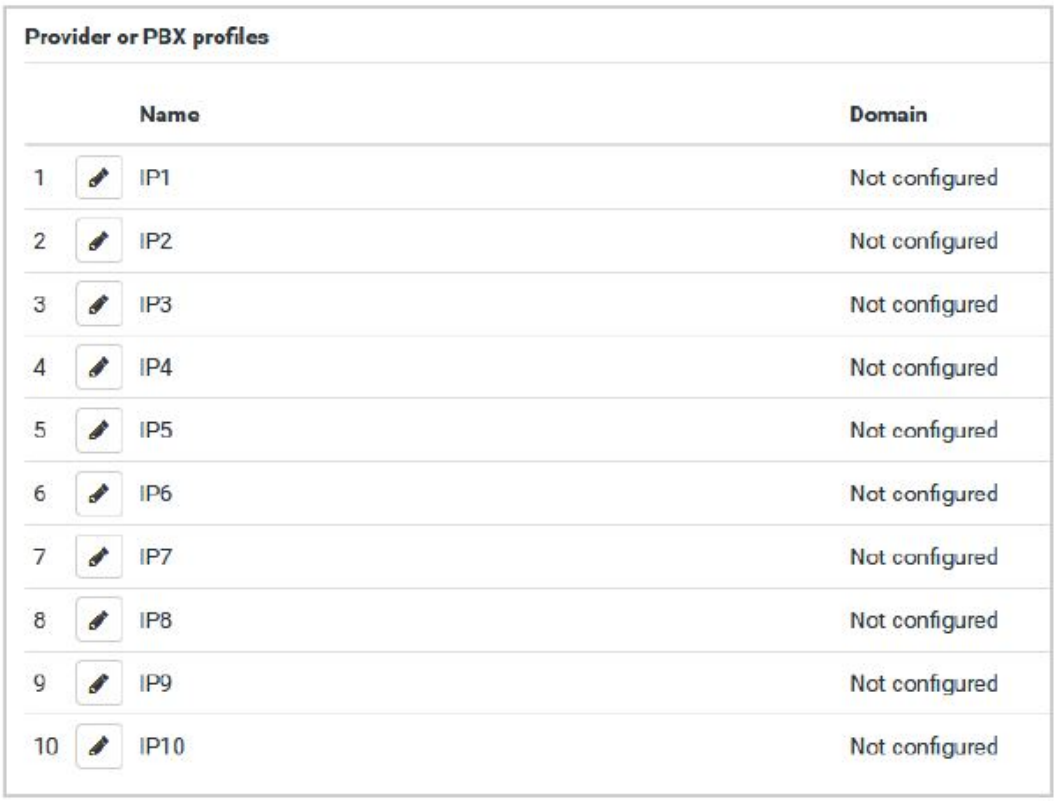
FAQ Nx70 - Provider and PBX profiles

Provider and PBX profiles

Valid for:	
N670	N870

You can use up to ten (with firmware 2.36.0 twenty) different VoIP PBX (Telephony Server) or VoIP provider profiles.

In the web-interface go to: **Settings Provider or PBX profiles**



The page lists the available VoIP connections.

Name:

