



**Inter-operability
Test Cases for a SIP
Back to Back User Agent
(B2BUA) and
the OSP Peering Protocol**

18 January 2007

1. Introduction.....	3
2. Test Cases.....	4
2.1 non-OSP Source to non-OSP Destination.....	4
2.1.1 Call Rejected or No Circuit and Retry	4
2.1.2 No Response or No Connection and Retry - B2BUA Times Out.....	12
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
2.2 non-OSP Source to OSP Destination.....	18
2.2.1 Call Rejected or No Circuit and Retry	19
2.2.2 No Response or No Connection and Retry - B2BUA 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
2.3 OSP Source and non-OSP Destination	25
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 - B2BUA 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.....	37
2.3.7 Look Ahead Routing: No Response or No Connection - B2BUA Times Out.....	38
2.3.8 Look Ahead Routing: No Response or No Connection - Source Times Out.....	39
2.3.9 Look Ahead Routing: Call Duration Limit Exceeded	40
2.3.10 Look Ahead Routing: Protocol Error.....	41
2.4 OSP Source to OSP Destination	42
2.4.0 Invalid Authorization Token.....	42
2.4.1 Call Rejected or No Circuit and Retry	43
2.4.2 No Response or No Connection and Retry - B2BUA Times Out.....	44
2.4.3 No Response or No Connection and Retry - Source Times Out.....	45
2.4.4 Call Duration Limit Exceeded	46
2.4.5 Look Ahead Routing	47
2.4.6 Look Ahead Routing: Call Rejected or No Circuit.....	48
2.4.7 Look Ahead Routing: No Response or No Connection - B2BUA Times Out.....	49
2.4.8 Look Ahead Routing: No Response or No Connection - Source Times Out.....	50
2.4.9 Look Ahead Routing: Call Duration Limit Exceeded	51

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 Back to Back User Agent (B2BUA). 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.

The test cases in this document are divided into sub-sections based on whether or not the source and destination devices support OSP. The focus of these test cases is on the B2BUA which is presented as gray box in the middle of each test case illustration. Note, these test cases assume the B2BUA 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 SIP peering. The OSP Toolkit is an open source OSP client implementation available from <https://sourceforge.net/projects/osp-toolkit>. Each test case presents SIP messages in blue. OSP messages are presented in green. Application Program Interface (API) calls between the B2BUA 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. Detailed information on the OSP Toolkit API function calls is provided in the OSP Toolkit Programming Interface document available on http://www.transnexus.com/OSP%20Toolkit/OSP%20Toolkit%20Documents/Programming_Interface%20V.3.3.1.pdf.

A basic requirement for these test cases is the ability of the B2BUA to enroll with the OSP server or certificate authority. The enrollment process is a two step process. First, the B2BUA requests the public key of the OSP server. Second, the B2BUA 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 B2BUA 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 B2BUA 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 http://www.transnexus.com/OSP%20Toolkit/OSP%20Toolkit%20Documents/Device_Enrollment.pdf.

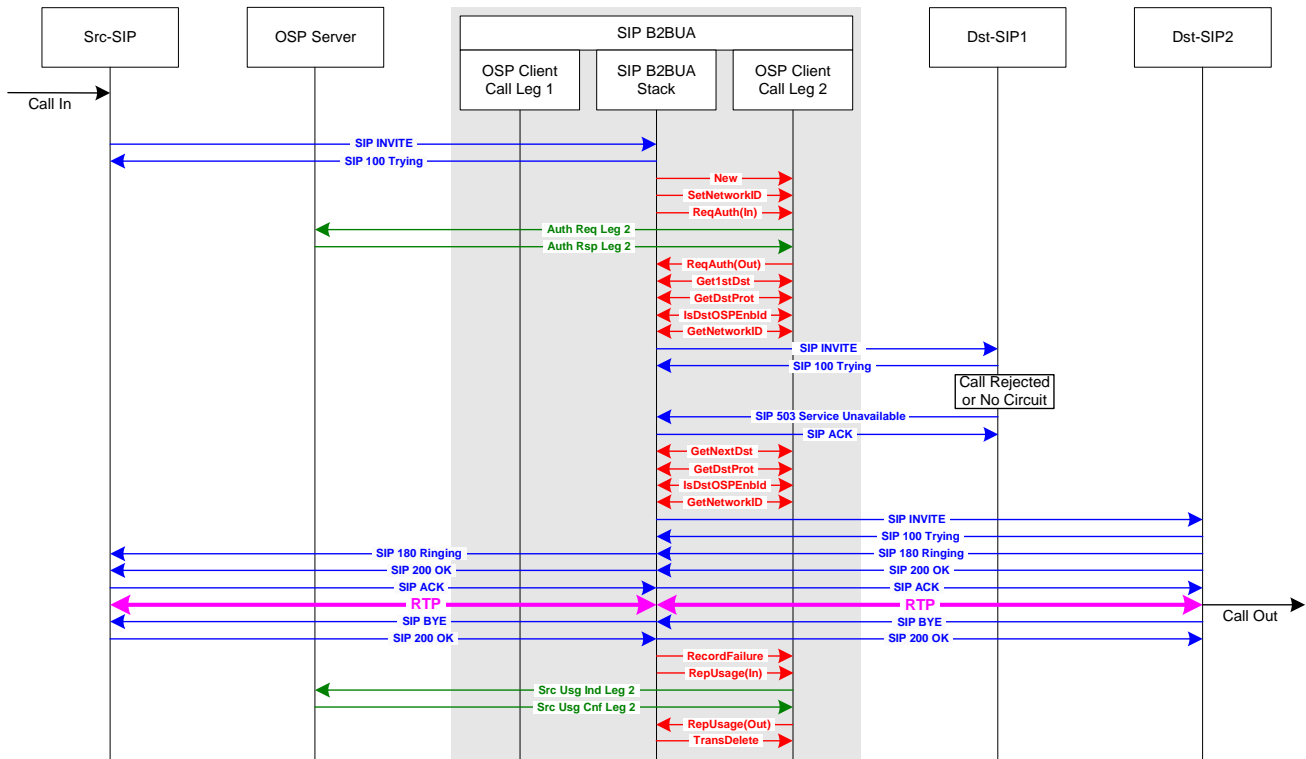
2. Test Cases

2.1 non-OSP Source to non-OSP Destination

This subsection defines test cases when both the source and destination SIP devices are not OSP enabled. In these test cases, the B2BUA sends an OSP AuthorizationRequest to an OSP server to determine routing and report call detail records. OSP interdomain 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-SIP	SIP	0.0.0 (Not OSP Enabled)
SIP B2BUA	SIP	2.1.1 or 4.1.1
Dst-SIP1	SIP	0.0.0 (Not OSP Enabled)
Dst-SIP2	SIP	0.0.0 (Not OSP Enabled)

2.1.1 Call Rejected or No Circuit and Retry



Test Case 2.1.1: non-OSP Source to SIP B2BUA to non-OSP Destination: Call Rejected or No Circuit & Retry
 Legend: SIP Messages in Blue, 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), 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 SIP B2BUA. These call scenarios for the B2BUA, have two call legs. One inbound call leg from the source

SIP B2BUA – OSP Peering Test Cases

SIP device to the B2BUA and a second outbound call leg from the B2BUA to the destination SIP device. Each of these call legs require a message transaction between the B2BUA and the OSP Toolkit. 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 B2BUA. 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 B2BUA.
3. **SIP 100 Trying.** The B2BUA receives the SIP INVITE and responds to the source SIP device.
4. **NEW.** The B2BUA does not have a route defined to complete the call to the dialed number. The B2BUA will query an OSP server for a route to an inter-domain destination to complete the call. The B2BUA establishes a new transaction with the OSP client Toolkit using OSPTransactionNew function. Please see the OSP Toolkit Programming Interface V3.3.1 document for details on this and other function calls.
5. **SetNetworkID.** The OSPTransactionSetNetworkIds function call identifies the trunk group or partition in the source device which originated the call. In this test case, where the B2BUA 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.
6. **ReqAuth(In).** The B2BUA calls the OSP client Toolkit function OSPTransactionRequestAuthorisation.
7. **Auth Req Leg 2.** The B2BUA 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 B2BUA. An OSP AuthorizationResponse includes a list of one or more destinations enabling the B2BUA 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.
9. **ReqAuth(Out).** The OSP Toolkit responds to the B2BUA that the OSPTransactionRequestAuthorisation function is complete.
10. **Get1stDst.** The B2BUA calls the OSP client Toolkit function OSPTransactionGetFirstDestination to get the IP address of the first destination gateway.

11. **GetDstProt.** The B2BUA 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 SIP (i.e. `H323_SETUP`, `H323_LRQ` or `IAX`), the B2BUA should reject the call and report a `FailureReason` of 111. If `DestinationProtocol` is unknown or undefined, the B2BUA should assume the destination protocol is SIP and complete the call.
12. **IsDstOSPEnabled.** The `OSPPTtransactionDestOSPEnabled` function tells the B2BUA 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 B2BUA should not include the OSP authorization token in the SIP INVITE to the destination device. (Note, to ensure backward compatibility with OSP V1.3.4, if `OSPE_OSP` is unknown or undefined, the B2BUA should assume the destination is OSP enabled and include the OSP authorization token in the SIP INVITE to the destination.)
13. **GetNetworkID.** The B2BUA calls the OSP client Toolkit function `OSPPTGetDestNetworkID` 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.
14. **SIP INVITE.** The B2BUA 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. The SIP INVITE should NOT include the source trunk group information from the source device.
15. **SIP 100 Trying.** The destination SIP device receives the INVITE and responds to the B2BUA.
16. **SIP 503 Service Unavailable.** The destination SIP device does not accept the call setup and returns a SIP 503 Service Unavailable to the B2BUA. This test case applies for any case when the destination SIP device rejects the INVITE. The call may be rejected for a variety of reasons such as unauthorized access or no circuits available.
17. **SIP ACK.** The B2BUA responds with a SIP ACK.
18. **GetNextDst.** The B2BUA 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 `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 503.
19. **GetDstProt.** The B2BUA gets the destination protocol of the second destination SIP device. In this test case the destination protocol is SIP. If `DestinationProtocol` is not SIP (i.e. `H323_SETUP`, `H323_LRQ` or `IAX`), the B2BUA should reject the call and report a `FailureReason` of 111. If `DestinationProtocol` is unknown or undefined, the B2BUA should assume the destination protocol is SIP and send a SIP INVITE to the destination.

20. **IsDstOSPEnabled.** The OSPPTTransactionDestOSPEnabled function tells the B2BUA 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 B2BUA should not include the OSP authorization token in the SIP INVITE to the destination device. (Note, to ensure backward compatibility with OSP V1.3.4, if OSPE_OSP is unknown or undefined, the B2BUA should assume the destination is OSP enabled and include the OSP authorization token in the SIP INVITE to the destination.)
21. **GetNetworkID.** The B2BUA 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.
- 22-29. Standard SIP communications for the completing the call.
30. **RecordFailure.** At the completion of the call, the B2BUA reports the call disconnect reason for the successful retry, to the OSP Toolkit using the OSPPTTransactionRecordFailure function.
31. **RepUsage(In).** The B2BUA calls the OSPPTTransactionReportUsage function to report the call duration.
32. **Src Usg Ind Leg 2.** The OSP client Toolkit sends an OSP UsageIndication message (Call Detail Record) to the OSP server. The UsageIndication is a type 'source' call detail record since the B2BUA is the source device for the second leg of the call.
33. **Src Usg Cnf Leg 2.** The OSP server responds with an OSP UsageConfirmation message.
34. **RepUsage(Out).** The OSP Toolkit closes the ReportUsage transaction.
35. **TransDelete.** The B2BUA 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 B2BUA 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-SIP1. In this example, the SIP response is 503, but other SIP responses are also valid. For the successful retry call, the B2BUA 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-SIP	Dst-SIP1	503	0
2	source	Src-SIP	Dst-SIP2	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)

SIP B2BUA – OSP Peering Test Cases

```
POST /osp HTTP/1.1
Host: IP Address of OSP server
content-type: text/plain
Content-Length: 467
Connection: Keep-Alive
```

```
<?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-SIP IP Address]</DeviceInfo>
    <SourceAlternate type="transport">[B2BUA IP address]</SourceAlternate>
    <SourceAlternate type="network">Partition</SourceAlternate>
    <DestinationInfo type="e164">Called Number</DestinationInfo>
    <Service/>
    <MaximumDestinations>Number of Destinations</MaximumDestinations>
  </AuthorizationRequest>
</Message>
```

OSP XML Tag	Toolkit Variable	Note
<CallId encoding="base64">	CallId	CallID from call leg 1 setup
<SourceInfo type="e164">	CallingNumber	
<DeviceInfo type="transport">	SourceDevice	Src-SIP IP Address
<SourceAlternate type="transport">	Source	B2BUA 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)

```
HTTP/1.1 200 OK
Server: Name of OSP server
Date: Thu, 12 May 2005 18:32:59 GMT
Connection: Keep-Alive
Keep-Alive: timeout=3600, max=5000
Content-Length: 1996
Content-Type: text/plain
```

```
<?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-SIP1 IP Address]</DestinationSignalAddress>
      <Token encoding='base64'>OSP Token</Token>
      <UsageDetail>
        <Amount>14400</Amount>
        <Increment>1</Increment>
```

SIP B2BUA – OSP Peering Test Cases

```

<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-SIP2 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'></SourceInfo>
<DestinationAlternate type='network' critical='False'></DestinationAlternate>
</Destination>
</AuthorizationResponse>
</Message>

```

OSP XML Tag	Toolkit Variable	Note
<TransactionId>		Transaction ID from OSP server
<CallId encoding="base64">	CallId	CallID from call leg 1 setup
<DestinationInfo type="e164">	CalledNumber	May be translated in AuthResponse
<DestinationSignalAddress>	Destination	Dst-SIP1 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-SIP1
<OSPVersion>	DestinationOSPStatus	Version of OSP supported by Dst-SIP1
<SourceInfo type='e164'>	CallingNumber	May be translated in AuthResponse
<DestinationAlternate type='network'>	DstNetworkID	Partition or trunk group of Dst-SIP1
<CallId encoding="base64">	CallId	CallID from call leg 1 setup
<DestinationInfo type="e164">	CalledNumber	May be translated in AuthResponse
<DestinationSignalAddress>	Destination	Dst-SIP2 IP Address
<Token encoding='base64'>	Token	Authorization token
<Amount>	TimeLimit	Authorized call duration in seconds
<Increment>		Default is 2

SIP B2BUA – OSP Peering Test Cases

OSP XML Tag	Toolkit Variable	Note
<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-SIP2
<OSPVersion>	DestinationOSPStatus	Version of OSP supported by Dst-SIP2
<SourceInfo type='e164'>	CallingNumber	May be translated in AuthResponse
<DestinationAlternate type='network'>	DstNetworkID	Partition or trunk group of Dst-SIP2

Source UsageIndication Leg 2 (generated by OSPPTtransactionReportUsage)

POST /osp HTTP/1.1

Host: IP address of OSP server

content-type: text/plain

Content-Length: 1844

Connection: Keep-Alive

```

<?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-SIP IP Address]</DeviceInfo>
<SourceAlternate type="transport">[B2BUA IP Address]</SourceAlternate>
<DestinationInfo type="e164">Called Number</DestinationInfo>
<DestinationAlternate type="transport">[Dst-SIP1 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-SIP IP Address]</DeviceInfo>
<SourceAlternate type="transport">[B2BUA IP Address]</SourceAlternate>
<DestinationInfo type="e164">Called Number</DestinationInfo>
<DestinationAlternate type="transport">[Dst-SIP2 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">

```

SIP B2BUA – OSP Peering Test Cases

```

<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 1 st try of call leg 2
<TransactionId>		Transaction ID from OSP server
<CallId encoding="base64">	CallId	CallID from call leg 1 setup
<SourceInfo type="e164">	CallingNumber	May be translated in AuthResponse
<DeviceInfo type="transport">	SourceDevice	Src-SIP IP Address
<SourceAlternate type="transport">	Source	B2BUA IP Address
<DestinationInfo type="e164">	CalledNumber	May be translated in AuthResponse
<DestinationAlternate>	Destination	Dst-SIP1 IP Address
<FailureReason>	FailureReason	Call Release Code
<Role>		Source CDR for 2 nd try of call leg 2
<TransactionId>		Transaction ID from OSP server
<CallId encoding="base64">	CallId	CallID from call leg 1 setup
<SourceInfo type="e164">	CallingNumber	May be translated in AuthResponse
<DeviceInfo type="transport">	SourceDevice	Src-SIP IP Address
<SourceAlternate type="transport">	Source	B2BUA IP Address
<DestinationInfo type="e164">	CalledNumber	May be translated in AuthResponse
<DestinationAlternate>	Destination	Dst-SIP2 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 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)

