Lawful Intercept Interface

Specification Guide

Release 14.0

Document Version 1

220 Perry Parkway
Gaithersburg, MD USA 20877
Tel +1 301.977.9440
Fax +1 301.977.8846

WWW.BROADSOFT.COM

BroadWorks® Guide

Copyright Notice

Trademarks

Document Revision History

Release	Version	Reason for Change	Date	Author
14.0	1	Updated document for re-branding.	February 3, 2006	Roberta Boyle
14.0	1	Updated CLI information.	March 29, 2006	Michael Boyle
14.0	1	Updated with Release 14 enhancements: ▪ JSTD025a CDC format ▪ calloutETSI call content link type ▪ Optional Calling Line ID (CLID)	August 3, 2006	Martin Perron
14.0	1	Edited document.	September 06, 2006	Patricia Renaud
14.0	1	Made minor editorial changes.	September 13, 2006	Martin Perron
14.0	1	Edited document.	September 15, 2006	Patricia Renaud

Table of Contents

Table of Figures

1 Overview

BroadWorks implements lawful interception according to the Communication Assistance for the Law Enforcement Act (CALEA) requirements set forth in the following documents:

- *J-STD-025A, TIA and ANSI Committee T1, Lawfully Authorized Electronic Surveillance, May 2000*
- *J-STD-025B, TIA and ANSI Committee T1, Lawfully Authorized Electronic Surveillance, December 2003*

BroadWorks also implements lawful interception according to the following ETSI specification. In this case, it is expected that a mediation system will transform the JSTD interception data into ETSI interception data.

- *Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic; ETSI ES 201 671 V2.1.1 (2001-09)*

The lawful intercept administrator uses the surveillance administration function to assign surveillances to users. The BroadWorks Application Server command line interface (CLI) is the interface used to perform the administration functions.

During a call interception, a Call Data Channel (CDC) is set up between the Application Server and the Lawful Enforcement Agency (LEA)/Mediation Device (MD). The Application Server encodes the following call processing events in ASN.1 format using Basic Encoding Rules (BER):

- Origination
- Termination Attempt
- Answer
- SubjectSignal
- NetworkSignal
- DialedDigitExtraction
- Redirection
- Release
- Connection/ConnectionBreak
- CCOpen
- CCChange
- CCClose
- ServingSystem

Also, if media monitoring is enabled for a particular surveillance, the Application Server sets up two Call Content Channels (CCCs) to the LEA/MD. The transmitted media and the received media are both delivered to the LEA/MD on separate CCCs.

The purpose of this document is to provide a detailed description of the BroadWorks Lawful Intercept interface. This document covers:

- Functional description of the BroadWorks Lawful Intercept interface.
- Administration functionality for BroadWorks Lawful Intercept interface.

- Detailed description of the Lawful Intercept events generated by BroadWorks over the CDC.
- Call scenarios involving the generation of Lawful Intercept events and the delivery of media over CCCs.

1.1 Summary of Changes for Releases 13 and 14

1.1.1 CLID for Outgoing Calls to LEA

An optional calling line ID (CLID) is configurable on callout-type call content links. If configured, the CLID is used for outgoing calls made to the Law Enforcement Agency (LEA) device instead of the monitored user's phone number.

1.1.2 JSTD025A-compliant CDC Format

The administrator can configure the format of messages sent to the LEA over the Call Data Channel (CDC). In Release 14, a JSTD025A-compliant format can be configured for the CDC. This is in addition to the existing BroadWorks format.

1.1.3 ETSI Specification Compliance

For compliance with ETSI lawful intercept specifications (ES 201 671), correlation information is inserted in the Call Content Channel (CCC) SIP INVITE and mapped to the PRI User-to-User parameter (UUS1) by a SIP/PRI gateway. It allows the Law Enforcement Agency (LEA) to map a CCC stream to a Call Data Channel (CDC) stream (also known as IRI in ETSI terminology) instead of using the CCC phone number.

1.1.4 Call Redirections

Prior to this release, the call identifier for a call trace would change upon reporting a redirection via the CDC. The redirection message would include the former call identifier and the new call identifier. With this release, the call identifier for a call trace remains the same for the duration of the call and only the redirection message includes the unique call identifier for that call trace. Sections *4 Event Definitions* and *5 BroadWorks ASN.1 Definitions* have been modified to reflect this change.

2 Functional Description

The BroadWorks Application Server determines whether a call needs to be monitored and manages the CDC and CCC to the LEA/MD. The Application Server intercepts call signaling and sends the appropriate Lawful Intercept events to the LEA/MD over the CDC.

The BroadWorks Media Server is used as a proxy for the interception of the call contents for calls involving a subject under surveillance. Each time a call involving call content interception or dialed digit extraction is set up by the Application Server, the endpoints are instructed to send their media to the Media Server, as opposed to being sent directly to the opposite endpoint. This media relay is necessary so that the intercepted call content can be delivered to the LEA/MD or so that dialed digits can be extracted from the media stream and delivered to the LEA/MD as call-identifying information.

The following figure shows the Lawful Intercept interfaces. Notice that the network gateway shown in the diagram is an alternative for terminating the CCCs from BroadWorks. Interfaces and other alternatives for terminating the CCCs are described in the following sections.

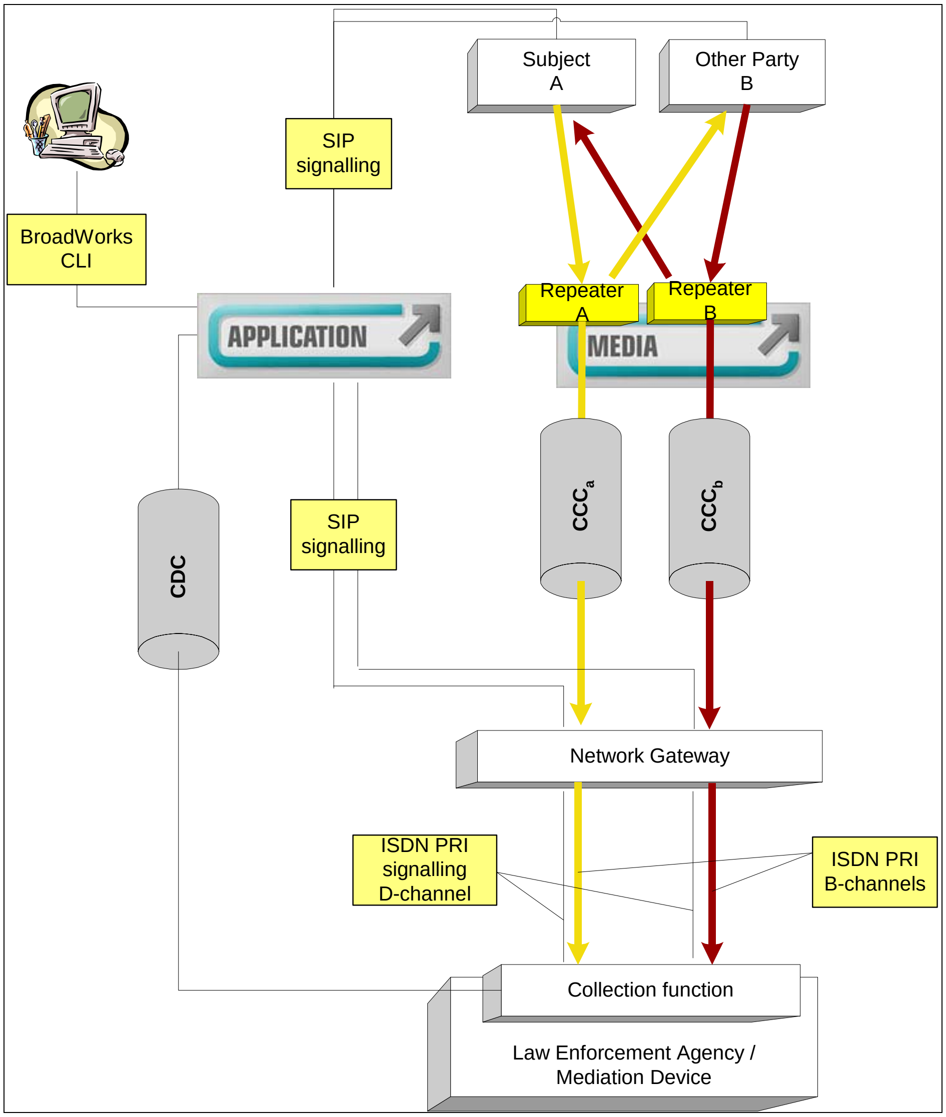


Figure 1 Lawful Intercept Interfaces

The lawful intercept administrator uses the BroadWorks command line interface (CLI) to assign and configure surveillances on users and to define call content links for the delivery of intercepted media. Details for CLI commands are provided in section *3 Administration Functions*.

2.1 Surveillances

A user can be assigned up to five surveillances, typically for different law enforcement agencies (LEAs). The lawful intercept administrator enters five individual surveillances for the user.

For each surveillance type, the lawful intercept administrator enters a case identifier. This case identifier is provided by the LEA and is unique across all surveillances assigned to the user. It is also unique across all surveillances requested for by the LEA. The Application Server uses this case identifier in all Lawful Intercept events it sends to the LEA/MD over the CDC. The LEA/MD uses the case identifier to distinguish all incoming messages across this CDC.

Upon entering a surveillance type for a user, the lawful intercept administrator is also prompted for the following information:

- Type of surveillance: event monitoring only or event and media monitoring
- IP address and port of LEA/MD's to use for CDC
- Call content link of LEA/MD to use for CCC

The surveillances are independently provisioned and can be set to send Lawful Intercept events to different LEA/MDs over different CDCs.

Similarly, surveillances can be set so that the intercepted media is repeated to different LEA/MDs over different call content links.

2.2 Call Content Links

A call content link is an aggregation of resources that is used by the Application Server when setting up CCCs to the LEA/MD. The Application Server sets up two CCCs for each call content interception to deliver the two media paths of the call on two separate channels.

- One CCC is set up to deliver the intercepted media in the transmit direction.
- One CCC is setup to deliver the intercepted media in the receive direction.

A CCLink can be configured as either independent or shared using the independent option. Note that when a multiple call appearance device such as a SIP phone[1] or trunking device is used, the CCLink is always considered independent regardless of the independent option setting.

Also note that if a subject redirects a call, then the call content interception that is resumed at the redirected call is always considered independent. The shared setting (independent option set to "false") only applies to the interception of calls the subject has not redirected.

A CCLink can also be configured to intercept or not intercept content while held using the interceptHeld option. When interceptHeld is set to "false", no content is intercepted while the call (or BroadWorks Conference) being monitored is held by the subject.

[1] Analog telephone adapters used to interconnect legacy telephones to BroadWorks are SIP phones from the perspective of the Application Server. These devices have an analog interface to the phone, but a SIP interface to the Application Server.

The Application Server reserves and uses two resources from the CCLink for each call involving content surveillance when the CCLink's independent option is set to "true". Because a user can also be involved in many simultaneous calls, it is expected that the lawful intercept administrator sets up more than two resources per call content link.

For example, the following scenarios involve simultaneous calls:

- **Call Waiting**: The user is already involved in a call and receives a second call. The user can place the original call on hold and answer the incoming call.
- **Consultations**: The user is already involved in a call and places this call on hold to initiate a second consultative call.
- **Call redirections**: The call to the user is redirected to a provisioned destination (for example, voice mail) in which case the call content interception is resumed on the redirected call.

If the CCLink independent option is set to "false", then new resources are used only when the subject makes a first call. Subsequent calls (for example, Call Waiting or Consultations) reuse the two resources from the first call. If the independent option is set to "false", fewer resources are used.

The lawful intercept administrator must carefully engineer the number of resources provisioned on a particular call content link.

- The lawful intercept administrator can set up a unique call content link that is assigned to multiple surveillances. In this case, the resources are pooled together and can be used for different surveillances on different users.
- The lawful intercept administrator can set up a different call content link for each surveillance entity. In this case, the maximum number of simultaneous calls under content surveillance can be controlled on a surveillance basis.

There are three types of call content links: "direct" call content link, "callout" call content link, and "callout-ETSI" call content link.

2.2.1 Direct Call Content Link

The first type of call content link is referred to as a "direct" call content link. The administrator configures this call content link by providing the LEA/MD's IP address and a range of contiguous ports. When setting up a CCC for a particular intercepted call, the Application Server reserves and uses two even-numbered ports from the provisioned range. The Application Server then instructs the Media Server to repeat the intercepted media to the specified IP address and port as a raw RTP stream.

Upon completion of the intercept, the two used ports are returned to the pool of available ports and can be used for another call-content interception.

