

# SIP Private Networking

## DESCRIPTION



## NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

## TRADEMARKS

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at [legal@mitel.com](mailto:legal@mitel.com) for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

© Copyright 2019, Mitel Networks Corporation

All rights reserved

## 1

## GENERAL

This document gives an overview of the handling of network services data for SIP tie-lines, i.e. private network services. The services are used for trunks and for attendants (the Mitel InAttend client).

There is a separate description for the ISDN, H.323 and DPNSS private network services, see “ISDN, H.323 and DPNSS Networking”.

Detailed descriptions can be found in the descriptions and operational directions for each one of the command groups. The command groups mentioned in this document are *AS*, *EX*, *extension*, *ip\_extension*, *KS*, *RO*, and *sip\_route*.

**Note:** To use the network services described in this document, the add-on feature Network Services is required.

In a private SIP network, it is possible to execute various supplementary services. The supplementary services described in this document are for:

**IETF RFCs**

- basic calls, including early media (RFC 3261, 3960)
- call completion/callback, on busy/not-available, and on no reply (RFC 6910)
- call forwarding, including bypass (RFC 4244, 5806)
- calling line identity presentation/CLIR and COLP/COLR (RFC 3323, 3325, 3966)
- call intrusion (RFC 3911, 5850)
- call offer/waiting (RFC 2976, 3261)
- call transfer (RFC 3891, 3892)
- DTMF signalling (RFC 4377)
- hold/parking/retrieve (RFC 3261)
- keep-alive mechanism, supervision (RFC 4028)
- name identity (RFC 3261)

**Proprietary**

- call diversion/re-direction, backward notification
- customer identity
- deflection/single step transfer
- dialled number information service, DNIS
- forced release of third party from intrusion
- message waiting indication
- repeated individual diversion
- rerouting
- voice mail type information

For the SIP tie-line, all services are supported both for mixed, closed (coordinated number plan), and open numbering plans (uniform numbering plan), by using Type Of Number (TON) information. For information about numbering plans, see the operational directions for *Numbering*.

Some SIP signaling protocol options are selected by means of the VARI and VARO parameters in command *RODAI*.

SIP routes used as public trunks are not in the scope of this document. SIP tie-line routes support the services listed above.

**Note:** Advice of charge, malicious call tracing and path replacement/route optimization are not supported by the SIP trunk. The network services are not supported in mixed networks (interworking, gateway scenarios) with ISDN, DPNSS or H.323, although certain Diversion and History data can be conveyed also in inter-working cases.

## 1.1

## LICENSES FOR SIP NETWORKING

The SIP trunk functionality requires different licenses depending on the wanted level of services. There is one license for public SIP trunk, another license for a basic SIP tie-line (only basic call services), and a third premium license for a full service SIP tie-line (adding for example Callback, Forwarding, Intrusion, Call offer, and Message waiting).

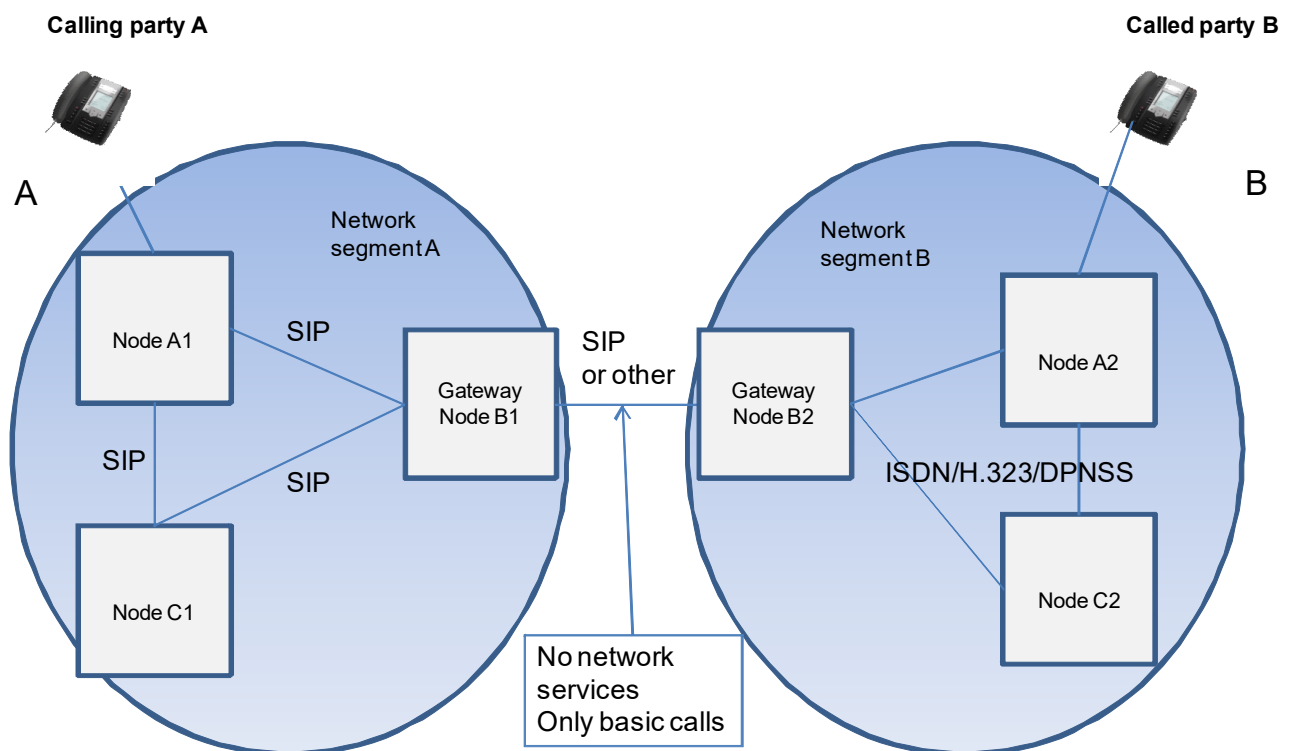
## 1.2

## PRIVATE NETWORK CONFIGURATIONS

To use network services between the parties within a private network, the network must be homogeneous. That is, the connections between the exchanges use the same signaling system, either SIP, or DPNSS, or ISDN/H.323. The reason for this is that network services are not supported in a DPNSS - ISDN/H.323 gateway, nor in ISDN/H.323 - SIP gateway or DPNSS - SIP gateway.