```

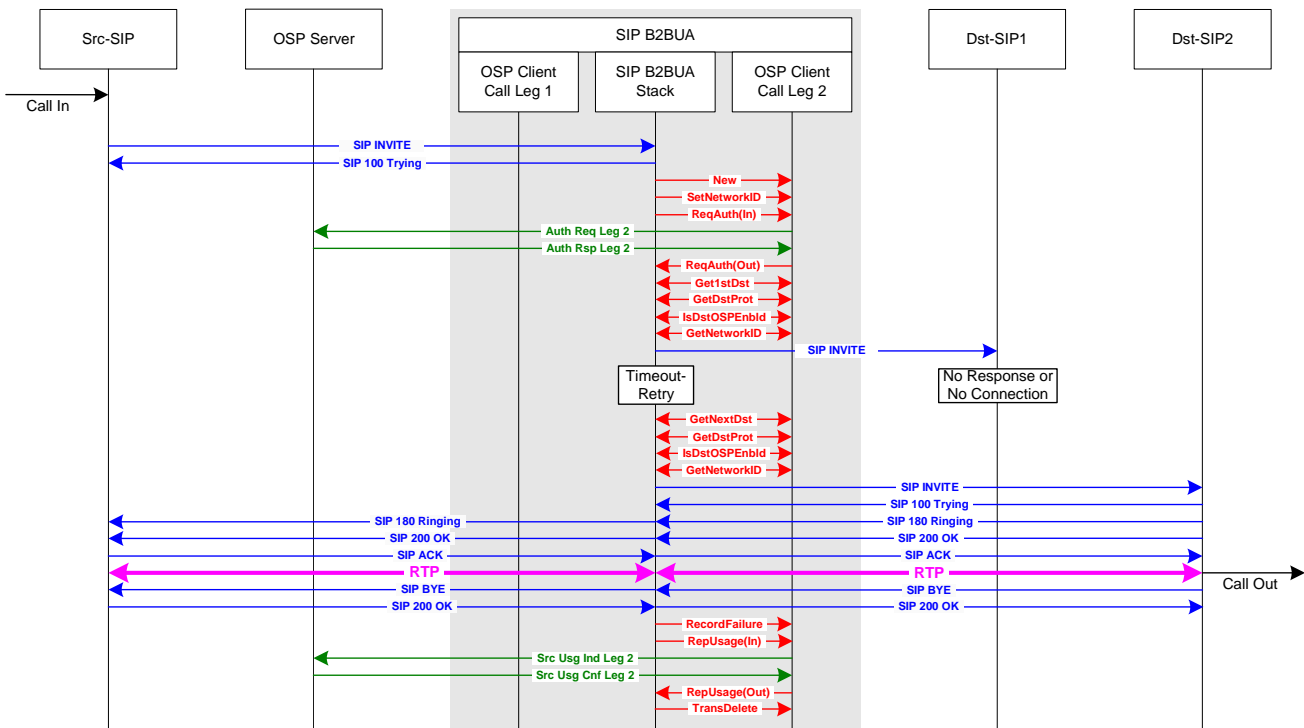
HTTP/1.1 200 OK
Server: Name of OSP server
Date: Thu, 12 May 2005 18:33:34 GMT
Connection: Keep-Alive
Keep-Alive: timeout=3600, max=5000
Content-Length: 456
Content-Type: text/plain

```

SIP B2BUA – OSP Peering Test Cases

