Aastra Business Communication Solution

AIN and IP system phones as of R1.0

System Manual

Platforms supported:

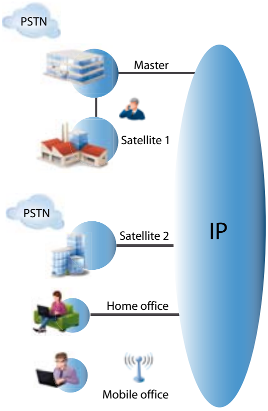
Aastra 415

Aastra 430

Aastra 470

This system manual is designed to assist you with the planning and implementation of VoIP-based installations.

It describes how to connect IP system phones to the communication server and to network several communication servers via the IP network to create an Aastra Intelligent Net (AIN).



syd-0401_en / 1.0 – R1.0 – © 06.2011

Content

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).

Aastra Intelligent Net (AIN) networks several Aastra 400 communication servers into a single fully-fledged communication system with a complete range of features. The individual nodes are independent of one another in terms of location and are controlled by a Master node. Networking is via the IP network.

User groups

The phones, softphones 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 the PC operator console or call centre applications do require training of the personnel.

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 DocFinder:	www.aastra.com/DocFinder

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 documentation packs. 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 a Aastra 400 communication solution into operation.
- Ensure that all end users have access to the User's Guides.

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.

Trade names

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 relating to these third-party products is listed in the User's Guide of the Aastra 400 product in question.

Exclusion of Liability

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 is 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

Hazard warning

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. 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 an Aastra 470 communication server can also be operated in a redundant configuration 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 unauthorized 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 authorized persons have access to the IP addresses of the Aastra 400 products.
- Limit the number of user accounts to the minimum necessary and only assign the authorization profiles actually required to the user accounts.
- 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 to 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 can only be used in compliance with national data protection provisions.

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

- 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 system manual

This System Manual describes how to connect IP system phones to a communication server and how to network several communication servers to create a Aastra Intelligent Net (AIN). While it complements the Aastra 400 System Manual it does not replace it. The Manual is available in German, English, French, Italian and Spanish.

The system manual is intended for planners, installers and maintenance personnel. The configuration, commissioning and successful operation of an Aastra Intelligent Net (AIN) requires knowledge of the contents of the manual. All guidelines, user notes and hazard alert messages must be observed.

Document information

- Document number: syd-0401
- Document version: 1.0
- Valid as of: R1.0
- © 06.2011 Aastra Technologies Limited
- In PDF viewer, click on this link to download the latest version of this document: *https://pbxweb.aastra.com/doc_finder/DocFinder/syd-0401_en.pdf?get&DNR=syd-0401*

Hazard alert messages

Special hazard alert messages with pictograms are used to signal areas of particular risk to people or equipment.

Hazard:
Failure to observe information identified in this way can put people and hardware at risk through electrical shock or short-circuits respectively.

Warning:
Failure to observe information identified in this way can cause a defect of the product or to a module.

Note:
Failure to observe information identified in this way can lead to equipment faults or malfunctions or affect the performance of the system.

1. 5 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 communications 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.

2 System description

Aastra Intelligent Net (AIN) networks several Aastra 400 communication servers into a single fully-fledged communication system with a complete range of features. The individual nodes are independent of one another in terms of location and are controlled by a Master node. Networking is via the IP network.

With its consistent array of features throughout and a shared numbering plan the system as a whole presents itself as a single, homogeneous communication system, and the individual nodes are not perceived as such by the users.

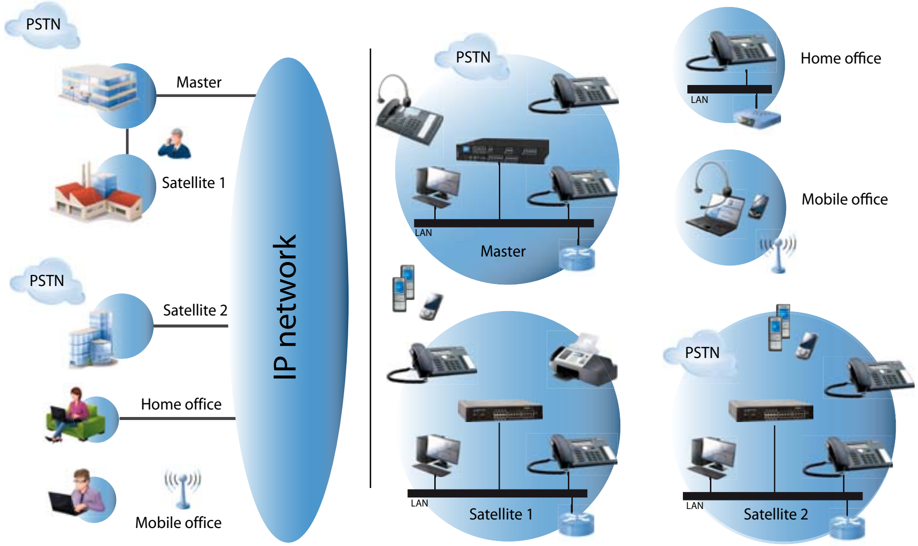


Fig. 1 AIN and IP system phones expand the Aastra 400 platform to the IP network

One node (Master) controls the other nodes (satellites). The Master is used to configure the satellites and update their software. This unique architecture greatly expands the application possibilities of Aastra 400 systems, e. g.:

- The modular expansion of the system limits in areas that are otherwise covered only by larger and more expensive communication servers.
- The integration of several sites and branch offices (up more than 40 nodes) even beyond national and language borders.
- The expansion of the DECT coverage range through genuine roaming between nodes with overlapping radio area.

Network properties

All IP system phones are fully integrated in the AIN. They are controlled directly by the Master, independently of the location at which they are operated.

Connections are set up with a minimum of VoIP channels and resources since the terminals involved are always connected with one another by a direct route and are no transit-routed via nodes that are not involved.

An ingenious bandwidth control prevents poor connection quality due to lack of bandwidth on the IP network.

Optional encryption of call and signalling data provides protection against any tapping and/or tampering of IP phone calls. The encryption methods used guarantee a high level of data protection, authenticity, integrity and protection against replay attacks throughout the network.

If a node is isolated from the Master by an interruption in the IP connection, it continues to operate in offline operating mode with its own local configuration until contact with the AIN is restored.

User benefits

These variety of expansion opportunities offer the user a number of exemplary advantages:

- Networked, locally remote and already installed single systems can be grouped together cost-effectively to form a single telecommunication system. This increases the telephony convenience for all users, from staff members to customers.
- Call charges are reduced inasmuch as phone calls made between nodes do not incur any charges, unlike networking via the public telephone network.
- A complete range of features across the entire AIN, regardless of the location of the individual nodes. The AIN eliminates the limits of PISN networking, and features such as forwarding and three-party telephony, text messages or announcements are available between all the nodes without restriction. Other features that were previously limited to a single system are available throughout the AIN, e.g. user groups with members from the entire network, central operator console, voice mail, announcement service with node-specific texts, network-wide call logging, coded ringing/general bell and door intercom systems.
- Thanks to integrated IP system phones, small branches no longer have to dispense with their own communication servers. Home office staff and users who travel a great deal can be fully integrated.
- Use of satellites as DECT server for implementing large DECT systems.

- Roaming between the nodes of an AIN enables DECT radio coverage to be expanded almost at random using only one cellular network. The cellular networks of individual DECT systems no longer have to be overlapped; what’s more the number of radio units is reduced, which also helps to lower costs.
- Telephone lines do not have to be extended when expanding an existing infrastructure with new connections for PCs and telephones.
- As a result of the expansion of the Aastra 400 platform to the IP data network the network used becomes part of the Aastra 400 system. As an alternative calls can also be routed via the PSTN (PSTN overflow) so that communication quality is not affected by interruptions or bottlenecks in the IP network.
- The PSTN overflow allows also a cost-optimised routing configuration in the AINso far as the VoIP channels and bandwidths in the IP network are designed for an average traffic load, and part of the calls during peak times are routed via the public network.

Benefits for planners, installers and dealers

The same tried-and-tested aids are used whether you want to operate single systems or AIN networks:

- The Aastra Plan Project Manager is used for planning and drawing up quotations for an AIN.
- For the configuration and administration use AMS, the tried-and-tested configuration interface also for single systems.
- For user and call charge administration use the System Assistant access of the web-based communication interface WebAdmin.
- For remote access use your region's SRM platform.

Likewise there are very few differences with regard to the telephony-side configuration: When you configure an AIN, you essentially configure the Master node.

3 Setting up an AIN

This chapter takes you through the planning and implementation of an Aastra Intelligent Net with Master, satellites and IP system phones. With the aid of a reference network it guides you through the planning, installation, configuration and commissioning procedures.

The following Aastra 400 communication servers can be used as AIN nodes:

- **Aastra 470** – can be used as Master or satellite.
- **Aastra 430** – can be used as Master or satellite. Restriction: Can only be used as a satellite if the AIN has one or more Aastra 470 nodes.
- **Aastra 415** – can only be used as a satellite.

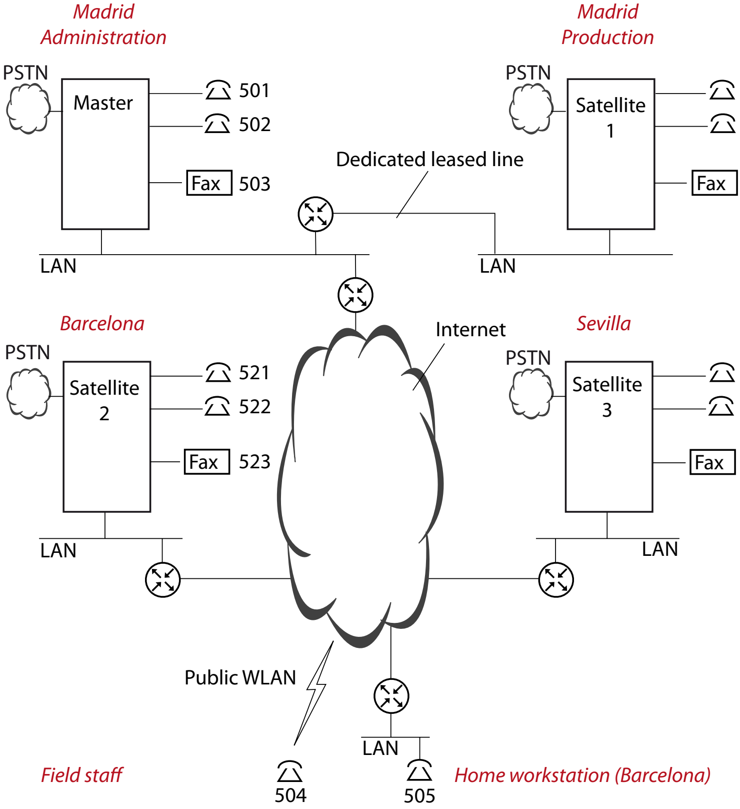


Fig. 2 The AIN of a sample business organization as a reference network

Tab. 1 The node locations in the reference network

Node	Organizational unit	Location	Designation
Master	Administration headquarters	Madrid	Madrid Administration
Satellite 1	Production headquarters	Madrid	Madrid Production
Satellite 2	Branch office	Barcelona	Barcelona
Satellite 3	Branch office	Seville	Seville
Home workstation	Home workstation	Barcelona	Barcelona HO
Mobile workstation	Field staff		Field staff

3. 1 Planning

The aim of the planning phase is to provide all the necessary data to install, configure and commission an AIN.

This chapter takes you through the necessary planning steps using a reference network. The following assumptions provide the starting point:

- The sample business organization operates an IP network that covers all its sites.
- Single systems are in operation at three locations and are to be integrated into the AIN.
- At the Seville location a new system is used as an additional AIN node.

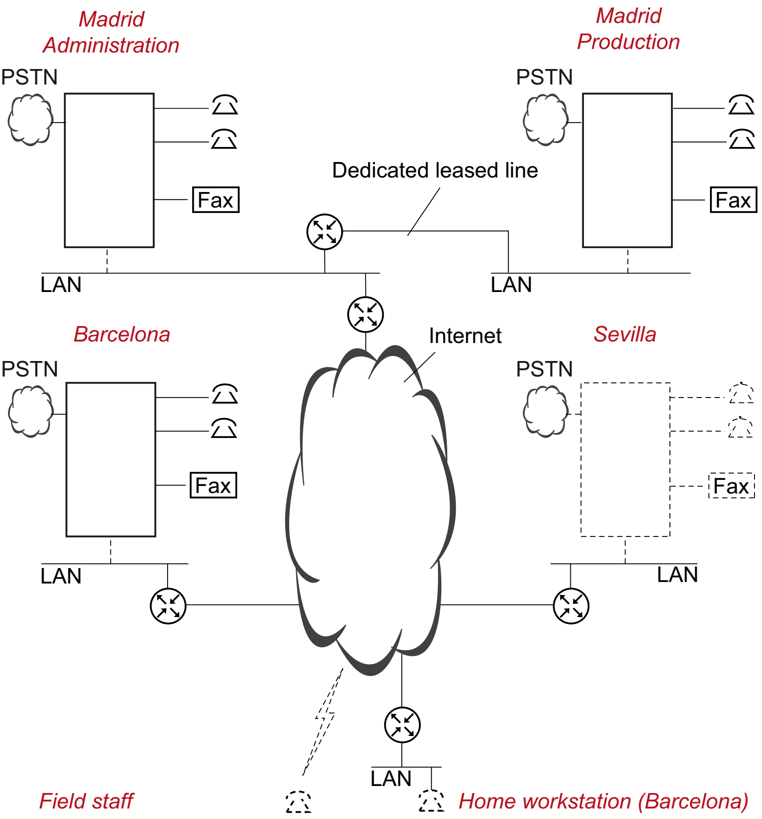


Fig. 3 Basic situation within the reference network

Tab. 2 Single systems to be connected as nodes to the AIN reference network

Node	Communication server / IP system phones	Status
A	Aastra 470	In operation as a single system
B	Aastra 430	In operation as a single system
C	Aastra 430	In operation as a single system
D	Aastra 415	Planned
Home workstation	Aastra 5370ip	Planned
Mobile workstation	Aastra 2380ip	Planned

3. 1. 1 Auxiliary

Planning an AIN requires a careful and meticulous procedure as aspects of both IT and telephony need to be taken into account. That's why we strongly recommend that you use the aids listed here when planning your project.

AIN/VoIP planning document

The planning document is an online form drawn up in MS Word format. Together with the System Manual and the Aastra Plan Project Manager this document helps you to plan an AIN or to plan the use of IP system phones and SIP phones.

Planning an AIN usually requires a co-operative effort involving the customer and telephone and IT specialists. The planning document facilitates communication between the subscribers. Also our specialists will be happy to assist you on the basis of the completed checklist.

You can print out the document and fill it out by hand; however the support of the dropdown lists will not be available if you do.

This document also includes an MS PowerPoint file with an icon library, which you can use to visualise the project.

The document can be downloaded from the DocFinder: document number appl-003 (German) or appl-004 (English).
(http://www.aastra.com/docfinder).

Aastra Plan Project Manager

The Aastra Plan Project Manager uses the requirements determined on the customer's premises to calculate the optimum configuration for the Aastra 400 system or even several systems connected into a single Aastra Intelligent Net (AIN). It selects the appropriate Aastra 400 models for your requirements and generates diagrams, priced parts lists and offers based on Word and Excel formats, which you can then easily edit.

3. 1. 2 Specifying nodes and networking them into an AIN

The instructions below explain the procedure for defining the nodes in the AIN and the number of IP system phones. Use the Aastra Plan Project Manager to specify the hardware required.

Specify the AIN nodes

1. Define which of the existing single systems you want to integrate into the AIN.
2. Check whether the rating of the single systems already in operation is sufficiently large. If a single system has reached its expansion limits, an additional node can be used at its location.
3. Define which new single systems are needed to implement all the AIN nodes (in the reference network a new single system is to be added to the node at the Seville site).

Note:
In the case of a cross-national AIN, make sure you order single systems that are designed for the country in question.

While you can subsequently change the country (sales channel), any licences already acquired will lose their validity (see also"AIN areas", page 58).

4. Check whether it would make sense to set up separate nodes as DECT servers. If for instance in the reference network the Production and Administration Divisions are in the same location and a DECT system is to be set up with full area coverage, it makes sense to set up a particularly node as a DECT server.

Note:
Configuring and maintaining the offline mode of a DECT server is relatively complex as user mutations always have to be carried out once in AIN mode and once in offline mode.

If the DECT server is located in the same bandwidth area as the Master, you can dispense with setting up an offline mode as the likelihood of a connection interruption between Master and satellite is small.

5. Determine which node is to be used as Master. All the other nodes are then satellites.

Specify the codecs

The G.711 codec (uncompressed) or G.729 codec (compressed) is used to digitise or convert the call data into a VoIP channel for transmission in the IP network. DSP resources are required in the nodes and the IP terminals for the encoding and decoding process in real time. While G.711 needs fewer DSP resources for processing but more bandwidth within the IP network, G.729 needs more DSP resources but less bandwidth.

IP and SIP system phones have sufficient DSP resources to process both codecs. DSP resources in the nodes are scalable and also assignable to other applications.

You can choose whether G.711 is to be used exclusively in your AIN or whether G.711 or G.729 is to be used depending on the link. You can also choose between the non-encrypted and the encrypted variant:

- Select the G.711 or secure G.711 codec if there is plenty of bandwidth available for all the IP links over which call data is to be transmitted[1)].
- Select the G.711/G.729 or secure G.711/G.729 codec if there are IP links on which the bandwidth on offer is unknown, tight or expensive.

Map AIN in the Aastra Plan Project Manager

1. Open Aastra Plan and log on.
2. On the home page click the *Plan several nodes* button and start a new configuration.

   The network view appears.
3. Enter the nodes of your AIN one by one. Make sure you select nodes of the type *Aastra 400*.
4. Add a node of the type *IP network*.

   All the nodes are now shown on the networking diagram. The nodes are listed in table form below the diagram.
5. In the diagram click first on the node you want to specify as the Master, then on the *IP network* nodes.

   A *Connect* button appears at both nodes.
6. Click one of the *Connect* buttons

   The Connection dialog box appears.

[1)] Node ↔ node / IP or SIP phone ↔ node / node ↔ SIP provider

7. Select the codec you want (see "Specify the codecs", page 20) and click the *Ok* button.

   The IP link is drawn in. The specified codec is valid for the entire AIN, i.e. also for the IP links to the satellites, which you create next.

8. Create the IP links for the satellites by repeating the procedure step by step for each satellite, but without setting the codec separately in the Connection dialog box.

   The nodes are now defined and networked with one another via the IP network. To configure an individual node, click the 📄 pictogram in the node in question.

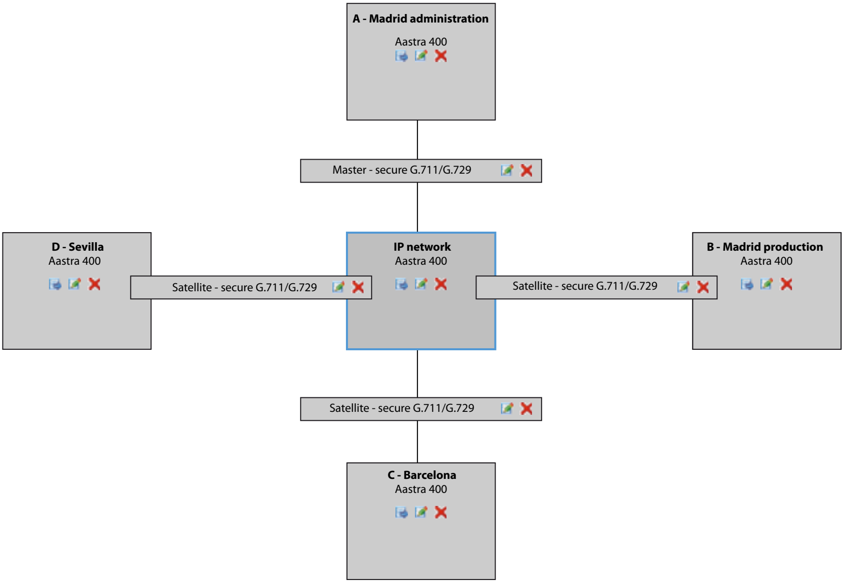

A - Madrid administration
Aastra 400
Master - secure G.711/G.729
D - Sevilla
Aastra 400
Satellite - secure G.711/G.729
IP network
Aastra 400
Satellite - secure G.711/G.729
B - Madrid production
Aastra 400
Satellite - secure G.711/G.729
C - Barcelona
Aastra 400

Fig. 4 The reference network in Aastra Plan

3. 1. 3 Configuring the node expansion

In the following you use Aastra Plan to configure the expansion of each individual node. The sequence is irrelevant. You do not need to enter every single detail at this point; however it is important for calculating the VoIP channels required and therefore for the rating of the DSP resources that you enter all the components that generate a traffic load in the AIN. That includes in particular the terminals and the exchange accesses. The following sections explain various aspects you need to pay particular attention to with regard to the AIN.

To access the expansion configuration of an individual node, click the pictogram of the node in question either in the networking diagram or in the networking table.

Note:
For the sake of clarity, only individual phones have been configured in the reference network.

IP and SIP phones

Regardless of their location the IP and SIP phones for AIN operation are all registered with the Master (see "IP system phones", page 67). However, in the expansion configuration with Aastra Plan they are entered at the relevant nodes:

- Enter the IP and SIP phones of a particular location at the node of that particular location.
- Enter remote IP and SIP phones in a similar way to home workstations or mobile workstations on the Master.

In the example of the reference network the following IP phones are configured in the Master:

- An Aastra 5370ip for the home workstation
- An Aastra 2380ip for the mobile workstation
- An Office 1560IP as PC operator console (located at the Madrid administration)

Connections to the public network

Exchange accesses can be set up at each node for all AIN users so that each node does not necessarily have to have its own exchange access. Criteria for a separate exchange access include:

- If a satellite is located in a different area to the Master, so that regional emergency destinations can be reached directly.
- If the connection to the Master is interrupted and the satellite is to enable telephone traffic in offline mode also (see "Satellite in Offline Mode", page 62).
- If you want to provide an overflow to the public network (see "PSTN Overflow", page 47).
- If you prefer to route calls from individual users via the PSTN (e. g. for fax connections without T.38 or connections with PISN users or integrated mobile phones).

