



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

7 June 2006

1. Introduction	3
2. Gateway to Gateway 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 - Proxy Times Out	11
2.1.3. No Response or No Connection and Retry - Source Times Out.....	12
2.1.4. Call Duration Limit Exceeded	13
2.1.5. Call Rejected – Protocol Error and Retry	14
2.1.6. Number Translation.....	15
2.2. non-OSP Source to OSP Destination	16
2.2.1. Call Rejected or No Circuit and Retry.....	17
2.2.2. No Response or No Connection and Retry - Proxy Times Out	18
2.2.3. No Response or No Connection and Retry - Source Times Out.....	19
2.2.4. Call Duration Limit Exceeded	20
2.2.5. Number Translation.....	21
2.3. OSP Source and non-OSP Destination	23
2.3.0. Invalid Authorization Token.....	23
2.3.1. Call Rejected or No Circuit and Retry.....	24
2.3.2. No Response or No Connection and Retry – Proxy Times Out.....	26
2.3.3. No Response or No Connection and Retry - Source Times Out.....	28
2.3.4. Call Duration Limit Exceeded	29
2.3.5. Look Ahead Routing	30
2.3.6. Look Ahead Routing: Call Rejected or No Circuit.....	32
2.3.7. Look Ahead Routing: No Response or No Connection - Proxy Times Out	33
2.3.8. Look Ahead Routing: No Response or No Connection - Source Times Out.....	34
2.3.9. Look Ahead Routing: Call Duration Limit Exceeded	35
2.3.10. Look Ahead Routing: Protocol Error.....	36
2.4. OSP Source to OSP Destination	37
2.4.0. Invalid Authorization Token.....	37
2.4.1. Call Rejected or No Circuit and Retry.....	38
2.4.2. No Response or No Connection and Retry - Proxy Times Out	39
2.4.3. No Response or No Connection and Retry - Source Times Out.....	40
2.4.4. Call Duration Limit Exceeded	41
2.4.5. Look Ahead Routing	42
2.4.6. Look Ahead Routing: Call Rejected or No Circuit.....	43
2.4.7. Look Ahead Routing: No Response or No Connection - Proxy Times Out	43
2.4.8. Look Ahead Routing: No Response or No Connection - Source Times Out.....	44
2.4.9. Look Ahead Routing: Call Duration Limit Exceeded	45

H.323 Proxy – OSP Peering Test Cases

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 H.323 proxy. The OSP protocol, designed for inter-domain authorization, routing and accounting, is well suited for secure management of peer to peer IP applications such as VoIP and video over IP. For more information on ETSI, please refer to www.etsi.org.

The test cases are divided into four sections based on whether or not the source and destination devices support OSP. Each-section contains between five and eleven test cases. The focus of these test cases is on the H.323 proxy which is presented as gray box in the middle of each test case illustration. Note, these test cases assume the H.323 proxy being tested is capable of tracking the call state from beginning to end and then reporting call duration in a call detail record.

A basic requirement for these test cases is the ability of the H.323 proxy to enroll with the OSP server. The enrollment process is a two step process. First, the H.323 proxy requests the public key of the OSP server. Second, it sends a certificate request to the OSP server which returns a signed certificate to the inter-working proxy. Secure inter-domain access control requires that the inter-working proxy be able to validate an OSP authorization token digitally signed by the OSP server.

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

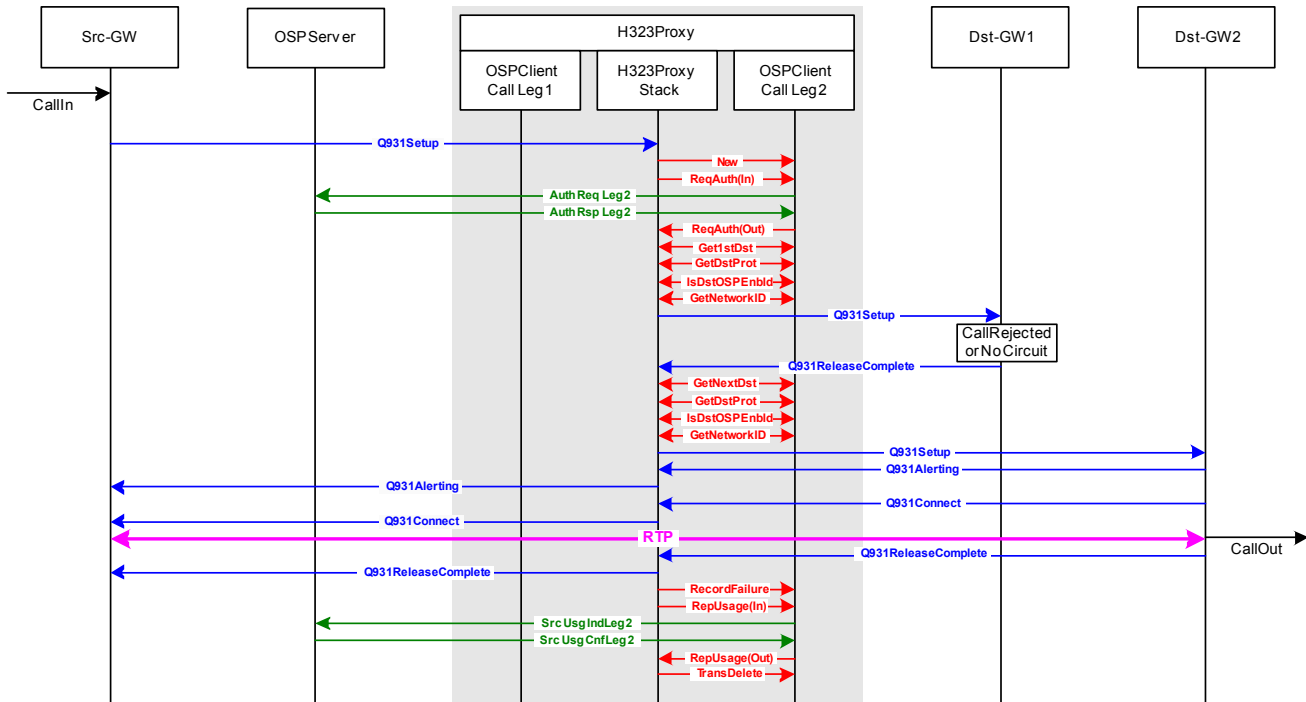
2. Gateway to Gateway Test Cases

2.1. non-OSP Source to non-OSP Destination

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

Configuration of VoIP devices on OSP server for test cases in section 2.1		
Device	Destination Protocol	OSP Version
Src-GW	H323-Q931	0.0.0 (Not OSP Enabled)
H.323 Proxy	H323-Q931	2.1.1 or 4.1.1
Dst-GW1	H323-Q931	0.0.0 (Not OSP Enabled)
Dst-GW2	H323-Q931	0.0.0 (Not OSP Enabled)

2.1.1. Call Rejected or No Circuit and Retry



Test Case 2.1.1: Gateway to Proxy to Gateway - Call Rejected or No Circuit & Retry
Legend: H.323 Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

For this test case, the OSP server is configured with two routes, or destination gateways, to complete the call to the called number from the H.323 proxy. The proxy attempts the call which is rejected by the first destination gateway. The proxy then fails over to the second destination gateway and completes the call.

This acceptance test case covers all cases when the first destination gateway accepts the call setup message but does not allow the call to complete. At a minimum, the following two cases must be tested.

H.323 Proxy – OSP Peering Test Cases

1. The source gateway IP address is not in the IP access list of the first destination gateway. Therefore the destination gateway does not accept the call.
2. The first destination gateway does not have a circuit available to complete the call.

Detailed Description of Test Case

The call scenario diagram above illustrates the H.323 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 H.323 proxy. These call scenarios for the proxy, have two call legs. One inbound call leg is from the source device to the proxy and the second outbound call leg from the proxy to the destination device. Each of these call legs require a message transaction between the proxy 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 proxy. The test case is described in detail below.

1. **Call In.** The call begins at a PTSN trunk on the source H.323 gateway.
2. **Q931 Setup.** The source H.323 gateway sends a Q931 call setup message to the H.323 proxy.
3. **NEW.** The H.323 proxy establishes a new transaction with the OSP client Toolkit using OSPTransactionNew function. Please see the OSP Toolkit Programming Interface document for details on this and other function calls.
4. **ReqAuth(In).** The H.323 proxy calls OSP client Toolkit function OSPPTtransactionRequestAuthorisation.
5. **Auth Req Leg 2.** The OSP client Toolkit 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 gateway.
6. **Auth Rsp Leg 2.** The OSP server sends an OSP AuthorizationResponse to the H.323 proxy. The response includes the IP addresses of two destination gateways, the signaling protocol required by the gateways and the version of OSP supported.
7. **ReqAuth(Out).** The OSP Toolkit responds to the H.323 proxy that the OSPPTtransactionRequestAuthorisation function is complete.
8. **Get1stDst.** The H.323 proxy calls the OSP client Toolkit function OSPPTtransactionGetFirstDestination to get the IP address of the first destination gateway.
9. **GetDstProt.** The H.323 proxy calls the OSP client Toolkit function OSPPTtransactionGetDestProtocol to get the signaling protocol required by the destination device. In this case, the DestinationProtocol is H323-Q931.
10. **IsDstOSPEnabled.** The H.323 proxy calls the OSP client Toolkit function OSPPTtransactionIsDestOSPEnabled to get the version of the OSP standard supported by the destination device. Version 0.0.0 indicates the destination gateway does not

H.323 Proxy – OSP Peering Test Cases

support OSP and that an OSP peering authorization token should not be included in the call setup signal to the destination device.

11. **GetNetworkID.** The H.323 proxy calls the OSP client Toolkit function OSPPGetDestNetworkID to get the destination trunk group (H.323 parameter destinationCarrierID) if it is available.
12. **Q931 Setup.** The H.323 proxy sends a Q931 call setup message to the first destination H.323 gateway. An OSP authorization token is not included in the Q931 setup message since the destination gateway does not support OSP.
13. **Q931 Release Complete.** The destination H.323 device does not accept the Q931 call setup and returns a Q931 release complete to the H.323 proxy. The call may be rejected for a variety of reasons such as unauthorized access or no circuits available.
14. **GetNextDst.** The H.323 proxy prepare to retry the call to a second destination an calls OSP Toolkit function OSPPTTransactionGetNextDestination to obtain the IP address of the next destination gateway.
15. **GetDstProt.** The H.323 proxy gets the destination protocol of the second destination gateway.
16. **IsDstOSPEnabled.** The H.323 proxy call the OSP toolkit to determine the OSP version supported by the destination gateway. For this test case the OSP version is 0.0.0 indicating the destination does not support OSP.
17. **GetNetworkID.** The H.323 proxy calls the OSP client Toolkit function OSPPGetDestNetworkID to get the destination trunk group (H.323 parameter destinationCarrierID) if it is available.
18. - 25. Standard H.323 communications.
26. **RecordFailure.** At the completion of the call, the H.323 proxy reports the call disconnect reason, for all call attempts, to the OSP Toolkit using the OSPPTTransactionRecordFailure function.
27. **RepUsage(In).** The H.323 proxy calls the OSPPTTransactionReportUsage function to report the call duration.
28. **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 H.323 proxy is the source device for the second leg of the call.
29. **Src Usg Cnf Leg 2.** The OSP server responds with an OSP UsageConfirmation message.
30. **RepUsage(Out).** The OSP Toolkit closes the ReportUsage transaction.
31. **TransDelete.** The H.323 proxy deletes the OSP Toolkit transaction.

Expected CDRs for Test Case 2.1.1

This test case should generate two OSP UsageIndication messages, or CDRs, from the H.323 proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the first call attempt should be the response from Dst-GW1.

H.323 Proxy – OSP Peering Test Cases

In this example, the response is 21, but other responses are also valid. For the successful retry call, the proxy should set the FailureReason to 16 or 1016.

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

Expected OSP Messages for Test Case 2.1.1

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

Auth Req Leg 2 (generated by OSPPTTransactionRequestAuthorisation)

```
<?xml version="1.0"?>
<Message messageId="3964120231" random="396412023">
<AuthorizationRequest componentId="3964120230">
<Timestamp>2006-03-08T20:13:12Z</Timestamp>
<CallId encoding="base64">Call ID</CallId>
<SourceInfo type="e164">Calling Number</SourceInfo>
<DeviceInfo type="transport">[Src-GW IP Address]</DeviceInfo>
<SourceAlternate type="transport">[Proxy IP Address]</SourceAlternate>
<SourceAlternate type="network">Partition</SourceAlternate>
<DestinationInfo type="e164">Called Number</DestinationInfo>
<Service/>
<MaximumDestinations>3</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-GW IP Address
<SourceAlternate type="transport">	Source	Proxy IP Address
<SourceAlternate type="network">	NetworkId	Partition or trunk group
<DestinationInfo type="e164">	CalledNumber	
<MaximumDestinations>	NumberOfDestinations	Maximum number of possible destinations requested.

Auth Rsp Leg 2 (response from OSP server)

```
<?xml version='1.0'?>
<Message messageId='3964120231' random='31098'>
<AuthorizationResponse componentId='3964120230'>
<Timestamp>2006-03-08T20:13:12Z</Timestamp>
<Status>
<Description>SUCCESS</Description>
<Code>200</Code>
</Status>
<TransactionId>Transaction ID</TransactionId>
<Destination>
<CallId encoding='base64'>Call ID</CallId>
<DestinationInfo type='e164'>Called Number</DestinationInfo>
<DestinationSignalAddress>[Dst-GW1 IP Address]</DestinationSignalAddress>
```

H.323 Proxy – OSP Peering Test Cases

```

<Token encoding='base64'>OSP Token</Token>
<UsageDetail>
<Amount>60</Amount>
<Increment>1</Increment>
<Service/>
<Unit>s</Unit>
</UsageDetail>
<ValidAfter>2006-03-08T20:08:12Z</ValidAfter>
<ValidUntil>2006-03-08T20:18:12Z</ValidUntil>
<DestinationProtocol critical='False'>h323-Q931</DestinationProtocol>
<OSPVersion critical='False'>0.0.0</OSPVersion>
<SourceInfo type='e164' critical='False'>Calling Number</SourceInfo>
<DestinationAlternate type='network' critical='False'></DestinationAlternate>
</Destination>
<Destination>
<CallId encoding='base64'>Call ID</CallId>
<DestinationInfo type='e164'>Called Number</DestinationInfo>
<DestinationSignalAddress>[Dst-GW2 IP Address]</DestinationSignalAddress>
<Token encoding='base64'>OSP Token</Token>
<UsageDetail>
<Amount>60</Amount>
<Increment>1</Increment>
<Service/>
<Unit>s</Unit>
</UsageDetail>
<ValidAfter>2006-03-08T20:08:12Z</ValidAfter>
<ValidUntil>2006-03-08T20:18:12Z</ValidUntil>
<DestinationProtocol critical='False'>h323-Q931</DestinationProtocol>
<OSPVersion critical='False'>0.0.0</OSPVersion>
<SourceInfo type='e164' critical='False'>Calling Number</SourceInfo>
<DestinationAlternate type='network'
critical='False'></DestinationAlternate>
</Destination>
</AuthorizationResponse>
</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-GW1 IP Address
<Token encoding='base64'>	Token	Authorization token
<Amount>	TimeLimit	Authorized call duration in seconds
<Increment>		Default is 1
<Service>		Default is voice
<Unit>		Default is seconds
<ValidAfter>	ValidAfter	Time after which call is authorized
<ValidUntil>	ValidUntil	Time until which call is authorized
<DestinationProtocol>	DestinationProtocol	VoIP signaling protocol expected by Dst-GW1
<OSPVersion>	DestinationOSPStatus	Version of OSP supported by Dst-GW1
<SourceInfo type='e164'>	CallingNumber	May be translated in AuthResponse

