Aastra Business Communication Solution

SIP and SIP terminals as of R1.0

System Manual

Platforms supported:

Aastra 415

Aastra 430

Aastra 470

This system manual deals with connecting SIP terminals to an Aastra 400, connecting Aastra 400 to a SIP provider and networking of communication servers via the SIP protocol.

It is intended for planners, installers and system managers of Aastra 400 communication systems.

syd-0407_en / 1.0 – R1.0 – © 06.2011

Content

1	**Safety Information**	**4**
1. 1	About the products	4
1. 2	About this document	6
2	**Introduction**	**8**
2. 1	What is SIP?	8
2. 1. 1	System components	9
2. 1. 2	Types of connection setup	10
2. 2	Security aspects with VoIP	12
2. 3	SIP in Aastra 400	14
2. 4	SIP RFCs supported by Aastra 400	15
3	**SIP terminals**	**18**
3. 1	Types of terminal	18
3. 2	SIP terminals of the Aastra 6700i series	19
3. 2. 1	Integration in Aastra 400	20
3. 2. 2	Configuration of terminal data via AMS	22
3. 2. 3	System menu	27
3. 2. 4	Presence menu	29
3. 2. 5	Configuration methods	30
3. 2. 5. 1	Configuration using configuration files	31
3. 2. 5. 2	Web user interface	33
3. 2. 5. 3	Terminal user interface	35
3. 2. 5. 4	Priority of the configuration methods	36
3. 2. 6	Existing infrastructure	37
3. 2. 7	Registering a terminal of the series Aastra 6700i	38
3. 2. 8	Software Update	41
3. 2. 9	Language concept	43
3. 3	Other Aastra SIP terminals and by other manufacturers	45
3. 3. 1	Overview	46
3. 3. 2	Registration process	47
3. 4	Features Overview	50
4	**SIP access**	**58**
4. 1	Introduction	58
4. 2	Routing elements	59
4. 3	Configuring the system for SIP access	59
4. 4	Configuration tables	61

5 SIP Networking 67
5. 1 Introduction 67
5. 2 SIP networking with two systems 68
5. 3 SIP networking with several systems 70
5. 4 Features supported with SIP networking 70

1 Safety Information

This Chapter contains information about the products of the Aastra 400 series and this document itself as well as definitions relating to safety and general considerations. Please read through these safety instructions carefully.

1. 1 About the products

Purpose and function

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

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

User groups

The phones, 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 operator consoles 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.

Trademarks

The software and hardware designations referred to in this document are registered trademarks and are subject to statutory provisions.

All mentioned trademarks are trademarks of their respective proprietors.

User information

Aastra 400 products are supplied complete with safety and product information, quick user's guides and user's guides.

These and all other user documents such as System Manuals are available for download from the Aastra document portal as individual documents or as documentation packs. Some user documents are accessible only via a partner login.

Document portal:	www.aastra.com/docfinder

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 a 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.

Exclusion of Liability

The products of the Aastra 400 family have been manufactured in accordance with ISO 9001 quality guidelines. The relevant user information has been compiled with the utmost care. The functions of the product and of all part products have been checked and released as a result of extensive approval 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 on the part of a product. Potential areas of particular risk are signalled in the appropriate sections of the user information. Liability for loss of profit shall be excluded in any case.

1. 2 About this document

This System Manual provides information on how SIP (Session Initiation Protocol) is supported in communication server of the Aastra 400 series. It deals with connecting SIP terminals to communication servers, connecting communication servers to an SIP provider, and coupling communication servers systems to one another via the SIP protocol. The expansion stages, system capacity, installation, configuration, operation and maintenance, technical data, DECT planning, and the possibilities for networking several systems into a private ISDN network (PISN) or an Aastra Intelligent Net (AIN) are not part of this Manual. They are described in separate documents.

The System Manual is available only in electronic form as a document in Acrobat Reader format, and can be printed out. Navigation in PDF format is based on the bookmarks, table of contents, cross references and index. All these navigation aids are linked, i.e. a mouse click takes you directly to the corresponding section of the document. We have also ensured that the page numbering in the PDF navigation corresponds to the page numbering of the document, making it much easier to jump to a particular page.

Referenced menu entries and parameters appearing on terminal displays or in AMS (Aastra Management Suite) are *highlighted* in italics and in colour for a clearer orientation.

Document information

- Document number: syd-0407
- Document version: 1.0
- Valid as of: R1.0
-
- In PDF Viewer, click on this link to download the latest version of this document: *https://pbxweb.aastra.com/doc_finder/DocFinder/syd-0407_en.pdf?get&DNR=syd-0407*

General Considerations

Special symbols for additional information and document references.

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

Tip
Additional information on the handling or alternative operation of equipment.

See also
Reference to other documents

Aastra Intelligent Net:
Particularities that have to be observed in an AIN.

Safety Considerations

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.

Caution
Failure to observe information identified in this way can cause a defect in the product or one of its modules.

Warning
Failure to observe information identified in this way can lead to damage caused by electrostatic discharge.

2 Introduction

This chapter provides a short introduction to the subject of SIP and explains the different principles involved when a connection is set up between two SIP subscribers. It also discusses the three application instances of SIP in Aastra 400 and refers to the corresponding chapters. The chapter ends with a table summarising the SIP-relevant protocols and methods currently supported by Aastra 400.

2. 1 What is SIP?

The Session Initiation Protocol (SIP) is a network protocol used for setting up, controlling and clearing down a communication session between two or more subscribers (source: Wikipedia). SIP is an open standard and was developed by an IETF (Internet Engineering Task Force) working group. While the text-based protocol has a great deal in common with HTTP (Hypertext Transfer Protocol) in terms of both structure and sequence, it is not compatible with it.

SIP is now widely used in IP telephony. However SIP alone cannot enable VoIP connections. With the aid of the Session Description Protocol (SDP), SIP merely negotiates the communication modalities between the SIP subscribers. The actual audio data stream is exchanged via other, more suitable protocols, such as the Real-Time Transport Protocol (RTP) or the encrypted Secure Real-Time Transport Protocol (SRTP). For this, the coded and compressed data is packed into packets and sent via the User Datagram Protocol (UDP) or the Transmission Control Protocol (TCP).

The SIP connection is used to transmit not just voice but other multimedia data, too (video, fax, text, etc.).

SIP subscribers have an address whose structure is similar to that of an e-mail address (e.g. URL: "sip:12345@sip-server.com"). SIP subscribers can be reached via this address, regardless of their location. However, this is only possible if they register with an SIP provider and regularly update their IP address.

Gateways at the SIP providers enable the transition into the public telephone network, for example the leased-line network or the mobile phone network.

2. 1. 1 System components

SIP is based on a client-server architecture. Components may include a User Agent, Registrar Server, Proxy Server and Redirect Server. The three servers are located at the SIP provider and may be installed on the same system.

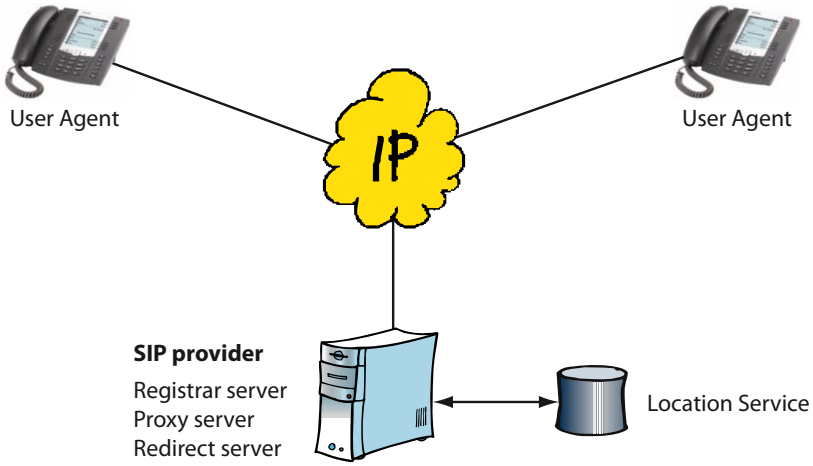

Fig. 1 SIP components

- User Agent
  User Agents are applications at SIP endpoints, i.e. software or hardware-based components. The caller is referred to as the User Agent Client; the called party, as the User Agent Server.
- Registrar Server
  An SIP subscriber regularly sends his registration data and his IP address to the Registrar Server. This information is stored in a database (Location Service).
- Proxy Server
  The Proxy Server is responsible for contacts between the subscribers. Following a request from a User Agent Client, the Proxy Server contacts the Registrar Server to determine the current IP address of the User Agent Server. It then tries to make contact with the User Agent Server.
- Redirect Server
  The Redirect Server works in a way similar to the Proxy Server. However it hands over the IP address of the User Agent Server directly to the User Agent Client, who then takes charge of the connection setup.

2. 1. 2 Types of connection setup

Requests and responses are defined in SIP in order to set up a connection between two subscribers. The User Agent Client generates a request, to which the User Agent Server responds with a response.

There are essentially three methods for setting up an SIP connection. The descriptions below are greatly simplified and explain only the principle and the different methods.

Method 1: Direct connection setup between the User Agents

The User Agent Client sends the "INVITE" request for a connection setup to the User Agent Server. If the User Agent Server takes the call, he sends back the response "OK" together with the connection parameters. The User Agent Client confirms this with an "ACKNOWLEDGE" and the call connection is set up.

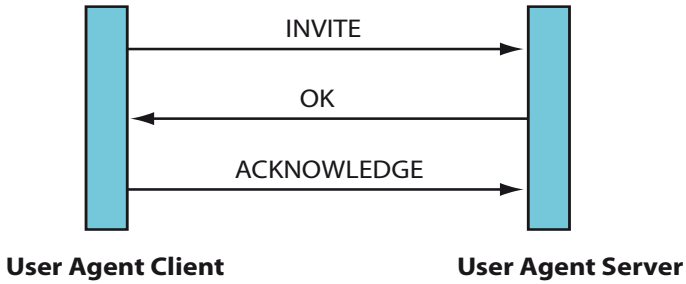

Fig. 2 Direct connection setup

As the IP address changes depending on the User Agent's location, this method does not guarantee that the connection is set up.

Method 2: Connection setup using a Proxy Server

The User Agent Client sends the "INVITE" request for a connection setup with the User Agent Server to the Proxy Server. The Proxy Server retrieves the current IP address of the User Agent Server from the database of the location service and forwards the connection request to the User Agent Server. If the User Agent Server takes the call, it sends the response "OK" back to the Proxy Server, which in turn forwards it to the User Agent Client. The response contains all the connection parameters. From this point onwards the two User Agents communicate directly with each other. The User Agent Client confirms the connection parameters with an "ACKNOWLEDGE" and the call connection is set up.

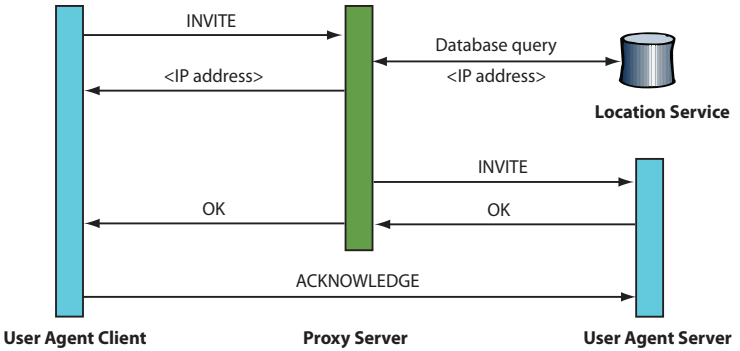

Fig. 3 Connection setup using a Proxy Server

This type of connection requires that the User Agents register with the Registrar Server and regularly update their data.

Method 3: Connection setup using a Redirect Server

The User Agent Client sends the "INVITE" request for a connection setup to the Redirect Server. The Proxy Server retrieves the current IP address of the User Agent Server from the database of the location service and sends it back to the User Agent Client, who confirms the action with an "ACKNOWLEDGE". The User Agent Client now sets up a direct connection with the User Agent Server, as described in "Method 1: Direct connection setup between the User Agents", page 10.

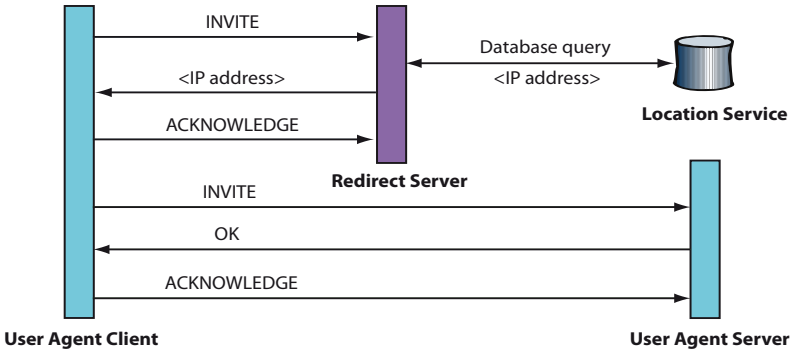

Fig. 4 Connection setup using a Redirect Server

This type of connection also requires that the User Agents register with the Registrar Server and regularly update their data.