2.2.2 Callout Call Content Link

The second type of call content link is referred to as a "callout" call content link. The administrator configures this call content link by providing a set of numbers. When setting a CCC for a particular intercepted call, the Application Server reserves and uses two numbers from the set. The Application Server then initiates two calls to the reserved phone numbers and upon answer, instructs the Media Server to repeat the intercepted media to the terminating endpoints as a raw RTP stream.

The Calling Line ID (CLID) for these calls is the monitored user's phone number. Optionally, the administrator can configure an alternate CLID if using the monitored user's phone number would compromise the surveillance.

Upon completion of the intercept, the two used numbers are returned to the pool of available numbers and can be used for another call-content interception. In the case of early release from the LEA/MD, the resources remain reserved until the call is effectively released or redirected by the user under surveillance.

2.2.3 Callout-ETSI Call Content Link

The last type of call content link is referred to as a “calloutETSI” call content link. The “calloutETSI” call content link is similar to the “callout” type, but it allows a LEA to correlate a CCC stream to a CDC stream in compliance with ETSI regulations.

The functional differences between a regular “callout” and “calloutETSI” are:

- CCLinks of type “calloutETSI” include correlation information in the CCC SIP Invite sent by the Application Server to the network gateway. The correlation information is encoded in the User-To-User Information (UUS) parameter of a Generic Transparency Descriptor (GTD), which is included in the CCC SIP INVITE request. This information is encoded in ASN.1 format using Basic Encoding Rules (BER) and included in the UUS according to the ASN.1 definitions provided in specification ES 201 671.
- CCLinks of type “calloutETSI” can only have one callout phone number configured for them.
- CCLinks of type “calloutETSI” must have an operator identifier. This field is configurable, but cannot be empty.

The following correlation information is included in the origination CCC SIP INVITE sent by BroadWorks to the network gateway:

Information	Description	Source
Lawful interception identifier (LIID)	Identifier, identifying target identity	BroadWorks Case Identifier
Communication Identifier (CID)	Identifier, identifying specific call of target identity	Communication Identity Number = Call ID Operator Identifier = CCLink operator ID value. Network Element ID = HostId
CC link identifier (CCLID), if required	Identifier, used for correlation CCC link-CDC messages	BroadWorks ccLinkId of the CCLink
Direction indication	Signal from (Tx)/towards (Rx) target identity	1 = from subject 2 = to subject

2.3 Call Data Channel

Lawful Intercept events are generated by the call processing system and sent to the LEA/MD’s collection function over a Call Data Channel (CDC).

The Call Data Channel consists of a TCP/IP connection between the Application Server and the LEA/MD. The lawful intercept administrator uses the administration function to specify the IP address and port of the LEA/MD. A socket connection is set up at the beginning of each intercepted call, and taken down when the call completes. The connection is maintained during the length of the call interception.

The details of the Lawful Intercept events, sent to the LEA/MD over the CDC, are described in section *4 Event Definitions*. The events reported to the LEA are encoded in ASN.1 format using Basic Encoding Rules (BER). Two ASN.1 formats are supported by the Application Server: BroadWorks or J-STD-025A. The "BroadWorks" ASN.1 definitions are described in this document in section *5 BroadWorks ASN.1 Definitions*.

2.4 Call Content Channel

If the surveillance on the user is also set up for media monitoring, then two Call Content Channels (CCCs) are set up at the beginning of the intercepted call. Depending on the type of call content link configured on the surveillance, the Application Server establishes the CCCs to the LEA/MD, and instructs the Media Server to repeat the intercepted media accordingly.

When the Application Server establishes a CCC, a CCOpen event is sent to the LEA/MD over the CDC. This allows the LEA/MD to correlate the incoming CCC with a particular call, user, and case identifier. Correspondingly, when the CCC is closed, a CCClose event is sent to the LEA/MD over the CDC. Also, when one intercepted endpoint changes its SDP, then a CCChange event is sent over the CDC.

2.5 Media Relay Restrictions

The use of the media relay function (for call content interception and dialed digit extraction) may be restricted for a given user under surveillance and for a given call. In some cases, service providers may determine that they are not legally required to intercept traffic that does not touch their network. Hence, for a call that is local to one site, the call-identifying information is subject to interception (in the form of signaling) but the call content is not.

Media relay restrictions can be configured for each subject using a surveillance option. By default, the *Media Relay Restrictions* option is set to "none". In this case, the call content intercept and/or dialed digit extraction apply as usual and the media of any call involving the subject is relayed through the media server.

Two other options are offered:

- *Exclude-Group-Calls* – When the *Media Relay Restrictions* attribute is set to *Exclude-Group-Calls*, the media of the calls involving the subject can always be relayed unless BroadWorks can establish that the call is intra-group.
- *Exclude-Enterprise-Calls* – When the *Media Relay Restrictions* attribute is set to *Exclude-Enterprise-Calls*, the media of the calls involving the subject can always be relayed unless BroadWorks can establish that the call is intra-enterprise or intra-group.

Although media relay restrictions are configured on a per-surveillance basis, it is expected that, as a policy, surveillances for users within an enterprise will always be configured with the same type of media relay restrictions. That is, when the service provider deploys service for an enterprise, it determines whether all members of an enterprise are located on the same customer site/LAN or whether user groups are partitioned to match the boundaries of customer sites/LANs. The LI administrator is then instructed to apply media relay restrictions based on the type of enterprise.

It should be noted that call-identifying information (other than dialed digits) is always reported regardless of the presence of media relay restrictions.

3 Administration Functions

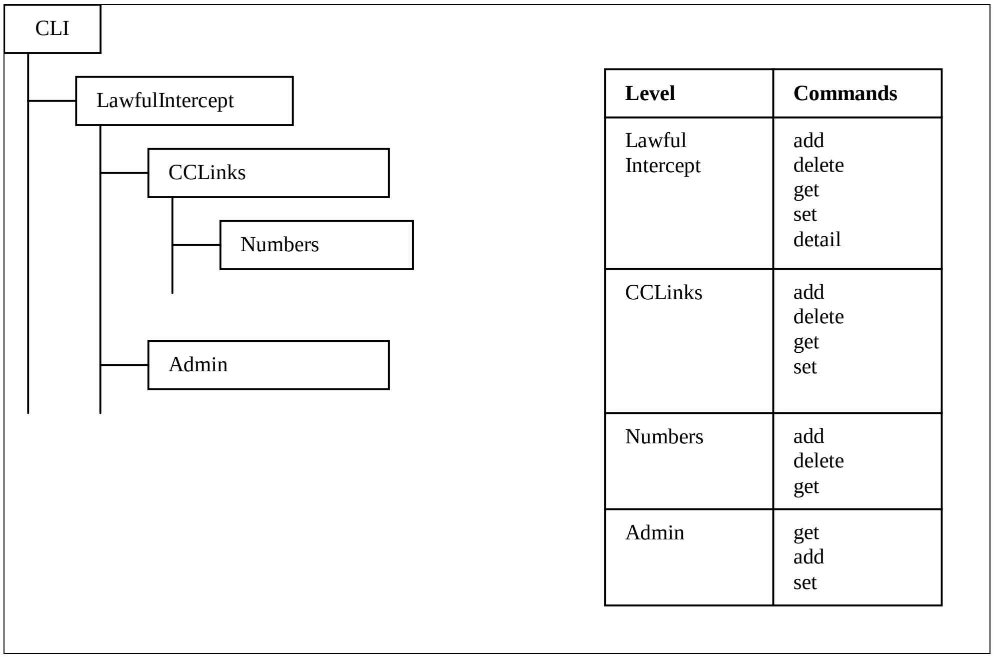
3.1 Summary

The lawful intercept administrator accesses the Lawful Intercept context to provision surveillances on a user. There are two types of surveillances: event monitoring only, and event and media monitoring.

For event monitoring, the lawful intercept administrator indicates the IP address and port of the LEA or mediation device's collection function.

If media monitoring is required for the surveillance, then the lawful intercept administrator first provisions a call content link (CCLink). The lawful intercept administrator can then provision a new surveillance on a user and allocate the CCLink to this surveillance, or simply allocate the CCLink to an existing surveillance.

The following sections provide detailed information on the syntax of the CLI commands and provide example usage of these commands.



Level	Commands
Lawful Intercept	add delete get set detail
CCLinks	add delete get set
Numbers	add delete get
Admin	get add set

Figure 2 CLI Command Hierarchy for Lawful Intercept

3.2 Lawful Intercept Context

3.2.1 Get

This command allows you to view existing surveillances in the system.

1) Ensure you are at the `LawfulIntercept>` level.
2) Enter:

   `get` ↵

Example:

```
CLI/LawfulIntercept> get

   User ID          Phone      Case ID    Status     Type
=========================================================
     user1   +15146972004      FBI9923    active     both
     user2   +15146971000     LAPD3324  inactive    event

2 entries found.
```

3.2.2 Add

This command allows you to add a new surveillance to the system.

1) Ensure you are at the `LawfulIntercept>` level.
2) Enter:

   `add <attribute> <caseId> <eventIpAddress> <eventIpPort> <cdcFormat> [<attribute>]` ↵

   where:

Variable	Field	Type	Valid Values	Description
<attribute>	userId	String	2 to 161 characters	The subject's identification.
	phone	String	0 to 17 characters	The subject's phone number.
<caseId>		String	1 to 25 characters	Specifies the case identifier for each surveillance.
<eventIpAddress>		IP address, host, domain	2 to 80 characters	Specifies the IP address used by the LEA/MD to receive surveillance events from the Call Data Channel (CDC).
<eventIpPort>		Integer	1025 to 65535	Specifies the port used by the LEA/MD to receive surveillance events from the CDC.

Variable	Field	Type	Valid Values	Description
<cdcFormat>		Choice	broadworks, jstd025a	Indicates the CDC format type. The default is “broadworks”. When set to the “broadworks” legacy format, outgoing CDCs are encoded as usual. When set to the “jstd025a” format, outgoing CDCs are encoded with compliance to the JSTD025 A standard specifications.
<attribute>	type	Choice	event	Indicates the type of surveillance is event monitoring only.
			both	Indicates the type of surveillance is event and media monitoring. ccLink, string, 1 to 25 characters. The call content link provisioned for this surveillance.
	status	Choice	active, inactive	Specifies if this surveillance is active or inactive.
	dialDigit Extraction	Choice	false, true	Specifies if dial digit extraction is performed on this surveillance.
	subjectSignal	Choice	false, true	When set to “true” any signal that is initiated by the intercept subject is reported.
	mediaRelay Restrictions	Choice	none	When set to none, the call content intercept and/or dialed digit extraction apply as usual and the media of any call involving the subject is relayed through the Media Server.

Variable	Field	Type	Valid Values	Description
			excludeGroupCalls	When set to excludeGroupCalls, the media of the calls involving the subject can always be relayed unless BroadWorks can establish that the call is intra-group.
			excludeEnterpriseCalls	When set to excludeEnterpriseCalls, the media of the calls involving the user can always be relayed unless BroadWorks can establish that the call is intra-enterprise or intra-group.

Examples:

```
CLI/LawfulIntercept> add phone 5146971000 LAPD6712 type both ccLinkA
…Done


CLI/LawfulIntercept> add phone 5146980605 testcaseID 192.168.8.136 4040
jstd025a type both testcclink
…Done
```

3.2.3 Set

This command allows you to modify an existing surveillance in the system.

1) Ensure you are at the `LawfulIntercept>` level.

2) Enter:

`set <attribute> <caseId> <attribute> ↵`

where:

Variable	Field	Type	Valid Values	Description
<attribute>	userId	String	2 to 161 characters	The subject's identification.
	phone	String	0 to 17 characters	The subject's phone number.
<caseId>		String	1 to 25 characters	Specifies the case identifier for each surveillance.
<attribute>	eventIpAddress	IP address, host, domain	2 to 80 characters	Specifies the IP address used by the LEA/MD to receive surveillance events from the Call Data Channel (CDC).

Variable	Field	Type	Valid Values	Description
	eventIpPort	Integer	1025 to 65535	Specifies the port used by the LEA/MD to receive surveillance events from the CDC.
	<cdcFormat>	Choice	broadworks, jstd025a	Indicates the CDC format type. The default is “broadworks”. When set to the “broadworks” legacy format, outgoing CDCs are encoded as usual. When set to the “jstd025a” format, outgoing CDCs are encoded with compliance to the JSTD025 A standard specifications.
	type	Choice	event	Indicates the type of surveillance is event monitoring only.
			both	Indicates the type of surveillance as event and media monitoring. ccLink, string, 1 to 25 characters. The call content link provisioned to this surveillance.
	status	Choice	active, inactive	Specifies if this surveillance is active or inactive.
	dialDigitExtraction	Choice	false, true	Specifies if the dial digit extraction is performed on this surveillance.
	subjectSignal	Choice	false, true	When set to “true” any signal that is initiated by the intercept subject is reported.
	mediaRelayRestrictions	Choice	none	When set to none, the call content intercept and/or dialed digit extraction apply as usual and the media of any call involving the subject is relayed though the Media Server.

