MIVOICE OFFICE 400

MITEL ADVANCED INTELLIGENT NETWORK (AIN)

AS OF VERSION R4.0

SYSTEM MANUAL

Mitel®

syd-0560_en / 1.1 – R4.1 – © 07.2016

NOTICE

TRADEMARKS

PATENT NOTE ON POWER OVER ETHERNET

Mitel Advanced Intelligent Network (AIN)

syd-0560/1.1 – 07.2016

Content

1 Product and Safety Information

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

Please read through the product and safety information carefully.

1. 1 About Mitel

Mitel (Nasdaq:MITL) (TSX:MNW) is a leading global company in the corporate communications industry that connects employees, partners clients worldwide with its technology – everywhere, around the clock and with all terminals, no matter what the size of the business. Mitel offers its customers a great choice with one of the largest portfolios in the industry and direct access to the cloud. With a combined turnover of over 1 billion USD annually and 60 million customers globally, Mitel is the market leader in western Europe and a major player on the corporate communications market. Further information is available at www.mitel.com.

1. 2 Product information

Purpose and function

MiVoice Office 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 co-ordinated 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).

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

User groups

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

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

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

User information

MiVoice Office 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 MiVoice Office 400 DocFinder as individual documents or as a documentation set. Some user documents are accessible only via a partner login.

It is your responsibility as a specialist retailer to keep up to date with the scope of functions, the proper use and the operation of the MiVoice Office 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 MiVoice Office 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 MiVoice Office 400 products used and that you have the latest editions.
- Always read the user documents first before you install, configure and put a MiVoice Office 400 communication solution into operation.
- Ensure that all end users have access to the user's guides.

MiVoice Office 400 Download documents from: www.mitel.com/DocFinder

Conformity

Mitel Schweiz AG hereby declares that

- the MiVoice Office 400 products conform to the basic requirements and other relevant stipulations of Directives EMC (2014/30/EU) and LVD (2014/35/EU).
- all our products are manufactured in conformity with RoHS and WEEE (2002/95/EC and 2002/96/EC).

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

Usage of third party software

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

Exclusion of Liability

(Not valid for Australia. See Chapter "Limited Warranty (Australia only)", page 10 on the limited warranty in Australia.)

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

Environment

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

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

MiVoice Office 400 products are disassembled exclusively using detachable screwed connections.

1. 3 Safety information

Reference to hazards

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

Operating safety

MiVoice Office 400 communication servers are operated on 230 VAC mains power. Communication servers and all their components (e.g. telephones) will not operate when mains power fails. Interruptions in the power supply will cause the entire system to restart. A UPS system has to be connected up-circuit to ensure an uninterruptible power supply. Up to a specific performance limit a Mitel 470 communication server can also be powered redundantly using an auxiliary power supply. For more information please refer to your communication server's system manual.

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

Installation and operating instructions

Before you begin with the installation of the MiVoice Office 400 communication server:

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

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

1. 4 Data protection

Protection of user data

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

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

Protection against listening in and recording

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

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

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

1. 5 About this System Manual

This System Manual describes how to network several communication servers to create a Mitel Advanced Intelligent Network (AIN). While it complements the MiVoice Office 400 System Manual it does not replace it. The Manual is available in German, English, French, Italian and Spanish.

The System Manual is intended for planners, installers and maintenance personnel. The configuration, commissioning and successful operation of an Mitel Advanced Intelligent Network (AIN) requires knowledge of the contents of the Manual. All guidelines, user notes and hazard alert messages must be observed.

Document information

- Document number: syd-0560
- Document version: 1.1
- Valid as of / based on: R4.0 / R4.1
- © 07.2016 Mitel Schweiz AG
- In PDF viewer, click on this link to download the latest version of this document: *https://pbxweb.aastra.com/doc_finder/DocFinder/syd-0560_en.pdf?get&DNR=syd-0560*

Hazard alert messages

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

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

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

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

General highlighting

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 another section in the same document or to other documents.

Mitel Advanced Intelligent Network
Specific points to note in a AIN.

References to the MiVoice Office 400 configuration tool WebAdmin

If you enter an equals sign in the WebAdmin search window □ 🔍 followed by a two-digit navigation code, the view assigned to the code will automatically be displayed.
Example: View *licence overview* (🔍*=q9*)
You will find the navigation code on the help page for the view.

1. 6 Limited Warranty (Australia only)

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

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

Exclusions

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

To the extent permitted by law, Mitel shall not be liable for any incidental damages, including, but not limited to, loss, damage or expense directly or indirectly arising from your use of or inability to use this product, either separately or in combination with other equipment. This paragraph, however, is not intended to have the effect of excluding, restricting or modifying the application of all or any of the provisions of Part 5-4 of Schedule 2 to the Competition and Consumer Act 2010 (the ACL), the exercise of a right conferred by such a provision or any liability of Mitel in relation to a failure to comply with a guarantee that applies under Division 1 of Part 3-2 of the ACL to a supply of goods or services.

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

Repair Notice

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

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

Warranty Repair Services

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

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

Limitation of liability

1.1 To the extent permitted by law and subject to clause 1.2 below, the liability of Mitel to you for any non-compliance with a statutory guarantee or loss or damage arising out of or in connection with the supply of goods or services (whether for tort (including negligence), statute, custom, law or on any other basis) is limited to:

- a) in the case of services:
  - i) the resupply of the services; or
  - ii) the payment of the cost of resupply; and
- b) in the case of goods:
  - i) the replacement of the goods or the supply of equivalent goods; or
  - ii) the repair of the goods; or
  - iii) the payment of the cost of replacing the goods or of acquiring equivalent goods; or
  - iv) the payment of the cost of having the goods repaired.

1.2 Clause 1.1 is not intended to have the effect of excluding, restricting or modifying:

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

After Warranty Service

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

Manufacturer: Mitel South Pacific Pty Ltd ("Mitel") Level 1, 219 Castlereagh Street Sydney, NSW2000, Australia Phone: +61 2 9023 9500	**Note:** Repairs to this product may be made only by the manufacturer and its authorized agents, or by others who are legally authorized. Unauthorized repair will void this express warranty.

2 System Description

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

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

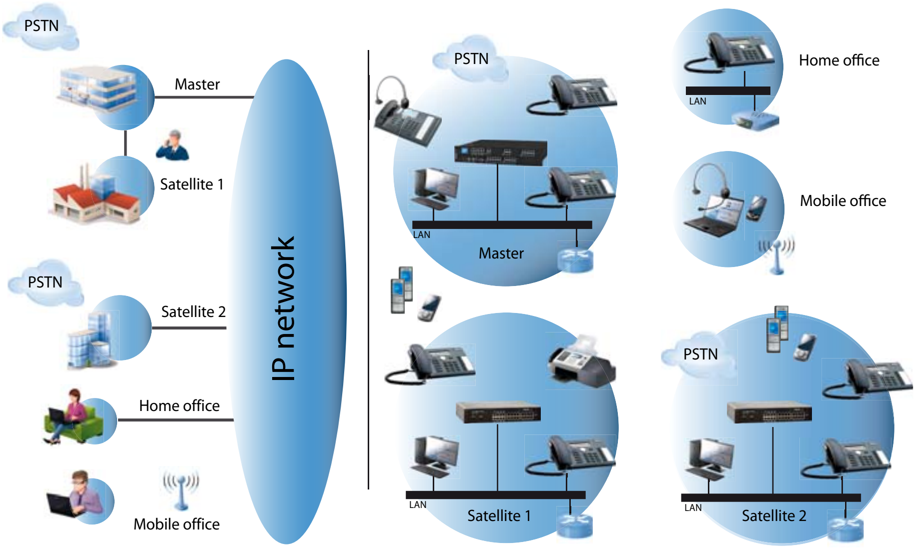


Fig. 1 AIN and IP system phones expand the MiVoice Office 400 platform to the IP network

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

- The modular expansion of the system limits in areas that are otherwise covered only by larger and more expensive communication servers.
- The integration of several sites and branch offices (up to maximal than 41 nodes)[1] even beyond national and language borders.
- The expansion of the DECT coverage range through roaming between nodes with overlapping radio area.

Network properties

Mitel SIP phones and IP system phones are fully integrated into AIN. They are controlled directly by the Master, independently of the location at which they are operated.

You can choose whether voice will be transmitted directly between two endpoints in the AIN (Direct switching) or via the Master (Indirect switching) (Setting (*Relay RTP data via communication server* 🔍 *=32*). Direct switching (default setting) needs less resources, while indirect-switching is the potent method for systems with more demanding network configuration requirements. The signalling is always via the Master for both methods.

An ingenious bandwidth control (🔍 *=q2*) prevents poor connection quality due to lack of bandwidth on the IP network. Optional encryption of call and signalling data (🔍 *=3n*) provides protection against any tapping of and/or tampering with IP phone calls. The encryption methods used guarantee a high level of data protection, authenticity, integrity and protection against replay attacks throughout the network.

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

User benefits

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

- Networked, locally remote and already installed single systems can be grouped together cost-effectively to form a single telecommunication system. This increases the telephony convenience for all users, from staff members to customers.
- Call charges are reduced inasmuch as phone calls made between nodes do not incur any charges, unlike networking via the public telephone network.
- A complete range of features across the entire AIN, regardless of the location of the individual nodes. The AIN eliminates the limits of PISN networking, and features

[1] Values may differ depending on the sales channel and the configuration. Please check the System Manual for information on the values that apply to you regarding the communication server you are using as master.

such as forwarding and three-party telephony, text messages or announcements are available between all the nodes without restriction. Other features that were previously limited to a single system are available throughout the AIN, e.g. user groups with members from the entire network, central operator console, voice mail, announcement service with node-specific texts, network-wide call logging, coded ringing/general bell and door intercom systems.

- Thanks to integrated IP system phones, small branches no longer have to dispense with their own communication servers. Home office staff and users who travel a great deal can be fully integrated.
- Use of satellites as DECT server for implementing large DECT systems.
- Roaming between the nodes allows the radio coverage of a DECT system to be extended across the entire AIN using only one mobile network (handover between the nodes is not possible).
- Telephone lines do not have to be extended when expanding an existing infrastructure with new connections for PCs and telephones.
- As a result of the expansion of the MiVoice Office 400 platform to the IP data network the network used becomes part of the MiVoice Office 400 system. As an alternative calls can also be routed via the PSTN (PSTN overflow) so that communication quality is not affected by interruptions or bottlenecks in the IP network.
- The PSTN overflow allows also a cost-optimised routing configuration in the AINso far as the VoIP channels and bandwidths in the IP network are designed for an average traffic load, and part of the calls during peak times are routed via the public network.

Benefits for planners, installers and dealers

When you configure an AIN, you essentially configure the Master node. You use the same tried-and-tested tools you also use to configure an individual system.

- The Mitel Plan Project Manager is used for planning and drawing up quotations for an AIN.
- Use the WebAdmin administration access for configuration and administration.
- For user and call charge administration use the System Assistant access of WebAdmin.

3 Setting up an AIN

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

The following MiVoice Office 400 communications servers can be used as AIN nodes:

- Virtual Appliance – can be used as Master.
- Mitel 470 – can be used as Master or satellite.
- Mitel 430 – can be used as Master or satellite. Restriction: Can not be used as a Master if the AIN has one or more Mitel 470 nodes.
- Mitel 415 – can only be used as a satellite.