H.323 Proxy – OSP Peering Test Cases

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

Source Usage Ind Leg 2 (generated by OSPPTransactionReportUsage)

```

<?xml version="1.0"?>
<Message messageId="49041890973023273173" random="865742176">
<UsageIndication componentId="49041890973023273172">
<Timestamp>2006-03-08T20:13:22Z</Timestamp>
<Role>source</Role>
<TransactionId>Transaction ID</TransactionId>
<CallId encoding="base64">Call ID</CallId>
<SourceInfo type="e164">Calling Number</SourceInfo>
<DeviceInfo type="transport">[Src-GW IP Address]</DeviceInfo>
<SourceAlternate type="transport">[Proxy IP Address]</SourceAlternate>
<DestinationInfo type="e164">Called Number</DestinationInfo>
<DestinationAlternate type="transport">[Dst-GW1 IP Address]</DestinationAlternate>
<transnexus.com:FailureReason>111</transnexus.com:FailureReason>
</UsageIndication>
<UsageIndication componentId="49041890973023273174">
<Timestamp>2006-03-08T20:13:22Z</Timestamp>
<Role>source</Role>
<TransactionId>Transaction ID</TransactionId>
<CallId encoding="base64">Call ID</CallId>
<SourceInfo type="e164">Calling Number</SourceInfo>
<DeviceInfo type="transport">[Src-GW IP Address]</DeviceInfo>
<SourceAlternate type="transport">[Proxy IP Address]</SourceAlternate>
<DestinationInfo type="e164">Called Number</DestinationInfo>
<DestinationAlternate type="transport">[Dst-GW2 IP Address]</DestinationAlternate>
<UsageDetail>
<Amount>10</Amount>
<Increment>1</Increment>
<Unit>s</Unit>
<StartTime>2006-03-08T20:13:12Z</StartTime>
<EndTime>2006-03-08T20:13:22Z</EndTime>
<AlertTime>2006-03-08T20:13:12Z</AlertTime>
<ConnectTime>2006-03-08T20:13:15Z</ConnectTime>
<ReleaseSource>0</ReleaseSource>

```

H.323 Proxy – OSP Peering Test Cases

```

</UsageDetail>
<transnexus.com:FailureReason>0</transnexus.com:FailureReason>
</UsageIndication>
</Message>

```

OSP XML Tag	Toolkit Variable	Note
<Role>		Source CDR for 1st try of call leg 2
<TransactionId>		Transaction ID from OSP server
<CallId encoding="base64">	CallId	CallID from call leg 1 Setup
<SourceInfo type="e164">	CallingNumber	May be translated in AuthResponse
<DeviceInfo type="transport">	SourceDevice	Src-GW IP Address
<SourceAlternate type="transport">	Source	Proxy IP Address
<DestinationInfo type="e164">	CalledNumber	May be translated in AuthResponse
<DestinationAlternate>	Destination	Dst-GW1 IP Address
<Role>		Source CDR for 2nd 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-GW IP Address
<SourceAlternate type="transport">	Source	Proxy IP Address
<DestinationInfo type="e164">	CalledNumber	May be translated in AuthResponse
<DestinationAlternate>	Destination	Dst-GW2 IP Address
<Amount>	Duration	Call duration in seconds
<Increment>		Default is 1
<Unit>		Default is seconds
<StartTime>	StartTime	Time stamp when Setup is sent to the destination device.
<EndTime>	EndTime	Time stamp when ReleaseComplete message is received from source or destination.
<AlertTime>	AlertTime	Time stamp when Processing message is received.
<ConnectTime>	ConnectionTime	Time stamp when Connecting message 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 Usage Cnf Leg 2 (confirmation from OSP server)

```

<?xml version='1.0'?>
<Message messageId='49041890973023273173' random='2873'>
<UsageConfirmation componentId='49041890973023273172'>
<Timestamp>2006-03-08T20:13:22Z</Timestamp>
<Status>
<Description>SUCCESS</Description>
<Code>200</Code>
</Status>
</UsageConfirmation>

```

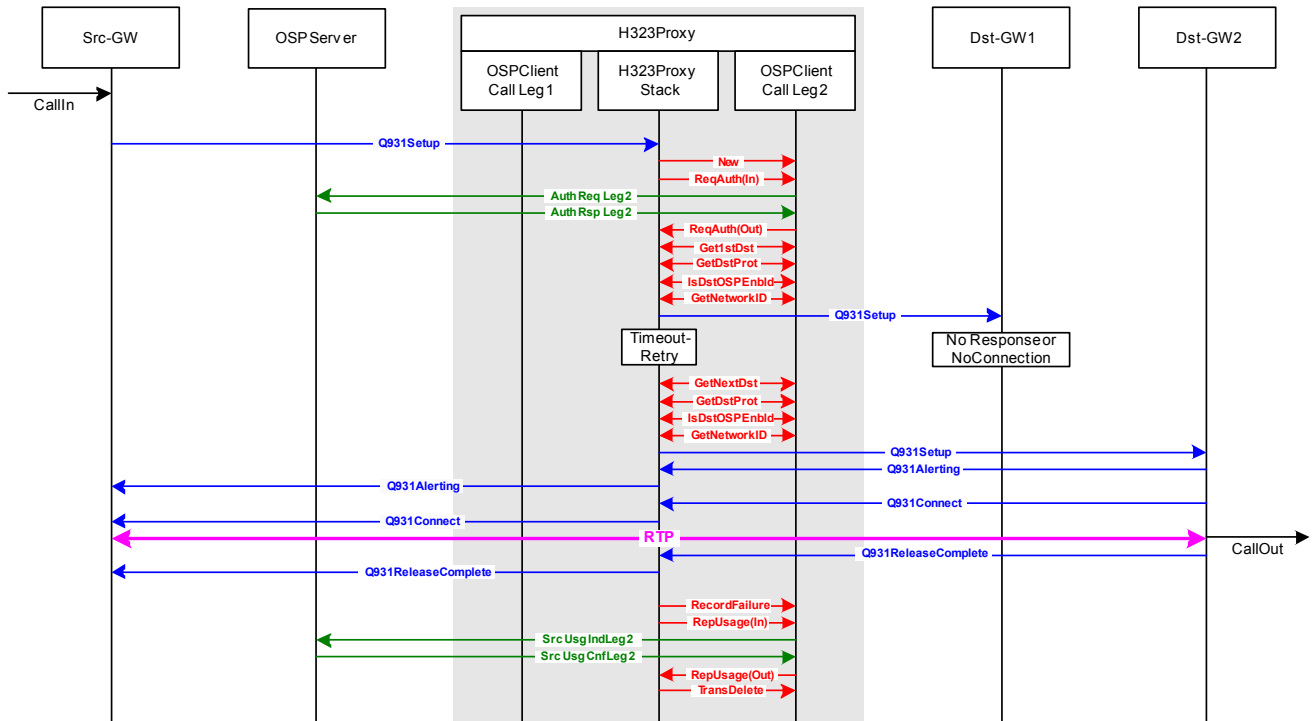
H.323 Proxy – OSP Peering Test Cases

```

<UsageConfirmation componentId='49041890973023273174'>
<Timestamp>2006-03-08T20:13:22Z</Timestamp>
<Status>
<Description>SUCCESS</Description>
<Code>200</Code>
</Status>
</UsageConfirmation>
</Message>

```

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



Test Case 2.1.2: Gateway to Proxy to Gateway - No Response or No Connection and Retry - Proxy Times Out
Legend: H.323 Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

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

1. The H.323 proxy cannot establish a TCP connection with Dst-GW1. After TCP timeout, the proxy should retry call to Dst-GW2. (When OSP Toolkit function OSPPTTransactionGetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 47 – resource unavailable, unspecified.)
2. No route to IP address of Dst-GW1 device. The H.323 proxy should retry call to Dst-GW2. (When OSP Toolkit function OSPPTTransactionGetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 2 – no route to specified transit network.)

H.323 Proxy – OSP Peering Test Cases

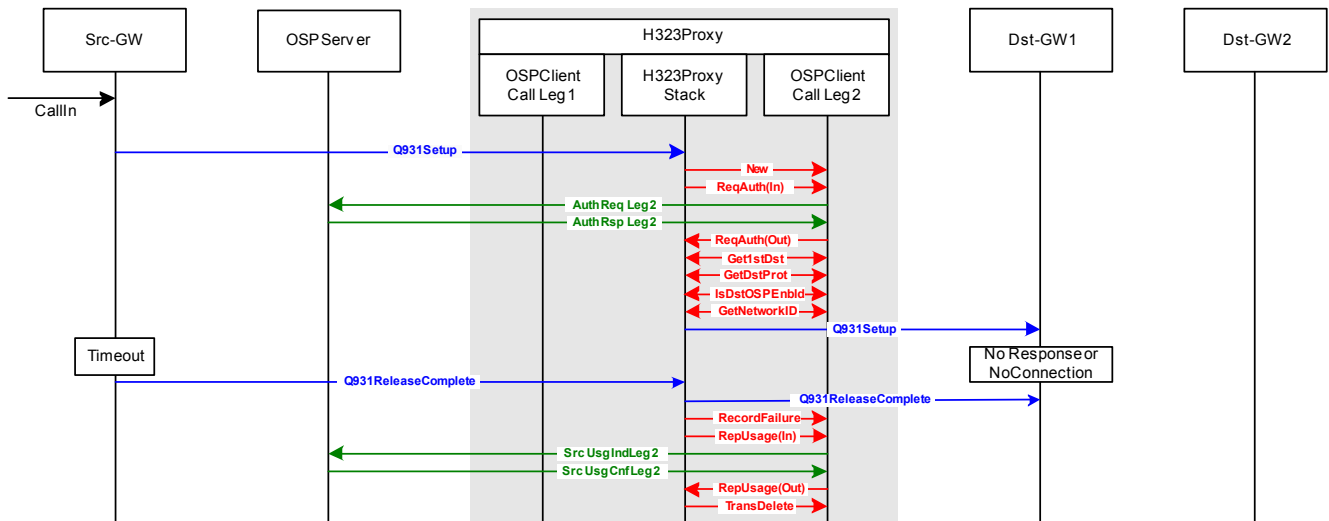
3. TCP connection refused by destination, Dst-GW1. After TCP connection is refused, the H.323 proxy should retry the call to Dst-GW2. (When OSP Toolkit function OSPPTtransactionGetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 63 – service or option not available, unspecified.)
4. No response from Dst-GW1. The H.323 proxy establishes TCP connection with Dst-GW1, but Dst-GW1 never responds to Setup. The proxy should time-out and retry the call to Dst-GW2. (When OSP Toolkit function OSPPTtransactionGetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 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 H.323 proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the first call attempt should be determined by the proxy based on the reason for the failure. For the successful retry call, the proxy should set the FailureReason to 16 or 101.

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

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



Test Case 2.1.3: Gateway to Proxy to Gateway - No Response or No Connection - Source Times Out
Legend: H.323 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-GW1 responds to the Setup from the H.323 proxy. In these cases, the proxy should terminate the call and report usage to the OSP server. The OSP Toolkit parameter

H.323 Proxy – OSP Peering Test Cases

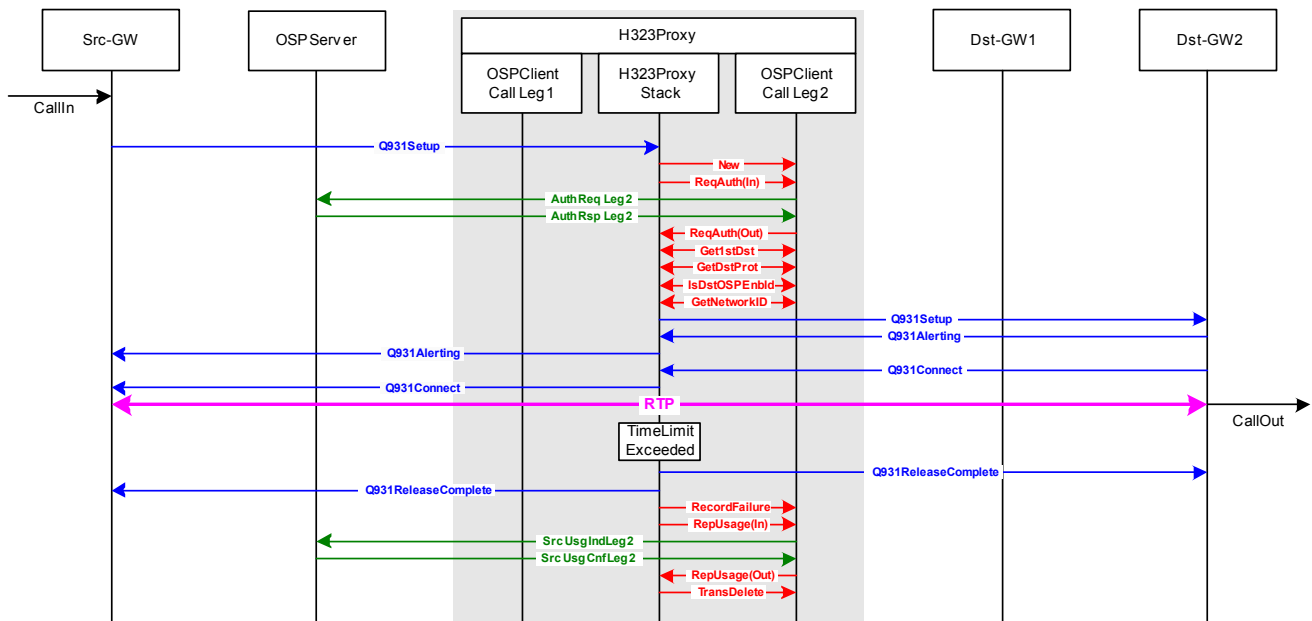
FailureReason reported with the OSPTransactionRecordFailure function should be set to the release cause reported in the ReleaseComplete from the source device, Src-GW.

Expected CDRs for Test Case 2.1.3

This test case should generate one OSP UsageIndication message, or CDR, from the H.323 proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the call should be determined by the release reason included in the ReleaseComplete message from Src-GW.

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

2.1.4. Call Duration Limit Exceeded



Test Case 2.1.4: Gateway to Proxy to Gateway - Call Time Limit Exceeded
Legend: H.323 Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

This call scenario tests the H.323 proxy's ability to end a call when its authorized call duration has been exceeded. In the AuthorizationResponse, the OSP server includes the authorized call duration. The OSP Toolkit parameter TimeLimit, returned in the GetFirstDestination or GetNextDestination function calls, defines the maximum duration for each call. The proxy should terminate a call when the call duration exceeds the TimeLimit. In this case, when the proxy forcefully ends a call that has exceeded its maximum call duration, the proxy should use the RecordFailure OSP Toolkit function call to report a FailureReason of 8 (preemption) and then use the ReportUsage OSP Toolkit function call to send a UsageIndication call detail record to the OSP server.