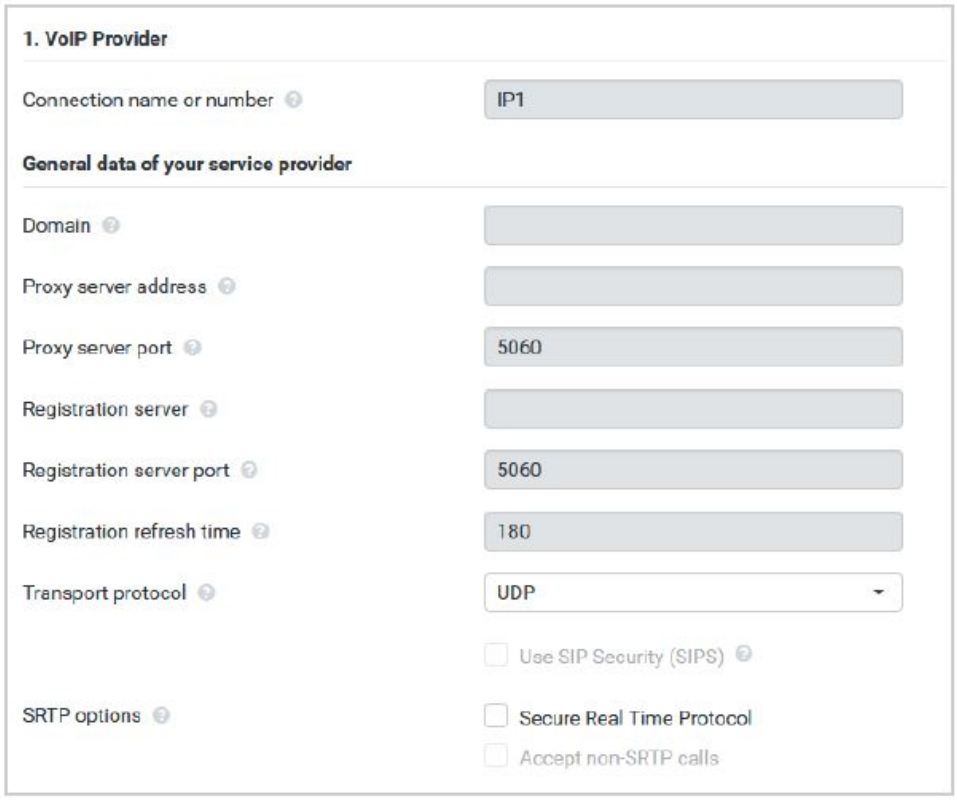
- The name that you have defined for the connection is displayed, or the default name (IP1 - IP20). It can be edited.

Domain:

- Domain part of the user address. In the case that a connection is not used Not configured is displayed.

Configuring provider and/or PBX profiles

Click on  next to the name of the VoIP connection you want to edit the provider/PBX configuration page is opened.



On this page you can edit the data for the selected telephony server profile.

Enter a name for the provider or PBX profile. This name is shown in the Provider/PBX list. To distinguish between different connections it should specify the respective VoIP service provider.

Examples: sip.domain.net for john.smith@sip.domain.net

10.100.0.45 for 02871913000@10.100.0.45

Proxy server address

The SIP proxy is your VoIP provider's gateway server and the first SIP server, where the device should send SIP requests and expects to receive requests.

- Enter the IP address or the (fully qualified) DNS name of your SIP proxy server (max. 74 characters, 0 - 9, a - z, A - Z, -, ., _).

Examples: **10.100.0.45** or **sip.domain.net** or **sipproxy01.domain.net**

Proxy server port

- Enter the port number of the first SIP server, where the device should send SIP requests and expects to receive requests.

Range: 1-65535; Default: 5060 (for UDP/TCP), 5061 (for TLS)

DNS SRV SIP server redundancy lookup might provide a different server port which is used then.

Registration server

The registration server assigns the public IP address/port number that was used by the phone on registration to your SIP address (username@domain). With most VoIP providers, the registrar server is identical to the SIP server. But it is also possible to address another service for registrationof this account.

- Enter the IP address or the (fully qualified) DNS name of the registration server. (max. 74 characters, 0 - 9, a - z, A - Z, -, ., _)

Examples: 10.100.0.45 or sip.domain.net or sipproxy01.domain.net

Registration server port

- Enter the communication port used on the registrar.

Range: 1-65535; Default: **5060** (for UDP/TCP), **5061** (for TLS)

Registration refresh time

- Enter the time intervals (in seconds) at which the phone should repeat the registration with the VoIP server (SIP proxy). A request will be sent to establish a session so that the phone's entry in the tables of the SIP proxy is retained and the phone can therefore be reached. The repeat will be carried out for all enabled VoIP connections.