2. 2 Security aspects with VoIP

Security is an important aspect of VoIP telephony. The table below shows the three security objectives of data protection, authentication and integrity as well as ways of achieving those objectives:

Tab. 1 Security objectives

Security objective	Meaning	Remedy
Data Protection	Third parties must not be able to read the exchanged data	Data encryption
Authentication	Verifying the identity of the remote station	Using shared passwords and certificates
Integrity	Third parties must not be able to modify the transmitted data	Using checksums

With these considerations it is important to note that the voice data and the signalling data do not always run in parallel and may well take separate paths, as the following example shows:

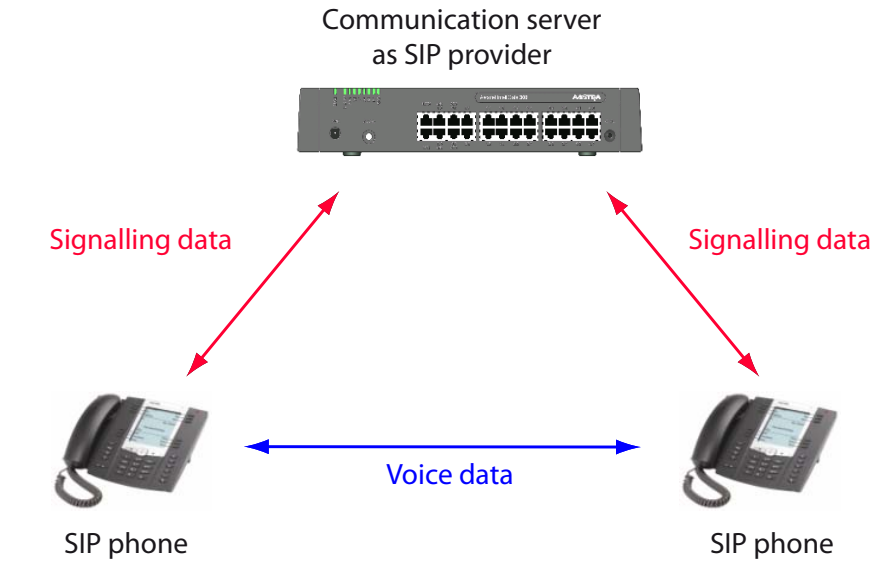

Fig. 5 SIP data streams

Situation without encryption (SIP/RTP)

If the signalling data and voice data are considered separately, the situation is as follows if encryption is not used:

Tab. 2 Situation without encryption

Security objective	Signalling data	Voice data
Data Protection	Not guaranteed.	Not guaranteed
Authentication	Partially guaranteed through password protection	Not guaranteed
Integrity	Not guaranteed	Not guaranteed

Solutions

Encryption of the SIP and RTP data at IP level using IPSec (Internet Protocol Security) and VPN (Virtual Private Network). The signalling data and the voice data are protected if all the SIP components involved are within the VPN.

Encryption of the SIP signalling data at the transport level using TLS (Transport Layer Security) and of the voice data at application level using SRTP (Secure Real-Time Transport Protocol). TLS works by exchanging certificates and requires the TCP transport protocol.

For WAN links via the internet it makes sense to combine both methods.

See also
For more details on this subject please refer to the “Aastra Intelligent Net (AIN) and IP Terminals” System Manual.

2. 3 SIP in Aastra 400

If SIP is supported in Aastra 400, Method 2: Connection setup using a Proxy Server is used exclusively.

A distinction is made between the following three application cases:

- Connection of SIP terminals as internal subscribers to Aastra 400:

  In this case Aastra 400 assumes the role of an SIP provider for the SIP terminal and provides the Registrar and the Proxy Servers internally. The terminal can be connected either internally on the same IP network as the Aastra 400 communication server or externally via a VPN connection or using SRTP and TLS. This particular application is described in "Chapter 3 SIP terminals".

- Connection of Aastra 400 to one or more SIP providers:

  Here the Aastra 400 communication server itself is the User Agent. Access to an SIP Provider is provided via an SIP network interface (SIP access). One SIP access supports up to 30 SIP channels, i.e. up to 30 connections to one SIP provider are possible simultaneously. Access to the public telephone network is via a gateway at the SIP provider. The connection to an SIP provider is described in "Chapter 4 SIP access".

- Networking Aastra 400 communication servers via SIP:

  It is possible to network two or more Aastra 400 communication servers via SIP. The principle is comparable to QSIG networking on an ISDN basis. In the same way as with QSIG networking, star-shaped centralised networking configurations as well as meshed networking configurations are possible. More details can be found in "Chapter 5 SIP Networking".

Data encryption is designed to ensure that security is taken into account in all three application cases, especially when the VoIP data leaves the LAN. They can be external home workstations, a connection of the communication server to the public network via an SIP provider or the SIP networking of several systems at different locations.

SIP support in Aastra 400 is continually being expanded and therefore depends on the software version of the communication server. A general overview of the protocols and methods currently supported can be found in Tab. 3, page 16.

See also

You can find more useful information on SIP in Aastra 400 such as FAQs, compatibility lists, restrictions and support tips in the Knowledge Base on the Extranet site: https://pbxweb.aastra.com.

2. 4 SIP RFCs supported by Aastra 400

RFCs (Request for Comments) are numbered, freely accessible technical and organisational documents on the internet. They are drawn up by the IETF (Internet Engineering Task Force) and go through various stages until in the ideal scenario they establish themselves as a standard. There is a whole series of RFCs dealing directly or indirectly with SIP.

The RFCs are published on the following web site. Specific RFCs can be displayed directly using a search engine; you can also search for RFCs using keywords: http://www.rfc-editor.org

The following RFCs are supported for connecting Aastra 400 to SIP service providers on the one hand and SIP terminals to Aastra 400 on the other.

Tab. 3 SIP RFCs supported by Aastra 400

RFC	Title	Status	Supported as of	Remarks
2617	HTTP Authentication: Basic and Digest Access Authentication, June 1999	Draft Standard	R1.0	
3261	SIP: Session Initiation Protocol, June 2002	Proposed Standard	R1.0	
3263	Session Initiation Protocol (SIP): Locating SIP Servers, June 2002	Proposed Standard	R1.0	
3264	An Offer/Answer Model with the Session Description Protocol, (SDP), June 2002	Proposed Standard	R1.0	
3265	Session Initiation Protocol (SIP)-Specific Event Notification, June 2002	Proposed Standard	R1.0	
3311	The Session Initiation Protocol (SIP) UPDATE Method, October 2002	Proposed Standard	R1.0	
3323	A Privacy Mechanism for the Session Initiation Protocol (SIP), November 2002	Proposed Standard	R1.0	
3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks, November 2002	Informa-tional	R1.0	
3326	The Reason Header Field for the Session Initiation Protocol (SIP), December 2002	Proposed Standard	R1.0	
3398	The Reason Header Field for the Session Initiation Protocol (SIP), December 2002	Proposed Standard	R1.0	
3515	The Session Initiation Protocol (SIP) Refer Method, April 2003	Proposed Standard	R1.0	
3550	RTP: A Transport Protocol for Real-Time Applications, July 2003	Standard	R1.0	
3551	RTP Profile for Audio and Video Conferences with Minimal Con-trol, July 2003	Standard	R1.0	
3578	Mapping of Integrated Services Digital Network (ISDN) User Part (ISUP) Overlap Signalling to the Session Initiation Protocol (SIP), August 2003	Proposed Standard	R1.0	"Overlap dialing features" only

RFC	Title	Status	Supported as of	Remarks
3581	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing, August 2003	Proposed Standard	R1.0	
3711	The Secure Real-time Transport Protocol (SRTP), March 2004	Proposed Standard	R1.0	
3842	A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP), August 2004	Proposed Standard	R1.0	SIP terminals only
3891	The Session Initiation Protocol (SIP) Replaces Header, September 2004	Proposed Standard	R1.0	
4028	Session Timers in the Session Initiation Protocol (SIP), April 2005	Proposed Standard	R1.0	
4235	An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP), November 2005	Proposed Standard	R1.0	SIP terminals only
4488	Suppression of Session Initiation Protocol (SIP) REFER Method Implicit Subscription, May 2006	Proposed Standard	R1.0	SIP access only
4566	SDP: Session Description Protocol, July 2006	Proposed Standard	R1.0	
4612	Real-Time Facsimile (T.38) - audio/t38 MIME Sub-type Registration, August 2006	Historic	R1.0	
4662	A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists, August 2006	Proposed Standard	R1.0	SIP terminals only
4733	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, December 2006	Proposed Standard	R1.0	
4855	Media Type Registration of RTP Payload Formats, February 2007	Proposed Standard	R1.0	
5246	The Transport Layer Security (TLS) Protocol Version 1.2, August 2008	Proposed Standard	R1.0	
5806	Diversion Indication in SIP	Historic	R1.0	

3 SIP terminals

This chapter looks at the differences between the SIP terminals of Aastra and those of other manufacturers and explains step by step the different types of registration. The SIP terminals of the Aastra 6700i series are discussed separately. The overview table at the end of the chapter shows how Aastra 400 features can be activated on the SIP terminals.

3. 1 Types of terminal

SIP terminals are VoIP-based terminals which use the SIP protocol for the connection setup, control and connection clear-down. SIP terminals on Aastra 400 fall into two categories of terminals:

- SIP terminals of the Aastra 6700i series (see page 19 ff.)
  This group includes the SIP terminals Aastra 6730i, Aastra 6731i, Aastra 6739i, Aastra 6753i, Aastra 6755i and Aastra 6757i. These terminals have close ties with Aastra 400 and can be configured via AMS. Compared with other SIP terminals a number of Aastra 400 features can be activated in a convenient way using menu prompting. Convenient and automated configuration of these terminals is also possible using a configuration server integrated in Aastra 400.
- Other Aastra SIP terminals and by other manufacturers (see page 45 ff.)
  These include SIP terminals that have a less strong connection to Aastra 400. They include:
  - Aastra SIP-DECT terminals:
    They include cordless phones of the Aastra 600d series that are connected to Aastra 400 via radio units of the type RFP L32 IP, RFP L34 IP or RFP L42 WLAN. In a way similar to Aastra 6700i terminals, the configuration of these phones can be automated in part.
  - SIP softphones, as an application on a PC.
  - Line-based SIP desk phones
  - WLAN and DECT terminals connected with the IP network via an access point.

An SIP licence is required for each SIP terminal operated on Aastra 400.
The *Aastra SIP Terminals* licence is valid for terminals of the Aastra 6700i series as well as a number of other Aastra SIP terminals.

The *Standard SIP Terminals* licence is valid for all the other SIP terminals made by Aastra and other manufacturers. This licence is expensive.

Tab. 11, page 46 lists all SIP terminals by Aastra and other manufacturers with the licences required in each case.

Note
A free *Standard SIP Terminals* licence can replace a *Aastra SIP Terminals* licence. This does not work the other way round.

3. 2 SIP terminals of the Aastra 6700i series

The SIP terminals of the Aastra 6700i product family differ mainly in the size of the display and the menu guidance, in the number of configurable keys and the possibility of connecting expansion key modules. They are all XML brower-compatible, have an integrated switch for connecting a PC, and can be operated via PoE (Power over Ethernet).

Fig. 6 Aastra SIP terminals of the series Aastra 6700i

3. 2. 1 Integration in Aastra 400

With the Aastra 6700i series now integrated in Aastra 400 the terminals are particularly easy to register, configure and operate. The depth of integration of terminals depends on the version of the communication server software.

Terminal integration offers the following characteristics and advantages:

- Synchronisation of lists and status displays:
  Where there are several terminals per user, all the lists (such as calls lists, phone books, etc.) and the status of forwarded calls are synchronised and displayed. This is particularly useful when switching from one terminal to another.
- Configuration of terminal data via AMS:
  Some terminal parameters and the freely configurable keys on terminals and expansion key modules can be configured via AMS. This makes it easier for the system administrator to pre-configure the terminals (see "Configuration of terminal data via AMS", page 22).
- Status display of other users visible on the terminal:
  With the configuration of busy indicator keys the status of other users (idle state, ringing, talking) is now visible at a glance. The key is also used for fetching a call or dialling a user directly (see "Freely configurable keys", page 24).
- Menu-prompted navigation for lists and frequently used features:
  Menus are available for lists and frequently used features allowing easy operation without the need to enter */#-procedures. Access is obtained directly using softkeys or a system menu (see "System menu", page 27).
- Voice mail that is easy to use and operate
  New received voice messages are displayed and can be listened to directly from the call list by pressing a single key or by calling the number of the voice mail system. Softkeys can be used to navigate while the voice messages are played back (see "System menu", page 27).
- Separate configuration server on Aastra 400:
  Automated configuration of the terminals is therefore possible. The configuration data is saved in separate text files and stored on the configuration server. This means the configuration data is not lost even if the terminal is reset to the factory setting (see "Configuration using configuration files", page 31).
- Multicast DNS Responder in Aastra 400:
  With Multicast DNS now supported, the terminals are able to obtain the IP address of the configuration server themselves during startup. This option means terminals can register automatically with Aastra 400 even without a DHCP server. (see "Existing infrastructure", page 37.)

