Aastra Business Communication Systems

Private Netorking with Aastra 400

System Manual

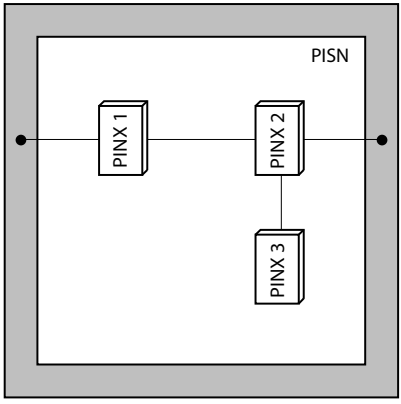
Supported platforms:

Aastra 415/430

Aastra 470

This document describes the networking possibilities of several communication servers to one private network (PISN). Homogeneous networks with Aastra 400 communication server can also be created just like heterogeneous networks with third-party systems.

The document is intended for planners, installers and system managers of telephone installations.



syd-0551_en / 1.0 – R1 – © 12.2014

Content

1	**Product and Safety Information**	**5**
1. 1	Product information	5
1. 2	Safety Information	7
1. 3	Data protection	8
1. 4	About this document	9
1. 5	Limited Warranty (Australia only)	10
1. 6	About Aastra	13
2	**Private ISDN-Based Network (PISN)**	**14**
2. 1	Networking variants (topologies)	16
2. 1. 1	QSIG networking via the IP network	16
2. 1. 2	Leased-line Networking (Leased-line Network)	17
2. 1. 3	Virtual networking (virtual network)	19
2. 1. 4	Combining Leased-line and Virtual Networking	20
2. 1. 5	Virtual networking with virtual communication server	21
2. 2	Choosing the right networking type	22
2. 3	Communication protocols	23
2. 3. 1	Protocol and topology type	23
2. 3. 2	Connection between Protocol and Range of Services Available	25
2. 4	Connecting PISN nodes	25
2. 4. 1	Connection via Basic and Primary Rate Access	25
2. 4. 2	Connection via Ethernet	27
2. 5	Numbering Plan and Regions	28
2. 5. 1	Shared Numbering Plan	28
2. 5. 2	PISN with Regions	29
2. 5. 2. 1	Numbering Plan for Two Regions	31
2. 5. 2. 2	Call Routing in Regions	32
2. 6	Services and Functions	34
2. 6. 1	Network services	34
2. 6. 2	Other services	35
2. 6. 3	Break-out	37
2. 6. 4	Break-In for virtual PISN users	38
2. 7	Glossary	38

3	**Planning a private network**	**41**
3. 1	Planning aid	41
3. 1. 1	Specify the nodes	42
3. 1. 2	Past traffic volume	42
3. 1. 3	Routing in a private network	43
3. 1. 3. 1	Connections between nodes	44
3. 1. 3. 2	Accesses to the public network	44
3. 1. 3. 3	Traffic volume in the private network	45
3. 1. 3. 4	Determining the B channels	45
3. 1. 4	Connection between permanently networked nodes	45
3. 1. 4. 1	Connections with primary rate accesses	46
3. 1. 4. 2	Connections with basic accesses	47
3. 1. 5	Protocols and licences	48
3. 1. 6	Reliability aspects	49
3. 1. 7	Synchronization	50
3. 1. 7. 1	Clock propagation diagram	50
3. 1. 7. 2	Planning rules	53
3. 1. 8	Numbering	54
3. 1. 8. 1	Numbering with blocks (shared numbering plan)	55
3. 1. 8. 2	Numbering with regions	56
3. 1. 9	Link-up to a public network	57
3. 1. 9. 1	Direct dialling in at the gateway PINX	59
3. 1. 9. 2	Identification of calls to the public network	60
3. 1. 9. 3	Definition of the transit route	61
3. 2	Example of networking	61
3. 2. 1	Creating the routes	63
3. 2. 1. 1	Replicating the nodes on routes	63
3. 2. 1. 2	Defining the routes to the public network	64
3. 2. 2	Creating the trunk groups	65
3. 2. 2. 1	Creating the trunk groups between the nodes	65
3. 2. 2. 2	Creating the exchange trunk group	65
3. 2. 3	Route configuration	66
3. 2. 4	Creating the numbering plan	69
3. 2. 4. 1	Numbering with blocks	69
3. 2. 4. 2	Numbering with regions	72
3. 2. 5	Setting up direct dialling in	76
3. 3	Networking via a public network	77
3. 3. 1	Tying-in an individual user	77
3. 3. 2	Networking two nodes	79
3. 4	Networking with a virtual communication server	81
3. 5	Networking with third-party systems	83

4	**SIP Networking**	**86**
4. 1	Introduction	86
4. 2	SIP networking with two nodes	87
4. 3	SIP networking with several nodes	90
4. 4	Features supported	90

1 Product and Safety Information

Here you will find information relating to safety, data protection and legal matters besides product and documentation information.

Please read through the product and safety information carefully.

1. 1 Product information

Purpose and function

Aastra 400 is an open, modular and comprehensive communication solution for the business sector with several communication servers of different performance and expansion capacity, an extensive telephone portfolio and a multitude of expansions. They include an application server for unified communications and multimedia services, an FMC controller for mobile phone integration, an open interface for application developers, and a multitude of expansion cards and modules.

The business communication solution with all its elements was designed to cover the full spectrum of communication requirements of businesses and organizations in a user and maintenance-friendly way. The individual products and parts are coordinated and cannot be used for other purposes or replaced by outside products or parts (except to connect up other authorized networks, applications and phones to the interfaces certified for that purpose).

User groups

The phones, soft phones and PC applications of the Aastra 400 communication solution are particularly user friendly in design and can be used by all end users without any specific product training.

The phones and PC applications for professional applications such as PC operator consoles or call centre applications require training of the end user.

Specialist knowledge of IT and telephony is assumed for the planning, installation, configuration, commissioning and maintenance. Regular attendance at product training courses is strongly recommended.

User information

Aastra 400 Products are supplied complete with safety and product information, Quick User's Guides and User's Guides.

These and all other user documents such as system manuals are available for download from the Aastra 400 DocFinder as individual documents or as a documentation set. Some user documents are accessible only via a partner login.

It is your responsibility as a specialist retailer to keep up to date with the scope of functions, the proper use and the operation of the Aastra 400 communication solution and to inform and instruct your customers about all the user-related aspects of the installed system:

- Please make sure you have all the user documents required to install, configure and commission an Aastra 400 communication system and to operate it efficiently and correctly.
- Make sure that the versions of the user documents comply with the software level of the Aastra 400 products used and that you have the latest editions.
- Always read the user documents first before you install, configure and put an Aastra 400 communication system into operation.
- Ensure that all end users have access to the User Guides.

Aastra 400 DocFinder: www.aastra.com/DocFinder

Conformity

Aastra Telecom Schweiz AG hereby declares that

- the Aastra 400 products conform to the basic requirements and other relevant stipulations of Directive 1999/5/EC.
- all our products are manufactured in conformity with RoHS and WEEE (2002/95/EC and 2002/96/EC).

The product-specific declarations of conformity can be found on the Aastra 400 DocFinder.

Trademarks

Aastra® is a registered trademark of Aastra Technologies Limited.

All other trademarks, product names and logos are trademarks or registered trademarks of their respective proprietors.

Use of third-party software

Aastra 400 products comprise, or are partially based on, third-party software products. The licence information for these third-party products is given in the user's guide of the Aastra 400 product in question.

Exclusion of Liability

(Not valid for Australia. See Chapter on the limited warranty in Australia.)

All parts and components of the Aastra 400 communication solution are manufactured in accordance with ISO 9001 quality guidelines. The relevant user information has been compiled with the utmost care. The functions of the Aastra 400 products have been tested and approved after comprehensive conformity tests. Nonetheless errors cannot be entirely excluded. The manufacturers shall not be liable for any direct or indirect damage that may be caused by incorrect handling, improper use, or any other faulty behaviour. Potential areas of particular risk are signalled in the appropriate sections of the user information. Liability for loss of profit shall be excluded in any case.

Environment

Aastra 400 products are delivered in recycled, chlorine-free corrugated cardboard packaging. The parts are also wrapped inside a protective fleece made of polyethylene foam fleece or polyethylene film for added protection during shipping. The packaging is to be disposed of in accordance with the guidelines stipulated under current legislation.

Aastra 400 products contain plastics based on a pure ABS, sheet steel with an aluminium-zinc or zinc finish, and epoxy resin-based PCBs. These materials are to be disposed of in accordance with the guidelines stipulated under current legislation.

Aastra 400 products are disassembled exclusively using detachable screwed connections.

1. 2 Safety Information

Reference to hazards

Hazard warnings are affixed whenever there is a risk that improper handling may put people at risk or cause damage to the Aastra 400 product. Please take note of these warnings and follow them at all times. Please also take note in particular of hazard warnings contained in the user information.

Operating safety

Aastra 400 communication servers are operated on 230 VAC mains power. Communication servers and all their components (e.g. telephones) will not operate when mains power fails. Interruptions in the power supply will cause the entire system to restart. A UPS system has to be connected up-circuit to ensure an uninterruptible

power supply. Up to a specific performance limit a Aastra 470 communication server can also be powered redundantly using an auxiliary power supply. For more information please refer to your communication server's system manual.

When the communication server is started for the first time, all the configuration data is reset. You are advised to backup your configuration data on a regular basis as well as before and after any changes.

Installation and operating instructions

Before you begin with the installation of the Aastra 400 communication server:

- Check that the delivery is complete and undamaged. Notify your supplier immediately of any defects; do not install or put into operation any components that may be faulty.
- Check that you have all the relevant user documents at your disposal.
- During the installation follow the installation instructions for your Aastra 400 product and observe to the letter the safety warnings they contain.

Any servicing, expansion or repair work is to be carried out only by technical personnel with the appropriate qualifications.

1. 3 Data protection

Protection of user data

During operation the communication system records and stores user data (e.g. call data, contacts, voice messages, etc.). Protect this data from unauthorised access by using restrictive access control:

- For remote management use SRM (Secure IP Remote Management) or set up the IP network in such a way that from the outside only authorised persons have access to the IP addresses of the Aastra 400 products.
- Restrict the number of user accounts to the minimum necessary and assign to the user accounts only those authorisation profiles that are actually required.
- Instruct system assistants to open the remote maintenance access to the communication server only for the amount of time needed for access.
- Instruct users with access rights to change their passwords on a regular basis and keep them under lock and key.

Protection against listening in and recording

The Aastra 400 communication solution comprises features which allow calls to be monitored or recorded without the call parties noticing. Inform your customers that these features may only be used in compliance with national data protection provisions.

Unencrypted phone calls made in the IP network can be recorded and played back with the right equipment:

- Use encrypted voice transmission whenever possible.
- For WAN links used for transmitting calls from IP or SIP phones, use preferably either the customer's own dedicated leased lines or VPN encrypted connection paths.

1.4 About this document

This document describes the networking possibilities of several communication servers to one private network (PISN). Homogeneous networks with Aastra 400 communication server can also be created just like heterogeneous networks with third-party systems. The document is intended for planners, installers and system managers of telephone installations. A basic knowledge of telephony, in particular of ISDN and IP technology, is required to understand the content of the System Manual.

This document does not describe networking to an Aastra Intelligent Net (AIN). AIN networks several Aastra 400 communication servers into a single fully-fledged Aastra 400system with a complete range of features.

Document information

- Document number: syd-0551
- Document version: 1.0
- Valid as of: R1
-
- In PDF Viewer, click on this link to download the latest version of this document: *https://pbxweb.aastra.com/doc_finder/DocFinder/syd-0551_en.pdf?get&DNR=syd-0551*

1. 5 Limited Warranty (Australia only)

The benefits under the Aastra Limited Warranty below are in addition to other rights and remedies to which you may be entitled under a law in relation to the products.

In addition to all rights and remedies to which you may be entitled under the Competition and Consumer Act 2010 (Commonwealth) and any other relevant legislation, Aastra warrants this product against defects and malfunctions in accordance with Aastra's authorized, written functional specification relating to such products during a one (1) year period from the date of original purchase ("Warranty Period"). If there is a defect or malfunction, Aastra shall, at its option, and as the exclusive remedy under this limited warranty, either repair or replace the product at no charge, if returned within the warranty period.

Repair Notice

To the extent that the product contains user-generated data, you should be aware that repair of the goods may result in loss of the data. Goods presented for repair may be replaced by refurbished goods of the same type rather than being repaired. Refurbished parts may be used to repair the goods. If it is necessary to replace the product under this limited warranty, it may be replaced with a refurbished product of the same design and colour.

If it should become necessary to repair or replace a defective or malfunctioning product under this warranty, the provisions of this warranty shall apply to the repaired or replaced product until the expiration of ninety (90) days from the date of pick up, or the date of shipment to you, of the repaired or replacement product, or until the end of the original warranty period, whichever is later. Proof of the original purchase date is to be provided with all products returned for warranty repairs.

Exclusions

Aastra does not warrant its products to be compatible with the equipment of any particular telephone company. This warranty does not extend to damage to products resulting from improper installation or operation, alteration, accident, neglect, abuse, misuse, fire or natural causes such as storms or floods, after the product is in your possession. Aastra will not accept liability for any damages and/or long distance charges, which result from unauthorized and/or unlawful use.

To the extent permitted by law, Aastra shall not be liable for any incidental damages, including, but not limited to, loss, damage or expense directly or indirectly arising from your use of or inability to use this product, either separately or in combination with other equipment. This paragraph, however, is not intended to have

the effect of excluding, restricting or modifying the application of all or any of the provisions of Part 5-4 of Schedule 2 to the Competition and Consumer Act 2010 (the ACL), the exercise of a right conferred by such a provision or any liability of Aastra in relation to a failure to comply with a guarantee that applies under Division 1 of Part 3-2 of the ACL to a supply of goods or services.

This express warranty sets forth the entire liability and obligations of Aastra with respect to breach of this express warranty and is in lieu of all other express or implied warranties other than those conferred by a law whose application cannot be excluded, restricted or modified. Our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and for compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure.

Warranty Repair Services

Procedure: Should the product fail during the warranty period and you wish to make a claim under this express warranty, please contact the Aastra authorized reseller who sold you this product (details as per the invoice) and present proof of purchase. You will be responsible for shipping charges, if any.

Limitation of liability for products not of a kind ordinarily acquired for personal, domestic or household use or consumption (e.g. goods/services ordinarily supplied for business-use).

Tab. 1 Limitation of liability

1.1		To the extent permitted by law and subject to clause 1.2 below, the liability of Aastra to you for any non-compliance with a statutory guarantee or loss or damage arising out of or in connection with the supply of goods or services (whether for tort (including negligence), statute, custom, law or on any other basis) is limited to:
	a)	in the case of services:
		i) the resupply of the services; or
		ii) the payment of the cost of resupply; and
	b)	in the case of goods:
		i) the replacement of the goods or the supply of equivalent goods; or
		ii) the repair of the goods; or
		iii) the payment of the cost of replacing the goods or of acquiring equivalent goods; or
		iv) the payment of the cost of having the goods repaired.
1.2		Clause 1.1 is not intended to have the effect of excluding, restricting or modifying:
	a)	the application of all or any of the provisions of Part 5-4 of Schedule 2 to the Competition and Consumer Act 2010 (the ACL); or

b) the exercise of a right conferred by such a provision; or

c) any liability of Aastra in relation to a failure to comply with a guarantee that applies under Division 1 of Part 3-2 of the ACL to a supply of goods or services.

After Warranty Service

Aastra offers ongoing repair and support for this product. If you are not otherwise entitled to a remedy for a failure to comply with a guarantee that cannot be excluded under the Australian Consumer Law, this service provides repair or replacement of your Aastra product, at Aastra's option, for a fixed charge. You are responsible for all shipping charges. For further information and shipping instructions contact:

Tab. 2 Manufacturer

Manufacturer:	Note:
Aastra Telecom Australia Pty Ltd ("Aastra") Level 12, 45 William Street Melbourne, Victoria 3000, Australia, ABN: 16 140 787 195 Phone: +61 3 8628 9500	Repairs to this product may be made only by the manufacturer and its authorized agents, or by others who are legally authorized. Unauthorized repair will void this express warranty.

1.6 About Aastra

Aastra Technologies Limited is one of the world's leading manufacturers of communication systems. When developing products and solutions the prime objective is always to optimise the communication processes of small, medium and large companies and cut costs as a result.

Aspects of modern office communications such as mobility, future viability, security and availability are as much an integral part of the development work as user friendliness and product design. The offer covers the entire range of VoIP and SIP solutions, including communication servers, gateways, system phones and process-oriented software solutions.

With its pioneering innovations Aastra consistently promotes the convergence of voice and data communications in its solutions. Aastra's clientele includes acknowledged telephone and data network operators in North America, Europe and Africa as well as Internet Service Providers and distributors of renown.

Aastra Technologies Limited, (TSX: "AAH"), is a leading company at the forefront of the enterprise communication market. Headquartered in Concord, Ontario, Canada, Aastra develops and delivers innovative communication products and applications for businesses. Aastra's operations are truly global with more than 50 million installed lines around the world and a direct and indirect presence in more than 100 countries. Aastra is entirely dedicated to enterprise communications and offers one of the most complete portfolios of unified communications solutions individually tailored to satisfy its customers' requirements. These range from feature-rich call managers for small and medium businesses and highly scalable ones for large enterprises, integrated mobility, call centre solutions to a wide selection of phones. With a strong focus on open standards, Aastra enables enterprises to communicate and collaborate more efficiently.

For additional information on Aastra, visit our website: www.aastra.com.

2 Private ISDN-Based Network (PISN)

This chapter contains the basic information about creating a private network with Aastra 400 communication server.

A private network based on the ISDN standard is referred to as a PISN (Private Integrated Services Network). Its characteristic feature is that all connected users can communicate with one another in the same way as internal users. This applies to both voice traffic and to ISDN-based data traffic. A PISN is the keystone of any corporate communication structure optimized in terms of flexibility, user convenience and cost.

A PISN consists of several interconnected communication servers which form the network node. The PISN can be meshed or star-shaped. Hybrid forms are also possible.