Values: 1 - 5 digits, > 0; Default: 180 seconds

Transport protocol

- Select between UDP, TCP and TLS.

UDP:

(User Datagram Protocol) UDP is a non session-based protocol. UDP does not establish a fixed connection. The data packets ("datagrams") are sent as a broadcast. The recipient is solely responsible for making sure the data is received. The sender is not notified about whether it is received or not.

TCP:

(Transmission Control Protocol) TCP is a session-based transmission protocol. It sets up, monitors and terminates a connection between sender and recipient for transporting

TLS:

(Transport Layer Security) TLS is a protocol for encrypting data transmissions on the Internet.TLS is a superordinate transport protocol.

Use SIP Security (SIPS)

Only if TLS is selected. SIPS enhances SIP with TLS/SSL encryption. Using SIPS makes it more difficult to listen in on the connection. Data is transmitted encrypted over the internet.

- Mark/unmark the check box to enable/disable the use of SIPS.

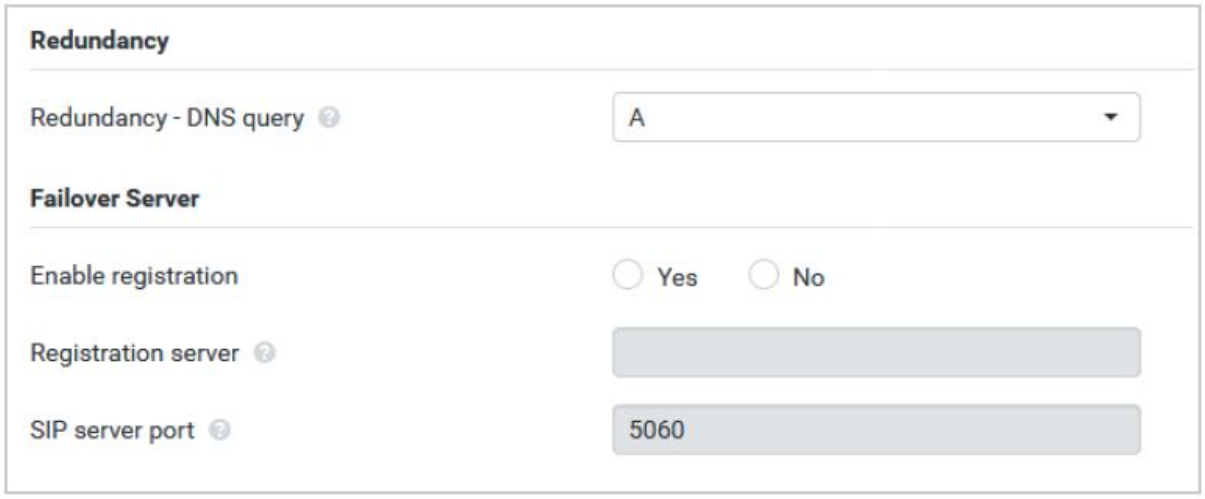
SRTP options

Only available if TLS is selected. SRTP (Secure Realtime Protocol) is a security profile to ensure confidentiality, integrity, replay protection and message authentication for audio-visual data transmission over IP-based networks.

- Select which calls should be accepted:

Secure Real Time Protocol Security is activated for voice connections.
Accept non-SRTP calls Insecure calls are accepted even when SRTP is activated.

Redundancy settings



Redundancy - DNS query

VoIP providers provide SIP server redundancy for load balancing and service reliability. SIP servers can be identified by DNS using different queries:

A Records just the specified IP addresses and the related port numbers.

SRV + A Finds an available server port for the specified proxy and registration server. DNS SRV allows a client to only have to know what type of service it is looking for instead of the actual server.

Failover server

If Redundancy - DNS query = A

In case your provider supports a failover server you can enter the data here.

- Enable/disable the use of a failover server via the radio boxes next to Enable registration.

Registration server

- Enter the IP address or the (fully qualified) DNS name of the failover registration server.

SIP server port

- Enter the communication port used on the failover registrar.