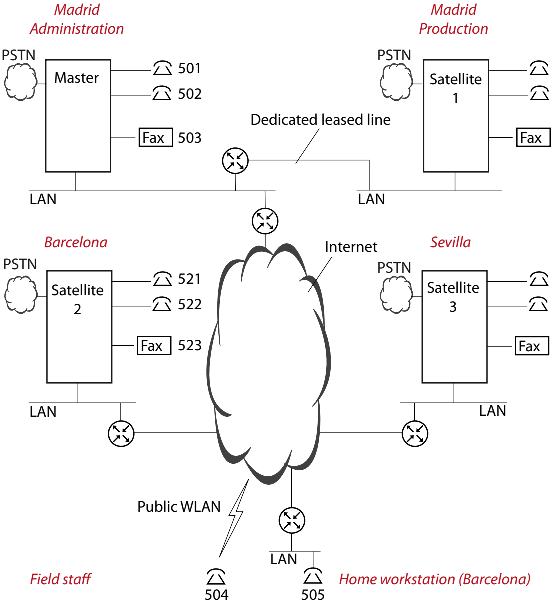


Fig. 2 The AIN of a sample business organization as a reference network

Tab. 1 The node locations in the reference network

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

3. 1 Planning

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

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

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

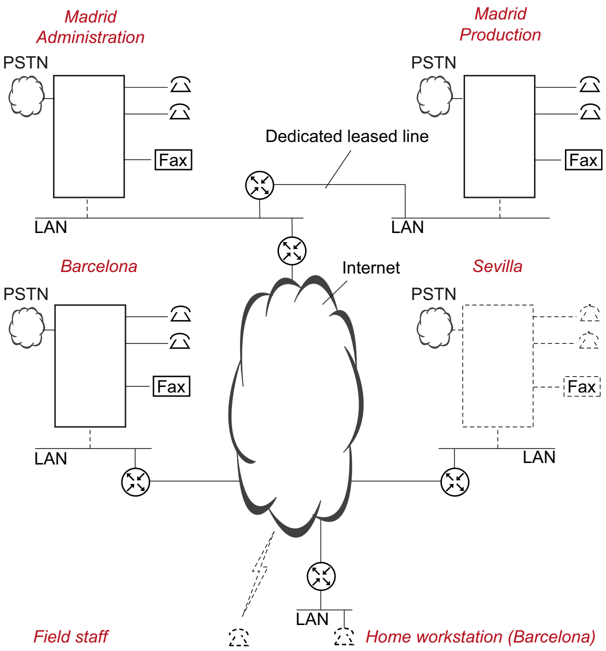


Fig. 3 Basic situation within the reference network

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

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

3. 1. 1 Auxiliary

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

Mitel CPQ Project Manager

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

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

The instructions below explain the procedure for defining the nodes in the AIN, specifying the codec and opening the AIN for further planning in Mitel CPQ.

Specify the AIN nodes

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

Note:

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

While you can subsequently change the country (sales channel), any licences you may already have acquired by that stage will be lost along with the node's configuration data. (see also "AIN areas", page 52).

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

Note:

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

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

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

Specify the codecs

The G.711 codec (64 kbit/s Bit rate) or G.729 codec (8 kbit/s Bit rate) is used to digitise or convert the call data for transmission on the IP network. Media resources are required for real-time encoding and decoding processes in the nodes and IP terminals. G.711 requires less media resources for processing, and more bandwidth on the IP network, G.729 requires more media resources and less bandwidth. Media resources are provided in the form of VoIP channels, see "Designing the VoIP channels", page 23.

G.729 requires a licence (*G.729 Codec* licence). One licence allows the use of a VoIP channel. The licences are acquired on the master and are always used wherever they are currently needed.

You can choose whether in your AIN only G.711 will be used or whether G.729 may also be used. You can also choose between the non-encrypted and the encrypted variant:

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

More information on encrypted transmission can be found under "Encrypted transmission", page 63.

Mapping AIN in Mitel CPQ

1. Log on to the Mitel Connect Portal and open Mitel CPQ.
2. In the list box choose *MiVoice Office 400* for configuration type, tick the *Project several nodes* checkbox then click *Start* to start a new configuration.

   A new networking project is opened and the first MiVoice Office 400 node is added.
   To map an AIN, add all the nodes in the next few steps and create the connections between the nodes. Besides the master and the satellites you also need to create the IP network itself as a node. Each node connection is routed via the IP network node, ultimately creating a star-shaped topology with the IP network node at the centre.
   First specify the master node and set the codec:
3. Add an *IP network* type node. If you do not give the node a name, it will be named *IP network* .
4. Click on the two visible nodes one after the other. A *Connect* button appears on both nodes. Click one of the buttons.

   The Connection dialog box appears.

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

5. Choose *Master* as node type then select the codec you want. (see "Specify the codecs", page 20)
6. Select the validity period you want for the software subscription licence. During the validity period you have access to all updates without incurring additional licence fees. Click *OK*.

   The Connection dialog box closes.
7. In *Node1* click the *Edit* icon and enter the name of the master as the node name.

   You have now created the master and specified the codec for the entire AIN. Next add the satellites.
8. Add one after the other for each satellite an *MiVoice Office 400 satellite type node to the IP network*.

   Connection to the *IP network* node is automatically set up after you have closed the connection dialogue.
   All the nodes are now shown on the networking diagram.

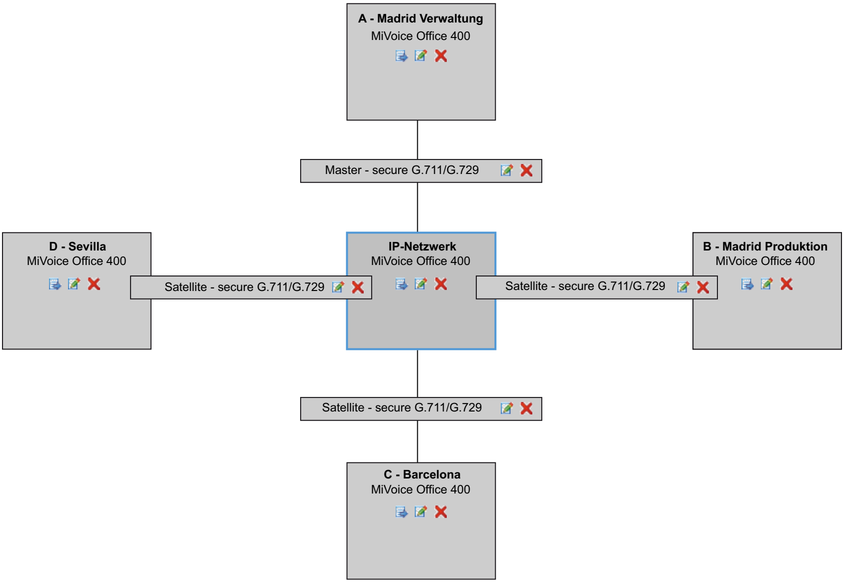


Fig. 4 The reference network in Mitel CPQ

The nodes are now defined and networked with one another via the IP network. The nodes are listed in table form below the networking diagram. To configure an individual node, click the pictogram in the node in question. However, before proceeding with the configuration in Mitel CPQ, you should save the project:

1. Use the Mitel CPQ menu bar to change to the *Result* view.

   Mitel CPQ calculates the necessary components for implementing the networking project you have created.
2. Now, save the project as an XML file in the section entitled *Save configuration* for further processing on your system.

3. 1. 3 Configuring the node expansion

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

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

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

IP and SIP phones

Regardless of their location the IP and SIP phones for AIN operation are all registered with the Master. However, in the expansion configuration with Mitel CPQ they are entered at the relevant nodes:

- Enter the IP and SIP phones of a particular location at the node for that location. Mitel CPQ then calculates VoIP channels for these phones at the location.
- Enter remote IP and SIP phones in a similar way to home workstations or mobile workstations on the Master.

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

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

Connections to the public network

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

- If a satellite is located in a different area to the Master, so that regional emergency destinations can be reached directly.
- If the connection to the Master is interrupted and the satellite is to enable telephone traffic in offline mode also (see "Satellite in Offline Mode", page 55).
- If you want to provide an overflow to the public network (see "PSTN overflow", page 42).
- If you prefer to route calls from individual users via the PSTN (e.g. for fax connections without T.38 or connections with PISN users or integrated mobile phones).

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

Configuration in Mitel CPQ

1. Use the Mitel CPQ menu bar to open the *System* / *AIN* view.

   The *AIN* table and the *Resource overview* table are displayed.
2. Define the exchange access for each node in the *Exchange access* column of the *AIN* table and click the *Recalculate* button.

Defining supplementary equipment

Plan the use of additional functions and equipment such as voice mail, CTI applications, door intercom systems, external switching of the switch group or fax transmission. Many of these additional functions and equipment are set up on the master only. Also take note of the instructions as set out in the Chapter "Region-related settings", page 52.

3. 1. 4 Designing the VoIP channels

Real time conversion of the call data for transmission in the IP network requires some media resources at the transitions between IP and non-IP endpoints. They are provided in the form of VoIP channels. For Virtual Appliance, the media resources are dynamically provided by the integrated Mitel Media Server.

Note:
The available media resources are scalable and assignable in the hardware-based communication servers and must be configured. IP and SIP system phones, as well as Virtual Appliance communication servers, dynamically provide the necessary media resources.

Mitel CPQ (*System* / *AIN* view) calculated based on the configured phones, terminals and exchange line circuits, the anticipated traffic load and the VoIP channels required as a result. Both the traffic load within the AIN and the traffic load generated by the exchange transit traffic are taken into account (provided the exchange accesses have been entered). For call connections between two IP endpoints the required VoIP channels for indirect switching are calculated. The result is based on the assumption of an average traffic density. However you have the possibility of manually correcting the calculated value upwards or downwards if required.

Mitel CPQ then assigns the most suitable media resources to the calculated VoIP channels and determines the licences required.

Requiered VoIP channels

The following example (Fig. 5) shows the required VoIP channels for a call connection between two possible endpoints. In normal operation all IP endpoints are registered with the master, even if they are located on the satellite.

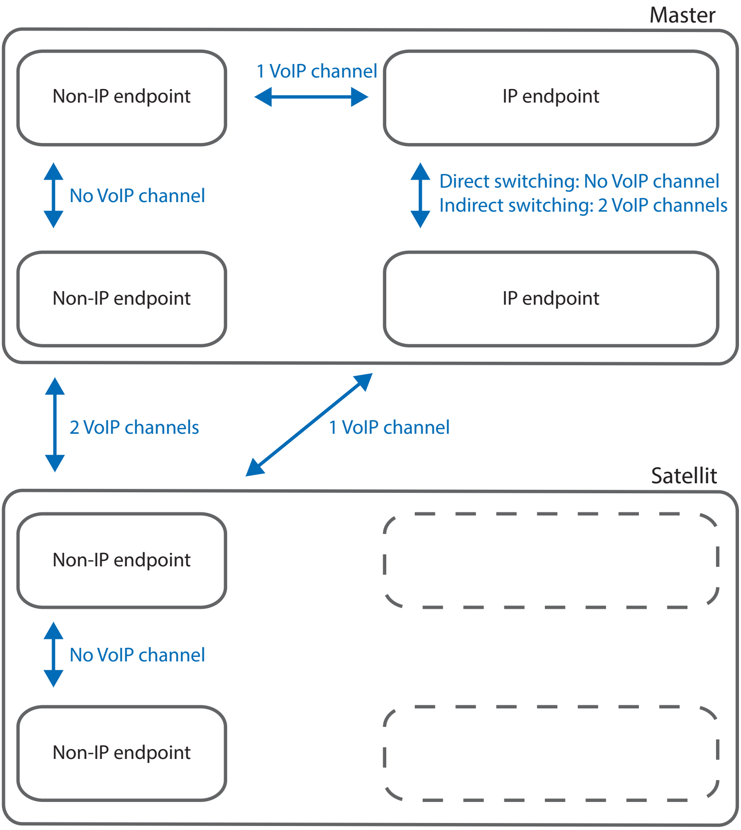


Fig. 5 Required VoIP channels between two possible endpoints.

Tab. 3 IP endpoints and non-IP endpoints

IP endpoints	Non-IP endpoints
• IP system phone • Mitel SIP terminal • Standard SIP terminal • DECT cordless phone via ?SIP DECT • WiFi cordless phone via ?SIP DECT • WiFi cordless phone via ?SIP access point • WiFi mobile phone via ?AMC-Controller • External via SIP provider	• Analogue terminal (FXS) • Digital system terminal (DSI) • DECT cordless phone (DSI) • ISDN phone (BRI-S) • External via analogue exchange (FXO) • External via ISDN exchange (BRI-T/PRI) • Internal voice mail system • Auto attendant • Internal announcement service • Music on hold • Conversation recording • Queue with announcement • Conference bridge

3. 1. 5 Specifying the numbering plan

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

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

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

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

Tab. 4 Numbering the users in the reference network (see Fig. 2)

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

3. 1. 6 Specifying the IP addressing

You can address AIN nodes as well as SIP and IP phones either via DHCP and DNS or statically. Hybrid forms are also possible. The communication servers of the MiVoice Office 400 series also have an integrated DHCP server. This provides many possibilities for the IP addressing.

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

Note:

- Static node addressing is stable and in most cases the simplest addressing.
- A Virtual Appliance communication server can only be addressed statically.
- Whatever form of addressing you opt for: make sure you allow for the highest possible availability for all the nodes, but particularly for the master as central AIN element.
- Whatever the addressing method used, it is important to ensure that the AIN elements recognise one another via the WAN links too.