```
<?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>
```

2.1.2 No Response or No Connection and Retry - B2BUA Times Out



Test Case 2.1.2: non-OSP Source to SIP B2BUA to non-OSP Destination
No Response or No Connection & Retry - SIP B2BUA Times Out
Legend: SIP Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

This case tests the call scenario when a destination SIP device does not respond to the B2BUA. This test case requires that the OSP server return two or more destinations in the AuthorizationResponse to the B2BUA. After the first call attempt fails, the B2BUA must retry the call to second destination. This test case must be executed four times to test the following four different call scenarios.

SIP B2BUA – OSP Peering Test Cases

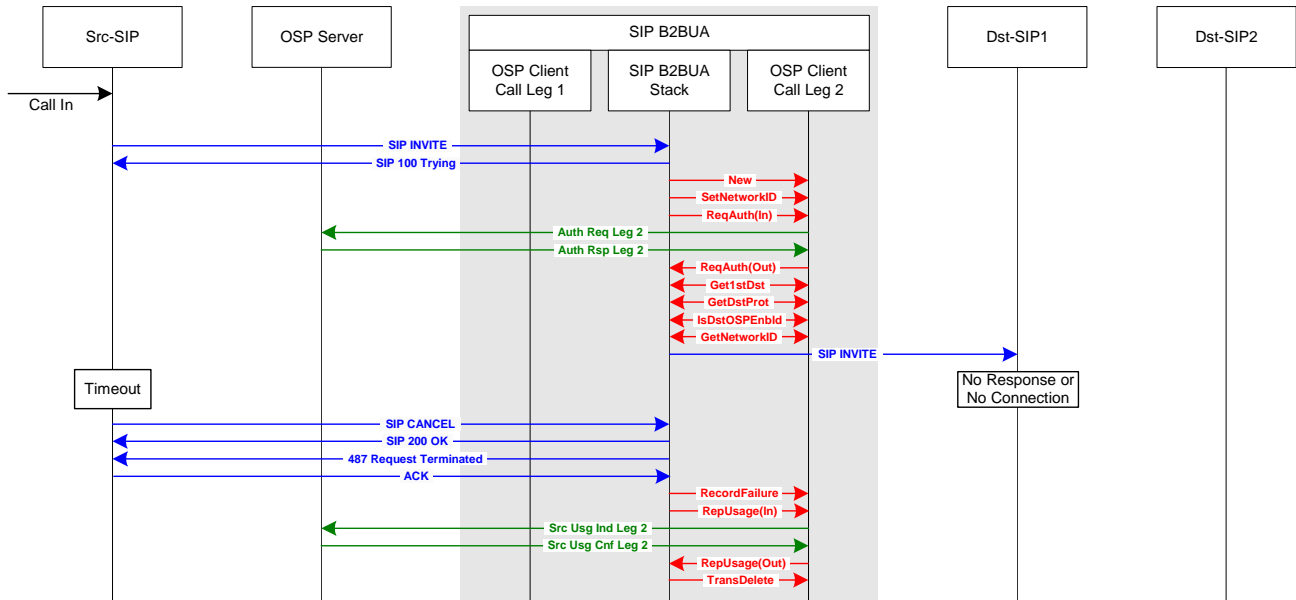
1. The B2BUA cannot establish a TCP connection with Dst-SIP1. After TCP time-out, the B2BUA should retry call to Dst-SIP2. (When OSP Toolkit function OSPPTtransactionGetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 47 – resource unavailable, unspecified.)
2. No route to IP address of Dst-SIP1 device. The B2BUA should retry call to Dst-SIP2. (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-SIP1. After TCP connection is refused, the B2BUA should retry the call to Dst-SIP2. (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-SIP1. The B2BUA establishes TCP connection with Dst-SIP1, but DST-SIP1 never responds to SIP INVITE. The B2BUA should time-out and retry the call to Dst-SIP2. (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 2.1.2

This test case should generate two OSP UsageIndication messages, or CDRs, from the B2BUA 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 B2BUA based on the reason for the failure. For the successful retry call, the B2BUA 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-SIP	Dst-SIP1	47, 2, 63 or 27	0
2	source	Src-SIP	Dst-SIP2	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 Source to SIP B2BUA to non-OSP Destination
No Response or No Connection & Retry - Source Times Out**
Legend: SIP Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

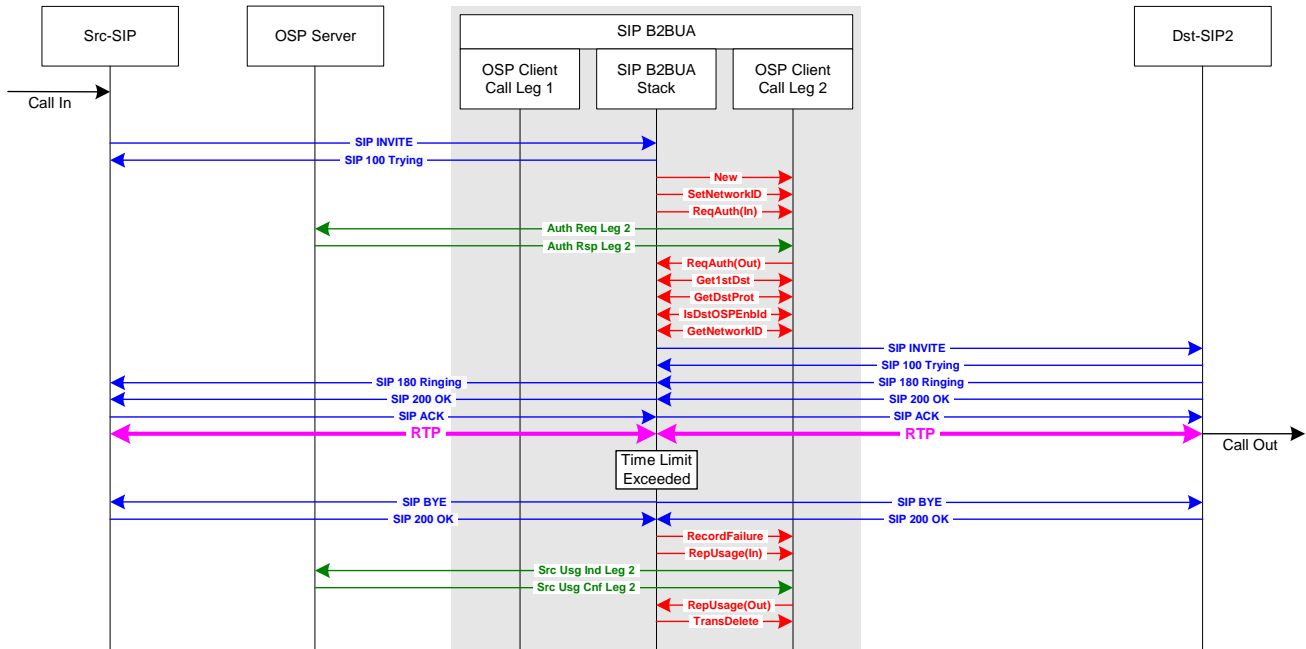
This case tests the call scenario when the source ends the call before the first destination Dst-SIP1 responds to the SIP INVITE from the B2BUA. In these cases, the B2BUA should terminate the call and report usage to the OSP server. The OSP Toolkit parameter FailureReason reported with the OSPTransactionRecordFailure function should be set to the release cause reported in the CANCEL message from the source device, Src-SIP. If no release reason is reported in the CANCEL message, the B2BUA should set the FailureReason to 487.

Expected CDRs for Test Case 2.1.3

This test case should generate one OSP UsageIndication message, or CDR, from the B2BUA 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 SIP CANCEL message from Src-SIP. If no release reason is included in the SIP CANCEL message, the B2BUA 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-SIP	Dst-SIP1	487	0

2.1.4 Call Duration Limit Exceeded



Test Case 2.1.4: non-OSP Source to SIP B2BUA to non-OSP Destination: Time Limit Exceeded
Legend: SIP Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

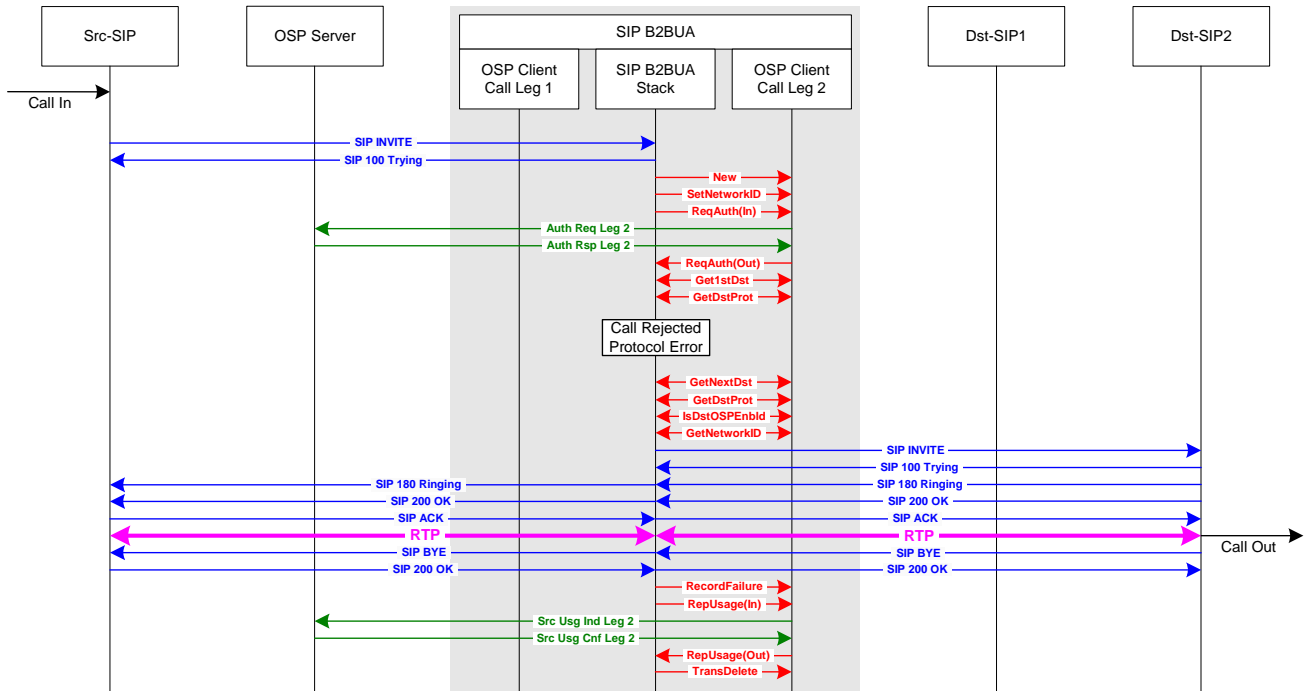
This call scenario tests the B2BUA’s ability to end a call when its authorized call duration has been exceeded. In the AuthorizationResponse, the OSP server includes the authorized call duration. The OSP Toolkit parameter TimeLimit, returned in the GetFirstDestination or GetNextDestination function calls, defines the maximum duration for each call. The B2BUA should terminate a call when the call duration exceeds the TimeLimit. In this case, when the B2BUA forcefully ends a call that has exceeded its maximum call duration, the B2BUA 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 B2BUA as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the call should be set by the B2BUA to 8 to indicate the call was forcefully shutdown by the B2BUA.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-SIP	Dst-SIP2	8	greater than 0

2.1.5 Call Rejected – Protocol Error and Retry



Test Case 2.1.5: non-OSP Source to SIP B2BUA to non-OSP Destination: Protocol Error & Retry
Legend: SIP Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

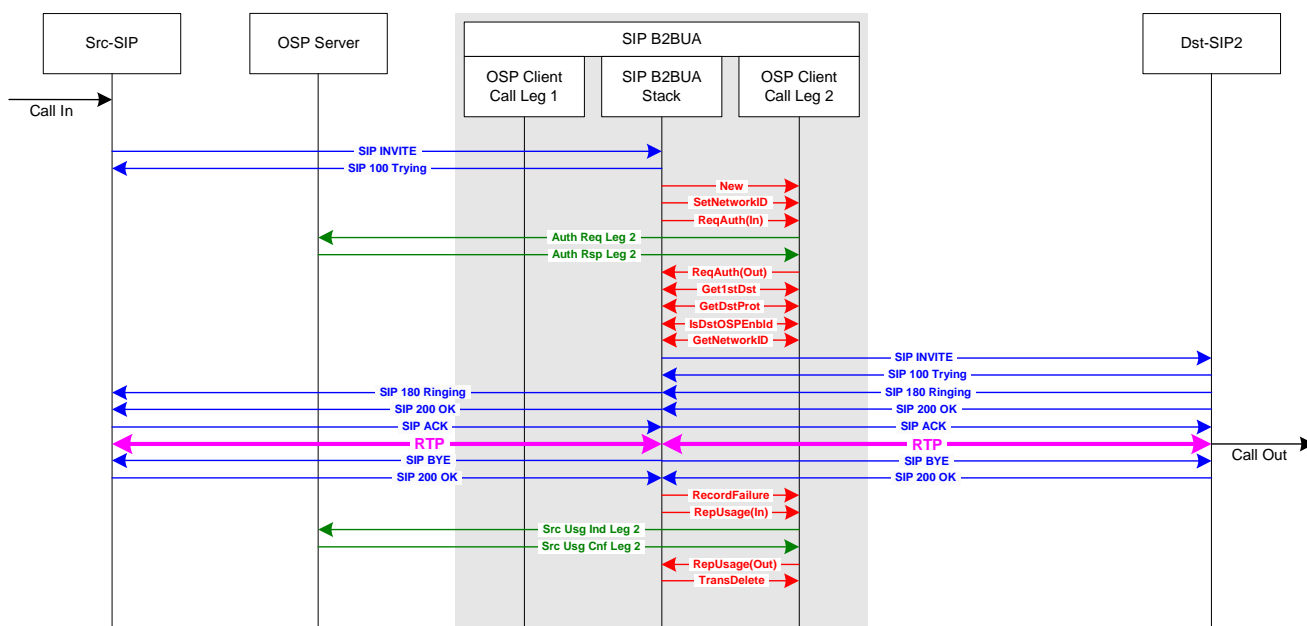
This case tests the error condition when the OSP server returns a DestinationProtocol that is not supported by the SIP B2BUA, such as H323_SETUP, H323_LRQ or IAX. When this occurs, the B2BUA should reject the destination, record FailureReason 111 (protocol error) and retry the call to the next destination if it is available.

Note: For this test case, the destination protocol for device Dst-SIP1 is NOT configured as SIP on the OSP server. The OSPTransactionGetDestProtocol function call returns a DestinationProtocol incompatible with SIP. The B2BUA should recognize the protocol error and reject the call attempt. Note, if the DestinationProtocol is unknown or undefined, the B2BUA should assume the destination device supports SIP and should send an INVITE to the destination device.

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-SIP	Dst-SIP1	111	0
2	source	Src-SIP	Dst-SIP2	16 or 1016	greater than 0

2.1.6 Number Translation



Test Case 2.1.6: non-OSP Source to SIP B2BUA to non-OSP Destination: Number Translation
 Legend: SIP Messages in Blue, 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 B2BUA. When this occurs, the called and calling numbers in the SIP INVITE from the B2BUA 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 B2BUA 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 2.1.6

This test case should generate one OSP UsageIndication message, or CDR, from the B2BUA as the source of call leg 2. The called and calling numbers reported in the OSP UsageIndication message from the B2BUA, 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.

Call Leg	Role	Source IP Address	Destination IP Address	Calling Number	Called Number	Release Reason or TC Code	Call Duration
2	source	Src-SIP	Dst-SIP2	Not Translated	Not Translated	16 or 1016	greater than 0

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

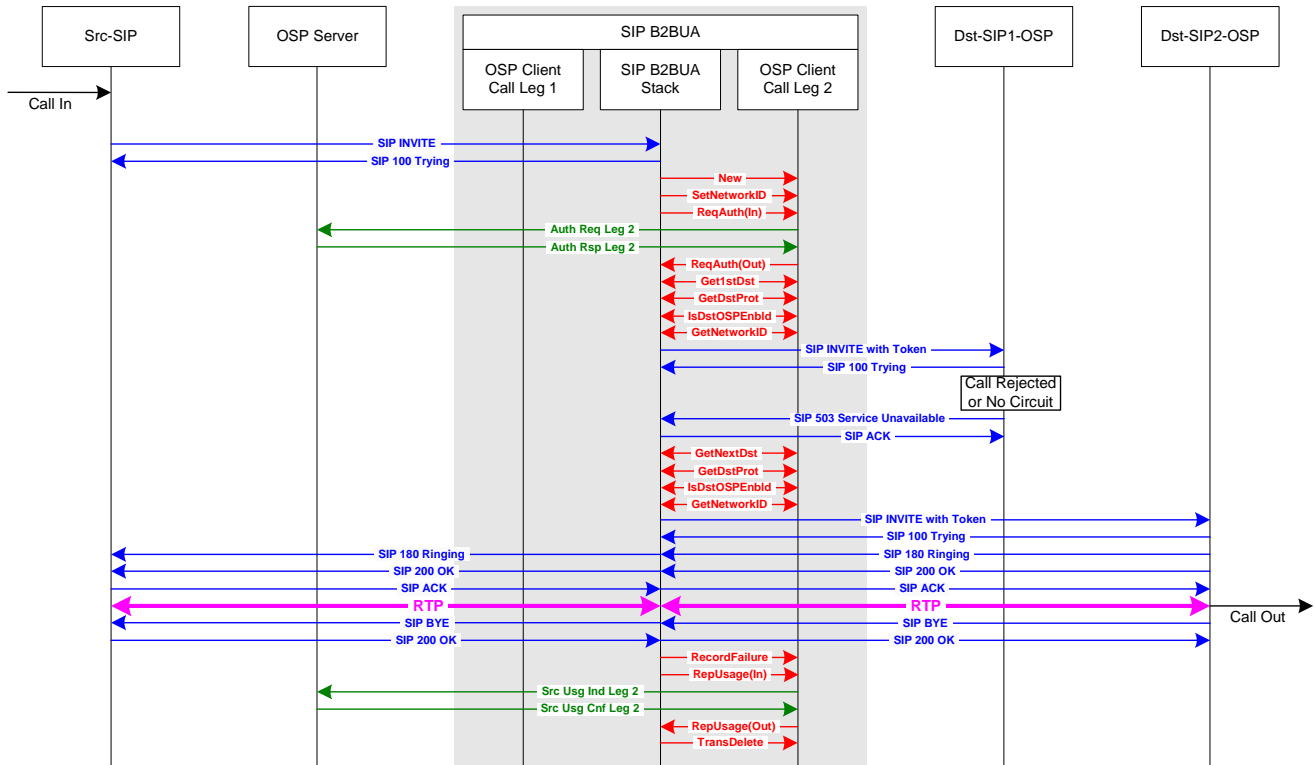
2.2 *non-OSP Source to OSP Destination*

This subsection of cases tests call scenarios when the destination is an OSP enabled SIP device. In these call scenarios, the B2BUA must include the OSP 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 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 B2BUA 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-SIP	SIP	0.0.0 (Not OSP Enabled)
SIP B2BUA	SIP	2.1.1 or 4.1.1
Dst-SIP1-OSP	SIP	1.3.4, 2.1.1 or 4.1.1
Dst-SIP2-OSP	SIP	1.3.4, 2.1.1 or 4.1.1

2.2.1 Call Rejected or No Circuit and Retry



Test Case 2.2.1: non-OSP Source to SIP B2BUA to OSP Destination: Call Rejected or No Circuit & Retry
 Legend: SIP Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

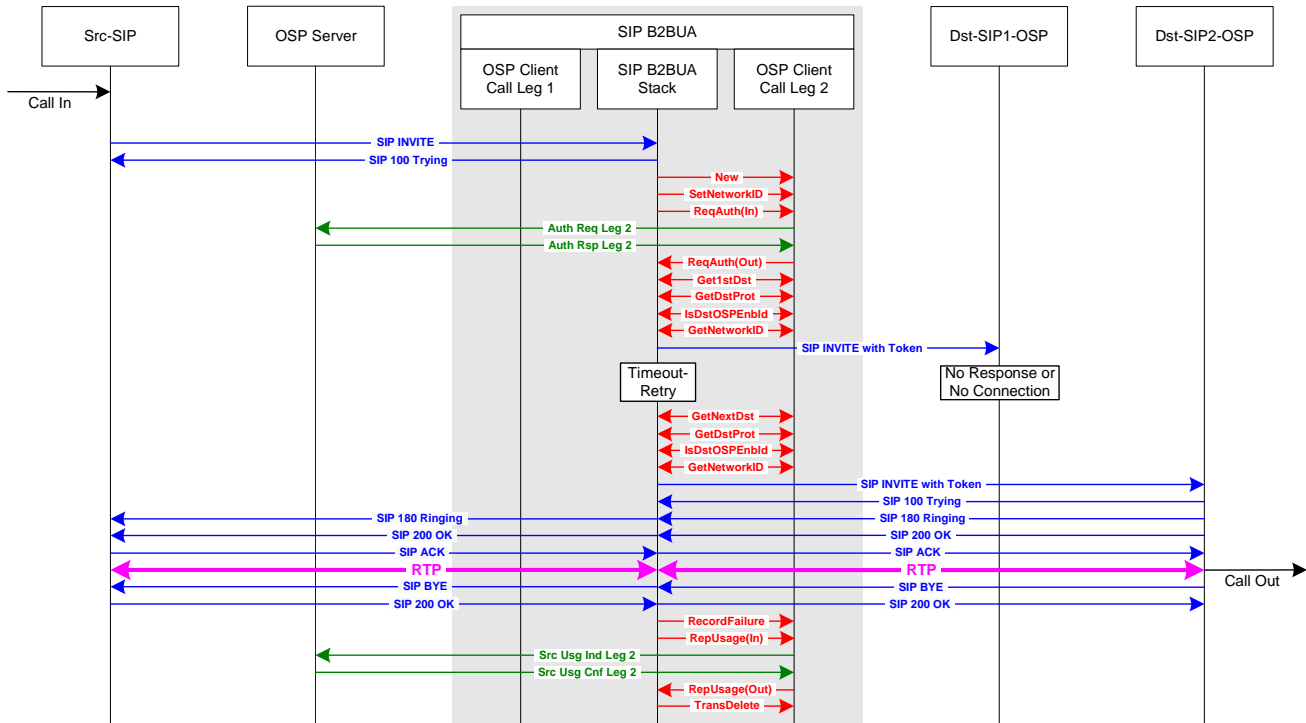
This test case identical to test case 2.1.1 except that the OSP token returned in OSPTransactionRequestAuthorization function should be included in the header of the SIP INVITE message to the destination.

Expected CDRs for Test Case 2.2.1

