ISDN, H.323 and DPNSS Private Networking

DESCRIPTION

Mitel®

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.

1 GENERAL

This document gives an overview of the handling of network services data. Detailed descriptions can be found in the descriptions and operational directions for each one of the command groups. The command groups handled in this document are AS, EX, extension, ip_extension, KS, number (analysis), number_conversion, RI, RO, and SY.

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

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

ECMA

- advice of charge
- name identity

ETSI

- malicious call tracing (although it is a public network service)

ISO

- advice of charge
- call completion
- call forwarding
- call offer
- call transfer
- name identity
- path replacement
- path retention

Proprietary

- call back
- call diversion
- call offer
- customer identity
- deflection/single step transfer
- repeated individual diversion
- intrusion and forced release
- rerouting
- route optimization
- transfer

For ISDN and H.323, all services are supported both for mixed, closed (coordinated number plan), and open numbering plans (uniform numbering plan), by using ISDN Type Of Number (TON) information. For information about numbering plans, see the operational directions for *Numbering*.

The MX-ONE supports both ECMA and ISO ISDN signaling protocols. The required type of ISDN signaling protocol is selected by means of the VARI and VARO parameters in command *RODAI*.

Note: SIP trunk networking is described in a separate document, SIP Private Networking (67/1551-ANF 901 14 Uen).

1.1 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 DPNSS or ISDN/H.323. The reason for this is that network services are not supported in an DPNSS - ISDN/H.323 gateway.

Note: The H.323 trunk tunnels the ISDN QSIG protocol, i.e. it does not support H.450.x supplementary services.

The connections between the exchanges using ISDN and H.323 signaling systems are considered as an homogeneous network where network services are supported.

In figure 1 below, the A-party cannot invoke any network services against the B-party as the path contains a gateway PBX.

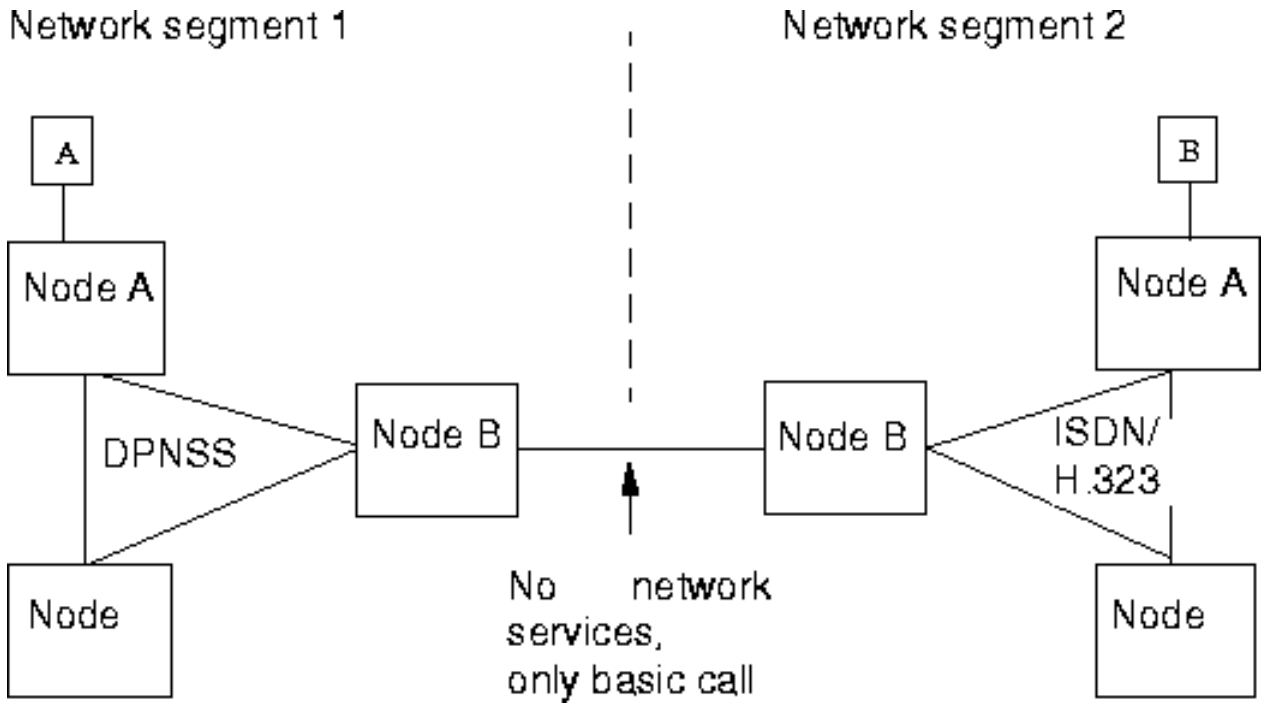


Figure 1: Gateway blocks network services

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. If the network is a DPNSS network, it is also necessary to set the VARC parameter in command *RODAI* to not support network diversion.

1.1.1 DPNSS/APNSS

APNSS is not supported by MX-ONE but the MX-ONE can be a part of a network that consists of both APNSS and DPNSS. The APNSS/DPNSS network has the same limitations as in ASB 501 04 R2/n.

A DPNSS network supports network services via transit exchanges.

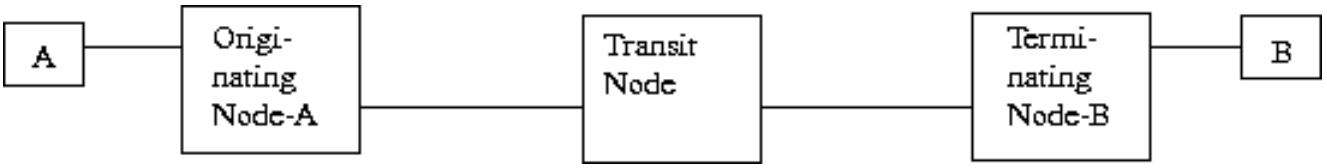


Figure 2: DPNSS

1.1.2 ISDN USING THE PROPRIETARY UUI PROTOCOL

An ISDN network using the proprietary UUI protocol supports network services via transit exchanges.

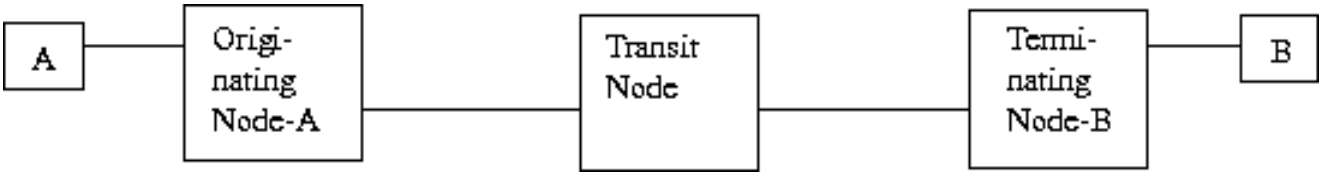


Figure 3: ISDN with UUI

1.1.3 H.323 USING THE PROPRIETARY UUI PROTOCOL

An H.323 network using the proprietary UUI protocol supports network services via transit exchanges by embedding the QSIG over H.323.

1.1.4 QSIG WITH EMBEDDED UUI IN THE GENERIC FUNCTIONAL PROTOCOL

QSIG with embedded UUI in the Generic Functional Protocol (GFP), that is, UUI tunneling, is a method that makes it possible to send UUI through a combined network where not the whole network supports UUI signaling. The combined network can consist of other MX-ONE or ASB 501 04 PBXs, non-Mitel PBXs and, for example, IP Gateways. Signaling according to the GFP has to be supported by the network. The method embeds the UUI-information in the Manufacturer Specific Information (MSI) field of the GFP.

The figure 4 below shows an ISDN network consisting of MX-ONE, or ASB 501 04/R6 or later, using UUI tunneling for network services via an intervening network.

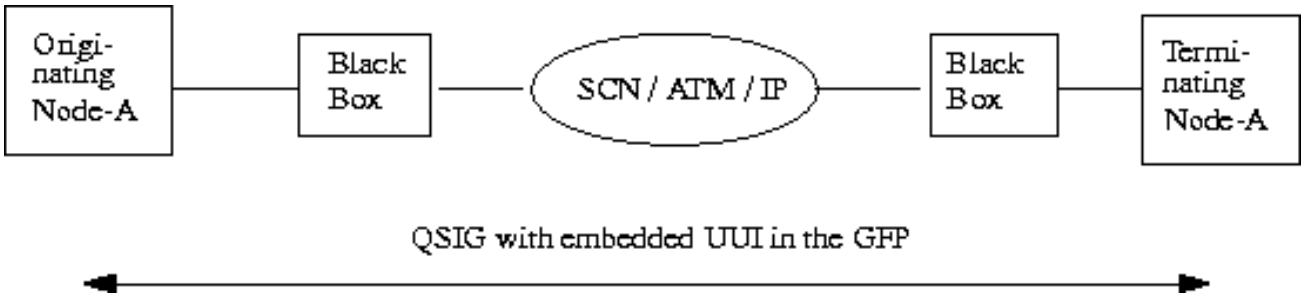


Figure 4: ISDN QSIG with GFP, intervening network

The figure 5 below shows a mixed network consisting of MX-ONE or ASB 501 04/R8 PBXs and non-Mitel PBXs. UUI-tunneling is used to signal network services between the MX-ONE or ASB 501 04/R8 PBXs.

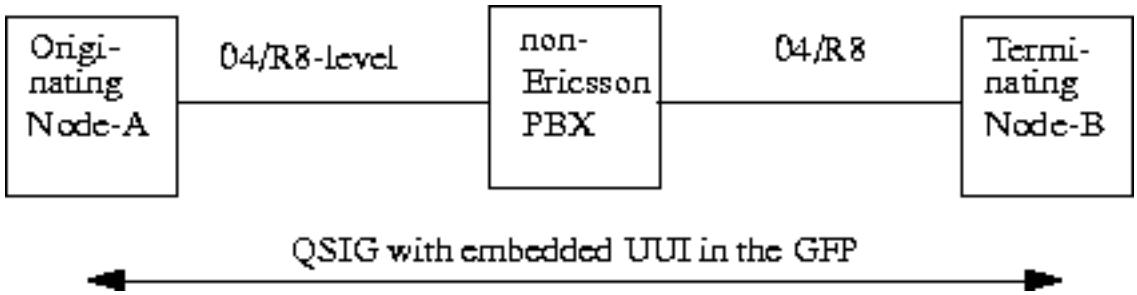


Figure 5: ISDN QSIG with GFP

1.1.5 VIRTUAL PRIVATE NETWORK

Virtual Private Network (VPN) is a method in the private exchange to establish private calls to another private exchange across a public network. MX-ONE or ASB 501 04 exchanges being parts in a VPN are connected through either a public transparent ISDN network, in case of ISDN signaling, or through a public transparent IP network, in case of H.323 signaling. If a call terminates in the public network, the call is not considered as VPN call. In this case, the call is treated as a normal public basic call.

In case of H.323, the network service information is conveyed through the IP network in a proprietary way, that is, the corresponding complete ISDN QSIG message with the service information is embedded inside the nonStandardControl Information Element (IE) of an H.323 message. Network services will be available as long as the public H.323 connections allow the conveyance of the nonStandardControl parameter (and therefore the QSIG UUI IE with proprietary information). This means that a kind of VPN over public IP network is implemented.

For private calls that use the VPN function, the service level is the same as for a private network using tie lines, except for the standard supplementary services Call completion, Call forwarding, Call transfer and Path replacement. These services are not supported in the VPN case. Instead, the type of network services must be set to Call back, Call diversion, Transfer and Route optimization. The network services can be used as in the private network, but the public network may impose some restrictions, for example, on the number of USER INFORMATION messages allowed to be sent and also the number of octets allowed in the UUI element.

Note: The Dynamic Route Allocation feature is no longer supported.

1.1.5.1 VPN and Intelligent Network Node

When an Intelligent Network (IN) node is available in the public ISDN network, the IN-node knows about the private numbering plan and it is possible to send a private number to the public network in the called party IE. The public network is then able to route the call based on the received private number. See parameter ADC, D_2 and D_{19} in the command *RODDI*.

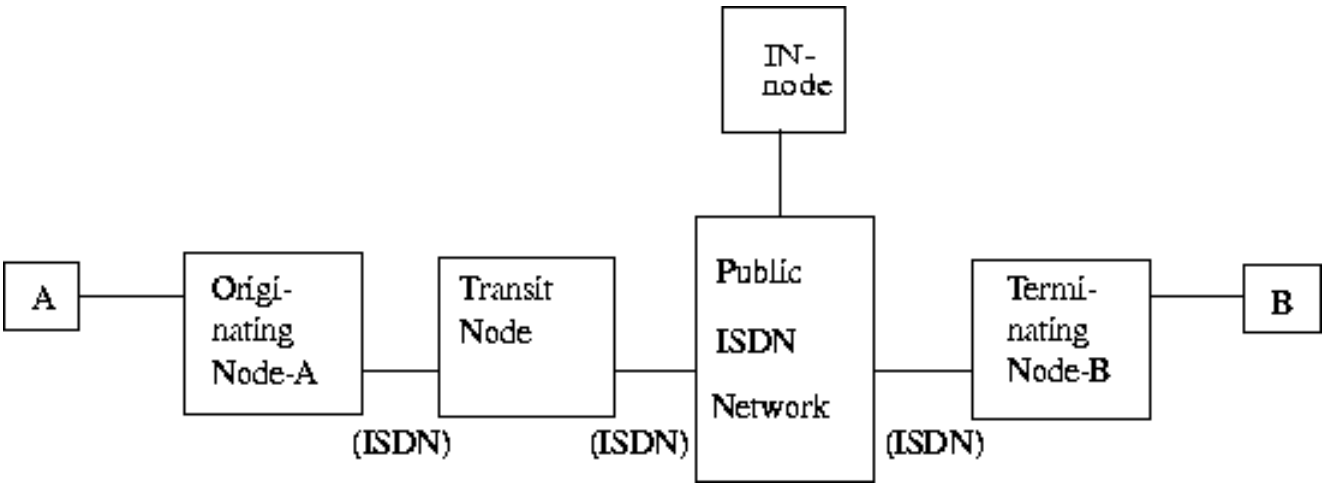


Figure 6: VPN with IN-Node

When a public network without an IN-node is used, the private network must always send the public number to the public network in the called party IE. See parameter ADC, D_2 and D_{19} in the command *RODDI*.

