

Network Centric PBX

Instruction manual

Release 1.15

Table of Contents

INTRODUCTION	6
WHAT'S NEW	7
1. System architecture	8
1.1. System elements – Call Manager	9
1.2. System elements - GWx shelves	11
1.3. System elements - EMx expansion modules	14
1.4. System elements – SWS24S switch.....	15
2. System configuration	15
3. Network configuration.....	17
3.1. IP configuration	17
3.2. DNS configuration	21
3.3. SIP and RTP configuration	21
3.4. NAT Configuration.....	21
3.5. Firewall	21
3.5.1 Rules.....	21
3.5.2 Black list.....	22
3.6. Static routing	22
3.7. WWW server.....	23
3.8. Certificates	23
3.9. SMTP client	24
3.10. TAPI configuration	24
3.11. CTIP configuration	25
3.12. Web and XML protocols.....	25
3.12.1. XML protocol	26
3.12.2. Web.IVR protocol	27
3.12.3. Web.API protocol	28
3.13. eSSL system	28
3.13.1. eSSL protocol	29

3.13.2. eSSL status	30
3.13.3. Solving conflicts.....	31
3.14. Redundancy system.....	31
4. Accounts	33
5. Operation.....	34
5.1. Configuration recovery points	34
5.2. Backups.....	34
5.3. Software updates.....	35
5.4. Licences	36
5.5. System clock.....	36
5.6. Name and description	37
5.7. System Commands	37
5.8. System reboot.....	37
5.9. Factory format	37
6. Hardware configuration	38
6.1. Adding shelves	38
6.2. Adding modules	39
6.3. Port configuration	39
6.4. Switch	41
7. Internal numbers.....	42
7.1. Settings	42
7.2. Subscribers.....	42
7.3. Call distribution groups	52
7.4. IVR.....	53
7.5. Call center queues.....	56
7.5.1 How to configure the CallCenterMAN application	59
7.6. Service codes	61
7.7. Other extensions	61
7.7.1. Voice mail.....	61
7.7.2. Speaking clock service.....	62

7.7.3. Echo test	62
7.7.4. Play music.....	63
7.7.5. My internal number	63
7.7.6. Conference calls.....	63
7.7.7. Fax2mail gateways.....	65
7.7.8. Web.IVR.....	65
7.7.9. Paging	66
7.7.10. Lines	66
7.8. Sets.....	67
7.9. Provisioning.....	67
7.10. Devices	68
7.10.1. MAB	69
7.10.2. AUD.IP	69
7.10.3. DPH.IP	70
7.10.4. Cameras	74
8. Operators.....	74
8.1. TDM operators	75
8.2. VoIP operators	75
9. Call routing.....	77
9.1. Settings	78
9.2. Predefined prefixes	78
9.2.1. Predefined prefixes - outgoing traffic	79
9.2.2. Predefined prefixes - incoming traffic.....	79
9.3. Outgoing traffic.....	80
9.4. Incoming traffic.....	83
9.4.1. Incoming rules	84
9.4.2 Caller ID routing	87
9.4.3. Dynamic routing	89
9.4.4. Caller's presentation	90
10. PBX features	91

10.1. Phonebook	91
10.2. Time ranges	91
10.3. Manual operating modes.	92
10.4. Call recording	93
10.4.1. Recorded objects	94
10.4.2. Access to records - application settings	94
10.4.3. Settings - basic configuration	96
10.4.4. Access levels	96
10.5. Call billing	97
10.6. Text message support	97
10.7. Access control system	98
10.8. AudioMAN	98
10.9. CallCenterMAN	98
11. Media.....	98
11.1. MoH - Music on hold	98
11.2. Announcements	99
11.2.1. Announcement upload procedure via sound manager	99
11.2.2. Uploading announcements to queues	100
11.2.3. Uploading announcements using Text2speech.....	100
12. Diagnostics	101
12.1. Summary information	101
12.2. System alarm	101
12.3. Connection Monitor.....	101
12.4. Status.....	102
12.4.1. Providers	102
12.4.2. Extensions	103
12.4.3. Services.....	104
12.4.4. CTI applications.....	104
12.5. Logs	104
12.5.1. Calls log	104

12.5.2. SMS log	105
12.5.3. Service states log.....	105
12.5.4. Event logs	105
12.6. Statistics.....	106
12.6.1. IVR statistics.....	106
12.6.2 Calls statistics graph	106
12.6.3 Calls Traffic graph.....	106
12.7. Tools	107
12.7.1. Calls simulator.....	107
12.8. Network traffic analysis	108
12.7.3 ISDN analyzer	108
12.7.4. Console commands	109
ADDITIONAL INFORMATION	109

INTRODUCTION

Thank you for purchasing the NCP PBX. It is an innovative corporate-class IP PBX device, also intended for small and medium businesses (SMBs). The advanced hardware platform and revolutionary software features offer breakthrough solutions for voice, image, data and fax handling. Modular design enables easy system upgrading and scalability according to business needs.



Alterations or modifications of the product that have not been expressly approved by Slican, or operation of the product in a manner other than described in the operating manual may result in loss of manufacturer's warranty.

The programming manual is intended for administrators who are required to prepare, install and configure the phone system for operation. In this document we have included detailed information on the NCP system's features and configuration.

This manual is compatible with software versions 1.15.xxxx

The latest software version is available for download at: <https://slican.com/servnet>.

WHAT'S NEW

New features brought by the latest software version, described in this manual:

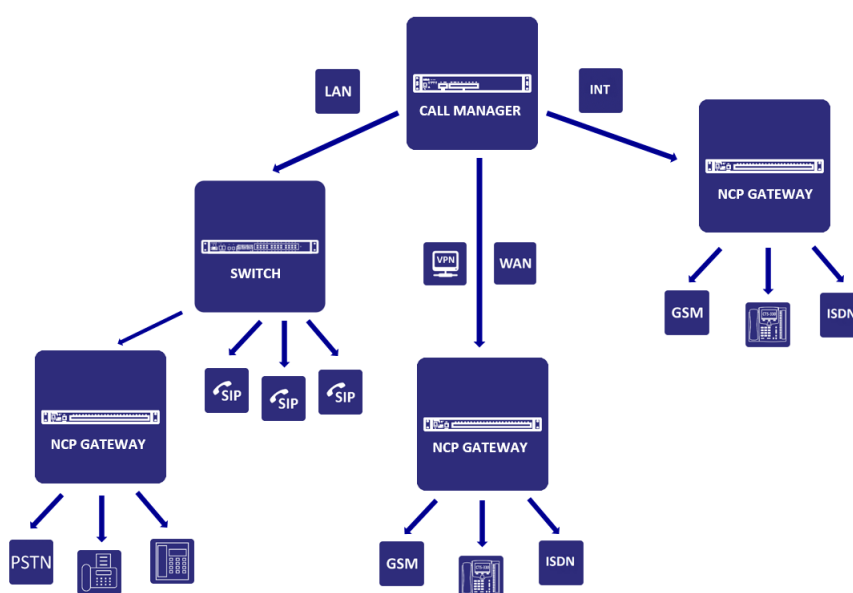
- ACS - possibility of synchronous opening of several DPH.IPs within a zone
- New type of MAB (FXS) equipment with VOX recording for e.g. fire radios in the Fire Department
- Ability to enable the welcome announcement in the CC queue
- WebIVR - the ability to control outgoing traffic through an external application
- WebAPI - sending SMS from GSM gateway
- Calling on MobilePhone when DND
- Possibility to modify provisioning files with variables specific to a given SIP subscriber
- Possibility of SMS system notifications via GSM gates
- Information in the Log and Connection Monitor if the connection was generated from the MessengerCTI application
- Adding of the IVR usage statistics report
- Addition of a beep informing about the transfer of the call after notification
- ACS - Proximity card reader, facilitating mass management of proximity cards
- Entering CDR logs into the system log (detailed logs)
- Possibility of viewing the current time range (operating mode) on the CTS display
- Chart of telephone traffic measured in the number of answered / rejected calls by the PBX per hour (BHCA)
- Possibility to change extensions (manually and according to rules) in serial edition of subscribers
- Tools for testing the network connection with the MessengerCTI.Mobile application
- Tidy up System Log and Notifications now as Notification, System and Detailed Log Log
- Adding an additional (advertising) announcement to the queue announcement
- Possibility of individual scheduling of announcements about the call center queue position
- Possibility to configure switches and SIP devices when managed by Keeper / WAN
- Possibility of presenting the agent for outgoing calls with the queue number
- Added ISDN ports monitor and DSS1 signaling analyzer
- Adding a Numbering Plan to speed up dialing on CTS, FXS phones

1. System architecture

The full name of the system is **Network Centric PBX**, while the acronym is **NCP**, which is used for designating system elements:

- **NCP-CM** – Call Manager: main control unit,
- **NCP-GW** – Gateway: external and internal TDM port expansion shelf,
- **NCP-SW** – Switch: network switch,
- **NCP-EMS/EMD** – Subscriber port and metropolitan line expansion modules.

The NCP-CM Call Manager PBX specifies the main system shelf containing the main system CPU and SD mass storage units for storing billing information, recorded calls and system configuration. Secondary NCP-GW shelves are connected to NCP-CM both through LAN and a dedicated INT network. For dedicated INT networks, all system elements connected to INT sockets (or by a switch), obtain their IP addresses from Call Manager, which acts as a DHCP server. On the other hand, NCP-GW shelves are fitted with NCP-EMS/EMD expansion modules for connecting subscriber equipment and metropolitan lines. Thanks to the system's modular design, hardware capacity can be expanded as required for the given configuration. Building the system always begins with configuring its heart, i.e. the **Call Manager** shelf, to which individual **NCP-GWx** gateway shelves and any **NCP-SW** switch shelves are connected. Below is shown a diagram of a sample system and connections of its constituent elements:



As seen above, NCP-GWx gateway and any NCP-SW switch shelves are connected to the **INT** port, as well as **LAN** and **WAN** ports.

The following are connected to their respective **TDM** ports:

- analog phones
 - CTS-Up system phones
- or
- digital metropolitan translations: BRI, E1, GSM

- FXO analog metropolitan translations

SIP phones, softphones and IP system phones can be connected directly from a LAN.

1.1. System elements – Call Manager

The main management unit of the NCP system is Call Manager.

It contains information about, for example:

- system configuration (subscribers, incoming/outgoing traffic, call history)
- records, announcements
- configuration of attached GWx shelves

Depending on the model, it has enough network interfaces to handle traffic, management, communication with subordinate GWx shelves and operation in redundancy mode (CM hardware safety). The interfaces have the following functions:

- **LAN** – used for connecting GWx shelves, VoIP operators, SIP terminals
- **WAN** – dedicated mainly for connecting VoIP operators when they are unavailable from the LAN side (the operator only handles voice traffic)
- **INT** – only for connecting GWx shelves and CTS.IP system phones
- **RDU/INT** – pair of interfaces intended for connecting the CM system in redundancy mode

Aside from the network interfaces, the front panel includes the **SET** button – used for formatting.

Call Manager is available in 3 hardware variants (CM300P, CM400P, CM600P). Each variant differs in performance and supported resources. Working as an independent unit without additional gates (GWx), it is a fully functional telephone PBX based on the VoIP technology. The shelf's technical structure and ergonomic issues require it to be installed in a rack in an appropriate room (server room) to ensure optimum operating conditions, described in more detail in the technical documentation.

CALL MANAGER – resource and performance comparison:

PARAMETER	CM300P	CM400P	CM600P	Notes
No. of modules				
Maximum no. of GW shelves	5	20	127	
Maximum no. of FXS	240	960	6096	
Maximum no. of CTS.Upn	64	400	800	
Maximum no. of CTS.IP	64	400	800	Total CTS (IP/Upn)
Maximum no. of E1	1	6	13	Limit is due to maximum number of concurrent calls.
Maximum no. of 2B+D translations	16	32	32	Limit is due to maximum number of concurrent calls.
Maximum no. of FXO	64	64	64	
Maximum no. of GSM	58	120	120	
Maximum no. of SIP subscribers	200	1000	10000	
Maximum no. of SIP translations	50	128	128	
General resources				
Total users	300	1000	10000	FXS + SIP + CTS.Upn + CTS.IP + Virtual accounts
Maximum no. of DHP.IP	100	200	200	Possible number of DHP.IP intercoms
Maximum no. of audio devices	100	400	800	Possible number of MAB/AUD.IP devices
No. of concurrent calls	40	100	300	currently only 250 calls by TDM equipment, the rest by SIP

No. of concurrent EbdREC records	40	100	300	CM.300 - SSD 60GB (~1000 h recorded) CM.400 - SSD 128GB (~3300 h recorded) CM.600 - SSD 240GB (~6600 h recorded)
T.38 codec	1	10	10	FAX by VoIP support
No. of concurrent video calls	3	20	20	Video calls with H.263/263+/264 codec support
Contact book (public + private)	30000	30000	30000	maximum no. of numbers in contacts (and consequently no. of contacts), up to 5 numbers per contact, up to 100 contact groups
Maximum no. of WebCTI/PhoneCTI	100	400	800	limited by no. of private books, history, CTS number
No. of own MoH announcements	300	300	300	No. of user's own announcements
No. of IVR menus	1000	1000	1000	IVR menu configured in the system
Rate buffer capacity	200000	200000	200000	applies to metropolitan and internal calls and service status changes

LED INDICATORS – Call Manager front panel LED indicators of device status

LED	STATUS
PWR	related to power supply, lit constantly if the PBX is on
STAT	<ul style="list-style-type: none"> • indicates PBX error and warning status • critical errors are indicated by rapid LED blinking, non-criticals with slower blinking • during PBX startup, the diode is off • after startup, if there are no PBX errors, it is lit continuously, dimming once every 3-4 seconds • blinks rapidly during resetting
LINES	lights according to status priority from 'a' to 'd': <ul style="list-style-type: none"> • a. any line damaged - blinks quickly. • b. any line calls in incoming traffic - blinks slowly (not applicable to SIP) • c. at least one line busy - lit continuously • d. all lines free - unlit
RDU	signals related to redundancy system functionality (not applicable to CM300P) <ul style="list-style-type: none"> • lit continuously - running (CM RUN) • blinks quickly - synchronisation in progress (CM STANDBY)
BAT	related to battery power (1BATC charging module body rear) <ul style="list-style-type: none"> • battery disconnected or malfunctioning - not lit • battery charging - lit with dimming • battery charged - lit continuously • device on battery power - blinks 0.4 s/0.4 s

TECHNICAL SPECIFICATION – Call Manager hardware resources

Interfaces	
CM300 network interfaces	8xFE(6xINT, 1xINT/WAN, 1xLAN)
CM400 network interfaces	8xFE(6xINT, 1xLAN, 1xINTWAN), 2xGbE(1xINT,1xINT/RDU)
CM600 network interfaces	8xFE(6xINT, 1xLAN, 1xINTWAN), 2xGbE(1xINT,1xINT/RDU)
LED indicators	Power, Status, Lines, RDU
Reset	SET (factory reset)
Voice/Video	
Voice and FAX codecs	G.711 A-law/U-law, G.722, G.729, GSM, ADPCM, Speex, T.38

Video codecs	H.263, H.263+, H264
signalling/Protocols	
DTMF mode	RFC2833, SIP INFO, in-band
Digital signalling	DSS1, QSIG
Provisioning	HTTP/HTTPS, SIP multicast
Network protocols	TCP/UDP/IP, FTP, RTP/RTCP, ICMP, ARP, DNS, DHCP, NTP, SIP, SRTP, TLS, LDAP
Disconnection methods	Call Progress Tone, Polarity Reversal, Hook Flash Timing, Busy Tone,
Safety	
Protocols	SRTP, TLS, HTTPS, LDAPS
Advanced	e-mail notifications, strong password, IP filtering

More details in technical documentation available here [HERE](#).

1.2. System elements - GWx shelves

In order to expand NCP system resources with TDM PBX ports, both external and internal, connect dedicated NCP-GWx (Gateway) shelves to Call Manager. The GWx symbol indicates GWS or GWD variant. GWx shelves can be connected to the following network interfaces:

- **INT** - directly to CM or through a standard L2/L3 switch (internal system network)
- **LAN** – via local network
- **WAN** – in special cases for remote shelves outside LAN (Internet, VPN)

There are two modes of remote shelf operation:

- **local mode**: connected via INT or LAN
- **remote mode**: VPN remote network or Internet

Local mode operation: requires connecting the shelf to an INT network with a default DHCP server on, or to a LAN with an active DHCP server. In this mode, shelves are managed entirely from Call Manager, meaning they have no logic of their own in this respect, and consequently no static IP address assigned. In this mode, shelves connected to the network and assigned with an IP address send a broadcast to find Call Manager. Every broadcast is recorded by the CM system and added to the list of shelves awaiting approval (assignment) to the system. A recorded shelf is identified by its unique serial number. After approval in CM, shelves are ready for further configuration.

Remote mode operation: requires access to shelf configuration. In order to unlock configuration, press and hold the **UID** button for several seconds - until a double acoustic signal is given and the UID diode lights. After unlocking you can access configuration through a web page without any authorisation, by entering an address of the following format in the browser:

[slican-gw-xxxxxxx.local/](#)

where: **xxxxxxx** – is the serial number of the shelf to be configured

example:

[slican-gw-01009912.local/](#)

The above address is only available in the local network.

In the shelf configuration, enter the following information:

- IP address of Call Manager (local or public)

- signalling port (default TCP 5521)
- acoustics port (default TCP 5535)
- software update port (default TCP 5580)
- automatic or static IP address configuration (IP address, mask and network gateway)

When the CM address information is entered, the shelf will attempt to connect with the CM of the given address only. The configuration page ceases to be available after 5 minutes. The time to logout is given in the upper right corner. In order to gain access to shelf configuration again, unlock it again using the UID button. Also pay attention to correct addressing of acoustics and signalling ports at the edge router. If a shelf is configured for remote operation and firmware in the PBX is replaced with an older version (not supporting remote operation of shelves), the shelf must be formatted by pressing the UID button until PWR and LINK diodes start blinking quickly and a double acoustic signal is emitted. Failure to completely format the shelf will prevent it from connecting to CM.

Sending voice frames through the network in remote mode requires ensuring sufficient symmetric bandwidth as indicated below, and jitter of no more than 50 ms.

Shelf type	No. of call channels	Required guaranteed symmetric bandwidth
GWx	1	200kb/s
GWS	24	2Mb/s
GWD	48	4Mb/s
GWS with 2xE1	60	5Mb/s

Correctly configured shelves will await for approval in their dedicated CM. After approval in CM, shelves are ready for further configuration.

GWx shelves are fitted with expansion modules compatible with the following telecommunication contacts:

- in internal network
 - by IP-LAN with SIP-VoIP, SIP-Video, CTS.IP terminals
 - by POTS-FXS ports with analog phones
 - by CTS-Up0 ports with Slican CTS system phones
- in external network
 - by IP-WAN with SIP/SIP-Trunk translations
 - by POTS-FXO ports with POTS-CO metropolitan lines
 - by ISDN-BRI ports with ISDN-S(2B+D) contact
 - by ISDN-E1 ports with ISDN-E1(30B+D) contact
 - by GSM ports with mobile metropolitan lines

GATEWAY - available hardware solutions

GATEWAY	DESCRIPTION
---------	-------------

NCP-GWS2B	BOX body – dimensions 218 x 44 x 225 mm (WxHxD) Capacity up to 8 modules, output through 8 sockets Motherboard NCP-SP2BP.GWB (2 slots for EMS cards) Driver NCP-SP1CU.GWS Power supply – external 12 V with 5.5 x 2.1 mm connector
NCP-GWD2B	BOX body – dimensions 218 x 44 x 225 mm (WxHxD) Capacity up to 16 modules, output through 16 sockets Motherboard NCP-SP2BP.GWB (2 slots for EMD cards) Driver NCP-SP1CU.GWS (on OMAP-L138 CPU) Power supply – external 12 V with 5.5 x 2.1 mm connector
NCP-GWS6S	SHELF RACK-1U body – depth 310 mm Capacity up to 24 modules, output through 24 sockets Motherboard NCP-SP6BP.GWS (6 slots for EMS cards) Driver NCP-SP1CU.GWS Power supply 230 V
NCP-GWD6S	SHELF RACK-1U body – depth 310 mm Capacity up to 48 modules (CTS, FXS), output through 48 sockets Motherboard NCP-SP6BP.GWS (6 slots for EMD cards) Driver NCP-SP1CU.GWS Power supply 230 V

LED INDICATORS – front panel LED indicators of device status

LED lighting	STATUS
PWR	related to power supply <ul style="list-style-type: none"> lit continuously if the PBX is on (operation on main power supply) blinks in 0.4 s/0.4 s intervals – operation on battery power
LINK	<ul style="list-style-type: none"> starts to blink slowly when system is booted: among others, means IP address is being acquired from DHCP, and CM approval is in progress after GW is accepted at main shelf and connected correctly, is lit continuously and dims for a moment once every 3-4 seconds blinks quickly – CM communication error firmware change – blinks quickly
UID	two-way communication between shelf and ConfigWEB management software, to be identified uniquely in the system <ul style="list-style-type: none"> lit continuously when shelf is selected in ConfigWEB blinks quickly – CM communication error firmware change – blinks quickly
BAT	related to battery power (1BATC charging module body rear) <ul style="list-style-type: none"> battery disconnected or malfunctioning – not lit battery charging – lit with dimming battery charged – lit continuously device on battery power – blinks 0.4 s/0.4 s

GATEWAY – hardware resources

GWS/GWD GATEWAY RESOURCES	
MAXIMUM NO. OF CALLS FROM GATEWAY	60
DTMF RECEIVER	16

DTMF TRANSMITTER	1
FSK RECEIVER	4
FSK TRANSMITTER	16

More details in technical documentation available here [HERE](#).

1.3. System elements - EMx expansion modules

Expansion modules installed in NCP-GW shelves depending on system capacity. The modules can be freely installed within NCP-GW shelves. Attention must only be paid to the module and shelf type: **EMS->GWS, EMD->GWD**.

MODULE	DESCRIPTION
NCP-EMS4FXS	4 POTS equipment slots (analog ports) Output to 4 RJ-45 sockets Socket no.1 has terminals for 4 additional equipment slots Module comprising a NCP-4FXS.H card and NCP-P4C1P connector
NCP-EMS4FXO	4 POTS equipment slots (metropolitan analog ports) Terminating in 4 RJ-45 sockets Socket no.1 has terminals for 4 additional equipment slots Module comprising only a NCP-4FXO card
NCP-EMS4CTS	4 equipment slots for CTS phones Terminating in 4 RJ-45 sockets Module comprising a NCP-4CTS.H card and NCP-P4C1P connector
NCP-EMS4BRI	4 ISDN-BRI (2B+D) equipment slots Terminating in 4 RJ-45 sockets Module comprising a NCP-2BRI.L card and NCP-2BRI.M submodule
NCP-EMS2BRI	2 ISDN-BRI (2B+D) equipment slots Terminating in 2 RJ-45 sockets Module comprising a NCP-2BRI.L card
NCP-EMS1E1	1 ISDN-BRI (30B+D) equipment slot Terminating in 4 RJ-45 sockets Module comprising a NCP-1E1 card
NCP-EMS1GSM	1 GSM equipment slots Terminating in 1 SMA antenna connector SIM card available outside the body Module comprising only a NCP-1GSM card
NCP-EMS2GSM	2 GSM equipment slots Terminating in 2 SMA antenna connectors SIM card available outside the body Module comprising only a NCP-2GSM card
NCP-EMD8FXS	8 POTS FXS equipment slots (analog subscribers) Terminating in 8 RJ-45 sockets Sockets no.1 and 5 have terminals for 4 additional equipment slots each Module comprising a NCP-4FXS.H and NCP-4FXS.L card
NCP-EMD8CTS	8 equipment slots for CTS phones Terminating in 8 RJ-45 sockets Module comprising a NCP-4CTS.H and NCP-4CTS.L card
NCP-EM1BC	Optional 12 V emergency power supply and 12 V battery charging module, installed in SlotEM1BC inside NCP-GWS6S or NCP-GWD6S or NCP-SW24S shelves

1.4. System elements – SWS24S switch

The NCP system also includes the NCP-SWS24S network switch, available in two variants.

- NCP-SWS24S – L2 switch without management
- NCP-SWS24S.P150 – switch managed via a www interface, including optical ports

SWITCH - available hardware solutions

SWITCH	DESCRIPTION
NCP-SWS24S.P150	Managed network switch (L2 & L3) Body: SHELF RACK-1U - depth 310 mm, width 482 mm, height 44 mm Interfaces: 2xRJ45GbE or 2xSFP Mni-GBIC, 24xFE(PoE 802.3af), 230 V power supply, emergency power supply (optional) Maximum power: 150W
NCP-SWS24S	Network switch (L2) Body : SHELF RACK-1U - depth 310 mm, width 482 mm, height 44 mm Interfaces: 2xRJ45 1GbE; 24xFE(PoE), 230 V power supply, emergency power supply Maximum power: 100W

2. System configuration

NCP-PBX is configured using a web browser and Call Manager's integrated messenger: **ConfigWEB**. First login using the INT interface, where login is **admin** and password is **admin**.

The configurator is used to make all changes, e.g. concerning:

- NCP hardware equipment
- incoming/outgoing traffic
- services
- features
- networks
- internal numbers
- troubleshooting

Navigation around **ConfigWeb** is simple and intuitive. On the left there is a drop-down **Menu** with the individual options. On the right, the main configuration panel. Additionally, for selected configuration options, we offer a convenient **Filter** and a search window.