The connections between the exchanges using ISDN/H.323 mixed with SIP signaling systems are NOT considered as an homogeneous network, so network services are generally not supported.

In the figure below, the A-party cannot invoke any network services against the B-party as the path contains a gateway PBX.



**Figure 1: Gateway blocks network services**

The signaling systems connecting two different network segments **must be initiated not to support** network services. This is done by setting the SIG parameter in the command *ROCAI* to no net service facilities.

### 1.2.1 SIP USING IETF RFC PROTOCOLS

A SIP (private) network using the SIP protocol according to IETF RFCs supports network services via transit exchanges.

### 1.2.2 SIP USING PROPRIETARY PROTOCOLS

A SIP (private) network using proprietary additions to the SIP protocol does not support network services via transit exchanges.

### 1.2.3 PRIVATE SIPNETWORK BASED ON STANDARDIZED IETF RFCS

Some of the services supported by the SIP networks are based on the Standardized RFCs produced by IETF. These services are not supported in mixed SIP - ISDN/H.323/DPNSS networks. The following services are based on standardized RFCs.

- Call completion (Callback)
- Call forwarding (also has proprietary additions)
- Call offer
- Call intrusion
- Call transfer

Call offer has the same functionality as Call waiting has in an ASB 501 04 network. Call offer is set per destination.

#### 1.2.4

### PRIVATE SIP NETWORK BASED ON PROPRIETARY PROTOCOLS

Some of the services supported by the SIP networks are based on proprietary protocols (additions to SIP RFCs). These services are not supported in mixed SIP - ISDN/H.323/DPNSS networks.

The following services use proprietary protocol additions:

- Call forwarding/deflect/rerouting notifications backwards
- Call Rerouting
- Customer identity
- DNIS number
- Forced release of third party from intrusion
- Message Waiting indication (for centralized Voice Mail)
- Voice mail type conveyed (for centralized Voice Mail)

#### 1.2.5

### PUBLIC SIP NETWORK

There are a number of services that are supported for public SIP trunks. These are however not described in this document, since no private networking is involved, but for example the following are supported:

- calling/connected line identity
- calling/connected name identity
- diversion/call forwarding (partially)

See Operation & Maintenance/IP Networking for details.

## 1.3

## LIMITATIONS

#### 1.3.1

### GENERAL

- Network services are generally not supported together with Least Cost Routing. There is only one situation where network services are available for a call which has been set up using LCR, namely when the LCR call has been routed entirely in the private network (a private destination is in the ENT table that is, off net to on net routing). The services Repeated Individual Diversion, Personal number, External follow me, Advice Of Charge and Original A-number are supported also when LCR has been executed.
- To be able to optimize the service level of the network, it is advisable that the alternative routes for a destination are initiated in a decreasing network support order that is, the external lines that support network services should be the first choices. The external lines that do not support network services, should be the last choices.
- Network services are **not** supported in DPNSS - SIP or ISDN - SIP or H.323 - SIP gateway situations.

- Number conversion is not recommended to use together with network services. It may work in some configurations, and for some services, but not all.

### 1.3.2

### COMPARED TO ISDN/H.323 AND DPNSS

- Path Replacement service is not supported. The Path Replacement information received from ISDN/H.323/DPNSS networks is not transferred through the SIP tie-lines.
- Centralized answer position functions (Status Notification and certain Rerouting functionality) are not supported by the SIP tie-line.
- Advice of Charge service is not supported. The Advice of Charge information possibly received from the public ISDN network is not transferred through the SIP tie-lines.
- Malicious Call Tracing service is not supported by the SIP trunk.

## 1.4

## INTERWORKING WITH ASB 501 04

The ASB 501 04 does not support SIP trunks, so there is no interworking. Other signaling systems, like ISDN, H.323 or DPNSS would have to be used.

## 1.5

## INTERWORKING CONSIDERATIONS IN SIP NETWORKS

### 1.5.1

### INTERWORKING IN HOMOGENEOUS SIP NETWORKS

In homogeneous MX-ONE SIP networks between different MX-ONE systems of the same release, the services based on proprietary protocol additions, and the services based on the standard IETF RFCs should all work.

In homogeneous MX-ONE SIP networks between different MX-ONE systems of different release versions, the service level will/may be restricted to the level supported by the oldest system release. Preferably all systems in the network should run the same version of SIP trunk.

### 1.5.2

### INTERWORKING WITH THIRD PARTY SYSTEMS IN 'HETEROGENEOUS' SIP NETWORKS

Services based on standard IETF RFCs are or may be supported in heterogeneous SIP networks, when one end node where the services are executed is an MX-ONE, and another end node is a third party application or system. Examples are Microsoft Lync, MiCollab Advanced Messaging Voice Mail, and the Mitel InAttend application.

In any other case (where proprietary protocols are used) the services are usually not supported in heterogeneous SIP networks.

A certain amount of transparency for non-standard SIP headers is achieved through MX-ONE by specifying in SIP trunk profiles; where SIP headers transparently transfer information between a-side and b-side.

## 1.5.3

## INTERWORKING WITH OTHER SIGNALING SYSTEMS

No gateway functionality for the network services is implemented to DPNSS, ISDN, ISDN-VPN or H.323 signaling systems. Basic calls will work, and also some History and Diversion information can be forwarded, but services will generally not be supported.

## 1.6

## GLOSSARY

For a complete list of abbreviations and glossary, see the description for *ACRONYMS, ABBREVIATIONS AND GLOSSARY*.

**Originating Node (MX-ONE, or PBX)**

The exchange where the party that initiates the call is located. If the call is an incoming external call, the originating exchange is where the call enters the CCS network.

**Gateway Node**

A gateway exchange is an exchange where the incoming and outgoing signaling systems are not the same for example, ISDN to DPNSS, ISDN to SIP, or vice versa.

A node with incoming signaling system defined as Public ISDN and an outgoing signaling system defined as Private ISDN or vice versa is also considered as a gateway node. Ditto for Public and Private SIP.

**Transit Node**

An exchange which a call just passes through, and where the incoming and outgoing signaling systems are the same and have the same characteristics that is, both sides are programmed as tie line or public.

**Terminating Node**

The exchange where the called party is located.