After the first start of a communication server dynamic addressing with DHCP is activated; the model name followed by the MAC address is specified as the host name (e.g. Mitel430-00085d8031a6).

SIP and IP system phones are always logged on to the Master regardless of their location in the AIN and are also configured there. For the offline operation of a satellite IP system phones can also be logged on to the satellite, see "IP system phones in offline mode", page 58.

Static addressing in the reference network

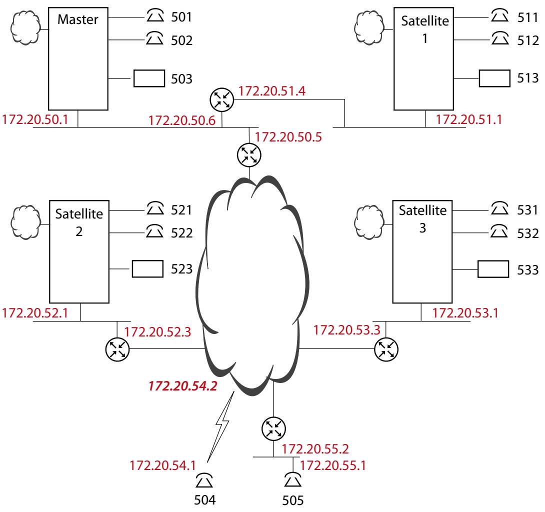


Fig. 6 Network diagram with IP addresses

Tab. 5 IP addresses of the nodes in the reference network

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

Overview of possible IP configurations

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

Tab. 6 Examples of possible IP configurations in the reference network

Parameter	Static	DHCP/DNS	Static and DNS
Master:			
• *Host name*	-	MiVO400master[1]	MiVO400master[1]
• *IP address*	172.20.50.1	[2]	172.20.50.1
• *Subnet mask*	255.255.255.0	[2]	255.255.255.0
• *Gateway*	172.20.50.5	[2]	172.20.50.5
• *Master address*	-	-	-
• *DHCP*	No	Yes	No

Parameter	Static	DHCP/DNS	Static and DNS
• *Primary DNS server*	-	[2]	<IP address>
• *Secondary DNS server*	-	[2]	<IP address>
• *Domain name*	-	[2]	<Name>
Satellite 1:			
• *Host name*	-	MiVO400sat1	MiVO400sat1
• *IP address*	172.20.51.1	[2]	172.20.51.1
• *Subnet mask*	255.255.255.0	[2]	255.255.255.0
• *Default gateway*	172.20.51.4	[2]	172.20.51.4
• *Master address*	172.20.50.1	*MiVO400master*	*MiVO400master*
• *DHCP*	No	Yes	No
• *Primary DNS server*	-	[2]	<IP address>
• *Secondary DNS server*	-	[2]	<IP address>

[1] The default value is the model designation followed by the MAC address (e.g. Mitel430-00085d8031a6).

[2] Automatically assigned values are displayed.

3. 1. 7 Planning an IP network

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

Notes:
Please note that the know-how of an experienced network technician is essential for assessing and optimizing the network neighbourhood.

1. Check whether your network neighbourhood meets our recommendations ("IP network requirements", page 60) and if necessary take the necessary measures to fulfil the requirements.
2. Plan the VLAN and specify the DiffServ classes as indicated under "Prioritization and QoS", page 62.

3. 2 Installation

The aim of this installation phase is to commission the AIN nodes. This requires various configuration operations in addition to the actual installation.

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

- Finding the communication server on the IP network – page 30
- Integrating single systems into the IP network – page 32
- Checking AIN operation – page 33

- Commissioning Mitel SIP phones and IP system phones – page 35 .
- Synchronizing the application software in the AIN – page 35

3. 2. 1 Finding the communication server on the IP network

New hardware-based communication servers connected to the IP network may not be reachable under all circumstances without the prior configuration of the IP addressing. This chapter explains how to set up a connection to the new systems.

Default values of the IP addressing

Tab. 7 Default values for IP addresses

Parameter	Parameter value
IP address	192.168.104.13
Subnet mask	255.255.255.0
Gateway address	0.0.0.0
DHCP	On
Host name	-
• Mitel 415	*mitel415*-<MAC address>
• Mitel 430	*mitel430*-<MAC address>
• Mitel 470	*mitel470*-<MAC address>

Note:

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

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

– To detect a hardware-based communication server on the IP network, proceed according to "Finding the communication server on the IP network", page 30.

First-start behaviour and standard values of IP addressing

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

- If a DHCP server offers the communication server an IP address, the address is used and the communication server attempts to register with the DNS server under the name <Model name>-<MAC address>.
- If the communication server is not offered an IP address, it starts up under its default address 192.168.104.13.
- If a manually entered IP address is already stored at the time of the first start, the communication server deactivates DHCP and starts with this address.

Tab. 8 Default values for IP addresses

Parameter	Parameter value
IP address	192.168.104.13
Subnet mask	255.255.255.0
Gateway address	0.0.0.0
DHCP	On
Host name	-
• Mitel 415	*mitel415*-<MAC address>
• Mitel 430	*mitel430*-<MAC address>
• Mitel 470	*mitel470*-<MAC address>

Note:

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

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

– To detect a hardware-based communication server on the IP network, proceed according to "Finding the communication server on the IP network", page 30.

Finding a hardware-based communication server on the same subnet

The tool System Search contains a function for finding hardware-based MiVoice Office 400 communication servers on the IP network. The search function finds all connected hardware-based communication servers on the same subnet. Newly added communication servers can be addressed directly with System Search and opened with WebAdmin. Moreover, you can perform an emergency upload or downgrade the system with System Search.

Finding a hardware-based communication server on another subnet

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

- If a communication server was able to register successfully with the DNS server, it can be reached under the host name <Model name>-<MAC address> (e. g. Mitel430-00085d8031a6).
- If the communication server has logged on with the default address, you must modify your PC's IP configuration in such a way that the subnet corresponds to that of the communication server. To do so proceed as follows:

1. Adjust your PC’s IP address so that it is within the same address range as the communication server’s default address (see Tab. 9).

2. Connect the Ethernet interface directly to the PC or via a switch with the Ethernet interface on the communication server.

Note:
You can use either a conventional patch cable or a crossover cable to do so.

3. Start System Search.

   The communication server is now displayed.
4. Use System Search to modify the communication server IP address.
5. Reconnect the communication server to the IP network and restart.
6. Restore the correct IP configuration on your PC and connect the PC to the IP network.
7. Restart System Search.

   The communication server is now visible and accessible under the new IP address.

Tab. 9 Default values of the IP addressing

Parameter	Parameter value
IP address	192.168.104.13
Subnet mask	255.255.255.0
Gateway address	0.0.0.0
DHCP	*Yes*
Host name	<Model name>-<MAC address> (for example “Mitel430-00085d8031a6")

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

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

Commissioning hardware-based master

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

1. Connect the communication server to the IP network and start it.
2. With System Search find the communication server on the IP network and configure the IP addresses. Then click *Configure...*.

   The WebAdmin login window opens.
3. Log on, navigate to the *AIN* / *General* (🔍 *=3q*) then change the communication server back to *AIN master*.
4. Activate the AIN licence and enter the new licence number.

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

Commissioning Virtual Appliance master

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

1. Connect the communication server to the IP network and start it.
2. Enter the master's IP address in your browser.

   The WebAdmin login window opens.
3. Log on, navigate to the *AIN* / *General* (🔍 *=3q*) then change the communication server back to *AIN master*.
4. Activate the AIN licence and enter the new licence number.

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

Putting the satellites into operation

First configure the Master's IP address in the satellite:

1. Integrate the future satellite into the IP network following Steps 1 and 2 in the previous section.
2. Log on via WebAdmin then navigate to the *AIN* / *General* (🔍 *=3q)*.view.
3. Select *Operating mode* = *AIN satellite* then under *Master IP address* enter the master IP address.
4. Make the modifications and restart the system.

Then integrate the satellite into the AIN:

1. Log on via WebAdmin to Master then navigate to *System* / *Cards and modules* (🔍 *=4g)*.

   The satellite is now visible as another node with its expansion cards and modules.
2. Confirm the new satellite by clicking in the line with the satellite mainboard on the *Confirm new satellite* button.

   The satellite is now working.

3. 2. 3 Checking AIN operation

Once all the nodes have been commissioned the AIN is set up: The master knows all the satellites, and the signalling between master and satellites is up and running. However, call connections can only be set up after you have manually configured media resources for VoIP in all the AIN nodes.

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

The AIN operation status indication on the Mitel 470

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

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

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

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

The AIN operation status indication on the Mitel 430

LED display of the satellite offline operation:

- Operation status indication on the Master:

  No indication of the operation status of the AIN.
- Operation status indication on the satellite:

  If the SYS LED is flashing green/orange, the node is in offline mode and has lost its connection with the Master.

Connection to the Master interrupted

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

1. Check whether the missing satellite is up and running. If the satellite itself has no malfunction, it is either running in offline mode or currently carrying out a restart (see also "Satellite in Offline Mode", page 55).
2. Try and ping the missing satellite. If it cannot be pinged, the cause could be an error in the IP addressing.
3. For dynamic IP addressing: Check whether the Master is entered under its host name in the DNS server by entering the command "*nslookup* <Host Name>" at the DOS prompt.
4. Check the Master to see whether a sufficient number of satellites have been licensed.
5. Check whether the Master’s name and/or IP address are correctly entered in the satellite configuration. If the input is incorrect, the satellite will be unable to find the Master.
6. Check whether the satellite has the same software version as the Master.
7. Once the connection to the Master is restored, the satellite automatically carries out a restart in offline mode before logging on with the Master again. You can also run

the restart manually if you do not want to wait for the timeout of the connection monitors.

3. 2. 4 Commissioning Mitel SIP phones and IP system phones

The instructions below explain the procedure for installing and commissioning Mitel SIP phones and IP system phones. Please note that all Mitel SIP phones and IP system phones are always logged on to the Master and configured for AIN operation regardless of their location.

3. 2. 5 Synchronizing the application software in the AIN

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

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

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

3. 2. 6 Excluding a satellite

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

Note:
When a satellite is deleted the entire data configured in connection with this node is lost. First create a backup for the Master.

1. Cut the satellite's IP network connection.
2. Log on via WebAdmin, navigate to the *AIN* / *General* (🔍 *=3q*) view then choose *Operating mode* = *Individual system*.

3. Restart the communication server (Menu *Reset communication server* / *Restart* 🔍 *=4e*).

   The communication server starts as a single system and is no longer connected to the Master.

Now delete the satellite in the master configuration:

1. Log on via WebAdmin to Master then navigate to *System* / *Cards and modules* (🔍 *=4g*).

   The satellite is now visible as another node with its expansion cards and modules.
2. Delete the removed satellite by clicking in the line with the satellite mainboard on the *Delete* button.

3. 3 Configuration

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

The instructions below explain the procedure for first configuring AIN operation; the configuration is then transferred to the satellite offline configuration using the WebAdmin Import/Export function. If required you can also proceed in reverse order and configure the satellite offline operation first and then transfer the satellite configurations for AIN operation.

3. 3. 1 Configuring AIN operation

Configuring AIN operation (guide)

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

Also take note of the indications provided under "Region-related settings", page 52 and "Restricted functions in the AIN", page 59.

1. First create or complete the basic data such as the direct dialling plan, numbering plan, users and abbreviated dialling lists. If your AIN consists of nodes which were already operational beforeAIN integration and whose numbering plans can be merged into a single numbering plan without clashes, you can apply the user and terminal data with the relevant numbering plan and port data with the WebAdminin the AIN. *Import* 🔍 *=0k*

2. Configure the media resources (🔍 *=ym*) following the instructions in "Designing the VoIP channels", page 23 and according to the calculated values of the Mitel CPQ project manager.
3. Configure the node-specific settings for the AIN.
4. Configure the AIN regions in accordance with the information given in "Region-related settings", page 52.
5. Configure the PSTN overflow in accordance with the information given in "PSTN overflow", page 42.
6. Configure the routing for integrated mobile phones and PISN users in accordance with "Routing outgoing calls via local nodes", page 47.
7. Configure the emergency number destinations for the AIN. Please note that nodes in other areas usually also have other emergency destinations. These nodes should have their own exchange accesses so that the emergency destinations can be dialled directly.
8. Configure the switch groups for the AIN.
9. Configure the DECT system.