SIICAN ConfigWEB NCP DWT [NCP000119.34] Logged in as: admin@siican.pl

Gateway shelves

No.	Shelf device	Serial no.	Status	UID	Note
1	[NCP-GWS2B] Gateway box NCP-GWS2B (8 ports)	00846171	OK		obok Lecha
2	[NCP-GWD6S] Gateway shelf NCP-GWD6S (48 ports)	00000700	OK		
3	[NCP-GWD6S] Gateway shelf NCP-GWD6S (48 ports)	00000701	OK		

Annotations:

- CONFIGURATION MANEU TREE**: Points to the left sidebar menu.
- CONTROL PANEL**: Points to the 'Add shelves' and 'Remove' buttons.
- LOG MENU LANGUAGE VERSION**: Points to the top right corner.

SIICAN ConfigWEB Filter extensions

Manage extensions

Extension	Type	Name
1027	CTS (4-1)	CTS 1027
1028	CTS (3-6)	CTS 1028
1029	CTS (3-7)	CTS 1029
1030	CTS (3-8)	CTS 1030
1032	CTS (4-2)	CTS 1032
1033	CTS (4-3)	CTS 1033
1034	CTS (4-4)	CTS 1034
1234567890123456	CTS (3-5)	CTS 11027

Annotations:

- ADDITIONAL FILTER**: Points to the 'View: CTS' dropdown.
- SEARCH WINDOW**: Points to the search bar.

The login panel includes:

- information on the logged-in administrator
- my account
- program information
- help
- language version selection (Polish, English)

Record editing

Depending on which section of the menu you are in, in order to add a new record click the button:

- **Add shelves** - when adding a shelf, section *Hardware configuration->Shelves*
- **Add SIP operator** - when adding an operator, section *Operators->VoIP Operators*
- **Add rule** - when adding an outgoing traffic rule *Outgoing and internal traffic->Dialled number analysis*
- **Apply** – option used in certain forms to accept the changes made without leaving the currently edited form

For further editing of individual records, use the **Edit** link, or for certain records, the other links, e.g.: **Rights** in section *Outgoing and internal traffic->Dialled number analysis*. For records with complex configurations, editing is done in additional tabs. In such cases, edit individual fields in tabs and accept by pressing **OK** or **Apply**.

To remove a given record, highlight the selection field in the first column of given record, then select the **Delete** button.

Slican ConfigWEB

- Summary information
- Diagnostics
- Maintenance
- Networking
- Hardware
- Extensions
 - Settings
 - All
 - Subscribers

Filter extensions

View: All subscribers in set: All subscribers Search:

Manage extensions 21 | 1000

Add Batch edit **Delete**

Extension	Type	Name		
<input checked="" type="checkbox"/> 1001	SIP (robert)	SIP 1001	Edit	WebCTI
<input type="checkbox"/> 1002	SIP (1002)	SIP 1002	Edit	WebCTI
<input type="checkbox"/> 1003	SIP (1003)	SIP 1003	Edit	WebCTI

3. Network configuration

Network settings are configured in the Call Manager shelf only via a web browser. The PBX has integrated WAN/LAN/INT/RDU network interfaces. By default, the LAN port is configured as a DHCP client, while the WAN port is turned off. INT ports are mainly used for connecting NCP system elements, i.e. GWx shelves, CTS.IP system phones, and connecting the redundant system. We do not recommend connecting SIP phones or other network equipment of the customer to INT ports due to no connection (packet routing) with customer's LAN or the Internet. All INT ports have a DHCP server on by default, with specific internal addressing (network **169.254.0.1/17**). The INT/RDU interface is not configurable and is only used for connecting with another CM in the redundant system (RDU licence purchased), or GWx shelves when redundancy is not used.

First login and assigning IP addresses to LAN/WAN interfaces is done using:

- any INT socket, by connecting the computer directly using an ETH cable with DHCP server active on the computer, entering the following address in the web browser: <http://169.254.0.1/admin/>. Default login data are user: **admin** password: **admin**.
- the system will force a password and username change in an e-mail format, e.g.: example@com.pl

The PBX can be accessed:

- locally, after configuring one of the LAN or WAN interfaces (forwarded ports)
- remotely over the Internet, through a dedicated **KEEPER-SLICAN** server, after registering it in the [ServNET](#) service PBX Database

3.1. IP configuration

This menu contains information on the available network interfaces and assigned IP address ranges. We recommend the LAN interface (DHCP client on by default) has a static IP address on account of later logging in of SIP and CTS.IP phones or softphone applications.

In the **Network->IP configuration** tab, complete all field required for the LAN/WAN port:

- IP address** - address assigned by the network administrator
- mask** - network of the mask within which the PBX is going to operate
- gateway** - IP address (usually edge router) to which the PBX is going to send packets in outgoing traffic

Each time that network settings are changed, restart Call Manager (the system gives a notification about requiring a restart to apply changes).

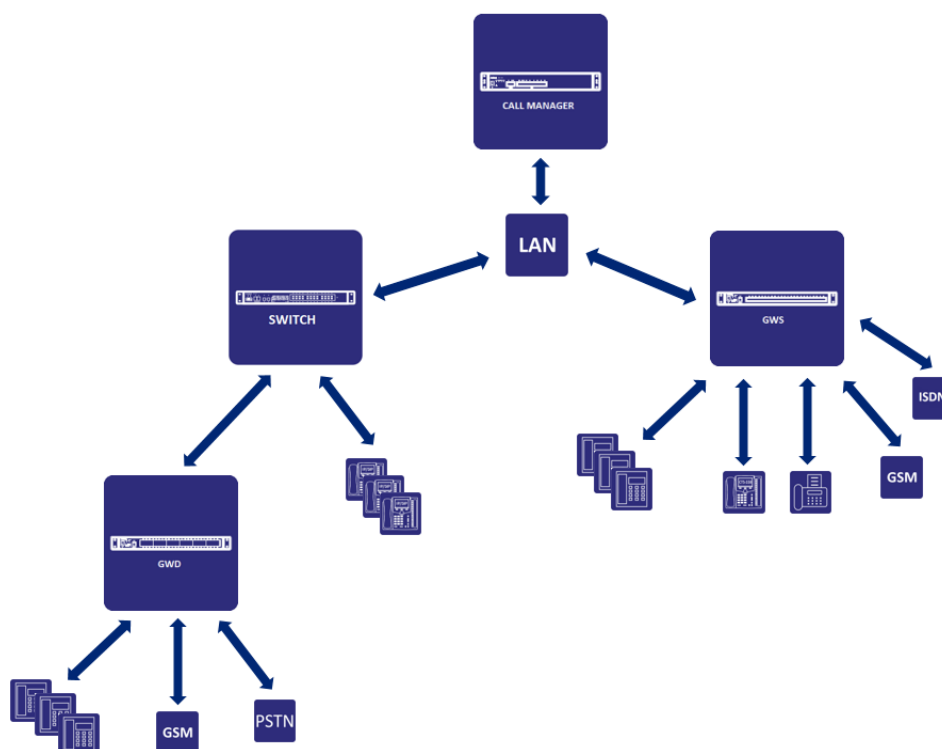
INT network is a separate network available only for elements of the NCP system like GWx.

We **do not recommend** connecting terminal devices, such as SIP phones, to this network. It is not possible to connect it through other local devices (e.g. PCs).

Advantages of INT networks:

- maximum system security
- separated from local traffic in LANs
- logical grouping of equipment
- easier locating of equipment

▪ **through the customer's LAN - LAN interface**



Use of existing LAN infrastructure. Due to the specific nature of signalling between NCP-CM and NCP-GW shelves, it is required that latency in the network was **no greater than 5 ms**. For greater latencies, there is a possibility of incorrect call handling (lack of synchronisation of voice frames).

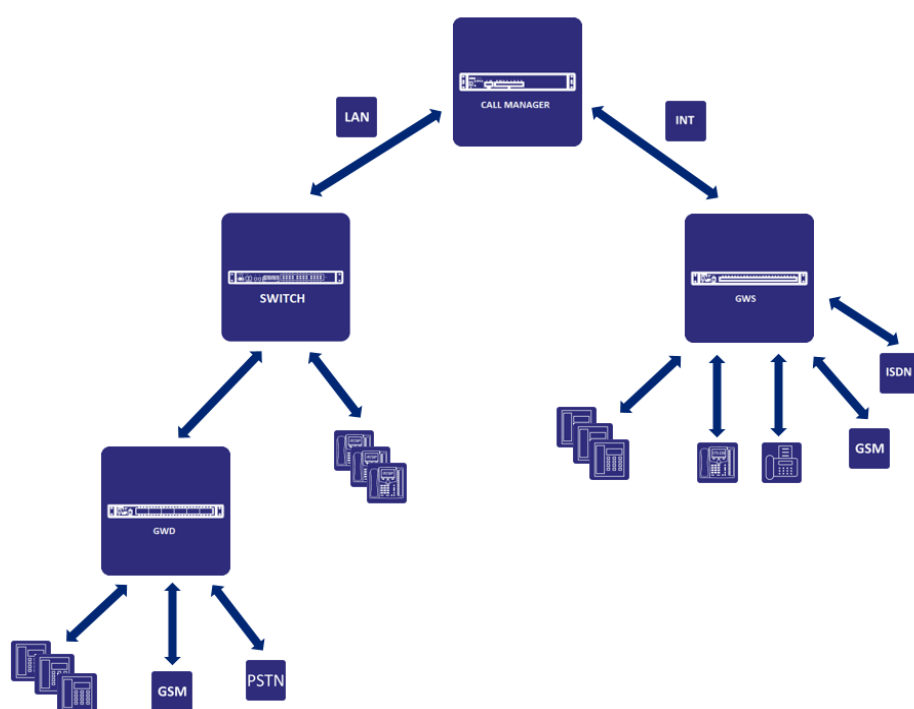
Advantages of LANs:

- simple integration with existing network infrastructure
- greater freedom in arranging equipment within the customer's network
- ability to connect customer's computers to VoIP and CTS.IP phones

▪ **through WAN/VPN**

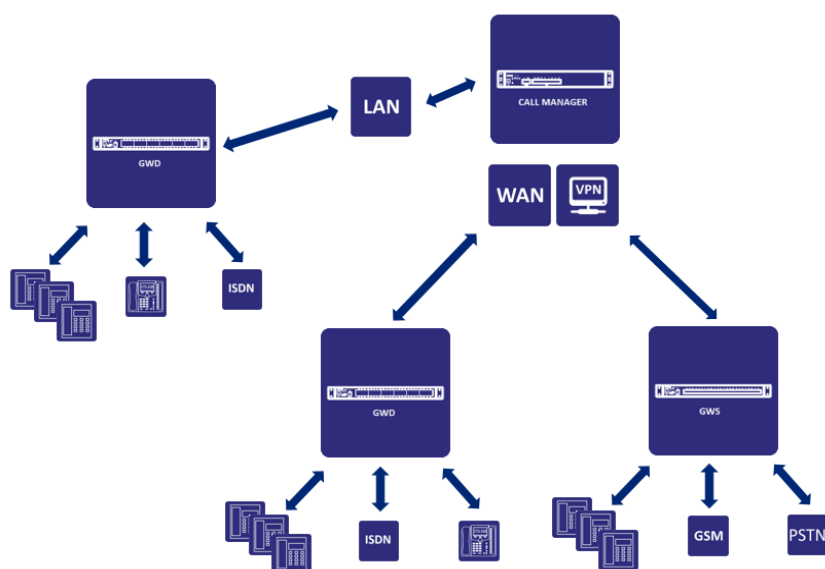
WAN/VPN - by connecting GWx shelves from public Internet or through dedicated VPN tunnels Preparing shelves for remote operation is described in chapter (6) on equipment. Also remember to ensure sufficient bandwidth (more on this subject in chapter (6) on equipment), as well as maximum jitter (10 ms).

- mixed configuration LAN/INT interface



The INT/LAN mixed structure enables system capacity to be increased.

- mixed configuration LAN/WAN interface



3.2. DNS configuration

DNS server configuration: automatically or manually by entering addresses: primary and alternative.
Configuration of static domain names: we assign server IP addresses for appropriate domain names.

3.3. SIP and RTP configuration

SIP and RTP parameters are limited to configuring:

- time (in seconds) of SIP registration expiry (registration at VoIP operator)
- listening ports on the PBX side for individual TCP/UDP/TLS protocols
- RTP port range for handling VoIP acoustics (default range: 10000-20000),

3.4. NAT Configuration

If the PBX is located behind NAT, remember to forward ports on the edge router appropriately. This is important when SIP subscribers of the PBX are outside the local network, and in certain cases of connections to the VoIP operator.

Obtaining public IP address by the NCP-CM:

- Slican server (KEEPER)
- STUN server - enter server name and refresh time
- own configuration - manual configuration of public IP address

Edge router configuration:

- SIP and RTP ports forwarding to local IP address of Call Manager
- active SIP ALG(port forwarding is not required)

3.5. Firewall

3.5.1 Rules

Firewall rule configuration specifies which selected protocols and their related ports will be handled. Select the rule for which network traffic is to be handled from the drop-down list. Specify which interface (LAN, WAN), network address or host the rule applies. Access to rules not on the list is blocked by default.

Access to elements not on the list will be blocked. List of available rules:

- VoIP/SIP/ESSL
- WWW server
- Secure WWW server
- Slican RecordMAN and access to recorded calls by FTP
- Gateway shelves (GWx devices)
- Slican SenderSMS and CTIP
- Hotel protocol (HOTELP)
- Slican PhoneCTI and Slican XML and eSSL protocols
- CTS.IP

- Remote PBX search protocol (USRP)
- ICMP (ping, traceroute)
- LDAP/ TLS LDAP server
- NTP server: unblocking queries for the LAN / WAN port (available on the INT port by default)

Default list of rules:

Firewall rules			
Add accept rule		Delete	
	Scope	Accept from	Note
<input type="checkbox"/>	Web server	LAN interface	Edit
<input type="checkbox"/>	Secure web server	LAN and WAN interfaces	Edit
<input type="checkbox"/>	Silicant RecordMAN and FTP access to call recordings	LAN interface	Edit
<input type="checkbox"/>	Gateway shelves	LAN interface	Edit
<input type="checkbox"/>	Silicant SenderSMS and CTIP protocol	LAN interface	Edit
<input type="checkbox"/>	Silicant PhoneCTI, Silicant XML and eSSL protocols	LAN interface	Edit
<input type="checkbox"/>	CTS.IP	LAN and WAN interfaces	Edit
<input type="checkbox"/>	Remote PBX discovery protocol (USRP)	LAN interface	Edit
<input type="checkbox"/>	LDAP server	LAN interface	Edit
<input type="checkbox"/>	Secure LDAP server	LAN interface	Edit
<input type="checkbox"/>	Hotel protocol (HOTELP)	LAN interface	Edit
<input type="checkbox"/>	Silicant SenderSMS and CTIP protocol	LAN and WAN interfaces	Edit
<input type="checkbox"/>	ICMP (ping, traceroute)	LAN and WAN interfaces	Edit
<input type="checkbox"/>	VoIP/SIP/eSSL	LAN and WAN interfaces	Edit
Access to unlisted items is denied		-	

3.5.2 Black list

A mechanism to block unwanted IP addresses identified as hacker attacks. This applies to incorrect SIP authorization and ConfigWEB login.

Suspicious addresses that make incorrect attempts at authorization via the SIP protocol or login to ConfigWEB are blacklisted.

This address will not be considered as suspicious if:

- is on the list of exceptions
- is on the list of approved addresses (has permission in the IP Filter)

We add an exception if we want to exclude a host or network address from the list of suspects.

If this IP address has been blacklisted (e.g. by multiple incorrect login attempts), it will be unblocked by adding it to the exceptions list.

3.6. Static routing

Adding static routes for directing network traffic depending on individual requirements. Adding a static route will direct packets based on the parameters entered: destination network address, mask, interface (LAN/WAN), or indicated packet routing address (gateway).

A useful feature when the WAN interface is only used as a gateway for handling VoIP traffic (without other network features). In such cases, additionally configure a static route for connecting with keeper.silicant.pl (IP address 5.135.168.169) for remote management and directing queries to DNS if it is not set by the network administrator.

Example static routing entry for keeper.silicant.pl

3.7. WWW server

Configuring the system using ConfigWEB and managing contacts using WebCTI can be done both in the local and public network. Depending on your connection, select the HTTP/HTTPS transport protocol (with data encryption):

- **ConfigWEB**
 - HTTP/HTTPS - from local network
 - HTTPS - from public network.
- **WebCTI**
 - HTTP/HTTPS - from local network
 - HTTPS - from public network.

Connections using the HTTPS protocol require configuring correct certificates defined in section: **Network->Certificates**

3.8. Certificates

SSL certificates are tools that provide website protection, as well as a warranty of maintaining confidentiality of data sent by electronic means. Complete security is the result of using encrypted communication between computers. SSL certificates are registered for the specific domain name, and contain information about the domain owner, their address, etc. The data is protected cryptographically and you cannot change them yourself. The SSL mechanism provides encryption of data exchanged between server and client, and additionally provides the ability to verify server identity.

WWW certificate

Ensuring confidentiality of data exchanged (e.g. during configuration) between the administrator's computer and the PBX requires:

- activating secure connections (HTTPS) for connection from ConfigWEB and/or WebCTI in section: **Network->WWW server**
- importing the SSL key file obtained from the Certification Centre (CA)

Configuration details:

- **server.pem file** - contains information about the certificate issued, i.e.: its validity, issuer, entity, and generated private key
- **overwrite with new file** - the *.pem file obtained from the issuer can be replaced with a new one

- **ca.crt file** - contains information on public certification offices (CA offices)
- **overwrite with new file** - the *.crt file obtained from the issuer can be replaced with a new one
- **verify certificates** - verification of assigned and generated certificates
- **accept current files and restart WWW server** - accept the uploaded files and restart the WWW server
- **restore** - restore default certificates

VoIP certificate

Enables activating encryption of both connection signalling and their contents (acoustics) Similar to secure HTTPS sessions, request the VoIP operator for an appropriate certificate.

Configuration details:

- **asterisk.pem file** - contains information on the certificate, provided by the VoIP service provider, and the generated private key
- **ca.crt file** - contains information on VoIP server certification centres
- **verify certificates** - verification of assigned and generated certificates

The default certificate generated in the PBX enables you to encrypt calls on SIP phones logged in the PBX. This requires downloading and importing the certificate on the phone.

In order to enable encryption of calls from the operator in the PBX:

- import VoIP operator certificates in the PBX, in section: *Network->Certificates->VoIP*

In order to enable call encryption at the SIP subscriber:

- turn on the "Only secure calls" option in the section *SIP subscribers->Advanced settings*
- set the listening port for TLS calls (default 5061) in the section *SIP configuration->TLS port*
- import the default certificate and enable TLS and SRTP call encryption in the phone

NOTE

The default certificate does not guarantee correct authorisation, and consequently the browser will report that it is not trusted. It is highly recommended to change this certificate to one signed by an official certification centre (CA).

3.9. SMTP client

Enables selecting the SMTP server for sending serviceing notifications to the defined e-mail address. Configure account data: login, password, server address, port.

3.10. TAPI configuration

The TAPI protocol enables programs of other providers to communicate with Slican networks through an interface created and developed by Microsoft. With its use, you can control basic phone functions, such as

- caller identification by their presented CLIP number;
- call answering;
- call initiating;

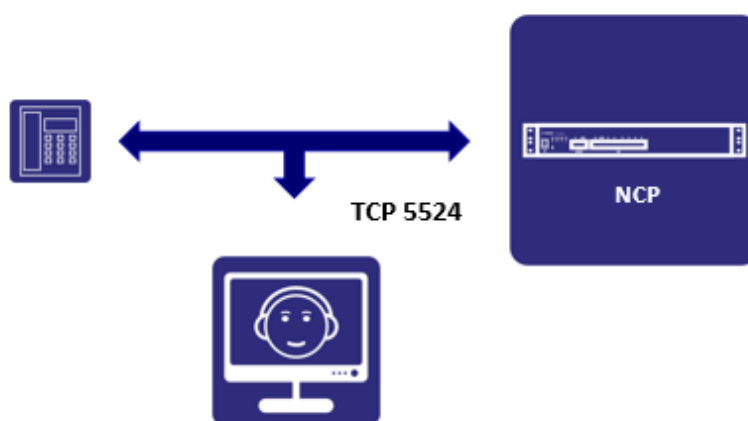
For the above actions, it is necessary to install the [TAPI.workstation](#) application, which enables access to messages sent and received by the PBX, concerning a single piece of subscriber equipment. The simplest method of using its features is to install an MS Outlook plugin and use it to manage calls.

When working with a larger number of subscriber devices, it is necessary to install the [TAPI.server](#) application. This application in itself does not provide any functionalities to the user, in order to use it, connect it with external software that supports the TAPI protocol.

Configuration details:

- **TAPI.server driver password:** password to be entered in the application
- **TAPI.workstation driver password:** numeric password for service access, section: *Subscribers->Service settings->Numeric password*

3.11. CTIP configuration



The **Computer Telephony Integration Protocol** is intended for managing the calls of the given phone.

Management actions can be done

- from an external computer through Ethernet, using the LAN interface.

Signalling enables:

- status viewing
- caller identification
- number dialling
- deactivating PBS services
- sending and receiving text messages
- call recording messages

Configure the following in the PBX:

- numeric password for the application with multiple concurrent subscriber access.
- for logging in of single subscribers, set the password in the section: **Subscribers->CTI settings**

3.12. Web and XML protocols

Web and **XML Slican** protocols enable PBX integration with external software and servers. They provide access to: managing incoming calls, generating outgoing calls, sending/receiving text messages, monitoring subscriber status, and accessing many other functions.

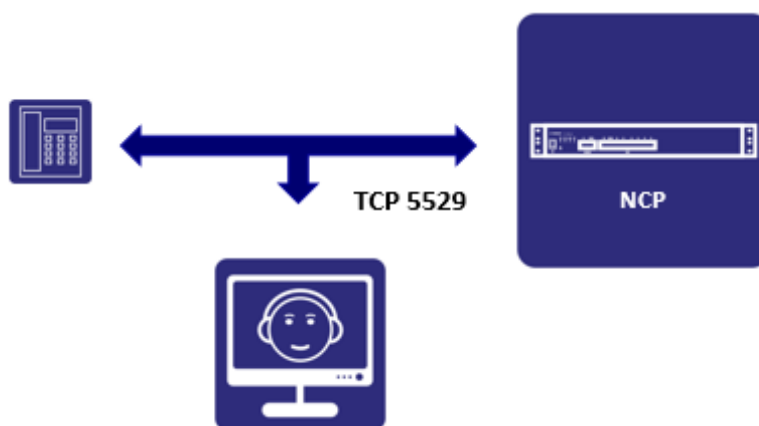
Configuring the PBX requires creating:

- an access account (with login and password, **up to 5 accounts**) - modules: PBX, XML.CDR, WebAPI
- a CTI account - subscriber module: assigning CTI signalling transmission rights
- Web.IVR number - with external server address stated (does not require authorisation)

Also remember to purchase the necessary licences for using your selected products.

Signalling for individual protocols is accessed using the LAN interface (default) or WAN, by listening on the appropriate port. Details on access ports can be found in the chapter “**IP configuration**”.

3.12.1. XML protocol



The **XML** protocol enables the following, among others:

- managing subscriber calls
- monitoring statuses
- contact book access

The following variants of XML protocol support are implemented in the PBX:

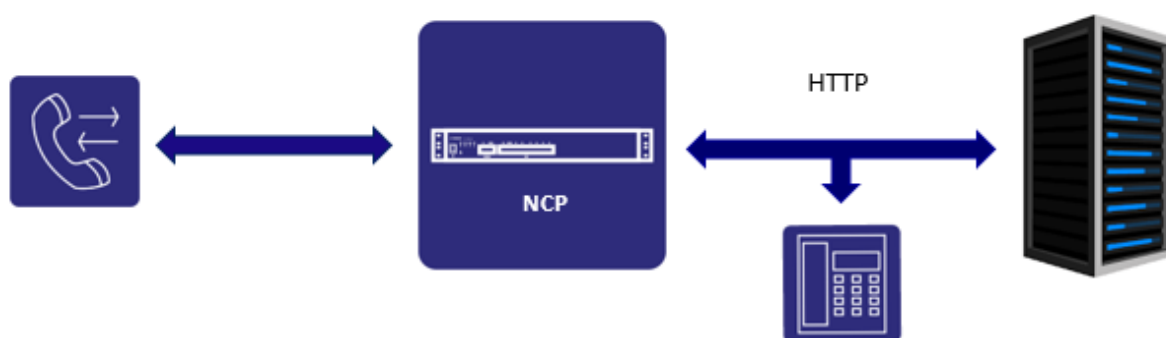
- **PBX module** with access to:
 - **XML.PBX** – PBX configuration (time adjustment)
 - **XML.Status** – internal number status
 - **XML.GSM** – text sending/receiving support
- **Subscriber module** with access to:
 - **XML.Term** – functions on devices
 - **XML.Service** – subscriber services
 - **XML.Calls** – call support
- **CDR module** with access to:
 - **XML.CDR** – access to individual PBX event records (licence required)
- **IVR module** with access to:
 - **XML.IVR** – control of the PBX by an external program (licence required)

The configuration of an XML account of the PBX module can be found in: **Network->Web and XML Slican protocols.**

Subscriber module configuration requires:

- access to CTI transmissions in the section **Internal numbers->Subscribers->CTI settings:**
Access to CTI application

3.12.2. Web.IVR protocol



Web.IVR – enables controlling the PBX using an external server, based on data collected from incoming calls, e.g. based on CLIP presentation or selected PIN. In order to activate the Web.IVR feature, you need to write your own application on a HTTP server, e.g. in PHP. The mechanism is based on the PBX sending a POST query using HTTP, whose parameters contain the received DTMF digits and additional information about the call, such as: call initiator, number dialed, etc. Based on the received information, the HTTP server sends a response in the form of XML commands to the PBX.