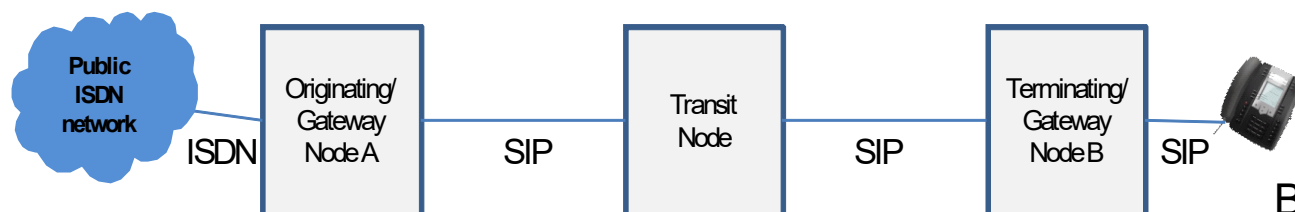


Figure 2: Types of nodes



## 2

## PREREQUISITES

The number series for the following must be initiated:

- Extension numbers, number analysis-command
- PBX operator numbers, number analysis-command
- Route access codes, number analysis-command
- Own exchange number, number analysis-command

Other general prerequisites are:

- For SIP it is required that the destination is in another MX-ONE or a third party system/application that supports standard SIP RFCs.
- Number Prefixes may have to be set, depending on numbering plan (RO-commands), see the operational directions for *NUMBERING*.
- Name on route can be initiated by use of the command *name - i*.

## 3 USER SERVICES

### 3.1 BASIC CALLS

Basic voice and video calls are supported in a private SIP network using standard RFC signaling. Early media handling (in order to facilitate for example voice announcements in queueing or other non-active call states) is also supported.

Interworking with other trunk signaling systems is supported.

See description *IP networking* and operational directions for *sip\_route* for further details.

### 3.2 CALL COMPLETION/CALLBACK

The Call Back features offer a user who meets busy or no answer the possibility of having the call completed automatically when the called party becomes free or at no answer that is, there are two types of Call Back services available:

- Call Back when free (CBWF), which includes not-available and busy cases.
- Call Back at no answer (CBNA), which includes alerting cases.

The called party may be located in another PBX (within a private network). Call back is supported in a homogeneous SIP network. To allow Call Back in a network, the called party must be an extension. Call Back can be invoked from an extension or a PBX operator.

Interworking with other trunk signaling systems in gateway cases is not supported.

No specific I/O data settings are required for Call back, except that network services must be supported on the SIP tie-line.

There are a number of application system parameters used for Call back, to select timer lengths. These timers are usually valid for both internal and network call back.

### 3.3 CALLING/CONNECTED LINE IDENTITY PRESENTATION/RESTRICTION

Numbers and presentation restriction information (CLIP, CLIR, COLP, COLR) are supported, as part of basic calls and of services, in a network consisting of SIP tie-lines.

Interworking with other trunk signaling systems is supported.

### 3.4 CALL DIVERSION

#### 3.4.1 GENERAL

Network diversion services make it possible for a user to have voice calls forwarded for various reasons, to an answering position within the private network. Network diversion is possible in SIP networks consisting of SIP tie-lines (similar to ISDN/H.323/DPNSS tie-lines or ISDN public external lines (for VPN)).

**Note:** Activation/deactivation of Follow-me (\*21\*number#) and other diversion procedures via SIP network are not supported.

The Diversion services described in this document are as follows:

- bypass of diversion (and of deflect and DND)
- direct diversion
- diversion on busy
- diversion on no answer
- follow me
- external follow me

The diverted-to position can be an extension, an ACD group, an internal group hunting group, an individual PBX operator or a PBX operator group.

### 3.4.2

## NETWORK CONFIGURATIONS AND A BASIC TRAFFIC CONCEPT

The figure below shows a possible SIP network configuration, where all parties involved are located in different PBXes, but of course, the parties can be located in different PBXes, in any combination. If all parties are located in the same PBX, then it is the internal diversion case.

The diversion information (reason, diverted's number, name, and URI) is sent in the forward direction, but diversion information can also be sent in notifications backwards, partly as proprietary data.

### **Originating MX-ONE**

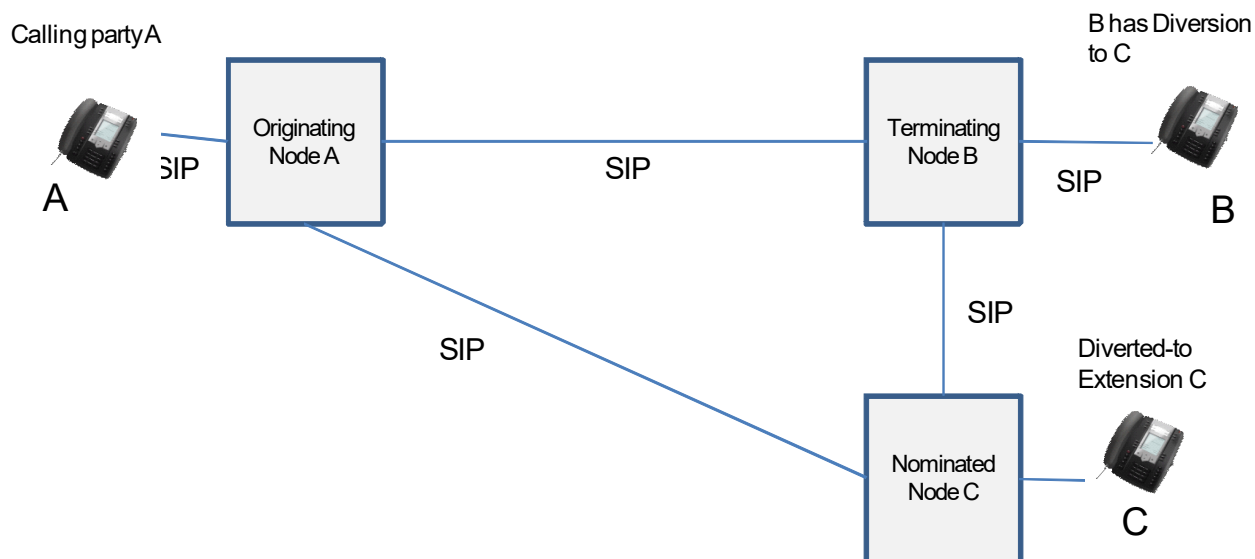
The exchange from where the call originates. The A-party can be an internal party or an external party calling from a network that does not support Diversion service, a non-SIP network. Thus the signaling system changes, so the originating node is also a gateway exchange.