Variable	Field	Type	Valid Values	Description
			excludeGroupCalls	When set to excludeGroupCalls, the media of the calls involving the subject can always be relayed unless BroadWorks can establish that the call is intra-group.
			excludeEnterpriseCalls	When set to excludeEnterpriseCalls, the media of the calls involving the subject can always be relayed unless BroadWorks can establish that the call is intra-enterprise or intra-group.

Example:

```
CLI/LawfulIntercept> set phone 5146971000 LAPD7065 type both ccLinkA
status active

...Done
```

3.2.4 Delete

This command allows you to delete an existing surveillance from the system.

1) Ensure you are at the `LawfulIntercept>` level.

2) Enter:

   `delete <attribute> <caseId>` ↵

   where:

Variable	Field	Type	Valid Values	Description
<attribute>	userId	String	2 to 161 characters	The subject's identification.
	phone	String	0 to 17 characters	The subject's phone number.
<caseId>		String	1 to 25 characters	The case ID for the specific surveillance.

Example:

```
CLI/LawfulIntercept> delete phone 5146971000 LAPD6712

...Done
```

3.2.5 Detail

This command allows you view all surveillances assigned to a specific subject.

1) Ensure you are at the `LawfulIntercept>` level.

2) Enter:

`detail <attribute>` ↵

where:

Variable	Field	Type	Valid Values	Description
<attribute>	userId	String	svcProviderId, groupId, or userId	The ID of the service provider, group, or user. Choice as follows: svcProviderId, string, 1 to 30 characters groupId, string, 1 to 30 characters userId, string, 2 to 161 characters
	phone	String	0 to 17 characters	The subject's phone number.

Example:

```
CLI/LawfulIntercept> detail phone +15146980605

Case Id     Status  Type   DDE   //…// Net Address  Event Port  CDC
Format   CCLink Id
=========================================================================
===============

testcaseID  active  both  false  //…// 192.168.8.136     4040    jstd025a
anylink
```

3.2.6 CCLink

This level allows you view, add, modify, or delete a call content link that is assigned for a surveillance.

3.2.6.1 Get

This command allows you to view call content links that are allocated to existing surveillances. To view all CCLinks, you use this command with no parameters.

1) Ensure you are at the `LawfulIntercept/CCLink>` level.
2) Enter:

`get [<ccLinkId>]` ↵

where:

Variable	Field	Type	Valid Values	Description
<ccLinkId>		String	1 to 25 characters	The ID for the call content link.

Example:

```
AS_CLI/LawfulIntercept/CCLinks> get

CC Link Id       Type     Net Address  Low Port  High Port  Independent
Intercept Held  CLID Phone Number OperatorId
=========================================================================
callOut1    callout
false                 false
```

```
     direct1     direct           192.168.1.1      1112       1227
true                   false
    etsiLink     calloutETSI
false                  false                  2403649000
UNKNOWN
```

3.2.6.2 Add

This command allows you to allocate a call content link to a specific surveillance. Call content link types include direct, callOut, or callOutETSI. The callOut or callOutETSI link types can have a CLID configured for them.

1) Ensure you are at the `LawfulIntercept/CCLink>` level.

2) Enter:

`add <ccLinkId> <independent> <interceptHeld> <type> ↵`

where:

Variable	Field	Type	Valid Values	Description
<ccLinkId>		String	1 to 25 characters	The ID for the call content link.
<independent>		Choice	false, true	Specifies if this call content link is independent or shared.
<interceptHeld>		Choice	false, true	When set to “false”, no content is intercepted while the call (or BroadWorks conference) being monitoring is held by the subject.
<type>		Choice	direct	When “direct” is selected, the administrator configures this call content link by providing the LEA/MD’s IP address and a range of contiguous ports. When setting up a CCC for a particular intercepted call, the Application Server reserves and uses two even-numbered ports from the provisioned range. The Application Server then instructs the Media Server to repeat the intercepted media to the specified IP address and port as a raw RTP stream. ipAddress, IP address, host, domain, 2 to 80 characters. Specifies the LEA/MD’s IP address. lowPort, integer, 1026 to 65534. Specifies the lowest port in the range for this call content link. highPort, integer, 1027 to 65535. Specifies the highest port in the range for this call content link.
			callout	When “callout” is selected, the administrator configures the call content link by

Variable	Field	Type	Valid Values	Description
				providing a set of numbers. When setting a CCC for a particular intercepted call, the Application Server reserves and uses two numbers from the set. The Application Server then initiates two calls to the reserved phone numbers and upon answer, instructs the Media Server to repeat the intercepted media to the terminating endpoints as a raw RTP stream. CLID, string, 1 to 17 characters. Specifies an optional calling line ID. Callouts to the LEA device currently contain the number of the party under surveillance in the FROM field of SIP INVITE. This could compromise surveillance. If configured, this number is used in callouts to the LEA device instead of the surveillance user number.
			calloutETSI	Choice of: operatorId, string, 1 to 80 characters. Specifies the operator identifier. CLID, string, 1 to 17 characters. Specifies an optional calling line ID. Callouts to the LEA device currently contain the number of the party under surveillance in the FROM field of SIP INVITE. This could compromise surveillance. If configured, this number is used in callouts to the LEA device instead of the surveillance user number.

Examples:

```
CLI/LawfulIntercept/CCLinks> add etsiLink false false callOutETSI UNKNOWN
2403659000

CLI/LawfulIntercept/CCLink> add ccLinkA direct 224.1.1.1 5050 5069 true
false
…Done

CLI/LawfulIntercept/CCLink> add ccLinkB callout true true
…Done
```

3.2.6.3 Set

This command allows you to modify a call content link.

1) Ensure you are at the `LawfulIntercept/CCLink>` level.

2) Enter:

```
set <ccLinkId> <attribute> ↵
```

where:

Variable	Field	Type	Valid Values	Description
<ccLinkId>		String	1 to 25 characters	The ID for the call content link.
<attribute>	independent	Choice	false, true	Specifies if this call content link is independent or shared.
	interceptHeld	Choice	false, true	When set to “false”, no content is intercepted while the call (or BroadWorks conference) that is being monitored is held by the subject.
	type	Choice	direct	ipAddress, IP address, host, or domain, 2 to 80 characters.
				lowPort, integer, 1026 to 65534.
				highPort, integer, 1027 to 65535.
			callout	CLID, string, 1 to 17 characters. Specifies an optional calling line ID. Callouts to the LEA device currently contain the number of the party under surveillance in the FROM field of SIP INVITE. This could compromise surveillance. If configured, this number is used in callouts to the LEA device instead of the surveillance user number.
			calloutETSI	operatorId, string, 1 to 80 characters.
				CLID, string, 1 to 17 characters. Specifies an optional calling line ID. Callouts to the LEA device currently contain the number of the party under surveillance in the FROM field of SIP INVITE. This could compromise surveillance. If configured, this

Variable	Field	Type	Valid Values	Description
				number is used in callouts to the LEA device instead of the surveillance user number.

To remove a CLID from a link, enter the ccLinkId and type (callout or calloutETSI) but do not enter a CLID, as shown in the following example.

```
CLI/LawfulIntercept/CCLink> set etsiLink type calloutETSI  UNKNOWN

…Done
```

Examples:

```
CLI/LawfulIntercept/CCLink> set ccLinkA type callout false true

…Done


CLI/LawfulIntercept/CCLink>set etsiLink type calloutETSI UNKNOWN
2403649999

…Done
```

3.2.6.4 Delete

This command allows you to delete an existing call content link from the system.

1) Ensure you are at the `LawfulIntercept/CCLink>` level.

2) Enter:

   `delete <ccLinkId>` ↵

   where:

Variable	Field	Type	Valid Values	Description
<ccLinkId>		String	1 to 25 characters	The ID for the call content link.

Example:

```
CLI/LawfulIntercept/CCLink> delete ccLinkA

…Done
```

3.2.6.5 Numbers

This level allows you view, add, or delete a numbers that are assigned to a specific call content link.

3.2.6.5.1 Get

This command allows you to retrieve all numbers assigned to a specific call content link.

1) Ensure you are at the `LawfulIntercept/CCLink/Numbers>` level.

2) Enter:

`get [<ccLinkId>]` ↵

where:

Variable	Field	Type	Valid Values	Description
<ccLinkId>		String	1 to 25 characters	The ID for the call content link.

Example:

```
CLI/LawfulIntercept/CCLink/Numbers> get ccLinkA

Phone Numbers                    CCLink
=================================
+1-5146972000 - +1-5146972003  ccLinkA
+1-5146972005                  ccLinkB

2 entries found.


CLI/LawfulIntercept/CCLink/Numbers> get

Phone Numbers                    CCLink
=================================
+1-5146972000 - +1-5146972003  ccLinkA
+1-5146972005                  ccLinkB
+1-5146972006 - +1-5146972009  ccLinkC

3 entries found.
```

3.2.6.5.2 Add

This command allows you to assign a single or range of numbers to a call content link.

1) Ensure you are at the `LawfulIntercept/CCLink/Numbers>` level.

2) Enter:

`add <ccLinkId> <startNumber> [<endNumber>]` ↵

where:

Variable	Field	Type	Valid Values	Description
<ccLinkId>		String	1 to 25 characters	The ID for the call content link.
<startNumber>		String	1 to 17 characters	The starting number in the range of numbers to add for the call content link.
<endNumber>		String	1 to 17 characters	The ending number in the range of numbers to add for the call content link.

Example:

```
CLI/LawfulIntercept/CCLink/Numbers> add ccLinkA 5146972000 5146972005

…Done
```

3.2.6.5.3 Delete

This command allows you to un-assign a single or range of numbers from a call content link.

1) Ensure you are at the `LawfulIntercept/CCLink/Numbers>` level.
2) Enter:

```
delete <ccLinkId> <startNumber> [<endNumber>] ↵
```

where:

Variable	Field	Type	Valid Values	Description
<ccLinkId>		String	1 to 25 characters	The ID for the call content link.
<startNumber>		String	1 to 17 characters	The starting number in the range of numbers to delete for the call content link.
<endNumber>		String	1 to 17 characters	The ending number in the range of numbers to delete for the call content link.

3.2.7 Admin

This level allows you view, add, modify, or remove a Lawful Intercept administrator in the system.

3.2.7.1 Get

This command allows you to view the Lawful Intercept administrators currently set on the system.

1) Ensure you are at the `LawfulIntercept/Admin>` level.
2) Enter:

```
get [<attribute>] ↵
```

Variable	Field	Type	Valid Values	Description
<attribute>	userId	String	2 to 161 characters	The administrator's ID.
	firstName	String	0 to 30 characters	The administrator's first name.
	lastName	String	0 to 30 characters	The administrator's last name.

3.2.7.2 Add

This command allows you to add a new Lawful Intercept administrator to the system.

1) Ensure you are at the `LawfulIntercept/Admin>` level.
2) Enter:

```
add <userId> [<attribute>] ↵
```

where:

Variable	Field	Type	Valid Values	Description
<userId>		String	2 to 161 characters	The administrator’s ID.
<attribute>	firstName	String	0 to 30 characters	The administrator’s first name.
	lastName	String	0 to 30 characters	The administrator’s last name.

Example:

```
CLI/LawfulIntercept/Admin> add liadmin2
Initial Password:
Re-type Initial Password:
...Done
```

3.2.7.3 Set

This command allows you to modify a Lawful Intercept administrator’s attributes, such as the name or login information.

1) Ensure you are at the `LawfulIntercept/Admin>` level.
2) Enter:

   `set <userId> <attribute>` ↵

   where:

Variable	Field	Type	Valid Values	Description
<userId>		String	2 to 161 characters	The administrator’s identification.
<attribute>	firstName	String	0 to 30 characters	The administrator’s first name.
	lastName	String	0 to 30 characters	The administrator’s last name.
	Password	String		The associated password for the administrator’s ID.

Example:

```
CLI/LawfulIntercept/Admin> set password

Reset Password:
Re-type New Password:
...Password changed

...Done
```

3.2.7.4 Delete

This command allows you to delete an existing Lawful Intercept administrator from the system.

1) Ensure you are at the `LawfulIntercept/Admin>` level.
2) Enter:

`delete <userId>` ↵

where:

Variable	Field	Type	Valid Values	Description
<userId>		String	2 to 161 characters	The administrator’s ID.