Note:
If a node does not have its own exchange line circuit and its exchange connections are set up via another node (transit node), the traffic load between the two nodes can rise considerably and increase the number of VoIP channels required.

Defining supplementary equipment

Plan the use of additional functions and equipment such as voice mail, CTI applications, door intercom systems, external switching of the switch group or fax transmission. Also take note of the instructions as set out in the Chapter "Region-related Settings", page 58.

3. 1. 4 Designing the VoIP channels

A VoIP channel is set up for every call connection via the AIN. The real-time processing of the call data requires DSP resources at the source and end nodes (see also "Specify the codecs", page 20).

Aastra Plan (*System* / *AIN* view) calculated based on the configured phones, terminals and exchange line circuits, the anticipated traffic load and the VoIP channels required as a result. Both the traffic load within the AIN and the traffic load generated by the exchange transit traffic are taken into account. The result is based on the assumption of an average traffic density. However you have the possibility of manually correcting the calculated value upwards or downwards if required.

Aastra Plan then assigns the most suitable DSP resources to the calculated VoIP channels and determines the licences required.

3. 1. 5 Specifying the numbering plan

As far as the numbering plan is concerned there is only one Call Manager with a single numbering plan. This is the Master's internal numbering plan. It contains all the users and call numbers of the AIN. The individual nodes have neither a separate call number nor a separate call number prefix.

The instructions below explain the procedure for specifying the numbering plan in the AIN:

1. Specify the call number range and the call numbers of the individual users. It is up to you whether you number all the users in sequence for the entire AIN or whether you specify a separate number range for each node.
2. Assign the appropriate phones and terminals to each user.

   For the sake of simplicity the users in the reference network are assigned only one phone or terminal in each case.

Tab. 3 Numbering the users in the reference network (see Fig. 2)

Call number	Node	Terminal	Call number	Node	Terminal
501	Master	Aastra 5370ip	511	Satellite 1	Aastra 5370ip
502	Master	Aastra 5370ip	512	Satellite 1	Aastra 5370ip
503	Master	Group 3 fax machine	513	Satellite 1	Group 3 fax machine
521	Satellite 2	Aastra 5370ip	531	Satellite 3	Aastra 5370ip
522	Satellite 2	Aastra 5370ip	532	Satellite 3	Aastra 5370ip
523	Satellite 2	Group 3 fax machine	533	Satellite 3	Group 3 fax machine
504	Mobile office	Aastra 2380ip	505	Home workstation	Aastra 5370ip

3. 1. 6 Specifying the IP addressing

You can address AIN nodes as well as SIP and IP phones either via DHCP and DNS or using static addressing. Hybrid forms are also possible. The communication servers of the Aastra 400 series also have an integrated DHCP server. This provides many possibilities for the IP addressing. However please note the following:

In the AIN, satellites as well as SIP and IP phones each search for the Master and register with it. The Master therefore acts as a server for the other AIN elements.

Tip:
Static node addressing is stable and in most cases it is simplest.

An overview of the different possible types of addressing can be found under "Overview of possible IP configurations", page 28

After the first start of a communication server dynamic addressing with DHCP is activated; the model name followed by the MAC address is specified as the host name (e. g. Aastra430-00085d8031a6).

SIP and IP system phones are always logged on to the Master regardless of their location in the AIN and are also configured there. For the offline operation of a satellite IP system phones can also be logged on to the satellite, see "IP system phones in offline mode", page 65.

Note:
Whatever the addressing method used, it is important to ensure that the AIN elements recognise one another via the WAN links too.

Static addressing in the reference network

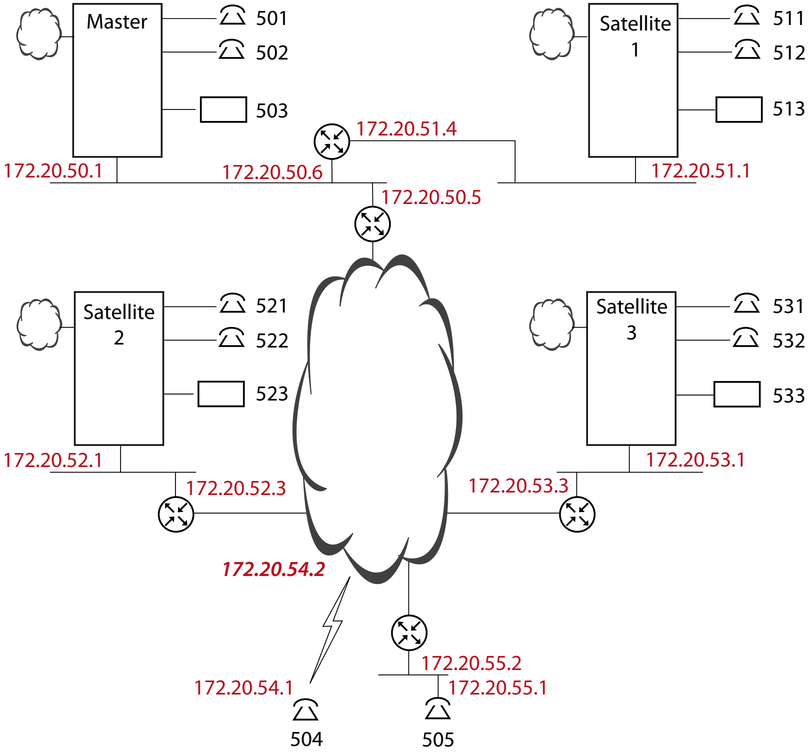


Fig. 5 Network diagram with IP addresses

Tab. 4 IP addresses of the nodes in the reference network

Node	IP address	Subnet mask	Gateway address
Master	172.20.50.1	255.255.255.000	172.20.50.5
Satellite 1	172.20.51.1	255.255.255.000	172.20.51.4
Satellite 2	172.20.52.1	255.255.255.000	172.20.52.3
Satellite 3	172.20.53.1	255.255.255.000	172.20.53.3

Overview of possible IP configurations

The table below illustrate you the different possibilities for IP addressing using the example of the Master and the first satellite in the reference network.

Tab. 5 Examples of possible IP configurations in the reference network

Parameter	Static	DHCP/DNS	Static and DNS
Master:			
• *Host name*	-	aastra400master[1]	aastra400master[1]
• *IP address*	172.20.50.1	[2]	172.20.50.1
• *Subnet mask*	255.255.255.0	[2]	255.255.255.0
• *Gateway*	172.20.50.5	[2]	172.20.50.5
• *Master address*	-	-	-
• *DHCP*	No	Yes	No
• *Primary DNS server*	-	[2]	<IP address>
• *Secondary DNS server*	-	[2]	<IP address>
• *Domain name*	-	[2]	<Name>
Satellite 1:			
• *Host name*	-	aastra400sat1	aastra400sat1
• *IP address*	172.20.51.1	[2]	172.20.51.1
• *Subnet mask*	255.255.255.0	[2]	255.255.255.0
• *Default gateway*	172.20.51.4	[2]	172.20.51.4
• *Master address*	172.20.50.1	*aastra400master*	*aastra400master*
• *DHCP*	No	Yes	No
• *Primary DNS server*	-	[2]	<IP address>
• *Secondary DNS server*	-	[2]	<IP address>

[1] The default value is the model designation followed by the MAC address (e. g. Aastra430-00085d8031a6.

[2] Automatically assigned values are displayed.

3. 1. 7 Planning an IP network

The instructions below explain the procedure for checking your IP network and specifying the necessary measures to make it compatible with VoIP.

Note:

- Please note that the know-how of an experienced network technician is essential for assessing and optimizing the network neighbourhood.
- We urge you to examine the network using a special check list, which you can download from our document server (http://www.aastra.com/docfinder, appl-003 document (German) and appl-004 (English)). Our specialists will be happy to assist you on the basis of the completed checklist.

1. Check whether your network neighbourhood meets our recommendations ("IP network requirements", page 84) and if necessary take the necessary measures to fulfil the requirements.
2. Specify the prioritization method as set out under "Prioritization", page 87.

   DiffServ is activated as default value. ToS and CoS are deactivated (DiffServ is recommended if the voice connection is to be set up via a WAN link. CoS prioritizes voice traffic at the level of the switches).

   Plan the use of VPN in accordance with the instructions set out in "Using VPN", page 90.
3. Plan the bandwidth control in accordance with the instructions set out in "Bandwidth control", page 93.

3. 2 Installation

The purpose of the installation phase is to set up the AIN so that it can be configured. However unlike a single system a number of basic configurations are required during the installation phase and the nodes must already be in operation before configuration begins.

The following steps are required to set up an AIN using single systems:

- Integrating single systems into the IP network – page 30
- Checking AIN operation – page 36
- Putting IP system phones into operation – page 38 .
- Synchronizing the application software in the AIN – page 38

3. 2. 1 Integrating single systems into the IP network

The instructions below explain the procedure for configuring the IP address coordinates of the single systems:

- Detecting the communication servers in the IP network – page 30
- Static IP addressing – page 33
- Dynamic IP addressing using DHCP and DNS – page 35

3. 2. 1. 1 Detecting the communication servers in the IP network

New communication servers connected to the IP network may not be reachable under all circumstances without the prior configuration of the IP addressing. In this chapter you learn how to establish a connection between AMS and the new systems.

First-start behaviour

If a manually entered IP address is already stored at the time of the first start, the communication server deactivates DHCP and DNS and starts with the static IP address.

When you connect a communication server to the IP network for the first time, it attempts to reach an IP address via DHCP:

- If a DHCP server offers the communication server an IP address, the address is used and the communication server attempts to register with the DNS server under the name <Model name>-<MAC address>.
- If the communication server is not offered an IP address, it starts up under its entered default address.

Detecting a communication server with System Search

AMS comprises a tool called System Search used for detecting Aastra 400 communication servers in the IP network. With System Search AMS is able to find all the connected communication servers located in the same subnet as the PC with AMS. Newly added communication servers can be addressed directly with System Search and can be opened automatically in AMS.

Detecting a communication server without System Search

If System Search is unable to detect a new communication server because it is connected in a different subnet, you have the following possibilities for contacting the communication server:

- If the communication server was able to register successfully with the DNS server, it can be reached under the host name <Model name>-<MAC address> (e. g. Aastra430-00085d8031a6).
- If the communication server logged on under the static default IP address, it can only be reached via the IP network if the address happens to be in the subnet’s address range. If not, you need to preconfigure the communication server's IP address in accordance with the instructions set out in the next section.

Preconfiguration of the IP addressing

If the communication server cannot be reached via the IP network, its IP address has to be adjusted first. To do so proceed as follows:

1. Adjust your PC's IP address so that it is within the same address range as the communication server's default address (see Tab. 6).
2. Connect the Ethernet interface on the PC with AMS directly to the Ethernet interface on the communication server or via a switch.

   Note:
   You can use either a conventional patch cable or a crossover cable to do so.
3. Open a communication server and enter the default address under *IP address or host name* (see Tab. 6).
4. Set up an AMS online connection and configure the IP addressing under CM_2.2.1.
5. Disconnect the AMS online connection and put your PC's IP address back to its original setting.
6. Reconnect the communication server to the IP network and restart.

   The communication server can now be reached under the newly configured address.

Tab. 6 Default values for IP addresses

Parameter	Parameter value
IP address	192.168.104.13
Subnet mask	255.255.255.0
Gateway address	0.0.0.0
DHCP	*Yes*
Host name	<Model name>-<MAC address> (e. g. Aastra430-00085d8031a6)

3. 2. 1. 2 Static IP addressing

Follow these instructions to set up an AIN using new single systems and to address them statically in the IP network.

Putting the Master into operation

The Master must always be put into operation as the first system so that the satellites can then log on to it. To do so proceed as follows:

1. Connect the communication server to the IP network and start it.
2. Use System Search to find the communication server. Select it and adapt the IP addressing:
   - Deactivate DHCP (*DHCP*=*No*).
   - Carry out the IP addressing (enter the IP address, subnet mask and default gateway) and click the *Save* button.
3. Click the *Configure..* button. The communication server is then added in the AMS Shell under the selected group.
4. In the AMS Shell define the communication server as Master (*Mode*=*Master*)
5. Read out the EID number and purchase an AIN licence (CM_1.2). Enter the new licence number.
6. Disconnect the AMS online connection and transfer the configuration data to the AMS database.

   The Master is now in operation and ready to receive satellite registrations.

Putting the satellites into operation

Next put the satellites into operation:

1. Connect the communication server to the IP network and start it.
2. Use System Search to find the communication server. Select it and adapt the IP addressing:
   - Deactivate DHCP (*DHCP*=*No*).
   - Carry out the IP addressing (enter the IP address, subnet mask and default gateway) and click the *Save* button.
3. Click the *Configure..* button. The communication server is then added in the AMS Shell under the selected group.
4. In the AMS Shell define the communication server as a satellite (*Mode*=*Satellite*)
5. Set up the AMS online connection and enter the IP address of the Master under *Master address* (CM_2.2.1).
6. Transfer the configuration data to the AMS database and restart the communication server.

   The satellite searches for the Master and logs on to it.
7. Set up the AMS online connection to the Master and open the Card Configuration (CM_2.1.1).
8. Select the satellite mainboard and activate the function *Confirm system configuration*. The mainboard and expansion cards are confirmed and included in the AMS configuration.
9. Put the next satellite into operation.

Note:
If the communication server is not in the same subnet as the PC with AMS, System Search will not be able to find it. If so, alter the procedure as indicated under "Detecting a communication server without System Search", page 31).

3. 2. 1. 3 Dynamic IP addressing using DHCP and DNS

Follow these instructions to set up an AIN using new single systems and to address them in the IP network using DHCP/DNS.

Putting the Master into operation

The Master must always be put into operation as the first system so that the satellites can then log on to it. To do so proceed as follows:

1. Configure the DNS server so that it allows dynamic DNS updates.
2. Connect the communication server to the IP network and start it. This registers with the DNS server under the name <Model name>-<MAC address>.
3. Use System Search to find the communication server. Select the communication server and click the *Configure* button. It's added under the selected group in the AMS Shell.

   You can also open the communication server in AMS without System Search and enter the host name manually (*IP address or host name* setting).
4. In the AMS Shell define the communication server as Master (*Mode*=*Master*)
5. Set up the AMS online connection, read out the EID number and purchase the AIN licence. Enter the new licence number.
6. Transfer the configuration data to the AMS database and save.

Putting the satellites into operation

To put the satellites into operation proceed as follows:

1. Connect the communication server to the IP network and start it.
2. Use System Search to find the communication server. Select it and click the *Configure…* button. It is then added in the AMS Shell under the selected group.
3. In the AMS Shell define the communication server as a satellite (*Mode*=*Satellite*)
4. Set up the AMS online connection and adjust the IP addressing:
   - Enter the name of the satellite under *Host name* (e. g. *A400sat1*).
   - Enter the name of the Master under *Master address*, (e. g. *A400master)*.
5. Restart the communication server: Satellite logs on to the Master.
6. Set up the AMS online connection to the Master and open the Card Configuration (CM_2.1.1).

7. Select the satellite mainboard and activate the function *Confirm system configuration*. The mainboard and expansion cards are confirmed and included in the AMS configuration.
8. Disconnect the AMS online connection and transfer the configuration data to the AMS database.
9. Put the next satellite into operation.

Note:
If the communication server is not in the same subnet as the PC with AMS, System Search will not be able to find it. If so, alter the procedure as indicated under "Detecting a communication server without System Search", page 31).

3. 2. 2 Checking AIN operation

Once all the nodes have been commissioned the AIN is operational: The Master has identified all the satellites; the signalling between Master and satellites is working; and call connections can be set up.

You can also check the status of the AIN on site without the aid of AMS using the display on the individual nodes.

The AIN operation status indication on the Aastra 470

On the Master the integrated user interface provides the following information:

- IP addresses of all the satellites.
- Call connection status of each satellite with the Master (online/offline)

On the Satellite the integrated user interface provides the following information:

- IP address of the Master
- Call connection status with the Master (online/offline).

The AIN operation status indication on the Aastra 430

LED display of the satellite offline operation:

- Operation status indication on the Master:
  No indication of the operation status of the AIN.
- Operation status indication on the satellite:
  If the SYS LED is flashing green/orange, the node is in offline mode and has lost its connection with the Master.

Connection to the Master interrupted

To determine why a satellite cannot establish a connection with the Master, proceed as follows:

1. Check whether the missing satellite is up and running. If the satellite itself has no malfunction, it is either running in offline mode or currently carrying out a restart (see also "Satellite in Offline Mode", page 62).
2. Try and ping the missing satellite. If it cannot be pinged, the cause could be an error in the IP addressing.
3. For dynamic IP addressing: Check whether the Master is entered under its host name in the DNS server by entering the command "*nslookup* <Host Name>" at the DOS prompt.
4. Check the Master to see whether a sufficient number of satellites have been licensed.
5. Check whether the Master's name and/or IP address are correctly entered in the satellite configuration. If the input is incorrect, the satellite will be unable to find the Master.
6. Check whether the satellite has the same software version as the Master.
7. Once the connection to the Master is restored, the satellite automatically carries out a restart in offline mode before logging on with the Master again. You can also run the restart manually if you do not want to wait for the timeout of the connection monitors.

3. 2. 3 Putting IP system phones into operation

The instructions below explain the procedure for installing and commissioning the IP system phones. To do so proceed as indicated under "IP system phones", page 67. Please note that all IP system phones are always logged on to the Master and configured for AIN operation regardless of their location.

3. 2. 4 Synchronizing the application software in the AIN

Note:
It is imperative that all the nodes in the AIN always have the same software standard. For this reason you should always synchronize the application software at the nodes before definitively commissioning the operation of the AIN.

The node application software is synchronized using the Upload Manager. First load the software onto all the nodes; next on the Master initiate the software update on all the nodes. To do so follow the detailed instructions in the Upload Manager Help and the instructions related to your System Manual.

Besides the system software the software package also includes the software for the IP and SIP system phones.

3. 2. 5 Excluding a satellite

Proceed as follows to exclude from AIN operation any satellite that has already been set up:

1. Use AMS to set up an online connection with the satellite and open the IP configuration (CM_2.1.1).
2. Delete the Master’s address under *Master Address*.
3. Restart the satellite (menu *Reset communication server* / *Restart*).
4. Use AMS to set up an online connection with the Master and open the Card Configuration (CM_2.1.1_*Slot configuration*).
5. Select the satellite mainboard and activate the function *Confirm system configuration*. The mainboard and expansion cards of the satellite are now deleted from the configuration.
6. Open the view *AIN nodes* (CM_6.1.1) and delete the satellite from the list of satellites.
   The satellite and all the relevant data are now deleted from the AIN.

3. 3 Configuration

The purpose of the configuration phase is to set all the parameters of the AIN, for both AIN operation and satellite offline operation. AIN operation is configured entirely via the Master; satellite offline operation is configured directly on each of the satellites.

The instructions below explain the procedure for first configuring AIN operation; the configuration is then transferred to the satellite offline configuration using a special AMS function designed specifically for this purpose. If required you can also proceed in reverse order and configure the satellite offline operation first and then transfer the satellite configurations for AIN operation.

3. 3. 1 Configuring AIN operation

You can carry out the settings for AIN operation online directly on the Master using AMS or prepare all the settings in the AMS offline mode and then load them onto the Master. Refer to the AIMS online Help for more information AMS.

The entire AIN is configured via the Master as if it were a single communication server. The individual nodes are identified by their node numbers. Node 0 is always the Master. The satellites are numbered in the sequence in which they logged on to the Master. The complete port address is therefore *Node 2 Port 0.10-1*.

Also take note of the indications provided under "Region-related Settings", page 58 and "Restricted functions in the AIN", page 66.

First configure the basic data such as the direct dialling plan, numbering plan, users and abbreviated dialling lists. You have the possibility of re-using data that has already been entered.

1. Log on to the Master system online or offline using AMS and open the Configuration Manager.
2. If your AIN consists of nodes that were already in operation prior to AIN integration and if their numbering plans can be merged into a single numbering plan without conflict, you can transfer the basic data to the AIN. To do so, select the function *Transfer AINbasic configuration from satellites* in the AMS Shell.

   The function transfers the user and terminal data complete with the relevant numbering plan and port data. It always takes the data from all the satellites in the AIN. It is not possible to transfer data from individual satellites.
3. Draw up or complement the AIN’s basic configuration.

Next complete the AIN configuration:

1. Configure the node-specific settings for the AIN.
2. Configure the AIN regions in accordance with the information given in "Region-related Settings", page 58.
3. Configure the PSTN overflow in accordance with the information given in "PSTN Overflow", page 47.
4. Configure the routing for integrated mobile phones and PISN users in accordance with "Routing outgoing calls via local nodes", page 52.
5. Configure the emergency number destinations for the AIN. Please note that nodes in other areas usually also have other emergency destinations. These nodes should have their own exchange accesses so that the emergency destinations can be dialled directly.
6. Configure the switch groups for the AIN.
7. Configure the DECT system.

   In regular AIN operation all the cordless phones are logged on to the Master. Users are able to use their cordless phones on the same call number in the radio area of each node without having to log on there specially (roaming).
   Log the cordless phones onto DECT system A to ensure that the software of the cordless phones is also updated whenever the Master software is updated.
8. Configure the other devices and features such as LCR, door intercom systems, music on hold or a voice mail system.

3. 3. 2 Configuring offline operation for the satellites

You can carry out the settings for offline operation of a satellite online directly on the satellite using AMS or prepare all the settings in the AMS offline mode and then load them onto the satellite.

To speed up your configuration work, you can use an AMS function to copy part of the configuration data automatically from AIN operation to the satellite configuration.

To configure offline operation proceed as follows:

1. From the AMS Shell select any node in the AIN.
2. From the *Tools* menu select the function *Transfer basic satellite configuration from AIN*.
   This node's data configured in the configuration for AIN operation is imported into the satellite's database and is then available for offline operation.
3. From the AMS Shell select the first satellite, log on offline and open the Configuration Manager.
4. Complete the offline configuration, taking account of the indications in the Chapter "Satellite in Offline Mode", page 62.
5. Save the data and log out again.
6. Load the configuration data into the communication server using an upload.
7. Repeat the procedure as of step 4 for each satellite.