Usually a PISN is connected to the public network in at least 1 place.

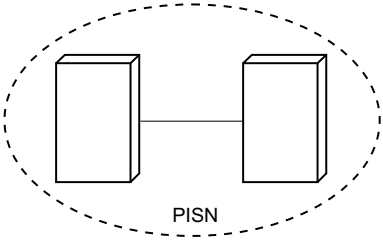


Fig. 1 PISN with at least two nodes

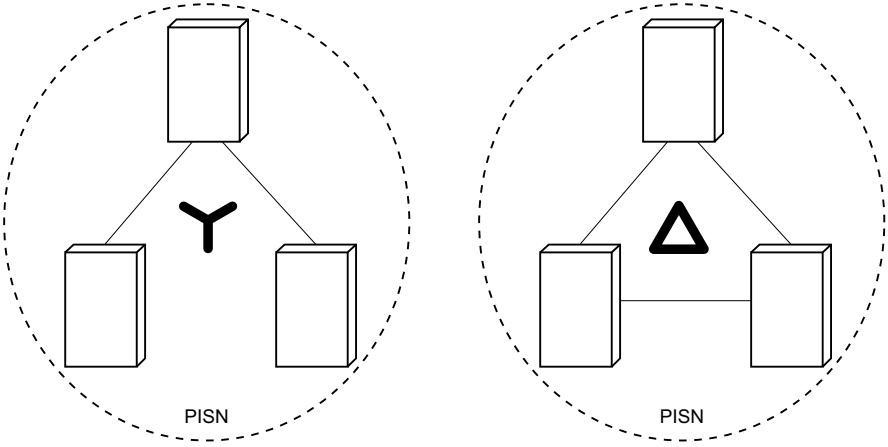


Fig. 2 Star-shaped and meshed PISN

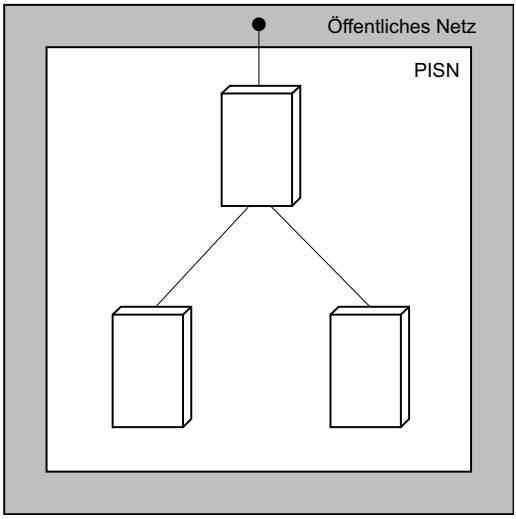


Fig. 3 A PISN usually has at least 1 connection to the public network

Networking Philosophy

Owing to the Aastra 400 communication server's sophisticated networking options, it is possible to set up a whole range of private networks (PISN). Homogeneous networks with Aastra 400 communication server can also be created just like heterogeneous networks with third-party communication servers.

The Aastra 400 networking philosophy is based on the assumption that the user does not need any prior knowledge of the network topology. He can use the available features always in the same way, regardless of whether and how he is networked.

Homogeneous and heterogeneous PISN

Each communication server in the PISN is a node. Nodes are called PINX (Private Integrated Services Network eXchange) in the network terminology: A PINX can be set up with the following communication servers:

- Aastra 400 communication server
- Third-party communication servers
- Virtual communication servers (private numbering plan from a public network provider)

In a homogeneous network all the Aastra 400 PINXs are communication servers. If communication servers from other manufacturers are also used in a network, we talk of a heterogeneous network.

2. 1 Networking variants (topologies)

Taking technical, organizational and tariff conditions into account calls for a flexible networking concept so that optimum customer solutions can be implemented. Other factors that influence the choice of networking type are the density and nature of the communication relations.

Supported networking variants

The following standardised PISN (Private Integrated Services Network) variants are supported:

- QSIG networking over IP network (see page 16):
- QSIG networking via ISDN leased lines (leased-line networking, see page 17):
- Virtual networking via public ISDN (see page 19).

Hybrid forms are also possible. Instructions on how to choose the right network variants is given in "Choosing the right networking type", page 22).

Additional PISN notes can be found in the system manual "System functions and Features".

The fully integrated networking of Aastra 400 communications server to an Aastra Intelligent Net (AIN) is described in a separate manual and not in the present manual.

2. 1. 1 QSIG networking via the IP network.

With QSIG networking over IP network voice data and QSIG signalling are transmitted on the Intranet as IP data packets. The intranet with QSIG / PSS1 supports the same scope of features as networking via leased lines ("QSIG tunnelling").

If an existing intranet can be used for voice connection (QoS must be supported), ISDN network call charges do not apply (tollbypass). If all the voice channels are busy, the calls can automatically be routed via the ISDN network (see system manual "Features of Aastra IntelliGate").

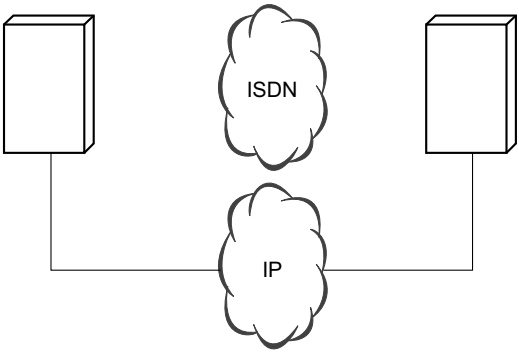
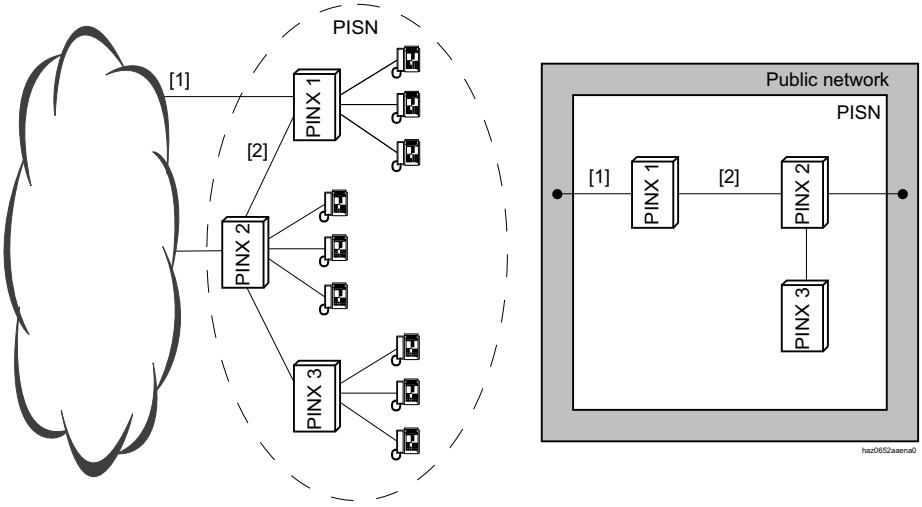


Fig. 4 QSIG via the IP network

2. 1. 2 Leased-line Networking (Leased-line Network)

With leased line networking the PINXs are connected via dedicated or leased lines. The characteristics of this type of networking are:

- fixed line resources
- fixed costs



[1] Connection to the public network

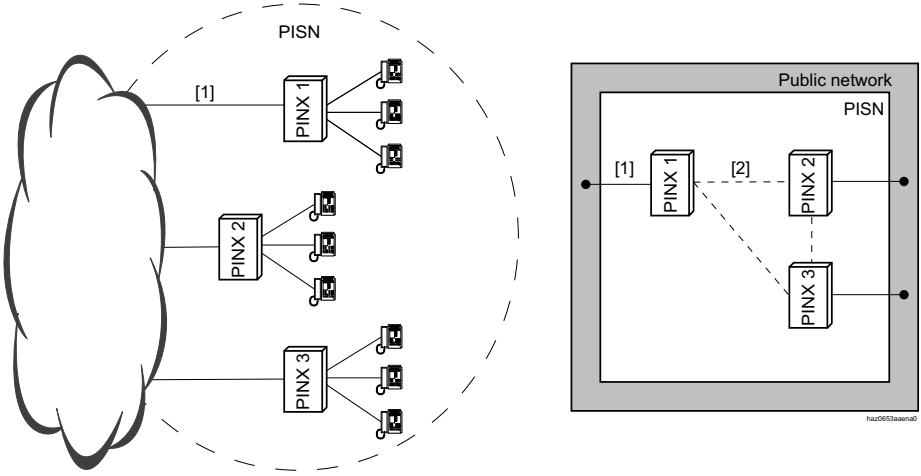
[2] Physical connection between two PINXs

Fig. 5 [2]Physical connection between two PINXs

2. 1. 3 Virtual networking (virtual network)

With virtual networking all the PINXs are connected via the public ISDN network. The connections between PINXs are dial-up connections, no direct physical connections. The characteristics of this type of networking are:

- Line resources are required for the current connections only.
- Voice and data traffic via the public network is charged according to duration and distance.
- The necessary networking-specific equipment is minimal.
- The range of services available in a virtual network depends on the range of services offered by the network provider.



[1] Connection to the public network

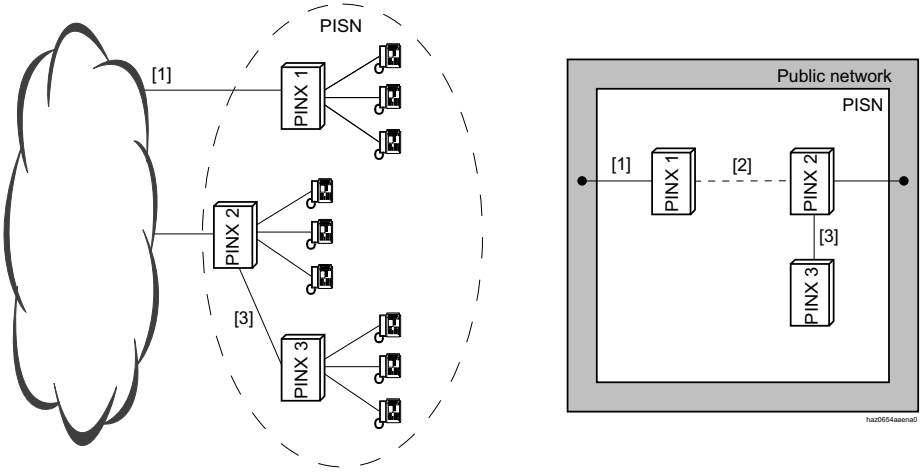
[2] Virtual connection between two PINXs

Fig. 6 Example of a virtual network

In this example (Fig. 6) all three PINXs are virtually interconnected via the public virtual network. This depends on the configuration. If for example there is no need for a virtual connection between PINX 1 and PINX 3, the configuration can be implemented accordingly.

2. 1. 4 Combining Leased-line and Virtual Networking

Leased-line and virtual networking can also be combined within a PISN.



[1] Connection to the public network

[2] Virtual connection between two PINXs

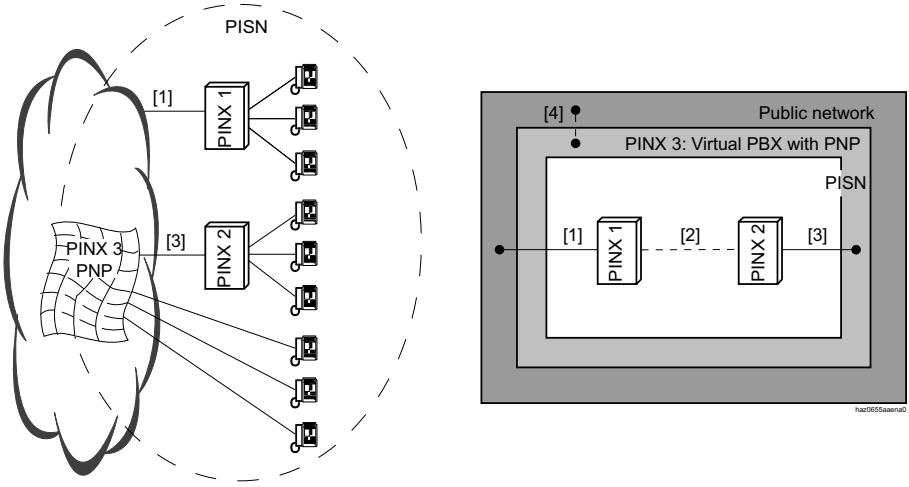
[3] Physical connection between two PINXs

Fig. 7 Example of a combined network

2. 1. 5 Virtual networking with virtual communication server

Some network providers offer a private numbering plan (PNP) as a service. Together with ISDN supplementary services, e. g. rerouting services, this means that the customer has a virtual communication server at his disposal.

A virtual communication server can easily be integrated as a PINX in a PISN. Aastra 400 Communication servers support external private numbering plans and can be seamlessly integrated into an own network function.



[1] Connection to the public network

[2] Virtual connection between two PINXs

[3] Physical connection to a virtual communication server on the public network

[4] Virtual connection between a virtual PINX and the public network

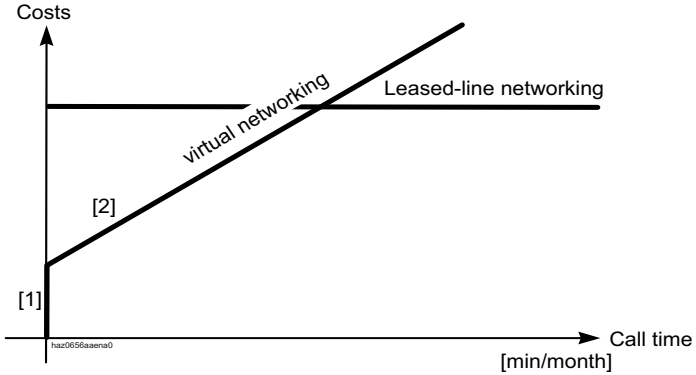
Fig. 8 Example of a virtual network with a virtual communication server

2. 2 Choosing the right networking type

The choice of the appropriate topology depends on the following factors, among others:

- Number of locations
- Distance between the locations
- Calling rate between the locations
- Networking equipment required
- IP network
- Scope of performance required

With virtual networking, the costs incurred consist of the basic charge for connections and DDI numbers and the charges per call, while a dedicated line incurs only fixed costs (for the rental of the leased line, for example). The following comparison (Fig. 9) shows that virtual networking is better suited to systems with lower calling rates while networking with leased lines can be more advantageous for higher calling rates.
As Fig. 7 shows, combinations of both networking types are also possible.



[1] Basic charge

[2] Charges per call and time unit

Fig. 9 Cost structure between leased-line and virtual networking

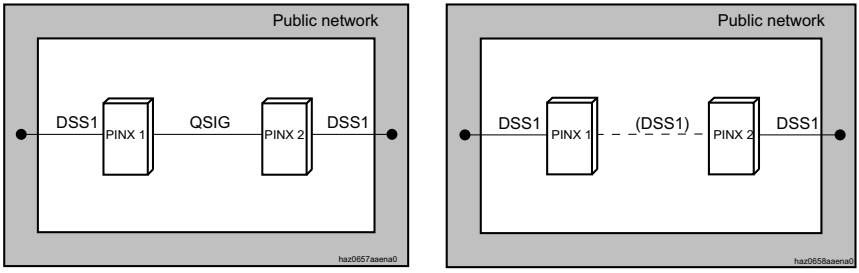
2. 3 Communication protocols

Aastra 400 communication servers support the two main protocols for setting up a PISN:

- The ISDN protocol DSS1 is used mainly in virtual networks.
- The QSIG / PSS1 protocol is based on an international standard that is supported by all leading providers. QSIG / PSS1 is used to set up private networks with very high performance and capacity.

2. 3. 1 Protocol and topology type

Aastra 400 communication servers support any combination of protocol and topology type. Normally, however, the QSIG / PSS1 protocol is used for leased-line networking and the DSS1 protocol for virtual networking.



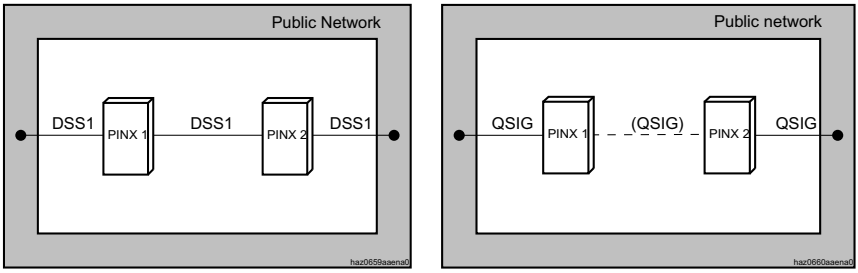
[1] [2]

[1] QSIG / PSS1 protocol in a leased-line network

[2] DSS1 protocol in a virtual network

Fig. 10 Normally used protocols

In special cases the DSS1 protocol can also be used for leased-line networking and the QSIG / PSS1 protocol for virtual networking.



[1] [2]

[1] DSS1 protocol in a leased-line network

[2] QSIG / PSS1 protocol in a virtual network

Fig. 11 Protocols used in special cases

If different topologies are combined within a PISN, then different protocols are normally also used.

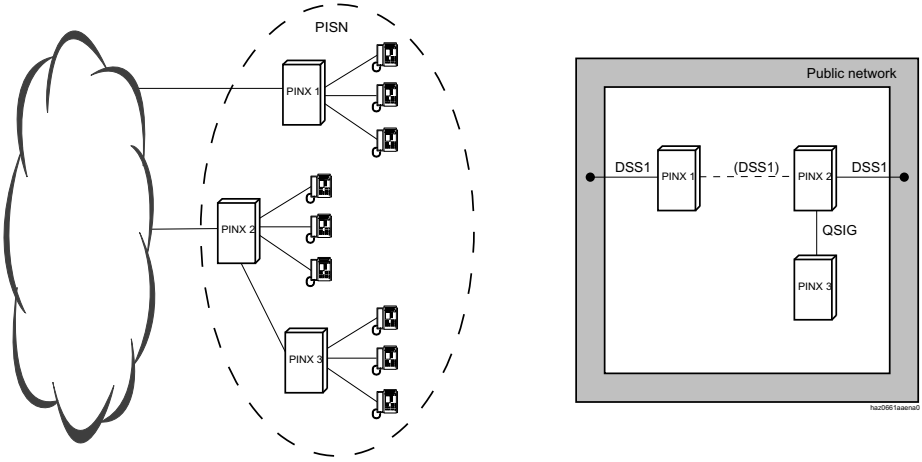


Fig. 12 Combined network: Combined network: virtual connections with DSS1, fixed connections with QSIG / PSS1

2. 3. 2 Connection between Protocol and Range of Services Available

The range of services available in a PISN is determined by the protocol used and the local features of the communication server. The services offered under QSIG / PSS1 and DSS1 differ only marginally. With virtual networking the range of services available also depends on the public network provider. Aastra 400 Communication servers support a multitude of the ISDN services on offer and combine them effectively with its own features.