   In regular AIN operation all the cordless phones are logged on to the Master. Users are able to use their cordless phones on the same call number in the radio area of each node without having to log on there specially (roaming).
   For Office 135 and Office 160pro/Safeguard/ATEX only: Log the cordless phones onto DECT system A to ensure that the software of the cordless phones is also updated whenever the Master software is updated.

   Only Mitel 600 DECT: Configure the selected software update locally on the devices under the *Download server*. menu entry.
10. Configure the other devices and features such as LCR, door intercom systems, music on hold or a voice mail system.

3. 3. 2 Configuring offline operation for the satellites

You can make the settings for a satellite's offline operation directly on the satellite. To do so, follow the instructions given under "Configuring offline operation", page 56.

4 Communication server as AIN node

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

4. 1 Routing in the AIN

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

- Direct routing of the call data between the AIN nodes and separate transmission of signalling and call data, Seite 38
- Optimized resource management, Seite 39
- PSTN overflow, to cover connection resources during peak loads, Seite 42

4. 1. 1 Direct / Indirect Switching of the Voice Data

A call is always controlled and signalled by the Master, even if the Master itself is not involved in the call. IP endpoints and satellites never exchange signalling data directly.

The voice data exchange (RTP stream) between two IP endpoints is either directly (direct switching) or via the Master (indirect switching). You can define this for each endpoint (*Relay RTP data via communication server* 🔍 *=32*).

The example below illustrates the direct switching using a simple call connection (Fig. 7). The advantage of the direct-switching is that, for this connection, neither VoIP channels nor bandwidth resources are charged on the communication server (see Tab. 3, on page 3).

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

- Satellite 1 notifies the Master that it wants to set up a connection to satellite 3 (signalling).
- The Master checks whether a free VoIP channel is available at both nodes.
- If a VoIP channel is available at both nodes, the Master uses bandwidth control to analyse whether there is sufficient bandwidth available for the connection (see "Bandwidth Control", page 69).

- If so, the Master instructs satellite 3 to call user 531 and satellite1 to feed the ring-back tone to user 511 (signalling).
- Satellite 3 signals to the Master that user 531 has answered the call; the Master then instructs satellite 1 and satellite 3 to set up the connection (signalling).
- The call connection between satellite 1 and satellite 3 is set up.

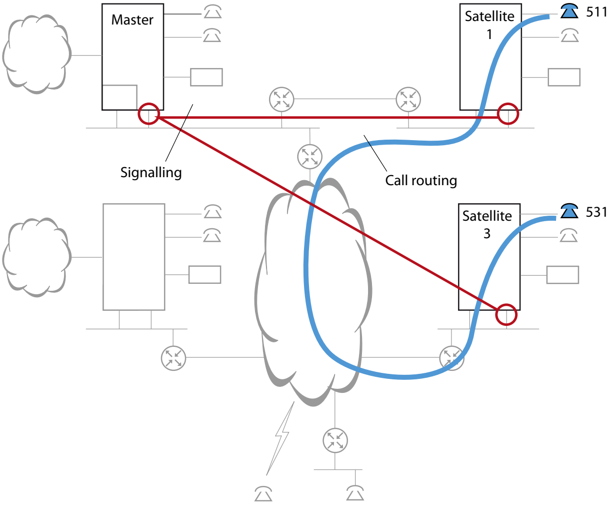


Fig. 7 Routing a simple call

4. 1. 2 Optimized Resource Management

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

Note:
If the WAN links via the Internet are protected in each case with independent VPNs, calls are always routed via the IP network with the Master, which largely cancels out the resource-saving function of resource management. Therefore always try and implement VPNs routed via an internet provider (see "Using VPN", page 65).

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

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

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

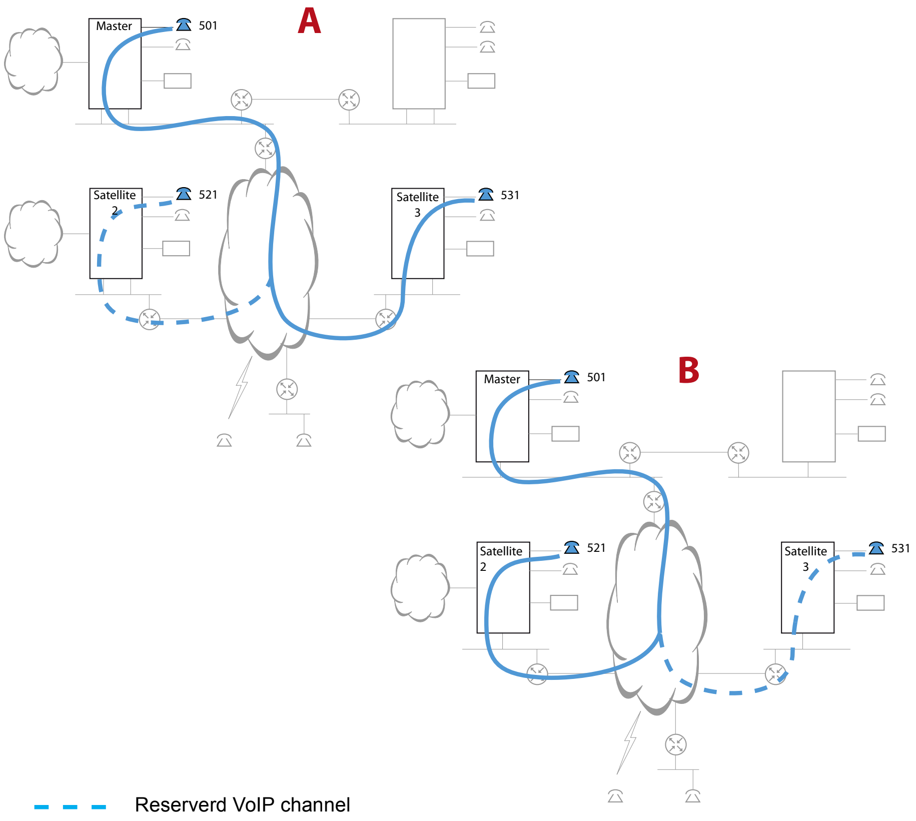


Fig. 8 Callback and brokering in the AIN

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

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

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

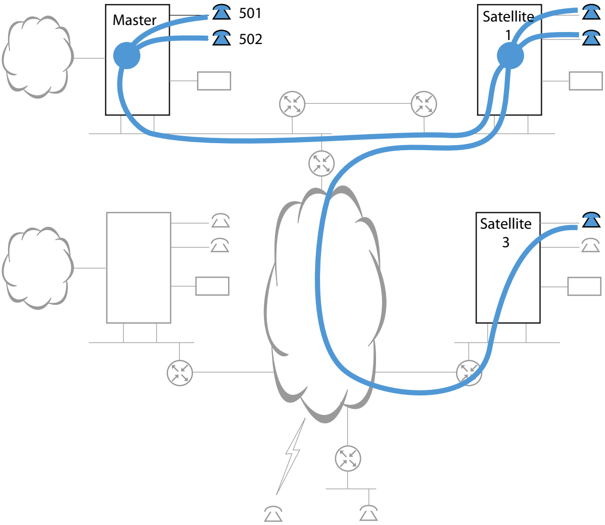


Fig. 9 Conference circuit in the AIN

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

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

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

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

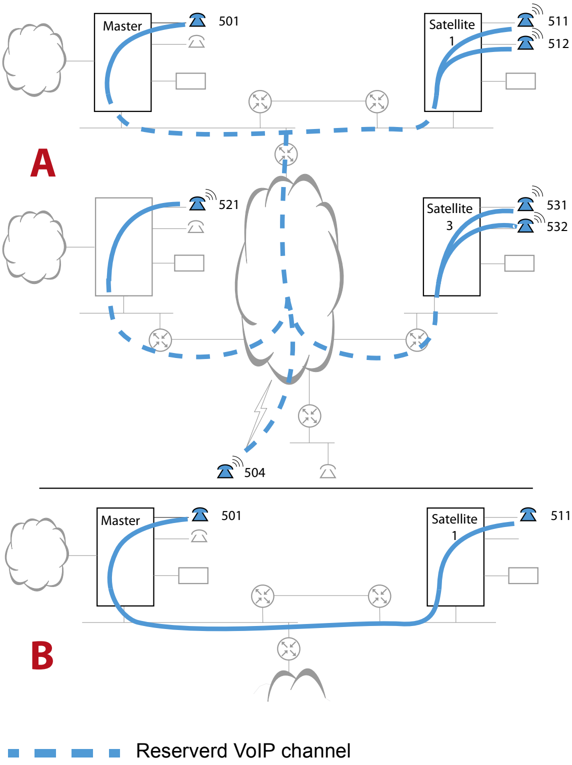


Fig. 10 Call to a user group in the AIN

4. 1. 3 PSTN overflow

The PSTN overflow automatically routes calls via the public network if there are no more voice channels available via the IP network.

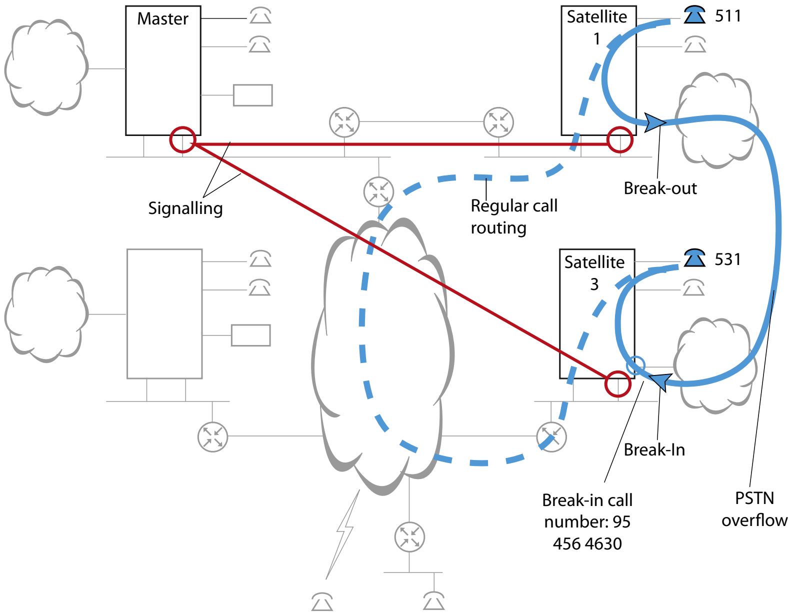
Using the PSN overflow routing, you can in AIN, for instance, define the audio channels and bandwidths on the IP networks for a medium traffic load and relay part of the calls via the PSTN during peak periods. This makes for a rapid configuration of call routing.

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

The example below shows the function of PSTN overflow using a simple call connection. (Fig. 11 on Seite 44).

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

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



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

The call is then routed via the public network.

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

Fig. 11 PSTN overflow

Call routing via the PSTN can also be forced for individual users. Calls by these users are then routed via the PSTN even if there are still sufficient VoIP channels available to route the call by regular means via the IP network. In this way you can consistently route fax calls, for example, via the public network (see also "Fax date transmission in the AIN", page 49).

4. 1. 3. 1 Suitability and limitations

PSTN overflow is suitable for the following applications:

- Routing peak loads between AIN nodes via the PSTN.
- Routing fax connections in the AIN (as an alternative to FoIP, see Seite 50).

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

Please take good note of the following restrictions:

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

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

To set up PSTN overflow, first specify the authorisations then create the break-in and break-out configuration:

Specifying authorisations

1. Enable PSTN overflow in general for the entire AIN (*authorise PSTN overflow in AIN* 🔍 =kx).

   Nodes connected via QSIG can be separately enabled for PSTN overflow (Enable PSTN overflow on PISN 🔍 *=kx*).
2. Disable PSTN overflow for all phones and terminals to be barred from this feature (*Terminals* table, setting *Enable PSTN overflow* = *No* 🔍 *=kx*).

3. In the call distribution elements, disable PSTN overflow for phones on the DDI numbers to be barred from this feature (*Terminals* table, Setting Enable PSTN overflow = *No* 🔍 *=kx*).
4. Enable PSTN overflow for all phones and terminals whose calls are to be routed via the PSTN only if the connection cannot be set up via the IP network (e.g. for all fax machines if FoIP is to be used for the fax connections in normal operation (*Terminals* table *PSTN overflow* = *If necessary* 🔍 *=kx*).
5. Force PSTN overflow for all phones and terminals whose calls are always to be routed via the PSTN and never via the IP network, e.g. for all fax machines (*Terminals* table, Setting *PSTN overflow* = *Always* 🔍 *=kx*).