This test case should generate two OSP UsageIndication messages, or CDRs, from the B2BUA 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-SIP1-OSP. In this example, the SIP response is 503, but other SIP responses are also valid. For the successful retry call, the B2BUA 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-SIP	Dst-SIP1	503	0
2	source	Src-SIP	Dst-SIP2	16 or 1016	greater than 0

2.2.2 No Response or No Connection and Retry - B2BUA Times Out



**Test Case 2.2.2: non-OSP Source to SIP B2BUA to OSP Destination
No Response or No Connection & Retry - SIP B2BUA Times Out**
Legend: SIP Messages in Blue, 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 token returned in OSPTransactionRequestAuthorization 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 B2BUA. This test case requires that the OSP server return two or more destinations in the AuthorizationResponse to the B2BUA. After the first call attempt fails, the B2BUA 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 B2BUA cannot establish a TCP connection with Dst-SIP1-OSP. After TCP time-out, the B2BUA should retry call to Dst-SIP2-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-SIP1-OSP device. the B2BUA should retry call to Dst-SIP2-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 B2BUA should retry the call to Dst-SIP2-OSP. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the

SIP B2BUA – OSP Peering Test Cases

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

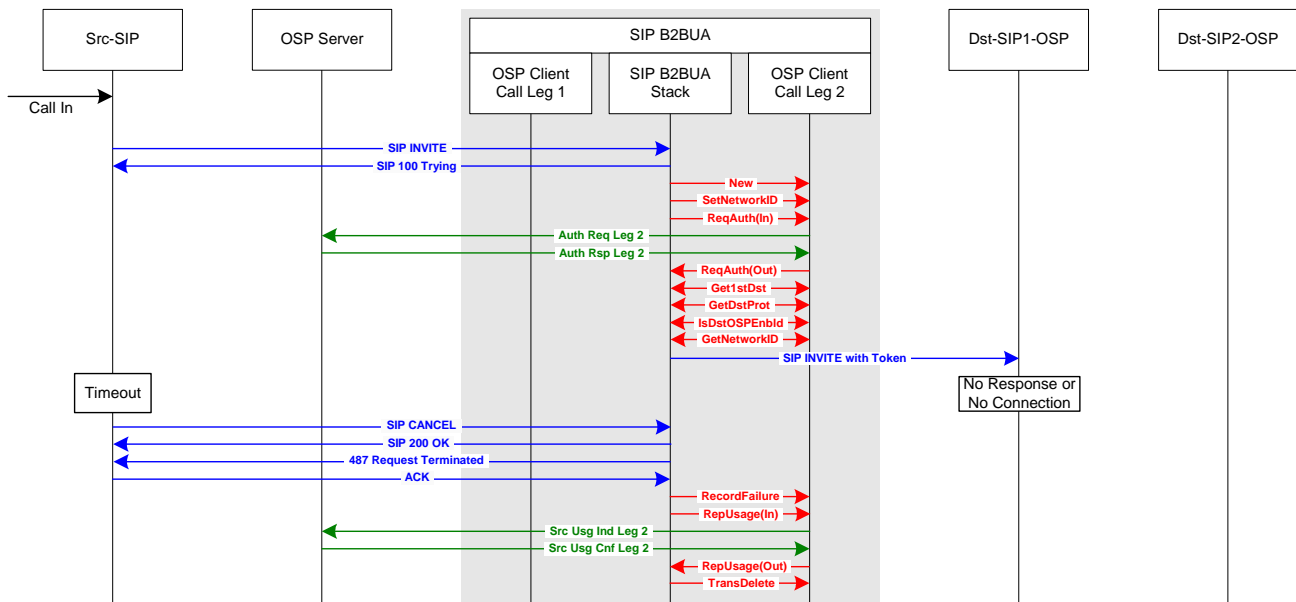
- No response from Dst-SIP1-OSP device. the B2BUA establishes TCP connection with Dst-SIP1-OSP, but DST-SIP1-OSP never responds to SIP INVITE. The B2BUA should time-out and retry the call to Dst-SIP2-OSP. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, 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 B2BUA 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 B2BUA based on the reason for the failure. For the successful retry of call leg 2, the B2BUA 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-SIP	Dst-SIP1-OSP	47, 2, 63 or 27	0
2	source	Src-SIP	Dst-SIP2-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 Source to SIP B2BUA to OSP Destination
No Response or No Connection & Retry - Source Times Out

Legend: SIP Messages in Blue, 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 token returned in OSPTransactionRequestAuthorization function should be included in the header of the SIP INVITE message to the destination.

SIP B2BUA – OSP Peering Test Cases

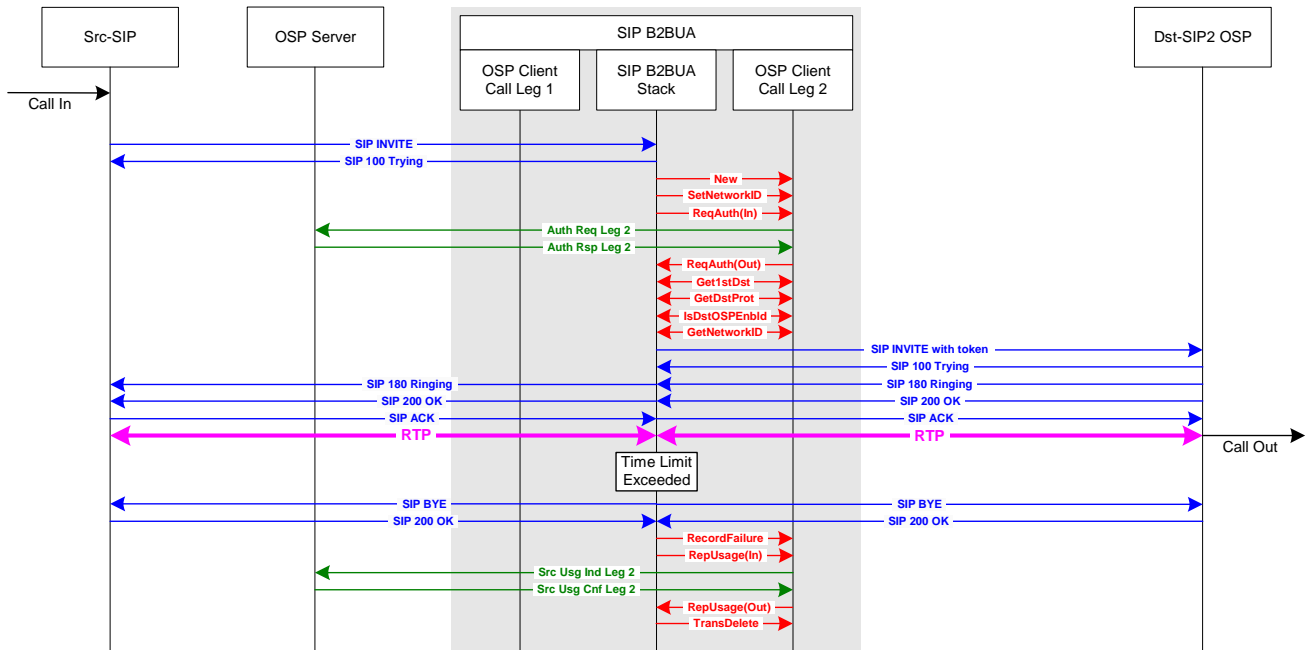
This case tests the call scenario when the source ends the call before the first destination Dst-SIP1-OSP responds to the SIP INVITE from the B2BUA. In these cases, the B2BUA should terminate the call and report usage to the OSP server. The OSP Toolkit parameter FailureReason reported with the OSPTransactionRecordFailure function should be set to the release cause reported in the CANCEL message from the source device, Src-SIP. If no release reason is reported in the CANCEL message, the B2BUA 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 B2BUA 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-SIP. If no release reason is included in the SIP CANCEL message, the B2BUA 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-SIP	Dst-SIP1-OSP	487	0

2.2.4 Call Duration Limit Exceeded



Test Case 2.2.4: non-OSP Source to SIP B2BUA to OSP Destination: Time Limit Exceeded
Legend: SIP Messages in Blue, 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 token returned in OSPTransactionRequestAuthorization function should be included in the header of the SIP INVITE message to the destination.

This call scenario tests the B2BUA's ability to end a call when its authorized call duration has been exceeded. In the AuthorizationResponse, the OSP server includes the

SIP B2BUA – OSP Peering Test Cases

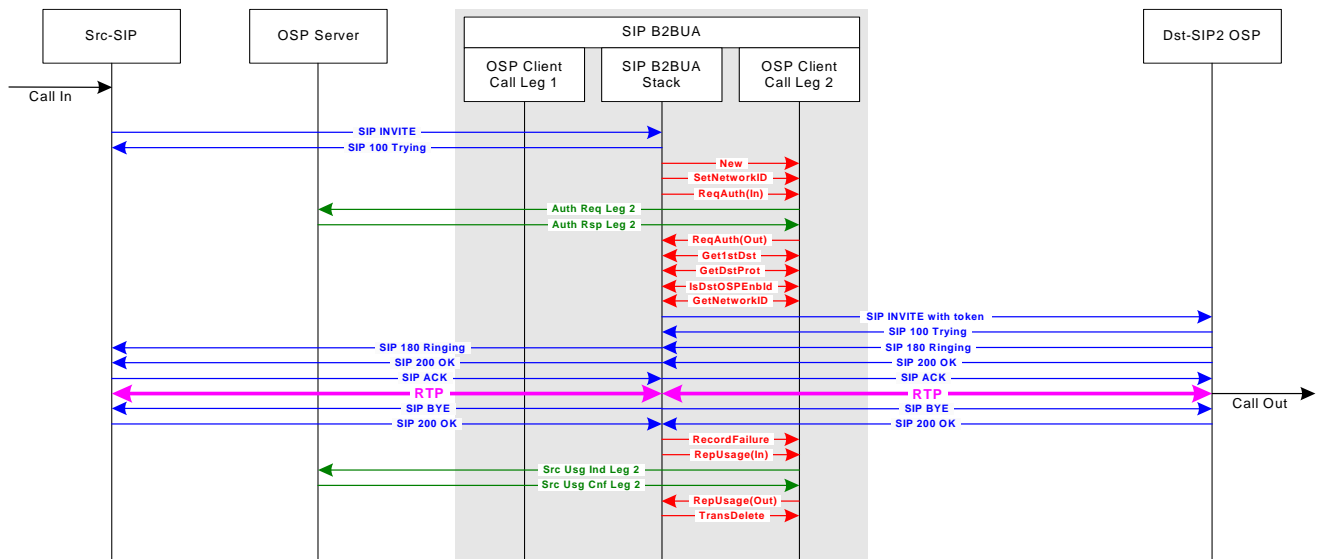
authorized call duration. The OSP Toolkit parameter `ospvTimeLimit`, returned in the `GetFirstDestination` or `GetNextDestination` function calls, defines the maximum duration for each call. The B2BUA should terminate a call when the call duration exceeds the `TimeLimit`. In this case, when the B2BUA forcefully ends a call that has exceeded its maximum call duration, the B2BUA 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 2.2.4

This test case should generate one OSP `UsageIndication` message, or CDR, from the B2BUA as the source of call leg 2. The release reason (`ospvFailureReason`), or termination cause code, for the call should be set by the B2BUA to 8 to indicate the call was forcefully shutdown by the B2BUA.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-SIP	Dst-SIP2-OSP	8	greater than 0

2.2.5 Number Translation



Test Case 2.2.5: non-OSP Source to SIP B2BUA to OSP Destination: Number Translation
Legend: SIP Messages in Blue, 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 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 B2BUA. When this occurs, the called and calling numbers in the SIP INVITE from the B2BUA to the destination gateway should be the translated called and calling numbers from the OSP `AuthorizationResponse`.

SIP B2BUA – OSP Peering Test Cases

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 OSPTransactionReportUsage function should report the un-translated called and calling numbers.

Expected CDRs for Test Case 2.2.5

This test case should generate one OSP UsageIndication message, or CDR, from the B2BUA as the source of call leg 2. The called and calling numbers reported in the OSP UsageIndication message from the B2BUA, 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.

Call Leg	Role	Source IP Address	Destination IP Address	Calling Number	Called Number	Release Reason or TC Code	Call Duration
2	source	Src-SIP	Dst-SIP2	Not Translated	Not Translated	16 or 1016	greater than 0

Note: OSP Toolkit version 3.3.3 and before report translated numbers in the CDR.

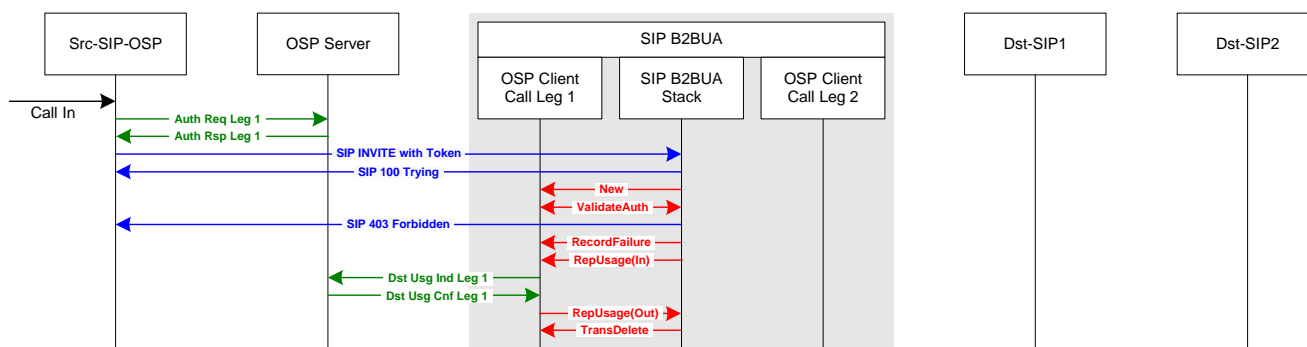
Version 3.3.4 reports translated calling number and not translated called number.

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 SIP device is not OSP enabled. In these test cases, the B2BUA will receive a SIP INVITE message which includes an OSP token. The B2BUA must validate the digitally signed token to determine whether or not to accept the call. On the second call leg, the B2BUA must not include an OSP 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 2.3		
Device	Destination Protocol	OSP Version
Src-SIP-OSP	SIP	1.3.4, 2.1.1 or 4.1.1
SIP B2BUA	SIP	2.1.1 or 4.1.1
Dst-SIP 1	SIP	0.0.0 (Not OSP enabled)
Dst-SIP 2	SIP	0.0.0 (Not OSP enabled)

2.3.0 Invalid Authorization Token



Test Case 2.3.0: OSP Source to SIP B2BUA to non-OSP Destination: Invalid Authorization Token

Legend: SIP Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

In this test case, the token included in the SIP INVITE message cannot be validated by the B2BUA. 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 B2BUA 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).

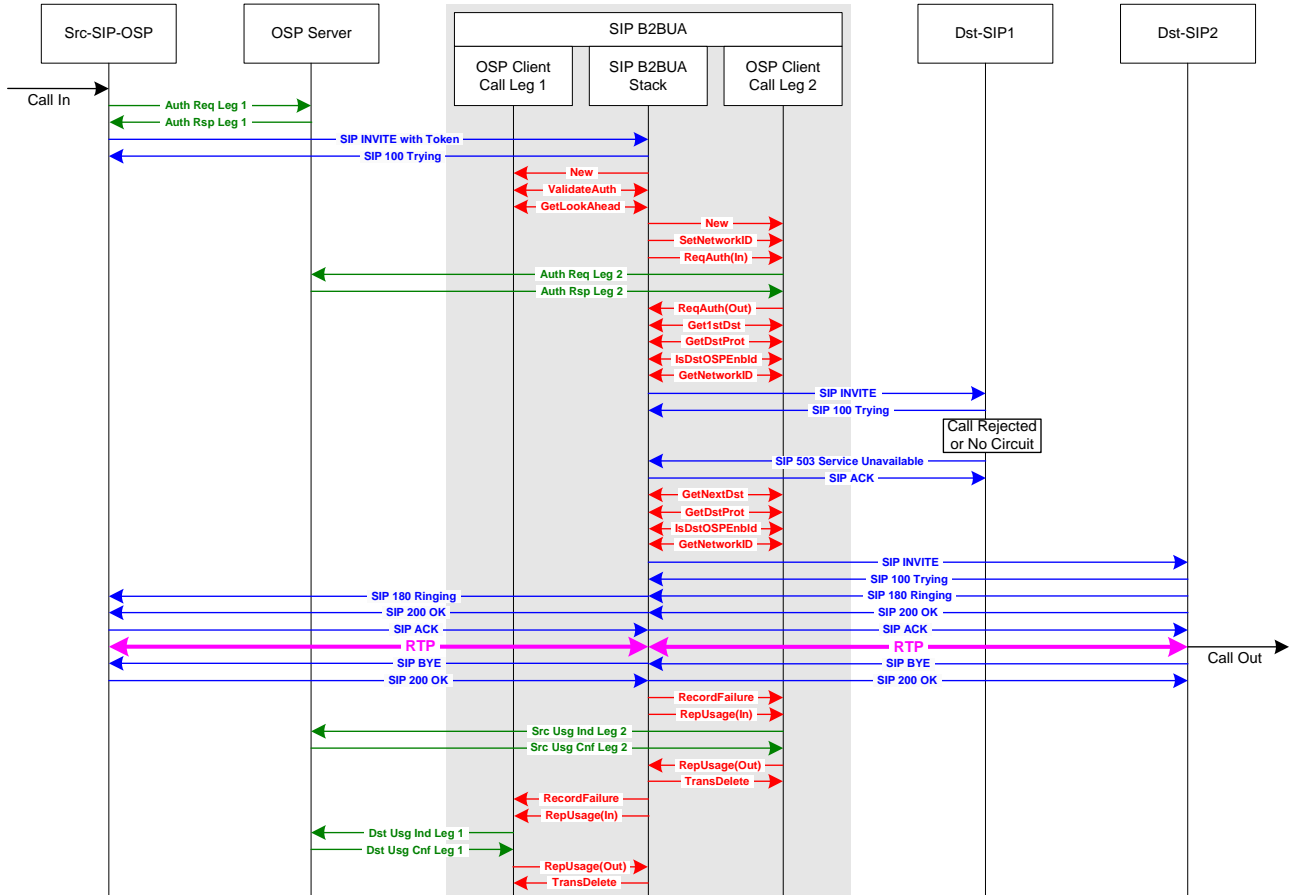
The B2BUA responds to the source that the call is forbidden and then performs the OSP Toolkit function calls OSPPTtransactionRecordFailure and OSPPTtransactionReportUsage to create an OSP destination UsageIndication Call Detail Record which is sent to the OSP server. The FailureReason for this call should be 403.