4 Communication server as AIN node

This Chapter contains information on the basic properties of the AIN and the specific properties of a communication server used as an AIN node.

4. 1 Routing in the AIN

In normal operation, routing between the AIN nodes is entirely via the IP network. Locally separated AIN nodes must then often be connected to the IP network via tightly calculated WAN links. Routing in the AIN has therefore been designed so that a minimum of bandwidth resources are used even for complex routing situations such as a global call to a user group with scattered users. The following methods are used to achieve this:

- Direct routing of the call data between the AIN nodes and separate transmission of signalling and call data, page 42
- Optimized resource management, page 43
- PSTN overflow, to cover connection resources during peak loads, page 47

4. 1. 1 Direct routing of call data

A call is always controlled and signalled by the Master, even if the Master itself is not involved in the call. This means that the nodes and IP system phones only communicate with the Master and never directly with one another. Unlike the actual call connection is always set up directly between the nodes and the IP system phones concerned.

The example below illustrates this situation using a simple call connection. (Fig. 6).

User 511 on satellite 1 calls user 531 on satellite 3:

- Satellite 1 notifies the Master that it wants to set up a connection to satellite 3 (signalling).
- The Master checks whether a free VoIP channel is available at both nodes.
- If a VoIP channel is available at both nodes, the Master uses bandwidth control to analyse whether there is sufficient bandwidth available for the connection (see "Bandwidth control", page 93).
- If so, the Master instructs satellite 3 to call user 531 and satellite 1 to feed the ring-back tone to user 511 (signalling).

- Satellite 3 signals to the Master that user 531 has answered the call; the Master then instructs satellite 1 and satellite 3 to set up the connection (signalling).
- The call connection between satellite 1 and satellite 3 is set up.

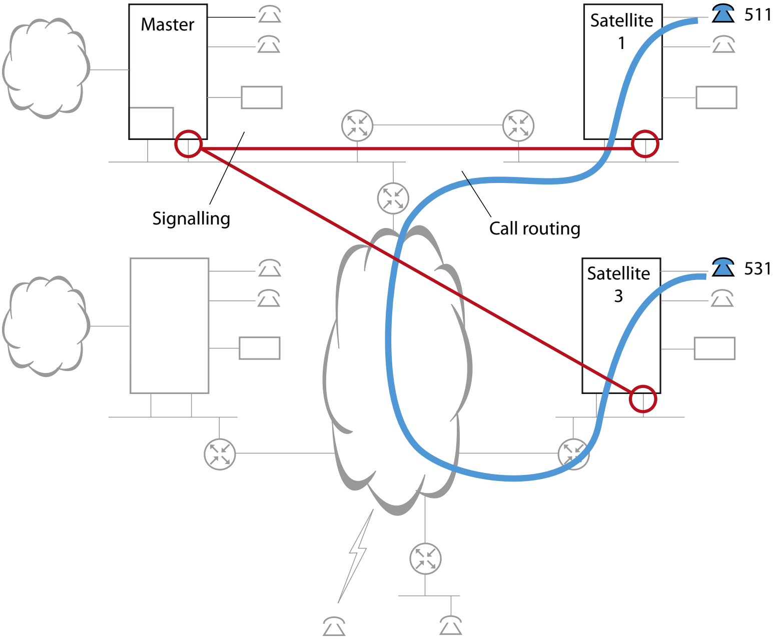


Fig. 6 Routing a simple call

4. 1. 2 Optimized Resource Management

Routing in the AIN is designed so that a routing situation can be implemented with a minimum of media and bandwidth resources. In the following you will find out more about resource management for enquiry calls, conferences and user groups.

Note:
If the WAN links via the Internet are protected in each case with independent VPNs, calls are always routed via the IP network with the Master, which largely cancels out the resource-saving function of resource management. Therefore always try and implement VPNs routed via an internet provider (see "Using VPN", page 90).

4. 1. 2. 1 Enquiry call and brokering in the AIN

The destination user for an enquiry call can be anywhere in the AIN. During the enquiry call the active connection is put on hold. Brokering is used to switch back and forth between the enquiry call connection and the original connection. To avoid having to reserve an unnecessary amount of bandwidth in the IP network, only one VoIP channel is used on the common section of the two connections, and that channel is used by whichever of the two connections is active.

In the example below user 501 brokers between user 521 and user 531.

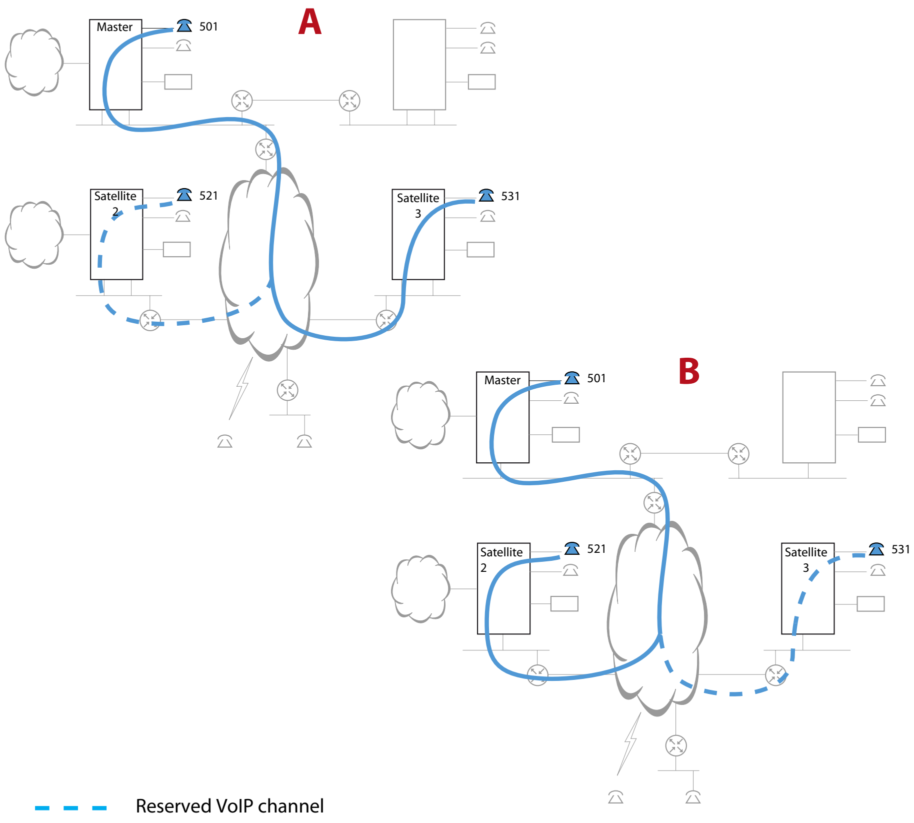


Fig. 7 Callback and brokering in the AIN

4. 1. 2. 2 Conference circuit and announcement in the AIN

A conference circuit in the AIN never requires more than one VoIP channel between two AIN nodes. This is enabled with the following resource management:

- The Master always places the conference node in the AIN node with the most conference participants. Which of the users involved actually set up the conference is irrelevant.
- A conference can also have several conference nodes: As soon as more than one user is involved in the conference at one AIN node, another conference node is set up at that node.
- With each change in the user constellation the optimum conference configuration is recalculated and the conference is set up anew without the participants in the conference noticing.

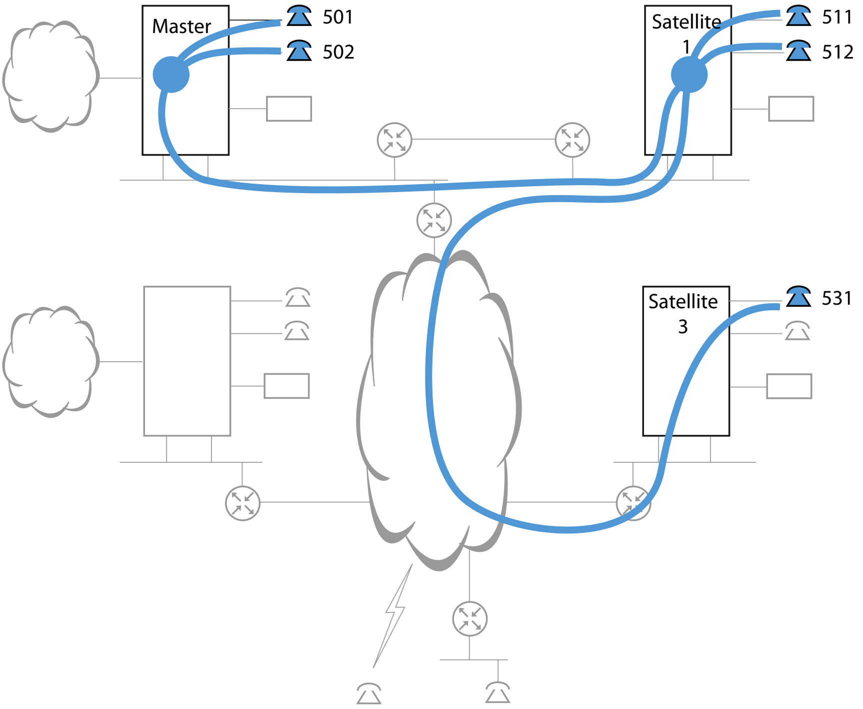


Fig. 8 Conference circuit in the AIN

The same method is also used for an announcement to several users.

4. 1. 2. 3 User group with global call

Members of a user group can be scattered throughout the AIN. The necessary bandwidth resources have to be available in the IP network to ensure that the connection is set up the instant a call is answered. If the call distribution is made simultaneously (globally) to all the users, the bandwidth resources must be available to each user even though once the call is answered the resources are required for one connection only. To avoid having to reserve an unnecessary amount of bandwidth, thereby obstructing the voice traffic in the AIN, only a single VoIP channel is reserved on each section. As soon as a user answers the call, the connection is set up and the reserved bandwidth is freed up on the sections that are not concerned.

In the example below, user 501 dials the call number of a user group with global call distribution. User 511 answers the call.

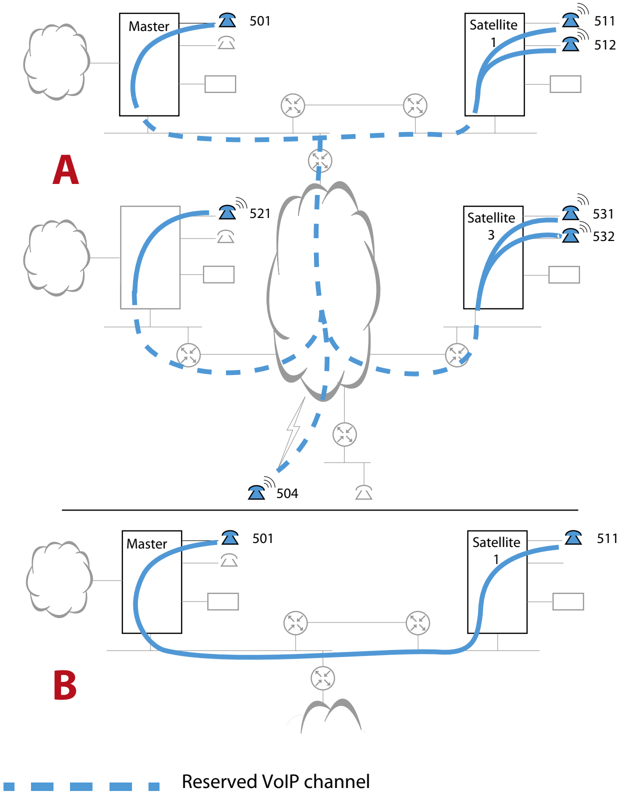


Fig. 9 Call to a user group in the AIN

4. 1. 3 PSTN Overflow

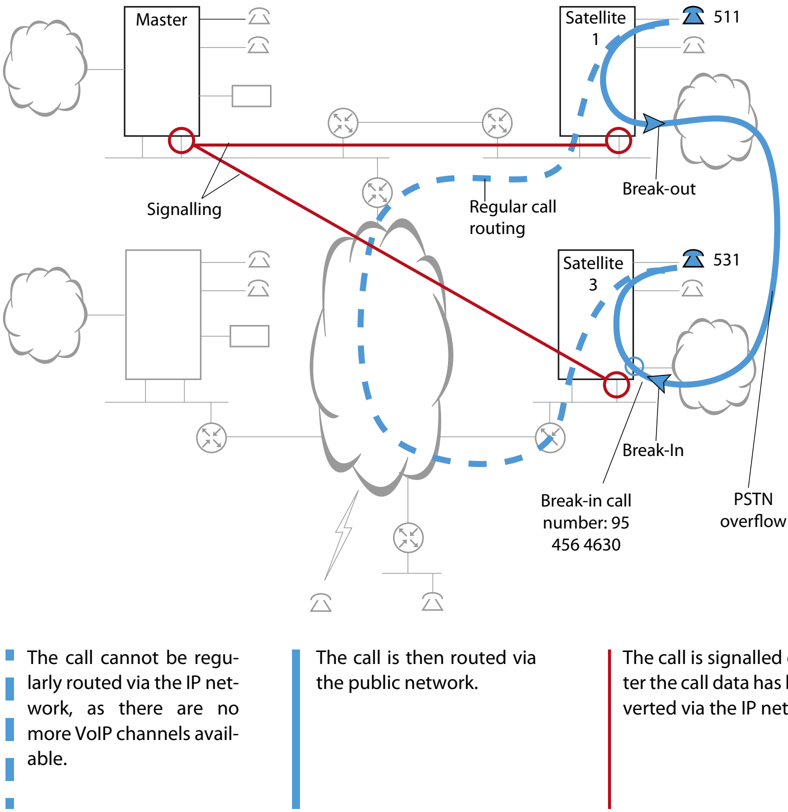
The PSTN overflow automatically routes calls via the public network if there are no more VoIP channels available via the IP network. This allows a cost-optimised routing configuration in the AIN so far as the VoIP channels and bandwidths in the IP network are designed for an average traffic load, and part of the calls during peak times are routed via the public network.

PSTN overflow is supported for direct internal to internal, internal to external, and external to internal connection. Caller identification (CLIP) is also automatically transmitted.

The example below shows the function of PSTN overflow using a simple call connection. (Fig. 10 on page 48).

User 511 on satellite 1 calls user 531 on satellite 3:

- Satellite 1 notifies the Master that it wants to set up a connection to satellite 3.
- The Master checks whether a free VoIP channel is available at both nodes.
- If no free VoIP channel is available at least at one of the nodes, the Master checks whether the conditions for PSTN overflow are in place.
- If overflow can be initiated, the Master triggers the dialling of one of the direct dialling numbers at the source node (satellite 1) set up for the destination node (satellite 3). At the same time he signals to satellite 3 that there is a call on this direct dialling number and for which destination user the call is intended.
- On the one hand the Master instructs satellite 3 to call user 531 and on the other satellite 1 to feed the ring-back tone to user 511.
- Satellite 3 signals to the Master that user 531 has answered the call and the connection is set up via the public network.



The call cannot be regularly routed via the IP network, as there are no more VoIP channels available.

The call is then routed via the public network.

The call is signalled even after the call data has been diverted via the IP network.

Fig. 10 **PSTN overflow**

Call routing via the PSTN can also be forced for individual users. Calls by these users are then routed via the PSTN even if there are still sufficient VoIP channels available to route the call by regular means via the IP network. In this way you can consistently route fax calls, for example, via the public network (see also "Fax data transmission in AIN", page 54).

4. 1. 3. 1 Suitability and limitations

PSTN overflow is suitable for the following applications:

- Routing peak loads between AIN nodes via the PSTN
- Routing fax connections in the AIN (as an alternative to FoIP, see page 55).
- Emergency routing between AIN nodes via the PSTN in the event of interruptions in the IP network.

It is not suitable for routing all call connections in an AIN via the PSTN as a matter of principle.

Please take good note of the following restrictions:

- The break-in and break-out of the PSTN overflow is supported via ISDN network interfaces (BRI-T and PRI).
- If a satellite is connected with the Master via QSIG, the break-in and break-out of the PSTN overflow is also supported via the QSIG interfaces. This, however, only if the AIN has one satellite.
- A call that has already been answered via PSTN overflow cannot be forwarded via PSTN overflow.
- Calls to or from IP and SIP phones are always routed via the IP network.
- PSTN overflow is available only for point-to-point connections. The function is not available for conference, call waiting, intrusion and announcements.
- With calls to a user group whose members are spread over several satellites, only members of the first satellite are called via the PSTN overflow. Members at the other nodes are called only if the connection can be set up via the IP network. This also applies if the other satellites are connected to the Master via the PSTN.
- Throughout the AIN a maximum of 30 calls can be routed via the PSTN simultaneously using PSTN overflow.

4. 1. 3. 2 Configuration of the PSTN overflow

To set up the PSTN overflow proceed as follows:

Specifying authorisations

1. Enable PSTN overflow in general for the entire AIN (CM_6.1.3, setting *Enable PSTN overflow in AIN*).

   Nodes connected via QSIG can be separately enabled for PSTN overflow (CM_6.1.3, setting *Enable PSTN overflow on PISN*).
2. Disable PSTN overflow for all phones and terminals to be barred from this feature (CM_4.1, setting *PSTN overflow = No*).
3. Disable PSTN overflow for external calls to the direct dialling numbers to be barred from this feature (CM_3.1.3, setting *Enable PSTN overflow in the (AIN) = No*).
4. Enable PSTN overflow for all phones and terminals whose calls are to be routed via the PSTN only if the connection cannot be established via the IP network (e.g. for all fax machines if FoIP is to be used for the fax connections in normal operation (CM_4.1), setting *PSTN overflow = if necessary*.
5. Force PSTN overflow for all phones and terminals whose calls are always to be routed via the PSTN and never via the IP network, e. g. for all fax machines (CM_4.1, setting *PSTN overflow = Always*).

Creating the break-in configuration

1. Define for each node a direct dialling number via which a diverted call is to be routed from the public network to the node in question (CM_6.1.1, setting *Break-in call number*)
2. Link all the direct dialling numbers created in this way for break-in with the same call distribution element. For all three switching positions select *PSTN overflow* (CM_3.1.4, *CDE Destinations*) as the CDE destination.

   Leave the remaining CDE settings unchanged on their default values.

Creating the break-out configuration

1. Specify for each node the route to be used for the break-out. (CM_6.1.1, *Break-out route* setting).
2. Specify for each node how many calls from each node can be routed via the public network (CM_6.1.1, setting *Allowed break-out connections*).

The PSTN overflow is now set up.

Tab. 7 PSTN overflow on the example of the reference network

Parameter[1]	Parameter value	Explanation
Classes of service:		
• System-wide: *Enable PSTN overflow in AIN*	*Yes* or *No*	Allows you to enable or disable PSTN overflow throughout the system (CM_6.1.3)
• Terminal-specific: *PSTN overflow*	*No* / *If necessary* / *Always*	Allows you to enable, disable or force PSTN overflow specifically for individual terminals. (CM_4.1)
• Direct dialling number-specific: *Enable PSTN overflow*	*Yes* or *No*	Allows you to enable or disable PSTN overflow specifically for individual direct dialling numbers (using CDE) (CM_3.1.3)
Break-In configuration:		
• *Direct dialling number → CDE No.*		Break-in direct dialling number with allocation to the break-in CDE (CM_3.1.4_*CDE destinations*)
Master	600 → 601	
- Satellite 1	610 → 601	
- Satellite 2	620 → 601	
- Satellite 3	630 → 601	
• *Break-in call number*		Enter complete call number without access prefix. Complement with country code if nodes are in different countries. (CM_6.1.1_*AIN nodes*)
Master	91 123 1600	
- Satellite 1	91 234 2610	
- Satellite 2	93 345 3620	
- Satellite 3	95 456 4630	
• Call Distribution Element for Break-In:		Only one break-in CDE is required in the entire AIN (CM_3.1.4_*CDE destinations*).
- *Name*	Break-In	
- *Call number*	601	
- *CDE destination*	*PSTN overflow*	
Break-out configuration (to be configured for all the nodes):		
• *Break-Out route*	1	Outgoing routing configuration (CM_6.1.1)
• *Allowed break-out connections*	10	Restriction in the number of break-out connections (CM_6.1.1)

[1] All the settings are made on the Master

4. 1. 4 Routing outgoing calls via local nodes

Outgoing calls from integrated mobile phones and PISN users are routed according to their allocated routes. This may result in unwanted detours in the AIN that can be avoided by a customised route configuration.

Without a customised route configuration, the call will always be routed to the public network via the first route defined in the trunk group, no matter from which node the call originates. With an optimised route configuration, the calls to integrated mobile phones and PISN users are routed into the public network at the node on which the caller is located (assuming the node has access to the public network).

Proceed as follows to configure the routes of integrated mobile phones and PISN users for optimised call routing:

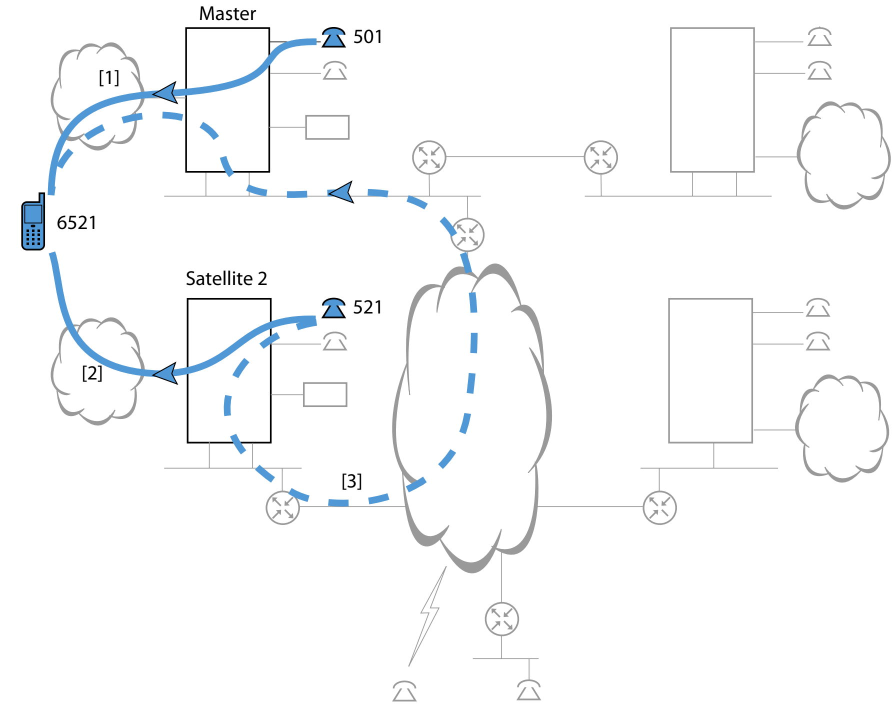
1. Configure a route for integrated mobile phones users and one for PISN users.
2. Allocate trunk groups of all nodes with network connections to the routes.
3. Select *Yes* for the route setting *Use network interfaces first.*

The following example (Tab. 8 and Fig. 11) shows the route when internal users on the master and on satellite 2 call the integrated mobile phone user 6521.