- Automatic update of the terminal software:
  At each restart the terminals check whether new terminal software is available on the configuration server. If so, they automatically load it into the internal memory. The terminal software is part of the software package for the communication server. This ensures that the system software and the terminal software are compatible at all times (see "Software Update", page 41).
- Country-related language packages
  Besides English the terminals also support four other languages simultaneously. They are defined in different language packages, which are loaded automatically during terminal startup, according to the country set in AMS. Alternatively the system administrator also has the possibility of defining a different language as the default language for all the terminals or for individual terminals (see "Language concept", page 43).
- Supports the CTI basic functions Seize, Dial and Go On-hook.

3. 2. 2 Configuration of terminal data via AMS

Compared with other SIP terminals Aastra SIP terminals allow additional terminal data to be configured using AMS (CM_4.2, Tab *Aastra SIP terminal data*). The data is not written directly into the terminal; instead it is stored in files and then loaded into the terminal. Here is an overview of the additional configuration possibilities:

Aastra SIP terminal data

Tab. 4 Terminal data: *AastraSIP terminal data* tab

Parameter	Setting	Note
Idle text	<String>	This character sequence appears on the display in the idle state (default value = call number).
Idle text 2	<String>	Other character sequence which can be defined for display in the idle state (no default value)
Language	<Language from the list>	The language must be available on the configuration server; it takes effect only once the terminal has been restarted (see "Language concept", page 43).
Expansion key module position x	<Aastra M670i/ Aastra M675i>	Possibility of configuring up to 3 expansion key modules (depending on the terminal)

Aastra SIP settings

Tab. 5 Terminal data: *Aastra SIP settings*.

Parameter	Setting	Explanation
Broadband range	Select from list	Bandwidth area within which the SIP terminal is to be used.
Application software version	not editable	If the terminal is registered, the software version loaded on the terminal is displayed here.
Status	not editable	The terminal's registration status is displayed here.
MAC address	<XX.XX.XX.XX.XX.XX>	The MAC address is a unique terminal identification and is used to assign the terminal to a stored configuration profile (see "Registering a terminal of the series Aastra 6700i", page 38).
IP address	not editable	If the terminal is registered, the terminal's IP address is displayed here.
RTP port	<1024...65534>	The port for the voice data is defined here (default value: 3000)
SIP port	not editable	If the terminal is registered, the port for the signalling data is displayed here.
Activate 'Keep alive'	<*Yes* / *No*>	If this setting is on *Yes* the communication server periodically sends messages (OPTIONS) to the SIP terminal in order to maintain the NAT connection. This is necessary for example if the SIP terminal is connected to the communication server downstream from an NAT server or via the public IP network.

Parameter	Setting	Explanation
SIP user name	String	Random character sequence generated by AMS. It can be edited, but must be unique.
SIP password	String	Random character sequence generated by AMS. It can be edited, but must be unique.
Registration code	<String>	Assigns a terminal to a configuration profile by entering a registration code directly on the terminal if the MAC address is not known (see "Registering a terminal of the series Aastra 6700i", page 38)
Send redirection information	Select from list	Redirecting information allows the called party to see whether the call was redirected and, if so, by whom. The caller also sees whether his call was redirected and if so, to whom. This setting applies only to this terminal and not to the terminal at the call destination or at the location at which the call originated. *No*: No redirection information is displayed. *Yes, using 'Diversion header (recursing)'*: The call is forwarded directly in the communication server. With this setting redirection information is displayed only in the case of incoming calls. *Yes, using 'Diversion header (non recursing)'*: With outgoing calls the forwarding of the call is indirect, with the communication server sending Response 302 (Moved Temporarily) back to the terminal along with the necessary redirection information. The terminal itself then puts the call through to the forwarding destination and uses the redirection information for display purposes on its own display. This means that with this setting redirection information can be displayed for both incoming and outgoing calls. **Note:** Forwarding with Response 302 is not possible in all cases.
Transport protocol	<*UDP or TCP* / *TCP* / *UDP* / *Persistent TLS*>	The transport protocol is selected here. For a secure connection between the terminal and the communication server the parameter must be configured to *Persistent TLS* (see "Securing the connection with SRTP/TLS", page 23).
Restart terminal	Button	The changes made to some parameters only take effect once the terminal has been restarted. This means a terminal restart is always required e. g. to load a new language or a new terminal software.

Securing the connection with SRTP/TLS

For a secure connection both the voice data and the signalling data must be secured (see "Security aspects with VoIP", page 12).

Securing the signalling data:

- To secure the signalling data the communication server operates with certificates. It generates a trusted certificate and automatically uploads it to the Aastra SIP terminals, which then restart. A call connection between communication server and terminal is established only if the two certificates match.
- Certificates remain valid for long periods; however for security reasons they should be replaced at regular intervals. New certificates must also be generated manually whenever the IP address of the communication system changes.
- For standard SIP terminals the trusted certificate must be exported as a file and uploaded to the terminal. The trusted certificate can be generated and exported using the VoIP settings under CM_2.2.5_*TLS*. The period of validity and the time at which the certificate is generated after it has expired are also specified here.

Securing the voice data:

The SRTP protocol is used to secure the voice data. Please note the following points:

- Under CM_2.2.5_*Encryption* the *VoIP data encryption* setting valid throughout the system must be configured to *Yes*.
- In the DSP settings the *VoIP mode* parameter must be configured to *secure G.711* or *secure G.711/G.729*.
- Under CM_2.3.3 the *NTP service* parameter must be configured to *Yes*.
- A *Secure VoIP* licence is required.

Freely configurable keys

As with digital system terminals the freely configurable keys of the Aastra 6700i series of terminals and the connectable expansion key modules can also be configured via AMS. The Aastra 6751i terminal does not have any freely configurable keys. Once they have been stored, the modified key assignments are immediately available on the terminal.

There are three different storage types for freely configurable keys:

- *Number*
  Number keys are used to store internal or external call numbers together with the corresponding names for frequently dialled call parties.
- *Busy lamp field*
  This storage type is used to display the status of other internal users and is based

on RFC4235 and RFC4662: (see Tab. 3, page 16.) The LED next to the key indicates the status of another user:

- LED off:
  idle state. The user is available. Clicking the busy indicator key dials the user directly.
- LED flashing:
  the user is being called. Clicking the busy indicator key can be used to retrieve the call and route the call to your own terminal.
- LED lit:
  the user is busy, i. e. he is making a call to someone or is already in a call.

- *Function*
  This allows you to choose from a list of different functions:
  - *System menu*:
    Access to the system menu (see "System menu", page 27).
  - *Call lists*, *System phonebook*, *Voice mail* and *Call forwarding*:
    Direct access to the menu entries in the system menu (see "System menu", page 27).
  - *Missed calls*, *Answered calls*, *Redial list*:
    Direct access to the menu entry *Call lists* in the system menu (see "System menu", page 27).
  - *Presence menu*
    Access to the presence menu (see "Presence menu", page 29).
  - *Local phonebook*:
    Access to the local phone book. The phone book is stored on the terminal itself and cannot be configured via AMS.
  - *Do not disturb (local)*:
    The terminal does not ring and is busy as far as incoming calls are concerned. Outgoing calls are possible.
    Note: This is a local function of the terminal and must not be confused with the system feature of the same name *26.
  - *Do not disturb (*26)*:
    The terminal does not ring. Incoming calls are diverted to an alternative destination. The destination is specified in the system configuration and is the same for all users. Outgoing calls are possible.
  - *Phone lock*:
    The terminal is locked. Outgoing calls are not possible; incoming calls can be answered.
    Note: This is a local feature of the terminal and should not be confused with the system feature of the same name, which can be activated using *33.

- *Take (pick up own active call)*:
  This function picks up an active call connection from one terminal to another terminal belonging to the same user.
- *Call pick up*:
  This function picks up an incoming call to a different user, to a user group or to a call distribution element.
- *Log-in/out*:
  If the terminal is in a free seating pool, it is possible to log in and then log out again using this key and entering the user number and PIN.
- *Deflect*:
  This feature is used for deflecting (transferring) calls, with or without inquiry call.
- *Conference*:
  This feature is used to set up a conference call.
- *Empty*:
  Key not assigned. The following softkeys do not move up.

Notes

- The choice of features that can be configured depends on the terminal type.
- Once a terminal has registered with Aastra 400 a number of keys are preconfigured, depending on the terminal type (e. g. access to the system phone book, the call lists, the voice mail system, etc.)
- Freely configurable keys can be configured not only via AMS but also via the terminal interface or the web user interface. However only those functions that can also be selected via AMS are usable. It is also important to take note of which configuration takes priority (see "Priority of the configuration methods", page 36).

3. 2. 3 System menu

The system menu is accessed using the *Menu* softkey. The menu entries and the features available in the submenus are explained in the table below:

Tab. 6 Menu entries in the system menu

Call lists — *Unanswered calls* — *Answered calls* — *Redial list*	Access to the lists of unanswered calls, answered calls and outgoing calls Softkeys in the lists for the following features: • Vertical scrolling (with cursor keys) • Deleting a single entry • Deleting all entries • Dialling the number of an entry • Accessing the detailed view of an entry • Listening to a voice message (unanswered call list only) • Back to the higher-order menu **Note**: Deleting an entry in the list of unanswered calls also deletes any existing voice messages relating to that entry. Entries with voice messages that have not yet been played back cannot be deleted.
Directory search — *Quickdial* — *Name* — *Advanced search*	Searching for an entry in the user's phone book (private contacts), in the system's phone book or in attached external directories. Explanations relating to the input mask: • *Quickdial*: The search is carried out using a string of digits. A digit represents the letters printed on the key. Press the digit key only once for each letter. Use the #-key to separate the surname and first name. • *Name*: The search is carried out using a text string. For each letter press the digit key several times until the right letter appears. Use a space to separate the surname and first name. • *Advanced search*: Appears only if external directories are attached. The search is carried out using a text string. For each letter press the digit key several times until the right letter appears. Use a space to separate the surname and first name. **Note**: The search always involves the string on which the cursor is currently positioned. Softkeys in the input mask for the following features: • Positioning the cursor (using the cursor keys) • Deleting individual digits or letters • Deleting all the inputs • Switching from letters to digits in the case of text strings • Starting a search in the directory • Back to the higher-order menu Softkeys in the result mask for the following features: • Vertical scrolling (with cursor keys) • Dialling the number of an entry • Accessing the detailed view of an entry • Back to the higher-order menu

Voice mail	Selecting this entry triggers a call to the number of the voice mail system. If there are any voice messages, they are played back in chronological order, starting with the most recent voice message that has not yet been played back. Once the last voice message has been played back or if there are no voice messages at all, you obtain a special tone sequence and the connection to the voice mail system is disconnected. Softkeys during playback for the following features: • Cancel playback • Repeat voice message • Playback the next voice message (where available) • Delete the current voice message (only if it has already been played back) **Note**: With SIP terminals it is not possible to run the features using digit keys, as announced by the Audio Guide.
Forward — *Off* — *All* — *Busy* — *Call Forwarding on No Reply*	After you have accessed the call forwarding menu, the current status and the destination of the last completed call forwarding operation are displayed. Softkeys in the call forwarding menu for the following features: • Vertical scrolling (with cursor keys) • Execute the selected call forwarding operation • Modify the selected call forwarding operation (leads to a submenu) • Back to the higher-order menu In the submenu you have a choice of two destinations: • *User*: An input mask is displayed. Enter the number of the call forwarding destination and confirm with a softkey. → The call forwarding is carried out. • *Voice mail*: Confirm with a softkey. → The call forwarding is carried out.