Expected CDR for Test Case 2.3.0

This test case should generate one OSP UsageIndication message, or CDR, from the B2BUA as the destination of call leg 1. The release reason (ospvFailureReason), or termination cause code, for the call should be set by the B2BUA 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-SIP-OSP	B2BUA	403	0

2.3.1 Call Rejected or No Circuit and Retry



Test Case 2.3.1: OSP Source to SIP B2BUA to non-OSP Destination: Call Rejected or No Circuit & Retry
Legend: SIP Messages in Blue, 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 B2BUA, 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 B2BUA. The SIP INVITE message header includes an OSP authorization token.
5. **SIP 100 Trying.** The B2BUA receives the SIP INVITE message and responds.

6. **NEW.** The B2BUA recognizes the presence of an OSP authorization token in the SIP INVITE message call setup and establishes a transaction with the OSP Toolkit to validate the token.
7. **ValidateAuth.** The B2BUA 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 B2BUA. In this call scenario, the token is valid and the call processing continues. If the token was not valid, the B2BUA 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. If the call duration exceeds the authorized time limit, the B2BUA should end the call (test case 2.3.4).
8. **GetLookAhead.** The B2BUA 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 B2BUA 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 B2BUA does not have a route defined to complete the call to the dialed number. The B2BUA will query an OSP server for a route to an inter-domain destination to complete the call. The B2BUA establishes a new transaction with the OSP client Toolkit 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 B2BUA 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 B2BUA calls the OSP client Toolkit function `OSPPTtransactionRequestAuthorisation`.
12. **Auth Req Leg 2.** The B2BUA 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 B2BUA. 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.
14. **ReqAuth(Out).** The OSP Toolkit responds to the B2BUA that the `OSPPTtransactionRequestAuthorisation` function is complete.

SIP B2BUA – OSP Peering Test Cases

15. **Get1stDst.** The B2BUA calls the OSP client Toolkit function `OSPPTtransactionGetFirstDestination` to get the IP address of the first destination gateway.
16. **GetDstProt.** The B2BUA 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 SIP (i.e. H323_SETUP, H323_LRQ or IAX), the B2BUA should reject the call and report a `FailureReason` of 111 (test case 2.1.5). If `DestinationProtocol` is unknown or undefined, the B2BUA should assume the destination protocol is SIP and complete the call.
17. **IsDstOSPEnabled.** The `OSPPTtransactionDestOSPEnabled` function tells the B2BUA 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 B2BUA should not include the OSP authorization token in the SIP INVITE to the destination device. (Note, to ensure backward compatibility with OSP V1.3.4, if `OSPE_OSP` is unknown or undefined, the B2BUA should assume the destination is OSP enabled and include the OSP authorization token in the SIP INVITE to the destination.)
18. **GetNetworkID.** The B2BUA 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.
19. **SIP INVITE.** The B2BUA 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 SIP INVITE from the source device, it should NOT be included in the SIP INVITE to the destination.
20. **SIP 100 Trying.** The destination SIP device receives the INVITE and responds to the B2BUA.
21. **SIP 503 Service Unavailable.** The destination SIP device does not accept the call setup and returns a SIP 503 Service Unavailable to the B2BUA. This test case applies for any case when the destination SIP device rejects the INVITE. The call may be rejected for a variety of reasons such as unauthorized access or no circuits available.
22. **SIP ACK.** The B2BUA responds with a SIP ACK.
23. **GetNextDst.** The B2BUA 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.
24. **GetDstProt.** The B2BUA 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 SIP (i.e. H323_SETUP, H323_LRQ or IAX), the B2BUA should reject the call and report a FailureReason of 111 (test case 2.1.5). If DestinationProtocol is unknown or undefined, the B2BUA should assume the destination protocol is SIP and complete the call.

25. **IsDstOSPEnabled.** The OSPPTxactionDestOSPEnabled function tells the B2BUA 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 B2BUA should not include the OSP authorization token in the SIP INVITE to the destination device. (Note, to ensure backward compatibility with OSP V1.3.4, if OSPE_OSP is unknown or undefined, the B2BUA should assume the destination is OSP enabled and include the OSP authorization token in the SIP INVITE to the destination.)
 26. **GetNetworkID.** The B2BUA calls the OSP client 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 SIP INVITE to the destination.
- 27-33. Standard SIP communications for the completing the call.
18. **RecordFailure.** At the completion of the call, the B2BUA reports the call disconnect reason for the successful retry of the second call leg, to the OSP Toolkit using the OSPPTxactionRecordFailure function.
 19. **RepUsage(In).** The B2BUA calls the OSPPTxactionReportUsage function to report the call duration for the second call leg.
 20. **Src Usg Ind Leg 2.** The OSP client Toolkit sends an OSP UsageIndication message (Call Detail Record) to the OSP server. The UsageIndication is a type 'source' call detail record since the B2BUA is the source device for the second leg of the call.
 21. **Src Usg Cnf Leg 2.** The OSP server responds with an OSP UsageConfirmation message.
 22. **RepUsage(Out).** The OSP Toolkit closes the ReportUsage transaction.
 23. **TransDelete.** The B2BUA deletes the OSP Toolkit transaction for the second call leg.
 24. **RecordFailure.** The B2BUA reports the call disconnect reason, for the first call leg, to the OSP Toolkit using the OSPPTxactionRecordFailure function.
 25. **RepUsage(In).** The B2BUA calls the OSPPTxactionReportUsage function to report the call duration for the first call leg.
 26. **Src Usg Ind Leg 1.** The OSP client Toolkit sends an OSP UsageIndication message (Call Detail Record) to the OSP server. The UsageIndication is a type 'destination' call detail record since the B2BUA is the destination device for the first leg of the call.
 27. **Src Usg Cnf Leg 1.** The OSP server responds with an OSP UsageConfirmation message.

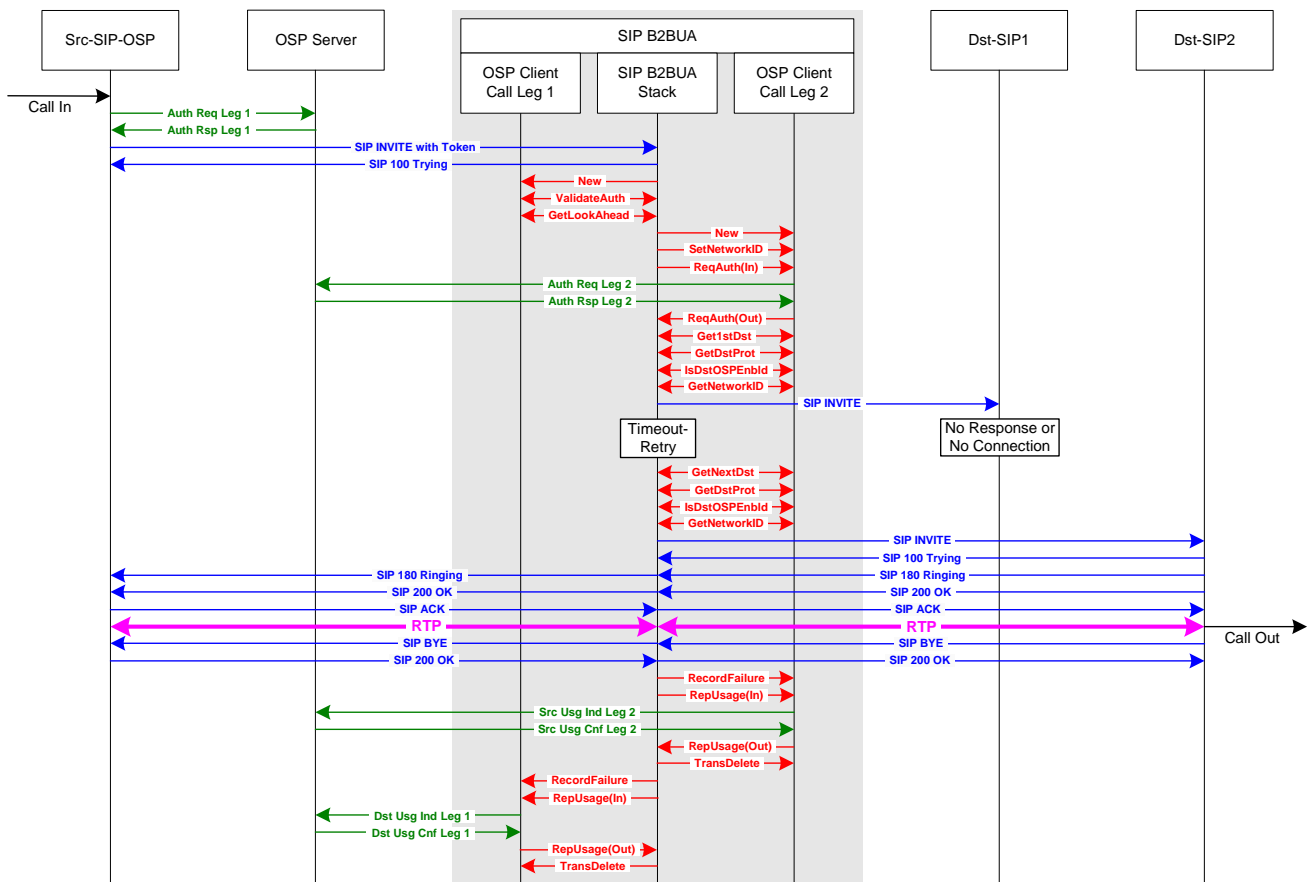
- 28. **RepUsage(Out)**. The OSP Toolkit closes the ReportUsage transaction.
- 29. **TransDelete**. The B2BUA deletes the OSP Toolkit transaction for the first call leg.

Expected CDRs for Test Case 2.3.1

This test case should generate three OSP UsageIndication messages, or CDRs, from the B2BUA. 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-SIP1. In this example, the SIP response is 503, but other SIP responses are also valid. For the successful retry for call leg 2, the B2BUA should set the FailureReason to 16 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 by the B2BUA.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	Source	Src-SIP-OSP	Dst-SIP1	503	0
