3.5.

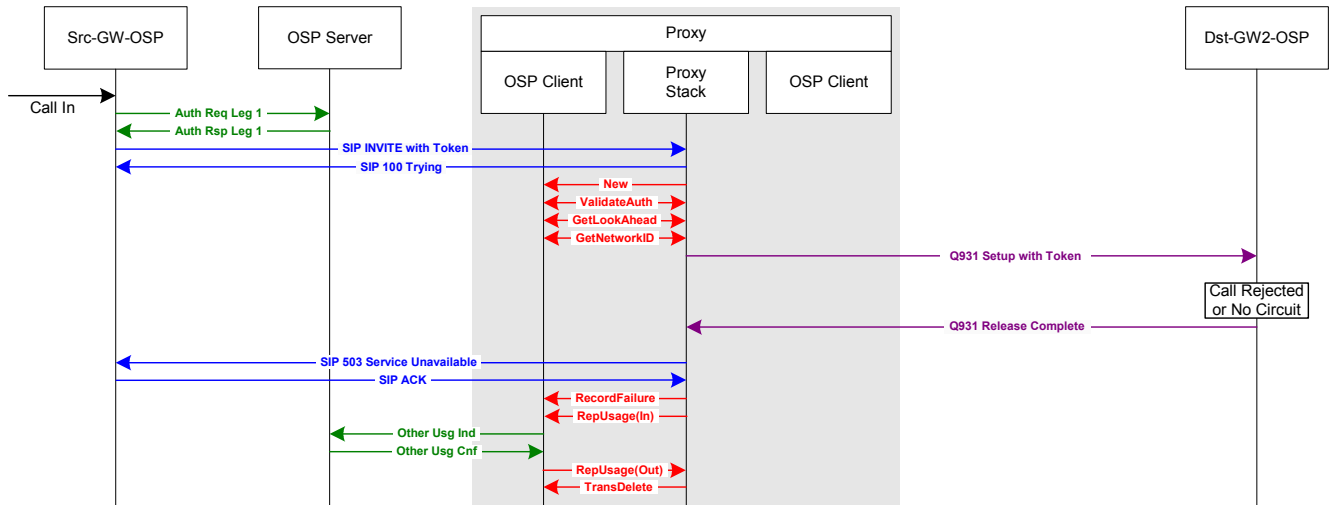
#### Expected CDR for Test Case 2.4.5

This test case should generate one OSP UsageIndication message, or CDR from the proxy. Look Ahead Routing is a unique case when one OSP Toolkit transaction validates inbound call leg 1 and routes outbound call leg 2. Since one CDR is used to report usage for both the destination of call leg 1 and the source of call leg 2, the role is defined as other. As with other call scenarios, the FailureReason should be determined by the release code included in a SIP CANCEL header from the source SIP device, or by the response from the H.323 destination device. If the call is successful and there is no release code reported, the proxy should report the FailureReason as 16 or 1016 to the OSP Toolkit ReportUsage function.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2-OSP	16 or 1016	greater than 0

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

### 2.4.6. Look Ahead Routing: Call Rejected or No Circuit



**Test Case 2.4.6: OSP SIP Source to Proxy to OSP H.323 Destination:  
Look Ahead Routing - Call Rejected or No Circuit & Retry**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

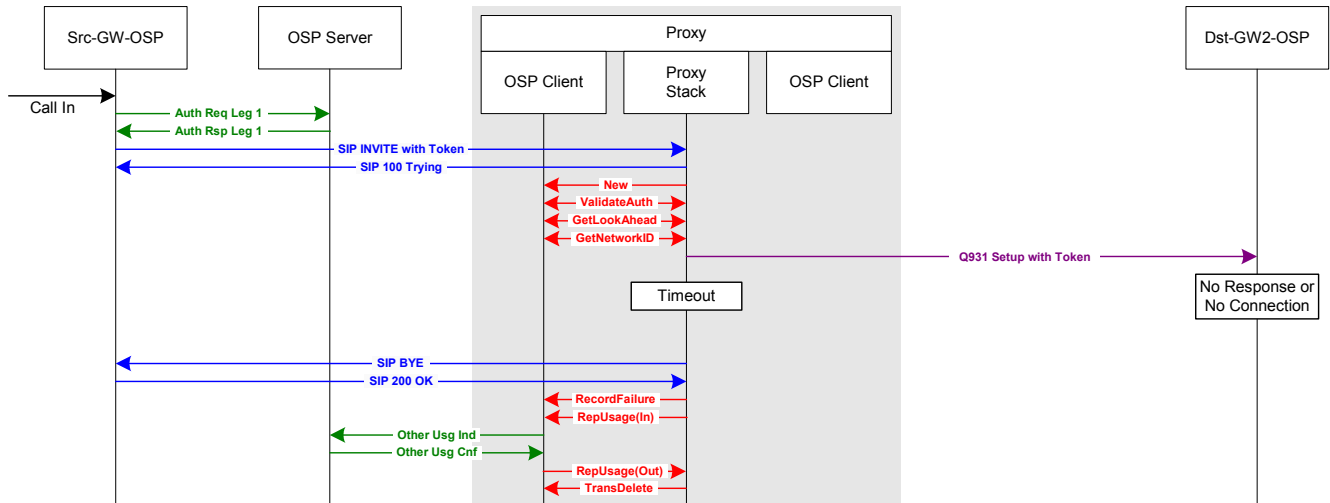
See test case 2.3.6.

#### Expected CDR for Test Case 2.4.6

This test case should generate one OSP UsageIndication message, or CDR from the proxy. The role should be 'other' and the FailureReason should be determined by the response from the destination H.323 device. In this example, the response is 21, but other responses are also valid.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2-OSP	21	0

### 2.4.7. Look Ahead Routing: No Response or No Connection - Proxy Times Out



**Test Case 2.4.7: OSP SIP Source to Proxy to OSP H.323 Destination:  
Look Ahead Routing - No Response or No Connection - Proxy Times Out**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

This case is very similar to test case 2.3.7 and tests a Look Ahead call scenario when the destination SIP device does not respond to the proxy. This test case must be executed four times to test the following four different call scenarios.

1. The proxy cannot establish a TCP connection with Dst-GW1-OSP. After TCP time-out, the proxy should retry call to Dst-GW2-OSP. (When OSP Toolkit function RecordFailure is called, the FailureReason for the call attempt should be set to 47 – resource unavailable, unspecified.)
2. No route to IP address of Dst-GW1-OSP. The proxy should retry call to Dst-GW2-OSP. (When OSP Toolkit function RecordFailure is called, the FailureReason for the call attempt should be set to 2 – no route to specified transit network.)
3. TCP connection refused by Dst-GW1-OSP. After TCP connection is refused, the proxy should retry the call to Dst-GW2-OSP. (When OSP Toolkit function RecordFailure is called, the FailureReason for the call attempt should be set to 63 – service or option not available, unspecified.)
4. No response from Dst-GW1-OSP. The proxy establishes TCP connection with Dst-GW1, but Dst-GW1-OSP never responds to Q931 Setup. The proxy should time-out and retry the call to Dst-GW2-OSP. (When OSP Toolkit function RecordFailure is called, the FailureReason for the call attempt should be set to 27 – destination out of order.)

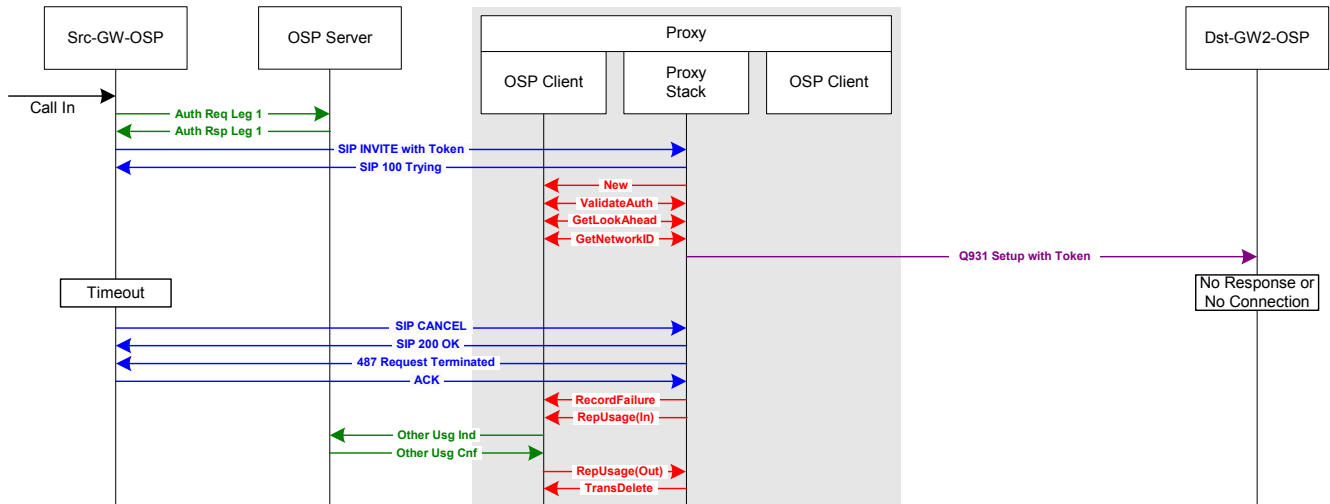
#### Expected CDR for Test Case 2.4.7

This test case should generate one OSP UsageIndication message, or CDR, from the proxy. The role should be 'other' and the FailureReason should be determined by the proxy based on the failure reasons described above.

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2-OSP	47, 2, 63 or 27	0

### 2.4.8. Look Ahead Routing: No Response or No Connection - Source Times Out



**Test Case 2.4.8: OSP SIP Source to Proxy to OSP H.323 Destination:  
Look Ahead Routing - No Response or No Connection - Source Times Out**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

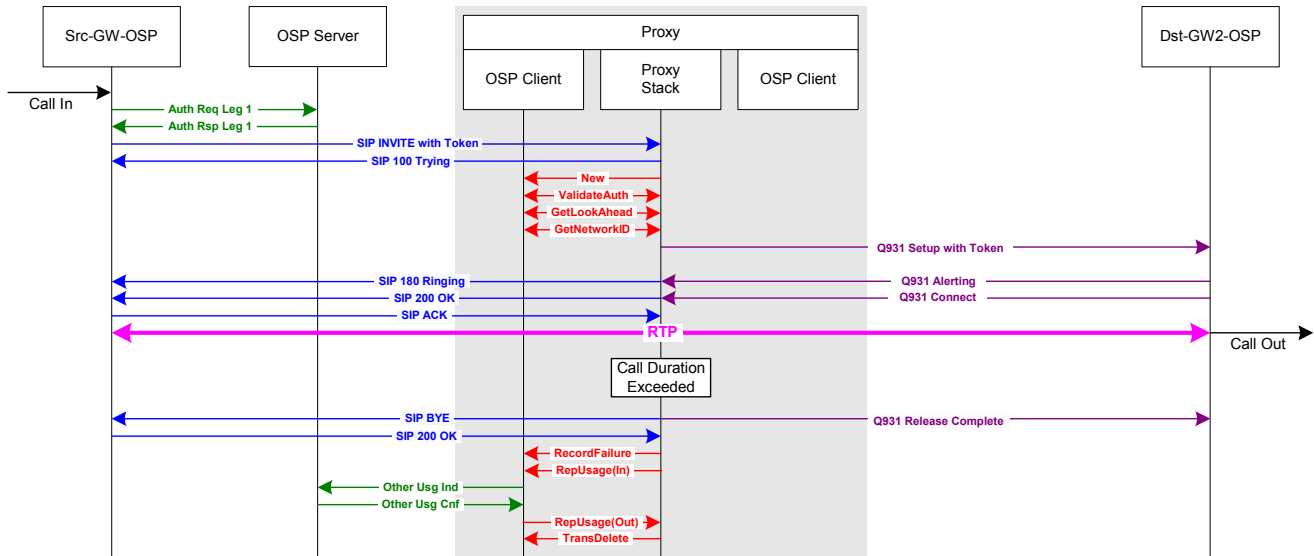
See test case 2.3.8.

#### Expected CDR for Test Case 2.4.8

This test case should generate one OSP UsageIndication message, or CDR, from the proxy. The role should be 'other' and the FailureReason should be determined by the release reason in the SIP CANCEL message from Src-GW-OSP. If no release reason is provided in the SIP message, the proxy should set the FailureReason to 487.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2-OSP	487	0

### 2.4.9. Look Ahead Routing: Call Duration Limit Exceeded



**Test Case 2.4.9: OSP SIP Source to Proxy to OSP H.323 Destination:  
Look Ahead Routing - Call Duration Limit Exceeded**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

If the call duration exceeds the authorized call duration set by `ospvTimeLimit` value returned from the `OSPPTTransactionValidateAuthorisation` function, the proxy should forcefully end the call. When the proxy forcefully ends the call because the call duration exceeded the authorized time limit, the `FailureReason` parameter reported in the `RecordFailure` function should be set to 8 (preemption).

#### Expected CDR for Test Case 2.4.9

This test case should generate one OSP UsageIndication message, or CDR from the proxy. The role should be 'other' and the `FailureReason` should be 8 to indicate the call was forcefully shutdown by the proxy.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2-OSP	8	0

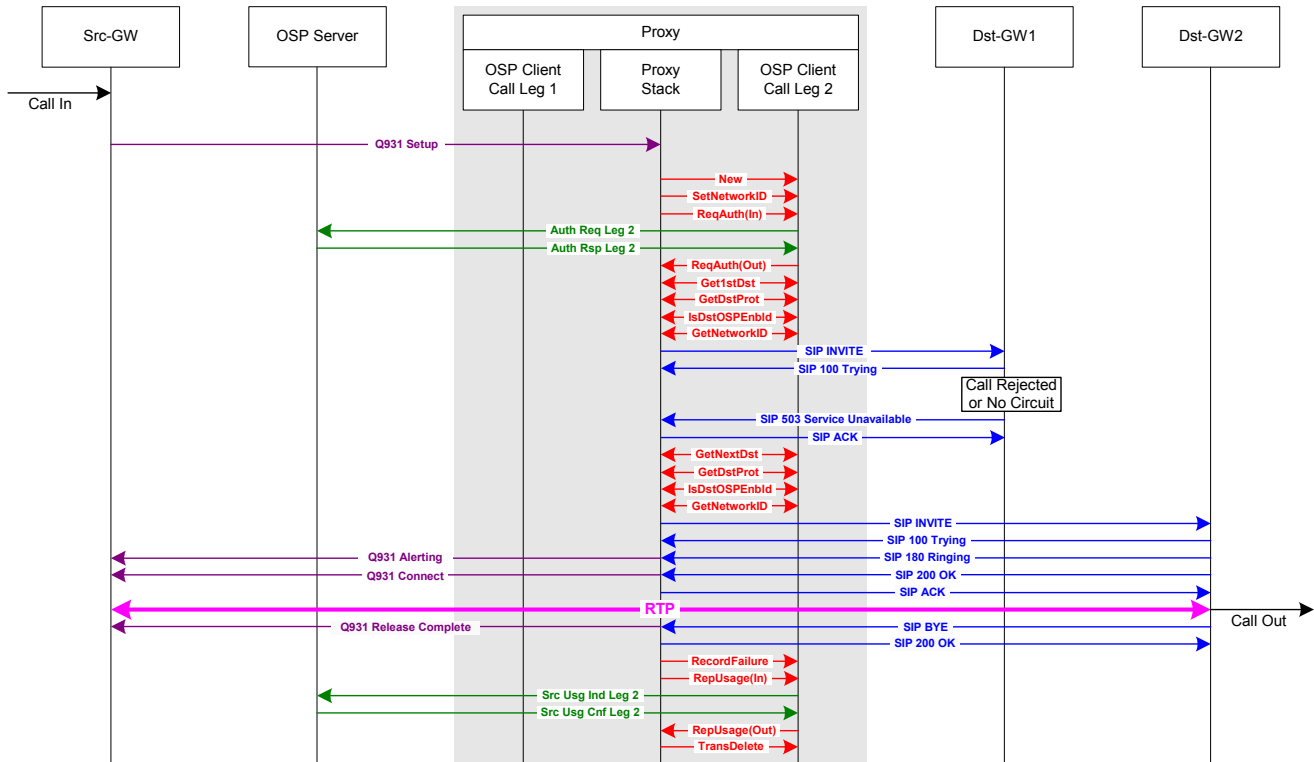
### 3. H.323 to SIP Test Cases

#### 3.1. non-OSP Source to non-OSP Destination

This subsection defines test cases when both the source H.323 and destination SIP devices are not OSP enabled. In these test cases, the proxy sends an OSP AuthorizationRequest to an OSP server to determine routing and report call detail records. OSP peering authorization access tokens are not used in section 3.1 test cases.

Configuration of VoIP devices on OSP server for test cases in section 3.1		
Device	Destination Protocol	OSP Version
Src-GW	H323_Q931	0.0.0 (Not OSP Enabled)
Proxy	SIP or H323_Q931	2.1.1 or 4.1.1
Dst-GW1	SIP	0.0.0 (Not OSP Enabled)
Dst-GW2	SIP	0.0.0 (Not OSP Enabled)

#### 3.1.1. Call Rejected or No Circuit and Retry



**Test Case 3.1.1: non-OSP H.323 Source to Proxy to non-OSP SIP Destination: Call Rejected or No Circuit & Retry**  
**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Detailed Description of Test Case

The call scenario diagram above illustrates the SIP messages (in blue), H.323 messages (in plum), OSP messages (in green) and OSP Toolkit function calls (in red) for this test case. (Please see the OSP Toolkit Programming Interface V3.3.1 document for details on OSP Toolkit function calls.) The gray box in the middle of the illustration represents the proxy. The call scenarios for the proxy, have two call legs. One inbound call leg from

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

the source H.323 device to the proxy and a second outbound call leg from the proxy to the destination SIP device. Each of these call legs require a message transaction between the proxy and the OSP client. To illustrate different OSP Toolkit transactions for the inbound (call leg 1) and outbound (call leg 2) call legs, the OSP client is shown twice in the gray box representing the proxy. The test case is described in detail below.

1. **Call In.** The call begins at the source H.323 device. The source of the H.323 call could be from a variety of devices, such as a H.323 phone registered a H.323 gatekeeper or a PSTN trunk which is connected to H.323 gateway.
2. **Q931 Setup.** The source H.323 device sends a Q931 call setup message to the proxy.
3. **NEW.** The proxy does not have a route defined to complete the call to the dialed number. The proxy sends a query to the OSP server for a route to a destination peer to complete the call. The proxy establishes a new transaction with the OSP client using `OSPPTTransactionNew` function. Please see the OSP Toolkit Programming Interface V3.3.1 document for details on this and other function calls.
4. **SetNetworkID.** The `OSPPTTransactionSetNetworkIds` function call identifies the trunk group or partition in the source device which originated the call. The `ospvSrcNetworkId` (trunk group or partition of the source device) must be taken from the Q931 call setup message from the source device. The `SrcNetworkId` is included in the `AuthorizationRequest` to the OSP server and may be used by the OSP server operator for routing and billing of calls by source trunk group or partition.
5. **ReqAuth(In).** The proxy calls the OSP Toolkit function `OSPPTTransactionRequestAuthorisation`.
6. **Auth Req Leg 2.** The OSP client sends an `OSP AuthorizationRequest` to the OSP server requesting a list of devices which can complete the call. The OSP request includes the calling and called telephone numbers, and the IP address of the source H.323 device.
7. **Auth Rsp Leg 2.** The OSP server sends an `OSP AuthorizationResponse` to the OSP client. An `OSP AuthorizationResponse` includes a list of one or more destination peers enabling the proxy to retry the call setup multiple times to different destinations until the call is completed. In this test case, the response includes the IP addresses, signaling protocol and OSP version supported by two destination SIP devices.
8. **ReqAuth(Out).** The OSP Toolkit responds to the proxy that the `OSPPTTransactionRequestAuthorisation` function is complete.
9. **Get1stDst.** The proxy calls the OSP Toolkit function `OSPPTTransactionGetFirstDestination` to get the IP address of the first destination gateway.
10. **GetDstProt.** The proxy calls the OSP Toolkit function `OSPPTTransactionGetDestProtocol` to get the signaling protocol required by the destination SIP device. In this case, the `DestinationProtocol` is SIP. If `DestinationProtocol` is not supported by the proxy (i.e. H323\_LRQ or IAX), the proxy should reject the destination and report a `FailureReason` of 111. If `DestinationProtocol` is unknown or undefined, the proxy may either reject the destination and report a `FailureReason` 111 or attempt to complete the call using the proxy's default signaling protocol.