Example:

```
CLI/LawfulIntercept/Admin> delete liadmin

...Done
```

4 Event Definitions

Every call involving a surveillance subject is traced and Lawful Intercept (LI) events characterizing that call are sent to the delivery function. By default, LI events include the following information:

- **Case_Id**: The LEA-provided case identifier.
- **Accessing_Element_Id**: The Application Server identifier. This is the Solaris host ID.
- **Call_Id**: The BroadWorks call identifier. The system identity field of the call identifier also contains the Solaris host ID.
- **Event_time**: The date and time (GMT) at which the event was detected.

The following sections describe each LI event sent in the context of call data surveillance, and describe which information, if any, is provided to the delivery function.

The events reported to the LEA are encoded in ASN.1 format using Basic Encoding Rules (BER).

4.1 Origination

The Origination event is generated for the calls originated by a surveillance subject. The following information is provided with the Origination event:

- **Calling_Party_Id**: The phone number or extension that identifies the calling party (the surveillance subject),
- **Called_Party_Id**: The phone number or extension that identifies the called party, and
- **User_Input**: The digits input by the user.

Parameter Description	Example Data
Case Identifier	FBI000192
Intercept Access Element	80c2cb50
Time of event	20010922154536.125Z
Call Identifier Sequence Number System Identity	 1321:0 80c2cb50
Calling Party Identifier DN	 5146972000
Called Party Identifier DN	 6134442001
User Input	16134442001

4.2 TerminationAttempt

The TerminationAttempt event is generated for incoming calls to a surveillance subject. The following information is provided with the TerminationAttempt event:

- **Calling_Party_Id**: The phone number or extension that identifies the calling party,
- **Called_Party_Id**: The phone number or extension that identifies the called party (the surveillance subject), and
- **Redirected_From_Info**: The information about previous redirections (last redirection number, original called number, number of redirections) for the incoming call, if available.

Parameter Description	Example Data
Case Identifier	FBI000192
Intercept Access Element	80c2cb50
Time of event	20010922154536.125Z
Call Identifier Sequence Number System Identity	 1321:0 80c2cb50
Calling Party Identifier DN	 5146972000
Called Party Identifier DN	 5146972004
Redirected From Information Party Identity (last) Party Identity (first) number	 5146972002 5146972003 2

4.3 Answer

The Answer message reports when a call under surveillance is answered. The following information is provided with the Answer event:

Answering_Party_Id: If the call is terminated on the BroadWorks Application Server, this is the number of the answering party. If the call is terminated on a PSTN gateway, this is the identity of the last known destination for this call.

Parameter Description	Example Data
Case Identifier	FBI000192
Intercept Access Element	80c2cb50
Time of event	20010922154536.125Z
Call Identifier Sequence Number System Identity	 1321:0 80c2cb50
Answering Party Identifier DN	 5146972000

4.4 SubjectSignal

The SubjectSignal message reports any signal that is initiated by the intercept subject. In the context of BroadWorks, the following signal is detected and reported:

- **Flash** – The user flashes:

1) To put a call on hold and originate a second call,
2) To answer a second incoming call and toggle between two calls,
3) To transfer a consultation call, or
4) To conference two calls together.

When a surveillance subject flashes, the appropriate SubjectSignal message is sent out to the LEA.

NOTE: The flash is only reported for BroadWorks-controlled devices such as MGCP devices. A flash performed on an analog device located behind an analog telephone adapter is not reported. In these cases, the flash event is not propagated to the Application Server; hence it is not reported to the LEA.

The following information is provided with the SubjectSignal event:

- **Signal**: This is the actual signal received from the user. It can only be a switch-hook flash.

Parameter Description	Example Data
Case Identifier	FBI000192
Intercept Access Element	80c2cb50
Time of event	20010922154536.125Z
Call Identifier Sequence Number System Identity	 1321:0 80c2cb50
Signal Switch-hook Flash	 FLASH

4.5 NetworkSignal

The NetworkSignal CDC message reports any BroadWorks-induced signal that is sent to the surveillance subject. The term BroadWorks-induced is meant to include prompts or tones locally played back by the Media Server to the subject or tones provided by the devices under direct BroadWorks instruction.

The NetworkSignal message is not reported for the following cases:

- If the prompts or tones are remotely provided (for example, early media)
- If the prompts or tones are provided in the context of a service (for example, call forward programming), in which case they are considered as call content, not as call-identifying information

This functionality is not impacted by the capabilities of the device to report the network signals. A NetworkSignal message is generated even when the subject's device is unable to present the signal to the subject.

The following information is provided with the NetworkSignal event:

- **Alerting Signal**: The type of alerting signal sent to the subject's line.
- **Audible Signal**: The type of audible signal sent to the subject's line.
- **Terminal Display Info**: The remote party's name and number. This is also used when the message waiting indicator (MWI) is sent to the subject's line.
- **Other Signaling Info**: The name of the announcement file played to the subject, when applicable.

Parameter Description	Example Data
Case Identifier	FBI000192
Intercept Access Element	80c2cb50
Time of event	20010922154536.125Z
Call Identifier Sequence Number System Identity	 1321:0 80c2cb50
Alerting Signal	1
Audible Signal	3
Terminal Display Info Calling Number Calling Name Message Waiting Notification	 5145552214 John Smith 0
Other	TrtDialToneTimeout.wav

4.6 DialedDigitExtraction

The DialedDigitExtraction message captures the digits dialed by the subject under surveillance once the call is connected. Extracted digits are reported individually in separate DialedDigitExtraction messages. The following information is provided with the DialedDigitExtraction event:

Dialed Digits: This is the digits dialed by the subject under surveillance, (once the call is connected). Digits are reported one by one in different messages.

Parameter Description	Example Data
Case Identifier	FBI000192
Intercept Access Element	80c2cb50
Time of event	20010922154536.125Z
Call Identifier Sequence Number System Identity	 1321:0 80c2cb50
Dialed Digits	5

4.7 Redirection

The Redirection event reports the redirection of a call under surveillance. The Redirection message is generated for calls redirected by the surveillance subject or the surveillance subject's service. For example:

- When call termination special features are encountered
- Due to the subject's direct actions on a terminating call
- Due to the subject's initiating a call transfer

Once a call is redirected, one of the two remaining parties in the call becomes the surveillance subject until the call is eventually released. If the new surveillance subject is another BroadWorks user and redirects the call, then the Redirection event is again generated and a new surveillance subject is identified.

The following information is provided with the Redirection event:

- **Redirected_From_Party_Id**: The phone number or extension that identifies the redirected-from party.
- **Redirected_To_Party_Id**: The phone number or extension that identifies the redirected-to party.

Parameter Description	Example Data
Case Identifier	FBI000192
Intercept Access Element	80c2cb50
Time of event	20010922154536.125Z
Call Identifier Sequence Number System Identity	 1321:0 80c2cb50
Redirected To Party Identifier DN	 6134442001
Redirected From Party Identifier DN	 5146972000

4.8 Release

The Release event reports the release of resources used for a call under surveillance. Beyond the basic information described earlier, there is no additional information sent with the Release event.

Parameter Description	Example Data
Case Identifier	FBI000192
Intercept Access Element	80c2cb50
Time of event	20010922154536.125Z
Call Identifier Sequence Number System Identity	 1321:0 80c2cb50

4.9 Connection/ConnectionBreak

The Connection and ConnectionBreak CDC messages report the parties that are able to communicate to each other in a subject-initiated conference call under surveillance.

In particular, this applies when the user initiates a BroadWorks three-way call via:

1) Flash,

2) Call client interface,

3) Device interface, or

4) Directed pickup barge-in.

This does not apply for a meet-me conference (for example, BroadWorks Conference Server) or a device-initiated conference where the conference mixing occurs on the device itself.

Typically, the Connection message is sent whenever a party is added to the conference bridge. The message reports the connected party identities. The ConnectionBreak message is sent whenever a party is removed from the conference bridge. The message reports the remaining party identities.

> NOTE: In the context of a conference call, multiple call traces are in progress. The connected parties and intercepted media (if applicable), are reported on one of the call traces (also known as the active call trace). The intercepted media is not reported for the other redundant call traces, and a ConnectionBreak message is reported with no remaining parties. In the cases where the user has made or received another call and where the remote party is not joined to the conference call, then that call is traced independently.

The following information is provided with the Connection message:

- **Connected parties**: Identifies the parties able to communicate with each other.

Parameter Description	Example Data
Case Identifier	FBI000192
Intercept Access Element	80c2cb50
Time of event	20010922154536.125Z
Call Identifier Sequence Number System Identity	 1321:0 80c2cb50
Connected Parties	5145552219 5145552214 2405552454

The following information is provided with the ConnectionBreak message:

- **Remaining parties**: Identifies the parties able to communicate with each other.

Parameter Description	Example Data
Case Identifier	FBI000192
Intercept Access Element	80c2cb50
Time of event	20010922154536.125Z
Call Identifier Sequence Number System Identity	 1321:0 80c2cb50
Remaining Parties	5145552219 2405552454

4.10 CCOpen

The CCOpen event is generated for calls under interception that require the delivery of call contents to the LEA. It identifies the beginning of the delivery of call content information.

The following information is provided with the CCOpen event:

- **CCC_ID**: Depending on the type of CC resource used for media monitoring, the field either contains an IP address and port (for example, 192.168.8.41:5050) or a phone number (for example, 5146972000).
- **Originating_SDP**: The Session Descriptor Protocol (SDP) information for the originating endpoint.
- **Terminating_SDP**: The Session Descriptor Protocol (SDP) information for the terminating endpoint.

If the maximum number of call interceptions for a given CCLink is reached (meaning there are no available phone numbers or ports), then the CCOpen is still generated. In these cases, the CCCId provides empty values for the “sepXmitCCC” and/or “sepRecvCCC” fields.

Parameter Description	Example Data
Case Identifier	FBI000192
Intercept Access Element	80c2cb50
Time of event	20010922154536.125Z
Call Identifier Sequence Number System Identity	 1321:0 80c2cb50
CCC Identity Separate CCC Pair Separate Xmit CCC Separate Recv CCC	 192.168.8.41:5050 192.168.8.41:5052

Originating SDP	o=Vega50 1234 0 IN IP4 192.168.12.20
	s=Sip Call
	c=IN IP4 192.168.12.20
	t=0 0
	m=audio 10014 RTP/AVP 0
	a=rtpmap:0 PCMU/8000

Terminating SDP	o=- 10 1 IN IP4 192.168.13.30
	s=Cisco SDP 0
	c=IN IP4 192.168.13.30
	t=0 0
	m=audio 16390 RTP/AVP 0

4.11 CCChange

The CCChange event is generated prior to or coincident with a change in the SDP information for either the originating or terminating endpoint. The following information is provided with the CCChange event:

- **CCC_ID**: Depending on the type of CC resource used for media monitoring, the field either contains an IP address and port (for example, 192.168.8.41:5050) or a phone number (for example, 5146972000).
- **Originating_SDP**: The Session Descriptor Protocol (SDP) information for the originating endpoint, and

- **Terminating_SDP**: The Session Descriptor Protocol (SDP) information for the terminating endpoint.

Parameter Description	Example Data
Case Identifier	FBI000192
Intercept Access Element	80c2cb50
Time of event	20010922154536.125Z
Call Identifier Sequence Number System Identity	 1321:0 80c2cb50
CCC Identity Separate CCC Pair Separate Xmit CCC Separate Recv CCC	 192.168.8.41:5050 192.168.8.41:5052

Originating SDP	o=Vega50 1234 0 IN IP4 192.168.12.20
	s=Sip Call
	c=IN IP4 192.168.12.20
	t=0 0
	m=audio 10014 RTP/AVP 0
	a=rtpmap:0 PCMU/8000

Terminating SDP	o=- 10 1 IN IP4 192.168.13.30
	s=Cisco SDP 0
	c=IN IP4 192.168.13.30
	t=0 0
	m=audio 16390 RTP/AVP 0

4.12 CCClose

The CCClose message reports the end of call content delivery for a call under surveillance. The following information is provided with the CCClose event:

CCC_ID: Depending on the type of CC resource used for media monitoring, the field either contains an IP address and port (for example, 192.168.8.41:5050) or a phone number (for example, 5146972000).

Parameter Description	Example Data
Case Identifier	FBI000192
Intercept Access Element	80c2cb50
Time of event	20010922154536.125Z
CCC Identity Separate CCC Pair Separate Xmit CCC Separate Recv CCC	 192.168.8.41:5050 192.168.8.41:5052

4.13 ServingSystem

The ServingSystem CDC message reports the registration information of SIP registering devices for a particular subject under surveillance. A user can have one or more of the following device types:

- Primary device – Exists if the user has a primary device configured against its profile.
- Alternate device – Exists if the user has any of the Shared Call Appearance services assigned and configured.