2	Source	Src-SIP-OSP	Dst-SIP2	16 or 1016	greater than 0
1	destination	Src-SIP-OSP	the B2BUA	16 or 1016	greater than 0

2.3.2 No Response or No Connection and Retry - B2BUA Times Out



**Test Case 2.3.2: OSP Source to SIP B2BUA to non-OSP Destination
No Response or No Connection & Retry - SIP B2BUA Times Out**
Legend: SIP Messages in Blue, 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 B2BUA. This test case requires that the OSP server return two or more destinations in the AuthorizationResponse to the B2BUA. After the first call attempt fails, the B2BUA 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 B2BUA cannot establish a TCP connection with Dst-SIP1. After TCP time-out, the B2BUA should retry call to Dst-SIP2. (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-SIP1 IP device. the B2BUA should retry call to Dst-SIP2. (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-SIP1. After TCP connection is refused, the B2BUA should retry the call to Dst-SIP2. (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-SIP1. the B2BUA establishes TCP connection with Dst-SIP1, but DST-SIP1 never responds to SIP INVITE. the B2BUA should time-out and retry the call to Dst-SIP2. (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.)

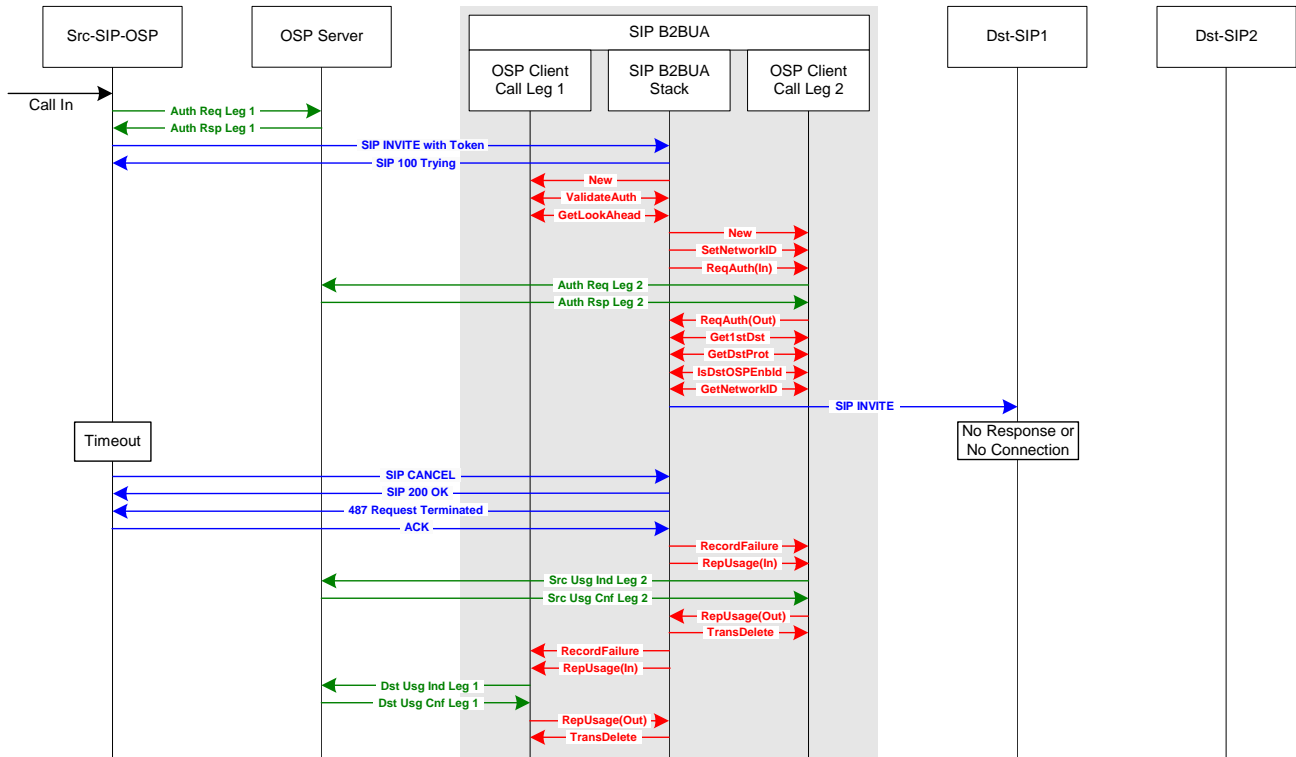
Note: The destination UsageIndication call detail record for call leg one, should have FailureReason set to the release code for the last call attempt. If no call release reason is included with the BYE from the destination for a successful call, the FailureReason should be set to 16.

Expected CDRs for Test Case 2.3.2

This test case should generate three OSP UsageIndication messages, or CDRs, from the B2BUA. 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 B2BUA based on the reason for the failure. For the successful retry of call leg 2, the B2BUA should set the FailureReason to 16, 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.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-SIP-OSP	Dst-SIP1	47, 2, 63 or 27	0
2	source	Src-SIP-OSP	Dst-SIP2	16 or 1016	greater than 0
1	destination	Src-SIP-OSP	B2BUA	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 Source to SIP B2BUA to non-OSP Destination
No Response or No Connection & Retry - Source Times Out**
Legend: SIP Messages in Blue, 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-SIP1 responds to the SIP INVITE from the B2BUA. In these cases, the B2BUA 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 CANCEL message from the source device, Src-SIP. If no release reason is reported in the CANCEL message, the B2BUA 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 B2BUA. 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-SIP-OSP. If no release reason is included in the SIP CANCEL message, the B2BUA 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-SIP-OSP	Dst-SIP1	487	0
1	destination	Src-SIP-OSP	B2BUA	487	0

2.3.4 Call Duration Limit Exceeded



Test Case 2.3.4: OSP Source to SIP B2BUA to non-OSP Destination: Call Duration Limit Exceeded
Legend: SIP Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

This call scenario tests the B2BUA’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 B2BUA should terminate a call when the call duration exceeds the `TimeLimit`. In this case, when the B2BUA forcefully ends a call that has exceeded its maximum call duration, the B2BUA 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 B2BUA to determine when to forcefully end a call.

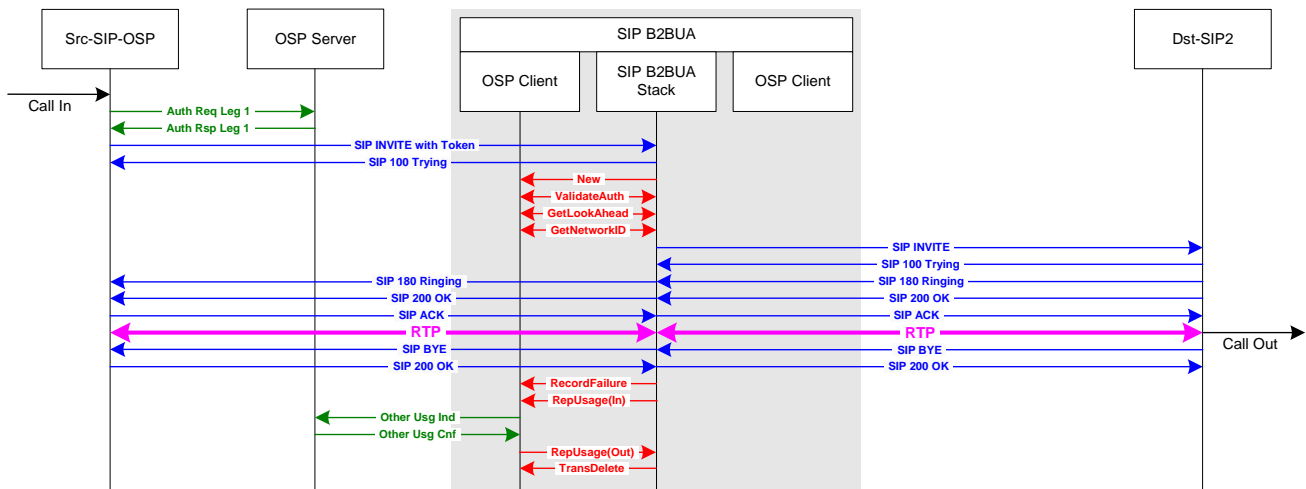
Expected CDRs for Test Case 2.3.4

This test case should generate two OSP UsageIndication messages, or CDRs. One from the B2BUA as the source of call leg 2 and another as the destination for call leg 1. The release reason (ospvFailureReason), or termination cause code, for the call should be set by the B2BUA to 8 to indicate the call was forcefully shutdown by the B2BUA.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-SIP-OSP	Dst-SIP2	8	greater than 0
1	destination	Src-SIP-OSP	B2BUA	8	greater than 0

2.3.5 Look Ahead Routing

Look Ahead Routing is a unique OSP application for SIP proxies and B2BUAs. 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 B2BUA. When the B2BUA validates the OSP token, the B2BUA calls the function OSPPTtransactionGetLookAheadInfoIfPresent. If Look Ahead Routing information is available, it is passed from the OSP client to the B2BUA and eliminates the need for a second lookup to the OSP server. Note that only one OSP Toolkit transaction between the B2BUA and the OSP Toolkit is required when Look Ahead Routing is used. Note: To test Look Ahead Routing, the B2BUA must be configured in the OSP server with OSP Version = 2.1.1-P.



Test Case 2.3.5: OSP Source to SIP B2BUA to non-OSP Destination: Look Ahead Routing
 Legend: SIP Messages in Blue, 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 B2BUA, 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 B2BUA. The SIP INVITE message header includes an OSP authorization token.
5. **SIP 100 Trying.** The B2BUA receives the SIP INVITE message and responds.
6. **NEW.** The B2BUA recognizes the presence of an OSP authorization token in the SIP INVITE message call setup and establishes a transaction with the OSP Toolkit to validate the token.
7. **ValidateAuth.** The B2BUA 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 B2BUA. In this call scenario, the token is valid and the call processing continues. If the token was not valid, the B2BUA 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. If the call duration exceeds the authorized time limit, the B2BUA should end the call (test case 2.3.4).
8. **GetLookAhead.** The B2BUA 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 B2BUA should assume the destination is a SIP device and complete the call. If `OSPE_DEST_PROT` is `H323_SETUP` or `H323_LRQ`, the proxy should reject the call 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 Look Ahead token should be included, as is, in the SIP INVITE to the destination. If `OSPE_OSP` is `UNKNOWN` or `UNDEFINED`, the B2BUA should assume the Look Ahead destination is OSP enabled and include the Look Ahead token in the SIP INVITE to the destination.

9. **GetNetworkID.** The B2BUA 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.
10. **SIP INVITE.** The B2BUA sends a call setup message to the 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 SIP INVITE from the source device, it should NOT be included in the SIP INVITE from the B2BUA to the destination.

SIP B2BUA – OSP Peering Test Cases

- 11-17. Standard SIP communications for the completing the call.
18. **RecordFailure.** At the completion of the call, the B2BUA reports the call disconnect reason for the call to the OSP Toolkit using the OSPTransactionRecordFailure function.
 19. **RepUsage(In).** The B2BUA calls the OSPTransactionReportUsage function to report the call duration for the second call leg.
 20. **Other Usg Ind.** The OSP client Toolkit 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 B2BUA is the destination device for the first call leg and the source device for the second call leg.
 21. **Other Usg Cnf.** The OSP server responds with an OSP UsageConfirmation message.
 22. **RepUsage(Out).** The OSP Toolkit closes the ReportUsage transaction.