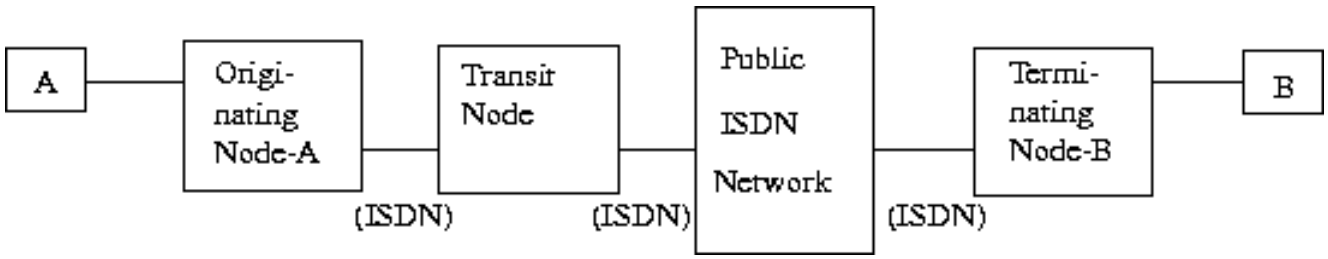


Figure 7: VPN without IN-Node

1.1.6 PRIVATE ISDN NETWORK USING STANDARDIZED GFP

All services mentioned in this document work in a private ISDN network. Some of them require a standardized GFP and will also work in a network with other vendors that support the same protocol. The following services require standardized GFP:

- Call completion
- Call forwarding
- Call offer
- Call transfer
- Path replacement

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

Call forwarding has the same functionality as Call diversion has in an ASB 501 04 network. Call forwarding is set per system with an AS parameter, *PARNUM = 223*.

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

Call transfer has the same functionality as Transfer has in an ASB 501 04 network. Call transfer is set per system with an AS parameter, *PARNUM = 223*.

Path replacement has the same functionality as Route optimization has in an ASB 501 04 network. Path replacement is set per system with an AS parameter, *PARNUM = 223*.

1.1.7 PRIVATE H.323 NETWORK BASED ON THE STANDARDIZED GENERIC FUNCTIONAL PROTOCOL

Some of the services supported by the H.323 networks are based on the Standardized Generic Functional Protocol. These services will also work in mixed ISDN/H.323 networks. The following services are based on the Standardized GFP.

- Call completion
- Call forwarding
- Call offer
- Call transfer
- Advice of charge

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

Call forwarding has the same functionality as Call diversion has in an ASB 501 04 network. Call forwarding is set per system with an AS parameter, *PARNUM = 223*.

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

Call transfer has the same functionality as Transfer has in an ASB 501 04 network. Call transfer is set per system with an AS parameter, *PARNUM = 223*.

Private H.323 routes need charging categories to allow request of Advice of Charge service. The Advice of Charge information received from the public ISDN network is transferred backwards through the H.323 private trunks.

1.1.8 PUBLIC ISDN NETWORK

There are a few services that can be requested towards the Public ISDN network. These are not described in this document, since no private networking is involved, but one is mentioned anyway:

- Malicious call tracing (identification)

Other services towards the public network not described here are for example:

- advice of charge
- calling/connected line identity
- calling party name or common company name for particular customer only for ISDN T1(Nortel DMS-100/250 protocol)
- request for User-to-User signaling

Both advice of charge and user-to-user signaling can be requested in different ways, both with generic functional protocol (GFP-based) and according to various national

requirements (Charge advice or Keypad). The support for this is controlled by market dependent parameters and by the VARI/VARO parameters.

1.2 LIMITATIONS

- Number conversion is not supported together with network services.
- 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 - ISDN or DPNSS - H.323 gateway situations.
- If an ISDN interface, 30B+D is divided into more than one route, there is no possibility to use virtual calls (temporary signaling connections) on any of the defined routes. See parameter SERV in parameter description for *ROUTE DATA*.
- The public ISDN may also limit the number of octets that can be sent in an UUI element (35 octets instead of 131). If so, this must be indicated on the route by setting the route parameter VARC, Limitations of octets in UUI element in the command *RODAI*. This should only be set for public connections. If this limitation exists, the following information is removed from the UUI element:
  - transparent UUI from an S_0 -terminal
  - calling/connected name
  - account code
  - authority's CIL-code
  - embedded transit counter
  - priority routing information
  - C-party number information at diversion and rerouting
- It is not possible to divide an interface in one public and one private route.
- The maximum size of an ISDN message can be up to 2013 octets with the support of segmentation.

1.3 INTERWORKING WITH ASB 501 04

The functionality between a MX-ONE and an ASB 501 04 exchange with a certain release, will be the same as between two ASB 501 04 exchanges with the same release.

When a cooperating ASB 501 04 exchange of earlier release supports the parameters SIG net service facilities, VARC supporting network diversion for DPNSS and VARC

full ISDN functionality for ISDN, the same value as in the ASB 501 04 R6 (see below) shall be used for the route between the exchanges.

1.3.1 DPNSS

If the cooperating exchange is ASB 501 04 R2 or later, and if all services that the release supports should be supported, the SIG parameter in the command *ROCAI* must be set to net service facilities. The VARC parameter in command *RODAI* must be set to supporting network diversion.

If the cooperating exchange is ASB 501 04 R1 or earlier release, the SIG parameter in the command *ROCAI* must be set to no net service facilities. The VARC parameter in command *RODAI* must be set to not supporting network diversion.

The AS parameter, *PARNUM = 223*, Type of network services has to be set to Call diversion, Transfer, Route optimization.

1.3.2 ISDN

The basic call service as well as the supplementary services which carry less than 260 octets message, will be provided when the cooperating exchange is ASB 501 04 R8 or earlier which supports the same service but does not support the ISDN segmentation.

In case the cooperating exchange is ASB 501 04 R8 or earlier and if the message size exceeds the 260 octets, in order to support at least the basic call service the involved ISDN route is to be setup for not supporting the UUI and GFP. The VARI parameter in the *RODAI* command and the ADC parameter in the *RODDI* command must be set accordingly. The route that is being setup for not supporting UUI and GFP does not support any supplementary service.

If the cooperating exchange is ASB 501 04 R6 or earlier, the option Type of protocol to use for Supplementary service Call back/Call completion in the ADC parameter must be set to Proprietary UUI protocol.

If any of the PBXs in the network is ASB 501 04 R7 or earlier, the AS parameter, *PARNUM= 223*, Type of network services has to be set to Call diversion, Transfer, Route optimization.

If the cooperating exchange is ASB 501 04 R4, the VARC parameter for full ISDN functionality in command *RODAI* can be set to **Yes** or **No** depending on if the functionality implemented in ASB 501 04 R4 should be supported.

If the cooperating exchange is ASB 501 04 R2/n, using ISDN tie lines or VPN, the VARC parameter for full ISDN functionality, must be set to **No**.

The services Intrusion, Call offer, and Call back can be supported when cooperating with an ASB 501 04 R2/n using ISDN, if the 04/R2/n does not act as a Transit PBX, and if the SIG parameter in the command *ROCAI* is set to net service facilities.

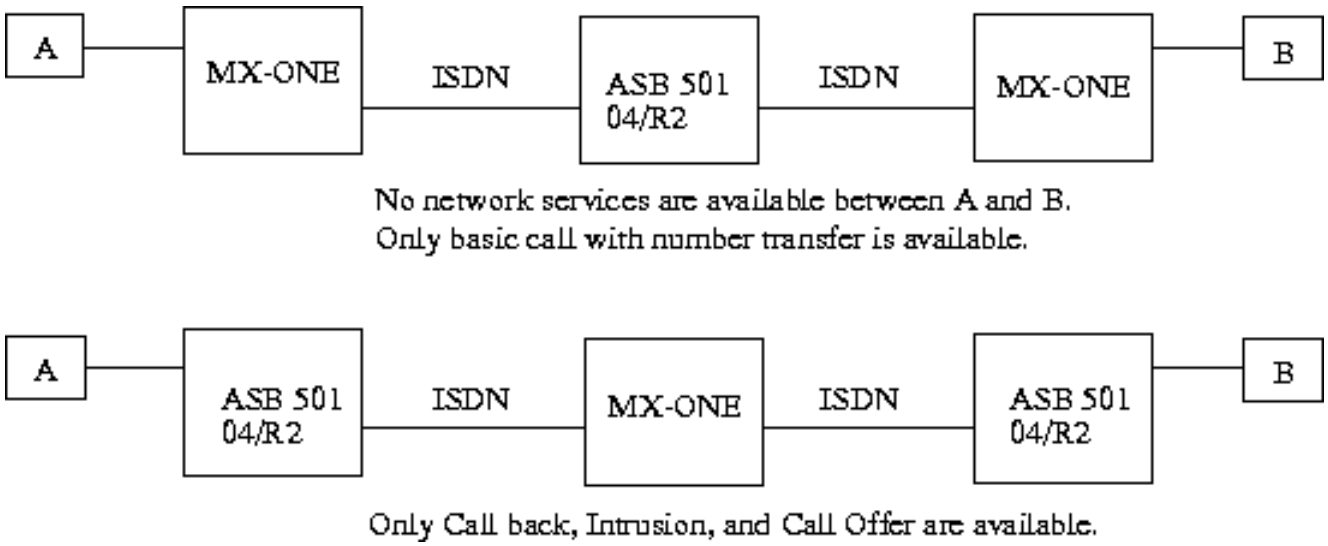


Figure 8: ISDN

1.3.3 H.323

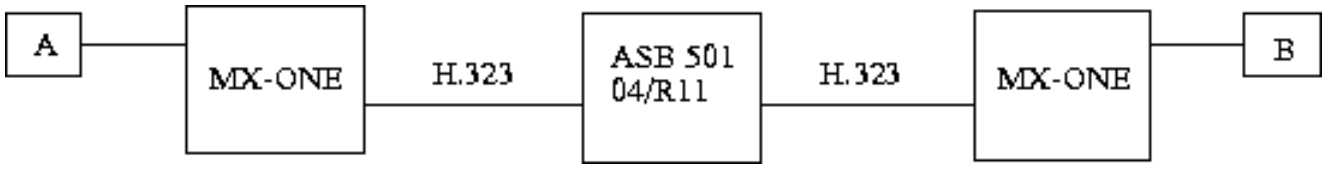


Figure 9: H.323

H.323 networking requires ASB 501 04 R11 or later.

1.3.4 GATEWAY WITH BOTH ISDN AND DPNSS

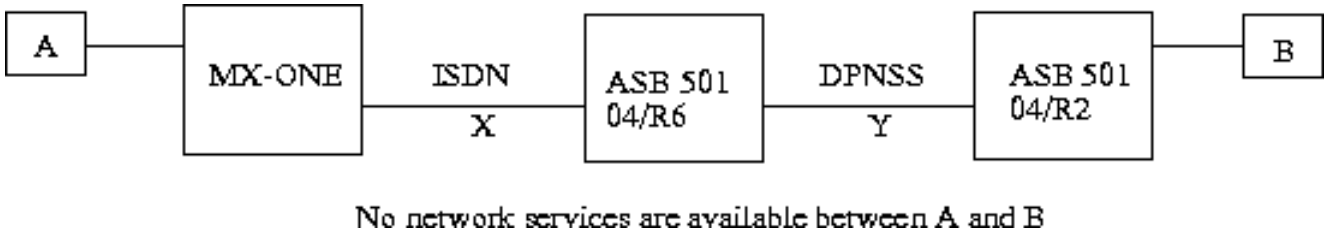
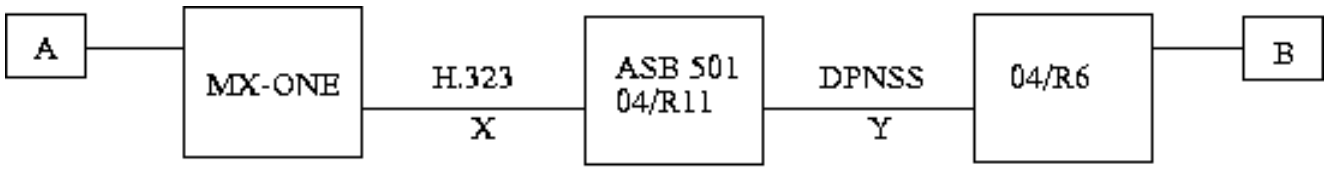


Figure 10: Gateway ISDN-DPNSS

Since two different signaling systems are connected, either the ISDN route must have the SIG parameter set to no net service facilities, or the DPNSS route must have the SIG parameter set to no net service facilities and the VARC parameter set to not supporting network diversion.

The ADC parameter in command *RODDI* for the ISDN route X (destination B) should be set to allow Supplementary Services Using UUI (that is, UUI element is allowed to be sent) even if link Y does not support network services. The reason for this is to convey the correct private number which is sent to the B-party within the UUI element.

1.3.5 GATEWAY WITH BOTH H.323 AND DPNSS



No network services are available between A and B

Figure 11: Gateway H.323-DPNSS

Since two different signaling systems are connected, either the H.323 route must have the SIG parameter set to no net service facilities, or the DPNSS route must have the SIG parameter set to no net service facilities and the VARC parameter set to not supporting network diversion.

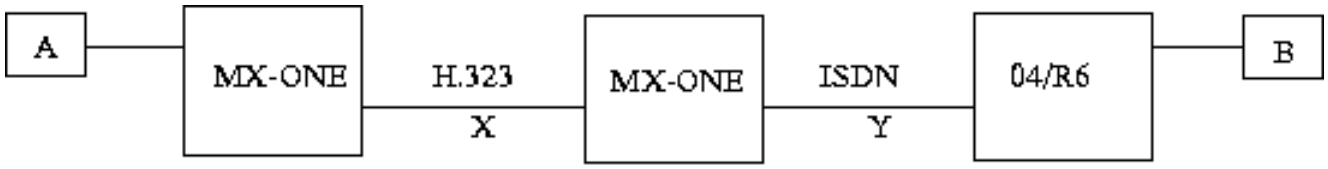
The ADC parameter in command *RODDI* for the H.323 route X (destination B) should be set to allow Supplementary Services Using UUI (that is, UUI element is allowed to be sent) even if link Y does not support network services. The reason for this is to convey the correct private number which is sent to the B-party within the UUI element.

1.3.6 GATEWAY WITH BOTH H.323 AND ISDN

From the supplementary services point of view, a network made up of H.323 and ISDN signaling systems can be considered as a homogeneous network. Availability of Network services between A and B depends on the interworking between different releases in the link Y (described below) and the services supported in the release used between the H.323 and ISDN signaling system in the link X.

Only Call back, Intrusion, and Call Offer are available.

Figure 12: Gateway H.323-ISDN, limited services



Network services are available between A and B.

Figure 13: Gateway H.323-ISDN

The basic call service as well as the supplementary services which carry less than 260 octets message, will be provided when the cooperating exchange is MX-ONE or earlier ASB 501 which supports the same services but does not support the ISDN segmentation.

In case the cooperating exchange is MX-ONE or earlier ASB 501 and if the message size exceeds the 260 octets, in order to support at least the basic call service the involved H.323 and ISDN routes are to be setup for not supporting the UUI and GFP.

For ISDN the VARI parameter in the *RODAI* command and the ADC parameter in the *RODDI* command must be set accordingly. For H.323 the SIG parameter must be set to no net service facilities. The routes which are being setup for not supporting UUI and GFP do not support any supplementary service.

If the cooperating exchange is ASB 501 04 R6 or earlier, the option Type of protocol to use for Supplementary service Call back/Call completion in the ADC parameter must be set to Proprietary UUI protocol in every exchange.

If any of the PBXs in the network is ASB 501 04 R7 or earlier, the AS parameter, *PARNUM= 223*, Type of network services has to be set to Call diversion, Transfer, Route optimization.

If the cooperating exchange is ASB 501 04 R4, for ISDN the VARC parameter for full ISDN functionality in command *RODAI* can be set to **Yes** or **No** depending on if the functionality implemented in ASB 501 04 R4 should be supported. For H.323 the SIG parameter must be set to **Yes** or **No** net service facilities depending on if the functionality implemented in ASB 501 04 R4 should be supported.