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

11. **IsDstOSPEnabled.** The OSPPTTransactionDestOSPEnabled function tells the proxy whether or not the destination device is OSP enabled and capable of validating the OSP authorization token. In this case the destination SIP device is not OSP enabled (OSPE\_OSP\_FALSE). The proxy should not include the OSP authorization token in the SIP INVITE to the destination device. (Note, to ensure backward compatibility with OSP V1.4.3, if OSPE\_OSP is unknown or undefined, the proxy should assume the destination is OSP enabled and include the OSP authorization token in the SIP INVITE to the destination.)
12. **GetNetworkID.** The proxy calls the OSP Toolkit function OSPPGetDestNetworkID to get the destination trunk group if it is available. If the destination trunk group is available, it should be included in the SIP INVITE to the destination.
13. **SIP INVITE.** The proxy sends a call setup message to the first SIP destination device. An OSP peering authorization token is not included in the SIP INVITE message since the destination gateway does not support OSP. The SIP INVITE should NOT include the source trunk group information from the source H.323 device.
14. **SIP 100 Trying.** The destination SIP device receives the SIP INVITE and responds to the proxy.
15. **SIP 503 Service Unavailable.** The destination SIP device does not accept the call setup and returns a SIP 503 Service Unavailable to the proxy. This test case applies for any case when the destination SIP device rejects the SIP INVITE. The call may be rejected for a variety of reasons such as unauthorized access or no circuits available.
16. **SIP ACK.** The proxy responds with a SIP ACK.
17. **GetNextDst.** The proxy retries the call to the second destination and calls OSP Toolkit function OSPPTransactionGetNextDestination to obtain the IP address of the next destination SIP device. The OSPPTransactionGetNextDestination function call should include the FailureReason for the previous failed call attempt. In this test case the FailureReason should be the release cause reported by the destination or 503.
18. **GetDstProt.** The proxy gets the destination protocol of the second destination SIP device. In this test case the destination protocol is SIP. If DestinationProtocol is not supported by the proxy (i.e. H323\_LRQ or IAX), the proxy should reject the destination and report a FailureReason of 111. If DestinationProtocol is unknown or undefined, the proxy may either reject the destination and record a FailureReason of 111 or attempt to complete the call using the proxy's default signaling protocol.
19. **IsDstOSPEnabled.** The OSPPTTransactionDestOSPEnabled function tells the proxy whether or not the destination device is OSP enabled and capable of validating the OSP authorization token. In this case the destination SIP device is not OSP enabled (OSPE\_OSP\_FALSE). The proxy should not include the OSP authorization token in the SIP INVITE to the destination device. (Note, to ensure backward compatibility with OSP V1.4.3, if OSPE\_OSP is unknown or undefined, the proxy should assume the destination is OSP enabled and include the OSP authorization token in the SIP INVITE to the destination.)

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

20. **GetNetworkID.** The proxy calls the OSP Toolkit function OSPPGetDestNetworkID to get the destination trunk group if it is available. If the destination trunk group is available, it should be included in the SIP INVITE to the destination.
21. – 32. Standard H.323 to SIP communications for the completing the call.
33. **RecordFailure.** At the completion of the call, the proxy reports the call disconnect reason for the successful retry, to the OSP Toolkit using the OSPPTtransactionRecordFailure function.
34. **RepUsage(In).** The proxy calls the OSPPTtransactionReportUsage function to report the call duration.
35. **Src Usg Ind Leg 2.** The OSP client sends an OSP UsageIndication message (Call Detail Record) to the OSP server. The UsageIndication is a type ‘source’ call detail record since the proxy is the source device for the second leg of the call.
36. **Src Usg Cnf Leg 2.** The OSP server responds with an OSP UsageConfirmation message.
37. **RepUsage(Out).** The OSP Toolkit closes the ReportUsage transaction.
38. **TransDelete.** The proxy deletes the OSP Toolkit transaction.

### Expected CDRs for Test Case 3.1.1

This test case should generate two OSP UsageIndication messages, or CDRs, from the proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the first call attempt should be the SIP response from Dst-GW1. In this example, the SIP response is 503, but other SIP responses are also valid. For the successful retry call, the proxy should set the FailureReason to 16 or 1016, since there is no release reason in a SIP BYE message for a successful call.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW1	503	0
2	source	Src-GW	Dst-GW2	16 or 1016	greater than 0

### Expected OSP Messages for Test Case 3.1.1

This section presents the expected OSP messages for Test Case 3.1.1. After each OSP message is a table correlating each XML tag in the OSP message with a corresponding OSP Toolkit variable

#### AuthorizationRequest Leg 2 (generated by OSPPTtransactionRequestAuthorisation)

```
<?xml version="1.0"?>
<Message messageId="11703738491" random="1170373849">
<AuthorizationRequest componentId="11703738490">
<Timestamp>2005-05-12T17:32:57Z</Timestamp>
<CallId encoding="base64">Call ID</CallId>
<SourceInfo type="e164">Calling Number</SourceInfo>
<DeviceInfo type="transport">[Src-GW IP Address]</DeviceInfo>
<SourceAlternate type="transport">[proxy IP address]</SourceAlternate>
<SourceAlternate type="network">Partition</SourceAlternate>
<DestinationInfo type="e164">Called Number</DestinationInfo>
<Service/>
<MaximumDestinations>Number of Destination</MaximumDestinations>
</AuthorizationRequest>
```

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

</Message>

OSP XML Tag	Toolkit Variable	Note
<CallId encoding="base64">	CallId	
<SourceInfo type="e164">	CallingNumber	
<DeviceInfo type="transport">	SourceDevice	Src-GW IP Address
<SourceAlternate type="transport">	Source	proxy IP Address
<SourceAlternate type="network">	NetworkId	Partition or trunk group
<DestinationInfo type="e164">	CalledNumber	
<MaximumDestinations>	NumberOfDestinations	Maximum number of possible destinations requested.

### AuthorizationResponse Leg 2 (response from OSP server)

```

<?xml version='1.0'?>
<Message messageId='11703738491' random='21655'>
<AuthorizationResponse componentId='11703738490'>
<Timestamp>2005-05-12T18:32:59Z</Timestamp>
<Status>
<Description>SUCCESS</Description>
<Code>200</Code>
</Status>
<TransactionId>Transaction ID</TransactionId>
<Destination>
<CallId encoding='base64'>Call ID</CallId>
<DestinationInfo type='e164'>Called Number</DestinationInfo>
<DestinationSignalAddress>[Dst-GW1 IP Address]</DestinationSignalAddress>
<Token encoding='base64'>OSP Token</Token>
<UsageDetail>
<Amount>14400</Amount>
<Increment>1</Increment>
<Service/>
<Unit>s</Unit>
</UsageDetail>
<ValidAfter>2005-05-12T18:27:59Z</ValidAfter>
<ValidUntil>2005-05-12T18:37:59Z</ValidUntil>
<DestinationProtocol critical='False'>sip</DestinationProtocol>
<OSPVersion critical='False'>0.0.0</OSPVersion>
<SourceInfo type='e164' critical='False'>Calling Number</SourceInfo>
<DestinationAlternate type='network' critical='False'></DestinationAlternate>
</Destination>
<Destination>
<CallId encoding='base64'>Call ID</CallId>
<DestinationInfo type='e164'>Called Number</DestinationInfo>
<DestinationSignalAddress>[Dst-GW2 IP Address]</DestinationSignalAddress>
<Token encoding='base64'>OSP Token</Token>
<UsageDetail>
<Amount>14400</Amount>
<Increment>1</Increment>
<Service/>
<Unit>s</Unit>
</UsageDetail>
<ValidAfter>2005-05-12T18:27:59Z</ValidAfter>
<ValidUntil>2005-05-12T18:37:59Z</ValidUntil>
<DestinationProtocol critical='False'>sip</DestinationProtocol>
<OSPVersion critical='False'>0.0.0</OSPVersion>
<SourceInfo type='e164' critical='False'>Calling Number</SourceInfo>
<DestinationAlternate type='network' critical='False'></DestinationAlternate>

```

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

```
</Destination>
</AuthorizationResponse>
</Message>
```

OSP XML Tag	Toolkit Variable	Note
<TransactionId>		Transaction ID from OSP server
<CallId encoding="base64">	CallId	
<DestinationInfo type="e164">	CalledNumber	May be translated in AuthResponse
<DestinationSignalAddress>	Destination	Dst-GW1 IP Address
<Token encoding="base64">	Token	Authorization token
<Amount>	TimeLimit	Authorized call duration in seconds
<Increment>		Default is 1
<Service>		Default is voice
<Unit>		Default is seconds
<ValidAfter>	ValidAfter	Time after which call is authorized
<ValidUntil>	ValidUntil	Time until which call is authorized
<DestinationProtocol>	DestinationProtocol	VoIP signaling protocol expected by Dst-GW1
<OSPVersion>	DestinationOSPStatus	Version of OSP supported by Dst-GW1
<SourceInfo type="e164">	CallingNumber	May be translated in AuthResponse
<DestinationAlternate type="network">	DstNetworkID	Partition or trunk group of Dst-GW1
<CallId encoding="base64">	CallId	
<DestinationInfo type="e164">	CalledNumber	May be translated in AuthResponse
<DestinationSignalAddress>	Destination	Dst-GW2 IP Address
<Token encoding="base64">	Token	Authorization token
<Amount>	TimeLimit	Authorized call duration in seconds
<Increment>		Default is 1
<Service>		Default is voice
<Unit>		Default is seconds
<ValidAfter>	ValidAfter	Time after which call is authorized
<ValidUntil>	ValidUntil	Time until which call is authorized
<DestinationProtocol>	DestinationProtocol	VoIP signaling protocol expected by Dst-GW2
<OSPVersion>	DestinationOSPStatus	Version of OSP supported by Dst-GW2
<SourceInfo type="e164">	CallingNumber	May be translated in AuthResponse
<DestinationAlternate type="network">	DstNetworkID	Partition or trunk group of Dst-GW2

### Source UsageIndication Leg 2 (generated by OSPPTTransactionReportUsage)

```
<?xml version="1.0"?>
<Message messageId="47850982870685430173" random="1140717192">
<UsageIndication componentId="47850982870685430172">
<Timestamp>2005-05-12T17:33:33Z</Timestamp>
<Role>source</Role>
<TransactionId>Transaction ID</TransactionId>
<CallId encoding="base64">Call ID</CallId>
<SourceInfo type="e164">Calling Number</SourceInfo>
<DeviceInfo type="transport">[Src-GW IP Address]</DeviceInfo>
```

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

```

<SourceAlternate type="transport">[proxy IP Address]</SourceAlternate>
<DestinationInfo type="e164">Called Number</DestinationInfo>
<DestinationAlternate type="transport">[Dst-GW1 IP address]</DestinationAlternate>
<FailureReason>503</FailureReason>
</UsageIndication>
<UsageIndication componentId="47850982870685430174">
<Timestamp>2005-05-12T17:33:33Z</Timestamp>
<Role>source</Role>
<TransactionId>Transaction ID</TransactionId>
<CallId encoding="base64">Call ID</CallId>
<SourceInfo type="e164">Calling Number</SourceInfo>
<DeviceInfo type="transport">[Src-GW IP Address]</DeviceInfo>
<SourceAlternate type="transport">[proxy IP Address]</SourceAlternate>
<DestinationInfo type="e164">Called Number</DestinationInfo>
<DestinationAlternate type="transport">[Dst-GW2 IP address]</DestinationAlternate>
<UsageDetail>
<Amount>23</Amount>
<Increment>1</Increment>
<Unit>s</Unit>
<StartTime>2005-05-12T17:33:10Z</StartTime>
<AlertTime>2005-05-12T17:42:12Z</EndTime>
<EndTime>2005-05-12T17:42:27Z</EndTime>
<ConnectTime>2005-05-12T17:42:17Z</ConnectTime>
<ReleaseSource>0</ReleaseSource>
</UsageDetail>
<FailureReason>1016</FailureReason>
<Statistics critical="False">
<LossSent critical="False">
<Packets critical="False">0</Packets>
<Fraction critical="False">0</Fraction>
</LossSent>
<LossReceived critical="False">
<Packets critical="False">0</Packets>
<Fraction critical="False">0</Fraction>
</LossReceived>
</Statistics>
</UsageIndication>
</Message>

```

OSP XML Tag	Toolkit Variable	Note
<Role>		Source CDR for 1st try of call leg 2
<TransactionId>		Transaction ID from OSP server
<CallId encoding="base64">	CallId	
<SourceInfo type="e164">	CallingNumber	May be translated in AuthResponse
<DeviceInfo type="transport">	SourceDevice	Src-GW IP Address
<SourceAlternate type="transport">	Source	proxy IP Address
<DestinationInfo type="e164">	CalledNumber	May be translated in AuthResponse
<DestinationAlternate>	Destination	Dst-GW1 IP Address
<FailureReason>	FailureReason	Call Release Code
<Role>		Source CDR for 2nd try of call leg 2
<TransactionId>		Transaction ID from OSP server
<CallId encoding="base64">	CallId	
<SourceInfo type="e164">	CallingNumber	May be translated in AuthResponse
<DeviceInfo type="transport">	SourceDevice	Src-GW IP Address

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

OSP XML Tag	Toolkit Variable	Note
<SourceAlternate type="transport">	Source	proxy IP Address
<DestinationInfo type="e164">	CalledNumber	May be translated in AuthResponse
<DestinationAlternate>	Destination	Dst-GW2 IP Address
<Amount>	Duration	Call duration in seconds
<Increment>		Default is 1
<Unit>		Default is seconds
<StartTime>	StartTime	Time stamp when SIP INVITE is sent to the first destination device.
<AlertTime>	AlertTime	Time stamp when SIP 180 Ringing message is received.
<EndTime>	EndTime	Time stamp when SIP BYE is received from source or destination.
<ConnectTime>	ConnectionTime	Time stamp when SIP OK is received.
<ReleaseSource>	ReleaseSource	0 for source, 1 for destination
<FailureReason>	FailureReason	Call Release Code
<LossSent><Packets>	LossPacketSent	
<LossSent><Fraction>	LossFractionSent	
<LossReceived><Packets>	LossPacketReceived	
<LossReceived><Fraction>	LossFractionReceived	

### Source UsageConfirmation Leg 2 (confirmation from OSP server)

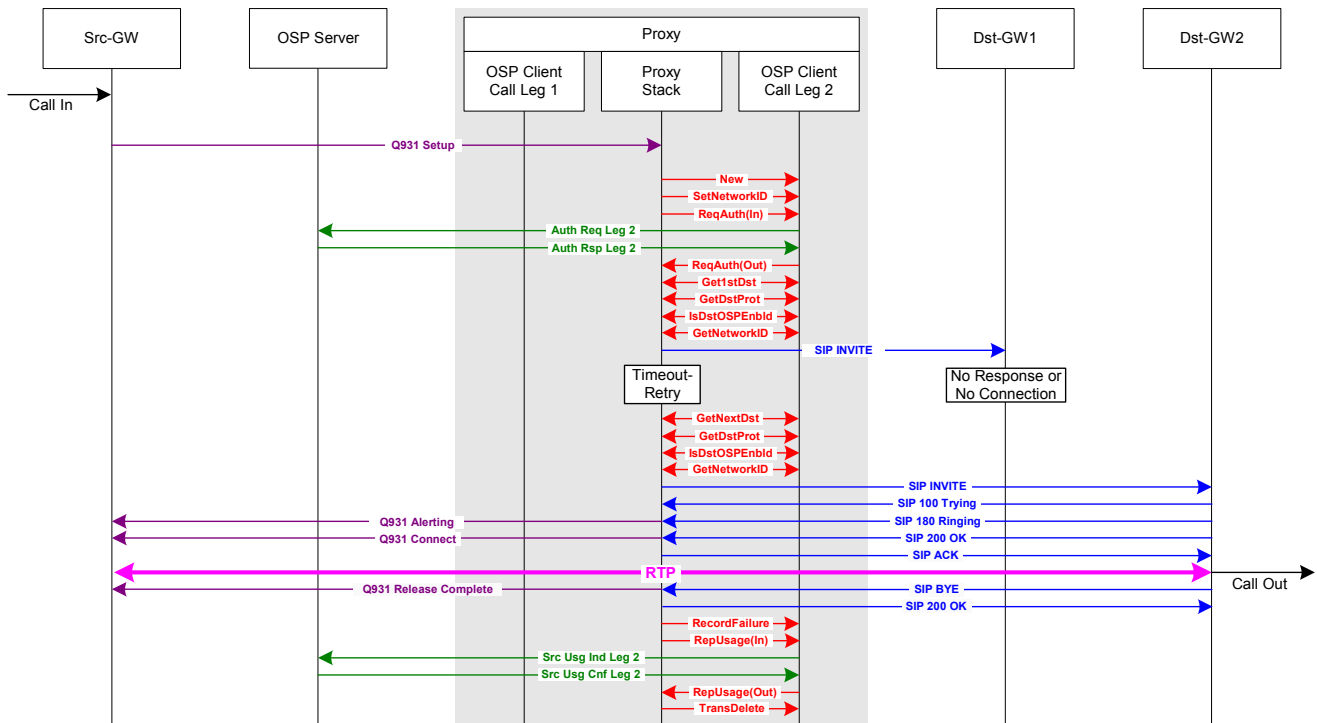
```

<?xml version='1.0'?>
<Message messageId='47850982870685430173' random='21172'>
<UsageConfirmation componentId='47850982870685430172'>
<Timestamp>2005-05-12T18:33:34Z</Timestamp>
<Status>
<Description>SUCCESS</Description>
<Code>200</Code>
</Status>
</UsageConfirmation>
<UsageConfirmation componentId='47850982870685430174'>
<Timestamp>2005-05-12T18:33:34Z</Timestamp>
<Status>
<Description>SUCCESS</Description>
<Code>200</Code>
</Status>
</UsageConfirmation>
</Message>

```

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

### 3.1.2. No Response or No Connection and Retry - Proxy Times Out



**Test Case 3.1.2: non-OSP H.323 Source to Proxy to non-OSP SIP Destination:  
No Response or No Connection & Retry - Proxy Times Out**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

This case tests the call scenarios when a destination SIP device does not respond to the proxy. This test case requires that the OSP server return two or more destinations in the AuthorizationResponse to the proxy. After the first call attempt fails, the proxy must retry the call to second destination. This test case must be executed four times to test the following four different call scenarios.

1. The proxy cannot establish a TCP connection with Dst-GW1. After TCP time-out, the proxy should retry call to Dst-GW2. (When OSP Toolkit function OSPPTTransactionGetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 47 – resource unavailable, unspecified.)
2. No route to IP address of Dst-GW1 device. The proxy should retry call to Dst-GW2. (When OSP Toolkit function OSPPTTransactionGetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 2 – no route to specified transit network.)
3. TCP connection refused by destination, Dst-GW1. After TCP connection is refused, the proxy should retry the call to Dst-GW2. (When OSP Toolkit function OSPPTTransactionGetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 63 – service or option not available, unspecified.)
4. No response from Dst-GW1. The proxy establishes TCP connection with Dst-GW1, but Dst-GW1 never responds to SIP INVITE. The proxy should time-out and retry

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

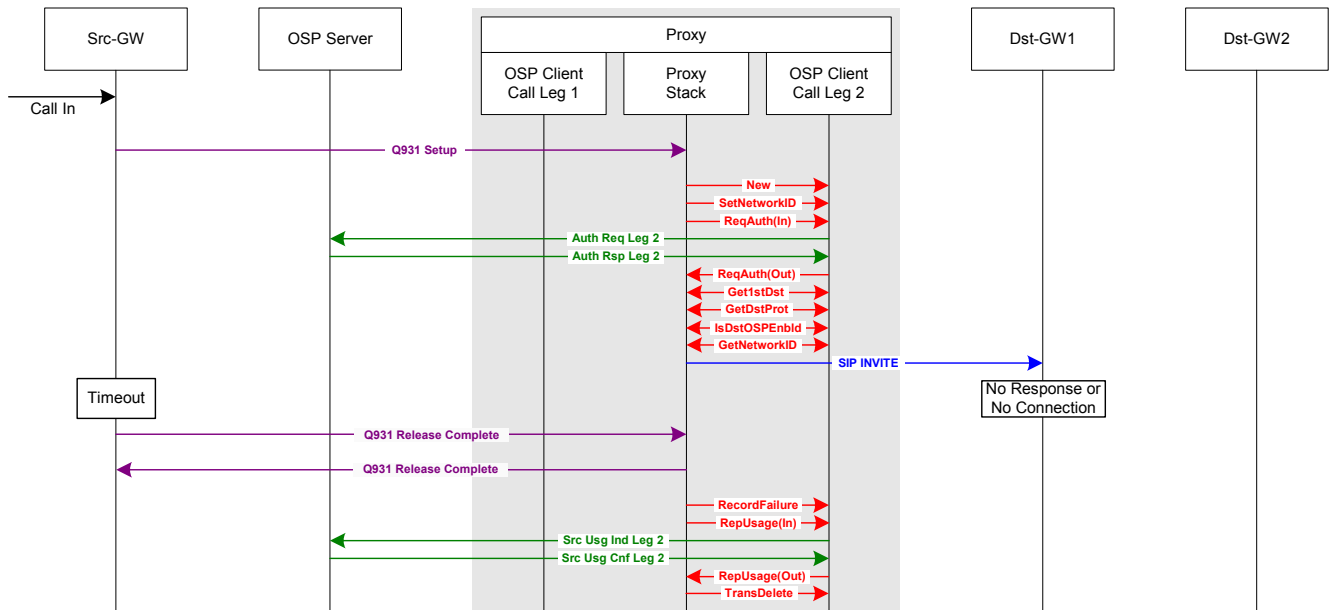
the call to Dst-GW2. (When OSP Toolkit function OSPPTtransactionGetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 27 – destination out of order.)