Expected CDRs for Test Case 2.1.4

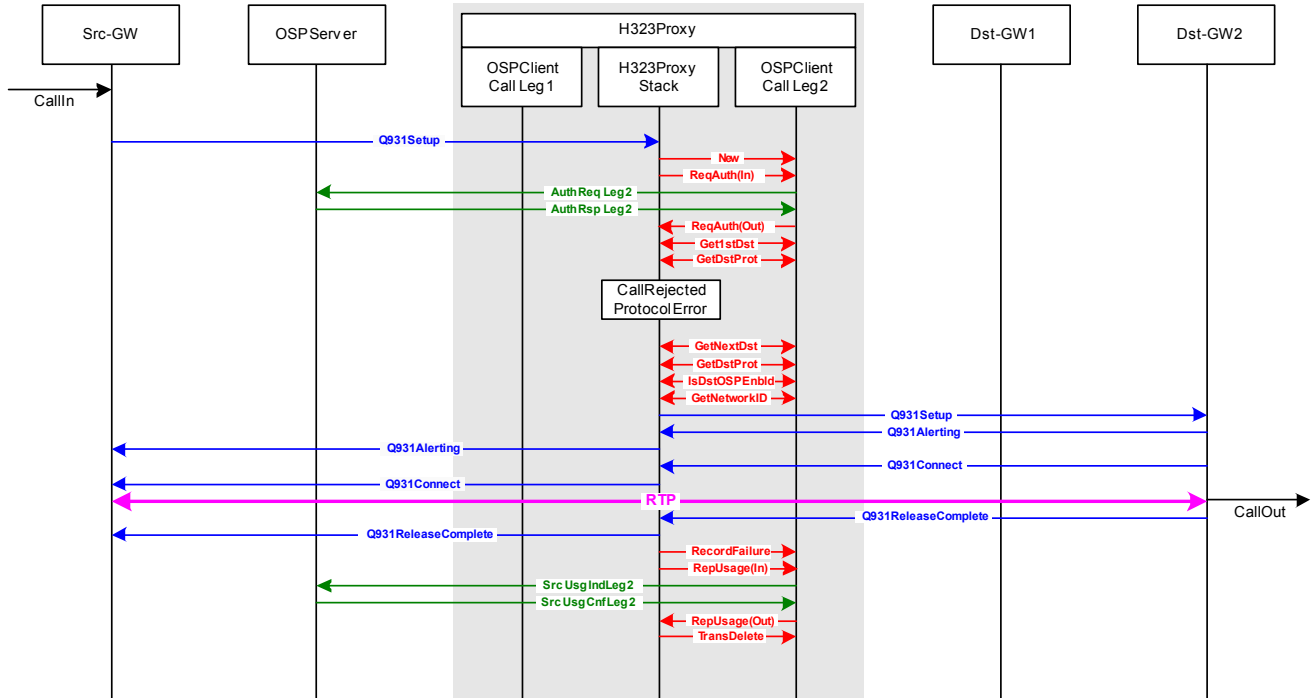
This test case should generate one OSP UsageIndication message, or CDR, from the H.323 proxy as the source of call leg 2. The release reason (ospvFailureReason), or

H.323 Proxy – OSP Peering Test Cases

termination cause code, for the call should be set by the proxy to 8 to indicate the call was forcefully shutdown by the proxy.

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

2.1.5. Call Rejected – Protocol Error and Retry



Test Case 2.1.5: Gateway to Proxy to Gateway - Call Rejected Protocol Error & Retry
Legend: H.323 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 H.323 proxy, such as SIP, H323_LRQ, or IAX. When this occurs, the proxy should reject the destination, record FailureReason 111 (protocol error), and retry the call to the next destination if it is available.

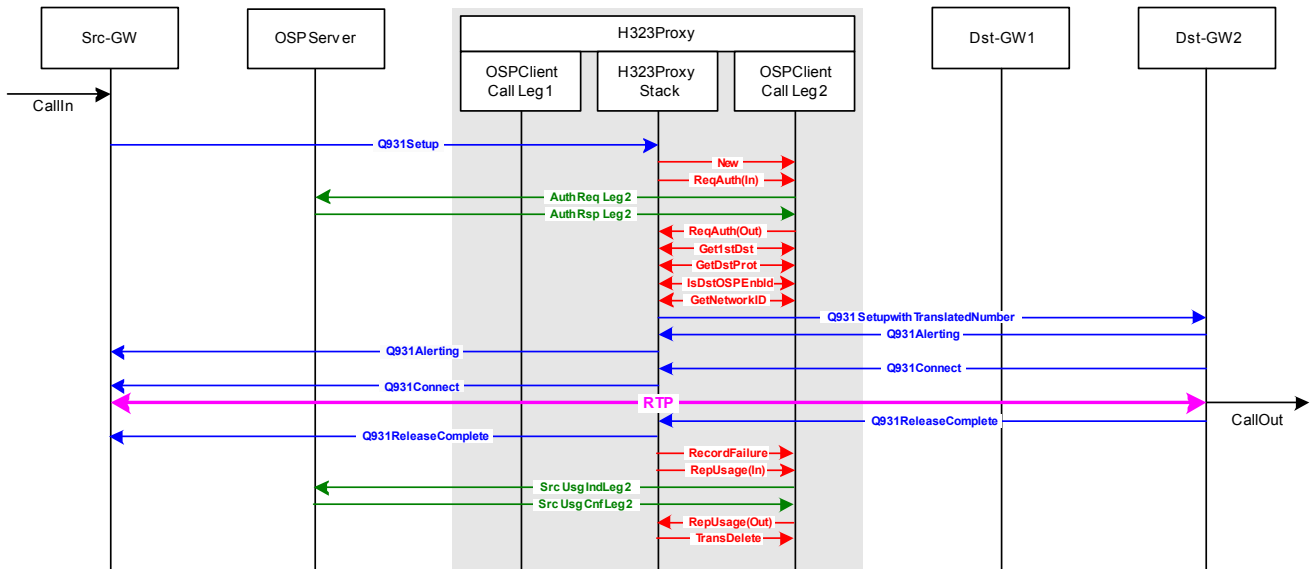
For this test case, the destination protocol for device Dst-GW1 is NOT configured as H323_Q931 on the OSP server. The OSPTransactionGetDestProtocol function call returns a DestinationProtocol incompatible with H323_Q931. The proxy should recognize the protocol error, reject the destination and record FailureReason 111. Note, if the DestinationProtocol is unknown or undefined, the proxy should assume the destination device supports H323_Q931 and send a call setup message 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-GW	Dst-GW1	111	0
2	source	Src-GW	Dst-GW2	16 or 1016	greater than 0

H.323 Proxy – OSP Peering Test Cases

2.1.6. Number Translation



Test Case 2.1.6: Gateway to Proxy to Gateway - Number Translation
Legend: H.323 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 H.323 proxy. When this occurs, the called and calling numbers in the call setup message from the proxy to the destination gateway should be the translated called and calling numbers from the OSP AuthorizationResponse.

For this test case, the OSP server should be configured to translate the called and calling numbers. The OSPPTTransactionGetFirstDestination function call returns the translated called and calling numbers. The proxy should send a call setup message with the translated numbers to the destination. The OSPPTTransactionReportUsage function should report the original (un-translated) called and calling numbers from the call setup message from the source (Src-GW).

Expected CDRs for Test Case 2.1.6

This test case should generate one OSP UsageIndication message, or CDR, from the H.323 proxy as the source of call leg 2. The called and calling numbers reported in the OSP UsageIndication message from the proxy, should be the called and calling numbers from the Setup received from the source gateway in call leg 1. The translated called and calling numbers should not be reported in the OSP UsageIndication message.

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

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

H.323 Proxy – OSP Peering Test Cases

2.2. non-OSP Source to OSP Destination

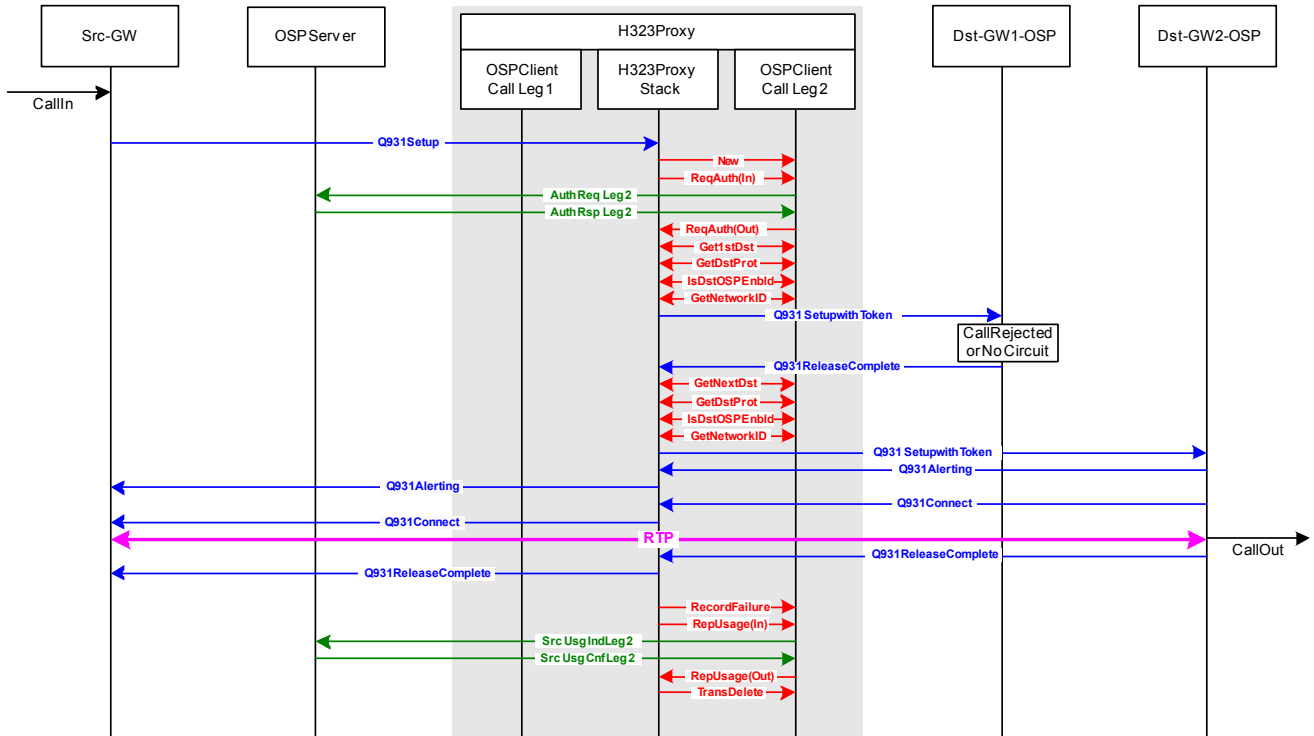
This section of cases tests call scenarios when the destination is an OSP enabled H.323 device. In these call scenarios, the H.323 proxy must include the OSP peering token, returned in the OSP AuthorizationResponse, in the Q931 call setup message to the destination device. The destination device, which must be enrolled with the OSP server, will extract the token from the call setup message and validate that the token was digitally signed by the OSP server. If the token is valid, the destination device will accept the call. If not, the Setup will be rejected by the destination 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 proxy should allow for call attempt retries to multiple destination devices and the list of destination devices may be any combination of non-OSP and OSP enabled devices.

Configuration of VoIP devices on OSP server for test cases in section 2.2		
Device	Destination Protocol	OSP Version
Src-GW	H323-Q931	0.0.0 (Not OSP Enabled)
H.323 Proxy	H323-Q931	2.1.1 or 4.1.1
Dst-GW1-OSP	H323-Q931	1.3.4, 2.1.1 or 4.1.1
Dst-GW2-OSP	H323-Q931	1.3.4, 2.1.1 or 4.1.1

H.323 Proxy – OSP Peering Test Cases

2.2.1. Call Rejected or No Circuit and Retry



Test Case 2.2.1: Gateway to Proxy to Gateway OSP - Call Rejected or No Circuit & Retry
Legend: H.323 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 OSPPTTransactionRequestAuthorization function should be included in the Setup to the destination.

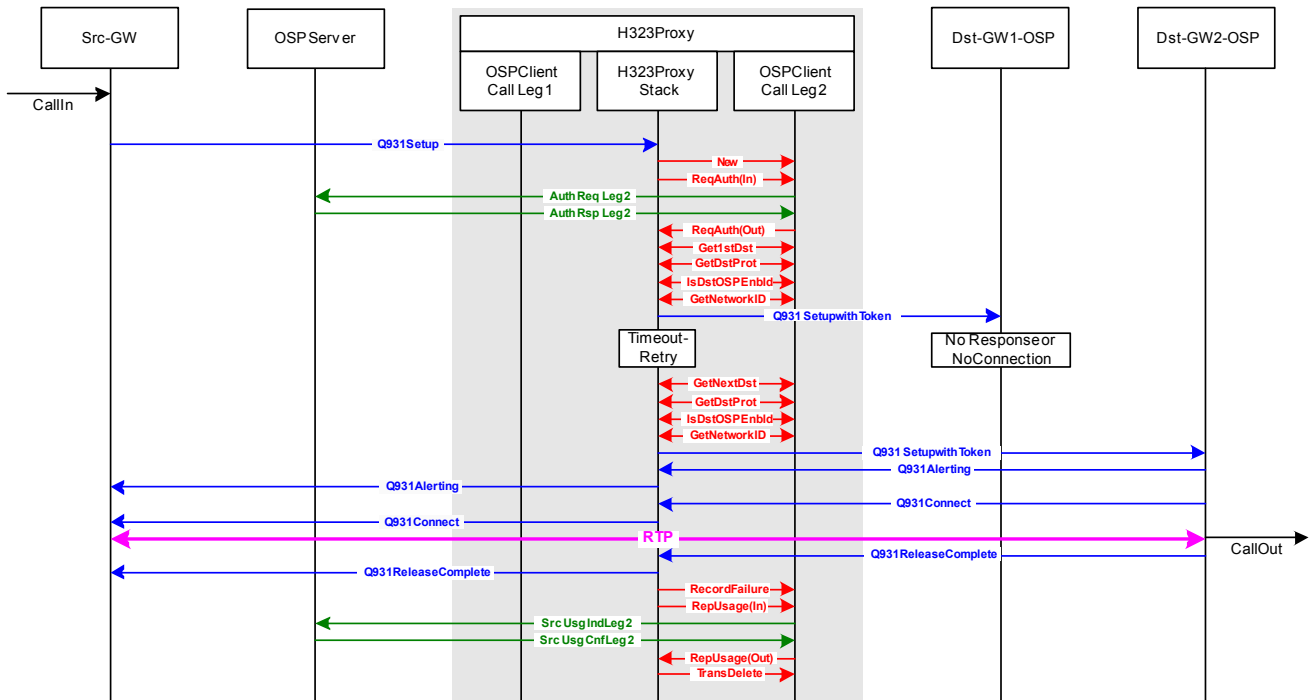
Expected CDRs for Test Case 2.2.1

This test case should generate two OSP UsageIndication messages, or CDRs, from the H.323 proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the first call attempt should be the response from Dst-GW1-OSP. In this example, the response is 21, but other responses are also valid. For the successful retry call, the proxy should set the FailureReason to 16 or 1016.

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

H.323 Proxy – OSP Peering Test Cases

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



Test Case 2.2.2: Gateway to Proxy to Gateway OSP - No Response or No Connection & Retry - Proxy Times Out
Legend: H.323 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 call setup message from the H.323 proxy to the destination.

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

1. The H.323 proxy cannot establish a TCP connection with Dst-GW1-OSP. After TCP time-out, the proxy should retry call to Dst-GW2-OSP. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 47 – resource unavailable, unspecified.)
2. No route to IP address of Dst-GW1-OSP device. The H.323 proxy should retry call to Dst-GW2-OSP. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 2 – no route to specified transit network.)
3. TCP connection refused by destination. After TCP connection is refused, the proxy should retry the call to Dst-GW2-OSP. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the

H.323 Proxy – OSP Peering Test Cases

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

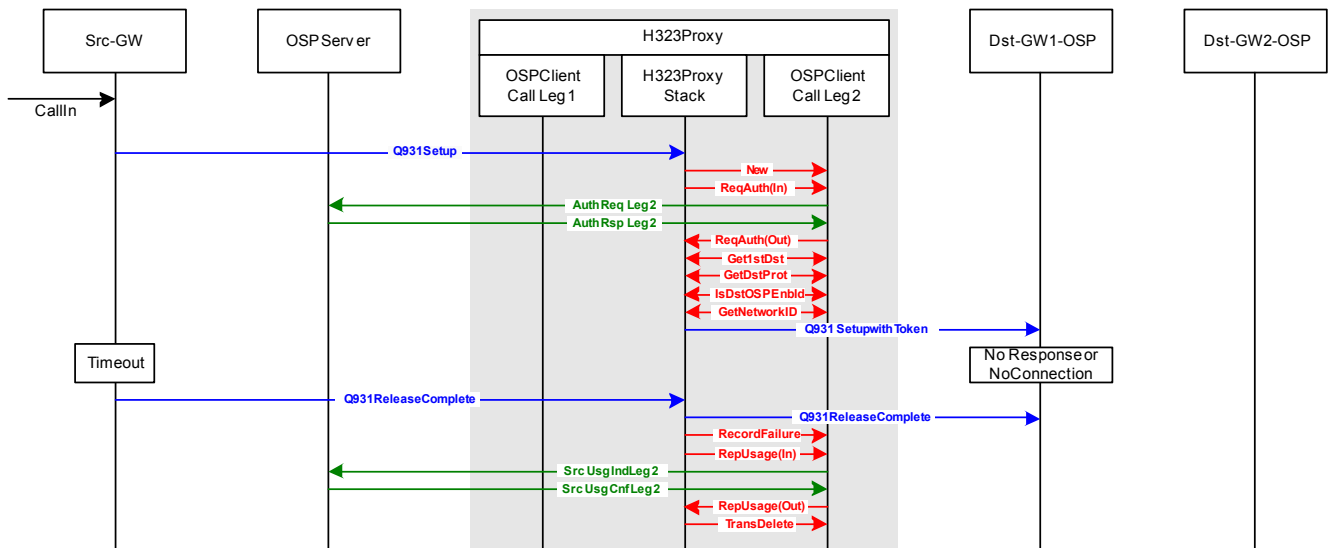
- No response from Dst-GW1-OSP device. The proxy establishes TCP connection with Dst-GW1-OSP, but DST-GW1-OSP never responds to Setup. The H.323 proxy should time-out and retry the call to Dst-GW2-OSP. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 27 – destination out of order.)