Creating the break-in configuration

1. For the entire AIN open only one call distribution element for break-in For this, open a new call distribution element and define for all switching positions the destination (*PSTN overflow*🔍 *=dh*). Leave the remaining CDE settings unchanged on their default values.
2. For each node define a DDI number for break-in and link it with the break-in call distribution element that has just been opened.
3. Enter the just defined break-in DDI number in the table *AIN* node (setting *Break-in call number* 🔍 *=kx*).

Creating the break-out configuration

1. Define the break-out route for each node (table *AIN* setting *Route* 🔍 *=kx*).
2. Specify for each node how many calls from each node can be routed via the public network (table *AIN node*, setting *Enabled break-out connections* 🔍 *=kx*).

The PSTN overflow is now set up.

Tab. 10 PSTN overflow on the example of the reference network

Parameter[1]	Parameter value	Explanation
Classes of service:		
• System-wide: *Enable PSTN overflow in AIN*	*Yes* or *No*	Allows you to enable or disable PSTN overflow throughout the system
• Terminal-specific: *PSTN overflow*	*No* / *If necessary* / Always	Allows you to enable, disable or force PSTN overflow specifically for individual terminals.
• Direct dialling number-specific: *Enable PSTN overflow*	*Yes* or *No*	Allows you to enable or disable PSTN overflow specifically for individual direct dialling numbers (using CDE).
Break-in configuration:		

Parameter[1]	Parameter value	Explanation
• *DDI number* → *CDE no* Master Satellite 1 Satellite 2 Satellite 3	 600 → 601 610 → 601 620 → 601 630 → 601	Break-in DDI number with assignment on the break-in CDE.

• *Break-in call number*
Master
Satellite 1
Satellite 2
Satellite 3
	
	91 123 1600
	91 234 2610
	93 345 3620
	95 456 4630
		Enter complete call number without access prefix. Complement with country code if nodes are in different countries.

• Call Distribution element for break-In: *- Name* *- Call number* *- CDE destination*	 Break-in 601 *PSTN overflow*	Only one break-in CDE is required in the entire AIN.
Break-out configuration (to be configured for all the nodes):		
• *Break-out route*	1	Outgoing routing configuration
• *Allowed break-out connections*	10	Restriction in the number of break-out connections

[1] All the settings are made on the Master

4. 1. 4 Routing outgoing calls via local nodes

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

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

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

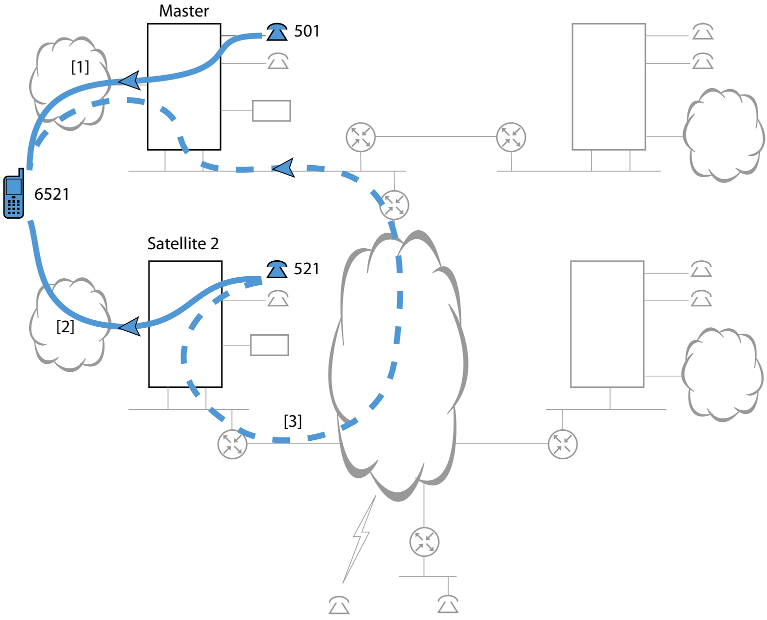
1. Configure a route for integrated mobile phones users and one for PISN users.
2. Allocate trunk groups of all nodes with network connections to the routes.
3. Select *Yes* for the route setting *Use node network interface first.*

The following example (Tab. 11 and Fig. 12) shows the route when internal users on the master and on satellite 2 call the integrated mobile phone user 6521.

Tab. 11 Example: Optimized route configuration for the user of an integrated mobile phone

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

[1)] All the settings are made on the Master



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

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

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

Fig. 12 Example: Routing outgoing calls to integrated mobile phones or PISN users

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

4. 2 Fax date transmission in the AIN

The AIN provides the following possibilities for transmitting fax data:

- Fax over IP (FoIP):
  Transmission of fax data in the IP network using fax transmission protocol T.38. This is the most reliable method for transmitting fax data directly in an IP network. See "Fax data transmission with T.38 (FoIP)", page 50.
- Fax over VoIP
  Transmission of fax data as voice data in the IP network. If this solution alone is used, a number of points and restrictions need to be taken into account. See "Restrictions for Fax-over-VoIP:", page 51.
- Fax traffic via the PSTN:
  Fax traffic is consistently handled via the PSTN using PSTN overflow. Each node with a fax machine then needs a PSTN connection. See "PSTN overflow", page 42.
- Using a fax server:
  The fax server receives faxes from outside the AIN and forwards them as e-mails and vice versa. Paper documents are read in using a scanner. Fax machines are then superfluous.
  - Advantage: Integrated solution.
  - Drawback: No real-time transmission.

Terminal interfaces supported

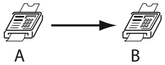
Fax machines can be connected to FXS and ISDN terminal interfaces. Analogue fax machines can also be connected to an SIP terminal interface using an analogue terminal adapter (analogue – SIP).

Configuration

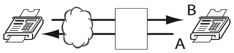
The fax connections are configured first and foremost using the *Fax device* setting. The setting value for external fax connections is available in the analogue interface view (🔍 *=cx*), it is available for internal fax connections in the analogue terminal view (🔍 *=sr*).

Fax connection in the AIN based on the *Fax device* setting

Tab. 12 Internal fax connection

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

Tab. 13 External fax connection

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

[1] Fax service Gr.2/3

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

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

- Each FoIP connection requires one VoIP channel and one FoIP channel in the system. Both VoIP and FoIP channels take up DSP resources. The following rule applies to FoIP channels: Not all DSP resources can be used for FoIP and the number of possible FoIP channels depends on the system.
- A FoIP compound needed bandwidth resources. The bandwidth model is dimensioned in such a way that, in the same way as for Fax-over-VoIP connections, the bandwidth requirement of G.711 is used with 20 ms frame length over the entire routing path (see also "Bandwidth Control", page 69).

Establishing an FoIP connection in the AIN

An FoIP connection is set up as follows:

- The criteria concerning when the Master attempts to establish an FoIP connection with T.38 are listed in Tab. 12 and on Tab. 13. The same table shows when the master first establishes a voice connection and only then attempts to change to a FoIP connection (use with combined units).

- The bandwidth control uses the same bandwidth values for a T.38 connection as for a G.711 connection with 20 ms.
- If the bandwidth calculation shows that enough bandwidth is available, an attempt is made to set up a fax connection:
  - If a free FoIP channel and a free VoIP channel are available at each node, the connection is set up as an FoIP connection.
  - If a free VoIP channel is available at each node, but not the two FoIP channels required, the connection is set up as a Fax-over-VoIP connection.
- If the bandwidth is insufficient or if the FoIP or VoIP channels available at the nodes are insufficient, the connection is not established, unless the PSTN overflow becomes active and attempts to establish the fax connection via the PSTN (see "PSTN overflow", page 42.

Restrictions:

Please note the following limitations when using FoIP:

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

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

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

- Fax over IP cannot be compressed in the same way as call data. For this reason fax data must always be transmitted with the non-compressing codec G.711. 20 ms is used as the frame length. With WAN links this influence the bandwidth dimensioning.
- Jitter, high delay values (in particular round-trip delay values) and packet loss can result in the direct loss of information during Fax over IP data transmission. For this reason prioritising VoIP in the IP network using QoS measures is particularly important (specially on WAN links with limited bandwidth). For the minimal requirements refer to Tab. 19.
- Fax machines that support standard T.30 - Annex A have a sufficiently large send and receive memory and retransmission function (ECM), and are able to correct

transmission errors up to a certain extent, where the protocol has to be supported by both fax machines involved.

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

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

1. Configure the fax connection as follows: *Fax device* = *Fax over VoIP (G.711)* (🔍*=sr*).
2. Check that there is sufficient bandwidth available on all the links between the fax machines. A calculation example is in "Fax over VoIP connection", page 73. Bear in mind that when you are using VPN it is not always the shortest link that is used (see "Using VPN", page 65).
3. Check whether QoS can be set up particularly on WAN links with limited bandwidth.
4. Make sure that WAN links without QoS are only used to transmit fax data from fax machines with sufficient memory and integrated retransmission function (ECM).
5. Check the reliability of the fax transmission with a test set-up.

4. 3 Region-related settings

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

- Configurable parameters (settings) which, once an AIN area is selected, can be allocated for the entire AIN or for individual nodes, trunk groups or users (see Tab. 15).
- Country-related, non-configurable system parameters which, once an AIN area is selected, can be allocated for the entire AIN or for individual nodes, trunk groups or users (see Tab. 16).
- Functions that can be configured depending on the region, without an AIN area being assigned (see "Configuration of region-dependent parameters", page 55).

4. 3. 1 AIN areas

An AIN area comprises a group of settings that differ from one region to the next (see Tab. 14).

Tab. 14 Parameters that can be set for each AIN area (🔍 =*zz*).

Parameter/parameter group	Explanation
AIN regions	Reference number of the AIN area.
Name	Name of the AIN area
Country	The values of the country-related, non-configurable parameters are determined by the selection of the country (Tab. 16). After the first start the country of the AIN area 1 corresponds to the country stored on the EIM card.
Time zones	+/- deviation from the Master's time
Own regional prefixes	International and national prefix, country code and toll area code
Call logging	Various settings for the output of the call charge information
Loop break signalling	Settings for analogue exchange and terminal interfaces

Each node is necessarily allocated an AIN area. After the first start this is the AIN region 1. After the first start that area is an area. If a satellite is situated in an area that requires other settings, you need to create a new AIN area, modify the settings and allocate the new AIN area to the node.

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

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

Tab. 15 lists the configurable parameters which, once an AIN region is selected, can be allocated for the entire AIN or for individual nodes, trunk groups or users.

Tab. 15 Potential allocation of configurable parameters of an AIN area

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

Tab. 16 lists the country-related, non-configurable system parameters which, once an AIN region is selected, can be allocated for the entire AIN or for individual nodes, trunk groups or users.

Note:

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

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

Tab. 16 Possible allocation of the country-related, non-configurable system parameters

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

The scope can be determined in part using the configuration:

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

Tab. 17 Allocation examples of AIN areas

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

4. 3. 2 Configuration of region-dependent parameters

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

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

Tab. 18 Parameters which can be defined depending on the region through configuration

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

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

4. 4 Satellite in Offline Mode

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

Switching to offline mode and back to AIN mode

The switchover to the offline mode is as follows:

- The signalling connections between Master and satellites are permanently supervised by connection monitors.
  The monitoring interval can be configured and ranges from a few seconds to several minutes (*Monitoring interval*). 🔍 *=3q*

- As soon as the connection monitors of the Master and the satellite concerned detect an interruption, the satellite is restarted. The Master deactivates the AIN configuration data of this satellite and generates the event message *Node x lost*. If configured, a user-definable text is displayed on the system phones during offline operation (see also "Configuring offline operation", page 56)
- The satellite restarts and loads the offline configuration data, and starts up offline operation. The offline mode is signalled in the operation status indication (Mitel 415/430: green/orange flashing SYS LED. Mitel 470: *Offline* is indicated on the user interface.

