



OSP Toolkit

SIP Implementation Guide

Release 3.1.2

July 1, 2004

## Revision History

Revision	Date of Issue	Changes
3.0	March 11 <sup>th</sup> , 2004	First Draft
3.1	April 8 <sup>th</sup> , 2004	No Changes
3.1.1	May 12 <sup>th</sup> , 2004	No Changes
3.1.2	July 1 <sup>st</sup> , 2004	No Changes

## Contents

Revision History .....	2
Contents .....	3
Introduction .....	4
Call flow 1 (SIP GW to SIP GW) .....	5
Call flow 2 (SIP GW to SIP GW through SIP Proxies) .....	10
Call flow 3 (SIP UA to SIP UA through SIP Proxies).....	15
Call flow 4 (SIP UA to SIP UA using ENUM numbering scheme).....	21
Call flow 5 (SIP UA to H323 GW using look ahead route).....	27

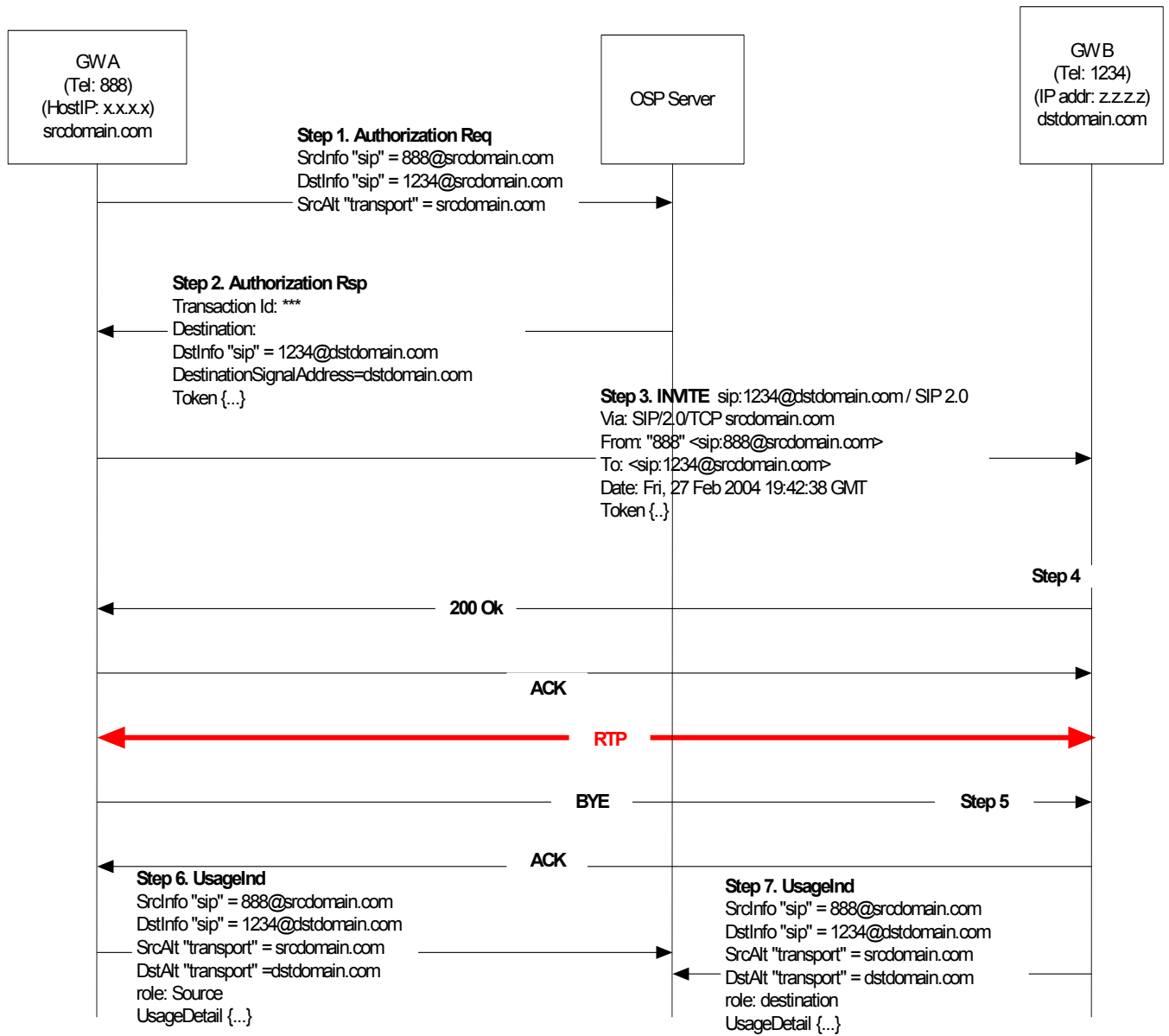
## Introduction

The purpose of this document is to outline the inter-working of OSP with SIP. The document contains the following call flows:

- SIP GW to SIP GW
- SIP GW to SIP GW through two proxies
- SIP UA to SIP UA through two proxies
- SIP UA to SIP UA using ENUM numbering scheme.
- SIP UA to H.323 GW using look ahead route.

**Call flow 1 (SIP GW to SIP GW)**

The following diagram illustrates a SIP GW to SIP GW call scenario. The source gateway has address x.x.x.x and a Fully Qualified domain name (FQDN) – srcdomain.com, and the destination gateway has address z.z.z.z and the FQDN – dstdomain.com. The call scenario begins with a call made from the telephone connected to the source gateway; the calling number is 888, and the called number is 1234.



Call Scenario: SIP GW to SIP GW

Step 1: Source gateway sends OSP AuthorizationRequest to OSP Server The significant elements within the <AuthorisationRequest> include

<Timestamp>	Time of request
<CallId>	SIP Call Identifier to be used for the call
<SourceInfo type="sip">	The SIP URI that would eventually be passed in the "From" field of the SIP INVITE message – <a href="mailto:888@srcdomain.com">888@srcdomain.com</a>
<SourceAlternate type="transport">	DNS name or IP address of Gateway A – srcdomain.com
<SourceAlternate type="network">	Any network specific information from Gateway A, for example trunk group id (Optional)
<DestinationInfo type="sip">	The SIP URI that would eventually be passed in the "To" field of the SIP INVITE message – <a href="mailto:1234@srcdomain.com">1234@srcdomain.com</a>
<Service/>	Empty (for basic service)
<MaximumDestinations>	The maximum number of destinations, including alternatives, Gateway A will consider

If using the OSP Toolkit, Gateway A can generate this message by calling OSPPTtransactionRequestAuthorisation() with the following significant parameters:

ospvSource	DNS name or IP address of Gateway A, for example "srcdomain.com"
ospvSourceDevice	not needed in peer-to-peer environments; empty string ("") in this example
ospvCallingNumber	The SIP URI that would eventually be passed in the "From" field of the SIP INVITE message – <a href="mailto:888@srcdomain.com">888@srcdomain.com</a>
ospvCalledNumber	The SIP URI that would eventually be passed in the "To" field of the SIP INVITE message – <a href="mailto:1234@srcdomain.com">1234@srcdomain.com</a>
ospvCallingNumberFormat	Sip
ospvCalledNumberFormat	Sip
ospvUser	optional user identification; empty string ("") in this example
ospvNumberOfCallIds	the number of SIP Call Identifiers given to the OSP server; if all INVITE attempts for this call will use the same Call Identifier value (as in this example), this parameter value is 1
ospvCallIds	an array (containing, in this example, but a single element) of SIP Call Identifiers; the array structure includes a size field which indicates the size of the value
ospvPreferredDestinations	optional list of preferred destination gateways; empty string ("") in this example
ospvNumberOfDestinations	the maximum number of potential destinations that Gateway A is prepared to consider for the call; for example 3

Step 2: OSP Server replies with an <AuthorisationResponse> message. The message indicates the destination as Gateway B. In particular, the <AuthorisationResponse> contains the following elements.

<Timestamp>	time of response
<Status>	result of response, e.g. <Code>200</Code>

<TransactionId>	transaction identifier assigned by settlement provider
<Destination>	first destination gateway to try for call
<DestinationInfo type="sip">	The SIP URI at which the destination can be contacted – <a href="mailto:1234@dstdomain.com">1234@dstdomain.com</a>
<DestinationSignalAddress type="transport">	DNS name or IP address of Gateway B, for example dstdomain.com
<Token>	authorization token to be passed to Gateway B
<ValidAfter>	time after which token for Gateway B is valid
<ValidUntil>	time until which token for Gateway B is valid
<UsageDetail>	how much service is authorized with Gateway B
<Service/>	empty (for basic service)
<Amount>	amount of authorized service, e.g. 3600
<Increment>	increment of service measurement, e.g. 1
<Unit>	unit of service measurement, e.g. s for seconds
<CallId>	SIP Call Identifier to be used for the call to Gateway B

Step 3: Source gateway sends an INVITE message to destination gateway. The significant fields within the INVITE message are:

<Request URI>	The destination as returned by the OSP Server – <a href="mailto:1234@dstdomain.com">1234@dstdomain.com</a>
<CallId>	SIP Call Identifier to be used for the call
<From>	Calling party's SIP URI – <a href="mailto:888@srcdomain.com">888@srcdomain.com</a>
<Via>	DNS name or IP address of Gateway A – srcdomain.com
<To>	Called party's SIP URI – <a href="mailto:1234@dstdomain.com">1234@dstdomain.com</a>
<Token>	The token sent by the OSP Server in the Authorization Response.