Based on the data sent, the protocol enables:

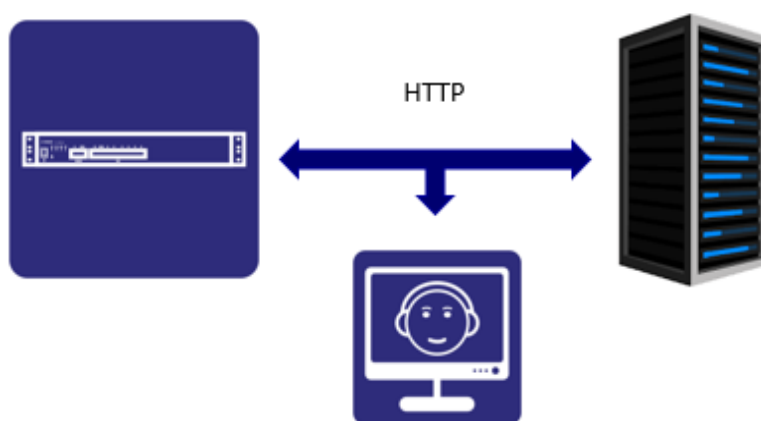
- check the protocol call source based on name sent
- verify the person calling based on their number
- analyse the DTMF digits read
- send digits in DTMF
- check the caller's destination based on number dialed
- read stored own data in the user's field
- direct the call to any metropolitan or internal number
- disconnect the call
- replay the announcement, signal or music

The Web.IVR protocol is configured in the section **Internal numbers->Other: Web.IVR**, which contains the following settings:

- basic settings:
 - assign internal number (not required)
 - assign name

- set HTTP server
 - URL address of server with access path to script
 - maximum number of concurrent queries
 - maximum waiting time for server response
 - action in the event of error or no response by HTTP server

3.12.3. Web.API protocol



Web.API – enables making queries from external servers to the PBX, which performs the required actions in response.

Based on the queries sent, the protocol enables:

- obtaining information on the status of the subscriber's phone call
- summarising phone calls
- setting descriptions or additional statuses to subscribers
- changing descriptions on system phone displays
- downloading information about call center queues

To configure an PBX, a Web/XML account must be created in **Network->Web and XML Slican protocols**.

The query mechanism is based on sending queries using the POST method to the PBX's HTTP server, containing parameters in the **application/x-www-form-urlencoded** format.

More details on Web and XML protocol support, including documentation, can be found on the [Slican SDK website](#).

3.13. eSSL system

PBX networking using the internal [eSSL2\(extended Smart Slican Link v2\)](#) protocol enables connecting Slican exchanges into a single system with common internal numeration. This protocol utilises elements of SIP signalling to PBX information between such systems as:

- PBX type and serial number

- catalogue numbers and comments
- call statuses: free, busy, damaged, being dialled, DND
- information on: subscribers, accounts, groups, sensors, intercoms

Each PBX in the network knows the configuration of its neighbours, so internal traffic in linked exchanges is routed automatically and does not require programming. The internal numbers book contains a list of all subscribers in the linked exchanges, subject to the "do not show entry in internal numbers book" flag.

3.13.1. eSSL protocol

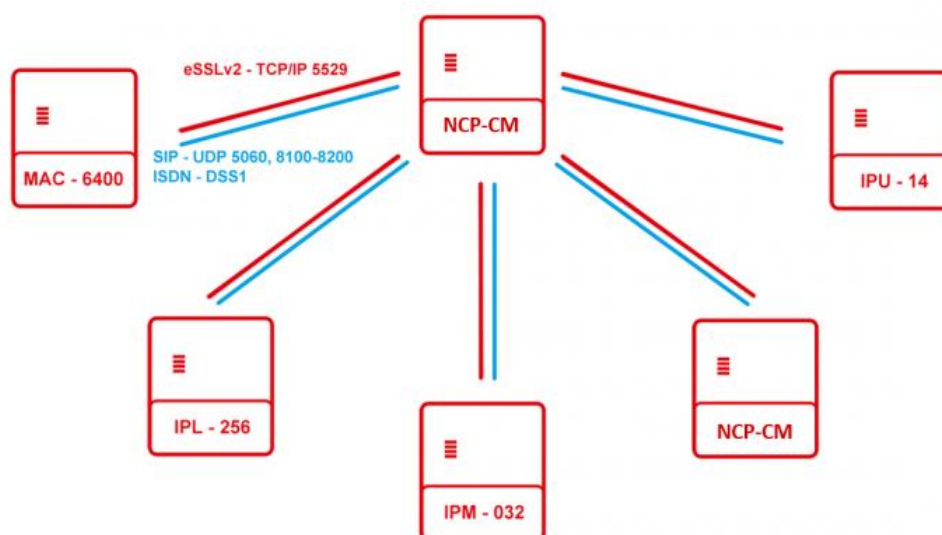
An important characteristic of NCP exchanges is the ability to network systems, based on the eSSL2 protocol. Aside from all networking attributes, based on the previous version of the eSSL protocol, the latest one provides new additional abilities:

- networking of up to 50 exchanges
- system capacity is 10000 linked numbers + PBX own numbers
- dividing eSSL signalling (by TCP/IP port 5529 connection to acoustic connections)
- public book synchronisation between networked exchanges
- chat in the PhoneCTI application between networked exchanges
- forwarding PhoneCTI application status and description between networked exchanges
- non-published numbers can overlap in each PBX and it generates no conflicts
- ability to send text messages through a GSM gateway located in a server

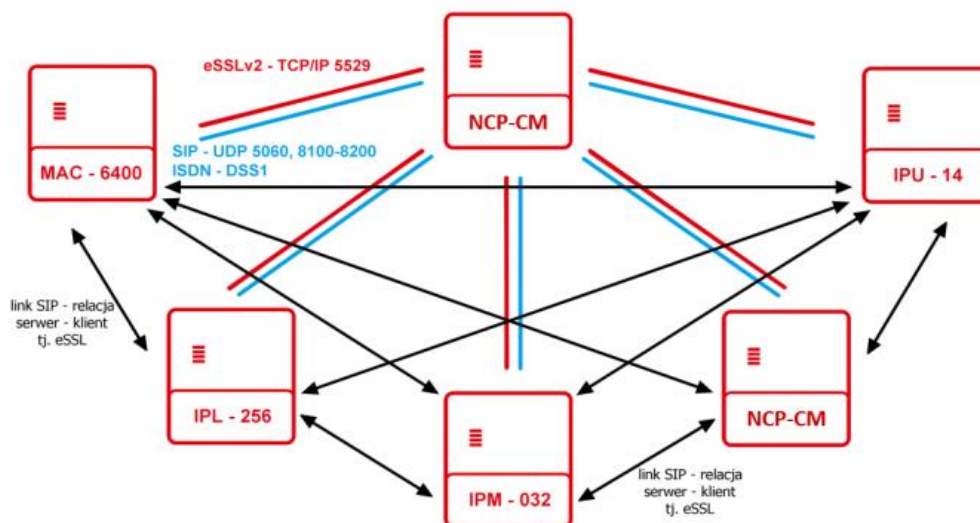
For linking with the use of an ISDN connection remember that contact synchronisation and statuses are sent through the LAN using TCP (port 5529), which means a need to configure the network on both ends of the link.

Sample eSSLv2 network topologies

- **star topology**



- **full mesh topology**



Configuration eSSL

Preliminary configuration applies to selection of PBX operation mode and setting the server/client relations.

eSSL protocol: eSSL server - configuration of server functions

- **disable contact book synchronisation** - synchronisation of public book contacts
- **disable chat message transmission using eSSL connections** - access to the chat feature using the PhoneCTI application
- **enable text message transmission using eSSL connections** - permit sending/receiving text messages using the PBX
- **exchanges other than NCP are connected to eSSL** – enables correct handling of traffic when exchanges other than NCP are in the system
- **SIP** - linking using SIP Operators->VoIP Operators
- **ISDN protocol** - linking using ISDN (QSIG) protocol Operators->TDM Operators

eSSL protocol: eSSL client - client configuration

- **host name or eSSL server IP address** - set the IP address of the eSSL server
- **SIP** - linking using SIP Operators->VoIP Operators
- **ISDN protocol** - linking using ISDN (QSIG) protocol Operators->TDM Operators

3.13.2. eSSL status

Contains information on available systems synchronised using the eSSL protocol:

- **type** - PBX type, e.g. NCP
- **number** - PBX serial
- **function** - server/client
- **status** - connected/not connected
- **address** - IP address of the server/client
- **synchronisation** - current status of information synchronisation between systems
- **name** - descriptive name of the synchronised systems

- **description** – any description of the link

3.13.3. Solving conflicts

Information for the administrator about number conflicts between synchronised exchanges, and information on non-published numbers.

3.14. Redundancy system

Redundancy in communication enables defining excess communication routes that can be used interchangeably (a sort of hot reserve). Redundancy finds its use mainly in the case of extremely important information, of strategic importance for the system. Particularly frequent is data redundancy in telecommunication systems, where reliability of transfer is crucial during transmissions. Utilisation of redundancy in NCP-PBX systems involves doubling the critical system element that Call Manager is. Full synchronisation of system data (MAIN-BACKUP) depends on the CM type and takes **20 minutes** on average.

From the point of view of the redundancy system, there are 3 NCP-CM types:

- **ALONE** - an independent unit without the redundancy system
- **MAIN** – main CM
- **BACKUP** - backup CM

A more detailed specification of the CM type is its operating mode:

- **ACTIVE** - currently active
- **STANDBY** - hot reserve

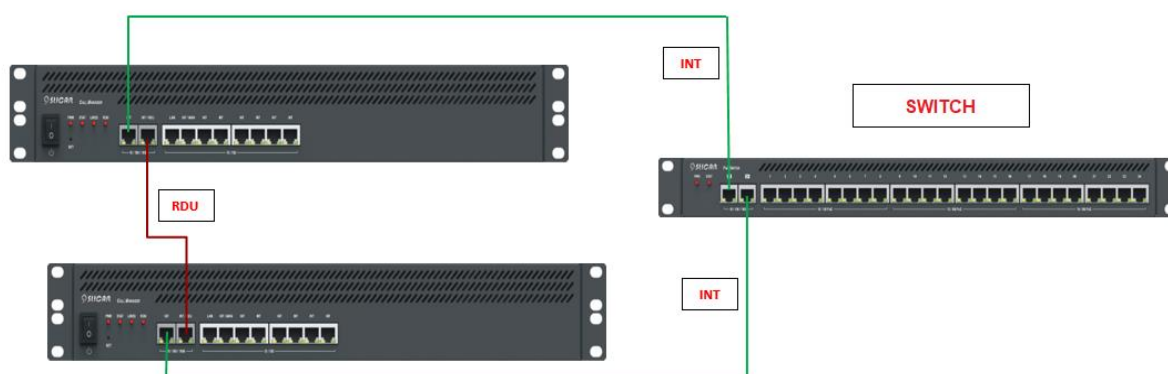
The entire configuration, as well as changes made to CM MAIN, are automatically copied and sent to CM BACKUP. In the event of CM MAIN failure, CM BACKUP begins operation based on the latest data backup. Utilising the RDU system requires configuring a static IP address of the LAN and/or WAN interface. This is related to smooth taking over of the CM MAIN IP address by CM BACKUP and logging in of VoIP terminals. Estimated time to system switchover: approximately **2 minutes**.

Configuration details

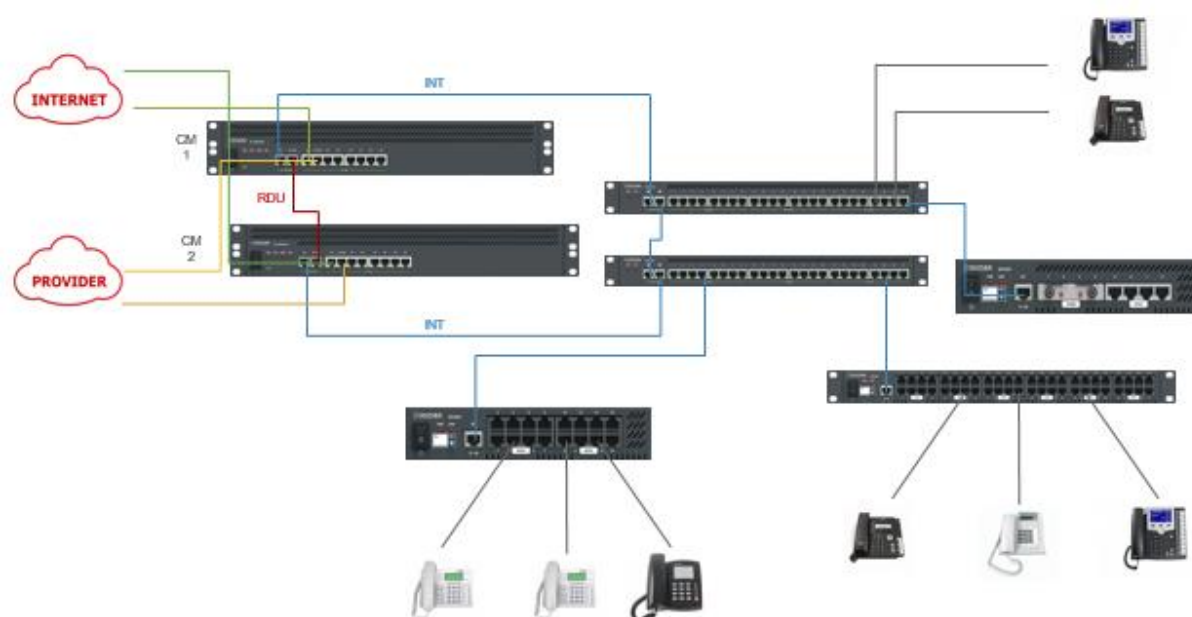
Connecting two Call Manager devices into a functional redundant system requires:

- formatting one Call Manager as MAIN, and the other as BACKUP in the section *Operation->Factory Format*
- entering the right licence in CM MAIN
- connecting the right CM ports (RDU and INT interfaces) - as per the figure below
- full data synchronisation between CM MAIN-BACKUP(check LED indicators)

For the redundancy to work properly, it is necessary that the RDU and INT interfaces are connected to each other. If we use LAN or WAN interfaces, they must also be connected to the network with both CM MAIN and CM BACKUP. It is important to pay attention when connecting the interfaces so that no loops are created that may prevent the network from working properly. As there are built-in switches in Call Managers, it is not allowed to use multiple INT sockets and connect them in a way that may cause a loop. Sample configuration using one switch.



Sample configuration using two switches..



After the two Call Managers are synchronised correctly, system functioning can be monitored in the **Redundancy status** tab:

Silcan ConfigWEB

Summary information

Diagnostics

Maintenance

Networking

- IP configuration
- DNS configuration
- Static routing
- Firewall
- SIP and RTP configuration
- Web server
- Certificates
- SMTP client
- Web and XML Silcan Protocols
- TAPI configuration
- CTIP configuration
- eSSL system

Redundancy system

- Redundancy status
 - Failover

Redundancy system status

Redundancy system ready to failover

Active call manager:MAIN (NCP000001)

Diagnostic informations

Connections status

Connection on interface INT:

Connection on interface RDU:

Redundancy system components

Call manager	Serial number	Firmware version	
MAIN	NCP000001	1.11.0096	Running
BACKUP	NCP000006	1.11.0089	Standing by

Additionally, the redundancy system enables **automatic switching** of the RUNNING mode between MAIN and BACKUP devices according to a scheduled time scope. A feature useful from the standpoint of RDU system prevention, ensuring reliability of its functioning.

The screenshot shows the Slican ConfigWEB interface. On the left is a navigation menu with categories like Summary information, Diagnostics, Maintenance, and Networking. The 'Failover' option under the 'Redundancy system' is selected. The main content area is titled 'Manual failover' and includes a link to 'Maintenance > System reload'. Below this, there is a 'Scheduled failover' section with a checkbox for 'Scheduled failovers' and a dropdown menu for 'Choose time frame to schedule automatic failover:' set to 'Weekends only'. A 'Save' button is located at the bottom of the configuration area.

4. Accounts

A single account with **administrator** (admin) rights is created in the startup option of the PBX.

The system provides information about the currently logged-in account in the top right corner of the ConfigWEB configurator.

The other account information is configured in the following forms:

My account

This tab provides the ability to change the password of the currently logged-in account. Additionally, you can configure sending of notifications about events in the PBX to the e-mail address provided as the account login.

Furthermore, information about available new firmware versions can be enabled.

Administrator accounts

This tab enables addition further system administrator accounts. Accounts can be created permanently or with a time limit. There is also a technical support account (support@slican.pl) with system configuration rights available, deactivated by default.

Adding further administrator accounts:

- **Login** – in e-mail address format, e.g. *admin@slican.pl*
- **Password** - account access password
- **Password change required on next login** - option to enforce password change when the user logs in next time
- **Send notifications to administrator e-mail account** – sending messages about events in the PBX

- **Send activation e-mail** – administrator password information will be sent to the e-mail address indicated in the login
- **Language** - language version setting for the account
- **Description** - optional account description
- **Time-limited account** – account expiry date setting, after which the account will be deleted
- **Show information about available new firmware versions** – the Updates tab and the upper section of the configuration panel will display information about new software versions

Account access rights configuration:

Specify access rights to:

- **ConfigWEB** - application access
- **Administrator accounts** - creating and editing accounts with admin rights
- **Access control system (ACS)** - rights to the access control application
- **AudioMAN** – rights to manage Audio Slican system
- **WebCTI** -

There are three levels of access to administrator accounts and configuration:

- **Disable** - administrator accounts/configuration cannot be edited
- **View only** - accounts/configuration cannot be edited
- **Enable** - system configuration and adding administrator accounts are allowed

5. Operation

This section of the configuration includes access to basic and advanced features of the PBX, e.g.: software updates, system formatting and backups.

5.1. Configuration recovery points

Each time changes are made to the PBX configuration, an automatic configuration recovery point is created. These points are used to quickly cancel undesired modifications or to restore an earlier, stable PBX configuration. Each point is described with the date and time of configuration change, and the login of the administrator who made the change in the system configuration. It is also possible to create manual configuration recovery points with additional description of the changes made. A recovery point is created during one login session. In order to restore a correct system configuration, select the option: **Restore**. In order to delete subsequent recovery points from the list, highlight the given record and select the option: **Delete**.

5.2. Backups

It is a full backup containing PBX configuration, announcement, hold music, provisioning files, certificates, recovery points and contact book. Restoring a backup overwrites all data in the PBX and should be done only in the event of data loss from the carrier.

From version 1.14, Call Manager allows you to perform backups on an external FTPS server. In the backup copy settings we define: the location of the backup copy - on an external FTPS server or on a local disk, the time of backup and the number of copies that was stored on the media. If you choose the location of the

backup copy on an external server, you must configure the connection parameters: FTPS server address, port, login details.

In order to create a backup, select: **Create backup**. A backup file will be created on the PBX hard disk or on the FTPS server. In order to download it and save on any carrier, select the option: **Download**. Restore configuration from a saved backup file by selecting: **Select file** then **Upload**. It is recommended to create backups in the event of problems with system functioning. Restore backups from a file saved on the PBX or on the server, by selecting: **Restore**. The backup from the file saved on the PBX will be prepared without overwriting files. It will be restored only after rebooting the system. Until it is done, the action can be cancelled. The backup is created obligatorily (automatically) when software is updated. Do not modify the backup file names.

5.3. Software updates

NCP system update

PBX software can be updated in two modes:

- **Update from ServNET** - the PBX will check whether the latest retail software version is available on the dedicated ServNET server. If it is, the PBX will show a notification about the available remote update. Notifications about available new software versions are on by default. They can be disabled in the *Update settings* tab. This mode also enables downloading the list of changes in the software. Additionally, you can download the update changelist file.
- **Manual update from file** - you need to have a current software file, downloaded from the [ServNET](#) access resource. Upload the downloaded software file to the PBX by selecting: **Select file**, and indicating the location of the software file, then: **Upload**.

For a full update, **PBX REBOOT** is required. The PBX creates a backup each time before an update is performed.

In the event of unexpected problems after updating the software, the previous version can be restored by scheduling an PBX reboot.

Software updating without an additional licence is possible for 12 months from the date it is issued.

If there are problems after a software update and PBX configuration cannot be accessed, it is possible to restore its previous version as follows:

- turn the PBX off,
- press and hold the **SET** button on the device body,
- turn the PBX on,
- wait for about 7 seconds and release the **SET** button when the acoustic signal ends (the first acoustic signal).

PhoneCTI application update

Automatic PhoneCTI application update. All logged-in PhoneCTI applications will be updated to the latest version.

Available methods of updating the PhoneCTI application

- from an installer file in the PBX - by downloading it
- by uploading the installer file to the PBX from your own resources
- automatic update from ServeNET

The PhoneCTI application is no longer developed and supported !!!

MessengerCTI application update

Automatic MessengerCTI application update. All logged-in MessengerCTI applications will be updated to the latest version.

Available methods of updating the MessengerCTI application

- from an installer file in the PBX - by downloading it
- by uploading the installer file to the PBX from your own resources
- automatic update from ServeNET

Update settings

Configuration of settings concerning notifications about available new updates: PBX software and the PhoneCTI and MessengerCTI applications.

NOTE

Do not modify the name of the downloaded file before it is uploaded.

5.4. Licences

Individual PBX features require purchasing a licence. Lack of licence or attempt to go beyond current terms will be indicated in ConfigWEB by no ability to configure the given feature. When planning resources, estimate the number of subscriber accounts and other features to select the appropriate licence. Licence codes are entered in the **Maintenance->Licences** tab. Licences can be added individually or in series.

Slican ConfigWEB		Licences codes	
<ul style="list-style-type: none"> Summary information Diagnostics Maintenance <ul style="list-style-type: none"> Configuration restore points Security backups Updates Licences System clock Name and description System reload Factory format Networking <ul style="list-style-type: none"> Hardware Extensions Providers 		Add Add multiple Delete	
		Code	Description
		3GFLB-BK5MR-QEPK3-RL7ZP-H9UZ8	NCP base licence (NCP.Base40) Subscribers: NCP.Base40: 52 / 40 / 1000 Concurrent calls: NCP.Calls: 40 / 100
		8KBPS-JAQ95-0KAEQ-1CZ7F-9H47G	Call recording Base licence: NCP.Base40: 5 / 100 Concurrent recordings: NCP.RecChannel: 4 / 1 / 30 RecordMAN.client users: NCP.RecordMANclient: 4 / 1 / 30 RecordMAN.server: NCP.RecordMANserver: ✓ / ✗ Other applications: NCP.ServerFTP: ✓ / ✗
		5P3T6-SUR11-X9MG4-UH2S3-LCR5D	Conferences Base licence: NCP.Base40: 15 / 60 Concurrent participants: NCP.ConfMembers: 15 / 60

The appropriately formatted fields enable entering licences by copy/paste.

Modify licence code	
Activated:	<input checked="" type="checkbox"/>
Licence code:	3GFLB - BK5MR - QEPK3 - RL7ZP - H9UZ8
type in code from a printout or copy/paste full code (including dashes) into first input field	
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/>	

A detailed description of current licences can be found in the product catalogue.

PBX users can run a trial of the licensed PBX features before purchasing the licences for the features they are interested in. To this end, enter a **“TRIAL”** licence code. A **“TRIAL”** licence is issued for the duration stated in the licence (usually 1 month) and entering this code results in unlocking any licensed features with the maximum values determined by the PBX's hardware capacity. As mentioned above, **“MAX-TRIAL”** licences have a limited duration, the licence validity period can be found in the *Operation->Licences* section. The PBX also provides information on the licences required after TRIAL licence expiration. Once a TRIAL licence expires, the PBX returns to the values determined by the remaining licences.

5.5. System clock

System date and time can be set in two ways:

Changing the date and time manually by selecting the **None** option from the **System clock synchronisation** drop-down menu.

- **date setting** - by clicking the date field, you can set the appropriate date using the calendar form.
- **time setting** - by clicking the time field, you can set the appropriate time using the calendar form.

Automatic synchronisation of system clock downloaded from the NTP server.

- **Time zone** - select the appropriate time zone, e.g. Europe/Warsaw
- **NTP server address** - select the time server (default: tempus1.gum.gov.pl)

5.6. Name and description

Additional information in the form a description, identifying the given PBX. The name entered will be visible in the upper part of the ConfigWEB window.

5.7. System Commands

In Call Manager, you can use system commands that change the default settings of some parameters.

5.8. System reboot

The system can be rebooted in one of several ways:

- **immediate reboot** - all active calls will be terminated;
- **safe reboot** - restart after terminating all active calls, new calls will be blocked
- **discrete reboot** - restart when there are no active calls, new calls will be initiated correctly
- **configuration reload** - full configuration synchronisation without restarting the PBX, does not terminate current software update processes or backup restoration.

