We change the shape of the world

White Paper

NovaTec
Access Media Gateway

Version 1.0 / October 26th, 2010

This document is subject to changes.

INHALT

1 Introduction

This white paper describes the characteristics, configuration, operation and connections of NovaTec A-MGWs in a VoIP network or in interaction with e.g. the Cisco Unified Communications Manager over a SIP trunk.

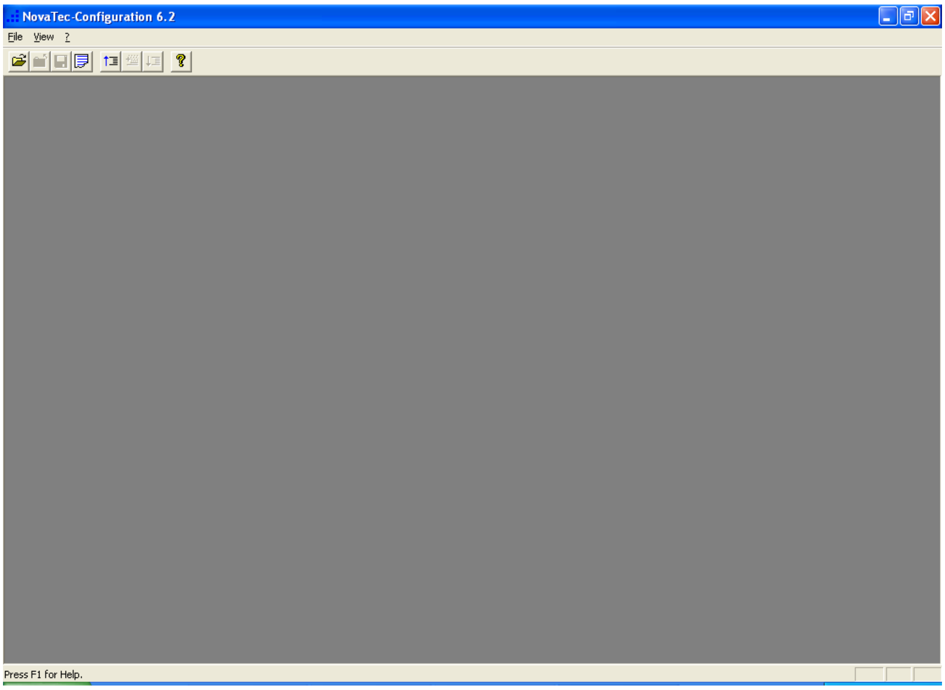
The NovaTec A-MGWs provide all usual TDM based interfaces (PRI, BRI, analog, GSM, Uk0). The NovaTec Sx models can be connected e.g. as third party device to a Cisco Unified Communications Manager.

Amongst other things this document covers the general procedure for the TLS encryption, a detail description how TLS is set up, how DHCP has to be installed, a step by step guide of how the Sx has to be configured if connected over a SIP trunk, how the NovaTec Management System needs to be set up and how it works with the Sx.

2 Configuration instruction

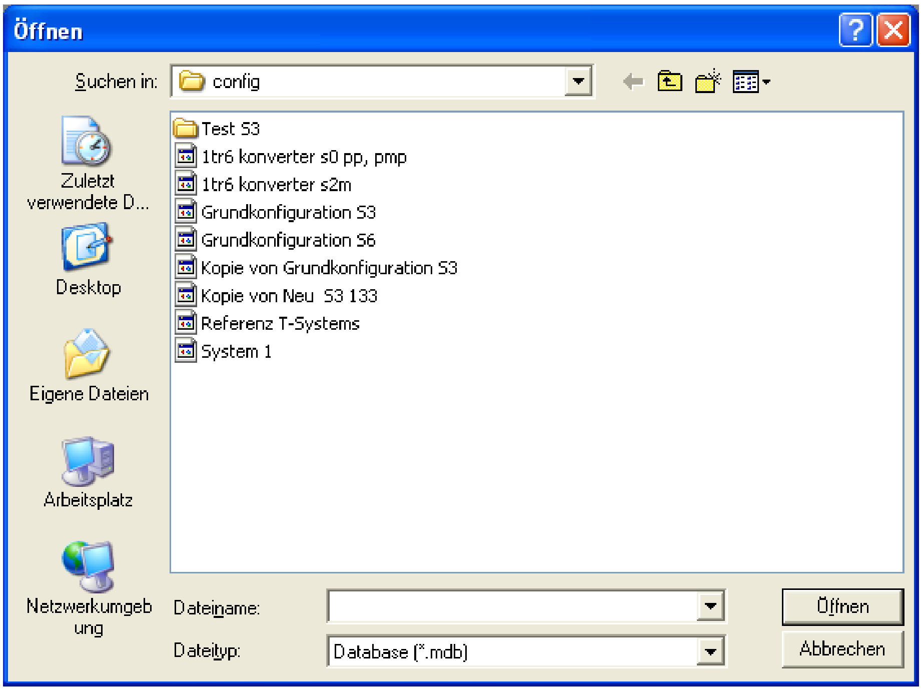
2.1 Starting the configuration interface:

Start the configuration interface via the Windows start menu:
Start menu → Programs → NovaTec → NMP 6.2 → NovaTec Configuration



2.2 Open the data base

Choose „File/open“ in the menu bar. Choose the needed file in the open dialogue.

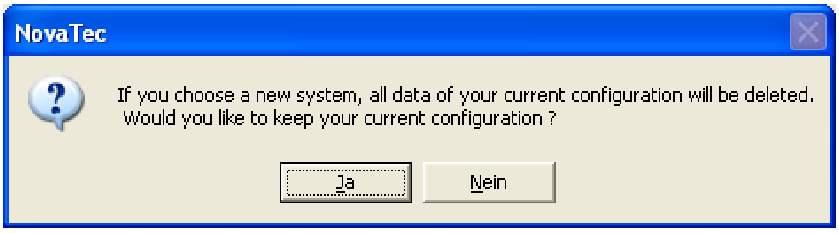


Suchen in: config

Dateityp: Database (*.mdb)

2.3 Chassis configuration (S20, S6, S5+ or S3)

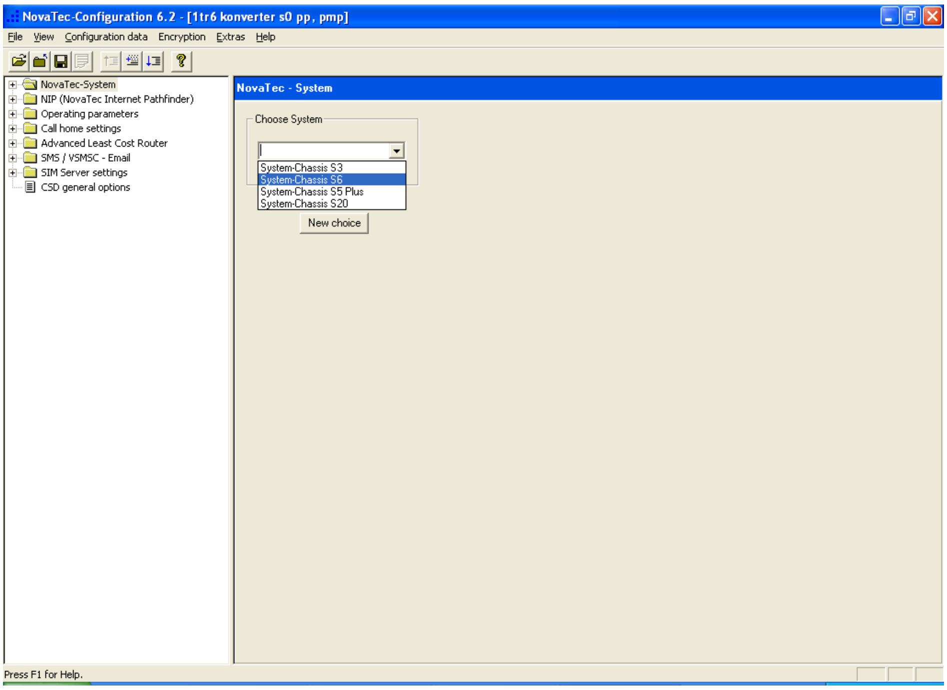
Click on „Novatec-System“ in the left tree first and afterwards on the button „New choice“ in the right window.



If you choose a new system, all data of your current configuration will be deleted.
Would you like to keep your current configuration ?

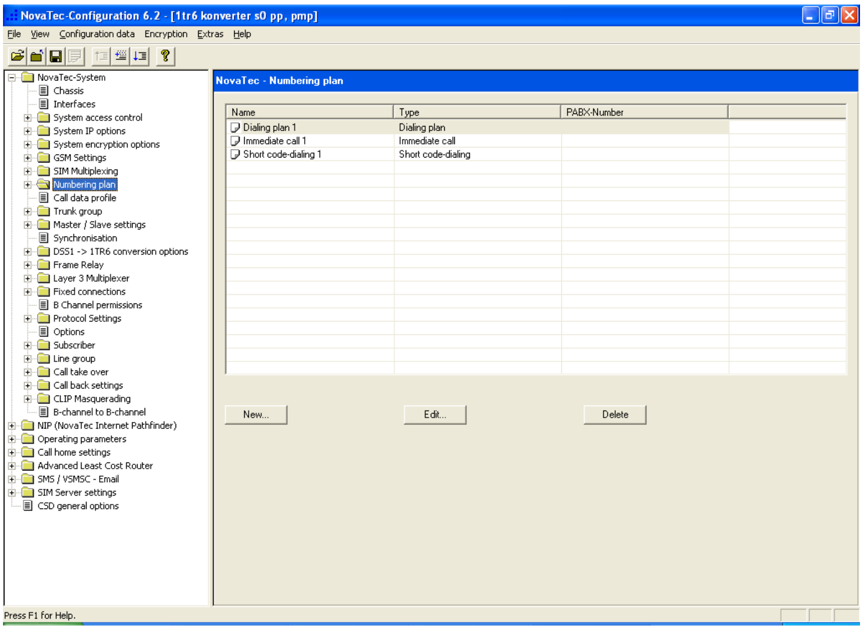
Confirm the pop-up-dialogue with „No“. Thereby the existing adjustments in the data base are deleted. You thereby setup a new configuration.

Choose e.g. „System-Chassis S6“ as chassis to configure a NovaTec S6.



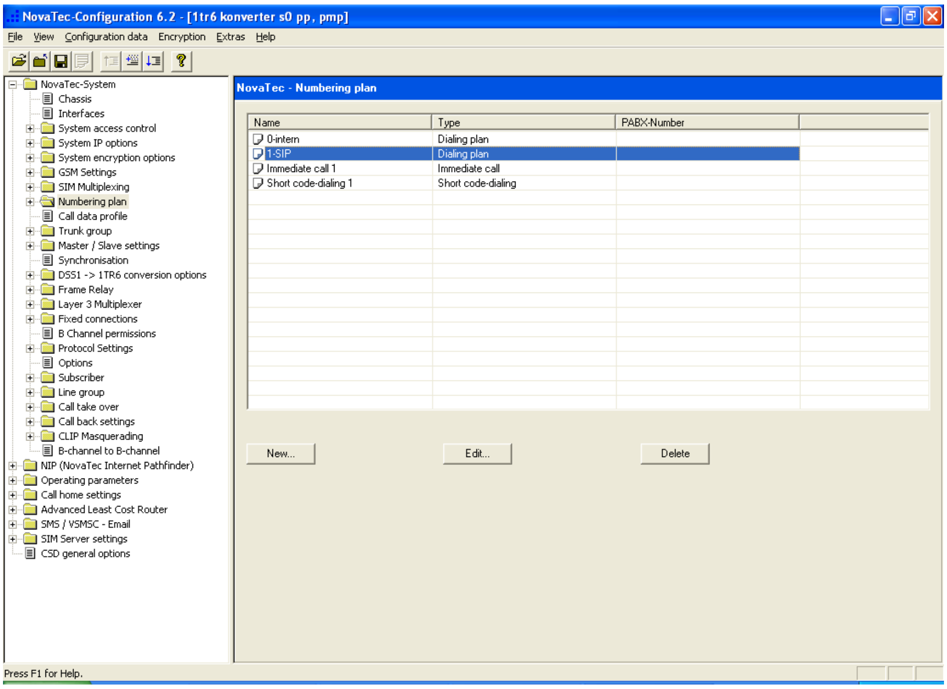
2.4 Defining the numbering plan

Select „NovaTec-System/Numbering plan“ in the left menu tree and click button „New“ in the right window.



Name	Type	PABX-Number
Dialing plan 1	Dialing plan	
Immediate call 1	Immediate call	
Short code-dialing 1	Short code-dialing	

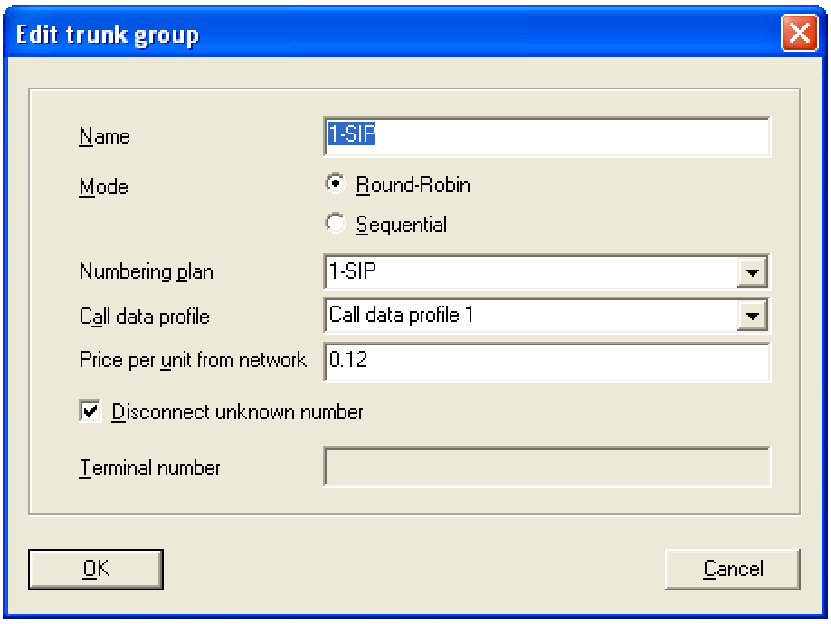
In the window „New numbering plan“ you enter „0-intern“ as name and choose „Dialing plan“ as type. The box *„PABX-Number“* remains empty. Confirm with „Ok“. Repeat the procedure and set-up a second dialing plan with the name „1-SIP“.Choose the same setup as before.



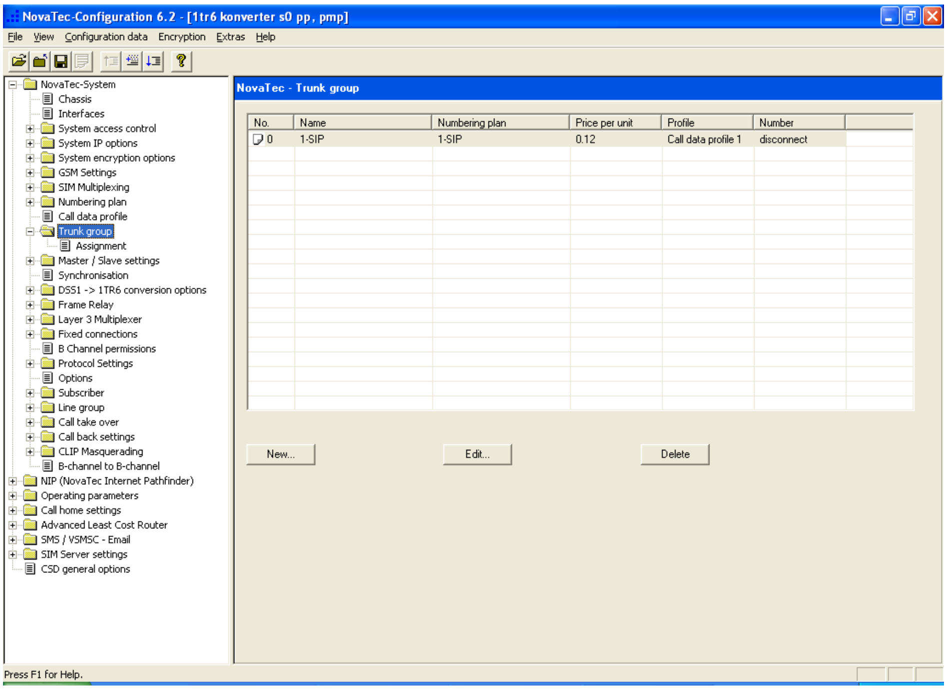
Name	Type	PABX-Number
0-intern	Dialing plan	
1-SIP	Dialing plan	
Immediate call 1	Immediate call	
Short code-dialing 1	Short code-dialing	

2.5 Configuration of SIP Trunk group

Pick „NovaTec-System/Trunk group“ in the left tree and click „Edit“ in the right window. Create a trunk group with the name „1-SIP“ and the calibrations/data as given below. Confirm with “Ok”.



Name	1-SIP
Mode	● Round-Robin ○ Sequential
Numbering plan	1-SIP
Call data profile	Call data profile 1
Price per unit from network	0.12
☑ Disconnect unknown number	
Terminal number	



- NovaTec-System
  - Chassis
  - Interfaces
  - System access control
  - System IP options
  - System encryption options
  - GSM Settings
  - SIM Multiplexing
  - Numbering plan
  - Call data profile
  - Trunk group
    - Assignment
  - Master / Slave settings
  - Synchronisation
  - DSS1 -> 1TR6 conversion options
  - Frame Relay
  - Layer 3 Multiplexer
  - Fixed connections
  - B Channel permissions
  - Protocol Settings
  - Options
  - Subscriber
  - Line group
  - Call take over
  - Call back settings
  - CLIP Masquerading
  - B-channel to B-channel
- NIP (NovaTec Internet Pathfinder)
- Operating parameters
- Call home settings
- Advanced Least Cost Router
- SMS / VSMSC - Email
- SIM Server settings
- CSD general options

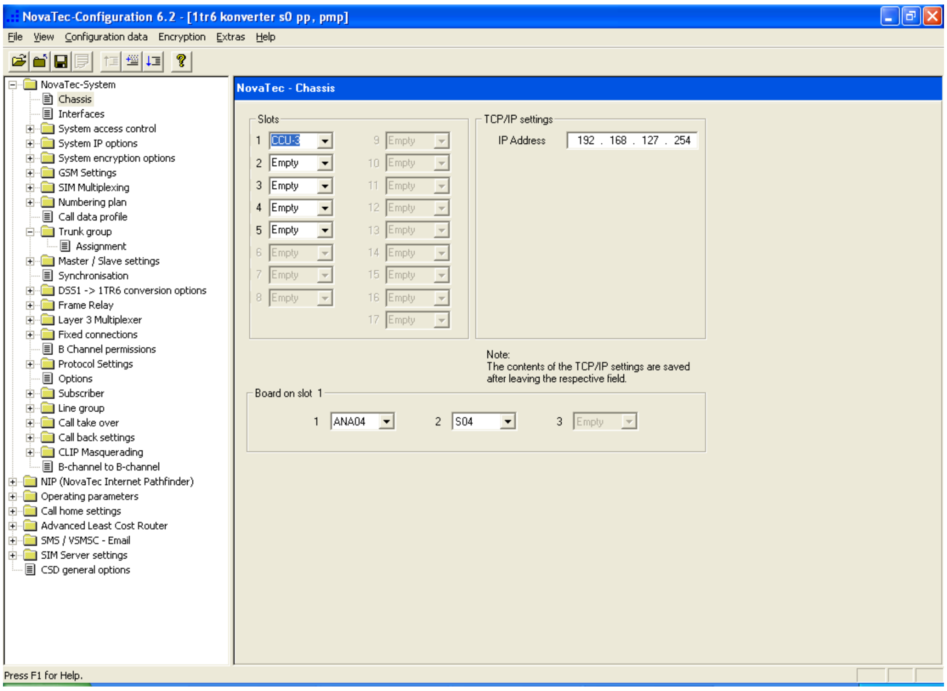
NovaTec - Trunk group

No.	Name	Numbering plan	Price per unit	Profile	Number
0	1-SIP	1-SIP	0.12	Call data profile 1	disconnect

2.6 Configuring modules (e.g. S6 build up)

In this example the S6 consist of the following hardware:
CCU with an analog slip on board ANA4 and an ISDN to BRI board S04,
ULU with 4 Uk$_0$ interfaces, BCU 16 with 16 VoIP canals.

Pick „NovaTec System/Chassis“ in the left tree. Choose „CCU 3“ for slot 1 under „Slots“ in the right window. Choose “ANA04” in space 1 under “Board on slot 1” in the bottom half of the window and “S04” in space 2.



NovaTec - Chassis

Slots

1	CCU-3	9	Empty
2	Empty	10	Empty
3	Empty	11	Empty
4	Empty	12	Empty
5	Empty	13	Empty
6	Empty	14	Empty
7	Empty	15	Empty
8	Empty	16	Empty
		17	Empty

TCP/IP settings

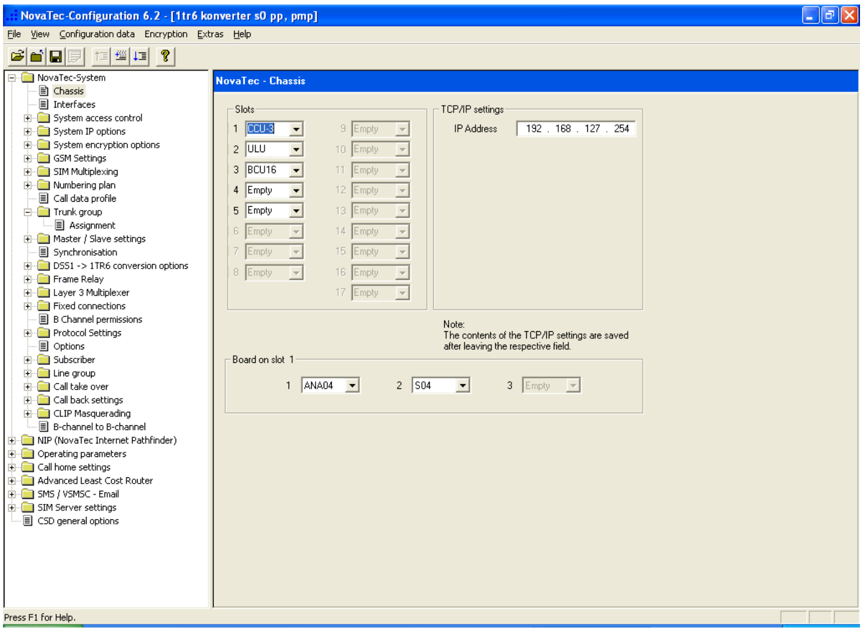
IP Address 192 . 168 . 127 . 254

Note:
The contents of the TCP/IP settings are saved after leaving the respective field.

Board on slot 1

1 ANA04 2 S04 3 Empty

Choose „ULU“ for slot 2 and „BCU16“ for slot 3. As these boards have no slip on spaces you don’t have to make further adjustments for slots 2 and 3.



NovaTec - Chassis

Slots

1	CCU-3	9	Empty
2	ULU	10	Empty
3	BCU16	11	Empty
4	Empty	12	Empty
5	Empty	13	Empty
6	Empty	14	Empty
7	Empty	15	Empty
8	Empty	16	Empty
		17	Empty

TCP/IP settings

IP Address 192 . 168 . 127 . 254

Note:
The contents of the TCP/IP settings are saved after leaving the respective field.