- Video Add-On device – Exists if the user has the Video Add-On service assigned and configured.
- Messenger device – Exists if the user has the Windows Messenger service assigned.

Registration failures are also reported via the ServingSystem message. For example, if a registration attempt originates from outside of an established emergency zone, then a failure response is returned to the registering device and is reported to the LEA.

The following information is provided with the ServingSystem event:

- **Address Registration Type**: Identifies whether this is for a registration or de-registration.
- **Registering Party Identity**: Identifies the registering party. This consists of the user's primary phone number.
- **Registrar Identity**: Identifies the registrar. This is always set to the IP address of the Application Server.
- **Request Address Information**: Identifies the contact information (IP address, port, and expiration) of the registering device, as included in the REGISTER request.
- **Response Address Information**: Identifies the contact information (IP address, port, and expiration) of the registering device, as included in the REGISTER response.
- **Failure Reason**: Identifies the reason for failure when the Application Server rejects the REGISTER request.
- **Expiration Period**: Identifies the registration expiration period.

Parameter Description	Example Data
Case Identifier	FBI000192
Intercept Access Element	80c2cb50
Time of event	20010922154536.125Z
Call Identifier Sequence Number System Identity	 1321:0 80c2cb50
Address Registration Type	1
Registering Party Identity	lineport@domain
Registrar Identity address port	 C0A80825 (binary for 192.168.8.37) 5060
Request Address Information address expiration	 sip:lineport@domain:5060 3599
Response Address Information address expiration	 sip:lineport@domain:5060 3599
Failure Reason generic	 Authentication Failure
Expiration Period generic	 3599

5 BroadWorks ASN.1 Definitions

This section describes the ASN.1 definitions that are used for encoding call data information when the “BroadWorks” CDC format is configured.

```
Laesp DEFINITIONS IMPLICIT TAGS::=
BEGIN

IMPORTS  UTF8String, VisibleString, GeneralizedTime FROM ASN-USEFUL;

LAESMessage ::= CHOICE {
   answer               [1] Answer,
          ccclose              [2] CCClose,
          ccopen               [3] CCOpen,
                        [4] NULL,   --Reserved
          origination          [5] Origination,
                        [6] NULL,   --Reserved
          redirection          [7] Redirection,
          release              [8] Release,
          servingSystem   [9] ServingSystem,
          terminationattempt [10] TerminationAttempt,
                        [11] NULL,  --Reserved
          ccchange             [12] CCChange,
          connection           [13] Connection,
          connectionBreak      [14] ConnectionBreak,
          dialedDgtExtrn       [15] DialedDigitExtraction,
          networkSignal        [16] NetworkSignal,
          subjectSignal        [17] SubjectSignal

}

Answer ::= SEQUENCE {
                        [0] CaseId,
                        [1] AccessingElementId,
                        [2] EventTime,
                        [3] CallId,
          answering     [4] PartyId OPTIONAL
}

CCChange::= SEQUENCE {
                        [0] CaseId,
                        [1] AccessingElementId,
                        [2] EventTime,
                        [3] CallId,
                        [4] EXPLICIT CCCId OPTIONAL,
          originating   [5] SDP OPTIONAL,
          terminating   [6] SDP OPTIONAL
}

CCClose ::= SEQUENCE {
                        [0] CaseId,
                        [1] AccessingElementId,
                        [2] EventTime,
                        [3] EXPLICIT CCCId OPTIONAL
}

CCOpen::= SEQUENCE {
                        [0] CaseId,
                        [1] AccessingElementId,
                        [2] EventTime,
                        CHOICE {
                             [3] SEQUENCE OF CallId,
                             [4] NULL         --Reserved
                        },
                        [5] CCCId OPTIONAL,
           originating     [6] SDP OPTIONAL,
           terminating     [7] SDP OPTIONAL
}

Connection ::= SEQUENCE {
                  [0] CaseId,
                  [1] AccessingElementId OPTIONAL,
                  [2] EventTime,
                  [3] SEQUENCE OF CallId,
    connectedParties [4] SEQUENCE OF PartyId OPTIONAL,
    newParties    [5] SEQUENCE OF PartyId OPTIONAL
}

ConnectionBreak ::= SEQUENCE {
                  [0] CaseId,
                  [1] AccessingElementId OPTIONAL,
                  [2] EventTime,
                  [3] SEQUENCE OF CallId,
    removedParties       [4] SEQUENCE OF PartyId OPTIONAL,
    remainingParties [5] SEQUENCE OF PartyId OPTIONAL,
    droppedParties       [6] SEQUENCE OF PartyId OPTIONAL
}

DialedDigitExtraction ::= SEQUENCE  {
                         [0] CaseId,
                         [1] AccessingElementId OPTIONAL,
                         [2] EventTime,
                         [3] CallId,
           digits        [4] VisibleString (SIZE (1..32))
}

NetworkSignal ::= SEQUENCE {
                  [0] CaseId,
                  [1] AccessingElementId OPTIONAL,
                  [2] EventTime,
                  [3] CallId OPTIONAL,
    alertingSignal       [4] AlertingSignal OPTIONAL,
    subjectAudibleSignal [5] AudibleSignal OPTIONAL,
    terminalDisplayInfo  [6] TerminalDisplayInfo OPTIONAL,
    other         [7] VisibleString (SIZE (1..128)) OPTIONAL,
    signalToParty   [8] PartyId
}

Origination ::= SEQUENCE {
                        [0] CaseId,
                        [1] AccessingElementId,
                        [2] EventTime,
                        [3] CallId,
           calling              [4] PartyId,
           called               [5] PartyId OPTIONAL,
           input                CHOICE {
           userinput            [6] VisibleString (SIZE (1..32)),
           translationinput     [7] VisibleString (SIZE (1..32))
                         },
                         [9] TransitCarrierId OPTIONAL
}

Redirection ::= SEQUENCE {
```

```
                         [0] CaseId,
                         [1] AccessingElementId,
                         [2] EventTime,
                         [3] CallId,
      redirectedto       [4] PartyId,
                         [5] TransitCarrierId OPTIONAL,
      redirectedfrom     [9] PartyId OPTIONAL
}

Release ::= SEQUENCE {
                         [0] CaseId,
                         [1] AccessingElementId,
                         [2] EventTime,
                         [3] CallId
}

ServingSystem ::= SEQUENCE  {
                        [0] CaseId,
                        [1] AccessingElementId  OPTIONAL,
                        [2] EventTime,
          systemIdentity       [3] VisibleString (SIZE (1..15))
OPTIONAL,
   networkAddress       [4] VisibleString (SIZE (1..15)) OPTIONAL,
          requestId     [5] CallId OPTIONAL,
          registrationType [6] AddressRegistrationType,
          registering   [7] PartyId,
          requesting    [8] PartyId OPTIONAL,
          registrar     [9] PartyId,
          requestAddressInfo  [10] CHOICE  {
          generic             [0] SEQUENCE OF SEQUENCE  {
            address            [0] PartyId,
            expirationPeriod   [1] INTEGER}
          } OPTIONAL,

          responseAddressInfo [11] CHOICE  {
          generic             [0] SEQUENCE OF SEQUENCE  {
            address            [0] PartyId,
            expirationPeriod   [1] INTEGER}
          } OPTIONAL,
          failureReason [12] Cause OPTIONAL,
          expirationPeriod [13] CHOICE  {
          generic              [0] INTEGER
                } OPTIONAL
}

SubjectSignal ::= SEQUENCE  {
                        [0] CaseId,
                        [1] AccessingElementId OPTIONAL,
                        [2] EventTime,
                        [3] CallId OPTIONAL,
          signalingPartyId [4] PartyId OPTIONAL,
          signal        [6] SEQUENCE {
          switchhookFlash      [0] VisibleString (SIZE (1..128))
OPTIONAL,
          dialedDigits         [1] VisibleString (SIZE (1..128))
OPTIONAL,
          featureKey           [2] VisibleString (SIZE (1..128))
OPTIONAL,
          otherSignalingInformation [3] VisibleString (SIZE (1..128))
OPTIONAL}
}
```

```
TerminationAttempt ::= SEQUENCE {
                        [0] CaseId,
                        [1] AccessingElementId,
                        [2] EventTime,
                        [3] CallId,
          calling          [4] PartyId,
          called           [5] PartyId OPTIONAL,
                        [7] RedirectedFromInfo OPTIONAL
}


AccessingElementId ::= VisibleString (SIZE(1..15))

AddressRegistrationType ::= ENUMERATED {
     unknown                          (0),
     registration              (1),
     deregistration                   (2),
     registrationAndDeregistration    (3)
}

CallId ::= SEQUENCE {
     sequencenumber     [0] VisibleString (SIZE(1..25)),
     systemidentity     [1] VisibleString (SIZE(1..15))
}

CaseId ::= VisibleString (SIZE(1..25))

Cause ::= SEQUENCE {
     signalingType       [0] UTF8String,
     cause               [1] ParameterFormat OPTIONAL
}

CCCId ::= CHOICE {
     combCCC            [0] VisibleString (SIZE(1..20)),
     sepCCCpair         [1] SEQUENCE {
     sepXmitCCC             [0] VisibleString (SIZE(1..20)),
     sepRecvCCC             [1] VisibleString (SIZE(1..20))
                        }
}

EventTime ::= GeneralizedTime

PartyId ::= SEQUENCE {
                        [0] NULL OPTIONAL, -- Reserved
                        [1] NULL OPTIONAL, -- Reserved
                        [2] NULL OPTIONAL, -- Reserved
                        [3] NULL OPTIONAL, -- Reserved
                        [4] NULL OPTIONAL, -- Reserved
                        [5] NULL OPTIONAL, -- Reserved
     dn                 [6] VisibleString (SIZE(1..15)) OPTIONAL,
     userProvided       [7] VisibleString (SIZE(1..15)) OPTIONAL,
                        [8] NULL OPTIONAL, -- Reserved
                        [9] NULL OPTIONAL, -- Reserved
     ipAddress           [10] IpAddress                OPTIONAL,
                        [11] NULL OPTIONAL, -- Reserved
     trunkId            [12] VisibleString (SIZE(1..32)) OPTIONAL,
                        [13] NULL OPTIONAL, -- Reserved
     genericAddress     [14] VisibleString (SIZE(1..32)) OPTIONAL,
     genericDigits      [15] VisibleString (SIZE(1..32)) OPTIONAL,
     genericName        [16] VisibleString (SIZE(1..48)) OPTIONAL,
     port               [17] VisibleString (SIZE(1..32)) OPTIONAL,
     context            [18] VisibleString (SIZE(1..32)) OPTIONAL,
     uri          [21] SET OF UTF8String OPTIONAL,
     fqdn                [29] UTF8String OPTIONAL
}

RedirectedFromInfo ::= SEQUENCE {
           lastRedirecting  [0] PartyId OPTIONAL,
           originalCalled   [1] PartyId OPTIONAL,
           numRedirections  [2] INTEGER (1..100) OPTIONAL
}

SDP ::= VisibleString (SIZE(1..2048))

TransitCarrierId ::= VisibleString (SIZE(3..7))

AlertingSignal ::= ENUMERATED {
    notUsed              (0),
    alertingPattern0     (1),
    alertingPattern1     (2),
    alertingPattern2     (3),
    alertingPattern3     (4),
    alertingPattern4     (5),
    callWaitingPattern1  (6),
    callWaitingPattern2  (7),
    callWaitingPattern3  (8),
    callWaitingPattern4  (9),
    bargeInTone          (10)
}



AudibleSignal ::= ENUMERATED {
    notUsed              (0),
    dialTone             (1),
    recallDialTone              (2),
    ringbackTone         (3),
    reorderTone          (4),
    busyTone             (5),
    confirmationTone     (6),
    expensiveRouteTone   (7),
    messageWaitingTone   (8),
    receiverOffHookTone  (9),
    specialInfoTone      (10),
    denialTone           (11),
    interceptTone               (12),
    answerTone           (13),
    tonesOff             (14),
    pipTone              (15),
    abbreviatedIntercept        (16),
    abbreviatedCongestion       (17),
    warningTone          (18),
    dialToneBurst               (19),
    numberUnObtainableTone      (20),
    authenticationFailTone      (21)
}

TerminalDisplayInfo ::= SEQUENCE {
    generalDisplay              [0] VisibleString (SIZE (1..80))
OPTIONAL,
    calledNumber         [1] VisibleString (SIZE (1..40)) OPTIONAL,
    callingNumber               [2] VisibleString (SIZE (1..40))
OPTIONAL,
    callingName          [3] VisibleString (SIZE (1..40)) OPTIONAL,
   originalCalledNumber        [4] VisibleString (SIZE (1..40))
OPTIONAL,
   lastRedirectingNumber       [5] VisibleString (SIZE (1..40))
OPTIONAL,
   redirectingName      [6] VisibleString (SIZE (1..40)) OPTIONAL,
   redirectingReason    [7] VisibleString (SIZE (1..40)) OPTIONAL,
   messageWaitingNotif  [8] VisibleString (SIZE (1..40)) OPTIONAL
}

IpAddress ::= CHOICE
{
          ipV4                 [1] IPvalue,
          ipV6                 [2] IPvalue
}

IPvalue ::=  OCTET STRING (SIZE(4..16))      -- binary encoding

ParameterFormat ::= CHOICE {
          generic                     [0] UTF8String
}

END
```

6 Event Scenarios

The following scenarios provide details regarding the generation of events over the CDC. For all scenarios, the independent and interceptHeld options for the CCLinks in use are set to “true” unless specified otherwise.