If the cooperating exchange is ASB 501 04 R2/n, using ISDN tie lines or VPN, for ISDN the VARC parameter for full ISDN functionality, must be set to **No**. For H.323 the SIG parameter must be set to **No** for avoiding support net service facilities.

The services Intrusion, Call offer, and Call back can be supported when cooperating with an ASB 501 04 R2/n using ISDN, if the 04/R2/n does not act as a Transit PBX, and if the SIG parameter in the command *ROCAI* is set to net service facilities.

1.3.7 ISDN WITH VPN

The supplementary services Call completion, Call forwarding, Call transfer and Path replacement cannot be used when VPN is in use. The AS parameter, *PARNUM = 223*, Type of network services has to be set to Call diversion, Transfer and Route optimization.

In a scenario like the one in the figure 14 below, a VPN where one or more nodes are ASB 501 04 R2/n, it is required to set full ISDN functionality = **No** for the public ISDN routes in all other nodes (MX-ONE or ASB 501 04 R6). The reason is that the terminating node cannot determine which version of the system the calling party was in.

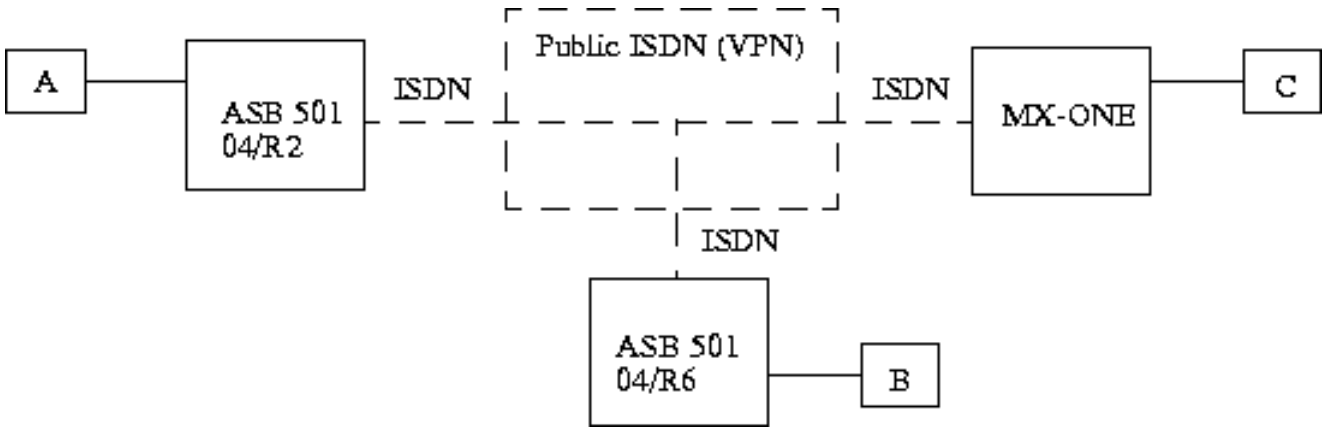


Figure 14: VPN using ISDN

1.4 INTERWORKING WITH OTHER VENDOR'S EQUIPMENT, SUPPORTING STANDARD ISDN SERVICES

For ISDN the basic call service as well as the supplementary services which carry less than 260 octets message, will be provided when interworking with a non-Mitel node which supports the same service but does not support the ISDN segmentation. The Supplementary services, for which the message length exceeds 260 octets, need support of segmentation.

In case the interworking PINX does not support the Segmentation and if the message size exceeds the 260 octets, in order to support at least the basic call service, the involved ISDN route is to be setup for not supporting the UUI and GFP. The VARI parameter in the *RODAI* command and the ADC parameter in the *RODDI* command must be set accordingly. The route that is being configured for not supporting UUI and GFP does not support any supplementary service.

Basic Call, Calling or Connected Line Identification, Advice Of Charge, and Name Identification are supported according to ECMA-QSIG and ISO-QSIG standards, and can thus be supported when interworking with a non-Mitel node which supports the same service.

Call completion is supported according to ISO-QSIG and can be supported when interworking with a non-Mitel node which supports the same service. In that case the option Type of protocol to use for Supplementary service Call back/Call completion in the ADC parameter must be set to Standardized Generic Functional Protocol.

Call forwarding is supported according to ISO-QSIG and can be supported when interworking with a non-Mitel node which supports the same service. In that case the AS parameter, *PARNUM = 223* Type of network services must be set to Call forwarding and the entire network segment must use the same type of service.

Call offer is supported according to ISO-QSIG and can be supported when interworking with a non-Mitel node which supports the same service. In that case the option Type of protocol to use for Supplementary service Call Offer in the ADC parameter must be set to Standardized Generic Functional Protocol.

Call transfer is supported according to ISO-QSIG and can be supported when interworking with a non-Mitel node which supports the same service. In that case the AS parameter, *PARNUM = 223* Type of network services must be set to Call transfer and the entire network segment must use the same type of service.

Path replacement is supported according to ISO-QSIG and can be supported when interworking with a non-Mitel node which supports the same service. In that case the AS parameter, *PARNUM = 223* Type of network services must be set to Path replacement and the entire network segment must use the same type of service.

Other standard services can be supported in transit situations. This requires that the involved ISDN routes are initiated for support of the Generic Functional protocol, that is, the VARI parameter in the *RODAI* command must be set accordingly.

1.5 INTERWORKING CONSIDERATIONS IN H.323 NETWORKS

1.5.1 INTERWORKING IN HOMOGENEOUS MIVOICE MX-ONE OR ASB 501 04 H.323 NETWORKS

No gateway functionality is implemented in homogeneous MX-ONE H.323 networks between the services based on the specific protocol in UUI message and Information field and the services based on the GFP and QSIG standard information elements.

1.5.2 INTERWORKING WITH OTHER MANUFACTURER'S SYSTEMS

Services based on the specific protocol in UUI message and Information field and services based on the GFP and QSIG standard information elements are supported in heterogeneous H.323 networks when the end nodes where the services are executed are the MX-ONE or an ASB 501 04, and the non-ASB 501 04 transit H.323 nodes support the conveyance of the H.323 nonStandardControl parameter.

In any other case the services are not supported in heterogeneous H.323 networks.

1.5.3 INTERWORKING WITH OTHER SIGNALING SYSTEMS

No gateway functionality for the services is implemented to DPNSS signaling systems.

Services based on the specific protocol in UUI message are supported in mixed networks with H.323 and ISDN QSIG signaling systems using user-to-user signaling only when the MX-ONE or an ASB 501 04 are the gateways between both signaling systems.

Services based on the GFP and QSIG standard information elements are supported in mixed networks with H.323 and ISDN QSIG signaling systems only when the MX-ONE or an ASB 501 04 are the gateways between both signaling systems.

1.5.4 INTERWORKING WITH THE VPN

For ISDN VPN the gateway functionality is supported only for the services based on the specific protocol in UUI message and only when the MX-ONE or an ASB 501 04 are the gateways between the H.323 and the ISDN signaling systems.

The services based on the specific protocol in UUI message and Information field and the services based on the GFP and QSIG standard information elements are supported in the VPN over the public H.323 network when the public H.323 network supports the conveyance of the H.323 nonStandardControl parameter.

1.6 GLOSSARY

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

Informative signaling

Proprietary UUI signaling is to be used together with public destinations in case of External follow me or Deflection to public. This is applicable when the gateway to the public network and the diverting/deflecting PINX are two separate nodes in a private network.

Originating Node (MiVoice 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 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.

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.

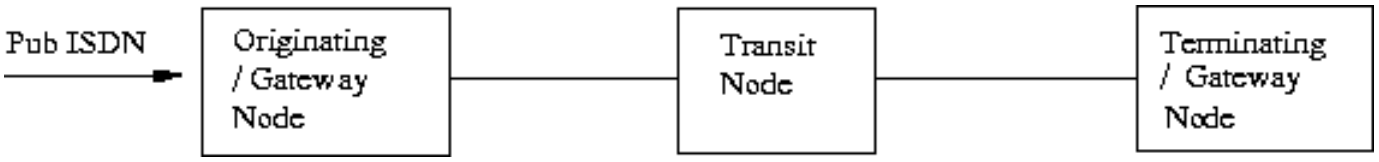


Figure 15: Types of nodes

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:

- In order to get the network services for Networking, the add-on feature Network Services must be available.
- Network services allowed both in originating and terminating exchange, that is, the SIG parameter in the command *ROCAI* must be set to network service supported. In a VPN scenario, the same thing is valid although the route is defined as consisting of public external lines instead of tie lines.
- For ISDN/H.323 it is required that the destination is in another MX-ONE or an ASB 501 04, that is, that the ADC parameter in *RODDI* is set accordingly.
- If the scenario permits, it must be set in the VARC parameter, that full ISDN functionality shall be available. For public ISDN routes it is required that the UUI supported in Alerting category and support for UUS1, 2, 3 as applicable, are set in the VARO and VARI parameters respectively (in the *RODAI* command).
- Number Prefixes may have to be set, depending on numbering plan (RO-commands), see the operational directions for *NUMBERING*.
- If the public network supports 35 or 131 octets in the UUI element this is set in the VARC parameter (limitations of octets).
- The type of QSIG protocol supported, if used, is set in the VARI-parameter (ECMA or ISO).
- UUI tunneling shall be used in a network that includes exchanges from other vendors. It is set in the VARI parameter (QSIG with embedded UUI in the GFP).
- Name on route can be initiated by use of the command *name - i.*

3 USER SERVICES

3.1 ADVICE OF CHARGE

3.1.1 GENERAL

Advice of Charge (AOC) is a service that provides display of charging information (in currency) received from the public ISDN network, to a charged extension with an appropriate display, in the PBX. The information is conveyed through the private homogeneous ISDN/H.323 network based on the ISO standard for AOC. H.323/ISDN transit is also considered an homogeneous network.

When the standard protocols for AOC are used, the type of charging desired is set per route in the VARO parameter in the command *RODAI*. The different types of AOC services that can be set are charge during the call (AOC-D) or charge at the end of the call (AOC-E) or both. The initiation of AOC related data (command groups RO, AS and KS) is described below.

Multi-party calls, calls set up using External Follow-me, and calls set up via VPN will not get AOC information. Calls that have been transferred or extended to a party not located in the transferring node, or calls that have been Route optimized, will also cease to receive AOC information.

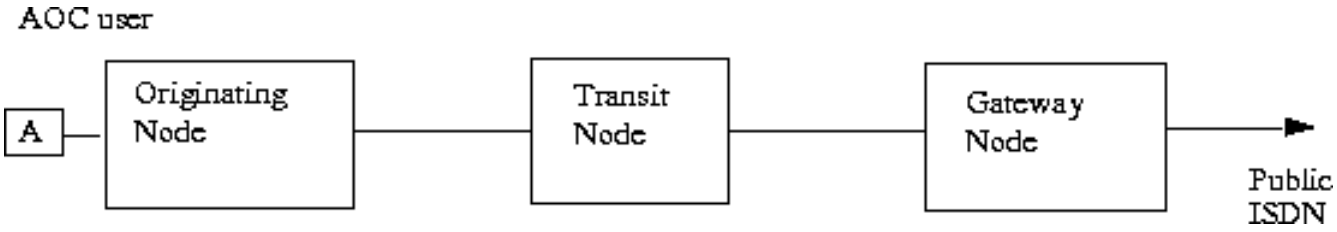


Figure 16: Advice of charge

3.1.2 PREREQUISITES, PROCEDURE

1. Extensions must be initiated (*KS, extension, ip_extension*)
2. Initiate public ISDN and private ISDN/H.323 charging routes (*RO*), with AOC and GFP support
3. Initiate cost per charging unit (pulse) for pulse-currency conversion
4. Initiate correct text strings, and currency format *(KS/AS)*

3.1.3 EXECUTION

Extensions are assumed to be initiated. Both private and public ISDN/H.323 routes should be initiated as charging routes. Private ISDN/H.323 routes should have network services supported. Key the commands:

***ROCAI*:...,SIG=;** or

***ROCAC*:...,SIG=;**

The support for the standardized Generic Functional protocol must be initiated on each route that uses the standard protocols for AOC. This applies both for private and public

routes. The support of the Generic Functional protocol is set per route in the VARI parameter for the command *RODAI*. H.323 routes support GFP as a standard.

The MX-ONE only supports AOC according to the ISO standard in private networks.

For public routes, several different charging protocols are supported in addition to the standard version (ETSI). If the public network does not support AOC according to the ETSI standard, the type of protocol used is controlled by market dependent parameters.

When the standard protocols for AOC are used, the type of charging desired is set per route in the VARO parameter in the command *RODAI*. The different types of AOC services that can be set are charge during the call (AOC-D) or charge at the end of the call (AOC-E) or both. The services can be set independently. The charging information from the public ISDN is available for all calls, or requested on a per call basis. If it is requested on a per call basis and the public network supports AOC according to the ETSI standard for AOC, then the type of charging request used must be set. This is also set per route in the VARO parameter for the command *RODAI*.

Initiation of cost per charging unit (pulse)

Charging information may be received either as a cost in a currency amount or as units (pulses). The cost is always displayed as a currency amount at the user. If the cost information is received as units it is always necessary to calculate the corresponding currency amount. On the other hand, the charging counters only use charging information stored as units (pulses). This means that if the cost information is received as a currency amount, it is always necessary to calculate the corresponding cost in units.

The cost per unit (pulse) is controlled per exchange with an application system parameter. Key the command:

***ASPAC*:PARNUM=150,PARVAL=...;**

Finally, set an application system parameter controlling the currency format, using the command:

***ASPAC*:PARNUM=150,PARVAL=...;**

in order, for example, to select whether to use decimal point (cost per pulse in hundredths, depending on the currency) or not. If the charging information was received as units and the cost per unit was entered in fractions, the cost amount will also be displayed with fractions (hundredths).

Initiation of default AOC text strings (currency)

The currency identifier is normally transferred from the public network to the private network. If no currency identifier has been received from the public network, a default currency identifier string must be used. There are two different strings that can be set. The first string is used in a public gateway exchange before sending any cost information to the private network. It is set with an application system parameter:

***ASPAC*:PARNUM=185,PARVAL=...;**

The parameter uses the corresponding currency code for the desired currency identifier according to the standard ISO 4217. A currency identifier is always received from the private network in the originating exchange. However it is not mandatory from a public network.