Expected CDRs for Test Case 2.2.2

This test case should generate two OSP UsageIndication messages, or CDRs, from the H.323 proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the first call attempt should be determined by the proxy based on the reason for the failure. For the successful retry of call leg 2, the proxy should set the FailureReason to 16 or 1016.

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

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



Test Case 2.2.3: Gatewayto Proxyto Gateway OSP- No Response or No Connection - Source Times Out
Legend: H.323 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 OSPPTTransactionRequestAuthorization function should be included in the call setup message from the H.323 proxy to the destination.

This case tests the call scenario when the source ends the call before the first destination Dst-GW1-OSP responds to the Setup from the H.323 proxy. In these cases, the proxy should terminate the call and report usage to the OSP server. The OSP Toolkit parameter FailureReason reported with the OSPPTTransactionRecordFailure function should be set

H.323 Proxy – OSP Peering Test Cases

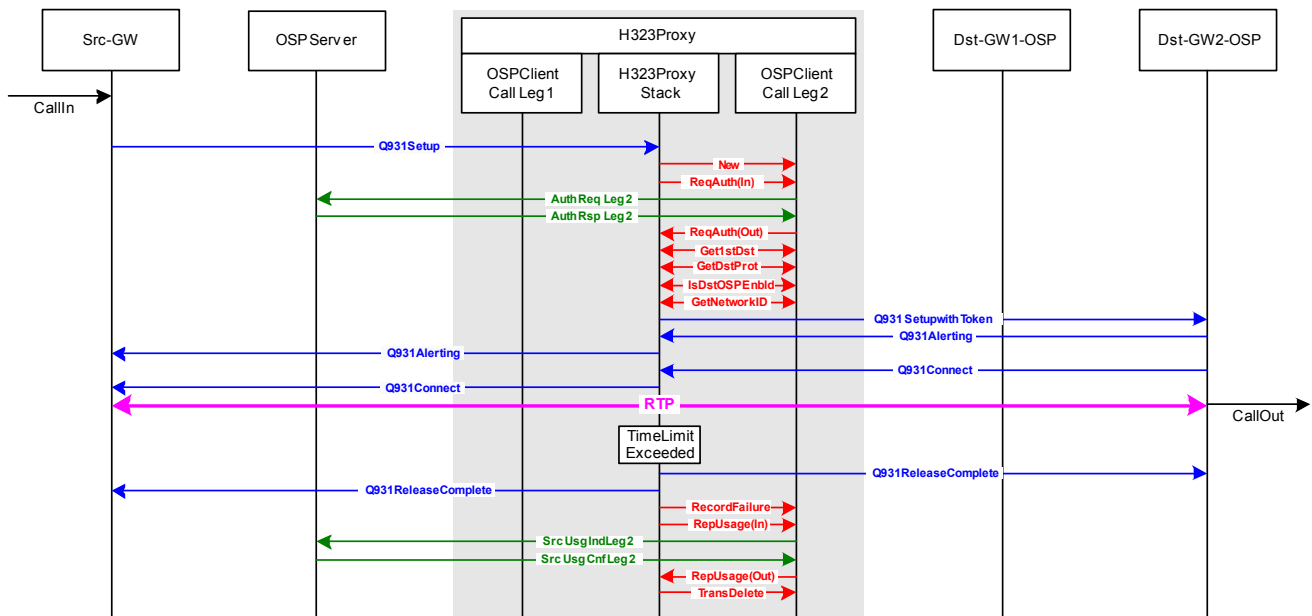
to the release cause reported in the ReleaseComplete message from the source device, Src-GW.

Expected CDRs for Test Case 2.2.3

This test case should generate one OSP UsageIndication message, or CDR, from the H.323 proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the call attempt should be determined by the release reason included in the ReleaseComplete message from Src-GW.

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

2.2.4. Call Duration Limit Exceeded



Test Case 2.2.4: Gateway to Proxy to Gateway OSP - Time Limit Exceeded
Legend: H.323 Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

This test case is identical to test case 2.1.4 except that the OSP token returned in OSPTransactionRequestAuthorization function should be included in the Setup message to the destination.

This call scenario tests the H.323 proxy's ability to end a call when its authorized call duration has been exceeded. In the AuthorizationResponse, the OSP server includes the authorized call duration. The OSP Toolkit parameter ospvTimeLimit, returned in the GetFirstDestination or GetNextDestination function calls, defines the maximum duration for each call. The proxy should terminate a call when the call duration exceeds the TimeLimit. In this case, when the proxy forcefully ends a call that has exceeded its maximum call duration, the proxy should use the RecordFailure OSP Toolkit function call to report a FailureReason of 8 (preemption) and then use the ReportUsage OSP Toolkit function call to send a UsageIndication call detail record to the OSP server.

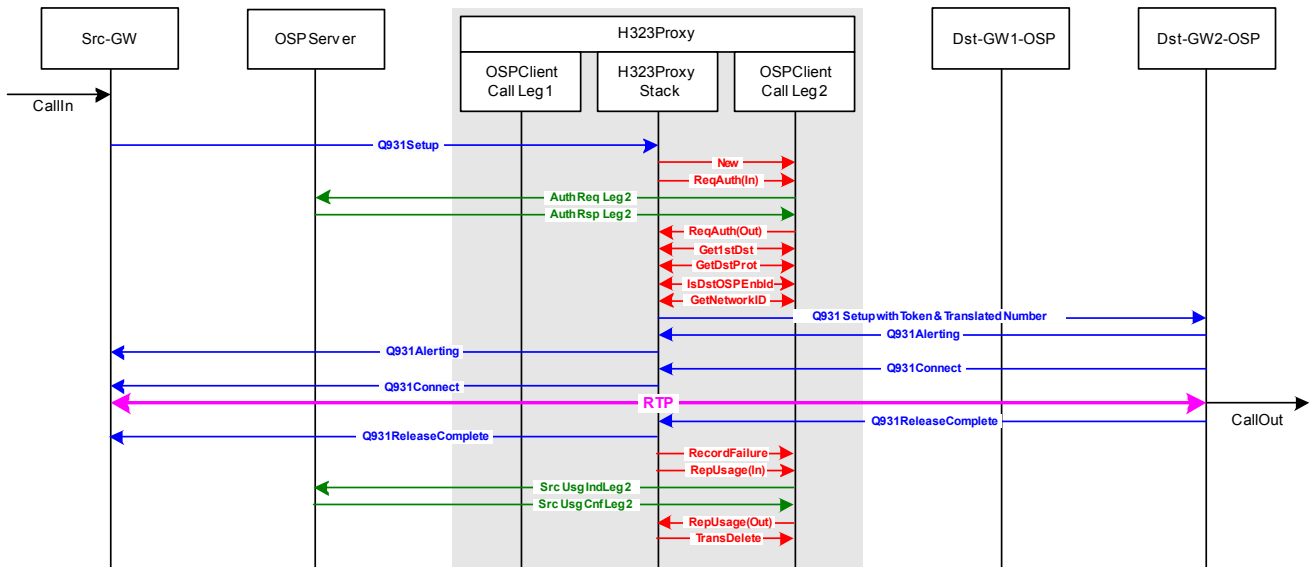
H.323 Proxy – OSP Peering Test Cases

Expected CDRs for Test Case 2.2.4

This test case should generate one OSP UsageIndication message, or CDR, from the H.323 proxy as the source of call leg 2. The release reason (ospvFailureReason), or termination cause code, for the call should be set by the proxy to 8 to indicate the call was forcefully shutdown by the proxy.

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

2.2.5. Number Translation



Test Case 2.2.5: Gateway to Proxy to Gateway OSP - Number Translation
Legend: H.323 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 Setup message to the destination.

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

For this test case, the OSP server should be configured to translate the called and calling numbers. The OSPPTTransactionGetFirstDestination function call returns the translated called and calling numbers. The OSPPTTransactionReportUsage function should report the un-translated (original) called and calling numbers.

This test case should generate one OSP UsageIndication message, or CDR, from the H.323 proxy as the source of call leg 2. The called and calling numbers reported in the OSP UsageIndication message from the proxy, should be the called and calling numbers from the call setup message the H.323 proxy received from the source gateway in call leg

H.323 Proxy – OSP Peering Test Cases

1. The translated called and calling numbers should not be reported in the OSP UsageIndication message.

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

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

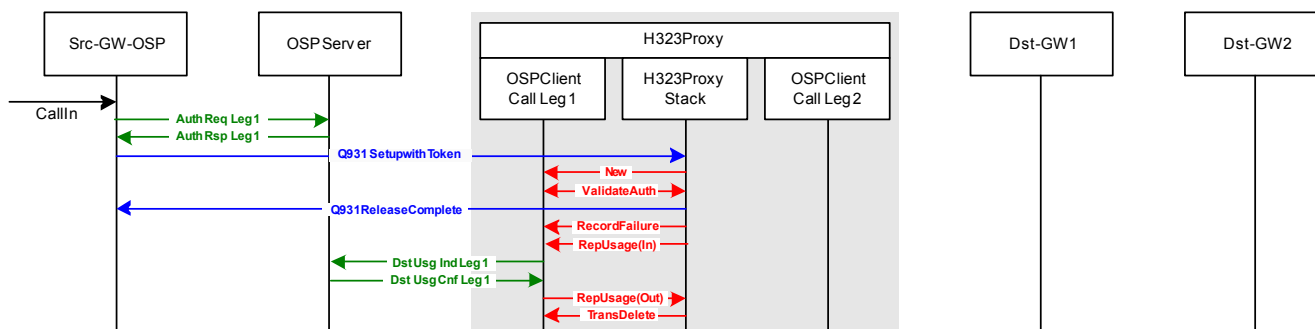
H.323 Proxy – OSP Peering Test Cases

2.3. OSP Source and non-OSP Destination

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

Configuration of VoIP devices on OSP server for test cases in section 2.3		
Device	Destination Protocol	OSP Version
Src-GW-OSP	H323-Q931	1.3.4, 2.1.1 or 4.1.1
H.323 Proxy	H323-Q931	2.1.1 or 4.1.1
Dst-GW1	H323-Q931	0.0.0 (Not OSP Enabled)
Dst-GW2	H323-Q931	0.0.0 (Not OSP Enabled)

2.3.0. Invalid Authorization Token



Test Case 2.3.0: Gateway OSP to Proxy to Gateway - Invalid Authorization Token
Legend: H.323 Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

In this test case, the OSP peering token included in the Q931 call setup message cannot be validated by the H.323 proxy. The token could be invalid for different reasons such as: the token contents or digital signature has been corrupted, the token has expired, the token is not signed or the proxy does not have the public key of the OSP server that signed the authorization token (the public key is used to validate the digital signature). The proxy responds to the source that the call is forbidden and then performs the OSP Toolkit function calls OSPTransactionRecordFailure and OSPTransactionReportUsage to create an OSP destination UsageIndication Call Detail Record which is sent to the OSP server. The FailureReason for this call should be 21.

Expected CDR for Test Case 2.3.0

This test case should generate one OSP UsageIndication message, or CDR, from the H.323 proxy as the destination of call leg 1. The release reason (ospvFailureReason), or termination cause code, for the call should be set by the proxy to 21 to indicate the authorization token was invalid.

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

H.323 Proxy – OSP Peering Test Cases

the call processing continues. If the token was not valid, the H.323 proxy would end the transaction with the OSP Toolkit and reject the call.

7. **GetLookAhead.** The H.323 proxy calls the OSP client Toolkit function OSPPTtransactionGetLookAhead to determine if routing information for the second call leg was embedded in the OSP token. In this test case, no Look Ahead routing information is included in the token and the inter-working proxy must query the OSP server for a destination gateway to complete the second call leg. (Subsection 2.3.5 provides an explanation of Look Ahead routing.)
8. - 34. Messages and OSP Toolkit function calls for the second call leg from the inter-working proxy to the destination device. See subsection 2.1.2 for a detailed description.
35. **RecordFailure.** This refers to the second RecordFailure OSP Toolkit call shown in the test case illustration when the H.323 proxy reports the call termination cause for the first call leg to the OSP Toolkit.
36. **RepUsage(In).** The H.323 proxy reports call duration to the OSP Toolkit using the OPPTtransactionReportUsage function call.
37. **Dst Usg Ind Leg 1.** The OSP client reports an OSP UsageIndication message to the OSP server. This call detail record is destination CDR for the first call leg.
38. **Dst Usg Cnf Leg 1.** The OSP server confirms receipt of the OSP UsageIndication message with a UsageConfirmation message.
39. **RepUsage(Out).** The OSP client closes the OPPTtransactionReportUsage function.
40. **TransDelete.** The H.323 proxy deletes the OSP Toolkit transaction.