6.1 Call Originated by Subject with No Early Media

The originating subject (A) dials an extension number to reach the terminating party (B). The terminating endpoint device does not provide early media so the originating endpoint device provides ring back locally. The CCOpen event is sent only once the call is actually answered.

LI Event	Common Attributes		Specific Attributes
Origination	CaseIdentity IAPSystemIdentity TimeStamp CallIdentity SequenceNumber SystemIdentity	FBI1234 DEFAULT 20020423183017.220Z 2:0 DEFAULT	Calling Party Identifier: 5146972000 Called Party Identifier: 5146972004 User Input: 2004

CCOpen	CaseIdentity
	IAPSystemIdentity
	TimeStamp
	CallIdentity
	SequenceNumber
	SystemIdentity
		FBI1234
		DEFAULT
		20020423183019.754Z
		
		2:0
		DEFAULT
			CCCIdentity
			SepCCCpair
			SepXmitCCC +15146975000
			SepRecvCCC +15146975001
			Originating SDP
			v=0
			o=Vega50 18 1 IN IP4 192.168.13.2
			s=Sip Call
			c=IN IP4 192.168.13.2
			t=0 0
			m=audio 10032 RTP/AVP 0
			a=rtpmap:0 PCMU/8000
			Terminating SDP
			v=0
			o=CiscoSystemsSIP-IPPhone-UserAgent 10829 28346 IN IP4 192.168.8.244
			s=SIP Call
			c=IN IP4 192.168.8.244
			t=0 0
			m=audio 21336 RTP/AVP 0
			a=rtpmap:0 PCMU/8000

Answer	CaseIdentity IAPSystemIdentity TimeStamp CallIdentity SequenceNumber SystemIdentity	FBI1234 DEFAULT 20020423183019.744Z 2:0 DEFAULT	Answering Party Identifier: 5146972004

LI Event	Common Attributes		Specific Attributes	
CCClose	CaseIdentity IAPSystemIdentity TimeStamp CallIdentity SequenceNumber SystemIdentity	FBI1234 DEFAULT 20020423183249.859Z 2:0 DEFAULT	CCCIdentity SepCCCpair SepXmitCCC SepRecvCCC	 +15146975000 +15146975001
Release	CaseIdentity IAPSystemIdentity TimeStamp CallIdentity SequenceNumber SystemIdentity	FBI1234 DEFAULT 20020423183249.859Z 2:0 DEFAULT		

6.2 Subject Receives Call and Endpoint Device Provides Early Media

The originating party (A) dials an extension number to reach the terminating subject (B). The terminating endpoint device provides early media. In this case, the terminating endpoint device provides remote ring back to the originating endpoint device, and the CCOpen is sent when the 180 Ringing is received from the terminating endpoint device.

LI Event	Common Attributes	Specific Attributes
Termination Attempt	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423183403.936Z CallIdentity SequenceNumber: 11:0 SystemIdentity DEFAULT	Calling Party Identifier: 5146972004 Called Party Identifier: 5146972000 Redirected From Information Last Party Identity: First Party Identity: Number of Redirections:

CCOpen	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20020423183404.226Z
	CallIdentity
	SequenceNumber 11:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975000
		SepRecvCCC +15146975001
		Originating SDP
		v=0
		o=CiscoSystemsSIP-IPPhone-UserAgent 4023 6204 IN IP4 192.168.8.244
		s=SIP Call
		c=IN IP4 192.168.8.244
		t=0 0
		m=audio 21338 RTP/AVP 0 8 18 100
		a=rtpmap:0 PCMU/8000
		a=rtpmap:100 telephone-event/8000
		a=fmtp:100 0-15
		Terminating SDP
		v=0
		o=Vega50 19 1 IN IP4 192.168.13.2
		s=Sip Call
		c=IN IP4 192.168.13.2
		t=0 0
		m=audio 10034 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

Answer	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423183412.959Z CallIdentity SequenceNumber 11:0 SystemIdentity: DEFAULT	Answering Party Identifier: 5146972000

LI Event	Common Attributes	Specific Attributes
CCClose	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423183646.620Z CallIdentity SequenceNumber 11:0 SystemIdentity: DEFAULT	CCCIdentity SepCCCpair SepXmitCCC +15146975000 SepRecvCCC +15146975001
Release	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423183646.620Z CallIdentity SequenceNumber 11:0 SystemIdentity: DEFAULT	

6.3 Subject Receives a Call (Previously Redirected)

The incoming call to the subject was redirected on the public network or on BroadWorks. The incoming INVITE contains a diversion header. This scenario demonstrates how the diversion information is captured in the Termination Attempt event sent to the LEA.

LI Event	Common Attributes	Specific Attributes
Termination Attempt	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423183935.072Z CallIdentity SequenceNumber 18:0 SystemIdentity: DEFAULT	Calling Party Identifier: 5146972004 Called Party Identifier: 5146972000 Redirected From Information Last Party Identity: 5146971000 First Party Identity: 5146971000 Number of Redirections: 1

CCOpen	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20020423183935.433Z
	CallIdentity
	SequenceNumber 18:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975000
		SepRecvCCC +15146975001
		Originating SDP
		v=0
		o=CiscoSystemsSIP-IPPhone-UserAgent 13494 1210 IN IP4 192.168.8.244
		s=SIP Call
		c=IN IP4 192.168.8.244
		t=0 0
		m=audio 21340 RTP/AVP 0 8 18 100
		a=rtpmap:0 PCMU/8000
		a=rtpmap:100 telephone-event/8000
		a=fmtp:100 0-15
		Terminating SDP
		v=0
		o=Vega50 21 1 IN IP4 192.168.13.2
		s=Sip Call
		c=IN IP4 192.168.13.2
		t=0 0
		m=audio 10036 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

Answer	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423183948.862Z CallIdentity SequenceNumber 18:0 SystemIdentity: DEFAULT	Answering Party Identifier: 5146972000
CCClose	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423184246.437Z CallIdentity SequenceNumber 18:0 SystemIdentity: DEFAULT	CCCIdentity SepCCCpair SepXmitCCC +15146975000 SepRecvCCC +15146975001

LI Event	Common Attributes	Specific Attributes
Release	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423184246.437Z CallIdentity SequenceNumber 18:0 SystemIdentity: DEFAULT	

6.4 Call is Held and Retrieved by Surveillance Subject

In this scenario, the originating subject (A) simply puts the called party (B) on hold. This is also typical of a call waiting scenario where the user switches back and forth between two calls. The events are shown below from the perspective of a single call.

For this scenario, it is assumed that the interceptHeld option is set to “false”. This means that the LEA collection function must not receive the intercepted media. This is accomplished by removing the appropriate listeners from the MS repeaters as indicated in the following table.

If the interceptHeld option is set to “true”, then the listeners are not removed and the LEA collection function is allowed to listen to the intercepted media, assuming that the other party’s device is transmitting media.

LI Event	Common Attributes	Specific Attributes
Origination	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423202748.129Z CallIdentity SequenceNumber 545:0 SystemIdentity: DEFAULT	Calling Party Identifier: 5146972000 Called Party Identifier: 5146973000 User Input: 5146973000

CCOpen	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20020423202749.761Z
	CallIdentity
	SequenceNumber 545:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975000
		SepRecvCCC +15146975001
		Originating SDP
		v=0
		o=Vega50 46 1 IN IP4 192.168.13.2
		s=Sip Call
		c=IN IP4 192.168.13.2
		t=0 0
		m=audio 10062 RTP/AVP 0
		a=rtpmap:0 PCMU/8000
		0
		Terminating SDP
		v=0
		o=Vega50 3 1 IN IP4 192.168.12.20
		s=Sip Call
		c=IN IP4 192.168.12.20
		t=0 0
		m=audio 10002 RTP/AVP
		a=rtpmap:0 PCMU/8000

Answer	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423202752.615Z CallIdentity SequenceNumber 545:0 SystemIdentity: DEFAULT	Answering Party Identifier: 5146973000

LI Event	Common Attributes	Specific Attributes

CCChange	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20020423202833.764Z
	CallIdentity
	SequenceNumber 545:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975000
		SepRecvCCC +15146975001
		Originating SDP
		v=0
		o=BroadWks 19 0 IN IP4 192.168.8.41
		s=SIP Call
		c=IN IP4 0.0.0.0
		t=0 0
		m=audio 5000 RTP/AVP 0
		Terminating SDP
		v=0
		o=Vega50 3 1 IN IP4 192.168.12.20
		s=Sip Call
		c=IN IP4 192.168.12.20
		t=0 0
		m=audio 10002 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

CCChange	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20020423202837.480Z
	CallIdentity
	SequenceNumber 545:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975000
		SepRecvCCC +15146975001
		Originating SDP
		v=0
		o=Vega50 46 1 IN IP4 192.168.13.2
		s=Sip Call
		c=IN IP4 192.168.13.2
		t=0 0
		m=audio 10062 RTP/AVP 0
		a=rtpmap:0 PCMU/8000
		Terminating SDP
		v=0
		o=Vega50 3 1 IN IP4 192.168.12.20
		s=Sip Call
		c=IN IP4 192.168.12.20
		t=0 0
		m=audio 10002 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

CCClose	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423202840.093Z	CCCIdentity SepCCCpair SepXmitCCC +15146975000 SepRecvCCC +15146975001
Release	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423202840.093Z CallIdentity SequenceNumber 545:0 SystemIdentity: DEFAULT	

6.5 Call Waiting

In this scenario, the originating subject (A) calls party B, and then answers the call waiting call from party C. After this, party C releases its call, subject A retrieves the now held call to party B, and finally party B releases its call. The scenario is shown for both cases of independent CCLinks (independent option set to “true”) and shared CCLinks (independent option set to “false”). Also, for both scenarios, it is assumed that the interceptHeld option is set to “true”.

6.5.1 Independent CCLink (Independent Option True)

LI Event	Common Attributes	Specific Attributes
Origination	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20030815181824.703Z CallIdentity SequenceNumber 2:0 SystemIdentity: DEFAULT	Calling Party Identifier: 5146972000 Called Party Identifier: 5146972004 User Input: 2004

CCOpen	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20030815181824.954Z
	CallIdentity
	SequenceNumber 2:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975000
		SepRecvCCC +15146975001
		Originating SDP
		v=0
		o=Vega50 18 1 IN IP4 192.168.13.2
		s=Sip Call
		c=IN IP4 192.168.13.2
		t=0 0
		m=audio 10032 RTP/AVP 0
		a=rtpmap:0 PCMU/8000
		Terminating SDP
		v=0
		o=CiscoSystemsSIP-IPPhone-UserAgent 10829 28346 IN IP4 192.168.8.244
		s=SIP Call
		c=IN IP4 192.168.8.244
		t=0 0
		m=audio 21336 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

Answer	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20030815181828.429Z CallIdentity SequenceNumber 2:0 SystemIdentity: DEFAULT	Answering Party Identifier: 5146972004
Termination Attempt	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20030815181834.097Z CallIdentity SequenceNumber 2:1 SystemIdentity: DEFAULT	Calling Party Identifier: 5146972008 Called Party Identifier: 5146972000 Redirected From Information Last Party Identity: First Party Identity: Number of Redirections:

LI Event	Common Attributes	Specific Attributes

CCChange	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20030815181834.097Z
	CallIdentity
	SequenceNumber 2:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975000
		SepRecvCCC +15146975001
		Originating SDP
		v=0
		o=BroadWks 19 0 IN IP4 192.168.8.41
		s=SIP Call
		c=IN IP4 0.0.0.0
		t=0 0
		m=audio 5000 RTP/AVP 0
		Terminating SDP
		v=0
		o=Vega50 3 1 IN IP4 192.168.12.20
		s=Sip Call
		c=IN IP4 192.168.12.20
		t=0 0
		m=audio 10002 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