Digital networking is based on the ISDN standard and therefore supports both voice and data traffic.

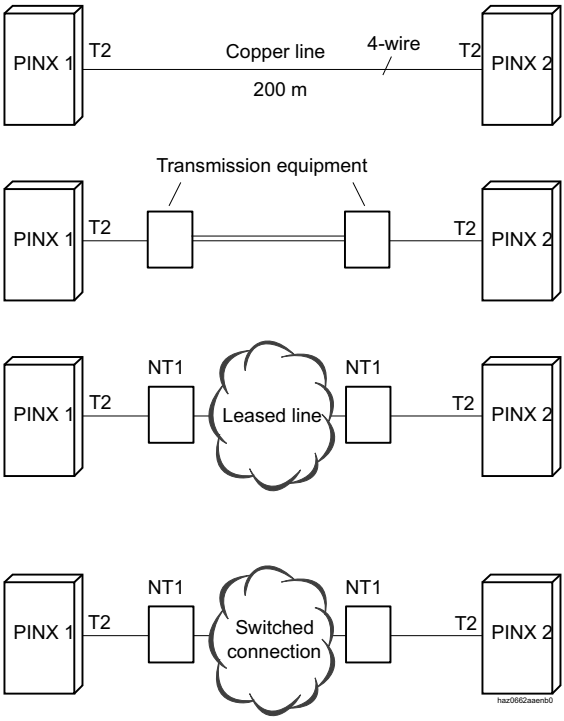
2. 4 Connecting PISN nodes

The nodes of a PISN (PINX) can be connected via basic, primary-rate or Ethernet accesses. For short distances the connection can consist of one copper cable without any ancillary equipment. For longer distances transmission equipment or leased lines of the public network need to be used.

2. 4. 1 Connection via Basic and Primary Rate Access

PINX connections are connected to an S external, BRI-T or PRI interface. Each of these interfaces can be configured as an interface with QSIG / PSS1 or DSS1 protocol.

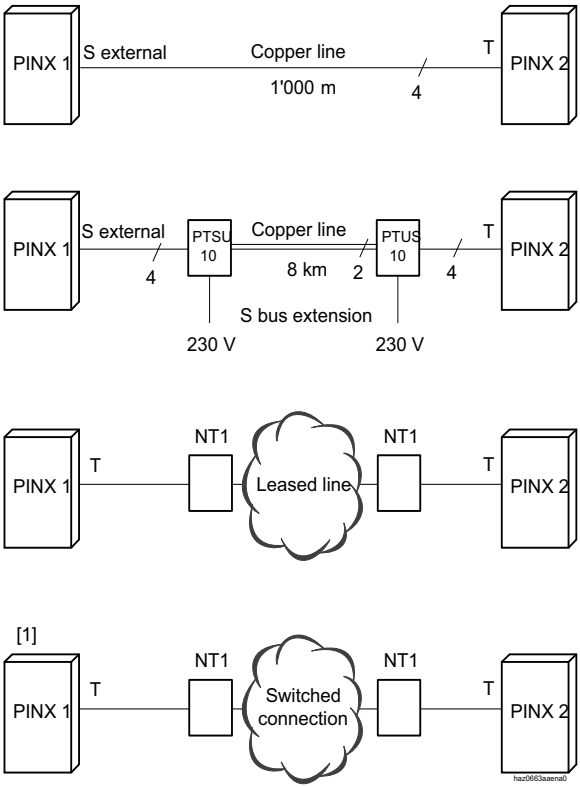
With the DSS1 protocol, only Base Call is supported on the BRI-S external interface.



T2: PRI primary rate interface

NT1: Network termination

Fig. 13 Primary access connections between two PINXs



T: BRI basic rate interface

S: Interface BRI-S external

[1] Not available in all countries

Fig. 14 Basic access connections between two PINXs

2. 4. 2 Connection via Ethernet

For QSIG networking on the IP network, connection is via the communication server Ethernet interface. The communication servers require some VoIP resources.

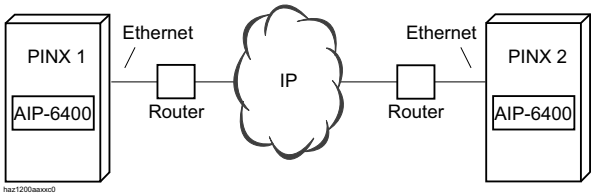


Fig. 15 Ethernet connection between 2 PINXs

2. 5 Numbering Plan and Regions

Users connected directly to a PINX are always internal users. Users of a different PINX in the same private network are PISN users. Several PINXs can be grouped together into regions. All the regions together form the PISN.

The relationships between PINX and PISN users are specified in the internal numbering plans of the individual PINXs.

2. 5. 1 Shared Numbering Plan

If two or more PINXs are structured in such a way that they split the users' number range among themselves, we talk of a shared numbering plan. Each number can occur in the PISN only once. Together the PINXs form a region, in which all the users can be reached under internal call numbers.

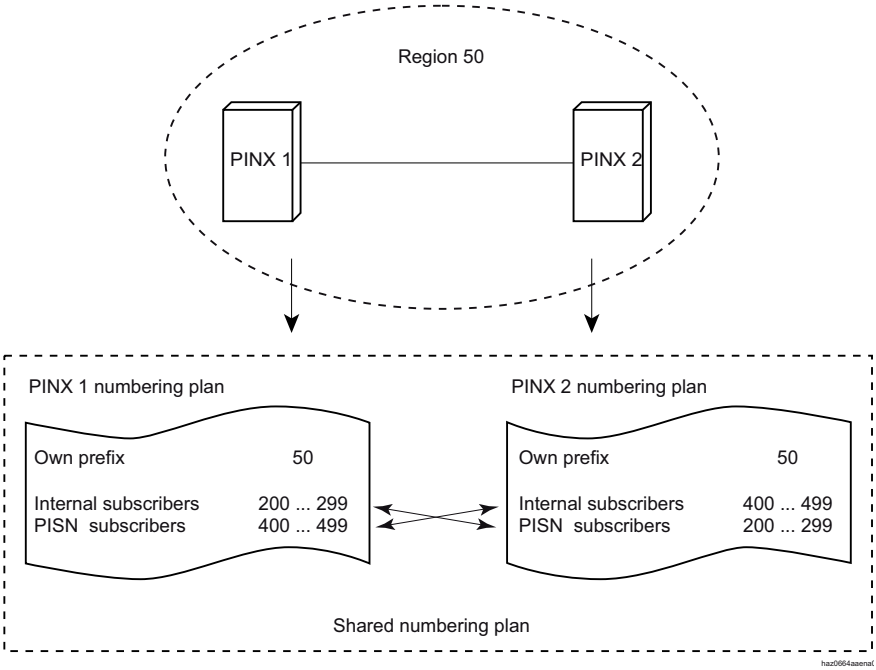


Fig. 16 Shared numbering plan: two PINXs share the numbers of a numbering plan.

2. 5. 2 PISN with Regions

If a PISN is subdivided into several regions, each own regional prefix is determined in the internal numbering plan of each PINX.

Users who call a user in a different region first dial the prefix of the destination region, then the internal number of the user they want.

The numbering plan is organized independently of the PISN topology.

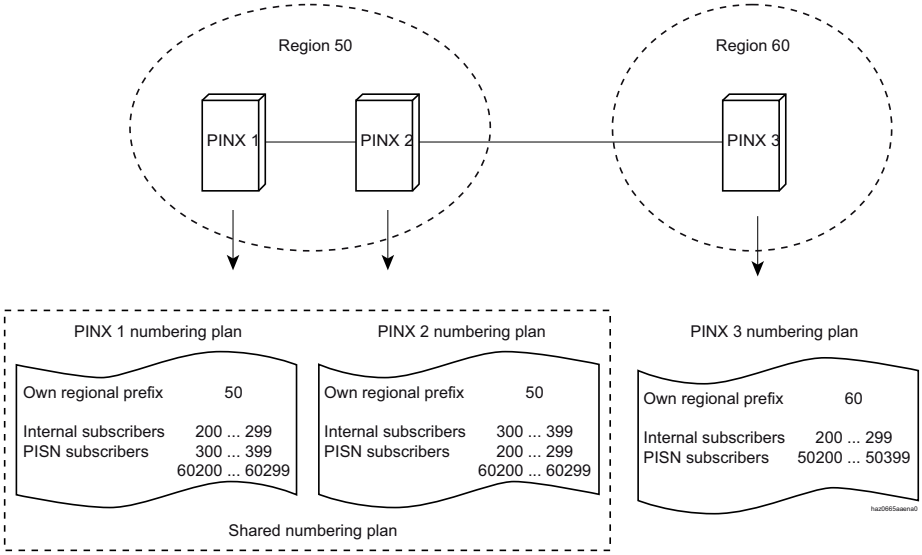


Fig. 17 PISN with two regions and shared numbering plan for Region 50

The purpose of the division into regions is that then the existing DDI numbers can continue to be used.

2. 5. 2. 1 Numbering Plan for Two Regions

Even a virtual communication server can easily be integrated into a PISN.

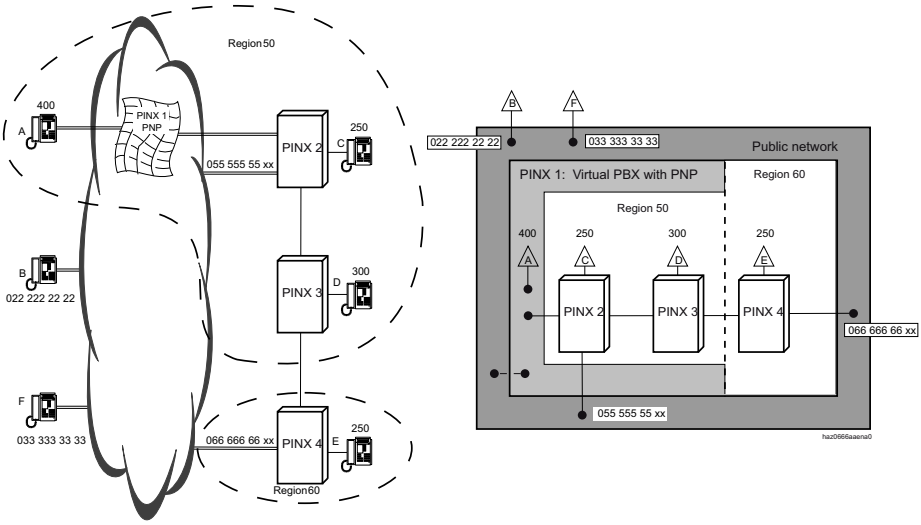


Fig. 18 Example: PISN with two regions and a shared numbering plan for Region 50

Tab. 3 Entries in the numbering plans for the above example

Numbering plan of	Own region prefix	Internal (local) users	PISN numbers	
			PISN users	in regions
PINX 1	50	400 … 499	2xx, 3xx 602xx	50 (specific) 60
PINX 2	50	200 … 299	3xx, 4xx 602xx	50 (specific) 60
PINX 3	50	300 … 399	2xx, 4xx 602xx	50 (specific) 60
PINX 4	60	200 … 299	– 502xx to 504xx	60 (specific) 50

PINX 1, 2 and 3 share a numbering plan. PINX 4 has its own, specific numbering plan.

2. 5. 2. 2 Call Routing in Regions

The following sections illustrate how calls are routed in a PISN with regions.

Call within the Same Region

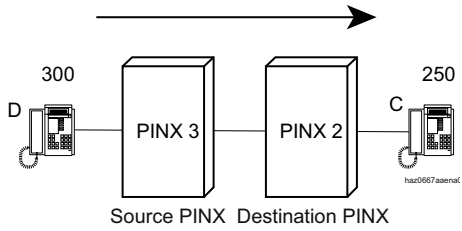


Fig. 19 User D dials 250 (user C)

The call is routed as follows:

1. In PINX 3's internal numbering plan the number 250 is entered as a PISN user. The call is routed to PINX 2 via the allocated route.
2. Under the number 250 PINX 2 finds the internal user C. The connection is set up.

Call to a Different Region

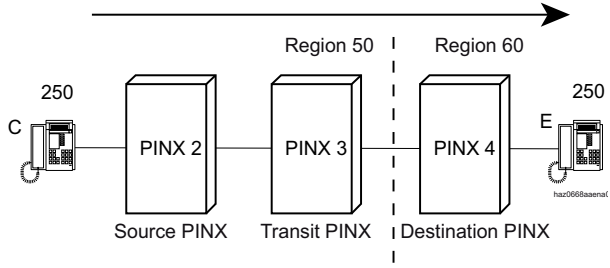


Fig. 20 User C dials 60 250 (user E)

The call is routed as follows:

1. In PINX 2's internal numbering plan the number 60250 is known for a PISN user in a different network region. The call is routed to PINX 3 via the allocated route.
2. In PINX 3's internal numbering plan the number 60250 is also known. The call is routed to PINX 4 via the allocated route.
3. PINX 4 recognizes the number 60 as a specific prefix and truncates the digits. Under the number 250 it finds the internal user E. The connection is set up.

Call to a virtual communication server

This is a call within the PISN Region 50.

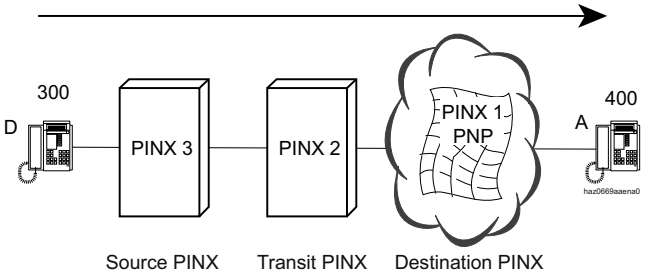


Fig. 21 User D dials 400 (user A on the virtual communication server)

The call is routed as follows:

1. In PINX 3's internal numbering plan the number 400 is entered as a PISN user. The call is routed to PINX 2 via the allocated route.
2. In PINX 2's internal numbering plan the number 400 is also entered as a PISN user. The call is routed to PINX 1 via the allocated route.
3. Under the number 400 PINX 1 finds the internal user A. The connection is set up.

Call from the Public Network

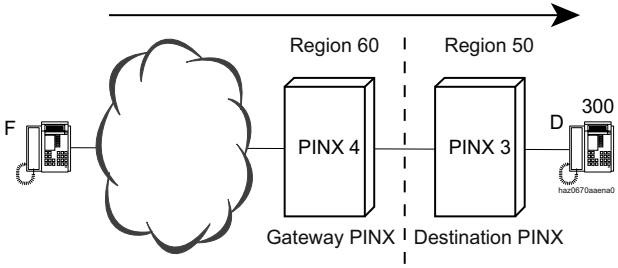


Fig. 22 User F dials 066 666 66 30 (user D)

The call is routed as follows:

1. In PINX 4's direct dialling plan the number 630 is linked with the PISN user number 50 300. The call is routed to PINX 3 via the allocated route. The configuration of the routes and DDI numbers is done via WebAdmin.
2. PINX 3 recognizes the first 2 digits (50) as a specific prefix and truncates them. Under the number 300 PINX 3 finds the internal user D. The connection is set up.

2. 6 Services and Functions

Aastra 400 communication servers support the services outlined below. For the services to be offered in PISN, they must be supported by all PINX and by the deployed terminals.

2. 6. 1 Network services

Tab. 4 Supported network services

Abbreviation	Designation		Remarks
	International	Aastra 400	
	Base Call	Basic service	
CCBS	Call Completion to Busy Subscriber	Callback if busy	Possible everywhere if supported by the public network
CFB	Call Forwarding Busy	Call Forwarding Busy	Executed locally in the PINX concerned, with display on the terminal
CFNR	Call Forwarding No Reply	Call Forwarding on No Reply CFNR	Executed locally in the PINX concerned, with display on the terminal
CFU	Call Forwarding Unconditional	Call Forwarding Unconditional CFU	Executed locally in the PINX concerned, with display on the terminal
3pty	Three-party services		In a heterogeneous network these features also depend on the third-party PINX.
	• Call Transfer by join	Call transfer	Always possible under QSIG / PSS1, with correct display. The transferring PINX becomes a transit PINX.
	• Call Enquiry	Enquiry	Executed locally in the PINX concerned, with display on the terminal
	• Brokering	Brokering	Executed locally in the PINX concerned, with display on the terminal
	• Conference	Conference	Under QSIG / PSS1 with correct display
	• Recall	Recall	Only under QSIG / PSS1
CLIP	Calling Line Identification Presentation	Caller Identification (Call number)	
CLIR	Calling / Connected Line Identification Restriction	Suppress CLIP	

Abbreviation	Designation		Remarks
	International	Aastra 400	
CNIP	Calling Name Identification Presentation	Caller identification (name)	Defined only in QSIG / PSS1
CNIR	Calling / Connected Name Identification Restriction	Suppress CNIP	Together with CLIR
COLP	Connected Line Identification Presentation	Identification (call number) of the called party	
CONP	Connected Name Identification Presentation	Identification (name) of the called party	Defined only in QSIG / PSS1
DDI	Direct Dialling In	Direct dialling plan	
HOLD	Hold	Hold	
PARE	Partial Rerouting	Partial Rerouting	Not supported in QSIG / PSS1
CD	Call Deflection	Call Deflection	Implemented locally as a user-related feature in the relevant PINX
PNP	Private Numbering Plan	Private numbering plan	Centrex is supported and integrated into a region.
UUS	User-to-User Signalling	User-to-user signalling	Not supported in QSIG / PSS1
SUB	Subaddressing	Subaddress	Not supported in QSIG / PSS1

2. 6. 2 Other services

Dialling by name

A PISN user can dial any other PISN users by name, irrespective of region, topology and protocol, if the PISN user is explicitly listed by name in the numbering plan of the source PINX.