If no currency identifier has been received from a public network connection, another default currency identifier string is added in the originating exchange. The string is set with the command:

extension_text -c --ext-display-option MIS14 --ext-display-string

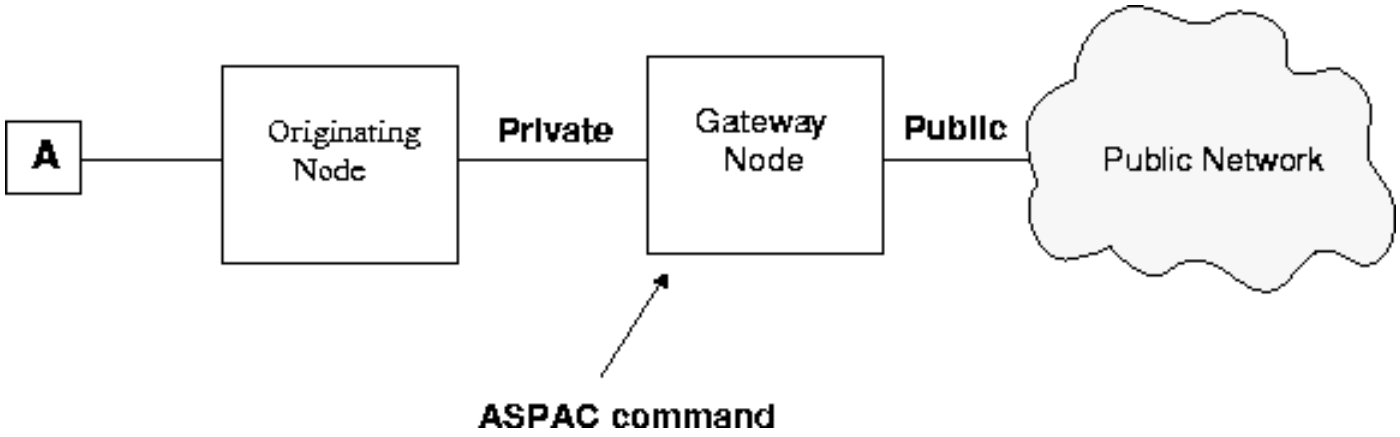


Figure 17: Initiation of default AOC text string in the gateway exchange

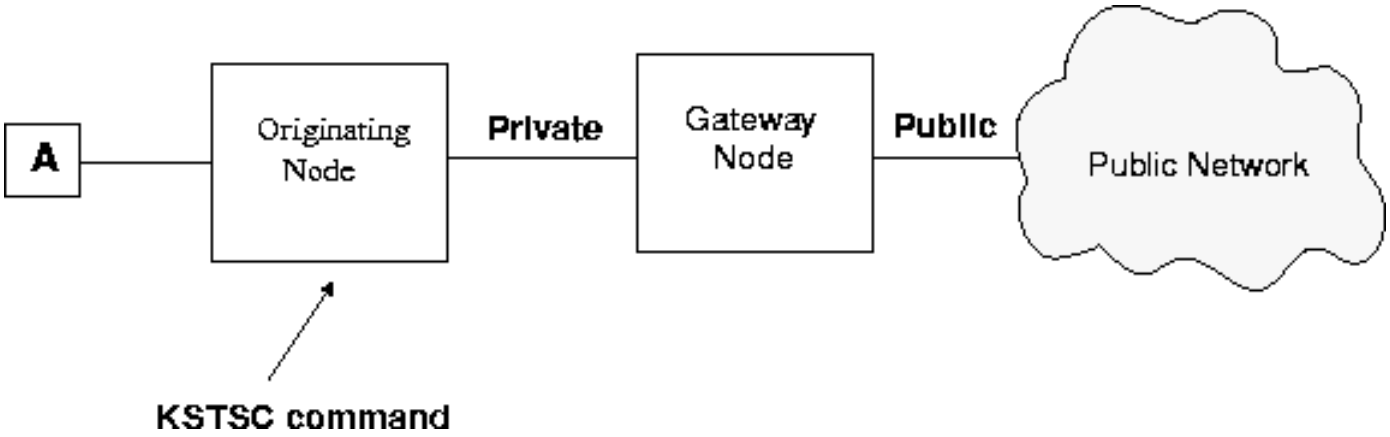


Figure 18: Initiation of default AOC text string in the originating exchange

3.2 CALL BACK

3.2.1 GENERAL

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).
- Call Back at no answer (CBNA)

The called party may be located in another PBX (either within a private network or via the public network). Call back is supported in a homogeneous DPNSS network, in a homogeneous ISDN network, in a homogeneous H.323 network or in a mixed ISDN-H.323 network (see 1.5 Interworking considerations in H.323 networks on page 15). 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.

3.2.1.1 Call set-up at network Call Back

There are currently two methods which can in private networks be used to establish the call set-up of network Call Back, **Path reservation method** or **Non reservation method**. DPNSS networks are always using call set-up **Path reservation method.** ISDN/H.323 networks use the call set-up **Non reservation method**. The difference between the two methods can briefly be described as follows:

- **Path reservation method**

  After free notification a transmission path between the originating and terminating node is established **before** the initiating party is recalled. When the initiating party answers, the party in the terminating node is called.

- **Non reservation method**

  After free notification there is **no** transmission path between the originating and terminating node when the initiating party is recalled. When the initiating party answers the call a new call set up is performed towards the terminating node and the party in the terminating node is called.

3.2.2 EXECUTION, INITIATION OF CALL BACK RELATED DATA

No specific I/O data are required for Call back, except that network services must be supported. For ISDN, Call back works also if full ISDN functionality is set to **No**, when cooperating with an ASB 501 04 R2/n.

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

3.3 CALL COMPLETION

3.3.1 GENERAL

The Call Completion 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:

- Completion of Calls to Busy Subscriber (CCBS).
- Completion of Calls on No Reply (CCNR)

The called party may be located in another MX-ONE (within a private network). Call Completion is supported in a homogeneous ISDN network, in homogeneous H.323 networks or in mixed H.323/ISDN networks 1.5 Interworking considerations in H.323 networks on page 15. To allow Call Completion, the called party must be an extension.

Call Completion can be invoked from an extension or a PBX operator.

3.3.1.1 Signaling connection for Call Completion

There are two methods which can be used for call independent signaling connection of Call Completion, Connection retention and Connection release. The difference between the two versions can briefly be described as follows:

- Connection retention method

The signaling connection is maintained until completion or cancellation of the call completion mission. This is to avoid bouncing of call independent signaling connections.

- Connection release method

  The signaling connection is cleared after each phase of call independent signaling and a new signaling connection is established for each subsequent phase of call independent signaling.

3.3.1.2 Call set-up at Call Completion

There are currently two methods which can be used to establish the call set-up of Call Completion, **Path reservation method** or **Non reservation method**. The difference between the two methods can briefly be described as follows:

- **Path reservation method**

  After free notification a transmission path between the originating and terminating node is established **before** the initiating party is recalled. When the initiating party answers, the party in the terminating node is called.

- **Non reservation method**

  After free notification there is **no** transmission path between the originating and terminating node when the initiating party is recalled. When the initiating party answers the call a new call set up is performed towards the terminating node and the party in the terminating node is called.

3.3.1.3 Service retention

The ISO standard includes **service retention** and **service cancellation.**

The MX-ONE supports **only service cancellation**, which means that the CC Request is cancelled at the originating and terminating side.

3.3.2 EXECUTION, INITIATION OF CALL COMPLETION RELATED DATA

The following I/O data are required for Call Completion:

- Full ISDN functionality must be set to **Yes**.
- Selection of QSIG protocol must be set to include ISO QSIG.
- Support of Generic Functional Protocol (GFP) must be set to **Yes**.
- Type of protocol to use for Supplementary Service Call back/Call completion must be set to Standardized Generic Functional Protocol.

There are a number of application system parameters used for Call Completion, to select timer lengths. These timers are the same as for Call Back.

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 CCS networks consisting of DPNSS tie lines or ISDN tie lines or ISDN public external lines (for VPN). Network diversion is also possible in packet networks based on H.323 tie lines and/or H.323 public external lines and even in mixed ISDN-H.323 networks 1.5 Interworking considerations in H.323 networks on page 15. The Diversion services described in this document are as follows:

- 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 PREREQUISITES

If Call diversion is to be used

- The AS parameter, *PARNUM = 223*, Type of network services has to be set to Call Diversion.

3.4.3 NETWORK CONFIGURATIONS AND A BASIC TRAFFIC CONCEPT

The figure 19 below shows a possible DPNSS or homogeneous ISDN/H.323 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.

Originating MiVoice 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-CCS network. Thus the signaling system changes, so the originating node is also a gateway exchange.

Terminating MiVoice MX-ONE

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

Nominated MiVoice MX-ONE

The exchange where the diverted-to party is located.

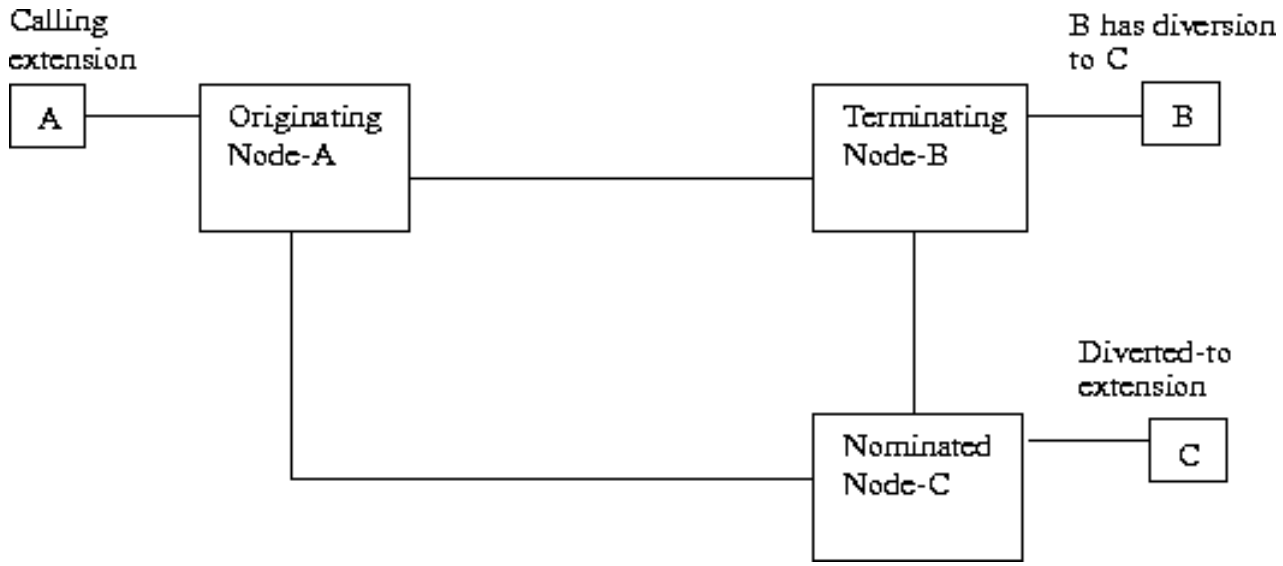


Figure 19: Diversion

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. The terminating exchange continues by sending the identity of extension C back to the originating exchange together with a divert request.

The principle of returning to the originating/gateway node for a new call set up after diversion has occurred in the terminating exchange is always used and the reason is of course to minimize occupied network resources. The originating exchange then proceeds with a new call setup to extension C in the nominated exchange.

3.4.4 CHAINING OF NETWORK DIVERSION

A diverted-to position for diversion, but not message diversion, may be diverted with follow me. A diverted-to position may also be diverted with diversion on no reply, but only if the previous diversion reason is direct diversion or follow me. All other repeated diversions are blocked.

For network diversion there is a counter, set by the *diversion_system* command, stating the maximum number of chained network diversions that is allowed for one call. This counter is placed in the originating node and is increased each time a new diversion call set up is done.

The following figure 20 shows a possible DPNSS or homogeneous ISDN/H.323 network configuration, where the maximum number of repeated diversions is set to 2 in the originating PBX-A by command:

diversion_system -c--div-network-chaining 2 --div-no-reply-first 15
--div-no-reply-second 5 --div-type-priority 1

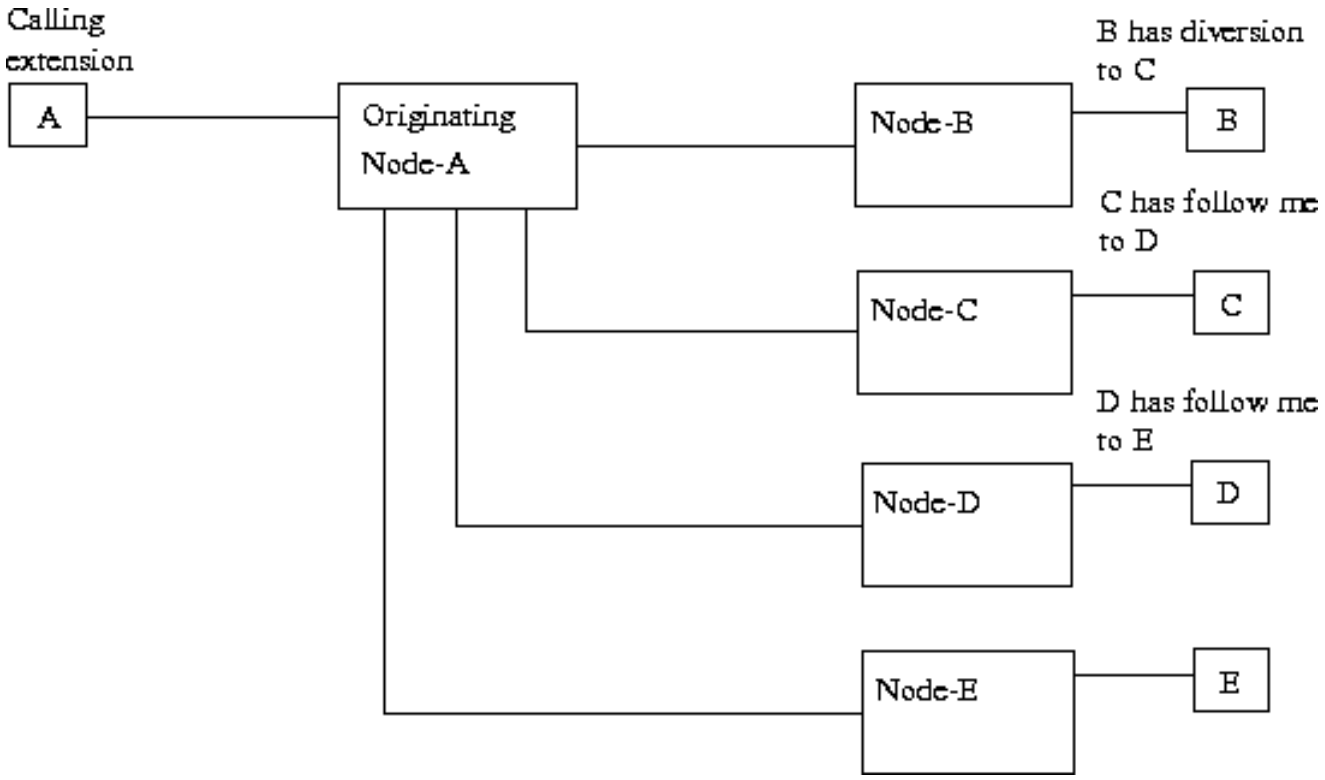


Figure 20: Diversion chaining

Extension A calls extension B. Extension B has activated diversion (that is, any of busy, direct diversion, or no answer diversion) to extension C. Node-A receives the C identity from Node-B and proceeds by increasing the diversion counter to one before a new call set up is done to extension C. Extension C has activated follow me to extension D. Node-A receives the D identity from Node-C and proceeds by increasing the diversion counter to two before a new call set up is done to extension D. Extension D has activated follow me to extension E. Node-A receives the E identity from Node-D and proceeds by increasing the diversion counter to three. But only two chainings are allowed.