CCOpen	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20030815181839.855Z
	CallIdentity
	SequenceNumber 2:1
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975002
		SepRecvCCC +15146975003
		Originating SDP
		v=0
		o=CiscoSystemsSIP-IPPhone-UserAgent 4023 6204 IN IP4 192.168.8.244
		s=SIP Call
		c=IN IP4 192.168.8.244
		t=0 0
		m=audio 21338 RTP/AVP 0 8 18 100
		a=rtpmap:0 PCMU/8000
		a=rtpmap:100 telephone-event/8000
		a=fmtp:100 0-15
		Terminating SDP
		v=0
		o=Vega50 19 1 IN IP4 192.168.13.2
		s=Sip Call
		c=IN IP4 192.168.13.2
		t=0 0
		m=audio 10034 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

Answer	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20030815181839.855Z CallIdentity SequenceNumber 2:1 SystemIdentity: DEFAULT	Answering Party Identifier: 5146972000
CCClose	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20030815181847.636Z CallIdentity SequenceNumber 2:1 SystemIdentity: DEFAULT	CCCIdentity SepCCCpair SepXmitCCC +15146975002 SepRecvCCC +15146975003
Release	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20030815181847.636Z CallIdentity SequenceNumber 2:1 SystemIdentity: DEFAULT	

LI Event	Common Attributes	Specific Attributes

CCChange	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20030815181851.021Z
	CallIdentity
	SequenceNumber 2:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975000
		SepRecvCCC +15146975001
		Originating SDP
		v=0
		o=Vega50 20 1 IN IP4 192.168.13.2
		s=Sip Call
		c=IN IP4 192.168.13.2
		t=0 0
		m=audio 10032 RTP/AVP 0
		a=rtpmap:0 PCMU/8000
		Terminating SDP
		v=0
		o=CiscoSystemsSIP-IPPhone-UserAgent 10830 28347 IN IP4 192.168.8.244
		s=SIP Call
		c=IN IP4 192.168.8.244
		t=0 0
		m=audio 21336 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

CCClose	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20030815181853.645Z CallIdentity SequenceNumber 2:0 SystemIdentity: DEFAULT	CCCIdentity SepCCCpair SepXmitCCC +15146975000 SepRecvCCC +15146975001
Release	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20030815181853.655Z CallIdentity SequenceNumber 2:0 SystemIdentity: DEFAULT	

6.5.2 Shared CCLink (Independent Option False)

LI Event	Common Attributes	Specific Attributes
Origination	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20030815181356.348Z CallIdentity SequenceNumber 2:0 SystemIdentity: DEFAULT	Calling Party Identifier: 5146972000 Called Party Identifier: 5146972004 User Input: 2004

CCOpen	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20030815181356.608Z
	CallIdentity
	SequenceNumber 2:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975000
		SepRecvCCC +15146975001
		Originating SDP
		v=0
		o=Vega50 18 1 IN IP4 192.168.13.2
		s=Sip Call
		c=IN IP4 192.168.13.2
		t=0 0
		m=audio 10032 RTP/AVP 0
		a=rtpmap:0 PCMU/8000
		Terminating SDP
		v=0
		o=CiscoSystemsSIP-IPPhone-UserAgent 10829 28346 IN IP4 192.168.8.244
		s=SIP Call
		c=IN IP4 192.168.8.244
		t=0 0
		m=audio 21336 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

Answer	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20030815181400.443Z CallIdentity SequenceNumber 2:0 SystemIdentity: DEFAULT	Answering Party Identifier: 5146972004
Termination Attempt	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20030815181404.780Z CallIdentity SequenceNumber 2:1 SystemIdentity: DEFAULT	Calling Party Identifier: 5146972008 Called Party Identifier: 5146972000 Redirected From Information Last Party Identity: First Party Identity. Number of Redirections:

CCChange	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20030815181410.328Z
	CallIdentity
	SequenceNumber 2:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975000
		SepRecvCCC +15146975001
		Originating SDP
		v=0
		o=BroadWks 19 0 IN IP4 192.168.8.41
		s=SIP Call
		c=IN IP4 0.0.0.0
		t=0 0
		m=audio 5000 RTP/AVP 0
		Terminating SDP
		v=0
		o=Vega50 3 1 IN IP4 192.168.12.20
		s=Sip Call
		c=IN IP4 192.168.12.20
		t=0 0
		m=audio 10002 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

LI Event	Common Attributes	Specific Attributes
CCChange	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20030815181410.388Z CallIdentity SequenceNumber 2:0 SystemIdentity: DEFAULT	CCCIdentity SepCCCpair SepXmitCCC +15146975000 SepRecvCCC +15146975001 Originating SDP UNKNOWN Terminating SDP UNKNOWN

CCOpen	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20030815181410.418Z
	CallIdentity
	SequenceNumber 2:1
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975000
		SepRecvCCC +15146975001
		Originating SDP
		v=0
		o=CiscoSystemsSIP-IPPhone-UserAgent 4023 6204 IN IP4 192.168.8.244
		s=SIP Call
		c=IN IP4 192.168.8.244
		t=0 0
		m=audio 21338 RTP/AVP 0 8 18 100
		a=rtpmap:0 PCMU/8000
		a=rtpmap:100 telephone-event/8000
		a=fmtp:100 0-15
		Terminating SDP
		v=0
		o=Vega50 19 1 IN IP4 192.168.13.2
		s=Sip Call
		c=IN IP4 192.168.13.2
		t=0 0
		m=audio 10034 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

Answer	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20030815181410.418Z CallIdentity SequenceNumber 2:1 SystemIdentity: DEFAULT	Answering Party Identifier: 5146972000
Release	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20030815181426.671Z CallIdentity SequenceNumber 2:1 SystemIdentity: DEFAULT	

CCChange	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20030815181430.657Z
	CallIdentity
	SequenceNumber 2:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975000
		SepRecvCCC +15146975001
		Originating SDP
		v=0
		o=Vega50 20 1 IN IP4 192.168.13.2
		s=Sip Call
		c=IN IP4 192.168.13.2
		t=0 0
		m=audio 10032 RTP/AVP 0
		a=rtpmap:0 PCMU/8000
		Terminating SDP
		v=0
		o=CiscoSystemsSIP-IPPhone-UserAgent 10830 28347 IN IP4 192.168.8.244
		s=SIP Call
		c=IN IP4 192.168.8.244
		t=0 0
		m=audio 21336 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

LI Event	Common Attributes	Specific Attributes
CCClose	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20030815181437.016Z CallIdentity SequenceNumber 2:0 SystemIdentity: DEFAULT	CCCIdentity SepCCCpair SepXmitCCC +15146975000 SepRecvCCC +15146975001
Release	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20030815181437.036Z CallIdentity SequenceNumber 2:0 SystemIdentity: DEFAULT	

6.6 Subject Blind Transfers Call to Third Party

In this scenario, the subject (B) transfers the calling party (A) to some other party (C) while the incoming call is in the alerting state. Here the terminating endpoint device (B) provides early media; hence CCCs are opened while the first call leg is ringing. The CCC is closed as soon as the call is redirected. The lawful interception is resumed on the second call leg and the original calling party (A) is designated as the surveillance subject.

LI Event	Common Attributes	Specific Attributes
Termination Attempt	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423204602.743Z CallIdentity SequenceNumber 576:0 SystemIdentity: DEFAULT	Calling Party Identifier: 5146973000 Called Party Identifier: 5146972000 Redirected From Information Last Party Identity: First Party Identity: Number of Redirections:

CCOpen	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20020423204605.276Z
	CallIdentity
	SequenceNumber 576:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975001
		SepRecvCCC +15146975000
		Originating SDP
		v=0
		o=Vega50 5 1 IN IP4 192.168.12.20
		s=Sip Call
		c=IN IP4 192.168.12.20
		t=0 0
		m=audio 10004 RTP/AVP 0
		a=rtpmap:0 PCMU/8000
		Terminating SDP
		v=0
		o=Vega50 47 1 IN IP4 192.168.13.2
		s=Sip Call
		c=IN IP4 192.168.13.2
		t=0 0
		m=audio 10064 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

Redirection	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423204610.964Z CallIdentity SequenceNumber 576:0 SystemIdentity: DEFAULT	Redirected To Party Identifier: 5146972004 Redirected From Party Identifier: 5146792000
CCClose	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423204611.055Z	CCCIdentity SepCCCpair SepXmitCCC +15146975001 SepRecvCCC +15146975000

LI Event	Common Attributes	Specific Attributes

CCOpen	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20020423204615.601Z
	CallIdentity
	SequenceNumber 575:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975000
		SepRecvCCC +15146975001
		Originating SDP
		v=0
		o=Vega50 5 1 IN IP4 192.168.12.20
		s=Sip Call
		c=IN IP4 192.168.12.20
		t=0 0
		m=audio 10004 RTP/AVP 0
		a=rtpmap:0 PCMU/8000
		
		Terminating SDP
		v=0
		o=CiscoSystemsSIP-IPPhone-UserAgent 11648 26294 IN IP4 192.168.8.244
		s=SIP Call
		c=IN IP4 192.168.8.244
		t=0 0
		m=audio 21368 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

Answer	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423204615.601Z CallIdentity SequenceNumber 575:0 SystemIdentity: DEFAULT	Answering Party Identifier: 5146972004
CCClose	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423204624.434Z	CCCIdentity SepCCCpair SepXmitCCC +15146975000 SepRecvCCC +15146975001
Release	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423204624.444Z CallIdentity SequenceNumber 575:0 SystemIdentity: DEFAULT	

6.7 Call Transferred by Remote Party

The remote party transfers the subject. In this case, the redirection event is not sent to the LEA/MD and the CCCs remain open. However, the CCChange event is sent to the LEA/MD to capture the change in the other party's SDP, and the new media path in the receive direction is delivered over the existing CCC.

LI Event	Common Attributes	Specific Attributes
Termination Attempt	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423200012.708Z CallIdentity SequenceNumber 517:0 SystemIdentity: DEFAULT	Calling Party Identifier: 5146973000 Called Party Identifier: 5146972000 Redirected From Information Last Party Identity: First Party Identity: Number of Redirections:

CCOpen	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20020423200013.479Z
	CallIdentity
	SequenceNumber 517:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975001
		SepRecvCCC +15146975000
		Originating SDP
		v=0
		o=Vega50 2 1 IN IP4 192.168.12.20
		s=Sip Call
		c=IN IP4 192.168.12.20
		t=0 0
		m=audio 10000 RTP/AVP 0
		a=rtpmap:0 PCMU/8000
		Terminating SDP
		v=0
		o=Vega50 44 1 IN IP4 192.168.13.2
		s=Sip Call
		c=IN IP4 192.168.13.2
		t=0 0
		m=audio 10060 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

Answer	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423200021.571Z CallIdentity SequenceNumber 517:0 SystemIdentity: DEFAULT	Answering Party Identifier: 5146972000

CCChange	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20020423200050.242Z
	CallIdentity
	SequenceNumber 517:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975001
		SepRecvCCC +15146975000
		Originating SDP
		v=0
		o=CiscoSystemsSIP-IPPhone-UserAgent 1948 8425 IN IP4 192.168.8.244
		s=SIP Call
		c=IN IP4 192.168.8.244
		t=0 0
		m=audio 21366 RTP/AVP 0
		a=rtpmap:0 PCMU/8000
		,
		Terminating SDP
		v=0
		o=Vega50 44 1 IN IP4 192.168.13.2
		s=Sip Call
		c=IN IP4 192.168.13.2
		t=0 0
		m=audio 10060 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

LI Event	Common Attributes	Specific Attributes
CCClose	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423200548.731Z	CCCIdentity SepCCCpair SepXmitCCC +15146975001 SepRecvCCC +15146975000
Release	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423200548.731Z CallIdentity SequenceNumber 517:0 SystemIdentity: DEFAULT	

6.8 Call Involves Two Surveillance Subjects

The originating subject (A) dials an extension number to reach the terminating subject (B).