3. 2. 4 Presence menu

The presence menu is accessed using the *Presence* softkey. The menu entries and the features available in the submenus are explained in the table below:

Tab. 7 Selection in the presence menu

Presence	Once the presence menu has been accessed, the active presence status is displayed by a radio button. There are five presence states: • *Available* (default setting) • *Absent* • *Meeting* • *Busy* • *Not available* A different presence status can be selected using the cursor keys and activated using the *Select* softkey. Note: The active presence status is indicated on the display when the phone is in its idle state (except for the *Available* status).
— *Change*	This softkey is used to jump to a submenu with the following 3 entries: • *Description*: An additional text can be typed in here to be displayed to the caller in addition to the presence status. Example: "Meeting until 4 pm." • *Personal call routing*: This specifies whether or not the presence profile is also to activate a personal call routing. The choice of options is as follows: *Retain setting*: No profile-specific actions are carried out. Any activated settings are retained. *None*: Personal call routing is deactivated. *<1...5>*: Activating a predefined call routing. • *Call forwarding*: This specifies whether or not the presence profile is also to activate a call forwarding. The choice of options is as follows: *Retain setting*: No profile-specific call forwarding actions are carried out. Any activated call forwarding actions are retained. *Do not redirect*: No call forwarding action is carried out. Any configured call forwarding action is deactivated. *User*: The user to which the call is to be forwarded is entered here. *Voice mail*: This activates call forwarding to voice mail.
— *Absent?*	This softkey is used to jump to a submenu in which the call number of a different user can be entered. After the selection has been confirmed by pressing the *Select* softkey the presence status of the user in question is displayed.
— *Detail*	This softkey is used to jump to a submenu in which the details of the selected presence status are displayed (*Description*, *Personal call routing* and *Call forwarding*).

3. 2. 5 Configuration methods

There are different methods for configuring a terminal of the Aastra 6700i series:

- With the aid of configuration files which are edited with AMS and downloaded onto the terminal. This is the most convenient and advantageous method and should therefore be the method of choice.
- Via the web user interface
- Via the terminal user interface

The principle and the particularities of the three possibilites are described in the following chapters.

3. 2. 5. 1 Configuration using configuration files

The communication servers of the Aastra 400 series comprise a configuration server. This allows an automated and therefore simplified configuration of Aastra 6700i terminals. With the help of the configuration files generated by the communication server the data is transferred to the terminals using TFTP. There are two types of configuration files on the configuration server:

- aastra.cfg
  This configuration file occurs only once on each communication server. It contains global parameters that are valid for all terminals. The file is created using the "aastra.txt" template. The significance of the parameters is documented in the file.
  The first part of the "aastra.txt" file contains global parameters which should only be modified in exceptional cases in order to meet customer-specific requirements.
  The second part of the "aastra.txt" file contains global parameters which must not be modified with a text editor. One part of the parameters is fixed and one part contains variables whose values are configured via AMS and then automatically written into the "aastra.cfg" file.
- <mac>.cfg
  This configuration file exists separately for each terminal of the Aastra 6700i series. The file name corresponds to the terminal's specific MAC address. The file is created using the "mac.txt" template when the MAC address is assigned to a terminal created in AMS. The address is assigned either manually in AMS or using the identification via a registration code when the terminal is started up for the first time (see "Registering a terminal of the series Aastra 6700i", page 38).
  The "mac.txt" template and therefore the "<mac>.cfg" file contain terminal-specific parameters which must not be modified with a text editor. The parameters contain variables whose values are configured via AMS and then automatically written into the file. The significance of the parameters is documented in the file.

The configuration files are stored in the "tftp" folder of the communication server's file system. The file system can be accessed with an FTP client (e. g. Filezilla) or with the Windows Explorer. The section below describes how the system is accessed using the Windows Explorer.

Accessing the communication server's file system

1. Start Windows Explorer.
2. In the address bar enter the communication server's IP address (ftp ://<IP address>).
   If the address bar is not visible, you can show it under "*View* - *Icon bars* - *Address bar*".
3. In the login window enter the communication server's user name and password.
   – You are now in the communication server's file system.
4. Open the folder "tftp".
   – You can now see the configuration templates "aastra.txt" and "mac.txt". If terminals have already been created and MAC addresses assigned, the "aastra.cfg" file will be visible as will a "<mac>.cfg" file for each terminal.

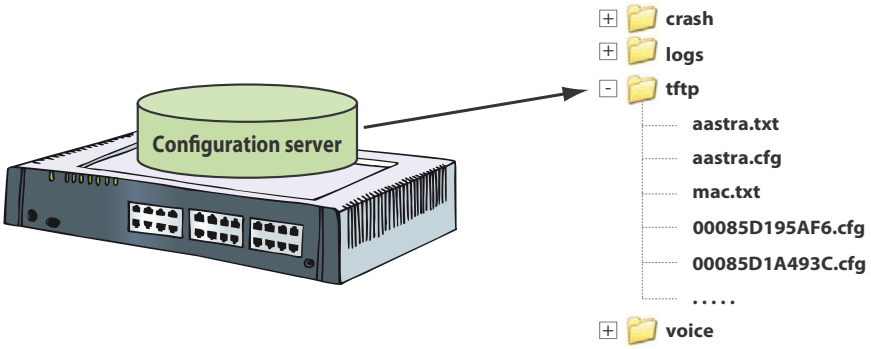

Fig. 7 Configuration server in Aastra 400

Notes

– Files cannot be edited directly in the tftp folder.
– Only the "aastra.txt" file can be edited. When the file is copied to the TFTP folder, "aastra.cfg" changes automatically.
– Updating the system software can also cause the template files "aastra.txt" and "mac.txt" to be modified. If this is the case, the files in the TFTP folder are automatically renamed "*.old". This allows you to transfer manually any changes you have made from the "*.old" to the "aastra.txt" file.

– The terminal may have to be restarted for the parameter changes in the terminal to become effective. This is indicated by a message when configuring with AMS.

See also
Detailed descriptions of all the possible parameters in the configuration files can be found in the Administrator User's Guide of the Aastra 6700i series of terminals (see http://www.aastra.com).

3. 2. 5. 2 Web user interface

The terminals of the Aastra 6700i series can also be configured via the web user interface using a web browser. This provides far more extensive configuration possibilities than is the case when using the terminal user interface. The web user interface can also be used to export directories and run a manual update of the terminal software.

Access to the web user interface

Requirement:
For web access, the terminal's IP address has to be known. If this is not the case, you can read out the IP address using the terminal user interface under *Terminal status*.

1. Start your web browser.
2. In the address field enter the terminal's IP address (http://<IP address>).
3. Enter the user name and password in the login window.
   (user name default value: "admin", password: "22222")

The terminal's status information is displayed and you can make the configurations you want.

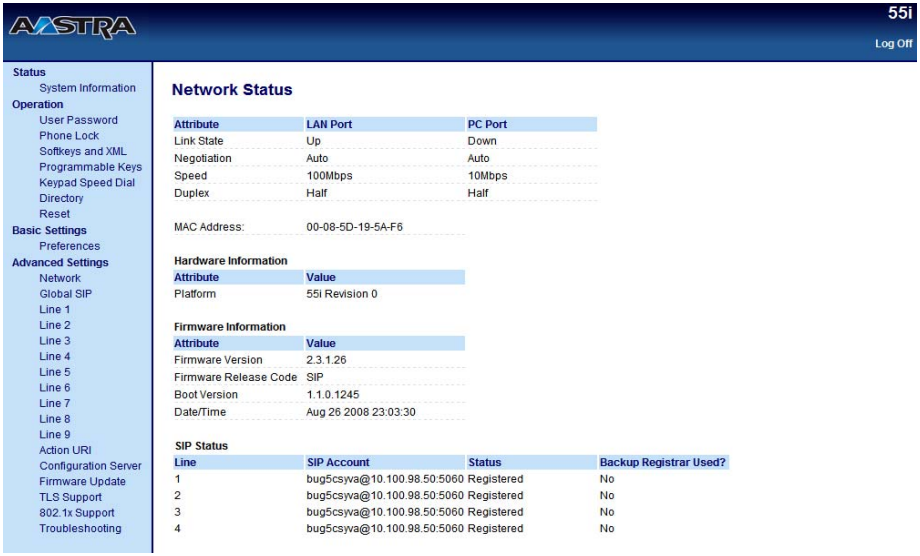

Fig. 8 Access view for the web user interface of an Aastra 6755i

Notes

- The changes made to some parameters only take effect once the terminal has been restarted. This is indicated by a message.
- Some parameters can only be accessed with the aid of configuration files.
- AMS (CM_2.5.6_*IP system terminals)* is used to change the administrator password for the system as a whole and to deactivate the web user interface throughout the system.

See also

Detailed descriptions of the individual menu items can be found in the User's Guide of the terminal in question or in the Administrator User's Guide for the Aastra 6700i series of terminals (see http://www.aastra.com).

3. 2. 5. 3 Terminal user interface

The terminal user interface is used to make personal and administrative configurations directly on the terminal. Only the access to the Administrator menu is described here.

Access to the Administrator menu

Requirement: The terminal is in the idle state.

1. Press the services key  or the options key  (depending on the terminal type)
2. From the *Options list* select the entry *Administrator Menu*.
3. Enter the Administrator password (default value: "22222").

You are now in the Administrator menu and ready to carry out the configurations you want.

Notes

- The terminal user interface covers only part of all the possible settings. For advanced settings use the web user interface or the configuration with the aid of configuration files.
- The scope of menu items can be restricted. If so, the Administrator menu is not visible. This global setting is made in the file "aastra.txt" (see "Configuration using configuration files", page 31).
- The administrator password can be changed for the system as a whole using AMS (CM_2.5.6_*IP system terminals)*.

See also

An overview and the exact procedure for the personal or administrative settings via the terminal user interface are described in detail in the User's Guide for the terminal in question and in the Administrator User's Guide for the Aastra 6700i series of terminals (see http://www.aastra.com).

3. 2. 5. 4 Priority of the configuration methods

Configuration using the terminal user interface and the web user interface is also referred to as local configuration as the data is stored locally in the terminal's internal flash memory. Both methods have equal priority, i. e. the parameter value is determined by whichever configuration was carried out last.

Configuration using configuration files is also referred to as a server configuration. While the data is also stored locally in the terminal's internal flash memory, it can be retrieved from the configuration server at any time.

A mix of the different configuration methods can be used. If so, it is important to bear in mind which method takes priority.

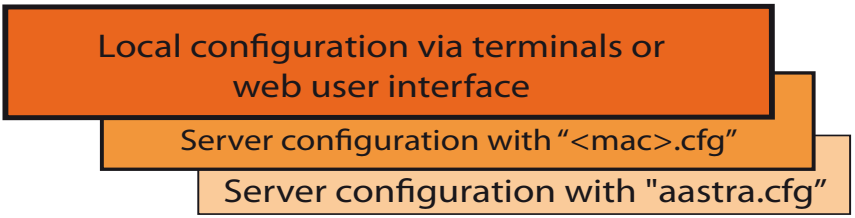

Fig. 9 Priority of the configuration methods

Rule 1:
The local configuration of a parameter always takes precedence over the configuration of the same parameter in a configuration file, regardless of the chronology of the configuration.

Rule 2:
If in a server configuration the same parameter is defined in both the "<mac>.cfg" file and the "aastra.cfg" file, the value of the parameter in the "<mac>.cfg" file takes precedence. If a parameter occurs several times in a file, the lowest entry is always the one that is effective.

Tips
- You can read out both the local configuration and the server configuration currently stored on the terminal in the form of files using the web user interface.
- To avoid confusion during the configuration, always use AMS to edit parameters that can be edited both via the server configuration (AMS) and local configuration.

3. 2. 6 Existing infrastructure

The terminals of the Aastra 6700i series are capable of registering with the system themselves during startup with the help of the configuration server. For this you need the IP address of the configuration server. There are different ways of obtaining the address, depending on the existing infrastructure.

- Dynamic allocation of the IP address using the integrated DHCP server or an external DHCP server.
- Automatic allocation of the IP address with Multicast DNS:
  The terminals support multicast DNS. Thanks to the multicast DNS responder integrated in Aastra 400 the terminals are also able to retrieve the address of the configuration server themselves. This requires that the terminals and the configuration server are in the same subnet and that the parameter CM_2.2.1_*IP*) the parameter *Multicast DNS Support* is configured to *Yes* under the IP settings in AMS.
- Manual allocation of the IP address:
  The IP address of the configuration server, the IP address of the terminal, and other parameters such as the subnet mask and gateway can also be configured manually in the terminals using the terminal or web user interfaces.

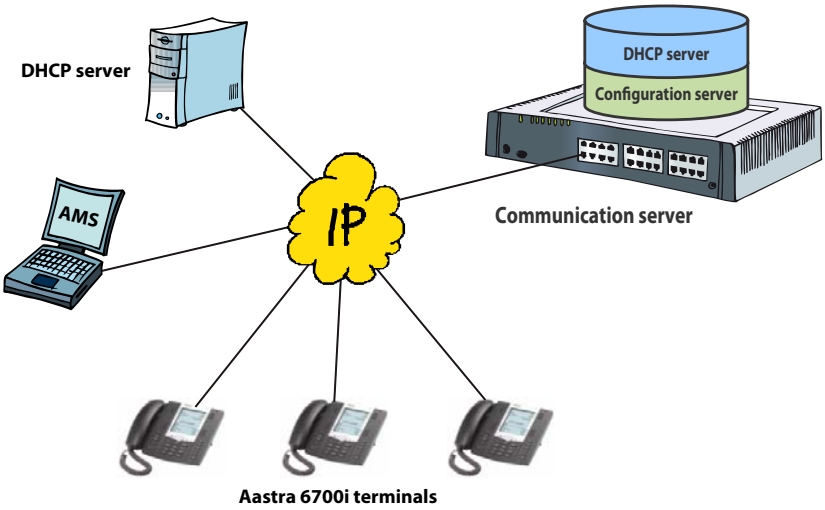

Fig. 10 Components involved in automated configuration

This broad support with different methods means that every network situation operated by the customer can be covered with an appropriate solution.