### **Terminating MX-ONE**

The exchange where the called party is located, and where the diversion is initiated.

### **Nominated MX-ONE**

The exchange where the diverted-to party is located.



**Figure 3: Diversion**

Extension A in the originating node calls extension B in the terminating node. Extension B has activated diversion (any of busy, direct, follow me, or no answer diversion) to extension C in the nominated node. After extension A has called extension B, diversion will take place in the terminating exchange.

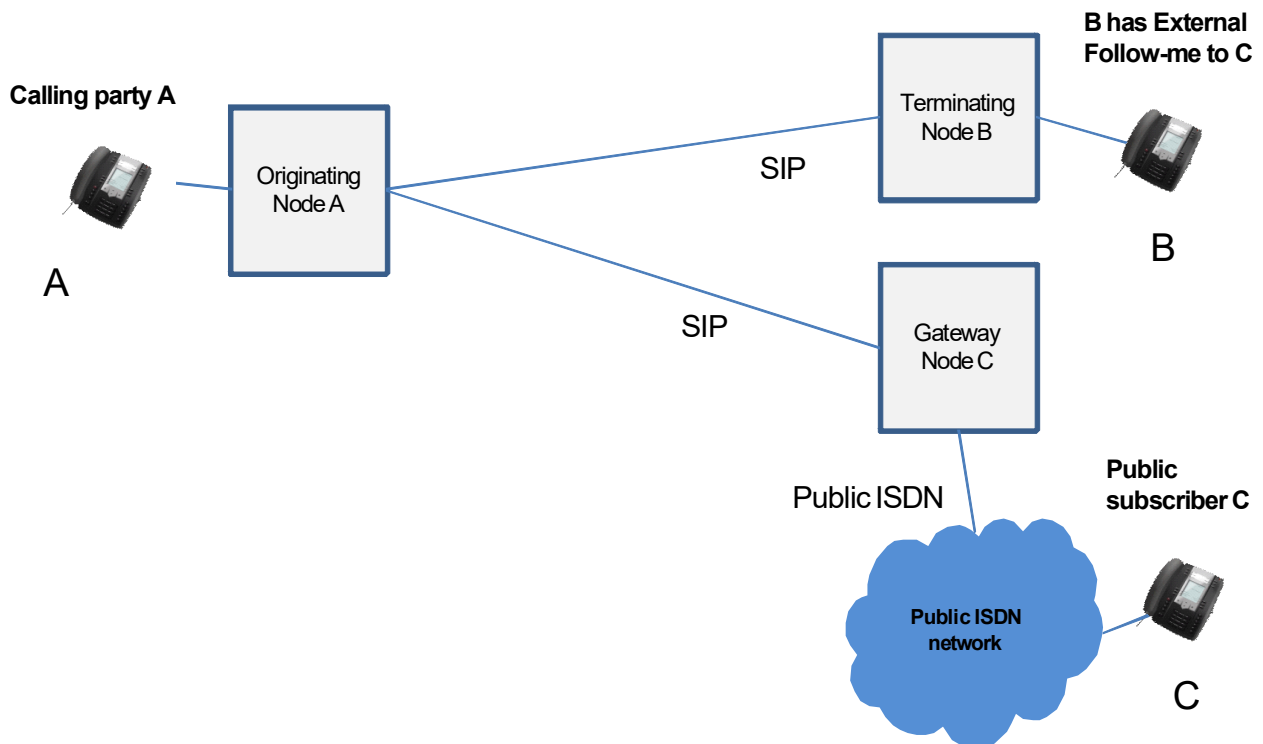
### 3.4.3

### EXTERNAL FOLLOW ME

External follow me is carried out as forward switching and signaled forward and backward in the private network.

## 3.4.3.1

## External follow me



**Figure 4: External follow me. The media path will be A-C, but the control signaling path will be A-B-C (from B via node A to node C)**

The company uses the private network to access the public network from Node-A. Data for the destinations to the public network in Node-A, Node-B and Node-C are set to not support services, and diverted party's (B-party's) number shall be sent as A-number at External follow me.

Extension A calls extension B in Node-B. Extension B has External follow me to a public subscriber C. The call is forwarded over the SIP network via Node-C to the public network. The B-party's information is sent as A-party information from Node-B to Node-C and the public network.

It is possible to use External follow me in conjunction with the Original A-number feature. This is done when it is desired to show calling party's (A-party's) number to the diverted-to public subscriber (C-party), see operational directions for *ORIGINAL A-NUMBER*.

## 3.5

## CALL OFFER/WAITING

## 3.5.1

## GENERAL

An extension who dials another extension number and receives busy message can invoke Call Offer/Waiting on the busy extension.

Call offer is supported in networks consisting of SIP tie-lines (in addition to networks using ISDN, H.323 or DPNSS tie-lines).

There is a COS (in the EX/GE/KS commands) which allows or denies the initiation of the Call Offer/Waiting request from the originating party (A party). The called (B) party

has a COS which allows or denies the acceptance of Call Offer/Waiting against it. The COS of party (C), who is connected to the busy (B) party, is not checked. When a PBX operator extends a call to a busy extension, if the checking of the COS has passed, then the system will generate a Call Offer/Waiting indication automatically.

An extension calling a busy extension, can order the system to send a Call Offer/Waiting tone to an analog extension or ringing signal to a digital extension. In addition to the COS for the busy extension (B), also an AS parameter, *PARNUM* = 35 controls if the Call Offer/Waiting shall be permitted.

If the incoming external line uses CCS, and the external originator is an extension or PBX operator, the COS of the incoming route does not matter. Automatic Call Offer/Waiting will not be executed.

No other specific I/O data are required for Call Offer, except that network services must be supported. If network services are not supported, and if calling party is a PBX operator, the Call offer request will be discarded, and the call will proceed as basic call.

## 3.6 CALL TRANSFER

### 3.6.1 GENERAL

Call transfer makes it possible for a user to connect the active calling or speaking party with a party that is on hold. The requesting user is then released from the speech connection.