Range: 1-65535; Default: 5060 (for UDP/TCP), 5061 (for TLS)

Network data of the service provider

Outbound proxy mode

The DECT IP multicell system allows you to configure an outbound proxy. Despite of any other SIP protocol rules, if activated (Always), the system will always send all outgoing requests towards this outbound proxy. It can be an outbound proxy in the local network provided by the local network provider or in the public network provided by the network/VoIP provider.

- Specify when the outbound proxy should be used.

Always: All signalling and voice data sent by the system is sent to the outbound proxy.

Never: The outbound proxy is not used.

If the further outbound proxy configuration is identical to the proxy and registrar configuration it is useless and will be ignored

> The DHCP option 120 ”sip server” sent by a SIP phone would internally overrule the outbound proxy address and port setting. Outbound proxy mode is still and exclusively in the hands of the local device administrator.
>
> By setting Outbound proxy mode to Never, you can prevent any usage of DHCP option 120 by the DECT VoIP phone. To allow for DHCP option 120, you should set Outbound proxy mode to Always.

Outbound server address

This is the address, where the device should send all SIP requests to and where (in case of successful registration) it expects to receive requests from.

- Enter the (fully qualified) DNS name or the IP address of your provider's outbound proxy.

Example: 10.100.0.45 or sip.domain.net or sipproxy01.domain.net.

If the Outbound server address field is empty, the system behaves independently of the selected mode, as with Outbound proxy mode = Never.

Outbound proxy port

This is the port number of the outbound proxy server, where the device should send all SIP requests to (and where it in case of successful registration expects to receive requests from)

- Enter the communication port used by the outbound proxy.

Range: 1-65535; Default: 5060 (for UDP/TCP), 5061 (for TLS)

Outbound proxy port is empty and Outbound server address is a name:

The RFC3263 rules will be used to locate SIP servers and select them for load balancing and redundancy.

Outbound proxy port is a fixed number:

The usage of DNS SRV records according to RFC3263 is blocked.

SIP SUBSCRIBE for Net-AM MWI

When activated a subscription is established for the purpose of receiving notifications about new messages on the network mailbox.

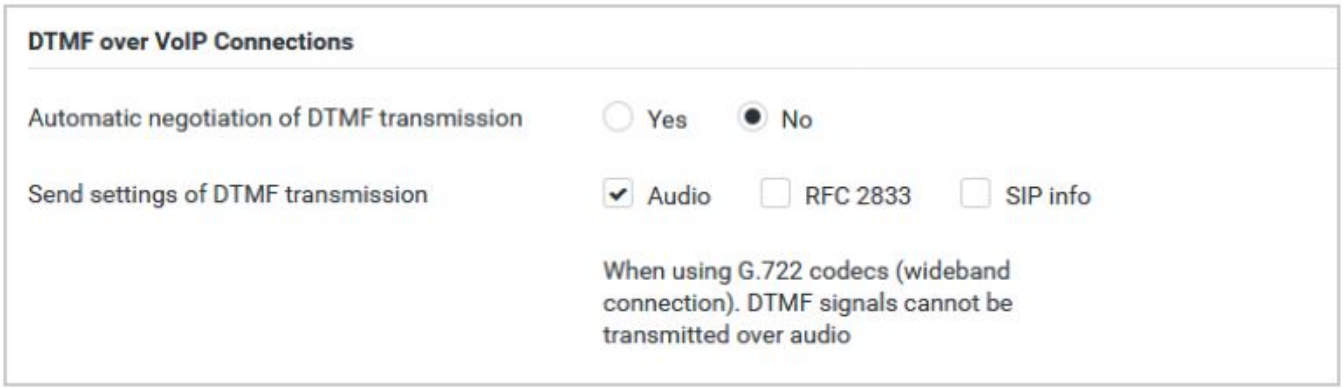
- Enable/disable SIP subscription via the radio boxes next to **SIP SUBSCRIBE for Net-AM MWI.**

DTMF over VoIP Connections

DTMF signalling (Dual Tone Multi Frequency) is required, for example, for querying and controlling certain network mailboxes via digit codes, for controlling of automatic directory enquiries or for remote operation of the local answering machine.