5.9. Factory format

If there are issues with configuration or system stability, as well as with creating a redundancy system, it is possible to format Call manager.

The Call Manager body is fitted with a **SET** button, which is used to perform the format.

Format procedure using the SET button:

- create a backup,
- select the type of format from ConfigWEB:
standard, for the redundancy system, redundancy system servicing
- turn the PBX off,
- press and hold the SET button on the device body,
- turn the PBX on,
- wait for about 19 seconds and release the SET button when the second acoustic signal ends.

Available format modes:

Standard format

- **soft format:** PBX configuration, contact book and recovery points will be lost. Recorded calls and billing data will be retained.

- **full format:** PBX configuration, announcements, hold music, provisioning files, certificates, recovery points, recorded calls, billing data and contact book will be lost.

Redundancy system creation (first startup) – formatting related to the first startup of a redundancy system. In this case, select one CM as MAIN, the other as BACKUP, and format them appropriately (RDU licence is always assigned to CM Main).

- **device format for redundant operation as MAIN:** PBX configuration, announcements, hold music, provisioning files, certificates, recovery points, recorded calls, billing data and contact book will be lost.
- **device format for redundant operation as BACKUP:** PBX configuration, announcements, hold music, provisioning files, certificates, recovery points, recorded calls, billing data and contact book will be lost.

Servicing an existing redundancy system - a formatting type with an existing redundancy system, activated if one unit is damaged after it is replaced as part of servicing.

- **device format for operation with an existing redundancy system as MAIN:** PBX configuration, announcements, hold music, provisioning files, certificates, recovery points, recorded calls, billing data and contact book will be lost. The device will be synchronised with the BACKUP device.
- **device format for operation with an existing redundancy system as BACKUP:** PBX configuration, announcements, hold music, provisioning files, certificates, recovery points, recorded calls, billing data and contact book will be lost. The device will be synchronised with the MAIN device.

If there are problems after a software update and PBX configuration cannot be accessed, it is possible to restore its previous version as follows:

- turn the PBX off,
- press and hold the SET button on the device body,
- turn the PBX on,
- wait for about 7 seconds and release the SET button when the acoustic signal ends (the first acoustic signal).

NOTE

IT IS RECOMMENDED TO CREATE A DATA BACKUP ON AN EXTERNAL DATA STORAGE BEFORE PERFORMING A FACTORY FORMAT.

6. Hardware configuration

Individual elements of the NCP system are configured in the Call Manager shelf. An exception to this are switches and configuration of IP addresses of remote GWx shelves.

In order for GWx shelves with modules to be visible in CM, they must be added and accepted. Ports in modules need to be configured appropriately.

6.1. Adding shelves

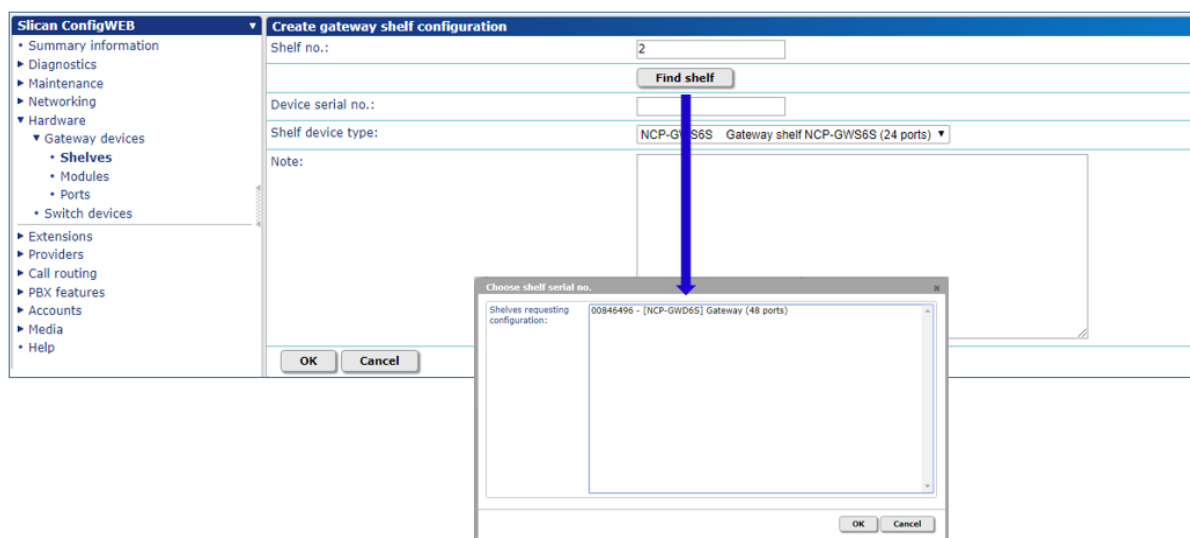
GWx shelves have an algorithm implemented for “searching” for Call Manager in the network. A GWx shelf sends its ID in the form of its serial number and hardware address. Call Manager identifies individual shelves and places them in its table, waiting for approval by the system administrator. When connecting

shelves in local mode via LAN, remember that CM and GWx need to be in the same network (subnetwork) - without an intermediary router. The remote mode requires the IP address of the Call Manager which the shelf is to be assigned to be configured.

The shelf adding procedure is as follows:

- determine the shelf number
- enter or select from the list the serial number of the shelf waiting to be configured, and enter its type.

Each shelf must also be assigned a detailed description for identification. For high-capacity systems and visual identification of shelves installed in a rack, enable/disable the **UID** marker in the main add shelf tab. The UID is used for two-way communication between the shelf and ConfigWEB management software, to be identified uniquely in the system



6.2. Adding modules

An PBX equipment module is an expansion card with a front panel fitted with external TDM port interfaces and internal equipment ports. All modules can be installed in GWx shelves in any slots of its motherboard. With the exception of the GSM module, all interfaces terminate with an RJ45 socket. Slots without modules are capped.

Module acceptance procedure:

GWx shelves will detect the type of the installed module themselves, you only need to accept or remove individual modules installed in a shelf in the *Hardware configuration->Modules* section. An additional filter enables selecting only a single module.

6.3. Port configuration

Depending on their type, configuring individual internal and external ports involves defining their essential parameters in the **Edit** and **Configuration** tabs of the section

Hardware->Gateway devices->Ports.

INTERNAL PORTS - EDITING

Editing internal ports is described in detail in Subscriber configuration (chapter 7, Internal Numbers).

INTERNAL PORTS - CONFIGURATION

Configuring physical parameters of internal ports:

- **FSK presentation content** - specification of the CLIP type received in FSK signalling (applies to FXS):
disabled, number-date, number-name-date (useful for devices with small displays)
- **echo cancellation level** - configuration of echo elimination level of the call (standard, comfortable background, strong echo elimination)

EXTERNAL PORTS - EDITING

Details of editing and configuring metropolitan line ports depend on the port type. Metropolitan line ports can also be configured in the *Operators->TDM* operators section.

Editing - TDM operator properties

- **TDM operator type** - select the specific operator (FXO, GSM, ISDN BRI, ISDN E1)
- **default forwarding** - enter the default internal number to which calls are forwarded
- **add ports** - select available ports from installed TDM modules (port bundle within the given operator)

EXTERNAL PORTS - CONFIGURATION

FXO - metropolitan analog line

Important parameters of analog operator configuration include:

- **main number** - operator's own (country prefix, direction prefix, number)
- **call billing** - by time or by polarity inversion
- **FSK signalling reception** - reception of the caller's presentation in FSK
- **400 Hz signal detection** - report and busy signals
- **billing method** - by polarity inversion or by billing time
- **echo cancellation level** - configuration of echo elimination level of the call (standard, comfortable background, strong echo elimination)
- **error notification** - servicing notifications about port status

GSM - metropolitan digital line

The main parameter for mobile operators is the SIM card's **PIN**. A second important parameter is the operator's main number, which needs to be configured.

Configuration details:

- **main number** - operator's own number (country prefix, number)
- **SIM card PIN code** - PIN code assigned to the card (applies to GSM ports only)
- **operator detection setting** - automatic or manual
- **echo cancellation level** - configuration of echo elimination level of the call (standard, comfortable background, strong echo elimination)
- **error notification** - servicing notifications about port status

ISDN BRI/ ISDN E1

For digital ISDN lines, it is important to define whether they operate in PP contact (point-point) or PMP (point-multipoint for MSN) configuration. The method of contact signalling operation also needs to be specified, where:

- **TE** - it is classic contact operation, working with the telecommunications operator as a slave PBX for another (master) PBX and receiving synchronisation from it.
- **NT** - it is a mode where the ISDN contact is master towards another PBX, used most commonly when working with other PBXs.

The contact enables receiving numeration in incoming traffic both as a block (En-block method) and digit after digit (Overlap method).

Configuration details:

- **main number** - operator's own number (country prefix, direction prefix, number)
- **ISDN signalling** - specifies the NT/TE signalling type and point of contact with the operator or another PBX
- **reference clock synchronisation** - clock synchronisation from master (public) PBX
- **method of dialled number reception for incoming traffic** - method of receiving digits for incoming calls: as a block (whole number) or overlap (digit after digit)
- **caller presentation transmission format** - specifies the method of presentation for outgoing traffic:
 - **national**: the presented number will comprise city prefix + subscriber number, e.g. 513251100
 - **international**: the presented number will comprise country prefix, city prefix + subscriber number, e.g. 48513251100
 - **internal (subscriber)**: the presented number will only comprise the subscriber number, e.g. 3251100
 - **unknown**: the presented number will comprise the subscriber number truncated to the number of digits set, e.g. 1100 (for number of digits = 4)
- **enable CLIRO** - override caller presentation blockade (licence required)
- **available channels** - configuration of the number of channels for traffic handling (unlimited by default)
- **echo cancellation level** - configuration of echo elimination level of the call (standard, comfortable background, strong echo elimination)
- **error notification** - servicing notifications about port status

6.4. Switch

Slican Switch PoE is a switch with the ability to manage its configuration. It contains 24 Fastethernet ports and 2 Gigabitethernet ports (including a 2xFSP optical contact).

The form contains a list of available switches. By selecting an appropriate link with an IP address, you receive direct access to the switch configuration panel (more details in the product catalogue). Additional device identification using a UID button.

7. Internal numbers

This chapter describes how to add and edit: internal numbers, service numbers, how to configure features, define queues and groups. The **All** menu displays a list of all numbers defined in the system. An additional filter enables listing services enabled for individual numbers or membership in a given set. Additionally, you can filter subscribers by: number, equipment type, service permission, or enabled.

7.1. Settings

Additional settings concerning internal numbers.

- **Default number of internal number digits** - from 2 to 16
- **subscriber idle duration** - number analysis duration within the 3 to 10 seconds range, after which the PBX will begin connecting the call once the last digit of the number is dialled
- **time until hotline selection** - time after which the call is directed to the hotline, if the subscriber has selected no number
- **shorten internal number dialling analysis** - if the subscriber dials a correct internal number, do not wait for # or analysis time, but immediately go to dialled number analysis: (practical for separable configuration of internal and metropolitan numbers)
- **show recording sign on system phone display** - additional information about recording the call on CTS phone displays
- **ringtone type for internal calls** - single, double and triple available
- **ringtone type for calls from operators** - single, double and triple available
- **host screen frequency** - checking of SIP subscriber equipment status (60s default)
- **voice mail settings** - advanced voice mail support, i.e. directing to internal number, forwarding when inbox is full
- **WebCTI application settings** – set host name or IP address of PBX for the configuration WebCTI application account (optional for connections outside the LAN also the port).
- **MessengerCTI settings**
 - set the public name or IP address of the PBX along with the XML Slican port (5529) to send authorization data and account configuration for the MessengerCTI application user
 - set the public name or IP address of the exchange along with the port for VoIP connections.
 - enter the public name or IP address of the PBX together with the port for file transfer
 - set telephone number to the PBX: the return number on which the connection for handling outgoing and incoming connections made from the MessengerCTI.mobile application working in GSM mode.

Above CTI settings and authorization data will be send via email (address must be set on subscriber account) to end user as a information about account logging.

7.2. Subscribers

In Slican exchanges, subscribers (and corresponding equipment) and accounts (virtual subscribers) are treated identically. All rights and permissions that can be set for **subscribers** with equipment also apply to **accounts**, which do not have permanently assigned equipment. There are many different types of internal numbers: system SIP, analog and virtual. They have mostly the same settings. The following types of users/internal subscribers can be created in the system:

- **FXS analog:** user equipped with an analog phone
- **CTS/CTS.IP system:** user equipped with a system phone
- **SIP:** user equipped with a VoIP phone or softphone
- **virtual account (number):** specifies a user without an individually assigned physical subscriber port in the PBX (without a personal phone) Accounts can be created on any phone in the PBX (CTS/CTS.IP, FXS, SIP)
- **MessengerCTI:** user account of MessengerCTI.Desktop application with active VoIP option or MessengerCTI.Mobile (active application for Android system)

Internal numbers of subscribers are assigned when the equipment (module) is detected by the system, SIP and virtual numbers are added manually. Subscribers of any type created in the system, which are not currently in use, can be disabled without deleting it.

Adding further number types is done individually, except for SIP numbers, where numbers can be added sequentially. An additional filter enables listing selected types of subscribers.

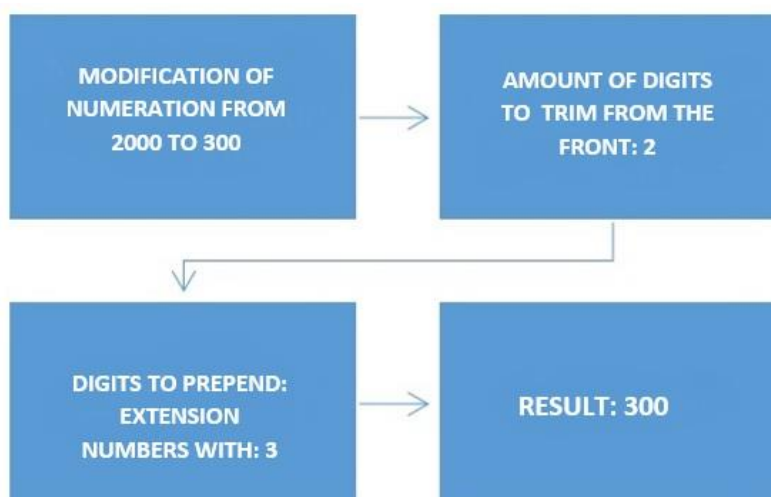
It is also possible to sequentially modify internal number numeration. Numbers of the same type are modified.

Numeration modification applies to:

- indicated digits within the numbers, e.g. digit 2 to 3, which results in a change from 2000 to 3000 (all digits 2 are changed to 3):



- modification of the whole or part of a number by truncating digits, e.g.: 2000 to 300, where the number of digits truncated from the beginning of the number is 2, and replaced (preceded) by the digit 3.



Aside from numeration, it is also possible to sequentially edit the other settings (which do not require individual settings), i.e.: services, CTI settings, dialled number analysis, etc.

Configuration details of individual port types:

ANALOG FXS

To configure an analog subscriber, select:

Subscriber settings - basic information

- ***FXS port*** - indicates the port assigned from the installed FXS modules
- ***internal number*** - internal number assigned
- ***visible in contact book*** - permission to show the number in the WebCTI book and on CTS phones
- ***name*** - optional additional description of the number, e.g. family and given name of the user (visible in CLIP)
- ***e-mail address*** - additional information useful when using the FAX2MAIL and VOICE2MAIL services
- ***language*** - language version setting for WebCTI accounts and service messages
- ***enable error notifications*** - servicing notifications about occurring errors

Service and feature settings - assigning rights to use services

- ***set numeric password*** - for access to services that require entering a PIN

Service and feature settings - cost information

- ***enable displaying estimated call costs*** - AOC (call cost) service, available in CTS system phones and CTI applications

Service and feature settings - service permissions

- ***permission to use voice mail*** - right to use voice mail
- ***permit call waiting*** - permission for call waiting (up to 1) by the administrator, the service itself is activated/deactivated by the subscriber using a service code
- ***permit join as third, whispering*** - access to monitoring services
- ***permit presentation reserving service*** - right to use CLP presentation reserving in outgoing traffic

- **permit paging and intercom** - rights to use paging and intercom services. The services are available to subscribers by using a service code with specified acoustics direction (both ways or one way audio)
- **permit call forwarding** - right to perform call forwarding, divided into: none, all except outgoing (when the forwarded is the initiator), or all

Service and feature settings - service execution blocking

- **block call interception of this subscriber** - call interception blockade
- **block join as third, whispering and tapping** - monitoring service blockade
- **block paging and intercom for this subscriber** - paging and intercom service blockade for this number

Service and feature settings - call center

- **call center agent** - enable number function as component of CC queues
- **call center agent manager** - manager of a group of agents with the right to monitoring services (join as third, tapping, whispering, available using service codes)

CTI settings - setting details for using CTI functions for PhoneCTI/WebCTI/TAPI

- **access to CTI application** - setting for access level to CTI protocol (none, CTI user, CTI user plus, ConsoleCTI user)
- **password** - defines access password for the PhoneCTI/MessengerCTI and WebCTI applications
- **password change required on next login** - enforces password change on logging into the application next time
- **access to public contacts** - sets the level of access to editing public book contacts
- **access to records** - permission to access recorded calls
- **WebCTI administrator** - assigns WebCTI administrator rights
- **allow control over Slican TAPI** - permits communication using the TAPI protocol
- **text message support** - permits using text messages (PhoneCTI) by local SMS Centre or via eSSL server.
- **GSM port for message sending** - any or specified

MobilePhone - mobile number service configuration

Integration of fixed phone function with mobile phone (GSM or DECT). These services primarily include call distribution to the mobile phone concurrently or with a configurable delay with the "main" phone, and text notifications about answered and missed calls. This service is licensed.

MobilePhone numbers can be external and internal numbers, where:

- external numbers, e.g. mobile phones - the PBX executes traffic through metropolitan ports,
- internal numbers, e.g. wireless phones (DECT) - the PBX executes traffic through internal ports.

Permissions to use the MobilePhone service can be configured only by the PBX administrator, including call distribution delays. The service can be activated and deactivated both by the administrator and the PBX user, using a service code, from WebCTI or using the CTS system phone menu. When a call is answered on Mobilephone, the "main" phone will also be busy until the call is finished.

Additionally, it is possible to distribute calls to the Mobilephone service on unlogged-in virtual accounts and SIP subscribers, as well as in situations where the main number is unavailable or damaged.

Service configuration from ConfigWEB:

- **enable MobilePhone** - access to service menu: quick enable/disable
- **add number** - adding mobile numbers
- **allow use of call service** - permission for administrator to distribute calls concurrently to the main number and Mobilephone, the service itself is enabled/disabled by the subscriber with a service code
- **call delay** - sets delay (in seconds) relative to the main phone
- **text notification sending** - about answered/missed calls, can either be sent always or when the concurrent call option is enabled (GSM module required)

Mobilephone configuration from ConfigWEB:

Log in to the WebCTI panel. Go to section Settings->Services->Mobilephone and select the service operation mode:

- mobilephone - concurrent calls
- mobilephone - calls when not logged in (mainly for SIP terminals and virtual accounts)

Details on the MobilePhone service can be found [HERE](#)

Outgoing traffic settings - configuration of outgoing traffic rights

Outgoing traffic for individual ports is determined by outgoing traffic rules and prefix rights. General rights in outgoing traffic include:

- own settings: the administrator sets rights to prefixes and to outgoing rules
- permission to make outgoing and internal calls without restrictions
- complete outgoing block

If a subscriber does not have rights to dial the given number, they will be informed about the fact with an appropriate verbal message.

One rule for internal traffic is created by default. Further rules are created in: **Call routing->Outgoing and internal->Dialplan rules.**

Setting outgoing traffic rights

Outgoing traffic rights levels are set for each given number: own settings, allow making any calls (unrestricted), block outgoing traffic

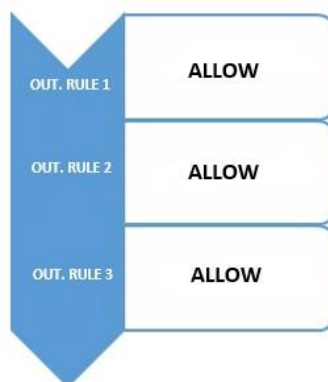
Subscriber rights to dialled number analysis rules

For each rule, you can define 3 levels of access for making outgoing calls:

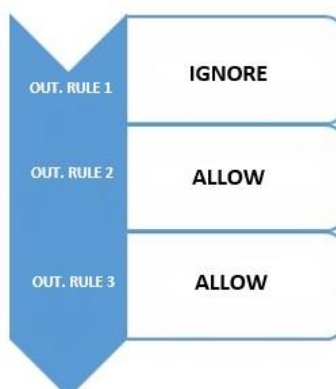
- **ignore** - skips the rule and searches for the next
- **allow** - allow outgoing traffic through this rule
- **block** - block outgoing traffic through this rule (does not check further rules)

The diagrams below show the level of subscriber rights to outgoing traffic through the available rules under the same match pattern:

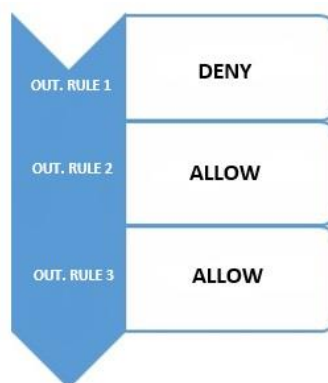
- a) rights level for outgoing traffic through each available rule: 1, 2, 3



- b) rights level for outgoing traffic through rules: 2 and 3, rule 1 is skipped



- c) no outgoing traffic by rule 1, others (2, 3) are allowed



Permissions to dialled number prefixes

Rights to prefixes allow you to further limit or broaden the ability to make outgoing calls based on the number dialled. Assign rights to subscribers with the following levels: block or allow.

By default, the following prefixes are created: emergency, national, Europe, World, Premium. Further prefixes are added in: **Call routing->Outgoing and internal->Dialled number->Permissions.**

Rights to calls using emergency prefixes also apply to outgoing traffic when the phone lock service is enabled.

Hotline

Configuration of the hotline service, i.e. a pre-set single number that will be dialled when the receiver is picked up after a pre-defined time to select the hotline passes (**Extensions->Subscribers->Settings** section). The hotline number can be an internal or a metropolitan number.

Internal number sets - adding numbers to sets

Ability to assign numbers to sets created in the system (a separate subset of internal numbers). By default, one set comprising all internal numbers is created in the PBX.

Fax - configuration of available fax gateways

- **fax2mail gateway:** support for fax directed to a number of forwarding to fax2mail service enabled - with T.30 and T.38 codec support
- **T30/T38 gateway:** support for incoming and outgoing fax, with T.30 codec conversion to T.38 and vice versa

Additionally, you can set error correction for the T.30 codec, and transmission speed range.

When using the fax2mail service for the given number, it is necessary to activate call forwarding to the fax2mail service (** by default).

Sample activation of the fax2mail service for forwarding all calls:

72101**

where:

*72 - forward all calls service code

*** - default forwarding to the fax2mail service

101 - internal number with the fax2mail service enabled

Others

Announcement settings

- **play calls waiting** - allows you to turn on or turn off the announcement of the waiting call information or another acoustic signal.

Caller presentation settings

- **present incoming calls with suspended as forwarded** - in incoming traffic for forwarded calls, present the suspended user instead of the user forwarding the call This is particularly important for analog phones, where CLIP presentation is sent in FSK only once.

Connection History

- **record direct missed calls** - signaling missed call history
- **record direct calls to busy** - signaling call history in case of busy

Notifications

- **record error notifications** - service notifications about errors that occur

CTS/CTS.IP SYSTEM PHONES

For system phones, basic settings (services, CTI, outgoing traffic, fax) are configured in a similar manner as for analog numbers (FXS). Additionally, the following can be configured for system phones:

CTI settings

- **access to operator console application (ConsoleCTI)** - allow console use

System phone settings

- phone settings: device type, ringtone type, ringtone volume, receiver speaker boost
- LCD settings: contrast, displayed name
- loudspeaker system settings: auto answer, auto dial, microphone mute
- headset settings: microphone boost, earphone speaker boost

Button settings

Configuration of programmable phone buttons, as well as attached consoles (and additional consoles).

The administrator can remotely select an action to bind it to the desired button. Some services can also be programmed directly from CTS phones.

Buttons can be assigned to

- Internal numbers
- external numbers
- 'call as' service
- VoIP operator status
- TDM port status (TDM operator monitoring, channels for BRI/E1)
- DND
- phone lock
- private contact book
- public contact book
- search
- earphones
- automatic call answering
- forwarding when - busy, not responding, unconditionally
- call to Mobilephone
- manual mode
- call storing

It is also possible to edit buttons sequentially by highlighting multiple configured numbers and selecting the **Sequential edit** button. For linked consoles, remember to select CTS phones of the same type (e.g. CTS-330 + CTS-338 console). Additionally, it is possible to print button labels in WebCTI (download the pdf file). 200 CTSs can be linked with: for CTS-2xx - 5 consoles, for CTS-3xx - 4 consoles. Additional power supply in CTS-2xx is required for two and more consoles, CTS-3xx from 1 console. If buffer power supply is used, select a battery of appropriate size, calculating the power balance for phone and console.