Least Cost Routing (LCR)

The Least Cost Routing (LCR) function is used for special network functions such as break-out or overflow (see system manual "Features of an Aastra IntelliGate").

Overflow routing

When a connection is set up the communication server checks the availability of the selected path. If the route is not available due to overloading or defect and if overflow routing has been put in place, the connection is set up via an alternative route (see system manual "Features of an Aastra IntelliGate").

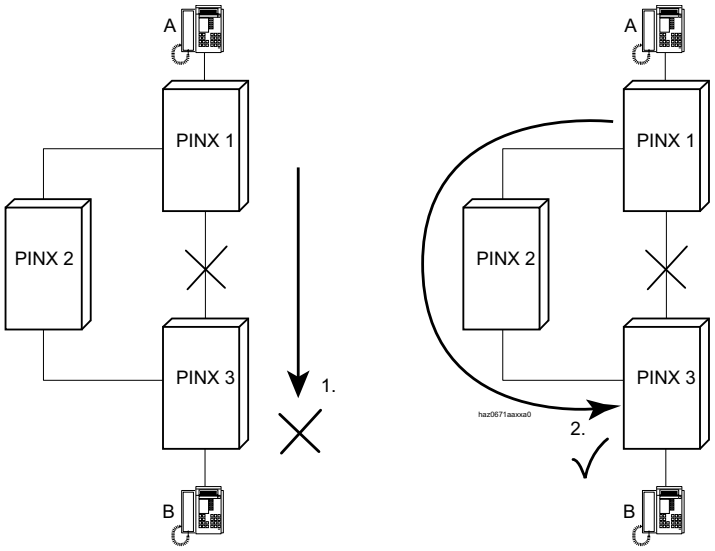


Fig. 23 Overflow via a leased line

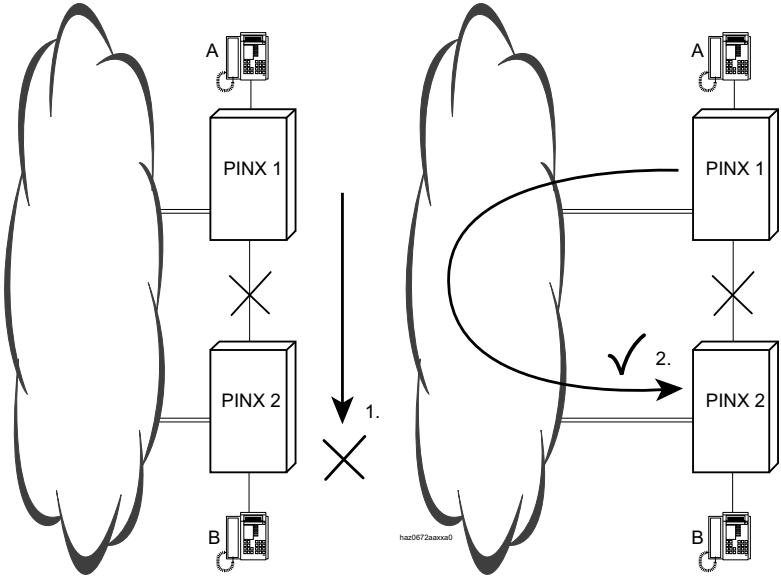


Fig. 24 Overflow via the public network -- the LCR function is used for this purpose

2. 6. 3 Break-out

An outgoing external call is routed into the public ISDN only at the PINX that is closest to the call destination. As the path in the public network is shorter, call charges can be saved in this way.

For more details, see System Manual "Features of an Aastra IntelliGate".

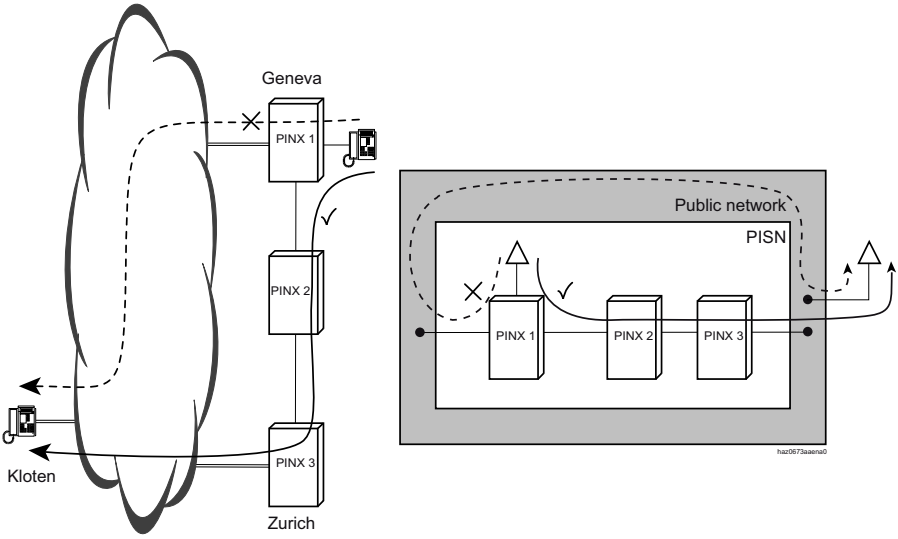


Fig. 25 Break-out: the shortest connection to a user in the public ISDN

2. 6. 4 Break-In for virtual PISN users

An incoming call from the outside is routed into the PISN at the PINX closest to the calling party. For this the calling party must know the dial-in number for the PISN. This number can be displayed to him as a CLIP number, for example when calling from the PISN. Typical break-in applications:

- A company with several different locations wishes to present itself to the outside through one location only.
- Traffic from a virtual node to other nodes in the leased-line network is always to be routed via the nearest node in the private network.

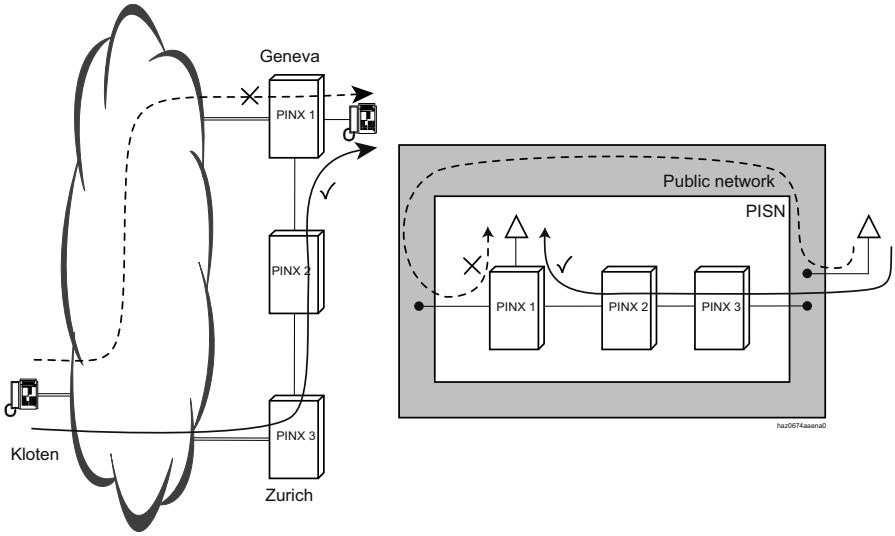


Fig. 26 Break-in: shortest connection from the public network to the PISN

2. 7 Glossary

Tab. 5 Networking technology terminology

Abbr.	Term	Explanation
–	Exchange	Short for → public phone network
–	Break-in	An external incoming → DDI connection for a PISN user is routed into the → PISN at the →PINX that is closest to the caller.
–	Break-out	An outgoing external connection is routed into the public ISDN only at the PINX that is closest to the call destination.

Abbr.	Term	Explanation
CTX	Centrex	The designation Centrex, for Central Office Exchange Service, is a product name which some network providers use for the services provided by the → virtual Call Managers.
DSS1	Digital Subscriber Signalling 1	Signalling protocol for ISDN networks (also called Euro-ISDN)
DDI	Direct Dialling In	DDI numbers enable internal users to be reached directly from a public network. In the direct dialling plan the end portion of a call number is allocated to the number of an internal users or → PISN user. Several direct dialling plans can be drawn up for each communication server.
DDO	Direct Dialling Out	The communication server can forward direct dial numbers to the private leased-line network via the interface S external.
E.164	–	• Numbering plan identifier of the public network as per ITU-T • Parameter value of parameter →NPI
–	Gateway PINX	A PINX is a gateway PINX for the duration of a connection if it routes that connection from the PISN to the public network or from the public network to the PISN.
–	Node	Branch point or end point in a communication network
LCR	Least Cost Routing	Routing function used to determine the network operators via which a call is to be routed. Usually the most cost-effective route (least cost) is selected. LCR is also needed for the overflow from the private to the public network.
–	Dialling by name	If a name is stored under a call number, the name can be used for dialling on the terminal instead of the call number.
–	QSIG networking in the IP network	Networking via an existing VoIP-capable IP network
NPI	Numbering plan identifier (Numbering Plan Identifier)	• In the public network, the numbering plan identifier used is →E.164. In the private area, the numbering plan identifier used is →PNP • Configuration parameter used for specifying the numbering plan identifier. Parameter values: E.164 / PNP / unknown
–	Overflow	If the chosen line of a→PINX is not available due to overloading or due to a defect, the connection pending is set up via an alternative path determined by the configuration.
PISN	Private Integrated Services Network	Private network based on the ISDN standard in which all the connected users can communicate with one another as internal users. This applies to both voice traffic and to ISDN-based data traffic.
–	PISN users	• User in a different →node of a private network • Category in the internal numbering plan used to replicate the users in the private network
PINX	Private Integrated Services Network eXchange	→ Communication server of a → PISN.

Abbr.	Term	Explanation
PNP	Private Numbering Plan	• Internal numbering plan of a communication server or PINX • Service offered by the network provider. Basically corresponds to the internal numbering plan of a communication server. Most important component of a → virtual communication server. • Parameter value of parameter →NPI
–	Private leased-line network	Private network implemented using dedicated lines. In the configuration we need to differentiate between the private leased-line network and the public network.
QSIG / PSS1	QSIG / PSS1 protocol	• ECMA-standardized signalling protocol used for networking several → PINXs. Now standardized worldwide (ISO / IEC) under the name PSS1 (Private Signalling System 1) • Parameter value of the "Protocol" trunk group parameter. Aastra 400 Communication servers support two versions of the QSIG / PSS1 protocol: QSIG (ETSI, 2nd edition) and QSIG/PSS1 ISO.
TON	Type of Number	Parameter used for classifying a call number: Parameter values, if the call number corresponds to a NPI = E.164: unknown / subscriber / national / international. Parameter values, if the call number corresponds to a NPI = PNP: unknown / level 0 / level 1 / level 2
–	Transit PINX	A PINX acts as a transit PINX for the duration of a connection if it routes that connection from one PINX to another PINX.
–	Source PINX	A PINX acts as a source PINX for the duration of a connection if the connection was set up by one of its users.
–	Virtual communication server	Network provider offer which comprises a → PNP and various ISDN supplementary services. Also known under the name → Centrex. With a virtual communication server the network provider is able to offer his customers a big part of the functionality of a communication server locally.
–	Destination PINX	A PINX acts as a destination PINX for the duration of a connection if the connection's destination user is one of its users.

3 Planning a private network

The following guide on how to plan private networks is designed to help you create a small, simple network. As the number of nodes increases, the requirements and potential sources of error also increase exponentially. For larger networks, experience and the assistance of specialists are invaluable.

When it comes to implementing a specific network there are always several solutions and configuration options. The following explanations must, therefore, be understood as a recommendation. Alternatives are always possible and, depending on the problem to be resolved, more appropriate.

This chapter consists of:

- a planning aid for converting the customer's ideas into a concrete project (as of page 41)
- Instructions for planning a simple specimen network (as of page 61)
- and other topics such as:
  - virtual networking (networking via the public network, as of page 77)
  - networking with a virtual communication server (Centrex, [1)], as of page 81)
  - networking with third-party systems (as of page 83)
  - other aspects of networking (as of page 84)

For planning an Aastra Intelligent Net (AIN) see manual "Aastra Intelligent Net (AIN) and IP terminals".

Additional PISN notes can be found in the system manual "Aastra IntelliGate Features".

3. 1 Planning aid

A customer has specific requirements for a telephony and data traffic infrastructure. The task is to determine how to convert these requirements into the best possible solution. The entire decision process is iterative. In other words, the items listed are not to be processed simply one after the other; instead, you need to return to previously defined parameters and, possibly, re-define them all over again.

The present planning aid will take you through the following topics:

- Specify the nodes
- Traffic Volume

[1)] depends on the network provider

- The routing in a private network
- Connection between two nodes
- Accesses to the public network
- Dialling through from the public network
- Incorporating virtual users
- Incorporating Centrex[1)]
- Numbering requirements
- Features to be supported

3. 1. 1 Specify the nodes

Criteria:

- What locations are there?
- Which locations are to be networked?
- Is a separate node required for each location?
- What is the optimum number of nodes for each location? Would it make sense to integrate a down-circuit cordless system?
- Which communication servers are the best suited?
- How should individual nodes be networked (virtual, fixed)?
- Is the integration of a virtual solution obvious? (for example, if some users are far a way from each other).

3. 1. 2 Past traffic volume

Over a representative period analyse the call logging values for the traffic volume between the locations using the previous solution:

- How high is the traffic volume?
- How is it spread out over time?
- Are there bottlenecks or restrictions?

Do you estimate together with the customer how strongly the traffic volume is changed with the new solution.

1) depends on the network provider

Calculate the potential savings of networking.

3. 1. 3 Routing in a private network

Determining the routing in a private network depends on the following factors:

- Connections between the nodes
- Accesses to the public network
- DDI requirements
- Overflow routing
- Volume of traffic in individual cases

Once the routing has been specified, you can estimate how many B channels are required between two nodes.

3. 1. 3. 1 Connections between nodes

Determine the nodes to be connected with one another:

- The topology can be star-shaped, meshed or a combination of both.
- For reasons of connection reliability it is advisable to ensure that each node can be reached via at least 2 independent routes (requirement for overflow routing). See also "Reliability aspects", page 49.
- Specify which connections are best implemented virtually via the public network (e.g. also the integration of GSM users into the private network).

3. 1. 3. 2 Accesses to the public network

Determine the nodes with accesses to the public network:

- Which nodes are to have virtual networking via the public network? This question is to be addressed in connection with the type of connection between two nodes. Virtual networking is particularly appropriate for greater distances with a relatively small volume of traffic.
- On which nodes should calls be routed to the public network (gateway PINX)? The traffic volume on a gateway PINX is the sum of the volume of traffic of the node's own traffic and the volume of traffic that telephone out into the public network using that system. The same thing applies to the nodes which route calls from one node to the other (Transit PINX).
- On which nodes are calls routed to the main number?
- On which nodes are calls to be routed directly from the public network to users on the private network (DDI)?
  - Should the users be reachable via several DDI numbers?
  - Should incoming calls be routed in accordance with break-in criteria? This requires other direct dialling numbers for the correct CLIP display (see "Break-In (Durchwahl für virtuell vernetzten PISN-Teilnehmer)", page 34).
- Where are additional connections to the public network required for overflow routing compatible with emergency operation? (See also "Reliability aspects", page 49).

3. 1. 3. 3 Traffic volume in the private network

With the results from the previous section and the previously estimated general traffic volume you can roughly estimate the volume of traffic for each node and for each connection between two nodes.

- How high is the traffic volume is for the following types:
  - Internal traffic
  - Transit traffic
  - Transferred calls
    (e.g. calls transferred via a main number)
  - Overflow routing
    (within the private network or via the public network)?
- How is the volume of traffic spread out over time?

3. 1. 3. 4 Determining the B channels

With the traffic volume estimate you can determine the number of B channels required.

3. 1. 4 Connection between permanently networked nodes

Each connection between two nodes can be implemented differently if required. The choice of the physical connection type depends on

- Distance and line length between the nodes
- Volume of traffic
- Existing infrastructure
- Financial resources

3. 1. 4. 1 Connections with primary rate accesses

Two nodes can be connected with one or several primary rate accesses. If necessary, transmission equipment can be used to extend the distance between the nodes.

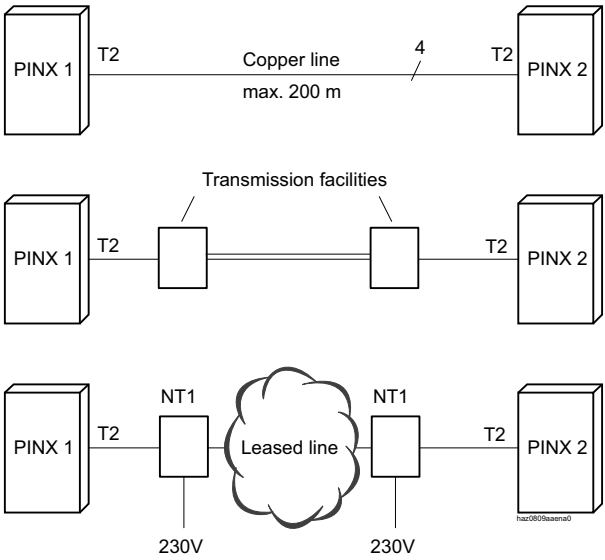


Fig. 27 Connection types via a primary rate access

Connection types for primary rate accesses:

- Copper lines without transmission equipment
- Unstructured leased lines with 30 B + D as per G.703
- Structured leased lines with (n x B) + D as per G.704
- Copper lines with transmission facilities
- Fibre optic cables with transmission facilities

The type of leased lines available depends on the service provider.