Tab. 8 Example: Optimized route configuration for the user of an integrated mobile phone

Parameter[1]	**Parameter values**
Configuration for a user with integrated mobile phone (CM_4.1):	
• *Call number*	6521
• *Route*	7
Trunk group configuration (CM_3.1.5):	
• Trunk group 1, 2	Network interfaces on the master
• Trunk group 11, 21 and 31	A network interface each is on satellite 1, 2 and 3
Route configuration of route 7 (CM_3.1.5):	
• Trunk group allocation	1, 2, 21, 31, 41
• *Use network interfaces on the node first.*	*Yes*

[1] All the settings are made on the Master



[1] Routing via trunk group 1 (setting *Use network interfaces first* =*Yes* or *No*)

[2] Routing via trunk group 21 (setting *Use network interfaces first* =*Yes*)

[3] Routing via trunk group 1 (setting *Use network interfaces first* =*No*)

Fig. 11 Example: Routing outgoing calls to integrated mobile phones or PISN users

User 521 on satellite 2 dials call number 6521. Based on the sequence of the trunk group allocation, the system first attempts to establish the call via trunk group 1 in the master. The setting *Use network interfaces first* =*Yes* reverses the trunk group sequence, and the trunk group with the network interfaces on the node of the caller is placed at the beginning. The allocation sequence of the trunk group is thus 21, 1, 2, 31, 41 and no longer 1, 2, 21, 31, 41 as specified in the route.

4. 2 Fax data transmission in AIN

The AIN provides the following possibilities for transmitting fax data:

- Fax-over-IP (FoIP):
  Transmission of the fax data in the IP network using the fax transmission protocol T.38. This is the most reliable method for transmitting fax data in an IP network. See "Fax data transmission with T.38 (FoIP)", page 55.
- Fax-over-VoIP:
  Transmission of the fax data as voice data in the IP network. If this solution alone is used, a number of points and restrictions need to be taken into account. See "Restrictions for Fax-over-VoIP:", page 56.
- Fax traffic via the PSTN:
  Fax traffic is consistently handled via the PSTN. Each node with a fax machine then needs a PSTN connection. See "PSTN Overflow", page 47.
- E-mail Fax server:
  The fax server receives faxes from outside the AIN and forwards them as e-mails and vice versa. Paper documents are read in using a scanner. Fax machines are then superfluous.
  - Advantage: Integrated solution.
  - Drawback: No real-time transmission.

Terminal interfaces supported

Fax machines can be connected to FXS, ISDN and PISN terminal interfaces. Analogue fax machines can also be connected to an SIP terminal interface using an analogue terminal adapter (analogue – SIP).

Configuration

Fax connections are configured primarily using the *Fax terminal* setting (CM_4.2) (see Tab. 53 on page 120). The system selects the type of fax connection based on this setting (see Tab. 54 and Tab. 55 on page 120).

4. 2. 1 Fax data transmission with T.38 (FoIP)

According to this method Aastra 400 tries to transmit fax data in the AIN as FoIP. Using the T.38 protocol ensures a reliable, low-loss transmission. The fax machines used can be conventional analogue (Group 3) or ISDN (Group 4) machines. The FoIP transmission must comply with the following requirements:

- Each FoIP connection requires one VoIP channel and one FoIP channel in the system. Both VoIP and FoIP channels take up DSP resources. The following rule applies to FoIP channels: Not all DSP resources can be used for FoIP and the number of possible FoIP channels depends on the system.
- An FoIP connection requires bandwidth resources. The bandwidth model is dimensioned in such a way that, in the same way as for Fax-over-VoIP connections, the bandwidth requirement of G.711 is used with 20 ms frame length over the entire routing path (see also "Bandwidth control", page 93).

Establishing an FoIP connection in the AIN

An FoIP connection is set up as follows:

- The criteria concerning when the Master attempts to establish an FoIP connection with T.38 are listed in Tab. 54 and Tab. 55 on page 120. The same table shows when the master first establishes a voice connection and only then attempts to change to a FoIP connection (use with combined units).
- The bandwidth control uses the same bandwidth values for a T.38 connection as for a G.711 connection with 20 ms.
- If the bandwidth calculation shows that enough bandwidth is available, an attempt is made to set up a fax connection:
  - If a free FoIP channel and a free VoIP channel are available at each node, the connection is set up as an FoIP connection.
  - If a free VoIP channel is available at each node, but not the two FoIP channels required, the connection is set up as a Fax-over-VoIP connection.
- If the bandwidth is insufficient or if the FoIP or VoIP channels available at the nodes are insufficient, the connection is not established, unless the PSTN overflow becomes active and attempts to establish the fax connection via the PSTN (see "PSTN Overflow", page 47.

Restrictions:

Please note the following limitations when using FoIP:

- The maximum transfer rate is 14,400 kbit/s.
- Exchange-to-exchange connections are not supported: At least one of the fax devices must be connected to an internal interface.

4. 2. 2 Restrictions for Fax-over-VoIP:

While fax transmission as language is possible without problem within a LAN area with 100 Mbit/s and correct configuration, there are restrictions for WAN links with limited bandwidth resources:

- Fax over IP cannot be compressed in the same way as call data. For this reason fax data must always be transmitted with the non-compressing codec G.711. 20 ms is used as the frame length. With WAN links this influence the bandwidth dimensioning.
- Jitter, high delay values (in particular round-trip delay values) and packet loss can result in the direct loss of information during Fax over IP data transmission. For this reason prioritising VoIP in the IP network using QoS measures is particularly important (specially on WAN links with limited bandwidth).
- Fax machines that support standard T.30 - Annex A have a sufficiently large send and receive memory and retransmission function, and are able to correct transmission errors up to a certain extent, where the protocol has to be supported by both fax machines involved.

  If a suitable device is selected, the necessary transmission reliability within one AIN can be realized. However, for fax traffic with unknown devices (e.g. beyond the limits of the AIN), this method only offers inadequate transmission reliability.

Tab. 9 Critical elements of fax transmission

Element	Fax transmission
Roundtrip Delay	200 - 300 ms
Jitter	5 ms
Packet Lost	0.1% (with call connections this value is around 3%)

To transmit fax data over the IP network using the Fax over VoIP method, proceed as follows:

1. Configure the fax connection in AMS under CM_4.1_*Analogue settings*, *Fax machine* = *Fax-over-VoIP (G.711)* setting.
2. Check that there is sufficient bandwidth available on all the links between the fax machines. A calculation example is in "Fax over VoIP connection", page 100. Bear in mind that when you are using VPN it is not always the shortest link that is used (see "Using VPN", page 90).
3. Check whether QoS can be set up particularly on WAN links with limited bandwidth.
4. Make sure that WAN links without QoS are only used to transmit fax data from fax machines with sufficient memory and integrated retransmission function.
5. Check the reliability of the fax transmission with a test set-up.

4. 3 Region-related Settings

In principle an AIN acts as a single communication server. However as the nodes can be in different locations and in different countries, system parameters and settings can vary from one region to the next. In configuration terms they can be classified as follows:

- Configurable parameters (settings) which, once an AIN area is selected, can be allocated for the entire AIN or for individual nodes, trunk groups or users (see Tab. 11).
- Country-related, non-configurable system parameters which, once an AIN area is selected, can be allocated for the entire AIN or for individual nodes, trunk groups or users (see Tab. 12).
- Functions that can be configured depending on the region, without an AIN area being assigned (see "Configuration of region-dependent parameters", page 61).

4. 3. 1 AIN areas

An AIN area comprises a group of settings that differ from one region to the next (see Tab. 10).

Tab. 10 Parameters that can be set for each AIN area (CM_6.1.1_Signalling areas)

Parameter/parameter group	Explanation
AIN Regions	Reference number of the AIN area.
Name	Name of the AIN area
Country	The values of the country-related, non-configurable parameters are determined by the selection of the country (Tab. 12). After the first start the country of the AIN area 1 corresponds to the country stored on the EIM card.
Time zone	+/- deviation from the Master's time
Call logging	Various settings for the output of the call charge information
Own regional prefixes	International and national prefix, country code and toll area code
Loop break signalling	Settings for analogue exchange and terminal interfaces

Each node is necessarily allocated an AIN area. After the first start that area is an AIN area. If a satellite is situated in an area that requires other settings, you need to create a new AIN area, modify the settings and allocate the new AIN area to the node.

AIN area 1 is permanently allocated to the Master (node 0).

Country-related settings that are the same throughout the AIN are taken from the settings of AIN area 1.

Tab. 11 lists the configurable parameters which, once an AIN area is selected, can be allocated for the entire AIN or for individual nodes, trunk groups or users.

Tab. 11 Potential allocation of configurable parameters of an AIN area

Parameter/parameter group	Possible allocation			
	AIN	Node	Trunk groups	User
Country		x		
Call logging		x	x	
Own regional prefixes		x	x	
Time zone		x		
Loop signalling, exchange		x		

Tab. 12 lists the country-related, non-configurable system parameters which, once an AIN area is selected, can be allocated for the entire AIN or for individual nodes, trunk groups or users.

Note:

The *Country* setting must match the country of the sales channel set on the EIM card as a number of county-related system parameters are determined by the EIM card, not the AIN area. Example: Congestion tone detection of an analogue network interface.

Make sure the correct sales channel is set on the EIM card already before the configuration. You can subsequently change the sales channel if you need to. However this involves a system first-start and the licences have to be re-enabled (licences depend on the sales channel).

Tab. 12 Possible allocation of the country-related, non-configurable system parameters

Parameter	Possible allocation			
	AIN	Node	Trunk groups	User
Ringing times	x			
Capolinea	x			
Interpretation method for direct dialling numbers		x	x	
Ringing patterns for the general bell	x			
ISDN error handling		x		
Number of announcement service groups	x			
Call charge format for ISDN terminals		x		x
Internal/external ringing patterns		x		x
Ring back tone, busy tone, park tone		x		x
Conference tone, call waiting tone, intrusion tone	x			
Parameters of the analogue network interface		x		
Parameters of the analogue terminal interface		x		
Wait for connection	x			
Maximum park duration	x			
CLIP on line keys	x			
ICL CLIP format	x			
Voice mail CLIP format	x			
Sales channel-related parameters	x			

The scope can be determined in part using the configuration:

- You can configure the same parameters throughout the AIN by allocating AIN area 1 to all the nodes
- The value of a parameter that can only be valid throughout the AIN is always determined by the setting in AIN area 1.

Tab. 13 Allocation examples of AIN areas

Situation	Allocation
All the nodes are in the same area	Each node is allocated an AIN area 1 (default value)
The Master is located in Spain, with a satellite in Portugal	Spain is selected as the country for the AIN area 1. For the satellite a new AIN area is created; Portugal is selected as the country and allocated to the satellite node. Note: The sales channel setting on the EIM card must match the country of the AIN area (see earlier remark).
The Master in Spain is located on the border with France and has a direct exchange line circuit with a French provider	AIN area 1 determines the settings for the node. A new AIN area is created for the trunk group with the French exchange line circuit; France is selected as the country and allocated to the trunk group.

4. 3. 2 Configuration of region-dependent parameters

For many parameters there is already the possibility of configuring several variants without using AIN areas and to allocate them as required. This can also be used to configure regional variants.

The table below lists the main parameters for which values with different regional settings are appropriate and which are not set using the AIN areas.

Tab. 14 Parameters which can be defined depending on the region through configuration

Parameter	Allocation			
	AIN	Node	Trunk groups	User
Exchange access prefix	x			
Call charge format	x			
Explicit Call Transfer yes/no			x	
Three-party conference in the exchange yes/no			x	
LCR	x			
Standard messages	x[1]			
Digit Barring				x
Priority ringing	x			
Clock reference/synchronization	x	x		
L2 activation			x	
Door Intercom Systems	x			
Emergency number destinations	x	x		x

[1] The standard messages available may however be predefined in different languages

4. 4 Satellite in Offline Mode

In normal operation the Master controls the entire telephone traffic in the AIN (AIN operating mode), so Master and satellite must be able to exchange signalling data at any time. If contact is lost, the satellite is no longer operational in the AIN operating mode. The satellite is switched to the offline operating mode to enable at least limited telephone traffic in this emergency situation. In offline mode the satellite operates as a single system and accesses the local configuration data while offline (offline configuration).

Switching to the offline mode and back to the AIN mode

The switchover to the offline mode is as follows:

- The signalling connections between Master and satellites are permanently supervised by connection monitors.
  The monitoring interval can be configured using AMS and ranges from a few seconds to several minutes (see Tab. 48 and Tab. 49).
- As soon as the connection monitors of the Master and the satellite concerned detect an interruption, the satellite is restarted. The Master deactivates the AIN configuration data of the satellite and generates the event message *Node x lost*. If configured, a user-definable text is displayed on the system phones during offline operation (see also "Configuring offline operation", page 63)
- The satellite restarts and loads the offline configuration data, and starts up offline operation. A small bar flashes in the middle of the 7-segment display.

The switchover to the AIN mode is as follows:

- During offline operation the satellite regularly tries to re-establish contact with the Master.
- The satellite is restarted after a definable period of time after its connection monitor was able to establish contact with the Master (see Tab. 48under *Minimum connection time*).
- When it starts up, the satellite logs back on with the Master and resumes AIN operation. The Master generates the event message *Node x reestablished*.

4. 4. 1 Configuring offline operation

Configure offline operation in accordance with the Chapter "Configuring offline operation for the satellites", page 41. Please note the following points:

- Numbering plan:
  Assign the users the same call numbers as in the AIN operating mode so that the users on the satellite can be reached on the usual numbers in offline mode. If you are using the data with AMS from AIN operation, this is done automatically.
- Routing:
  Only if the satellite has an exchange line circuit: For the most important users at the other nodes set up virtual PISN users that can be dialled via the public network. Allocate the PISN users the same call numbers as those used by the corresponding users in the AIN. Your internal contact partners connected to a different node can then still be reached on the usual call numbers.
  Tip: Instead of setting up a separate PISN number for each user, you can define a PISN number with a wildcard that covers all the users. For instance PISN number 3xx covers all the internal users from 300 to 399. For more information on this subject please refer to “System Functions and Features on Aastra 400” in the System Manual.
- IP system phones:
  The IP system phones are logged on to the Master in principle and cannot be configured for an offline mode. For the exception see "IP system phones in offline mode", page 65.
- Cordless phones:
  In regular AIN operation the cordless phones are logged on to the Master. To ensure the cordless phones can be used also in offline mode, register the handsets in offline mode of the satellites with the DECT system.
  Register the cordless phones using a system other than in the Master (e. g. System B) and set the cordless phones on *System* = *Auto* so that the cordless phones automatically log on to the active system.
- Displaying the offline mode:
  You can use the idle text of the system phones to display a text in offline mode. To do so, use AMS to open the Master’s configuration and select under CM_4.1_*Terminal data* the button *Set idle text globally*; you can then edit the text. Once you have selected *Finish*, the text is used for all the system phones with a display and is displayed in offline mode.

4. 4. 2 Restricted functions in offline mode

The following functions are not available in offline mode:

- Voice mail: The voice mail system is set up centrally on the Master for the entire AIN and is not available to a satellite operating in offline mode.
- All the properties licensed centrally in the Master for the AIN mode Exceptions: The licensed voice channels for VoIP, SIP access and QSIG are enabled for two hours so that connected IP terminals or QSIG nodes are available also in offline mode, provided they have been configured accordingly.
- OIP server and OIP server applications
- PSTN overflow.

The following functions are available only to a limited extent in offline mode:

- External phone traffic:
  If the satellite does not have its own exchange line circuit, users on the satellite can no longer be reached directly from the outside.
- DECT System:
  Only those cordless phones that are registered for offline operation are recognised by the communication server.
- IP system phones:
  Only those IP system phones that are registered for offline operation are recognised by the communication server (see "IP system phones in offline mode", page 65).

4. 4. 3 IP system phones in offline mode

In the AIN mode all the IP terminals are logged on to the Master and are controlled by it. For this reason they must also in principle be configured and registered with the Master.

IP system phones located in the vicinity of a satellite can also be set up so that they automatically log on with the satellite in offline mode.

For this the phones must be configured and registered both with the Master and the satellite.

An IP system phone that has also been configured for offline operation has the following properties:

- The phone is configured and registered on both the Master and a satellite.
- Even in the satellite's offline mode a sufficient number of VoIP channels is available.
- IP system phone and satellite are connected to the Master via the same WAN link.
- The satellite's IP address is stored in the IP system phone (*PBX adress* setting).

Logon procedure in AIN operating mode

During a restart an IP system phone logs on as follows:

- The phone tries to log on to the satellite.
- The satellite forwards the phone's request on to the Master and the logs on with the Master.

Switching to offline mode

After contact with the Master is lost, an IP system phone logs on to the satellite as follows:

- After contact with the Master is lost, the satellite runs a restart and starts in offline mode (see "Satellite in Offline Mode", page 62).
- The IP system phone also carries out a restart and tries to log on to the satellite.
- As soon as the satellite has adopted the offline mode, the IP system phone can log itself on. The satellite then controls it during offline operation.

Switching to AIN mode

After contact with the Master is restored, an IP system phone logs back on to the Master:

- The satellite restarts and starts up in AIN mode.
- The IP system phone loses contact with the satellite, restarts and tries to log on with the satellite again.
- As soon as the satellite has adopted the AIN mode, it forwards the IP system phone request on to the Master and the phone logs on with the Master.

4. 5 Restricted functions in the AIN

The AIN essentially provides the same features as a single system. Only a few functions are either not available or available only with restrictions:

ISDN Data Services

ISDN Data Services and consequently Group 4 fax machines are not supported between the nodes of an AIN.

CLIP/CNIP of Abbreviated Dialling Numbers

If two different abbreviated dialling numbers used in two nodes in different countries coincidentally have the same call number, the system does not know which name to display in the case of an incoming call. Remedy: Add the regional prefix to the call number.

Priority exchange allocation

The Priority Exchange Allocation system function is also available when subsections of active call connections are routed via IP links. However, on the IP link itself no active call connections can be established for a prioritized call. Thus, if a prioritized call is to be established via an IP link, the link must have sufficiently free band width to be able to establish the connection without first having to disconnect an already active connection.

Key telephones and operator consoles

Line keys of key telephones and operator consoles are not taken into account when the bandwidth model checks the bandwidth requirement. The result is that a call on a line key is signalled even when insufficient bandwidth is available for the connection set up. When an attempt is made to answer the call, the connection is interrupted.

5 IP system phones

This chapter contains the information you need to install, configure, commission and service IP system phones.

The specific installation and configuration instructions for Aastra SIP phones can be found in the “SIP and SIP terminals” system manual.

Data transmission

IP system phones communicate with the communication server in the same way as digital system phones, i.e. via the DSI AD2 protocol. But unlike those terminals, call and signalling data is transmitted in the IP network. The phones are connected directly to the IP network, making the DSI-AD2 connection superfluous.

The IP system phones can be operated anywhere in the IP network as long as the connection complies with the quality criteria required for VoIP (Voice over IP). This offers a whole range of user advantages:

- Unlike a connection via the public telephone network, no call charges are incurred, and users can be reached as internal users.
- Many features that are restricted when a remote user is integrated as a virtual user can be fully utilised, i. e. team keys, Call Forwarding Unconditional, voice mail, Courtesy, text messages, announcements.
- In the case of smaller branch offices the customer can dispense with using an additional communication system at the branch.
- Telephone lines do not have to be extended when expanding an existing infrastructure with new connections for PCs and telephones.

Portfolio

The portfolio of the Aastra 400 communication solution comprises the following IP system phones:

- IP hardphones of the Aastra 5300ip series
- Aastra 2380ip IP softphone (featurephone)
- Office 1560IP PC operator console (PC operator console)

Commercially available SIP phones can also be operated on the system.

Features

The IP system phones of the Aastra 5300ip series support the same range of features as the digital system phones of the Aastra 5300 series. More detailed information can be found in the “System Functions and Features on Aastra 400” System Manual and in the User’s Guides for the individual phone models.

IP system phones in the AIN

IP system phones can be used both on a single system and in the AIN. In the AIN operating mode the IP and the SIP phones are always connected directly to the Master, even if locally they are situated near a satellite. If the IP system phones close to the satellite are also to work when the satellite is in offline mode, you need to register them with the satellite also (see "IP system phones in offline mode", page 65).

Aastra SIP phones in the AIN

The Aastra SIP phones in AIN are always connected directly to the Master, even if locally they are situated near a satellite.

The specific installation and configuration instructions for Aastra SIP phones can be found in the “SIP in Aastra 400” System Manual.

Aastra 2380ip Softphone in the AIN

The Aastra 2380ip softphone is an autonomous and local application. The installation and connection to the Master are carried out using the software installation procedure on the PC and is not part of this Manual.

Office 1560IP PC operator console in the AIN

The Office 1560IP PC operator console is an OIP application and requires the operation of an OIP server. The installation and connection to the Master are carried out using the OIP installation procedure on the PC and is not part of this Manual.

In an AIN, the OIP server always communicates only with the Master.

5. 1 IP system phones of the Aastra 5300ip series

Apart from the socket connections, the IP system phones of the Aastra 5300ip series are identical in design to those of the Aastra 5300ip series. The individual models of the two series are identical in terms of operator prompting and range of features.