System phones can also display information on some enabled features/services:

- ✓ information on enabled voice mail (e.g. the letter **V** for CTS-220)
- ✓ information on the number of calls waiting in queue
- ✓ information on logging into a queue – “logged in” inscription
- ✓ information on enabled forwarding (e.g. the letter **F** for CTS-220)

CTS.IP - configuration

For CTS.IP, for the purpose of authentication, enter or select from the list the MAC address of the device awaiting configuration in the **Subscriber settings** tab. The MAC address of each system phone can be

found on the rating sticker placed on the body, or in the phone menu (**Menu/VoIP/Status**). Only phones whose addresses are entered in the **MAC** field of the field in question, will be able to work with the PBX.

Edit system extension properties

Extension number: 1006

Name: CTS.IP 1006

Subscriber settings | System phone settings | Services and features settings | Buttons settings | CTI settings | MobilePhone settings | Outgoing settings | Sets of extensions | Fax settings

Enabled: ☒

Visible in phonebook: ☒

Device MAC address: b0:b3:2b:00:06:51

E-mail address:

Language: Polish

Notifications

Generate error notifications: ☐

SIP SUBSCRIBER

For SIP subscribers, we can add numbers individually or sequentially.

Configuring a single SIP subscriber requires:

Setting up the subscriber - basic data for SIP configuration

- **enabled** - enable/disable the subscriber in the service (results in them being logged in/out of the PBX)
- **internal number** - internal number assigned
- **name** - optional additional user comment (shown in CLIP)
- **e-mail address** - additional information about the subscriber, useful when using fax2mail or CTI account notifications
- **login** - required for authentication when logging in a VoIP subscriber in the PBX
- **password** - required for authentication when logging in a VoIP subscriber in the PBX
- **generate password** - high-complexity password from a generator (recommended), will be visible to the administrator only for secure https connections

Advanced settings - detailed SIP settings

- **language** - language version setting for WebCTI, PhoneCTI, and announcements in the PBX
- **DTMF mode** - DTMF method of tone transmission (identification of digits sent during calls)
 - RTP ([RFC 2833](#)) (out-band)
 - SIP INFO (out-band)
 - in-band
- **caller presentation transmission method** - specify the source of presentation of the number of the incoming call. Depending on the terminal, the caller's presentation information can be sent in: RPID, PAI or FROM header.
- **only secure calls** - encrypted calls: signalling based on TLS (SIPS) and RTP (SRTP) voice sample transmission
- **subscriber is always registered** - unregistered subscriber will be treated as damaged and will be included in notifications for administrators about damaged ports
- **call limit** - configure the limit of concurrent calls (for forwarded calls, at least 2)
- **send only number without name** - caller presentation will only contain the number without comments (for phones with small displays)

- **audio codecs** - select the appropriate codes for processing acoustics. Remember to select the same codecs in the VoIP phone or softphone application settings. List of codecs supported by the PBX:
 - G.711(alaw)
 - G.711(ulaw)
 - G.722
 - G.729 (**ADDITIONAL LICENCE REQUIRED**)
 - GPRS
 - signed Linear PCM(16 bit)
 - ADPCM
 - SpeeX
- **video codecs** - select the appropriate codes for processing video calls. List of codecs supported by the PBX:
 - H.263+
 - H.263
 - H 264

IP filter - protection against unauthorised login

To provide additional protection against unauthorised attempts to access SIP subscriber accounts, you can configure an additional filter focused on a specific IP address (host) or network address (network address and mask). A tool useful when logging in SIP subscribers from outside the internal network. If the network from which the subscriber is going to login is not specified precisely, IP filtering can be disabled and a sufficiently strong password for authentication during login can be set up. By default, the filter only allows logging in from the local network.

Service and feature settings

Similar as for FXS subscribers.

CTI settings

Similar as for FXS subscribers.

An additional feature for SIP phones is access to the contact book using **LDPA (Lightweight Directory Access Protocol)**. This protocol is intended for using cataloguing services, which can be databases of information representing the network's users and resources, which aids in managing relations between them. A prerequisite for handling access to the book using LDAP is to assign CTI rights to the internal number in question (access level and password). The configuration of SIP terminals that support contact book downloading using LDPA is producer-specific. In this case, read the programming manual for the specific terminal. Details of LDAP service configuration for Slican VPS phones can be found [HERE](#).

NOTE

Access to LDAP requires purchasing an additional licence for VoIP subscribers.

Mobilephone

Similar as for FXS subscribers.

Outgoing traffic

Similar as for FXS subscribers.

internal number sets

Similar as for FXS subscribers.

Fax

Fax connection support configuration

- fax2mail gateway: support for fax directed to a number of forwarding to fax2mail service enabled - with T.30 and T.38 codec support
- T30/T38 gateway: support for incoming and outgoing fax, with T.30 codec conversion to T.38 and vice versa

Provisioning

To enable the automatic configuration function. Select the relevant phone model from the drop-down list. Search for the relevant MAC address in the list of devices awaiting configuration. For manual configuration, additional information provides the path to the provisioning server and a link for configuring advanced functions. For sequential adding, enter the initial number and amount of numbers to be created. Each line of the login and password fields concerns a consecutive SIP number.

MessengerCTI – number to support the application

Subscriber's account to handle the MessengerCTI application in the Desktop and / or Mobile version In the case of the Desktop option, you can use the VoIP mode (without an additional physical phone) using a headset with a microphone. All other functions are configured in the same way as for other equipment.

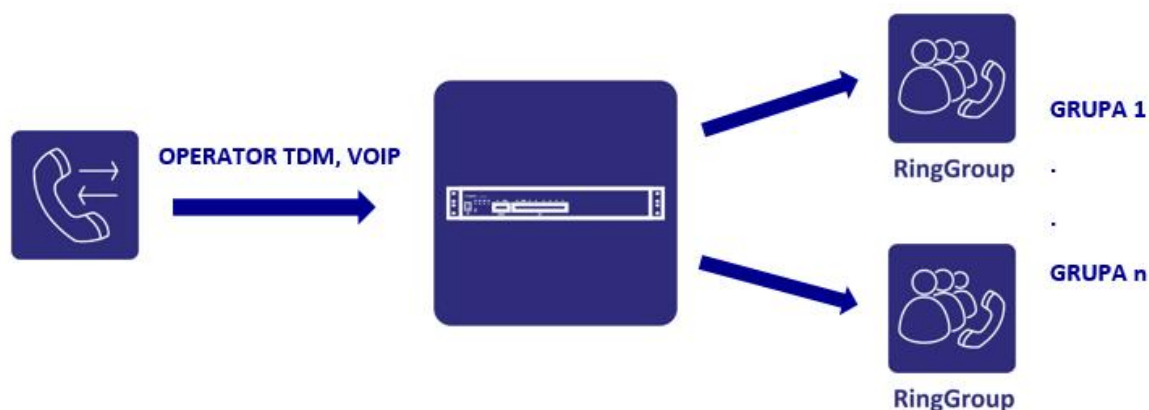
ACCOUNT - Virtual number

For virtual accounts, we can add numbers individually or sequentially. Individual data is configured in a similar way as for FXS subscribers. Register the account on the phone using a service code (see: Internal numbers->Service codes).

7.3. Call distribution groups

Group-based PBX functionality involves such redirecting of incoming traffic that it is possible to handle multiple callers directed to the same internal number at the same time. Calls to the group are handled by selected internal numbers configured as group components.

Below, a diagram of the group's functioning:



The maximum number of group components is **12**, with the maximum number of calls on hold in a group being **5**. The system supports up to **80** groups. Individual group components are added permanently with call distribution delay set in seconds. Remember that for the group to function correctly, you need to obtain connection with the PBX, i.e. set the on hold music as the call signal or use an incoming traffic rule with DISA announcement enabled. This is due to the maximum call time on metropolitan lines (most commonly 1 minute).

Call distribution group configuration comprises:

General settings

- **internal number** - set the group number
- **name** - group name

Group components

- **add internal number** - add a number from the internal number list (up to 12)
- **call assignment delay in seconds** - set the assignment interval between individual components
- **skip when busy** - skips calling the subscriber when he is busy

Caller handling

- **playback to persons calling the group** - select the playback signal: on hold music or call signal (default music)

Call distribution group - advanced settings

- **maximum queue wait time** - set the queue wait time (in minutes)
- **announcement after maximum time exceeded** - playback of an announcement when maximum wait time is exceeded, from tones available in the system or your own
- **group capacity** - maximum number of calls waiting (up to 5)
- **all subscribers busy** – you can to select the waiting mode in the group. When all components are busy, you can choose whether the callers receive a busy signal or wait for the group component to be released.

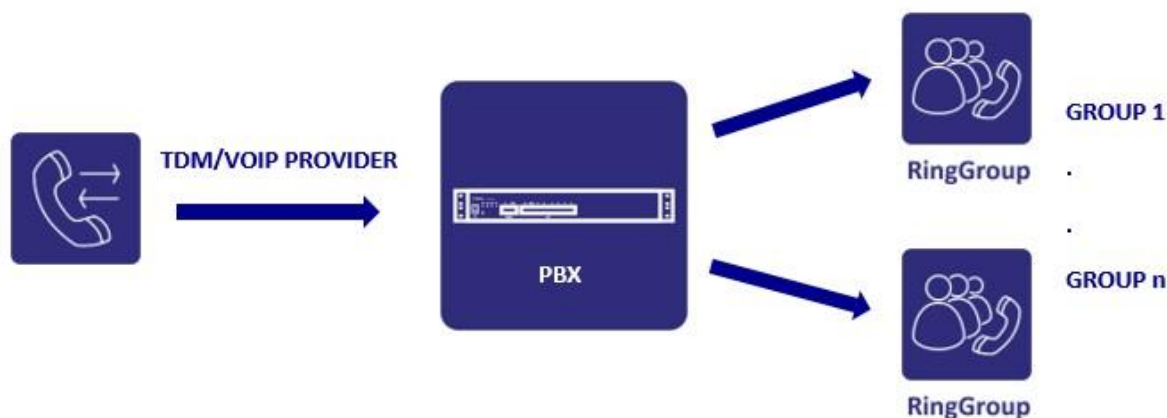
7.4. IVR

IVR (*Interactive Voice Response*) is the name of a system in telecommunications that enables interactive handling of a calling person. IVR therefore has the functionality of an automatic call center (or part thereof), where a complex menu can be used to determine interactions with your callers. IVR enables automatic selecting of:

- type of desired information or service
- service language - for example, Polish or English
- user identity verification by entering their number, PIN, password, or speaker recognition
- access to selected information from a database

IVR systems are most commonly used to handle large numbers of phone calls from customers, and thus reduce the costs or improve customer service. Typical uses of IVR applications are telephone banking, telemarketing, card handling systems. IVR is also frequently used to extend service time in companies to 24/7. The use of IVER systems enables improving customer service and reducing costs of this service, as customer inquiries can be answered without involving human work time, or forward the call directly to a team having the necessary competences. If the customer does not receive an answer to their question, or

they need a more detailed answer, their call can be forwarded to another agent. The NCP PBX is equipped with IVR mechanisms enabling a very broad scope of traffic handling scenarios, depending on the customer's individual needs. After a preliminary announcement, calls can be directed to: CC queue, group, internal number, fax2mail service, voice mail or another IVR menu.



IVR configuration details

Begin IVR configuration with creating an *IVR menu*. Next, add individual *Actions* and their corresponding *Digits*. In the **IVR events** sub-menu, define the method of handling traffic in the event of different behaviour of the caller, e.g. incorrect selection of digits. **Call events**, on the other hand, determine the handling of numbers dialled from IVR, e.g. calls to busy numbers or when calls are not answered.

The IVR menu is composed of a convenient *IVR tree*, which provides direct access to editing individual actions, digits and events. Handling of calls directed to IVR may or may not be related to an internal number. In such cases, enter the IVR menu name and direct incoming traffic to it.

General settings

Creating an internal number or name for handling traffic to IVR:

- **internal number (not required)** - set the number or, optionally, only name
- **name** - set the IVR menu name
- **description** - detailed description of the menu

IVR events - handling of IVR menu events if the caller behaves in a different way, including:

incorrect selection of digit or number

1. **play announcement** - play the appropriate announcement to the caller
2. **announcement language** - select the announcement language
3. **announcement** - select a system announcement or one you have recorded yourself
4. **go to** - select another menu from the list, specify an internal number or disconnect

waiting time for digit or number selection

1. **if the caller does not select a digit or number within** - waiting time for selecting a digit or number
2. **play announcement** - play the appropriate announcement to the caller
3. **announcement language** - select the announcement language
4. **go to** - select another menu from the list, specify an internal number or disconnect

re-selection of digit or number

1. **number of repetitions** - when the caller selects an incorrect option or waiting time passes multiple times
2. **after all repetitions, go to** - select another menu from the list, specify an internal number or disconnect

Call events - handling calls handled from the IVR menu

calls to busy

1. **play announcement** - play the appropriate announcement to the caller
2. **announcement language** - select the announcement language
3. **announcement** - select a system announcement or one you have recorded yourself
4. **go to** - select another IVR menu from the list, specify an internal number or disconnect

calls not answered

1. **if the call is not answered within** - set the waiting time in seconds
2. **play announcement** - play the appropriate announcement to the caller
3. **announcement language** - select the announcement language
4. **announcement** - select a system announcement or one you have recorded yourself
5. **go to** - select another IVR menu from the list, specify an internal number or disconnect

IVR menu - Actions

A menu for configuring actions that the PBX is to take when traffic is directed to the IVR menu. These include: dial internal number, play announcement, wait, disconnect.

Action type - action selection

- **play announcement**
 - **language** - select the announcement language
 - **announcement** - select the announcement: user, system
 - **announcement content** - content of a system announcement
 - **announcement can be interrupted** - ability to select a number during announcement playback
- **wait (silence)**
 - **waiting time in seconds** - time in seconds until next action
 - **waiting can be interrupted** - ability to select a number during silence
- **play busy signal**
 - **signal playback time in seconds** - duration of busy signal playback
- **disconnect** - disconnect the call
- **dial internal number**
 - **internal number** - select an internal number from the list
- **dial number**
 - **number** - select an external number
 - **outgoing traffic** - forwarding in accordance with outgoing traffic rules, remember that individual actions of the same IVR menu share the same outgoing traffic rights
- **forward to voice mail**
 - **internal number voice mail** - select the number to whose voice mail the action will be directed
 - **announcement language** - select the language version of the voice mail message

- **forward to fax2mail**
 - **e-mail address** - e-mail address to which the fax message is to be sent as an attachment
 - **message number** - select the language version of the e-mail message
- **go to IVR menu**
 - **go to IVR menu** - select from the list of defined IVR menus
- **depending on time**
 - **if current time is within range** - select a time range, e.g. holidays, weekend
 - **go to** - select another menu from the list, specify an internal number or disconnect
- **depending on manual operation mode**
 - **if manual operation mode is enabled** - traffic handling in accordance with the selected operating mode
 - **go to** - select another menu from the list, specify an internal number or disconnect

IVR menu - digits (options)

A menu for configuring selection digits by directing the call to:

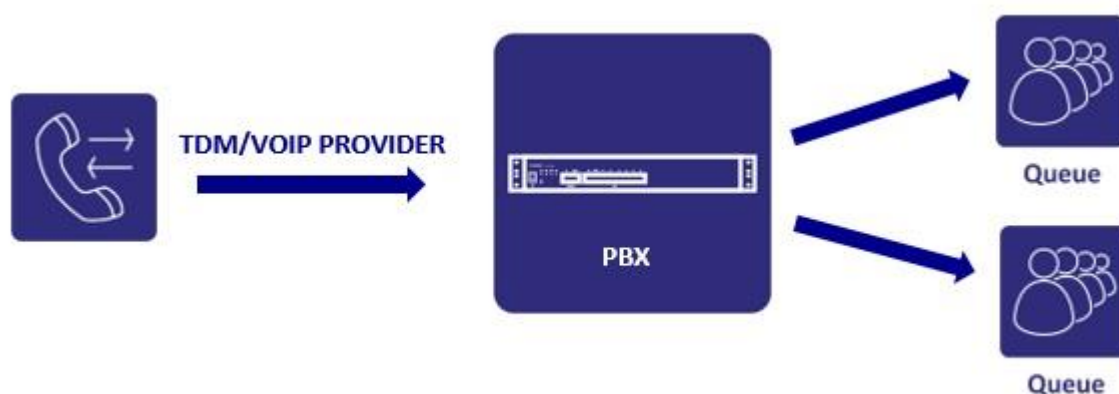
- **digit** - digit range [0-9] or the # or * characters
- **go to** - select another IVR menu from the list or specify an internal number

IVR reports

While working, statistics of calls going through IVR helplines are collected. They are available in the tab Diagnostics-> Statistics-> IVR report

7.5. Call center queues

A call center queue is the equivalent of the “group” feature with expanded functionality, providing the ability to handle more incoming traffic rules handled under one number by a specific number of logged in agents. Compared to a call distribution group, it provides greater ability to configure call distribution strategy of components assigned to it. Additionally, queue agents can be logged into the given queue permanently or log in using an appropriate service code. The PBX administrator can also enable announcement playback for the queue: about position in queue and waiting time. Additionally, you can create an agent manager, giving the manager the ability to use monitoring functions (join as third, whispering or tapping). Queue event handling includes: maximum waiting time (set in minutes and seconds), alternative traffic forwarding if no agents are logged in, queue capacity and queue exit digit. The administrator is able to set queue priority, then if an agent is logged into multiple queues, the first to call will be the queue with the highest priority. Traffic directed to the queues can be analysed thanks to the statistics collected, available in the *Diagnostics* section.



A queue components can only be an internal number with the following feature enabled: **Call center agent**(*Subscribers->Service settings*). This option is subject to licensing.

Queue configuration details:

General settings

- **internal number** - specify the internal number to which call handling traffic will be directed
- **name** - queue name

Queue components

Queue components can be internal numbers with the following feature enabled: **Call center agent**, as well as number sets (provided that queue components are Call center agents). A component can be logged into the queue permanently or log into it using the “Login agent” service, which means that an agent that is not logged in will not be assigned calls.

- **add internal number** - add agents
- **add set** - add created sets (components must be call center agents)
- **calling strategy** - specify in what way traffic in the queue is to be handled: whether assigned numbers shall call all at once, cyclically, at random, in sequence, or should the calls be distributed (call distribution group)
- **component calling time in seconds** - specify how long a given component is to be called, after this time passes, the component stops being called for the time specified below
- **number of seconds before calling components again** - downtime before calling components again (only for All At Once and Call Distribution Group strategies) after it has been called for the time specified above
- **interval before calling a component again after a completed call in seconds** - i.e. so called component downtime, before it is included in traffic handling again
- **queue priority** - queue importance configuration if the same agent is a component of multiple queues: calls directed to the agent will be sorted according to queue priority
- **play announcement after receiver is picked** - set announcement for when call is answered
- **reception of calls to busy** - if a queue component is busy, should it be notified about another incoming call (only applies to SIP phones)

- **enable concurrent calling of parallel phones Mobilephone, MessengerCTI.Mobile**- feature that enables calling parallel numbers, e.g. mobile agents as a Mobilephone service or via the MessengerCTI application
- **enable automatic collection of missed call numbers for call back** - the system will remember missed calls in the queue and they will be available on agents' system phones
- **do not include numbers from missed calls with a waiting time shorter than** – set the time in seconds after which the calls will be saved as missed calls back
- **enable collection also when the queue is closed** - it collects call back numbers while the queue is closed
- **delete all non-called numbers everyday at** - setting the time to delete stored non-called numbers of missed calls
- **sending text notifications about missed calls** - indicate the number to which text messages about missed calls redirected to queue will be sent Remember about configuring text notifications correctly on the given number. Notifications about answered calls will be sent to Mobilephones that answered them.

Caller handling

- **enable playback of the welcome announcement** - we can have an individual welcome announcement for a given queue, regardless of DISA
- **playback for waiting in queue** - signal played in the speakers of waiting people: music on hold (MoH) or calling signal
- **music on hold collection** - default or uploaded to the PBX by the administrator in the section: **Media->Music on hold**
- **enable announcement playback** - enables or disables playback of the announcement in the queue
- **announcement playback frequency** - sets the length of time between announcements
- **play queue position announcement** - play information about position in queue
- **play an announcement about a position in the queue no more than** - when there is more than the given parameter, the announcement for those waiting will not be played
- Replace the played announcement about the position in the queue - announcements about the position in the queue can be replaced by substituting the changed values
- **play estimated waiting time announcement** - play information about approximate time of waiting in queue
- call the agents while playing cyclical announcements - in this case, when the agent picks up, the announcement will be interrupted
- enable playing of informational announcements - during the waiting time, additional informational or advertising announcements can be played
- frequency of playing informational announcements - the number of seconds between the above announcements
- call agents during information announcements - the announcement will be interrupted when the agent answers the calls

Additionally, you can manage queue announcements

- **language** - select the language version of the announcements played

- **first in queue** - set information announcement
- **position in queue** - set announcement with information about queue position
- **waiting time** - set announcement with information about waiting time
- **thank you**

Queue events - forwarding calls in a queue

In this section, specify the details of managing traffic directed to the queue

- **maximum caller wait time in queue** - in minutes or seconds, if the field is empty, people on hold will remain in the queue without time limits
- **no components in queue** - if there are no agents logged into the queue, forward all incoming calls to an internal number, function, or wait for agent login
- **all components busy** - if all agents are busy, forward the call to an internal number, function, or wait for agent login
- **maximum number of missed calls in a queue** - specify queue capacity
- **guaranteed number of pending** - determines the guaranteed number of pending connections in a given queue when we anticipate more than one queue in the system, distributing traffic and waiting under the purchased license for the number of pending
- **queue capacity exceeded** - forward all incoming calls to an internal number if queue capacity is exceeded
- **closed queue** - determining the time range of the queue operation based on the configured time ranges with the option of playing an informative announcement and diverting the call to an extension or disconnection
- **allow callers on hold to select digit** - specify the queue exit digit [0-9] and # *
- **forward caller to internal number** - specify an internal number for handling calls after exiting the queue

7.5.1 How to configure the CallCenterMAN application

Slican Call Center is the integrated functionality of the exchange, which includes the CallCenterMAN application for managing and controlling the work of agents in Call Center Queues. The most important features of the application include:

- statistics on the total number of connections with clients in a given time unit (hour, day, week, month), segregated into phone contacts (incoming and outgoing calls), redirected through the queue
- statistics on the total number of unsuccessful calls in a given time unit (calls dropped, calls lost)
- statistics on the total number of connections with clients in a specified unit of time completed successfully in the first contact
- call back numbers abandoned and lost
- agent's working time and events,
- report distribution schedules (daily, weekly, monthly)
- generating graphs of average waiting times, incoming queue connections as well as connections with exceeded SLA time (Service Level Agreement)

- detailed view of agent connection logs and events, and queue connections
- agent's task list - call back numbers with call log
- listening to agent recordings
- joining an agent's conversation or wiretapping
- online observation of queue work

CONFIGURATION DETAILS

Configuration of administrator access accounts with rights to manage the call center system belongs to the PBX administrator from the ConfigWEB level.

The order of configuring the call center system is as follows:

in the Accounts / Administrator accounts menu:

- add administrator account: login, password
- grant access rights to the CallCenterMAN application
- assign agents to the account: all agents, sets of agents, agents not assigned to sets
- assign queues to the account: all or selected
- optionally give authorization to supervise agent connections: listening in, entering the third, whispering along with the internal number of the manager
- optionally allow listening to agent call recordings

in the menu Internal numbers / Subscribers / Services and functions / Call center:

- grant management rights - indicate the account of the appointed administrator (option for monitoring connections: listening in, entering third, whisper)

in the Internal numbers / Service codes menu:

- assign the extension number of the service activation code break (agent break)
- assign the extension number of the deactivation service of the break (agent return)

in the menu Internal numbers / Subscribers / Buttons for CTS subscriber:

- assign a button as an action - call back

in the menu Internal numbers / Call center queue / Inactive queue

- set the parameters of the queue's unavailability (time ranges in which it is out of service)

The service break code should be set when agents work exclusively on SIP or FXS equipment. Agents equipped with CTS system telephones can assign a button as a break service.

Particular attention should be paid to the correct selection of managed queues and agents assigned or not to individual queues. This is due to the correct display of statistics reports for individual agents and queues. After creating an administrator account, the administrator receives email credentials for logging in to the CallCenterMAN application. The application is available from a web browser under the same IP address as the PBX with "cc" suffix.

Sample application access address:

<http://192.168.0.254/cc>

After logging in correctly, the system will ask you to modify the password for the account.

The number of accounts with permission to manage the Call Center is not limited. The license limit applies only to the number of agents purchased, to whom we can increase the rights by including management functions of connection monitoring.

Details of the configuration of individual functions, i.e. break codes, reports, schedules available in the Application Help menu.

7.6. Service codes

Service codes in the system can be freely modified, giving the ability to specify the numbers (codes) assigned to individual services. A default list of services is available in the PBX. In the event of a mistake when calling a service, the PBX will notify you about the fact and will not allow the service to be called. A full list of services, with a description of their functions, is available on Servnet as a downloadable pdf file – “NCP services” .

7.7. Other extensions

7.7.1. Voice mail

The NCP system provides a comprehensive voice mail service. An intuitive menu enables free navigation by selecting the relevant options and managing messages in the inbox.

The voice mail service is available for any internal number, provided the administrator enables its use and the appropriate licence is purchased.