3. 2. 7 Registering a terminal of the series Aastra 6700i

A number of configurations are necessary in AMS so that a terminal of the Aastra 6700i series is able to register automatically with the system. The configuration steps and the registration process depend on whether or not the MAC address of the terminal is known. The MAC address is a unique terminal identification and is used by the system to assign the terminal to a stored configuration profile.

No manual input is necessary on the terminal during a registration process where the MAC address is entered. This allows remote configuration without the aid of an additional person standing by at the terminal.

If the MAC address is not known, the assignment of a terminal to the corresponding configuration profile in AMS first takes place by entering a registration code directly on the terminal. The terminal's MAC address is then automatically transferred to the configuration server and stored in the corresponding configuration profile.

These two methods are addressed separately in the following sections, with the necessary configurations and the registration process illustrated step by step.

Note
Prior to the registration, reset any terminals that were already in operation back to the factory setting. This avoids problems with the registration given that the local configuration overrides the configuration with the configuration files (see "Priority of the configuration methods", page 36).

Registering by entering the MAC address

Requirement:
A free *Aastra SIP Terminals* or *Standard SIP Terminals* licence is already in place.

1. Start AMS and set up a connection with the communication server.
2. In the Configuration Manager create a terminal of the type *Aastra SIP*.
3. Select the right model of the family Aastra 6700i (important!).
4. Enter the terminal's *MAC address*.
5. Assign an existing user or create a new user.
   – AMS generates random character sequences for the parameters *SIP user name* and *SIP password* and fills them in. These sequences of characters can be modified; however they need to be unique.
6. Configure the specific SIP settings as indicated in Tab. 5, page 22.
7. Save the configuration data in the communication server.
   – The "<mac>.cfg" file is generated from the "mac.txt" template and stored in the TFTP folder.
8. For static addressing only:
   Use the terminal or web user interface to configure the IP address of the configuration server (corresponds to the IP address of the communication server), the IP address of the terminal, the subnet mask, and the gateway address where applicable.
9. Connect the terminal to the IP network and restart it.
   – The terminal connects with the configuration server and downloads the files "aastra.cfg" and "<mac>.cfg" into its internal flash memory.
   – The terminal registers with the system using the registration information stored in "<mac>.cfg" such as the SIP user name and the SIP password. You can recognise this in AMS by the *Status* entry on the *Aastra SIP settings* tab under CM_4.2_*Terminal data*.

The basic configuration and the registration are now completed and you can start making and receiving phone calls with the terminal.

Registering without entering the MAC address

Requirement:
A free *Aastra SIP Terminals* or *Standard SIP Terminals* licence is already in place.

1. Start AMS and set up a connection with the communication server.
2. In the Configuration Manager create a terminal of the type *Aastra SIP*.

3. Select the model you want from the Aastra 6700i series.
4. Assign an existing user or create a new user.
   – AMS generates random character sequences for the parameters *SIP user name* and *SIP password* and fills them in. These sequences of characters can be modified; however they need to be unique.
   – AMS generates a *Registration code* and fills it in. Normally the code corresponds to the user's call number. The *registration code* can be modified; however it must be unique.
5. Configure the specific SIP settings as indicated in Tab. 5, page 22.
6. Save the configuration data in the communication server.
7. For static addressing only:
   Use the terminal or web user interface to configure the IP address of the configuration server (corresponds to the IP address of the communication server), the IP address of the terminal, the subnet mask, and the gateway address where applicable.
8. Connect the terminal to the IP network and restart it.
   – The terminal connects with the configuration server and downloads the file "aastra.cfg" into its internal flash memory.
   – The terminal display shows the prompt asking you to enter the registration code.
9. Enter the registration code.
   – The registration code is transmitted to the configuration server together with the terminal's MAC address. The "<mac>.cfg" file is then generated and stored in the TFTP folder.
   – The terminal is restarted automatically.
   – The terminal connects with the configuration server and downloads the file "<mac>.cfg" into its internal flash memory.
   – The terminal registers with the system using the registration information stored in "<mac>.cfg" such as the SIP user name and the SIP password. You can recognise this in AMS by the *Status* entry on the *Aastra SIP settings* tab under CM_4.2_*Terminal data*.

The basic configuration and the registration are now completed and you can start making and receiving phone calls with the terminal.

3. 2. 8 Software Update

The software for the Aastra 6700i terminals is part of the system software package and is stored in the TFTP folder in the communication server's file system. Besides the configuration files (see "Configuration using configuration files", page 31) and the language files (see "Language concept", page 43) the following software files are available there:

Tab. 8 Files in the TFTP folder

File name	Purpose
6730i.st	Aastra 6730i terminal software
6731i.st	Aastra 6731i terminal software
6739i.st	Aastra 6739i terminal software
53i.st	Aastra 6753i terminal software
55i.st	Aastra 6755i terminal software
57i.st	Aastra 6757i terminal software
omm_ffsip.tftp	Software for the OpenMobilityManager (DECT over SIP), which is used when using RFP L32 IP and RFP L34 IP base stations.
aafon6xxd.dnld	Software for the DECT handsets of the Aastra 600d series, if they are operated with the OpenMobilityManager (DECT over SIP).
lang_xx.txt	Language files for the display on the terminals of the Aastra 6700i series or on the corresponding web user interfaces.
contents.txt	File with information on the version, file name and size of the software and language files in the TFTP folder.

The terminal software for the Aastra 6700i series can be updated automatically for all the terminals together or manually for each terminal. Usually it is preferable to opt for automatic updating.

Automatic software updates for Aastra 6700i terminals

When the system software is updated, the software for the Aastra 6700i terminals is automatically copied to the TFTP folder in the communication server's file system. During the logon procedure it is compared with the software versions already uploaded on the Aastra 6700i terminals. If more recent versions are available, they are automatically uploaded to the Aastra 6700i terminals and activated.

If for whatever reason there are no software files for Aastra 6700i terminals available in the TFTP folder or if a different software is to be uploaded, proceed as follows:

1. Copy the required terminal software files (*.st) with an FTP client into the TFTP folder on the configuration server (see also "Accessing the communication server's file system", page 32).

2. Start AMS and set up a connection with the communication server.
3. From the Configuration Manager select from the *Online* menu the command *Restart all Aastra SIP terminals* or restart each terminal individually in CM_4.2__*Terminal data* using the button *Restart terminal*.

All the Aastra SIP terminals are restarted and automatically download the relevant software into their internal memory.

Note
For compatibility reasons we do not recommend uploading different software versions for the Aastra 6700i terminals than those contained in the system software package.

Manual software update of an Aastra 6700i terminal

1. Give the file a new name (<name>.st). The name must not be identical with the file names of the Aastra 6700i terminal in Tab. 8, page 41.
2. Copy the file with an FTP client to a TFTP server. You can use the configuration server in the communication server or a different TFTP server (see also "Accessing the communication server's file system", page 32).
3. Start the web user interface of the terminal and the *Software update* menu (see also "Access to the web user interface", page 33).
4. Specify the IP address of the configuration server and the file name of the terminal software.
5. Click the *Download software* button.

The terminal is restarted and automatically downloads the specific software into its internal memory.

Note
For compatibility reasons we do not recommend uploading different software versions for the Aastra 6700i terminals than those contained in the system software package.

3. 2. 9 Language concept

Different languages are available for the terminal and web user interfaces of the Aastra 6700i series of terminals. The languages are defined in text files, contained in the system software package and stored in the TFTP folder in the communication server's file system. Besides the configuration files (see "Configuration using configuration files", page 31) and the software files (see "Software Update", page 41) the following language files are available there:

Tab. 9 Languages supported for the terminals of the Aastra 6700i series

Languages[1)]	Abbreviation	File name
Basque	eu	lang_eu.txt
Danish	da	lang_da.txt
German	de	lang_de.txt
English	en	–
Estonian	et	lang_et.txt
Finnish	fi	lang_fi.txt
French	fr	lang_fr.txt
Galician	gl	lang_gl.txt
Greek	el	lang_el.txt
Dutch	nl	lang_nl.txt
Italian	it	lang_it.txt
Catalan	ca	lang_ca.txt
Norwegian	no	lang_no.txt
Polish	pl	lang_pl.txt
Portuguese	pt	lang_pt.txt
Portuguese-BR	pt-br	lang_pt_br.txt
Swedish	sv	lang_sv.txt
Spanish	es	lang_es.txt
Czech	cs	lang_cs.txt
Hungarian	hu	lang_hu.txt
Welsh	cy	lang_cy.txt

1) Other languages may be added

English is hard-coded into the terminal software. That is why there is no English text file.

Besides English the terminals also support four other languages simultaneously. The languages are defined in language packages for each country. The language package loaded depends on the value of the *Country* parameter, which can be

found on the *System* tab in the AMS Configuration Manager under CM_1.1_*System information*.

The table below shows which language packages are defined for each country, sorted alphabetically by country abbreviation.

Tab. 10 Language packages for terminals of the series Aastra 6700i

Country[1)]	Abbreviation	Language					
		0	1	2	3	4	Standard
Austria	AT	en	de	it	hu	cs	de
Australia	AU	en	fr	de	es	it	en
Belgium	BE	en	nl	fr	de	es	nl
Brazil	BR	en	pt-br	es	fr	pt	pt-br
Switzerland	CH	en	de	fr	it	es	de
Czech Republic	CS	en	cs	de	pl	fr	cs
Germany	DE	en	de	pl	fr	it	de
Denmark	DK	en	da	de	sv	no	da
Spain	ES	en	es	ca	gl	eu	es
Finland	FI	en	fi	sv	et	de	fi
France	FR	en	fr	de	es	it	fr
United Kingdom	GB	en	cy	fr	es	de	en
Greece	GR	en	en	es	it	fr	en
Italy	IT	en	it	fr	de	es	it
Netherlands	NL	en	nl	fr	de	es	nl
Norway	NO	en	no	sv	da	de	no
New Zealand	NZ	en	fr	de	es	it	en
Portugal	PT	en	pt	es	fr	de	pt
Sweden	SE	en	sv	no	da	fi	sv

1) Other countries may be added

The names of the four language files defined for each country are automatically written into the configuration file "aastra.cfg" when the first terminal is created. These languages are automatically loaded whenever the terminal starts up.

The relevant default language is activated the moment the terminal is started up for the first time.

Selecting the language

- Method 1
  One out of a total of five languages can be selected using the terminal interface or the web user interface. This method is intended for the user only. Method 2 is the preferred method for defining the language default setting during installation.
- Method 2
  The active language for each terminal can also be selected via AMS under CM_2.3. (parameter *Language)*. The advantage of this method is that you can choose from all the languages supported, not just from five of them. The selected language is written as language 4 into the file "<mac>.cfg". Providing the corresponding language file is stored in the TFTP folder on the configuration server, it is then loaded and activated whenever the terminal is restarted. The loaded language can then be selected via the terminal interface or the web user interface.

3. 3 Other Aastra SIP terminals and by other manufacturers

Besides terminals of the Aastra 6700i series other SIP terminals by Aastra and other manufacturers can be operated on Aastra 400. The design type ranges from softphones on the PC to line-based desk phones and WLAN and DECT terminals. Naturally the mode of operation and the features depend on the individual terminals (see also Tab. 14, page 50).

Special mention needs to be made of the Aastra SIP DECT terminals. These are cordless phones of the Aastra 600d series that are connected to Aastra 400 via radio units of the type RFP L32 IP, RFP L34 IP or RFP L42 WLAN. In a way similar to Aastra 6700i terminals the configuration of these phones can be partly automated using configuration files. The registration process for these terminals is not discussed further here. For the necessary information please refer to the documents in the “System Documentation Set SIP-DECT 2.1” (syd-0365).

3. 3. 1 Overview

The table below lists all the SIP terminals by Aastra and other manufacturers which can be operated on Aastra 400. Understandably, not all the SIP terminals by other manufacturers can be listed individually. In the table they are differentiated by design type only. The table also indicates the type which the terminals have in AMS and what kind of licence is required to operate them on Aastra 400.