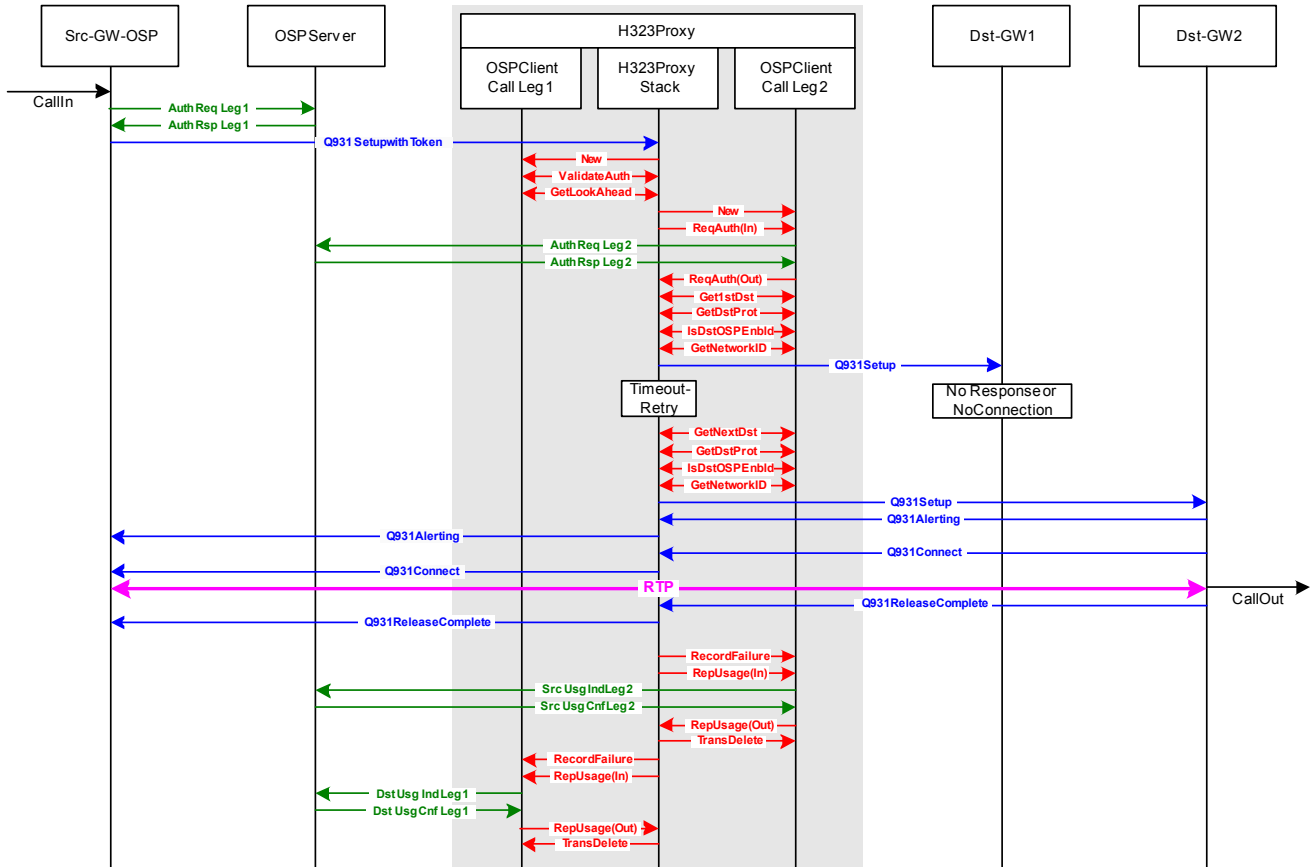
Expected CDRs for Test Case 2.3.1

This test case should generate three OSP UsageIndication messages, or CDRs, from the H.323 proxy. Two CDRs as the source of call leg 2 and one CDR as the destination of call leg 1. The release reason (ospvFailureReason) in the source CDR for call leg 2 for the first call attempt should be the response from DST-GW1. In this example, the response is 21, but other responses are also valid. For the successful retry for call leg 2, the proxy should set the FailureReason to 16 or 1016 in the source CDR. For the destination CDR for call leg 1, the FailureReason should also be set to 16 or 1016 by the proxy.

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

H.323 Proxy – OSP Peering Test Cases

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



Test Case 2.3.2: Gateway OSP to Proxy to Gateway - No Response or No Connection and Retry - Proxy Times Out
Legend: H.323 Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

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

1. The H.323 proxy cannot establish a TCP connection with Dst-GW1. After TCP timeout, the proxy should retry call to Dst-GW2. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 47 – resource unavailable, unspecified.)
2. No route to IP address of Dst-GW1 IP device. The H.323 proxy should retry call to Dst-GW2. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 2 – no route to specified transit network.)
3. TCP connection refused by destination Dst-GW1. After TCP connection is refused, the H.323 proxy should retry the call to Dst-GW2. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the

H.323 Proxy – OSP Peering Test Cases

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

4. No response from Dst-GW1. The H.323 proxy establishes TCP connection with Dst-GW1, but DST-GW1 never responds to the Q931 call setup message. The proxy should time-out and retry the call to Dst-GW2. (When OSP Toolkit function GetNextDestination is called to retry the call to the second destination, the FailureReason for the first call attempt should be set to 27 – destination out of order.)

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

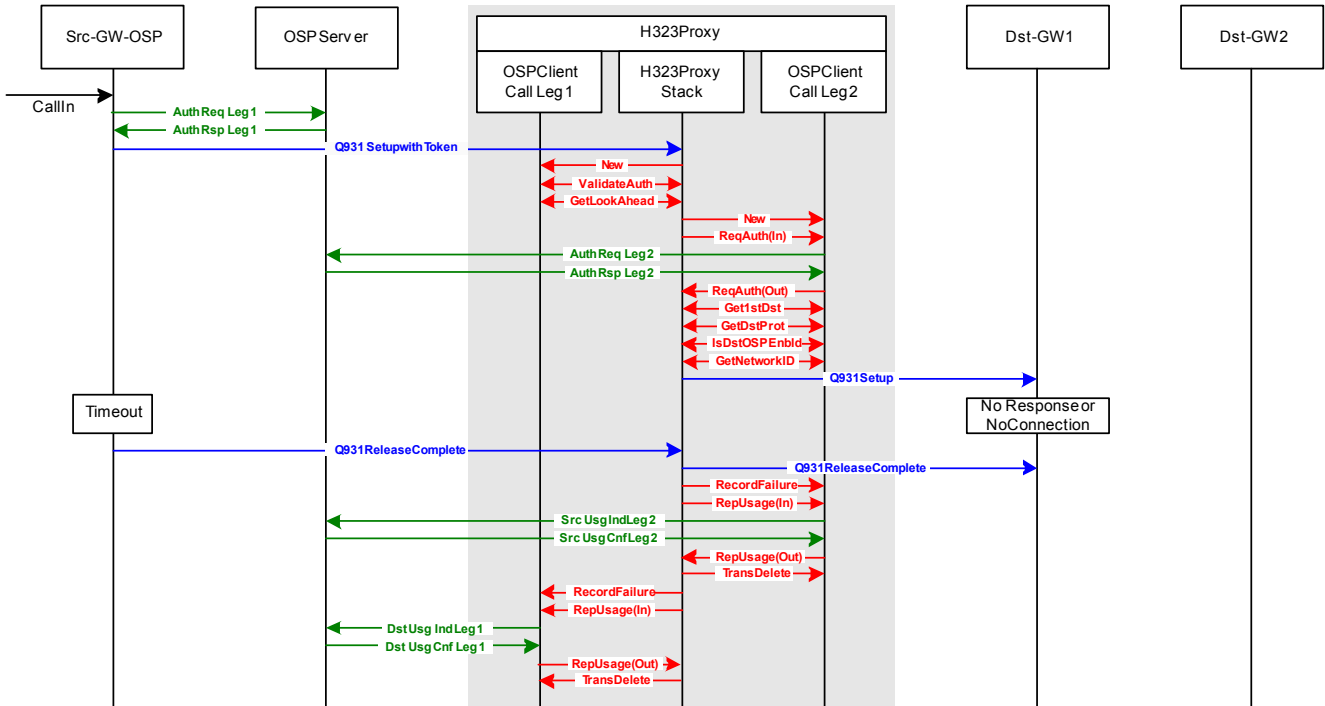
Expected CDRs for Test Case 2.3.2

This test case should generate three OSP UsageIndication messages, or CDRs, from the H.323 proxy. Two CDRs created as the source of call leg 2 and one CDR as the destination of call leg 1. The release reason (ospvFailureReason), or termination cause code, for the first attempt of call leg 2 should be determined by the proxy based on the reason for the failure. For the successful retry of call leg 2, the proxy should set the FailureReason to 16 or 1016. The FailureReason for the destination CDR of call leg 1 should be 16 or 1016.

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

H.323 Proxy – OSP Peering Test Cases

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



Test Case 2.3.3: Gateway OSP to Proxy to Gateway - No Response or No Connection - Source Times Out
Legend: H.323 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-GW1 responds to the Setup from the H.323 proxy. In these cases, the proxy should terminate the call and report usage to the OSP server. The OSP Toolkit parameter FailureReason reported with the OSPPTTransactionRecordFailure function should be set to the release cause reported in the ReleaseComplete message from the source device, Src-GW-OSP. 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.

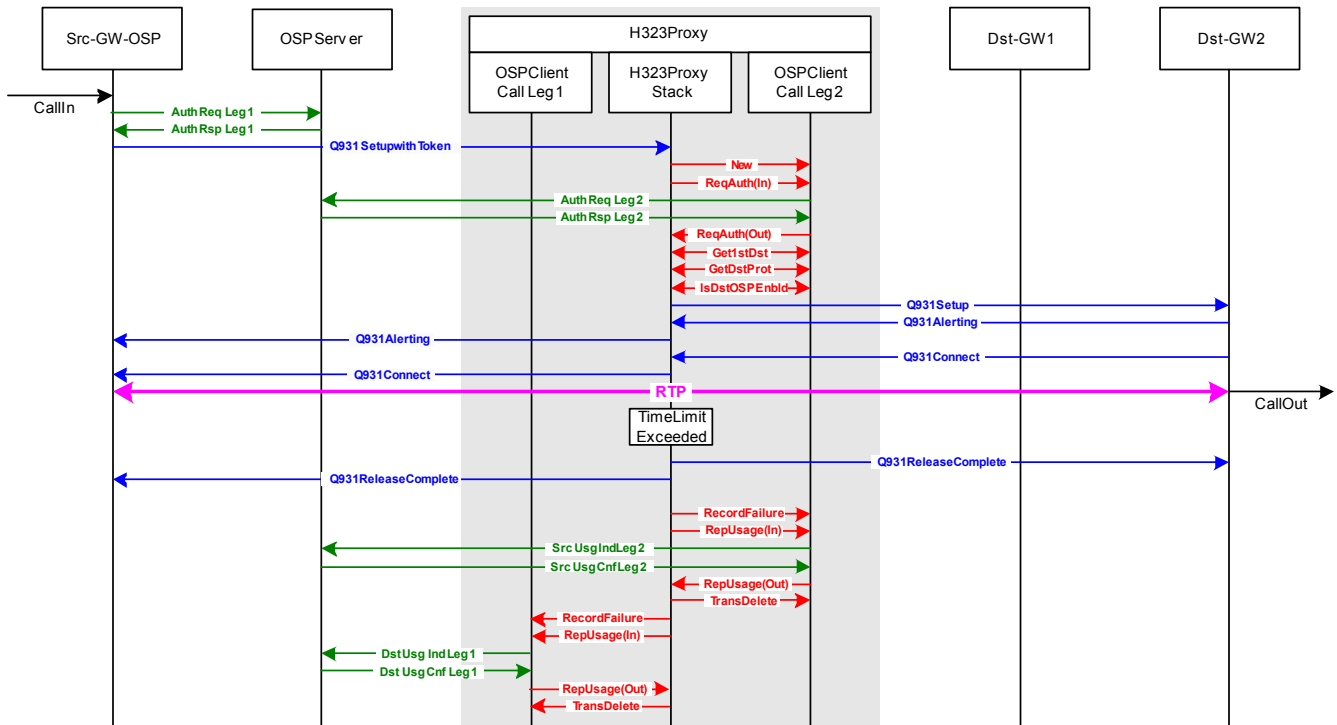
Expected CDRs for Test Case 2.3.3

This test case should generate two OSP UsageIndication messages, or CDRs, from the H.323 proxy. One CDR as the source of call leg 2 and another as the destination of call leg 1. The release reason (ospvFailureReason), or termination cause code, for the CDRs should be determined by the release reason included in the ReleaseComplete message from Src-GW-OSP.

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

H.323 Proxy – OSP Peering Test Cases

2.3.4. Call Duration Limit Exceeded



Test Case 2.3.4: Gateway OSP to Proxy to Gateway - Time Limit Exceeded
Legend: H.323 Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

This call scenario tests the H.323 proxy's ability to end a call when its authorized call duration has been exceeded. In the AuthorizationResponse, the OSP server includes the authorized call duration. The OSP Toolkit parameter `ospvTimeLimit`, returned in the `GetFirstDestination` or `GetNextDestination` function calls, defines the maximum duration for each call. The proxy should terminate a call when the call duration exceeds the `TimeLimit`. In this case, when the proxy forcefully ends a call that has exceeded its maximum call duration, the proxy should use the `RecordFailure` OSP Toolkit function call to report a `FailureReason` of 8 (preemption) and then use the `ReportUsage` OSP Toolkit function call to send a `UsageIndication` call detail record to the OSP server.

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

Expected CDRs for Test Case 2.3.4

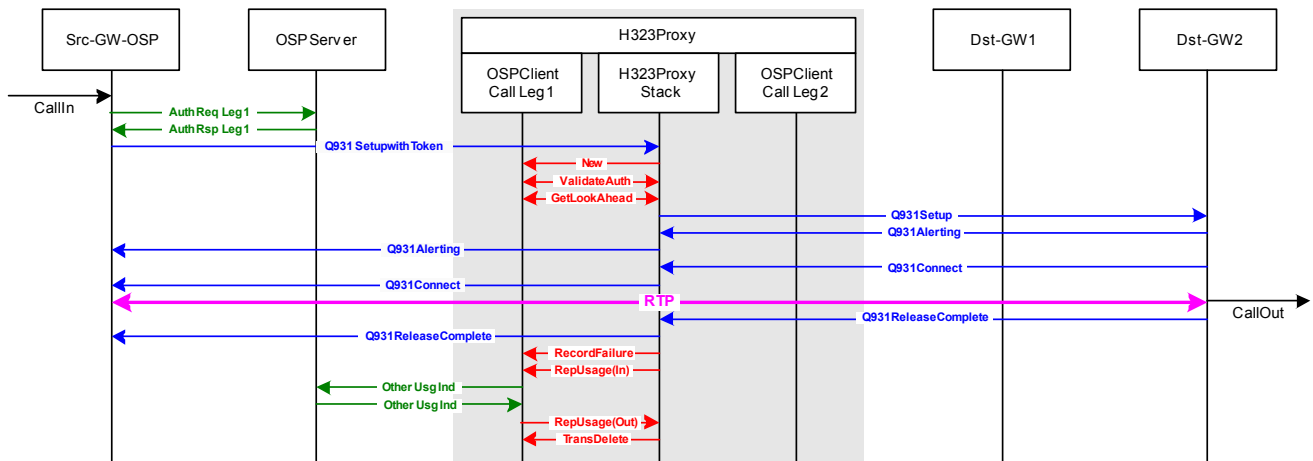
This test case should generate two OSP UsageIndication messages, or CDRs. One from the H.323 proxy as the source of call leg 2 and another as the destination for call leg 1. The release reason (`ospvFailureReason`), or termination cause code, for the call should be set by the proxy to 8 to indicate the call was forcefully shutdown by the proxy.

H.323 Proxy – OSP Peering Test Cases

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

2.3.5. Look Ahead Routing

Look Ahead Routing is a unique OSP application for H.323 proxies. In this test case for Look Ahead Routing, the IP address, destination protocol, OSP version and destination trunk group of the destination device are embedded in the OSP authorization token sent from the source device to the H.323 proxy. After the proxy validates the OSP token, the proxy calls the function OSPPTtransactionGetLookAheadInfoIfPresent. If Look Ahead Routing information is available, it is passed from the OSP client to the proxy and eliminates the need for a second lookup to the OSP server. Note that only one OSP Toolkit transaction between the proxy and the OSP Toolkit is required when Look Ahead Routing is used.



Test Case 2.3.5: Gateway OSP to Proxy to Gateway - Look Ahead Routing
Legend: H.323 Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

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 H.323 proxy can retry the call to other destinations if the call attempt to the first destination fails.

When Look Ahead Routing is used, only one OSP UsageIndication message is reported to the OSP server for both call legs. The UsageIndication Message for Look Ahead routing is neither a source nor destination call detail record. It is a type ‘other’ UsageIndication message.

Detailed Description of Test Case

1. **Call In.** The call begins at the source device.
2. **Auth Req Leg 1.** The source device sends an OSP AuthorizationRequest to the OSP server.