Depending on the state of extension B, the following will happen:

If extension B has activated direct diversion or follow me, a no-progress tone is sent to extension A. If extension B has activated diversion on busy, a busy tone is sent to extension A. If extension B has activated diversion on no answer it will keep on ringing on extension B.

3.4.5 EXTERNAL FOLLOW ME

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

3.4.5.1 Prerequisites

The ISDN/H.323 route must be set with the following data:

- Informative signaling, set by the ADC parameter in the command *RODDI*, must be allowed when using proprietary UUI, if the public destination is reached via a private route.

3.4.5.2 *External follow me*

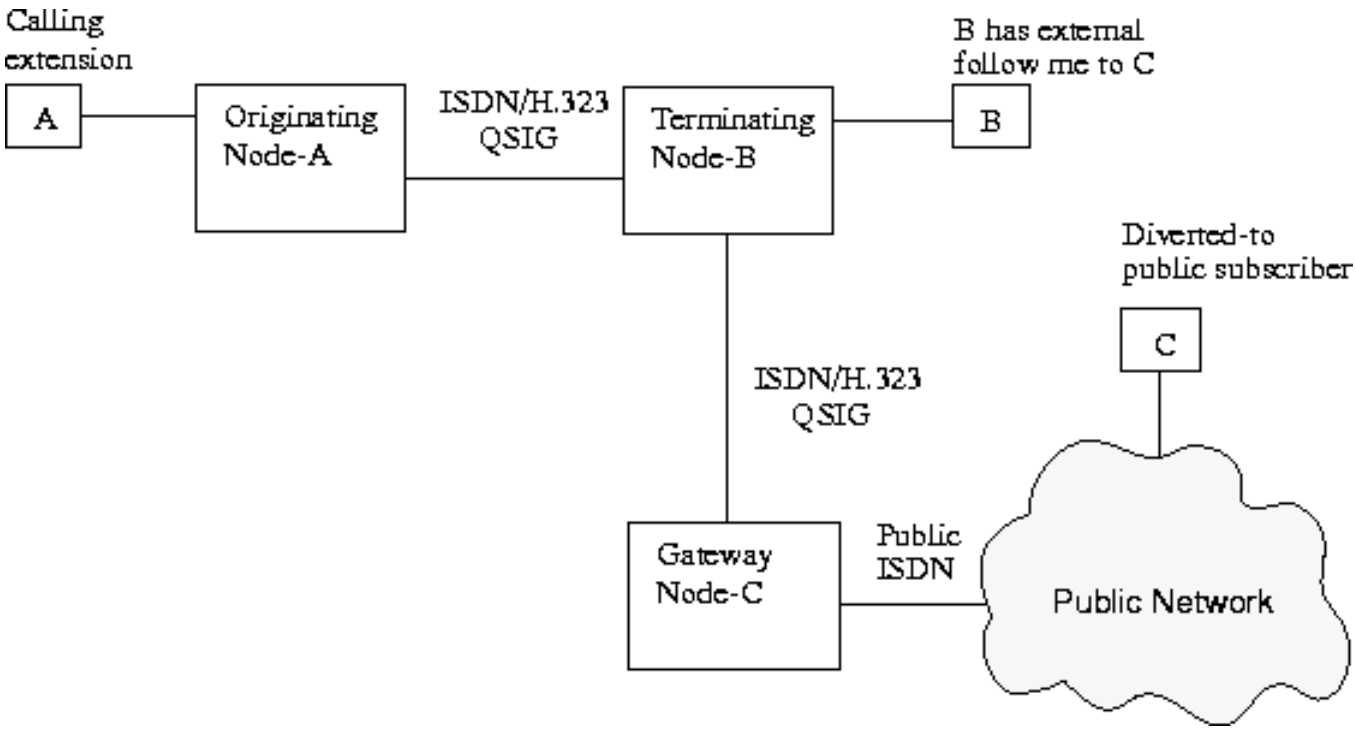


Figure 21: External follow me

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 supplementary services using UUI 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 QSIG 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*.

3.4.6 INTERWORKING WITH ASB 501 04

For the parameters SIG and VARC, see also the description in section General.

If the cooperating exchange is an ASB 501 04 R4, and ISDN is used, the VARC parameter for full ISDN functionality shall be set to **Yes**, if network diversion shall be allowed between the exchanges.

If the cooperating exchange is an ASB 501 04 R2/n and ISDN is used, the VARC parameter for full ISDN functionality shall be set to **No**.

If the cooperating exchange is an ASB 501 04 R4 or ASB 501 04 R2/n, and DPNSS is used, the VARC parameter shall be set to supporting network diversion, if network diversion shall be allowed between the exchanges.

If the cooperating exchange is an ASB 501 04 R1 or earlier release, and DPNSS is used, the VARC parameter shall be set to not supporting network diversion.

In the network configuration below, Node-B and Node-C are connected to PBX-A. PBX-A can, for example, be an ASB 501 04 R1 (or earlier release) using DPNSS, or an ASB 501 04 R2/n using ISDN.

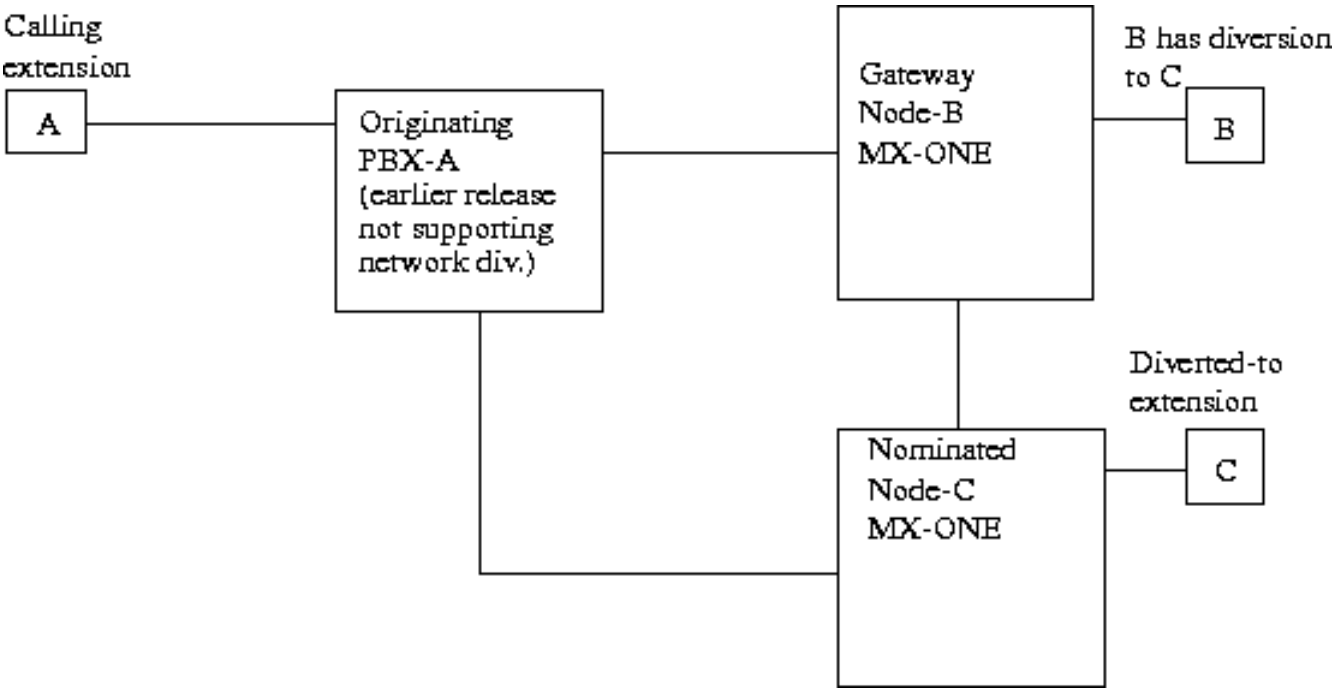


Figure 22: With ASB 501 04 of earlier releases, diversion

Extension A in originating PBX-A calls extension B. Extension B has activated diversion (that is, any of busy, direct, follow me, or no answer diversion) to extension C in the nominated node.

After A has called extension B, diversion will take place in Node-B. Node-B will in this case act as a gateway exchange. This means that Node-B will continue with a new call set up to extension C in the nominated exchange, that is, for earlier releases it is not possible to use the principle of returning to the originating PBX-A and set up a new call to the nominated Node-C.

3.5 CALL FORWARDING

3.5.1 GENERAL

Call forwarding services make it possible for a user to have voice calls forwarded for various reasons, to an answering position within the private network. Call forwarding is only possible in a network with ISDN/H.323 tie lines that supports the Standardized Generic Functional Protocol 1.5 Interworking considerations in H.323 networks on page 15. The Call forwarding services described in this document are as follows:

- Call forwarding unconditionally
- Call forwarding on busy
- Call forwarding on no answer

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.

3.5.2 PREREQUISITES

The ISDN/H.323 route must be set with the following data:

- Network services must be set to **Yes**. Set in parameter SIG in command *ROCAI*.
- Full ISDN functionality must be set to **Yes**. Set in parameter VARC in command *RODAI*.
- Selection of QSIG protocol must be set to include ISO-QSIG. Set in parameter VARI in command *RODAI*.
- Support of Generic Functional Protocol (GFP) must be set to **Yes**. Set in parameter VARI in command *RODAI*.
- The AS parameter, *PARNUM = 223*, Type of network services has to be set to Call Forwarding.
- Code UUI in Generic Functional Protocol has to be set to **Yes**, if proprietary UUI signaling is used in the network. Set in parameter VARI in command *RODAI*.

3.5.3 EXECUTION

3.5.3.1 Activation/Deactivation

Procedures to activate/deactivate Call Forwarding are the same as for Call Diversion.

3.5.3.2 Basic traffic concept

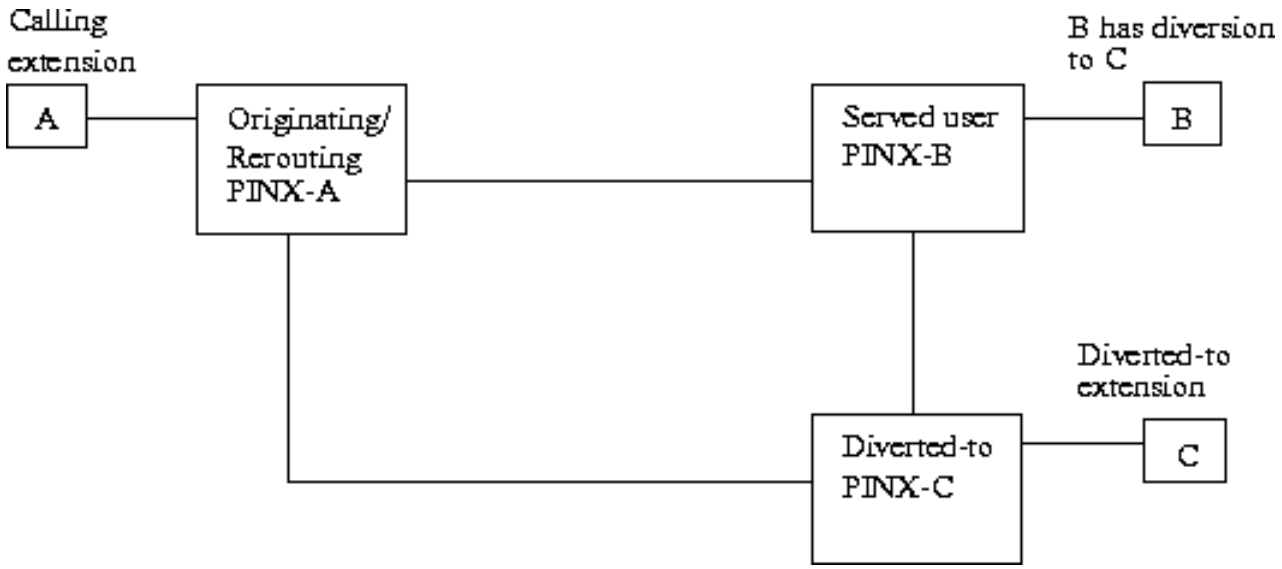


Figure 23: Call forwarding

To minimize occupied network resources the call always returns to the originating PINX when a diversion is detected in served user PINX. The originating PINX then proceeds with the new call setup to extension C in the diverted-to PINX.

However, forward switching from the served user PINX can be started, depending on a VAR parameter value in the RO command. In such a scenario, the served user PINX shall proceed with a new call setup to extension C in the diverted-to PINX.

3.5.3.3 *Multiple Call forwarding in network*

The function for multiple Call forwarding is the same as for chaining of network diversion.

The maximum number of diversions that is allowed for one call is set by the *diversion_system* command, in served user PINX. A counter, placed in the originating PBX, is increased each time a new Call forwarding is encountered and it is compared with the value set in the chaining parameter. If the counter equals the value set in the chaining parameter, actions depending on the originating Call forwarding reason will take place. The actions to take place are the same as for Call diversion.

3.5.4 EXTERNAL FOLLOW ME

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

3.5.4.1 *Prerequisites*

The ISDN/H.323 route must be set with the following data:

- When proprietary UUI signaling is used in the network and the public destination is reached via a private route, informative signaling, set by the ADC parameter in the command *RODDI*, must be allowed.

3.5.4.2 *External follow me*

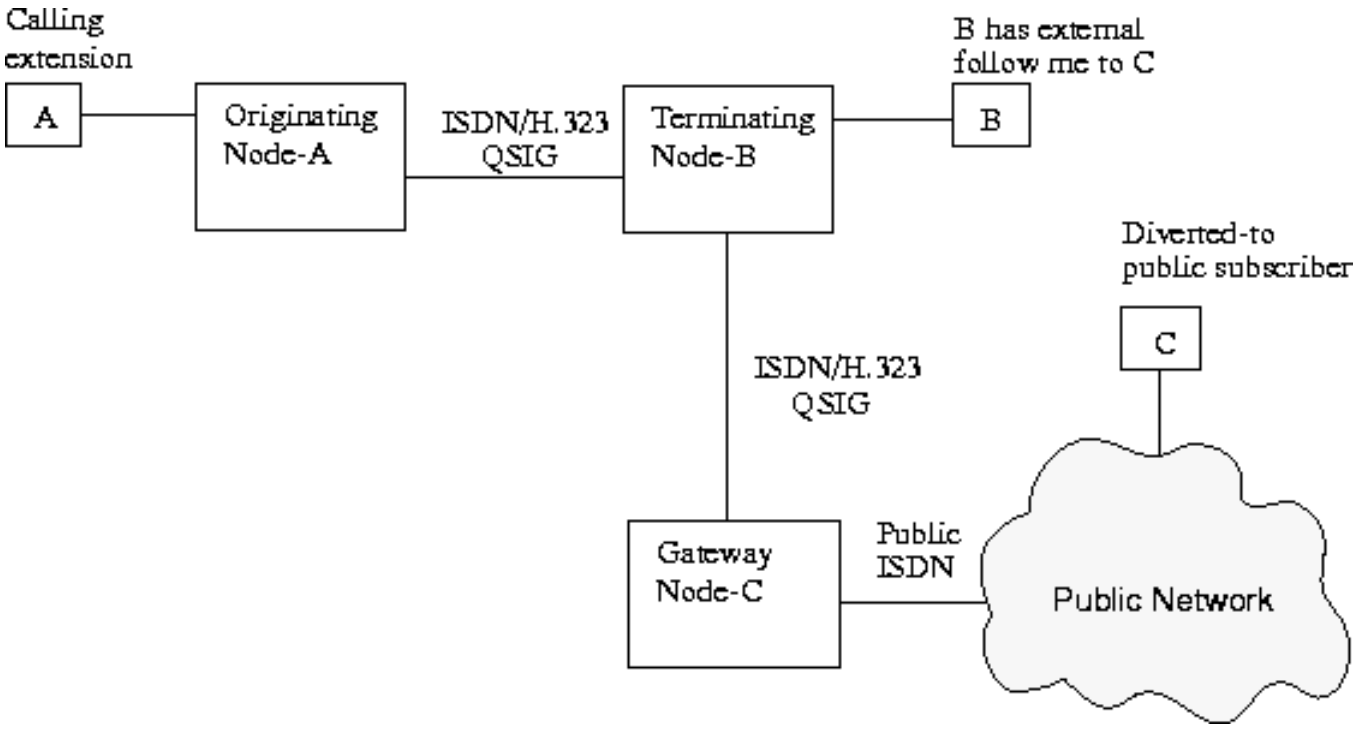


Figure 24: External follow me

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 supplementary services using UUI 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 QSIG 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*.