Transmission facilities for primary rate accesses:

- HDSL modems for primary rate accesses, 2 or 4-wire variants
- HDSL modems with multiplexer for combined telephony and data networks
- Transmission facilities for fibre optic cables

3. 1. 4. 2 Connections with basic accesses

Nodes can also be connected with one or several basic accesses.

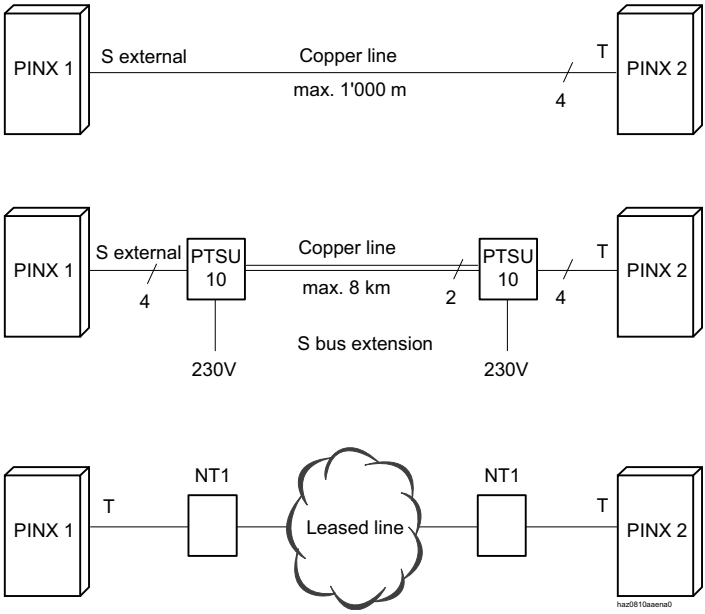


Fig. 28 Connection types via a basic access

It is important that an S bus be used on the one side (to which terminals are normally connected) and a BRI-T interface on the other side as for the public network.

The user interface with the S-Bus (BRI-S) is reset in the interface configuration to *BRI-S external*. As a result the user-network interface acts like a network interface. This means no more terminals can be operated there and no numbers allocated. In return the network interface can now be incorporated into a trunk group.

A gateway PINX should have an S-interface available to ensure node synchronisation (see also "Synchronization", page 50).

Several basic accesses between two nodes are grouped together in a trunk group.

Connection types for basic accesses:

- Copper lines without transmission equipment
- Leased lines
- Copper lines with transmission facilities
- Fibre optic cables with transmission facilities

The type of leased lines available depends on the service provider.

Transmission facilities for basic accesses:

- PT 10 S bus extension up to 8 km line length
- HDSL modem for basic accesses, 2 or 4-wire variants
- HDSL modem for multiplex for combined telephony and data networks

3. 1. 5 Protocols and licences

The PSS1 (QSIG) protocol is generally used in the private leased-line network. The appropriate licence is required. Connections to the public network normally use the DSS1 protocol.
DSS1 should not be used on S external as otherwise only Base Call is supported.

3. 1. 6 Reliability aspects

Connection reliability in a private leased-line network

If a network consists of several nodes, connection reliability can be increased if there are two or more paths in each case between two nodes.

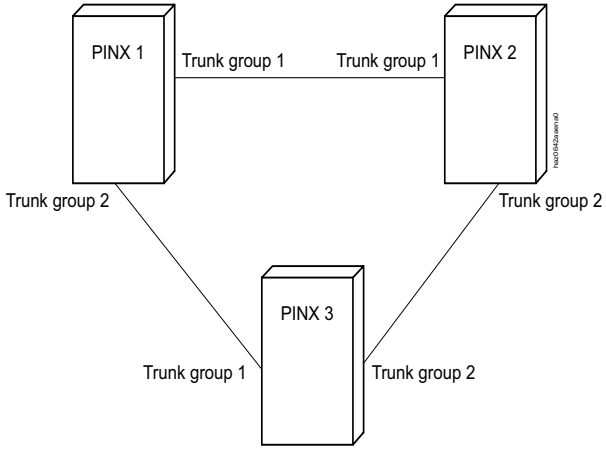


Fig. 29 Each node can be reached in two ways

Routes are used for outgoing routing, as described in "Example of networking", page 61.

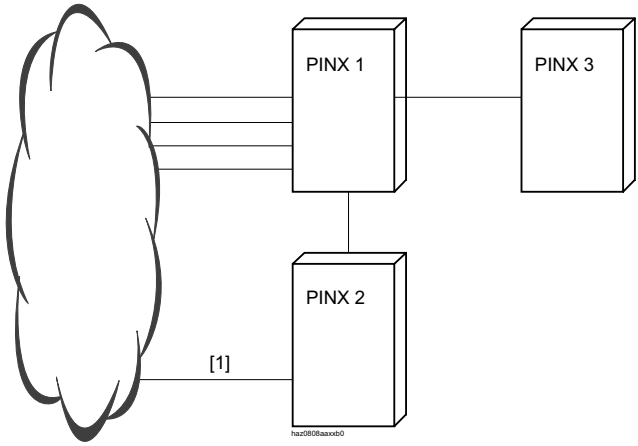
Path 2 is used in the example for connecting node 1 to node 2. In this route trunk group 1 is now added in the first position and trunk group 2 in the second.

Under normal circumstances calls will be routed directly from node 1 to node 2 via trunk group 1. If, however, the lines of trunk group 1 are faulty or if they are all busy, calls will be routed over trunk group 2 via node 3.

Connection reliability with the public network

To guarantee a high level of connection reliability also with the public network, it is useful to connect at least two nodes with the public network.

Overflow routing can then be implemented via the public network using Least Cost Routing.



[1] Basic access used to increase connection reliability

Fig. 30 Connection reliability in the public network

3. 1. 7 Synchronization

The clock frequency of a communication server is provided (synchronized) by the public network via the basic accesses BRI-T and the primary rate accesses PRI.

Should synchronization by the public network fail (due for example to exchange line interruptions), the communication server will use its own clock.

In a private leased-line network, nodes that are synchronized by the public network pass on the clock reference to nodes that are not connected directly to the public network.

3. 1. 7. 1 Clock propagation diagram

Synchronization in a private leased-line network has to be carefully planned to ensure that synchronization loops never occur. A synchronization loop occurs whenever two nodes synchronize each other.

The best solution is to sketch out a clock propagation diagram based on the following pattern:

1. Draw the PISN with its nodes and connections.

2. Determine the clock flow and view it with direction arrows. Ensure that you do not integrate any loops.

   Check the selected clock flow by following the direction arrows: If you never encounter the same node twice on the same path, you can assume that there are no loops.
3. Enter the network interfaces (PRI, BRI-T or BRI-S external).
4. For each node configure the network interfaces of all the trunk lines with an incoming arrow in the clock reference table. One of these will then be chosen as the original reference.

Example of a clock propagation diagram

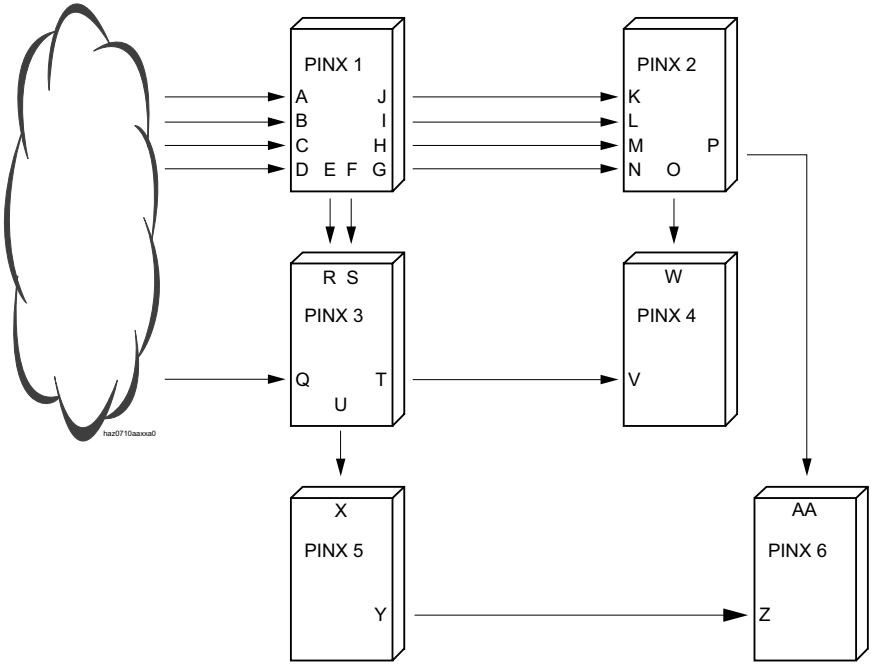


Fig. 31 Example of a clock propagation diagram (A to AA indicate the network network interfaces)

Tab. 6 Configuration for the above example

PINX	Original reference	Clock reference table	Remarks
1	A (or B or C or D)	A B C D	E and J propagate the timing and are therefore not entered in the clock reference table
2	K (or L or M or N)	K L M N	O and P propagate the clock and are therefore not entered in the clock reference table
3	Q	Q R S	T and U propagate the timing and are therefore not entered in the clock reference table.
4	V	V W	
5	X	X	Y propagates the timing and is therefore not entered in the clock reference table.
6	AA	AA Z	AA is better than Z because more lines to the public network are available.

Negative example with loops

In this example PINX 1 might synchronize with PINX 3 while at the same time as PINX 3 synchronizes with PINX 1. The nodes will run out of sync.

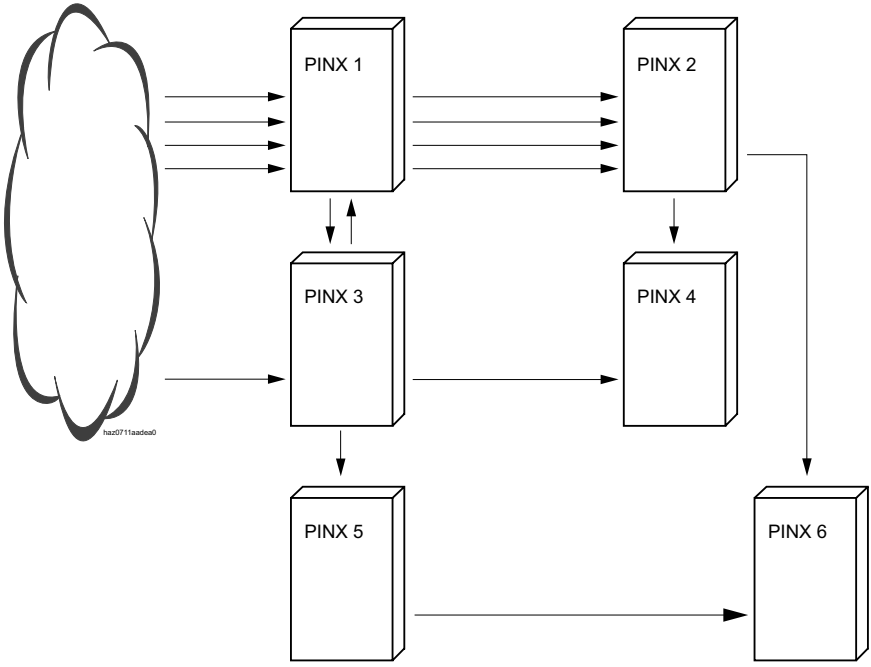


Fig. 32 Negative example: Network with synchronization loops

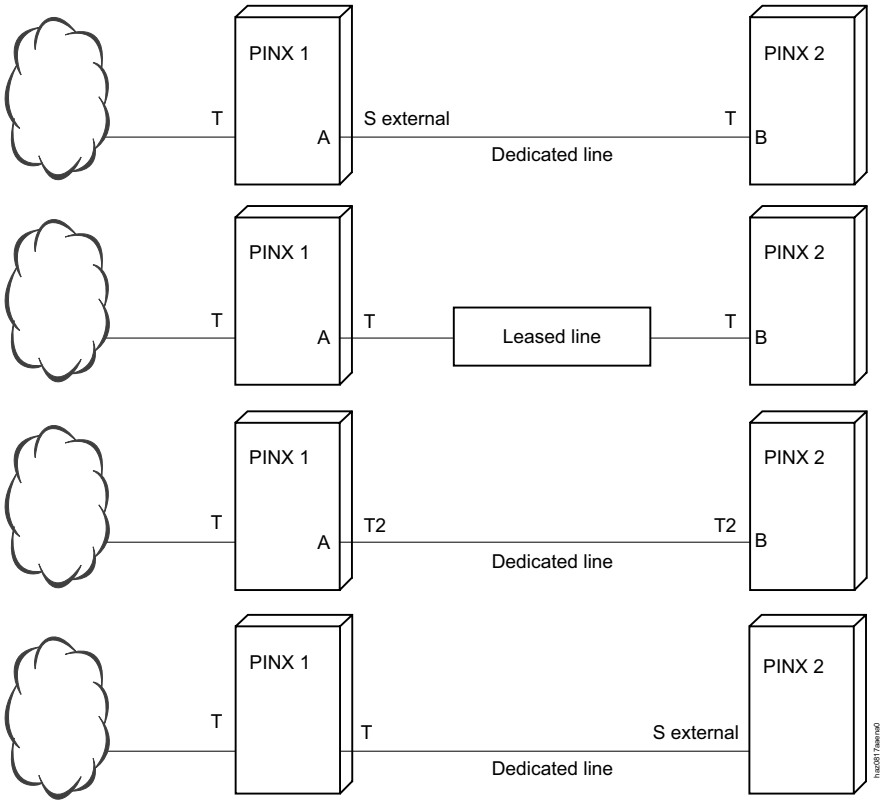
3. 1. 7. 2 Planning rules

The purpose of the planning is as follows:

- To use the clock propagation source to draw up the list of all the possible clock sources for each node (see Fig. 31).
- To determine the best possible clock source for each node. This is configured as original reference.

Follow the following rules when creating the clock propagation diagram:

- Each BRI-T or PRI- interface of a node can serve as the clock source for that node and be entered in the clock reference table.
- A PRI interface is preferable to a BRI-T interface.
- A connection to the public network is preferable to a connection to the private network.
- The original reference should always consist of the connection closest to the public network.
- Each PRI or S external interface is capable of passing the synchronization on to another node. However, such an interface must not be entered in the clock reference table or else synchronization loops may occur.
- An S external interface cannot be used as a clock source; it can, however, transfer the clock to another PINX. This should be taken into account when planning the network.
- A BRI-T interface is not suitable for passing on the timing as in fixed networking it can only be connected either to an S external interface or to a leased line. However, an S external interface cannot receive clock timing, and the timing from the public network is always supplied via a leased line.



A should not be in the clock reference table

B should be in the clock reference table

Fig. 33 Possible and prohibited connections

Initialization setting

All BRI-T interfaces are entered in the clock reference table. Therefore, if a node is integrated in a network, certain network interfaces will have to be excluded from the clock reference table.

3. 1. 8 Numbering

There are two methods for setting up the numbering plan of a private network:

- Numbering with blocks (shared numbering plan)
- Numbering with regions

3. 1. 8. 1 Numbering with blocks (shared numbering plan)

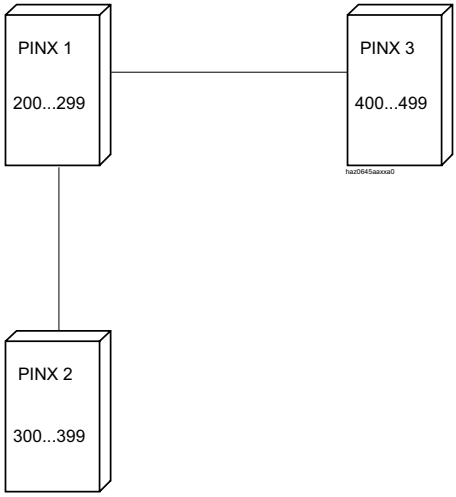


Fig. 34 Numbering with blocks (shared numbering plan)

The numbering range is divided into blocks. These latter are distributed among the nodes. This method is preferable as the user does not have to know the network topology. He can reach any user in the network simply by dialling the internal number, regardless of which node he is connected to. Drawbacks of the method:

- When networking standalone communication servers the existing numbering plans sometimes have to be adapted. Users must be assigned new numbers.
- The number of network users is limited by the number range available.

page 69 contains an implementation example for this method.

3. 1. 8. 2 Numbering with regions

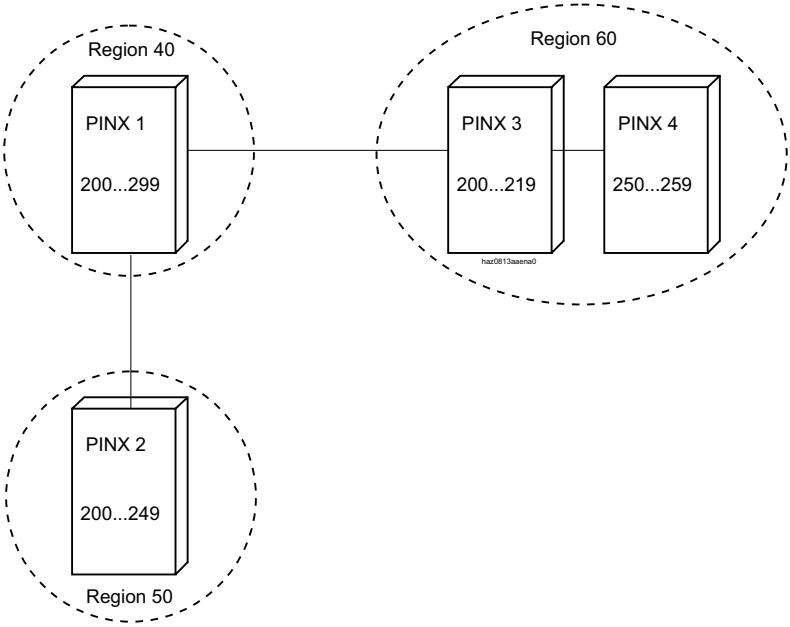


Fig. 35 Numbering with regions

The network is subdivided into regions. One or more nodes belong to each region. Each region has its own numbering plan. The nodes within a region share a numbering plan, with the number range divided up into blocks (see "Numbering with blocks (shared numbering plan)", page 55). Each node is allocated to a region using the setting "Own Regional Prefix".