Each token should be conveyed in the SIP message body using the application/osptoken MIME type, as defined in <http://www.ietf.org/internet-drafts/draft-johnstonsip-osp-token-05.txt>. (The OSP Toolkit document *Cisco Interoperability Example* provides additional information on OSP token formatting in Appendix A.)

Step 4: The destination GW B validates the token and accepts the call. If using the OSP Toolkit, Gateway B must call the Toolkit function `OSPTransactionValidateAuthorisation()` to verify the authorization token in the INVITE message. It would call it with the following parameters.

OspvSource	DNS name or IP address of Gateway A, for example "srcdomain.com"
OspvDestination	DNS name or IP address of Gateway B, for example dstdomain.com
OspvSourceDevice	not needed in peer-to-peer environments; empty string ("") in this example
OspvDestinationDevice	not needed in peer-to-peer environments; empty string ("") in this example
OspvCallingNumber	Calling party's SIP URI – <a href="mailto:888@srcdomain.com">888@srcdomain.com</a>
ospvCalledNumber	Called party's SIP URI – <a href="mailto:1234@dstdomain.com">1234@dstdomain.com</a>

ospvCallingNumberFormat	Sip
ospvCalledNumberFormat	Sip
ospvCallId	SIP Call Identifier received in Setup message
ospvToken	authorization token presented to Gateway B in the INVITE message

The `OSPPTTransactionValidateAuthorisation()` function will return an indication of whether or not the call is authorized (`ospvAuthorised`), and, if so, how much service is authorized (`ospvTimeLimit`).

Step 5: The call is disconnected after a while.

Step 6: Gateway A sends a `<UsageIndication>` message to the OSP server. If Gateway A is not using any protocol extensions, the message will contain the following elements.

<code>&lt;Timestamp&gt;</code>	time of request
<code>&lt;Role&gt;</code>	for Gateway A, source
<code>&lt;TransactionId&gt;</code>	transaction ID assigned by OSP server in authorization response
<code>&lt;CallId&gt;</code>	SIP Call Identifier used for the call
<code>&lt;SourceInfo type="sip"&gt;</code>	calling party's SIP URI as returned in the authorization response, e.g. <a href="mailto:888@srcdomain.com">888@srcdomain.com</a>
<code>&lt;SourceAlternate type="transport"&gt;</code>	DNS name or IP address of Gateway A, for example <code>srcdomain.com</code>
<code>&lt;SourceAlternate type="network"&gt;</code>	Any network specific information from Gateway A, for example <code>trunk group id</code> . (Optional)
<code>&lt;DestinationInfo type="sip"&gt;</code>	called party's SIP URI as returned in the authorization response, e.g. <a href="mailto:1234@dstdomain.com">1234@dstdomain.com</a>
<code>&lt;DestinationAlternate type="transport"&gt;</code>	DNS name or IP address of Gateway B, for example, <code>dstdomain.com</code>
<code>&lt;UsageDetail&gt;</code>	usage information for the call
<code>&lt;Service/&gt;</code>	empty (for basic service)
<code>&lt;Amount&gt;</code>	amount of service used, e.g. 300
<code>&lt;Increment&gt;</code>	increment of service measurement, e.g. 1
<code>&lt;Unit&gt;</code>	unit of service measurement, e.g. <code>s</code> for seconds

If using the OSP Toolkit, Gateway A can generate that message by calling `OSPPTTransactionReportUsage()` with the following significant parameters

<code>ospvDuration</code>	length of the call in seconds, e.g. 300
<code>OspvStartTime</code>	time stamp of when the call started
<code>ospvLossPacketsSent</code>	value ignored (because of following parameter value)
<code>ospvLossFractionSent</code>	-1 if not reported
<code>ospvLossPacketsReceived</code>	value ignored (because of following parameter value)
<code>ospvLossFractionReceived</code>	-1 if not reported

Step 7: Gateway B sends a `<UsageIndication>` message to the OSP server. If Gateway B is not using any protocol extensions, the message will contain the following elements.

<Timestamp>	time of request
<Role>	for Gateway B, destination
<TransactionId>	transaction ID assigned by OSP server in authorization response
<CallId>	SIP Call Identifier used for the call
<SourceInfo type="sip">	calling party's SIP URI as returned in the authorization response, e.g. <a href="mailto:888@srcdomain.com">888@srcdomain.com</a>
<SourceAlternate type="transport">	DNS name or IP address of Gateway A, for example srcdomain.com
<SourceAlternate type="network">	Any network specific information from Gateway A, for example trunk group id. (Optional)
<DestinationInfo type="sip">	called party's SIP URI as returned in the authorization response, e.g. <a href="mailto:1234@dstdomain.com">1234@dstdomain.com</a>
<DestinationAlternate type="transport">	DNS name or IP address of Gateway B, for example, dstdomain.com
<UsageDetail>	usage information for the call
<Service/>	empty (for basic service)
<Amount>	amount of service used, e.g. 300
<Increment>	increment of service measurement, e.g. 1
<Unit>	unit of service measurement, e.g. s for seconds

If using the OSP Toolkit, Gateway A can generate that message by calling OSPPTTransactionReportUsage () with the following significant parameters

ospvDuration	length of the call in seconds, e.g. 300
OspvStartTime	time stamp of when the call started
ospvLossPacketsSent	value ignored (because of following parameter value)
ospvLossFractionSent	-1 if not reported
ospvLossPacketsReceived	value ignored (because of following parameter value)
ospvLossFractionReceived	-1 if not reported

## Call flow 2 (SIP GW to SIP GW through SIP Proxies)

The following diagram illustrates a SIP GW to SIP GW call scenario. However, both gateways are behind proxies. The source gateway has address x.x.x.x and the source proxy has a Fully Qualified Domain Name (FQDN) – srcdomain.com. The destination gateway has address z.z.z.z and the destination proxy has a Fully Qualified Domain Name (FQDN) – proxy.dstdomain.com. The call scenario begins with a call made from the telephone connected to the source gateway; The calling number is 888, and the called number is 1234.

Step 1: Source gateway (GW A) sends an INVITE message to source proxy (Proxy A). The significant fields within the INVITE message are:

<Request URI>	The URI of the destination device as known to the source GW – <a href="mailto:1234@srcdomain.com">1234@srcdomain.com</a>
<CallId>	SIP Call Identifier to be used for the call
<From>	Calling party's SIP URI – <a href="mailto:888@srcdomain.com">888@srcdomain.com</a>
<Via>	DNS name or IP address of Gateway A– x.x.x.x
<To>	Called party's SIP URI as known to the source – <a href="mailto:1234@srcdomain.com">1234@srcdomain.com</a>

Step 2: Source Proxy sends OSP AuthorizationRequest to OSP Server The significant elements within the <AuthorisationRequest> include

<Timestamp>	Time of request
<CallId>	SIP Call Identifier to be used for the call
<SourceInfo type="sip">	The SIP URI that was passed in the "From" field of the SIP INVITE message – <a href="mailto:888@srcdomain.com">888@srcdomain.com</a>
<DeviceInfo type="transport">	DNS name or IP address of Gateway – x.x.x.x
<SourceAlternate type="transport">	DNS name or IP address of Proxy A – srcdomain.com
<DestinationInfo type="sip">	The SIP URI that was passed in the "To" field of the SIP INVITE message – <a href="mailto:1234@srcdomain.com">1234@srcdomain.com</a>
<Service/>	Empty (for basic service)
<MaximumDestinations>	The maximum number of destinations, including alternatives, that the proxy will consider

If using the OSP Toolkit, proxy can generate this message by calling OSPPTtransactionRequestAuthorisation() with the following significant parameters:

ospvSource	DNS name or IP address of Proxy A, for example "srcdomain.com"
ospvSourceDevice	DNS name or IP address of gateway A, for example x.x.x.x
ospvCallingNumber	The SIP URI that was passed in the "From" field of the SIP INVITE message – <a href="mailto:888@srcdomain.com">888@srcdomain.com</a>
ospvCalledNumber	The SIP URI that was passed in the "To" field of the SIP INVITE message – <a href="mailto:1234@srcdomain.com">1234@srcdomain.com</a>
ospvCallingNumberFormat	Sip
ospvCalledNumberFormat	Sip

<code>ospvUser</code>	optional user identification; empty string ("") in this example
<code>ospvNumberOfCallIds</code>	the number of SIP Call Identifiers given to the OSP server; if all INVITE attempts for this call will use the same Call Identifier value (as in this example), this parameter value is 1
<code>ospvCallIds</code>	an array (containing, in this example, but a single element) of SIP Call Identifiers; the array structure includes a size field which indicates the size of the value
<code>ospvPreferredDestinations</code>	optional list of preferred destination gateways; empty string ("") in this example
<code>ospvNumberOfDestinations</code>	the maximum number of potential destinations that Gateway A is prepared to consider for the call; for example 3

Step 3: OSP Server replies with an `<AuthorisationResponse>` message. The message indicates the destination as Proxy B. In particular, the `<AuthorisationResponse>` contains the following elements.