### Expected CDRs for Test Case 3.1.2

This test case should generate two OSP UsageIndication messages, or CDRs, from the proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the first call attempt should be determined by the proxy based on the reason for the failure. For the successful retry call, the proxy should set the FailureReason to 16, since there is no release reason in a SIP BYE message for a successful call.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW1	47, 2, 63 or 27	0
2	source	Src-GW	Dst-GW2	16 or 1016	greater than 0

### 3.1.3. No Response or No Connection and Retry - Source Times Out



**Test Case 3.1.3: non-OSP H.323 Source to Proxy to non-OSP SIP Destination:  
No Response or No Connection & Retry - Source Times Out**

Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green

### Test Case Notes

This case tests the call scenario when the source device ends the call before the first destination Dst-GW1 responds to the SIP INVITE from the proxy. In these cases, the proxy should terminate the call and report usage to the OSP server. The OSP Toolkit parameter FailureReason reported with the OSPPTtransactionRecordFailure function should be set to the release cause reported in the Q931 Release Complete from the source device, Src-GW.

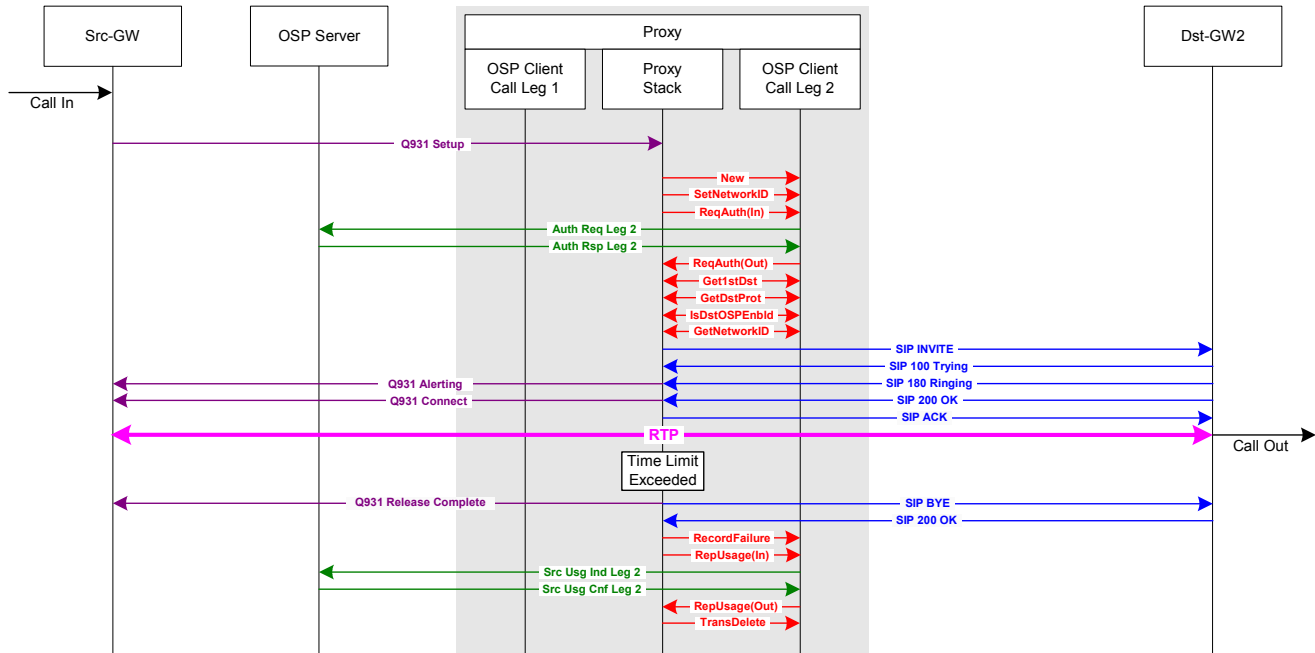
### Expected CDRs for Test Case 3.1.3

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

This test case should generate one OSP UsageIndication message, or CDR, from the proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the call should be determined by the release reason included in the Q931 Release Complete from Src-GW.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW1	16 or 1016	0

### 3.1.4. Call Duration Limit Exceeded



**Test Case 3.1.4: non-OSP H.323 Source to Proxy to non-OSP SIP Destination: Time Limit Exceeded**  
**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

This call scenario tests the proxy's ability to end a call when its authorized call duration has been exceeded. In the AuthorizationResponse, the OSP server includes the authorized call duration. The OSP Toolkit parameter TimeLimit, returned in the GetFirstDestination or GetNextDestination function calls, defines the maximum duration for each call. The proxy should terminate a call when the call duration exceeds the TimeLimit. In this case, when the proxy forcefully ends a call that has exceeded its maximum call duration, the proxy should use the RecordFailure OSP Toolkit function call to report a FailureReason of 8 (preemption) and then use the ReportUsage OSP Toolkit function call to send a UsageIndication call detail record to the OSP server.

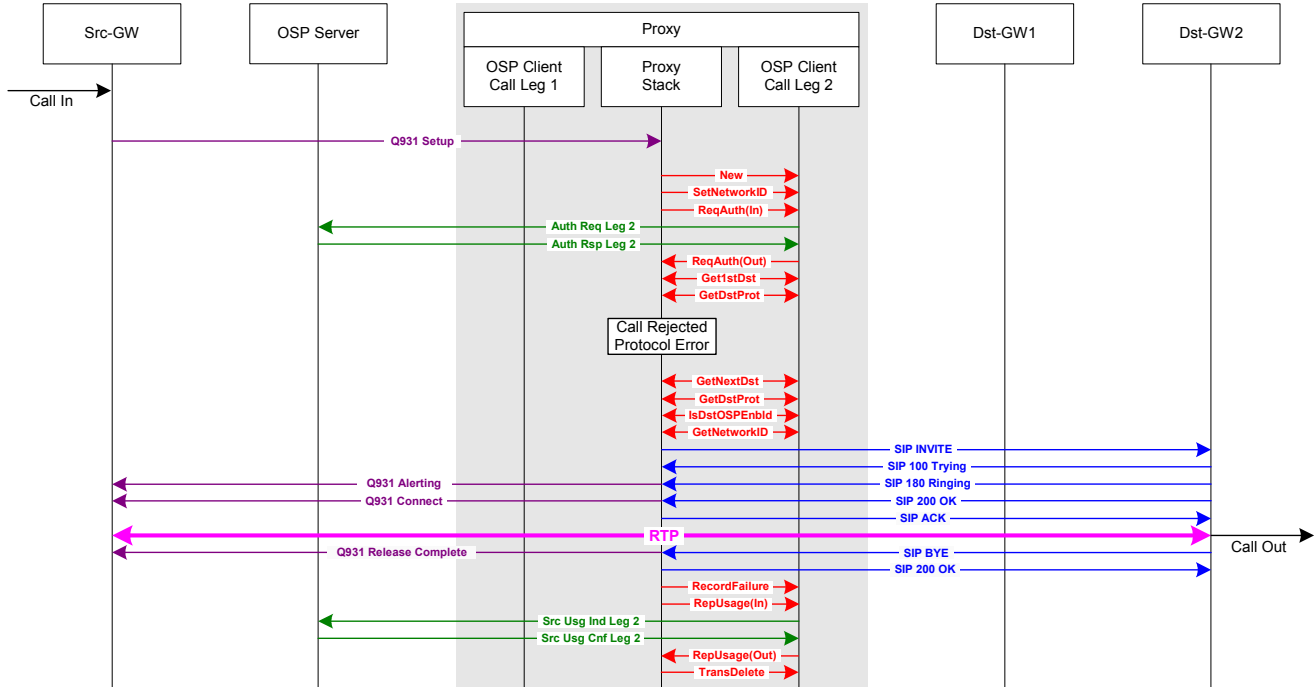
#### Expected CDRs for Test Case 3.1.4

This test case should generate one OSP UsageIndication message, or CDR, from the proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the call should be set by the proxy to 8 to indicate the call was forcefully shutdown by the proxy.

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW2	8	greater than 0

### 3.1.5. Call Rejected - Protocol Error and Retry



**Test Case 3.1.5: non-OSP H.323 Source to Proxy to non-OSP SIP Destination: Protocol Error & Retry**  
**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

This case tests the error condition when the OSP server returns a DestinationProtocol that is not supported by the proxy, such as H323\_LRQ or IAX. When this occurs, the proxy should reject the destination, record FailureReason 111 (protocol error) and retry the call to the next destination if it is available.

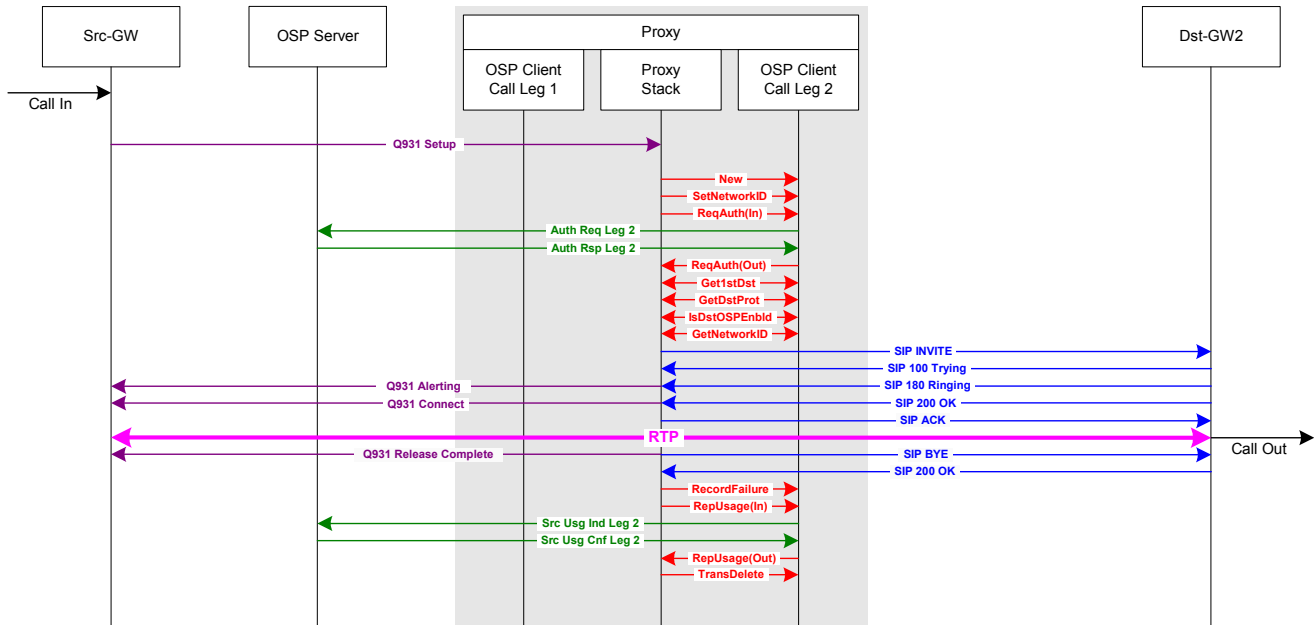
For this test case, the destination protocol for device Dst-GW1 is NOT configured as SIP on the OSP server. The OSPPTtransactionGetDestProtocol function call returns a DestinationProtocol not supported by the proxy. The proxy should recognize the protocol error and reject the call attempt. Note, if the DestinationProtocol is unknown or undefined, the proxy may either reject the destination, and report FailureReason 111, or attempt to complete the call to the destination with the proxy's default signaling protocol.

#### Expected CDRs for Test Case 3.1.5

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW1	111	0
2	source	Src-GW	Dst-GW2	16 or 1016	greater than 0

# SIP/H.323 Interworking Proxy – OSP Peering Test Cases

## 3.1.6. Number Translation



**Test Case 3.1.6: non-OSP H.323 Source to Proxy to non-OSP SIP Destination: Number Translation**  
**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

### Test Case Notes

This case tests the call scenario when the OSP server returns translated called and calling numbers in the OSP AuthorizationResponse to the proxy. When this occurs, the called and calling numbers in the SIP INVITE from the proxy to the destination gateway should be the translated called and calling numbers from the OSP AuthorizationResponse.

For this test case, OSP server should be configured to translate the called and calling numbers. The OSPPTtransactionGetFirstDestination function call returns the translated called and calling numbers. The proxy should send a SIP INVITE with the translated numbers to the destination. The OSPPTtransactionReportUsage function should report the un-translated called and calling numbers.

### Expected CDRs for Test Case 3.1.6

This test case should generate one OSP UsageIndication message, or CDR, from the proxy as the source of call leg 2. The called and calling numbers reported in the OSP UsageIndication message from the proxy, should be the called and calling numbers from the Q931 call setup received from the source gateway in call leg 1. The translated called and calling numbers should not be reported in the OSP UsageIndication message.

Call Leg	Role	Source IP Address	Destination IP Address	Calling Number	Called Number	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW2	Not Translated	Not Translated	16 or 1016	greater than 0

**Note:** OSP Toolkit version 3.3.3 and earlier report translated numbers in the CDR. Version 3.3.4 reports translated calling number and not translated called number.

### 3.2. *non-OSP Source to OSP Destination*

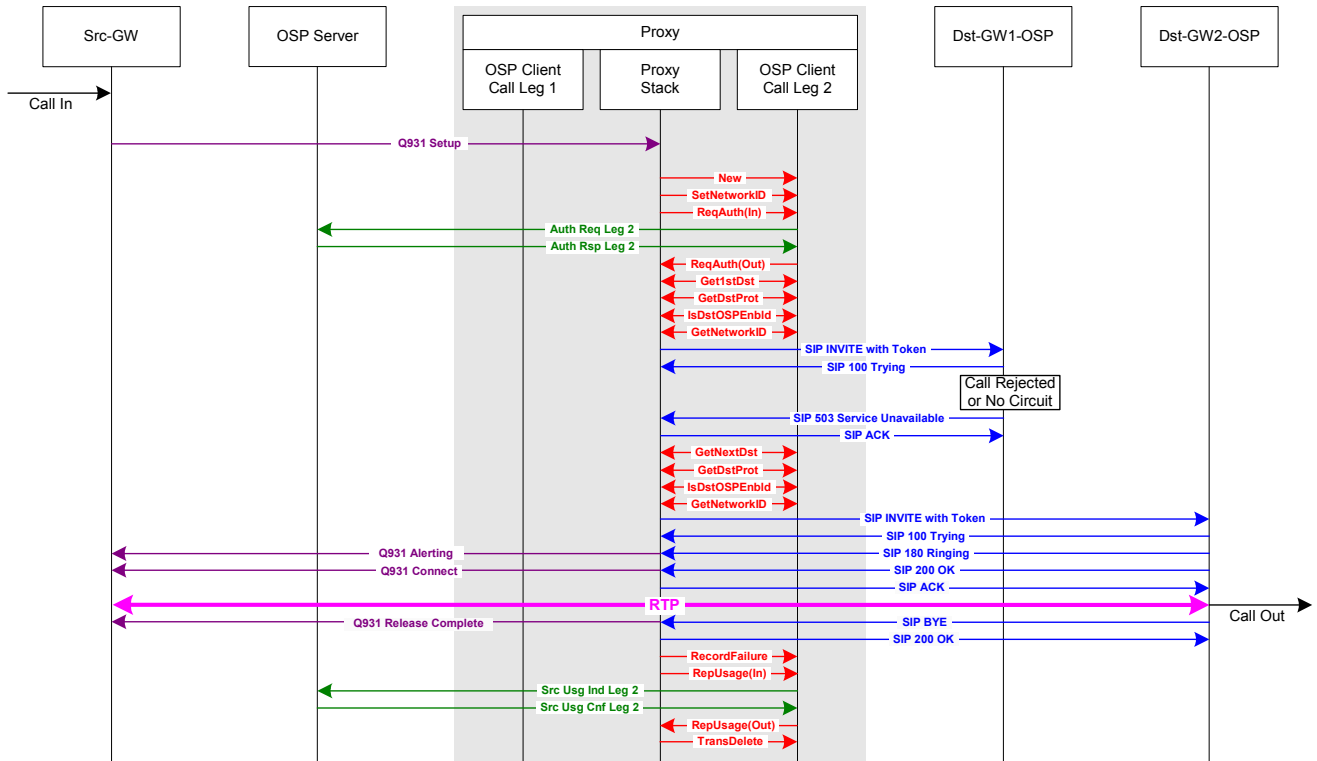
This subsection of cases tests call scenarios when the destination is an OSP enabled SIP device. In these call scenarios, the proxy must include the OSP peering token, returned in the OSP AuthorizationResponse, in the SIP INVITE message to the destination SIP device. The destination SIP device, which must be enrolled with the OSP server, will extract the token from the SIP INVITE message and validate that the token was digitally signed by the OSP server. If the token is valid, the destination SIP device will accept the call. If not, the SIP INVITE will be rejected by the destination SIP device.

Subsection 3.1 presented failover (retry call attempt) test cases with non-OSP destination devices. This subsection presents failover test cases with OSP destination devices. The implementer should note that an OSP AuthorizationResponse can contain a list of multiple destination devices and that the list may contain OSP and non-OSP enabled destination devices. An OSP implementation with the proxy should allow for call attempt retries to multiple destination devices and the list of destination devices may be any combination of non-OSP and OSP enabled devices.

Configuration of VoIP devices on OSP server for test cases in section 3.2		
Device	Destination Protocol	OSP Version
Src-GW	H323_Q931	0.0.0 (Not OSP Enabled)
Proxy	SIP or H323_Q931	2.1.1 or 4.1.1
Dst-GW1	SIP	1.4.3, 2.1.1 or 4.1.1
Dst-GW2	SIP	1.4.3, 2.1.1 or 4.1.1

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

### 3.2.1. Call Rejected or No Circuit and Retry



**Test Case 3.2.1: non-OSP H.323 Source to Proxy to OSP SIP Destination: Call Rejected or No Circuit & Retry**  
**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

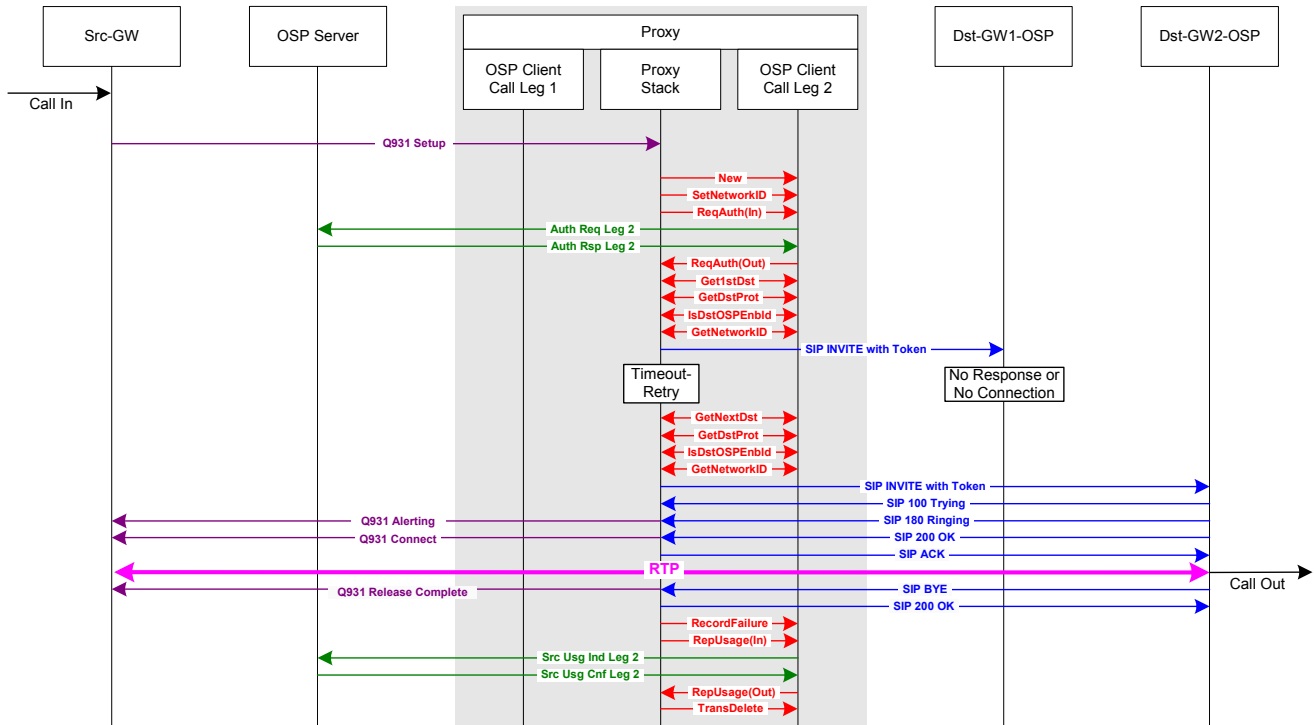
This test case identical to test case 3.1.1 except that the OSP token returned in OSPPTTransactionRequestAuthorization function should be included in the header of the SIP INVITE message to the destination.