Board on slot 1

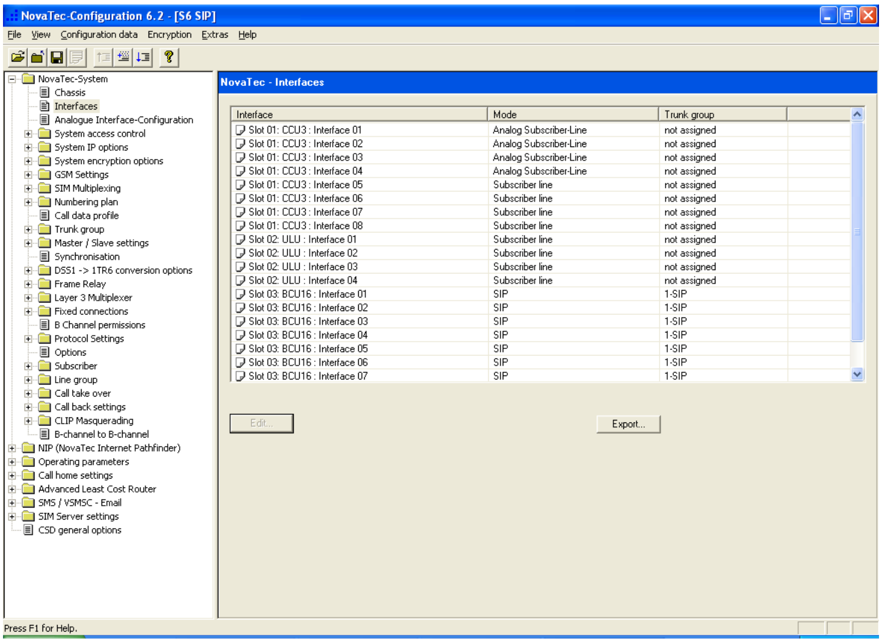
1 ANA04 2 S04 3 Empty

2.7 Defining interfaces

Pick „NovaTec System/Interfaces“ in the left tree. Select the particular interface and click the button „Edit“. Execute the following adjustments for the different interface types:
For BRI and Uk$_0$ interfaces choose „Subscriber line“. The position “Trunk group” remains “not assigned”.

For the analog interfaces (ANA4) choose the mode *„Analog Subscriber line“*. The position “Trunk group” remains “not assigned”.

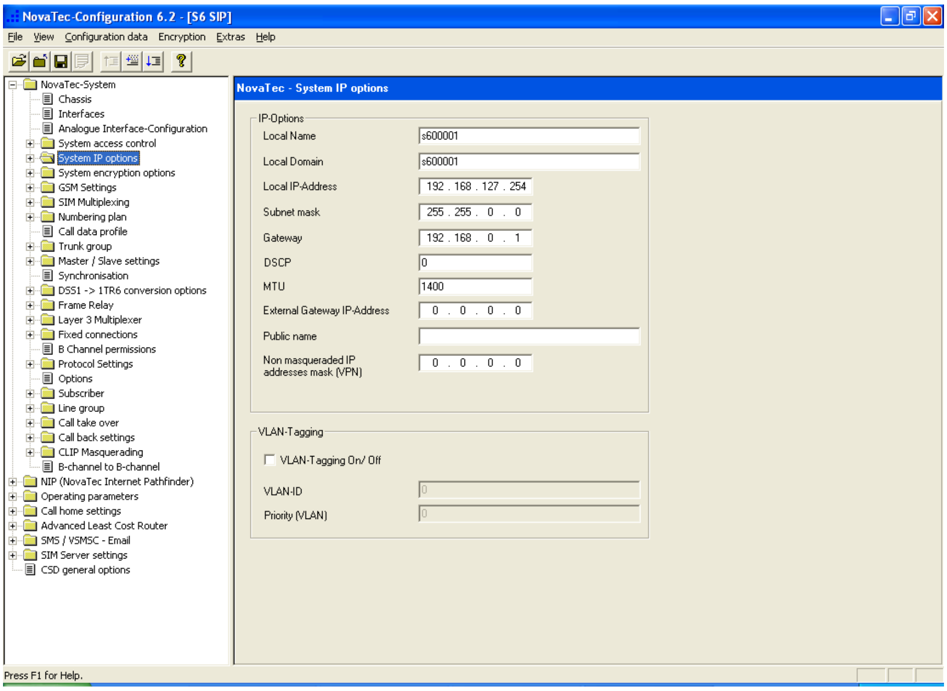
For VoIP interfaces (BCU16) choose mode *„SIP“* and *„Trunk group“* ***„**1-SIP**“***.



Interface	Mode	Trunk group
Slot 01: CCU3 : Interface 01	Analog Subscriber-Line	not assigned
Slot 01: CCU3 : Interface 02	Analog Subscriber-Line	not assigned
Slot 01: CCU3 : Interface 03	Analog Subscriber-Line	not assigned
Slot 01: CCU3 : Interface 04	Analog Subscriber-Line	not assigned
Slot 01: CCU3 : Interface 05	Subscriber line	not assigned
Slot 01: CCU3 : Interface 06	Subscriber line	not assigned
Slot 01: CCU3 : Interface 07	Subscriber line	not assigned
Slot 01: CCU3 : Interface 08	Subscriber line	not assigned
Slot 02: ULU : Interface 01	Subscriber line	not assigned
Slot 02: ULU : Interface 02	Subscriber line	not assigned
Slot 02: ULU : Interface 03	Subscriber line	not assigned
Slot 02: ULU : Interface 04	Subscriber line	not assigned
Slot 03: BCU16 : Interface 01	SIP	1-SIP
Slot 03: BCU16 : Interface 02	SIP	1-SIP
Slot 03: BCU16 : Interface 03	SIP	1-SIP
Slot 03: BCU16 : Interface 04	SIP	1-SIP
Slot 03: BCU16 : Interface 05	SIP	1-SIP
Slot 03: BCU16 : Interface 06	SIP	1-SIP
Slot 03: BCU16 : Interface 07	SIP	1-SIP

2.8 System IP options

Choose *„NovaTec-System/System IP options“ in the left tree*. Enter the appropriate settings for your network and installations.



NovaTec - System IP options

IP-Options

Local Name: s600001

Local Domain: s600001

Local IP-Address: 192 . 168 . 127 . 254

Subnet mask: 255 . 255 . 0 . 0

Gateway: 192 . 168 . 0 . 1

DSCP: 0

MTU: 1400

External Gateway IP-Address: 0 . 0 . 0 . 0

Public name:

Non masqueraded IP addresses mask (VPN): 0 . 0 . 0 . 0

VLAN-Tagging

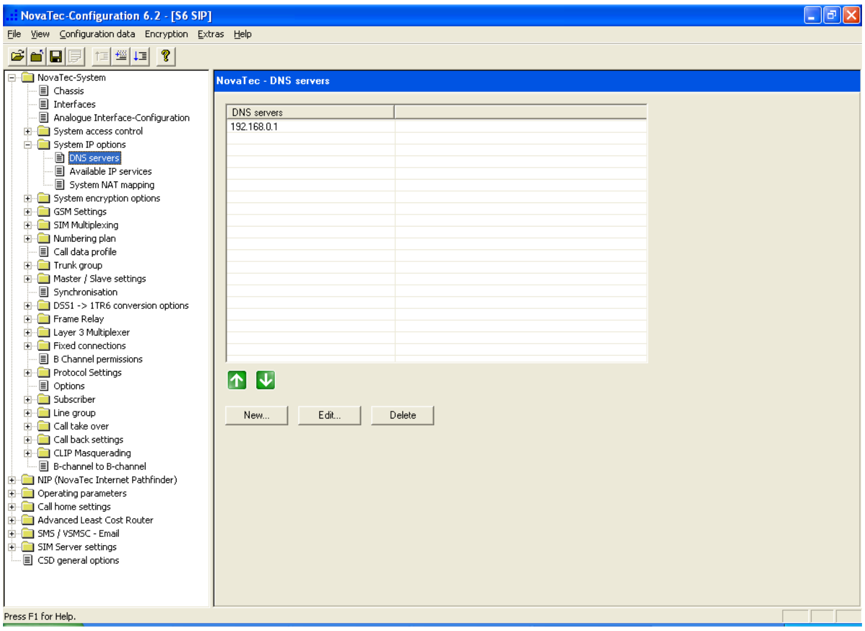
□ VLAN-Tagging On/ Off

VLAN-ID: 0

Priority (VLAN): 0

Go to *„NovaTec-System/System IP options/DNS Server“* in the menu tree.

Click *„New“* and enter the address of your DNS server.



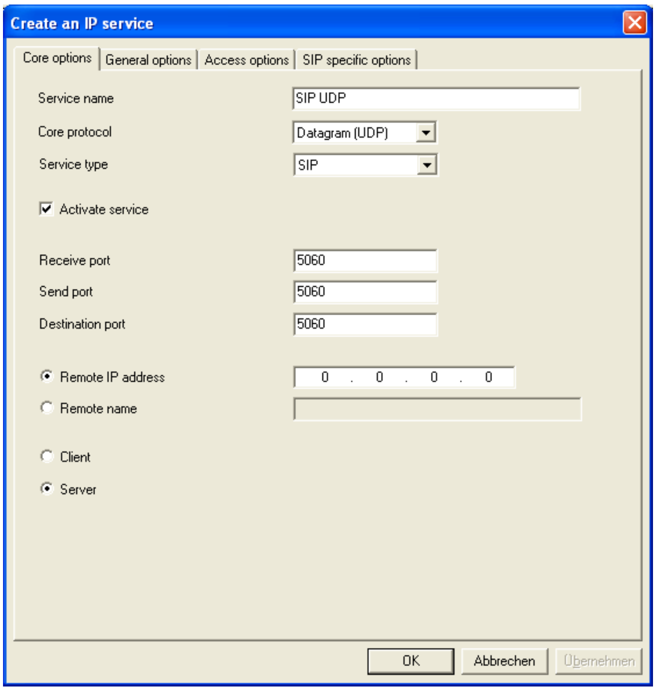
NovaTec - DNS servers

DNS servers	
192.168.0.1	

Go to *„NovaTec-System/System IP options/Available IP services“.*

Click *„New“* and process the setups as shown in the next four pictures in order to activate SIP over UDP (via IP-Port 5060).

Confirm with *„OK“.*



Create an IP service

Service name: SIP UDP

Core protocol: Datagram (UDP)

Service type: SIP

☑ Activate service

Receive port: 5060

Send port: 5060

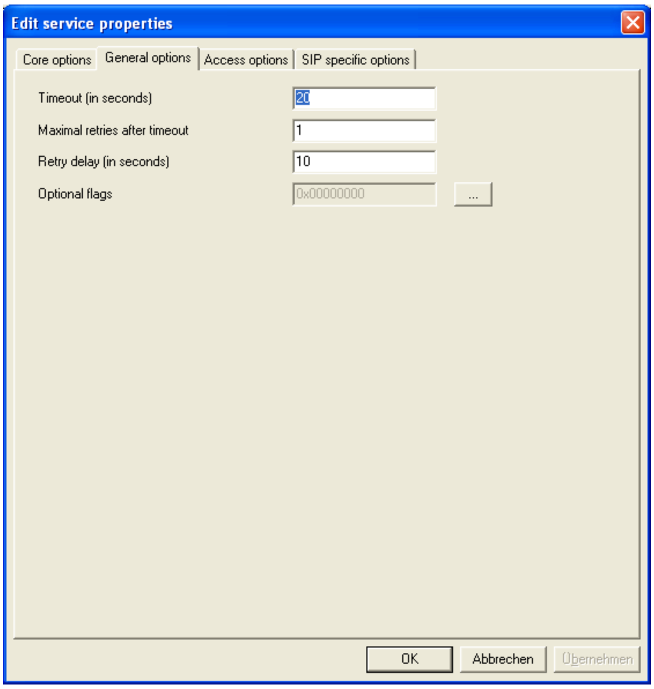
Destination port: 5060

● Remote IP address: 0 . 0 . 0 . 0

○ Remote name

○ Client

● Server



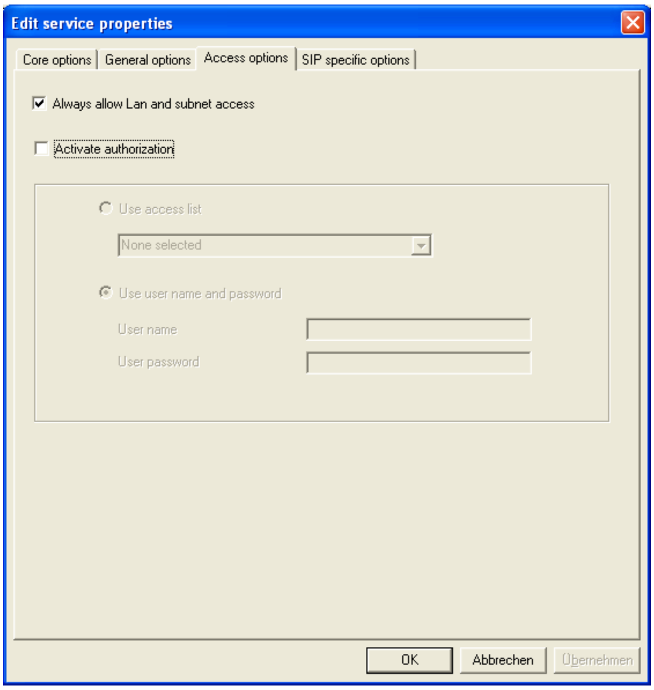
Edit service properties

Timeout (in seconds): 20

Maximal retries after timeout: 1

Retry delay (in seconds): 10

Optional flags: 0x00000000



☑ Always allow Lan and subnet access

☐ Activate authorization

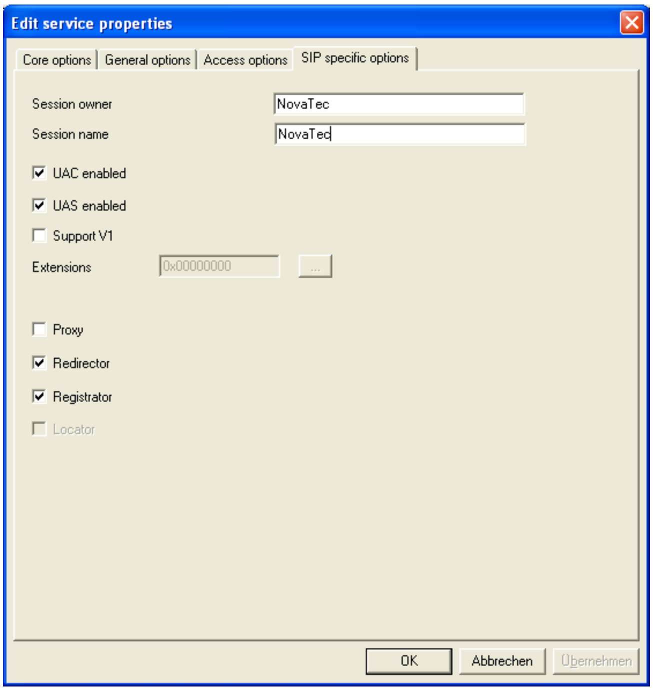
○ Use access list

None selected

● Use user name and password

User name

User password



Session owner: NovaTec

Session name: NovaTec

☑ UAC enabled

☑ UAS enabled

☐ Support V1

Extensions: 0x00000000

☐ Proxy

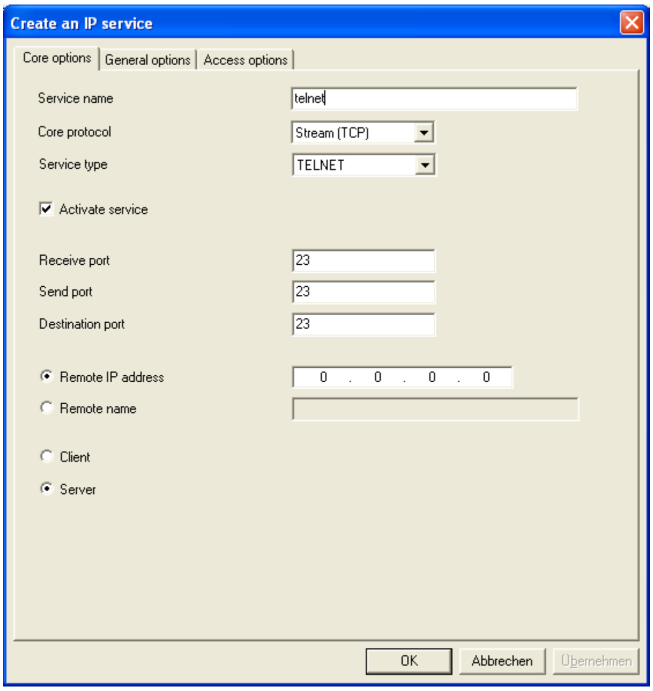
☑ Redirector

☑ Registrator

☐ Locator

Click *„New“* anew and carry out the settings shown in the next three pictures in order to activate the service Telnet (via IP port 23).

Confirm with *„OK“*.



Service name: telnet

Core protocol: Stream (TCP)

Service type: TELNET

☑ Activate service

Receive port: 23

Send port: 23

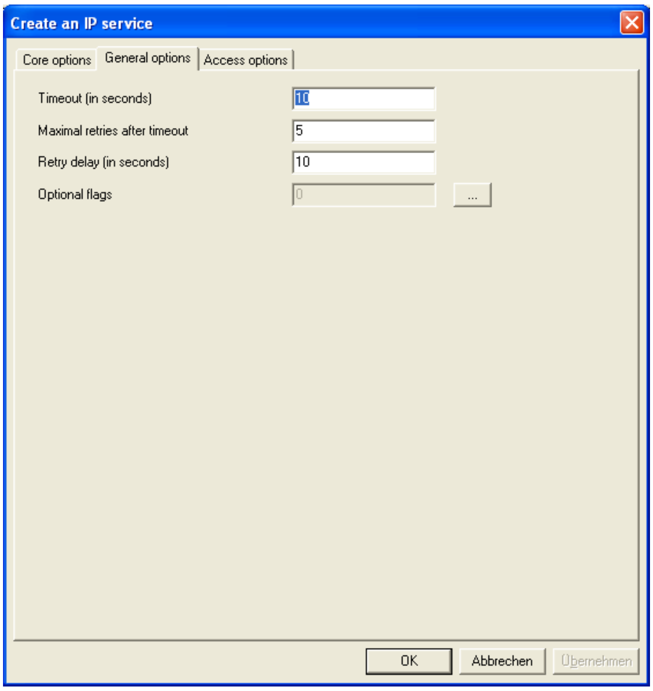
Destination port: 23

● Remote IP address: 0 . 0 . 0 . 0

○ Remote name

○ Client

● Server

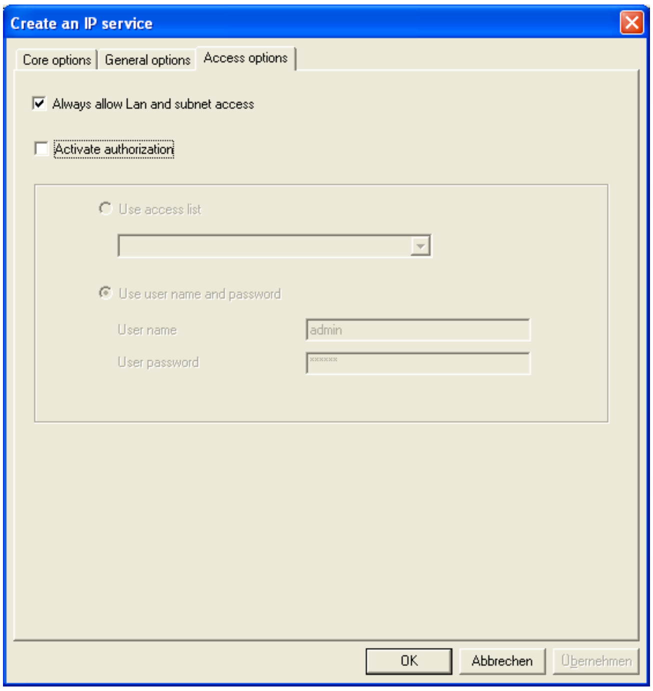


Timeout (in seconds): 10

Maximal retries after timeout: 5

Retry delay (in seconds): 10

Optional flags: 0



Create an IP service

☑ Always allow Lan and subnet access

□ Activate authorization

○ Use access list

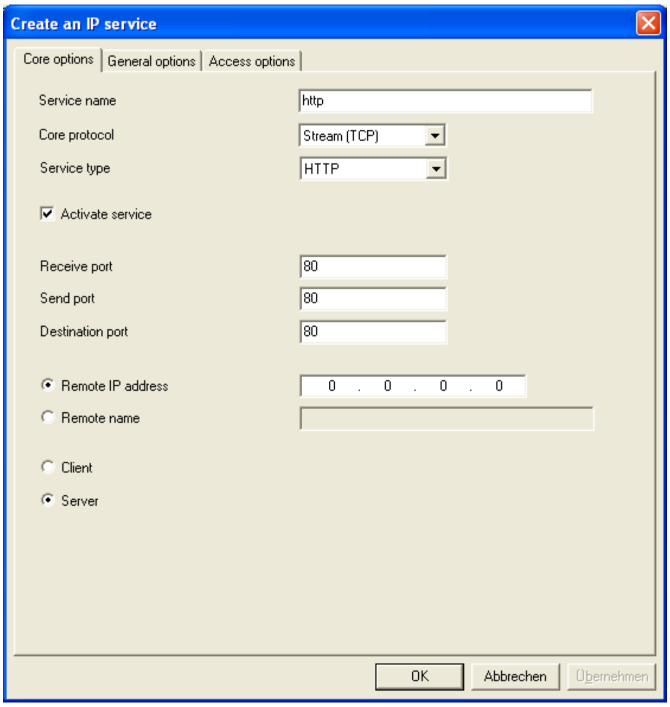
● Use user name and password

User name: admin

User password: xxxxxx

Click *„New“* again and proceed with the settings in the next pictures to activate the service http (via IP port 80).

Confirm with *„OK“*.



Create an IP service

Service name: http

Core protocol: Stream (TCP)

Service type: HTTP

☑ Activate service

Receive port: 80

Send port: 80

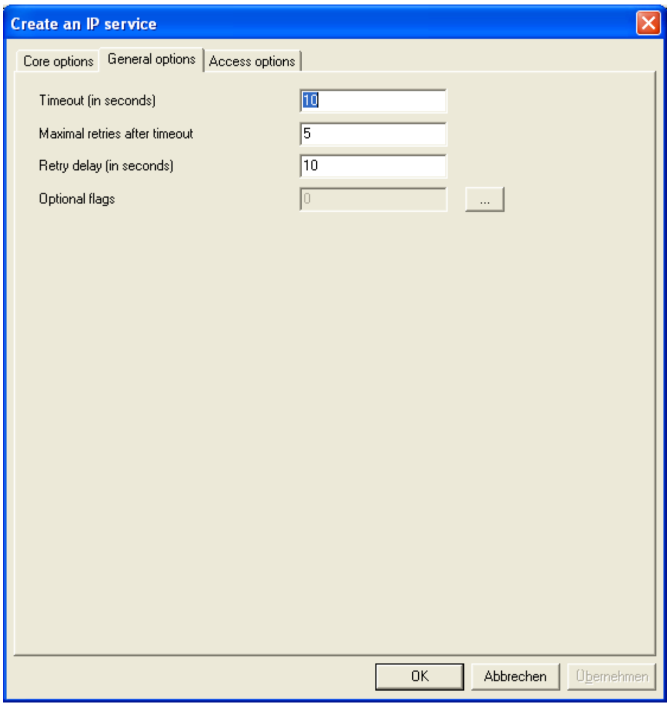
Destination port: 80

● Remote IP address: 0 . 0 . 0 . 0

○ Remote name

○ Client

● Server



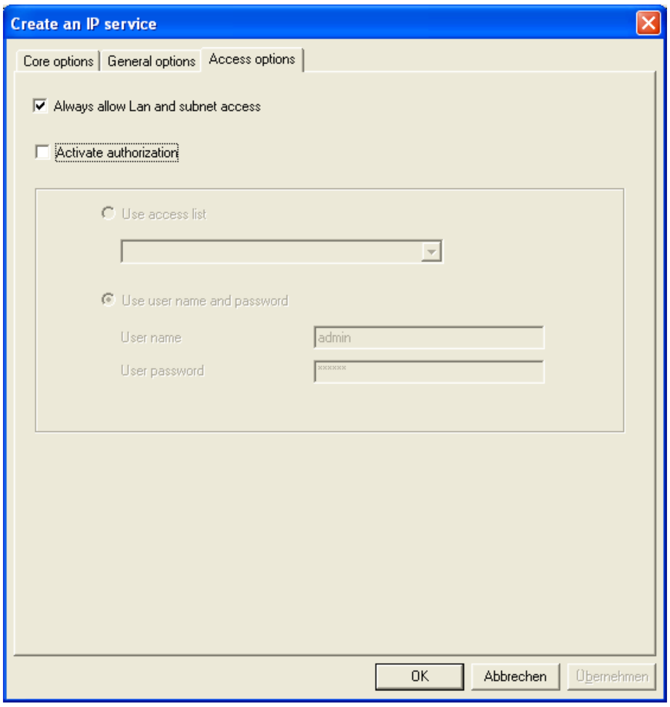
Create an IP service

Timeout (in seconds): 10

Maximal retries after timeout: 5

Retry delay (in seconds): 10

Optional flags: 0



Create an IP service

☑ Always allow Lan and subnet access

□ Activate authorization

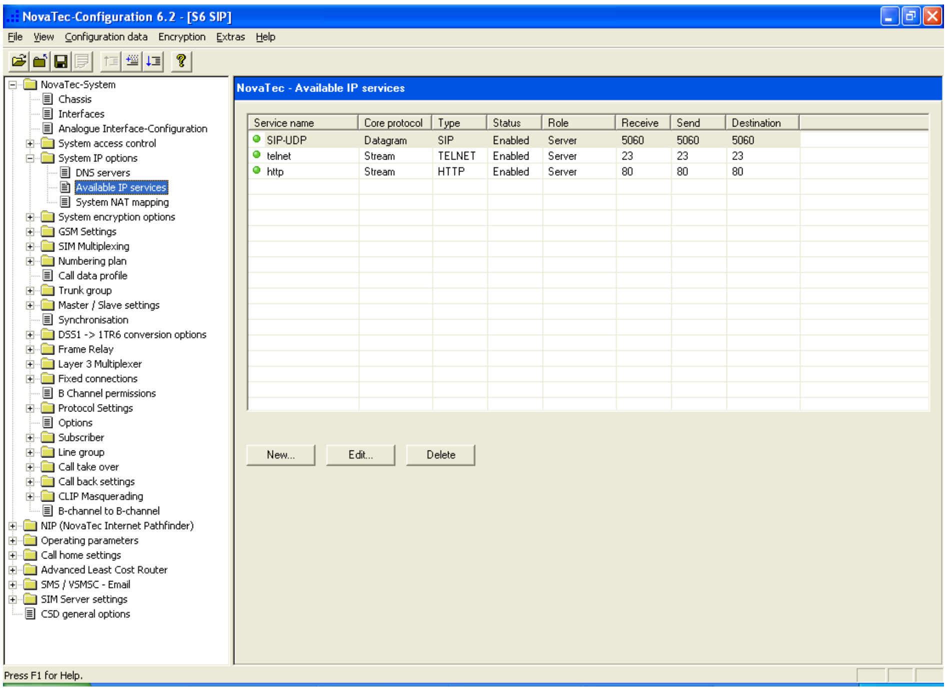
○ Use access list

● Use user name and password

User name: admin

User password: ******

If you have activated all services as given above the overview will look as shown in the picture below.