The switchover to the AIN mode is as follows:

- During offline operation the satellite regularly tries to re-establish contact with the Master.
- The satellite is restarted after its connection monitor has established contact with the Master over a minimum duration.
- When it starts up, the satellite logs back on with the Master and resumes AIN operation. The Master generates the event message *Node x reestablished.*

4. 4. 1 Configuring offline operation

Configure offline operation in accordance with the Chapter "Configuring offline operation for the satellites", page 37. Please note the following points:

- Numbering plan:
  Assign the users the same call numbers as in the AIN operating mode so that the users on the satellite can be reached on the usual numbers in offline mode.
- Routing:
  If the satellite has an exchange line circuit: For the most important users at the other nodes set up virtual PISN users that can be dialled via the public network. Allocate the PISN users the same call numbers as those used by the corresponding users in the AIN. Your internal contact partners connected to a different node can then still be reached on the usual call numbers.
  Tip: Instead of setting up a separate PISN number for each user, you can define a PISN number with a wildcard that covers all the users. For instance PISN number 3xx covers all the internal users from 300 to 399. For more information on this subject please refer to “System Functions and Features on MiVoice Office 400” in the System Manual.
- IP system phones
  The IP system phones are logged on to the Master in principle and cannot be configured for an offline mode. For the exception see "IP system phones in offline mode", page 58.

- Cordless phones:
  The cordless phones are registered with the master server in regular AIN operation mode. To ensure the cordless phones can be used also in offline mode, register the handsets in offline mode of the satellites with the DECT system.
  Register the cordless phones using a system other than in the Master (e.g. System B) and set the cordless phones on *System* = *Auto* so that the cordless phones automatically log on to the active system.
- Displaying the offline mode:
  You can use the idle text of the system phones to display a text in offline mode (🔍 *Set idle text globally*).

4. 4. 2 Restricted functions in offline mode

The following functions are not available in offline mode:

- Voice mail: The voice mail system is set up centrally on the Master for the entire AIN and is not available to a satellite operating in offline mode.
- All the properties licensed centrally in the Master for the AIN mode Exceptions: The licensed voice channels for VoIP, SIP access and QSIG are enabled for 36 hours so that connected IP terminals or QSIG nodes are available also in offline mode, provided they have been configured accordingly (refer to your communication server's system manual).
- Mitel 470 only: All the applications of the CPU2 application card (provided one is used in the master).
- OIP server and all OIP-based applications
- TWP with all modules
- Server-based third-party applications
- PSTN overflow

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

- External phone traffic:
  If the satellite does not have its own exchange line circuit, users on the satellite can no longer be reached directly from the outside.
- DECT system:
  Only those cordless phones that are registered for offline operation are recognised by the communication server.
- IP system phones
  Only those IP system phones that are registered for offline operation are recognised by the communication server (see "IP system phones in offline mode", page 58).

4. 4. 3 IP system phones in offline mode

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

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

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

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

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

Logon procedure in AIN operating mode

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

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

Switching to offline mode

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

- After contact with the Master is lost, the satellite runs a restart and starts in offline mode (see "Satellite in Offline Mode", page 55).
- The IP system phone also carries out a restart and tries to log on to the satellite.
- As soon as the satellite has adopted the offline mode, the IP system phone can log itself on. The satellite then controls it during offline operation.

Switching to AIN mode

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

- The satellite restarts and starts up in AIN mode.

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

4. 5 Restricted functions in the AIN

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

ISDN data services

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

CLIP/CNIP of Abbreviated Dialling Numbers

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

Priority exchange allocation

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

Key telephones and operator consoles

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

5 Network Environment

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

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

5. 1 IP network requirements

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

General requirements

- Ethernet 100Base-T (or higher) /full-duplex If you avoid the use of the *Auto* setting and you set instead a permanent value, the voice quality is increased.
- Sufficient bandwidth throughout the AIN.
- Use of network components with high fail-safe reliability.
- Use of standardized and compatible network components:
  Whenever possible use components made by the same manufacturer for the same functions. Thoroughly test the interplay between components made by different manufacturers under laboratory conditions first before deploying them.
- Use of Layer 2 network components that allow a VLAN configuration. Avoid the use of hubs
- Integrate the IP hardphones in a WLAN (recommended if you are using several IP hardphones, see "QoS on layer 2 with VLAN", page 62)
- Use of Layer 3 network components that support prioritization using the DiffServ method see "QoS on Layer 3 with DiffServ (Differentiated Services):", page 62.
- Administration access to the relevant network components, e.g. access to the DHCP server to configure the DHCP options or access to the port configuration of firewalls (see "TCP/IP Ports and Firewall", page 85).

Special requirements for WAN links over the internet

- Use of VPN connections.
  Try and implement VPN connections with a single internet provider whenever possible. This simplifies the routing of calls in the IP network (see "Using VPN", page 65).
- No dial-up connections:
  High costs will be incurred if the communication server periodically contacts the satellites and IP system phones via a dial-up connection.

5. 1. 1 Delay and jitter

High delay and jitter values have a hugely detrimental effect on the call quality.
The delay values for the voice packets should be kept as small as possible. Take note of the minimum requirements for operating an AIN in Tab. 19.

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

- Prioritizing the voice packets before other data packets: see Chapter ("Prioritization and QoS", page 62).
- Jitter management:
  Compensation of the time fluctuations between the arrival of individual packets (jitter management) is automatically regulated in the AIN and does not require any additional settings. The better the jitter is compensated, the larger the delay values. The dejitter buffers used therefore adapt their size dynamically to the situation and ensure a balanced ratio between jitter and delay.
- Fragmenting the IP packets:
  Large data packets increase the delay of waiting voice packets. By fragmenting large packets into several small packets, prioritized voice packets can be sent through in between the data packets.
- Frame length of voice packets:
  The smaller the frame length of voice packets, the smaller the delay values generated but the greater the bandwidth requirement. For this reason we recommend that the frame length of voice packets be kept relatively small within the LAN area and relatively large for WAN connections with limited bandwidth (🔍 *Preferred frame length*).

Tab. 19 Key data for operating an AIN

Property	Value
Roundtrip Delay	< 100 ms
Jitter voice data	< 20 ms
Jitter fax data	< 5 ms

Property	Value
Packet lost voice data	< 1%
Packet lost fax data	< 0.1%
Consecutive Packet Loss	< 2 packets (non consecutive)

5. 2 Prioritization and QoS

In order to ensure that an IP network with limited bandwidth resources can also supply the necessary bandwidth for call connections, the voice packets should be separated and prioritised over other data packets.

QoS on layer 2 with VLAN

If several IP hardphones are used locally, it is recommended to separate the call data from the other data on the IP network and set up a VLAN. Set it up using VLAN-compatible switches and connect the communication server and the IP hardphones to the ports configured for this VLAN (see Tab. 20).

Tab. 20 VLAN configuration)

AIN element	VLAN configuration
Switch	Configure VLAN with the following ports: • Access port for communication server (node) • Trunk port for IP hardphones
Communication server	*Frame type* = *Standard (no QoS)* (🔍 *=48*) **Note:** This setting allows you to switch off the CoS and VLAN functionality of the communication server . This is available for reasons of compatibility with older systems and normally not used.
IP hardphones	Assign the intended VLAN to the telephone. This setting can be carry out locally on the phone or via DHCP options ("DHCP options", page 85). If necessary, you can also assign the PC port to an (other) VLAN.

As IP softphones are connected with the IP network via a computer's Ethernet interface, they cannot be integrated into the VLAN.

QoS on Layer 3 with DiffServ (Differentiated Services):

The DiffServ method is used for the classification and prioritisation of data on the IP network, and is particularly recommended for WAN links. In so doing, it interprets the value of the first six bits of the ToS field as the DSCP class. In theory, it can differentiate between up to 64 classes. The standardised values are listed in the Internet standard documents rfc-2597 and rfc-2598.

From R2.1 onwards, the data for signalling, language and video can be classified individually. For FoIP (T.38), the DSCP class of the language applies.

DSCP classes have to be defined in the master. The master then transmits the values automatically to the satellites and the IP system phones and Mitel SIP phones.

Prioritization takes place in the routers or in Layer 3 switches. The routers or Layer 3 switches used must therefore support DiffServ in general and the selected DSCP classes in particular and must be configured accordingly.

Tab. 21 Recommended DiffServ settings (*VoIP* view, *QoS settings* 🔍 *=48* section)

Parameter	Parameter value[1]
Layer 3: DSCP signalling	*40*
Layer 3: DSCP voice	*46*
Layer 3: DSCP video	*34*

[1] All here correspond to the standard values.

QoS on layer 3 with ToS

With the ToS method (RFC 791, page 11 and RFC 1349), the same six bits in the ToS/DSCP field are interpreted as in the DiffServ method (RFC 2474).

The ToS method interprets the first three bits (priority) in order to specify the priority level. With bit three to five, the transmission can be optimised according to one of the following criteria: High throughput, high reliability or low latency. The routers used must thus support ToS prioritisation and be configured accordingly. Non-prioritised data packets are given the standard priority by the router.

Using the following table, DiffServ classes can be converted to ToS values and vice versa. Example: DiffServ class 46 corresponds to ToS prioritisation *Critical* and the ToS service type *High Througput and Low Latency*.

Tab. 22 Conversion table DiffServ/ToS

ToS service type (right) ToS prioritisation (bottom)	Standard Service	High Reliability	High Throughput	Low Latency	High Throughput / Low Latency
Best Routine	0	1	2	4	6
Priority	8	9	10	12	14
Immediate	16	17	18	20	22
Flash	24	25	26	28	30
Flash Override	32	33	34	36	38
Critical	40	41	42	44	46
Internetwork Control	48	49	50	52	54
Network Control	56	57	58	60	62

5. 3 Encrypted transmission

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

You can also choose for each node whether to use a non-encrypted or an encrypted transmission method.

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

Tab. 23 Configuration parameter for specifying the transmission method

VoIP mode	Encrypted transmission	Non-encrypted transmission
Node connections in Mitel Plan	secure G.711 secure G.711/G.729	G.711 G.711/G.729
DSP configuration *VoIP encryption (SRTP)* (🔍 *=3n*)	☑	□
Configuration of IP security: *VoIP mode* (🔍 *=ym*)	*secure G.711* *secure G.711/G.729*	*G.711* *G.711/G.729*
Licensing (🔍 *=q9*):	Licence *Secure VoIP* per node	-

The IP system phones are switched over automatically.

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

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

For WAN links over the internet we also recommend that you set up a VPN (see Chapter "Using VPN", page 65) or use dedicated leased lines.

5. 3. 1 Other encryption methods

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

Voice data encryption

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

Signalling data encryption

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

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

5. 4 Using VPN

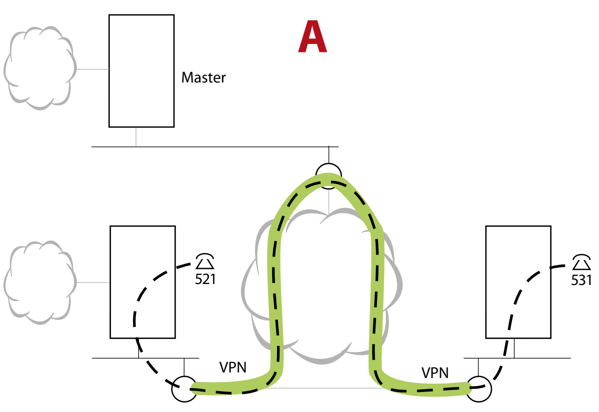
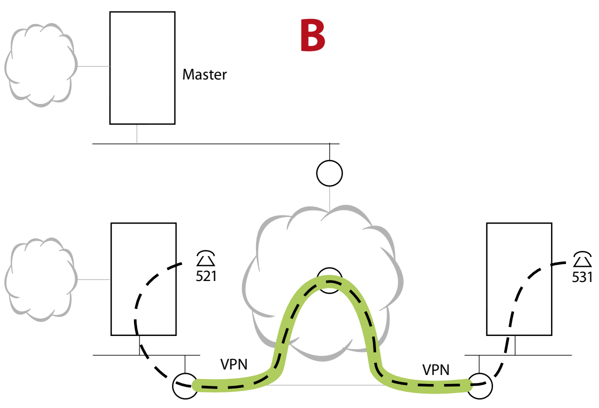
When you encrypt voice data in the AIN, it is encrypted within the LAN but not necessarily on WAN links. If a connection runs for example to a remote IP system phone via various internet providers, the voice data on the internet is not automatically encrypted. To encrypt the entire link you also need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

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

A simple VPN connects only two terminals or two locations with each other (see Tab. 24, variant A). To connect several terminals or locations with one another via VPN, you can make use of the VPN services of the internet provider (see Tab. 24, variant B).

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

Tab. 24 Possible VPN configurations in the AIN

	Simple VPN connections: A VPN connection to the master location is set up for each remote IP system phone and for each remote satellite. For a call connection between User 521 and User 531 the WAN link to the router at the master location is charged with 2 VoIP connections.
	Routed VPN connections or VPN connections with any-to-any connectivity: The internet provider routes the VPN connections. For a call connection between User 521 and User 531 the WAN link to the router at the master location is not charged.