#### Expected CDRs for Test Case 3.2.1

This test case should generate two OSP UsageIndication messages, or CDRs, from the proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the first call attempt should be the SIP response from Dst-GW1-OSP. In this example, the SIP response is 503, but other SIP responses are also valid. For the successful retry call, the proxy should set the FailureReason to 16 or 1016, since there is no release reason in a SIP BYE message for a successful call.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW1-OSP	503	0
2	source	Src-GW	Dst-GW2-OSP	16 or 1016	greater than 0

### 3.2.2. No Response or No Connection and Retry - Proxy Times Out



**Test Case 3.2.2: non-OSP H.323 Source to Proxy to OSP SIP Destination:  
No Response or No Connection & Retry - Proxy Times Out**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

This test case is identical to test case 3.1.2 except that the OSP token returned in OSPPTtransactionRequestAuthorization function should be included in the header of the SIP INVITE message to the destination.

This case tests the call scenarios when a destination SIP device does not respond to the proxy. This test case requires that the OSP server return two or more destinations in the AuthorizationResponse to the proxy. After the first call attempt fails, the proxy must retry the call to the second destination. This test case must be executed four times to test the following four different call scenarios.

1. The proxy cannot establish a TCP connection with Dst-GW1-OSP. After TCP timeout, the proxy should retry call to Dst-GW2-OSP. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 47 – resource unavailable, unspecified.)
2. No route to IP address of Dst-GW1-OSP device. The proxy should retry call to Dst-GW2-OSP. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 2 – no route to specified transit network.)
3. TCP connection refused by destination. After the TCP connection is refused, the proxy should retry the call to Dst-GW2-OSP. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

FailureReason for the first call attempt should be set to 63 – service or option not available, unspecified.)

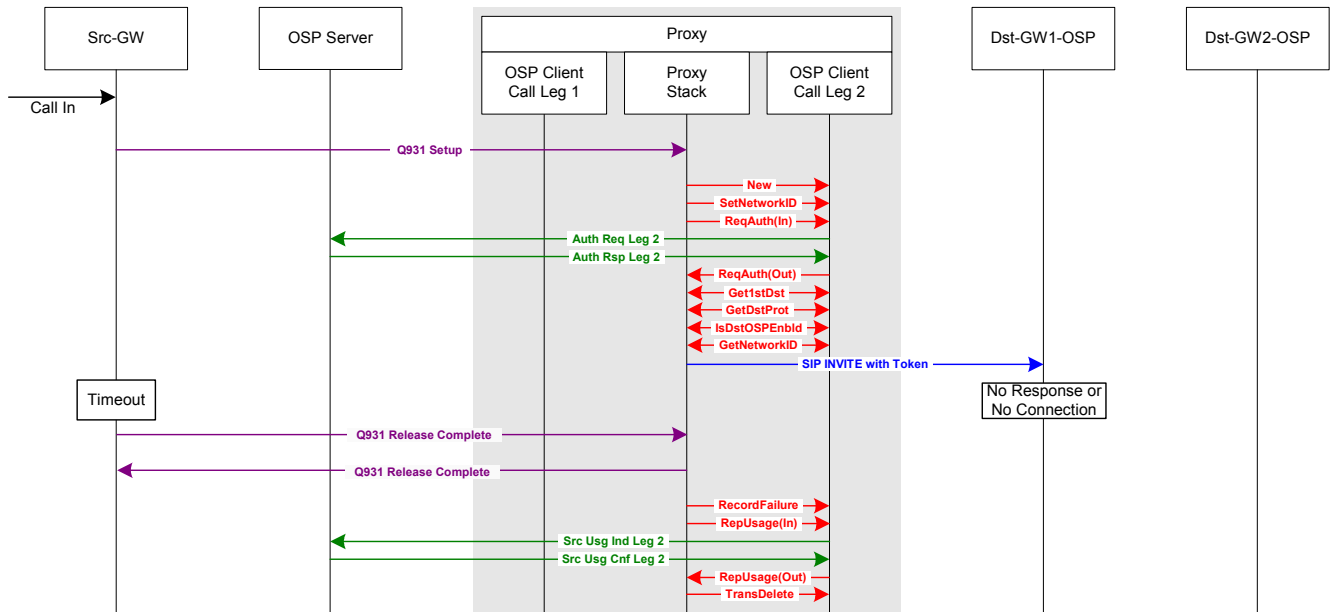
4. No response from Dst-GW1-OSP device. The proxy establishes a TCP connection with Dst-GW1-OSP, but Dst-GW1-OSP never responds to SIP INVITE. The proxy should time-out and retry the call to Dst-GW2-OSP. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 27 – destination out of order.)

### Expected CDRs for Test Case 3.2.2

This test case should generate two OSP UsageIndication messages, or CDRs, from the proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the first call attempt should be determined by the proxy based on the reason for the failure. For the successful retry of call leg 2, the proxy should set the FailureReason to 16 or 1016, since there is no release reason in a SIP BYE message for a successful call.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW1-OSP	47, 2, 63 or 27	0
2	source	Src-GW	Dst-GW2-OSP	16 or 1016	greater than 0

### 3.2.3. No Response or No Connection and Retry - Source Times Out



**Test Case 3.2.3: non-OSP H.323 Source to Proxy to OSP SIP Destination:  
No Response or No Connection & Retry - Source Times Out**

Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green

### Test Case Notes

This test case identical to test case 3.1.3 except that the OSP token returned in OSPPTtransactionRequestAuthorization function should be included in the header of the SIP INVITE message to the destination.

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

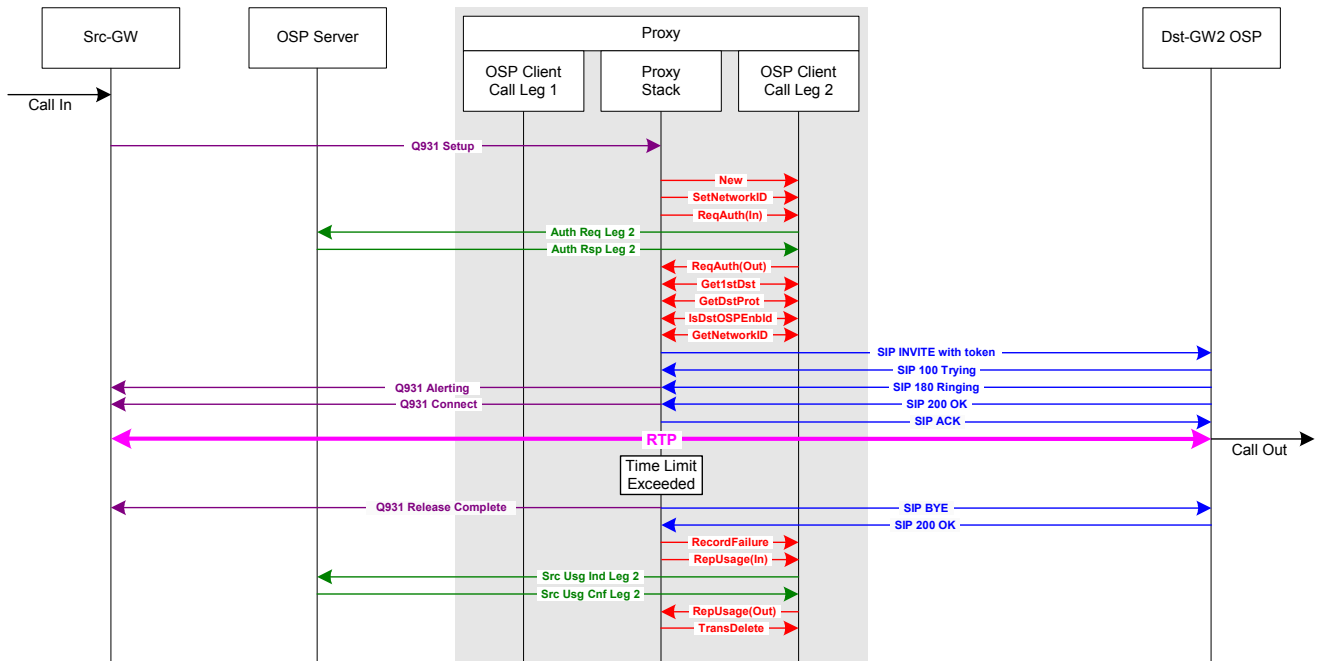
This case tests the call scenario when the source ends the call before the first destination Dst-GW1-OSP responds to the SIP INVITE from the proxy. In these cases, the proxy should terminate the call and report usage to the OSP server. The OSP Toolkit parameter FailureReason reported with the OSPTransactionRecordFailure function should be set to the release cause reported in the Q931 Release Complete from the source device, Src-GW.

### Expected CDRs for Test Case 3.2.3

This test case should generate one OSP UsageIndication message, or CDR, from the proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the call attempt should be determined by the release reason included in the Q931 Release Complete from Src-GW.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW1-OSP	16 or 1016	0

### 3.2.4. Call Duration Limit Exceeded



Test Case 3.2.4: non-OSP H.323 Source to Proxy to OSP SIP Destination: Time Limit Exceeded  
 Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green

### Test Case Notes

This test case identical to test case 3.1.4 except that the OSP token returned in OSPTransactionRequestAuthorization function should be included in the header of the SIP INVITE message to the destination.

This call scenario tests the proxy's ability to end a call when its authorized call duration has been exceeded. In the AuthorizationResponse, the OSP server includes the authorized call duration. The OSP Toolkit parameter ospvTimeLimit, returned in the GetFirstDestination or GetNextDestination function calls, defines the maximum duration for each call. The proxy should terminate a call when the call duration exceeds the

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

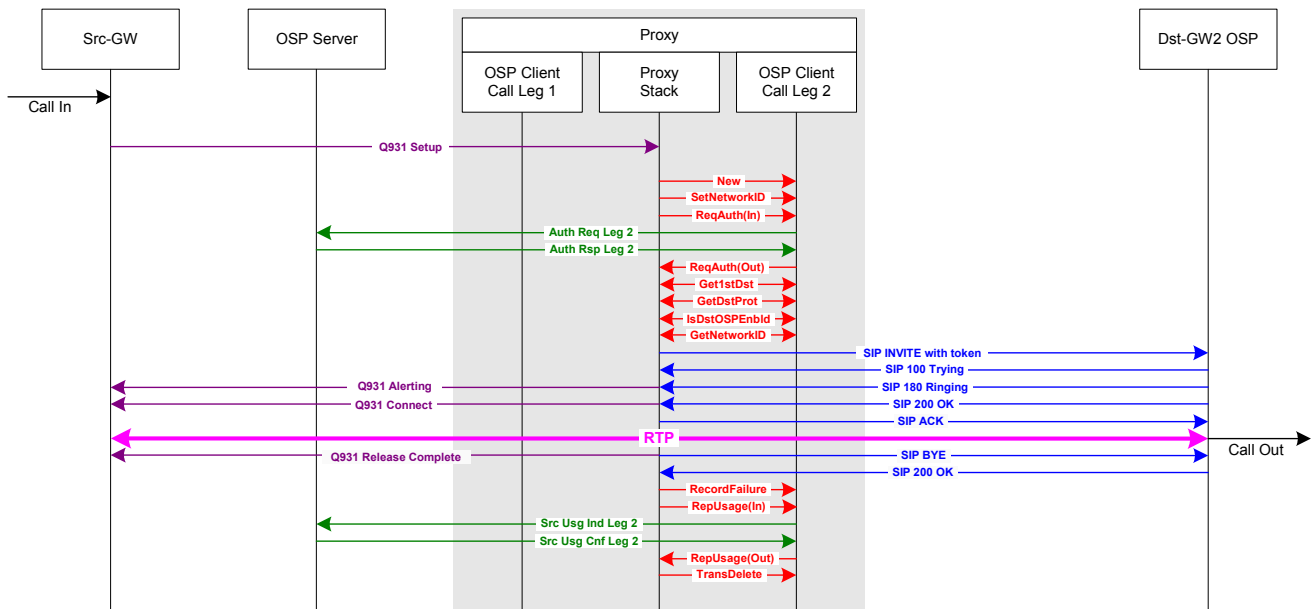
TimeLimit. In this case, when the proxy forcefully ends a call that has exceeded its maximum call duration, the proxy should use the RecordFailure OSP Toolkit function call to report a FailureReason of 8 (preemption) and then use the ReportUsage OSP Toolkit function call to send a UsageIndication call detail record to the OSP server.

### Expected CDRs for Test Case 3.2.4

This test case should generate one OSP UsageIndication message, or CDR, from the proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the call should be set by the proxy to 8 to indicate the call was forcefully shutdown by the proxy.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW2-OSP	8	greater than 0

### 3.2.5. Number Translation



**Test Case 3.2.5: non-OSP H.323 Source to Proxy to OSP SIP Destination: Number Translation**  
**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

### Test Case Notes

This test case identical to test case 3.1.6 except that the OSP token returned in OSPPTtransactionRequestAuthorization function should be included in the header of the SIP INVITE message to the destination.

This case tests the call scenario when the OSP server returns translated called and calling numbers in the OSP AuthorizationResponse to the proxy. When this occurs, the called and calling numbers in the SIP INVITE from the proxy to the destination gateway should be the translated called and calling numbers from the OSP AuthorizationResponse.

For this test case, the OSP server should be configured to translate the calling and called numbers. The OSPPTtransactionGetFirstDestination function call returns the translated called and calling numbers. The OSPPTtransactionReportUsage function should report the un-translated called and calling numbers.

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

### Expected CDRs for Test Case 3.2.5

This test case should generate one OSP UsageIndication message, or CDR, from the proxy as the source of call leg 2. The called and calling numbers reported in the OSP UsageIndication message from the proxy, should be the called and calling numbers from the Q931 Setup received from the source gateway in call leg 1. The translated called and calling numbers should not be reported in the OSP UsageIndication message.

Call Leg	Role	Source IP Address	Destination IP Address	Calling Number	Called Number	Release Reason or TC Code	Call Duration
2	source	Src-GW	Dst-GW2-OSP	Not Translated	Not Translated	16 or 1016	greater than 0

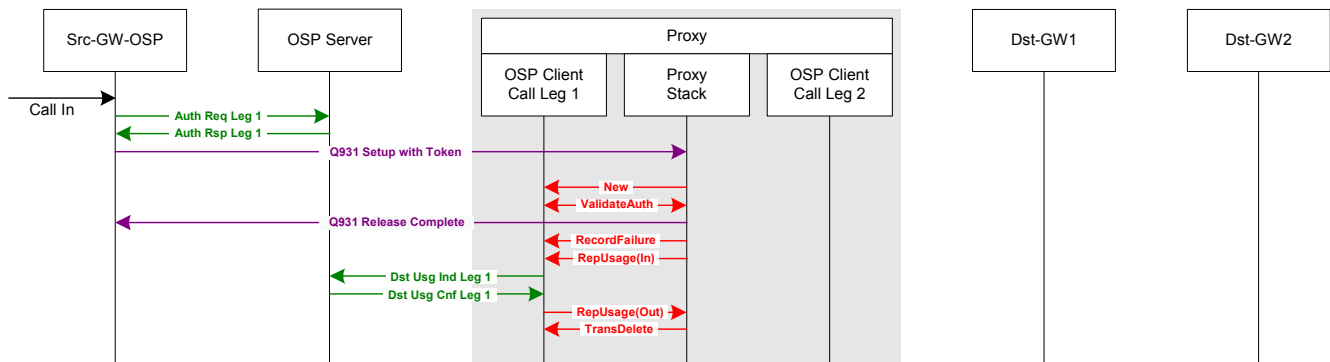
**Note:** OSP Toolkit version 3.3.3 and earlier report translated numbers in the CDR. Version 3.3.4 reports translated calling number and not translated called number.

### 3.3. OSP Source and non-OSP Destination

This subsection tests call scenarios when the source is an OSP enabled H.323 device and the destination SIP device is not OSP enabled. In these test cases, the proxy will receive a Q931 call setup message which includes an OSP peering token. The proxy must validate the digitally signed token to determine whether or not to accept the call. On the second call leg, the proxy must not include an OSP peering token in the SIP INVITE message to the destination SIP device since the destination SIP device is not OSP enabled and cannot validate an OSP token.

Configuration of VoIP devices on OSP server for test cases in section 3.2		
Device	Destination Protocol	OSP Version
Src-GW-OSP	H323_Q931	1.4.3 or 2.1.1
Proxy	SIP or H323_Q931	2.1.1
Dst-GW1	SIP	0.0.0 (Not OSP Enabled)
Dst-GW2	SIP	0.0.0 (Not OSP Enabled)

#### 3.3.0. Invalid Authorization Token



**Test Case 3.3.0: OSP H.323 Source to Proxy to non-OSP SIP Destination: Invalid Authorization Token**  
 Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green

#### Test Case Notes

In this test case, the token included in the Q931 call setup message cannot be validated by the proxy. The token could be invalid for different reasons such as: the token contents or digital signature has been corrupted, the token has expired, the token is not signed or the proxy does not have the public key of the OSP server that signed the authorization token (the public key is used to validate the digital signature).

The proxy responds to the source that the call is forbidden and then performs the OSP Toolkit function calls OSPPTTransactionRecordFailure and OSPPTTransactionReportUsage to create an OSP destination UsageIndication Call Detail Record which is sent to the OSP server. The FailureReason for this call should be 21.

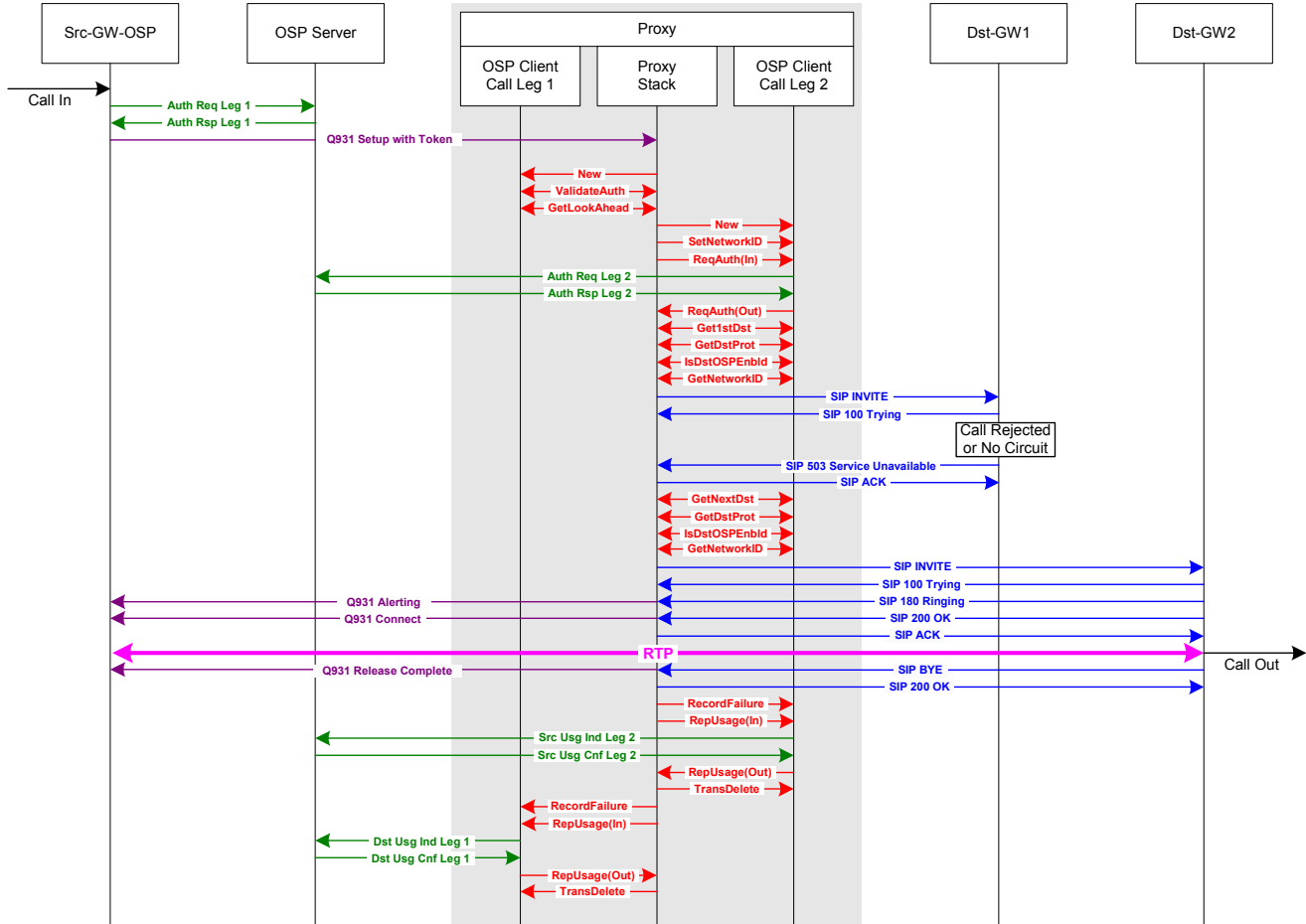
#### Expected CDR for Test Case 3.3.0

This test case should generate one OSP UsageIndication message, or CDR, from the proxy as the destination of call leg 1. The release reason (ospvFailureReason), or termination cause code, for the call should be set by the proxy to 21 to indicate the authorization token was invalid.