NovaTec - Available IP services

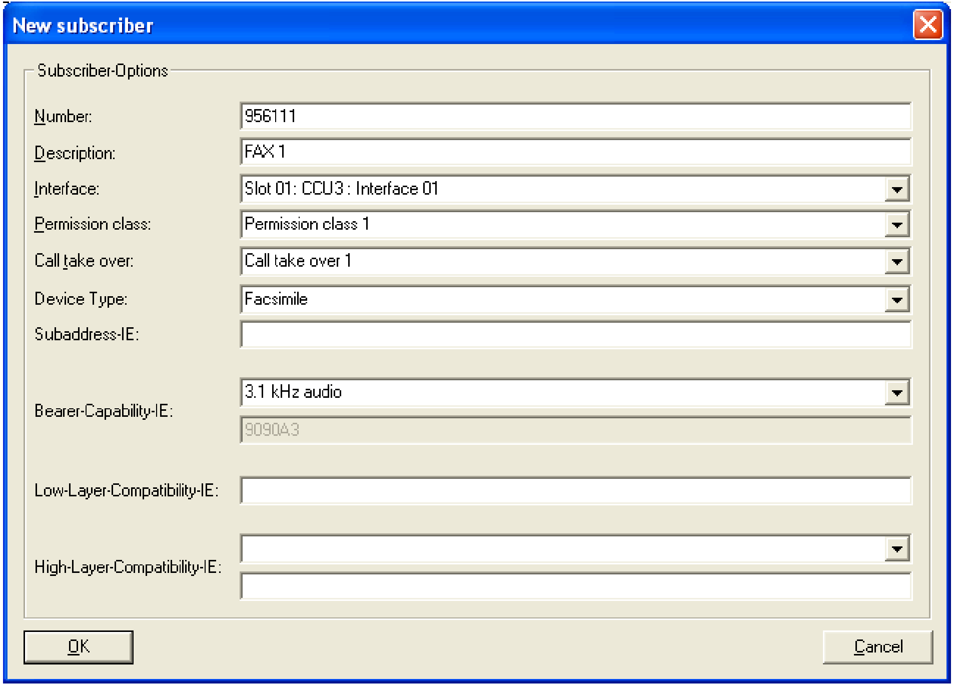
Service name	Core protocol	Type	Status	Role	Receive	Send	Destination
SIP-UDP	Datagram	SIP	Enabled	Server	5060	5060	5060
telnet	Stream	TELNET	Enabled	Server	23	23	23
http	Stream	HTTP	Enabled	Server	80	80	80

2.9 Configuring subscriber and permission class

Go to the left tree and choose „*New*“ under „*NovaTec-System/Subscriber*“.

Enter the below given data setup in order to configure a fax on the first analog interface with number „956111“.

Confirm with „Ok“.


New subscriber

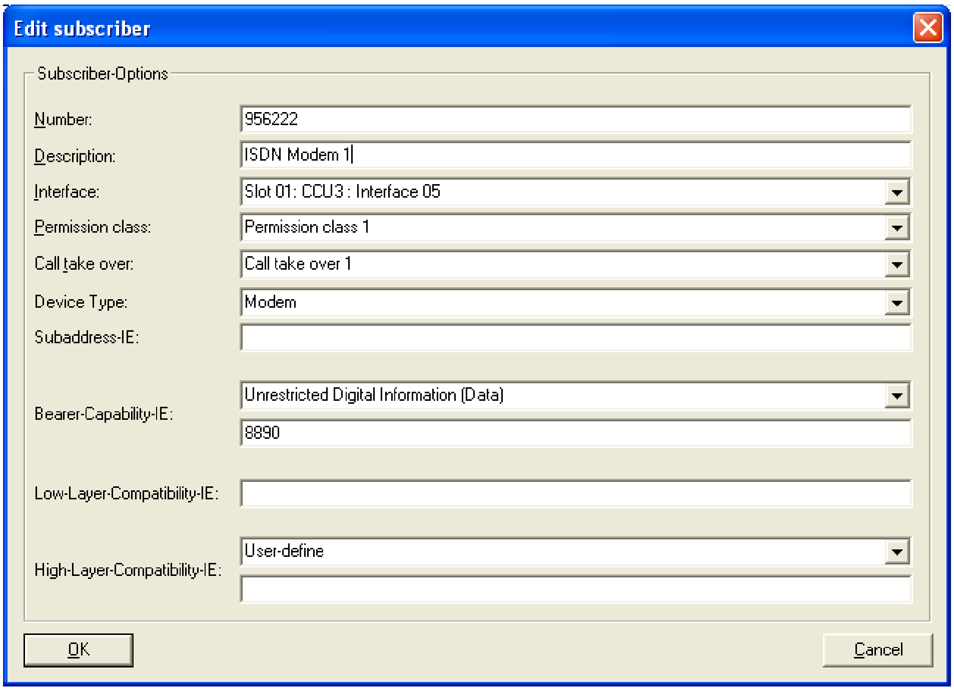
Subscriber-Options

Number:	956111
Description:	FAX 1
Interface:	Slot 01: CCU3 : Interface 01
Permission class:	Permission class 1
Call take over:	Call take over 1
Device Type:	Facsimile
Subaddress-IE:	
Bearer-Capability-IE:	3.1 kHz audio 9090A3
Low-Layer-Compatibility-IE:	
High-Layer-Compatibility-IE:	

Click „New“ again.

Enter the below given setup data in order to configure a modem on the first ISDN interface with number „956222“.

Confirm with “Ok”.



Number: 956222

Description: ISDN Modem 1

Interface: Slot 01: CCU3 : Interface 05

Permission class: Permission class 1

Call take over: Call take over 1

Device Type: Modem

Subaddress-IE:

Bearer-Capability-IE: Unrestricted Digital Information (Data)
8890

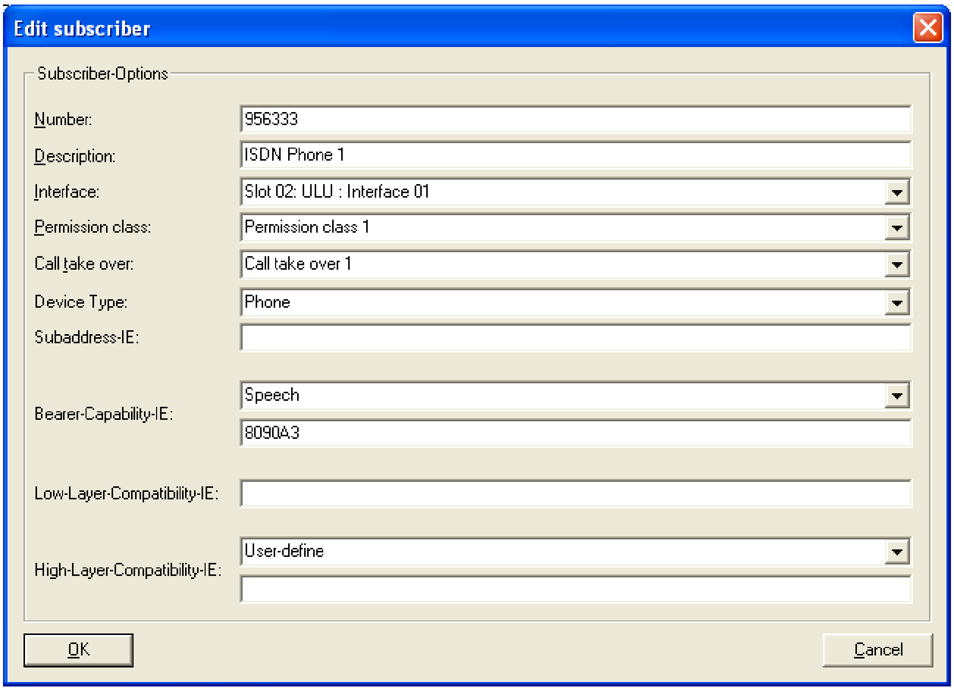
Low-Layer-Compatibility-IE:

High-Layer-Compatibility-IE: User-define

Click „New“ again.

Enter the below given setup data in order to configure a modem on the first U_{K0} interface with number „9566333“.

Confirm with „Ok".



Edit subscriber

Subscriber-Options

Number: 956333

Description: ISDN Phone 1

Interface: Slot 02: ULU : Interface 01

Permission class: Permission class 1

Call take over: Call take over 1

Device Type: Phone

Subaddress-IE:

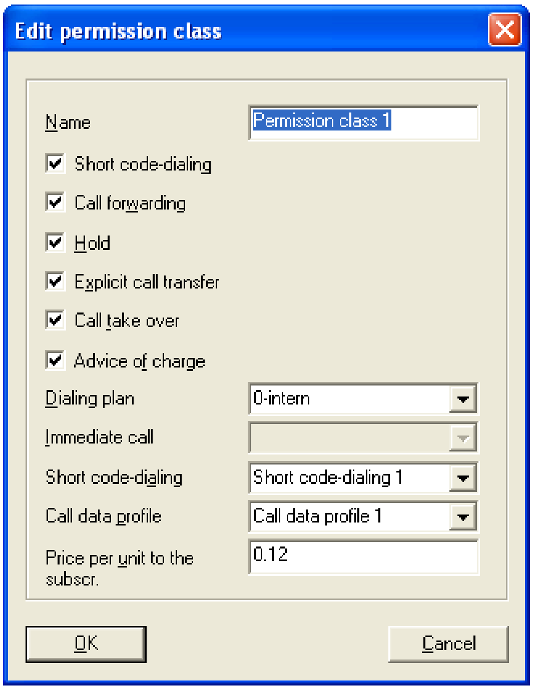
Bearer-Capability-IE: Speech
8090A3

Low-Layer-Compatibility-IE:

High-Layer-Compatibility-IE: User-define

Go to the tree on the left hand of the window and select „Permission class 1" under „NovaTec-System/Subscriber/Permission class". Click "Edit" after doing so.

Adjust the setup as given below and confirm with „Ok".



Edit permission class

Name: Permission class 1

☑ Short code-dialing

☑ Call forwarding

☑ Hold

☑ Explicit call transfer

☑ Call take over

☑ Advice of charge

Dialing plan: 0-intern

Immediate call:

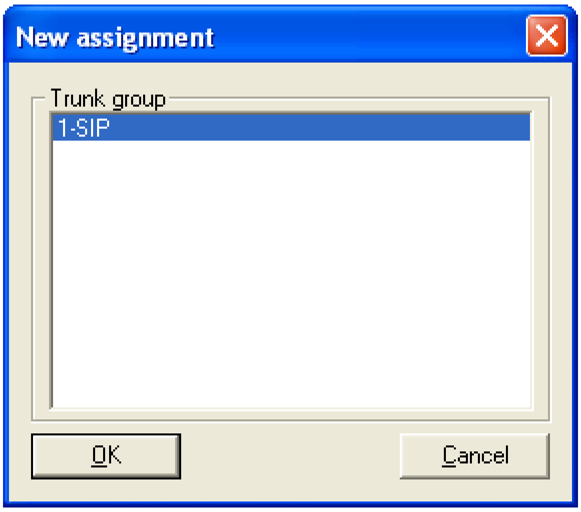
Short code-dialing: Short code-dialing 1

Call data profile: Call data profile 1

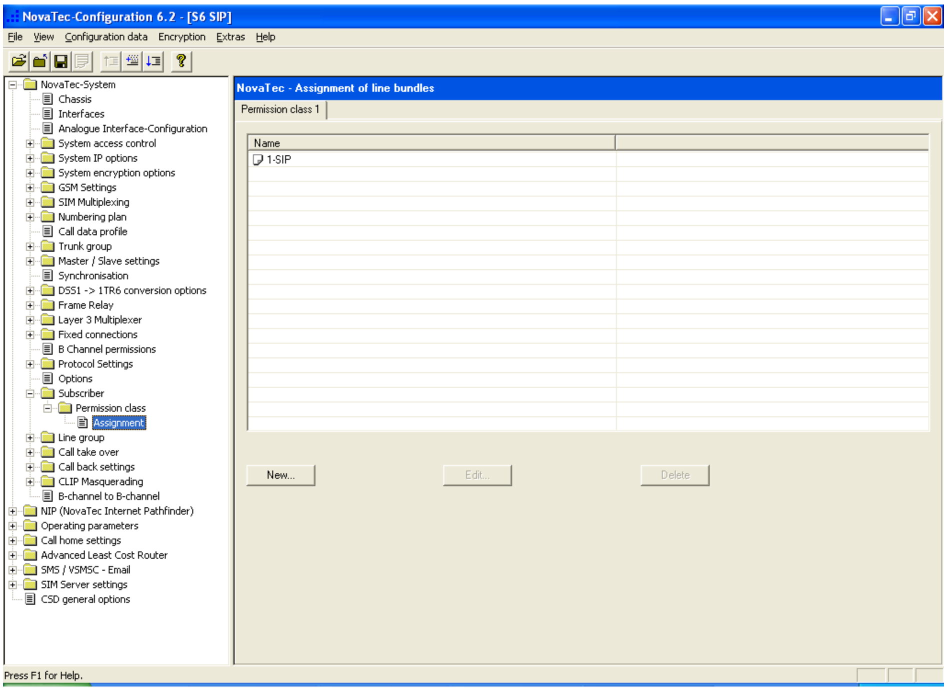
Price per unit to the subscr.: 0.12

Click „New“ in the tree on the left hand under „NovaTec-System/Subscriber/Permission class/Assignment“.

Choose the trunk group „1-SIP“ as shown below and confirm with “Ok”.



Below you can view the window shown after „1-SIP“ was included in “Permission class 1”.

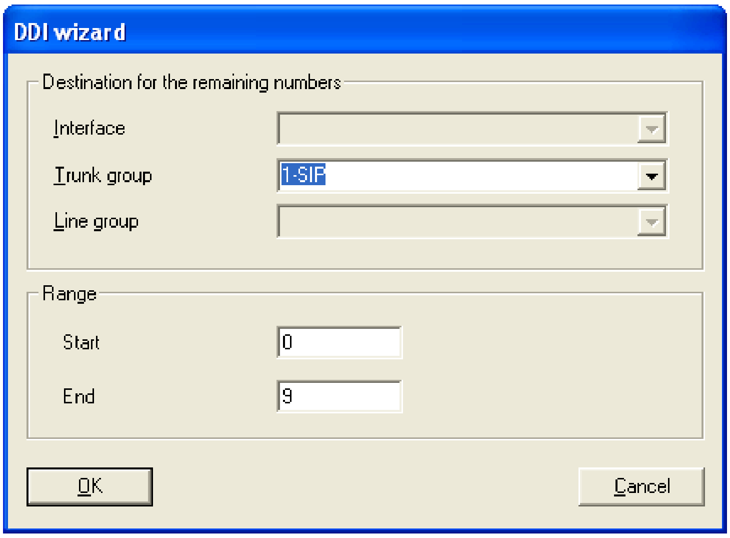


2.10 Configuration of dialing plans

Two dialing plans have to be configured.

The internal dialing plan (Name: „0-intern“) is used by all subscribers (end devices) of the system.

Choose „NovaTec-System/Numbering plan/Dialing plans“ in the left hand tree. Go to the flag “0-intern”. Click “DDI Wizard”. Carry out the below given adjustments and confirm with „Ok“.



DDI wizard

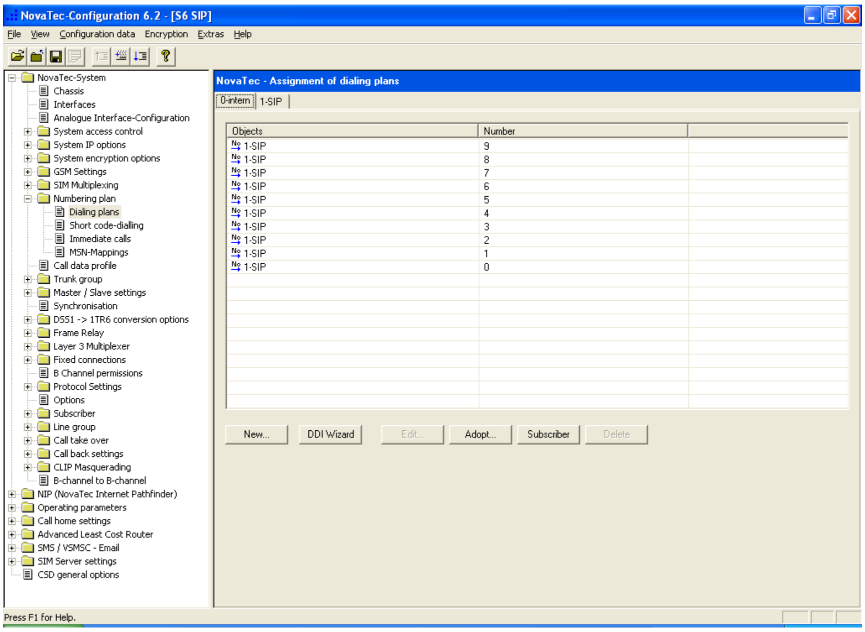
Destination for the remaining numbers

Interface:
Trunk group: 1-SIP
Line group:

Range

Start: 0
End: 9

The picture below shows the setup of the dialing plan „0-intern“. All calls are routed to the trunk group “1-SIP”.



NovaTec-Configuration 6.2 - [S6 SIP]

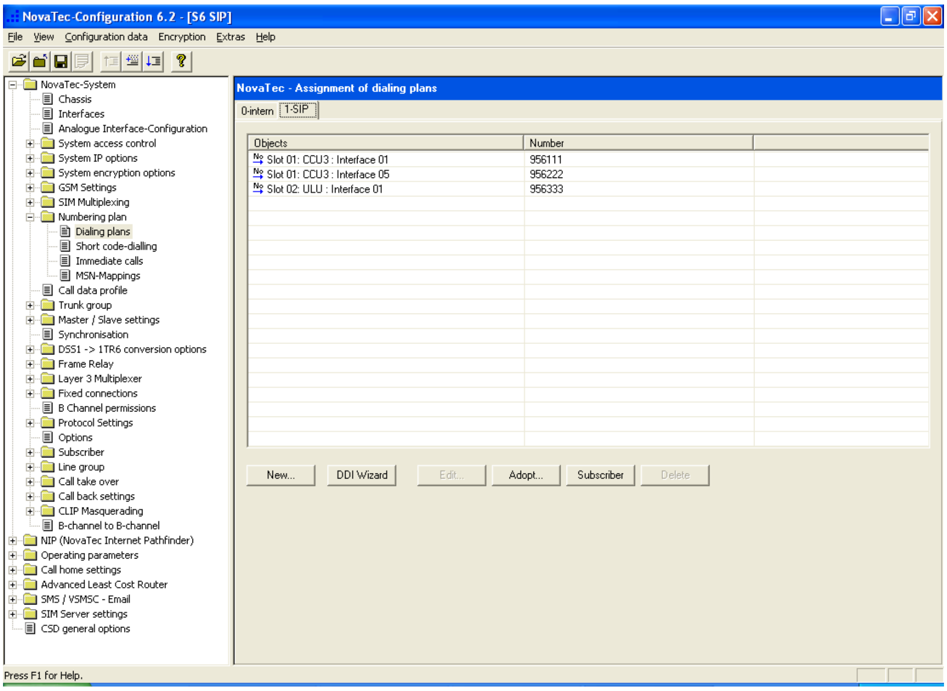
NovaTec - Assignment of dialing plans

Objects	Number
1-SIP	9
1-SIP	8
1-SIP	7
1-SIP	6
1-SIP	5
1-SIP	4
1-SIP	3
1-SIP	2
1-SIP	1
1-SIP	0

The calls from the end devices are routed using the SIP call number plan.

Pick „NovaTec-Systems/Numbering plan/Dialing plans“.

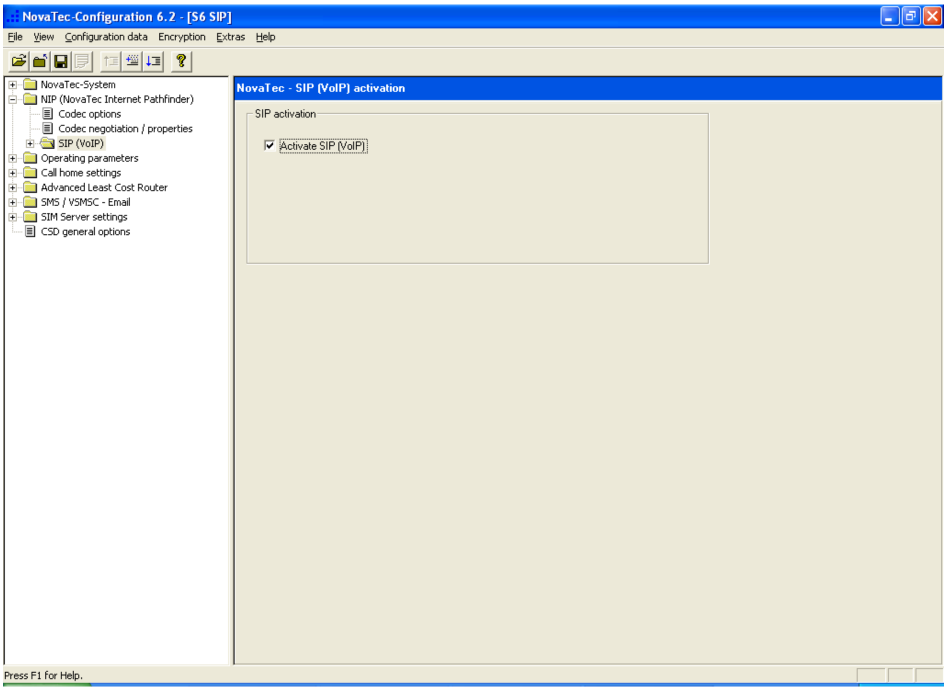
Go to tab „1-SIP“ and click button „Subscriber“. By doing so all of the configured subscribers are entered in the call number plan. (see below)



Objects	Number
Slot 01: CCU3 : Interface 01	956111
Slot 01: CCU3 : Interface 05	956222
Slot 02: ULU : Interface 01	956333

2.11 Activating SIP

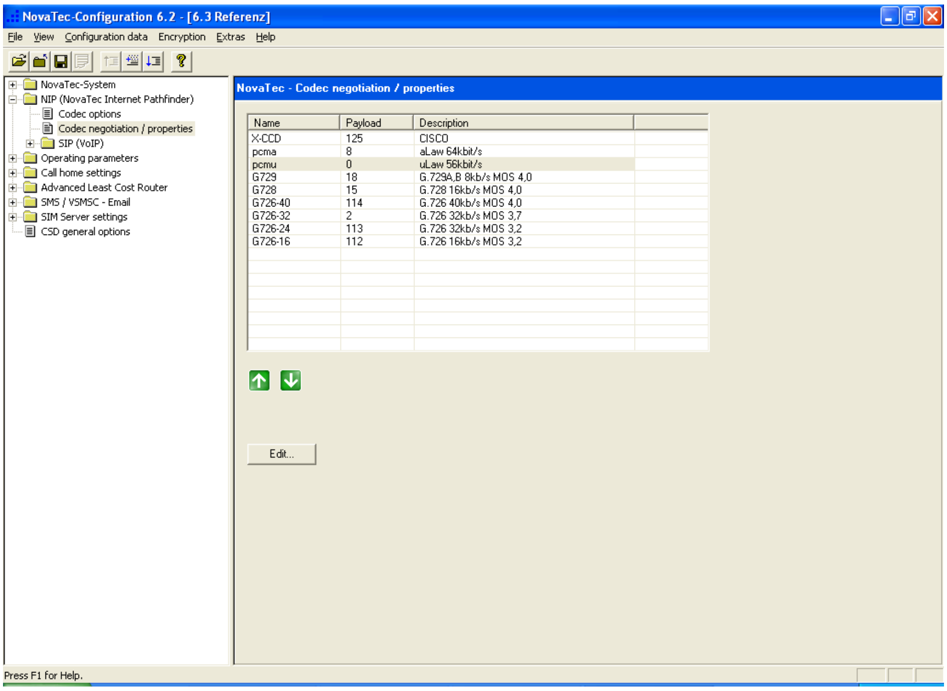
Open „NIP/SIP“ in the tree on the left and activate the option „Activate SIP“.