LI Event	Common Attributes	Specific Attributes
Origination – A	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423195030.371Z CallIdentity SequenceNumber 457:0 SystemIdentity: DEFAULT	Calling Party Identifier: 5146972004 Called Party Identifier: 5146972000 User Input: 2000
Termination Attempt - B	CaseIdentity: FBI0000 IAPSystemIdentity: DEFAULT TimeStamp: 20020423195030.371Z CallIdentity SequenceNumber 460:0 SystemIdentity: DEFAULT	Calling Party Identifier: 5146972004 Called Party Identifier: 5146972000 Redirected From Information Last Party Identity: First Party Identity: Number of Redirections:

CCOpen - A	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20020423195031.803Z
	CallIdentity
	SequenceNumber 457:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146976000
		SepRecvCCC +15146976001
		Originating SDP
		v=0
		o=CiscoSystemsSIP-IPPhone-UserAgent 28441 22653 IN IP4 192.168.8.244
		s=SIP Call
		c=IN IP4 192.168.8.244
		t=0 0
		m=audio 21364 RTP/AVP 0 8 18 100
		a=rtpmap:0 PCMU/8000
		a=rtpmap:100 telephone-event/8000
		a=fmtp:100 0-15
		Terminating SDP
		v=0
		o=Vega50 42 1 IN IP4 192.168.12.6
		s=Sip Call
		c=IN IP4 192.168.12.6
		t=0 0
		m=audio 11674 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

LI Event	Common Attributes	Specific Attributes

CCOpen – B	CaseIdentity: FBI0000
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20020423195031.693Z
	CallIdentity
	SequenceNumber 460:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975001
		SepRecvCCC +15146975000
		Originating SDP
		v=0
		o=CiscoSystemsSIP-IPPhone-UserAgent 28441 22653 IN IP4 192.168.12.6
		s=SIP Call
		c=IN IP4 192.168.12.6
		t=0 0
		m=audio 11672 RTP/AVP 0 8 18 100
		a=rtpmap:0 PCMU/8000
		a=rtpmap:100 telephone-event/8000
		a=fmtp:100 0-15
		Terminating SDP
		v=0
		o=Vega50 42 1 IN IP4 192.168.13.2
		s=Sip Call
		c=IN IP4 192.168.13.2
		t=0 0
		m=audio 10058 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

Answer – A	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423195040.135Z CallIdentity SequenceNumber 457:0 SystemIdentity: DEFAULT	Answering Party Identifier: 5146972000
Answer – B	CaseIdentity: FBI0000 IAPSystemIdentity: DEFAULT TimeStamp: 20020423195040.135Z CallIdentity SequenceNumber 460:0 SystemIdentity: DEFAULT	Answering Party Identifier: 5146972000
CCClose – A	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423195647.553Z	CCCIdentity SepCCCpair SepXmitCCC +15146976000 SepRecvCCC +15146976001
Release – A	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423195647.553Z CallIdentity SequenceNumber 457:0 SystemIdentity: DEFAULT	
CCClose – B	CaseIdentity: FBI0000 IAPSystemIdentity: DEFAULT TimeStamp: 20020423195647.563Z	CCCIdentity SepCCCpair SepXmitCCC +15146975001 SepRecvCCC +15146975000
Release – B	CaseIdentity: FBI0000 IAPSystemIdentity: DEFAULT TimeStamp: 20020423195647.683Z CallIdentity SequenceNumber 460:0 SystemIdentity: DEFAULT	

6.9 Subject Transfers Call to Third Party in Consultation Mode

In this scenario, the subject has a first party on hold and is in consultation mode with a third party. The subject selects to transfer the first party to the third party. For this scenario, it is assumed that the CCLink is configured with the interceptHeld and independent options are set to “true”.

LI Event	Common Attributes	Specific Attributes
Termination Attempt	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190852.339Z CallIdentity SequenceNumber 359:0 SystemIdentity: DEFAULT	Calling Party Identifier: 5146973000 Called Party Identifier: 5146972000 Redirected From Information Last Party Identity First Party Identity: Number of Redirections:

CCOpen	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20020423190853.270Z
	CallIdentity
	SequenceNumber 359:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975001
		SepRecvCCC +15146975000
		Originating SDP
		v=0
		o=Vega50 12 1 IN IP4 192.168.12.20
		s=Sip Call
		c=IN IP4 192.168.12.20
		t=0 0
		m=audio 10012 RTP/AVP 0
		a=rtpmap:0 PCMU/8000
		Terminating SDP
		v=0
		o=Vega50 38 1 IN IP4 192.168.13.2
		s=Sip Call
		c=IN IP4 192.168.13.2
		t=0 0
		m=audio 10054 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

Answer	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190856.525Z CallIdentity SequenceNumber 359:0 SystemIdentity: DEFAULT	Answering Party Identifier: 5146972000

CCChange	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20020423190859.689Z
	CallIdentity
	SequenceNumber 359:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975001
		SepRecvCCC +15146975000
		Originating SDP
		v=0
		o=Vega50 12 1 IN IP4 192.168.12.20
		s=Sip Call
		c=IN IP4 192.168.12.20
		t=0 0
		m=audio 10012 RTP/AVP 0
		a=rtpmap:0 PCMU/8000
		Terminating SDP
		v=0
		o=BroadWks 13 0 IN IP4 192.168.8.41
		s=SIP Call
		c=IN IP4 0.0.0.0
		t=0 0
		m=audio 5000 RTP/AVP 0

Origination	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190902.714Z CallIdentity SequenceNumber 359:1 SystemIdentity: DEFAULT	Calling Party Identifier: 5146972000 Called Party Identifier: 5146972004 User Input: 2004

LI Event	Common Attributes	Specific Attributes

CCOpen	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20020423190905.798Z
	CallIdentity
	SequenceNumber 359:1
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975002
		SepRecvCCC +15146975003
		Originating SDP
		v=0
		o=Vega50 39 1 IN IP4 192.168.13.2
		s=Sip Call
		c=IN IP4 192.168.13.2
		t=0 0
		m=audio 10054 RTP/AVP 0
		a=rtpmap:0 PCMU/8000
		Terminating SDP
		v=0
		o=CiscoSystemsSIP-IPPhone-UserAgent 4694 4121 IN IP4 192.168.8.244
		s=SIP Call
		c=IN IP4 192.168.8.244
		t=0 0
		m=audio 21358 RTP/AVP 0

Answer	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190905.798Z CallIdentity SequenceNumber 359:1 SystemIdentity: DEFAULT	Answering Party Identifier: 5146972004
CCClose	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190956.912Z	CCCIdentity SepCCCpair SepXmitCCC +15146975001 SepRecvCCC +15146975000
CCClose	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190956.922Z	CCCIdentity SepCCCpair SepXmitCCC +15146975002 SepRecvCCC +15146975003
Redirection	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190956.922Z CallIdentity SequenceNumber 359:1 SystemIdentity: DEFAULT	Redirected To Party Identifier: 5146972004 Redirected From Party Identifier: 5146792000
Release	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190956.922Z CallIdentity SequenceNumber 359:0 SystemIdentity: DEFAULT	

LI Event	Common Attributes	Specific Attributes

CCOpen	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20020423190957.843Z
	CallIdentity
	SequenceNumber 188:5
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975000
		SepRecvCCC +15146975001
		Originating SDP
		v=0
		o=CiscoSystemsSIP-IPPhone-UserAgent 4694 4121 IN IP4 192.168.8.244
		s=SIP Call
		c=IN IP4 192.168.8.244
		t=0 0
		m=audio 21358 RTP/AVP 0
		a=rtpmap:0 PCMU/8000
		Terminating SDP
		v=0
		o=Vega50 12 1 IN IP4 192.168.12.20
		s=Sip Call
		c=IN IP4 192.168.12.20
		t=0 0
		m=audio 10012 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

CCClose	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423191043.679Z	CCCIdentity SepCCCpair SepXmitCCC +15146975000 SepRecvCCC +15146975001
Release	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423191043.679Z CallIdentity SequenceNumber 188:5 SystemIdentity: DEFAULT	

6.10 Subject Conferences Two Calls

In this scenario, the subject has a first party on hold and is in consultation mode with a third party. The subject selects to conference the two calls together. For this scenario, it is assumed that the CCLink is configured with the interceptHeld and independent options are set to “true”.

LI Event	Common Attributes	Specific Attributes
Termination Attempt	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190852.339Z CallIdentity SequenceNumber 359:0 SystemIdentity: DEFAULT	Calling Party Identifier: 5146973000 Called Party Identifier: 5146972000 Redirected From Information Last Party Identity: First Party Identity: Number of Redirections:

CCOpen	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20020423190853.270Z
	CallIdentity
	SequenceNumber 359:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975001
		SepRecvCCC +15146975000
		Originating SDP
		v=0
		o=Vega50 12 1 IN IP4 192.168.12.20
		s=Sip Call
		c=IN IP4 192.168.12.20
		t=0 0
		m=audio 10012 RTP/AVP 0
		a=rtpmap:0 PCMU/8000
		Terminating SDP
		v=0
		o=Vega50 38 1 IN IP4 192.168.13.2
		s=Sip Call
		c=IN IP4 192.168.13.2
		t=0 0
		m=audio 10054 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

Answer	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190856.525Z CallIdentity SequenceNumber 359:0 SystemIdentity: DEFAULT	Answering Party Identifier: 5146972000

CCChange	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20020423190859.689Z
	CallIdentity
	SequenceNumber 359:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975001
		SepRecvCCC +15146975000
		Originating SDP
		v=0
		o=Vega50 12 1 IN IP4 192.168.12.20
		s=Sip Call
		c=IN IP4 192.168.12.20
		t=0 0
		m=audio 10012 RTP/AVP 0
		a=rtpmap:0 PCMU/8000
		Terminating SDP
		v=0
		o=BroadWks 13 0 IN IP4 192.168.8.41
		s=SIP Call
		c=IN IP4 0.0.0.0
		t=0 0
		m=audio 5000 RTP/AVP 0

Origination	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190902.714Z CallIdentity SequenceNumber 359:1 SystemIdentity: DEFAULT	Calling Party Identifier: 5146972000 Called Party Identifier: 5146972004 User Input: 2004

LI Event	Common Attributes	Specific Attributes

CCOpen	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20020423190905.798Z
	CallIdentity
	SequenceNumber 359:1
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975002
		SepRecvCCC +15146975003
		Originating SDP
		v=0
		o=Vega50 39 1 IN IP4 192.168.13.2
		s=Sip Call
		c=IN IP4 192.168.13.2
		t=0 0
		m=audio 10054 RTP/AVP 0
		a=rtpmap:0 PCMU/8000
		Terminating SDP
		v=0
		o=CiscoSystemsSIP-IPPhone-UserAgent 4694 4121 IN IP4 192.168.8.244
		s=SIP Call
		c=IN IP4 192.168.8.244
		t=0 0
		m=audio 21358 RTP/AVP 0

Answer	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190905.798Z CallIdentity SequenceNumber 359:1 SystemIdentity: DEFAULT	Answering Party Identifier: 5146972004

CCChange	CaseIdentity: FBI1234
	IAPSystemIdentity: DEFAULT
	TimeStamp: 20020423190935.689Z
	CallIdentity
	SequenceNumber 359:0
	SystemIdentity: DEFAULT
		CCCIdentity
		SepCCCpair
		SepXmitCCC +15146975001
		SepRecvCCC +15146975000
		Originating SDP
		v=0
		o=Vega50 38 1 IN IP4 192.168.13.2
		s=Sip Call
		c=IN IP4 192.168.13.2
		t=0 0
		m=audio 10054 RTP/AVP 0
		a=rtpmap:0 PCMU/8000
		Terminating SDP
		v=0
		o=Vega50 42 1 IN IP4 192.168.12.6
		s=Sip Call
		c=IN IP4 192.168.12.6
		t=0 0
		m=audio 11024 RTP/AVP 0
		a=rtpmap:0 PCMU/8000

CCChange	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190935.689Z CallIdentity SequenceNumber 359:1 SystemIdentity: DEFAULT	CCCIdentity SepCCCpair SepXmitCCC +15146975001 SepRecvCCC +15146975000 Originating SDP UNKNOWN Terminating SDP UNKNOWN
Connection	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190935.689Z CallIdentity SequenceNumber 359:0 SystemIdentity: DEFAULT	ConnectedParties: 5146972000
Connection	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190935.689Z CallIdentity SequenceNumber 359:0 SystemIdentity: DEFAULT	ConnectedParties: 5146972000 5146972004

LI Event	Common Attributes	Specific Attributes
Connection	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190935.689Z CallIdentity SequenceNumber 359:0 SystemIdentity: DEFAULT	ConnectedParties: 5146972000 5146972004 5146973000
Connection Break	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190935.689Z CallIdentity SequenceNumber 359:1 SystemIdentity: DEFAULT	Remaining Parties: <empty>
CCClose	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190956.912Z	CCCIdentity SepCCCpair SepXmitCCC +15146975001 SepRecvCCC +15146975000
CCClose	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190956.922Z	CCCIdentity SepCCCpair SepXmitCCC +15146975002 SepRecvCCC +15146975003
Release	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190956.922Z CallIdentity SequenceNumber 359:0 SystemIdentity: DEFAULT	
Release	CaseIdentity: FBI1234 IAPSystemIdentity: DEFAULT TimeStamp: 20020423190956.922Z CallIdentity SequenceNumber 359:1 SystemIdentity: DEFAULT	