Voice mail is activated by enabling incoming call forwarding if the following occur:

- busy
- no answer
- unconditionally (all)

Voice mail parameters

- maximum number of messages in one inbox = 10
- maximum message duration = 3 min
- minimum message duration = 3 sec

Information about the voice mail number is located in the tab: **Internal numbers->Other**.

Additional voice mail global settings can be found in the tab **Internal numbers->Settings**.

This tab contains additional forwarding options in the event the inbox is full, and inbox skipping.

Default voice mail forwarding service code:

* internal number of the inbox owner


Methods of enabling call forwarding to voice mail by the user:

- using the phone, by selecting the appropriate forwarding type (below, an example for forwarding all calls, where call is *72 and cancel is *73):

Call      internal number of the inbox owner

Cancel:    

- from the WebCTI application, activate forwarding in the Settings->Forwarding->Type tab (below, an example for forwarding all calls):

 **SLICAN** My subscriber account

1004. 1004

MobilePhone	
MobilePhone number:	Not defined
Forward all calls	
Servis activated:	<input checked="" type="checkbox"/>
Number:	*1020
Forward if phone is busy	
Servis activated:	<input type="checkbox"/>
Forward if call not answered	
Servis activated:	<input type="checkbox"/>
Do not disturb (DND)	
Servis activated:	<input type="checkbox"/>
I am there	
Servis activated:	<input type="checkbox"/>

OK Cancel

Access to voice mail message playback is available by dialling the voice mail number (1000 by default) from your internal number. Users navigate the voice mail MENU by selecting the appropriate options. Among others, the menu allows saving, deleting, forwarding and repeating the recorded messages.

Additionally, SIP phones provide notification about messages left with a visual signal, highlighting the MESSAGE button (envelope). CTS system phones indicate it visually on the LCD.

Configuration details:

- **internal number** - specify the internal number for the voice mail
- **do not require password when caller calls from their internal number** - otherwise, a password (PIN) is required, defined in the *Subscribers->Numeric password* section

7.7.2. Speaking clock service

- **internal number** - specify the internal number for the speaking clock service

7.7.3. Echo test

- **internal number** - specify the internal number for the speaking echo level testing function

7.7.4. Play music

Music playback on hold function. By default, the standard music implemented in the PBX is played. You can create your own collection in the Tools->Music on hold section.

- **internal number** - specify the internal number
- **music collection** - select from among collections available in the PBX

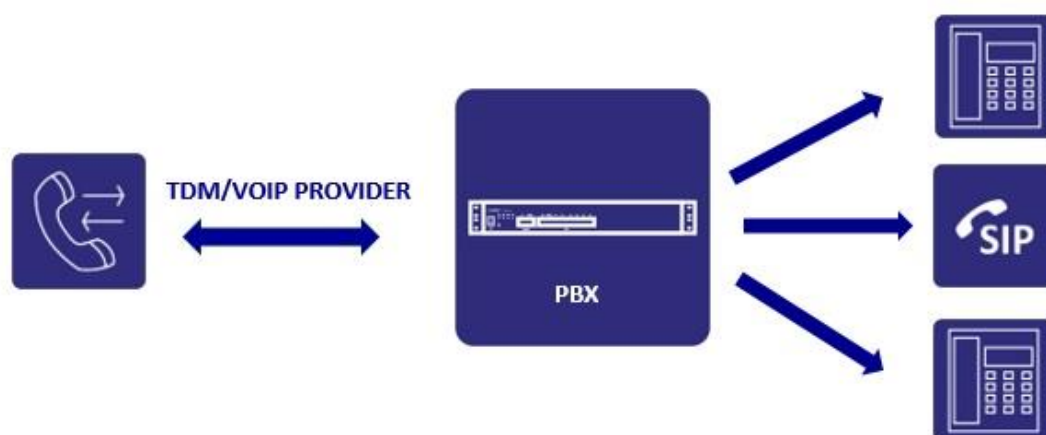
7.7.5. My internal number

- **internal number** - specify the internal number for the function of checking the user's own internal number with a voice message

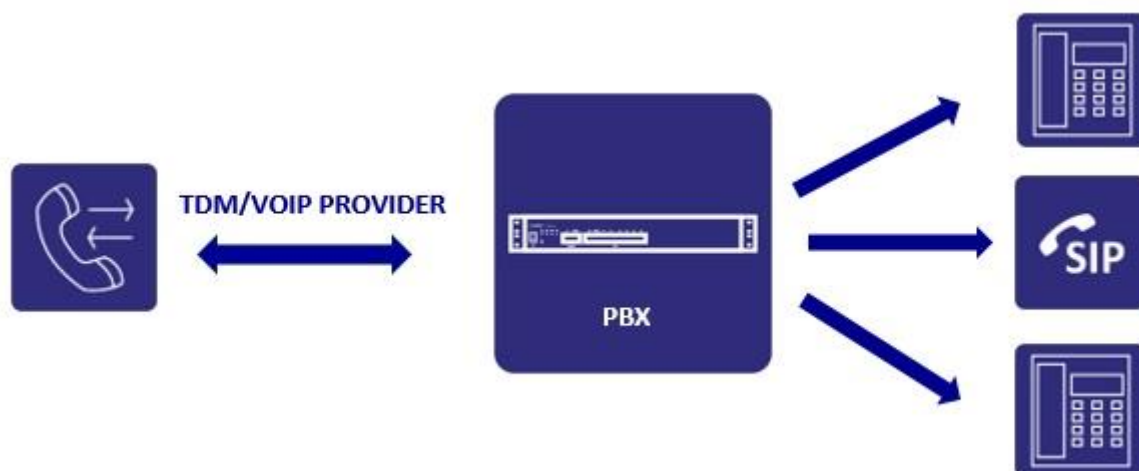
7.7.6. Conference calls

Conference bridges can be created in two ways:

- **CONFERENCE ROOM** - a conference call between participants who call a specific number, which can be any internal or metropolitan subscriber. This solution only requires configuring the number which all conference participants can call. Additionally, you can define a PIN that will authorise conference participants.



- **CONFERENCE GROUP** - calling defined components (regular participants) by the initiator, which can be any internal or participant subscriber (conference PIN must be entered) A solution for subscribers who hold regular conferences with fixed participants.



Both the room and the group must have at least one Conference Administrator defined. Conference Administrators can add, remove and mute participants. They can also lock the conference to prevent further subscribers from logging in. The full administrator menu is available via the asterisk button (e.g. adding metropolitan numbers). Administrators also do not have to enter PIN codes.

Configuration details

General settings

- **internal number** - specify a unique internal number for the conference room
- **name** - conference room ID
- **conference room PIN code** - specify the authorisation PIN for conference calls
- **default announcement language** - select the language version of the announcements played
- **music on hold collection** - default or uploaded to the PBX by the administrator in the section: *Media->Music on hold*
- **play music while waiting for participants with microphone active** - music will be played when one person is waiting for other conference participants
- **play announcements on participant join/leave** - indicate whether announcement should be played when a participants joins or leaves the conference
- **announcement type** - announcement or announcement and participant name
- **conference participant can select # to be forwarded to internal number** - after selecting #, participants can be forwarded to the selected internal number
- **maximum call duration** - maximum conference duration in minutes (default: 120 minutes)

Conference administrators

Conference administrators can add, remove and mute participants using the asterisk (*) button menu .

- **add internal number** - specify the conference supervisor
- **add sets** - add sets

Administrator settings

- **only conference administrators have microphone active** - other participants can only listen
- **before administrator joins, conference users have microphones off** - only when the administrator logs in, microphones of the other conference participants activate
- **end conference when last administrator leaves** - when the last conference administrator leaves, the conference is ended
- **administrators have access to the conference menu** - we define whether the administrator can have access to the conference menu

Regular conference participants

Regular participants are always added without the need to enter the PIN. Subscribers who are not regular participants can log into the conference by dialling its internal number and entering the PIN. Maximum number of conference components: **60**.

- **add internal number** (adding metropolitan numbers only possible from the administrator menu)
- **add sets** - add defined sets

- **maximum duration of calling regular participants** - specify the time (in seconds) of calling regular participants when setting up conferences

Outgoing traffic

Administrators can add external (metropolitan) numbers as conference participants by selecting numbers consistent with the allowed outgoing traffic rules and prefix rights.

Conference administrator menu

DIGIT	ADMINISTRATOR OPTIONS
1	enable/disable own microphone
2	lock/unlock conference
3	remove last conference member
4	reduce conference volume
5	expand conference
6	increase conference volume
7	reduce own volume
8	leave conference
9	increase own volume

7.7.7. Fax2mail gateways

Configuration of gateways for handling fax messages sent to the recipient as files attached to e-mails. The gateway supports T.30 and T.38 codecs.

When configuring the gateway, specify:

- **internal number** - not obligatory
- **e-mail address** - address to which messages are to be sent
- **service language** - select the service language
- **gateway settings** - error correction for T.30, min/max transmission speed

7.7.8. Web.IVR

Configuration of the number handling the Web.IVR feature, for handling call control in the PBX using an external server (more details in chapter 3.11.2).

Specify in the configuration:

- **internal number** - value not obligatory
- **server URL address** - address of the external server from and to which commands for the PBX will be sent
- **maximum amount of concurrent queries** - number of open sessions (channels) in accordance with the licence purchased
- **waiting time for server response** - specify the maximum time (in seconds) of waiting for server response when handling events

- **exceeded response time or maximum number of queries** - if the above conditions have been exceeded, then the following actions are possible: end call or redirect to an internal number

Number dial commands from the server require assigning appropriate outgoing traffic rights both to prefixes and dialled number analysis rule.

7.7.9. Paging

Configuration of so called paging group. If the group is called, all destination devices automatically have increased acoustics (in system and SIP phones) and a warning signal is generated (at the beginning and end). After the signal, the call initiator is able to convey the information. The feature can be utilised, for example, in notification and warning systems.

Paging group configuration comprises:

- **internal number** - group number
- **music on hold collection** - the music collection played until the paged numbers answer the call
- **maximum waiting time for call answer** - amount of time to answer the call by the called number
- **announcement configuration** - language and announcements at the start and end
- **subscribers (numbers called)** - add group components or sets

7.7.10. Lines

A **line**-type internal number can be used as a convenient tool enabling consultants to more easily handle mass telephone traffic. The service enables monitoring, organising and handling incoming calls in the PBX. It provides the ability to manage traffic in a manner similar to operator console, which has multiple metropolitan telephone lines connected. With its flexibility, it is possible to use it both in large institutions, e.g. offices, banks, hospitals or control centres, and for running small consulting points. The line is operated using the dedicated application **ConsoleCTI**. It is an integrated computer and telephone system, installed on the computer used by subscriber of the PBX internal number. It provides a visual representation of incoming traffic directed to the line. It enables handling calls directing from the application, instead of buttons and phone keypads. All displayed statuses readable and intuitive - with a large amount of additional information, configurable contact list, call history, internal dialler and phone book.

ConsoleCTI works **only with CTS equipment**. Configured lines are added to the application's PBX. Each incoming call directed to the line can be answered from the application and executed in the telephone system.

Configuration details:

- **internal number** - specify the line number
- **password** - authorisation password in ConsoleCTI (CTI password of the subscriber associated with the application)
- **maximum number of waiting calls** - number of channels available for operating the line
- **maximum call wait time** - specify the maximum time of waiting for call with a consultant
- **playback to waiting** - type of music on hold played to people calling the line

7.8. Sets

This feature is used to logically group internal numbers, e.g. departments in a company, queue handling. By default, a set of all internal numbers is created.

Set configuration

- **name** - group ID
- **description** - detailed description of the group, e.g. Builders room 101
- **set components can intercept calls between one another** - using the call intercept service
- **add internal number** - add internal numbers from the list as set components

7.9. Provisioning

Provisioning (self-configuration) in telecommunications means a process of preparation and fitting of a network in order to enable it to provide services for users. Most VoIP phone models available on the market have the manual and automatic self-configuration ability. During initialisation, telephones connected to a network send special frames in search of a provisioning server to obtain the data necessary for self-configuration.

As part of self-provisioning, IP phones obtain, for example, the following from the NCP PBX:

- login, password and server address for automatic logging in of the device
- defined lamps and function buttons for devices with the BLF (Busy Lamp Field) feature
- phone book (up to 1000 contacts)
- time zone settings
- NTP server address
- time format
- language version

Provisioning configuration

- **plug&play server** - enables sharing server address provisioning
- **remember unknown devices looking for server** - remembers and makes available on the list for mac authorization the addresses of devices looking for server
- **use secure HTTPS connection** - enables or disables encrypted phone connections

The PBX supports the following provisioning types:

- **automatic** - with the use of the SIP multicast process (plug&play server enabled)

In order to initiate the provisioning process:

- **in server configuration**: in the *Internal numbers->Provisioning* tab, enable the *Plug&play server* option and tick the *Remember unknown devices searching for provisioning server* option, so the PBX saves all MAC addresses of devices searching for the provisioning server. In the tabs of individual phones, you can download/upload or edit the default provisioning file when defining settings other than default. Setting editing in the provisioning file involves changing the appropriate parameters. Depending on the phone model, the meaning and value of each parameter is described in detail.
- in the **SIP number configuration**: in the *Internal numbers->Provisioning subscribers* tab, enable the provisioning option. Next, select phone model and type, and in the *Device MAC*

address field, enter the hardware address of the phone or select the appropriate one from the list, based on the devices that have connected to the PBX. Phones with the sip.mcast.net feature implemented and plug&play server enabled will automatically download configuration settings from the NCP PBX.

- **manual** - by entering the server access path in the SIP phone settings

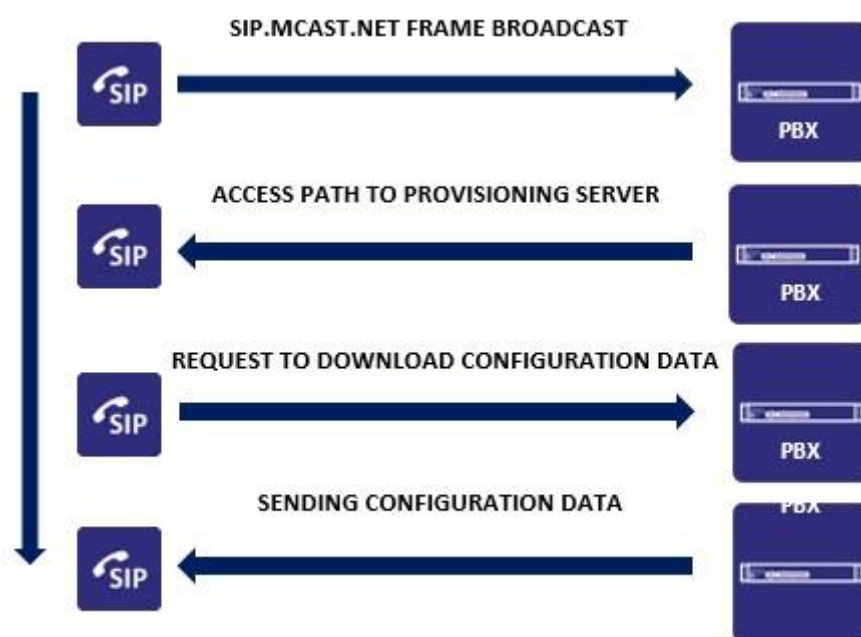
In order to initiate the provisioning process:

- **in the SIP number configuration:** in the *Internal numbers->Provisioning subscribers* tab, enable the provisioning option. Next, select phone model and type, and in the *Device MAC address* field, enter the hardware address of the phone. Below is the access path (e.g. <https://192.168.189.1/vsx/phoneprov/>) to the provisioning server that needs to be entered in the phone menu.

Due to a lack of a unified self-provisioning standard, the list of phone models supported is limited to the following:

- Slican VPS8xx
- Yealink T2x, T3x and VP530, W5xP

Below, the self-provisioning process with plug&play server enabled (sip.mcast.net method):



NOTE

Access to self-provisioning requires purchasing an additional licence for VoIP subscribers.

7.10. Devices

Internal numbers also include periphery devices.

These include:

- DPH.IP intercoms - a family of intercoms connected via Ethernet
- MAB(Multi Audio Box) - audio devices
- AUD.IP - digital speakers connected via Ethernet
- cameras - video transmission devices

7.10.1. MAB

MAB - an acronym for **Multi Audio Box**, is a device intended to ensure that a telephone PBX works with external sound sources or sound systems. Each device of this type takes up one analog equipment slot. A typical example of the use of audio devices is connecting to an external sound system (e.g. broadcast system). A typical example of the use of audio devices is connection to an external sound system (e.g. radio system) or to an audio signal source that will be recorded. The device can work in the paging mode, which allows to transmit the acoustic signal from the telephone line to the paging system, or in the VOX mode, where it is possible to record the signal from the line. Recording can be done in two ways. As continuous recording, or as sound detection recording - i.e. the recording will start when the acoustics level exceeds the set threshold..

In the configuration of announcements in the Paging mode, we define the type of signal that is to be played in the system speakers before the acoustics between the audio device and the subscriber are established.

To configure the MAB audio equipment in Paging mode, you must:

- specify the internal number
- indicate the FXS port
- select mode (currently only paging)
- set the announcement language
- select an appropriate announcement

Additionally, you can add sets of internal numbers that will be additionally notified as part of MAB device call.

To configure the MAB audio equipment in Record mode (VOX):

- enter the extension number
- indicate the FXS port
- select the Record mode
- set recording mode - continuous or with sound detection
- • set the sound detection parameters - sensitivity and delay times

7.10.2. AUD.IP

Audio.

A new family of Slican Audio products dedicated to the operation of public address and broadcast systems.

The system consists of:

- network speakers
- music encoder
- microphone

The configuration of individual devices requires an indication of its type and specific settings. Some of the settings are similar for all types.

Speakers, music encoder

- **device type** - selecting the appropriate device
- **MAC address** - search in the list or enter the device's hardware address manually for its authorization in the system
- **network settings** - configuring network settings automatically or manually
- **loudspeaker gain** - gain level for phone calls, announcements and music
- **announcement** - language, announcement at the beginning and end of recall

Microphone

- **button settings** - paging group or speaker number indication
- **outgoing traffic** - configuration of restrictions for outgoing connections
- **sets** - assignment to a set

7.10.3. DPH.IP

DPH.IP - is a new series of doorphone connected to a telephone PBX using Ethernet.

Basic intercom features include:

- call handling
- video stream transmission - an option requiring a camera module to be purchased
- opening gates and doors using proximity cards and IDs (keychain), PIN codes or DTMF digits thanks to an integrated RFID reader in the Unique 125kHz standard
- display definitions - text visible on the LCD
- number lists - quick number selection list

Advanced features (licence required) include:

- buffering and sending events (log) registered in the device memory, thanks to which it is able to serve as a fully functional access control system
- access zone configuration - assigning intercoms to zones

The registered event log is accessed using a dedicated ACS application, described in detail in another manual. The ACS application is subject to licensing. If the ACS feature is used and the intercom loses contact with the PBX, it continues to perform its ACS-related functions (events, zones) thanks to integrated

internal memory. The event buffer has a capacity of 2000 records. If the intercom buffer is filled, newest data does not overwrite existing events (it is discarded). When the intercom connects to the PBX, the event buffer will automatically be downloaded to the ACS system. If the ACS licence is not purchased, the intercom performs its basic functions.

DHP.IP intercoms are connected to the local network using existing LAN infrastructure and PoE power supply or local power supply. For the DPH.IP-KS16 model, it is possible to register it from an external network (Internet).

Remember, that intercoms obtain dynamic IP addresses by default. For this reason, they need to be operated within a network with a DHCP server enabled. Only after logging into an PBX (identical rules as for CTS.IP system phones) and correct assigning of MAC addresses it is possible to change the IP addresses to static ones from ConfigWEB. An exception can be the DPH.IP-KS16, where static IP addresses can be configured from the LCD.

A description of the individual models and variants is available on the [pubwiki](#) website.

Configuration details

The first step in configuration is to create the equipment in the PBX - *Internal numbers->DPH.IP->Intercoms* section and select the *Add* option. The PBX will assign an internal number and name by default.

Configuration of individual parameters depends on the device type. For this reason, you need to know its type and select it before commencing comprehensive configuration.

Configuration parameters available in individual tabs:

Device

- **device type** - select the device type (select it before configuring the other settings)
- **MAC address** - select from the list or enter manually
- **network settings** - dynamic (default) or static, set the appropriate data

Doorphone

- **display definitions** - text visible on the screen when not in use
- **number list** - quick number selection list during scrolling with up/down buttons
- **contrast** - display settings
- **sound settings** - system settings, microphone/speaker boost, microphone sensitivity, ringtone type
- **enable selecting any number** - permit numbers to be selected in accordance with outgoing traffic settings (restrictions) for the given intercom
- **time to select last digit** - set in seconds
- **pressing select button** - assign the number to the select button (green receiver, only applicable to the KS1 model)
- **camera** - URL (link) of the video stream, downloaded using the DPH.IP Camera Config application

ACS

- **access control enabled** - assign the intercom to the ACS system
- **access zone** - assign the intercom to a pre-defined zone

EZ output

- **mode** - select operating mode of the EDS relay
 1. **electric door strike** - applying voltage through the intercom will open the door
 2. **electromagnetic armature** - cutting voltage will result in opening the door
- **lock opening duration** - specify the time of voltage application (EDS) or cutting (armature)
- **opening signal duration** - duration of the acoustic signal informing about triggering the EZ relay

STA output

- **mode** - select operating mode of the STA transceiver
 1. **relay normally open** - standby status open, triggered - closed
 2. **relay normally closed** - standby status closed, triggered - open
 3. **lighting control** - any action at the intercom will trigger the relay
- **relay lighting release duration** - STA trigger duration (depending on operating mode)
- **time until lighting disable** - time after which the lighting is disabled (relay release)

SW input

- **SW1 input** - assign number dialling to the button
- **SW2 input** - configurable work mode as:
 1. **sabotage sensor** - standby status open, triggered - closed
 2. **button** - assign number dialling to the button
- **relay release duration** - STA trigger duration (depending on operating mode)

COD (Door Open Sensor) input

- **standby status** - specify status as normally open or closed
- **register door opening time events** - recording of events when doors were open longer than their maximum open time in ACS, CDR protocol
- **register events** - door opening without intercom action (EDS activation) as:
 1. **register entry events** - if door is opened mechanically
 2. **register forced entry events** - in the event of unauthorised forced entry (door prying)

POD (Door Open Button) input

- **standby status** - specify status as normally open or closed
- **mode** - specify work mode as:
 1. **door open button** - with the following actions available: event registration, EDS lock opening, STA trigger, number selection
 2. **invasion button** - with the following actions available: event registration, EDS lock opening, STA trigger, number selection (DOB release will result in ending the call)

Opening actions

Here you specify what actions will be taken depending on the entry method:

- **using a proximity card will result in** - opening the EDS lock, releasing STA, optional output selection: digit selection in DTMF:1(EDS), 2(STA), 3(EDS and STA)

- **using a user PIN code will result in** - opening the EDS lock, releasing STA, optional output selection: digit selection in DTMF:1(EDS), 2(STA), 3(EDS and STA)
- **using a telephone (number dialling) will result in** - opening the EDS lock, releasing STA, optional output selection: digit selection in DTMF:1(EDS), 2(STA), 3(EDS and STA), *(EDS and STA)

Phone calls

Configuration of parameters concerning handling of phone traffic from the intercom:

- **outgoing traffic** - maximum waiting time for call, type of music on hold, maximum call duration
- **outgoing traffic** - actions (automatic answering, calling, listening, rejecting), maximum call duration

Outgoing permissions

Specify restrictions in outgoing traffic (as for regular subscribers)

Set

Assign the intercom to a specific set

Display definitions

Define the text to be displayed (on standby) on the LCD, and assign it to a specific intercom.

Number lists

Define a scrollable quick selection number list and assign it to a specific intercom.

Access zones

Create access zones in the PBX, which are defined as a certain limited area, which can be entered using one or more intercoms. In the configuration, specify the zone name and assign to it an intercom or intercom group.

Settings

Settings related to global intercom configuration.

- **Configuration access PIN** - a unique key to the configuration (menu access after pressing the key symbol on the keypad twice and entering the PIN code)
- **time range for holidays** - range of time that will be considered holidays for the purposes of access rules defined in the ACS

Timetable

It allows temporary control of the doorphone in the context of: opening / closing the door and / or controlling external devices connected to the DPH.IP STA contact. The release of a specific action requires the creation of a single rule. In order to control the opening and closing of the door, we must create two separate rules defining the time frame for each of them.

Action will be perform:

- non-holiday days of the week
- holidays

Defined actions:

- opening
- closing
- advanced mode - combinations of EZ and STA contacts settings for performing an action

Actions can be recalled or canceled as part of doorphone control by assigning them to the system telephone button or using Mobilephone and MessengerCTI.Mobile.

7.10.4. Cameras

The system enables integrating internal numbers with IP cameras. Assigning a number is necessary due to how connections with camera-type objects are executed. In the case of cameras integrated with DPH.IP intercoms, they are intercom numbers. In the case of autonomous cameras, they need to be assigned virtual numbers.

We prefer cameras offered with DPH.IP intercoms or as independent devices. Cameras of any other manufacturer can also be used (provided they support libraries based on the VLC software).

Image is previewed using the dedicated Slican MessengerCTI application (configuration of the camera operating application is described in detail in a separate manual).

Calls executed by MessengerCTI.Desktop, both from and to numbers integrated with cameras, result in image being previewed automatically as an additional window on the computer where the application is installed. The system supports up to **10 users** viewing a single camera feed.