NovaTec-Configuration 6.2 - [S6 SIP]
File View Configuration data Encryption Extras Help
NovaTec-System
NIP (NovaTec Internet Pathfinder)
Codec options
Codec negotiation / properties
SIP (VoIP)
Operating parameters
Call home settings
Advanced Least Cost Router
SMS / VSMSC - Email
SIM Server settings
CSD general options
NovaTec - SIP (VoIP) activation
SIP activation
Press F1 for Help.

☑ Activate SIP (VoIP)

2.12 Defining codec priorities

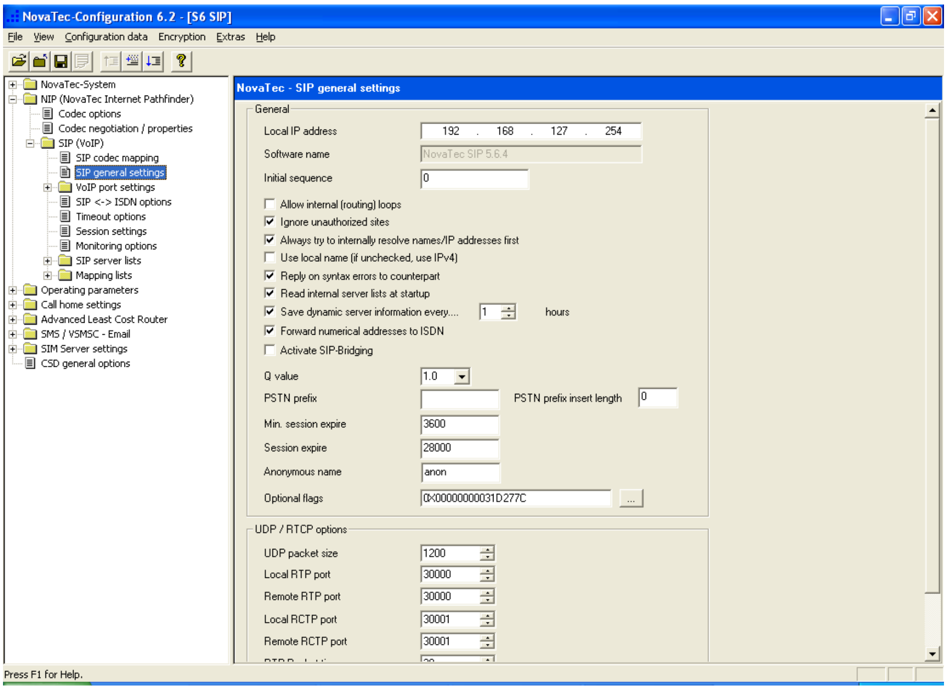
Choose „NIP/Codec negotiation“ in the left tree. Select a codec and use the buttons with the arrows to change the priority of the codec. The codec at the top of the list has the highest priority. The picture below shows a typical codec priority. The codec X-CCD (Cisco Clear Channel Codec) should always have the highest priority and be at the top of the list.


NovaTec-Configuration 6.2 - [6.3 Referenz]
File View Configuration data Encryption Extras Help
NovaTec-System
NIP (NovaTec Internet Pathfinder)
Codec options
Codec negotiation / properties
SIP (VoIP)
Operating parameters
Call home settings
Advanced Least Cost Router
SMS / VSMSC - Email
SIM Server settings
CSD general options
NovaTec - Codec negotiation / properties
Edit...
Press F1 for Help.

Name	Payload	Description
X-CCD	125	CISCO
pcma	8	aLaw 64kbit/s
pcmu	0	uLaw 56kbit/s
G729	18	G.729A,B 8kb/s MOS 4,0
G728	15	G.728 16kb/s MOS 4,0
G726-40	114	G.726 40kb/s MOS 4,0
G726-32	2	G.726 32kb/s MOS 3,7
G726-24	113	G.726 32kb/s MOS 3,2
G726-16	112	G.726 16kb/s MOS 3,2

2.13 Controlling general SIP settings

Choose „NIP/SIP/SIP general settings“ in the left hand tree. The setup should be shown as given below.



NovaTec - SIP general settings

General

Local IP address: 192 . 168 . 127 . 254

Software name: NovaTec SIP 5.6.4

Initial sequence: 0

☐ Allow internal (routing) loops
☑ Ignore unauthorized sites
☑ Always try to internally resolve names/IP addresses first
☐ Use local name (if unchecked, use IPv4)
☑ Reply on syntax errors to counterpart
☑ Read internal server lists at startup
☑ Save dynamic server information every.... 1 hours
☑ Forward numerical addresses to ISDN
☐ Activate SIP-Bridging

Q value: 1.0

PSTN prefix: PSTN prefix insert length: 0

Min. session expire: 3600

Session expire: 28000

Anonymous name: anon

Optional flags: 0X00000000031D277C

UDP / RTCP options

UDP packet size: 1200

Local RTP port: 30000

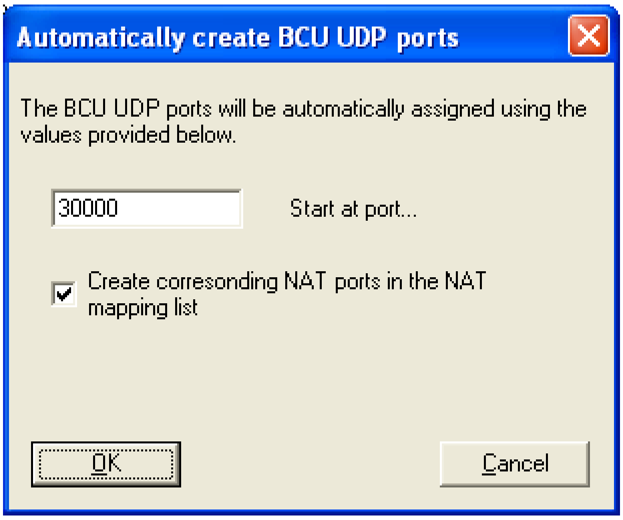
Remote RTP port: 30000

Local RCTP port: 30001

Remote RCTP port: 30001

2.14 Assignment of DP ports

Choose „NIP/SIP/VOIP port settings/VOIP UDP port assignment“ in the left hand tree and click on the button „Auto ports…“. Choose the IP port to be used for RTP by entering the first IP port to be used for RTP (see below).

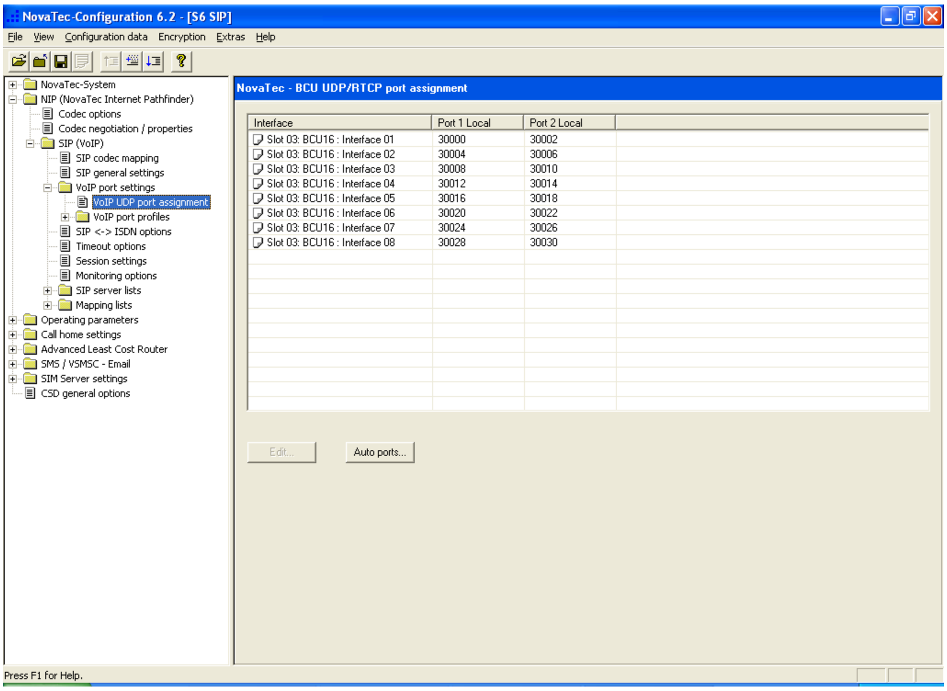


The BCU UDP ports will be automatically assigned using the values provided below.

30000 Start at port...

☑ Create corresonding NAT ports in the NAT mapping list

The configuration interface will then assign two IP ports for every VoIP interface. One for RTP and the next for RTCP.

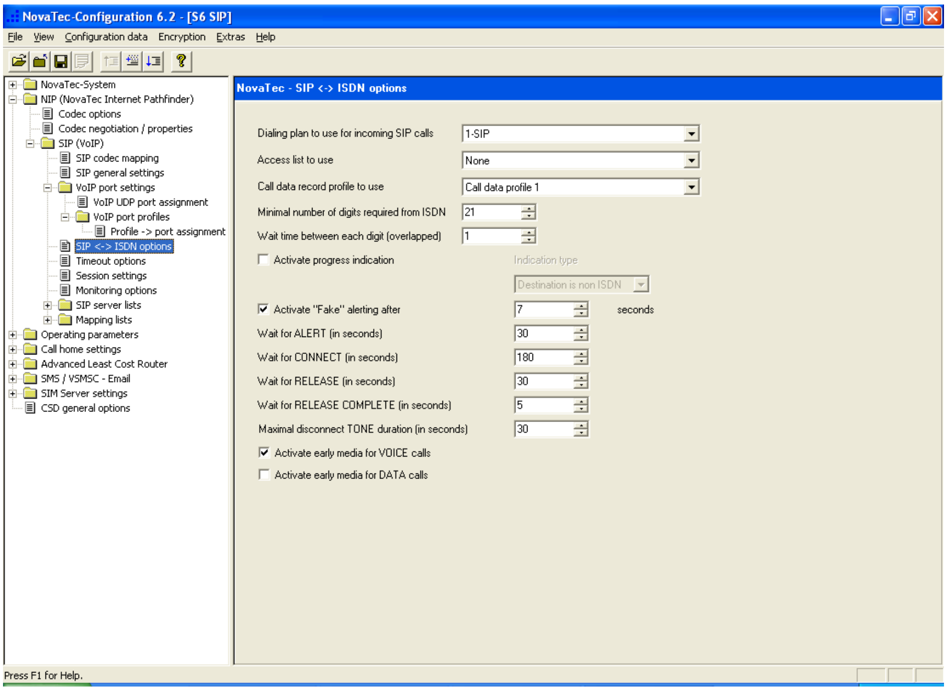


NovaTec - BCU UDP/RTCP port assignment

Interface	Port 1 Local	Port 2 Local
Slot 03: BCU16 : Interface 01	30000	30002
Slot 03: BCU16 : Interface 02	30004	30006
Slot 03: BCU16 : Interface 03	30008	30010
Slot 03: BCU16 : Interface 04	30012	30014
Slot 03: BCU16 : Interface 05	30016	30018
Slot 03: BCU16 : Interface 06	30020	30022
Slot 03: BCU16 : Interface 07	30024	30026
Slot 03: BCU16 : Interface 08	30028	30030

2.15 SIP ISDN options

Go to „NIP/SIP/SIP <-> ISDN options“ in the left hand tree and set up the following adjustments.



NovaTec - SIP <-> ISDN options

Dialing plan to use for incoming SIP calls: 1-SIP

Access list to use: None

Call data record profile to use: Call data profile 1

Minimal number of digits required from ISDN: 21

Wait time between each digit (overlapped): 1

☐ Activate progress indication

Indication type: Destination is non ISDN

☑ Activate "Fake" alerting after 7 seconds

Wait for ALERT (in seconds): 30

Wait for CONNECT (in seconds): 180

Wait for RELEASE (in seconds): 30

Wait for RELEASE COMPLETE (in seconds): 5

Maximal disconnect TONE duration (in seconds): 30

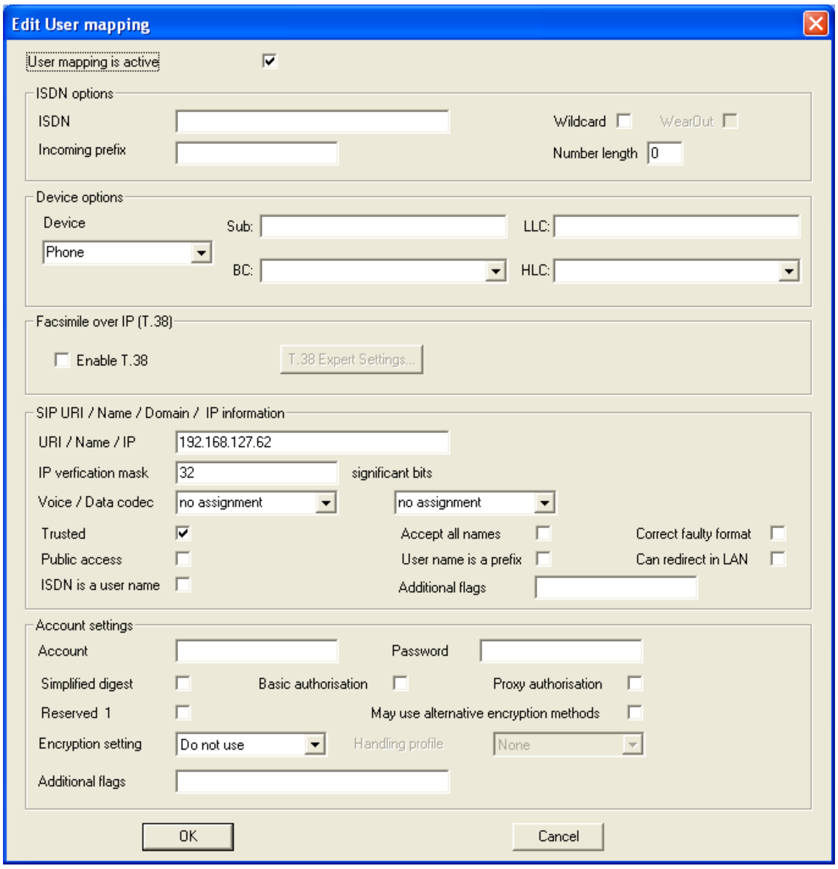
☑ Activate early media for VOICE calls

☐ Activate early media for DATA calls

2.16 Mapping Lists

Go to „NIP/SIP/Mapping lists/User mapping“ in the left hand tree and click „New“.

Adjust set up as given below. Enter the IP address of your Cisco Unified Communications Manager under “URI / Name / IP”.



Edit User mapping

User mapping is active ☑

ISDN options

ISDN:
Wildcard ☐ WearOut ☐
Incoming prefix:
Number length: 0

Device options

Device: Phone
Sub:
LLC:
BC:
HLC:

Facsimile over IP (T.38)

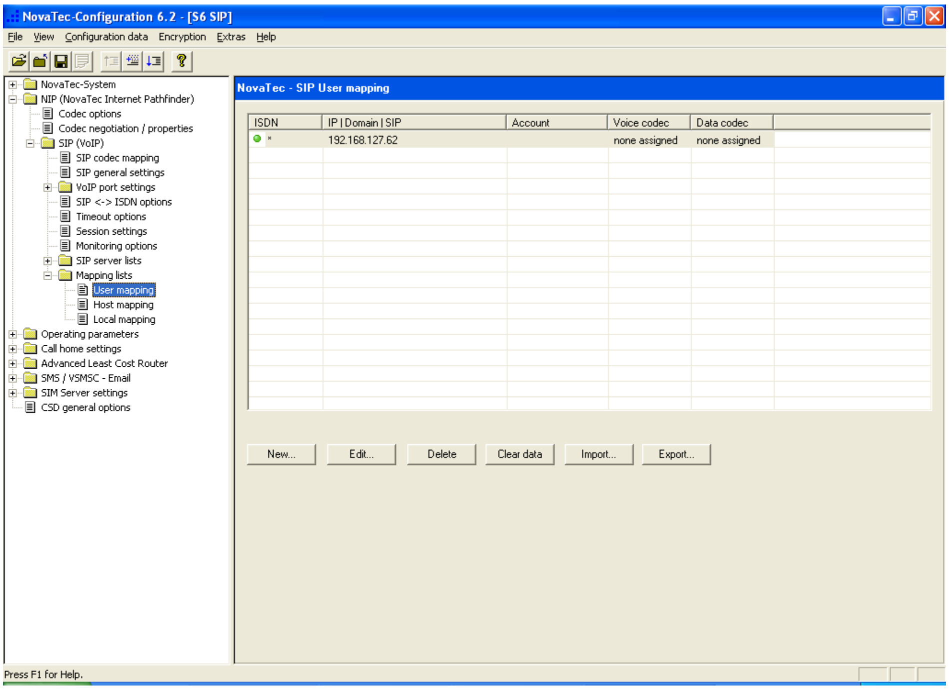
☐ Enable T.38

SIP URI / Name / Domain / IP information

URI / Name / IP: 192.168.127.62
IP verfication mask: 32 significant bits
Voice / Data codec: no assignment / no assignment
Trusted ☑
Public access ☐
ISDN is a user name ☐
Accept all names ☐
User name is a prefix ☐
Additional flags:
Correct faulty format ☐
Can redirect in LAN ☐

Account settings

Account:
Password:
Simplified digest ☐
Basic authorisation ☐
Proxy authorisation ☐
Reserved 1 ☐
May use alternative encryption methods ☐
Encryption setting: Do not use
Handling profile: None
Additional flags:



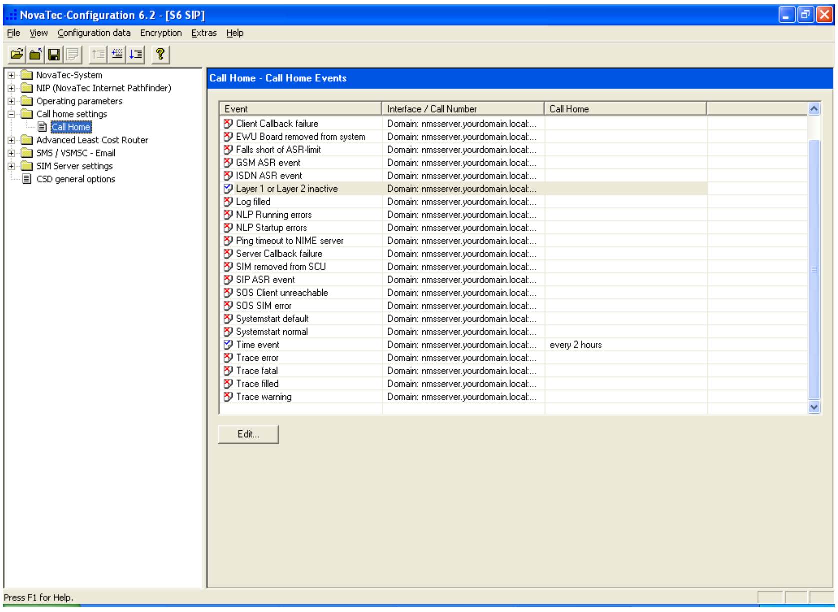
NovaTec - SIP User mapping

ISDN	IP | Domain | SIP	Account	Voice codec	Data codec
● *	192.168.127.62		none assigned	none assigned

After confirming with „Ok“ you will find the IP address of your Cisco Unified Communications manager in the overview.

2.17 Call Home Settings

Choose „Call home settings“ in the left hand tree and activate the desired call home events that are to be reported to the NovaTec network management system.

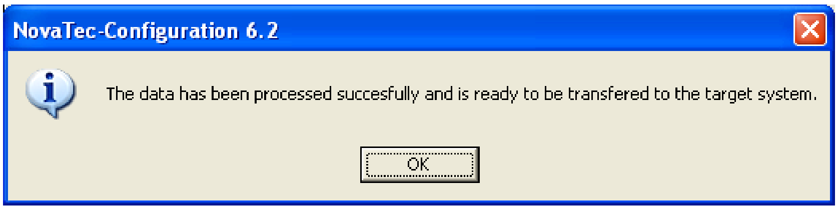

NovaTec-Configuration 6.2 - [S6 SIP]
File View Configuration data Encryption Extras Help
NovaTec-System
NIP (NovaTec Internet Pathfinder)
Operating parameters
Call home settings
Call Home
Advanced Least Cost Router
SMS / VSMSC - Email
SIM Server settings
CSD general options
Edit...
Press F1 for Help.

Call Home - Call Home Events

Event	Interface / Call Number	Call Home
☒ Client Callback failure	Domain: nmsserver.yourdomain.local:...	
☒ EWU Board removed from system	Domain: nmsserver.yourdomain.local:...	
☒ Falls short of ASR-limit	Domain: nmsserver.yourdomain.local:...	
☒ GSM ASR event	Domain: nmsserver.yourdomain.local:...	
☒ ISDN ASR event	Domain: nmsserver.yourdomain.local:...	
☑ Layer 1 or Layer 2 inactive	Domain: nmsserver.yourdomain.local:...	
☒ Log filled	Domain: nmsserver.yourdomain.local:...	
☒ NLP Running errors	Domain: nmsserver.yourdomain.local:...	
☒ NLP Startup errors	Domain: nmsserver.yourdomain.local:...	
☒ Ping timeout to NIME server	Domain: nmsserver.yourdomain.local:...	
☒ Server Callback failure	Domain: nmsserver.yourdomain.local:...	
☒ SIM removed from SCU	Domain: nmsserver.yourdomain.local:...	
☒ SIP ASR event	Domain: nmsserver.yourdomain.local:...	
☒ SOS Client unreachable	Domain: nmsserver.yourdomain.local:...	
☒ SOS SIM error	Domain: nmsserver.yourdomain.local:...	
☒ Systemstart default	Domain: nmsserver.yourdomain.local:...	
☒ Systemstart normal	Domain: nmsserver.yourdomain.local:...	
☑ Time event	Domain: nmsserver.yourdomain.local:...	every 2 hours
☒ Trace error	Domain: nmsserver.yourdomain.local:...	
☒ Trace fatal	Domain: nmsserver.yourdomain.local:...	
☒ Trace filled	Domain: nmsserver.yourdomain.local:...	
☒ Trace warning	Domain: nmsserver.yourdomain.local:...	