<code>&lt;Timestamp&gt;</code>	time of response
<code>&lt;Status&gt;</code>	result of response, e.g. <code>&lt;Code&gt;200&lt;/Code&gt;</code>
<code>&lt;TransactionId&gt;</code>	transaction identifier assigned by settlement provider
<code>&lt;Destination&gt;</code>	first destination gateway to try for call
<code>&lt;DestinationInfo     type="sip"&gt;</code>	The SIP URI at which the destination can be contacted – <a href="mailto:1234@proxy.dstdomain.com">1234@proxy.dstdomain.com</a>
<code>&lt;DestinationSignalAddress     type="transport"&gt;</code>	DNS name or IP address of Proxy B, for example <code>proxy.dstdomain.com</code>
<code>&lt;Token&gt;</code>	Authorization token to be passed to Proxy B
<code>&lt;ValidAfter&gt;</code>	time after which token for Proxy B is valid
<code>&lt;ValidUntil&gt;</code>	time until which token for Proxy B is valid
<code>&lt;UsageDetail&gt;</code>	how much service is authorized with Proxy B
<code>&lt;Service/&gt;</code>	Empty (for basic service)
<code>&lt;Amount&gt;</code>	Amount of authorized service, e.g. 3600
<code>&lt;Increment&gt;</code>	Increment of service measurement, e.g. 1
<code>&lt;Unit&gt;</code>	unit of service measurement, e.g. s for seconds
<code>&lt;CallId&gt;</code>	SIP Call Identifier to be used for the call to Proxy B

Step 4: Proxy A sends an INVITE message to Proxy B. The significant fields within the INVITE message are:

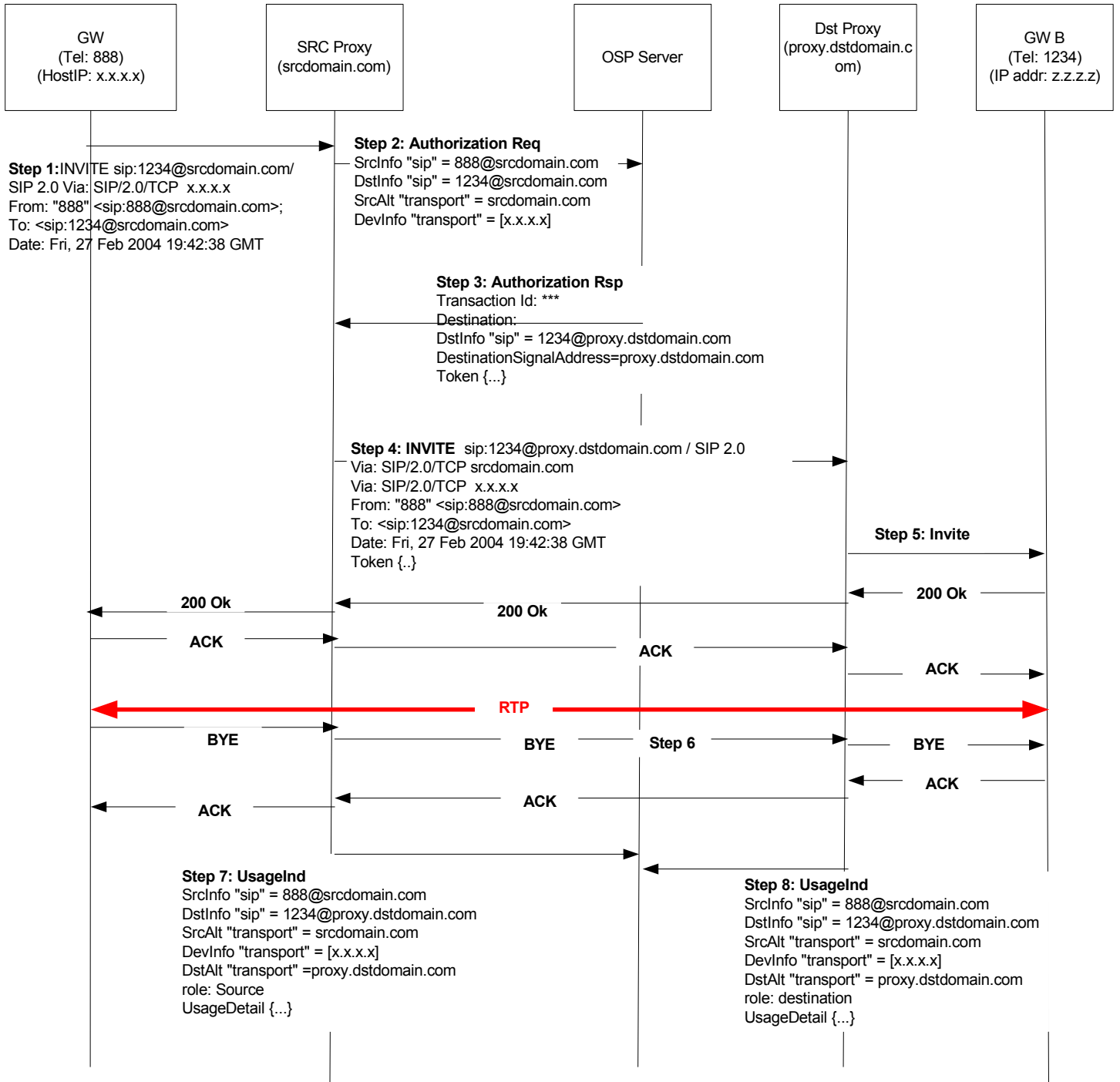
<code>&lt;Request URI&gt;</code>	The destination as returned by the OSP Server– <a href="mailto:1234@proxy.dstdomain.com">1234@proxy.dstdomain.com</a>
<code>&lt;CallId&gt;</code>	SIP Call Identifier to be used for the call
<code>&lt;From&gt;</code>	Calling party's SIP URI – <a href="mailto:888@srcdomain.com">888@srcdomain.com</a>
<code>&lt;Via&gt;</code>	DNS name or IP address of Proxy A– <code>srcdomain.com</code>
<code>&lt;Via&gt;</code>	DNS name or IP address of Gateway A– <code>x.x.x.x</code>
<code>&lt;To&gt;</code>	Called party's SIP URI that was present in the original request – <a href="mailto:1234@srcdomain.com">1234@srcdomain.com</a>

<Token>

The token sent by the OSP Server in the Authorization Response.

Step 5: Proxy B validates the token and accepts the call. If using the OSP Toolkit, Proxy B must call the Toolkit function `OSPPTransactionValidateAuthorisation()` to verify the

**Call Scenario: SIP GW to SIP GW through SIP Proxies**



authorization token in the INVITE message. It would call it with the following parameters.

OspvSource	DNS name or IP address of Proxy A, for example "srcdomain.com"
OspvDestination	DNS name or IP address of Proxy B, for example proxy.dstdomain.com
OspvSourceDevice	DNS name or IP address of GW A, for example "x.x.x.x"
OspvDestinationDevice	not needed ; empty string ("") in this example
OspvCallingNumber	Calling party's SIP URI – <a href="mailto:888@srcdomain.com">888@srcdomain.com</a>
OspvCalledNumber	Called party's SIP URI – <a href="mailto:1234@proxy.dstdomain.com">1234@proxy.dstdomain.com</a>
ospvCallingNumberFormat	Sip
ospvCalledNumberFormat	Sip
OspvCallId	SIP Call Identifier received in INVITE message
OspvToken	authorization token presented to Proxy B in the INVITE message

The `OSPPTransactionValidateAuthorisation()` function will return an indication of whether or not the call is authorized (`ospvAuthorised`), and, if so, how much service is authorized (`ospvTimeLimit`). After token validation, Proxy B forwards the request to GW B and the call completes.

Step 6: The call is disconnected after a while.

Step 7: Proxy A sends a `<UsageIndication>` message to the OSP server. If Proxy A is not using any protocol extensions, the message will contain the following elements.

<code>&lt;Timestamp&gt;</code>	time of request
<code>&lt;Role&gt;</code>	for Proxy A, source
<code>&lt;TransactionId&gt;</code>	Transaction ID assigned by OSP server in authorization response
<code>&lt;CallId&gt;</code>	SIP Call Identifier used for the call
<code>&lt;SourceInfo type="sip"&gt;</code>	calling party's SIP URI as returned in the authorization response, e.g. <a href="mailto:888@srcdomain.com">888@srcdomain.com</a>
<code>&lt;DeviceInfo type="transport"&gt;</code>	DNS name or IP address of GW A, for example x.x.x.x
<code>&lt;SourceAlternate type="transport"&gt;</code>	DNS name or IP address of Proxy A, for example srcdomain.com
<code>&lt;DestinationInfo type="sip"&gt;</code>	called party's SIP URI as returned in the authorization response, e.g. <a href="mailto:1234@proxy.dstdomain.com">1234@proxy.dstdomain.com</a>
<code>&lt;DestinationAlternate type="transport"&gt;</code>	DNS name or IP address of Proxy B, for example, proxy.dstdomain.com
<code>&lt;UsageDetail&gt;</code>	usage information for the call
<code>&lt;Service/&gt;</code>	empty (for basic service)
<code>&lt;Amount&gt;</code>	amount of service used, e.g. 300
<code>&lt;Increment&gt;</code>	increment of service measurement, e.g. 1
<code>&lt;Unit&gt;</code>	unit of service measurement, e.g. s for seconds

If using the OSP Toolkit, Proxy A can generate that message by calling `OSPPTransactionReportUsage()` with the following significant parameters

ospvDuration	length of the call in seconds, e.g. 300
OspvStartTime	time stamp of when the call started
ospvLossPacketsSent	value ignored (because of following parameter value)
ospvLossFractionSent	-1 if not reported
ospvLossPacketsReceived	value ignored (because of following parameter value)
ospvLossFractionReceived	-1 if not reported

Step 7: Proxy B sends a <UsageIndication> message to the OSP server. If Proxy B is not using any protocol extensions, the message will contain the following elements.