Tab. 11 Overview of SIP terminals by Aastra and other manufacturers

Terminal	Terminal type in AMS	Licence	Description
Aastra 6751i	*SIP*	*Standard SIP Terminals*	Line-based desk phone
Aastra 9112i	*SIP*	*Standard SIP Terminals*	Line-based desk phone
Aastra 9133i	*SIP*	*Standard SIP Terminals*	Line-based desk phone
Aastra 9143i	*SIP*	*Standard SIP Terminals*	Line-based desk phone
Aastra 9480i	*SIP*	*Standard SIP Terminals*	Line-based desk phone
Aastra SIP-DECT	*Aastra SIP*	*Standard SIP Terminals* or *Aastra SIP Terminals*	DECT cordless phone connected via RFP L32 IP, RFP L34 IP or RFP L42 WLAN radio unit
Aastra SIP-TWP	*Aastra SIP*	*Standard SIP Terminals* or *Aastra SIP Terminals*	SIP user for the TWP application (Telephony Web Portal)
Aastra_WLAN	*Aastra SIP*	*Standard SIP Terminals* or *Aastra SIP Terminals*	WLAN terminal connected via a commercially available Access Point
Outside manufacturer	*SIP*	*Standard SIP Terminals*	Line-based desk phones
Outside manufacturer	*SIP*	*Standard SIP Terminals*	Softphones, as an application on a PC
Outside manufacturer	*SIP*	*Standard SIP Terminals*	SIP-based WLAN terminals
Outside manufacturer	*SIP*	*Standard SIP Terminals*	SIP-based DECT terminals

3. 3. 2 Registration process

The registration process for the SIP terminals listed in Tab. 11, page 46 depends on the terminal type in AMS and is therefore not identical for all terminals. For this reason the two types are dealt with separately in the sections below:

Registration of terminals of the type Aastra SIP

Requirement:
A free *Aastra SIP Terminals* or *Standard SIP Terminals* licence is already in place.

1. Start AMS and set up a connection with the communication server.
2. In the Configuration Manager create a terminal of the type *Aastra SIP*.
3. Select the SIP terminal you want.
4. Assign an existing user or create a new user.
   – AMS generates random character sequences for the parameters *SIP user name* and *SIP password* and fills them in. These sequences of characters can be modified; however they need to be unique.
5. Configure the specific SIP settings as indicated in Tab. 5, page 22.
6. Save the configuration data in the communication server.
7. Configure the address and registration in the SIP terminals in accordance with Tab. 12, page 49. Bear in mind that the designation of the parameters differs depending on the terminal.
8. Connect the terminal to the IP network and restart it.
   – The SIP terminal registers with the system. You can recognise this in AMS by the entries on the *SIP settings* tab under CM_4.2_*AastraTerminal data*.
   – *Status* indicates whether or not the SIP terminal is currently registered on the system.
   – *IP address* indicates the IP address of the SIP terminal.
   – *SIP port* indicates the ports over which the connections to the SIP terminal are set up.

Registration of terminals of the type SIP

Requirement:
A free *Standard SIP Terminals* licence is already in place.

1. Start AMS and set up a connection with the communication server.
2. In the Configuration Manager create a terminal of the type *SIP*.
3. Assign an existing user or create a new user.
   – AMS generates random character sequences for the parameters *SIP user name* and *SIP password* and fills them in. These sequences of characters can be modified; however they need to be unique.
4. Configure the specific SIP settings.
   – Parameters as per Tab. 5, page 22
   – *Fax machine*: If the SIP terminal is a fax machine or a combined device (fax/phone), select the type of device. The phone application always takes priority over the fax application.
5. Save the configuration data in the communication server.
6. Configure the address and registration in the SIP terminals in accordance with Tab. 12, page 49. Bear in mind that the designation of the parameters differs depending on the terminal.
7. Connect the terminal to the IP network and restart it.
   – The SIP terminal registers with the system. You can recognise this in AMS by the entries on the *SIP settings* tab under CM_4.2_*Terminal data*.
   – *IP address* indicates the IP address of the SIP terminal.
   – *Port* indicates the port over which the connections to the SIP terminal are set up.
   – The status of the parameter *Registered* indicates whether or not the SIP terminal is currently registered on the system.

Tab. 12 Parameter on the SIP terminals

Parameter	Setting	Explanation
Proxy settings:		
Proxy	<IP address> or <name>	Address of the communication server. For static addressing, enter the IP address; for addressing via DHCP/DNS, enter the host name.
Registrar	<IP address> or <name>	Address of the communication server. For static addressing, enter the IP address; for addressing via DHCP/DNS, enter the host name.
Outband Proxy	-	Leave entry blank.
Port (Proxy and Registrar)	5060	Default value of the communication server. All SIP terminals use the same port.
Caller Identification	sip:<call number>@<proxy address>	• Enter as the call number the internal call number of the user to whom the SIP terminal is assigned. • Enter as the proxy address the IP address or the host name of the proxy server.
Registration:		
Account/user/user name	<SIP user name>	Transfer from AMS the value of the parameter *SIP user name*.
Authentication/Authentication name/Authentication ID	<SIP user name>	Transfer from AMS the value of the parameter *SIP user name*.
Password	<SIP password>	Transfer from AMS the value of the parameter *SIP password*.
Transfer:		
Transport protocol	UDP or TCP	

3. 4 Features Overview

The features available on the SIP terminals depend on the following factors:

- The performance spectrum of the SIP terminals themselves
- The depth of integration of the SIP terminals in Aastra 400
- The SIP features (RFC) supported in the system software

This table provides an alphabetical overview not only of the Aastra 400 features that can be actuated on the SIP terminals but also of the features supported for SIP terminals.

*/# procedures can only be carried out in prefix dialling, i.e. if no call or ringing connection has already been set up.

Tab. 13 Legend used in the table of features

*/# procedure	Feature can only be actuated using a */# procedure.
✓	Feature is available on the terminals.
TM	Feature depends on the terminal.
M	On these terminals the feature can be operated via the menu.
–	Feature is not supported by these terminals.

Tab. 14 Features overview (in alphabetical order)

Features	Aastra 6700i series of SIP terminals	Other SIP terminals
Abbreviated dialling numbers, throughout the system	✓	✓
Accept a call or data connection with preparation		
• Prepare to accept a call from nn to mm	*87 nn*mm#	*87 nn*mm#
• Prepare to accept a data connection from nn to mm	*84 nn*mm#	*84 nn*mm#
• Clear preparation for accepting a call from user	#87 SC No.	#87 SC No.
• Clear preparation for accepting a data connection from user	#84 SC No.	#84 SC No.
• Activate prepared acceptance	*88# or *87*88	*88# or *87*88
Accept a call or ringing connection without preparation (Fast Take)	*88 SC No.	*88 SC No.
Access to system phone book (name / numbers)	M	–
Allocate cost centre before the call	see "Exchange Access"	
Announcement		
• Answer within the group	–	–

Features	Aastra 6700i series of SIP terminals	Other SIP terminals
• Answer outside the group	*89	*89
• Initiate on a user	*7998 SC No.	*7998 SC No.
• Initiate in suffix dialling	–	–
• Initiate to a group	*79 Gr. No.	*79 Gr. No.
Announcement service		
• Recording a welcome announcement with a phone	*911 xx [*nn] #	*911 xx [*nn] #
• Recording a welcome announcement with audio equipment	*921 xx [*nn] #	*921 xx [*nn] #
• Check recording	*#911 xx [*nn] # or *#921 xx [*nn] #	*#911 xx [*nn] # or *#921 xx [*nn] #
• Delete recording	#911 xx [*nn] # or #921 xx [*nn] #	#911 xx [*nn] # or #921 xx [*nn] #
• Activate welcome announcement	*931 yy [*nn] #	*931 yy [*nn] #
• Deactivate welcome announcement	#931 yy [*nn] #	#931 yy [*nn] #
xx = file number <10...29> yy = Welcome announcement <01...20> for Aastra 415/430 or <01...50> for Aastra 470 nn = node number (optional)		
Answer general bell		
• Coded ringing	see "Coded ringing on generalcall"	
• Ringing signal	*83	*83
Appointment call		
• Activate individual call order	*55 hh mm	*55 hh mm
• Activate permanent call order	*56 hh mm	*56 hh mm
• Clear	#55 or #56	#55 or #56
Automated configuration	✓	–
Automatic software update	✓	–
Brokering		
• in enquiry	✓	TM
• with line key	✓	TM
Busy lamp field	✓	–
Call charge display		
• for outgoing exchange calls	–	–
• for switched exchange calls	–	–
Call charges		
• Call charge transfer	✓	✓
• Transfer current call to another cost centre	–	–
• Individual charge counting (ICC)	✓	✓
• Charge recall	–	–

Features	Aastra 6700i series of SIP terminals	Other SIP terminals
Call deflection (CD)	see "Deflect call during the ringing phase (CD)"	
Call door intercom system	✓	✓
Call Forwarding if Busy (CFB)		
• Activate	M	*67 destination No.
• Activate to last configured Dest. No.	M	*67#
• Clear	M	#67
Call Forwarding on No Reply (CFNR)		
• Activate	M	*61 destination No.
• to last configured Dest. No.	M	*61#
• Clear	M	#61
• Activate to preconfigured Dest. No.	*62	*62
• Clear on preconfigured Dest. No.	#62	#62
• Activate on general bell with coded ringing	*68	*68
• Clear to general bell with coded ringing	#68	#68
• Protect against	*02	*02
• Allow to own set	#02	#02
Call Forwarding Unconditional (CFU)		
• Activate	M	*21 destination No.
• Activate to last configured Dest. No.	M	*21#
• Clear	M	#21
• Activate to preconfigured Dest. No.	*22	*22
• Clear on preconfigured Dest. No.	#22	#22
• Activate on general bell with coded ringing	*28	*28
• Clear to general bell with coded ringing	#28	#28
• Activate to standard text	*24 text No. param.#	*24 text No. param.#
• Clear to standard text	#24	#24
• Protect against	*02	*02
• Allow to own set	#02	#02
Call pick-up (x = SC No. / UG No. / CDE No.)	Busy indicator key or *86 x	*86 x
Call take back from connection	see "Accept a call or ringing connection without preparation (Fast Take)"	
Call transfer		
• after enquiry	✓	TM
• without enquiry	✓	TM
• Explicit call transfer (ECT)	–	–
Call waiting		
• Activate	–	–

Features	Aastra 6700i series of SIP terminals	Other SIP terminals
• Reject	–	–
• Answer with hold	–	–
• Answer without hold	–	–
• Answer, with conference	–	–
• Protect against	–	–
• Allow to own set	–	–
Callback on busy (CCBS) / available (CCNR) user		
• Activate	–	–
• Clear	–	–
Change PIN x = old PIN y = new PIN	*47 x * y * y #	*47 x * y * y #
Coded ringing on generalcall		
• Activate in prefix dialling	*81 SC No.	*81 SC No.
• Activate in suffix dialling	–	–
• Answer	*82	*82
Conference		
• Set up (from connection)	✓	TM
• Set up (variable)	*71 SC No.1 * up to SC No.5 #	*71 SC No.1 * up to SC No.5 #
• Exclude internal conference participants	–	–
• Set up (predetermined)	*70 conf. No.	*70 conf. No.
Control output		
• Activate	*74 <Call number[1)]>	*74 <Call number[1)]>
• Deactivate	#74 <Call number[1)]>	#74 <Call number[1)]>
Deflect call during the ringing phase (CD)	–	–
Delete configuration (activated, personal functions deactivated)	*00 or #00	*00 or #00
Dialling by name	M	–
Discreet ringing		
• Activate	–	–
• Deactivate	–	–
Display caller's number (CLIP / COLP)	✓	TM
Display caller's name (CNIP / CONP)	✓	TM
Do not disturb		
• Activate	*26	*26
• Clear	#26	#26
DTMF dialling	✓	✓

Features	Aastra 6700i series of SIP terminals	Other SIP terminals
Duplex mode	see "Announcement"	
Emergency / priority exchange seizure	✓	✓
Emergency number	✓	✓
Enquiry		
• To own system	✓	TM
• To up-circuit system	–	–
Exchange Access		
• Business (example CH)	0	0
• Least Cost Routing	✓	✓
• LCR (fallback)	*90	*90
• Private (example CH)	10	10
• With cost centre nn	13nn	13nn
• With charge recall	–	–
• Route selection, targeted (n depends on the system)	170 to n	170 to n
Fast Take	see "Accept a call or ringing connection without preparation (Fast Take)"	
Follow me		
• Activate	*23 SC No.	*23 SC No.
• Clear	#23	#23
Function keys configurable via AMS	✓	–
Generate an event message (triggering a user alarm) nnnn = 0000...9999	*77 nnnn	*77 nnnn
Hold connection (HOLD)	✓	TM
Home Alone (busy when busy)		
• Activate	*49 UG No.	*49 UG No.
• Clear	#49 UG No.	#49 UG No.
Intrusion		
• Activate	–	–
• Reject	–	–
• Answer with hold	–	–
• Answer without hold	–	–
• Answer with conference	–	–
• Protect against	–	–
• Allow to own set	–	–
Leave message		
• Standard	*24 text No. param.#	*24 text No. param.#