Advantages of this method:

- When networking existing nodes the existing numbering plans may have to be adapted. Users do not have to be assigned new numbers.
- The number of network subscribers is not restricted by the number range of a single numbering plan as there is a separate numbering plan available for each region.

Numbering with regions can be implemented in two ways:

- Region selection via PISN user
- Region selection via route selection.

Region selection via PISN user

In each node, a PISN user is created for each region. For example, in node 1 a PISN subscriber 60xxxx is created for Region 60.

Advantage: individual users can also be allocated uniquely and are therefore reachable through dialling by name.

Drawback: Only numbers with the same digit length can be reached using the entry with wildcard characters.

page 73 contains an implementation example for this method.

Region selection via route selection.

In each node a route is created with the region's call number for each region in the numbering plan. For example, in node 1 a route is provided with call number 60.

Advantage: All the numbers in Region 60 are obtainable, regardless of how many digits they have.

Drawback: Users in the network cannot be dialled by name.

Note:
This method cannot be used in a gateway PINX as an incoming call from the public network cannot be routed to the destination node.

page 74 contains an implementation example for this method.

3. 1. 9 Link-up to a public network

On a private network any nodes can be provided for linking up to the public network. One or more nodes may be used. Nodes that route calls from other nodes to the public network are gateway PINX.

Calls from nodes not directly connected to the public network can be routed via several nodes up to the gateway PINX. These nodes are transit PINX.

The node on which a call is set up is the originating PINX. The node to which the destination user of a call is connected is the destination PINX.

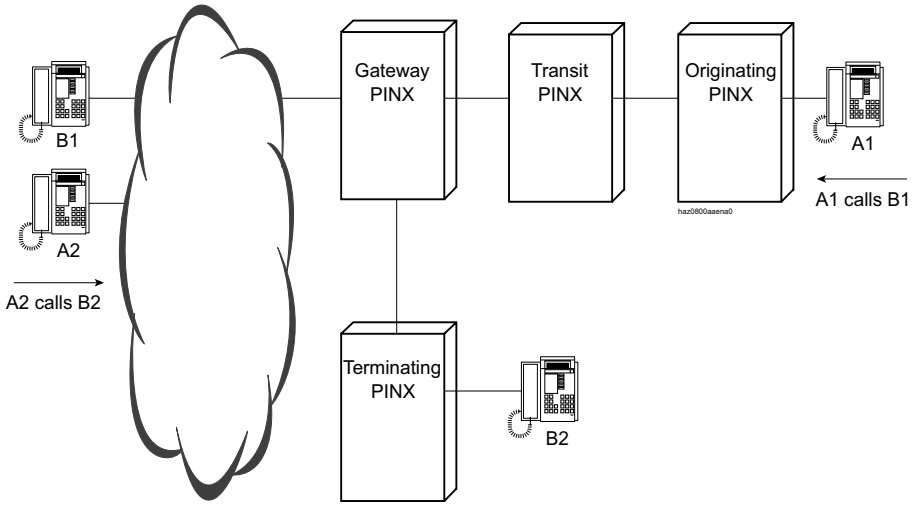


Fig. 36 The function of individual nodes for call traffic with the public network

For incoming traffic, DDI numbers have to be created at a gateway PINX for all the users in the private leased-line network who are to be directly reachable from the public network via this node (see "Direct dialling in at the gateway PINX", page 59).

The following points need to be taken into account for outgoing traffic:

- Ensure on the originating PINX that a call to the public network is recognisable as such (see "Identification of calls to the public network", page 60).
- Configure the transit and gateway PINX so that they forward a call to the public network (see "Definition of the transit route", page 61).

3. 1. 9. 1 Direct dialling in at the gateway PINX

In a gateway PINX DDI numbers are created for all the users of the private network who are to be obtainable directly from the public network, via the node. The destination users in their own node and in the other nodes are entered in the relevant call distribution elements for each switch position of the allocated switch group.

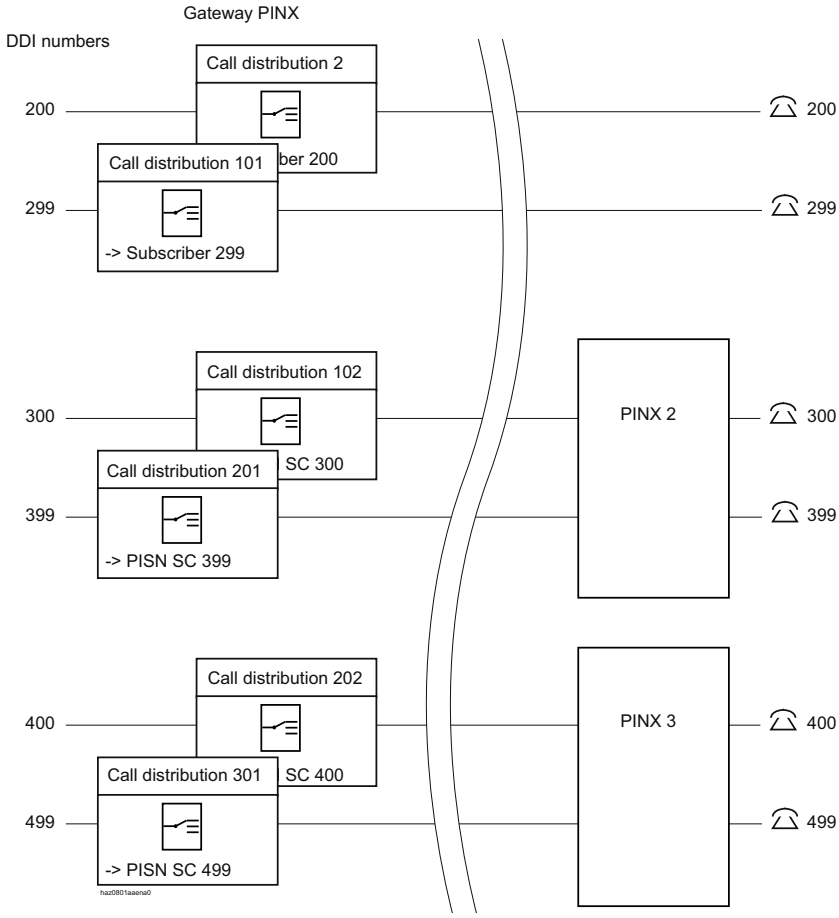


Fig. 37 In the gateway PINX DDI numbers are created for all the users in the network.

3. 1. 9. 2 Identification of calls to the public network

If a transit PINX or a gateway PINX is to recognize whether or not it should forward an incoming call to the public network, the call number must be an external number. As such it must

- either comply with numbering plan identifier (NPI) E.164 or
- be preceded by an exchange access prefix.

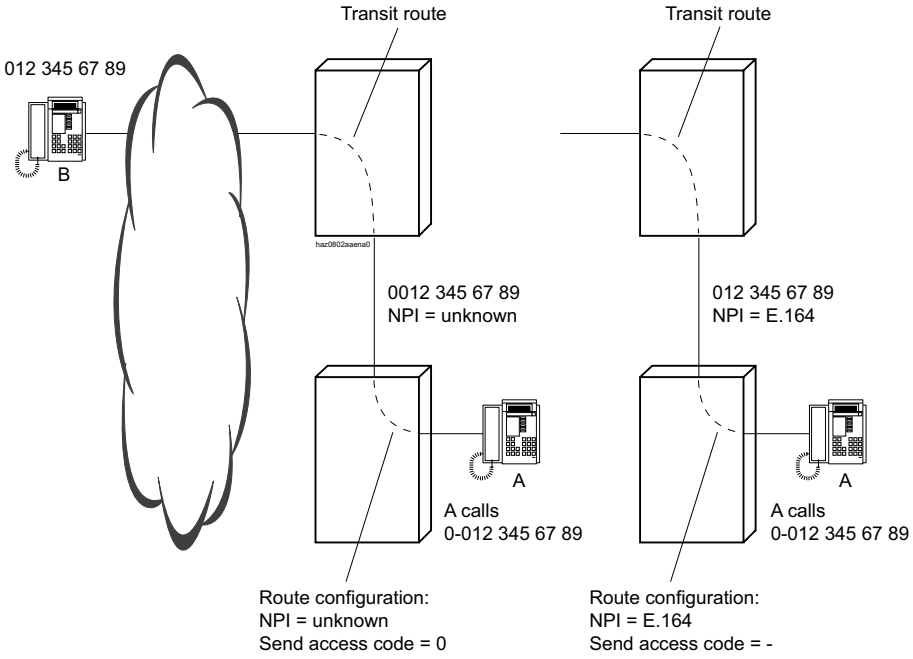


Fig. 38 Call number attributes for outgoing calls to the public network (2 variants)

Both attributes are set in the route configuration. This means that a separate route is always reserved for calls to the public network.

page 67 contains an implementation example.

3. 1. 9. 3 Definition of the transit route

On the transit PINX and gateway PINX you need to define the route via which calls to the public network are to be forwarded. In each node this is done with the aid of the "Transit Route" setting (under the PISN settings).

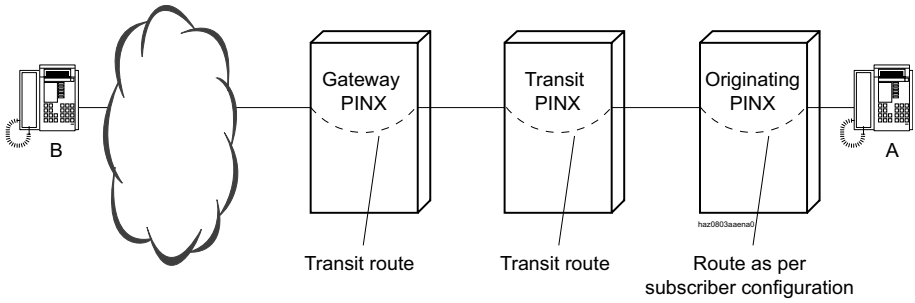


Fig. 39 A call to the public network is routed via the transit route in a Transit and gateway PINX

page 64 contains an implementation example.

3. 2 Example of networking

A small network will be used to describe a planning procedure. The node designation always precedes the nodes so that the configurations of the various nodes can be differentiated. For example , trunk group 5 of node 1 is designated as trunk group 1-5.

The following assumptions are made:

- Node 1 is connected with node 3 via a primary rate access.
- Node 1 is connected with node 2 with two basic accesses.
- Node 1 is connected with the public network via a primary rate access (node 1 is the gateway PINX).

Steps in the procedure:

1. Create the routes (as of page 63).
2. Create the trunk groups (as of page 65).
3. Configure the routes (as of page 66).
4. Create the numbering plan (as of page 69).
5. Set up direct dialling in (as of page 76).

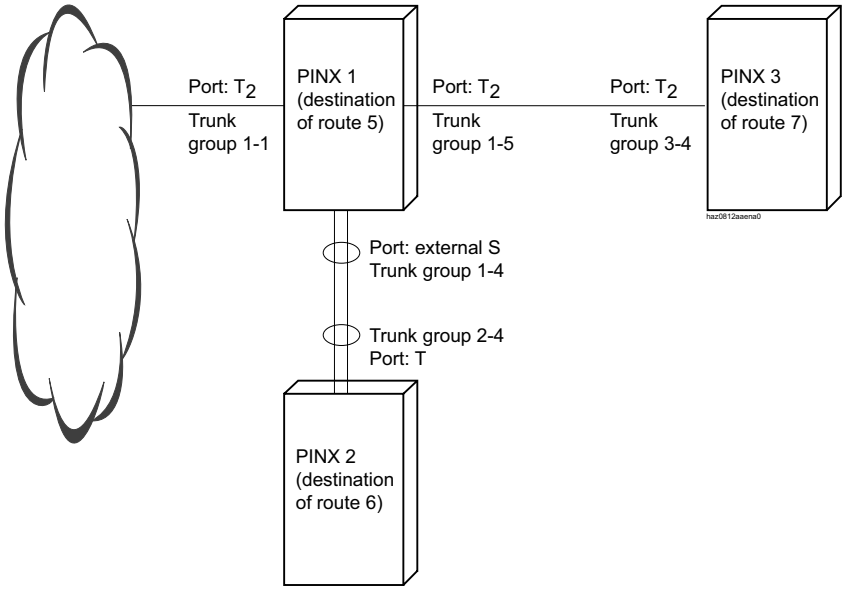


Fig. 40 The specimen network

3. 2. 1 Creating the routes

3. 2. 1. 1 Replicating the nodes on routes

A route always defines a destination. A destination is either a node in the network or a connection to the public network. You need to create as many routes as there are destinations. To have a good overview, the same route is always used in each node for the same destination. In other words, one route is reserved for each destination.

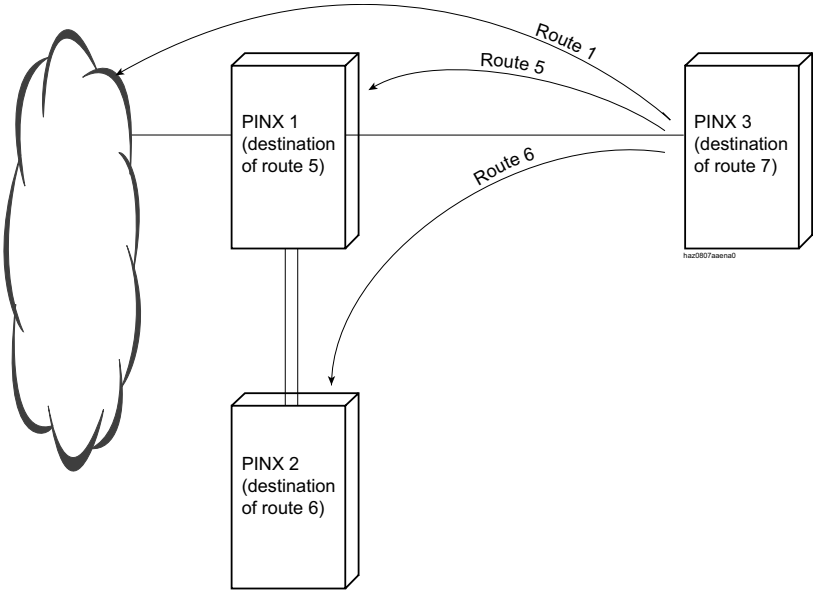


Fig. 41 One route is reserved for each destination

In each node create one route for each of the other nodes.

1. Create one route for each node:
   - For node 1: Route 5
   - For node 2: Route 6
   - For node 3: Route 7
2. In each node, name the routes you have just defined:
   - Route 5: for PINX 1
   - Route 6: for PINX 2
   - Route 7: for PINX 3

3. In node 1 create one route for node 3 (route 1-7) and one route for node 2 (route 1-6).
4. In node 2 create one route for node 1 (route 2-5) and one route for node 3 (route 2-7).
5. In node 3 create one route for node 1 (route 3-5) and one route for node 2 (route 3-6).

3. 2. 1. 2 Defining the routes to the public network

In each node create a route to the public network. The simplest way is to reserve one route number for the public network.

Node 1 is the gateway PINX, i.e. all the calls between the private leased-line network and the public network are routed via this node. The route that assumes this task must be specified.

1. Reserve route 1 for the public network.
2. In each node create a route to the public network.
   - Node 1: Route 1 (route 1-1)
   - Node 2: Route 1 (route 2-1)
   - Node 3: Route 1 (route 3-1)
3. In all the nodes, specify route 1 as "to the public network".
4. In node 1 specify route 1 for routing calls from other nodes to the public network: Transit route = route 1

3. 2. 2 Creating the trunk groups

3. 2. 2. 1 Creating the trunk groups between the nodes

Create a trunk group with all the lines between two nodes.

1. In node 1 create a trunk group with all the lines to node 2 (trunk groups 1-4) and a trunk group with all the lines to node 3 (trunk groups 1-5).
2. In node 2 create a trunk group with all the lines to node 1 (trunk groups 2-4). As there are no lines leading directly to node 3 and there are no other lines, you do not need to create any other trunk groups.
3. In node 3 create a trunk group with all the lines to node 1 (trunk groups 3-4).

   You need to set the trunk groups for a private network:
4. Select the following settings in the trunk group configuration for trunk groups 4 and 5 of all the nodes:
   - Network type = private
   - Protocol = PSS1

   Name the trunk groups as an orientation aid:
5. Name the trunk groups of node 1:
   - Trunk groups 1-4: Name = PINX 2
   - Trunk groups 1-5: Name = PINX 3
6. Name the trunk groups of nodes 2 and 3:
   - Trunk groups 2-4: Name = PINX 1
   - Trunk groups 3-4: Name = PINX 1

3. 2. 2. 2 Creating the exchange trunk group

1. An exchange trunk group is created in node 1 for the lines leading to the public network:
   Create a trunk group in node 1 with the line to the public network (trunk group 1-1).
2. You need to set the exchange trunk group for the public network:
   Select the following settings in the trunk group configuration of trunk group 1-1:
   - Name = public network

- Network type = public
- Protocol = DSS1

3. 2. 3 Route configuration

Once you have created the trunk groups, configure the routes.

Allocating the trunk groups

Three routes are provided for in each node (one for each node in the network and one for the public network. You do not need one for your own node). The trunk groups are now allocated to the routes:

1. In node 1 allocate the trunk groups to the routes:
   - Route 1-1: trunk group 1-1 (trunk group to the public network)
   - Route 1-6: trunk group 1-4 (trunk group to node 2)
   - Route 1-7: trunk group 1-5 (trunk group to node 3)
2. In node 2 allocate trunk group 2-4 to all the routes (all the routes use the same trunk group as all the calls go via node 1):
   - Route 2-1: trunk group 2-4 (trunk group to node 1)
   - Route 2-5: trunk group 2-4 (trunk group to node 1)
   - Route 2-7: trunk group 2-4 (trunk group to node 1)
3. In node 3 allocate trunk groups 3-4 to all the routes. (All the routes use the same trunk group as all the calls go via node 1):
   - Route 3-1: trunk group 3-4 (trunk group to node 1)
   - Route 3-5: trunk group 3-4 (trunk group to node 1)
   - Route 3-6: trunk group 3-4 (trunk group to node 1)

While nodes 2 and 3 have three routes, they contain the same trunk group. This is because calls with node 1, node 2 (or 3) and the public network as their respective destinations are routed via the same lines. If at a later date nodes 2 and 3 are connected with their own lines, simply create new trunk groups and re-assign the routes accordingly. All the rest remains the same; more importantly, you do not need to change the configuration of the network subscribers (PISN users).