3.6 CALL OFFER

3.6.1 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 a CCS network consisting of DPNSS tie lines or private homogeneous ISDN tie lines or ISDN public external lines (for VPN). Call offer is also supported in packet-switched networks based on H.323 tie lines and/or H.323 public external lines, and even in mixed ISDN-H.323 networks (1.5 Interworking considerations in H.323 networks on page 15).

There is a COS (in the *EX/KS* and *extension* 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. For ISDN, Call offer is available even if full ISDN functionality is not supported, that is, when cooperating with an ASB 501 04 R2/n.

3.7 CALL TRANSFER

3.7.1 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 user is then released from the speech connection. Call transfer is only possible in a network with ISDN tie lines that supports the Standardized Generic Functional Protocol.

The transfer can be made before or after answer.

3.7.2 PREREQUISITES

The ISDN route must be set with the following data:

- Network services must be set to **Yes**. Set in parameter SIG in command *ROCAI*.
- Full ISDN functionality must be set to **Yes**. Set in parameter VARC in command *RODAI*.
- Selection of QSIG protocol must be set to include ISO-QSIG. Set in parameter VARI in command *RODAI*.
- Support of Generic Functional Protocol (GFP) must be set to **Yes**. Set in parameter VARI in command *RODAI*.
- Code UUI in Generic Functional Protocol has to be set to **Yes**, if proprietary UUI signaling is used in the network. Set in parameter VARI in command *RODAI*.

The AS parameter, *PARNUM = 223*, Type of service in network has to be set to Call Transfer (standard QSIG signaling).

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 transfer before answer in the *global_traffic_data* commands is set to allow transfer before answer.

3.7.3 EXECUTION

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

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*.

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 only possible in a CCS network consisting of ISDN tie lines or ISDN public external lines (for VPN). Network deflection/SST is also supported in packet-switched networks consisting of H.323 tie lines and/or H.323 public external lines. Network deflection/SST is even possible in mixed ISDN-H.323 networks (1.5 Interworking considerations in H.323 networks on page 15).

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

3.8.2 NETWORK CONFIGURATIONS AND A BASIC TRAFFIC CONCEPT

The figure 25 shows a possible ISDN 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 MiVoice 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 MiVoice MX-ONE

The exchange where the called party is located.

Deflect-to MiVoice MX-ONE

The exchange where the deflect-to party is located.

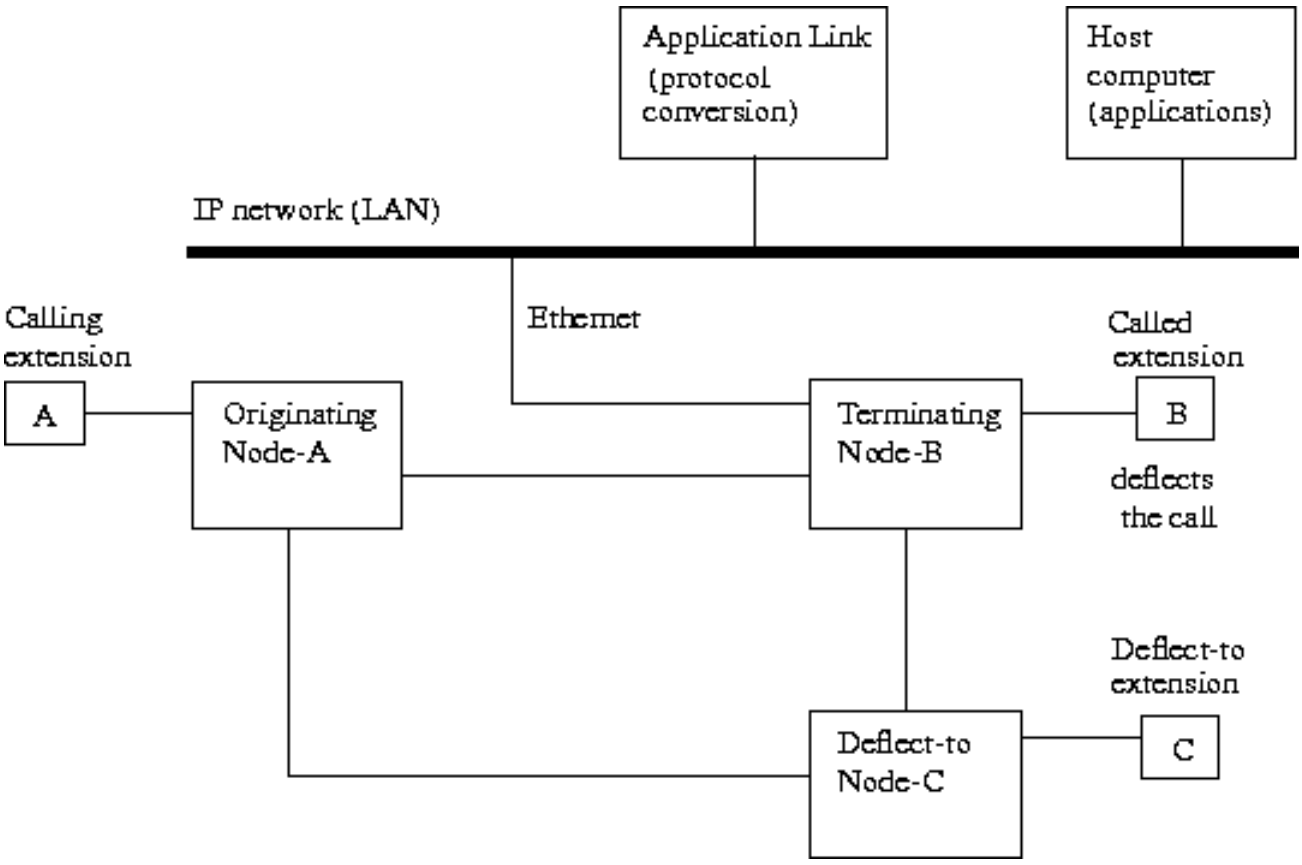


Figure 25: Deflection/SST

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 sends the identity of extension C and the deflect request back to the originating exchange.

The originating exchange then proceeds with a new call setup to extension C in the deflect-to exchange. The result of the call setup is sent from the deflect-to exchange to the originating exchange where it is sent to the terminating exchange.

When the originating exchange receives successful result for the deflect service, it releases the connection to the terminating exchange.

However, forward switching from the deflecting node can be started, depending on a VAR parameter value in the RO command. In such a scenario, the deflecting node shall proceed with a new call setup to extension C in the deflect-to node.

3.8.3 INTERWORKING WITH ASB 501 04

For the parameters SIG and VARC, see also the description in section General.

In the network configuration below, PBX-A is an ASB 501 04 R2/n or earlier release. The VARC parameter for full ISDN functionality shall be set to **No** between PBX-A and Node-B, and between PBX-A and Node-C. The VARC parameter for full ISDN functionality must be set to **Yes** between PBX-B and PBX-C, if deflect/SST shall be possible between these exchanges.

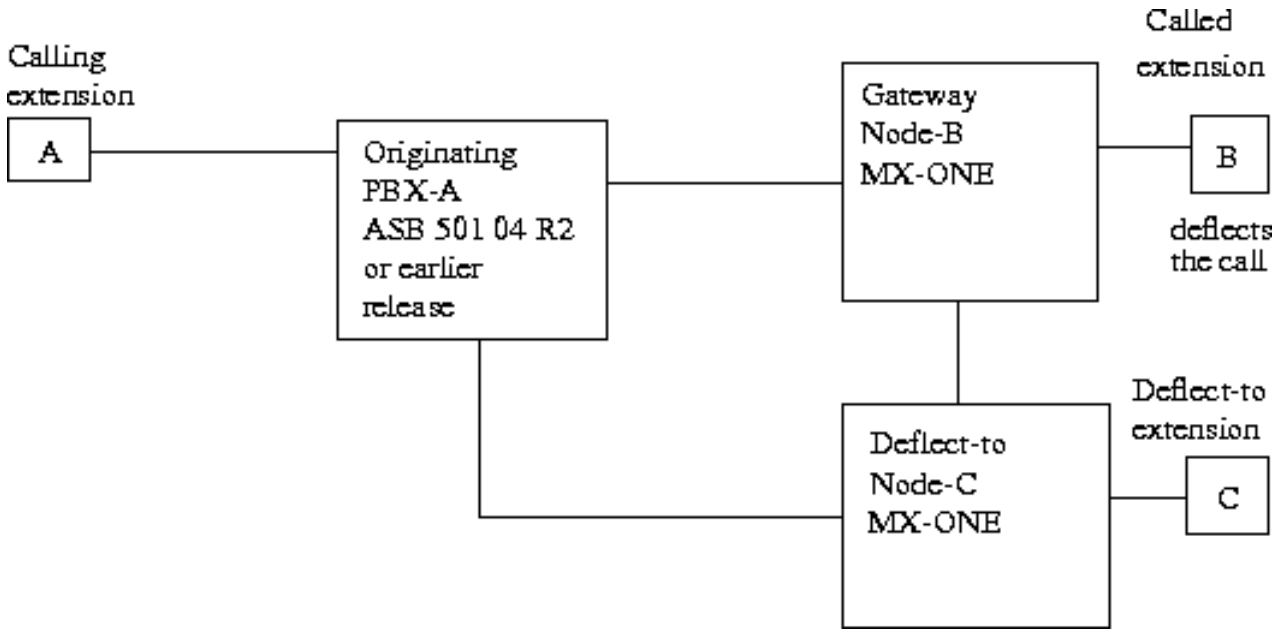


Figure 26: ASB 501 04 R2 or earlier releases, deflect/SST

Extension A in the originating node calls extension B. Extension B deflects the call to extension C in the deflect-to node. Unable to send the deflect request backwards in the network, Node-B launches the deflect request in its exchange. Node-B in this case acts as a gateway exchange. This means that Node-B continues with a new call set up to extension C in the deflect-to exchange.

In the network configuration below, PBX-A is an ASB 501 04 R4. The VARC parameter for full ISDN functionality can be set either to **Yes** or to **No** between PBX-A and Node-B, and between PBX-A and Node-C. The VARC parameter for full ISDN functionality must be set to **Yes** between Node-B and Node-C if deflect/SST shall be possible.

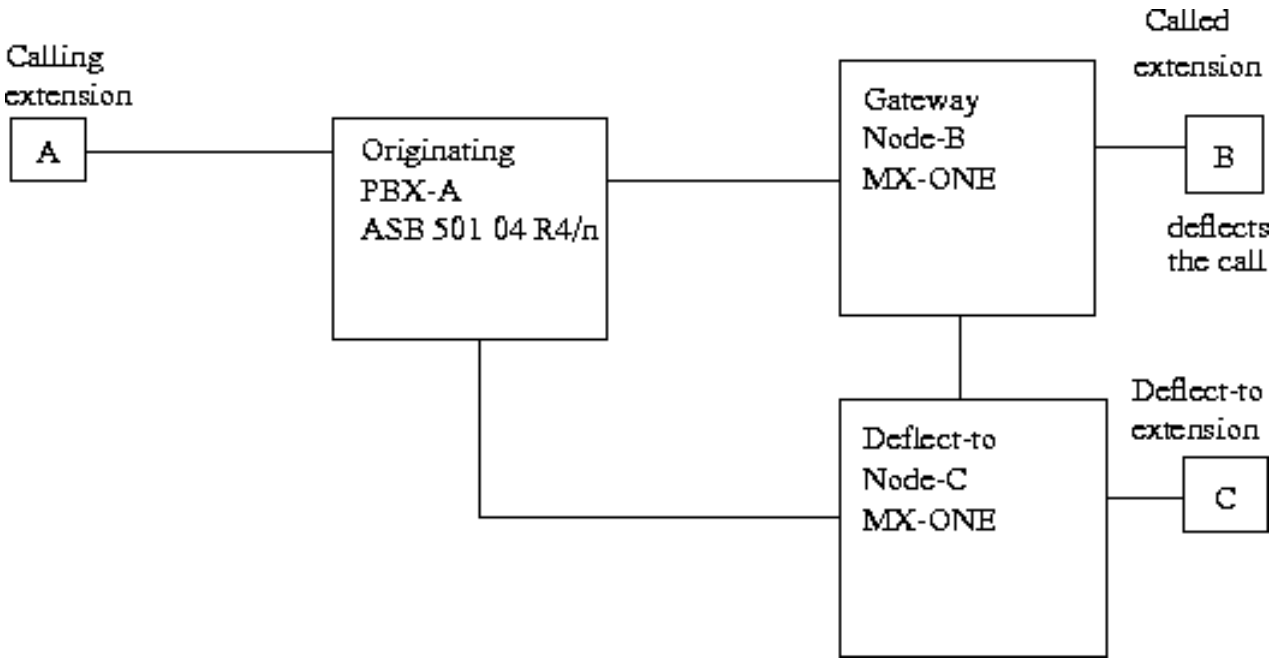


Figure 27: ASB 501 04 R4 releases, deflect/SST

Extension A in the originating node calls extension B. Extension B deflects the call to extension C in the deflect-to node. If the VARC parameter for full ISDN functionality is set to **Yes** between PBX-A and Node-B, the deflect request is sent to the originating exchange. Unable to fulfill the request, the originating exchange sends a reject message back to the gateway node. The deflect then takes place in Node-B. If the VARC parameter for full ISDN functionality is set to **No** between PBX-A and Node-B, Node-B is unable to send the deflect request back. Node-B launches the deflect request in its exchange. Node-B will in both cases act as a gateway exchange. This means that Node-B continues with a new call set up to extension C in the deflect-to exchange.

3.9 REPEATED INDIVIDUAL DIVERSION/PERSONAL NUMBER

3.9.1 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 ISDN and H.323 tie lines (in a homogeneous network configuration) are able to handle the RID deflection service 1.5 Interworking considerations in H.323 networks on page 15.

The service can be initiated in the system using call_list (Personal Number) commands.

3.9.2 NETWORK CONFIGURATIONS AND A BASIC TRAFFIC CONCEPT

The following figure 28 shows a possible ISDN or H.323 network configuration, where all parties involved are located in different MX-ONE, 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 MiVoice 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 MiVoice MX-ONE

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

Deflected-to MiVoice MX-ONE

The exchange where the answering position is located.