Features	Aastra 6700i series of SIP terminals	Other SIP terminals
• Own	–	–
• Clear / deactivate	#24	#24
List of callers	✓	TM
Making calls with your own settings on a third-party phone		
• Business calls	#36 SC No. PIN	#36 SC No. PIN
• Private calls	#46 SC No. PIN	#46 SC No. PIN
MESSAGE LED		
• Activate (prefix dialling)	*38 SC No.	*38 SC No.
• Activate (suffix dialling)	–	–
• Answer	–	–
• delete (on the destination phone)	–	–
• clear (on the executing phone)	#38 SC No.	#38 SC No.
Music on hold		
• Recording with the phone	*914 [*nn] #	*914 [*nn] #
• Record with audio device	*924 [*nn] #	*924 [*nn] #
• Check recording	*#914 [*nn] # or *#924 [*nn] #	*#914 [*nn] # or *#924 [*nn] #
• Delete recording	#914 [*nn] # or #924 [*nn] #	#914 [*nn] # or #924 [*nn] #
nn = node number (optional)		
Open door	*74<Door intercom system No.>	*74<Door intercom system No.>
Park		
• with line key	–	–
• with park key (local)	–	–
• Central parking	–	–
• Connect with centrally parked user	#76	#76
Personal call routing		
• Activate	*45 x	*45 x
• Deactivate	#45	#45
x = call routing [1...5]		
Phone lock		
• Lock terminal	*33 PIN #	*33 PIN #
• Lock all user's terminals	*33 * PIN #	*33 * PIN #
• Unlock terminal	#33 PIN #	#33 PIN #
• Unlock all user's terminals	#33 * PIN #	#33 * PIN #
• Unlock terminal for one call	#36 SC No. PIN	#36 SC No. PIN

Features	Aastra 6700i series of SIP terminals	Other SIP terminals
Presence		
• Activate presence status	M	*27 x
• Deactivate presence status	M	#27 or *27 0
x = profile number 0...4: 0 = Available (default), 1 = Absent, 2 = Meeting, 3 = Busy, 4 = Not available		
Private calls with PIN	#46 SC No. PIN	#46 SC No. PIN
Record malicious calls (MCID)	–	–
Reject call	✓	TM
Remote control features	*06 SC No. LM Proc.	*06 SC No. LM Proc.
Remote maintenance / configuration		
• Enable/bar a one-off remote maintenance	*754 / #754	*754 / #754
• Enable/bar a repeated remote maintenance access	*753 / #753	*753 / #753
Return to the call on hold	✓	TM
Ring Alone		
• Activate	*41	*41
• Deactivate	#41	#41
Ringing relay with delay (line keys and team keys)	–	–
Room monitoring (baby listening)		
• Activate x = mode [1â€¦3] y = level [1...3] (optional)	–	–
• Clear	–	–
Secret code (disable room-to-room barring)	*34	*34
Silent intrusion	–	–
Subaddressing (SUB)	–	–
Suppress the call number display (CLIR)		
• Activate permanently	*31#	*31#
• Deactivate permanently	#31#	#31#
• Activate for each call	*31 destination No.	*31 destination No.
• Deactivate for each call	#31 destination No.	#31 destination No.
Switch over switch groups 01...20		
• Switch group xx in pos. y xx = Group [01...20] y = switch pos. [1...3]	*85 xx y	*85 xx y
System time / System date		
• Set up the system time	*57 hh mm	*57 hh mm
• Set up the system date	*58 dd mm yyyy	*58 dd mm yyyy
Take	see "Accept a call or data connection with preparation"	
Team keys	–	–

Features	Aastra 6700i series of SIP terminals	Other SIP terminals
Text messages		
• View	–	–
• Send standard text with / without parameters to user	*3598 SC No. text No. #	*3598 SC No. text No. #
• Send standard text with / without parameters to group	*35 Gr. No. text No. #	*35 Gr. No. text No. #
• Send standard text with / without parameters to all	*3599 text No. #	*3599 text No. #
• Snd user-definable message text	–	–
Transfer current call to a different cost centre	see "Call charges"	
Trigger Redkey function	*73 Param. #	*73 Param. #
Two-company configuration	–	–
User groups (selectable)		
• Log into all user groups	*4800	*4800
• Log out of all user groups	#4800	#4800
• Log into specific user groups	*48 UG No.	*48 UG No.
• Log out of specific user groups	#48 UG No.	#48 UG No.
User-to-user signalling (UUS-1)	–	–
Voice mail (basic or Enterprise)		
• Record greeting with phone (x = 1,2,3,7,8)	*913x [*nn] #	*913x [*nn] #
• Record greeting with audio device (x = 1,2,3,7,8)	*923x [*nn] #	*923x [*nn] #
• Check recording (x = 1,2,3,7,8)	*#913x [*nn] # or *#923x [*nn] #	*#913x [*nn] # or *#923x [*nn] #
• Delete recording (x = 1,2,3,7,8)	#913x [*nn] # or #923x [*nn] #	#913x [*nn] # or #923x [*nn] #
• Activate greeting (x = 1,2,3)	*933x	*933x
• Deactivate greeting (x = 1,2,3)	#933x	#933x
• Listen to voice messages with audio guide	*#94	*#94
• Listen to voice messages without audio guide	*#916	*#916
• Signalling of new voice messages	✓	TM
x = 1,2,3: personal greeting 1,2,3 x = 7: global greeting x = 8: global overflow greeting nn = node No. (optional)		
Wait until free	see "Callback on busy (CCBS) / available (CCNR) user"	

1) call number assigned to this control output in the numbering plan

4 SIP access

4. 1 Introduction

The communication server can be connected to one or more SIP providers via the Ethernet interface. As this connection is not defined in the SIP standards, the solution approaches adopted by SIP providers vary slightly from one SIP provider to the next. The configuration required in the communication server is therefore not identical for all SIP providers.

The communication server handles the SIP access in the same way as analogue or digital network interfaces, i. e. they are grouped in one or more separate trunk groups. The allocation to an SIP provider is defined for each trunk group. This means for example that international calls can be routed via SIP providers in different countries.

The communication server must register with the Registrar of an SIP provider so that the SIP messages can be forwarded to the Proxy Server and from there to the public network via a gateway for example. At least one SIP account has to be set up for each SIP provider. Each account contains a user name and password for identification with the Registrar and an SIP identification number (SIP-ID). The SIP-ID is linked with a direct dial number so that outgoing and incoming connections can be made. A total of 500 SIP accounts can be set up and linked with the corresponding direct dialling numbers.

One SIP account per SIP provider can be set up as a default account. It can then be used by subscribers without an SIP account for outgoing calls via a corresponding route or for incoming calls via a special call routing.

The system supports 10 SIP accesses with up to 30 SIP voice channels per SIP access. One *SIP Access Channel* licence is required per SIP voice channel.

4. 2 Routing elements

The routing elements for distributing incoming and outgoing calls via SIP providers are essentially the same as in a connection to analogue or ISDN network interfaces.

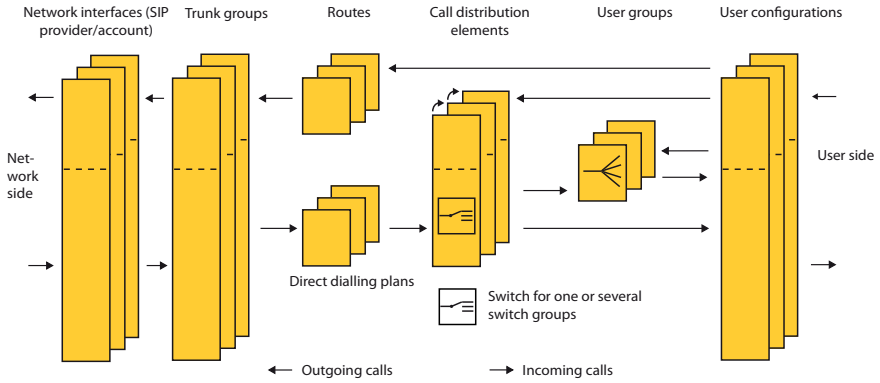

Fig. 11 Routing of SIP calls in the system

4. 3 Configuring the system for SIP access

There are different methods for connecting a system to an SIP provider, depending on the SIP provider. Only the basic configuration steps for an account are described below.

Requirements:
A sufficient number of *SIP Access Channels* licences is available.

1. Start AMS and set up a connection with the communication server.
2. Open an SIP provider under CM_3.2.4_*SIP provider/account* in the Configuration Manager and specify at least the IP address or the name of the Registrar.

   Notes:

   – If you enter a name as an address, a DNS server has to be configured under CM_2.2.4_*DHCP server*.

   – If you leave the data for the proxy blank, the data will be taken from the Registrar.
3. Clicking *Next* automatically creates a new trunk group and allocates it to the SIP provider.

4. Configure any other specific parameters for your SIP provider. Information on the parameters can be found in the tool tips and in the configuration tables relating to the SIP provider (Tab. 15 to Tab. 19).
5. Open an SIP account and specify at least the *SIP-ID* parameter. The SIP provider needs this data to identify the account.

   Notes:

   – If the SIP-ID does not correspond to the direct dial number, specify the direct dial number.
   – If the SIP account has to be authenticated with the SIP provider, specify the user name and password.
6. Click Next and configure the other parameters. Information on the parameters can be found in the tool tips and in the configuration table relating to the SIP account (Tab. 21).

   Note:

   If you specify a direct dial number, clicking Next automatically creates the direct dial number and you can allocate a call distribution element to it.

   Tip:

   If you configured the *Registration required* parameter to *Yes*, after refreshing the view you can now use the status display *Registered* = *Yes* / *No* to check whether or not the account was successfully registered with the SIP provider.
7. Allocate the destinations you want to the call distribution element.
8. To make outgoing SIP calls, select a free route under CM_3.1.6_*Routes* and allocate it the SIP trunk group you have just created.

   Tip:

   On the SIP account configure the *Default account* parameter to *Yes*. This means that all internal users can then make outgoing phone calls via the SIP network interface, not just the users with the set SIP direct dial numbers.
9. If you want to use bandwidth control, set a new bandwidth range under CM_2.5.1.2_*Bandwidth areas* and configure the WAN link to the SIP provider. Next assign the new bandwidth range to the SIP provider you have created. Details on bandwidth control can be found in the System Manual "Aastra Intelligent Net (AIN) and IP Terminals".
10. If you select *Persistent TLS* as the transport protocol, take note of the points set out under "Securing the connection with SRTP/TLS", page 66.

The basic configuration and registration with the SIP provider are now completed and you can receive and make calls via the SIP Access.

4. 4 Configuration tables

The tables below list all the AMS configuration parameters needed for connecting to an SIP provider.

Tab. 15 SIP provider configuration: General

Parameter	Parameter value	Remarks
SIP Provider	<ID>	System-internal reference number of the SIP provider.
Name	<Name>	System-internal designation of the SIP provider
Broadband range	<Name>	Predefined broadband range used for this SIP provider.
Use '+' for the international prefix	<*Yes / No*>	If the provider requires the number in canonical number format, the parameter must be set to *Yes*. In an outgoing call with an international prefix, the prefix is replaced by the "+" character (e.g. : 0049 becomes +49)
Try to make external calls: Timeout	<4…36> sec.	Once that time has elapsed, the system tries to set up the call via the next trunk group defined in the route (default value: 32 seconds).
'From' field for CLIR	Select from list	Display indicated to the recipient in the case of an outgoing call with activated CLIR. If the caller has suppressed caller identification (CLIR), the sender information transmitted may be any of the following, as required: *Anonymous (RFC 3261)*: Display name: anonymous@anonymous.invalid Address: anonymous@anonymous.invalid *As defined in SIP account (RFC 3323)*: Display name and address as defined in the SIP account *Displayed name is 'Anonymous'*: Display name: anonymous@anonymous.invalid Address remains unchanged
Use DNS_SRV (RFC 3263)	<*Yes / No*>	Mechanism for SIP server (or SIP service) resolution e. g. through a URI/URL with the aid of a DNS query. **Note:** If the name or the IP address is configured in the proxy settings, no search is carried out even if the parameter is set to *Yes*.
Send 'Session Refresh' (RFC 4028)	<*Yes / No*>	If this parameter is on *Yes*, the communication server will attempt to negotiate a period for regular "Session Refresh Messages" with the SIP provider. For this the SIP provider must also support RFC4028.
Use destination URL from	Select from list	The destination URL can be formed from the *'To' field* or the *'Request line'*. The choice depends on the SIP provider.
Music on hold	<*Yes / No*>	*Yes*: Music on hold is played, provided it is activated throughout the system.