Configuration details

The entire configuration is limited to

- **video stream URL** - link to the camera, downloaded from the camera operating application
- **internal number** - select an internal number associated with the camera

Searching cameras in the network and accessing their configuration and links is performed using a dedicated **DPH.IP Camera Config** application (available on the ServNET server). By default, cameras obtain IP addresses from the DHCP server, but for correct operation, it is recommended to set static addresses or associate camera MAC addresses with IP addresses in the DHCP server. This protects the system from incorrect functioning in the event of IP address change and link validity loss.

A sample format of camera access link:

<rtsp://192.168.155.12:554/user=admin&password=&channel=1&stream=0.sdp?>

Cameras of third party manufacturers must be compatible with VLC application libraries (video formats, codecs). We do not guarantee that they will work correctly with the DPH.IP Camera Config application. In the event of problems, use the given manufacturer's solutions.

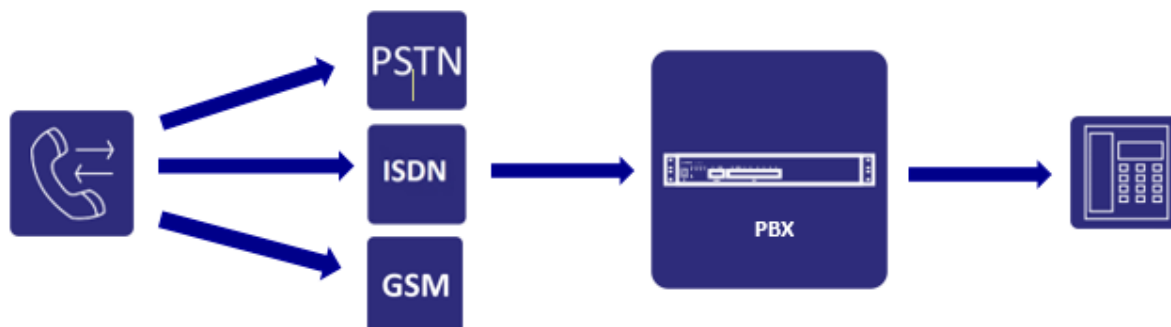
8. Operators

Traffic routing is the basic function of the PBX. Traffic can be routed depending on the equipment and metropolitan lines available. Preliminary configuration involves adding TDM or VoIP operators Next, specify the method of call routing in outgoing traffic, taking into account operators, dialled prefixes, and forwarding to specific numbers or groups in incoming traffic.

For correct presentation normalisation in main settings, enter the country prefix of the place where the PBX is located. Format with the + character, e.g. **+48**

8.1. TDM operators

TDM operators, i.e. providers of classic telecommunications services, such as FXO analog lines, ISDN BRI/E1 digital lines, GSM. In order to configure a TDM operator, install an appropriate module in an NCP-GW shelf and accept it in the section: **Hardware configuration->Modules**.



Operator configuration:

General settings

- **prefix of the country where the PBX is located** - the format with the + character, e.g.: +48
- **directional prefix of the PBX location** - city prefix for the given area, e.g.: 52

TDM operator - metropolitan connection types

- **FXO - analog** metropolitan line module (Foreign Exchange Office)
- **ISDN BRI - digital** external metropolitan line module (Integrated Services Digital Network Basic Rate Access)
- **ISDN E1 - digital** external metropolitan line module (Integrated Services Digital Network Primary Rate Access)
- **GSM - digital** external metropolitan line module (Global System Mobile)

Configuration details

- **name** - additional description, e.g. name of the service provider operator
- **operator type** - select the TDM operator type (in accordance with the installed metropolitan line module)
- **default routing** - default routing for handling of calls not specified in the incoming rule (the other calls rule)
- **add ports** - select available ports from installed TDM modules (port bundle within the given operator)

8.2. VoIP operators

VoIP operators, i.e. providers of voice services over the Internet.

This section configures the handling of VoIP operators and PBX networking using the internal eSSL protocol or networking with foreign exchanges (SIP protocol). In order to register an PBX with the VoIP provider, use the registration data obtained to configure: domain address or VoIP server IP address,

username and password. Remember that the method of VoIP operator registering can be based both on basic and more advanced data, i.e.: proxy server address, domain name, user authentication.



General settings configuration

- **enabled** - enable/disable the operator
- **name** - any description of the VoIP operator
- **SIP registration** - configuration of registration message sending/reception (specification of the client-server relation) depending on the operator's requirements. In special cases, e.g. for anonymous translation, the only authentication is the IP address from which calls are made (the do not send/do not wait option)
- **host name or IP address** - specify the domain or IP address of the VoIP operator, or in the case of PBX networking, server address
- **user** - name for user/account logging in with the VoIP operator or eSSL server
- **password** - password for logging in with the VoIP operator or eSSL server password
- **default routing** - specify how calls from this operator are to be routed if no specific destination in the incoming rule is indicated (this is the other calls rule)
- **main number** - in the following format: country prefix, direction prefix, number
- **DTMF mode** - DTMF transmission method setting (digit transmission/reception): [RFC 2833](#), SIP INFO, in-band
- **enable error notifications** - notifications sent to the administrator about line damage

Advanced settings - general

- **SIP port** - number of the SIP signalling listening port on the server side (default: 5060)
- **proxy host** - adding alternative host names or IP addresses of the operator
- **host screen** - enable screen
- **host screen frequency** - specify monitoring duration in seconds
- **only secure calls** - enable encryption for both SIP signalling and RTP voice frames
- **add user=phone to SIP URI** - additional information optionally added to signalling frames in the SIP protocol when the operator requires information that the call is made to a telephone number.

Advanced settings - authentication

- **domain name** - for some operators, additionally required domain name (optional)
- **username for authentication** - user name for registration, if other than account name in basic settings
- **incoming call authentication** - incoming call authorisation using source IP address and additional parameters sent in SIP signalling (disabled means that incoming calls are executed without additional verification)

Advanced settings - caller presentation

- **call presentation transmission method** - CLIP presentation transmission method setting depending on the operator's requirements (Remote-Party-ID, FROM header, P-Asserted-Identity)
- **transmission format** - caller presentation format: internal, national, international
- **ignore incoming presentation changes from the operator on outgoing calls COLP** - handling calls when the destination number had an active diversion and the number presentation changed
- **enable CLIRO** - override caller presentation blockade (licence required)

Advanced settings - identification

- **add alternative host name or IP address** - alternative domain name or IP address of the operator which the call is coming from (domain or address other than the one given for registration)

Dedicated circuit

- **PBX external IP address in dedicated network** - PBX external address for the operator working in a dedicated network

Advanced settings - call limit

Shaping incoming and outgoing traffic based on the number of concurrent calls, both total and broken down by call direction.

Advanced settings - audio codecs

Select voice transmission codecs from those available in the PBX.

NOTE

The G.729 codec is subject to additional licensing

Advanced settings - video codecs

Select available video transmission codecs.

IP filter

To provide additional protection against unauthorised access to VoIP accounts, you can configure an additional filter focused on a specific IP address or network address. A tool useful when linking exchanges via the Internet. By default, the filter allows any address.

Fax - settings

Error correction for T.38 codec.

9. Call routing

Outgoing and incoming traffic refers to the method of executing calls to and from the provider PBX or VoIP server by Slican NCP-PBX. To accurately describe the rules of traffic routing, the terms used in configuring traffic in the PBX must be defined first:

Operator - a physical (or logical, for VoIP traffic) port in the PBX, used to connect the PBX with the telecommunications service provider.

Rules - a set of rules defining how traffic, based on reaching the destination number for outgoing traffic, and appropriate routing of calls for incoming traffic, is directed.

Dialled number analysis - a list of rules for which you specify whether the given subscriber (internal number) has the necessary rights in outgoing traffic.

For outgoing traffic, one rule applying only to internal traffic is created by default. On the other hand, for incoming traffic, a default “other” rule (aimed at disconnecting) is created.

9.1. Settings

Call routing general settings

The following maximum durations are configured in general settings:

- **call duration**: default 960 minutes
- **transit call duration**: default 10 minutes
- **call wait duration**: default 180 seconds
- **forwarded call wait duration**: default 40 seconds

Outbound prefix settings added before dialled number to route a call using of dialplan rules :

- **none** – lack of outbound prefix
- **automatic for single prefix** - for this mode, specify the prefix of the output which will be added by the subscriber before the dialled number and directed to the analysis of the selected number
- **custom with multiple prefixes** - for this mode, the outbound prefix/prefixes are defined in the analysis of the selected number and on this basis it is directed to the appropriate outgoing rule
- **the numbers in the phonebook contain the exit prefix** - if the numbers in the phonebook contain the output prefix then they are analyzed according to the analysis rule of the selected number. If not then automatically such a prefix is added automatically
- **add the output prefix to all numbers in the LDAP phonebook** - in custome mode with support for multiple prefixes, add a prefix to contacts established from the LDAP phonebook for SIP phones to properly handle outgoing calls.

By default, all subscribers have rights in internal traffic. In order to impose restrictions in internal traffic between numbers, create an appropriate rule in outgoing traffic (*Call routing->Outgoing and internal*).

9.2. Predefined prefixes

Functionality that allows you to define a prefix or group of prefixes for which we can easily manage traffic. This applies to both outgoing and incoming traffic.

PBXs with the factory firmware version from 1.12 contain the default predefined prefixes:

- alarm prefixes
- cell prefixes
- premium prefixes

After updating, the other PBX will be available simultaneously with those already configured in the Call routing -> Outgoing and internal -> Dialed number -> Permissions.

The full PBX format removes "old" permissions by assigning new ones. You can also delete them manually while adding new predefined prefixes.

9.2.1. Predefined prefixes - outgoing traffic

To limit traffic for a prefix or group of prefixes, we add it to the predefined prefixes:

- in the form of a prefix number
- regular expressions

The use of regular expressions allows us to group prefixes covering a larger range of achieved combinations of numbers.

An example of the regular expression of cell prefixes for the leading digit 5:

5 [0 1 3 7]

gives the following prefix combinations:

50

51

53

57

which ultimately allows you to select the numbers in order, e.g.

501234567, 511234567, 531234567, 571234567

We define the numbering type as:

- national
- international
- unknown

Then we introduce restrictions (optional) as to the length of the number.

We assign the prefix to the outgoing rule, allowing connections only within it. In the next step, we assign the subscriber the rights in the outgoing traffic to exit using this rule.

9.2.2. Predefined prefixes - incoming traffic

Predefined prefixes can be used in incoming traffic in special cases.

In incoming traffic:

- rules of selected number - where defined prefixes can be directed in some special way
- static routing - static routing based on defined prefixes of incoming numbers
- modifications - transformation of the number presentation based on defined number prefixes

9.3. Outgoing traffic

This configuration section defines all aspects related to the methods of reaching the destination number. Outgoing traffic routing comprises:

- **dialled number analysis** - form for adding new outgoing rules
- **caller presentation** - presentation replacement depending on the rule selected
- **dialled number normalisation** - presentation normalisation before the PBX dials a number
- **rights** - rights to prefixes

Dialled number analysis by the PBX involves sequentially checking rules created in the dialled number analysis form. When the system encounters the first consistent entry, it checks whether the destination operator is free. If the operator is busy (condition: busy channels, damage), the system searches the database for an alternative operator that can execute the call.

If, during number analysis no rule for the selected prefix is found in the dialled number analysis form, the subscriber receives an appropriate system message. Each dialled number is subject to temporary analysis (time counted from the moment the last digit is dialled), after which the PBX begins the process of connecting the call with another PBX subscriber or metropolitan subscriber. This parameter can be configured in the PBX (*Internal numbers->Settings section*) and equals 5 seconds by default. In order to accelerate number analysis, select the # sign in the phone after dialling the complete number. Fast internal number analysis without ending the dialled number with the # sign can be enabled by configuring the "do not wait for #" option (system and analog phones), available in the menu: *Internal numbers->Settings*.

All traffic directed outside is subject to analysis based on the pre-set rules. Rules should include initial digits (prefixes) of the dialled numbers. Prefixes of dialled numbers can be grouped using **regular expressions**, i.e.: **()** and **|** e.g.: expression containing stationary number prefixes looks as follows - (12|22|32|42|52) or for a specific number (+48)523251100.

The general rule, i.e. leaving the "initial digits of the number" field empty means that subscribers can dial any prefix. Remember to place this rule at the end of the dialled number analysis.

By default, an overriding rule concerning internal traffic handling is available. Newly created rules have the "ignore" restriction level for all internal numbers by default. Permission for individual subscribers to go out using the given rule is enabled in the **Extensions->Subscribers->Outgoing settings** section.

If PBX networking using the eSSL protocol is enabled, a rule for routing outgoing traffic to "networked" exchanges is created by default.

The order of adding new outgoing traffic rules is important from the perspective of analysing the selected digits. Also remember that the PBX begins dialled number analysis "from the top", checking subsequent rules to find the best suited entry. Therefore it is reasonable for the internal traffic rule to be at the top of the rule list. On the other hand, the rule than encompasses all other dialled numbers that are not included in any matching rule is located at the bottom of the list. It is also possible to sort rules by dragging the given entry (up/down).

For each rule, the **Rights** tab contains a list of internal numbers authorised to use the given rule. Restriction settings for going out using the given rule can be found in the menu: **Extensions->Subscribers->Outgoing settings**

Configuration details

Adding rules - general settings

- **rule name** - descriptive name of the rule, e.g. GSM
- **description** - additional description of the rule

Adding rules - dialplan (match pattern)

- **initial number digits** - match patterns for initial digits of dialled numbers - it is possible to create a single rule for each prefix individually, or serial matching patterns using regular expressions containing brackets () and vertical lines |, e.g. pattern (52|22|58) for 521234567 and 581234567 (by default, an empty field means exit for all prefixes, subject to individual settings for each subscriber)
- **minimum length of the remaining part of the number** - specifies the minimum number of digits after which the PBX begins dialling a number once initial digits (e.g. 3) are selected
- **maximum length of the remaining part of the number** - specifies the maximum number of digits after which the PBX begins dialling a number once initial digits (e.g. 9) are selected

Adding rules - modification of numbers before calls

An option enabling number modification before it is dialled by the PBX.

- **number of digits to truncate from start of number** - number of initial digits to skip
- **add digits preceding dialled number** - e.g. adding operator prefix

A good example of using such modifications is the case where metropolitan numbers are reached by the “city exit” digit, e.g. 0. In such cases, the outgoing rule should contain the exit digit in its initial digits, e.g.: 0(52|22|58). Number modification should remove the leading digit (0 in this case) before the call: **Number of digits to truncate from start of number** (in this case 1).

Adding rules - call routing

- **primary operator** - call routing to the operator (TDM, VoIP or internal operators)
- **alternative operators** - call routing to an additional operator in the event of, for example, damage or unavailability (busy channels) of the primary operator
- **ignore prefix rights** - permission for internal numbers to exit using this rule, ignoring prefix rights

Adding rules - final rule

- **final rule** - i.e. do not check further outgoing rules if no operator is available
- **enable all subscribers to exit using this rule** - sets a permission for all internal numbers to exit using this rule without the need to configure rights levels for each of them individually. This field only appears during new rule creation.

Caller presentation

Depending on the call initiator (internal number, group, set), specify the manner in which to present (CLIP) the caller in outgoing traffic by selecting the given dialled number rule, both for internal and metropolitan traffic. By default, the “main number” rule is created, under which callers for whom no dedicated rule has been created, will present themselves in outgoing traffic using their main number. Rules with presentation modification only apply ISDN and VoIP operators. For FXO and GSM operators, presentation is only possible with the main number.

Rules can be added:

- **by numbers** - applicable to individual internal numbers or sets
- **by ranges** - applicable to ranges of internal numbers (e.g. DDI range) or to sets

Add rule for number

- **rule name** - detailed name of the rule
- **description** - additional description of the rule
- **outgoing call initiator** - select whether the rule is to apply to an internal number, set or operator (for transit calls)
- **internal/all internal** - select from a list of internal numbers or a set (if the initiator is to be an internal number)
- **call using a dialled number rule** - select available outgoing traffic rules from the list
- **caller's number (Caller ID)** - number to be presented outside in national or international format

Examples of static rule configuration with presentation modification in internal traffic:

Create caller ID rule

Rule name:

Note:

Caller ID rule routing

Caller to match with the outgoing call:

Call through dialed number rule:

Change caller ID to

Caller number:
use only national (ie. 523251100) or international format (ie. +49030220700)

Caller ID

	Name	Details
<input type="checkbox"/>	STATIC RULE	When extension <input type="text" value="1001. 1001"/> is making an outgoing call through <input type="text" value="rule: Internal"/> change their caller ID to <input type="text" value="1010"/>

Add range rule

- **rule name** - detailed name of the rule
- **description** - additional description of the rule
- **outgoing call initiator** - select whether the rule is to apply to numbers belong to a set or an internal number range
- **call using an outgoing traffic rule** - select available outgoing traffic rules from the list
- **number of digits to truncate** - set the number of digits to truncate from the start of the number
- **add digits before internal number** - string of digits added before an internal number in national or international format
- **add digits behind internal number** - any string of digits, added behind an internal number

An example of dynamic rule configuration with presentation modification in internal traffic for the specified number range:

Create caller ID rule

Rule name:

Note:

Caller ID rule routing

Caller to match with the outgoing call:

Extension range from:

Extension range to:

Call through outgoing rule:

Change caller number

Number of digits to trim from the front:

Prepend extension with digits:
use only national (ie. 5232511) or international format (ie. +490302207)

Append digits to extension:

Caller ID

	Name	Details
	DYNAMIC RULE	When extension in the range from <input type="text" value="100"/> to <input type="text" value="199"/> is making an outgoing call through <input type="text" value="rule: Any dialed number rule"/> change their caller ID to a number by prepending with <input type="text" value="523251"/>

Add transparent rule

A rule concerning allowing traffic without modifying the caller's presentation. Also related to call transit and transferring traffic between metropolitan lines or when networking with exchanges of other manufacturers.

Rights

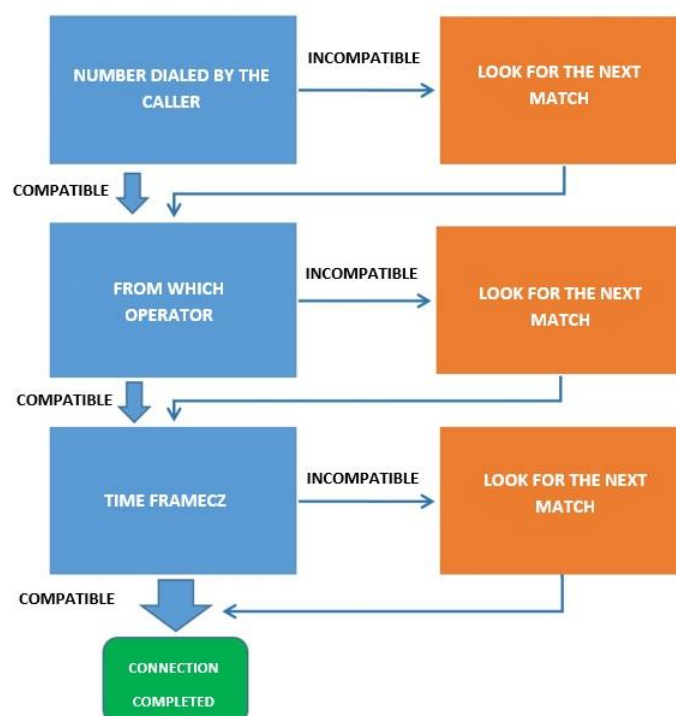
Configuration of rights to select specific prefixes in outgoing traffic. When making calls, prefixes are compared with the dialed number modified by dialed number analysis and normalisation.

9.4. Incoming traffic

Here you specify the basic conditions that must be met for incoming calls to reach their destination. Additionally, the criteria for call selection of incoming traffic routing when connecting to the indicated internal number involve meeting the following conditions:

- what number was dialed by the initiator
- what operator the call came from
- in what time range the PBX is located in

Incoming calls based on the created rules are executed in accordance with the following diagram:



Before an incoming call reaches a specific internal number, it is subjected to detailed analysis in the PBX. One of them is correct formatting of the incoming call CLIP number based on pre-defined rules of the *presentation normalisation* form. This form standardises the format to match one of the three possible: international, national, or other. Next, when the number is correctly classified, an appropriate prefix is added to it. This gives the ability to present the number to the internal subscriber in such a format that they can call the number back without additional modifications.

Additionally, it is possible to transit incoming calls by directing them to *Dialled number analysis* for further routing.

By default, the following rules will be created:

- other - for other calls that have arrived at the PBX (not configured based on the operator)
- Unknown VoIP - routing calls from unidentified VoIP operators

The above can be directed to: disconnect, unavailable signal, busy or internal number.

Incoming traffic routing comprises:

- **incoming traffic rules** - add further rules in accordance with call handling logic
- **routing according to caller presentation** - direct incoming traffic according to caller presentation (overrides incoming traffic rules)
- **presentation normalisation** - specify call category (national, international) based on received presentation and potentially modify it
- **zones** - zone names displayed on the phone based on the caller's prefix

9.4.1. Incoming rules

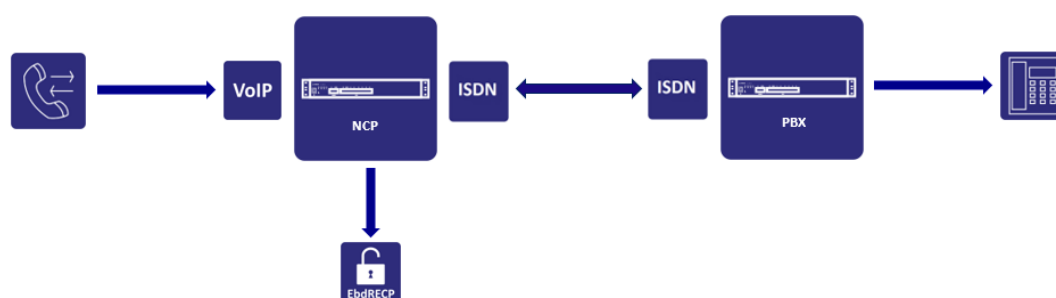
Adding rules by number - used for individual numbers

- **rule name** - any rule name
- **description** - additional detailed description of the rule

- **selected number for comparison** - number selected by the initiator in incoming traffic (required)
- **call provider** - select the operator (VoIP, TDM operators)
- **time range** - specify the time which the rule is to be applied to
- **manual operating mode** - specify a pre-defined operating mode which the rule is to be applied to
- **DISA** - playback of welcoming announcement before call is routed
- **language** - language version of the DISA announcement
- **call the extension number during the announcement** - in this case the subscriber's number will start to ring when the announcement starts to play,
- **skip the announcement if the extension is busy** - if the extension is busy, you can turn off the announcement
- **callers can select internal number during announcement** - number selection (in DTMF) during announcement playback
- **selectable internal number set** - by default, all internal numbers
- **fax support** - fax signal detection during DISA announcement with redirection to fax2mail gateway or to an internal number with a fax device connected (field revealed when DISA option is enabled)
- **internal fax number** - indicate an internal number with a fax device connected, or numbers with fax2mail gateway enabled
- **route to** - routes calls to a number or to dialled number analysis in the case of transit, or rejects
- **internal number** - route calls to selected internal number (subscriber, group or IVR)
- **rejection method** - in what way calls are to be rejected (disconnect, busy)
- **call not answered** - alternative call forwarding when the destination extension is not answering at the time of the call with the time to answer (time in seconds)

Call transit - configuration

If the NCP PBX is to serve as an intermediary system in traffic transferring as a media gate, e.g. VoIP/ISDN conversion, or the call transiting option can be used. In such cases, in the *Route to* section, select "Dilaplan rules" and indicate the payer to cover the costs of transit calls (necessary for collecting billing events). Next, specify what rule permits transit calls to exit and prefix permissions.



Adding rules by range - used when reaching DDI numbers

- **rule name** - rule ID
- **description** - additional detailed description of the rule
- **dialled number range from** - initial number of a range (complete metropolitan number, e.g. 523251100)
- **dialled number range to** - end number of a range (complete metropolitan number, e.g. 523251199)

- **call provider** - select provider (available providers: SIP, TDM)
- **time range** - specify the time which the rule is to be applied to
- **manual operating mode** - specify a pre-defined operating mode which the rule is to be applied to
- **DISA** - playback of welcoming announcement before call is routed
- **skip the announcement if the extension is busy** - if the extension is busy, you can turn off the announcement
- **call the extension number during the announcement** - in this case the subscriber's number will start to ring when the announcement starts to play,
- **language** - language version of the DISA announcement
- **callers can select internal number during announcement** - number selection (in DTMF) during announcement playback
- **selectable internal number set** - by default, all internal numbers
- **fax support** - fax signal detection during DISA announcement with redirection to fax2mail gateway or to an internal number with a fax device connected (field revealed when DISA option is enabled)
- **number of digits to truncate from the start of number** - specify the number of digits to skip from the start of the dialled number before call (number modification before call)
- **adding digits preceding the dialled number** - adding a string of digits preceding the dialled number (number modification before call)
- **adding digits to the end of the dialled number** - adding a string of digits at the end of the dialled number
- **route to** - routes calls to a number or to dialled number analysis in the case of transit, or rejects
- **rejection method** - in what way calls are to be rejected (disconnect, busy)
- **busy call** - an alternative call forwarding when the destination extension is busy
- **call not answered** - alternative call forwarding when the destination extension is not answering at the time of the call with the time to answer (time in seconds)

The below sample configuration shows incoming traffic routing to the DDI range. The internal number is the result of modifying the selected number by removing eg. the first 6 digits of the number dialled by the initiator:

Create DDI route	
Route name:	DDI ROUTE
Note:	<div></div>
Match incoming call	
Beginning range of incoming DDI:	523251100
End range of incoming DDI:	523251999
Incoming provider:	Any provider ▼
Additional conditions	
Time frames:	Any time ▼
or manual modes:	Any mode ▼
DISA	
Play announcement before routing the call:	<input type="checkbox"/>
Modify number before connecting the call	
Number of digits to trim from the front:	6
Digits to prepend to the number:	
Digits to append to the number:	
Route incoming call	
Route to:	Extension number ▼
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

9.4.2 Caller ID routing

Routing by presentation - static routing based on caller presentation

Special routing of calls based on caller presentation (full number or prefix). The PBX enables call routing support as:

Route call to extension number- allows you to forward the call to a defined extension number

- **rule name** - rule ID
- **description** - additional detailed description of the rule
- **incoming number comparison method** - by telephone number, prefix, predefined prefixes, MobilePhone subscriber's number or MessengerCTI subscriber's number or proprietary presentation
- **incoming number** - presentation of the incoming number, consistent with the specified format, e.g.: +48523251100
- **time range** - pre-defined time-range
 - **manual operating mode** - specify a pre-defined operating mode which the rule is to be applied to
- **manual operating mode** - selection
- **compare dialled number** - matching consistent with dialled number or prefix
- **redirect to internal number** - route calls to selected internal number, set or function.