5. 5 Methods for Reducing Bandwidth Requirements

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

- Using codecs to compress voice data: On a WAN link with limited bandwidth it is advisable to use a compressing codec such as G.729. It considerably reduces the bandwidth requirement and the loss of voice quality remains tolerable.

In the LAN area there is usually sufficient bandwidth available and better results are achieved with the uncompressed codec G.711 as the voice quality is not affected by a compressing method.

- Compressing the IP header:
  Voice packets are relatively small compared with their header (large overhead). On a point-to-point connection between two routers the header can be considerably compressed. The bandwidth resources available are then used more sparingly. The setting is made in the router. Possible method: CRTP compression. This method has to be supported and featured by the internet service provider for WAN links via the internet.
- Frame length of voice packets:
  The smaller the frame length of voice packets, the smaller the delay values generated but the greater the bandwidth requirement. For this reason we recommend that the frame length of voice packets be kept relatively small within the LAN area and relatively large for WAN connections with limited bandwidth.

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

Tab. 25 Usual settings in practice

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

5. 5. 1 Calculating the bandwidth requirements

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

Tab. 26 Formula for calculating the required bandwidth

$BW = n \cdot \left(\frac{PS + L2 + AP}{FL} \right)$	**BW**	:	Bandwidth requirement [kbit/s]
	PS	:	Packet size [Byte]
	L2	:	L2 overhead [Byte]
	AP	:	Authentication prefix (SRTP) [Byte]
	FL	:	Frame length [Byte]
	n	=	**7.8125** (conversion factor byte/ms → kbit/s)

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

Tab. 27 Table of values for packet size PS

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

Tab. 28 Table of values for L2 overheads

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

Tab. 29 Table of values for authentication prefix AP

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

Note:

The calculated bandwidth requirements apply only to the requirements for call connections. When rating a WAN link you also need to take account of the estimated requirements for data transmission just like, with video telephony, the estimated video data requirement. The bandwidth requirements for the exchange of signalling data between Master and satellites are relatively small and can be covered with a reserve supplement of one additional VoIP channel at most (G.711).

5. 6 Bandwidth Control

The available bandwidth on the IP network for a call connection can be very different as the connection may pass through different LAN areas and WAN links. Bandwidth control determines for each connection the optimum transmission parameters and monitors the number of simultaneous connections and their bandwidth requirement. If there is not enough bandwidth for another connection, said connection is not set up.

Bandwidth control depends on bandwidth model. This should actually reflect the bandwidth situation as much as possible.

Bandwidth model

In each case it calculates before a connection is set up whether or not the bandwidth available is sufficient. If not, the connection is not set up and the user obtains the congestion tone. The better the model simulates reality, the more reliably the bandwidth resources can be managed.

The model consists of bandwidth areas and WAN links. A bandwidth area is a network section with the same bandwidth properties. In most cases it is a LAN but the internet as a whole is also mapped as a bandwidth area.

A WAN link connects two bandwidth areas. Usually they consist of connections to an internet provider or leased lines. Frequently they have a limited bandwidth.

The WAN links are assigned to the bandwidth areas on the VoIP routing table. In the process the necessary WAN links are selected from a bandwidth area in order to set up a connection to each desired destination.

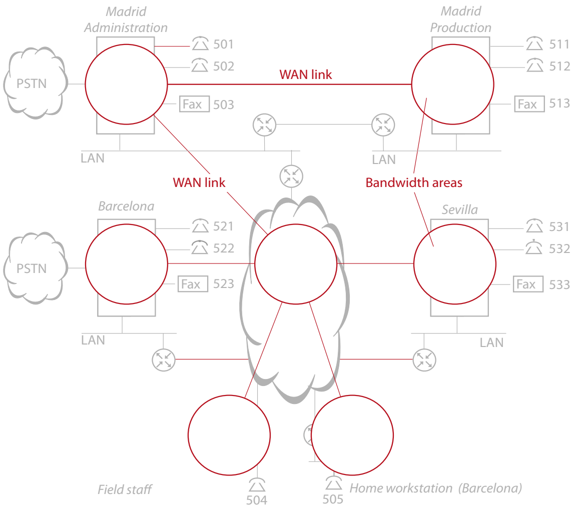


Fig. 13 **Model for bandwidth control**

5. 6. 1 Bandwidth control illustrated with an example

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

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

  Exception: In the case of a Fax over VoIP connection, calculations always involve codec G.711 and frame length 20 ms over the entire routing path, irrespective of the available bandwidth. In this way the best quality fax transmission is also guaranteed with the Fax over VoIP transmission type (see "Fax date transmission in the AIN", page 49).
- The bandwidth control calculates the bandwidth requirements of a connection for each WAN link on the routing path. To do so it uses the values from Tab. 28 and Tab. 27 as well as the bandwidth calculation formula on Seite 68.
- The bandwidth control checks whether or not the bandwidth required for audio stream is available. If so, the connection is set up. If not, the caller obtains congestion tone and a system message is generated.

Note:

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

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

5. 6. 1. 1 Single ringing tone

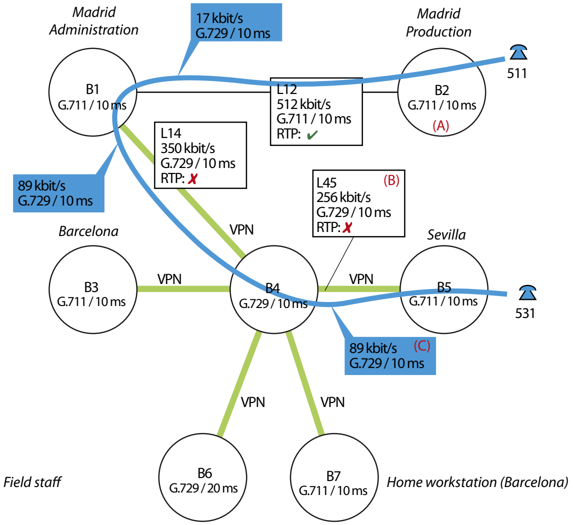
User 511 on satellite1 (Madrid Production) calls user 531 on satellite 3 in Seville (see Fig. 14).

Assumptions:

- PPP is used as the transmission protocol on the WAN links.
- Routed VPNs are used for the WAN links via the internet as indicated in Tab. 24, variant B).

Sequence:

- The bandwidth control selects the most space-saving variant of the codec and frame length on the routing path. G.711 / 10 ms could be used in the bandwidth areas and on the L12 link. However as the same settings have to apply for the entire connection, bandwidth control uses the more space-saving setting G.729 / 10 ms of WAN link L14 and L45.
- The bandwidth requirements on the WAN links L12, L14 and L45 are now calculated (see Tab. 30)
- On all three WAN links the bandwidth requirements are less than the available bandwidth so the connection is set up.



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

(C)

Codec / frame length actually used and resulting bandwidth requirements.

(B)

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

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

Tab. 30 Automatic calculation of the bandwidth requirements on the WAN links

WAN link	L2 overhead	Packet size	Frame length	Bandwidth		
				Requirement	Available	Free
	→Tab. 28	→Tab. 28		→Seite 68		
L12	6	16	10	17	512	495
L14	62	52	10	89	350	261
L45	62	52	10	89	256	167

5. 6. 1. 2 Second call via the same link

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

Assumptions:

- PPP is used as the transmission protocol on the WAN links.
- Routed VPNs are used for the WAN links via the internet as indicated in Tab. 24, variant B).

Sequence:

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

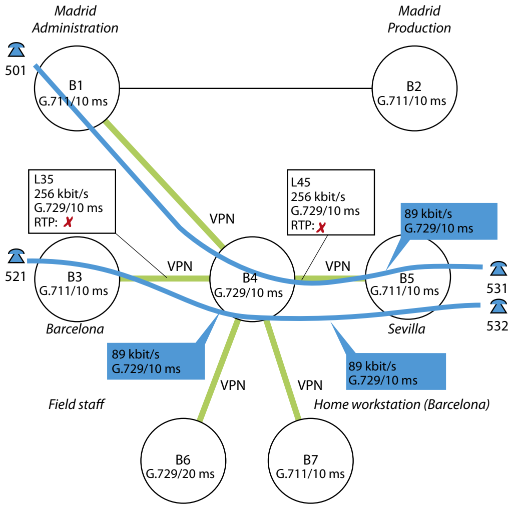


Fig. 15 Example of a connection set-up via WAN links L14 and L45

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

Call connec-tion	WAN link	L2 overhead	Packet size	Frame length	Bandwidth		
					Require-ment	Available	Free
		→Tab. 28	→ Tab. 27		→Seite 68		
501 ↔ 531	L45	62	52	10	89	256	167
532 ↔ 521	L45	62	52	10	89	167	78
532 ↔ 521	L34	62	52	10	89	256	167

5. 6. 1. 3 Fax over VoIP connection

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

Assumptions:

- PPP is used as the transmission protocol on the WAN links.
- Routed VPNs are used for the WAN links via the internet as indicated in Tab. 24, variant B).

Sequence:

- The bandwidth control selects the codec and frame length required for Fax over VoIP connections (G.711 / 20 ms).
- The bandwidth requirements on the WAN links L14 are now calculated (see Tab. 32).
- The bandwidth required is less than the available bandwidth and so the connection is set up.

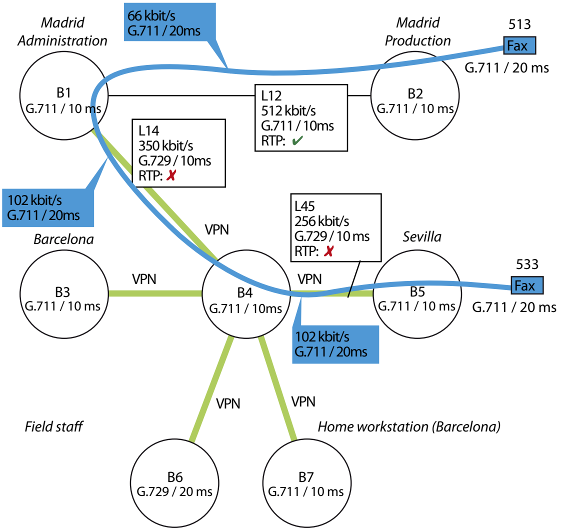


Fig. 16 Example of a connection set-up to an IP system phone

Tab. 32 Automatic calculation of the bandwidth requirements on WAN link L14

WAN link	L2 overhead	Packet size	Frame length	Bandwidth		
				Require-ment	Available	Free
	→Tab. 28	→Tab. 27		→Seite 68		
L12	6	164	20	66	512	446
L14	62	200	20	102	350	204
L45	62	200	20	102	256	154

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

5. 6. 1. 4 Call to an external SIP user

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

Assumptions:

- PPP is used as the transmission protocol on the WAN links.
- Routed VPNs are used for the WAN links via the internet as indicated in Tab. 24, variant B).
- The staff in Seville does not have direct internet access.

Sequence:

- The bandwidth control selects the most space-saving variant of the codec and frame length on the routing path. In this example this is G.729 / 10ms.
- The bandwidth requirements on the WAN links L45 and L14 are now calculated (see Tab. 33)
- The bandwidth required is less than the available bandwidth and so the connection is set up.

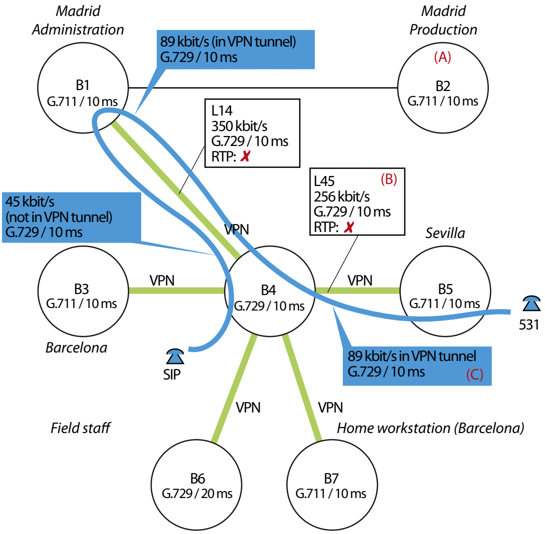


Fig. 17 Example of a connection set-up to an SIP phone

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

WAN link	L2 overhead	Packet size	Frame length	Bandwidth		
				Requirement	Available	Free
	→Tab. 28	→Tab. 27		→Seite 68		
L45	62	52	10	89	256	139
L14 VPN	62	52	10	89	350	261
L14	6	52	10	45	259	214

5. 6. 1. 5 Video call

A video call requires additional bandwidth for video data transmission (video stream), but no additional DSP resources, since video stream is not implemented via the communication server. The bandwidth requirement for video in the bandwidth model is considered as 2nd priority in the calculation: If enough bandwidth is not available for video stream, the connection is set up without video.