 23. **TransDelete.** The B2BUA deletes the OSP Toolkit transaction for the call.

Test Case Notes

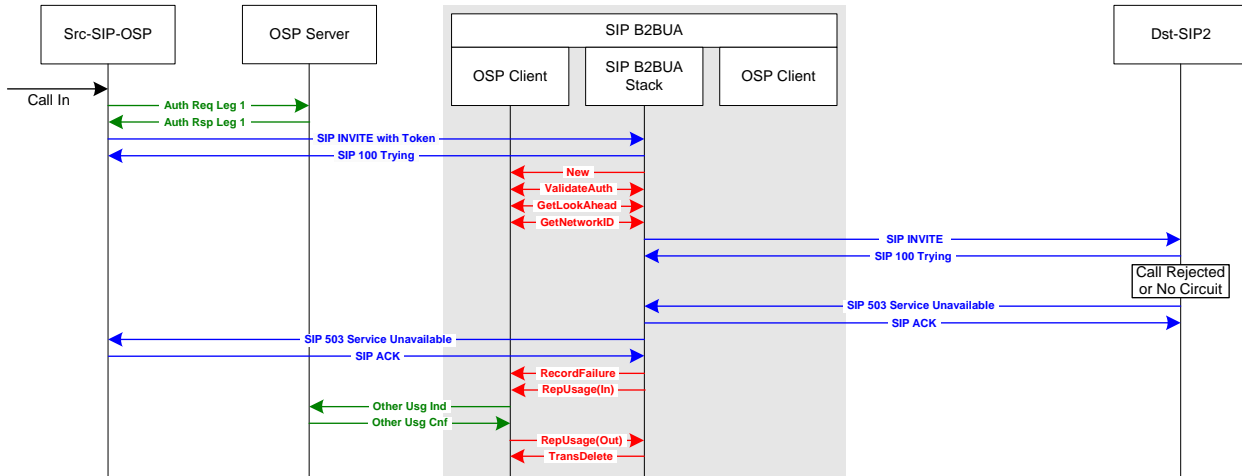
V3.3.1, and earlier versions, of the OSP Toolkit support only a single Look Ahead route embedded in an OSP authorization token. Future releases of the OSP Toolkit will support multiple destinations in a Look Ahead token so the B2BUA can retry the call to other destinations if the call attempt to the first destination fails.

Expected CDR for Test Case 2.3.5

This test case should generate one OSP UsageIndication message, or CDR, from the B2BUA. 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 or CANCEL header, or by the SIP response from the source or destination device. If the call is successful and there is no release code reported, the B2BUA should report the FailureReason as 16 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-SIP-OSP	Dst-SIP2	16 or 1016	greater than 0

2.3.6 Look Ahead Routing: Call Rejected or No Circuit



**Test Case 2.3.6: OSP Source to SIP B2BUA to non-OSP Destination:
Look Ahead Routing - Call Rejected or No Circuit & Retry**

Legend: SIP Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

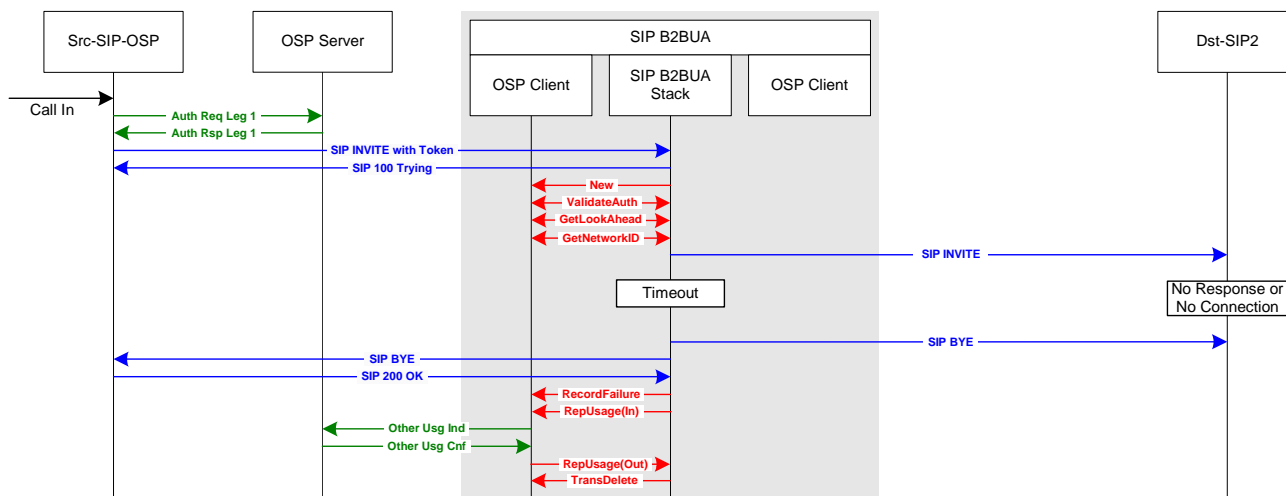
This case is similar to test case 2.3.1 and tests a Look Ahead call scenario when the destination SIP device rejects the call.

Expected CDR for Test Case 2.3.6

This test case should generate one OSP UsageIndication message, or CDR from the B2BUA. 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-SIP-OSP	Dst-SIP2	503	0

2.3.7 Look Ahead Routing: No Response or No Connection - B2BUA Times Out



**Test Case 2.3.7: OSP Source to SIP B2BUA to non-OSP Destination:
Look Ahead Routing - No Response or No Connection - SIP B2BUA Times Out**
Legend: SIP Messages in Blue, 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 SIP device does not respond to the B2BUA. This test case must be executed four times to test the following four different call scenarios.

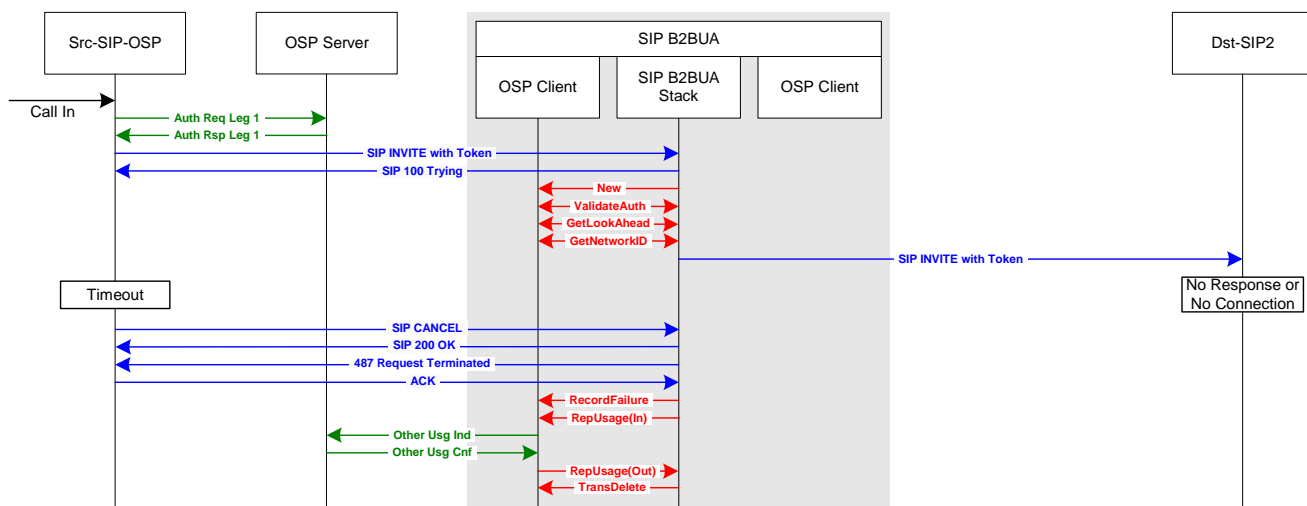
1. The B2BUA cannot establish a TCP connection with Dst-SIP1. After TCP time-out, the B2BUA should retry call to Dst-SIP2. (When OSP Toolkit function RecordFailure is called, the FailureReason for the call attempt should be set to 47 – resource unavailable, unspecified.)
2. No route to IP address of Dst-SIP1. the B2BUA should retry call to Dst-SIP2. (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 B2BUA should retry the call to Dst-SIP2. (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-SIP1. the B2BUA establishes TCP connection with Dst-SIP1, but DST-SIP1 never responds to SIP INVITE. the B2BUA should time-out and retry the call to Dst-SIP2. (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 B2BUA. The role should be “other” and the FailureReason should be determined by the B2BUA 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-SIP-OSP	Dst-SIP2	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 Source to SIP B2BUA to non-OSP Destination: Look Ahead Routing - No Response or No Connection - Source Times Out
Legend: SIP Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

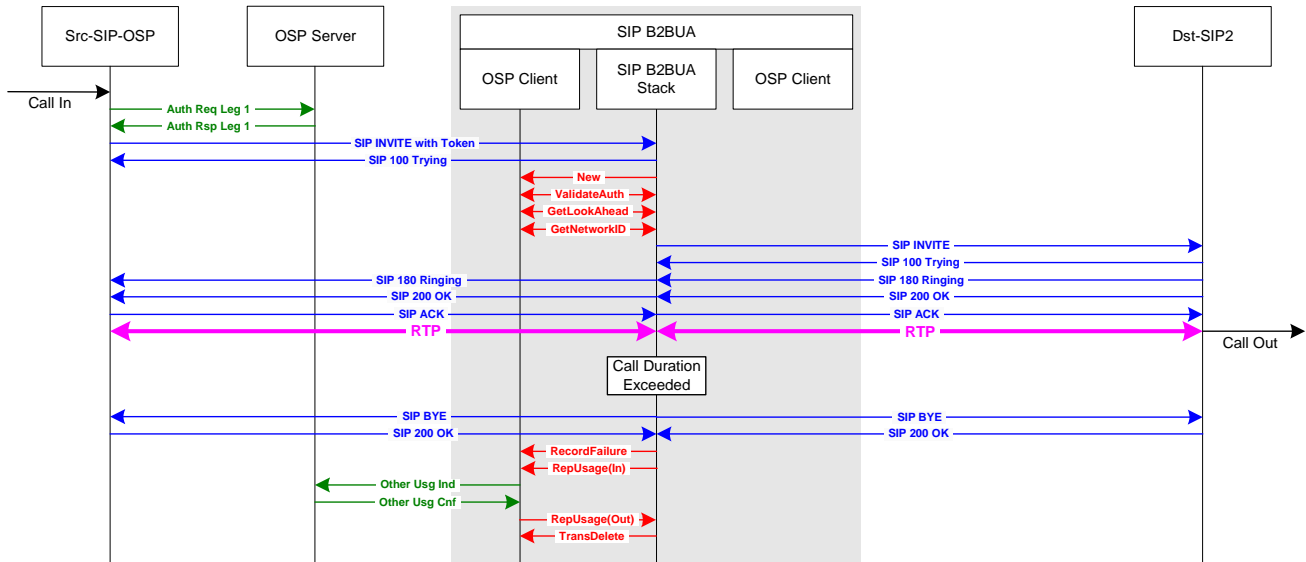
This test case is similar to test case 2.3.3 and tests the Look Ahead call scenario when the source ends the call before the destination Dst-SIP2 responds to the SIP INVITE from the B2BUA. In this case, the B2BUA should terminate the call and report usage to the OSP server. The OSP Toolkit parameter FailureReason reported with the OSPTransactionRecordFailure function should be set to the release cause reported in the BYE or Cancel message from the source device, Src-SIP. If no release reason is reported in the CANCEL message, the B2BUA 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 B2BUA. The role should be “other” and the FailureReason should be determined by the release reason in the SIP BYE or CANCEL message from Src-SIP. If no release reason is provided in the SIP message, the B2BUA 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-SIP-OSP	Dst-SIP2	487	0

2.3.9 Look Ahead Routing: Call Duration Limit Exceeded



**Test Case 2.3.9: OSP Source to SIP B2BUA to non-OSP Destination:
Look Ahead Routing - Call Duration Limit Exceeded**

Legend: SIP Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

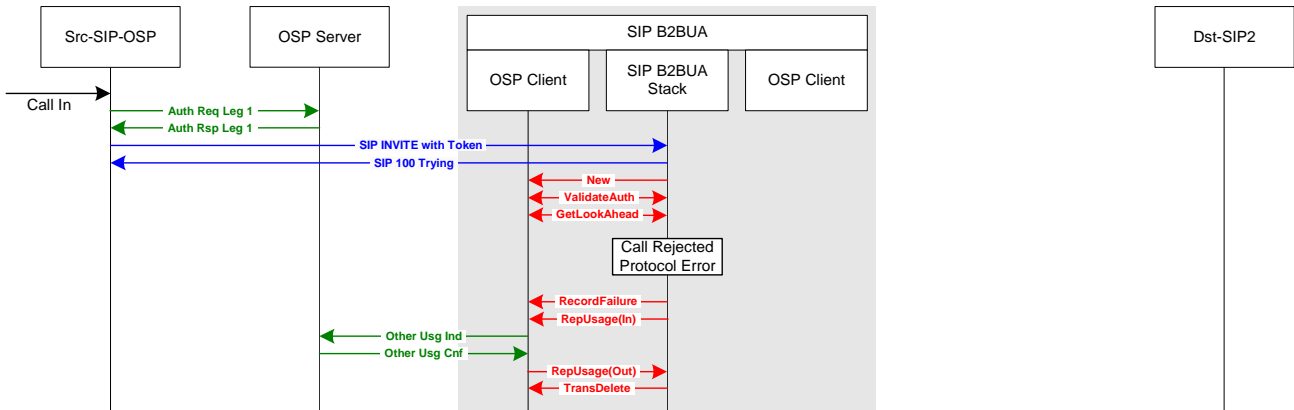
If the call duration exceeds the authorized call duration set by `ospvTimeLimit` value returned from the `OSPPTTransactionValidateAuthorisation` function, the B2BUA should forcefully end the call. When the B2BUA forcefully ends the call because the call duration exceeded the authorized time limit, the `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 B2BUA. The role should be “other” and the `FailureReason` should be 8 to indicate the call was forcefully shutdown by the B2BUA.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-SIP-OSP	Dst-SIP2	8	0

2.3.10 Look Ahead Routing: Protocol Error



Test Case 2.3.10: OSP Source to SIP B2BUA to non-OSP Destination: Look Ahead Routing
Legend: SIP Messages in Blue, 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 SIP B2BUA, such as H323_SETUP, H323_LRQ or IAX. When this occurs, the B2BUA should reject the destination, record FailureReason 111 (protocol error) and report usage.

For this test case, the destination protocol for device Dst-SIP2 is NOT configured as SIP on the OSP server. The OSPTransactionGetLookAheadInfoIfPresent function call returns a DestinationProtocol incompatible with SIP. The B2BUA should recognize the protocol error and reject the call attempt. Note, if the DestinationProtocol is unknown or undefined, the B2BUA should assume the destination device supports SIP and should send an INVITE to the destination device.

Expected CDRs for Test Case 2.3.10

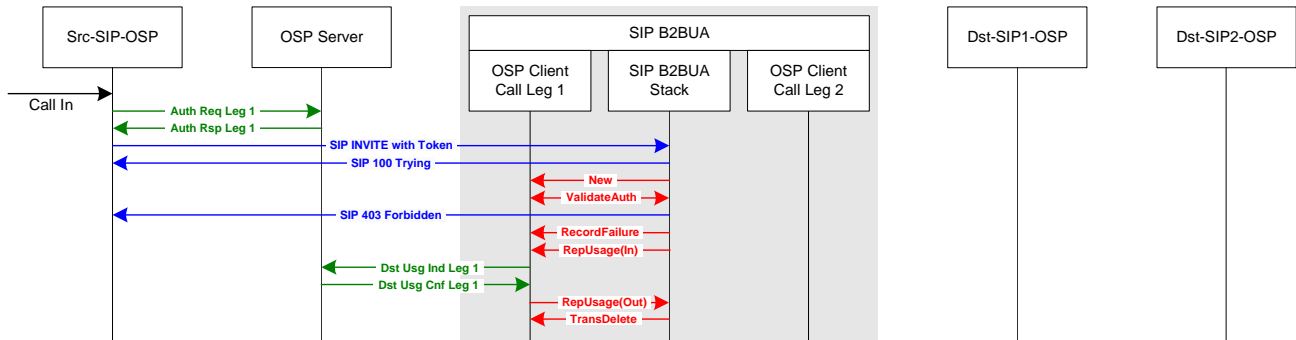
Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-SIP	Dst-SIP2	111	0

2.4 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 SIP device will include an OSP authorization token in the SIP INVITE message sent to the B2BUA. Based on the test case, the OSP token may or may not include Look Ahead routing information. To complete the call, the B2BUA 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 2.4		
Device	Destination Protocol	OSP Version
Src-SIP-OSP	SIP	1.3.4, 2.1.1 or 4.1.1
SIP B2BUA	SIP	2.1.1 or 4.1.1
Dst-SIP1-OSP	SIP	1.3.4, 2.1.1 or 4.1.1
Dst-SIP2-OSP	SIP	1.3.4, 2.1.1 or 4.1.1

2.4.0 Invalid Authorization Token



Test Case 2.4.0: OSP Source to SIP B2BUA to OSP Destination: Invalid Authorization Token
 Legend: SIP Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

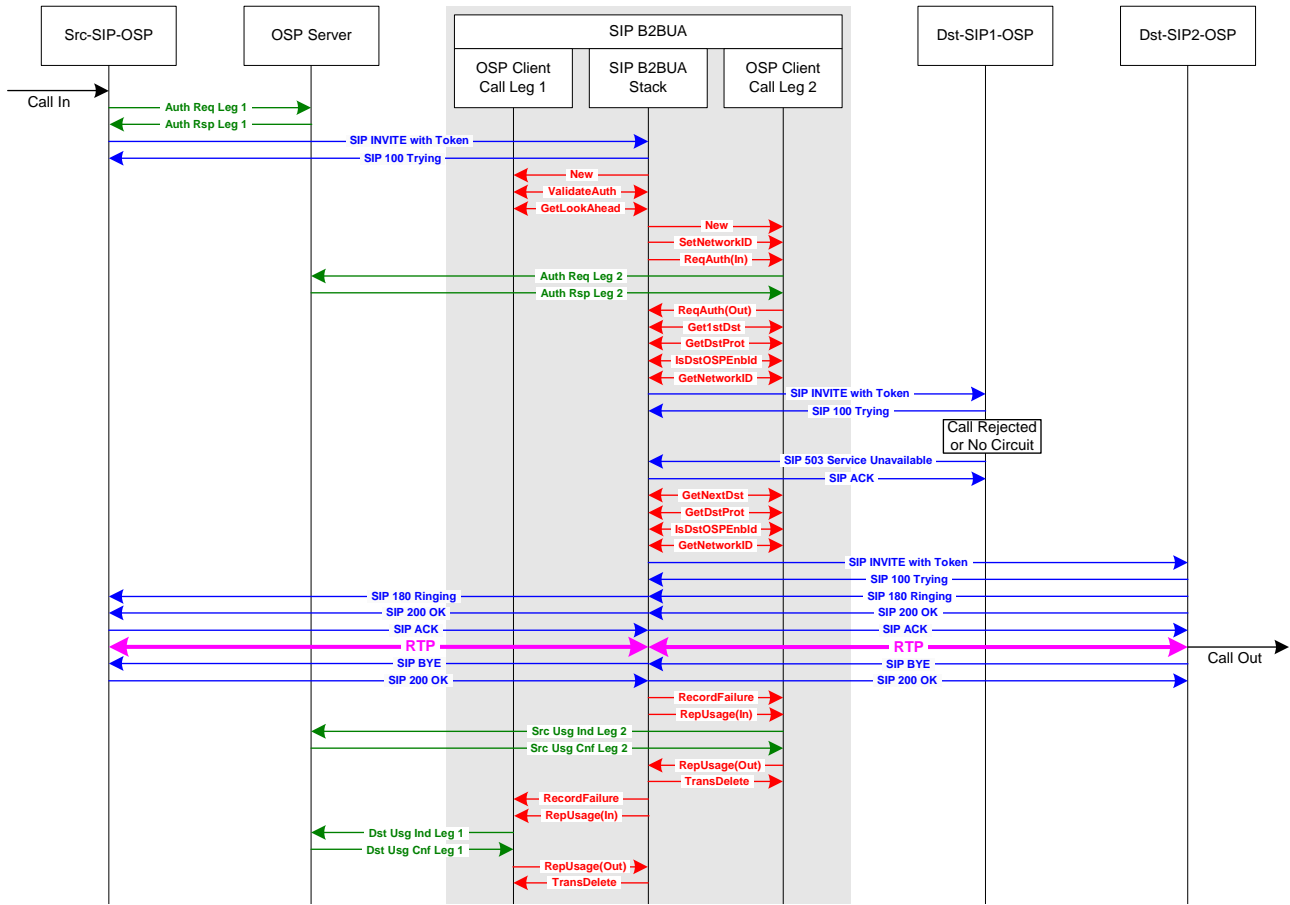
This test case is identical to 2.3.0.

Expected CDR for Test Case 2.4.0

This test case should generate one OSP UsageIndication message, or CDR, from the B2BUA as the destination of call leg 1. The release reason (ospvFailureReason), or termination cause code, for the call should be set by the B2BUA 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-SIP-OSP	B2BUA	403	0

2.4.1 Call Rejected or No Circuit and Retry



Test Case 2.4.1: OSP Source to SIP B2BUA to OSP Destination: Call Rejected or No Circuit & Retry
Legend: SIP Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

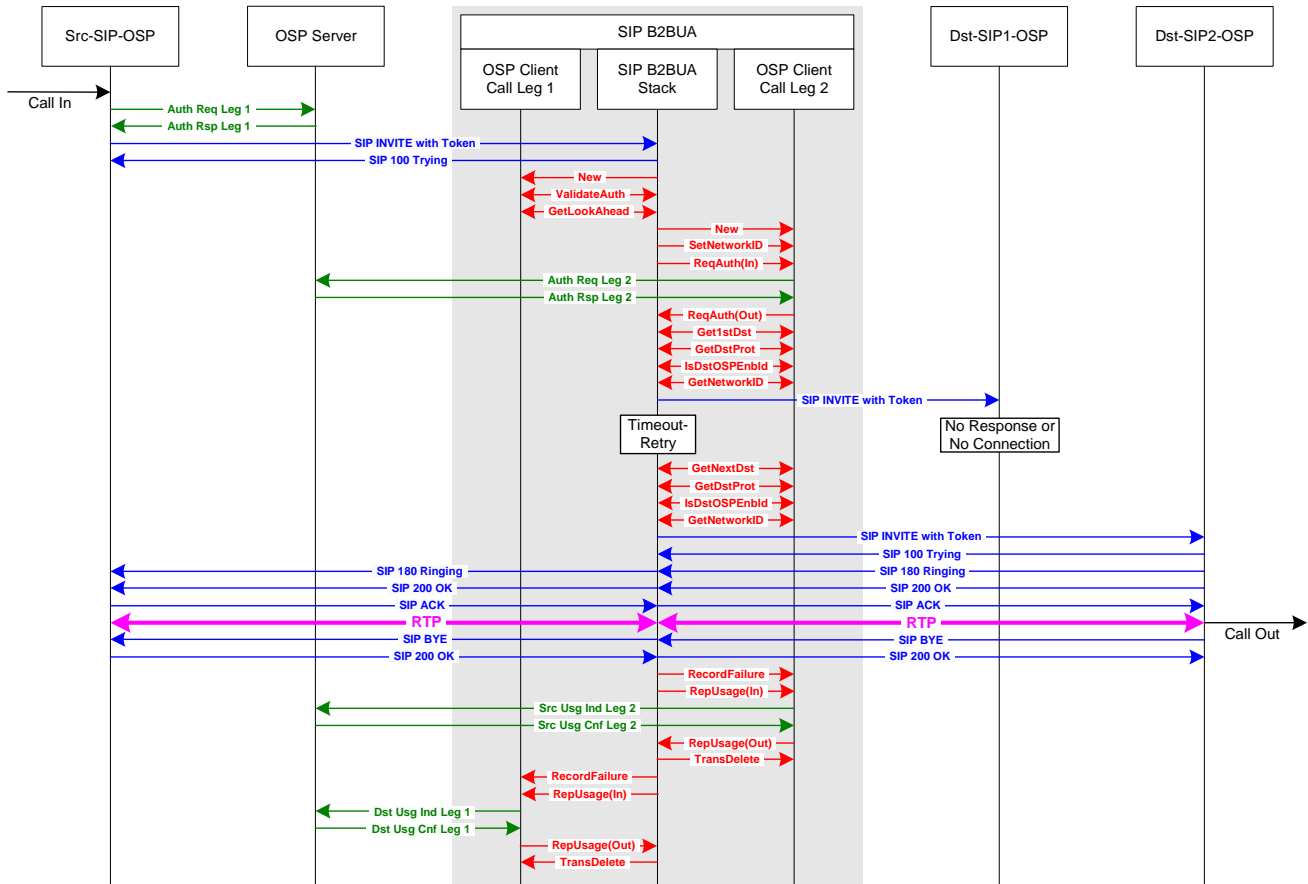
See test case 2.3.1.