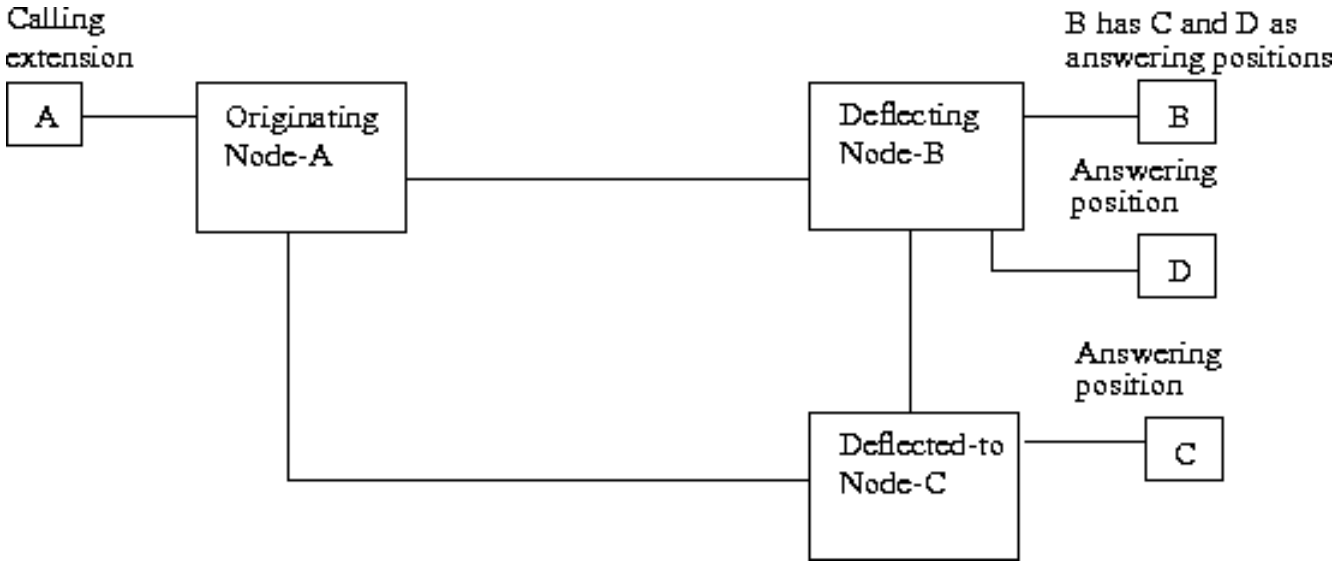


Figure 28: RID deflection

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 execution starts in the Deflecting exchange. The deflecting exchange continues by sending the identity of extension C back to the originating exchange together with a RID deflect request.

The principle of returning to the originating/gateway node for a new call set up after every deflection has occurred in the deflecting exchange is used whenever the answering position is located in the private network and the reason is of course to minimize occupied network resources. When the answering position is located in the public network, the call set up is started in the deflecting node.

The originating exchange then proceeds with a new call setup to extension C in the deflected-to exchange. This node is notified about the RID service and receives the identity of the 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 deflection request 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, a RID deflect stop request is sent to the originating node where the existing call towards the answering position C must be released. The result of the RID deflect stop request is sent to the deflecting node where a new RID deflection may 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 RID deflected 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.

3.9.3 RID DEFLECTION TO EXTERNAL PARTY

3.9.3.1 Prerequisites

The ISDN route must be set with the following data:

- Informative signaling, set by the ADC parameter in the command *RODDI*, must be allowed when using proprietary UUI, if the public destination is reached via a private route.

No prerequisites are required for H.323 routes.

3.9.3.2 RID to external party

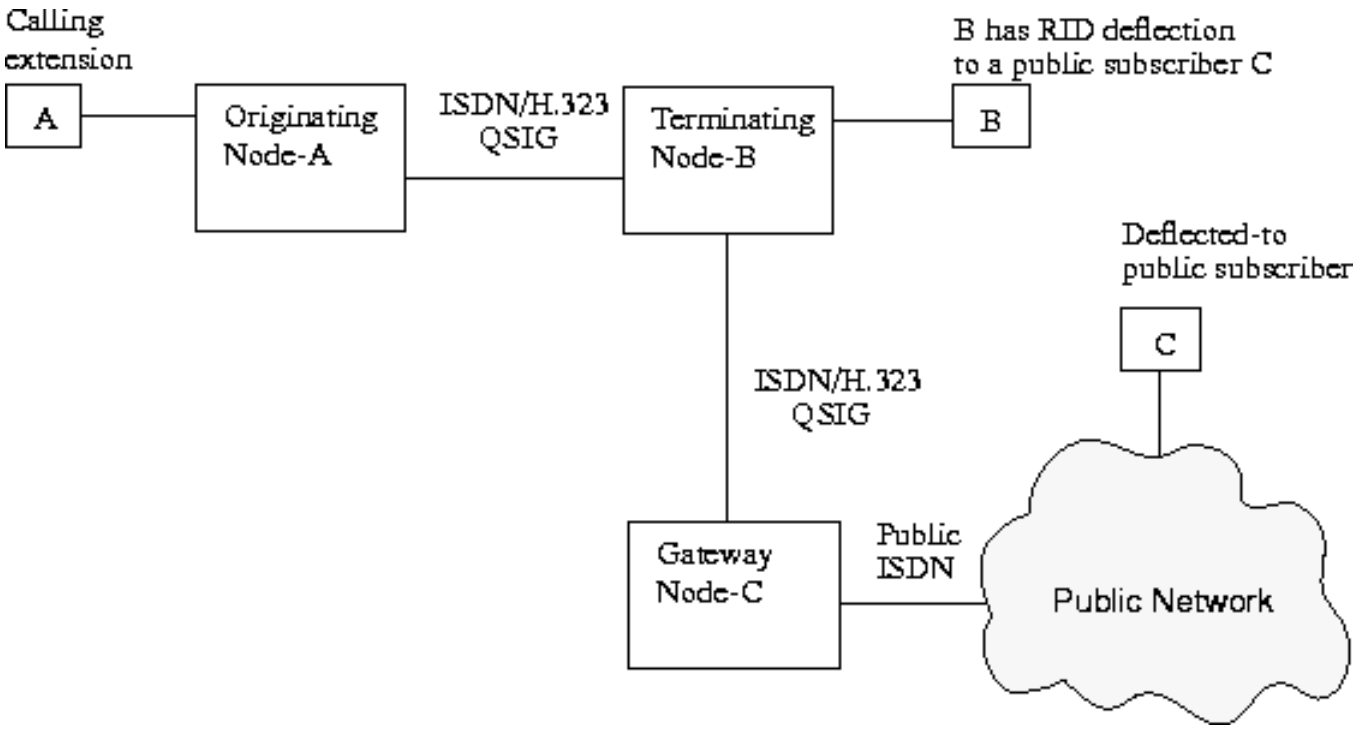


Figure 29: RID deflection to external party

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 to not support supplementary services using UUI 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 QSIG 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*.

3.9.4 INTERWORKING WITH ASB 501 04

For the parameters SIG and VARC, see also the description in section General.

If the cooperating exchange is an ASB 501 04 R2 or earlier release, and ISDN is used, the VARC parameter for full ISDN functionality shall be set to **No.**

If the cooperating exchange is an ASB 501 04 R4 or R6, and ISDN is used, the VARC parameter for full ISDN functionality can be set to **Yes.** RID deflection is not supported, but RID deflection request or notification can be sent. In this case, the cooperating exchange will reject the service request/notification.

In the network configuration below, Node-B and Node-C are connected to Node-A. Node-A can, for example, be an ASB 501 04 R2 (or earlier release) using ISDN, or an ASB 501 04 using any other signaling system. Node-C is an MX-ONE, or a ASB 501 04 R6 or R4 using ISDN.

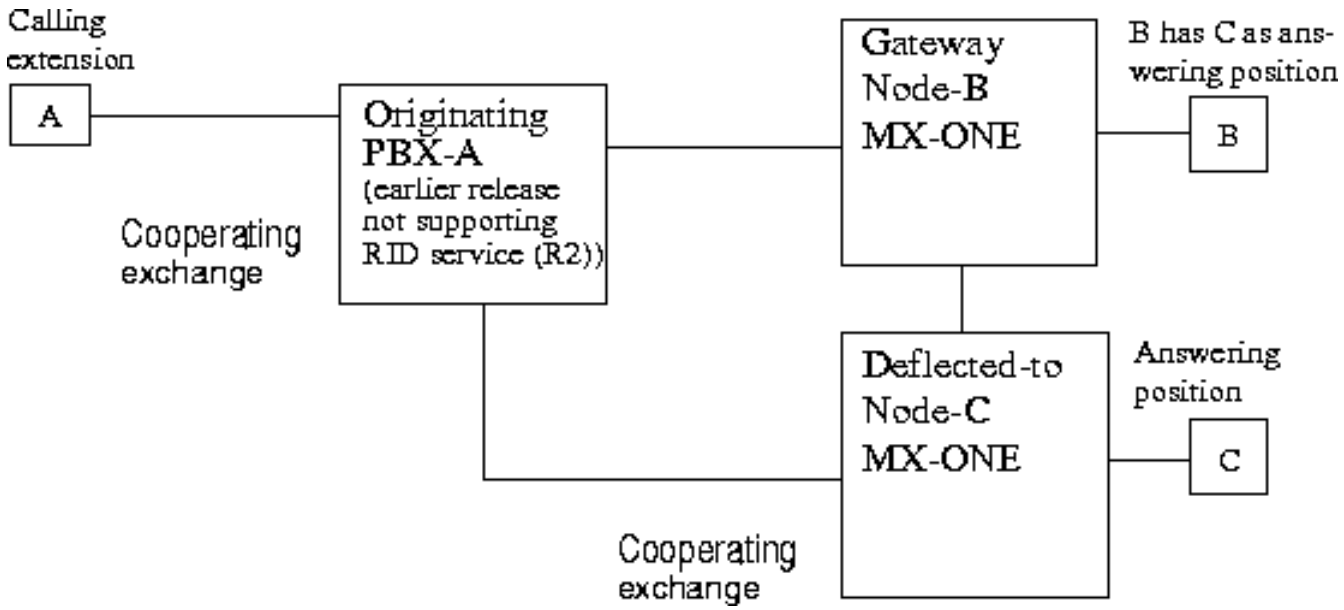


Figure 30: Earlier releases, RID deflection

Extension A in the originating node calls extension B. Extension B has the RID service activated and extension C as answering position in the deflected-to node.

After A has called extension B, the RID deflection will take place in Node-B. Node-B will in this case act as a gateway exchange for the RID service. This means that Node-B will continue with a new call set up to extension C in the deflecting exchange, that is, for earlier releases it is not possible to use the principle of returning to the originating Node-A and set up a new call to the deflected-to Node-C. As Node-C is an R6 release (which does not support RID service), it will not accept information about the service that is being executing (RID) and this call setup will be rejected. The deflecting node will then set up a second call towards the deflected-to Node-C, but this time without any RID service indication.

3.10 INTRUSION

3.10.1 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 is supported in a CCS network consisting of DPNSS tie lines or private homogeneous ISDN tie lines or ISDN public external lines (for VPN).

Intrusion is also supported in packet-switched networks consisting of private homogeneous H.323 tie lines, private mixed H.323/ISDN tie lines or H.323 public external lines (for VPN).

3.10.2 DPNSS/ISDN/H.323

For network Intrusion, network services must be supported, and there are several AS parameters which must be correctly set. For ISDN, Intrusion and Forced release work also if full ISDN functionality is set to **No**, when cooperating with an ASB 501 04 R2/n.

The Intrusion Capability Level (ICL) for the intruding party is set by the SERV parameter for the extension (*EX/KS* and *extension*). 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:

KSEXI*, *EXTEI*:...,SERV=...; or *extension_profile -i --ext-serv

The Intrusion Protection Level (IPL) for the intruded party is set by the SERV parameter for the extension (EX/KS) and by the --ext-serv parameter for Generic Extensions. The Intrusion Protection Level for the third party is set by the SERV (or --ext-serv) parameter for the extension. The PBX operator is totally barred, that is, has highest IPL.

The IPL for third party is sent for comparison to the terminating node after request from the terminating node. If it is not possible to fetch the IPL for the third party, the IPL is given with an AS parameter, *PARNUM = 130* in the terminating node. If Node-B is an ASB 501 04 R2 then ICL is set default to the highest value.

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 a SERV parameter 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

If 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.

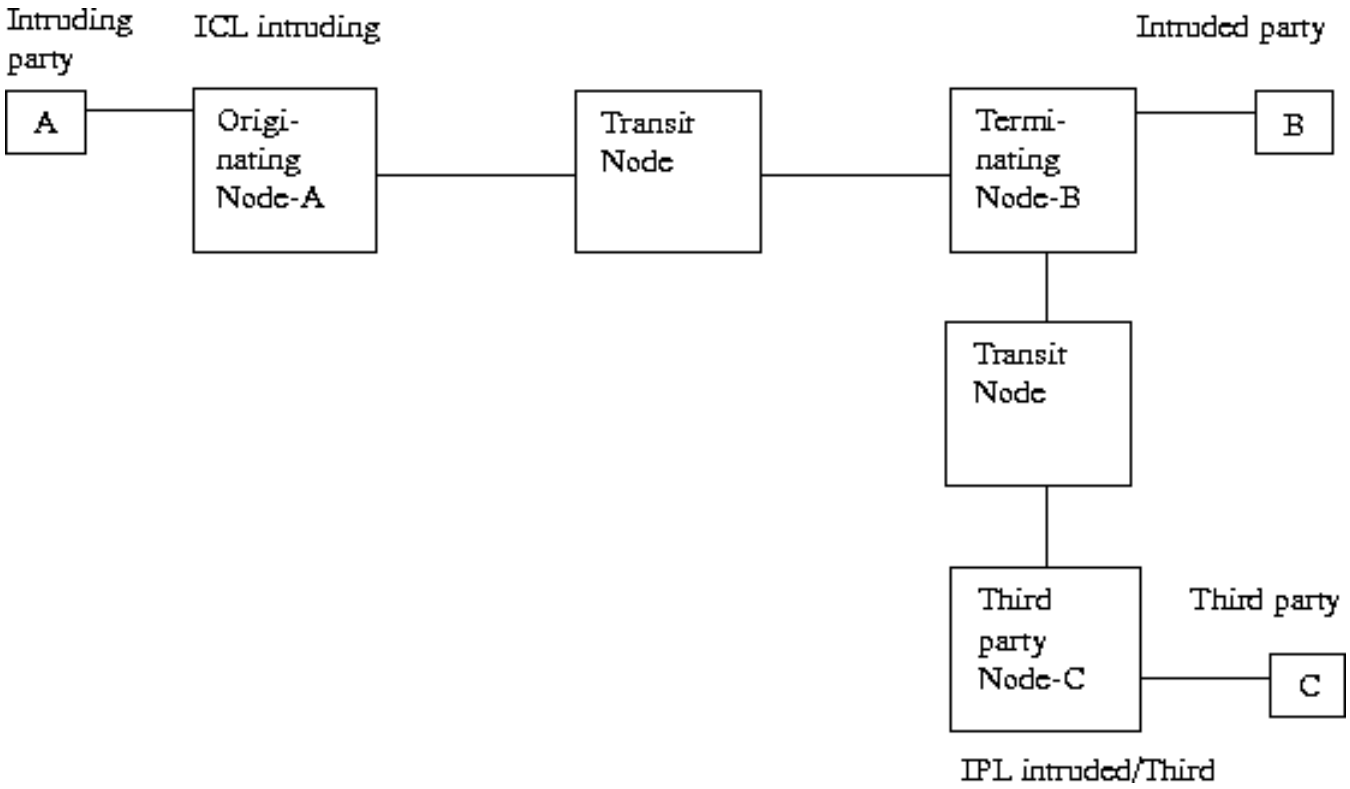


Figure 31: Intrusion

3.11 MALICIOUS CALL TRACING

3.11.1 GENERAL

Malicious Call Tracing, MCT, is a service that is used for tracing of malicious calls from the public ISDN network to a user in the MX-ONE. It is not supported in the private network, so it is not really networking, but still described here.