2.18 Preparing the data base and transferring it onto the system

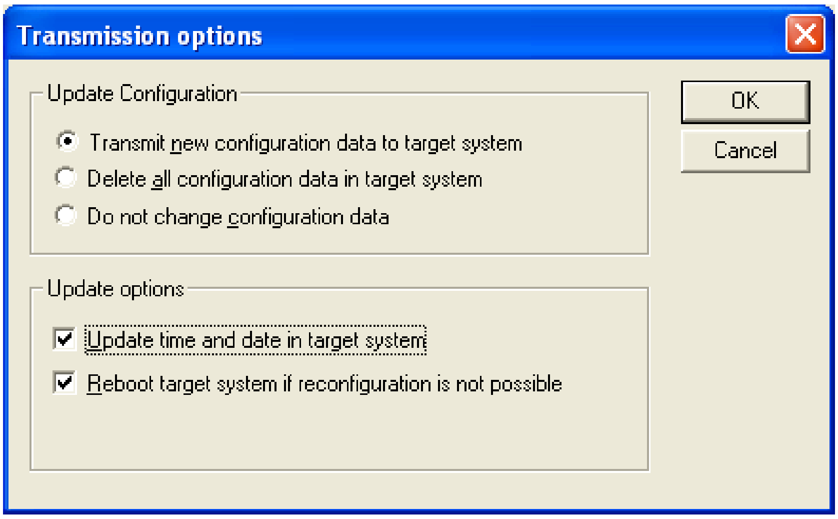
Press „Configuration data/Process“ in your menu bar. If no major mistakes or inconsistencies are existent in the configuration setup the following window will show up:


NovaTec-Configuration 6.2

The data has been processed succesfully and is ready to be transfered to the target system.

Confirm by pressing button „Ok“. Should you receive an error report please check your setup.

Choose „Configuration data/Transmit to target system“ in the menu.


Transmission options

Update Configuration

● Transmit new configuration data to target system
○ Delete all configuration data in target system
○ Do not change configuration data

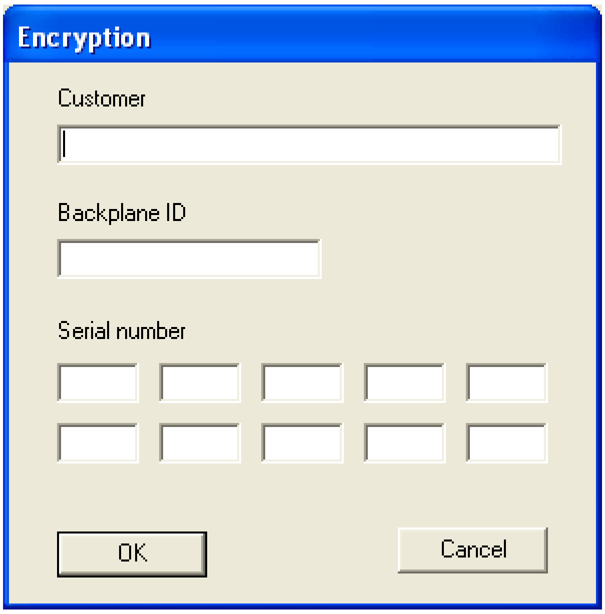
Update options

☑ Update time and date in target system
☑ Reboot target system if reconfiguration is not possible

Adjust as given above and confirm with „Ok“.

2.19 Activation of SRTP

Go to „Encryption/Enter serial number…“ in the left hand tree.



The encryption data is constructed by NovaTec and delivered to the customer in the following form:

User name: *xxxxxxxxxxxx (e.g. name of customer)*

Backplane ID: *000006767676*

Serial number:

FB11 - EF76 - CA90 - EC73 - EF00
BF12 - AE30 - CC47 - FC46 - AD47

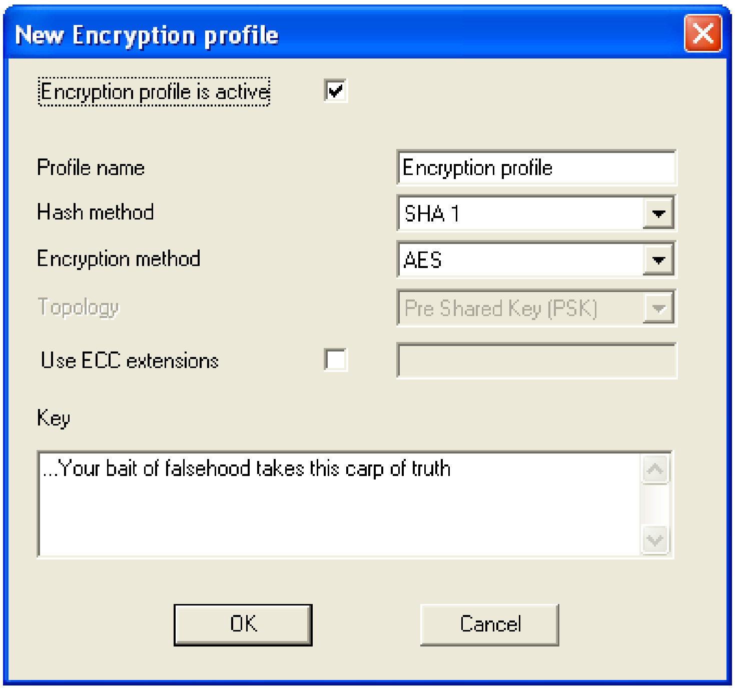
After the encryption data was entered close the data base and reopen it.

These steps are also necessary:

Go to „NovaTec-System/System encryption options/Encryption profiles“ in the left hand tree and click „New“.

Pick your encryption options (see below).

Confirm with „Ok“.



New Encryption profile

Encryption profile is active ☑

Profile name: Encryption profile

Hash method: SHA 1

Encryption method: AES

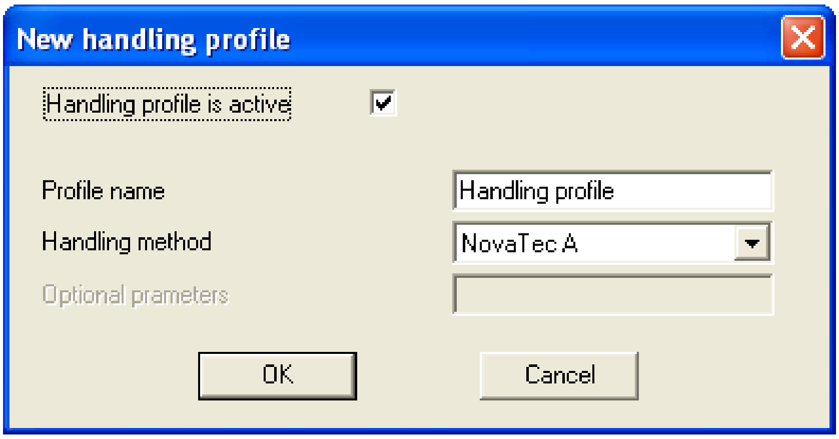
Topology: Pre Shared Key (PSK)

Use ECC extensions ☐

Key: ...Your bait of falsehood takes this carp of truth

Go to *„NovaTec-System/System encryption options/Encryption handling profiles“* in the left hand tree and click *„New“.*

Adjust setup as given below and confirm with “Ok”.



New handling profile

Handling profile is active ☑

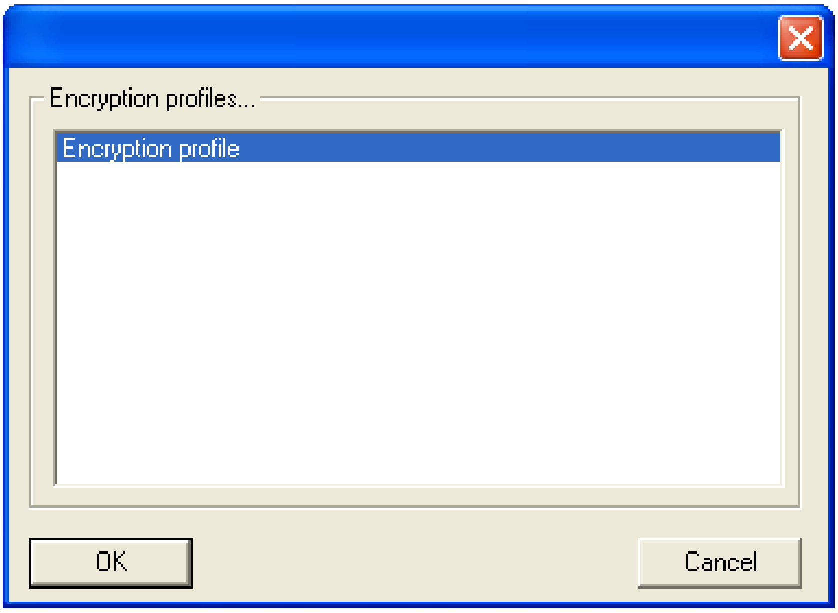
Profile name: Handling profile

Handling method: NovaTec A

Optional prameters

Select *“NovaTec-System/System encryption options/Encryption handling/profiles/Encryption ->Handling assignment“* and click *„New”*.

Choose *„Encryption profile“* and confirm *„OK“*.

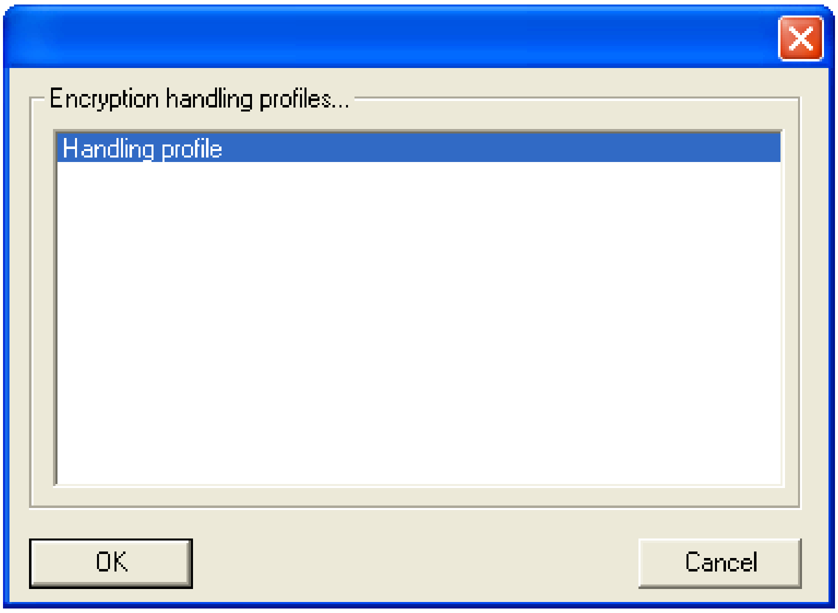


Encryption profiles...

Encryption profile

Pick *“NovaTec-System/System encryption options/System module / interface settings/Module assignment“* in the left hand tree and click *„New“*.

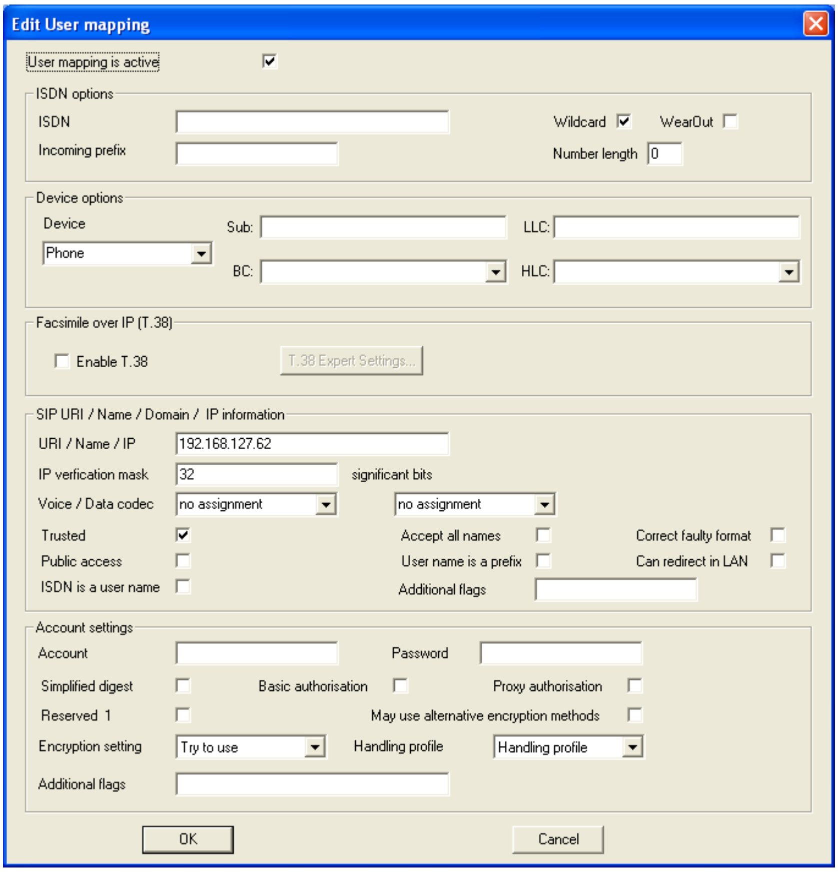
Choose *„Handling profile“* and confirm *„OK“*.



Encryption handling profiles...

Handling profile

Go to *„NIP/SIP/Mapping lists/User mapping“* in the left hand tree and click *„Edit“*. Choose “Try to use” for *„Encryption setting“* and *„Handling profile“* for *„Handling profile“*.



Edit User mapping

User mapping is active ☑

ISDN options

ISDN

Incoming prefix

Wildcard ☑ WearOut □

Number length 0

Device options

Device: Phone

Sub:

LLC:

BC:

HLC:

Facsimile over IP (T.38)

□ Enable T.38

SIP URI / Name / Domain / IP information

URI / Name / IP: 192.168.127.62

IP verfication mask: 32 significant bits

Voice / Data codec: no assignment, no assignment

Trusted ☑

Public access □

ISDN is a user name □

Accept all names □

User name is a prefix □

Additional flags

Correct faulty format □

Can redirect in LAN □

Account settings

Account

Password

Simplified digest □

Basic authorisation □

Proxy authorisation □

Reserved 1 □

May use alternative encryption methods □

Encryption setting: Try to use

Handling profile: Handling profile

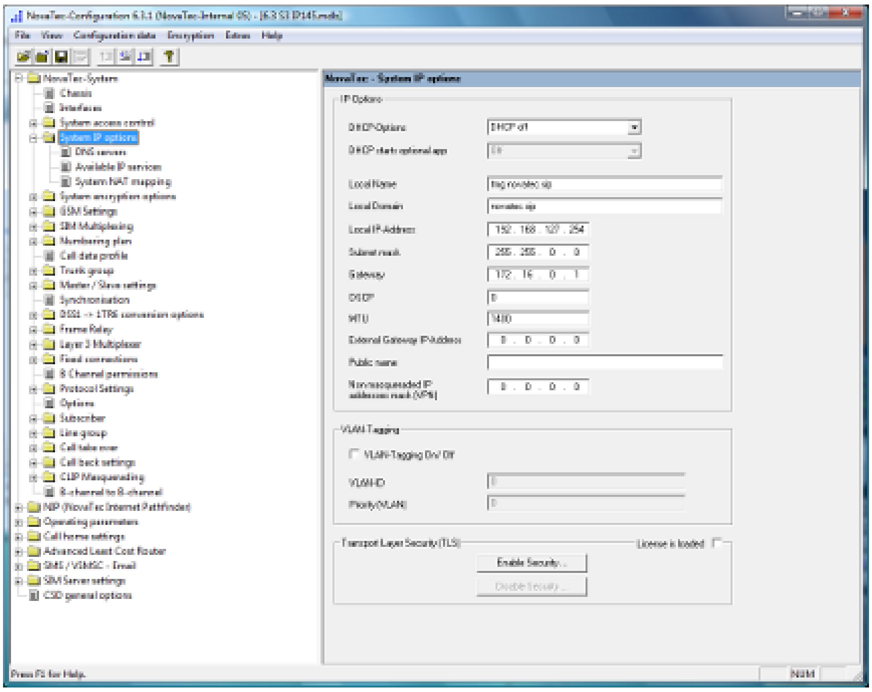
Additional flags

Confirm *„OK“*.

Repeat steps from 2.17. Call Home Settings.

3 Activate DCHP

By choosing „System-IP-Options“ in the left part of the application window „NTConf“ the following dialogue is shown on the right hand side of the window.



DHCP-Options: DHCP off
DHCP starts optional app:
Local Name: ntg.novatec.sip
Local Domain: novatec.sip
Local IP-Address: 192 . 168 . 127 . 254
Subnet mask: 255 . 255 . 0 . 0
Gateway: 172 . 16 . 0 . 1
DSCP: 0
MTU: 1400
External Gateway IP-Address: 0 . 0 . 0 . 0
Public name:
Non-masqueraded IP addresses mask (VPN): 0 . 0 . 0 . 0
□ VLAN-Tagging On/ Off
VLAN-ID: 0
Priority(VLAN): 0

Picture 1: DHCP options

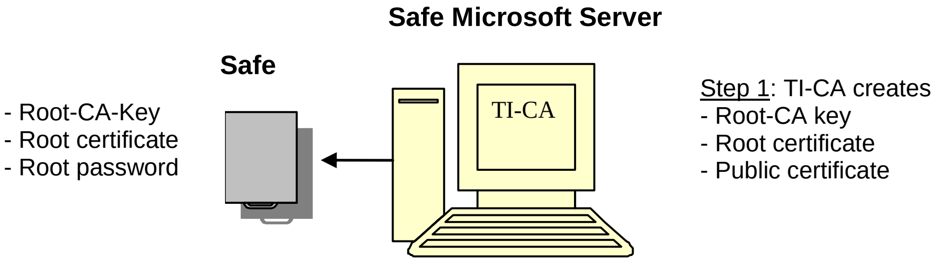
DHCP options can only be defined by choosing the appropriate items in the combo boxes (choice boxes).

If DHCP is activated unnecessary entry boxes are shown grey, i.e. are deactivated.

4 General procedure TLS

The following procedure is recommended to all customers for the safe handling of encryption (TLS/SRTP) between the NovaTec-Systems resp. with the Service-PC.

4.1 Creation of a "Root Certification Authority Certificate"



Picture 1: Create Root-CA

The first step in preparation for the customer is to uniquely generate a „Root Certification Authority Certificate" (Root-CA). Should the customer already have a certificate of a certifying body this step can be left out.
The creation of a Root-CA has to be done with the NovaTec tool „Trace Info Client" (TI-CA). The application needs to be installed on an access secure Microsoft server. Access secure means the server is within a locked room without LAN access.
Via the „Graphical User Interface" of the TI-CA application an encrypted Root-CA key (cakey.pem), a root certificate (cacert.pem) and a public certificate (cacert.crt) are created.

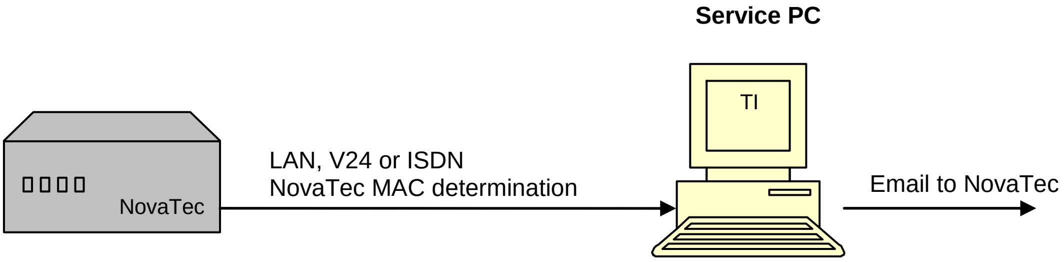
The Root-CA key (cakey.pem) and the password to this key are the most sensitive parts of a CA infrastructure and have to be kept within the customers safe together with the root certificate.

For the transport to the safe you can declare to the TI e.g. an USB stick as data carrier for the output file and store this within the safe.

The secured Root-CA is solely conducted to the signing of other certificates (see no. 5).

The public certificate (cacert.crt) is provided to all systems within this CA infrastructure (see no. 3).

4.2 Drawing a system clearing code

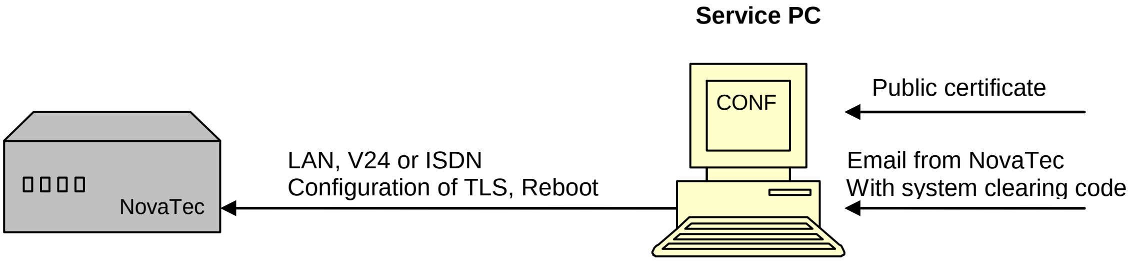


Picture 2: sourcing TLS license

In step 2 the customer has to read out the MAC address of the corresponding system (S3, S5, S6 or S20) with the help of the TI application and send this to NovaTec support via mail.

NovaTec determines an individual system clearing code for this system and forwards it to the customer via mail.

4.3 Configuring encryption



Picture 3: Configuring TLS for a NovaTec system

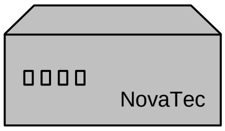
In this step only the system with the corresponding MAC address can be configured resp. be cleared for TLS via the NovaTec configuration program.

There are three categories in the configuration interface for this: NMS, SIP and Maintenance. Maintenance includes the applications TraceInfo Client, NovaTec Configuration and Call Server.

After entering the clearing codes (step 2) the three named categories can be engaged and configured for TLS/SRTP. Depending on the security grade the modes as given in tablet 1 are possible, e.g. importing of the public certificate (cacert.crt) from step 1.

The unsecured access to the systems on site is no longer possible after TLS was activated. All accesses via V24/USB, ISDN and IP like HTTP and TELNET are not accepted.

4.4 Creating the private key within the system



Creation of
- Encrypted private key
- Request for MNT, NMS and SIP

Picture 4: NovaTec system creates private key and requests

This step is only successful if the configuration in the prior step has been effected completely and flawlessly. This step is automatically run when rebooting and takes 20-30 seconds extra to the normal reboot time.

Beginning with the transfer of the configuration data onto the hardware it checks the clearing code after the necessary reboot for validity. If the check is positive the NovaTec hardware will accept the new configuration with encryption.

Additionally the reboot process causes the following system internal actions after a successful configuration:

- Creating a hardware private key

Creation of an encrypted private RSA key which is stored in the non-volatile memory of the hardware. There is no possibility to access this storage from the outside.
The key stays within the hardware device and can neither be read nor overwritten or deleted. The password for the key is not saved but generated individually and dynamically for the hardware runtime. As such for every system a new password is created.

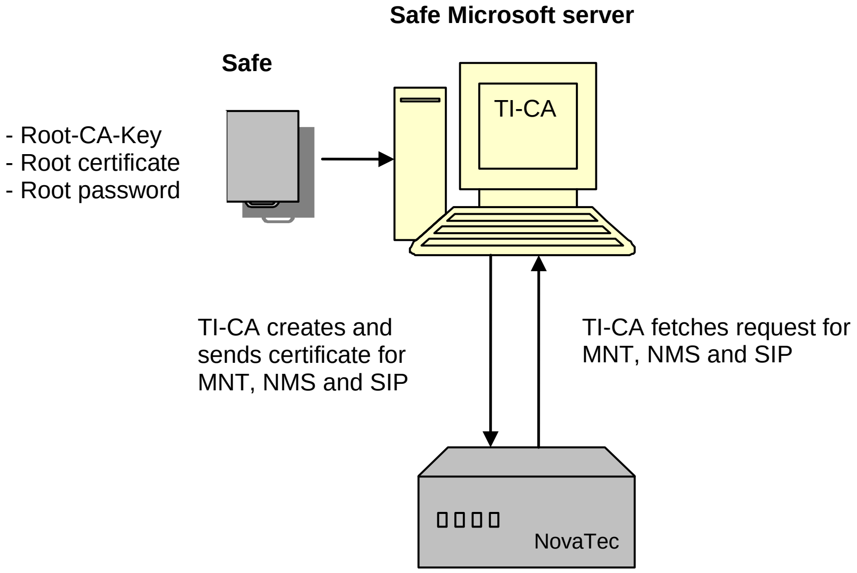
- Creating a hardware certificate signing request

After the creation of a private key each of the configured three categories (see no. 3) generates a corresponding certification signing request.