Expected CDRs for Test Case 2.4.1

This test case should generate three OSP UsageIndication messages, or CDRs, from the B2BUA. 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-SIP1-OSP. In this example, the SIP response is 503, but other SIP responses are also valid. For the successful retry for call leg 2, the B2BUA should set the FailureReason to 16 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 by the B2BUA.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-SIP-OSP	Dst-SIP1-OSP	503	0
2	source	Src-SIP-OSP	Dst-SIP2-OSP	16 or 1016	greater than 0
1	destination	Src-SIP-OSP	B2BUA	16 or 1016	greater than 0

2.4.2 No Response or No Connection and Retry - B2BUA Times Out



**Test Case 2.4.2: OSP Source to SIP B2BUA to OSP Destination
No Response or No Connection & Retry - SIP B2BUA Times Out**
Legend: SIP Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

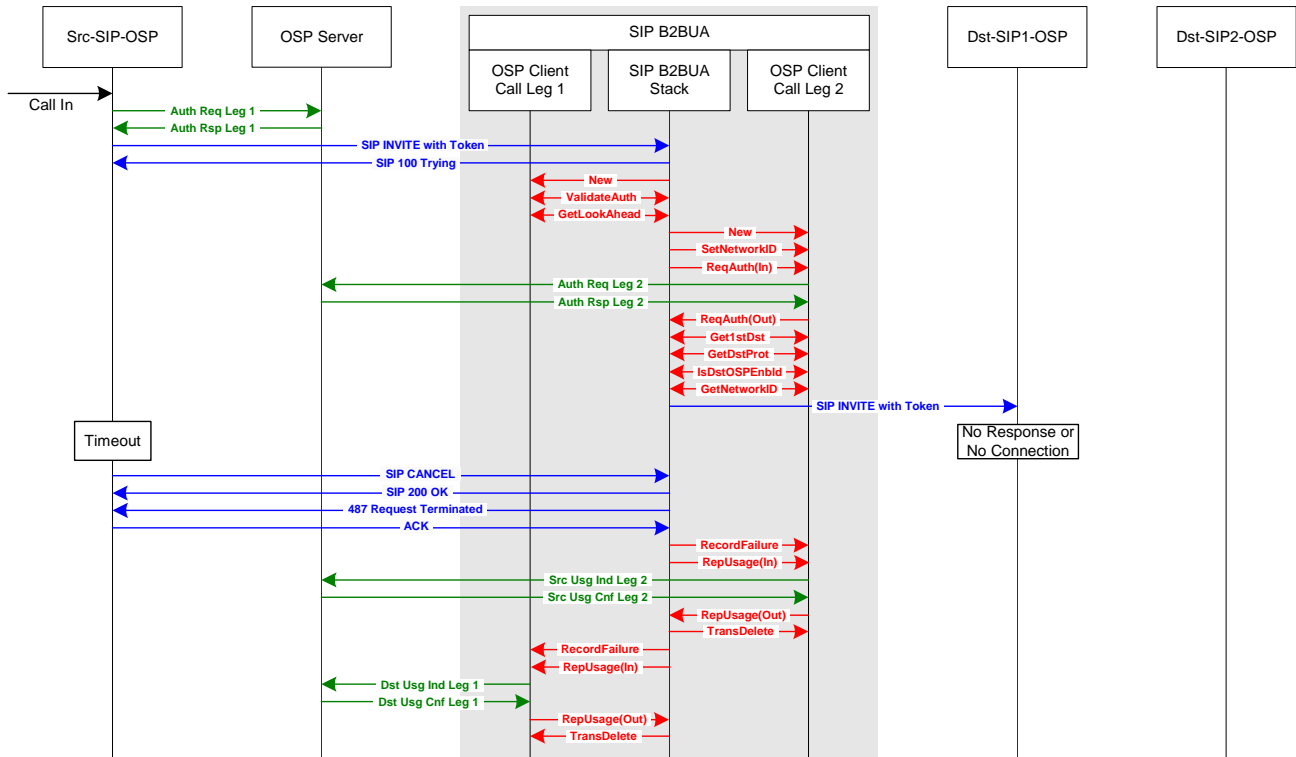
See test case 2.3.2.

Expected CDRs for Test Case 2.4.2

This test case should generate three OSP UsageIndication messages, or CDRs, from the B2BUA. 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 B2BUA based on the reason for the failure. For the successful retry of call leg 2, the B2BUA should set the FailureReason to 16, 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.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-SIP-OSP	Dst-SIP1-OSP	47, 2, 63 or 27	0
2	source	Src-SIP-OSP	Dst-SIP2-OSP	16 or 1016	greater than 0
1	destination	Src-SIP-OSP	B2BUA	16 or 1016	greater than 0

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



**Test Case 2.4.3: OSP Source to SIP B2BUA to OSP Destination
No Response or No Connection & Retry - Source Times Out**
Legend: SIP Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

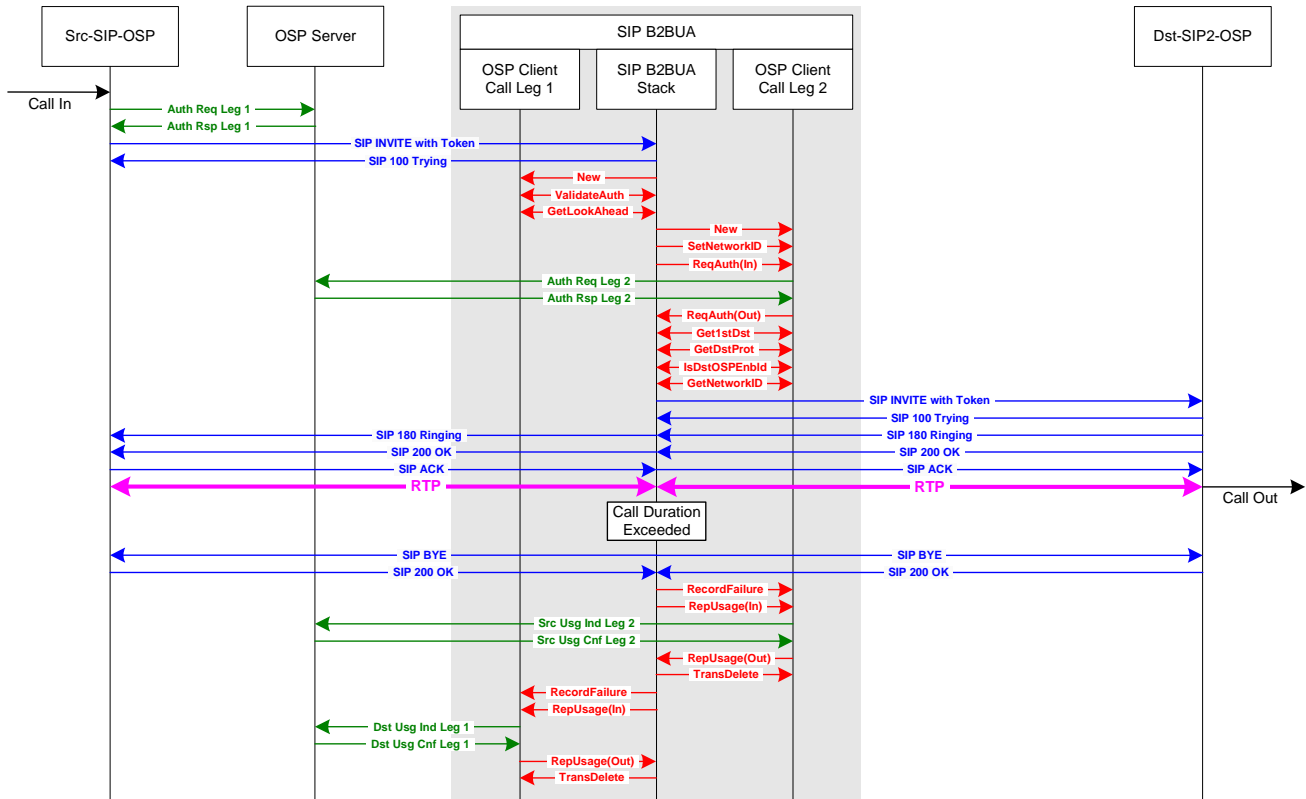
See test case 2.3.3.

Expected CDRs for Test Case 2.4.3

This test case should generate two OSP UsageIndication messages, or CDRs, from the B2BUA. 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-SIP-OSP. If no release reason is included in the SIP CANCEL message, the B2BUA 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-SIP-OSP	Dst-SIP1-OSP	487	0
1	destination	Src-SIP-OSP	B2BUA	487	0

2.4.4 Call Duration Limit Exceeded



Test Case 2.4.4: OSP Source to SIP B2BUA to OSP Destination: Time Limit Exceeded
Legend: SIP Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

This call scenario tests the B2BUA’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 B2BUA should terminate a call when the call duration exceeds the TimeLimit. In this case, when the B2BUA forcefully ends a call that has exceeded its maximum call duration, the B2BUA 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 B2BUA to determine when to forcefully end a call.

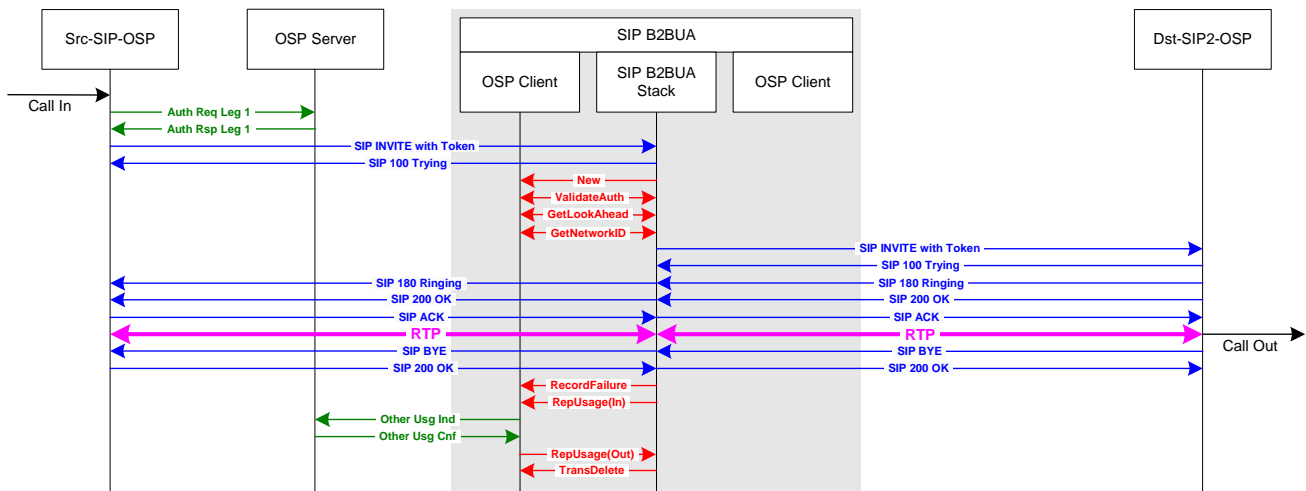
Expected CDRs for Test Case 2.4.4

SIP B2BUA – OSP Peering Test Cases

This test case should generate two OSP UsageIndication messages, or CDRs. One from the B2BUA as the source of call leg 2 and another as the destination for call leg 1. The release reason (ospvFailureReason), or termination cause code, for the call should be set by the B2BUA to 8 to indicate the call was forcefully shutdown by the B2BUA.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
2	source	Src-SIP-OSP	Dst-SIP2-OSP	8	greater than 0
1	destination	Src-SIP-OSP	B2BUA	8	greater than 0

2.4.5 Look Ahead Routing



Test Case 2.4.5: OSP Source to SIP B2BUA to OSP Destination: Look Ahead Routing
Legend: SIP Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

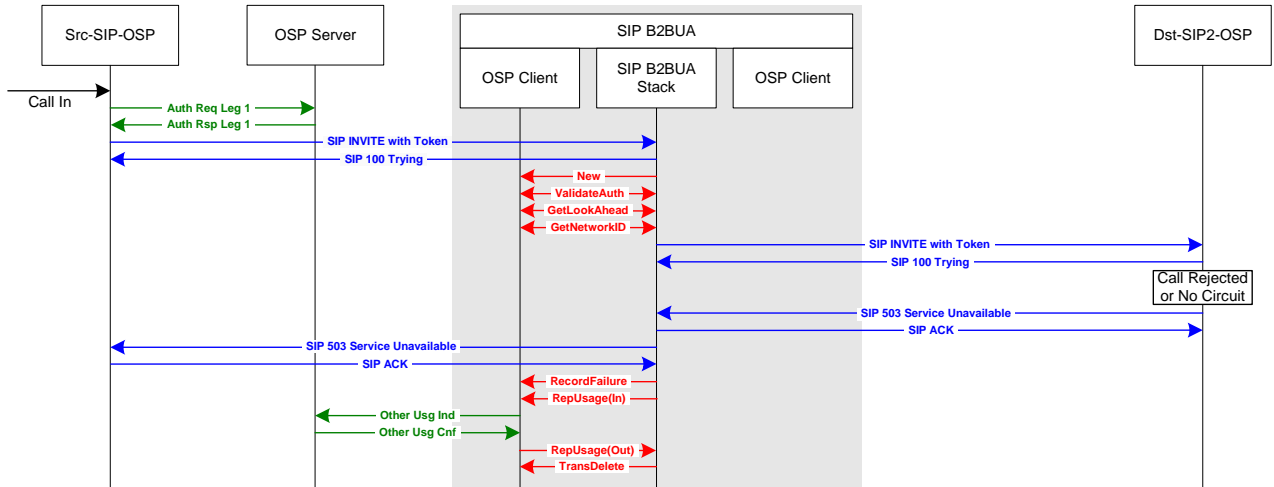
See test case 2.3.5. The SIP B2BUA should be configured in the OSP server with OSP version = 2.1.1-P.

Expected CDR for Test Case 2.4.5

This test case should generate one OSP UsageIndication message, or CDR from the B2BUA. 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 or CANCEL header, or by the SIP response from the source or destination device. If the call is successful and there is no release code reported, the B2BUA should report the FailureReason as 16 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-SIP-OSP	Dst-SIP2-OSP	16 or 1016	greater than 0

2.4.6 Look Ahead Routing: Call Rejected or No Circuit



**Test Case 2.4.6: OSP Source to SIP B2BUA to OSP Destination:
Look Ahead Routing - Call Rejected or No Circuit & Retry**
Legend: SIP Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

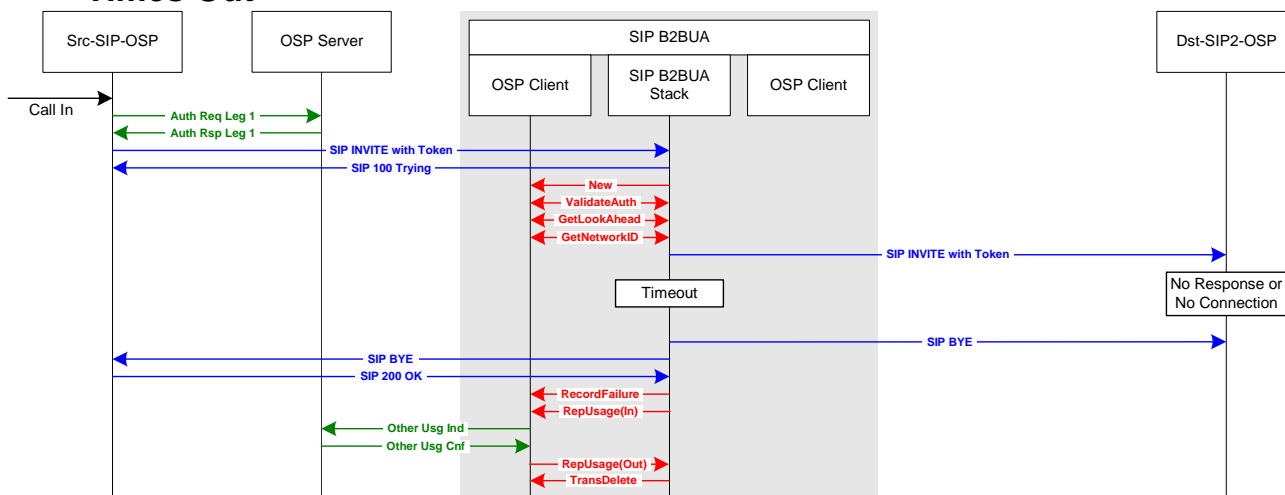
See test case 2.3.6.

Expected CDR for Test Case 2.4.6

This test case should generate one OSP UsageIndication message, or CDR from the B2BUA. 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-SIP-OSP	Dst-SIP2-OSP	503	0

2.4.7 Look Ahead Routing: No Response or No Connection - B2BUA Times Out



**Test Case 2.4.7: OSP Source to SIP B2BUA to OSP Destination:
Look Ahead Routing - No Response or No Connection - SIP B2BUA Times Out**
Legend: SIP Messages in Blue, 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 B2BUA. This test case must be executed four times to test the following four different call scenarios.

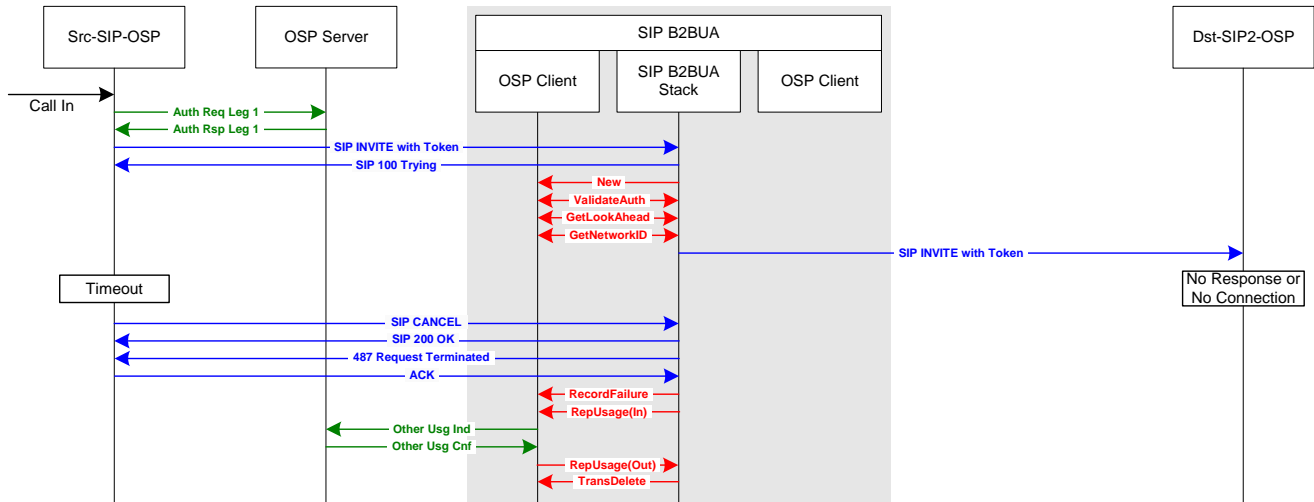
1. The B2BUA cannot establish a TCP connection with Dst-SIP1-OSP. After TCP time-out, the B2BUA should retry call to Dst-SIP2-OSP. (When OSP Toolkit function RecordFailure is called, the FailureReason for the call attempt should be set to 47 – resource unavailable, unspecified.)
2. No route to IP address of Dst-SIP1-OSP. the B2BUA should retry call to Dst-SIP2-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-SIP1-OSP. After TCP connection is refused, the B2BUA should retry the call to Dst-SIP2-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-SIP1-OSP. the B2BUA establishes TCP connection with Dst-SIP1, but DST-SIP1-OSP never responds to SIP INVITE. the B2BUA should time-out and retry the call to Dst-SIP2-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 B2BUA. The role should be “other” and the FailureReason should be determined by the B2BUA 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-SIP-OSP	Dst-SIP2-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 Source to SIP B2BUA to OSP Destination:
Look Ahead Routing - No Response or No Connection - Source Times Out**
Legend: SIP Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

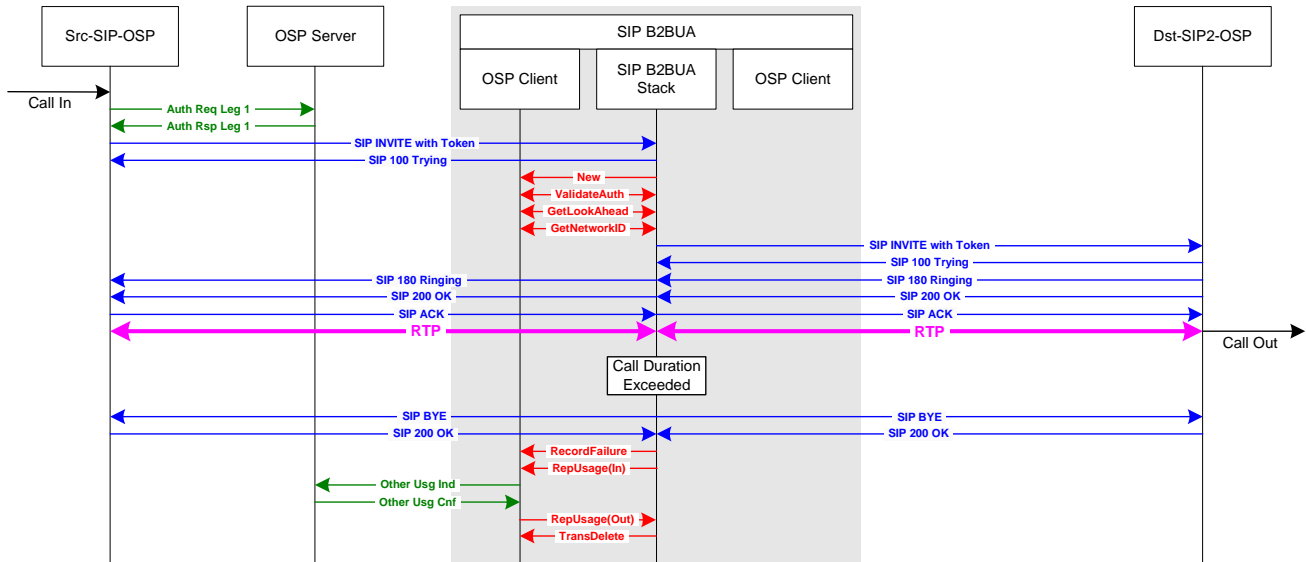
See test case 2.3.8.

Expected CDR for Test Case 2.4.8

This test case should generate one OSP UsageIndication message, or CDR, from the B2BUA. The role should be “other” and the FailureReason should be determined by the release reason in the SIP BYE or CANCEL message from Src-SIP-OSP. If no release reason is provided in the SIP message, the B2BUA 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-SIP-OSP	Dst-SIP2-OSP	487	0

2.4.9 Look Ahead Routing: Call Duration Limit Exceeded



**Test Case 2.4.9: OSP Source to SIP B2BUA to OSP Destination:
Look Ahead Routing - Call Duration Limit Exceeded**

Legend: SIP Messages in Blue, 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 B2BUA should forcefully end the call. When the B2BUA 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 B2BUA. The role should be “other” and the `FailureReason` should be 8 to indicate the call was forcefully shutdown by the B2BUA.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-SIP-OSP	Dst-SIP2-OSP	8	0