<Timestamp>	Time of request
<Role>	For Proxy B, destination
<TransactionId>	Transaction ID assigned by OSP server in authorization response
<CallId>	SIP Call Identifier used for the call
<SourceInfo type="sip">	calling party's SIP URI as returned in the authorization response, e.g. <a href="mailto:888@srcdomain.com">888@srcdomain.com</a>
<DeviceInfo type="transport">	DNS name or IP address of GW A, for example x.x.x.x
<SourceAlternate type="transport">	DNS name or IP address of Proxy A, for example srcdomain.com
<DestinationInfo type="sip">	called party's SIP URI as returned in the authorization response, e.g. <a href="mailto:1234@proxy.dstdomain.com">1234@proxy.dstdomain.com</a>
<DestinationAlternate type="transport">	DNS name or IP address of Proxy B, for example, proxy.dstdomain.com
<UsageDetail>	usage information for the call
<Service/>	empty (for basic service)
<Amount>	amount of service used, e.g. 300
<Increment>	increment of service measurement, e.g. 1
<Unit>	unit of service measurement, e.g. s for seconds

If using the OSP Toolkit, Proxy B can generate that message by calling OSPPTtransactionReportUsage() with the following significant parameters

ospvDuration	length of the call in seconds, e.g. 300
OspvStartTime	time stamp of when the call started
ospvLossPacketsSent	value ignored (because of following parameter value)
ospvLossFractionSent	-1 if not reported
ospvLossPacketsReceived	value ignored (because of following parameter value)
ospvLossFractionReceived	-1 if not reported

## Call flow 3 (SIP UA to SIP UA through SIP Proxies)

The following diagram illustrates a SIP UA to SIP UA call scenario. However, both user agents are behind proxies. The source UA (Agent A) has (hostId=host.srcdomain.com) and (username=srcua@srcdomain.com). The source proxy has a Fully Qualified Domain Name (FQDN) – srcdomain.com. The destination UA (Agent B) has ([username=dstua@proxy.dstdomain.com](mailto:dstua@proxy.dstdomain.com)) and the destination proxy has a Fully Qualified Domain Name (FQDN) – proxy.dstdomain.com. The source user agent calls the destination user agent.

Step 1: Source user agent (UA A) sends an INVITE message to source proxy (Proxy A). The significant fields within the INVITE message are:

<Request URI>	The URI of the destination device as known to the source UA – <a href="mailto:dstua@srcdomain.com">dstua@srcdomain.com</a>
<CallId>	SIP Call Identifier to be used for the call
<From>	Calling party's SIP URI – <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
<Via>	DNS name or IP address Src UA– host.srcdomain.com
<To>	Called party's SIP URI as known to the source – <a href="mailto:dstua@srcdomain.com">dstua@srcdomain.com</a>

Step 2: Source Proxy sends OSP AuthorizationRequest to OSP Server The significant elements within the <AuthorisationRequest> include

<Timestamp>	Time of request
<CallId>	SIP Call Identifier to be used for the call
<SourceInfo type="sip">	The SIP URI that was passed in the "From" field of the SIP INVITE message – <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
<DeviceInfo type="transport">	DNS name or IP address of Src UA – host.srcdomain.com
<SourceAlternate type="transport">	DNS name or IP address of Proxy A – srcdomain.com
<DestinationInfo type="sip">	The SIP URI that was passed in the "To" field of the SIP INVITE message – <a href="mailto:dstua@srcdomain.com">dstua@srcdomain.com</a>
<Service/>	Empty (for basic service)
<MaximumDestinations>	The maximum number of destinations, including alternatives, Proxy A will consider

If using the OSP Toolkit, Proxy A can generate this message by calling `OSPPTtransactionRequestAuthorisation()` with the following significant parameters:

ospvSource	DNS name or IP address of Proxy A, for example "srcdomain.com"
ospvSourceDevice	DNS name or IP address of Src UA, for example host.srcdomain.com
ospvCallingNumber	The SIP URI that was passed in the "From" field of the SIP INVITE message – <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
ospvCalledNumber	The SIP URI that was passed in the "To" field of the SIP INVITE message – <a href="mailto:dstua@srcdomain.com">dstua@srcdomain.com</a>
ospvCallingNumberFormat	Sip

ospvCalledNumberFormat	Sip
ospvUser	optional user identification; empty string ("") in this example
ospvNumberOfCallIds	the number of SIP Call Identifiers given to the OSP server; if all INVITE attempts for this call will use the same Call Identifier value (as in this example), this parameter value is 1
ospvCallIds	an array (containing, in this example, but a single element) of SIP Call Identifiers; the array structure includes a size field which indicates the size of the value
ospvPreferredDestinations	optional list of preferred destination gateways; empty string ("") in this example
ospvNumberOfDestinations	the maximum number of potential destinations that Gateway A is prepared to consider for the call; for example 3

Step 3: OSP Server replies with an <AuthorisationResponse> message. The message indicates the destination as Proxy B. In particular, the <AuthorisationResponse> contains the following elements.

<Timestamp>	time of response
<Status>	result of response, e.g. <Code>200</Code>
<TransactionId>	transaction identifier assigned by settlement provider
<Destination>	first destination gateway to try for call
<DestinationInfo type="sip">	The SIP URI at which the destination can be contacted – <a href="mailto:dstua@proxy.dstdomain.com">dstua@proxy.dstdomain.com</a>
<DestinationSignalAddress type="transport">	DNS name or IP address of Proxy B, for example proxy.dstdomain.com
<Token>	Authorization token to be passed to Proxy B
<ValidAfter>	time after which token for Proxy B is valid
<ValidUntil>	time until which token for Proxy B is valid
<UsageDetail>	how much service is authorized with Proxy B
<Service/>	Empty (for basic service)
<Amount>	Amount of authorized service, e.g. 3600
<Increment>	Increment of service measurement, e.g. 1
<Unit>	unit of service measurement, e.g. s for seconds
<CallId>	SIP Call Identifier to be used for the call to Proxy B

Step 4: Proxy A sends an INVITE message to Proxy B. The significant fields within the INVITE message are:

<Request URI>	The destination as returned by the OSP Server – <a href="mailto:dstua@proxy.dstdomain.com">dstua@proxy.dstdomain.com</a>
<CallId>	SIP Call Identifier to be used for the call
<From>	Calling party's SIP URI – <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
<Via>	DNS name or IP address of Proxy A – srcdomain.com
<Via>	DNS name or IP address of User Agent A – host.srcdomain.com
<To>	Called party's SIP URI that was present in the original request – <a href="mailto:dstua@srcdomain.com">dstua@srcdomain.com</a>

&lt;Token&gt;

The token sent by the OSP Server in the Authorization Response.