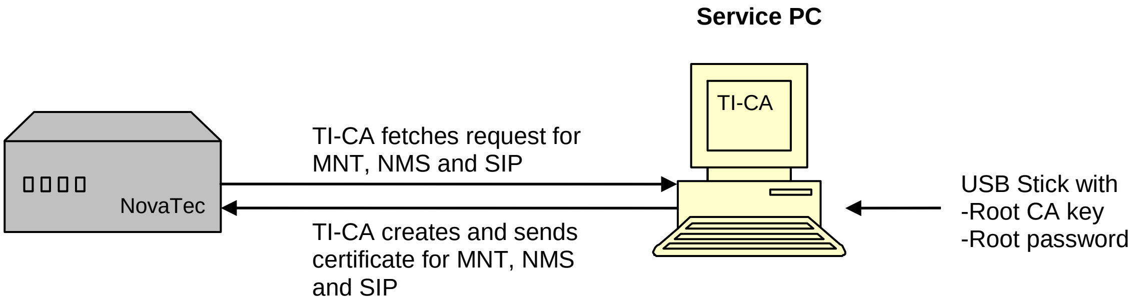
For Maintenance, NMS and SIP produce the files mtn_req.csr , nms_req.csr and sip_req.csr with the help of the private key and saves these in the freely accessible flash data system

Warning: The request files are automatically deleted directly after the first successful opening of the corresponding certificate.

4.5 Signing of the hardware certificate signing request


Safe Microsoft server
Safe
- Root-CA-Key
- Root certificate
- Root password
TI-CA
TI-CA creates and sends certificate for MNT, NMS and SIP
TI-CA fetches request for MNT, NMS and SIP
NovaTec

Picture 5: NovaTec system is locally signed by server


Service PC
TI-CA
NovaTec
TI-CA fetches request for MNT, NMS and SIP
TI-CA creates and sends certificate for MNT, NMS and SIP
USB Stick with
-Root CA key
-Root password

Picture 6: NovaTec system is signed by service PC

The three certification signing requests created by the hardware in step 4 have to be signed by the Root-CA (e.g. the next higher CA's, see also step 1).

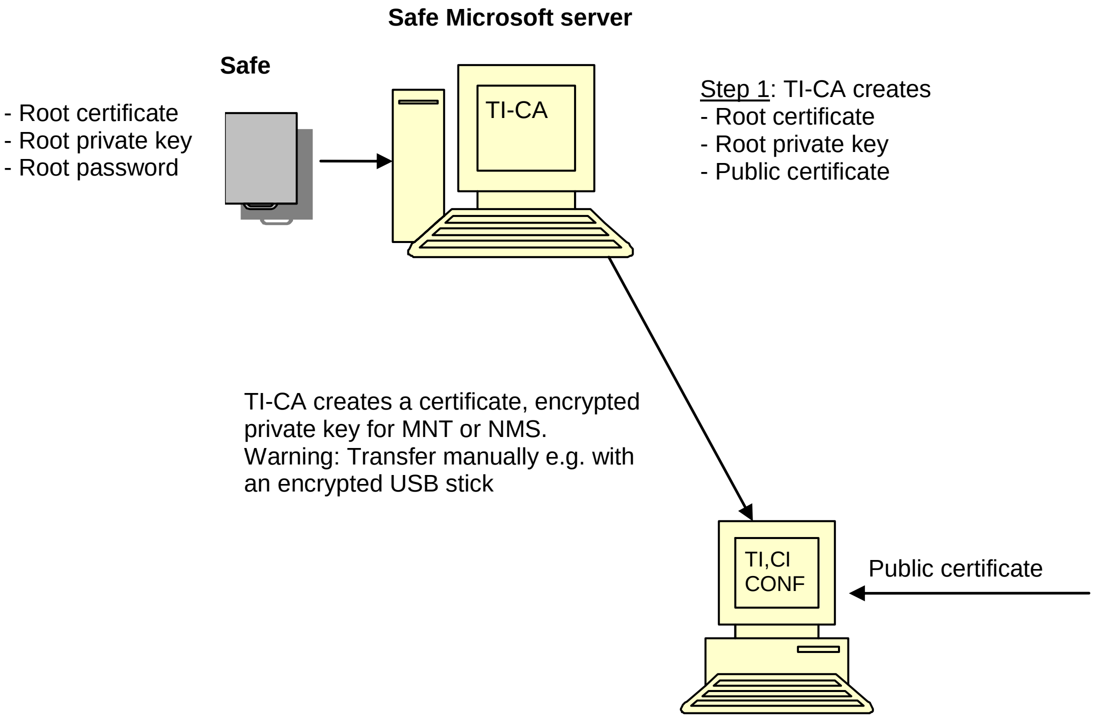
During this action you receive the corresponding certificates (data sets) for the hardware: mtn_cert.crt, nms_cert.crt and sip_cert.crt.

The procedure of step 5 is again safety problematical as for this purpose the encrypted Root CA key (cakey.pem from step 1) as well as the password are needed.

The transport of the key from the safe to the secure server (step 1) can be made by USB stick. The TI-CA can import the data set (cakey.pem) directly from the USB stick.

Warning: If the certificate is invalid the system blocks and has to be brought into default mode on site. In this mode the system cannot be used within the network and needs a corresponding configuration once again. The new configuration can be transferred onto the system with help of the NovaTec tools or you can change the IP settings of the system with help of e.g. Telnet in such way as to enable it to load the configuration from NMS.

4.6 Creation of the PC key and certificates



Picture 7: TI-CA signs the NovaTec PC tools MNT and NMS

In order to enable the service PC to communicate with the NovaTec hardware with TLS the PC applications have to be included in the CA infrastructure. TI-CA creates an encrypted private key and a certificate signed by the CA to achieve this. These data sets have to be saved on the service PC together with the public certificate of the CA and imported into TI, CI, CONF and NMS. The password of the private key also has to be imported (e.g. with an encrypted USB stick).

After this step all actions are completed and the service PC can communicate TLS encrypted with the NovaTec system.

This step is unnecessary with SIP connections in between the NovaTec systems.

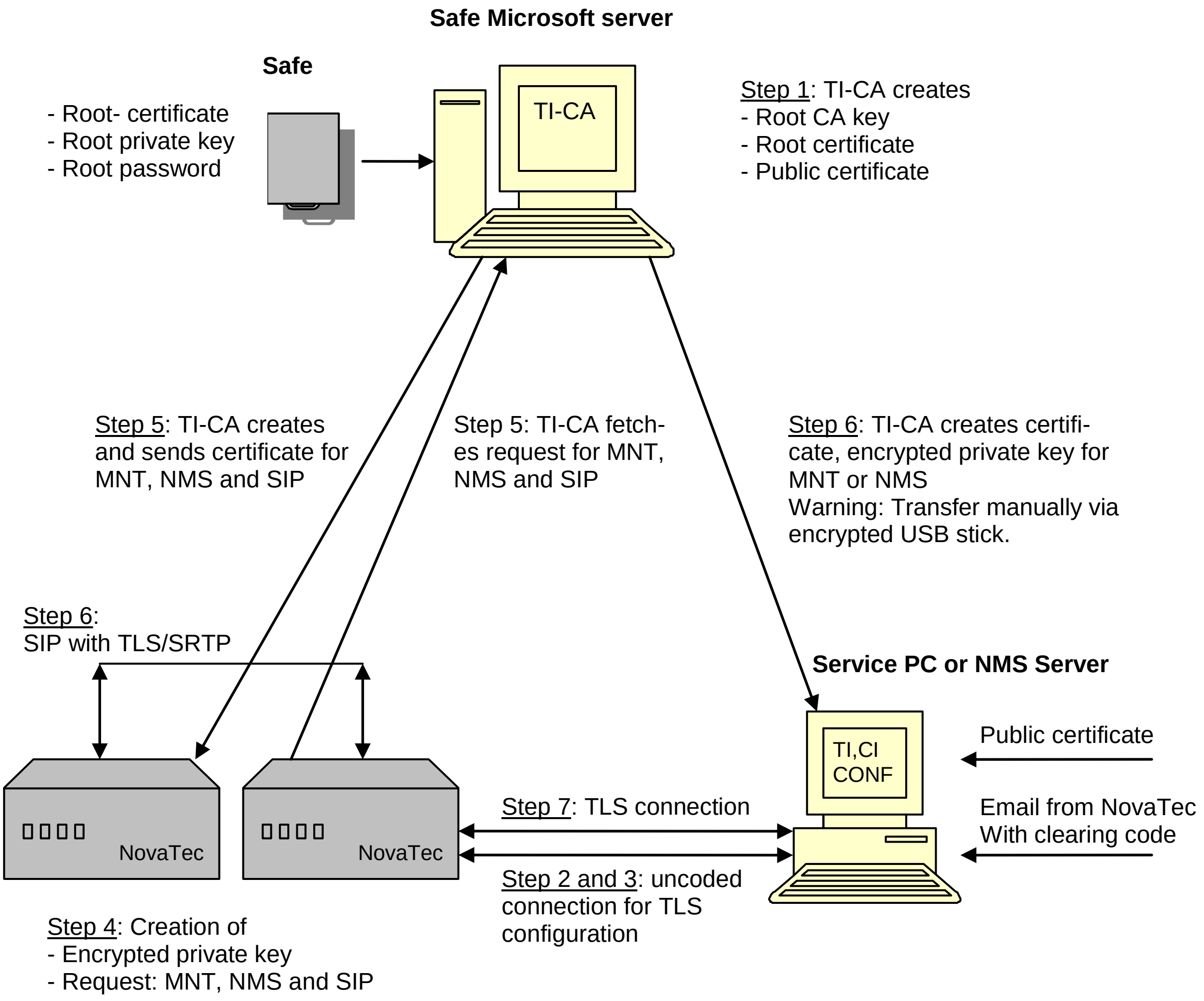
4.7 Explanation of hardware TLS1.0 Modi as per RFC4346

Server modes for the applications Maintenance (TI, NtConf, Callserver) and SIP

Mode	Server key	Server-Cert	CA-Cert	Notes
0	-	-	-	Encrypted
1	mandatory	-	-	Anonymous Mode Is not supported
2	mandatory	mandatory	-	Optional: No client check safety: medium
3	mandatory	mandatory	mandatory	Full check: Safety high
4-8	-	-	-	not permitted with TLS

Client modes for the applications NMS and SIP

Mode	Client key	Client-Cert	CA-Cert	Notes
1	mandatory	-	-	Anonymous Mode Is not supported
2	mandatory	-	mandatory	Optional: No client check safety: medium
3	mandatory	mandatory	mandatory	Full check: Safety high
4-8	-	-	-	Not permitted with TLS



Picture 8: CA infrastructure

Comments on step 5:

The communication between TI-CA and the NovaTec system is effected manually for the time being with their own MMX protocol. If the customer has no own CA server in the second step the protocol SCEP (Simple Certificate Enrollment Protocol) can make sure of an automatically encrypted data exchange (SCEP is not part of the delivery for the time being).

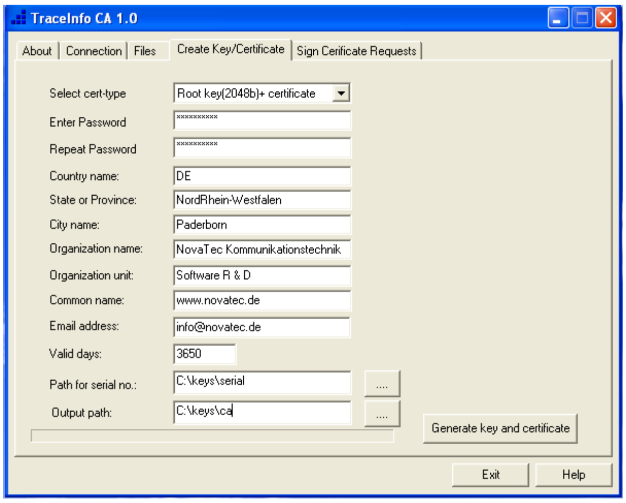
5 TLS

5.1 Creating a Root-CA

DE_TICA_CREATECERT

An user can create the following with the application TI-CA:

CA private key and root certificate
Certificate request for client or server



Select cert-type	Root key(2048b)+ certificate
Enter Password	**********
Repeat Password	**********
Country name:	DE
State or Province:	NordRhein-Westfalen
City name:	Paderborn
Organization name:	NovaTec Kommunikationstechnik
Organization unit:	Software R & D
Common name:	www.novatec.de
Email address:	info@novatec.de
Valid days:	3650
Path for serial no.:	C:\keys\serial
Output path:	C:\keys\ca

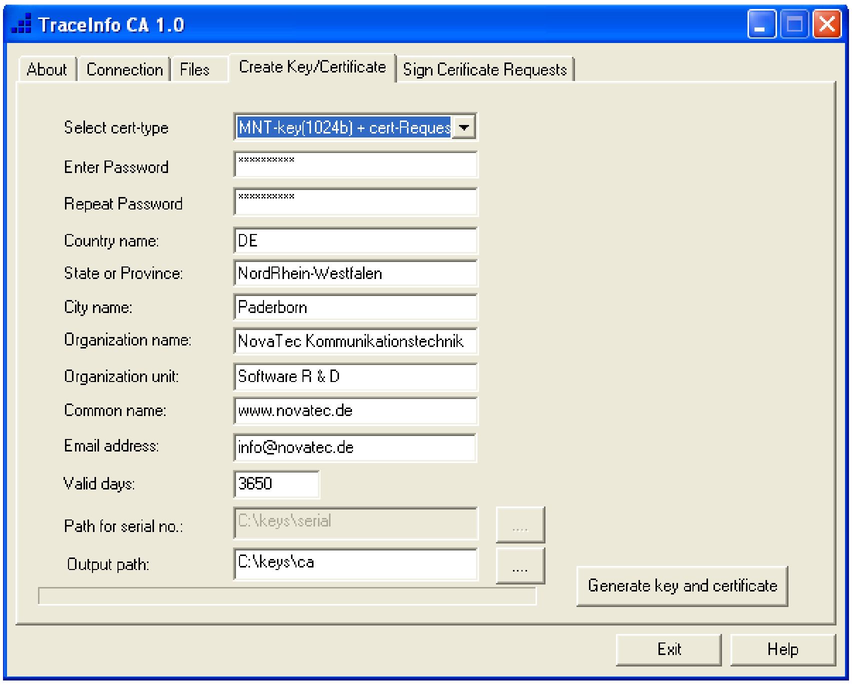
a) Creating CA private key and root certificate:

- Select flag “Create Key/Certificate”.
- A connection to the NovaTec system is not essentially necessary.
- Choose “Root key (2048b) + Certificate” in the combobox.
- Enter a CA password. The password has a minimum length of four and a maximum length of 20 figures.
- Repeat your CA password. Please keep your password in mind. If you wish to sign anything with this root certificate you will need it.
- The next steps are the entry of the CA identity such as land, province, town, organization, organization unit, common names and email address. For the Land you always need to enter two figures. The other entries may have a maximum length of 64 figures.
- Enter the validity of the root certificate in days.
- Enter an index path in which the data set serial.txt resides.(1)
- Enter the index path in which the created CA private key and root certificate are to be saved. The created data sets are named cakey.pem and ca_cert.crt.
- If all entries are completed press button „Generate key and certificate“. The application needs a few seconds to create the private key. Please confirm all notices with „Ok“.

Note(1)**:**

The serial number of a certificate is administered by a data set serial.txt. If this data set is not existent in the given path the application will design it anew and will assign a default start serial number.
If you want to assign the serial number yourself write a 16-digit hexadecimal number e.g. 0123456789ABCDEF into the data set serial.txt. After usage the number is incremented in serial.txt.

b) Creating certificate request for client or server:



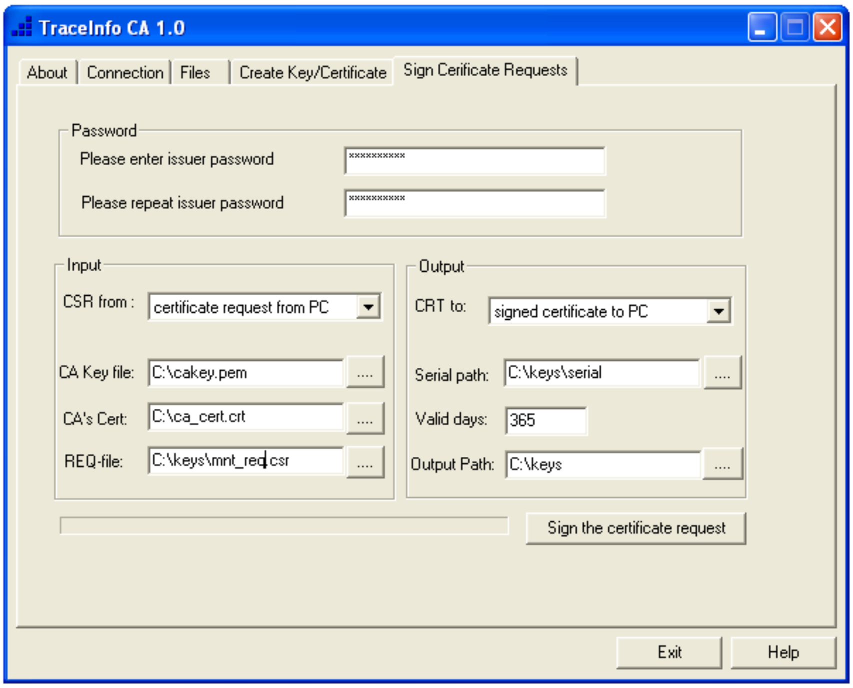
Select cert-type: MNT-key(1024b) + cert-Reques
Enter Password: **********
Repeat Password: **********
Country name: DE
State or Province: NordRhein-Westfalen
City name: Paderborn
Organization name: NovaTec Kommunikationstechnik
Organization unit: Software R & D
Common name: www.novatec.de
Email address: info@novatec.de
Valid days: 3650
Path for serial no.: C:\keys\serial
Output path: C:\keys\ca

- Select flag “Create Key/Certificate”.
- A connection to the NovaTec system is not essentially necessary.
- Choose “MNT-key (1024b) + Cert-Request” or “NMS-key (1024b) + Cert-Request” in the combobox. You need MNT request for Maintenance and NMS request for the NMS server.
- Enter a password. The password has a minimum length of four and a maximum length of 20 figures.
- Repeat your password. Please keep your password in mind. If you wish to sign anything with this root certificate you will need it.
- The next steps are the entry of the subjects identity such as land, province, town, organization, organization unit, common names and email address. For the Land you always need to enter two figures. The other entries may have a maximum length of 64 figures.
- Enter the validity of the request in days.
- Enter the index path in which the created CA private key and root certificate are to be saved.
- If all entries are completed press button “Generate key and certificate”. The application needs a few seconds to generate the private key. Please confirm the notices with “Ok“.

DE_TICA_SIGNCERT

With the application TI-CA you can sign a certificate request in a certificate during which the certificate request can be situated on a PC or in a NovaTec device.

Case 1)
Sign a certificate request whilst this request is situated on a PC. The signed data set is written in a PC path. If needed the signed data set can be written in a NovaTec device.



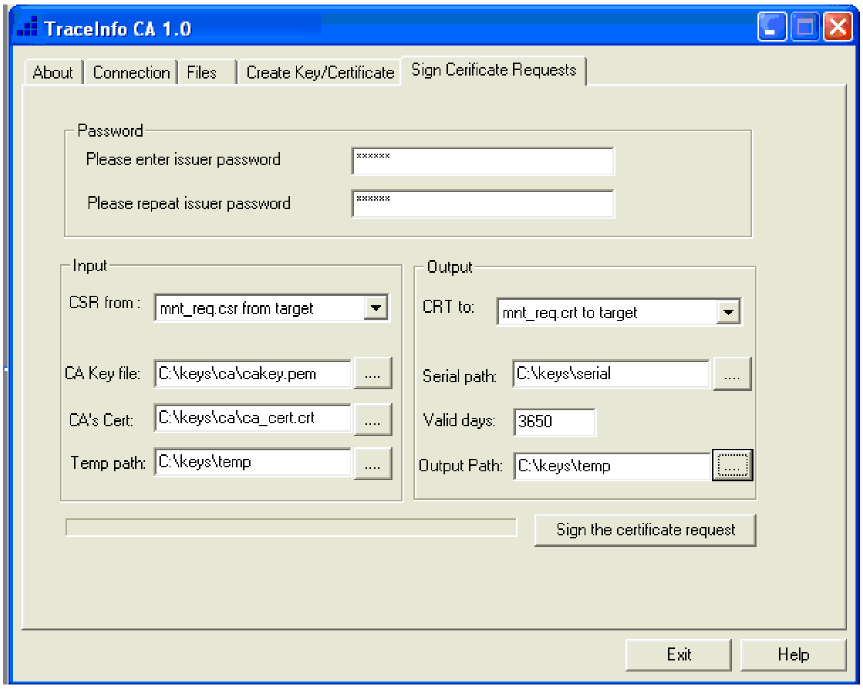
Password
Please enter issuer password: ***********
Please repeat issuer password: ***********

Input
CSR from : certificate request from PC
CA Key file: C:\cakey.pem
CA's Cert: C:\ca_cert.crt
REQ-file: C:\keys\mnt_req.csr

Output
CRT to: signed certificate to PC
Serial path: C:\keys\serial
Valid days: 365
Output Path: C:\keys

- Select flag “Sign Certificate Requests”.
- A connection to the NovaTec device is only necessary if you want to rewrite the signed data set onto the NovaTec device.
- Enter a CA password. This is the corresponding password to the CA private key.
- Repeat your password.
- Enter the following input feeds:
  - Select “certificate request from PC” in the combobox.
  - Enter the CA private key.
  - Enter the CA certificate.
  - Enter the certificate request to be signed.
- Enter the following output feeds:
  - Select “signed certificate to PC” in the combobox.
  - Enter the index path where the data set serial.txt is situated.(1)
  - Enter the validity of the certificate in days.
  - Enter the index path in which the signed certificate is to be written.
- If all entries are completed press the button “Sign the certificate request”.

Case 2)
Sign certificate requests whilst the request is situated on a NovaTec device. The signed data set can be rewritten on a NovaTec device or in the PC if necessary.



Password
Please enter issuer password: ******
Please repeat issuer password: ******

Input
CSR from : mnt_req.csr from target
CA Key file: C:\keys\ca\cakey.pem
CA's Cert: C:\keys\ca\ca_cert.crt
Temp path: C:\keys\temp

Output
CRT to: mnt_req.crt to target
Serial path: C:\keys\serial
Valid days: 3650
Output Path: C:\keys\temp

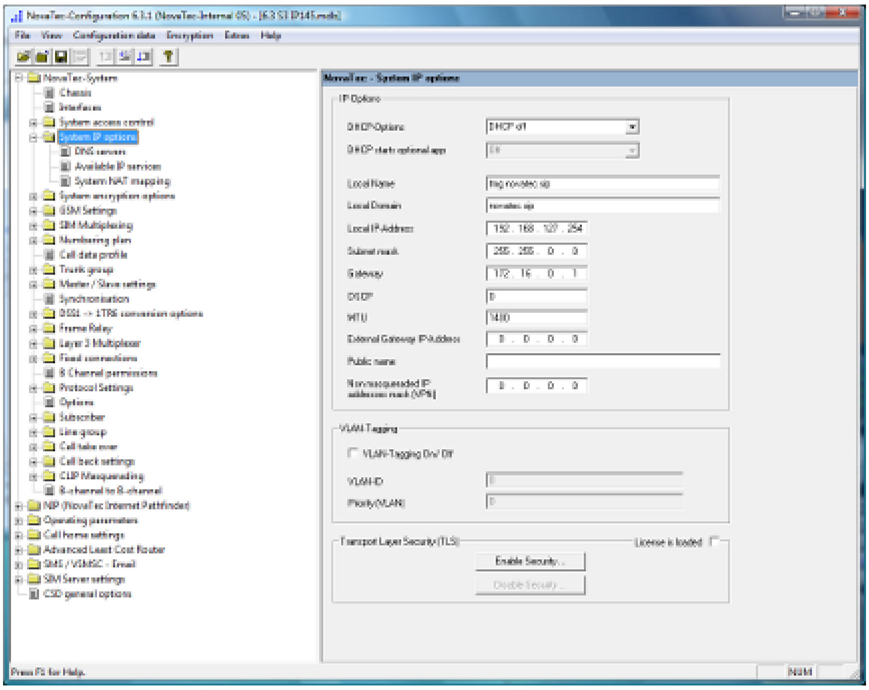
- Select flag “Sign Certificate Requests”.
- A connection to the NovaTec gateway is necessary if you want to rewrite the signed data set into the NovaTec device.
- Enter a CA password. This is the password to the private CA key.
- Repeat your CA password.
- Enter the following input feeds:
  - Select “certificate request from target” in the combobox.
  - Enter the private CA key.
  - Enter the CA certificate.
  - Enter a temporary file path in which the certificate request should be buffered.
- Enter the following output feeds:
  - Select “signed certificate to target” in the combobox.
  - Enter the file path in which the data set serial.txt resides.(1)
  - Enter the validity of the certificate in days.
  - Enter a temporary file path in which the signed certificate should be buffered.
- If all entries are completed press the button “Sign Certificate Requests”.