Settings for the routes to the other nodes

All the call numbers of calls within the network are network-internal (PISN-internal) numbers. As such they have two special properties:

- They must comply with numbering plan identifier PNP.
- They do not have to be checked by an external digit barring.

These properties are set in the configuration to the routes:

1. In node 1 select the settings for routes 1-6 and 1-7:
   - Numbering plan identifier (NPI) = PNP
   - Digit barring = no
2. In node 2 select the settings for routes 1-5 and 1-7:
   - Numbering plan identifier (NPI) = PNP
   - Digit barring = no
3. In node 3 select the settings for routes 1-5 and 1-6:
   - Numbering plan identifier (NPI) = PNP
   - Digit barring = no

Settings for the routes to the public network

All the call numbers of calls to the public network are external numbers. As such they must

- either comply with numbering plan identifier E.164 or
- be preceded by an exchange access prefix.

In addition they should be checked by an external digit barring if required.

These properties are set in the configuration for the routes.

Variant 1:

1. In node 1 select the settings for route 1-1:
   - Numbering plan identifier (NPI) = E.164
   - Digit barring = yes
2. In node 2 select the settings for route 2-1:
   - Numbering plan identifier (NPI) = E.164
   - Digit barring = yes
3. In node 3 select the settings for route 3-1:

- Numbering plan identifier (NPI) = E.164
- Digit barring = yes

Variant 2:

1. In node 1 select the settings for route 1-1:
   - Numbering plan identifier (NPI) = E.164
   - Digit barring = yes
2. In node 2 select the settings for route 2-1:
   - Numbering plan identifier (NPI) = PNP
   - Send access code = 0 (as the exchange access prefix)
   - Digit barring = yes
3. In node 3 select the settings for route 3-1:
   - Numbering plan identifier (NPI) = PNP
   - Send access code = 0 (as the exchange access prefix)
   - Digit barring = yes

3. 2. 4 Creating the numbering plan

Now that the network is defined through the definition of the routes and trunk groups, we need to specify the numbering within the network.

In the following we shall be looking at both methods described on page 54 .

3. 2. 4. 1 Numbering with blocks

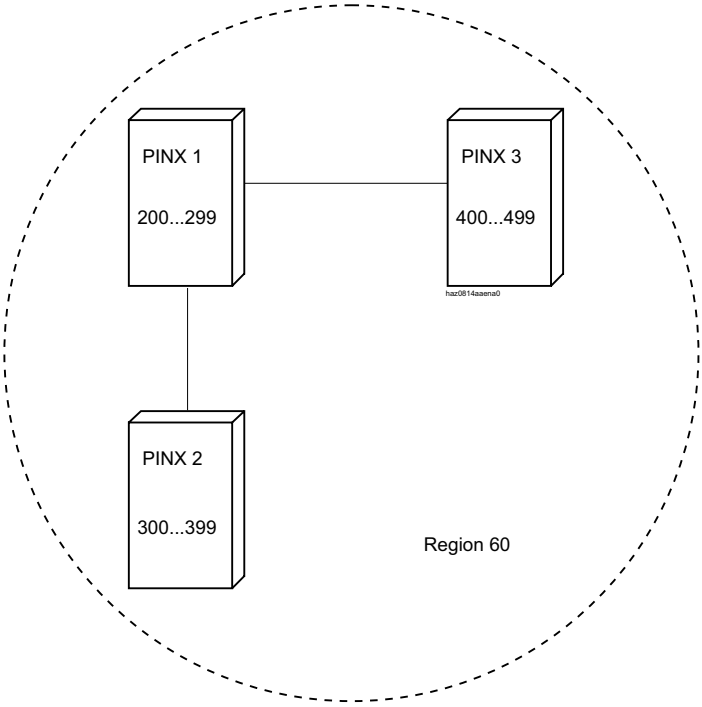


Fig. 42 Numbering with blocks (shared numbering plan)

Each node is assigned one (or more) number ranges. For example:

- Node 1: Number range 200…299
- Node 2: Number range 300…399
- Node 3: Number range 400…499

With this method all the nodes in the same region can be reached under the same regional prefix, which is why users no longer have to dial it.

Define a separate regional prefix nonetheless for all three nodes (e.g. prefix 60).
In each node configure the own region prefix under the basic settings:

1. Create the internal users:
   - Node 1: Internal users 200 to 299
   - Node 2: Internal users 300 to 399
   - Node 3: Internal users 400 to 499
2. Specify the regional prefix:
   - In node 1: Own region prefix = 60
   - In node 2: Own region prefix = 60
   - In node 3: Own region prefix = 60

With this method the local area network (see page 63) is not used. The number ranges of the other nodes have to be defined. To do so create numbers in the PISN users category in the numbering plan. There you can create either individual numbers or number ranges by specifying the range with "XX". Each "X" corresponds to one digit place.

1. Create the PISN users in node 1:
   - One PISN user 3XX (range of node 2)
   - One PISN user 4XX (range of node 3)
2. Create the PISN users in node 2:
   - One PISN user 2XX (range of node 1)
   - One PISN user 4XX (range of node 3)
3. Create the PISN users in node 3:
   - One PISN user 2XX (range of node 1)
   - One PISN user 3XX (range of node 2)

Under the user configuration are the PISN users you have just created, with the numbers 2XX, 3XX and 4XX.
The setting options for PISN users differ from those of ordinary internal users. Next use the "route" setting to allocate routes to the PISN users:

1. Assign the routes to the PISN users of node 1:
   - PISN user 3XX: Route 6
   - PISN user 4XX: Route 7
2. Assign the routes to the PISN users of node 2:
   - PISN user 2XX: Route 5
   - PISN user 4XX: Route 7

3. Assign the routes to the PISN users of node 3:
   - PISN user 2XX: Route 5
   - PISN user 3XX: Route 6

Leave the input "Number" empty. This is used if, for instance, the users are virtually networked.

Complete numbers can also be created as PISN users. Exceptions can thus be defined for the blocks. Such numbers can be assigned some names, available for name dial. Calling by name is then possible on the entire network.

Assuming that Mr Newton is a user on node 3, with the call number 420. He should also be reachable from the other nodes through name dial. For this, a PISN user is created in the other nodes with Mr Newton's complete call number:

1. In node 1 and node 2, create a PISN user with the call number 420.
2. In the user configuration of both nodes, assign this PISN user route 7.
3. In the user configuration of both nodes, enter the name for this PISN user.

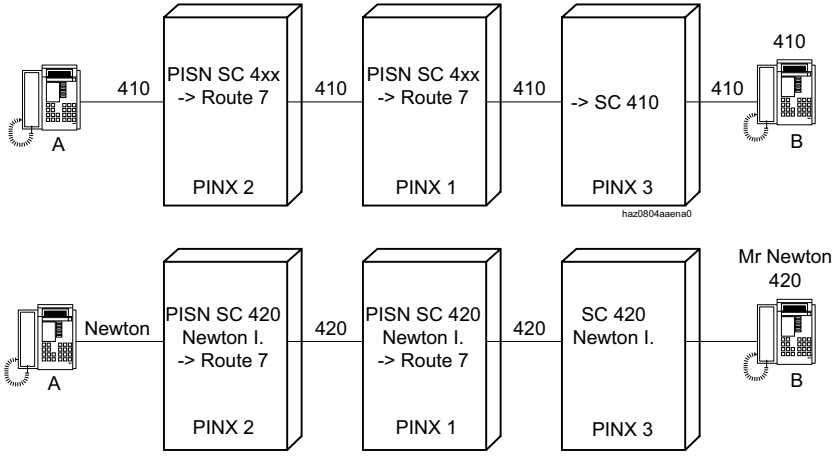


Fig. 43 Input as own PISN user (example)

3. 2. 4. 2 Numbering with regions

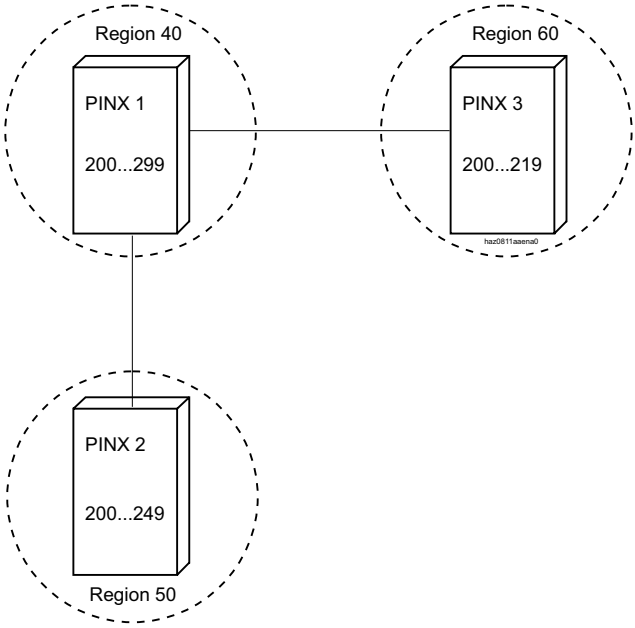


Fig. 44 Numbering with regions

Each node has its own numbering plan. The numbers always start with 200.

If the users of a node wish to call a user of another node, they must dial the corresponding prefix followed by the user number. For instance, if a user of node 2 wishes to reach number 210 on node 3: He dials 60210.

A separate region has to be created for each node (similarly to the regions on the public network). To this end we need to specify the regional prefix for each node:

1. Specify the region for each node:
   - Node 1: Region 40
   - Node 2: Region 50
   - Node 3: Region 60
2. In each node configure the own region prefix under the basic settings:
   - In node 1: Own regional prefix: 40
   - In node 2: Own regional prefix: 50
   - In node 3: Own regional prefix: 60

The further procedure depends on whether region selection is implemented via PISN user or via local area network (see also the explanations on page 54). In the following we shall be looking at both types.

Region selection via PISN user

The regions of all the other nodes are now entered in each node. To do so create numbers in the PISN users category in the numbering plan. There you can create either individual numbers or number ranges by specifying the range with "XX". Each "X" corresponds to one digit place.

1. In node 1 create the following PISN users:
   - One PISN user with the number 50XXX (region of node 2)
   - One PISN user with the number 60XXX (region of node 3)
2. In node 2 create the following PISN users:
   - One PISN user with the number 40XXX (region of node 1)
   - One PISN user with the number 60XXX (region of node 3)
3. In node 3 create the following PISN users:
   - One PISN user with the number 40XXX (region of node 1)
   - One PISN user with the number 50XXX (region of node 2)

Under the user configuration are the PISN users you have just created, with the numbers 40XXX, 50XXX and 60XXX.

The setting options for PISN users differ from those of ordinary internal users. Next use the "route" setting to allocate routes to the PISN users:

1. Assign the routes to the PISN users of node 1:
   - PISN user 50XXX: Route 6
   - PISN user 60XXX: Route 7
2. Assign the routes to the PISN users of node 2:
   - PISN user 40XXX: Route 5
   - PISN user 60XXX: Route 7
3. Assign the routes to the PISN users of node 3:
   - PISN user 40XXX: Route 5
   - PISN user 50XXX: Route 6

Leave the input "Number" empty. This is used if, for instance, the users are virtually networked.

Like for numbering methods with blocks, complete numbers can also be created as PISN users for name dial.

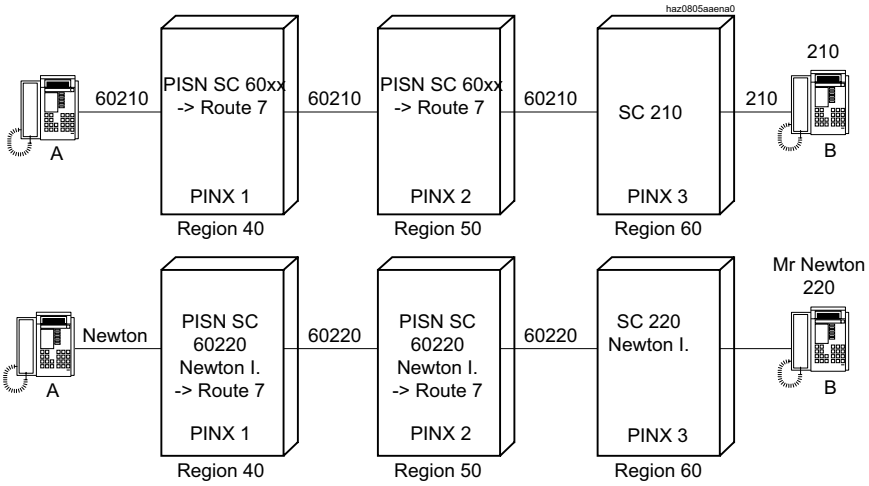


Fig. 45 Input as own PISN user (example)

Region selection via route selection.

The regions of the other nodes are now also entered in each node for this variant. In this case, however, a route with the region's call number is provided for each region in the numbering plan. Simply change the call number of the routes in all three nodes:

1. Change the call number of the routes in node 1:
   - Route 1-6: Call number 50
   - Route 1-7: Call number 60
2. Change the call number of the routes in node 2:
   - Route 2-5: Call number 40
   - Route 2-7: Call number 60
3. Change the call number of the routes in node 3:
   - Route 3-5: Call number 40
   - Route 3-6: Call number 50

A route number prefix (exchange access prefix for the local area network) is always truncated before the call is forwarded. As with this variant the route number prefix is also the regional prefix, the latter is lost. To ensure that a call can nonetheless be

routed to its destination via several transit PINXs, the regional prefix has to be added once again.

For this enter the regional prefixes in the route configuration under "Send Access Code":

1. Enter the regional prefixes of node 1:
   - Route 1-6: Send access code = 50
   - Route 1-7: Send access code = 60
2. Enter the regional prefixes of node 2:
   - Route 2-5: Send access code = 40
   - Route 2-7: Send access code = 60
3. Enter the regional prefixes of node 3:
   - Route 3-5: Send access code = 40
   - Route 3-6: Send access code = 50

With the route selection variant you cannot create complete numbers as PISN users. Dialling by name would have to be organized using abbreviated dialling. You can, however, reach any internal number of any other node, regardless of how long that number is. Assuming Mr Newton in node 3 with call number 220 has a handset with call number 5220. He can be reached by users in other nodes either directly on call number 60220 or on 605220.

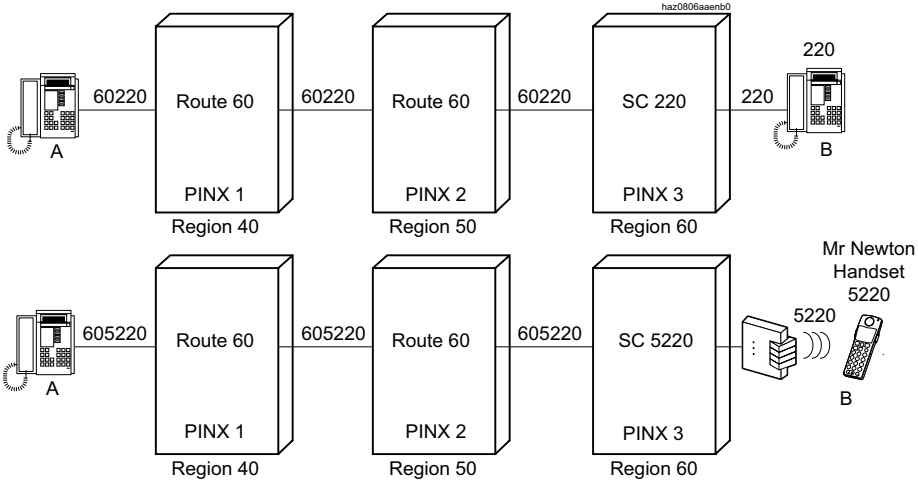


Fig. 46 Route selection with long call number (example)

Note:
With the local area network variant, PISN users cannot be entered as destinations in the call distribution elements. That is why it cannot be used in gateway PINXs in which direct dialling to the public network has been organized.

3. 2. 5 Setting up direct dialling in

In node 1 DDI numbers are created for all the users of the private network. In the corresponding call distribution elements the destination subscribers are entered for each switch position. For users of systems 2 and 3, precisely the same numbers are entered as those that would be dialled by a user of node 1 to call the users of those nodes.

The following example relates to numbering with blocks.

1. In node 1 create the DDI number range provided by your network provider. Each newly created DDI number is automatically assigned a new call distribution element.
2. In the corresponding call distribution elements (CDE) specify the destinations of the DDI numbers for the users of your particular node (node 1), for example:
   - CDE 2, switch position 1 to 3 = user 200
     till
   - CDE 101, switch position 1 to 3 = user 299
3. In the corresponding call distribution elements (CDE) specify the destinations of the DDI numbers for the users of node 2, for example:
   - CDE 102, switch position 1 to 3 = user 300
     till
   - CDE 201, switch position 1 to 3 = user 399
4. In the corresponding call distribution elements (CDE) specify the destinations of the DDI numbers for the users of node 3, for example:
   - CDE 202, switch position 1 to 3 = user 400
     till
   - CDE 301, switch position 1 to 3 = user 499

See also Fig. 37

3. 3 Networking via a public network

Virtual networking, making use of exchange-to-exchange connections, is supported by the node. This means that users can still divert to a destination in the public network, forward calls or set up conferences.

In addition to these options, it is also possible to obtain that subscribers in the public network appear and are handled as network-internal subscribers. For this characteristic to function it is a requirement that the users in the public network use CLIP to identify themselves. The node must use digital network interfaces to link up with the public network.

3. 3. 1 Tying-in an individual user

A remote user with one (or fewer) number(s) is to become part of a private network.