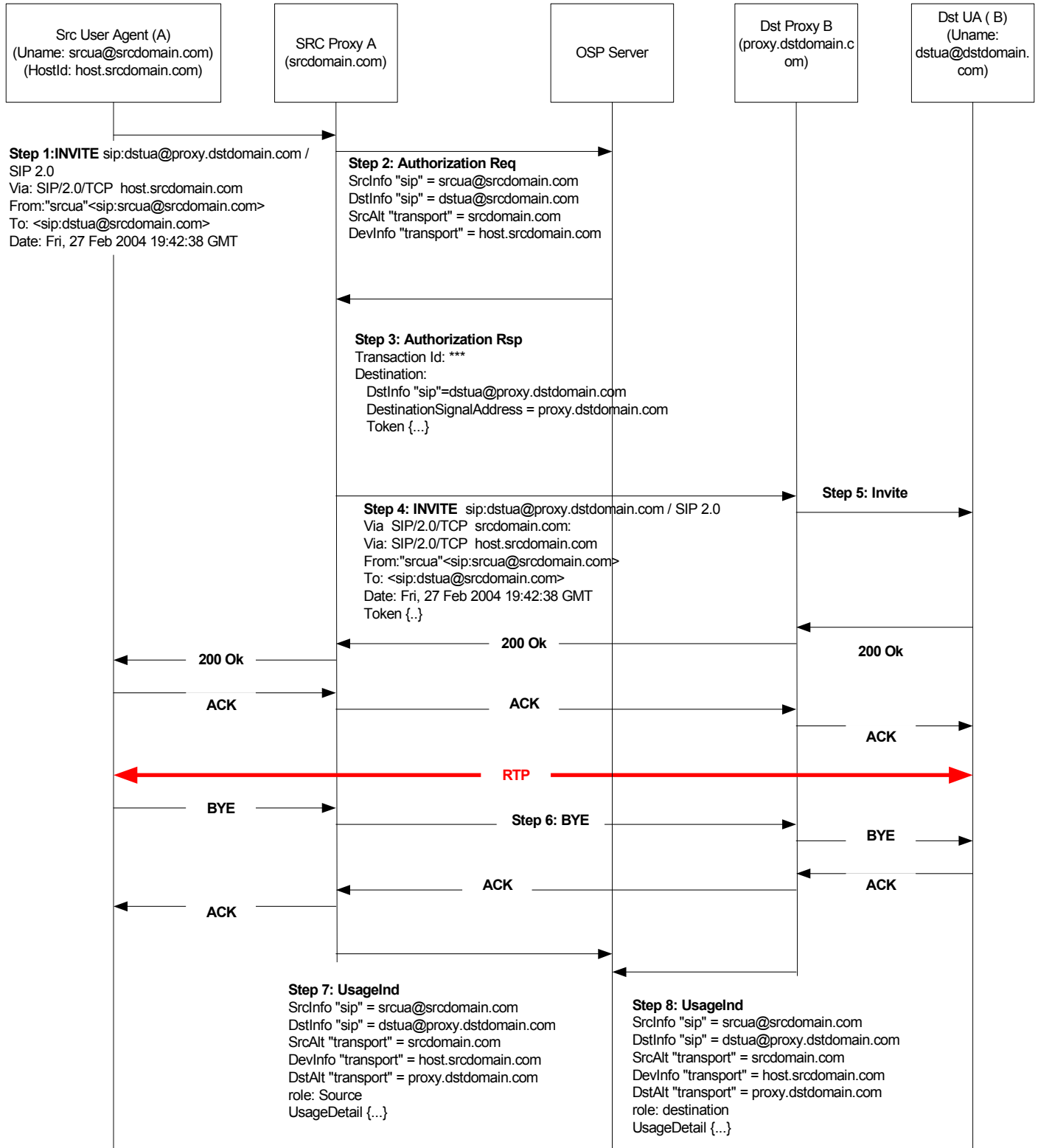
Step 5: Proxy B validates the token and accepts the call. If using the OSP Toolkit, Proxy B must call the Toolkit function `OSPPTransactionValidateAuthorisation()` to verify the authorization token in the INVITE message.

It would call it with the following parameters.

<code>OspvSource</code>	DNS name or IP address of Proxy A, for example "srcdomain.com"
<code>OspvDestination</code>	DNS name or IP address of Proxy B, for example proxy.dstdomain.com
<code>OspvSourceDevice</code>	DNS name or IP address of user agent A, for example "host.srcdomain.com"
<code>OspvDestinationDevice</code>	not needed ; empty string ("") in this example
<code>OspvCallingNumber</code>	Calling party's SIP URI – <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
<code>OspvCalledNumber</code>	Called party's SIP URI – <a href="mailto:dstua@proxy.dstdomain.com">dstua@proxy.dstdomain.com</a>
<code>ospvCallingNumberFormat</code>	Sip
<code>ospvCalledNumberFormat</code>	Sip
<code>OspvCallId</code>	SIP Call Identifier received in INVITE message
<code>OspvToken</code>	authorization token presented to Proxy B in the INVITE message

The `OSPPTransactionValidateAuthorisation()` function will return an indication of whether or not the call is authorized (`ospvAuthorised`), and, if so, how much service is authorized (`ospvTimeLimit`). After token validation, Proxy B forwards the request to the destination user agent (UA B) and the call completes.

Call Scenario: UA to UA



Step 6: The call is disconnected after a while.

Step 7: Proxy A sends a <UsageIndication> message to the OSP server. If Proxy A is not using any protocol extensions, the message will contain the following elements.

<Timestamp>	time of request
<Role>	for Proxy A, <i>source</i>
<TransactionId>	Transaction ID assigned by OSP server in authorization response
<CallId>	SIP Call Identifier used for the call
<SourceInfo type="sip">	calling party's SIP URI as returned in the authorization response, e.g. <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
<DeviceInfo type="transport">	DNS name or IP address of UA A, for example <a href="http://host.srcdomain.com">host.srcdomain.com</a>
<SourceAlternate type="transport">	DNS name or IP address of Proxy A, for example <a href="http://srcdomain.com">srcdomain.com</a>
<DestinationInfo type="sip">	called party's SIP URI as returned in the authorization response, e.g. <a href="mailto:dstua@proxy.dstdomain.com">dstua@proxy.dstdomain.com</a>
<DestinationAlternate type="transport">	DNS name or IP address of Proxy B, for example, <a href="http://proxy.dstdomain.com">proxy.dstdomain.com</a>
<UsageDetail>	Usage information for the call
<Service/>	Empty (for basic service)
<Amount>	Amount of service used, e.g. 300
<Increment>	Increment of service measurement, e.g. 1
<Unit>	Unit of service measurement, e.g. s for seconds

If using the OSP Toolkit, Proxy A can generate that message by calling `OSPPTransactionReportUsage()` with the following significant parameters

<code>ospvDuration</code>	length of the call in seconds, e.g. 300
<code>OspvStartTime</code>	time stamp of when the call started
<code>ospvLossPacketsSent</code>	value ignored (because of following parameter value)
<code>ospvLossFractionSent</code>	-1 if not reported
<code>ospvLossPacketsReceived</code>	value ignored (because of following parameter value)
<code>ospvLossFractionReceived</code>	-1 if not reported

Step 8: Proxy B sends a <UsageIndication> message to the OSP server. If Proxy B is not using any protocol extensions, the message will contain the following elements.

<Timestamp>	Time of request
<Role>	For Proxy B, <i>destination</i>
<TransactionId>	Transaction ID assigned by OSP server in authorization response
<CallId>	SIP Call Identifier used for the call
<SourceInfo type="sip">	calling party's SIP URI as returned in the authorization

	response, e.g. <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
<DeviceInfo type="transport">	DNS name or IP address of user agent A, for example host.srcdomain.com
<SourceAlternate type="transport">	DNS name or IP address of Proxy A, for example srcdomain.com
<DestinationInfo type="sip">	Called party's SIP URI as returned in the authorization response, e.g. <a href="mailto:dstua@proxy.dstdomain.com">dstua@proxy.dstdomain.com</a>
<DestinationAlternate type="transport">	DNS name or IP address of Proxy B, for example, proxy.dstdomain.com
<UsageDetail>	usage information for the call
<Service/>	empty (for basic service)
<Amount>	amount of service used, e.g. 300
<Increment>	increment of service measurement, e.g. 1
<Unit>	unit of service measurement, e.g. s for seconds

If using the OSP Toolkit, Proxy B can generate that message by calling `OSPPTTransactionReportUsage()` with the following significant parameters

<code>ospvDuration</code>	length of the call in seconds, e.g. 300
<code>ospvStartTime</code>	time stamp of when the call started
<code>ospvLossPacketsSent</code>	value ignored (because of following parameter value)
<code>ospvLossFractionSent</code>	-1 if not reported
<code>ospvLossPacketsReceived</code>	value ignored (because of following parameter value)
<code>ospvLossFractionReceived</code>	-1 if not reported

## Call flow 4 (SIP UA to SIP UA using ENUM numbering scheme)

The following diagram illustrates a SIP UA to SIP UA call scenario using enum-numbering scheme. The source UA (Agent A) has (hostId=host.srcdomain.com) and (username=srcua@srcdomain.com). The source proxy has a FQDN – srcdomain.com. The destination UA (Agent B) has (username=dstua@proxy.dstdomain.com) and the destination proxy has a FQDN – proxy.dstdomain.com. The source UA, however, knows the destination UA with its e.164 number (1234). The source user agent calls the destination user agent.

Step 1: Source user agent (UA A) sends an INVITE message to source proxy (Proxy A). The significant fields within the INVITE message are:

<Request URI>	The URI of the destination device as known to the source UA – <a href="mailto:1234@srcdomain.com">1234@srcdomain.com</a>
<CallId>	SIP Call Identifier to be used for the call
<From>	Calling party's SIP URI – <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
<Via>	DNS name or IP address Src UA– host.srcdomain.com
<To>	Called party's SIP URI as known to the source – <a href="mailto:1234@srcdomain.com">1234@srcdomain.com</a>

Step 2: Source Proxy sends OSP AuthorizationRequest to OSP Server. However, before sending the request, the proxy converts the e164 number contained in the To field of the sip URI to its ENUM equivalent. The significant elements within the <AuthorisationRequest> include

<Timestamp>	Time of request
<CallId>	SIP Call Identifier to be used for the call
<SourceInfo type="sip">	The SIP URI that was passed in the "From" field of the SIP INVITE message – <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
<DeviceInfo type="transport">	DNS name or IP address of Src UA – host.srcdomain.com
<SourceAlternate type="transport">	DNS name or IP address of Proxy A – srcdomain.com
<DestinationInfo type="url">	The ENUM converted e.164 number that was contained in SIP URI, which was passed in the "To" field of the SIP INVITE message – 4.3.2.1.e164.arpa
<Service/>	Empty (for basic service)
<MaximumDestinations>	The maximum number of destinations, including alternatives, Proxy A will consider