To prevent a WAN link from being blocked by a video call, you can reserve a minimum bandwidth requirement for audio stream. The minimum requirement must be such that the required number of simultaneous connections can be set up as audio connections.

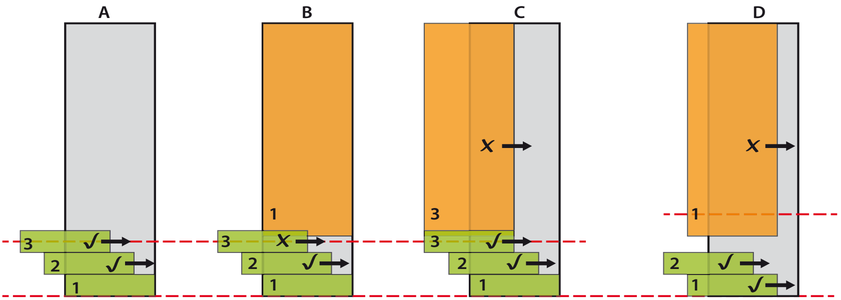


Fig. 18 Handling the video stream in bandwidth control

Tab. 34 Legend and explanations

□	Available bandwidth	🟧	Video stream of a call
═	Reserved bandwidth for audio (*Reserved bandwidth for audio* 🔍 *=q2*)	✓→	This connection or connection part can be set up.
🟩	Audio stream of a call	✗→	This connection or connection part cannot be set up.
A	One audio connection is set up, two others are added.		
B	One video connection is set up, a second audio connection is added, a third audio connection can no longer be set up.		

C	One audio connection is set up, another one is added. The third call is a video call. Due to lack of space, this is only set up as audio connection.
D	A video call is set up as audio connection since the bandwidth required for video stream is larger than the available bandwidth. A further audio call can be set up.

5. 6. 2 Creating the bandwidth model

The model is created step by step:

- Determining the bandwidth topology, Seite 77
- Configuring the bandwidth areas, Seite 78
- Configuring the WAN links, Seite 79
- Configuring the VoIP routing table, Seite 80

5. 6. 2. 1 Determining the bandwidth topology

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

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

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

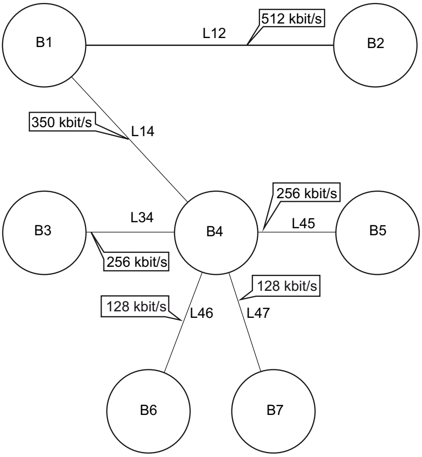


Fig. 19 Bandwidth areas and WAN links based on the example of the reference network

5. 6. 2. 2 Configuring the bandwidth areas

The instructions below explain the procedure for configuring the bandwidth areas (*Bandwidth areas* 🔍 *=q2*).

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

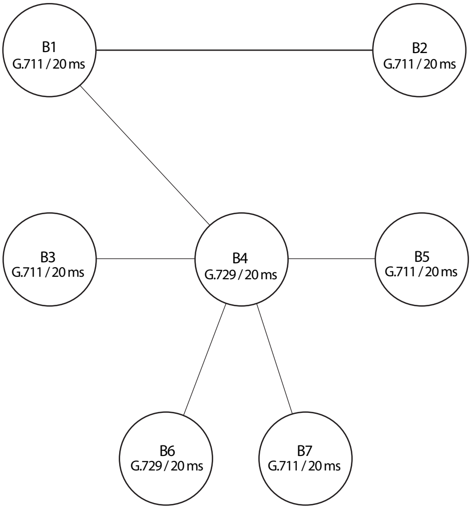


Fig. 20 Bandwidth control based on the example of the reference model

Tab. 35 Bandwidth area settings

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

5. 6. 2. 3 Configuring the WAN links

The instructions below explain the procedure for configuring the WAN links (*WAN links* 🔍 *=q2*).

1. First open one or more WAN links to the bandwidth area of the communication server/Master. Enter as available bandwidth the values fixed in the bandwidth topology.
2. Define the WAN link parameters. Fix the codec and frame length based on the available bandwidth.
3. Open and configure the remaining WAN links.

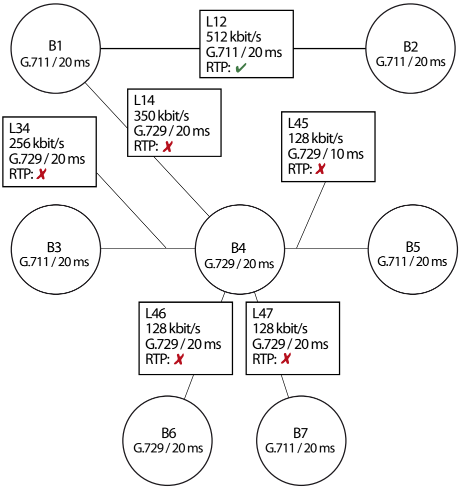


Fig. 21 Bandwidth control based on the example of the reference model

Tab. 36 WAN link settings

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

5. 6. 2. 4 Configuring the VoIP routing table

One entry in the VoIP routing table specifies which WAN link is to be used between two neighbouring bandwidth areas (*VoIP routing* 🔍 *=q2*).

The entries are specified for each bandwidth area. The following rules apply to the entries:

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

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

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

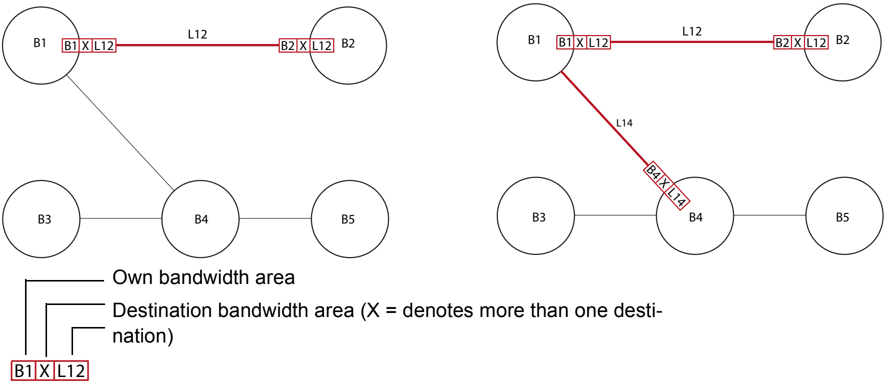


Fig. 22 Automatically generated entries when the WAN links L12 (left) and L14 (right) are created

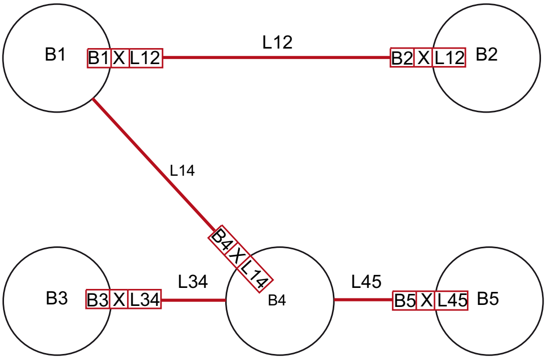


Fig. 23 Automatically generated entries when all the WAN links are created

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

1. Process all the entries one after the other until they comply with Fig. 24 and Tab. 37.
2. Repeat this step for all the bandwidth areas.

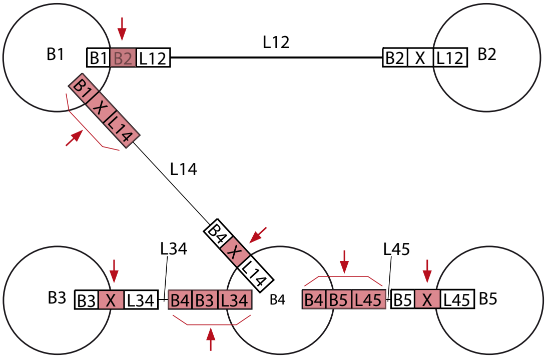


Fig. 24 Completed entries in the VoIP routing table illustrated in a diagram

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

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

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

If VPNs are used on the WAN links, the end of the VPN tunnel (*VPN peer*) must also be entered (see Tab. 38 and Tab. 39).

Tab. 38 VoIP routing table with VPN connections in accordance with Tab. 24, variant A

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

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

Tab. 39 VoIP routing table with VPN connections in accordance with Tab. 24, variant B

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

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

6 Annex

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

6. 1 Permanent parameters

The following parameters are set permanently and cannot be modified.

Tab. 40 Permanent parameters that cannot be set

Parameter	Parameter values
Silence Supression	Off
Echo Cancellation	On

6. 2 TCP/IP Ports and Firewall

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

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

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

6. 3 DHCP options

Vendor class identifier (Option 60)

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

Tab. 41 Option 60: Vendor class identifier for the IP system terminals

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

Tab. 42 Option 60: Vendor class identifier for Mitel SIP phones

IP system terminal	Vendor class identifier
Mitel 6753 SIP	AastraIPPhone53i
Mitel 6755 SIP	AastraIPPhone55i
Mitel 6757 SIP	AastraIPPhone57i
Aastra 6730i	AastraIPPhone6730i
Mitel 6731 SIP	AastraIPPhone6731i
Mitel 6739 SIP	AastraIPPhone6739i
Mitel 6863 SIP	AastraIPPhone6863i
Mitel 6865 SIP	AastraIPPhone6865i
Mitel 6867 SIP	AastraIPPhone6867i
Mitel 6869 SIP	AastraIPPhone6869i
OMM RFP	OpenMobility

Vendor-specific information (Option 43)

If the DHCP server is able to assign an address request to an IP system phone using the vendor class identifier, it sends it not only the address co-ordinates but also the configured vendor specific information. The information consists of phone configuration parameters. Use the information contained in Tab. 43 to map the required parameters in a DHCP server configuration.

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

Attribute	Option code	Hex	Length (octet)	Type	Explanation
PBX_ADDRESS	03	$03	4	UINT32	IP address of the communication server
SIP_PORT_PBX	04	$04	2	UINT16	SIP port of the communication server
SIP_PORT_PHONE	05	$05	2	UINT16	SIP port of the IP system phone
VLAN_PRIO	07	$07	1	UINT8	VLAN priority of the IP system phone (0 to 6)
VLAN_ID/VLAN_ENABLED	08	$08	2	UINT16	VLAN ID of the system phone (values between 0 and 4094, with value 0 deactivating the VLAN)

Attribute	Option code	Hex	Length (octet)	Type	Explanation
VLANPC_PRIO	09	$09	1	UINT8	VLAN priority of the PC interface on the IP system phone (0 to 6)
VLANPC_ID/VLANPC_ENABLED	10	$0A	2	UINT16	VLAN ID of the PC interface on the IP system phone (values between 0 and 4094, with value 0 deactivating the VLAN)
VLAN PC port TAGS	11	$0B	1	UINT8	VLAN tag of the PC interface on the IP system phone: 1 = activated 0 = deactivated

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

```
# This is a sample configuration file for the Aamadeus IP
phones.
# Depending on the Vendor Class Identifier different options are
# set.

# The Vendor Class for the Aamadeus IP phone
Option 60 == Aamadeus IP Phone

{
# Vendor specific information:
# PBX IP address: Code 0x03; Length 4; 172.020.054.001
# --> Hex string: 0x0304AC143601
# SIP Port PBX: Code 0x04; Length 2; 18060
# --> Hex string: 0x0402468C
# SIP Port Phone: Code 0x05; Length 2; 18060
# --> Hex string: 0x0502468C
# Put hex string parts together to get the whole option 43
string:
Option 43 = 0x0304AC1436010402468C0502468C
}
# From here on another vendor class can be defined.
```

Index