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1	destination	Src-GW-OSP	Proxy	21	0

### 3.3.1. Call Rejected or No Circuit and Retry



**Test Case 3.3.1: OSP H.323 Source to Proxy to non-OSP SIP Destination: Call Rejected or No Circuit & Retry**  
**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Detailed Description of Test Case

1. **Call In.** The call begins at the source H.323 device.
2. **Auth Req Leg 1.** The source H.323 device sends an OSP AuthorizationRequest to the OSP server.
3. **Auth Rsp Leg 1.** The OSP server returns the IP address, DestinationProtocol, and OSPVersion of the proxy, plus a signed authorization token, to the source H.323 device.
4. **Q931 Setup with Token.** The source H.323 device sends a Q931 call setup message to the proxy. The Q931 call setup includes an OSP peering authorization token.
5. **NEW.** The proxy recognizes the presence of an OSP peering token in the Q931 call setup message and establishes a transaction with the OSP Toolkit to validate the token.

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

6. **ValidateAuth.** The proxy calls the OSP Toolkit function `OSPPTTransactionValidateAuthorisation` and passes the OSP token to the OSP Toolkit for validation. The OSP Toolkit determines if the token signature is valid and responds to the proxy. In this call scenario, the token is valid and the call processing continues. If the token invalid, the proxy should end the transaction with the OSP Toolkit and reject the call (test case 3.3.0). An important variable passed in this function call is `ospvTimeLimit` – which is the maximum call duration authorized by the OSP server. If the call duration exceeds the authorized time limit, the proxy should end the call (test case 3.3.4).
7. **GetLookAhead.** The proxy calls the OSP Toolkit function `OSPPTTransactionGetLookAhead` to determine if routing information for the second call leg was embedded in the OSP token. In this test case, no Look Ahead Routing information is included in the token and the inter-working proxy must query the OSP server for a destination gateway to complete the second call leg. (test case 3.3.5 provides an explanation of Look Ahead Routing.)
8. **NEW.** The proxy does not have a route defined to complete the call to the dialed number. The proxy will query an OSP server for a route to an inter-domain destination to complete the call. The proxy establishes a new transaction with the OSP client Toolkit using `OSPPTTransactionNew` function.
9. **SetNetworkID.** The `OSPPTTransactionSetNetworkIds` function call identifies the trunk group or partition in the source device which originated the call. In this test case, where the proxy is acting as a proxy, the `ospvSrcNetworkId` (trunk group or partition of the source device) must be taken from the Q931 Setup from the source device. The `SrcNetworkId` is included in the `AuthorizationRequest` to the OSP server and may be used by the OSP server operator for routing and billing of calls by source trunk group or partition.
10. **ReqAuth(In).** The proxy calls the OSP Toolkit function `OSPPTTransactionRequestAuthorisation`.
11. **Auth Req Leg 2.** The OSP client sends an `OSP AuthorizationRequest` to the OSP server requesting a list of devices which can complete the call. The OSP request includes the calling and called telephone numbers, and the IP address of the source SIP device.
12. **Auth Rsp Leg 2.** The OSP server sends an `OSP AuthorizationResponse` to the OSP client. The response includes the IP addresses of two destination SIP devices, the signaling protocol required by the destination devices and the version of OSP supported.
13. **ReqAuth(Out).** The OSP Toolkit responds to the proxy that the `OSPPTTransactionRequestAuthorisation` function is complete.
14. **Get1stDst.** The proxy calls the OSP client Toolkit function `OSPPTTransactionGetFirstDestination` to get the IP address of the first destination gateway.
15. **GetDstProt.** The proxy calls the OSP client Toolkit function `OSPPTTransactionGetDestProtocol` to get the signaling protocol required by the destination SIP device. In this case, the `DestinationProtocol` is SIP. If `DestinationProtocol` is not supported by the proxy (i.e. H323\_LRQ or IAX), the proxy

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

should reject the call and report a FailureReason of 111 (test case 3.1.5). If DestinationProtocol is unknown or undefined, the proxy may either reject the destination, with FailureReason 111, or attempt to complete the call using the proxy's default signaling protocol.

16. **IsDstOSPEnabled.** The OSPPTtransactionDestOSPEnabled function tells the proxy whether or not the destination device is OSP enabled and capable of validating the OSP authorization token. In this case the destination SIP device is not OSP enabled (OSPE\_OSP\_FALSE). The proxy should not include the OSP authorization token in the SIP INVITE to the destination device. (Note, to ensure backward compatibility with OSP V1.4.3, if OSPE\_OSP is unknown or undefined, the proxy should assume the destination is OSP enabled and include the OSP authorization token in the SIP INVITE to the destination.)
17. **GetNetworkID.** The proxy calls the OSP client Toolkit function OSPPTtransactionGetDestNetworkID to get the destination trunk group if it is available. If the destination trunk group is available, it should be included in the SIP INVITE to the destination.
18. **SIP INVITE.** The proxy sends a call setup message to the first SIP destination device. An OSP authorization token is not included in the SIP INVITE message since the destination gateway does not support OSP. Note: If source trunk group was included in the Q931 call setup message from the source device, it should NOT be included in the SIP INVITE to the destination.
19. **SIP 100 Trying.** The destination SIP device receives the SIP INVITE and responds to the proxy.
20. **SIP 503 Service Unavailable.** The destination SIP device does not accept the call setup and returns a SIP 503 Service Unavailable to the proxy. This test case applies for any case when the destination SIP device rejects the SIP INVITE. The call may be rejected for a variety of reasons such as unauthorized access or no circuits available.
21. **SIP ACK.** The proxy responds with a SIP ACK.
22. **GetNextDst.** The proxy retries the call to the second destination and calls OSP Toolkit function OSPPTtransactionGetNextDestination to obtain the IP address of the next destination SIP device. The GetNextDestination function call should include the FailureReason for the previous failed call attempt. In this case the FailureReason should be the release cause reported by the destination or 503.
23. **GetDstProt.** The proxy calls the OSP client Toolkit function OSPPTtransactionGetDestProtocol to get the signaling protocol required by the destination SIP device. In this case, the DestinationProtocol is SIP. If DestinationProtocol is not supported by the proxy (i.e. H323\_LRQ or IAX), the proxy should reject the call and report a FailureReason of 111 (test case 3.1.5). If DestinationProtocol is unknown or undefined, the proxy may either reject the destination, with FailureReason 111, or attempt to complete the call using the proxy's default signaling protocol.
24. **IsDstOSPEnabled.** The OSPPTtransactionDestOSPEnabled function tells the proxy whether or not the destination device is OSP enabled and capable of validating the OSP authorization token. In this case the destination SIP device is not OSP enabled

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

(OSPE\_OSP\_FALSE). The proxy should not include the OSP authorization token in the SIP INVITE to the destination device. (Note, to ensure backward compatibility with OSP V1.4.3, if OSPE\_OSP is unknown or undefined, the proxy should assume the destination is OSP enabled and include the OSP authorization token in the SIP INVITE to the destination.)

25. **GetNetworkID**. The proxy calls the OSP client Toolkit function OSPPGetDestNetworkID to get the destination trunk group if it is available. If the destination trunk group is available, it should be included in the SIP INVITE to the destination.
26. – 36. Standard H.323 to SIP communications for the completing the call.
37. **RecordFailure**. At the completion of the call, the proxy reports the call disconnect reason for the successful retry of the second call leg, to the OSP Toolkit using the OSPPTtransactionRecordFailure function.
38. **RepUsage(In)**. The proxy calls the OSPPTtransactionReportUsage function to report the call duration for the second call leg.
39. **Src Usg Ind Leg 2**. The OSP client sends an OSP UsageIndication message (Call Detail Record) to the OSP server. The UsageIndication is a type ‘source’ call detail record since the proxy is the source device for the second leg of the call.
40. **Src Usg Cnf Leg 2**. The OSP server responds with an OSP UsageConfirmation message.
41. **RepUsage(Out)**. The OSP Toolkit closes the ReportUsage transaction.
42. **TransDelete**. The proxy deletes the OSP Toolkit transaction for the second call leg.
43. **RecordFailure**. The proxy reports the call disconnect reason, for the first call leg, to the OSP Toolkit using the OSPPTtransactionRecordFailure function.
44. **RepUsage(In)**. The proxy calls the OSPPTtransactionReportUsage function to report the call duration for the first call leg.
45. **Src Usg Ind Leg 1**. The OSP client sends an OSP UsageIndication message (Call Detail Record) to the OSP server. The UsageIndication is a type ‘destination’ call detail record since the proxy is the destination device for the first leg of the call.
46. **Src Usg Cnf Leg 1**. The OSP server responds with an OSP UsageConfirmation message.
47. **RepUsage(Out)**. The OSP Toolkit closes the ReportUsage transaction.
48. **TransDelete**. The proxy deletes the OSP Toolkit transaction for the first call leg.

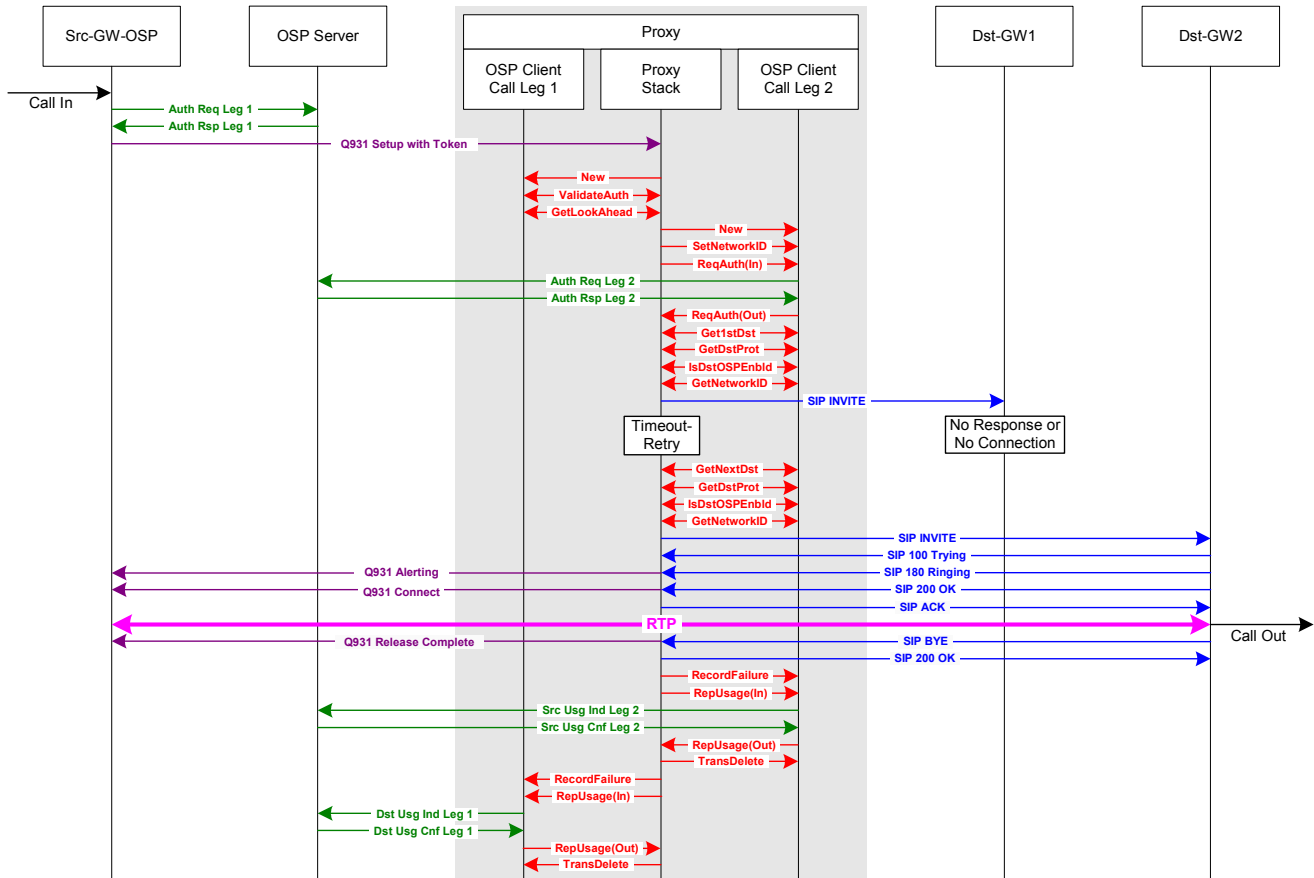
### Expected CDRs for Test Case 3.3.1

This test case should generate three OSP UsageIndication messages, or CDRs, from the proxy. Two CDRs as the source of call leg 2 and one CDR as the destination of call leg 1. The release reason (ospvFailureReason) in the source CDR for call leg 2 for the first call attempt should be the SIP response from Dst-GW1. In this example, the SIP response is 503, but other SIP responses are also valid. For the successful retry for call leg 2, the proxy should set the FailureReason to 16 or 1016 in the source CDR, since there is no release reason in a SIP BYE message for a successful call. For the destination CDR for call leg 1, the FailureReason should also be set to 16 or 1016 by the proxy.

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	Source	Src-GW-OSP	Dst-GW1	503	0
2	Source	Src-GW-OSP	Dst-GW2	16 or 1016	greater than 0
1	destination	Src-GW-OSP	Proxy	16 or 1016	greater than 0

### 3.3.2. No Response or No Connection and Retry - Proxy Times Out



**Test Case 3.3.2: OSP H.323 Source to Proxy to non-OSP SIP Destination:  
No Response or No Connection & Retry - Proxy Times Out**

Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green

#### Test Case Notes

This case tests the call scenarios when a destination SIP device does not respond to the proxy. This test case requires that the OSP server return two or more destinations in the AuthorizationResponse to the proxy. After the first call attempt fails, the proxy must retry the call to second destination. This test case must be executed four times to test the following four different call scenarios.

1. The proxy cannot establish a TCP connection with Dst-GW1. After TCP time-out, the proxy should retry call to Dst-GW2. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 47 – resource unavailable, unspecified.)

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

2. No route to IP address of Dst-GW1 IP device. The proxy should retry call to Dst-GW2. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 2 – no route to specified transit network.)
3. TCP connection refused by destination Dst-GW1. After TCP connection is refused, the proxy should retry the call to Dst-GW2. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 63 – service or option not available, unspecified.)
4. No response from Dst-GW1. The proxy establishes TCP connection with Dst-GW1, but Dst-GW1 never responds to SIP INVITE. The proxy should time-out and retry the call to Dst-GW2. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 27 – destination out of order.)

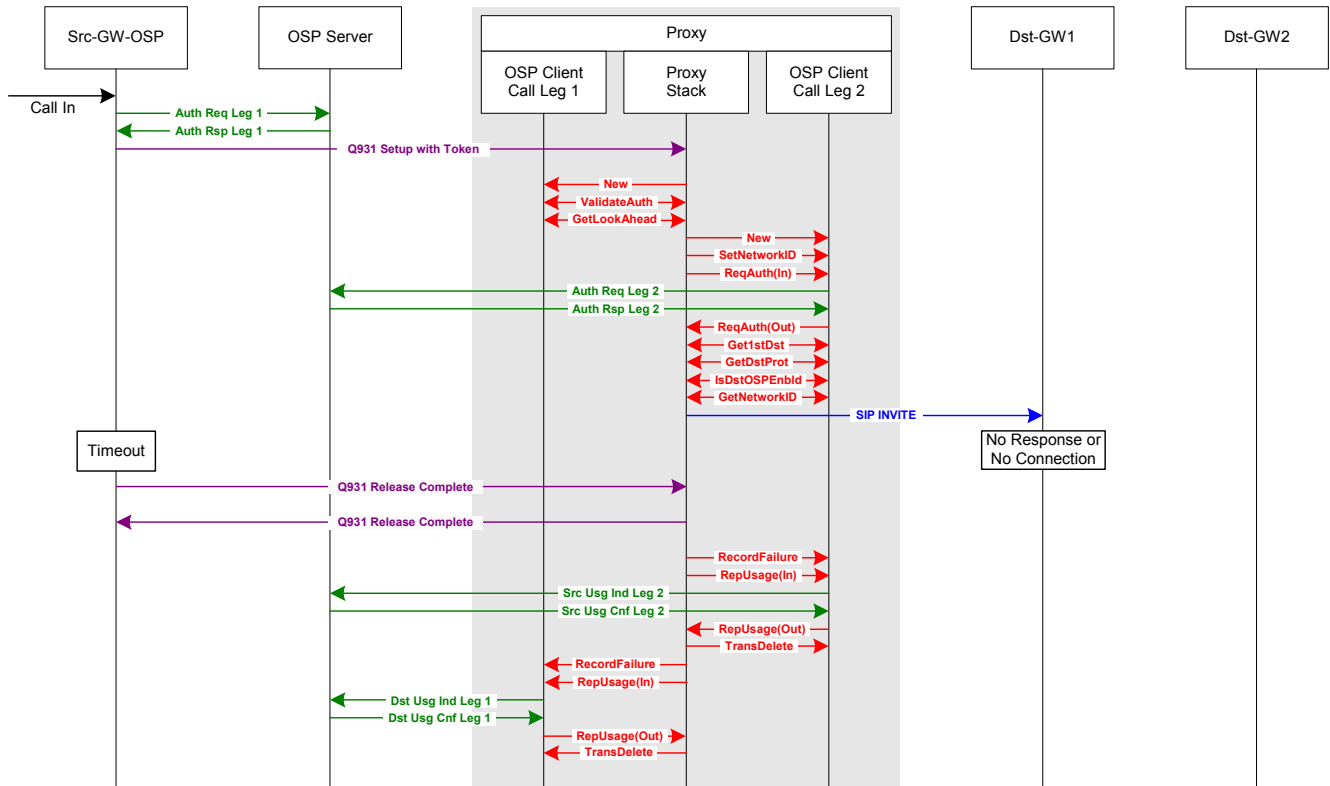
**Note:** The destination UsageIndication call detail record for call leg one, should have FailureReason set to the release code for the last call attempt. If no call release reason is included with the SIP BYE from the destination for a successful call, the FailureReason should be set to 16 or 1016.