If using the OSP Toolkit, Proxy A can generate this message by calling `OSPPTtransactionRequestAuthorisation()` with the following significant parameters:

ospvSource	DNS name or IP address of Proxy A, for example "srcdomain.com"
ospvSourceDevice	DNS name or IP address of Src UA, for example host.srcdomain.com
ospvCallingNumber	The SIP URI that was passed in the "From" field of the SIP INVITE message – <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
ospvCalledNumber	The ENUM converted e.164 number that was contained in SIP URI, which was passed in the "To" field of the SIP INVITE message –

	4.3.2.1.e164.arpa
ospvCallingNumberFormat	Sip
ospvCalledNumberFormat	url
ospvUser	optional user identification; empty string ("") in this example
ospvNumberOfCallIds	the number of SIP Call Identifiers given to the OSP server; if all INVITE attempts for this call will use the same Call Identifier value (as in this example), this parameter value is 1
ospvCallIds	an array (containing, in this example, but a single element) of SIP Call Identifiers; the array structure includes a size field which indicates the size of the value
ospvPreferredDestinations	optional list of preferred destination gateways; empty string ("") in this example
ospvNumberOfDestinations	the maximum number of potential destinations that Gateway A is prepared to consider for the call; for example 3

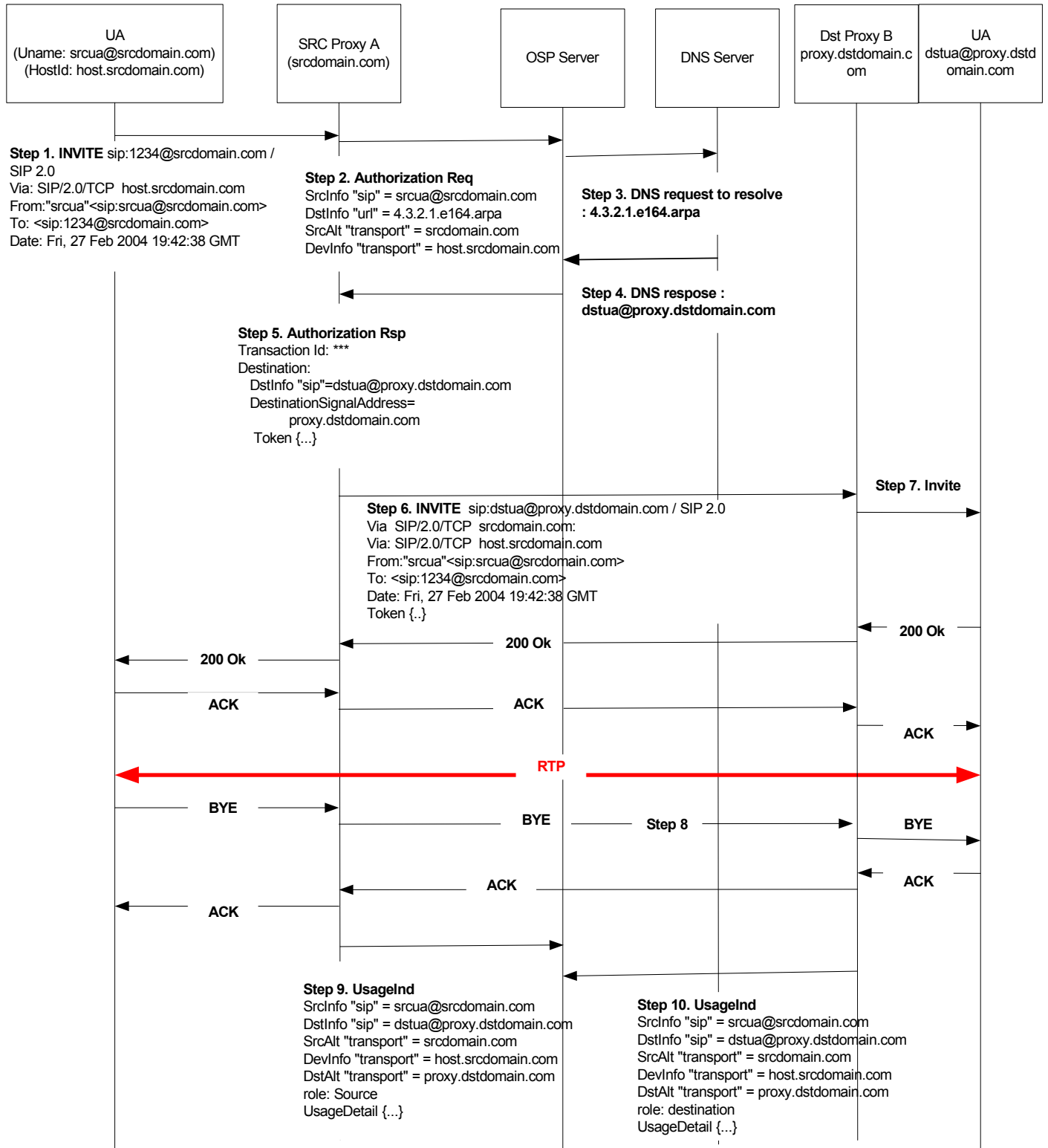
Step 3: OSP Server is not able to resolve the e.164 number locally. It thus sends a DNS query to resolve the destination e.164 number (1234) .

Step 4: The directory server replies back to the OSP Server with the SIP URI ([dstua@proxy.dstdomain.com](mailto:dstua@proxy.dstdomain.com)) that corresponds to the e.164 number (1234).

Step 5: OSP Server replies with an <AuthorisationResponse> message. The message indicates the destination as Proxy B. In particular, the <AuthorisationResponse> contains the following elements.

<Timestamp>	time of response
<Status>	result of response, e.g. <Code>200</Code>
<TransactionId>	transaction identifier assigned by settlement provider
<Destination>	first destination gateway to try for call
<DestinationInfo type="sip">	The SIP URI at which the destination can be contacted – <a href="mailto:dstua@proxy.dstdomain.com">dstua@proxy.dstdomain.com</a>
<DestinationSignalAddress type="transport">	DNS name or IP address of Proxy B, for example proxy.dstdomain.com
<Token>	Authorization token to be passed to Proxy B
<ValidAfter>	time after which token for Proxy B is valid
<ValidUntil>	time until which token for Proxy B is valid
<UsageDetail>	how much service is authorized with Proxy B
<Service/>	Empty (for basic service)
<Amount>	Amount of authorized service, e.g. 3600
<Increment>	Increment of service measurement, e.g. 1
<Unit>	unit of service measurement, e.g. s for seconds
<CallId>	SIP Call Identifier to be used for the call to Proxy B

Call Scenario: UA to UA (using ENUM numbering scheme)



Step 6: Proxy A sends an INVITE message to Proxy B. The significant fields within the INVITE message are:

<Request URI>	The destination as returned by the OSP Server – <a href="mailto:dstua@proxy.dstdomain.com">dstua@proxy.dstdomain.com</a>
<CallId>	SIP Call Identifier to be used for the call
<From>	Calling party's SIP URI – <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
<Via>	DNS name or IP address of Proxy A – srcdomain.com
<Via>	DNS name or IP address of User Agent A – host.srcdomain.com
<To>	Called party's SIP URI that was present in the original request – <a href="mailto:1234@srcdomain.com">1234@srcdomain.com</a>
<Token>	The token sent by the OSP Server in the Authorization Response.

Step 7: Proxy B validates the token and accepts the call. If using the OSP Toolkit, Proxy B must call the Toolkit function `OSPPTransactionValidateAuthorisation()` to verify the authorization token in the INVITE message.

It would call it with the following parameters.

<code>OspvSource</code>	DNS name or IP address of Proxy A, for example "srcdomain.com"
<code>OspvDestination</code>	DNS name or IP address of Proxy B, for example proxy.dstdomain.com
<code>OspvSourceDevice</code>	DNS name or IP address of user agent A, for example "host.srcdomain.com"
<code>OspvDestinationDevice</code>	not needed ; empty string ("") in this example
<code>OspvCallingNumber</code>	Calling party's SIP URI – <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
<code>OspvCalledNumber</code>	Called party's SIP URI – <a href="mailto:dstua@proxy.dstdomain.com">dstua@proxy.dstdomain.com</a>
<code>ospvCallingNumberFormat</code>	Sip
<code>ospvCalledNumberFormat</code>	Sip
<code>OspvCallId</code>	SIP Call Identifier received in INVITE message
<code>OspvToken</code>	authorization token presented to Proxy B in the INVITE message

The `OSPPTransactionValidateAuthorisation()` function will return an indication of whether or not the call is authorized (`ospvAuthorised`), and, if so, how much service is authorized (`ospvTimeLimit`). After token validation, Proxy B forwards the request to the destination user agent (UA B) and the call completes.

Step 8: The call is disconnected after a while.

Step 9: Proxy A sends a <UsageIndication> message to the OSP server. If Proxy A is not using any protocol extensions, the message will contain the following elements.