H.323 Proxy – OSP Peering Test Cases

3. **Auth Rsp Leg 1.** The OSP server returns the IP address, DestinationProtocol, and OSPVersion of the proxy, plus a signed peering authorization token, to the source device.
4. **Q931 Setup with Token.** The source device sends a call setup message to the proxy. The setup message includes an OSP peering authorization token.
5. **NEW.** The proxy recognizes the presence of an OSP peering token in the call setup message and establishes a transaction with the OSP Toolkit to validate the token.
6. **ValidateAuth.** The H.323 proxy calls the OSP Toolkit function OSPPTtransactionValidateAuthorisation and passes the OSP token to the OSP Toolkit for validation. The OSP Toolkit determines if the token signature is valid and responds to the proxy. In this call scenario, the token is valid and the call processing continues. If the token was not valid, the proxy would end the transaction with the OSP Toolkit and reject the call (test case 2.3.0). An important variable passed in this function call is ospvTimeLimit – which is the maximum call duration authorized by the OSP server. If the call duration exceeds the authorized time limit, the proxy should end the call (test case 2.3.4).
7. **GetLookAhead.** The H.323 proxy calls the OSP Toolkit function OSPPTtransactionGetLookAheadInfoIfPresent to determine if routing information for the second call leg was embedded in the OSP token. In this test case, Look Ahead routing information is present and the function call returns the destination IP address, the destination protocol (OSPE_DEST_PROT) and the destination OSP enabled status (OSPE_OSP).

Note: For this test case, the expected value for OSPE_DEST_PROT is H323_Q931. If OSPE_DEST_PROT is UNDEFINED or UNKNOWN, the proxy should assume the destination is a H.323 device and complete the call. If OSPE_DEST_PROT is a protocol not supported by the proxy, such as SIP or IAX, 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 the peering token should be included in the call setup to the destination. A value of OSPE_OSP_TRUE indicates that the Look Ahead destination is OSP enabled and that the LookAhead token should be included, as is, in the Setup to the destination. If OSPE_OSP is UNKNOWN or UNDEFINED, the proxy should assume the Look Ahead destination is OSP enabled and include the Look Ahead token in the Setup to the destination.

8. - 15. Standard H.323 communications for the completing the call.
16. **RecordFailure.** At the completion of the call, the H.323 proxy reports the call disconnect reason for the call to the OSP Toolkit using the OSPPTtransactionRecordFailure function.
17. **RepUsage(In).** The proxy calls the OSPPTtransactionReportUsage function to report the call duration for the second call leg.
18. **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

H.323 Proxy – OSP Peering Test Cases

detail record. In a Look Ahead call scenario, the proxy is the destination device for the first call leg and the source device for the second call leg.

19. **Other Usg Cnf**. The OSP server responds with an OSP UsageConfirmation message.

20. **RepUsage(Out)**. The OSP Toolkit closes the ReportUsage transaction.

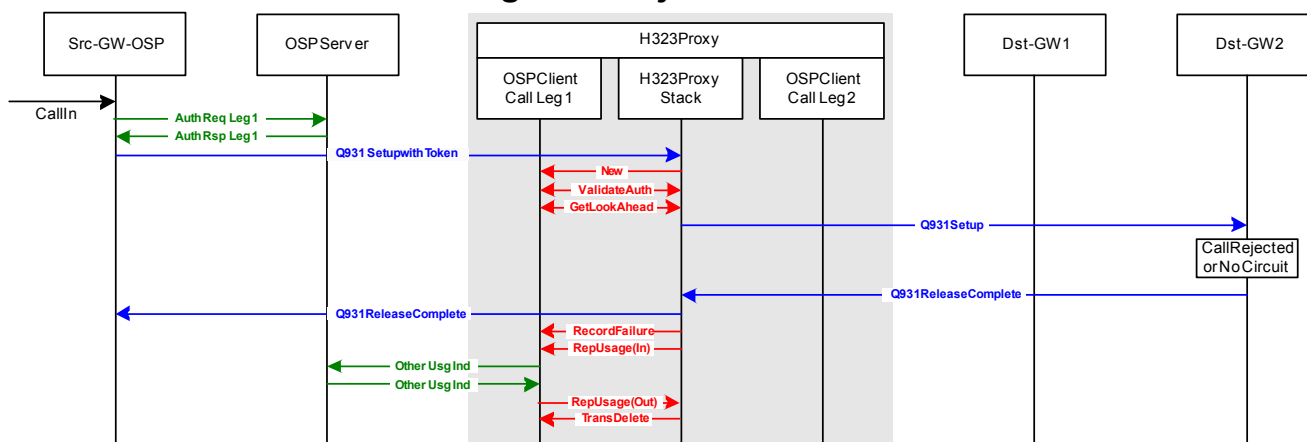
21. **TransDelete**. The H.323 proxy deletes the OSP Toolkit transaction for the call.

Expected CDR for Test Case 2.3.5

This test case should generate one OSP UsageIndication message, or CDR, from the H.323 proxy. Look Ahead Routing is a unique case when one OSP Toolkit transaction validates inbound call leg 1 and routes outbound call leg 2. Since one CDR is used to report usage for both the destination of call leg 1 and the source of call leg 2, the role is defined as other. As with other call scenarios, the FailureReason should be determined by the release code included in the response from the source or destination device.

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

2.3.6. Look Ahead Routing: Call Rejected or No Circuit



Test Case 2.3.6: Gateway OSP to Proxy to Gateway - Look Ahead Routing - Call Rejected or No Circuit
 Legend: H.323 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 device rejects the call.

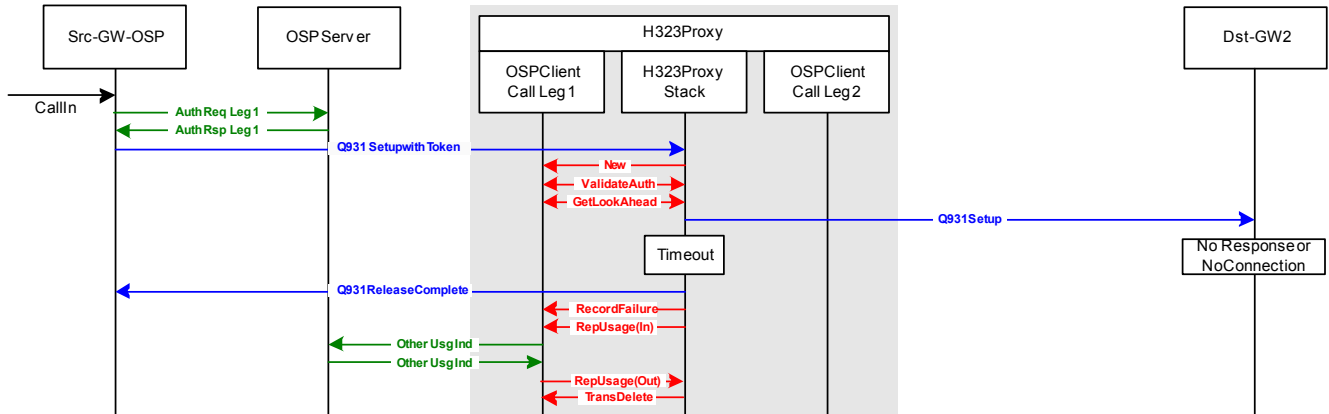
Expected CDR for Test Case 2.3.6

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

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

H.323 Proxy – OSP Peering Test Cases

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



Test Case 2.3.7: Gateway OSP to Proxy to Gateway Look Ahead Routing - No Response or No Connection - Proxy Times Out
Legend: H.323 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 device does not respond to the proxy. This test case must be executed four times to test the following four different call scenarios.

1. The H.323 proxy cannot establish a TCP connection with Dst-GW1. After TCP time-out, the proxy should retry call to Dst-GW2. (When OSP Toolkit function RecordFailure is called, the FailureReason for the call attempt should be set to 47 – resource unavailable, unspecified.)
2. No route to IP address of Dst-GW1. The H.323 proxy should retry call to Dst-GW2. (When OSP Toolkit function RecordFailure is called, the FailureReason for the call attempt should be set to 2 – no route to specified transit network.)
3. TCP connection refused by destination. After TCP connection is refused, the H.323 proxy should retry the call to Dst-GW2. (When OSP Toolkit function RecordFailure is called, the FailureReason for the call attempt should be set to 63 – service or option not available, unspecified.)
4. No response from Dst-GW1. The H.323 proxy establishes TCP connection with Dst-GW1, but DST-GW1 never responds to Setup. The proxy should time-out and retry the call to Dst-GW2. (When OSP Toolkit function RecordFailure is called, the FailureReason for the call attempt should be set to 27 – destination out of order.)

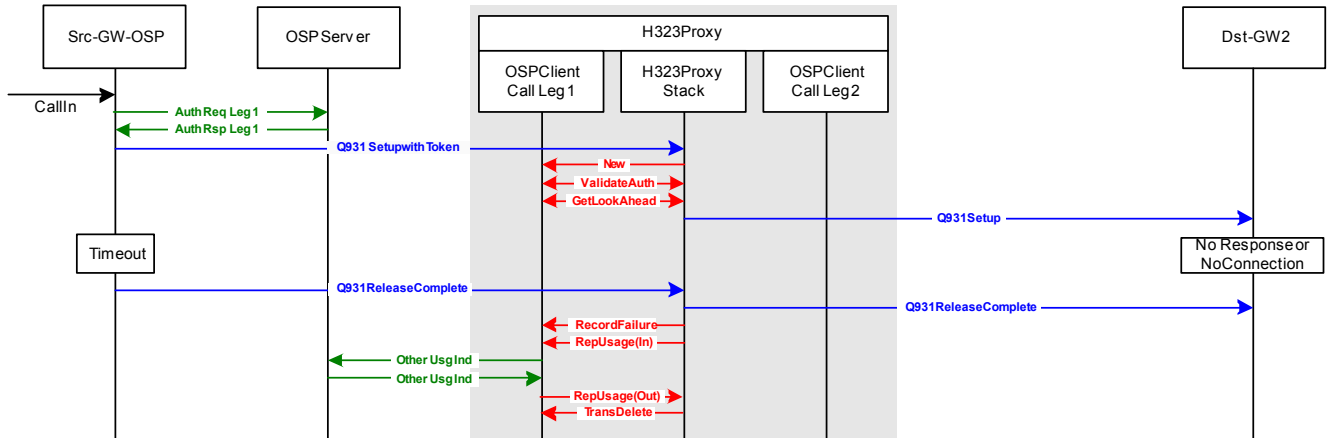
Expected CDR for Test Case 2.3.7

This test case should generate one OSP UsageIndication message, or CDR from the H.323 proxy. The role should be “other” and the FailureReason should be determined by the proxy based on the failure reasons described above.

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

H.323 Proxy – OSP Peering Test Cases

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



**Test Case 2.3.8: Gateway OSP to Proxy to Gateway
Look Ahead Routing - No Response or No Connection - Source Times Out**
Legend: H.323 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-GW2 responds to the Setup from the proxy. In this case, the proxy should terminate the call and report usage to the OSP server. The OSP Toolkit parameter FailureReason reported with the OSPPTTransactionRecordFailure function should be set to the release cause reported in the ReleaseComplete message from the source device, Src-GW.

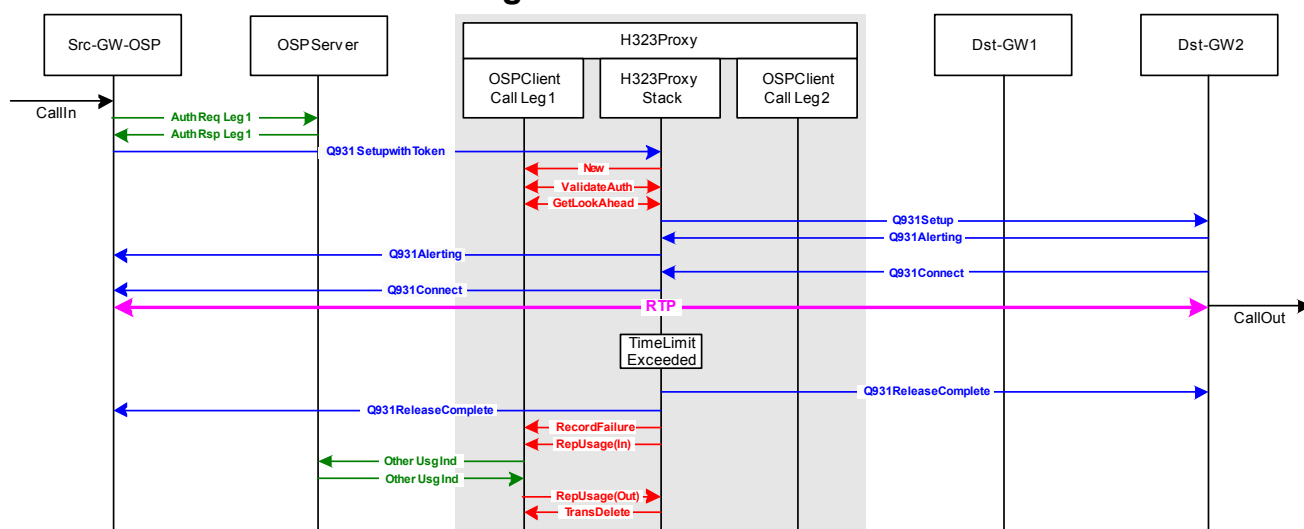
Expected CDR for Test Case 2.3.8

This test case should generate one OSP UsageIndication message, or CDR from the H.323 proxy. The role should be “other” and the FailureReason should be determined by the release reason in the ReleaseComplete message from Src-GW.

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

H.323 Proxy – OSP Peering Test Cases

2.3.9. Look Ahead Routing: Call Duration Limit Exceeded



Test Case 2.3.9: Gateway OSP to Proxy to Gateway - Look Ahead Routing - Time Limit Exceeded
Legend: H.323 Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

This test case is similar to test case 2.3.4 and tests the Look Ahead call scenario when the call duration exceeds the authorized call duration set by `ospvTimeLimit` value returned from the `OSPPTTransactionValidateAuthorisation` function, the proxy should forcefully end the call. When the proxy forcefully ends the call because the call duration exceeded the authorized time limit, the `FailureReason` parameter reported in the `RecordFailure` function should be set to 8 (preemption).

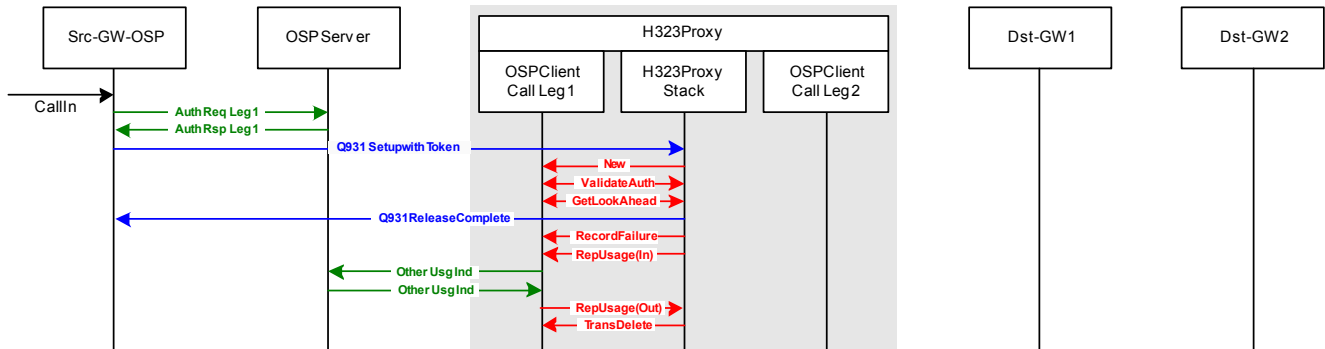
Expected CDR for Test Case 2.3.9

This test case should generate one OSP UsageIndication message, or CDR from the H.323 proxy. The role should be “other” and the `FailureReason` should be 8 to indicate the call was forcefully shutdown by the proxy.

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

H.323 Proxy – OSP Peering Test Cases

2.3.10. Look Ahead Routing: Protocol Error



Test Case 2.3.10: Gateway OSP to Proxy to Gateway-Look Ahead Routing - Protocol Error

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

Test Case Notes

This test case is similar to test case 2.1.5 and tests the Look Ahead error condition when the OSP server returns a DestinationProtocol in the Look Ahead token that is not supported by the H.323 proxy, such as SIP or IAX. When this occurs, the proxy should reject the destination, record FailureReason 111 (protocol error) and report usage.