The transfer can be made before (in alerting/queueing state) or after answer.

### 3.6.2 PREREQUISITES

The SIP route must be set with the following data:

- Network services must be set to **Yes**, set in the SIP trunk profile.

The following parameters can be altered for Call Transfer:

- With an AS parameter, *PARNUM* = 12 stating Maximum time before answer on recall due to unauthorized transfer before answer. Default value is 10 s.
- With an AS parameter, *PARNUM* = 67 stating Category check on transfer of outgoing external call.
- Parameter TBA in SY commands is set to allow transfer before answer.

### 3.6.3 EXECUTION

The procedure for Call transfer is the same as for Transfer, see directions for use for the extension.

## 3.7 CUSTOMER IDENTITY

Conveying of Customer Identity is supported in a network consisting of SIP tie-lines. The identity is proprietary data in the basic call signaling, sent in the forward direction only.

## 3.8 DEFLECTION/SINGLE STEP TRANSFER

### 3.8.1 GENERAL

Computer Supported Telecommunications Applications, CSTA is implemented in MX-ONE by using an Ethernet connection to the MX-ONE for supporting a CTI protocol between a computing domain and the telephony domain. This logical interface is used between the MX-ONE and a PC which functions as a protocol converter. For more information about CSTA see operational directions for *COMPUTER SUPPORTED TELECOMMUNICATIONS APPLICATIONS (CSTA)*, *CS and CSTA SERVER, PHASE III*.

One of the CSTA services for monitored devices is Deflection/Single Step Transfer.

Network deflection/single step transfer (SST) service makes it possible to move a call to another destination within the private network. Network deflection/SST is supported in networks consisting of SIP tie-lines.

The deflect-to position can be an extension (DTS, analog extension, CAS extension, remote extension or IP extension), a CTI/ACD group, a group hunting group, an individual PBX operator or a PBX operator group.

The deflect information (reason, deflected's number, name, and URI) is sent in the forward direction, but "diverted" information can also be sent in notifications backwards, partly as proprietary data.

### 3.8.2 NETWORK CONFIGURATIONS AND A BASIC TRAFFIC CONCEPT

The figure 5 shows a possible SIP network configuration, where all parties involved are located in different nodes. For SST, either the A-party or B-party can be the deflecting-party, making the other one the deflected-party. For deflect, only B-party can be the deflecting-party, making A-party the deflected-party.

#### **Originating MX-ONE**

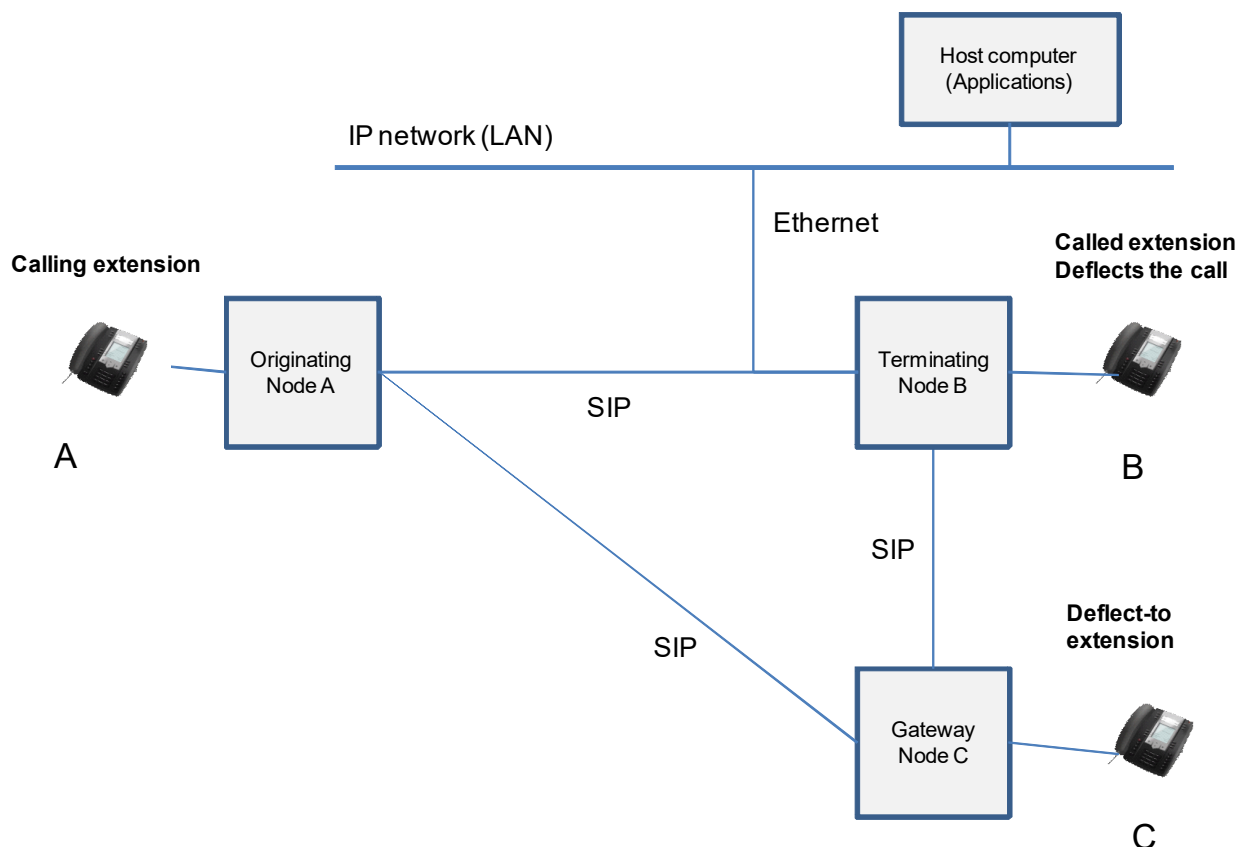
The exchange from where the call originates. A-party can be an internal party or an external party calling from a network that does not support network services, a non-CCS network. Thus the signaling system changes, so the originating node is also a gateway exchange.

#### **Terminating MX-ONE**

The exchange where the called party is located. The Deflect is requested in the Terminating node, for the called party.

#### **Deflect-to MX-ONE**

The exchange where the deflect-to party is located.