Note(1):
The serial number of a certificate is administered by a data set serial.txt. If this data set is not existent in the given path the application will design it anew and will assign a default start serial number.
If you want to assign the serial number yourself write a 16-digit hexadecimal number e.g. 0123456789ABCDEF into the data set serial.txt. After usage the number is incremented in serial.txt.

5.2 Clearing NovaTec for TLS

The customer has received his license data and can now clear his systems for TLS with help of the application “NovaTec Configuration”.

In order to achieve this he opens his conventional configuration with „NovaTec Configuration“ and chooses „System-IP-Option“ within the left hand tree.



IP Options

DHCP-Options: DHCP off

DHCP starts optional app: Off

Local Name: tmg.novatec.sip

Local Domain: novatec.sip

Local IP-Address: 192 . 168 . 127 . 254

Subnet mask: 255 . 255 . 0 . 0

Gateway: 172 . 16 . 0 . 1

DSCP: 0

MTU: 1400

External Gateway IP-Address: 0 . 0 . 0 . 0

Public name:

Non-masqueraded IP addresses mask (VPN): 0 . 0 . 0 . 0

VLAN-Tagging

□ VLAN-Tagging On/ Off

VLAN-ID: 0

Priority (VLAN): 0

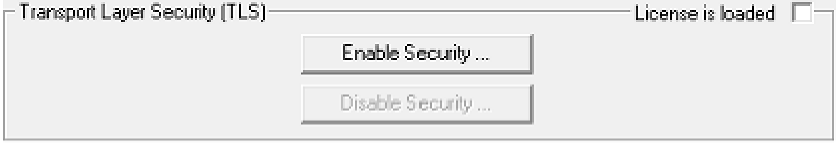
Transport Layer Security (TLS) License is loaded □

Enable Security ...

Disable Security ...

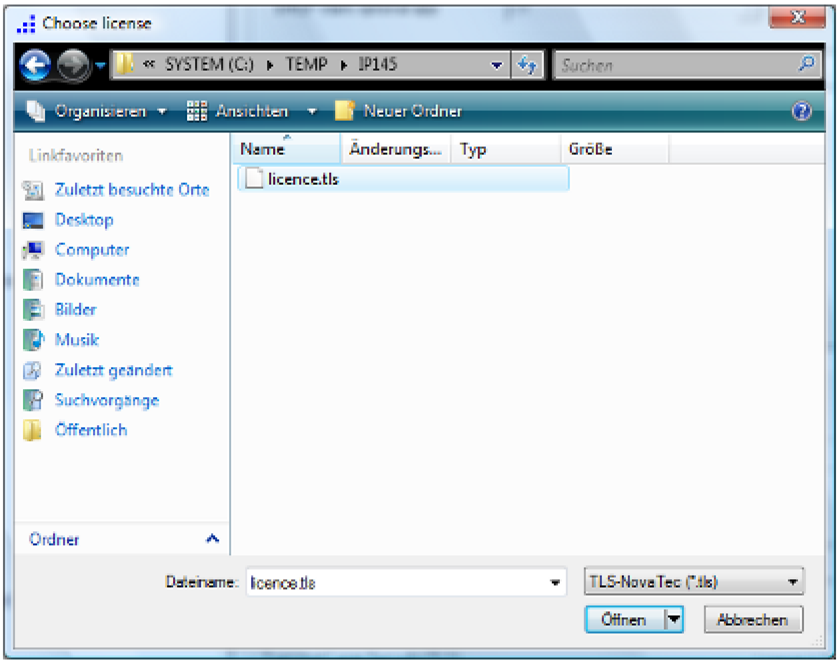
Picture 1: System-IP-Options

After doing so he presses the button „Enable Security…“ in the window on the right.


Transport Layer Security (TLS) License is loaded □

Picture 2: Activating TLS

A dialogue opens asking the customer to localize the received license within the data system.

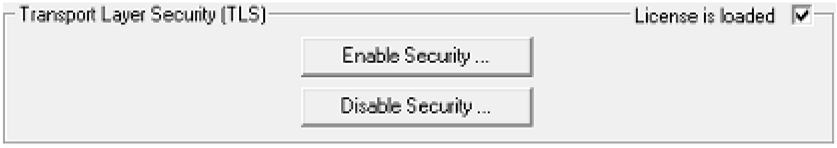


Dateiname: licence.tls

TLS-NovaTec (*.tls)

Picture 3: Import of a TLS license

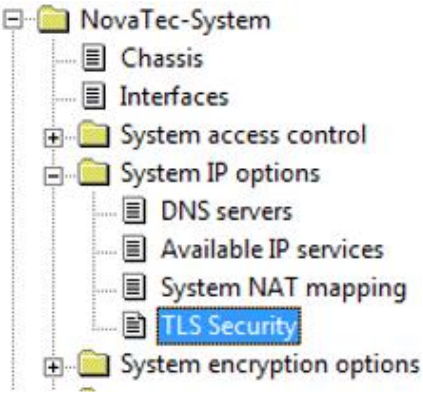
The successful import of the license is shown to the user by an activated check box „License is loaded“ in the right part window.



License is loaded ☑

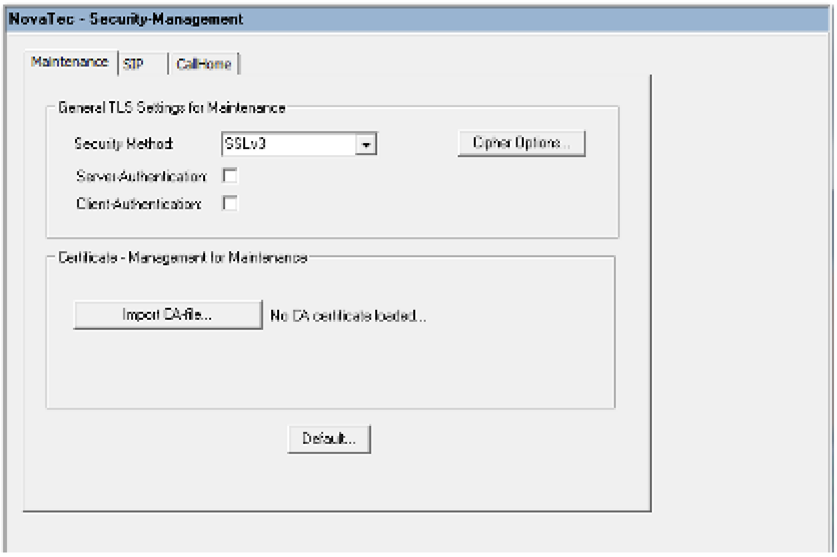
Picture 4: Successful import of a TLS license

Also within the tree in the left hand window a special node „TLS-Security“ shows up.



Picture 5: node "TLS-Security"

After picking this node three flags will appear in the right hand window: Maintenance, SIP and CallHome.



NovaTec - Security-Management

General TLS Settings for Maintenance

Security Method: SSLv3

Server-Authentication: □

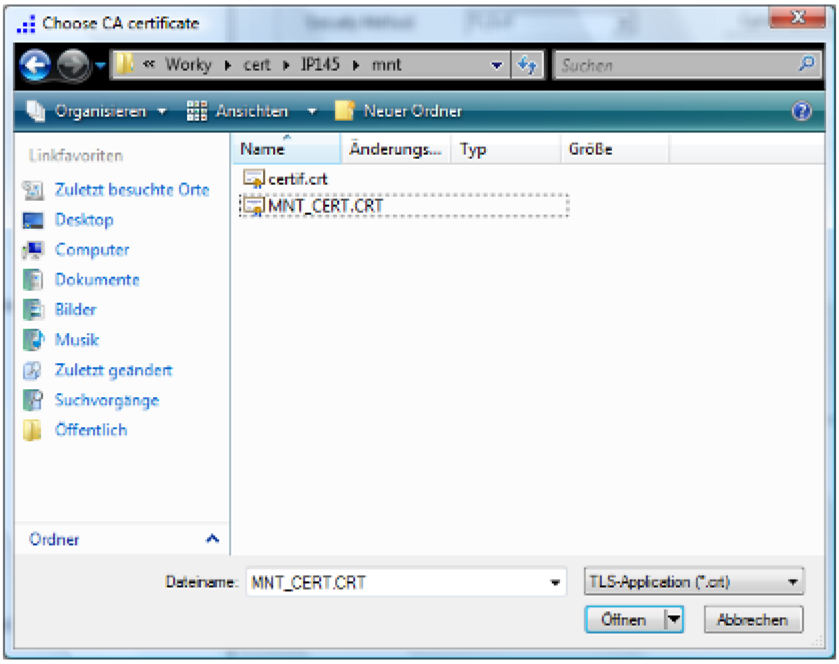
Client-Authentication: □

Certificate - Management for Maintenance

No CA certificate loaded...

Picture 6: Security Management

If you want to import a CA certificate you can initiate this by pressing the button „Import CA-file…“. A new dialogue shows up in order to localize the CA certificate within the data system.



Choose CA certificate

« Worky ▸ cert ▸ IP145 ▸ mnt

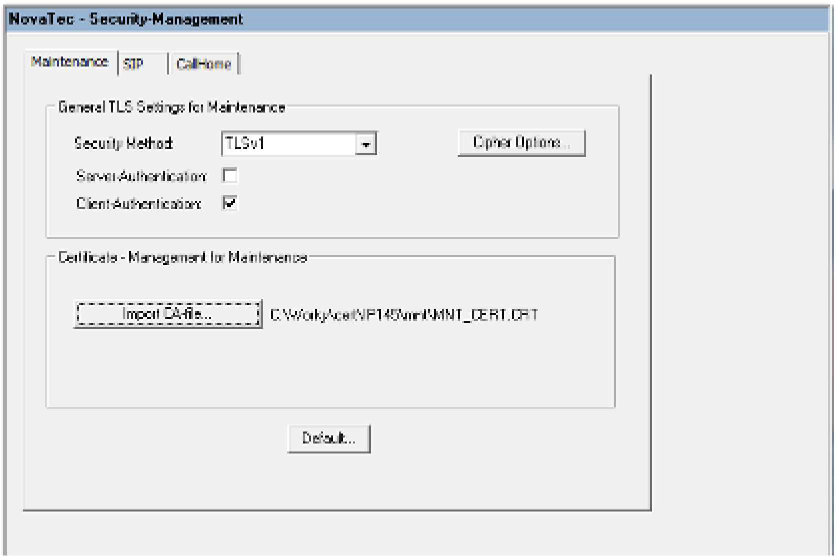
Name	Änderungs...	Typ	Größe
certif.crt			
MNT_CERT.CRT			

Dateiname: MNT_CERT.CRT

TLS-Application (*.crt)

Picture 7: Import of CA certificate

The successful import is shown in the right hand window.



General TLS Settings for Maintenance

Security Method: TLSv1

Server-Authentication ☐

Client-Authentication ☑

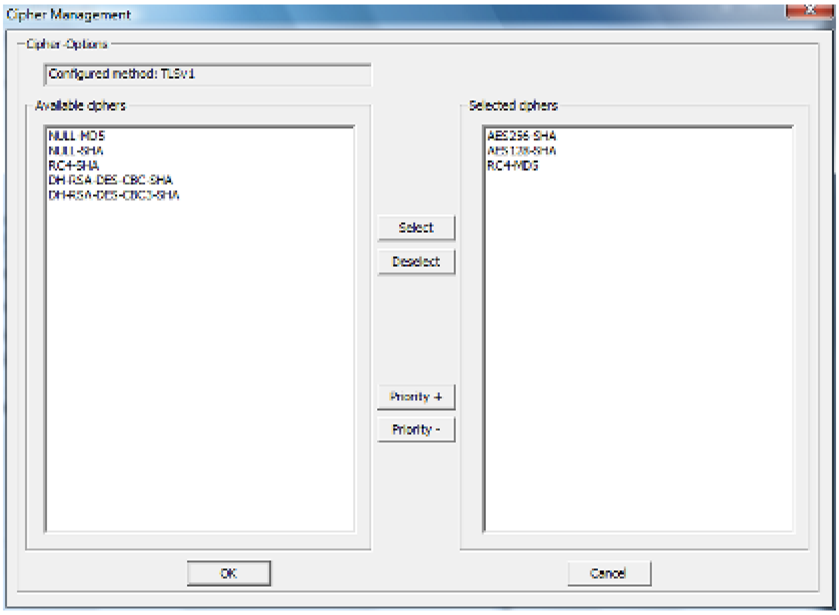
Certificate - Management for Maintenance

C:\Work\cert\VP145\mnt\MNT_CERT.CRT

Picture 8: Successful import of a CA certificate

If you want to restrict TLS e.g. to specific algorithms – this is if you want to define the cipher list – you can initialize this by pressing the button „Cipher Options….".

A dialogue shows up allowing the customer to restrict the given ciphers further.



Cipher-Options

Configured method: TLSv1

Available ciphers

NULL-MD5
NULL-SHA
RC4-SHA
DH-RSA-DES-CBC-SHA
DH-RSA-DES-CBC3-SHA

Selected ciphers

AES256-SHA
AES128-SHA
RC4-MD5

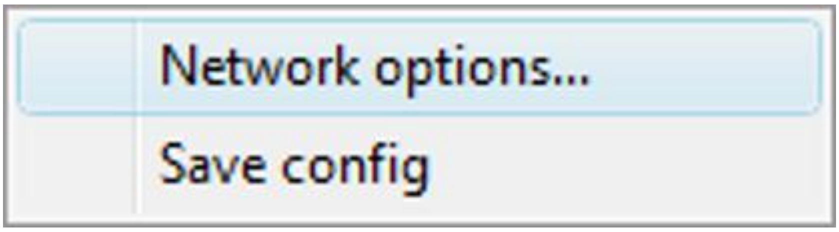
Picture 9: Cipher options

In the left part window the available ciphers are shown and the user defined cipher list in the right part window.

Ciphers from the left part window can be transferred into the right part window either by double clicking them or by pressing the button „Select". Equally ciphers are returned to the left part window and so deleted from the user specific list by double clicking or by pressing the button "Deselect".

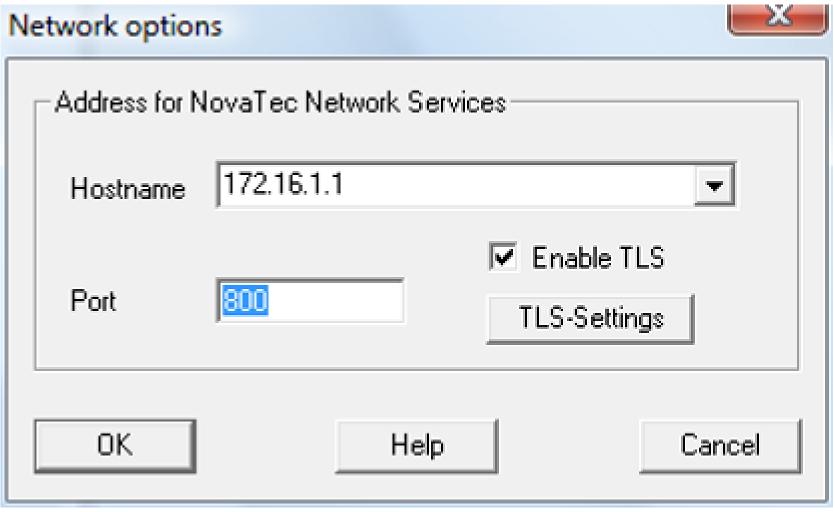
The priority of the cipher is very important – it can be changed with the buttons „Priority+“ and „Priority-“.

Is the TLS configuration constructed it can be transferred to the target system with the help of NovaTec Configuration.
If TLS is activated in the target system the configuration has to be transferred in TLS mode.
This is achieved by selecting „Network Options“ under the menu topic „Extras“.



Picture 10: Menu item "Network Options"

After the choice of this menu item a dialogue shows up allowing the definition of a connection partner.



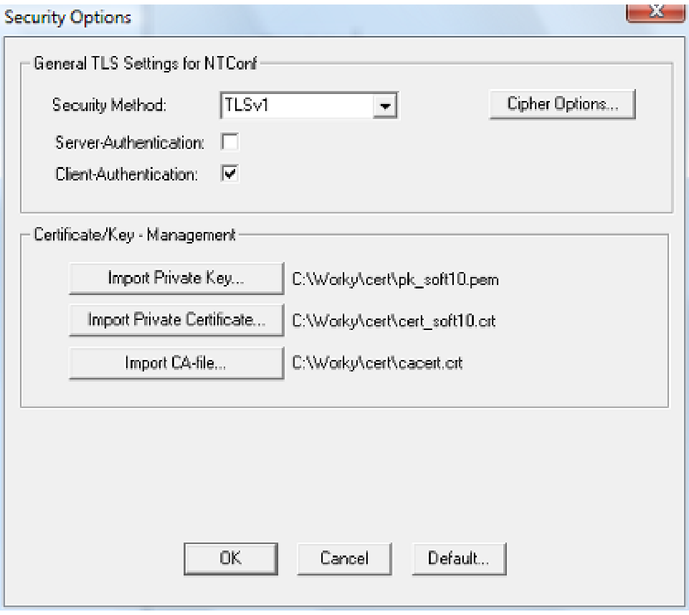
Hostname 172.16.1.1

Port 800

☑ Enable TLS

Picture 11: Network options

By activating the hooklet „Enable TLS“ the button „TLS-Settings“ just below it is engaged and operated.



Security Options

General TLS Settings for NTConf

Security Method: TLSv1

Server-Authentication: □

Client-Authentication: ☑

Certificate/Key - Management

Import Private Key... C:\Worky\cert\pk_soft10.pem

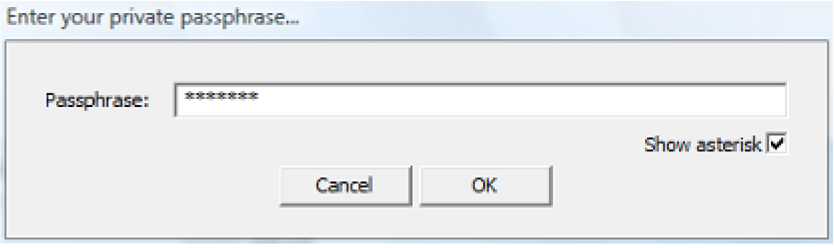
Import Private Certificate... C:\Worky\cert\cert_soft10.crt

Import CA-file... C:\Worky\cert\cacert.crt

Picture 12: Security options

After the above given options have already been chosen supplementary to the import of the CA certificate you can also import the private key and private certificate of the user within this dialogue.

Now you can transfer the configuration onto the target system. Whilst the connection to the target system is established the passphrase of the private key is required from the user. This is necessary to enable the system to open the private key.



Enter your private passphrase...

Passphrase: ********

Show asterisk ☑

Picture 13: Enter "passphrase"

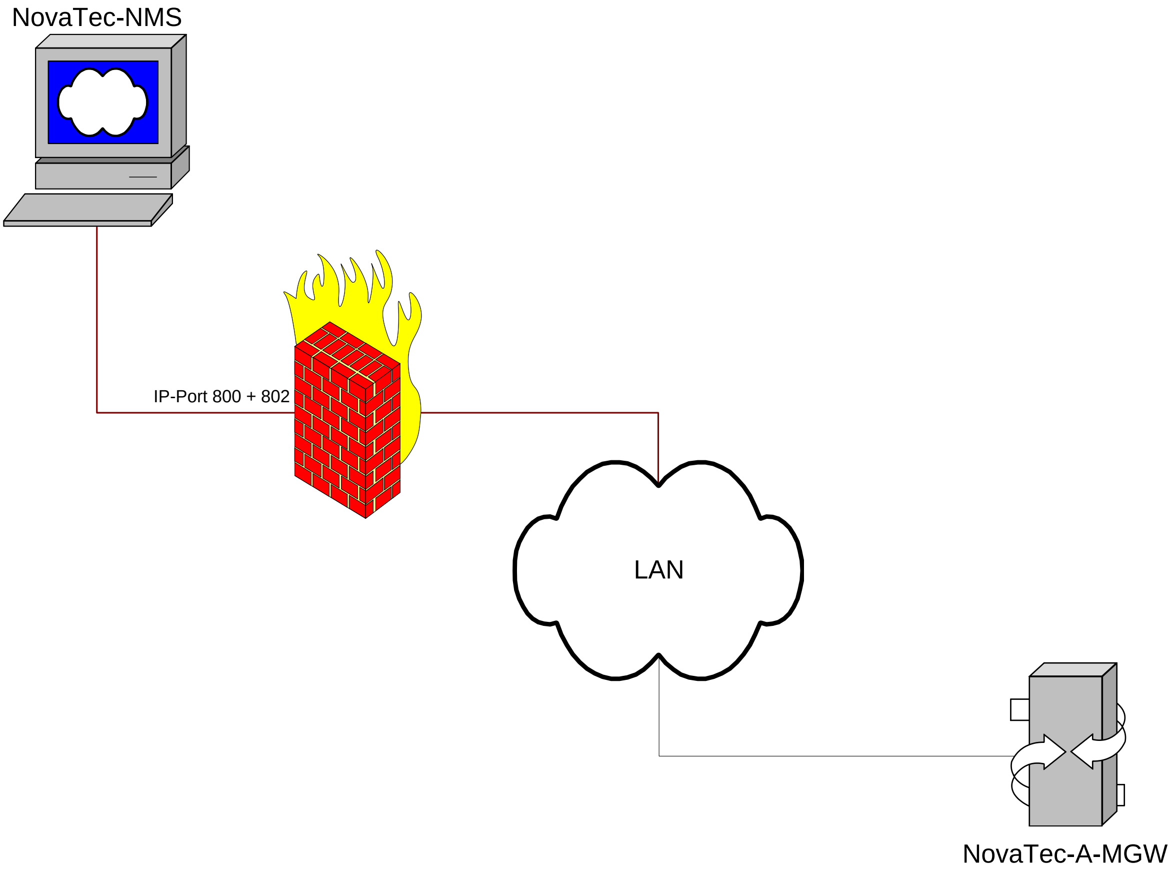
6 The Network Management System

6.1 Installation of NMS

The following software packages have to be installed on a server running the NovaTec Network Management System to enable the operation of NMS and to make direct access to an A-MGW possible:

- **NovaTec Network Management System**
- **NovaTec Maintenance Package**

The server has to be incorporated in a LAN network. The IP ports 800 and 802 have to be cleared in the firewall to enable access in both directions.