<Timestamp>	time of request
<Role>	for Proxy A, source
<TransactionId>	Transaction ID assigned by OSP server in authorization response
<CallId>	SIP Call Identifier used for the call

<SourceInfo type="sip">	calling party's SIP URI as returned in the authorization response, e.g. <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
<DeviceInfo type="transport">	DNS name or IP address of UA A, for example host.srcdomain.com
<SourceAlternate type="transport">	DNS name or IP address of Proxy A, for example srcdomain.com
<DestinationInfo type="sip">	called party's SIP URI as returned in the authorization response, e.g. <a href="mailto:dstua@proxy.dstdomain.com">dstua@proxy.dstdomain.com</a>
<DestinationAlternate type="transport">	DNS name or IP address of Proxy B, for example, proxy.dstdomain.com
<UsageDetail>	Usage information for the call
<Service/>	Empty (for basic service)
<Amount>	Amount of service used, e.g. 300
<Increment>	Increment of service measurement, e.g. 1
<Unit>	Unit of service measurement, e.g. s for seconds

If using the OSP Toolkit, Proxy A can generate that message by calling `OSPPTransactionReportUsage()` with the following significant parameters

<code>ospvDuration</code>	length of the call in seconds, e.g. 300
<code>OspvStartTime</code>	time stamp of when the call started
<code>ospvLossPacketsSent</code>	value ignored (because of following parameter value)
<code>ospvLossFractionSent</code>	-1 if not reported
<code>ospvLossPacketsReceived</code>	value ignored (because of following parameter value)
<code>ospvLossFractionReceived</code>	-1 if not reported

Step 10: Proxy B sends a `<UsageIndication>` message to the OSP server. If Proxy B is not using any protocol extensions, the message will contain the following elements.

<Timestamp>	Time of request
<Role>	For Proxy B, destination
<TransactionId>	Transaction ID assigned by OSP server in authorization response
<CallId>	SIP Call Identifier used for the call
<SourceInfo type="sip">	calling party's SIP URI as returned in the authorization response, e.g. <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
<DeviceInfo type="transport">	DNS name or IP address of user agent A, for example host.srcdomain.com
<SourceAlternate type="transport">	DNS name or IP address of Proxy A, for example srcdomain.com
<DestinationInfo type="sip">	Called party's SIP URI as returned in the authorization response, e.g. <a href="mailto:dstua@proxy.dstdomain.com">dstua@proxy.dstdomain.com</a>
<DestinationAlternate type="transport">	DNS name or IP address of Proxy B, for example, proxy.dstdomain.com
<UsageDetail>	usage information for the call

<Service/>	empty (for basic service)
<Amount>	amount of service used, e.g. 300
<Increment>	increment of service measurement, e.g. 1
<Unit>	unit of service measurement, e.g. s for seconds

If using the OSP Toolkit, Proxy B can generate that message by calling `OSPPTransactionReportUsage()` with the following significant parameters

<code>ospvDuration</code>	length of the call in seconds, e.g. 300
<code>OspvStartTime</code>	time stamp of when the call started
<code>ospvLossPacketsSent</code>	value ignored (because of following parameter value)
<code>ospvLossFractionSent</code>	-1 if not reported
<code>ospvLossPacketsReceived</code>	value ignored (because of following parameter value)
<code>ospvLossFractionReceived</code>	-1 if not reported

## Call flow 5 (SIP UA to H323 GW using look ahead route)

The following diagram illustrates a SIP UA to H323 GW call scenario. The source UA (Agent A) has (hostId=host.srcdomain.com) and (username=srcua@srcdomain.com). The source proxy has a Fully Qualified Domain Name (FQDN) – srcdomain.com. The destination GW has ip address – [x.x.x.x] and the destination inter-working device has a Fully Qualified Domain Name (FQDN) – dstdomain.com. The source user agent calls the destination.

Step 1: Source user agent (UA A) sends an INVITE message to source proxy (Proxy A). The significant fields within the INVITE message are:

<Request URI>	The URI of the destination device as known to the source UA – <a href="mailto:1234@srcdomain.com">1234@srcdomain.com</a> . The URI has the e.164 number embedded.
<CallId>	SIP Call Identifier to be used for the call
<From>	Calling party's SIP URI – <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
<Via>	DNS name or IP address Src UA– host.srcdomain.com
<To>	Called party's SIP URI as known to the source – <a href="mailto:1234@srcdomain.com">1234@srcdomain.com</a>

Step 2: The Src Proxy sends OSP AuthorizationRequest to OSP Server The significant elements within the <AuthorisationRequest> include

<Timestamp>	Time of request
<CallId>	SIP Call Identifier to be used for the call
<SourceInfo type="sip">	The SIP URI that was passed in the "From" field of the SIP INVITE message – <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
<DeviceInfo type="transport">	DNS name or IP address of the SIP UA – host.srcdomain.com
<SourceAlternate type="transport">	DNS name or IP address of Src Proxy – srcdomain.com
<DestinationInfo type="sip">	The SIP URI that was passed in the "To" field of the SIP INVITE message – <a href="mailto:1234@srcdomain.com">1234@srcdomain.com</a>
<Service/>	Empty (for basic service)
<MaximumDestinations>	The maximum number of destinations, including alternatives, the redirect server will consider

If using the OSP Toolkit, Redirect Server can generate this message by calling OSPPTtransactionRequestAuthorisation() with the following significant parameters:

OspvSource	DNS name or IP address of the Src Proxy , for example "srcdomain.com"
OspvSourceDevice	DNS name or IP address of user agent, for example host.srcdomain.com
OspvCallingNumber	The SIP URI that was passed in the "From" field of the SIP INVITE message – <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
OspvCalledNumber	The SIP URI that was passed in the "To" field of the SIP INVITE message – <a href="mailto:1234@srcdomain.com">1234@srcdomain.com</a>

ospvCallingNumberFormat	Sip
ospvCalledNumberFormat	Sip
OspvUser	Optional user identification; empty string ("") in this example
OspvNumberOfCallIds	the number of SIP Call Identifiers given to the OSP server; if all INVITE attempts for this call will use the same Call Identifier value (as in this example), this parameter value is 1
OspvCallIds	an array (containing, in this example, but a single element) of SIP Call Identifiers; the array structure includes a size field which indicates the size of the value
OspvPreferredDestinations	optional list of preferred destination gateways; empty string ("") in this example
OspvNumberOfDestinations	the maximum number of potential destinations that Gateway A is prepared to consider for the call; for example 3

Step 3: OSP Server replies with an `<AuthorisationResponse>` message. The message indicates the destination as the inter-working device. The token contains the look ahead route – [x.x.x.x] embedded in the token. In particular, the `<AuthorisationResponse>` contains the following elements.

<code>&lt;Timestamp&gt;</code>	time of response
<code>&lt;Status&gt;</code>	result of response, e.g. <code>&lt;Code&gt;200&lt;/Code&gt;</code>
<code>&lt;TransactionId&gt;</code>	transaction identifier assigned by settlement provider
<code>&lt;Destination&gt;</code>	first destination gateway to try for call
<code>&lt;DestinationInfo     type="sip"&gt;</code>	The SIP URI at which the destination can be contacted – <a href="mailto:1234@dstdomain.com">1234@dstdomain.com</a>
<code>&lt;DestinationSignalAddress     type="transport"&gt;</code>	DNS name or IP address of Inter-working device, for example <code>dstdomain.com</code>
<code>&lt;Token&gt;</code>	Authorization token to be passed to the inter-working device
<code>DestinationAlternate     type="transport"&gt;</code>	The look ahead route – [x.x.x.x]
<code>DestinationProtocol</code>	h.323-q931 (Indicating the protocol for x.x.x.x device)
<code>OSPVersion</code>	0.0.0 (Indicating Non-OSP device)
<code>&lt;ValidAfter&gt;</code>	time after which token for the inter-working device is valid
<code>&lt;ValidUntil&gt;</code>	time until which token for the inter-working device is valid
<code>&lt;UsageDetail&gt;</code>	how much service is authorized with the inter-working device
<code>&lt;Service/&gt;</code>	Empty (for basic service)
<code>&lt;Amount&gt;</code>	Amount of authorized service, e.g. 3600
<code>&lt;Increment&gt;</code>	Increment of service measurement, e.g. 1
<code>&lt;Unit&gt;</code>	unit of service measurement, e.g. s for seconds
<code>&lt;CallId&gt;</code>	SIP Call Identifier to be used for the call to the inter-working device

Step 4: Proxy A sends an INVITE message to the inter-working device. The significant fields within the INVITE message are:

<code>&lt;Request URI&gt;</code>	The destination as returned by the OSP Server- <a href="mailto:1234@dstdomain.com">1234@dstdomain.com</a>
----------------------------------	---

<CallId>	SIP Call Identifier to be used for the call
<From>	Calling party's SIP URI – <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
<Via>	DNS name or IP address of Src Proxy – srcdomain.com
<Via>	DNS name or IP address of User Agent – host.srcdomain.com
<To>	Called party's SIP URI that was present in the original request – <a href="mailto:1234@srcdomain.com">1234@srcdomain.com</a>
<Token>	The token sent by the OSP Server in the Authorization Response.

Step 5: The inter-working device validates the token and accepts the call. If using the OSP Toolkit, device must call the Toolkit function `OSPPTTransactionValidateAuthorisation()` to verify the authorization token in the INVITE message.

It would call the API with the following parameters.