To send DTMF signals via VoIP, you must define how key codes should be converted into and sent as DTMF signals: as audible information via the speech channel or as a "SIP Info" message.

Ask your VoIP provider which type of DTMF transmission it supports.



Automatic negotiation of DTMF transmission

- For each call, the phone attempts to set the appropriate DTMF signalling type for the codec currently being negotiated: select Yes.
- Specify the DTMF signalling type explicitly: select No Select the send settings for DTMF transmission.

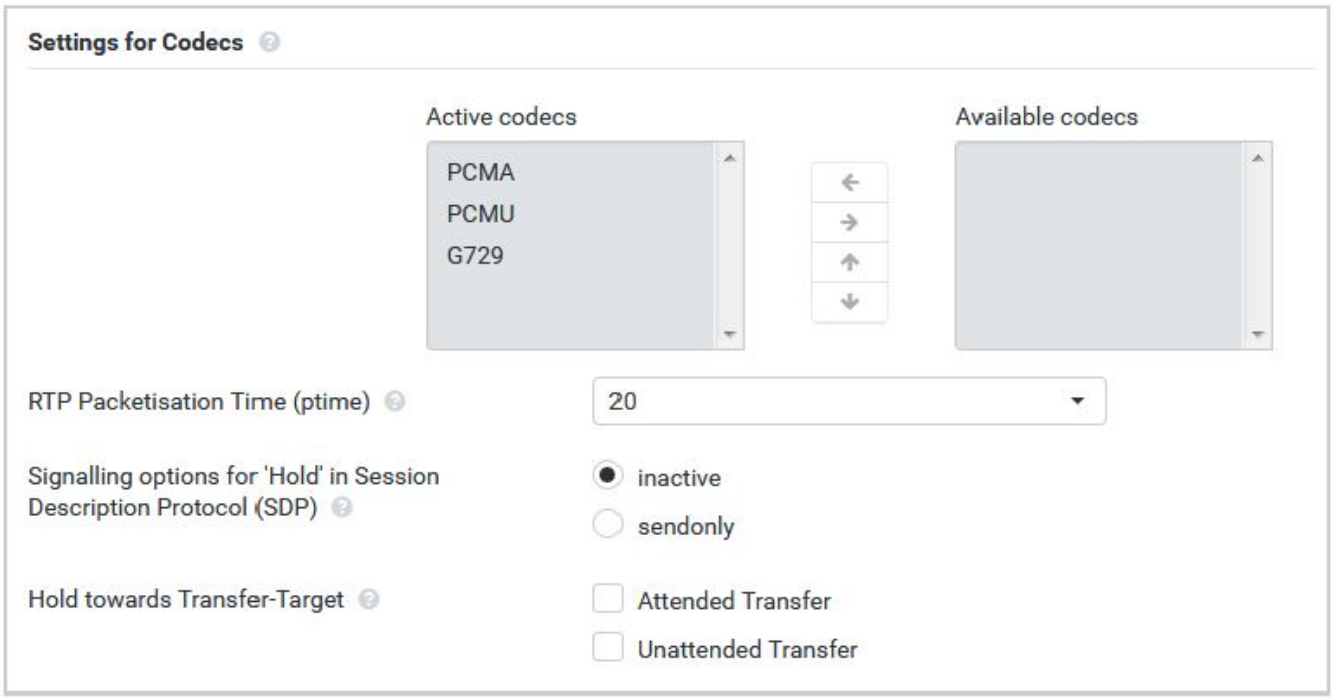
Send settings of DTMF transmission

- Make the required settings for sending DTMF signals:

Audio or RFC 2833 DTMF signals are to be transmitted acoustically (in voice packets). SIP Info DTMF signals are to be transmitted as code.