### Expected CDRs for Test Case 3.3.2

This test case should generate three OSP UsageIndication messages, or CDRs, from the proxy. Two CDRs created as the source of call leg 2 and one CDR as the destination of call leg 1. The release reason (ospvFailureReason), or termination cause code, for the first attempt of call leg 2 should be determined by the proxy based on the reason for the failure. For the successful retry of call leg 2, the proxy should set the FailureReason to 16 or 1016, since there is no release reason in a SIP BYE message for a successful call. The FailureReason for the destination CDR of call leg 1 should be 16 or 1016.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW-OSP	Dst-GW1	47, 2, 63 or 27	0
2	source	Src-GW-OSP	Dst-GW2	16 or 1016	greater than 0
1	destination	Src-GW-OSP	Proxy	16 or 1016	greater than 0

3.3.3. No Response or No Connection and Retry - Source Times Out



Test Case 3.3.3: OSP H.323 Source to Proxy to non-OSP SIP Destination: No Response or No Connection & Retry - Source Times Out

Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

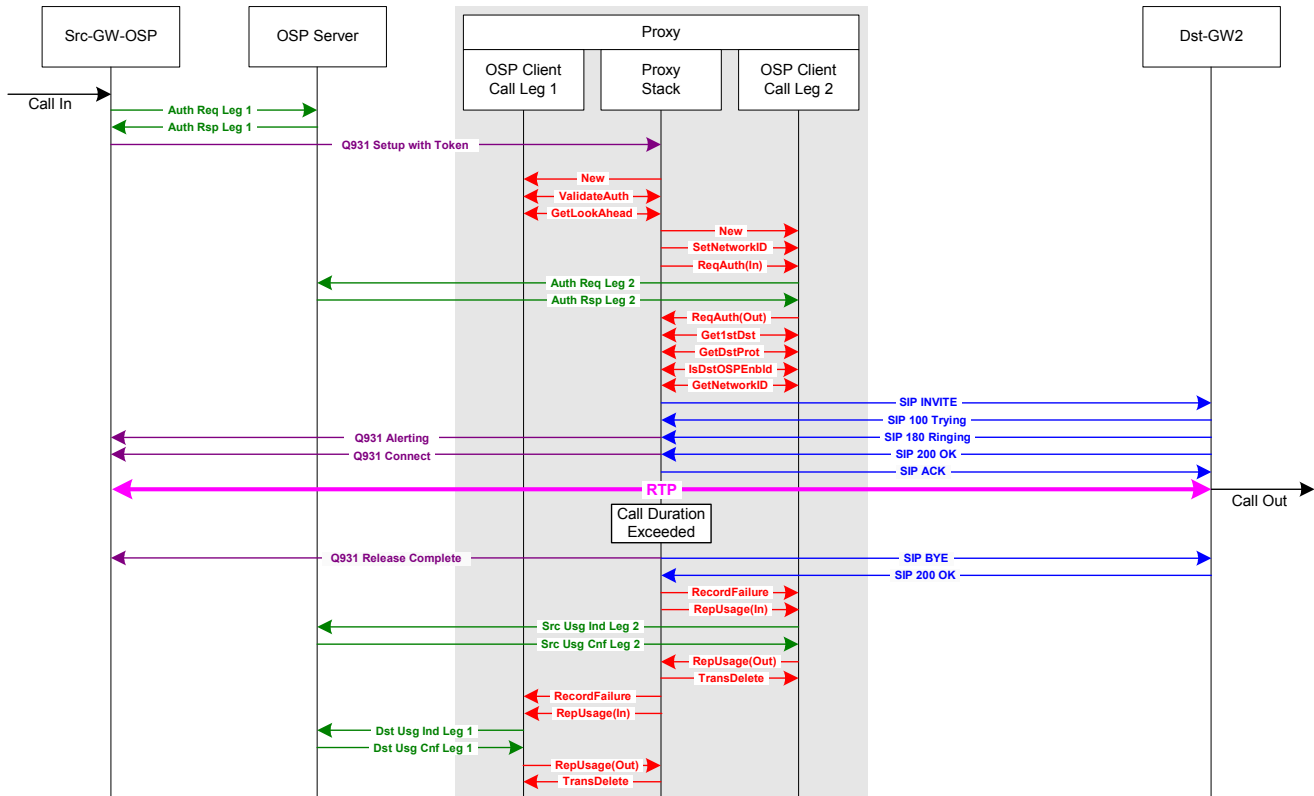
This case tests the call scenario when the source ends the call before the first destination Dst-GW1 responds to the SIP INVITE from the proxy. In these cases, the proxy should terminate the call and report usage to the OSP server. The OSP Toolkit parameter FailureReason reported with the OSPPTtransactionRecordFailure function should be set to the release cause reported in the Q931 Release Complete from the source device, Src-GW. The FailureReason should be the same and included in the RecordFailure function for both the source UsageIndication call detail record for call leg two and the destination UsageIndication call detail record for call leg one.

Expected CDRs for Test Case 3.3.3

This test case should generate two OSP UsageIndication messages, or CDRs, from the proxy. One CDR as the source of call leg 2 and another as the destination of call leg 1. The release reason (ospvFailureReason), or termination cause code, for the CDRs should be determined by the release reason included in the Q931 Release Complete message from Src-GW-OSP.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW-OSP	Dst-GW1	16 or 1016	0
1	destination	Src-GW-OSP	Proxy	16 or 1016	0

### 3.3.4. Call Duration Limit Exceeded



**Test Case 3.3.4: OSP H.323 Source to Proxy to non-OSP SIP Destination: Call Duration Limit Exceeded**  
**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

This call scenario tests the proxy’s ability to end a call when its authorized call duration has been exceeded. In the AuthorizationResponse, the OSP server includes the authorized call duration. The OSP Toolkit parameter `ospvTimeLimit`, returned in the `GetFirstDestination` or `GetNextDestination` function calls, defines the maximum duration for each call. The proxy should terminate a call when the call duration exceeds the `TimeLimit`. In this case, when the proxy forcefully ends a call that has exceeded its maximum call duration, the proxy should use the `RecordFailure` OSP Toolkit function call to report a `FailureReason` of 8 (preemption) and then use the `ReportUsage` OSP Toolkit function call to send a `UsageIndication` call detail record to the OSP server.

**Note:** In this call scenario, there are two authorized call durations. The authorized call duration for call leg one is defined by the `ospvTimeLimit` variable returned by the `OSPPTtransactionValidateAuthorization` function. The authorized call duration for call leg two is defined by the `ospvTimeLimit` variable returned by the `OSPPTtransactionGetFirstDestination` or `OSPPTtransactionGetNextDestination` functions. When the `ospvTimeLimit` for call leg one and two are different, the shorter `TimeLimit` takes priority and should be used by the proxy to determine when to forcefully end a call.

#### Expected CDRs for Test Case 3.3.4

This test case should generate two OSP `UsageIndication` messages, or CDRs. One from the proxy as the source of call leg 2 and another as the destination for call leg 1. The

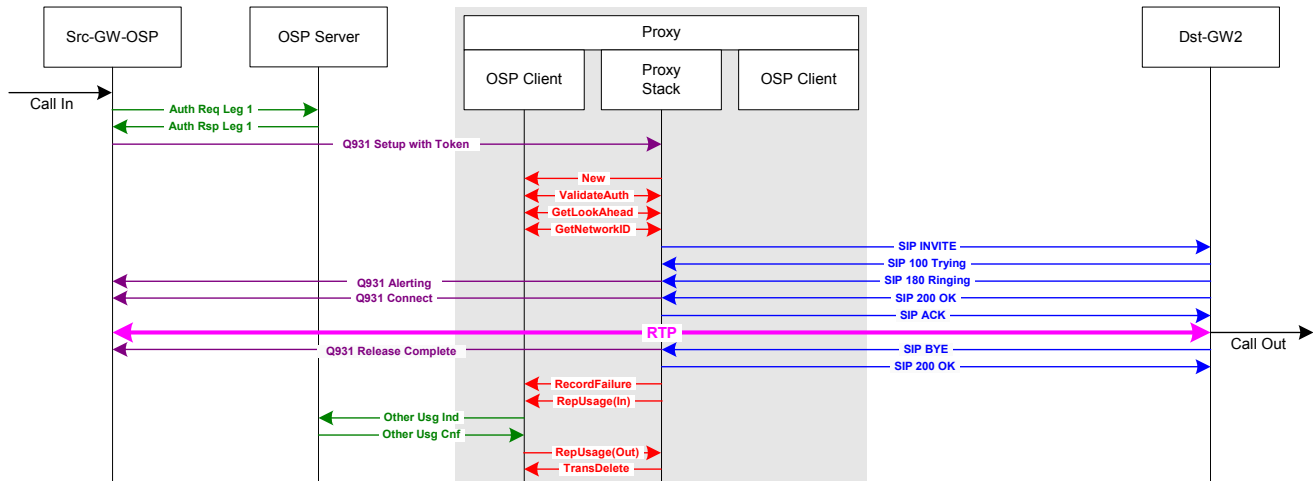
## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

release reason (ospvFailureReason), or termination cause code, for the call should be set by the proxy to 8 to indicate the call was forcefully shutdown by the proxy.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW-OSP	Dst-GW2	8	greater than 0
1	destination	Src-GW-OSP	Proxy	8	greater than 0

### 3.3.5. Look Ahead Routing

Look Ahead Routing is a unique OSP application for proxies. In this test case for Look Ahead Routing the IP address, destination protocol, OSP version and destination trunk group of the destination device are embedded in the OSP authorization token sent from the source device to the proxy. When the proxy validates the OSP token, the proxy calls the function OSPPTTransactionGetLookAheadInfoIfPresent. If Look Ahead Routing information is available, it is passed from the OSP client to the proxy and eliminates the need for a second lookup to the OSP server. Note that only one OSP Toolkit transaction between the proxy and the OSP Toolkit is required when Look Ahead Routing is used.



**Test Case 3.3.5: OSP H.323 Source to Proxy to non-OSP SIP Destination: Look Ahead Routing**  
**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Detailed Description of Test Case

1. **Call In.** The call begins at the source H.323 device.
2. **Auth Req Leg 1.** The source H.323 device sends an OSP AuthorizationRequest to the OSP server.
3. **Auth Rsp Leg 1.** The OSP server returns the IP address, DestinationProtocol, and OSPVersion of the proxy, plus a digitally signed peering authorization token, to the source H.323 device.
4. **Q931 Setup with Token.** The source H.323 device sends a Q931 call setup message to the proxy. The Q931 Setup header includes an OSP peering authorization token.
5. **NEW.** The proxy recognizes the presence of an OSP authorization token in the Q931 Setup message call setup and establishes a transaction with the OSP Toolkit to validate the token's digital signature.

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

6. **ValidateAuth.** The proxy calls the OSP Toolkit function `OSPPTTransactionValidateAuthorisation` and passes the OSP token to the OSP Toolkit for validation. The OSP Toolkit determines if the token signature is valid and responds to the proxy. In this call scenario, the token is valid and the call processing continues. If the token was not valid, the proxy would end the transaction with the OSP Toolkit and reject the call (test case 3.3.0). An important variable passed in this function call is `ospvTimeLimit` – which is the maximum call duration authorized by the OSP server. If the call duration exceeds the authorized time limit, the proxy should end the call (test case 3.3.4).
7. **GetLookAhead.** The proxy calls the OSP Toolkit function `OSPPTTransactionGetLookAheadInfoIfPresent` to determine if routing information for the second call leg was embedded in the OSP token. In this test case, Look Ahead Routing information is present and the function call returns the destination IP address, the destination protocol (`OSPE_DEST_PROT`) and the destination OSP enabled status (`OSPE_OSP`).

**Note:** For this test case, the expected value for `OSPE_DEST_PROT` is SIP. If `OSPE_DEST_PROT` is `UNDEFINED` or `UNKNOWN`, the proxy may reject the destination, and report `FailureReason 111`, or attempt to complete the call to the destination using the proxy's default signaling protocol. If `OSPE_DEST_PROT` is a protocol not supported by the proxy, such as `H323_LRQ` or `IAX`, the proxy should reject the destination and report a `FailureReason` of `111` (protocol error).

**Note:** For this test case, the expected value for `OSPE_OSP` is `FALSE`. The Look Ahead destination is not OSP enabled, therefore no token should be included in the SIP INVITE to the destination. A value of `OSPE_OSP_TRUE` indicates that the Look Ahead destination is OSP enabled and that the LookAhead token should be included, as is, in the SIP INVITE to the destination. If `OSPE_OSP` is `UNKNOWN` or `UNDEFINED`, the proxy should assume the Look Ahead destination is OSP enabled and include the Look Ahead token in the SIP INVITE to the destination.
8. **GetNetworkID.** The proxy calls the OSP client Toolkit function `OSPPTTransactionGetDestNetworkID` to get the destination trunk group if it is available. The Look Ahead token may also include the destination trunk group of the destination device. If the destination trunk group is available, it should be included in the SIP INVITE to the destination.
9. **SIP INVITE.** The proxy sends a call setup message to the SIP destination device. An OSP peering authorization token is not included in the SIP INVITE message since the destination gateway does not support OSP. Note: If source trunk group was included in the SIP INVITE from the source device, it should NOT be included in the SIP INVITE from the proxy to the destination.
10. – 20. Standard H.323 to SIP communications for the completing the call.
21. **RecordFailure.** At the completion of the call, the proxy reports the call disconnect reason for the call to the OSP Toolkit using the `OSPPTTransactionRecordFailure` function.
22. **RepUsage(In).** The proxy calls the `OSPPTTransactionReportUsage` function to report the call duration for the second call leg.

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

23. **Other Usg Ind.** The OSP client sends an OSP UsageIndication message (Call Detail Record) to the OSP server. The UsageIndication is a type ‘other’ call detail record. In a Look Ahead call scenario, the proxy is the destination device for the first call leg and the source device for the second call leg.
24. **Other Usg Cnf.** The OSP server responds with an OSP UsageConfirmation message.
25. **RepUsage(Out).** The OSP Toolkit closes the ReportUsage transaction.
26. **TransDelete.** The proxy deletes the OSP Toolkit transaction for the call.

### Test Case Notes

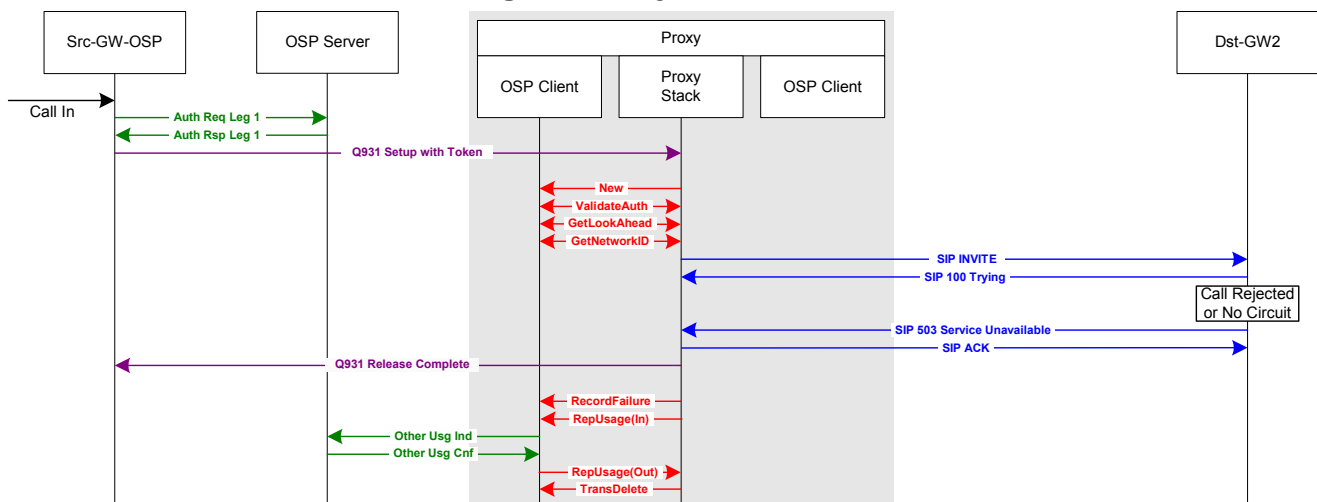
V3.3.6, and earlier versions, of the OSP Toolkit support only a single Look Ahead route embedded in an OSP authorization token. Future releases of the OSP Toolkit will support multiple destinations in a Look Ahead token so the proxy can retry the call to other destinations if the call attempt to the first destination fails.

### Expected CDR for Test Case 3.3.5

This test case should generate one OSP UsageIndication message, or CDR, from the proxy. Look Ahead Routing is a unique case when one OSP Toolkit transaction validates inbound call leg 1 and routes outbound call leg 2. Since one CDR is used to report usage for both the destination of call leg 1 and the source of call leg 2, the role is defined as other. As with other call scenarios, the FailureReason should be determined by the release code included in the Q931 Release Complete from the source device, or the SIP response from the destination device. If the call is successful and there is no release code reported, the proxy should report the FailureReason as 16 or 1016 to the OSP Toolkit ReportUsage function.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2	16 or 1016	greater than 0

### 3.3.6. Look Ahead Routing: Call Rejected or No Circuit



Test Case 3.3.6: OSP H.323 Source to Proxy to non-OSP SIP Destination:  
Look Ahead Routing - Call Rejected or No Circuit & Retry

Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

### Test Case Notes

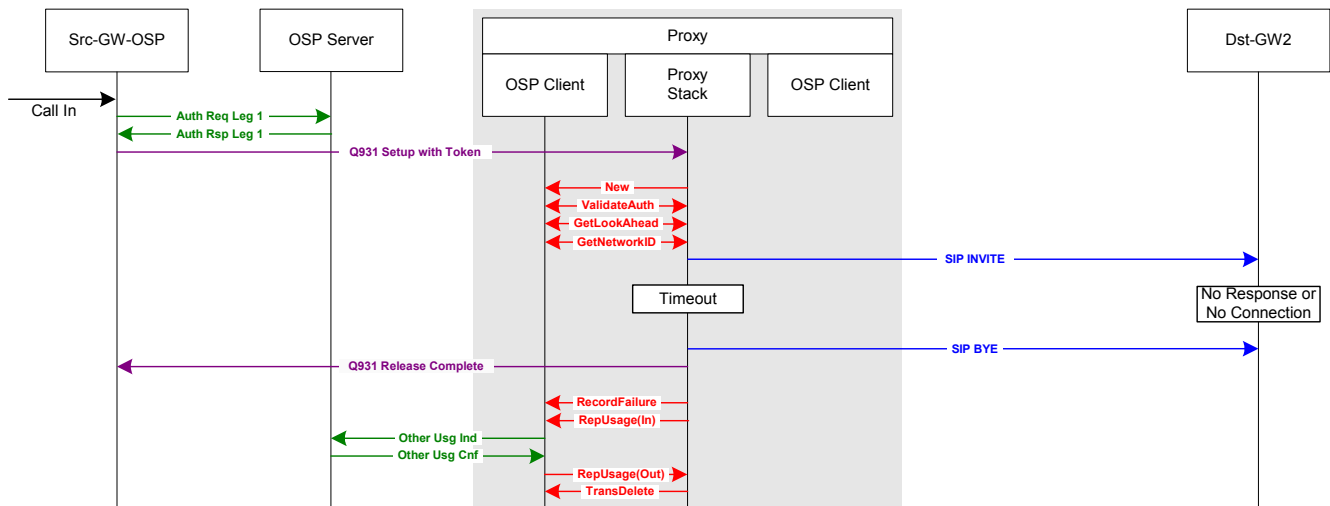
This case is similar to test case 3.3.1 and tests a Look Ahead call scenario when the destination SIP device rejects the call.

### Expected CDR for Test Case 3.3.6

This test case should generate one OSP UsageIndication message, or CDR, from the proxy. The role should be 'other' and the FailureReason should be determined by the SIP response from the destination device. In this example, the SIP response is 503, but other SIP responses are also valid.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2	503	0

### 3.3.7. Look Ahead Routing: No Response or No Connection - Proxy Times Out



**Test Case 3.3.7: OSP H.323 Source to Proxy to non-OSP SIP Destination:  
Look Ahead Routing - No Response or No Connection - Proxy Times Out**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

### Test Case Notes

This case is similar to test case 3.3.2 and tests a Look Ahead call scenario when the destination SIP device does not respond to the proxy. This test case must be executed four times to test the following four different call scenarios.

1. The proxy cannot establish a TCP connection with Dst-GW1. After a TCP time-out, the proxy should retry call to Dst-GW2. (When OSP Toolkit function RecordFailure is called, the FailureReason for the call attempt should be set to 47 – resource unavailable, unspecified.)
2. No route to IP address of Dst-GW1. The proxy should retry call to Dst-GW2. (When OSP Toolkit function RecordFailure is called, the FailureReason for the call attempt should be set to 2 – no route to specified transit network.)
3. TCP connection refused by destination. After the TCP connection is refused, the proxy should retry the call to Dst-GW2. (When OSP Toolkit function RecordFailure

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

is called, the FailureReason for the call attempt should be set to 63 – service or option not available, unspecified.)