**Figure 5: Deflection/SST**

Extension A in the originating node calls extension B in the terminating node. Extension B rings. Extension B deflects the call to extension C in the deflect-to node.

The terminating exchange executes a deflect call setup, i.e. does a forward switching to the deflect-to exchange C, and sends the identity of extension C to the originating exchange. Thus the control signaling path will be via node B, but the media path (after extension C has answered) can be direct between extensions A and C (if both are SIP terminals).

The result of the call setup is sent from the deflect-to exchange to the terminating exchange.

When the terminating exchange receives successful result for the deflect call setup, terminating exchange will release (stop ringing) extension B.

**Note:** A difference from ISDN/H.323's functionality is that the SIP tie-line always does a forward-switching, and does not convey specific Deflect information, so interactions with other services will differ compared to an ISDN/H.323 network.

### 3.9

## DNIS, DIALED NUMBER INFORMATION SERVICE

DNIS number (used in call centers for special routing purposes) is supported in a SIP tie-line network. The DNIS number can be conveyed in the forward direction as proprietary data.



## 3.10 DTMF SIGNALING

DTMF signaling is supported in a SIP tie-line network.

## 3.11 HOLD, PARKING

Hold/parking is supported in a SIP tie-line network. In the trunk profile, a parameter is being controlled if hold or parking is used.

If "TrunkProfile:XXX: TrunkParkingUsed: no" is configured, the other party in the call will not be affected.

If "TrunkProfile:XXX: TrunkParkingUsed: yes" is used, the other party in the call will be parked and will receive a continuous message depending on setting of parameter TrunkProfile:XXX: TrunkParkingContinuousMessage.

If the data is set to "0", the default market message setting is used by the other side. If the setting is not "0", the value in the parameter is used to send corresponding continuous message to the other side.

See the *Recorded Voice Announcement - Operational Directions* guide.

## 3.12 INTRUSION AND FORCED RELEASE

### 3.12.1 GENERAL

During reception of busy tone a user with suitable COS can invoke intrusion towards the called busy party. In fact three or more different nodes can be involved in the intrusion, that is:

- Originating MX-ONE where the intruding party is located.
- Terminating MX-ONE where the intruded party is located.
- Third party exchange where the third party is located (This exchange can of course be the same as Terminating or Originating node)

Intrusion (and forced release) is supported in networks consisting of private homogeneous SIP tie-lines. No interworking with ISDN, H.323 or DPNSS is supported.

### 3.12.2 SETTINGS FOR INTRUSION IN A SIP NETWORK

For network Intrusion, network services must be supported, and there are several AS parameters which must be correctly set. Interworking with ASB 501 04 is not possible (since SIP is not supported there).

The Intrusion Capability Level (ICL) for the intruding party is set as part of the extension service profiles. The ICL is sent to the terminating node for comparison with the IPL. PBX operator always has highest ICL by default. Set the ICL and IPL per extension with the commands:

***extension\_profile -i --ext-serv or KSEXI, EXTEI:....;SERV=....;***

The Intrusion Protection Level (IPL) for the intruded party is set in the extension service profiles. The Intrusion Protection Level for the third party is set by the extension service profile. The PBX operator is totally barred, that is, has highest IPL.

To fetch the IPL for the third party is not supported with SIP tie-line, so the IPL is given with an AS parameter, *PARNUM* = 130 in the terminating node.

If Node-C is an ASB 501 04 R2 then IPL is set with an AS parameter, *PARNUM* = 130.

Forced release is only available if an AS parameter, *PARNUM* = 57 allows. Key command:

**ASPAC:PARNUM=57,PARVAL=...;**

The following AS-values are used for network Intrusion:

**PARNUM=26**, Permission for incoming DID calls to automatically initiate Intrusion or Call Offer/Waiting.

**PARNUM=35**, Permission for an extension to initiate Intrusion on a busy analog extension, which has an IPL that allows Intrusion.

**PARNUM=36**, Permission to intrude on a party connected to a public trunk.

**PARNUM=57**, Forced release allowed or not.

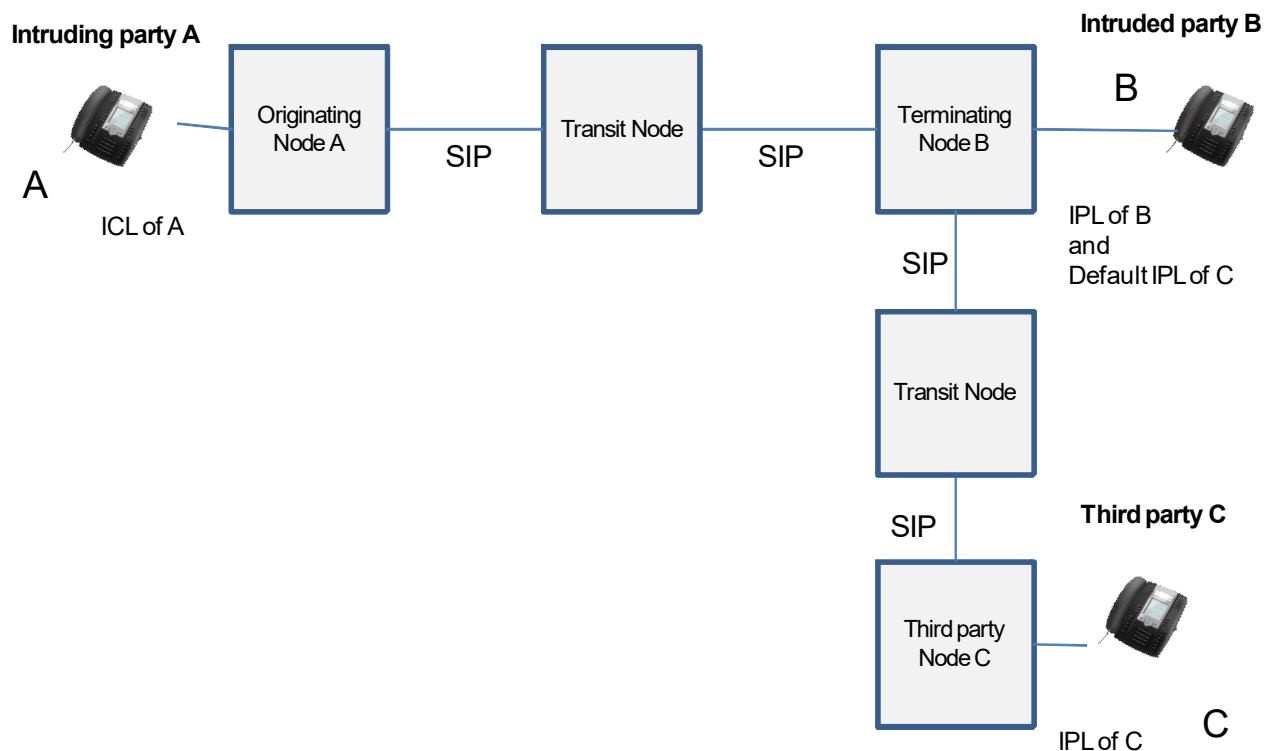
**PARNUM=130**, Default IPL value, used if the real IPL cannot be fetched.