Parameter	Parameter value	Remarks
Music on hold: signalling	Select from list	The type of signalling for music on hold depends on what the SIP provider supports: *According to RFC 3264*: The SIP provider supports the signalling according to RFC 3264. *According to RFC 2543*: The SIP provider supports the signalling according to RFC 2543 *Automatic*: The system tries to detect by itself which of the two RFCs the SIP provider supports. *No signalling (no media update)*: The SIP provider does not wish to have any signalling and the system feeds music on hold into the speech channel.
Send redirection information	Select from list	Redirecting information allows the called party to see whether the call was redirected and, if so, by whom. The caller also sees whether his call was redirected and if so, to whom. This setting also allows the SIP provider to identify the user who activated the call forwarding so that call charges can be billed correctly. *No*: No redirection information is displayed. *Yes, using 'Diversion header (recursing)'*: In the case of an external SIP call to a user who has activated call forwarding to an external destination the forwarding is carried out in the communication server. With this setting redirection information is displayed only at the forwarding destination. *Yes, using 'Diversion header (non recursing)'*: In the case of an external SIP call to a user who has activated call forwarding to an external destination, the communication server sends Response 302 (Moved Temporarily) with the necessary redirection information back to the SIP provider. Here the call forwarding does not take place in the communication server. With this setting the direction information can be displayed both at the forwarding destination and at the caller. **Note:** Forwarding with Response 302 is not possible in all cases.
Preferred codec	<*Unspecified*/ *G.711a* / *G.711u* / *G.729*>	This parameter is used to select the preferred codec setting for each SIP provider. If the parameter is set to *Not specified*, the codec setting at the corresponding bandwidth area (CM_2.5.1.2) is decisive.
Call forwarding method	<*Re-INVITE* / *REFER*>	
PPI header suppressed	<*Yes* / *No*>	

Tab. 16 SIP provider configuration: Registrar

Parameter	Parameter value	Remarks
IP address	<Address>	IP address of the Registrar at the SIP provider The communication server has to set up a connection to the address in order to register. **Note:** All that needs to be entered is either the IP address or the name. If both are entered, the name is resolved first and the resolved IP address is then used. However a DNS server has to be configured.
Port	<1…65535>	UDP port of the Registrar at the SIP provider
Name	<Name>	Domain name of the Registrar at the SIP provider **Note:** See IP address
Preferred registration interval	<60…65535> sec.	Once this period of time has elapsed, the communication server automatically registers with the SIP registrar on a regular basis in order to maintain a faultless connection.

Tab. 17 SIP provider configuration: Proxy

Parameter	Parameter value	Remarks
IP address	<Address>	IP address of the proxy server at the SIP provider All the communication server's external SIP messages are sent to this address (*Primary proxy*). If it is not available, the messages are sent to the alternative IP address (*Secondary proxy*). **Notes:** All that needs to be entered is either the IP address or the name. If both are entered, the name is resolved first and the resolved IP address is then used. However a DNS server has to be configured. If the fields for the proxy are left blank, the data will be taken from the Registrar.
Port	<1…65535>	UDP port of the SIP proxy server
Name	<Name>	Domain name of the SIP proxy server **Note:** See IP address

Tab. 18 SIP provider configuration: NAT

Parameter	Parameter value	Remarks
Activate 'Keep alive'	<*Yes / No*>	If the parameter is on *Yes* the system periodically updates the NAT table on its own firewall using "Notify" messages to the proxy server. This means that the system remains reachable for incoming SIP calls.
ALG support	<*Yes / No*>	Supports the connection to SIP providers (depends on the provider). If the parameter is configured as *Yes*, IP packets that contain SIP signalling information are opened by the ALG (Application Layer Gateway) and the private IP address is replaced by the public IP address. (The public IP address in the system must be configured.)

Tab. 19 SIP provider configuration: SIP access

Parameter	Parameter value	Remarks
Trunk groups	<Number>	Here the SIP provider is allocated to a trunk group.
Trunk group name	<Name>	System-internal designation of the trunk group
Maximum incoming calls	<30…240>	No further calls are routed via this trunk group once the set limit is reached. This is signalled to the caller by means of the congestion tone.
SIP access without accounts	<*Yes* / *No*>	

Tab. 20 SIP provider configuration: Transport protocol

Parameter	Parameter value	Remarks
Transport protocol	<*UDP or TCP* / *TCP* / *UDP* / *Persistent TLS*>	The transport protocol is selected here. For a secure connection between the communication server and the SIP provider the parameter must be configured to *Persistent TLS* (see "Securing the connection with SRTP/TLS", page 66).
Import certificates	Button	This button imports the certificate of the SIP provider to the communication server.
Delete certificates	Button	This button deletes the certificate in the communication server's file system.
Export certificates	Button	This button exports a certificate.

Tab. 21 SIP account configuration

Parameter	Parameter value	Remarks
SIP account	<ID>	System-internal reference number of the SIP account.
Name	<Name>	System-internal designation of the SIP account.
Display name	<String>	This entry is mandatory with some providers and optional with others. The SIP ID is often used.
SIP ID	<Number>	Identifier of this account with the SIP provider. This is the access number of the account which is then linked with a direct dialling number in the communication server. This parameter must be specified at all times.
User name	<Name>	User name of the SIP account with the SIP provider. This parameter is to be specified only if the SIP provider requires authentication.
Password	<Password>	Password of the SIP account with the SIP provider. This parameter is to be specified only if the SIP provider requires authentication.
Registration required	<*Yes* / *No*>	If the parameter is set to *Yes*, the SIP account will attempt to register with the provider. The SIP provider is then informed about the SIP user's current location.
Registered	<*Yes* / *No*>	Status field
Default account	<*Yes* / *No*>	The default account allows users without SIP account to make calls via the SIP trunk.

Parameter	Parameter value	Remarks
DDI number	<DDI No.>	The DDI number with which the SIP-ID is to be linked is entered in this field. The number must be created and configured in the direct dialling plan. The field can be left blank if the SIP-ID corresponds to the DDI number.
'From' field: Type	<*SIP ID* / *Direct dialling number* / *System CLIP* / *User defined*>	Specifies what is entered in the definable part of the 'From' field for outgoing calls.
'From' field: String	<String>	User-definable character sequence in the 'From' field for outgoing calls: • Character sequence without '@': The character sequence is complemented with '@' and the provider's IP address/name. • Character sequence with '@' as the last character: The character sequence is complemented with the communication server's IP address. • Character sequence with '@' followed by character sequence (e. g. of an IP address): The entire character sequence is neither complemented nor checked; instead it is transmitted as entered.

Securing the connection with SRTP/TLS

For a secure connection both the voice data and the signalling data must be secured (see "Security aspects with VoIP", page 12).

Securing the signalling data:

Certificates are used to secure the signalling data between the communication server and the SIP provider. Usually the certificate from the SIP provider is uploaded to the communication server. A call connection between communication server and terminal is established only if the two certificates match.

Securing the voice data:

The SRTP protocol is used to secure the voice data. Please note the following points:

- Under CM_2.2.5_*Encryption* the *VoIP data encryption* setting valid throughout the system must be configured to *Yes*.
- In the DSP settings the *VoIP mode* parameter must be configured to *secure G.711* or *secure G.711/G.729*.
- Under CM_2.3.3 the *NTP service* parameter must be configured to *Yes*.
- A *Secure VoIP* licence is required.

See also

More detailed information on the SIP access can be found in the User's Guide "SIP Access with Aastra IntelliGate" (syd-0176, currently available in English only).

5 SIP Networking

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

5. 1 Introduction

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

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

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

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

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

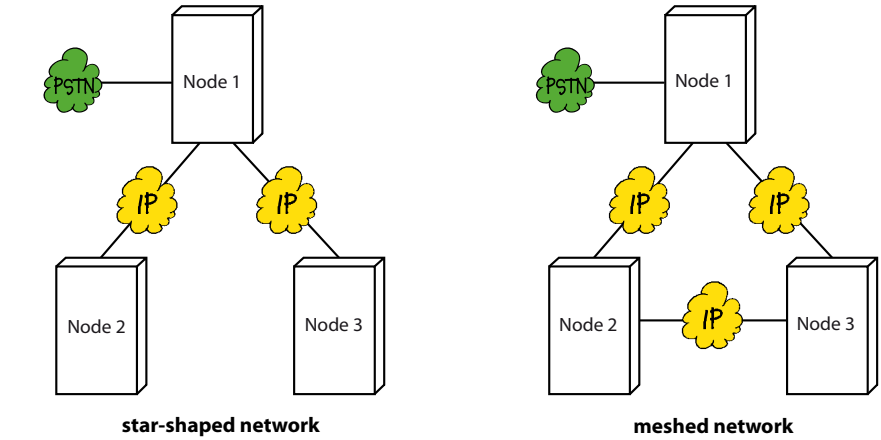

Fig. 12 SIP networking types

5. 2 SIP networking with two systems

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

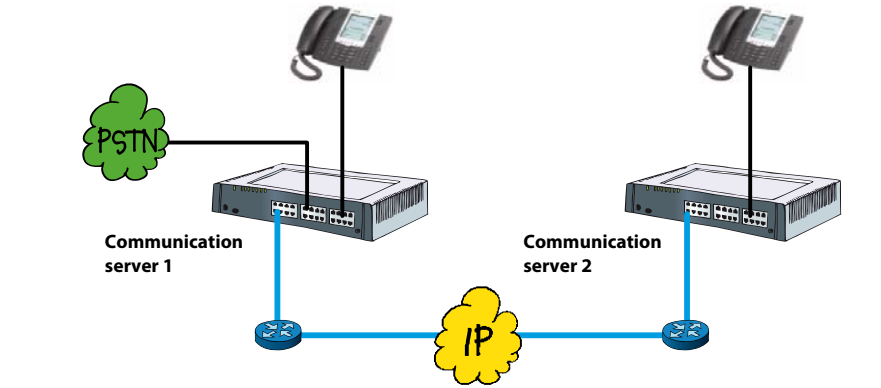

Fig. 13 SIP networking of two locally separate Aastra 400 systems

See also
The descriptions contained in the "PISN/QSIG Networking" System Manual also apply in principle to the planning and configuration.

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

Configuration of the communication server

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

Note:
Only those parameters that are necessary are listed here. The other parameters either remain set on their default value or are irrelevant.

1. Under CM_6.2.2 enter the *Authentication name* and *Authentication password* for the own node.
2. Create a new SIP node and enter the node name, IP address and port of the remote node.
3. Select the trunk group to be created and give the trunk group a name.
4. Configure the *Authentication required* parameter to *Yes*.
5. Enter the *Authentication name* and *Authentication password* for the remote SIP node. These indications must match the configuration in the remote communication server.
6. Configure the bandwidth area and the NAT settings.
7. Specify a route for internal connections to the remote node and give it a name. Assign the corresponding SIP trunk group to the route.
8. Communication server 1 only:
   - Configure a trunk group to the exchange, unless this has already been done.
   - Configure the route for external connections to the exchange (unless this has already been done) and assign the exchange trunk group.
   - Configure the *Transit route* in CM_6.2.1. It must correspond to the route to the public exchange.
9. Communication server 2 only:
   Specify the route for external connections to the public exchange indirectly via communication server 1. Configure the *Send access code* parameter (e. g. to 0: Exchange access, business) and assign the corresponding SIP trunk group.
10. Create the users of the remote node as PISN users and assign them the route to the remote node.
    Tip: If the communication servers were created in a PISN group, you can do this in the AMS Shell using the *PISN synchronization* function.

See also
The meaning of the parameters not described here under CM_6.2.2 is explained in the "Configuration tables", page 61 ff.

5. 3 SIP networking with several systems

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

- You need to create one SIP provider and one SIP trunk group for each connection to another communication server. For all the SIP nodes enter the IP address, port and access data to the corresponding communication servers.
- If the communication server has direct access to the public network, you also need to define a *Trunk group* for the exchange access and to configure the *Transit route*.
- For each internal connection to another communication server and for each connection possibility to the public network configure one *Route* and assign the corresponding *Trunk group*.
- Create the users of the other systems as *PISN users* on your own system.

5. 4 Features supported with SIP networking

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

The following features are supported:

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

Index

A

aastra.cfg 31
About this document 6
Administrator menu 35
AIMS configuration 22

B

Busy lamp field 24

C

Configuration files 31
Configuration methods 30, 36

D

Document information 6

F

Features Overview 50
File system of the communication server 32

G

Gateway 8

I

Infrastructure 37
Introduction to SIP 8

L

Language concept 43
Language packages 44

M

MAC address 38
mac.cfg 31
Multicast DNS 37

N

Networking via SIP 67
Notes about the Products 4

O

Overview of SIP terminals 18, 46

P

Presence menu 29
Proxy Server 9, 10

R

Redirect Server 9, 11
Registering SIP terminals 38, 47
Registrar 58
Registrar Server 9
Registration code 38
Request for Comments (RFC) 15

S

Safety icons 7
Safety Information 4
Selecting the language 45
Session Initiation Protocol (SIP) 8
SIP access 58
SIP application cases 14
SIP licence 18, 58
SIP networking 67
SIP Provider 58
Software Update 42
Symbols 7
System menu 27

T

TFTP folder 32, 41
Types of connection setup 10

U

User Agent 9, 10
User information 5
User interface 35

W

WAN 67