Settings for codecs

The voice quality of VoIP calls is mainly determined by the codec used for the transmission and the available bandwidth of your network connection. A "better" codec (better voice quality) means more data needs to be transferred, i.e. it requires a network connection with a larger bandwidth. You can change the voice quality by selecting the voice codecs your phone is to use, and specifying the order in which the codecs are to be suggested when a VoIP connection is established. Default settings for the codecs used are stored in your phone; one setting optimised for low bandwidths and one for high bandwidths.



Active codecs / Available codecs

The following voice codecs are supported:

G.722 Outstanding voice quality. The G.722 wideband voice codec works at the same bit rate as PCMA/PCMU (64 kbit/s per voice connection) but at a higher sampling rate (16 kHz). To enable wideband connections via G.722 you have to activate the codec explicitly on the Telephony – VoIP page.

PCMA/ (Pulse Code Modulation) Excellent voice quality (comparable with ISDN). The required bandwidth is 64 kbit/s per voice connection.

PCMU PCMA (G.711 a law): Used in Europe and most countries outside of USA. PCMU (G.711 law): Used in USA.

G.729A Average voice quality. The necessary bandwidth is less than or equal to 8 kbit/s per voice connection.

Activate/deactivate a codec:

- Select the required codec from the Available codecs/Active codecs list and click on **/ .**

Define the sequence in which the codecs should be used:

- In the Active codecs list select the required codec and click on **/** to move it up/down.

Selection of codecs G.722 and G.729 influence the system capacity in direction to lower amount of parallel calls per base station.

Number of parallel calls per base station depending on Codec / Bandwidth:

Codec	Narrow band / wide band	Number of parallel calls per base station
G711	Narrow band	10
G729 or G711	Narrow band	8
G722 or G729 or G711	Wide band	5

Provider and PBX profiles

RTP Packetisation Time (ptime)

Length of time in milliseconds represented by the audio data in one packet.

- Select the size of RTP packets to send. Select between 10 / 20 / 30 ms.

Signalling options for 'Hold' in Session Description Protocol (SDP)

Call hold means that a user request to put an active call on hold. The holding part sends a re-INVITE request to the held client with an SDP offer (Session Description Protocol). This SDP offer contains the attribute line a=inactive or a=sendonly.

- Select which attribute should be send in the SDP offer:

Inactive: The SIP endpoint would neither send nor receive data.
Sendonly: The SIP endpoint would only send and not receive data.

Hold towards Transfer-Target

Define how call transfer can be performed:

Attended Transfer The first call on the phone's VoIP connection must be held until the consultation call is accepted. Only then can two callers be connected with each other.

Unattended Transfer The caller must only be placed on hold until the user have started the consultation call (dialled the number). The user can transfer the call before the second participant registers.

Display of caller information

- From the Calling Party (User Part) option menu select which information is allowed to be transferred to the receiving part within the SIP header. Which information is actually transferred is determined by the provider.

FROM

Only the FROM information can be added.

Caller identity in the form number@server, e.g.:12345678@192.168.15.1

PPI+FROM

P-Preferred-Identity (PPI) or FROM can be added

The P-Preferred-Identity header field is used from a user agent to a trusted proxy to carry the identity the user sending the SIP message wishes to be used for the P-Asserted- Header field value that the trusted element will insert.

PAI+PPI+FROM

P-Asserted-Identity (PAI) or PPI or FROM can be added.

The P-Asserted-Identity header field is used among trusted SIP entities (typically intermediaries) to carry the identity of the user sending a SIPmessage as it was verified by authentication.

Service Codes

Service codes are key sequences provided by the provider or PBX in order to activate/deactivate specific functions on the handset. You can set the adequate service codes for activating/deactivating CCBS and CCNR.

CCBS (Completion of Call to busy Subscriber) Ringback if busy
CCNR (Completion of Calls on No Reply) Ringback if no answer

- In the text fields Call Completion on (CCBS, CCNR)/Call Completion off (CCBS, CCNR) enter the key sequence for activating/deactivating CCBS and CCNR.
- Click on Set to save the settings of this page.