<code>OspvSource</code>	DNS name or IP address of Proxy A, for example "srcdomain.com"
<code>OspvDestination</code>	DNS name or IP address of Proxy B, for example "dstdomain.com"
<code>OspvSourceDevice</code>	DNS name or IP address of user agent A, for example "host.srcdomain.com"
<code>OspvDestinationDevice</code>	not needed ; empty string ("") in this example
<code>OspvCallingNumber</code>	Calling party's SIP URI – <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
<code>OspvCalledNumber</code>	Called party's SIP URI – <a href="mailto:1234@dstdomain.com">1234@dstdomain.com</a>
<code>ospvCallingNumberFormat</code>	Sip
<code>ospvCalledNumberFormat</code>	Sip
<code>OspvCallId</code>	SIP Call Identifier received in INVITE message
<code>OspvToken</code>	authorization token presented to Proxy B in the INVITE message

The `OSPPTTransactionValidateAuthorisation()` function will return an indication of whether or not the call is authorized (`ospvAuthorised`), and, if so, how much service is authorized (`ospvTimeLimit`). After token validation, the inter-working device forwards the request to the destination GW which then completes the call.

In order to get the look ahead route, the inter-working device calls the `OSPPTTransactionGetLookAheadInfoIfPresent` API with the following parameters:

<code>ospvTransaction</code>	Transaction identifier of the previously created transaction
<code>ospvIsLookAheadInfoPresent</code>	Memory location that tells the device if look ahead route is present.
<code>ospvLookAheadDestination</code>	Memory location that tells the device about the look ahead route, e.g., "[x.x.x.x]"
<code>ospvLookAheadDestProt</code>	Memory location that stores the protocol for the look ahead destination, e.g., h323-q931
<code>ospvLookAheadDestOSPStatus</code>	Memory location that stores the OSP version for the look ahead destination. E.g., 0.0.0

The inter-working device then forwards a Q.931 setup message to the destination GW that completes the call.

Step 6: The call is disconnected after a while.

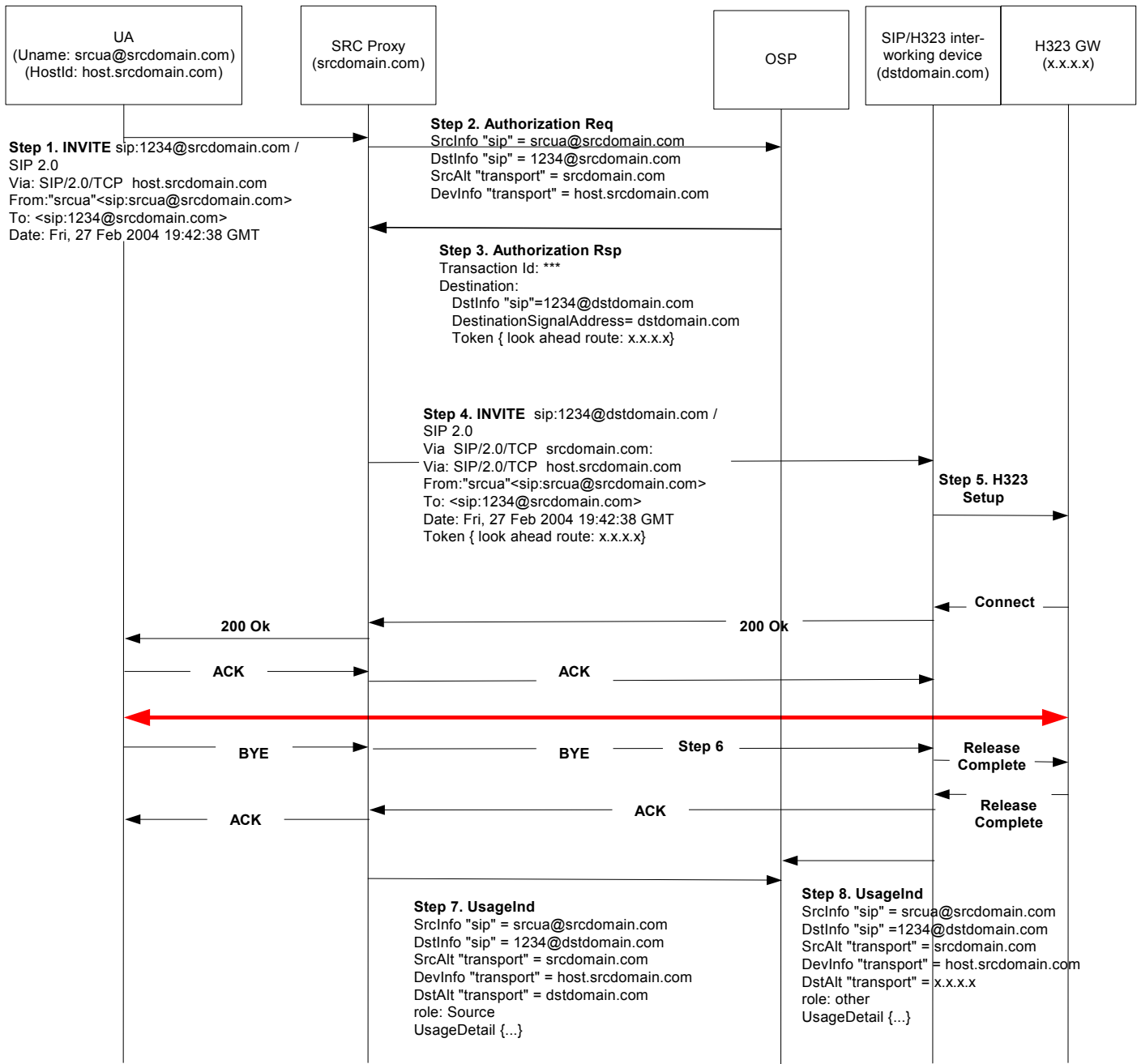
Step 7: Src Proxy A sends a <UsageIndication> message to the OSP server. If Proxy A is not using any protocol extensions, the message will contain the following elements.

<Timestamp>	Time of request
<Role>	For Proxy A, source
<TransactionId>	Transaction ID assigned by OSP server in authorization response
<CallId>	SIP Call Identifier used for the call
<SourceInfo type="sip">	calling party's SIP URI as returned in the authorization response, e.g. <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
<DeviceInfo type="transport">	DNS name or IP address of UA A, for example host.srcdomain.com
<SourceAlternate type="transport">	DNS name or IP address of Proxy A, for example srcdomain.com
<DestinationInfo type="sip">	called party's SIP URI as returned in the authorization response, e.g. <a href="mailto:1234@stdomain.com">1234@stdomain.com</a>
<DestinationAlternate type="transport">	DNS name or IP address of the inter-working device, for example, dstdomain.com
<UsageDetail>	Usage information for the call
<Service/>	Empty (for basic service)
<Amount>	Amount of service used, e.g. 300
<Increment>	Increment of service measurement, e.g. 1
<Unit>	Unit of service measurement, e.g. s for seconds

If using the OSP Toolkit, Proxy A can generate that message by calling `OSPPTransactionReportUsage()` with the following significant parameters

<code>ospvDuration</code>	length of the call in seconds, e.g. 300
<code>OspvStartTime</code>	time stamp of when the call started
<code>ospvLossPacketsSent</code>	value ignored (because of following parameter value)
<code>ospvLossFractionSent</code>	-1 if not reported
<code>ospvLossPacketsReceived</code>	value ignored (because of following parameter value)
<code>ospvLossFractionReceived</code>	-1 if not reported

Call Scenario: OSP w/ h323 inter-working device and look ahead route



Step 8: The inter-working device sends a <UsageIndication> message to the OSP server. If the device is not using any protocol extensions, the message will contain the following elements.

<Timestamp>	Time of request
<Role>	For inter-working device, <i>other</i>
<TransactionId>	Transaction ID assigned by OSP server in authorization response
<CallId>	SIP Call Identifier used for the call
<SourceInfo type="sip">	calling party's SIP URI as returned in the authorization response, e.g. <a href="mailto:srcua@srcdomain.com">srcua@srcdomain.com</a>
<DeviceInfo type="transport">	DNS name or IP address of user agent A, for example <a href="http://host.srcdomain.com">host.srcdomain.com</a>
<SourceAlternate type="transport">	DNS name or IP address of Proxy A, for example <a href="http://srcdomain.com">srcdomain.com</a>
<DestinationInfo type="sip">	Called party's SIP URI as returned in the authorization response, e.g. <a href="mailto:1234@dstdomain.com">1234@dstdomain.com</a>
<DestinationAlternate type="transport">	DNS name or IP address of the inter-working device, for example, <a href="http://dstdomain.com">dstdomain.com</a>
<UsageDetail>	usage information for the call
<Service/>	empty (for basic service)
<Amount>	Amount of service used, e.g. 300
<Increment>	Increment of service measurement, e.g. 1
<Unit>	unit of service measurement, e.g. s for seconds

If using the OSP Toolkit, the inter-working device can generate that message by calling `OSPPTTransactionReportUsage()` with the following significant parameters

<code>ospvDuration</code>	length of the call in seconds, e.g. 300
<code>OspvStartTime</code>	time stamp of when the call started
<code>ospvLossPacketsSent</code>	value ignored (because of following parameter value)
<code>ospvLossFractionSent</code>	-1 if not reported
<code>ospvLossPacketsReceived</code>	value ignored (because of following parameter value)
<code>ospvLossFractionReceived</code>	-1 if not reported