Tab. 15 IP system phones (hardphones) of the Aastra 5300ip series

Product	Main common features	Additional model-specific features
Aastra 5361ip Aastra 5370ip Aastra 5380ip	• Intuitive and user-friendly menu prompting with Foxkey and central navigation key • All the system features can be used • Excellent voice quality due to Aastra Hi-Q™ wideband audio technology • Automatic update of the phone software • Connection via Ethernet • Powered via Ethernet (PoE) or power supply • Possibility of wall mounting • Web configuration interface	Aastra 5370ip/Aastra 5380ip: • Possibility of connecting expansion key modules • Headset socket with DHSG standard • Integrated switch for connecting a PC Aastra 5380: • Backlit display • Optional Bluetooth module • Can be used as operator console when combined with expansion key module

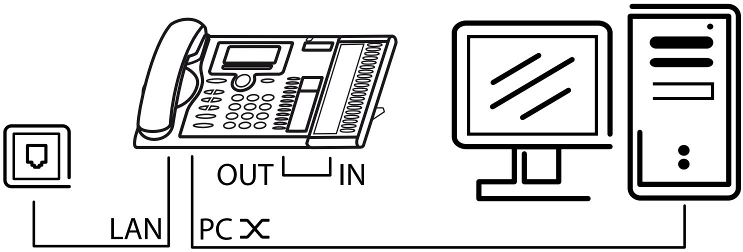
Note:
The Aastra 5360ip IP system phone is supported as before.

5. 1. 1 Connection features

Accesses

Tab. 16 Socket connections of the IP system phones of the Aastra 5300ip series

LAN	PoE Ethernet interface for connection to the IP network
PC ⤫	Socket connection for a workstation PC (integrated 100Base-T switch, available on Aastra 5370ip and Aastra 5380ip)
✆	Handset socket
🎧	Headset socket
🔌	Power supply socket for connecting a power supply if PoE is not available
OUT ▯	Connect expansion key module Aastra M530⁄Aastra M535 (available on Aastra 5370ip and Aastra 5380ip)



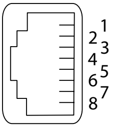
Integrated switch (Aastra 5370ip and Aastra 5380ip)

You can use the integrated 100Base-T mini-switch to connect other network terminals (e. g. PC, printer), thereby reducing the amount of cabling required.

Power supply

If your network supports Power-over-Ethernet, the IP system phone is powered directly via the LAN connection and there is no need to connect the powersupply available as an option.

Tab. 17 Power over Ethernet

RJ45 socket	Pin	Signal	PoE power supply (Variant 1)	PoE power supply (Variant 2)
	1	Rx	DC+	—
	2	Rx	DC+	—
	3	Tx	DC-	—
	4	—	—	DC+
	5	—	—	DC+
	6	Tx	DC-	—
	7	—	—	DC-
	8	—	—	DC-

Depending on the power requirements different classes are defined in the IEEE 802.3af standard. The following table provides information on the class allocation of the IP system phones.

Tab. 18 PoE class allocation

Class	Max. load, PSE[1]	Max. power requirement, PD[2]	IP system phones
1	4.0 W	0.44...3.84 W	Aastra 5360ip, Aastra 5361ip Aastra 5370ip[3], Aastra 5380ip[4]
2	7.0 W	3.84...6.49 W	
3	15.4 W	6.49...12.95 W	

[1] PSE (Power Source Equipment) = power supply device, e. g. a switch

[2] PD (Powered Device) = power consumer, e. g. an IP system phone

[3] including an Aastra M530 or Aastra M535 expansion keypad

[4] including up to three Aastra M530 or Aastra M535 expansion keypads

5. 2 Putting IP system phones into operation

In the AIN mode all the IP system phones are logged on to the Master and are controlled by it. For this reason they must also be configured and registered with the Master.

Phones located in the vicinity of a satellite can also be set up so that they automatically log on with the satellite in offline mode. For this the phones have to be set up on both the Master and the satellite.

- To set up the IP system phones for AIN operation only or for operation on a single system only, follow the instructions under "Commissioning on the single system or on the Master", page 72.
- If you also wish to set up all (or some of) the IP system phones on a satellite, follow the instructions under "Commissioning on the satellite and Master", page 72.

  You can also register IP system phones with the satellite at a later date, if required.

5. 2. 1 Commissioning on the single system or on the Master

You want to set up the IP system phones for operation on a single communication server or for AIN operation on the Master. To do so proceed as follows:

1. Open the IP system phones in the Master (AMS CM_4.1) and assign them your users.
2. Address the IP system phones as described under "Addressing IP system phones", page 74.
3. Log the IP system phones on to the communication server as indicated under "Registering IP system phones with the communication server", page 80

5. 2. 2 Commissioning on the satellite and Master

You want to set up the IP system phones on the Master for AIN operation and on the satellites for the offline mode in an AIN. Log the IP phones on to the satellite first and then on to the Master.

Preparations

1. Check that the satellite is equipped with a sufficient number of VoIP channels for the offline mode and expand if necessary.

   Tip:
   Aastra Plan always calculates a sufficient number of VoIP channels to operate the IP system phones on the satellites in offline mode.

2. Create the IP terminal data in both the Master and the satellites (AMS CM_4.1)

Log the phones on to the satellite

1. Start the satellite in offline mode by disconnecting the Master from the IP network and restarting the satellite.
2. Connect the first IP system phone to the power supply and the IP network.
3. Enter the satellite's IP address under *PBX adress* in the phone's local configuration. To do so, follow the instructions given under "Addressing IP system phones manually", page 76.
4. Restart the phone and register it with the satellite as indicated under "Registering IP system phones with the communication server", page 80.
5. Repeat the procedure in sequence from step 2 for all the other IP system phones.

Log the phones on to the Master

1. Disconnect the IP system phones on the satellites you have just set up from the IP network.
2. Connect the Master to the IP network.

   The satellite restarts and starts up in AIN operation mode.
3. Connect the first IP system phone to the IP network.

   The phone tries to log on to the satellite. However, the satellite forwards the request to the Master (see also "IP system phones in offline mode", page 65).
4. Next register the IP system phone to the Master as indicated under "Registering IP system phones with the communication server", page 80.
5. Repeat the procedure in sequence from step 3 for all the IP system phones.

5. 2. 3 Addressing IP system phones

IP addressing methods

For an IP system phone to register successfully with the communication server, it has to have its own address and it has to know the address of its communication server. When commissioning individual phones it is simplest to enter these co-ordinates manually in the phone's local configuration (either on the phone itself or via the browser access). See "Addressing IP system phones manually", page 76).

When commissioning several phones it is advisable to automate the local configuration on the phones. There are several possibilities:

- You use the integrated DHCP server of the communication server, which has already integrated the manufacturer-specific data (see "Using the integrated DHCP server", page 77).
- You expand the DHCP server in your IP network with manufacturer-specific data, which you then use to transfer the communication system's co-ordinates to the phones (see "Using the DHCP server with options", page 79).
- You use the DHCP server in your IP network without any manufacturer-specific data. Instead you enter the host name *intelligate* in the DNS server for the communication server (see "Using the DHCP and DNS servers", page 79).

Access to the local phone configuration

The address and connection settings are stored in the phone's local configuration menu and are accessible via a web browser or the operator prompting on the phone itself.

To activate changes in the IP addressing, you need to restart the phone. The changes remains stored even when power is disconnected.

Tab. 19 Access to the local configuration menu and navigation on the phone

Access on the phone	Keep the C-key pressed down or Foxkey *Menu* / *Settings* / *General* / *Local settings*
Access via the web browser	URL = IP address of the phone (default setting: 192.168.104.33)

User name (applies only to access via the web browser)	admin
Password	The default password is “0000” and can be changed under *Administration* / *general admin* (password syntax: 2 to 10 digits). **Note:** You can set the password for all the connected IP system phones globally using AMS (setting *Administrator password* under CM_2.5.6). Any passwords already set are then overwritten. To assign the passwords locally and individually for each phone, the entry must be blank. A phone first-start has to be carried out to reset the password to the default value ("First start and restart", page 81).
Navigation on the phone	• Select the menu item: Press Foxkey • Once level back: Press Foxkey • Exit: Press C-key

Tab. 20 Settings for IP addressing in the local configuration menu

Phone	Web browser	Explanation
IP addressing of the phone:		
• *DHCP*	*DHCP_ENABLED*	Activate or deactivate DHCP (*on* / *off* - default value: *on*)
• *IP-Adress*	*IP_ADRESS*	IP address of the phone. Configurable only if DHCP is deactivated.
• *Subnet Mask*	*SUBNET_MASK*	Subnet mask of the phone. Configurable only if DHCP is deactivated.
• *GW-Adress*	*GATEWAY*	Gateway address: Phone-side IP address of the router that provides the transition to the other partial areas of the IP network. If all the IP phones and all satellites are in the same LAN area as the Master, 000.000.000.000 can be used for the Gateway address (default value).
Address of the communication server:		
• *PBX adress*	*PBX_ADRESS*	Static IP address of the communication server. Read only if the *DNS name* entry is blank.
• *PBX adress backup*	*PBX_ADRESS_BACKUP*	This setting is of no relevance for operation on an Aastra 400 system and can be left blank.
DNS settings:		
• *DNS name*	*DNS_NAME*	Host name of the communication server. Default value: *intelligate*. If the IP address of the communication server is to be entered as static, you need to delete this entry.
• *DNS name backup*	*DNS_NAME_BACKUP*	This setting is of no relevance for operation on an Aastra 400 system and can be left blank
• *DNS server adress*	*DNS_SERVER*	Address of the DNS server (entered by the DHCP server)
• *DNS domain*	*DNS_DOMAIN*	Domain of the DNS server (entered by the DHCP server)

5. 2. 3. 1 Addressing IP system phones manually

You want to address an IP system phone manually. You have the possibility of using static addressing for the phone or the DHCP and DNS servers.

Using the example of user 504 in the reference network the table below shows how the relevant parameters need to be set for the different combinations of types of addressing.

1. Connect the IP system phone to the mains power and the IP network and wait for the phone to start up.
2. Open the local configuration menu by keeping the C-key pressed down.
3. Address the phone as indicated in Tab. 21.

Tab. 21 IP addressing on the phone for user 504

Phone	Web browser	Static	DHCP/DNS	DHCP
Phone address:				
• *DHCP*	*DHCP_ENABLED*	*off*	*on*	*on*
• *IP-Adress*	*IP_ADRESS*	172.020.054.001[1]	[2]	[2]
• *Subnet Mask*	*SUBNET_MASK*	255.255.255.000[1]	[2]	[2]
• *GW-Adress*	*GATEWAY*	172.020.054.002[1]	[2]	[2]
Addressing the communication server:				
• *PBX adress*	*PBX_ADRESS*	172.020.050.001[1]	[3]	172.020.050.001
• *DNS name*	*DNS_NAME*	-[4]	a400master	-[4]
• *DNS server adress*	*DNS_SERVER*	0.0.0.0	[2]	0.0.0.0

[1] Enter all 12 decimal places of the IP address (e. g. for IP address 172.20.54.1 enter the digit sequence “172.020.054.001”).

[2] Automatically assigned values are displayed

[3] The IP address retrieved from the DNS server is displayed.

[4] Please delete the default value *intelligate*.

Note:
Make sure the IP addressing of the communication server (see Tab. 5 on page page 28) and the IP addressing of the phone match up.

5. 2. 3. 2 Using the integrated DHCP server

You want to use the communication server's integrated DHCP server to address the IP system phones. The integrated DHCP server can tell from the address requests whether a request comes from an IP system phone. It can then send it not only the address co-ordinates for the phone but also the communication server's IP address as well as other configuration data (see Tab. 22).

To do so, the integrated DHCP server uses DHCP option 60 (vendor class identifier) to identify the IP system phones and DHCP option 43 (vendor-specific information) to transfer the configuration data. More information on the DHCP options can be found under "DHCP options", page 125).

Tab. 22 Configuration parameters transmitted as standard to the IP system phones

Attribute	Explanation
PBX_ADRESS	IP address of the communication server.
SIP_PORT_PBX	SIP port of the communication server
SIP_PORT_PHONE	SIP port of the IP system phone
VLAN_PRIO	The VLAN priority is read from the *CoS prioritization level* setting (CM_2_2_5_*QoS configuration*).
VLAN_ID/VLAN_ENABLED	The VLAN ID is read from the *VLAN-ID* setting (CM_2_2_5_*QoS configuration*).

As an alternative to the transfer of predefined configuration parameters, you can specify them yourself by creating a configuration file and storing in the communication server. An example can be found in Chapter "DHCP options", page 125).

Setting up the integrated DHCP server

To setup the integrated DHCP server proceed as follows:

1. Check whether the communication server (Master or single system) has a static address and DHCP is deactivated (CM_2.2.1, *DHCP client* = *no* setting).
2. Check whether any other DHCP server is active in the same IP network. If so, contact the IP administrator to specify an address range for IP and SIP system phones and exclude the address range on the active DHCP server.

Note:
Make sure the address range of the integrated DHCP server and the IP address of the communication server are in the same subnet.

3. Switch on the DHCP server (CM_2.2.4, *DHCP server* = *yes* setting) and enter the address range to be covered with the integrated DHCP server.
4. Specify whether the integrated DHCP client is to respond to all requests or only to requests from Aastra terminals (CM_2.2.4, *DHCP support* setting).

Note:
If the IP addressing of the satellites is also to be carried out using the integrated DHCP server, select the setting *DHCP support* = *All*.

5. Complete the basic setup as indicated in "DHCP server", page 116.

Integrating IPsystem phones

Once the DHCP server is set up, you can connect the IP system phones:

As soon as an IP system phone has started up, the following sequence begins (simplified):

- The IP system phone sends an address request together with its MAC address and the vendor class identifier.
- The integrated DHCP server responds to the request, creates and registers a new link between the MAC address and an IP address from its address range, and sends the IP system phone its address co-ordinates as well as the communication server's IP address.
- The system phone stores the received configuration data and logs on to the communication server. It is now ready for registration.

5. 2. 3. 3 Using the DHCP server with options

You want to use the DHCP server in the existing IP network to address the IP system phones. To do so, add the manufacturer-specific options 60 and 43 to the DHCP server via its configuration interface. More information can be found in Chapter "DHCP options", page 125).

5. 2. 3. 4 Using the DHCP and DNS servers

You want to use an active DHCP server to address the IP system phones and an active DNS server to find the communication server. The default value *intelligate* is entered in the configuration of an IP system phone as the communication server's host name.

If the DNS server has an entry under that name and the IP address of the Master or single system is entered there, the IP system phone finds its communication server.

You can carry out the DNS entry either manually or you can enter *intelligate* under the communication server's host name. The latter assumes that the function for dynamic updates is activated in the DNS server.

Once the DNS server is set up, you can connect the IP system phones.

As soon as an IP system phone has started up, the following sequence begins (simplified):

- The IP system phone sends an address request together with its MAC address and the vendor class identifier.
- The integrated DHCP server responds to the request, creates and registers a new link between the MAC address and an IP address, and sends the IP system phone its address co-ordinates.
- The system phone searches for its communication server under the name *intelligate*. The DNS server sends the IP system phone the communication server's address co-ordinates.
- The system phone logs on with the communication server. It is now ready for registration.

5. 2. 4 Registering IP system phones with the communication server

An IP system phone is registered with the communication server if it is assigned a set of terminal data. Its MAC address is used for the assignment.

You can either enter the MAC addresses individually (AMS CM_4.1_*IP settings*) or register the IP system phones with the aid of the system using the following method:

1. Check that all IP system phones are opened and their users assigned (AMS CM_4.1_*IP_Settings)*.
2. Enter a registration code in the terminal data for all the IP system phones, unless one has already been entered by the system (AMS CM_4.1_*IP_Settings*, *Registration code* setting).

   The registration code is used to allocate the IP system phone in the configuration to the IP phone created. The registration code is a number that has to be unique for each IP system phone. The call number of the assigned user is entered as standard.
3. Connect the IP system phones to the IP network or restart the phones if they are already connected to the IP network.

   Once the connection to the communication server has been set up, the display on the phones show the prompt: *Enter registration code:*
4. Enter the appropriate registration code on all the phones one after the other and confirm the input with *OK* or *Accept*.
   - Once the registration code is entered, the IP system phone logs on with the single system/Master with its MAC address and is connected with the relevant terminal data.
   - The Master checks the version of the phone’s application software. If the software stored on the communication server is more recent than that loaded on the phone, the Master updates the software and restarts the phone. This is indicated on the phone’s display.
   - The phone is now fully operational. If it is disconnected from the IP network or from the power supply or if a restart is carried out, it automatically logs back on to the node again correctly (see "Operation and maintenance", page 81).

Note:
- To clear any incorrect phone allocations to the terminal data, delete the MAC address (AMS CM_4.1_*IP_Settings*).
- The *Remove* Foxkey menu is currently unassigned.

5. 3 Operation and maintenance

This Chapter describes how to replace or move an IP system phone during operation and how to expand the communication system or the AIN with additional IP system phones.

First start and restart

Restarting the IP system phones initializes the local software and logs the phone back on to the Master.

You can trigger a restart either via the Offline menu or by briefly interrupting the power supply.

Note:
No calls can be made during the restart

A first start of the IP system phones resets all the addresses (see "Default values of the IP addressing", page 122).

You can trigger a first start either via the local configuration menu on the phone or using the following procedure:

1. Unplug the IP system phone's power supply cable.
2. Press the Correction key and reconnect the phone to the power supply.
   The boot menu is displayed.
3. Press the “8” key.
   The phone is reset to the initialization state and restarted.

Replacing an IP system phone

The instructions below explain the procedure for replacing an IP system phone.

1. Delete the MAC address of the previous phone in the communication server's terminal configuration (CM_4.1_*IP settings*).
2. Unplug all the IP system phone’s connectors.
3. Address the replacement phone as indicated under "Addressing IP system phones manually", page 76.
4. Register the new phone as indicated under "Registering IP system phones with the communication server", page 80.
5. Carry out a connection test.

Connect the IP system phone elsewhere

The instructions below explain how to change the connection point of an IP system phone without having to change the call number, user name and terminal settings. The communication server does not have to be taken out of service. To do so proceed as follows:

1. Unplug all the IP system phone's connectors.
2. Connect the IP system phone to the power supply and the IP network at the new location.
3. If the phone is statically addressed and the new location is in another subnet, you have to change the IP addressing in accordance with the specifications in "Addressing IP system phones", page 74. In all other cases this step is not necessary.
4. Carry out a connection test.

Deploying additional IP system phones

To use another IP system phone, proceed as follows:

1. Check the following expansion and design limits:
   - Permissible number of system phones is not exceeded.
   - There are enough VoIP channels available.
   - The bandwidth available in all the relevant parts of the IP network is sufficient.
2. Create the terminal data in the communication server and assign it to a user.
3. Address the phone as described under "Addressing IP system phones", page 74.
4. Register the phones as indicated under "Registering IP system phones with the communication server", page 80.
5. Use AMS to check the settings of the bandwidth control with regard to the new IP system phones (see Chapter "Bandwidth control", page 93).
6. Carry out connection tests.

Software upgrade on the IP system phone

The communication server automatically updates an IP system phone's application software.

The application software of the IP system phone is included in the software package of the communication server application software.

To upgrade the boot software you need to send in the phone. Contact your distributor to clarify whether or not the boot software needs to be upgraded.

You will find information about the current software versions in the Offline menu.

6 Network environment

This chapter provides background information on the main network properties to be taken into account. It is assumed that an IP network is already in place.

Please note that the know-how of an experienced network technician is essential for optimizing the network environment.

6. 1 IP network requirements

In the AIN the IP network used is part of the communication system and greatly influences the communication quality. The communication quality depends directly on availability, the available bandwidth, the quality of service (QoS) and the network topology. The general requirements are as follows:

- Ethernet 10 Base-T or 100 Base-T
- Use of terminals with high fail-safe reliability
- Using switches instead of hubs
- Using terminals that support QoS
- Sufficient bandwidth also via WAN links
- Using a DHCP and DNS server (optional)
- VPN connections for WAN links via the internet
- Administration access to the relevant network components, e. g. access to the DHCP server to configure the DHCP options or access to the port configuration of firewalls (see "TCP/IP Ports and Firewall", page 124).

Please take good note of the following recommendations:

- Also avoid the use of dial-up connections for WAN links as the communication server regularly establishes contact with the satellites and IP system phones, which could incur undesirable costs if a dial-up connection is used. Also take note of the security aspects with regard to the WAN link (see under "Using VPN", page 90.)
- Try and implement the WAN links with a single internet provider whenever possible. The more providers are involved, the more difficult it will be to pinpoint the causes of any malfunctions.
- Try and implement VPN connections with a single internet provider whenever possible. This simplifies the routing of calls in the IP network (see "Using VPN", page 90).
- Whenever possible try and use equipment by the same manufacturer for similar functions (e.g. for routers) or carry out laboratory tests of how equipment by different manufacturers interacts before you deploy the equipment.

6. 1. 1 Delay and jitter

High delay and jitter values have a hugely detrimental effect on the call quality. The delay values for the voice packets should be kept as small as possible. Take note of the minimum requirements for operating an AIN in Tab. 23.

The following methods are used to reduce delay and compensate jitter:

- Prioritizing the voice packets before other data packets: see Chapter ("Prioritization", page 87).
- Jitter management:
  Compensation of the time fluctuations between the arrival of individual packets (jitter management) is automatically regulated in the AIN and does not require any additional settings. The better the jitter is compensated, the larger the delay values. The dejitter buffers used therefore adapt their size dynamically to the situation and ensure a balanced ratio between jitter and delay.
- Fragmenting the IP packets:
  Large data packets increase the delay of waiting voice packets. By fragmenting large packets into several small packets, prioritized voice packets can be sent through in between the data packets.
- Frame length of voice packets:
  The smaller the frame length of voice packets, the smaller the delay values generated but the greater the bandwidth requirement. For this reason we recommend that the frame length of voice packets be kept relatively small within the LAN area and relatively large for WAN connections with limited bandwidth (see Tab. 56 for settings).