For this test case, the destination protocol for device Dst-GW2 is NOT configured as H323_Q931 on the OSP server. The OSPPTtransactionGetLookAheadInfoIfPresent function call returns a DestinationProtocol incompatible with H323_Q931. The proxy should recognize the protocol error and reject the destination. Note, if the DestinationProtocol is unknown or undefined, the proxy should assume the destination device supports H323_Q931 and should send a call setup message to the destination device.

Expected CDRs for Test Case 2.3.10

This test case should generate one OSP UsageIndication message, or CDR the H.323 proxy. The role should be “other”.

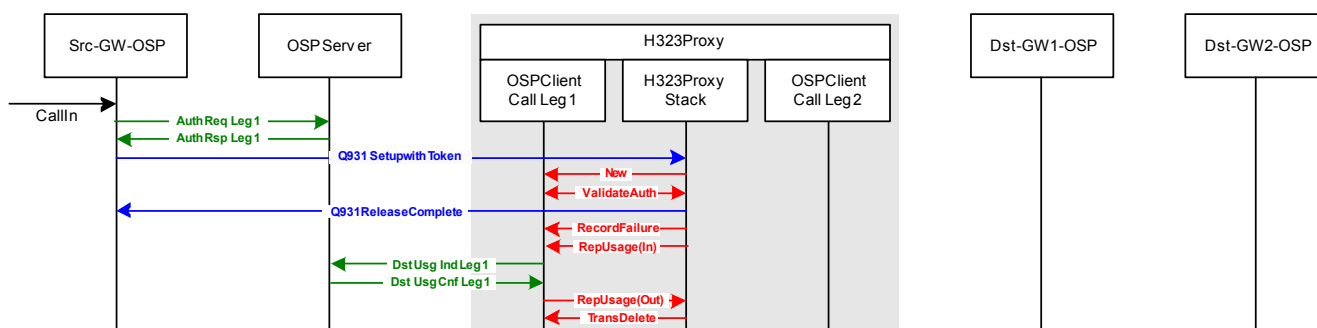
Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW	Dst-GW2	111	0

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 H.323 device will include an OSP peering authorization token in the Q931 call setup message sent to the proxy. Based on the test case, the OSP peering token may or may not include Look Ahead Routing information. To complete the call, the proxy must include an OSP peering authorization token in the call setup message to the destination device. The destination device will extract the token from the call setup message and validate the token signature to determine if the call from the proxy should be accepted.

Configuration of VoIP devices on OSP server for test cases in section 2.4		
Device	Destination Protocol	OSP Version
Src-GW-OSP	H323-Q931	1.3.4, 2.1.1 or 4.1.1
H.323 Proxy	H323-Q931	2.1.1 or 4.1.1
Dst-GW1-OSP	H323-Q931	1.3.4, 2.1.1 or 4.1.1
Dst-GW2-OSP	H323-Q931	1.3.4, 2.1.1 or 4.1.1

2.4.0. Invalid Authorization Token



Test Case 2.4.0: Gateway OSP to Proxy to Gateway OSP - Invalid Authorization Token

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

Test Case Notes

This test case is identical to 2.3.0.

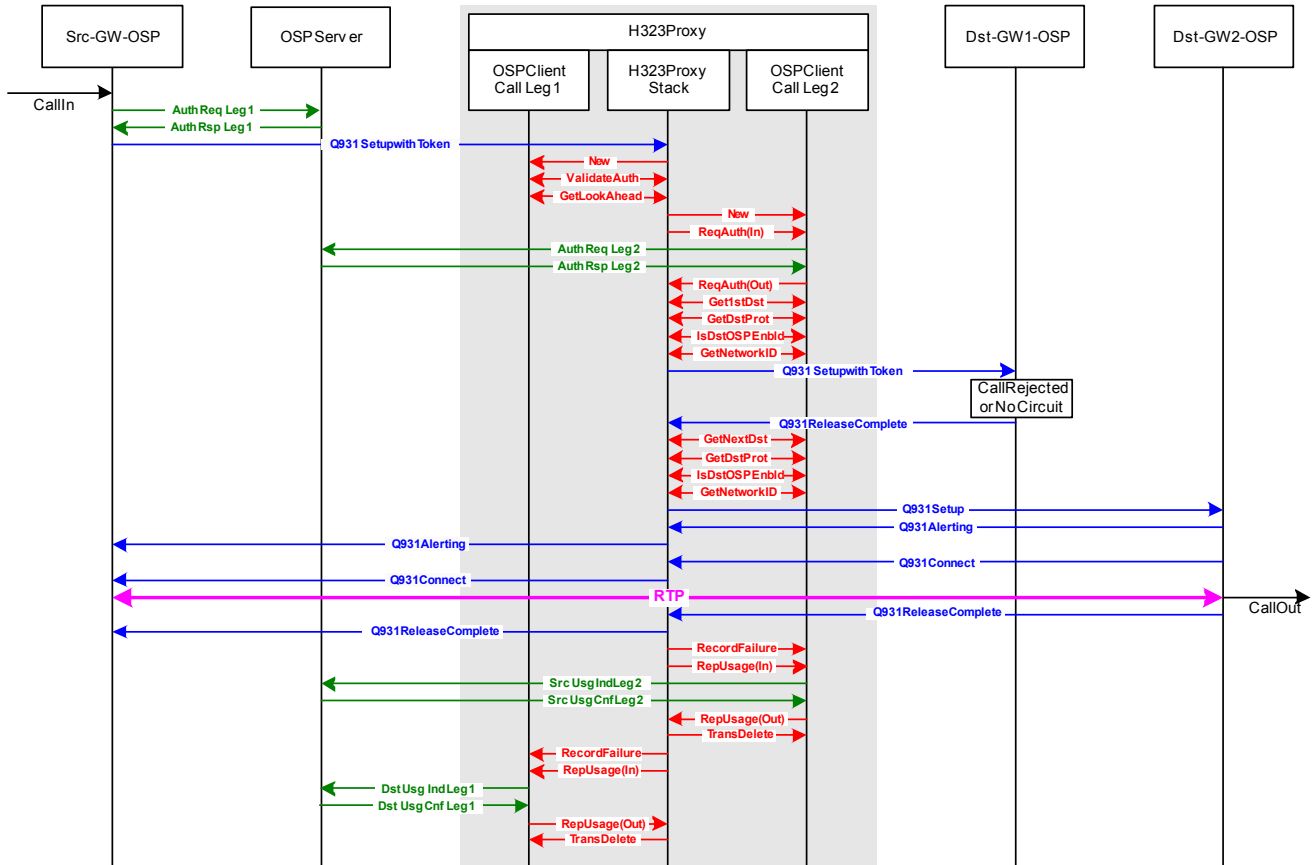
Expected CDR for Test Case 2.4.0

This test case should generate one OSP Usage Indication message, or CDR, from the H.323 proxy as the destination of call leg 1. The release reason (ospvFailureReason), or termination cause code, for the call should be set by the proxy to 21 to indicate the authorization token was invalid.

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

H.323 Proxy – OSP Peering Test Cases

2.4.1. Call Rejected or No Circuit and Retry



Test Case 2.4.1: Gateway OSP to Proxy to Gateway OSP - Call Rejected or No Circuit & Retry
Legend: H.323 Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

See test case 2.3.1.

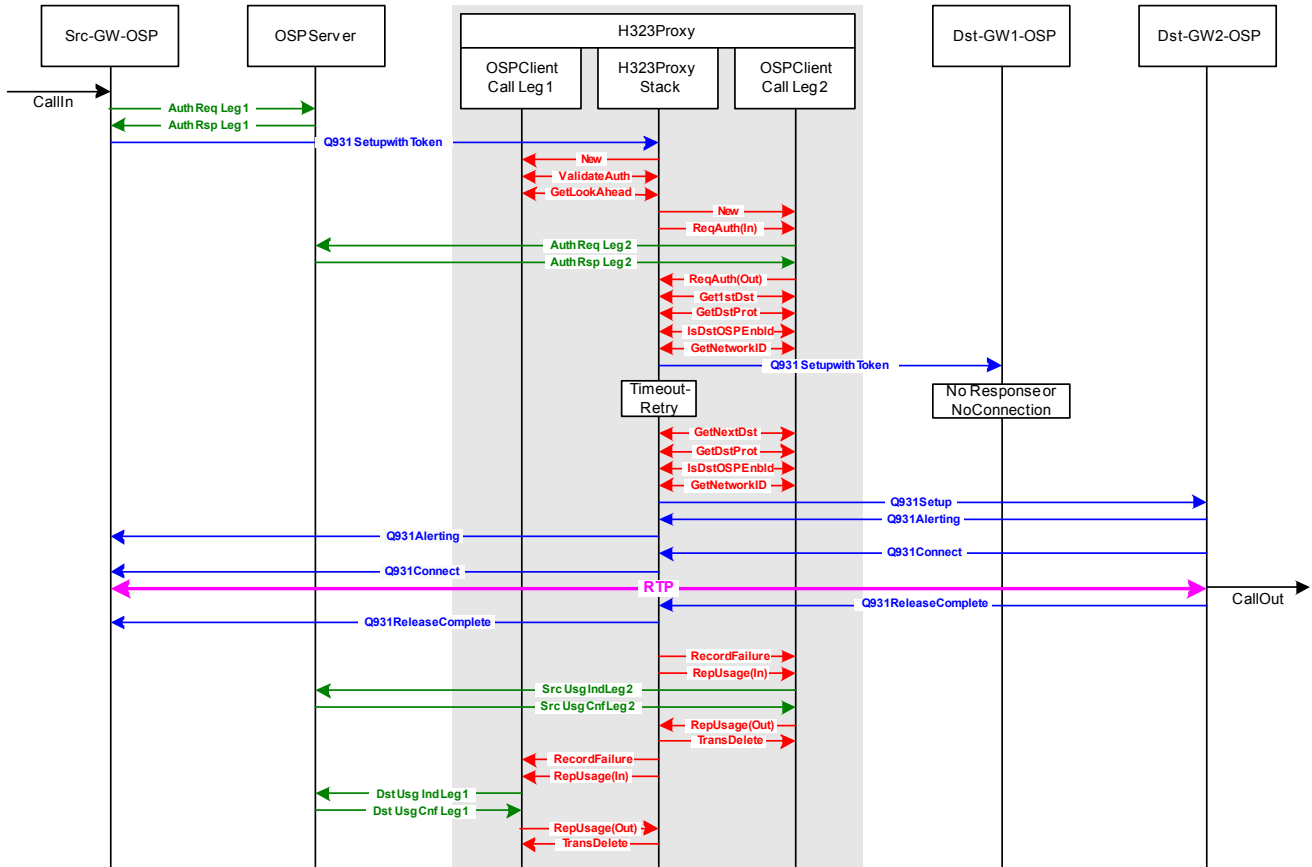
Expected CDRs for Test Case 2.4.1

This test case should generate three OSP Usage Indication messages, or CDRs, from the H.323 proxy. Two CDRs as the source of call leg 2 and one CDR as the destination of call leg 1. The release reason (ospvFailureReason) in the source CDR for call leg 2 for the first call attempt should be the response from DST-GW1-OSP. In this example, the response is 21, but other responses are also valid. For the successful retry for call leg 2, the proxy should set the FailureReason to 16 or 1016 in the source CDR. For the destination CDR for call leg 1, the FailureReason should also be set to 16 or 1016 by the proxy.

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

H.323 Proxy – OSP Peering Test Cases

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



Test Case 2.4.2: Gateway OSP to Proxy to Gateway OSP - No Response or No Connection and Retry - Proxy Times Out
 Legend: H.323 Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

See test case 2.3.2.

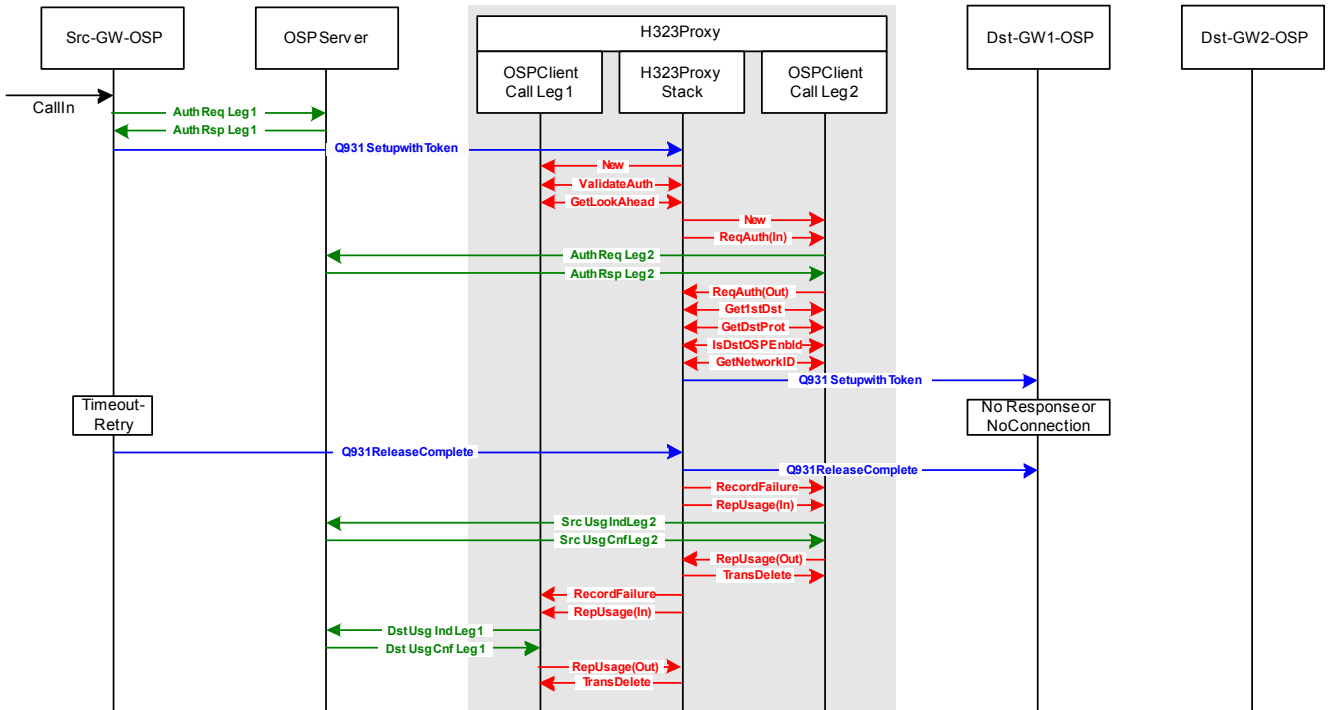
Expected CDRs for Test Case 2.4.2

This test case should generate three OSP UsageIndication messages, or CDRs, from the H.323 proxy. Two CDRs created as the source of call leg 2 and one CDR as the destination of call leg 1. The release reason (ospvFailureReason), or termination cause code, for the first attempt of call leg 2 should be determined by the proxy based on the reason for the failure. For the successful retry of call leg 2, the proxy should set the FailureReason to 16 or 1016. The FailureReason for the destination CDR of call leg 1 should be 16 or 1016.

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

H.323 Proxy – OSP Peering Test Cases

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



Test Case 2.4.3: Gateway OSP to Proxy to Gateway OSP - No Response or No Connection - Source Times Out
Legend: H.323 Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

See test case 2.3.3.