The tracing is activated by a procedure or programmable key (DTS). When activated it will cause an alarm and printout/log in the interworking exchange (in the public network). The printout/log will contain for example the calling number, dialled number, date and time.

Note: MCT is not possible in VPN calls.

3.11.2 PREREQUISITES, PROCEDURE

1. Initiate public ISDN route (RO)
2. Initiate digital extensions (KS)
3. Initiate analog extensions (EX)
4. Initiate generic extensions (extension)
5. Initiate/change application system parameter for MCT (AS)

3.11.3 EXECUTION

When the route is initiated (this is only valid for public ISDN routes), or at a later time by using the change command, set the SEL parameter to support MCT. Key the command:

***ROCAI* or *ROCAC*:...,SEL=...;**

To permit an extension to use the MCT service, a COS is required to be set. PBX operators are permitted to use MCT by default. The COS setting is done for analog extensions by keying the command:

***EXTEI* or *EXCAC*:...,ADC=...;**

COS setting is done for DTS extensions by keying the command:

***KSEXI* or *KSCAC*:...,ADC=...;**

plus *KSFKC* to initiate a FCN-key on the DTS.

COS setting is done for generic extensions by keying the command:

extension_profile -i* or *extension_profile -c with the **--ext-serv** parameter.

The results can be printed with the commands *ROCAP*, *EXCAP*, *KSCAP* and *extension_profile -p*.

Finally, set the application system parameters using command:

***ASPAC*:PARNUM=95,PARVAL=...;**

in order to select whether the MX-ONE or the public network shall generate the acknowledge/rejection tones for MCT, and select whether Call Information Logging shall set a condition code for MCT by keying:

***ASPAC*:PARNUM=135,PARVAL=...;**

The last parameter is *PARNUM=91*, which controls the time the call will be held if the external party attempts to go on-hook. Typically it can be 20 seconds, and must be shorter than the public exchange's timer. During this time MCT is possible to request. On time out the call will be released.

3.12 NAME IDENTIFICATION

Name Identification can be conveyed in a private ISDN network using Generic Functional Protocol according to ECMA or ISO and in a VPN scenario using UUI element. Name Identification can also use the UUI element in private networks.

Name Identification can also be conveyed in private H.323 networks, based on GFP, and in a VPN scenario, based on UUI. For ISDN-H.323 interworking 1.5 Interworking considerations in H.323 networks on page 15.

Name Identification can also be conveyed in public switch for the ISDN T1 with DMS-100 and the DMS-250 protocols.

In the VPN case, Name Identification will be the first information to be discarded if the UUI data are limited by the public ISDN.

The support for the standardized Generic Functional protocol must be initiated on each route that uses the standard protocols for Name Identification. This applies for private (tie line) routes. The support of the Generic Functional protocol is set per route in the VARI parameter for the command RODAI.

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

3.13 PATH REPLACEMENT

3.13.1 GENERAL

Path replacement is done to achieve the optimum path between two exchanges, and is a service which is automatically invoked by the network, not by a user.

Path replacement between exchanges can be desired when a direct route with free lines exists between two exchanges, but when the speech path is set up via another path through one or more other exchange(s).

Path replacement is only possible in a network with ISDN tie lines that supports the Standardized Generic Functional Protocol.

Path replacement is only applicable for voice calls in speech state.

Events that can lead to path replacement:

- Extending/transfer has occurred in another exchange
- Alternative routing
- Conference terminated with only two external parties remaining.

3.13.2 PREREQUISITES

The ISDN route must be set with the following data:

- The exchanges have been assigned own exchange number with the *global_traffic_data* command which must be external destination (ED) in the cooperating exchange.
- Netservices must be set to **Yes**.
- With an AS parameter, *PARNUM = 66* Route optimization availability must be set to available.
- Multiparty program and hardware must exist in the originating exchange.
- Route optimization program ROR/ROM must exist in the originating and terminating exchange.
- Code UUI in Generic Functional Protocol has to be set to **Yes**, if proprietary UUI signaling is used in the network. Set in parameter VARI in command *RODAI*.

The AS parameter, *PARNUM = 223*, Type of service in network has to be set to Path Replacement.

The following AS-values can be altered for Path replacement:

- With an AS parameter, *PARNUM = 71* stating Time before Route optimization starts when transfer, extending, and so on has been executed. Default value is 10 s.
- With an AS parameter, *PARNUM = 72* stating Time before restart of Route optimization when the request was denied. Default value is 60 s.
- With an AS parameter, *PARNUM = 73* stating Number of attempts to execute Route optimization when the request was denied. Default value is 3.

3.13.3 EXECUTION

The function for Path replacement is the same as for Route optimization.

3.14 PATH RETENTION

The retaining of the network connection between the Originating PINX and the Terminating PINX so that a supplementary service (such as SS-CO) can be invoked without establishing a new connection is known as Path Retention. This service is supported in ISDN and H.323 networks.

Path retention is a generic mechanism which is fully transparent to the user and can be used by supplementary services during call establishment. It is invoked by the Originating PINX either for one supplementary service or for several supplementary services at the same time.

Path Retention Invocation for a particular supplementary service means that the network connection is to be retained if the Terminating PINX encounters conditions in which it is appropriate to invoke that supplementary service. The Originating PINX is informed the reason for retaining the connection so that it can decide (for example, by consulting the calling user) whether to invoke the supplementary service.

Successive retentions of the network connection by the Terminating PINX following a single invocation of path retention by the Originating PINX are possible as a result of different conditions being encountered at the Terminating PINX.

No other specific I/O data are required for Path Retention, except that the type of protocol is set to use GFP for call offer for a particular destination.

3.15 REROUTING

Rerouting can be supported in a CCS network consisting of DPNSS tie lines, or an ISDN network. Rerouting is also possible in packet networks based on H.323 tie lines and/or H.323 public external lines, and even in mixed ISDN-H.323 networks (1.5 Interworking considerations in H.323 networks on page 15). The implementation is proprietary. See operational directions for *CENTRALIZED ANSWER POSITION* for details.

3.16 ROUTE OPTIMIZATION

3.16.1 GENERAL

Route optimization is done to achieve the optimum path between two exchanges, and is a service which is automatically invoked by the network, not by a user.

Route optimization between exchanges can be desired when a direct route with free lines exists between two exchanges, but when the speech path is set up via another path through one or more other exchange(s).

Route optimization is only possible in a CCS network consisting of DPNSS tie lines, or a **homogeneous** ISDN network.

Route optimization is only applicable for voice calls, in speech state.

Events that can lead to route optimization:

- Extending/transfer has occurred in another exchange
- Alternative routing
- Conference terminated with only two external parties remaining.

Route optimization between the exchanges means, for example, that a call from Node-A that is answered in exchange B, and thereafter transferred to Node-C shall

utilize the shortest path, that is, shall be set up directly between Node-A and C. The path through Node-B is then disconnected.

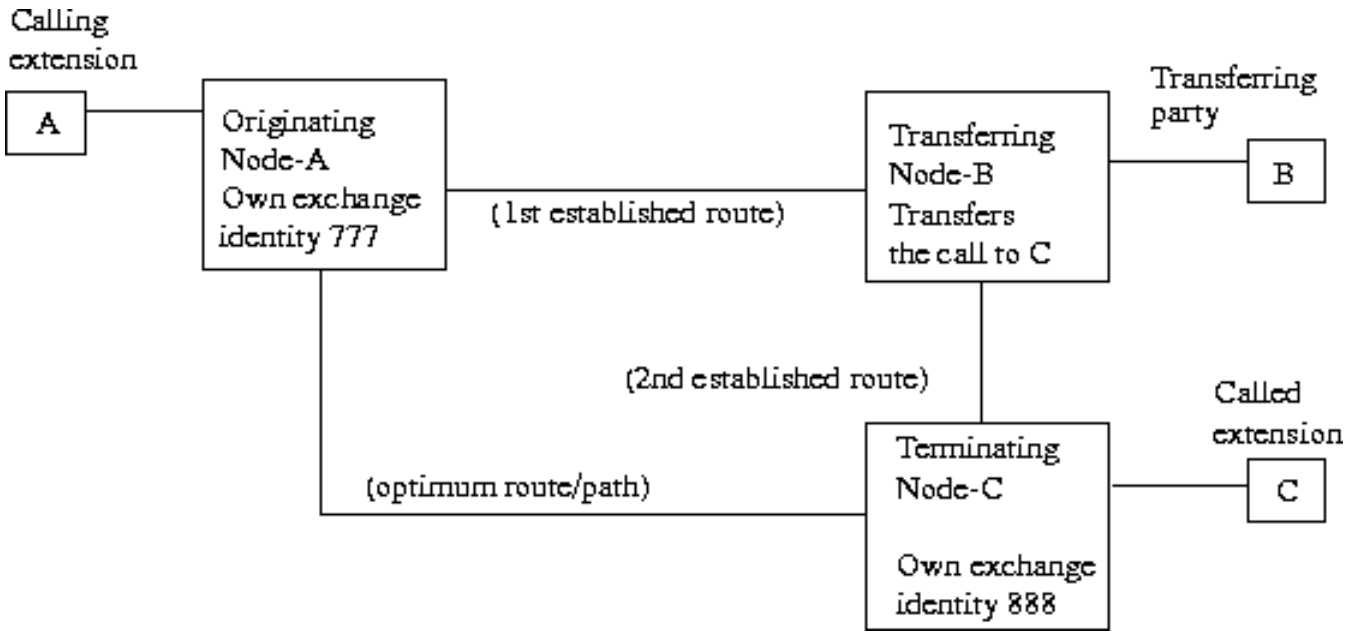


Figure 32: Route optimization

3.16.2 PREREQUISITES

- Shortest possible route between the exchanges can be seized (no alternative routing is allowed during the optimization attempt).
- The exchanges have been assigned own exchange number with the *global_traffic_data* command which must be external destination (ED) in the cooperating exchange.
- The exchanges belong to the same network.
- The route optimization function has been opened with an application system (AS) parameter.
- For ISDN, depending on the numbering plan and whether VPN is used, prefixes must have been initiated (RO-commands). This prefix together with the system identity number set with *global_traffic_data* command must be in the public DID number series, see operational directions for *NUMBERING*.
- Multi-party program and hardware exist in the originating exchange.
- Route optimization program exists in the originating and terminating exchange.

3.16.3 INITIATING ROUTE OPTIMIZATION RELATED DATA

The following AS-values are used for route optimization:

PARNUM=66, Route optimization permitted or not permitted.

PARNUM=70, Time delay for start of route optimization after alternative routing (60 s recommended).

PARNUM=71, Time delay for start of route optimization (10 s recommended).

PARNUM=72, Time before restart of route optimization when the request was denied.

PARNUM=73, Number of attempts to execute route optimization when the request was denied.

Example of initiation of Route optimization for non-VPN scenario

Originating exchange

***number_initiate* -number 777 -numbertype en** Own exchange-number within private network.

global_traffic_data -c --system_exchange_identity 777 System data, own exchange-number.

***ASPAC*:PARNUM=66,PARVAL=1;** Route optimization allowed.

Terminating exchange

***number_initiate* -number 777 -numbertype ed** Optimal destination code towards PBX 777.

***RODDI*:DEST=777;** Connection to the optimal route.

***ASPAC*:PARNUM=66,PARVAL=1;** Route optimization allowed.

Example of initiation of Route optimization for ISDN VPN scenario

Originating exchange

***number_initiate* -number 777 -numbertype en**

Own PBX-number within private network. This number must belong to the DID number series if VPN scenarios shall be possible to support.

global_traffic_data -c --system_exchange_identity 777 System data, own exchange-number.

***ASPAC*:PARNUM=66,PARVAL=1;** Route optimization allowed.

When ISDN is used, the own exchange number is possible to prefix for the route.

Terminating exchange

***number_initiate* -number 777 -numbertype ed** Optimal destination code towards node 777.

***RODDI*:DEST=777;** Connection to the optimal route.

***ASPAC*:PARNUM=66,PARVAL=1;** Route optimization allowed.

Transit. Transferring exchange

No specific initiations for route optimization but general prerequisites, like route access codes, and network service support must be initiated.

3.17 TRANSFER (PROPRIETARY SIGNALING)

3.17.1 GENERAL

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

Transfer is a proprietary service supported in ISDN and H.323 networks:

- In ISDN networks, proprietary UUI signaling is used.

- In H.323 networks, transfer in MX-ONE is supported in two proprietary formats: based on GFP and based on UUI (both are supported via the nonStandardControl information element).

  Transfer based on GFP can interwork with the ISDN ISO QSIG Call transfer.

  Transfer based on UUI can interwork with the ISDN transfer in MX-ONE described here.

The transfer can be made before or after answer.

3.17.2 PREREQUISITES

3.17.2.1 ISDN routes

The ISDN route must be set with the following data:

- Network services must be set to **Yes**. Set in parameter SIG in command *ROCAI*.
- Full ISDN functionality must be set to **Yes**. Set in parameter VARC in command *RODAI*.

The AS parameter, *PARNUM = 223*, Type of service in network has to be set to Transfer.

The following parameters can be altered for Transfer in an MX-ONE and ASB 501 04 network:

- 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 for transfer before answer in the *global_traffic_data* commands is set to allow transfer before answer.

3.17.2.2 H.323 routes (based on UUI)

The route must be set with the following data:

- Network services must be set to **Yes**. Set in parameter SIG in command *ROCAI*.

The AS parameter, *PARNUM = 223*, Type of service in network has to be set to Transfer based on UUI (0).

The following parameters can be altered for Transfer in an MX-ONE network:

- 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 transfer before answer in the *global_traffic_data* commands is set to allow transfer before answer.

3.17.2.3 H.323 routes (based on GFP)

The route must be set with the following data:

- Network services must be set to **Yes**. Set in parameter SIG in command *ROCAI*.

The AS parameter, *PARNUM = 223*, Type of service in network has to be set to Transfer based on GFP (2).

The following parameters can be altered for Transfer in an MX-ONE network:

- 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 transfer before answer in the *global_traffic_data* commands is set to allow transfer before answer.

3.17.3 EXECUTION

The procedure for Transfer in MX-ONE network is the same as for Call transfer, see directions for use for the appropriate extension type.

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.