Tab. 23 Key data for operating an AIN

Property	Value
Roundtrip Delay	< 200 ms
Jitter	< 80 ms
Packet Lost	< 5%

6. 2 Prioritization

For an IP network with limited bandwidth resources to be able to guarantee the necessary bandwidth for call connections, voice packets should to be prioritized compared with other data packets.

The AIN supports the following prioritization methods (QoS = Quality of Services):

- QoS on Layer 2 with CoS (Class of Services):
  The IP system phones use the prioritization field in the extended frame header to specify the priority (IEEE 802.1p/Q). Prioritization takes place in the switches. All the switches used must therefore support prioritization as per IEEE 802.1p/Q and be configured accordingly. QoS on Layer 2 with CoS can be activated either for all AIN components or for all AIN components without the IP system phones (see Tab. 46 on page 117).
- QoS on Layer 3 with ToS (Type of Services):
  The IP system phones set and interpret the first six bits of the ToS/DSCP field according to the ToS method (RFC 791, page 11 and RFC 1349). The ToS method interprets the first three bits (predicating) to specify the priority level. Bits 3 to 5 are used to optimize the transmission according to one of the following criteria: Throughput maximization (High Throughput), reliability maximization (High Reliability) or delay minimization (Low Latency). The routers used must therefore support ToS prioritization and be configured accordingly. Non-prioritized data packets are given standard priority by the router.
- QoS on Layer 3 with DiffServ (Differentiated Services):
  The IP system phones set and interpret the first six bits of the ToS/DSCP field according to the DiffServ method (RFC 2474).
  The DiffServ method interprets the value of the first six bits of the ToS field for classification (DSCP value). Theoretically, it can differentiate between up to 64 classes; the standardized values listed are in the Internet-standard documents rfc-2597 and rfc-2598.
  Prioritization takes place in the routers or in Layer 3 switches. The routers used must therefore support DiffServ in general and the selected DSCP value in particular and must be configured accordingly.

The DiffServ or ToS method can also be used simultaneously with the CoS method, thereby complementing it.

Tab. 24 Recommended values for the prioritization of call data (CM_2.2.5_*QoS configuration*)

Parameter	Parameter value[1]
CoS prioritization level	*5 Interactive Media*
ToS prioritization level (Precedence)	*5 CRITIC/ECP*
ToS type of service (ToS bits)	*8 Low Latency*
DSCP	*46*

[1] Here all values correspond to the default values

6. 3 Encrypted transmission

You want to encrypt phone calls and fax connections via the IP network to prevent them from being recorded and played back.

You can choose for the system as a whole whether to use a non-encrypted or an encrypted transmission method.

If you select the encrypted variant, you also need to adjust the VoIP mode of the DSP resources. The *Secure VoIP* licence is also required. The simplest way is to decide one way or the other already at the planning phase and then select the corresponding node connections in the Aastra Plan network diagram (see "Specifying nodes and networking them into an AIN", page 19). Aastra Plan will then take the necessary DSP resources into account in the calculations, along with the licence required.

Tab. 25 Configuration parameter for specifying the transmission method

VoIP mode	Encrypted transmission	Non-encrypted transmission
Node connections in Aastra Plan	secure G.711 secure G.711/G.729	G.711 G.711/G.729
Encryption of VoIP_data (CM_2.2.5_*Encryption*)	yes	no
VoIP mode (CM_2.1.3_*DSP configuration*)	secure G.711 secure G.711/G.729	G.711 G.711/G.729
Licence	Secure VoIP	-

The IP system phones are switched over automatically.

During the call the user sees an encryption symbol on the phone's display. The symbol is displayed only if the connection is genuinely encrypted and over the entire link.

The encryption methods used do not affect the quality of speech.

For WAN links over the internet we also recommend that you set up a VPN (see Chapter "Using VPN", page 90) or use dedicated leased lines.

6. 3. 1 Other encryption methods

Aastra 400 combines the two encryption methods SRTP and TLS into an encrypted transmission that is considered tap-proof. Data protection, authentication and integrity security as well as protection against replay attacks (replaying messages) are guaranteed to a high degree. No additional special software or special IP components are required for encryption. All that is needed for encryption and decoding is more VoIP resources in the communication server. The IP system phones support encrypted transmission without any need for you to expand the phones or configure them in any particular way.

Voice data encryption

Voice data is encrypted using SRTP (Secure Realtime Transport Protocol). The data is encrypted and decoded directly in the IP system phones and communication server respectively. The packet header information, which contains the sender and the recipient, is unaffected by the encryption.

Signalling data encryption

The signalling data between the nodes is proprietary and can only be read by the proprietary implemented link handlers.

Signalling data between SIP and IP phones and the communication server to which they are logged on is encrypted using TLS (Transport Layer Security). TLS works by exchanging certificates. The exchange between IP system terminals and the communication server is automatic.

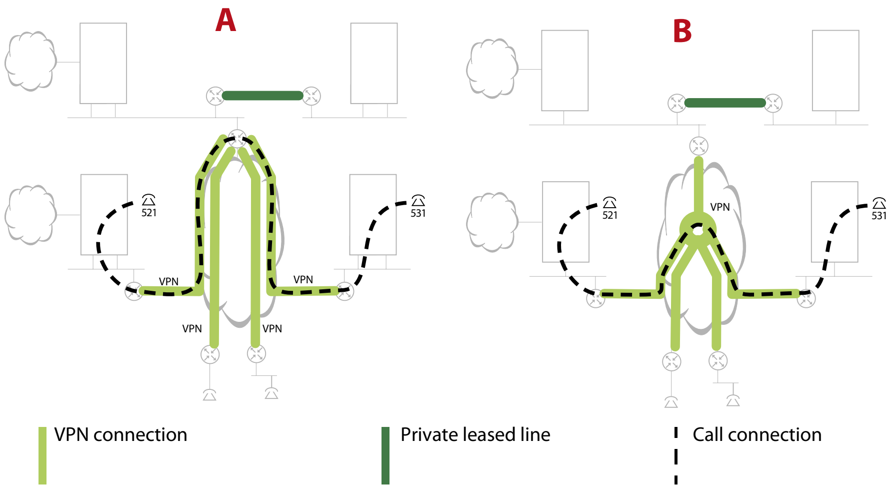
6. 4 Using VPN

When you encrypt voice data in the AIN, it is encrypted within the LAN but not necessarily on WAN links. If a connection runs for example to a remote IP system phone via various internet providers, the voice data on the internet is not automatically encrypted. To encrypt the entire link you also need to set up a VPN (Virtual Private Network) for WAN links.

A VPN provides a secure passage through the internet from one point to the next (e. g. from the Master to the IP system phone or to the satellite) and is therefore particularly well suited for WAN links over the internet. The IP packets to be transmitted are encoded and re-packaged in IP packets (tunnelling). The most frequently used VPN protocols are IPsec and SSL.

A simple VPN connects only two terminals or two locations with each other (see Fig. 12 , variant a). To connect several terminals or terminals with one another via VPN, you need to use a VPN router in the Internet (see Fig. 12 , variant b).

If using VPN in the AIN we recommend that whenever possible you work with a single internet provider who supports VPN routing and is able to cover all the locations. On the one hand this saves bandwidth resources and on the other it simplies the routing configuration.



a)Simple VPN connections:
One VPN in each case from the Master to the satellites. A call connection between user 521 and user 531 requires 2 VoIP channels from the Master to the internet.

b)Routed VPN connections:
The internet provider routes the VPN connections. A call connection between user 521 and user 531 does not require any VoIP channels from the Master to the internet.

Fig. 12 VPN in the reference network

6. 5 Methods for reducing bandwidth requirements

Voice data packets should be compressed whenever the available bandwidth resources are limited (which is the case particularly on WAN links). AIN supports the codecs used for this purpose. The bandwidth requirements can also be reduced by choosing the right frame length.

- Using codecs to compress voice data:
  On a WAN link with limited bandwidth it is advisable to use a compressing codec such as G.729. It considerably reduces the bandwidth requirement and the loss of voice quality remains tolerable.
  In the LAN area there is usually sufficient bandwidth available and better results are achieved with the uncompressed codec G.711 as the voice quality is not affected by a compressing method.
- Compressing the IP header:
  Voice packets are relatively small compared with their header (large overhead). On a point-to-point connection between two routers the header can be considerably compressed. The bandwidth resources available are then used more sparingly. The setting is made in the router. Possible method: CRTP compression. This method has to be supported and featured by the internet service provider for WAN links via the internet.
- Frame length of voice packets:
  The smaller the frame length of voice packets, the smaller the delay values generated but the greater the bandwidth requirement. For this reason we recommend that the frame length of voice packets be kept relatively small within the LAN area and relatively large for WAN connections with limited bandwidth.

Note:
Selecting a small frame length with the intention of keeping the delay values low in the case of very limited bandwidth resources can prove counter-productive as the amount of frame packets is then increased, which can lead to data congestion.

Tab. 26 Usual settings in practice

Network domain	Codec	Frame length	CRTP	Required bandwidth
LAN	G.711 secure G.711	20 ms	no	85 kbit/s 90 kbit/s
WAN link without VPN (PPP)	G.729 secure G.729	20 ms	yes	12 kbit/s 14 kbit/s
WAN link with VPN (PPP)	G.729 secure G.729	20 ms	no	48 kbit/s 50 kbit/s

6. 5. 1 Calculating the bandwidth requirements

With the formula below you can calculate the bandwidth requirements of a WAN link yourself:

Tab. 27 Formula for calculating the required bandwidth

$$BW = n \cdot \left(\frac{PS + L2 + AP}{FL} \right)$$

BW	:	Bandwidth requirement [kbit/s]
PS	:	Packet size [Byte]
L2	:	L2 overhead [Byte]
AP	:	Authentication prefix (SRTP) [Byte]
FL	:	Frame length [Byte]
n	=	**7.8125** (conversion factor byte/ms → kbit/s)

The values for the L2 overhead and the packet size can be found in the tables below.

Tab. 28 Table of values for packet size PS

Codec	G.711			G.729		
Frame length [ms]	**10 ms**	**20 ms**	**30 ms**	**10 ms**	**20 ms**	**30 ms**
Without CRTP compression	120	200	280	52	60	72
With CRTP compression	84	164	244	16	24	36

Tab. 29 Table of values for L2 overheads

Protocol	VPN (IPsec header = 56 bytes)	L2 overhead
Ethernet (ETH)	no	18
	yes	74
PPP / PPPoA / FrameRelay	no	6
	yes	62
PPPoE	no	26
	yes	82

Tab. 30 Table of values for authentication prefix AP

Codec	Authentication prefix (SRTP)	Explanation
G.711 / G.729	0	non-encrypted
secure G.711	10	encrypted (SRTP)
secure G.729	4	encrypted (SRTP)

Note:
The calculated bandwidth requirements apply only to the requirements for call connections. When rating a WAN link you also need to take account of the estimated requirements for data transmission. The bandwidth requirements for the exchange of signalling data between Master and satellites are relatively small and can be covered with a reserve supplement of one additional VoIP channel at most.

6. 6 Bandwidth control

If the bandwidth available for a call connection is insufficient, intermittent faults can occur as well as disruptive delays or even interruptions. One of the tasks of bandwidth control is to predict such situations and to prevent a call connection from being set up in the first place.

The bandwidth available in the AIN can vary greatly as it can comprise several LAN areas and several WAN links. A model is used to map the bandwidth situation as realistically as possible in the Master. In each case it calculates before a connection is set up whether or not the bandwidth available is sufficient. If not, the connection is not set up and the user obtains the congestion tone.

The better the model simulates reality, the more reliably the bandwidth resources can be managed.

The model consists of the following components:

- Bandwidth areas:
  A bandwidth area is a network section with the same bandwidth properties. In most cases it is a LAN but the internet as a whole is also mapped as a bandwidth area.
- WAN links:
  The WAN links connect the bandwidth areas with one another. Usually they consist of connections to an internet provider or leased lines. Frequently they have a limited bandwidth.
- VoIP routing table:
  This table indicates which bandwidth areas and WAN links can be used to set up a specific call connection.
- Fixed defaults for codec and frame length e. g. for Fax over VoIP because these data packets must not be compressed.

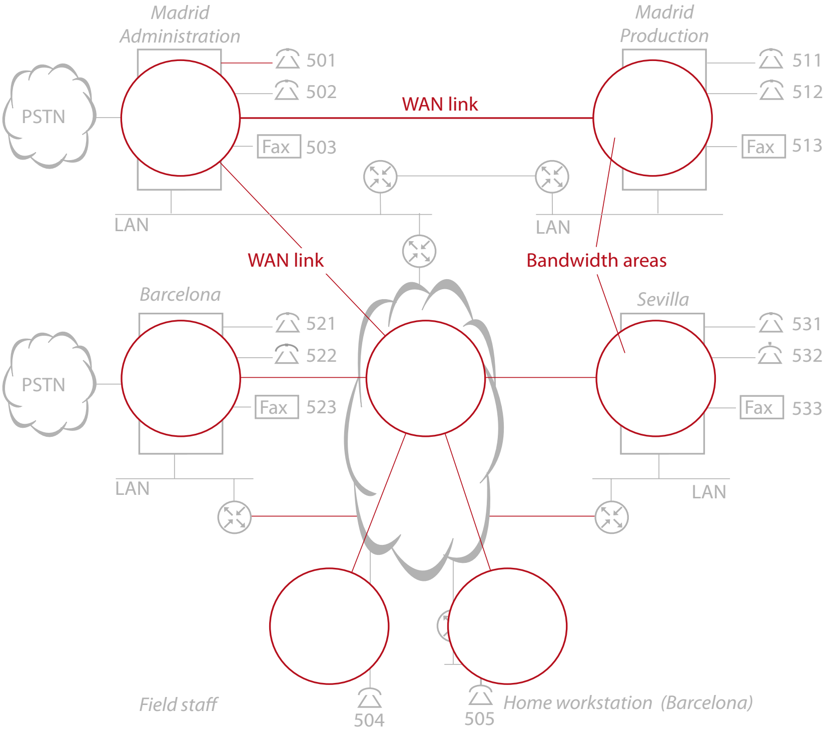


Fig. 13 Model for bandwidth control

6. 6. 1 Bandwidth control illustrated with an example

The following procedure takes place before the bandwidth control allows or denies a connection setup:

- The routing path for the connection is determined using the routing information in the VoIP routing tables.
- The bandwidth control specifies the codec and frame length for the connection. For this it selects from all the bandwidth areas and WAN links located on the routing path the most space-saving codec and the most space-saving frame length.

  Exception: In the case of a Fax over VoIP connection, calculations always involve codec G.711 and frame length 20 ms over the entire routing path, irrespective of the available bandwidth. In this way the best quality fax transmission is also guaranteed with the Fax over VoIP transmission type (see "Fax data transmission in AIN", page 54).
- The bandwidth control calculates the bandwidth requirements of a connection for each WAN link on the routing path. To do so it uses the values from Tab. 29 and Tab. 28 as well as the bandwidth calculation formula on page 92.
- The bandwidth control checks whether or not the bandwidth required is available. If so, the connection is set up. If not, the caller obtains congestion tone and a system message is generated.

Note:

– The bandwidth control only takes account of the traffic generated by the AIN. In other words the bandwidth control cannot detect whether other applications (e. g. a web radio) are routing data with the same or higher priority over the same WAN link.

– Line keys of key telephones and operator consoles are not taken into account by the bandwidth model.

6. 6. 1. 1 Single ringing tone

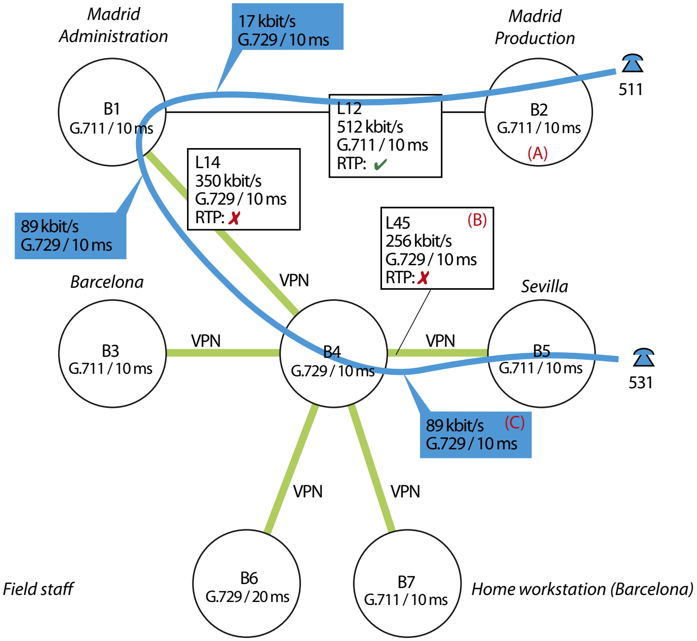
User 511 on satellite 1 (Madrid Production) calls user 531 on satellite 3 in Seville (see Fig. 14).

Assumptions:

- PPP is used as the transmission protocol on the WAN links.
- Routed VPNs are used for the WAN links via the internet as indicated in Fig. 12 , variant b).

Sequence:

- The bandwidth control selects the most space-saving variant of the codec and frame length on the routing path: G.711 / 10 ms could be used in the bandwidth areas and on the L12 link. However as the same settings have to apply for the entire connection, bandwidth control uses the more space-saving setting G.729 / 10 ms of WAN link L14 and L45.
- The bandwidth requirements on the WAN links L12, L14 and L45 are now calculated (see Tab. 31)
- On all three WAN links the bandwidth requirements are less than the available bandwidth so the connection is set up.



(A)
Bandwidth area with name of preferred codec / frame length

(C)
Codec / frame length actually used and resulting bandwidth requirements.

(B)

L45	Name of the WAN link
256 kbit/s	Available bandwidth
G.729/10 ms	Preferred codec / frame length
RTP	Use RTP compression yes/no

Fig. 14 Example of a connection set-up via WAN links L14 and L45

Tab. 31 Automatic calculation of the bandwidth requirements on the WAN links

WAN link	L2 overhead	Packet size	Frame length	Bandwidth		
				Requirement	Available	Free
	→Tab. 29	→Tab. 29		→page 92		
L12	6	16	10	17	512	495
L14	62	52	10	89	350	261
L45	62	52	10	89	256	167

6. 6. 1. 2 Second call via the same link

Users 501 and 531 are in a call. User 532 tries to call user 521 on satellite 2 in Barcelona (see Fig. 15).

Assumptions:

- PPP is used as the transmission protocol on the WAN links.
- Routed VPNs are used for the WAN links via the internet as indicated in Fig. 12 , variant b).

Sequence:

- The bandwidth control selects the most space-saving variant of the codec and frame length on the routing path. In this example this is G.729 / 10 ms.
- The bandwidth requirements on the WAN links L45 and L34 are now calculated (see Fig. 15)
- On both WAN links the bandwidth requirements are less than the available bandwidth so the enquiry call connection is set up.
- No more calls can be made on satellite 2 as the bandwidth available is now only 78 kbit/s.

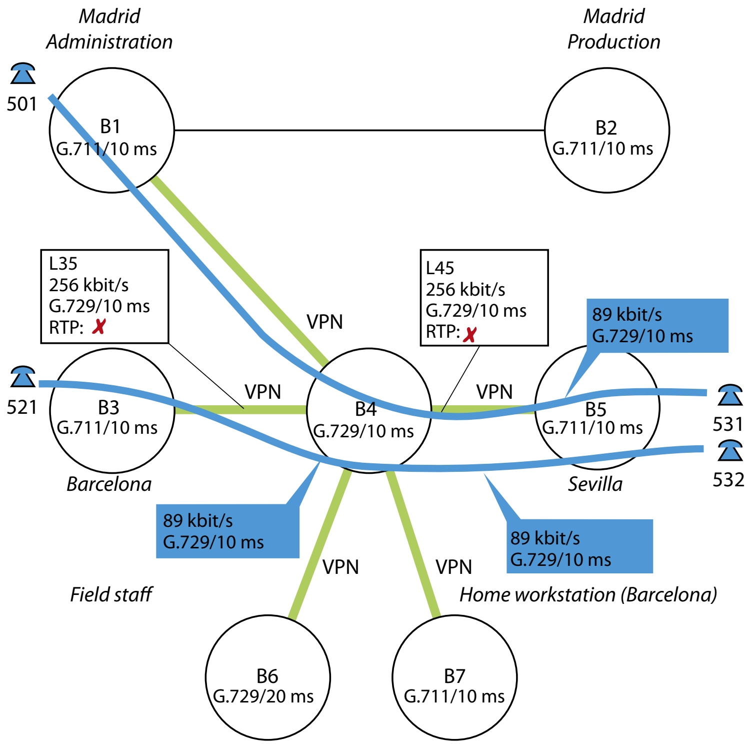


Fig. 15 Example of a connection set-up via WAN links L14 and L45

Tab. 32 Automatic calculation of the bandwidth requirements on the WAN links

Call connection	WAN link	L2 overhead	Packet size	Frame length	Bandwidth		
					Requirement	Available	Free
		→Tab. 29	→ Tab. 28		→page 92		
501 ↔ 531	L45	62	52	10	89	256	167
532 ↔ 521	L45	62	52	10	89	167	78
532 ↔ 521	L34	62	52	10	89	256	167

6. 6. 1. 3 Fax over VoIP connection

A fax is sent from fax machine 513 on satellite 1 (Madrid Production) to fax machine 533 on satellite 3 in Barcelona (see Fig. 16).

Assumptions:

- PPP is used as the transmission protocol on the WAN links.
- Routed VPNs are used for the WAN links via the internet as indicated in Fig. 12 , variant b).

Sequence:

- The bandwidth control selects the codec and frame length required for Fax over VoIP connections (G.711 / 20 ms).
- The bandwidth requirements on the WAN links L14 are now calculated (see Tab. 33).
- The bandwidth required is less than the available bandwidth and so the connection is set up.