The following system precondition should be fulfilled by the server in minimum to ensure a fast handling of a target system:

Windows XP
2 GB RAM
1 GHz CPU

6.2 Functionality of the NMS 6.x

The following applications are running on the server:

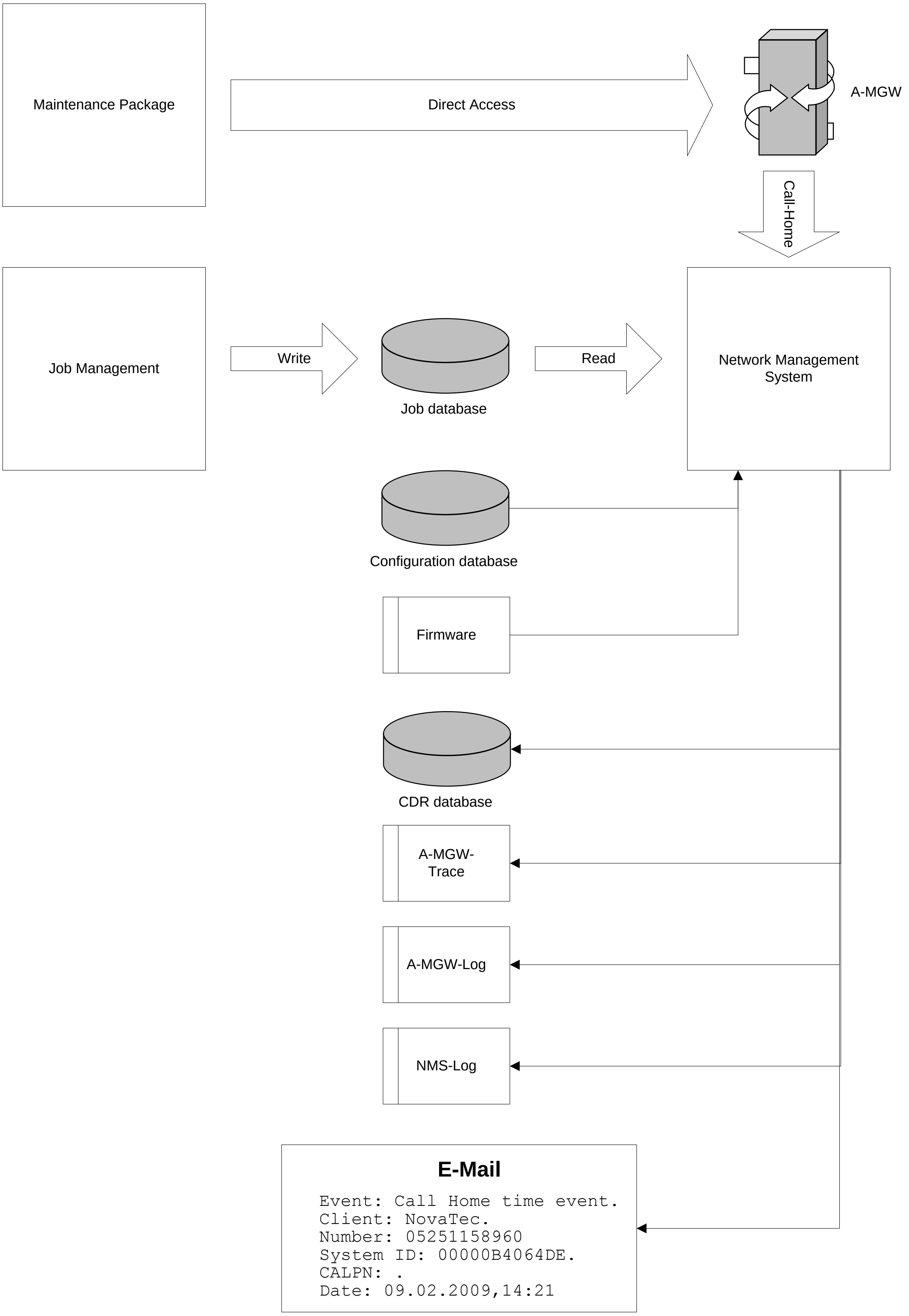
Maintenance Package:
Hereby the direct access onto the target system is effected. The package includes the necessary applications to enable you to access an A-MGW manually e.g. to read out the CDRs, update the firmware, read out traces and log files or query the status.

Job Management:
The Job Management application is part of the NovaTec NMS Package and controls which target systems are allowed to access NMS resp. which target systems are accepted by NMS and which jobs are to be carried out if a target system comes forward. All jobs can be controlled specifically per target system.

Network Management System:
The Network Management System is the application which receives inbound calls from target systems/A-MGWs and executes the necessary jobs in accordance with the specifications from the job management. Hence for the operation of NMS a job database has to exist in any case. If NMS is to update the configuration or firmware of a target system the according configuration (configuration database) and firmware have to be deposited for NMS. The data sets can reside locally on a server or on a file server. NMS needs the necessary access rights to these data sets. In order to save call data an existing (empty in the beginning) CDR database is needed. Traces and log files of the target system / A-MGW and the log file of NMS itself are created anew and not saved in a database.

The NMS hat no direct access to the target systems but waits until these come forward per call home. A target system carries out a call home as soon as an according event occurs and call home is configured for this event. If desired the target system can be configured in such way as that variable servers are called depending on the event.

On demand NMS sends an email to inform about the occurred event. The target systems are related to the customer. An email address can be configured for every customer.
The following picture shows how the access to the A-MGW takes place and which data sets are processed by NMS:



```
Event: Call Home time event.
Client: NovaTec.
Number: 05251158960
System ID: 00000B4064DE.
CALPN: .
Date: 09.02.2009,14:21
```

The following events are supported at the time being:

- **Budget Limit reached**
  The configured budget limit has been reached.
- **Call data filled**
  The CDR storage is full (resp. half full).
- **Client Callback failure**
  During a call back process an error on client side has occurred.
- **Server Callback failure**
  During a call back process an error has occurred on server side.
- **EWU Board removed from System**
  An EWU board has been removed from the target system.
- **SIM removed from SCU**
  A SIM card has been removed from a SCU board.
- **Falls short of ASR limit**
  The configured ASR threshold has been underrun.
- **GSM ASR event**
  The configured ASR threshold for the GSM network has been underrun.
- **ISDN ASR event**
  The configured ASR threshold for ISDN has been underrun.
- **SIP ASR event**
  The configured ASR threshold for the SIP network has been underrun.
- **Layer 1 or Layer 2 inactive**
  The layer 1 or layer 2 connection has broken down at a point to point interface.
- **Log filled**
  The log file is full.
- **Trace filled**
  The trace data storage is full.
- **Ping timeout to TIME server**
  The connection to the TIME server is broken down.
- **SOS client unreachable**
  The connection to the SOS client is broken down.
- **SOS SIM error**
  During the access to a SIM an error has occurred.
- **Systemstart default**
  The target system has carried out a reset and runs in default configuration.
- **Systemstart normal**
  The target system has carried out a restart and runs with the last transferred configuration.
- **Time event**
  The target system comes forward after a configurable time slot. No unexpected events have occurred.
- **TIP Running errors**
  An error has occurred in TIP operation.
- **TIP Startup errors**
  During startup of the TIP interfaces an error has occurred.
- **Trace warning**
  A warning was created in the target system.
- **Trace error**
  An error has occurred in the target system.

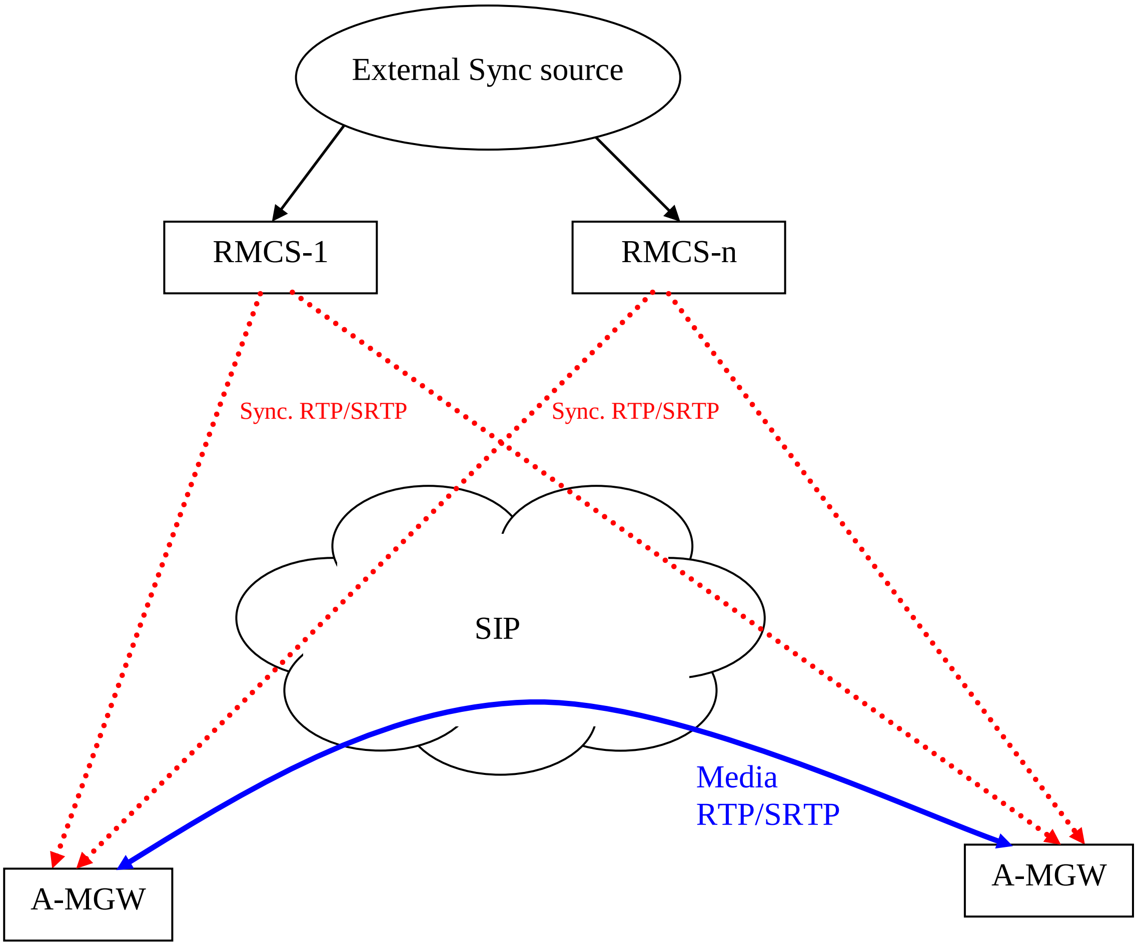
The events in grey are irrelevant for the planned application area of the A-MGW. They have been listed for reasons of completeness and to show that the different events can be implemented.

7 NovaTec Sync. Admin

The NovaTec Sync. Admin consists of several NovaTec hardware and software components which together provide for clock synchronization of all NovaTec components in a TDM, IP or mixed network. The components are:

1- The RTP Master Clock Source (RMCS)
2- The Sync. Manager tasks in the A-MGWs
3- The configuration tool

During synchronization with RMCS a SIP connection to a RMCS server is established before the actual SIP call is made. The synchronization results from the RTP stream received by the RMCS server. A RMCS server always has an external clock source (PRI/BRI or GPS). A system with a high-precision silica can be used as alternative.



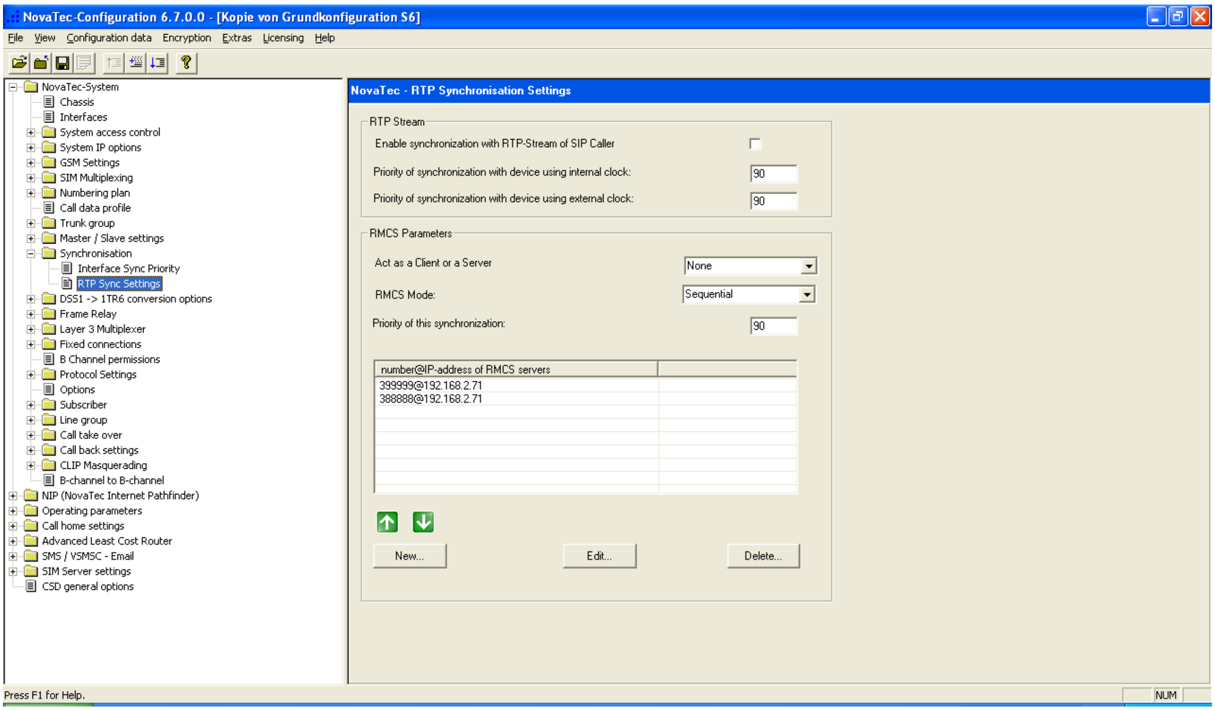
The following directives were transposed:

- A RMCS call is only established for data calls.
- In case a RMCS server is unavailable it is attempted to get through to the next configured RMCS server.
- If the RMCS connection breaks down during a SIP call the next RMCS server is contacted immediately.
- If no canal is free for the RMCS call the data call is rejected.
- If no RMCS server is available the data call is rejected.
- For the RMCS call any free VoIP channel can be used. Alternatively it is also possible to assign a channel on the A-MGW for the RMCS server to ensure that there is always a channel available for the synchronization connection.
- The choice of a RMCS is possible with the methods sequential or Round-Robin.

7.1 Configuration of the RMCS clients

When connecting the systems via a soft switch like Cisco CUCM extra adjustments have to be made:

7.1.1 RTP Sync. settings



NovaTec - RTP Synchronisation Settings

RTP Stream

Enable synchronization with RTP-Stream of SIP Caller ☐

Priority of synchronization with device using internal clock: 90

Priority of synchronization with device using external clock: 90

RMCS Parameters

Act as a Client or a Server: None

RMCS Mode: Sequential

Priority of this synchronization: 90

number@IP-address of RMCS servers	
399999@192.168.2.71	
388888@192.168.2.71	

The following adjustments have to be made:

Box „Act as a Client or a Server“:
Tells whether the system is run as client or server. Please choose „Client“.

Box „RMCS Mode“:
Tells whether the RMCS servers have been chosen with the method sequential or Round-Robin by the client. Both settings are possible. With method sequential the 1rst server is always called and the next server is only contacted if the call to the 1rst server cannot be established. With method Round-Robin the next server is chosen always. If the end of the list is reached it is restarted with the 1rst server.

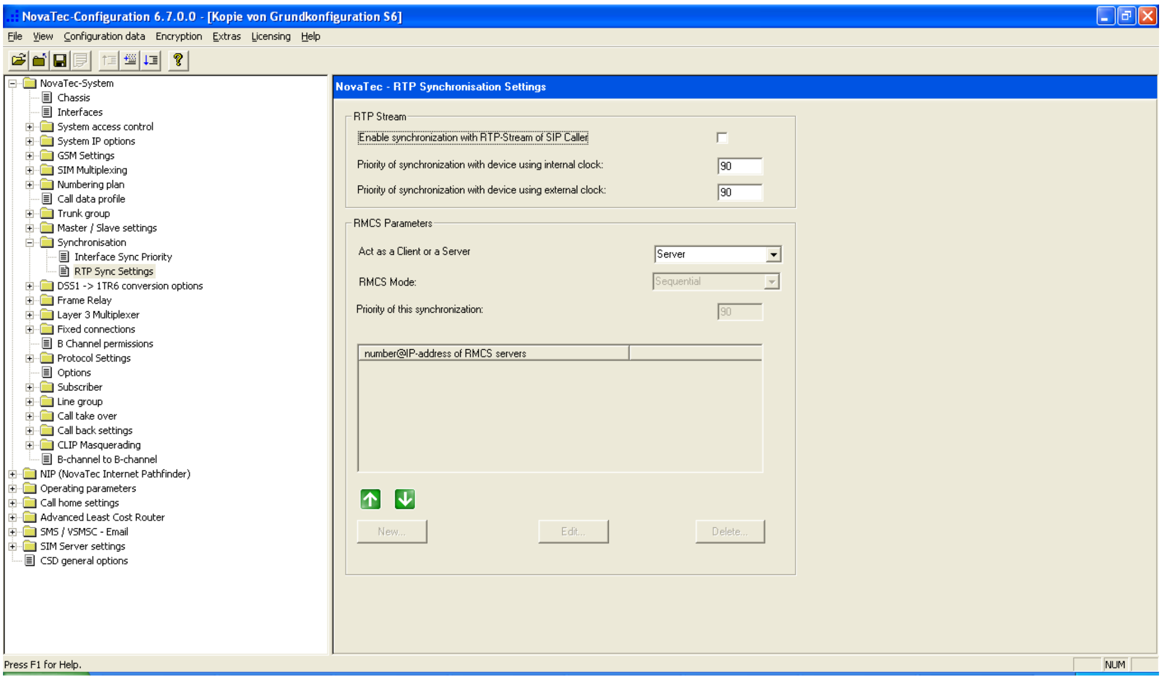
Box „Priority of this synchronization“:
Tells which synchronization priority the RTP stream of the RMCS server is given by the client. The entered value is also shown under „interface Sync Priority“ together with all other priorities.

List „number@IP-address of RMCS servers“:
All RMCS servers to which the client is supposed to have access are listed here. Only the number is essential. The IP address is only informative at this point. The number is transformed into a SIP address in the SIP user mapping. If the CUCM is not listed as SIP receiver for all call numbers nothing has to be changed in the SIP user mappings.

7.2 Configuration of the RMCS server

The following adjustments are to be made on the server side:

7.2.1 RTP-Sync settings



NovaTec - RTP Synchronisation Settings

RTP Stream

Enable synchronization with RTP-Stream of SIP Caller ☐

Priority of synchronization with device using internal clock: 90

Priority of synchronization with device using external clock: 90

RMCS Parameters

Act as a Client or a Server: Server

RMCS Mode: Sequential

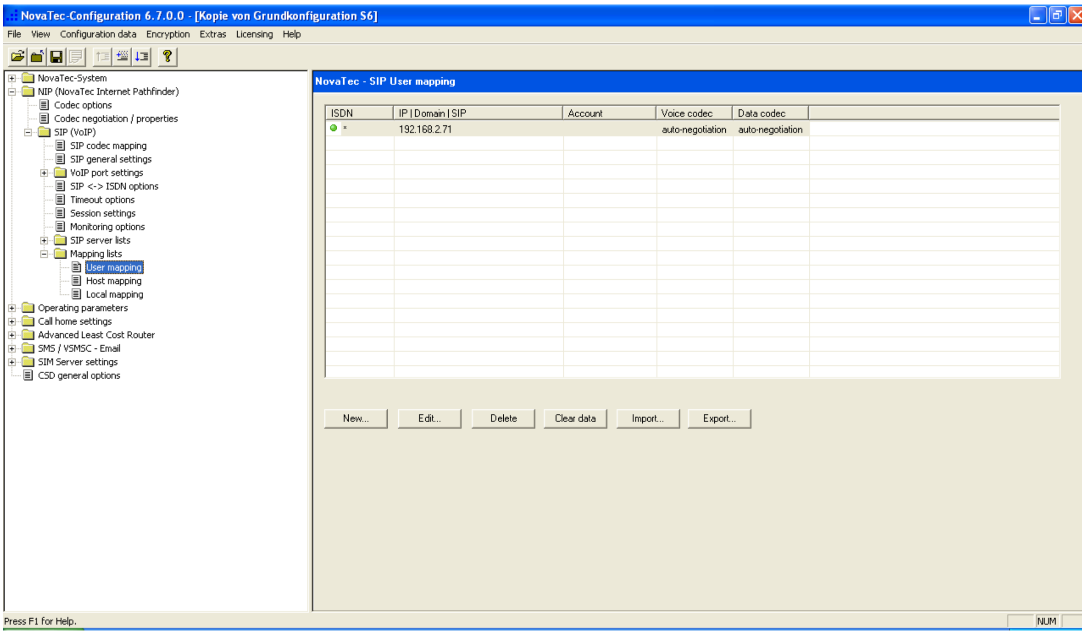
Priority of this synchronization: 90

number@IP-address of RMCS servers	

Box „Act as a Client or a Server“: Choose server.

All other boxes are irrelevant.

7.3 User Mapping



NovaTec-Configuration 6.7.0.0 - [Kopie von Grundkonfiguration S6]

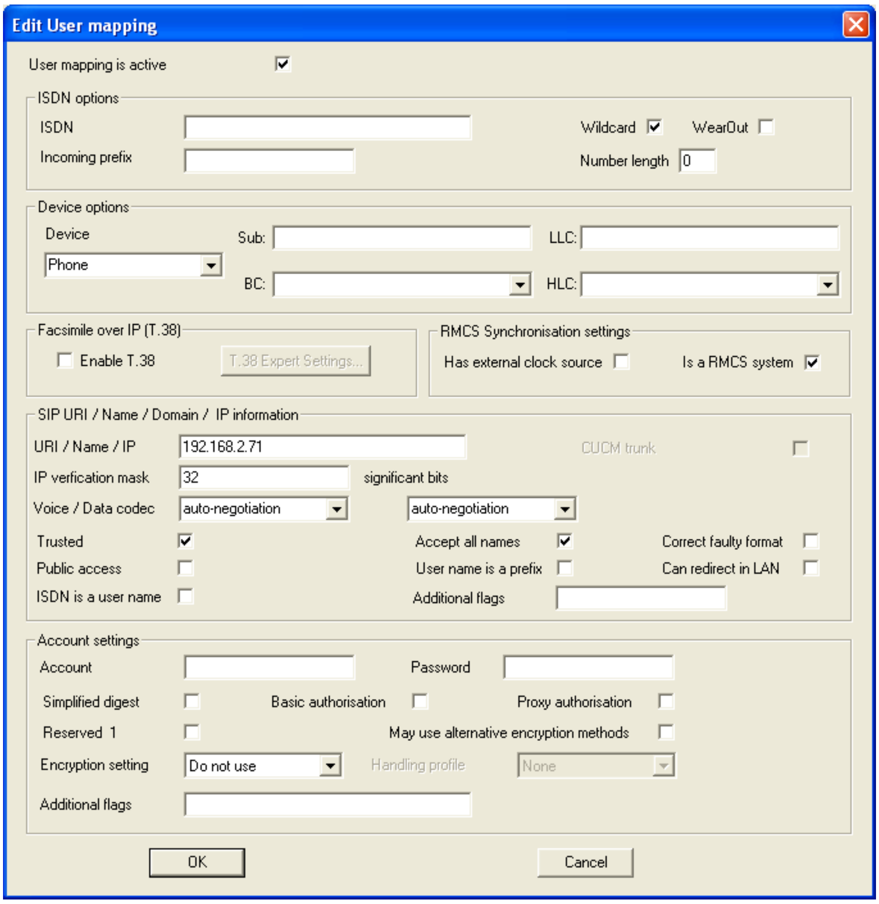
File View Configuration data Encryption Extras Licensing Help

- NovaTec-System
- NIP (NovaTec Internet Pathfinder)
  - Codec options
  - Codec negotiation / properties
  - SIP (VoIP)
    - SIP codec mapping
    - SIP general settings
    - VoIP port settings
    - SIP <-> ISDN options
    - Timeout options
    - Session settings
    - Monitoring options
    - SIP server lists
    - Mapping lists
      - User mapping
      - Host mapping
      - Local mapping
- Operating parameters
- Call home settings
- Advanced Least Cost Router
- SMS / VSMSC - Email
- SIM Server settings
- CSD general options

NovaTec - SIP User mapping

ISDN	IP | Domain | SIP	Account	Voice codec	Data codec
● *	192.168.2.71		auto-negotiation	auto-negotiation

All RMCS Server systems need an entry under „User Mappings“. The next screenshot shows which adjustments have to be made:



Edit User mapping

User mapping is active ☑

ISDN options
- ISDN:
- Wildcard ☑ WearOut □
- Incoming prefix:
- Number length: 0

Device options
- Device: Phone
- Sub:
- LLC:
- BC:
- HLC:

Facsimile over IP (T.38)
- □ Enable T.38

RMCS Synchronisation settings
- Has external clock source □
- Is a RMCS system ☑

SIP URI / Name / Domain / IP information
- URI / Name / IP: 192.168.2.71
- CUCM trunk □
- IP verfication mask: 32 significant bits
- Voice / Data codec: auto-negotiation / auto-negotiation
- Trusted ☑
- Accept all names ☑
- Correct faulty format □
- Public access □
- User name is a prefix □
- Can redirect in LAN □
- ISDN is a user name □
- Additional flags:

Account settings
- Account:
- Password:
- Simplified digest □
- Basic authorisation □
- Proxy authorisation □
- Reserved 1 □
- May use alternative encryption methods □
- Encryption setting: Do not use
- Handling profile: None
- Additional flags:

It is important that the hooklet „Is a RMCS system“ is activated to ensure that the RMCS server accepts the synchronization call. Otherwise all adjustments are to be made like the normal “User Mapping“. Any number can be entered in the box “ISDN” as the RMCS server is only called and does not build up calls itself.

The RMCS server is connected to CUCM with a SIP trunk like all other NovaTec systems.

With usage of TLS the appropriate adjustments are to be made like in other NovaTec systems.