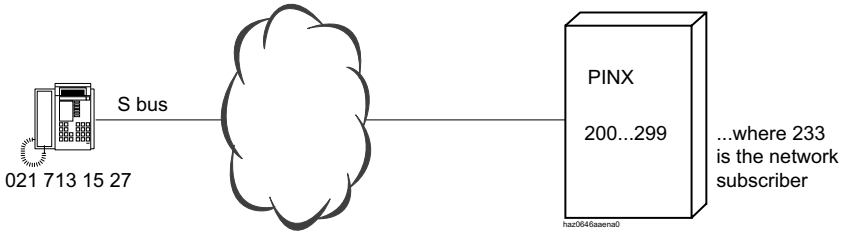


Fig. 47 Virtual network user

The following assumptions are made:

The node's number range is 200...299 and the number 233 should not be an internal number but the remote user. In other words, a call made to number 233 should ring at the remote user's. When the remote user himself makes a call, the call should be displayed as an internal call from number 233.

Route 1 contains the lines for calls to the public network.

Configuration steps:

1. In the node, the number 233 is created as a network user (category PISN users in the numbering plan).
2. The user's name is configured under the user configuration for number 233, along with route 1 and the number 0217131527. The number must be configured in precisely the same way as the public network supplies the number when the remote user makes a call.

The configuration procedure is now completed.

If an internal user dials the number 233, a line from route 1 is seized and the number is dialled.

Conversely, the transmitted CLIP is compared with the configured CLIP number if the remote user dials a number in the node (normally a DDI number). If the numbers match up, the number 233 and the caller's name will be displayed to the called user as the CLIP.

Note:
The incoming CLIP analysis only works once you have exited the configuration.

3. 3. 2 Networking two nodes

The procedure described above can also be used for networking two nodes via the public network.

The users of a node need to have the appropriate DDI numbers so they can be reached directly.

For the correct CLIP to be displayed, each user of the other node has to be entered individually as a PISN user.

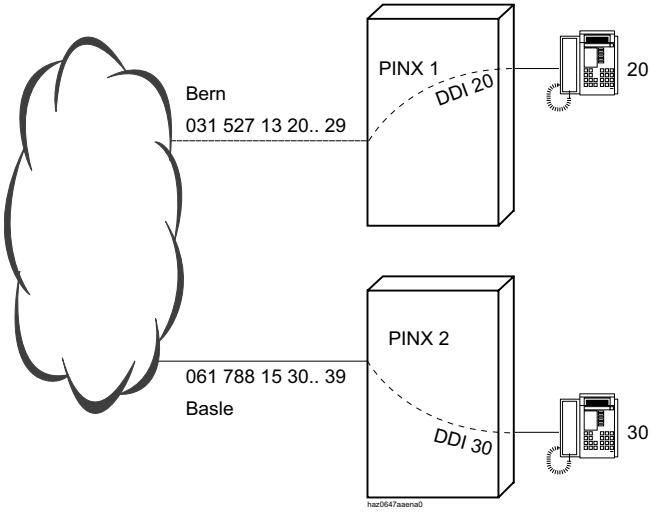


Fig. 48 Two nodes in a virtual network

Node 1 with the DDI range 031 52713 20...29 is located in Bern. The internal numbers 20...29 can also be reached via DDI.
Node 2 with the DDI range 061 788 15 30…39. is located in Basel. The internal numbers 30...39 can also be reached via DDI.
The users in Bern want to be able to reach the users in Basel as if they were internal users, using the numbers 30...39; conversely, the users in Basel want to be able to reach those in Bern with the numbers 20...29.

The direct dialling plan for both nodes and the internal users are configured. The following configurations are used for this purpose:

1. In node 1: in the numbering plan create the number 3x as PISN user.
2. For PISN user 3x enter the route and the number 061788153x.

3. In node 2: in the numbering plan create the number 2x as PISN user.
4. For PISN user 2x enter the route and the number 031527132x.

If user 20 now calls the number 30, the call is set up via the public network using network number 061 788 15 30 and routed to user 30 in node 2 via DDI. User 30 sees the number 20 as the CLIP as user 20 has identified himself in the public network with CLIP 031 527 13 20. This number is implemented in node 2 and displayed as internal user 20, including name and internal ringing.

Note:
The incoming CLIP analysis only works once you have exited the configuration.
If individual users are to be reached using dialling by name, the corresponding PISN numbers need to be created individually and provided with names.

3. 4 Networking with a virtual communication server

The link-up of a virtual communication server in the public network is implemented in exactly the same way as the networking of two nodes.

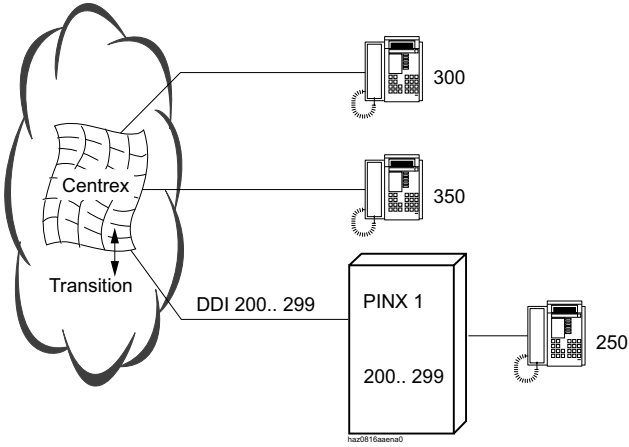


Fig. 49 Networking with Centrex

Node 1 is connected with Centrex. A DDI range 200...299 is defined there.

In other words, Centrex regards all numbers 200...299 as internal numbers in the Centrex range in node 1.

The Centrex range also contains other internal numbers, e.g. 300 and 350.

If user 300 wants to reach user 250, he simply dials 250.

If user 300 wants to reach a user in the public network, he dials 0 (exchange access prefix) followed by the user number, e.g. 032 6241399. For the operation to be exactly the same for a user of node 1, you need to set up the following configurations.

1. All the user numbers in the Centrex range, i.e. 300 and 350, are created as PISN users in node 1.
2. A route is defined (route 2) with the trunk group (trunk group 1) that contains all the exchange lines to the Centrex. PISN users 300 and 350 are allocated the corresponding route (route 2). The protocol in the trunk group must be configured to DSS1 and the type to "Public".

3. An additional route (route 1) is defined for calls to the public network. This is the route configured as the route for exchange output for internal users. Trunk group 1 is also configured in this route.
4. In addition, however, the parameter "Send Access Code" is configured with digit "0" in route 1. This is the exchange access prefix for the Centrex.

If a user in node 1 dials the exchange access prefix 0 followed by the public number, e.g. 032 6241399, node 1 will seize a line from route 1 and immediately dial the digits entered under "Send Access Code", i.e. in this case "0". Only then does the public number follow. Centrex sets up a connection to the public network.

Note:
Calls from the public network reach node 1 via Centrex. The CLIP number is preceded by an exchange access prefix as node 1 is simply an internal user from Centrex's point of view. For the CLIP to be correctly displayed on node 1, the exchange access prefix needs to be deleted again from the communication server. To this end, "Truncate CLIP = 0" is entered in the corresponding trunk group. This means that when a CLIP number beginning with "0" is received, the "0" is truncated.

3. 5 Networking with third-party systems

In principle all network-compatible third-party systems that support the QSIG standard can be used as node. However, some restrictions in the features available are possible. The following points are to be observed:

Compatible QSIG protocol

In practice, different QSIG protocols are used. The variants differ, above all, in terms of communication technology. Aastra 400 Communication servers support all listed versions. They can be selected under the *Protocol* trunk group setting. Make sure you always use the same version between two nodes.

Tab. 7 Supported QSIG variants

Aastra 400 QSIG variants	QSIG	Standard	Remarks
QSIG	ETSI-QSIG	ETS 300172-1 Issue (1994) (ETSI-QSIG)	Also known as: • ECMA • ECMA-1 • ECMA-V1
QSIG / PSS1 ISO	ISO-QSIG		For backward compatibility with older Aastra communication servers. Callback on busy is supported on a homogeneous network only.
QSIG / PSS1 ISO (2)	ISO-QSIG	ETS 300172-2 Issue (1995) - references ISO Standard 11572. (ISO-QSIG)	Also known as: • ECMA-2 • ECMA-V2

Outgoing calls via a third-party system

There are instances where third-party systems do not recognize a call to be forwarded to the public network based on its numbering plan identifier. For this reason an exchange access prefix for the third-party system should be sent with the call (see variant 2 on page 67).

Incoming calls via a third-party system

Aastra 400 communication servers can use the call number's numbering plan identifier to determine whether an incoming call is to be forwarded to the public network (NPI = E.164) or within the internal network (NPI = PNP). However, some third-

party systems use only NPI = E.164 in general. To enable a third-party system route the call correctly, proceed as follows:

1. Set up the third-party system in such a way that outgoing calls to the public network are not routed via the same lines as outgoing calls that remain within the private network.
2. In the Aastra 400 communication servers, set two trunk groups for the lines to the third-party system:
   – In the first trunk group combine all the lines via which calls to be forwarded on to the public network are received.
   – In the second trunk group combine all the lines via which calls to be forwarded on within the private network are received.
3. Set the parameters of the first trunk group as follows:
   – Protocol = PSS1
   – Network type = private
   – Overwrite NPI = no
4. Set the parameters of the second trunk group as follows:
   – Protocol = PSS1
   – Network type = private
   – Overwrite NPI = PNP

Incorrect CLIP indication

Third-party systems may not use the numbering plan identifier of a CLIP number to create a correct CLIP. This is why it is possible that the CLIP number of a call from a third-party system is not displayed correctly.
The settings need to be adapted accordingly for such cases (see Chapter " Identification elements" in the system manual "Features of an Aastra IntelliGate").

Cordless systems in a private leased-line network

The Aastra 400 DECT cordless system is tied to a single communication server. The radio area cannot be increased by networking several communication servers.

Abbreviated dialling and virtual network subscribers

In the past virtual network subscribers were set up with abbreviated-dialling numbers. While the same procedure can still be used, setting up a PISN user offers a number of significant advantages:

- An incoming call from a virtual network user is signalled internally and an internal number is displayed as the CLIP.
- A separate route can be defined for the outgoing routing.

4 SIP Networking

This chapter describes how two or more Aastra 400 communication servers can be networked via the SIP network interfaces. A brief introduction is followed by a step-by-step explanation of configurations involving a two-node network. The configuration in a network involving several nodes depends on the type of networking and is therefore described in principle only. The chapter ends with a list of the features available between the terminals of different systems when the systems are networked via SIP.

4. 1 Introduction

Two or more Aastra 400 communication servers (max. 100) can be networked via the SIP network interfaces. Networking with other systems is also possible (e.g. Aastra IntelliGate, Aastra 800 or Aastra 5000 systems). The principle is comparable to QSIG networking on an ISDN basis.

Just like with QSIG networking via the IP network, all nodes are interconnected via the IP network during SIP networking. If the systems are separated locally and interconnected via WAN (Wide Area Network), security using authentication (exchanging name and password), VPN (Virtual Private Network) and SRTP (Secure Real-Time Transport Protocol) and TLS (Transport Layer Security) is of the utmost importance.

In the same way as with QSIG networking, star-shaped centralised networking configurations as well as meshed networking configurations are possible.

In star-shaped networking, the signalling data always runs via the central communication server. The drawback is that delays can occur and that two SIP Access Channel licences are also required for each transit connection on the central communication server.

For these reasons meshed networking should be given preference over star-shaped networking.

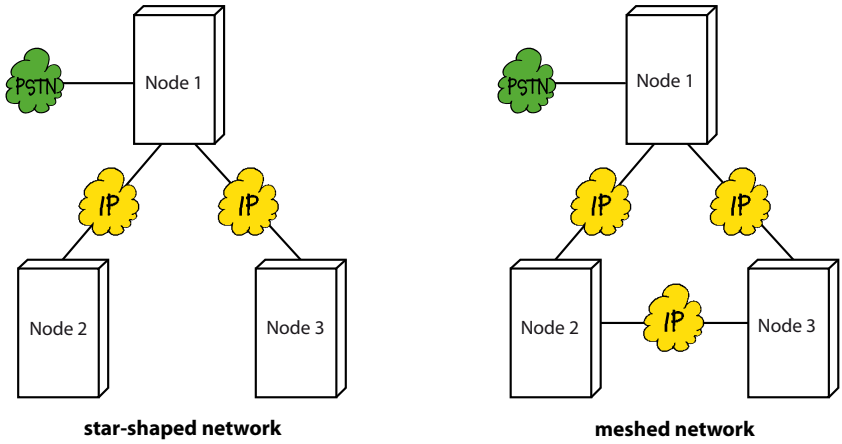


Fig. 50 SIP networking types

4. 2 SIP networking with two nodes

The figure below illustrates the way in which two locally separate nodes are networked, with only node 1 connected to the public network.

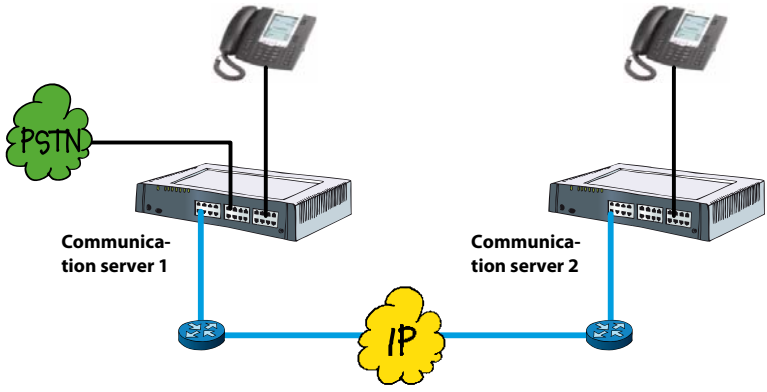


Fig. 51 SIP networking of two locally separate nodes

The section below describes the procedure in principle and the particularities of SIP networking. Here it is assumed that mutual authentication is required.

Configuring nodes

Requirement:
The communication servers must have a sufficient number of licences for SIP access channels and VoIP channels; VoIP resources must also be assigned to DSP chips.

They configure the nodes via the administration tool WebAdmin. To do so proceed as follows:

1. Navigate to the *SIP networking* (navigation code: =uy) and edit the user name and password of your node.
2. Create a new remote SIP node and enter the node name, a trunk group to be created complete with trunk group name, the IP address and the port of the remote node.
3. On the remote SIP node you have just created set the *Authentication required*parameter to *Yes*.
4. Enter the user name and password for the remote SIP node.
5. Configure the bandwidth area and the NAT settings.
6. Configure as indicated in Tab. 8 the SIP trunk group you have just created.
7. Specify a route for internal connections to the remote node and give it a name. Assign to the route the SIP trunk group you have just created and configure the parameters as indicated in Tab. 9.
8. Only nodes 1:
   - Configure a trunk group to the exchange, unless this has already been done.
   - Configure the route for external connections to the exchange (unless this has already been done) and assign the exchange trunk group.
   - Cofigure the *transit route* (PISN user, navigation code view: =gv). It must correspond to the route to the public exchange.
9. Only nodes 2:
   Specify a route for external connections to the public exchange via node 2 and give it a name. Assign to the route the SIP trunk group you have just created and configure it as indicated in Tab. 10.
10. Create the users of the remote node as PISN users and assign them the route to the remote node.

Tab. 8 Trunk group settings in nodes 1 and 2

Parameter	Setting	Note
Network type	*Private*	
Cut CLIP	0	Corresponds to "Exchange access, business"
Direct dialling plan	blank	Default value must be deleted
Transit CLIP format	*Unknown with national prefix*	
Transit exchange access prefix	0	Corresponds to "Exchange access, business"

Tab. 9 Route settings in nodes 1 and 2 for internal connections

Parameter	Setting	Explanation
Send access code	blank	
Numbering plan identifier (NPI)	*PNP*	

Tab. 10 Route settings in nodes 2 for external connections

Parameter	Setting	Explanation
Send access code	0	Corresponds to "Exchange access, business"
Numbering plan identifier (NPI)	*Unknown*	

4. 3 SIP networking with several nodes

SIP networking with several nodes is carried out in a way similar to SIP networking with two nodes. The configuration depends on the networking type and the number of gateways to the public telephone network. In principle, however, the following applies:

- You need to create one SIP node and one SIP trunk group for each connection to another node. For all SIP nodes enter the IP address, port and access data of the target node.
- If the node has direct access to the public network, you also need to define a *Trunk group* for the exchange access and to configure the*Transit route*.
- For each internal connection to another node and for each connection possibility to the public network configure one *Route* and assign the corresponding *Trunk group*.
- The users of other nodes must be created as *PISN users*.

4. 4 Features supported

The features available between the terminals of different nodes in SIP networking are restricted compared with PISN/QSIG networking.

The following features are supported:

- Display call number (CLIP) and name (CNIP)
- Enquiry/Hold/Brokering
- Call transfer with/without prior notice
- Conference (variable, preconfigured)
- Call Forwarding Unconditional (CFU) and Call Forwarding on No Reply (CFNR)
- Deflect/reject call during ringing phase
- Do not disturb
- Recall
- Transmit DTMF signals
- T.38 protocol for FoIP (Fax over IP)

Index

A

Aastra 13
About this document 9

B

Break-in 38
Break-out 37

C

Call routing 43
Clock propagation diagram 50
Communication protocol 23
Conformity 6
Connection 27, 44

D

Data protection 8
Data service 34

E

Environment 7
Exchange Access 44
Exclusion of Liability 7

F

Floor view 11

G

Gateway-PINX 59

H

Heterogeneous network 15
Homogeneous network 15

L

LCR 35
Leased-line network 17
Least Cost Routing (LCR) 35
Limited Warranty (Australia only) 10
List view 11

N

Networking 16
Networking type 16
Networking via SIP 86
Numbering 54
Numbering plan 28

O

Overflow routing 35

P

PISN 14
  nodes 25
Planning aid 41
Planning rule 53
Private network 14
Product information 5
Protocol 48
Public network 57

Q

QSIG networking via the IP network. 16

R

Regions 28
Reliability aspects 49

S

Safety information 7
Service 34
Shared Numbering Plan 28
SIP networking 86
Synchronisation 50

T

Topology 16
Trademarks 6
Traffic Volume 42, 45

U

User information 5

V

Virtual networking 19

W

WAN 86