The following comparison rules apply for IPL and ICL:

ICL INTRUDING	IPL INTRUDED/ THIRD	INTRUSION
3	3	=> not allowed
3	0-2	=> allowed
2	2-3	=> not allowed
2	0-1	=> allowed
1	1-3	=> not allowed
1	0	=> allowed
0	0-3	=> not allowed

#### Example of initiation in the figure below

Since the real IPL cannot be fetched from Third party Node-C, the default IPL value in Node-B will be used as Third party's IPL value.



**Figure 6: Intrusion**

### 3.13 MESSAGE WAITING/CENTRALIZED VOICE MAIL

Message Waiting Indication can be conveyed in a private SIP network using proprietary signaling.

The SIP tie-line can also convey “Voice Mail” as proprietary type of party, in order to facilitate automatic DTMF mode when connected to voice mail.

See also operational directions for *VOICE MAIL*, *VM* for further details.

### 3.14 NAME IDENTIFICATION

Name Identification can be conveyed in a private SIP network using standard RFC signaling.

See operational directions for *NAME IDENTITY*, *NI* for further details.

### 3.15 REPEATED INDIVIDUAL DIVERSION/PERSONAL NUMBER

#### 3.15.1 GENERAL

The Repeated Individual Diversion (RID) service is designed to provide the user with a set of several lists, each one containing up to 10 possible answering positions. When the user, with this service activated, receives a call, that call is repeatedly deflected to

the answering positions defined in the active list until the service is considered to be finished (for example, answer for called position).

The answering positions can be in the private or public network, but only SIP in a homogeneous network configuration is able to handle the RID deflection service (i.e. there is no interworking with ISDN or H.323 even if those protocols support the RID service).

The service can be initiated in the system using call\_list (Personal Number) commands.

The deflect information (reason, deflected's number, name, and URI) is sent in the forward direction, but "diverted" information can also be sent in notifications backwards, partly as proprietary data.

### 3.15.2

## NETWORK CONFIGURATIONS AND A BASIC TRAFFIC CONCEPT

The following figure (see figure 7) shows a possible SIP network configuration, where all parties involved are located in different MX-ONE systems, but of course, the parties can be located in different nodes, in any combination. If all parties are located in the same node, then it is the internal RID deflection case.

### Originating/Gateway MX-ONE

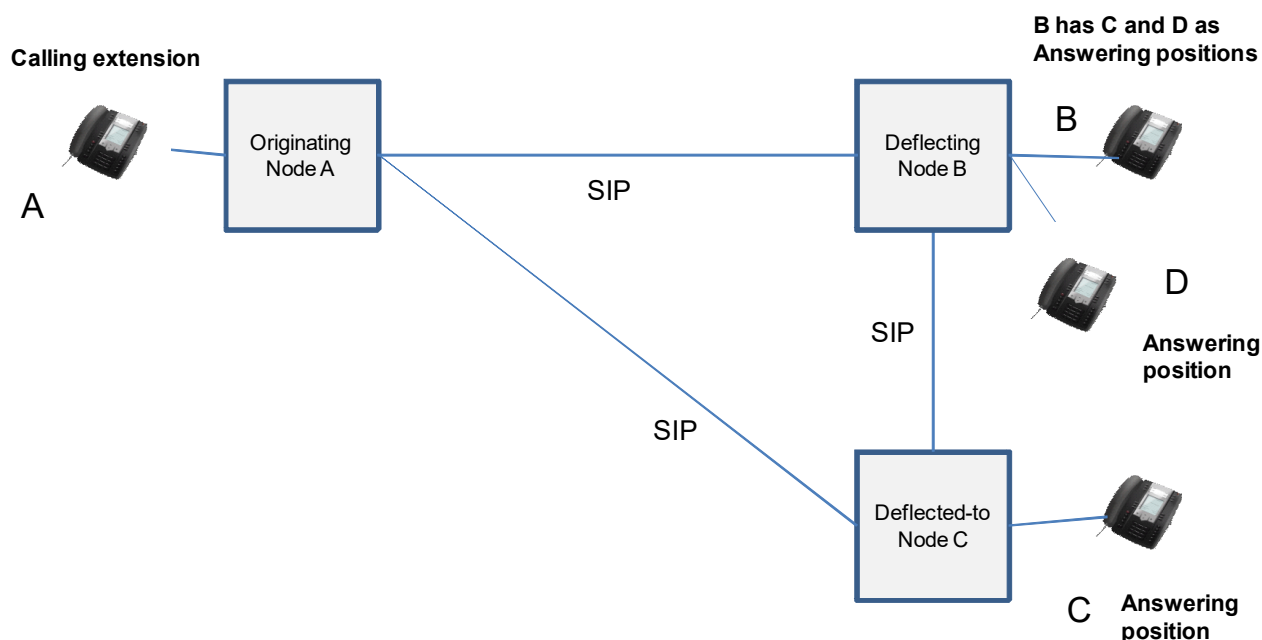
The exchange from where the call originates. A-party can be an internal party or an external party calling from a network that does not support the RID service, a non-ISDN network. Thus the signaling system changes, so the originating node is also a gateway exchange.

### Deflecting MX-ONE

The exchange where called party is located, and where the RID deflection is initiated.

### Deflected-to MX-ONE

The exchange where the answering position is located.