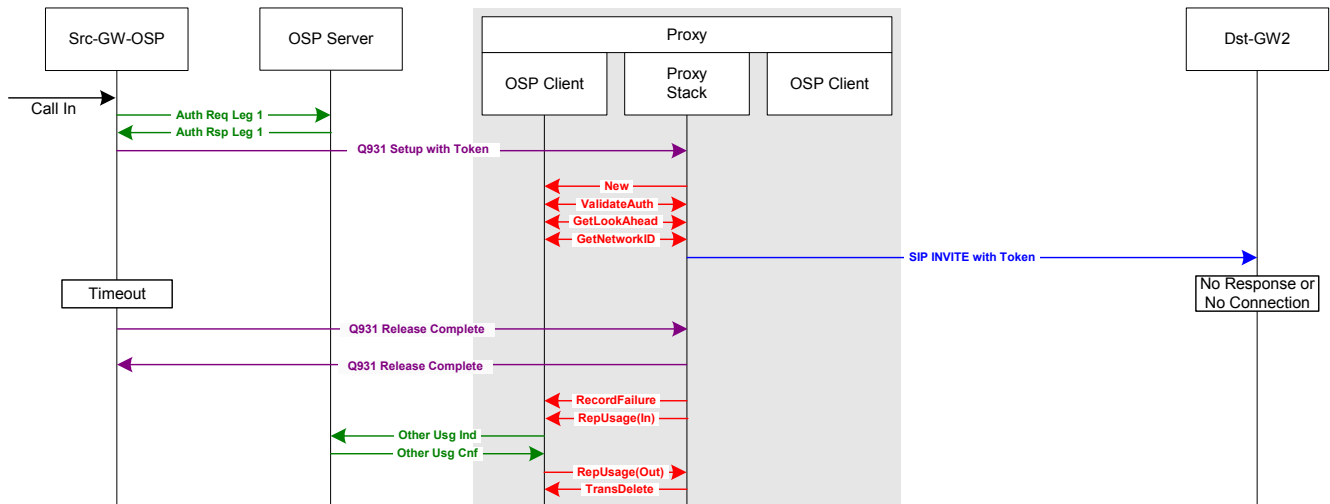
- No response from Dst-GW1. The proxy establishes a TCP connection with Dst-GW1, but Dst-GW1 never responds to SIP INVITE. The proxy should time-out and retry the call to Dst-GW2. (When OSP Toolkit function RecordFailure is called, the FailureReason for the call attempt should be set to 27 – destination out of order.)

### Expected CDR for Test Case 3.3.7

This test case should generate one OSP UsageIndication message, or CDR, from the proxy. The role should be ‘other’ and the FailureReason should be determined by the proxy based on the failure reasons described above.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2	47, 2, 63 or 27	0

### 3.3.8. Look Ahead Routing: No Response or No Connection - Source Times Out



**Test Case 3.3.8: OSP H.323 Source to Proxy to non-OSP SIP Destination: Look Ahead Routing - No Response or No Connection - Source Times Out**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

### Test Case Notes

This test case is similar to test case 3.3.3 and tests the Look Ahead call scenario when the source ends the call before the destination Dst-GW2 responds to the SIP INVITE from the proxy. In this case, the proxy should terminate the call and report usage to the OSP server. The OSP Toolkit parameter FailureReason reported with the OSPTransactionRecordFailure function should be set to the release cause reported in the Q931 Release Complete message from the source device, Src-GW.

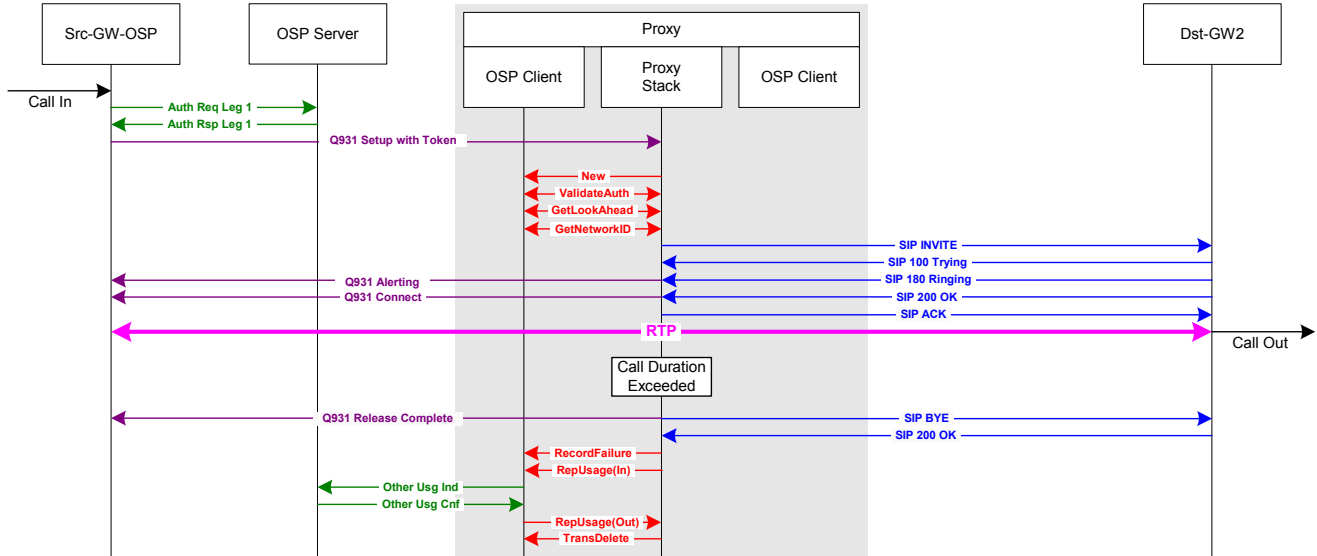
### Expected CDR for Test Case 3.3.8

This test case should generate one OSP UsageIndication message, or CDR, from the proxy. The role should be ‘other’ and the FailureReason should be determined by the release reason in the Q931 Release Complete message from Src-GW.

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2	16 or 1016	0

### 3.3.9. Look Ahead Routing: Call Duration Limit Exceeded



**Test Case 3.3.9: OSP H.323 Source to Proxy to non-OSP SIP Destination:  
Look Ahead Routing - Call Duration Limit Exceeded**

Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green

#### Test Case Notes

If the call duration exceeds the authorized call duration set by `ospvTimeLimit` value returned from the `OSPTransactionValidateAuthorisation` function, the proxy should forcefully end the call. When the proxy forcefully ends the call because the call duration exceeded the authorized time limit, the `FailureReason` parameter reported in the `RecordFailure` function should be set to 8 (preemption).

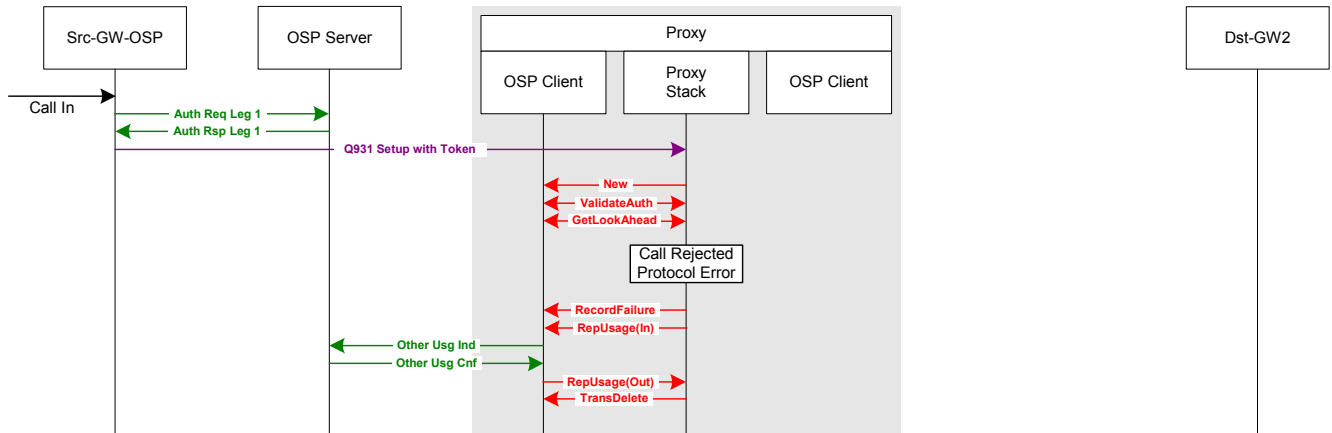
#### Expected CDR for Test Case 3.3.9

This test case should generate one OSP UsageIndication message, or CDR, from the proxy. The role should be 'other' and the `FailureReason` should be 8 to indicate the call was forcefully shutdown by the proxy.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2	8	0

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

### 3.3.10. Look Ahead Routing: Protocol Error



**Test Case 3.3.10: OSP H.323 Source to Proxy to non-OSP SIP Destination: Look Ahead Routing**  
**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

This case tests the error condition when the OSP server returns a DestinationProtocol in the Look Ahead token that is not supported by the proxy, such as H323\_LRQ or IAX. When this occurs, the proxy should reject the destination, record FailureReason 111 (protocol error) and report usage.

For this test case, the destination protocol configured on the OSP server for device Dst-GW2 is NOT supported by the proxy. The OSPPTTransactionGetLookAheadInfoIfPresent function call returns a DestinationProtocol which the proxy does not support. The proxy should recognize the protocol error and reject the call attempt. Note, if the DestinationProtocol is unknown or undefined, the proxy may either reject the destination, and report FailureReason 111, or attempt to complete the call using the proxy's default signaling protocol.

#### Expected CDRs for Test Case 3.3.10

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2	111	0

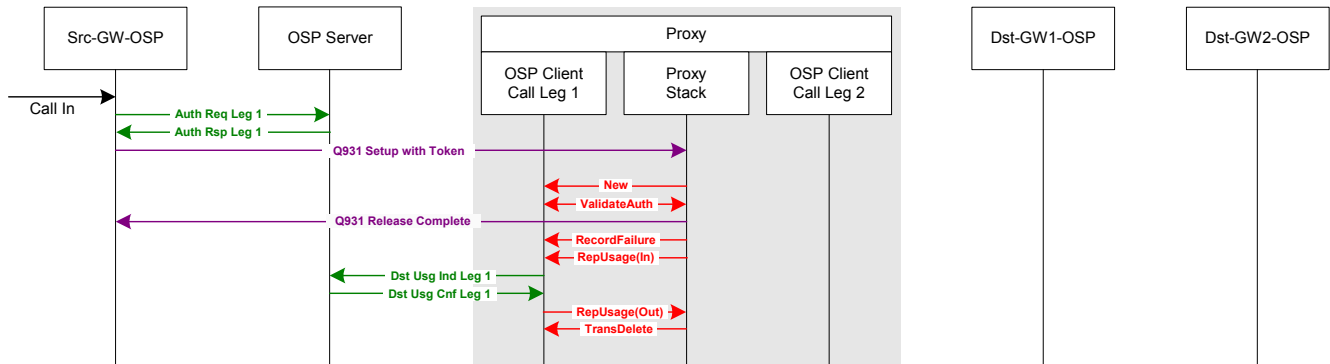
## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

### 3.4. OSP Source to OSP Destination

This subsection of test cases describes call scenarios where both the source and destination devices are OSP enabled. The source H.323 device will include an OSP authorization token in the Q931 call setup message sent to the proxy. Based on the test case, the OSP token may or may not include Look Ahead Routing information. To complete the call, the proxy must include an OSP authorization token in the SIP INVITE message to the destination SIP device. The destination SIP device will extract the token from the call setup and validate the token signature to determine if the call from the proxy should be accepted.

Configuration of VoIP devices on OSP server for test cases in section 3.4		
Device	Destination Protocol	OSP Version
Src-GW-OSP	H323_Q931	1.3.4 , 2.1.1 or 4.1.1
Proxy	SIP or H323_Q931	2.1.1 or 4.1.1
Dst-GW1-OSP	SIP	1.3.4 , 2.1.1 or 4.1.1
Dst-GW2-OSP	SIP	1.3.4 , 2.1.1 or 4.1.1

#### 3.4.0. Invalid Authorization Token



**Test Case 3.4.0: OSP H.323 Source to Proxy to OSP SIP Destination: Invalid Authorization Token**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

This test case is identical to 3.3.0.

#### Expected CDR for Test Case 3.4.0

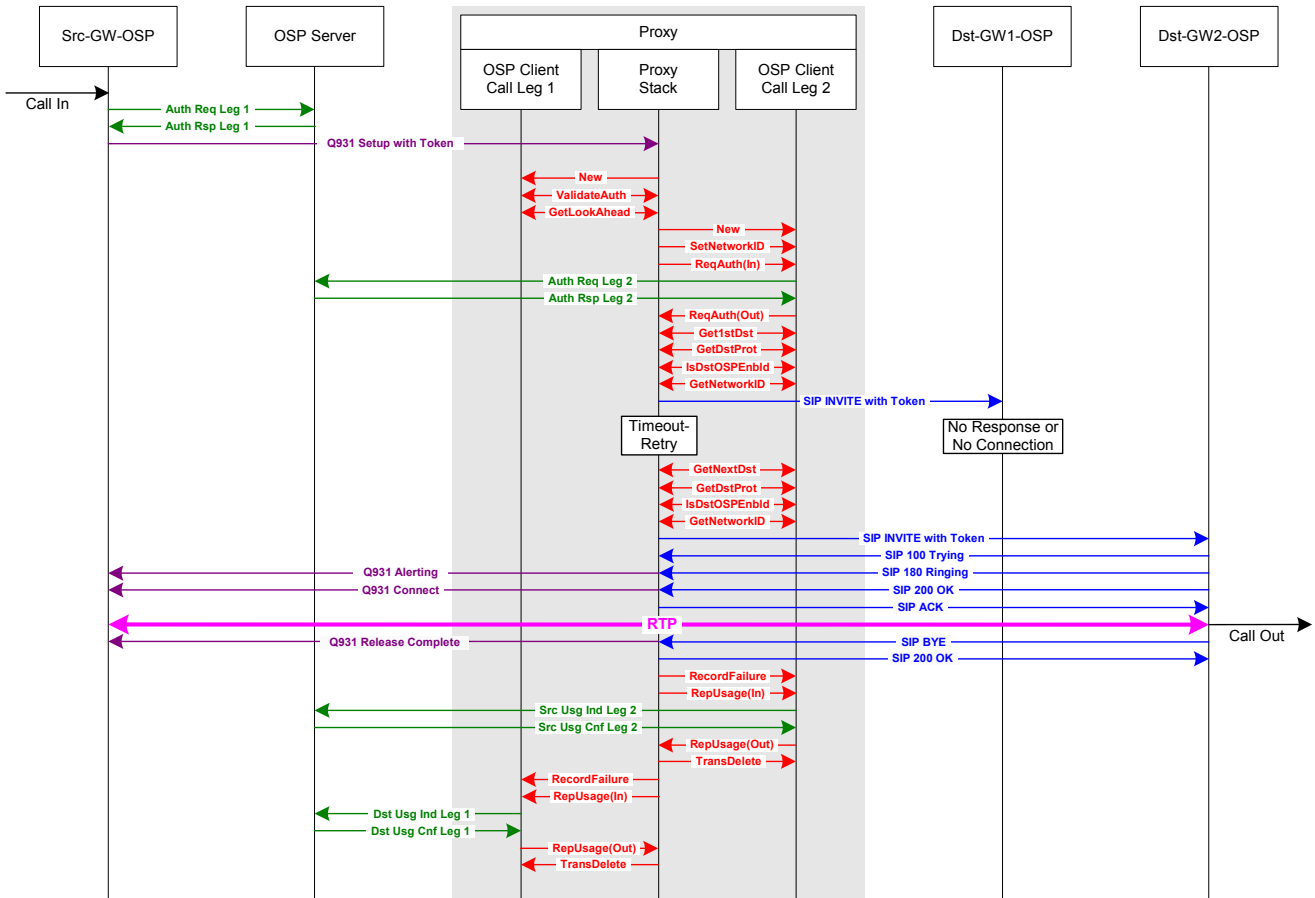
This test case should generate one OSP UsageIndication message, or CDR, from the proxy as the destination of call leg 1. The release reason (ospvFailureReason), or termination cause code, for the call should be set by the proxy to 21 to indicate the peering authorization token was invalid.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1	destination	Src-GW-OSP	Proxy	21	0



## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

### 3.4.2. No Response or No Connection and Retry - Proxy Times Out



**Test Case 3.4.2: OSP H.323 Source to Proxy to OSP SIP Destination:  
No Response or No Connection & Retry - Proxy Times Out**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

See test case 3.3.2.

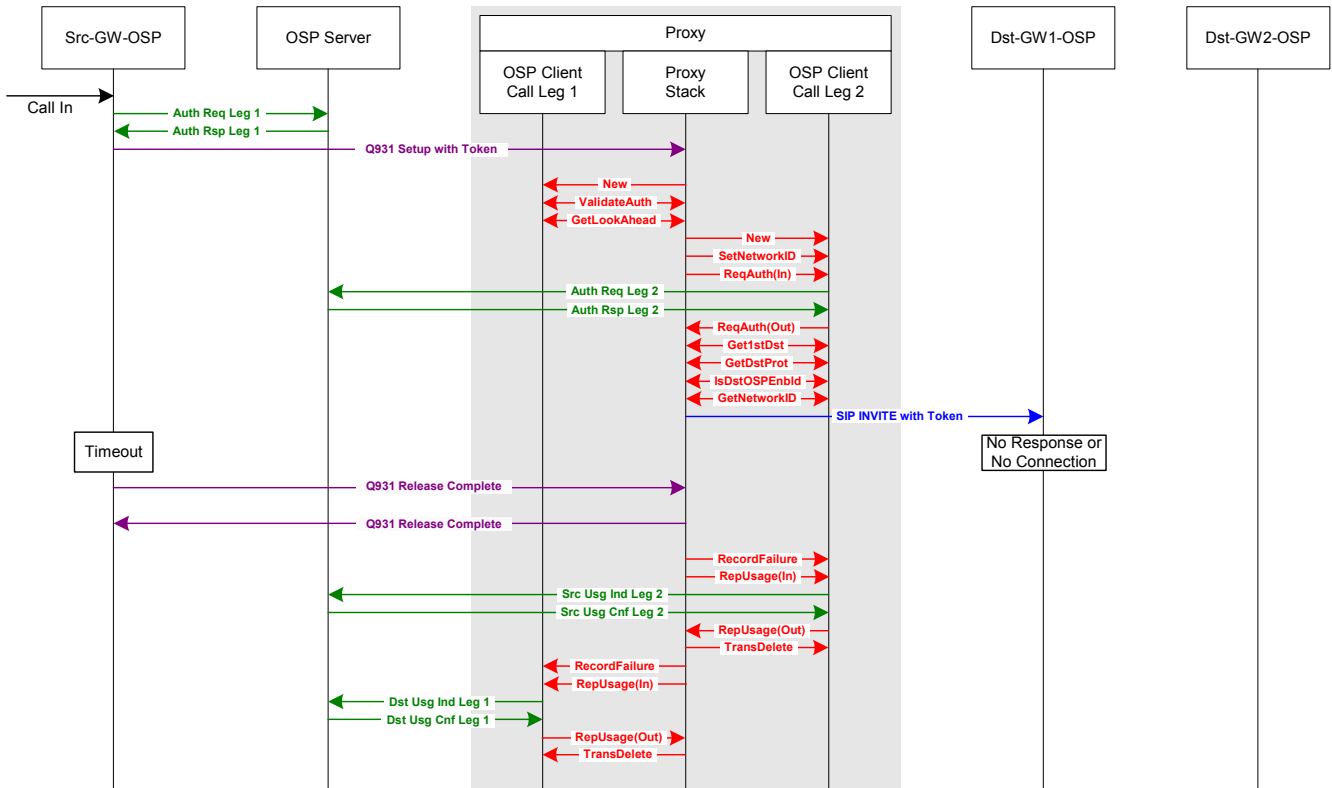
#### Expected CDRs for Test Case 3.4.2

This test case should generate three OSP UsageIndication messages, or CDRs, from the proxy. Two CDRs created as the source of call leg 2 and one CDR as the destination of call leg 1. The release reason (ospvFailureReason), or termination cause code, for the first attempt of call leg 2 should be determined by the proxy based on the reason for the failure. For the successful retry of call leg 2, the proxy should set the FailureReason to 16 or 1016, since there is no release reason in a SIP BYE message for a successful call. The FailureReason for the destination CDR of call leg 1 should be 16 or 1016.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW-OSP	Dst-GW1-OSP	47, 2, 63 or 27	0
2	source	Src-GW-OSP	Dst-GW2-OSP	16 or 1016	greater than 0
1	destination	Src-GW-OSP	Proxy	16 or 1016	greater than 0

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

### 3.4.3. No Response or No Connection and Retry - Source Times Out



**Test Case 3.4.3: OSP H.323 Source to Proxy to OSP SIP Destination:  
No Response or No Connection & Retry - Source Times Out**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

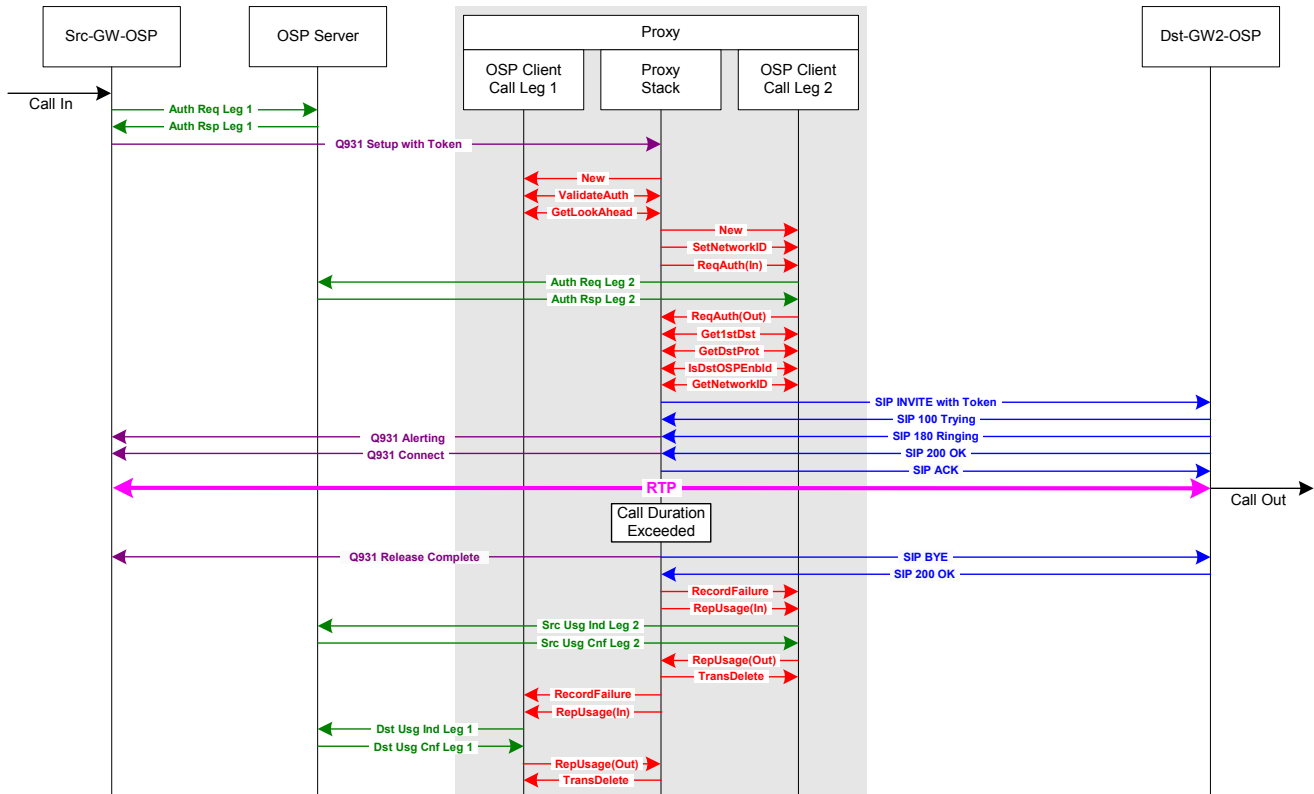
See test case 3.3.3.