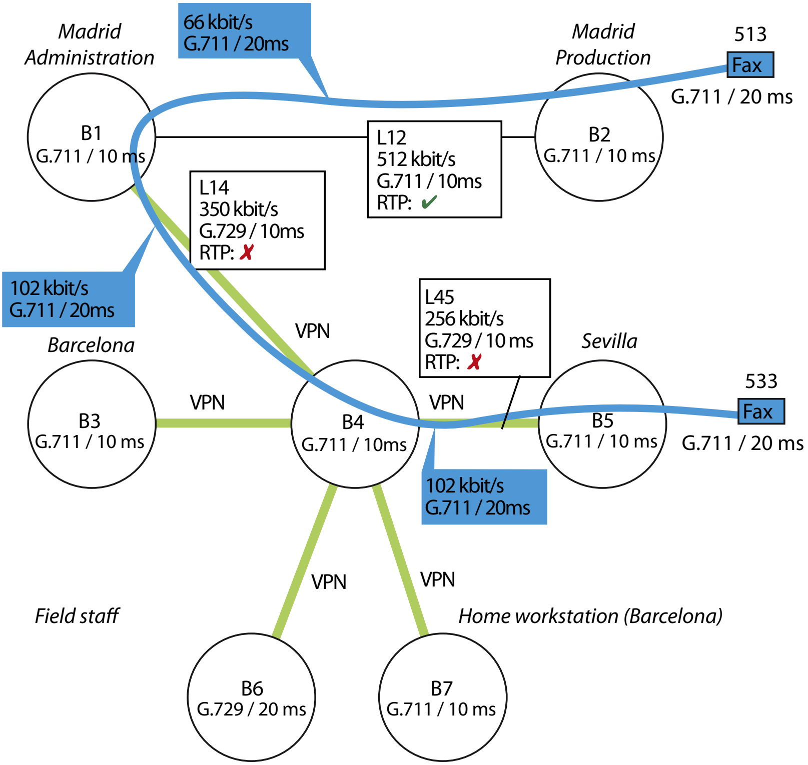


Fig. 16 Example of a connection set-up to an IP system phone

Tab. 33 Automatic calculation of the bandwidth requirements on WAN link L14

WAN link	L2 overhead	Packet size	Frame length	Bandwidth		
				Require-ment	Available	Free
	→Tab. 29	→Tab. 28		→page 92		
L12	6	164	20	66	512	446
L14	62	200	20	102	350	204
L45	62	200	20	102	256	154

The bandwidth requirement shows in this example that a Fax transmission according to the Fax over VoIP method requires considerably more bandwidth than a call connection.

6. 6. 1. 4 Call to an external SIP user

User 531 on satellite 3 in Barcelona calls an external SIP user (see Fig. 17).

Assumptions:

- PPP is used as the transmission protocol on the WAN links.
- Routed VPNs are used for the WAN links via the internet as indicated in Fig. 12 , variant b).
- The staff in Seville does not have direct internet access.

Sequence:

- The bandwidth control selects the most space-saving variant of the codec and frame length on the routing path. In this example this is G.729 / 10 ms.
- The bandwidth requirements on the WAN links L45 and L14 are now calculated (see Tab. 34)
- The bandwidth required is less than the available bandwidth and so the connection is set up.

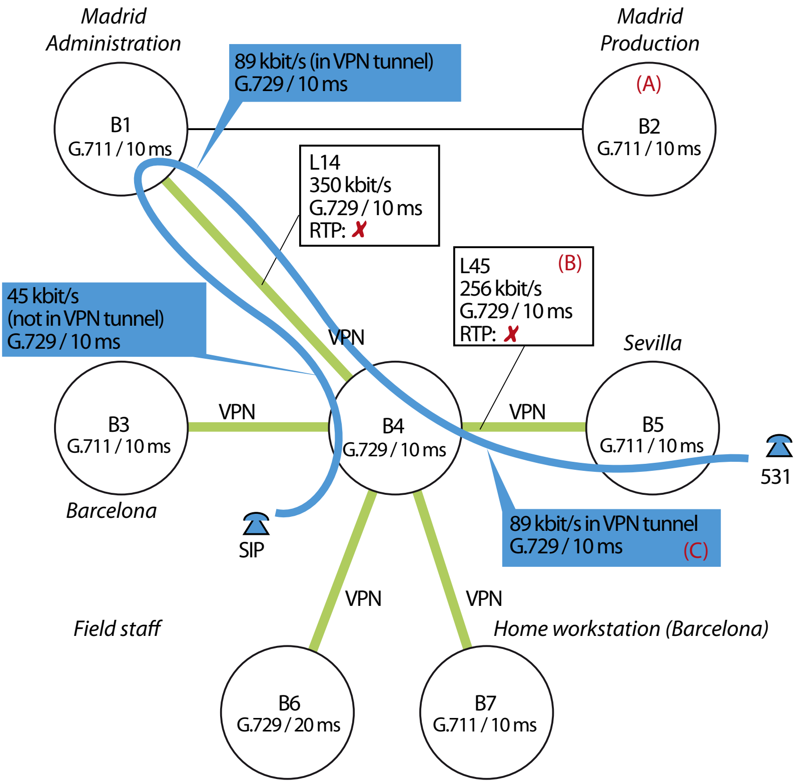


Fig. 17 Example of a connection set-up to an SIP phone

Tab. 34 Automatic calculation of the bandwidth requirements on WAN link L14

WAN link	L2 overhead	Packet size	Frame length	Bandwidth		
				Require-ment	Available	Free
	→Tab. 29	→Tab. 28		→page 92		
L45	62	52	10	89	256	139
L14 VPN	62	52	10	89	350	261
L14	6	52	10	45	259	214

6. 6. 2 Creating the bandwidth model

The model is created step by step:

- Determining the bandwidth topology, page 104
- Configuring the bandwidth areas, page 105
- Configuring the WAN links, page 106
- Configuring the VoIP routing tables, page 108

6. 6. 2. 1 Determining the bandwidth topology

In the following you map out the bandwidth areas and the WAN links.

1. Draw up a diagram of the bandwidth topology. To do so map out one bandwidth area for each IP section with its own LAN.
2. Map out another bandwidth area to represent the internet.
3. Map out the WAN links that connect the individual bandwidth areas.
4. For all the WAN links determine the bandwidth available for voice traffic. To do so measure the level of data traffic on the WAN link and subtract that value from the available bandwidth.

Note:
The model's accuracy depends on this calculation.

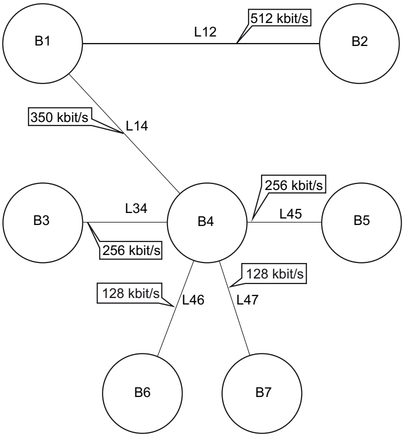


Fig. 18 Bandwidth areas and WAN links based on the example of the reference network

6. 6. 2. 2 Configuring the bandwidth areas

The instructions below explain the procedure for configuring the bandwidth areas:

1. In AMS (CM_6.1.2_*Bandwidth areas*) first create the bandwidth area in which the Master is located. Besides the name (B1 Madrid Administration) enter the values for the preferred frame length and codec. The bandwidth control uses these values to find the optimum setting for a call connection. As we are dealing with a LAN, a good choice is G.711 and a frame length of 20 ms.
2. Repeat this step for all the bandwidth areas.

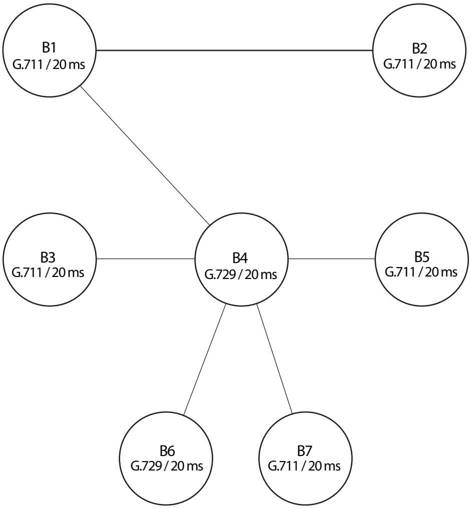


Fig. 19 Bandwidth control based on the example of the reference model

Tab. 35 Settings for the bandwidth areas (CM_6.1.2_*Bandwidth areas*)

Name	Node/Terminal	Codec	Frame length
B1 Madrid Administration	Master	G.711	20 ms
B2 Madrid Production	Satellite 1	G.711	20 ms
B3 Barcelona	Satellite 2	G.711	20 ms
B4 Internet	Satellite 3	G.729	20 ms
B5 Seville	Satellite 4	G.711	20 ms
B6 Barcelona HO	Office 35IP	G.711	20 ms
B7 Field staff	Aastra 2380ip	G.729	20 ms

6. 6. 2. 3 Configuring the WAN links

The instructions below explain the procedure for configuring the WAN links:

1. In AMS (CM_6.1.2_*WAN links*) first create the WAN link to the Master's bandwidth area. To do so select from the upper AMS table the bandwidth (reference No. B1 Madrid Administration1) and add the new WAN link to the lower AMS table. For the second bandwidth area enter bandwidth B2 Madrid Production (reference No. 2).
   Configure the parameters as follows:
   - *Bandwidth area A/B*: The two bandwidth areas connected with each other by the new WAN link.
   - Bandwidth: Enter here the value previously calculated (see "Determining the bandwidth topology", page 104).
   - *RTP compression*: If you are using RTP compression on this link, select *Yes*
   - *L2 overhead*: Enter the protocol-related size of the IP header here (see Tab. 29). Predefined values are available for the most common protocols. You can select one of these predefined values or enter your own value.
     Always enter the size of the header without the IPsec supplement of 56 bytes, even if VPN is used on this link (the IPsec supplement is taken into account in the configuration of the VoIP table, see page 108).
   - *Preferred codec and frame length*: The bandwidth control uses these values to find the optimum setting for a call connection. Enter the preferred values for this WAN link.
2. Repeat this step for all the WAN links.

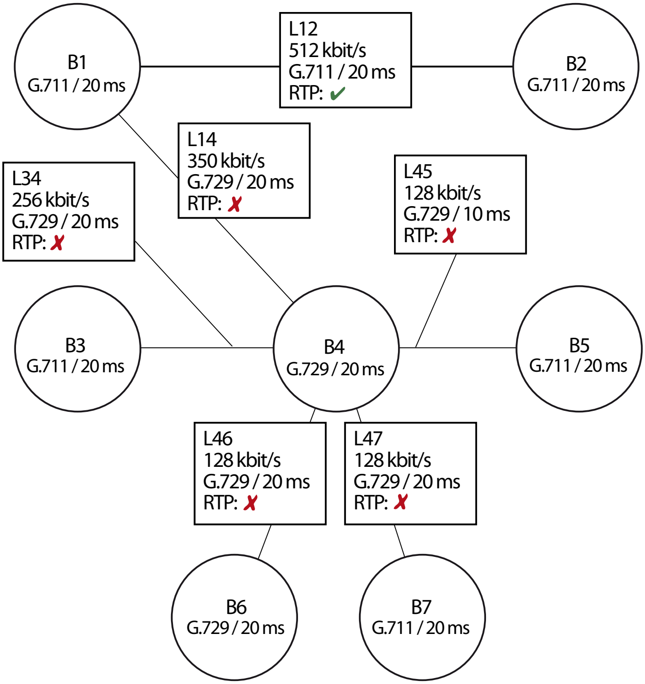


Fig. 20 Bandwidth control based on the example of the reference model

Tab. 36 Settings for the WAN links (CM_6.1.2_*WAN links*)

Bandwidth area		Bandwidth	RTP Compression	L2 overhead	Codec	Frame length
A	B					
L12 Madrid:						
B1	B2	512	on	6 bytes	G.711	20 ms
L14 Madrid - Internet:						
B1	B4	350	off	6 bytes	G.729	20 ms
L34 Barcelona - Internet:						
B3	B4	256	off	6 bytes	G.729	20 ms
L45 Seville - Internet:						
B4	B5	256	off	6 bytes	G.729	20 ms
L46 Barcelona HO - Internet:						
B4	B6	64	off	6 bytes	G.729	20 ms
L47 Field staff - Internet:						
B4	B7	64	off	6 bytes	G.729	20 ms

6. 6. 2. 4 Configuring the VoIP routing tables

One entry in the VoIP routing table specifies which WAN link is to be used between two neighbouring bandwidth areas. The entries are specified for each bandwidth area. The following rules apply to the entries:

- Each entry only specifies the link to the next bandwidth area.
- From the viewpoint of a bandwidth area the link must be defined to each possible destination.
- If the same link applies to several bandwidth areas, a capital X can be used as a wildcard. Exceptions must then be entered individually.
- You need to identify links with VPN by entering the VPN end (VPN peer). The bandwidth model then automatically takes the 56 byte larger L2 overhead into account when calculating the bandwidth requirements.

The procedure is described step by step below using the example of the reference network without VPN connections. For a clearer overview the bandwidth areas B6 and B7 have been omitted from the figures.

When the WAN links are created, the VoIP routing table is filled out automatically as much as possible:

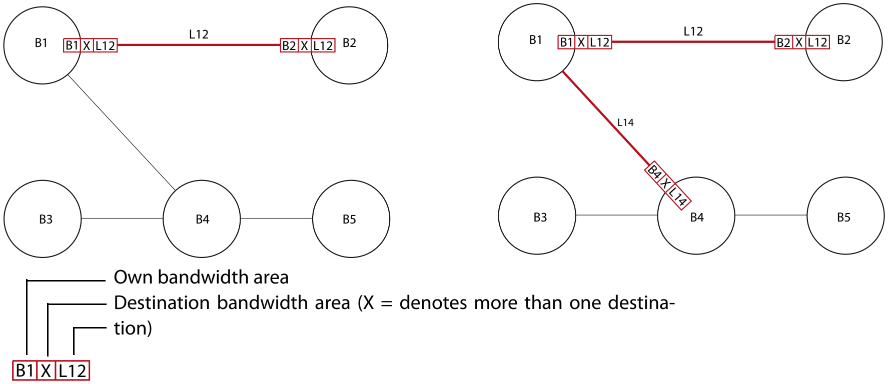


Fig. 21 Automatically generated entries when the WAN links L12 (left) and L14 (right) are created

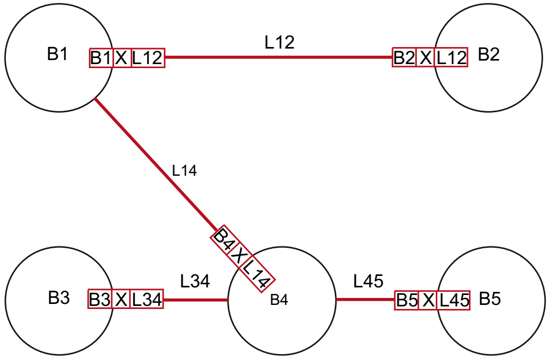


Fig. 22 **Automatically generated entries when all the WAN links are created**

The instructions below explain the procedure for completing the configuration of the VoIP routing table:

1. Use AMS (CM_6.1.2_*VoIP routing tables*) to process all the entries one after the other until they comply with Fig. 23 and Tab. 37.
2. Repeat this step for all the bandwidth areas.

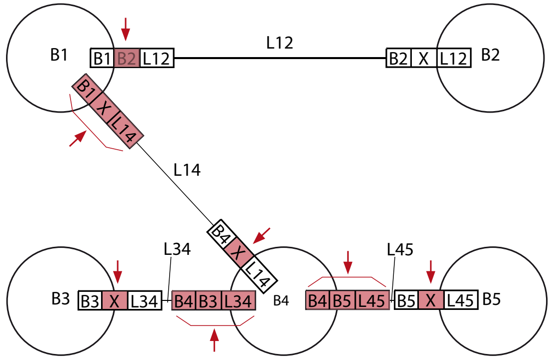


Fig. 23 **Completed entries in the VoIP routing table illustrated in a diagram**

Tab. 37 VoIP routing table for the reference network without VPN connections

Bandwidth area		WAN link	VPN-Peer
Own	Destination		
B1 Madrid Administration	B2 Madrid Production	L12 Madrid	-
B1 Madrid Administration	X	L14 Madrid - Internet	-
B2 Madrid Production	X	L12 Madrid	-
B3 Barcelona	X	L34 Barcelona - Internet	-
B4 Internet	X	L14 Madrid - Internet	-
B4 Internet	B3 Barcelona	L34 Barcelona - Internet	-
B4 Internet	B5 Seville	L45 Seville - Internet	-
B4 Internet	B6 Barcelona HO	L46 Barcelona HO - Internet	-
B4 Internet	B7 Field staff	L47 Field staff - Internet	-
B5 Seville[1]	X	L45 Seville - Internet	-
B6 Barcelona HO[1]	X	L46 Barcelona HO - Internet	-
B7 Field staff[1]	X	L47 Field staff - Internet	-

[1] In this example the LAN in this bandwidth area does not have a direct internet access.

If VPNs are used on the WAN links, the end of the VPN tunnel (*VPN-Peer*) setting) has to be entered in each case (see Tab. 38 and Tab. 39).

Tab. 38 VoIP Routing table with VPN connections in accordance with variant a) in Fig. 12

Bandwidth area		WAN link	VPN-Peer
Own	Destination		
B1 Madrid Administration	B2 Madrid Production	L12 Madrid	-
B1 Madrid Administration	B3 Barcelona	L14 Madrid - Internet	B3
B1 Madrid Administration	B4 Internet	L14 Madrid - Internet	-
B1 Madrid Administration	B5 Seville	L14 Madrid - Internet	B5
B1 Madrid Administration	B6 Barcelona HO	L14 Madrid - Internet	B6
B1 Madrid Administration	B7 Field staff	L14 Madrid - Internet	B7
B2 Madrid Production	X	L12 Madrid	-
B3 Barcelona	X	L34 Barcelona - Internet	B1
B3 Barcelona	B4 Internet	L34 Barcelona - Internet	-
B4 Internet	X	L14 Madrid - Internet	-
B4 Internet	B3 Barcelona	L34 Barcelona - Internet	-
B4 Internet	B5 Seville	L45 Seville - Internet	-
B4 Internet	B6 Barcelona HO	L46 Barcelona HO - Internet	-
B4 Internet	B7 Field staff	L47 Field staff - Internet	-
B5 Seville[1)]	X	L45 Seville - Internet	B1
B6 Barcelona HO1)	X	L46 Barcelona HO - Internet	B1
B7 Field staff 1)	X	L47 Field staff - Internet	B1

[1)] In this example the LAN in this bandwidth area does not have a direct internet access.

Tab. 39 VoIP Routing table with VPN connections in accordance with variant b) in Fig. 12

Bandwidth area		WAN link	VPN-Peer
Own	Destination		
B1 Madrid Administration	B2 Madrid Production	L12 Madrid	-
B1 Madrid Administration	B3 Barcelona	L14 Madrid - Internet	B3
B1 Madrid Administration	B4 Internet	L14 Madrid - Internet	-
B1 Madrid Administration	B5 Seville	L14 Madrid - Internet	B5
B1 Madrid Administration	B6 Barcelona HO	L14 Madrid - Internet	B6
B1 Madrid Administration	B7 Field staff	L14 Madrid - Internet	B7
B2 Madrid Production	X	L12 Madrid	-
B3 Barcelona	X	L34 Barcelona - Internet	B1
B3 Barcelona	B5 Seville	L34 Barcelona - Internet	B5
B3 Barcelona	B6 Barcelona HO	L34 Barcelona - Internet	B6
B3 Barcelona	B7 Field staff	L34 Barcelona - Internet	B7
B3 Barcelona	B4 Internet	L34 Barcelona - Internet	-
B4 Internet	X	L14 Madrid - Internet	-

Bandwidth area		WAN link	VPN-Peer
Own	Destination		
B4 Internet	B3 Barcelona	L34 Barcelona - Internet	-
B4 Internet	B5 Seville	L45 Seville - Internet	-
B4 Internet	B6 Barcelona HO	L46 Barcelona HO - Internet	-
B4 Internet	B7 Field staff	L47 Field staff - Internet	-
B5 Seville[1)]	X	L45 Seville - Internet	B1
B5 Seville	B3 Barcelona	L45 Seville - Internet	B3
B5 Seville	B6 Barcelona HO	L45 Seville - Internet	B6
B5 Seville	B7 Field staff	L45 Seville - Internet	B7
B6 Barcelona HO[1)]	X	L46 Barcelona HO - Internet	B1
B6 Barcelona HO	B3 Barcelona	L46 Barcelona HO - Internet	B3
B6 Barcelona HO	B5 Seville	L46 Barcelona HO - Internet	B5
B6 Barcelona HO	B7 Field staff	L46 Barcelona HO - Internet	B7
B7 Field staff [1)]	X	L47 Field staff - Internet	B1
B7 Field staff	B3 Barcelona	L47 Field staff - Internet	B3
B7 Field staff	B5 Seville	L47 Field staff - Internet	B5
B7 Field staff	B6 Barcelona HO	L47 Field staff - Internet	B6

[1)] In this example the LAN in this bandwidth area does not have a direct internet access.

7 Annex

Listed here is a summary of the main AIN parameters and default values as well as information on the TCP/IP ports used and the configuration of firewalls.

7.1 Reference for the main IP and AIN parameters

Listed below are the main parameters for commissioning and configuring an AIN, complete with brief explanations.

Tab. 40 Legend

Symbols	Meaning
*	Default value
(..)	Display, cannot be modified
<..>	Expected input

7.1.1 Parameters of the communication server

7.1.1.1 Default values of the IP addressing

Tab. 41 Default values for IP addresses

Parameter	Parameter value
IP address	192.168.104.13
Subnet mask	255.255.255.0
Gateway address	0.0.0.0
DHCP	On
Host name	
• Aastra 415	*aastra415*-<MAC address>
• Aastra 430	*aastra430*-<MAC address>
• Aastra 470	*aastra470*-<MAC address>

Note:

– If the communication server is unable to log on via DHCP/DNS after a first start (for instance because no DHCP server is available), it starts with the static default IP address.

– If a manually entered IP address is already stored at the time of the first start, the communication server deactivates DHCP and starts with this address.

– To detect the communication server in the IP network, proceed according to "Detecting the communication servers in the IP network", page 30.

7. 1. 1. 2 Permanent parameters

The following parameters are set permanently and cannot be modified.