**Figure 7: RID deflection**

Extension A in the originating node calls extension B in the terminating node. Extension B has C as first answering position in the deflected-to node. The RID deflection execu-

tion starts in the Deflecting exchange. The deflecting exchange continues by making a call setup to the C-party by forward-switching to the deflected-to exchange.

**Note:** The ISDN/H.323 principle of returning to the originating/gateway node for a new call set up from the originating/gateway node after every deflection has occurred in the deflecting exchange is not followed by the SIP tie-line.

The deflected-to exchange is not explicitly notified about the RID service, but receives the identity of the originally called B-party. If the C-party is free, the originating/gateway node sends the result to the deflecting node to notify that the first RID call setup has been successfully executed, and a supervision timer is started in the deflecting node (supervision timer defined for that answering position - time to answer).

If the supervision timer expires before the call is answered, the call towards the answering position C must be released. The deflecting node B decides if a new RID deflection shall be requested towards the next answering position programmed in the active list (if any).

The next answering position D is in the deflecting node. In this case, the originating node will be informed that the call has been re-directed (although not explicitly with RID deflect information) to a new free party (including the identity of the D- party). If the supervision timer also expires before this party answers the call, the originating node is also notified and the identity of the B-party is sent as connected party again.

A new RID deflection may be started and this process will continue until the RID service is finished (answer received, A-party clears, no more positions to call or any other reason to finish RID).

It is possible to use RID in conjunction with the Original A-number feature. This is done when it is desired to show calling party's (A-party's) number, if it exists, to the deflected-to public party subscriber (C-party), see operational directions for *ORIGINAL A-NUMBER*. The calling party can be either internal, private or public and the deflecting party can be situated in any node in the network.

### 3.15.3

### RID DEFLECTION TO EXTERNAL PARTY

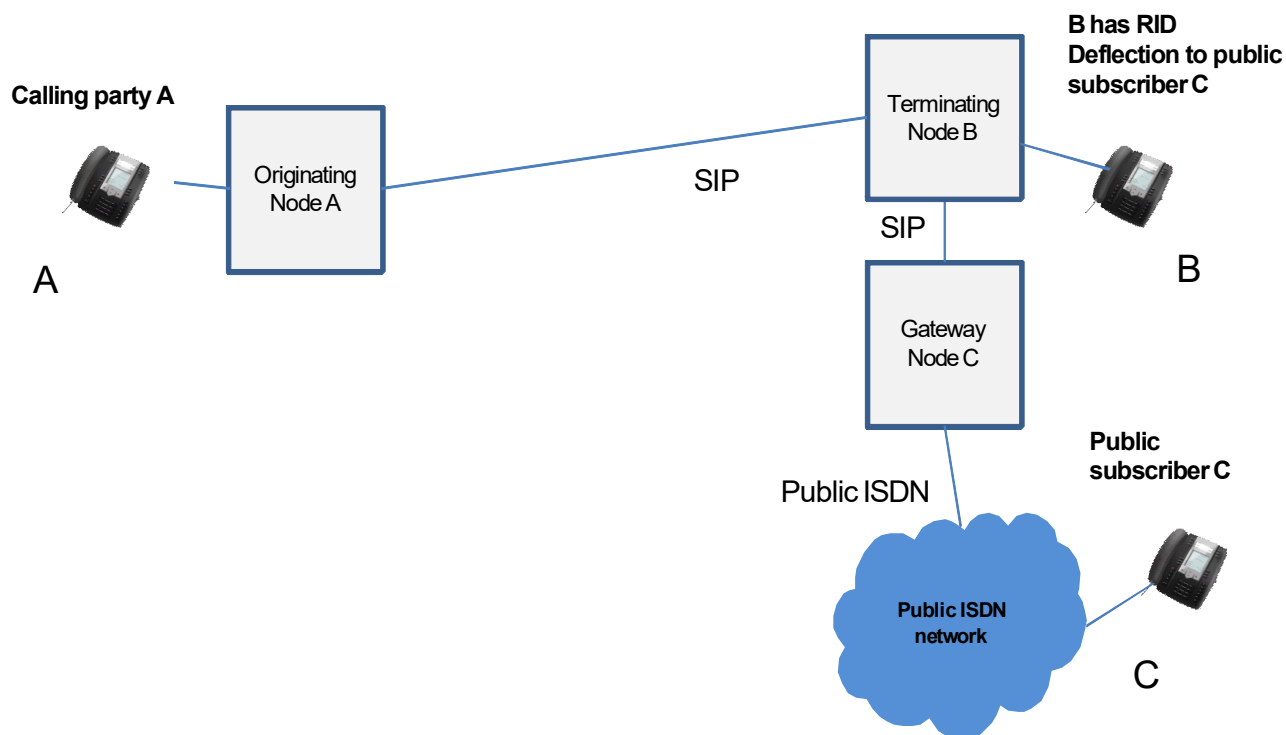
#### 3.15.3.1

#### *Prerequisites*

No specific RID prerequisites exist for SIP routes.

## 3.15.3.2

## RID to external party



**Figure 8: RID deflection to external party**

The company uses the private network to access the public network from Node-A. Data for the destinations to the public network in Node-A, Node-B and Node-C are set, and deflected party's (B-party's) number shall be sent as A-number at RID.

Extension A calls extension B in Node-B. Extension B has RID deflection to a public subscriber C. The call is forwarded over the SIP network via Node-C to the public network. The B-party's information is sent as A-party information from Node-B to Node-C and the public network.

It is possible to use RID deflection to a public subscriber in conjunction with the Original A-number feature. This is done when it is desired to show calling party's (A-party's) number to the deflected-to public subscriber (C-party), see operational directions for *ORIGINAL A-NUMBER*.

## 3.16

## REROUTING

Rerouting can be supported in a network consisting of SIP tie-lines (in addition to DPNSS, H.323 or ISDN networks). The SIP tie-line conveys rerouting service and reason information, but does not support Centralized answer position functionality (with status notification and new call setup from the centralized operator, as in ISDN, H.323 and DPNSS networks).

## 3.17

## SUPERVISION AND KEEP ALIVE FUNCTION

Supervision and Keep-alive functions are supported for SIP tie-lines.

## 3.18

## SECURITY

Security functions are supported according to RFCs, for SIP tie-lines, i.e. both signaling and media can be encrypted.

## 4

## TERMINATION

If exchange data have been altered, and no more commands are to be entered, then a dump to back-up media shall be done.