#### Expected CDRs for Test Case 3.4.3

This test case should generate two OSP UsageIndication messages, or CDRs, from the proxy. One CDR as the source of call leg 2 and another as the destination of call leg 1. The release reason (ospvFailureReason), or termination cause code, for the CDRs should be determined by the release reason included in the Q931 Release Complete message from Src-GW-OSP.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW-OSP	Dst-GW1-OSP	16 or 1016	0
1	destination	Src-GW-OSP	Proxy	16 or 1016	0

### 3.4.4. Call Duration Limit Exceeded



**Test Case 3.4.4: OSP H.323 Source to Proxy to OSP SIP Destination: Time Limit Exceeded**  
 Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green

#### Test Case Notes

This call scenario tests the proxy’s ability to end a call when its authorized call duration has been exceeded. In the AuthorizationResponse, the OSP server includes the authorized call duration. The OSP Toolkit parameter TimeLimit, returned in the GetFirstDestination or GetNextDestination function calls, defines the maximum duration for each call. The proxy should terminate a call when the call duration exceeds the TimeLimit. In this case, when the proxy forcefully ends a call that has exceeded its maximum call duration, the proxy should use the RecordFailure OSP Toolkit function call to report a FailureReason of 8 (preemption) and then use the ReportUsage OSP Toolkit function call to send a UsageIndication call detail record to the OSP server.

**Note:** In this call scenario, there are two authorized call durations. The authorized call duration for call leg one is defined by the ospvTimeLimit variable returned by the OSPPTtransactionValidateAuthorization function. The authorized call duration for call leg two is defined by the ospvTimeLimit variable returned by the OSPPTtransactionGetFirstDestination or OSPPTtransactionGetNextDestination functions. When the ospvTimeLimit for call leg one and two are different, the shorter TimeLimit takes priority and should be used by the proxy to determine when to forcefully end a call.

#### Expected CDRs for Test Case 3.4.4

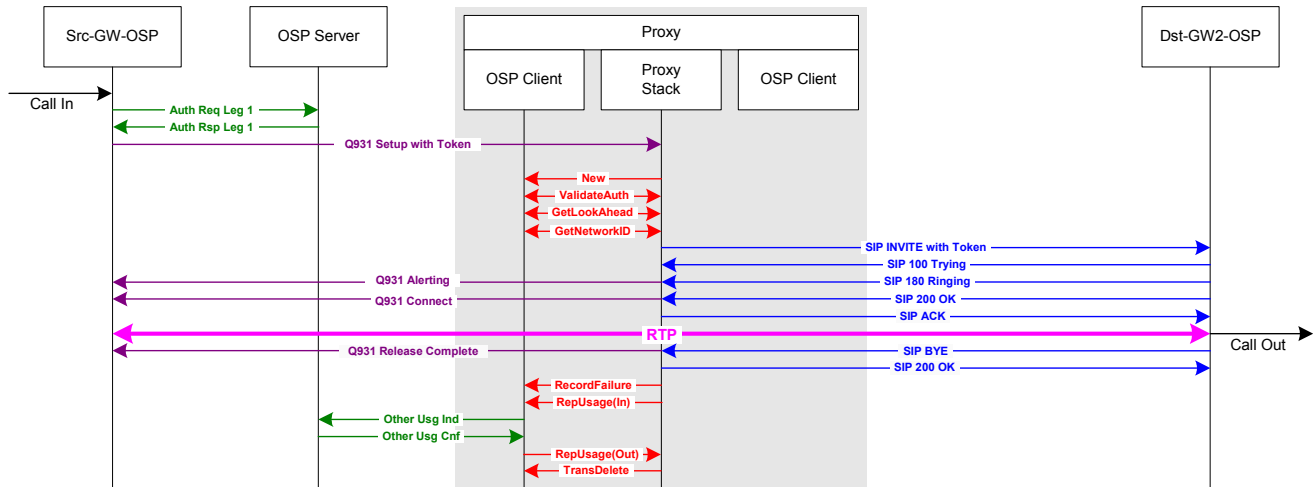
This test case should generate two OSP UsageIndication messages, or CDRs. One from the proxy as the source of call leg 2 and another as the destination for call leg 1. The

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

release reason (ospvFailureReason), or termination cause code, for the call should be set by the proxy to 8 to indicate the call was forcefully shutdown by the proxy.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-GW-OSP	Dst-GW2-OSP	8	greater than 0
1	destination	Src-GW-OSP	Proxy	8	greater than 0

### 3.4.5. Look Ahead Routing



Test Case 3.4.5: OSP H.323 Source to Proxy to OSP SIP Destination: Look Ahead Routing

Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green

#### Test Case Notes

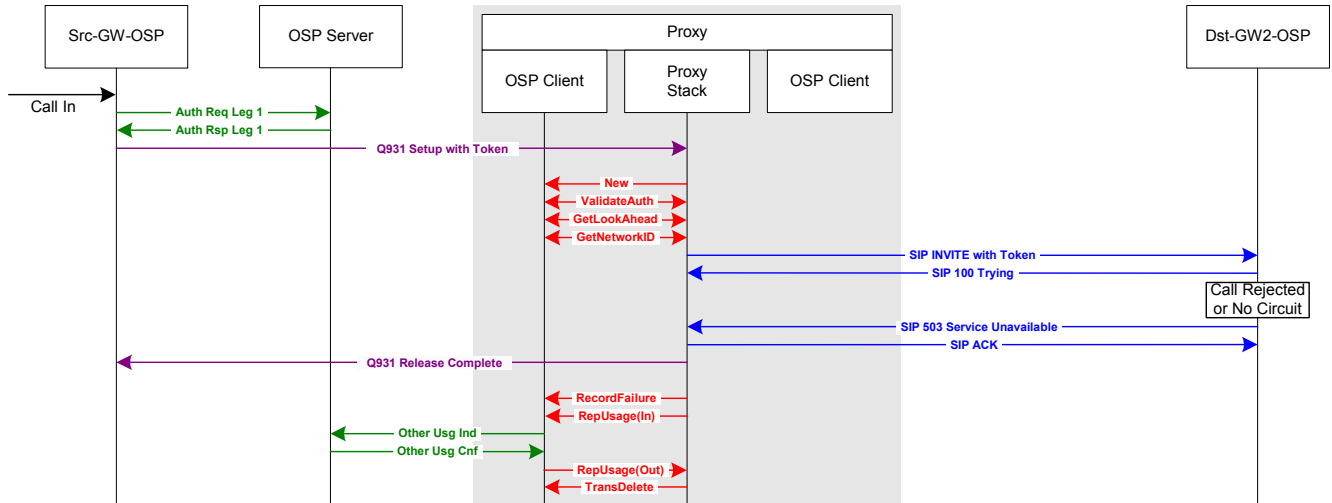
See test case 3.3.5.

#### Expected CDR for Test Case 3.4.5

This test case should generate one OSP UsageIndication message, or CDR, from the proxy. Look Ahead Routing is a unique case when one OSP Toolkit transaction validates inbound call leg 1 and routes outbound call leg 2. Since one CDR is used to report usage for both the destination of call leg 1 and the source of call leg 2, the role is defined as other. As with other call scenarios, the FailureReason should be determined by the release code included in the Q931 Release Complete from the source device, or by the SIP response from the destination device. If the call is successful and there is no release code reported, the proxy should report the FailureReason as 16 or 1016 to the OSP Toolkit ReportUsage function.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2-OSP	16 or 1016	greater than 0

### 3.4.6. Look Ahead Routing: Call Rejected or No Circuit



**Test Case 3.4.6: OSP H.323 Source to Proxy to OSP SIP Destination:  
Look Ahead Routing - Call Rejected or No Circuit & Retry**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

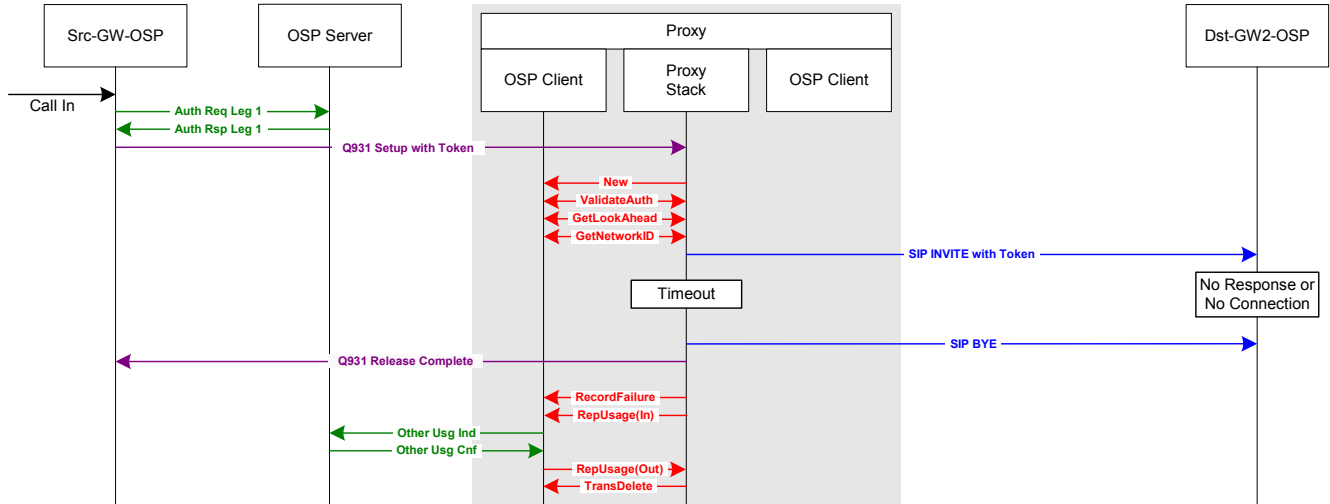
See test case 3.3.6.

#### Expected CDR for Test Case 3.4.6

This test case should generate one OSP UsageIndication message, or CDR, from the proxy. The role should be ‘other’ and the FailureReason should be determined by the SIP response from the destination device. In this example, the SIP response is 503, but other SIP responses are also valid.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2-OSP	503	0

### 3.4.7. Look Ahead Routing: No Response or No Connection - Proxy Times Out



**Test Case 3.4.7: OSP H.323 Source to Proxy to OSP SIP Destination:  
Look Ahead Routing - No Response or No Connection - Proxy Times Out**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

This case is very similar to test case 3.3.7 and tests a Look Ahead call scenario when the destination SIP device does not respond to the proxy. This test case must be executed four times to test the following four different call scenarios.

1. The proxy cannot establish a TCP connection with Dst-GW1-OSP. After a TCP time-out, the proxy should retry call to Dst-GW2-OSP. (When OSP Toolkit function RecordFailure is called, the FailureReason for the call attempt should be set to 47 – resource unavailable, unspecified.)
2. No route to IP address of Dst-GW1-OSP. The proxy should retry call to Dst-GW2-OSP. (When OSP Toolkit function RecordFailure is called, the FailureReason for the call attempt should be set to 2 – no route to specified transit network.)
3. TCP connection refused by Dst-GW1-OSP. After the TCP connection is refused, the proxy should retry the call to Dst-GW2-OSP. (When OSP Toolkit function RecordFailure is called, the FailureReason for the call attempt should be set to 63 – service or option not available, unspecified.)
4. No response from Dst-GW1-OSP. The proxy establishes TCP connection with Dst-GW1, but Dst-GW1-OSP never responds to SIP INVITE. The proxy should time-out and retry the call to Dst-GW2-OSP. (When OSP Toolkit function RecordFailure is called, the FailureReason for the call attempt should be set to 27 – destination out of order.)

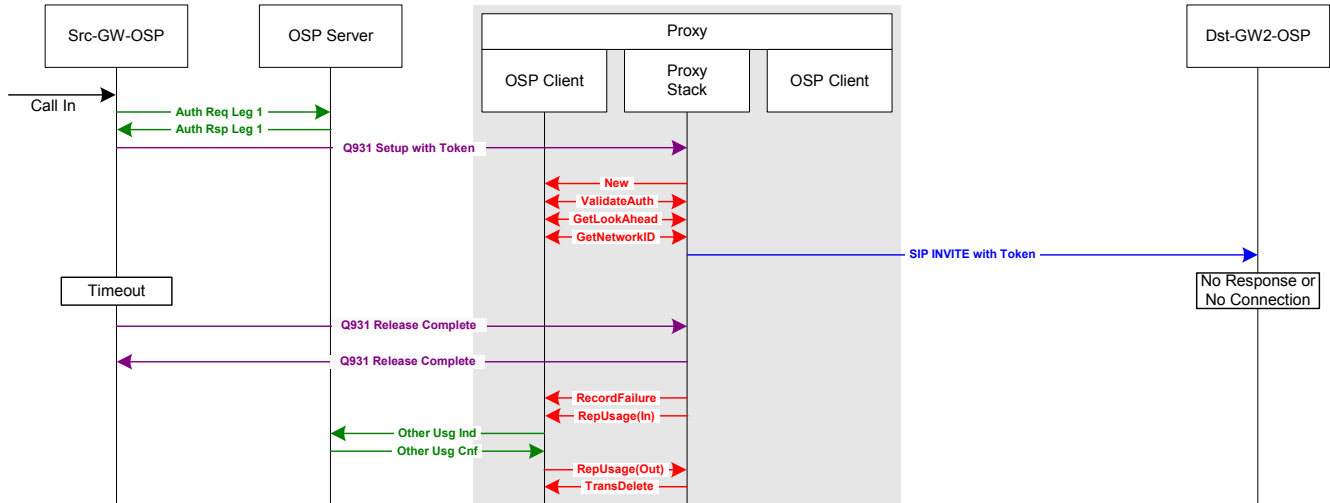
#### Expected CDR for Test Case 3.4.7

This test case should generate one OSP UsageIndication message, or CDR, from the proxy. The role should be ‘other’ and the FailureReason should be determined by the proxy based on the failure reasons described above.

## SIP/H.323 Interworking Proxy – OSP Peering Test Cases

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2-OSP	47, 2, 63 or 27	0

### 3.4.8. Look Ahead Routing: No Response or No Connection - Source Times Out



**Test Case 3.4.8: OSP H.323 Source to Proxy to OSP SIP Destination:  
Look Ahead Routing - No Response or No Connection - Source Times Out**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

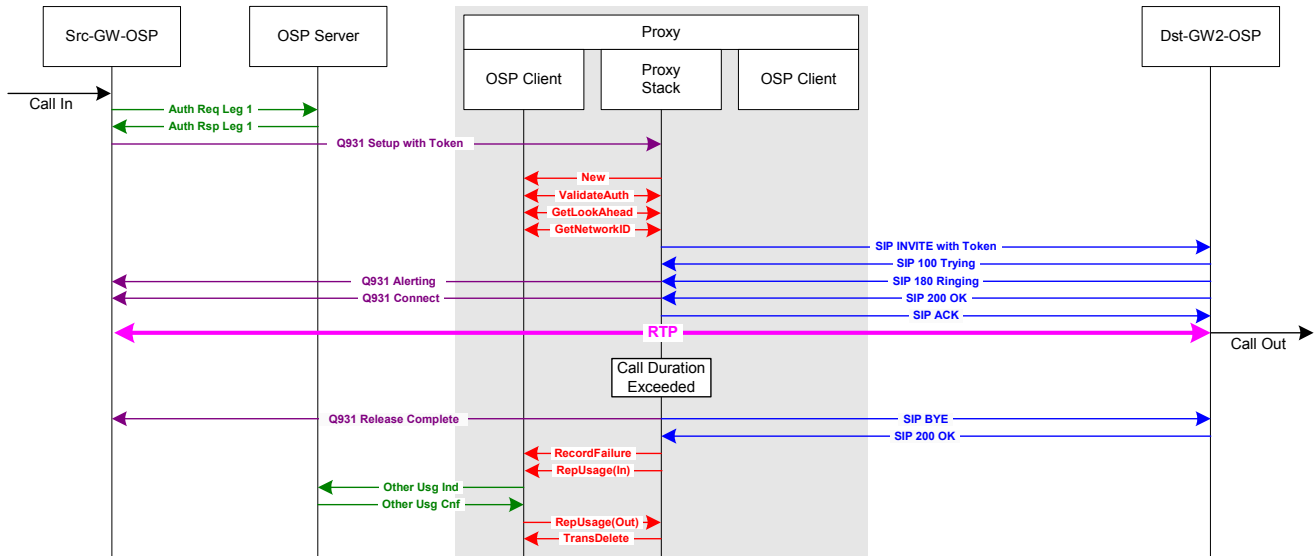
See test case 3.3.8.

#### Expected CDR for Test Case 3.4.8

This test case should generate one OSP UsageIndication message, or CDR, from the proxy. The role should be 'other' and the FailureReason should be determined by the release reason in the Q931 Release Complete message from Src-GW-OSP.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2-OSP	16 or 1016	0

### 3.4.9. Look Ahead Routing: Call Duration Limit Exceeded



**Test Case 3.4.9: OSP H.323 Source to Proxy to OSP SIP Destination:  
Look Ahead Routing - Call Duration Limit Exceeded**

**Legend: SIP Messages in Blue, H.323 Messages in Plum, OSP Toolkit Calls in Red, OSP Messages in Green**

#### Test Case Notes

If the call duration exceeds the authorized call duration set by ospvTimeLimit value returned from the OSPPTtransactionValidateAuthorisation function, the proxy should forcefully end the call. When the proxy forcefully ends the call because the call duration exceeded the authorized time limit, the FailureReason parameter reported in the RecordFailure function should be set to 8 (preemption).

#### Expected CDR for Test Case 3.4.9

This test case should generate one OSP UsageIndication message, or CDR, from the proxy. The role should be 'other' and the FailureReason should be 8 to indicate the call was forcefully shutdown by the proxy.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2-OSP	8	0