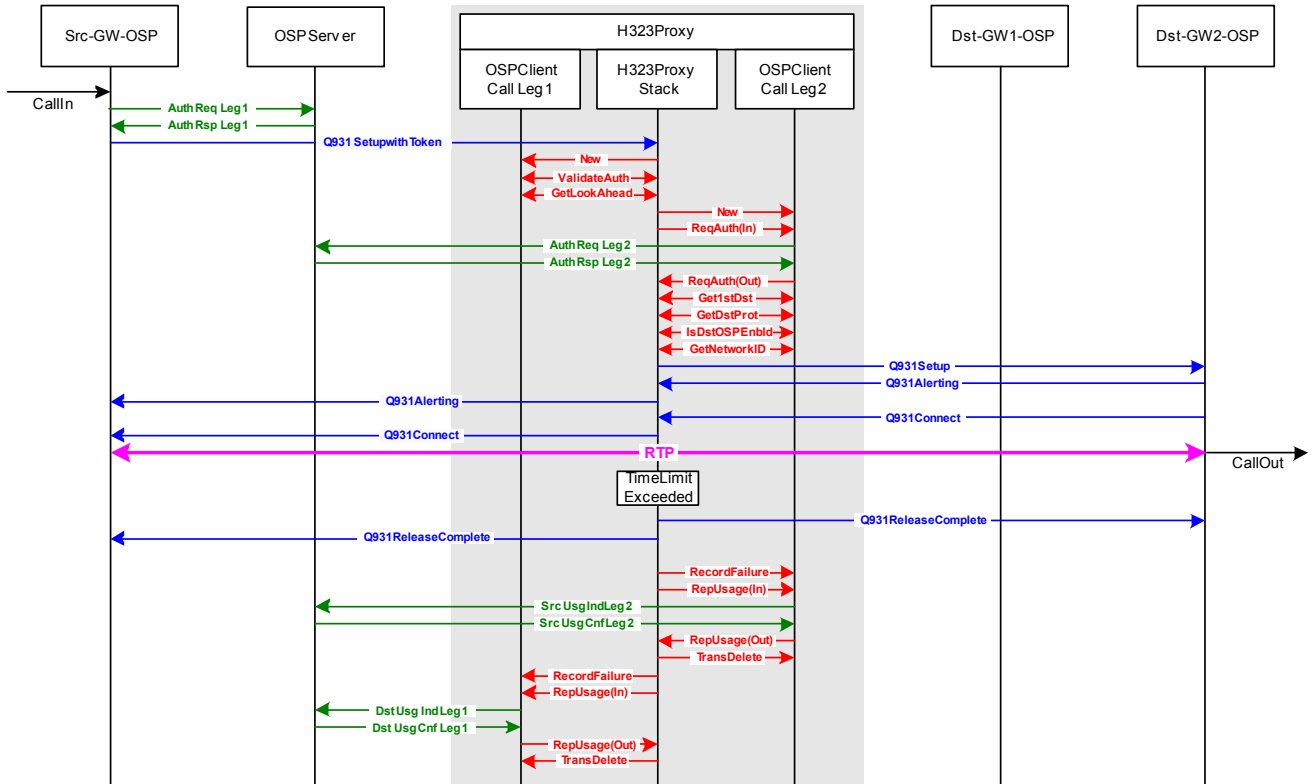
Expected CDRs for Test Case 2.4.3

This test case should generate two OSP Usage Indication messages, or CDRs, from the H.323 proxy. One CDR as the source of call leg 2 and another as the destination of call leg 1. The release reason (ospvFailureReason), or termination cause code, for the CDRs should be determined by the release reason included in the ReleaseComplete message from Src-GW-OSP.

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

H.323 Proxy – OSP Peering Test Cases

2.4.4. Call Duration Limit Exceeded



Test Case 2.4.4: Gateway OSP to Proxy to Gateway OSP - Time Limit Exceeded
Legend: H.323 Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

See test case 2.3.4.

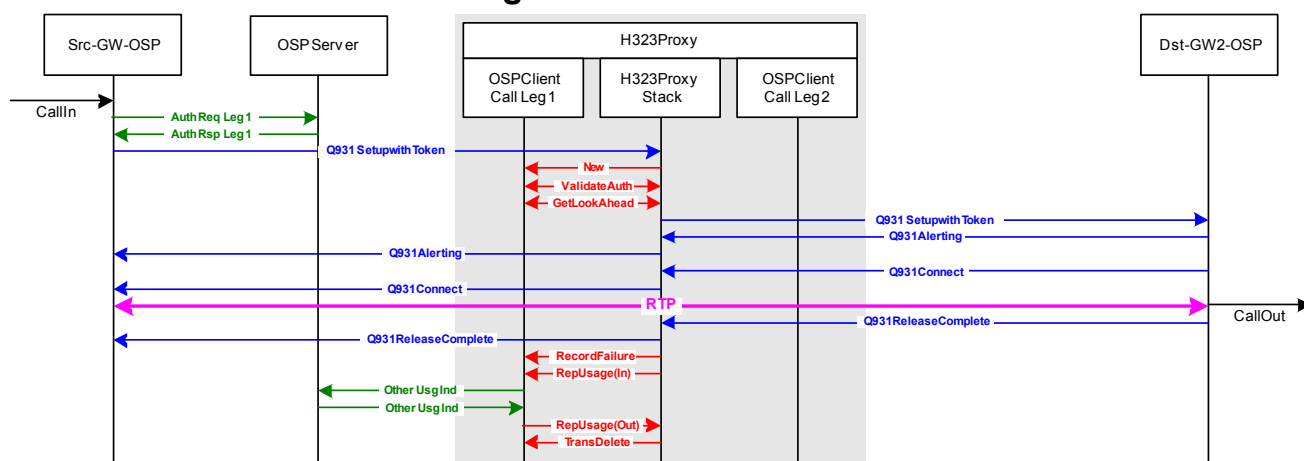
Expected CDRs for Test Case 2.4.4

This test case should generate two OSP Usage Indication messages, or CDRs. One from the H.323 proxy 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 proxy to 8 to indicate the call was forcefully shutdown by the proxy.

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

H.323 Proxy – OSP Peering Test Cases

2.4.5. Look Ahead Routing



Test Case 2.4.5: GatewayOSP to Proxy to GatewayOSP - LookAhead Routing
Legend: H.323 Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

See test case 2.3.5.

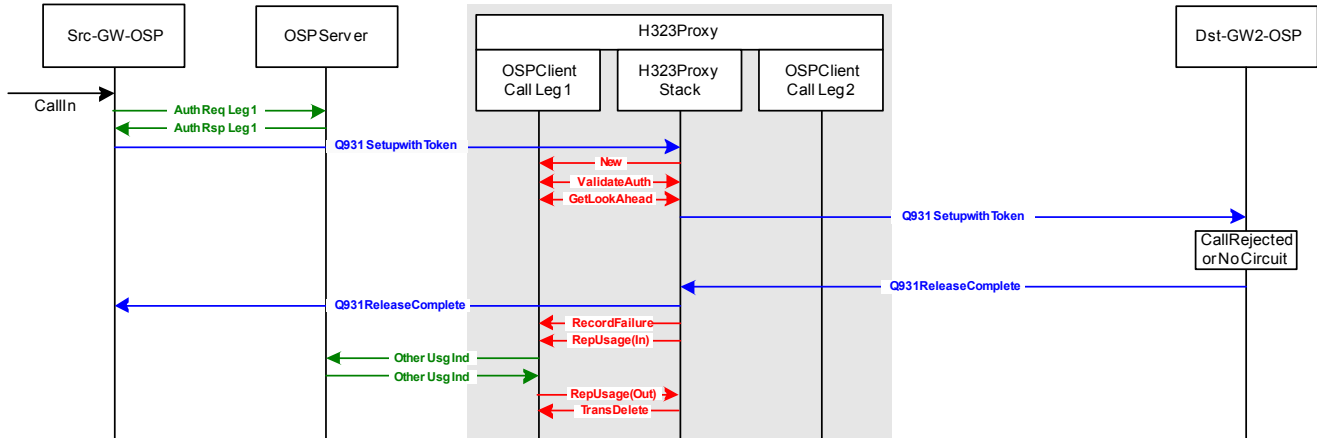
Expected CDR for Test Case 2.4.5

This test case should generate one OSP UsageIndication message, or CDR from the H.323 proxy. Look Ahead Routing is a unique case when one OSP Toolkit transaction validates inbound call leg 1 and routes outbound call leg 2. Since one CDR is used to report usage for both the destination of call leg 1 and the source of call leg 2, the role is defined as other. As with other call scenarios, the FailureReason should be determined by the release code included in the response from the source or destination device.

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

H.323 Proxy – OSP Peering Test Cases

2.4.6. Look Ahead Routing: Call Rejected or No Circuit



Test Case 2.4.6: Gateway OSP to Proxy to Gateway OSP - Look Ahead Routing - Call Rejected or No Circuit
Legend: H.323 Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

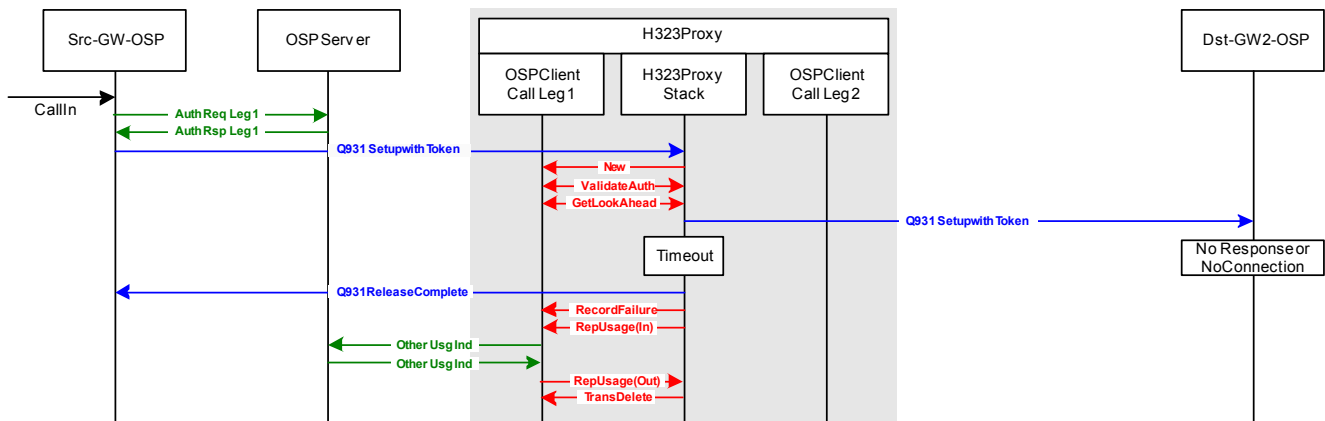
See test case 2.3.6.

Expected CDR for Test Case 2.4.6

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

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

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



Test Case 2.4.7: Gateway OSP to Proxy to Gateway OSP
Look Ahead Routing - No Response or No Connection - Proxy Times Out
Legend: H.323 Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

H.323 Proxy – OSP Peering Test Cases

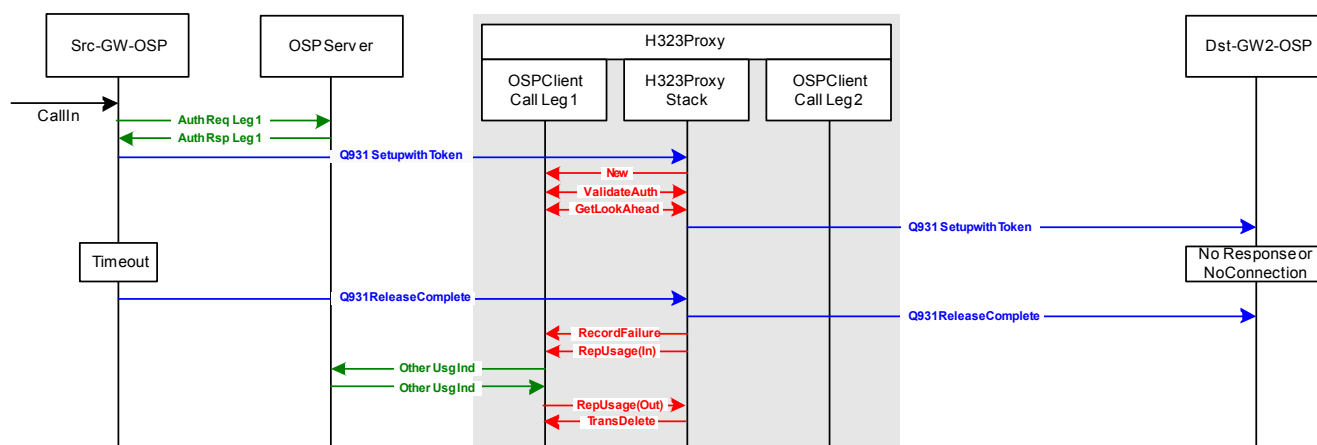
See test case 2.3.7.

Expected CDR for Test Case 2.4.7

This test case should generate one OSP UsageIndication message, or CDR, from the H.323 proxy. The role should be “other” and the FailureReason should be determined by the proxy based on the failure reasons described above.

Call Leg	Role	Source IP Address	Destination IP Address	Release Reason or TC Code	Call Duration
1 & 2	other	Src-GW-OSP	Dst-GW2-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: Gateway OSP to Proxy to Gateway OSP
Look Ahead Routing - No Response or No Connection - Source Times Out
Legend: H.323 Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

See test case 2.3.8.

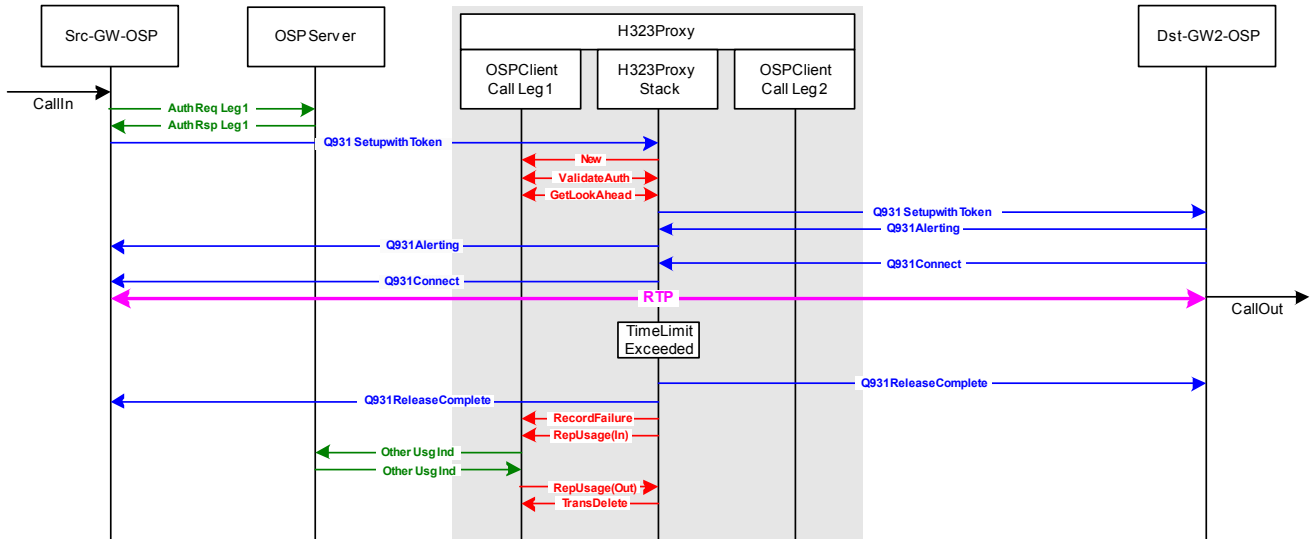
Expected CDR for Test Case 2.4.8

This test case should generate one OSP UsageIndication message, or CDR, from the H.323 proxy. The role should be “other” and the FailureReason should be determined by the release reason in the ReleaseComplete message from Src-GW-OSP.

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

H.323 Proxy – OSP Peering Test Cases

2.4.9. Look Ahead Routing: Call Duration Limit Exceeded



Test Case 2.4.9: Gateway OSP to Proxy to Gateway OSP - Look Ahead Routing
Legend: H.323 Messages in Blue, OSP Toolkit Calls in Red, OSP Messages in Green

Test Case Notes

See test case 2.3.9.

Expected CDR for Test Case 2.4.9

This test case should generate one OSP UsageIndication message, or CDR from the H.323 proxy. The role should be “other” and the FailureReason should be 8 to indicate the call was forcefully shutdown by the proxy.

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