Tab. 42 Permanent parameters that cannot be set

Parameter	Parameter values
Silence Supression	Off
Echo Cancellation	On

7. 1. 1. 3 IP addressing of the satellites

Tab. 43 Logged Satellites: CM_6.1.1

Parameter	Parameter values	Explanation
Satellite:		
• *Name*	(Name)	Satellite designation according to the system specifications in the AMS Shell
• *Connected to AIN since.*	(date) (time)	Date and time of the last logon to the Master
• *EID no.*	(number)	Satellite EID No. (stored on the EID card)
IP settings:		
• *Host name*	(Name)	Satellite name registered in the DNS server
• *IP address*	(IP address)	IP addressing of the satellites
• *Subnet mask*	(Subnet mask)	
• *Default gateway*	(IP address)	
DNS/DHCP settings::		
• *DHCP*	**Yes* / *No*	
• *Primary DNS server*	(IP address)	Address of the primary DNS server
• *Secondary DNS server*	(IP address)	Address of the secondary DNS server
• *Domain name*	(Name)	Domain name

7. 1. 1. 4 IP addressing on the Master

Tab. 44 Mainboard Ethernet Interface CM_2.2.1

Parameter	Parameter values	Explanation
IP settings for Ethernet interface:		See "Specifying the IP addressing", page 26, for more information.
• *Host name*	<Name>	Host name of the communication server for the address allocation in the DNS server
• *IP address*	<IP address>[1]	IP address of the communication server
• *Subnet mask*	<Subnet mask>[1]	
• *Gateway*	<IP address>[1]	Default gateway of the communication server
• *Ethernet MAC address*	(MAC address)	Unique MAC address of the Ethernet interface
Satellite settings:		See "Specifying the IP addressing", page 26, for more information.
• *Master address*	<empty/IP address/ name>	• If the communication server is the Master, leave the entry blank • If the communication server is a satellite and the Master is addressed via DHCP/DNS, enter the Master's host name • If the communication server is a satellite and the Master is addressed statically, enter the Master's IP address Please note that: This entry allows the communication server to detect whether it is to be used as Master or satellite in the AIN.
DNS/DHCP settings::		See AMS online help for more information.
• *DHCP*	**Yes* / *No*	
• *Primary DNS server*	<IP address>[1]	Address of the primary DNS server
• *Secondary DNS server*	<IP address>[1]	Address of the secondary DNS server
• *Domain name*	<Name>[1]	Domain name
IP settings for PPP over RAS connection:		See AMS online help for more information.
• *IP address*	<IP address>	
• *Subnet mask*	<Subnet mask>	
• *Gateway*	<IP address>	
• *Client range from*	<IP address>	
• *Client range to*	<IP address>	

[1] When DHCP is activated, the DHCP server address is entered.

7.1.1.5 DHCP server

Tab. 45 Basic settings of the integrated DHCP server

Parameter	Description
DHCP server	The internal DHCP server is switched on. **Note:** The DHCP server can only be switched on if the communication server itself has a static address and is addressed without DHCP.
DHCP support	*All*: All the devices in the subnet requesting an IP address (all DHCP clients) are provided with an IP address from the address range of the DHCP server, and the link is registered. *Aastra devices only*: Only Aastra DHCP clients such as IP-bound system phones are provided with an IP address and registered.
Manufacturer-specific options	Using the manufacturer-specific options the DHCP server can serve IP-bound system phones with specific configuration information. *Default*: The DHCP server provides the configuration data stored as standard. *Configuration file*: The DHCP server provides the configuration options specified in the *vendoroptions* configuration file. You need to store this configuration file beforehand in the */dhcp/* directory in the communication server's file management system. No manufacturer-specific options are provided if the DHCP server cannot find the configuration file. Information on how to create a separate configuration file can be found in Chapter "DHCP options", page 125)
DHCP settings:	
• *Subnet mask*	Subnet mask (use the same setting as in the communication server's IP addressing).
• *Gateway*	Subnet gateway (use the same setting as in the communication server's IP addressing).
• *First IP address*	First address of the address range controlled by the DHCP server.
• *Last IP address*	Last address of the address range controlled by the DHCP server.
• *Primary DNS server*	DNS server IP address (use the same setting as in the communication server's IP addressing).
• *Secondary DNS server*	IP address of the alternative DNS server (use the same setting as in the communication server's IP addressing).
• *Domain name*	Domain to which the DHCP server is to be connected. (Use the same setting as in the communication server's IP addressing).
• *Lease time*	Before the lease time expires, the DHCP clients (e.g. system phones) notify the DHCP server whether they want to maintain their link. Once the lease time has expired, the DHCP server extends the validity of all the links for which it received such requests and resets the timer for the lease time. All links for which no request was received are disconnected and the corresponding IP addresses are released. **Note:** If you modify the lease time, all non-reserved links are disconnected.

7.1.1.6 QoS Configuration

Tab. 46 Prioritization: CM_2.2.5_*QoS configuration*, Layer 2 settings

Parameter	Parameter values	Explanation
Layer 2 settings:		See "Prioritization", page 87 for information about CoS
• *Active for*	**Nodes only* / *Nodes and Terminals*	VLAN/CoS settings made here are not valid for IP system phones (setting: *Nodes only*) or affect all AIN components including IP phones.
• *Frame type*	**Standard (no QoS*) / *VLAN/CoS 802.1p/Q*)	For the tagged VLAN allocation of the communication server in accordance with IEEE 802.1/Q or to activate CoS prioritization, set the value to *VLAN/CoS* and assign the VLAN_ID further below. If the VLAN allocation is port-based on the switch used, set the value to *Default* (default value).
• *CoS prioritization level*	*0 Best Effort* *1 Background* *2 Standard* *3 Excellent Effort* *4 Streaming Multimedia* **5 Interactive Multimedia* *6 Interactive Voice*	Specifies the priority of the voice packets when CoS prioritization is switched on. Level 5 has to be set for a good voice quality.
• *VLAN ID*	*1 to 4094	ID of the VLAN to which the communication server is to be allocated. Note: If the IP phones are also integrated in the VLAN (setting *Active for* = *Nodes and terminals*), the IP phones must be allocated to the same VLAN (see Tab. 58).

Tab. 47 Prioritization: CM_2.2.5_*QoS configuration*, Layer 3 settings

Parameter	Parameter values	Explanation
Layer 3 settings:		See "Prioritization", page 87 for information about ToS
• *QoS Layer 3*	*ToS*/**DSCP*	Determines the QoS method
• *ToS prioritization*	*0 Best Routine* *1 Priority* *2 Immediate* *3 Flash* *4 Flash Override* **5 CRITIC/ECP* *6 Internetwork Control* *7 Network Control*	ToS IP Precedence: Specifies the Layer 3 priority for the voice packets. Level 5 has to be set for a good voice quality. Levels 6 and 7 are reserved for the network administration and should not be used.
• *ToS type of service*	*0 Normal Service* *2 High Reliability* *4 High Throughput* *8 *Low Latency*	
• *DSCP class*	0 to 63; *46	

7. 1. 1. 7 Satellite offline operation mode

Tab. 48 Satellites offline operation mode: CM_2.2.5_*Signalling connection*

Parameter	Parameter values	Explanation
Monitoring range	*Minimal* *Very short* *Short* **Medium* *Long* *Very long*	Specifies the interval according to which the signalling connections between Master and satellites are verified (see "Satellite in Offline Mode", page 62) Note: The monitoring interval must be set the same on all nodes in the AIN.
Minimum connection time	*5 .. 180000 s	Amount of time during which the test connection to the Master has to be stable in offline mode before the satellite switches back to online mode.
For more details about these settings, see "Satellite in Offline Mode", page 62		

Tab. 49 Satellites offline operation mode: Guideline values for the monitoring intervals

Monitoring range	Master-satellite connection is ..	
	intact[1)]	interrupted
Minimal	20 .. 120 ms	50 ms
Very short	0.5 .. 1.7 s	0.5 s
Short	4 .. 16 s	5 s
Medium	9 .. 37 s	12 s
Long	32 .. 102 s	30 s
Very long	110 ..240 s	60 s

[1)] The times can vary depending on the actual constellation, which is why time ranges are specified here. For more information about the Monitoring range see "Satellite in Offline Mode", page 62.

7. 1. 1. 8 Bandwidth areas

Tab. 50 VoIP routing: CM_6.1.2_*Bandwidth areas*[1)]

Parameter	Parameter values	Explanation
Name	<Name (max. 20 characters)>	Name of the bandwidth area.
Preferred Codec	**G711a/G711u/G729*	G.711a uses the German tone signalling process; G.711u, the US process. See "Methods for reducing bandwidth requirements", page 91 for more information.
Preferred frame length	*10/20/30 ms	See "Methods for reducing bandwidth requirements", page 91 for more information.

[1)] Configure the bandwidth areas in accordance with the Chapter "Configuring the bandwidth areas", page 105

Tab. 51 VoIP routing: CM_6.1.2_*WAN links*[1)]

Parameter	Parameter values	Explanation
WAN link name	<Name (max. 20 characters)>	Name of the WAN link
Bandwidth area A	<Bandwidth area)>	One of the previously defined bandwidth areas
Bandwidth area B	<Bandwidth area)>	One of the previously defined bandwidth areas
Bandwidth	<Bandwidth [kbit/s]>	Enter here the bandwidth available for VoIP on this WAN link.
VoIP channels	(Number)	Displays the maximum possible number of VoIP channels that can be set up simultaneously over this WAN link (see Chapter "Calculating the bandwidth requirements", page 92)
RTP compression	Yes/*No	Compressing the IP headers
L2 overhead	*18 Ethernet* *6 PPP/PPPoA/FrameRelay* *26 PPoE* *xx user-defined (0 to 255 [Byte])	The numerical value corresponds to the header size in bytes. See also Tab. 29.
Preferred Codec	**G.711a*/*G.711u*/*G.729*	G.711a uses the German tone signalling process; G.711u, the US process. See "Methods for reducing bandwidth requirements", page 91 for more information.
Preferred frame length	10/*20/30 ms	See "Methods for reducing bandwidth requirements", page 91 for more information about the frame length.

Tab. 52 VoIP routing: CM_6.1.2_*VoIP routing table*[2)]

Parameter	Parameter values	Explanation
Own bandwidth area	<Bandwidth area>	One of the previously defined bandwidth areas
Destination bandwidth area	<Bandwidth area>	One of the previously defined bandwidth areas

[1)] Configure the WAN links in accordance with the Chapter "Configuring the WAN links", page 106

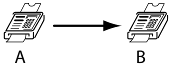
[2)] Configure the VoIP routing table in accordance with the Chapter "Configuring the VoIP routing tables", page 108

7. 1. 1. 9 Fax transmission

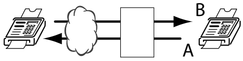
Tab. 53 Fax connection in the AIN: CM_4.2_*Analogue settings*

Parameter	Parameter values	Explanation
Fax device	*No fax device*	Terminal is not a fax machine. →voice connection is established.
	Fax machine (->T.38T.38)	Fax terminal without voice and voice-mail system. → For connections via IP a T.38 connection is set up whenever possible.
	Combined unit (->voice/T.38)	Fax terminal with voice and/or voice-mail system. → The voice connection is established first. When transmitting fax data, it is best to switch over to a T.38 connection whenever possible in the case of connections via IP.
	Fax over VoIP (->G.711)	→G.711 voice connection is established.

Tab. 54 Internal fax connection in the AIN based on the *fax device* setting

		**Terminal B**			
		No fax device	***Fax device***	***Combined unit***	***Fax over VoIP***
Terminal A	*No fax device*	Language	T.38	voice/T.38	G.711
	Fax device	T.38	T.38	T.38	G.711
	Combined unit	voice/T.38	T.38	voice/T.38	G.711
	Fax over VoIP	G.711	G.711	G.711	G.711

Tab. 55 Internal fax connection in the AIN based on the *fax device* setting

		**Network interface**	
		FXS, DSI-AD2, SIP	**T, T2, PISN** [1]
Terminal A/B	*No fax device*	Language	voice/T.38
	Fax device	T.38	T.38
	Combined unit	voice/T.38	voice/T.38
	Fax over VoIP	G.711	G.711

[1] Gr. 2/3 fax service

7. 1. 1. 10 IP terminal interface

Tab. 56 VoIP routing IP terminals: CM_4.2_*IP settings*

Parameter	Parameter values	Explanation
Terminal ID	(ID)	The ID is assigned by the system and is used for user allocation purposes
Bandwidth area	<Name of the bandwidth area>	At this point assign the terminal to a predefined bandwidth area
Hardware version	(hardware version)	The terminal's current hardware version (information read out from the terminal)
Name	(Name)	User name
Application software version	(<software version>)	Indicates the version of the application software.
Boot software version	(<software version>)	Indicates the boot software version.
Status	(Logged on/Not loggedon/ Upload/No terminal detected)	Indicates the current login status of the IP system phone.
MAC address	<MAC address>	MAC address of the IP system phone. Read in automatically when phones registers. The terminal data is assigned to the phone using this MAC address. Delete it if you wish to cancel the allocation of the terminal to the terminal data. As an alternative to registering the phone using the registration code you can also enter the phone's MAC address at this point.
IP address	<IP address>	IP address of the IP system phone. Read in automatically when phones registers.
RTP port	<IRTP port>	RTP port used. Default value is 30000. Does not, as a rule, have to be changed
Signalling port	(Signalling port)	Signalling port used. Non-configurable
Registration code	<Number>	Aid for allocating an IP system phone to the relevant terminal data. Enter this number on the phone when prompted to do so. Default value is the call number of the allocated user or a blank entry. Alternatively you can also make the allocation directly by entering the phone's MAC address (see *MAC address* setting above)

7. 1. 2 Local parameters of the IP system phones

7. 1. 2. 1 Default values of the IP addressing

Tab. 57 Default values Office 70IP-b

Parameter	Parameter value
Own addressing:	
• *IP-Adress*	192.168.104.33
• *Subnet Mask*	255.255.255.0
Gateway addressing:	
• *GW-Adress*	0.0.0.0
System addressing:	
• *PBX adress*	192.168.104.23
• *DHCP*	*on*
• *DNS name*	*intelligate*
• *DNS server adress*	0.0.0.0

7. 1. 2. 2 Local parameters for Aastra 5300 series

Tab. 58 Settings for IP addressing in the local configuration menu

IP addresses	Explanation
DHCP setting (in the *Administration* menu):	
• *DHCP*	Activate or deactivate DHCP (*on* / *off* - default value: *on*)
Phone address (in the menu *Administration* / *IP adress settings*):	
• *IP-Adress*	IP address of the IP system phone. Configurable only if DHCP is deactivated.
• *Subnet Mask*	Subnet mask of the IP system phone. Configurable only if DHCP is deactivated.
Gateway address (in the *Administration* menu):	
• *GW-Adress*	Gateway address: Phone-side IP address of the router that provides the transition to the other partial areas of the IP network. If all the IP phones and all satellites are in the same LAN area as the Master, 000.000.000.000 can be used for the Gateway address (default value).
Addressing of the single system/node (in the *Administration* / *PBX settings* menu):	
• *PBX adress*	Static IP address of the Ethernet interface on the basic system of the single system/ node. Read only if the *DNS name* entry is blank.
• *PBX adress backup*	This setting is of no relevance for operation on an Aastra 430 system and can be left blank
DNS settings (in the *Administration* / *DNS settings* menu):	
• *DHCP*	Activate or deactivate DHCP: Default value: on
• *DNS name*	Host name of the single system/node. Default value: *intelligate*. If the IP address of the communication server is to be entered as static, you need to delete this entry.

IP addresses	Explanation
• *DNS name backup*	This setting is of no relevance for operation on an Aastra 430 system and can be left blank
• *DNS server adress*	Address of the DNS server (entered by the DHCP server)
• *DNS domain*	Domain of the DNS server (entered by the DHCP server)
VLAN settings (in the *Administration* / *VLAN settings* menu):	
• *VLAN_ENABLED*	For the tagged VLAN allocation of the terminal in accordance with IEEE 802.1/Q set the value to *on* and allocate the VLAN_ID further below. If the phone is not to be allocated to any VLAN or if the VLAN allocation is port-based on the switch used, set the value to *off* (default value).
• *VLAN_PRIO*	VLAN priority. Only has an influence if *VLAN_ENABLED* = *on*
• *VLAN_ID*	ID of the VLAN to which the phone is to be allocated. Note: The communication server must be allocated to the same VLAN (see Tab. 46). Only has an influence if VLAN_ENABLED = *on*
VLAN PC settings (in the *Administration* / *VLAN PC port settings* menu): These settings are of significance only if a PC is connected to the IP phone.	
• *VLANPC_ENABLED*	With this setting you can connect assign the PC connected to the phone to a different VLAN than the phone. For the tagged VLAN allocation of the PC in accordance with IEEE 802.1/Q set the value to *on* and allocate the VLAN_ID further below. Set the value to *off* in the following cases: • Neither the IP phone nor the connected PC are allocated to a VLAN. • The connected PC is allocated to the same VLAN as the phone,
• *VLANPC_PRIO*	VLAN priority. Only has an influence if *VLANPC_ENABLED* = *on*
• *VLANPC_TAGS*	VLAN tags are not evaluated on the PC and the network card normally ignores them. Some older and low-cost network cards are unable to identify and successfully ignore the VLAN tags. This can result in transmission errors. You can prevent them with the setting *VLANPC_TAGS* = *off*. For reasons of compatibility with older terminal software the default value is on *on*
• *VLAN PC_ID*	ID of the VLAN to which the connected PC is to be allocated. Only has an influence if VLAN_ENABLED = *on*
The other settings of the local terminal configuration are for operating an IP terminal on a different communication system. Please leave the settings unchanged. In particular make sure that the entries in the *Administration* / *802.1x settings* menu remain blank. Also make sure that the *Public media port* entries in the menu *Administration* / *NAT settings* and *TOS value* do not correspond with the same settings in the communication server and are ignored at this point.	

7.2 TCP/IP Ports and Firewall

Firewalls used within the AIN must be configured for AIN operation. This includes opening the relevant ports and, when using VPN connections, the VPN configuration.

With VPN connections the following ports must be opened on a firewall:

- If a VPN connection terminates at the firewall itself, no port needs to be opened.
- If a VPN connection terminates behind the firewall, e. g. directly at the terminal, port 3389 needs to be opened at the firewall (VPN pass through).
- If a VPN connection terminates in front of the firewall, e. g. at a different firewall, the ports used by the AIN components need to be opened.
- If all the WAN links in the AIN are VPN connections throughout and if they do not terminate at the firewalls themselves, port 3389 only needs to be opened in the firewalls of the WAN links.
- If the WAN links are only partly or not at all designed as VPN connections or if firewalls are also used within the LAN, the ports used by the AIN components must be opened. A list with the used ports is published by Support and continually updated. The list can be accessed on the internet under FAQ entry 1049:
  https://PBXweb.aastra.com/extra/support/list.asp?Type=FAQ.

7. 3 DHCP options

Vendor class identifier (Option 60)

The broadcast address request of an IP system phone comprises the MAC address as well as the vendor class identifier. If the DHCP server finds an assignment for the identifier in its configuration, it is able to provide the IP system phone with the vendor-specific information (Option 43).

Tab. 59 Option 60: Vendor class identifier for the IP system terminals

IP system terminal	Vendor class identifier
Aastra 5360ip	Aamadeus IP phone
Aastra 5361ip	Aamadeus IP phone
Aastra 5370ip	Aamadeus IP phone
Aastra 5380ip	Aamadeus IP phone

Tab. 60 Option 60: Vendor class identifier for Aastra SIP phones

IP system terminal	Vendor class identifier
Aastra 6753i	AastraIPPhone53i
Aastra 6755i	AastraIPPhone55i
Aastra 6757i	AastraIPPhone57i
Aastra 6730i	AastraIPPhone6730i
Aastra 6731i	AastraIPPhone6731i
Aastra 6739i	AastraIPPhone6739i
OMM RFP	OpenMobility

Vendor-specific information (Option 43)

If the DHCP server is able to assign an address request to an IP system phone using the vendor class identifier, it sends it not only the address co-ordinates but also the configured vendor specific information. The information consists of phone configuration parameters. Use the information contained in Tab. 61 to map the required parameters in a DHCP server configuration.

Tab. 61 Option 43: Configuration parameters for IP system phones that can be adapted using Option 43.

Attribute	Option code	Hex	Length (octet)	Type	Explanation
PBX_ADRESS	03	$03	4	UINT32	IP address of the communication server
SIP_PORT_PBX	04	$04	2	UINT16	SIP port of the communication server
SIP_PORT_PHONE	05	$05	2	UINT16	SIP port of the IP system phone
VLAN_PRIO	07	$07	1	UINT8	VLAN priority of the IP system phone (0 to 6)
VLAN_ID/VLAN_ENABLED	08	$08	2	UINT16	VLAN ID of the system phone (values between 0 and 4094, with value 0 deactivating the VLAN)
VLANPC_PRIO	09	$09	1	UINT8	VLAN priority of the PC interface on the IP system phone (0 to 6)
VLANPC_ID/ VLANPC_ENABLED	10	$0A	2	UINT16	VLAN ID of the PC interface on the IP system phone (values between 0 and 4094, with value 0 deactivating the VLAN)
VLAN PC port TAGS	11	$0B	1	UINT8	VLAN tag of the PC interface on the IP system phone: 1 = activated 0 = deactivated

The example below shows a configuration file for the integrated DHCP server:

```
# This is a sample configuration file for the Aamadeus IP
phones.

# Depending on the Vendor Class Identifier different options are

# set.


# The Vendor Class for the Aamadeus IP phone

Option 60 == Aamadeus IP Phone


{

# Vendor specific information:

# PBX IP address:Code 0x03; Length 4; 172.020.054.001

# --> Hex string: 0x0304AC143601

# SIP Port PBX:Code 0x04; Length 2; 18060

# --> Hex string: 0x0402468C

# SIP Port Phone:Code 0x05; Length 2; 18060

# --> Hex string: 0x0502468C

# Put hex string parts together to get the whole option 43
string:

Option 43 = 0x0304AC1436010402468C0502468C

}

# From here on another vendor class can be defined.
```

Index