The below sample configuration shows incoming traffic routing based on caller presentation, with routing to an internal number in any time range.

Modify caller ID route	
Rule name:	CALLER ID TRANSFER
Note:	<div></div>
Caller ID	
Incoming number type:	Phone number ▼
Incoming number:	523251111
<small>use only unknown (ie. 1109) or international format (ie. +48523251100)</small>	
Additional conditions	
Time frames:	Any time ▼
or manual modes:	Any mode ▼
Dialed number	
Compare dialed number:	<input type="checkbox"/>
Transfer target	
Extension to transfer to:	1001. 1001 (SIP) ▼ Choose...
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/>	

Route call to number- enables call forwarding to a defined extension or outgoing call with the rights of the calling subscriber, which is identified by the MobilePhone or MessengerCTI.Mobile number declared in the PBX.

- **rule name** - rule ID
- **description** - additional detailed description of the rule
- **Incoming number** - Mobile number of the MobilePhone or MessengeraCTI subscriber
- **time range** - pre-defined time-range
 - **manual operating mode** - specify a pre-defined operating mode which the rule is to be applied to
- **manual operating mode** - selection
- **compare dialled number** - matching consistent with dialled number or prefix
- **number to dial** - directing the call to the defined number

Route call to DISA- calling subscriber who is identified by the MobilePhone or MessengerCTI.Mobile number declared in the PBX receives a PBX notification signal and can make any internal or external call in accordance with the outgoing traffic rights, an announcement can be played before the signal

- **rule name** - rule ID
- **description** - additional detailed description of the rule
- **Incoming number** - Mobile number of the MobilePhone or MessengeraCTI subscriber
- **time range** - pre-defined time-range
 - **manual operating mode** - specify a pre-defined operating mode which the rule is to be applied to
- **manual operating mode** - selection
- **compare dialled number** - matching consistent with dialled number or prefix
- **number to dial** - directing the call to the defined number

Add blockade - no call handling

- **rule name** - rule ID
- **description** - additional detailed description of the rule
- **incoming number comparison method** - by phone number or prefix
- **incoming number** - presentation of the incoming number, consistent with the specified format, e.g.: +48523251100
- **compare dialled number** - matching consistent with dialled number or prefix
- **blockade action** - define what action the PBX is to take based on the above rule: play busy signal, play unavailable signal, disconnect
- **time range** - specify the time to which the above rule is to apply: any time range, working hours, holidays, weekends
 - **manual operating mode** - specify a pre-defined operating mode which the rule is to be applied to

Opening doorphone - routing the connection to open the doorphone based on the presentation of the mobile number defined as Mobilephone or MessengerCTI.Mobile

- **rule name** - rule ID
- **description** - additional detailed description of the rule
- **Incoming number** - Mobile number of the MobilePhone or MessengeraCTI subscriber
- **compare dialled number** - matching consistent with dialled number or prefix
- **doorphone** - we define which doorphone should be opened

Doorphone control - routing the connection to call the doorphone configured action based on the presentation of the mobile number defined as Mobilephone or MessengerCTI.Mobile. In this way, we can force specific doorphone behavior using the EZ or STA input (e.g. additional lit lights)

- **rule name** - rule ID
- **description** - additional detailed description of the rule
- **Incoming number** - Mobile number of the MobilePhone or MessengeraCTI subscriber
- **compare dialled number** - matching consistent with dialled number or prefix
- **doorphone** - we define which doorphone should be opened
- **action** - input selection

9.4.3. Dynamic routing

PBX, allows you to create rules for remembering routes for the indicated types of connections for later use to directly set up the next connection. Dynamic routing works for both incoming (reconnection to the same extension) and outgoing (the ability to call the target subscriber to the internal subscriber).

If such a connection is found in the dynamic routing register, the traffic will be directed to the target subscriber in the entry recorded in this entry. If the registry does not contain an entry for an incoming call, it will be handled by the other incoming traffic rules.

Creating a dynamic routing rule:

- **rule name** - rule identifier
- **description** - additional detailed description of the rule
- **internal numbers** - select the set of internal numbers supported by the rule
- **Outgoing calls, missed calls** - enabling outgoing routing, the ability to select a specific rule or operator, or for all rules.
- **Incoming call, received** - Activate inbound routing, select a specific rule or operator, or all rules.
- **Expiry time of dynamic routes** - We set the time for remembering routes. The maximum adjustable is 99h.
- **Number selected by the caller** - Selecting this option means that, apart from the presentation, the condition will also be the number selected by the caller
- **Connection referring to a busy subscriber** - Selection of actions on the connection - disconnection or referral to incoming traffic rules, in case of disconnection, the option of deleting the dynamic route.

Dynamic routing does not work for connections initiated from ConfigWeb as a test connection.

Active routes

PBX allows you to view saved routes and delete them.

9.4.4. Caller's presentation

Presentation normalisation

Correct routing of incoming traffic based on CLIP presentations requires information on what type of number it is: international or national. This feature enables configuring automatic presentation recognition when it is not clearly specified in digital signalling. In particular, this applies to VoIP, FXO, GSM and ISDN operators when information about the number is in UNKNOWN (type unknown) form.

Zones

Numeration zone information added to the caller presentation. The system creates default numeration zone applicable in Poland, and numeration zones for Europe. Zone export or import as *.csv files enables free modification of their content and transferring it between NCP exchanges.

Modifications

Adding special rules that allow modifying the presentation in incoming traffic when certain conditions are met: arrival rule, caller's prefix. Additionally, we can block presentation the number calling.

Outbound prefix

Adding an outbound prefix to missed calls and calls from history. For this option, we can decide which prefixes are to be added to the presentation of the caller number in order to properly direct it to analyze the selected number. The form is available for the case of using the *Custom with multiple prefixes*.

10. PBX features

A set of additional PBX features, such as: contact book, working time range, call recording and billing, or text message support.

10.1. Phonebook

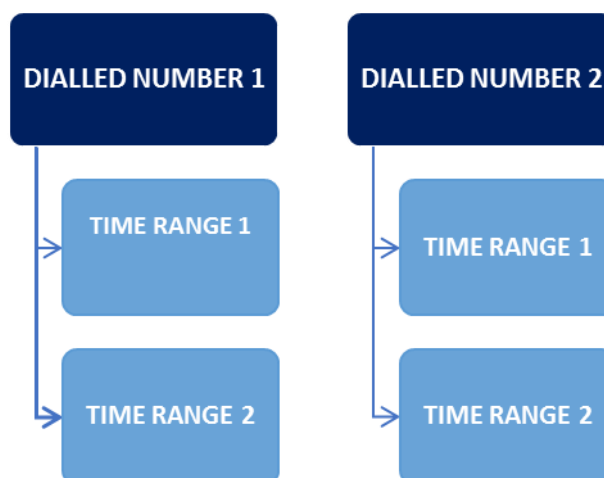
The contact database is managed using the dedicated WebCTI application from an Internet browser. Connect to the WebCTI application by entering the LAN interface IP address in the browser's address bar (e.g. IP address of the PBX/CTI 192.168.0.248/ WebCTI), or from ConfigWEB menu (administrator access) **Exchange features->Contact book**. By default, access to the contact book for users is possible only within the network. For subscribers residing outside the customer's network (Internet), it is possible to enable remote access to the contact book using appropriate network configuration by its administrator. In such cases, we recommend enabling the secure data access protocol (https). Level of access to contact management for users depends on the assigned rights available in the network. **Extensions->Subscribers->CTI settings**. A detailed description of contact management and other features of the WebCTI application can be found at: [WEBCTI](#). The maximum book capacity (public and private) is 30 000 contacts (including up to 5 numbers per contact).

10.2. Time ranges

Depending on the time: hour, day of week, month, year, holidays, the manner of routing calls in the PBX can be defined. Defined ranges can be freely assigned to rules in incoming traffic, as well as in the IVR menu. In such cases, the given entry will be analysed based on the conditions defined in it.

By default, there are several ranges defined in the PBX: holidays, working hours, weekends. The "holidays" range contains a list of fixed (repeating yearly) work-free days and moveable holidays (i.e. Easter, Corpus Christi). For moveable holidays, the point of reference is the first day of Easter. For the other ranges, the conditions can be set depending on traffic handling needs. The PBX analyses incoming traffic rules (from the top) based on the combination of fields: "dialled number" and "time range", and decides where to direct the given call. If you do not want to specify any particular time range and want to always route calls the same way (regardless of time), select the "Any time range" option.

In step one, add a time range, then specify the conditions for which the given time range is to be active. Below, a diagram of rule analysis based on time ranges:



Configuration details

Add time range

- **name** - define the given range

Add conditions

- **year** - specify the year for the defined range, if the field is empty, the condition applies to any year
- **month** - specify the month for the defined range, if the field is empty, the condition applies to any month
- **day of the week** - specify the day of the week for the defined range, if the field is empty, the condition applies to any day of the week
- **until day of week** - specify the day of week (until) for the defined range, if the field is empty, the condition applies to a specific day of the month
- **day** - specify the day of the month for the defined range, if the field is empty, the condition applies to any day of the month
- **time** - specify the initial time for the defined range, if the field is empty, the condition applies to any time (in HH:MM format)
- **until time** - specify the end time for the defined range, if the field is empty, the condition applies to any time (in HH:MM format)
- **number of days from the first day of Easter** - enter zero, a positive number or a negative number, when the field is empty, the condition is not taken into account

The above give the ability to specify moveable holidays that depend on Easter. In such cases, define the number of days from/to the next holiday, basing on the date of Ester.

10.3. Manual operating modes.

For special incoming traffic routing outside a time range, the PBX can take into account the operating mode defined by the administrator. This feature enables flexible modification of incoming traffic rules to match an unexpected case of different traffic routing compared to default configuration. The manual operating mode is configured by the administrator, and the administrator can enable and disable it. Without the

administrator, users enable or disable the given mode using service codes assigned to the given mode, or using a button on CTS system phones. Information on the active operating mode is available in the *Collective information* tab in ConfigWEB, as well as after pressing the phone button.

Configuration details:

Adding modes by the administrator:

- **add mode** - mode adding (creating a name)
- **activate** - configure the method of its activation
 - **until manual deactivation** - mode activity duration until it is cancelled manually
 - **until selected hour** - configure the time until which the mode is to be active
 - **until selected time ranges** - indicated the time range until which the mode is to be active

Adding a service code by the administrator for handling operating modes:

- **internal number** - assign a service code number (default activation by *87)
- **manual operating mode to be activated** - assign operating mode
- **numeric password** - additional protection for mode activation by the user
- **deactivate when mode active** - deactivate using the same service code
- **activity period** - configure the method of mode activation
 - **until manual deactivation** - mode activity duration until it is cancelled manually
 - **until selected hour** - configure the time until which the mode is to be active
 - **until hour entered as parameter** - enables manual configuration of the hour of mode activity by the user
 - **until selected time ranges** - indicated the time range until which the mode is to be active

When mode parameters (activation, time) are changed using a service code, parameters of mode activation by the administrator are overwritten. Also note the order of incoming rules, so that the rule associated with the mode was analysed first, if there are no other rules encompassing the given entry. It is also possible to combine both time ranges and operating modes.

10.4. Call recording

The NCP PBX has an integrated recording system based on an internal protocol enabling recording of calls made in outgoing, incoming and internal traffic. When configuring the system, the administrator sets the rules concerning call recording. They apply to specifying what calls re to be recorded, recorded objects, and level of access to records. Access to records is possible using the dedicated RecordMAN.server or RecordMAN.client application, or via FTP. Due to data safety, the recording module is equipped with a special file encryption system.

The carrier for the recorded calls is an integrated hard disk.

Below, approximate data concerning the capacity of memory intended for the recording system.

No. of concurrent EbdREC records	CM.300 - SSD 60GB (680h/1300h/6000h of records) CM.400 - SSD 128GB (1500h/3000h/13000h of records) CM.600 - SSD 240GB (3400h/6800h/30000h of records)
----------------------------------	---

10.4.1. Recorded objects

The integrated recording feature enables:

- activating recording
- preventing (blocking) recording

The recorded objects are:

- sets
- subscribers and devices
- paging
- lines
- conference calls
- operators (VoIP, TDM)
- dialled number analysis - transit calls
- incoming traffic rules - select one rule
- routing by presentation - recording calls related to static routing.

The level of access to records is set by the system administrator. Depending on the configuration, the administrator can assign full access to records or limit it to a specific level. The system enables assigning subscribers or sets to one of 8 levels (**PBX features->Call recording->Access levels**) When configuring recorded objects, set the level they belong to. Subsequently, in the application accounts, set what level they are going to have access to.

Add recording

Adding objects (numbers) who are allowed to record calls

Configuration details:

- **object type** - specify the object type (subscribers, set, operator)
- **type of calls to be recorded** - external or internal calls
- **access to records** - specify the level of access (full or indicated group)
- **begin recording** - specify the moment when recording is to start

Add blocking

Configure objects for which recording is prohibited. This means that calls with this object participating will not be recorded. This means that regardless whether the call is executed by an operator, rule or internal call with the recorded objects, the call will not be recorded

Configuration details:

- **object type** - specify the type of object (subscribers, set, operator) for which recording is to be prohibited.

10.4.2. Access to records - application settings

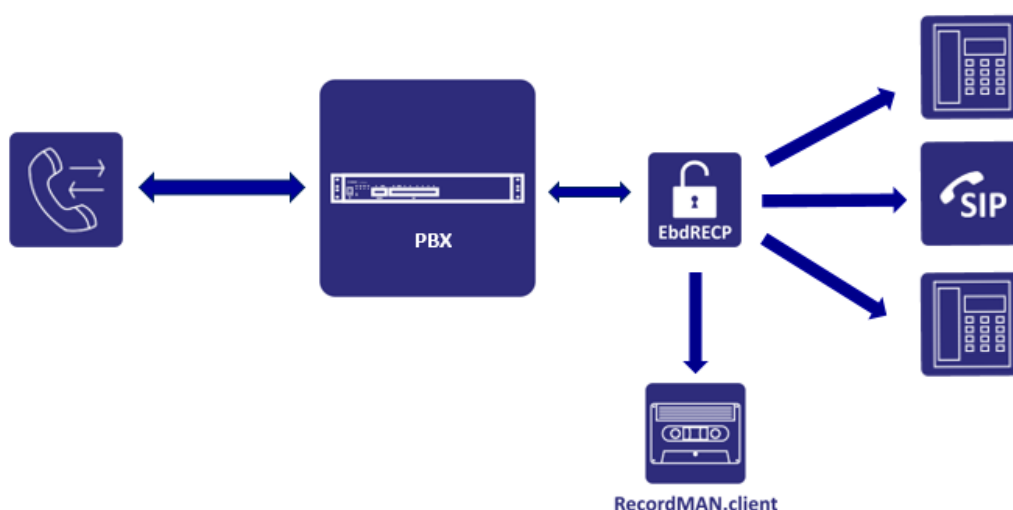
Access to records in the PBX is possible using dedicated external applications: *RecordMAN.client* or *RecordMAN.server* and the integrated EbdREC protocol (Slican proprietary). Access to records is also possible using any FTP client. For the *RecordMAN.client* application, any user can be assigned rights to play records at the given station (playback stations are subject to licensing).

RecordMAN.client is the basic application for handling records. After appropriate configuration, the application connects with the PBX or the computer where the given program is installed. RecordMAN.client only downloads a list of records in the form of daily folders. Only when commanded to play a record, individual files are downloaded to the hard drive and played. For security reasons, transmissions between application and PBX can be encrypted.

Configuration details

The *RecordMAN.client* application is configured in the section: *Exchange features->Call recording->Application accounts*. For correct authentication of the given account, set its login and access password. An additional element of account user authorisation is the hardware key of the RecordMAN.client software as a unique code for each computer where the application is installed (the **HardKey** parameter in application settings). Permission to copy files from the PBX is additionally configured by the PBX administrator. Another element is to set the level of access to records. By defining application users, each of them can be assigned rights to play records for the given group of numbers/sets, or full access to records. In such a case, indicate in the account settings which level the given account has access to (*Access to records->Access limitations*). Playback of records of the given internal line is possible when using an additional filter (*Internal line filter*). It is also possible to set time-limited access for each account, providing the playback ability for a specific number of days before. The latest application version is available [HERE](#).

A diagram of configuration of a system with the RecordMAN.client application:



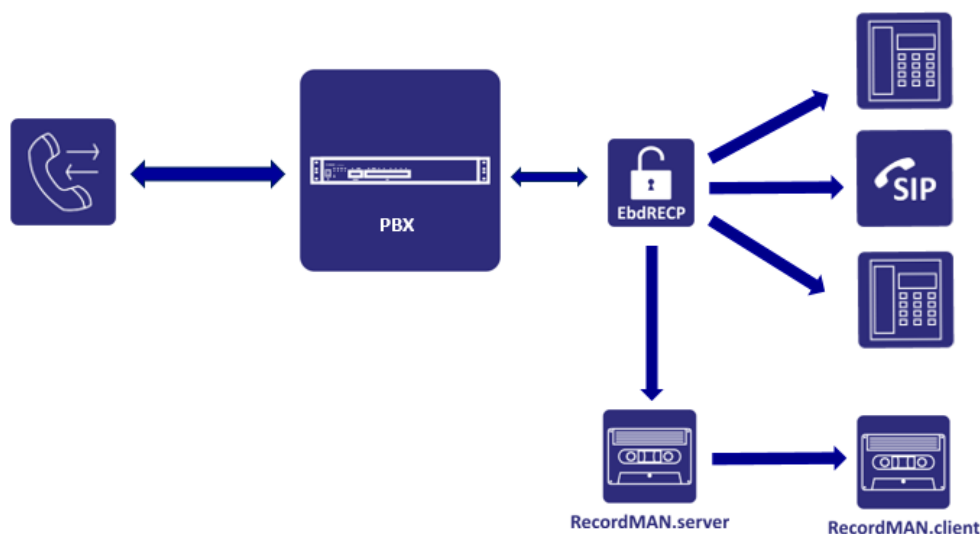
RecordMAN.server is a tool whose task is to download records from the carrier in the PBX and store them on the computer's hard drive, creating a full copy of the records. For security reasons, transmissions between application and PBX can be encrypted. Furthermore, *RecordMAN.server* can share recordings (also archived ones) with the *RecordMAN.client* application. Records are shared based on identification of rights granted to *RecordMAN.client* software users, so that changing their configuration in the PBX affects access both to records that are still in the PBX, and to archived records. In itself, the application has no ability to playback records.

Configuration details

Access to the RecordMAN.server application is configured in the section *Exchange features->Call recording->Access authentication*. The basic parameter in PBX configuration is the *Hardware key*, which

can be read in the relevant tab of application settings (the **HardKey** parameter). Records can also be stored in encrypted form. The latest application version is available [HERE](#).

A diagram of configuration of a system with the RecordMAN.server application:



FTP server, i.e. access using external applications. Access to records is protected by the permanent **recordman** login (cannot be changed) and FTP server password, which the PBX is. The password is configurable in the *Exchange features->Call recording->Access authentication* section. For security reasons, transmissions between the external application and PBX can be encrypted.

10.4.3. Settings - basic configuration

The system enables recording calls in two file formats:

- G.711(alaw) 64kb/s (default)
- GSM 13kb/s

Format selection depends on the amount of calls recorded. Files in GSM format take up less hard disk space, but are of inferior quality.

Additionally, you can also provide notification about call recording by configuring an announcement informing about the fact. Information about recorded calls is available for calls: outgoing, incoming and internal.

10.4.4. Access levels

The PBX enables using up to 8 levels of access to records. It is only possible to edit the names of individual levels.

NOTE

Call recording is subject to licensing. This applies both to recording channels and to access to RecordMAN.server and RecordMAN.client applications, as well as access using an FTP client.

10.5. Call billing

The NCP PBX enables specifying costs of calls using an independent billing settlement application - *BillingMAN*. Call recording options enable buffering PBX events or blocking their recording.

The PBX enables recording of the following events:

- answered/unanswered outgoing calls
- answered/unanswered incoming calls
- answered/unanswered internal calls
- services
- outgoing text messages

Configuration details

Recording settings

Call billing is configured in the section: **PBX features->Billing**. First, specify what kind of information about calls you want to record (in the **PBX features->Billing->Register settings** section).

BillingMAN application accounts

Next, define authentication data for the BillingMAN application, where you set login and password (section: **PBX features->Billing->BillingMAN accounts**).

Call rates

Next, set call rates (**PBX features->Billing->Call rates**) for individual prefixes specified in national or international format.

Subscriber limits

Another element is to set limits (**PBX features->Billing->Subscriber limits**) for individual internal numbers. Enter the limit type: monthly, manual, hotel, then specify its value. The PBX provides the current balance based on rates for individual numbers. The administrator can reset the balance at any time before the time specified in the limit type expires. By default, for SIP subscribers an amount of PLN 500 is set.

10.6. Text message support

When you expand the system with a GSM module, you receive a fully functional GSM gateway able to route calls and handle text messages. The integrated "Text message centre" manages text message routing in both incoming and outgoing traffic. Text message support using external applications is possible thanks to protocols (CTIP/XML) implemented in the PBX. Additionally, NCP-CM also works with the SenderSMS application for sending/receiving group text messages.

Text message configuration:

- **name** - text message service ID
- **text message handling** - select your text message handling type: Text Message Centre, external applications, SenderSMS
- **incoming message forwarding** - select an internal number to which SMS messages from the text message centre will be directed
- **add ports** - select GSM module and port installed in an NCP-GWS shelf

The PhoneCTI, SenderSMS and external applications require licences for sending text messages.

When the GSM gateway is configured to work with external applications, servicing notifications and messes about calls in the Mobilephone service are not supported.

10.7. Access control system

Direct link to the ACS application. Adding rights to application support can be found in the section *Accounts/Administrator accounts/Access rights*. A description of the ACS application functions can be found in another manual, available on the wiki.slican.pl website and from Servnet.

10.8. AudioMAN

Direct link to the AudioMAN application to support Slican Audio system devices. AudioMAN is a Web App designed to manage the integrated Slican audio system. It was created to separate the configuration functions of the NCP system and audio system management.

Authorizing rights to use the application is located in the *Accounts / Admins Accounts / Access rights section*.

From the application level, we can enter the options:

- **preview** - shows online operation of all audio zones with connected speakers.
- **settings** - allows you to change the music source, set the volume of individual zones, and set the music volume and announcement volume for each speaker.
- **announcements** - allows editing announcements that have rights to change audioman
- **music sources** - allows you to add and edit audio streams and playlists
- **Schedule** - allows you to add and edit music playback schedules for audio zones

10.9. CallCenterMAN

Direct link to the CallCenterMAN application. Application designed for agents managing the work and service of Call Center Queues. Granting permissions to operate the application is located in the *Accounts / Administrator Accounts / Access Permissions section*.

11. Media

11.1. MoH - Music on hold

“Music on hold” can be selected for waiting and parked calls and for queues. One default tune is available in the system. Depending on preferences, you can implement your own music. Supported file formats:

- Microsoft wave (*.wav)
- G.711(a-law) without wave header
- MPEG-2 Audio Layer III (*.mp3)

Files in your own collection are played at random from the beginning for each new call.

11.2. Announcements

Verbal announcements can be configured (assigned) to the entire system and individually to each user. The PBX as a default list of system announcements available, played depending on the context of the actions taken. By default, there are two language versions of announcements: Polish and English. The system allows you to generate additional announcements using the text2speech system, which will have the same voice as the other system announcements, and add / record your own announcements. Recording your own announcements using a phone is done by setting a given internal number from configuration. An internal filter enables selecting system and user announcements.

Adding your own announcements involves uploading your file with an announcement, or recording it with a phone. It is also possible to replace system announcements with your own.

The maximum number of custom announcements is **300**. Uploaded announcements share disk space with records.

Announcements from the PBX can be downloaded a *.wav of *.mp3 files.

Configuration details

- **name** - set the announcement name
- **select folder** - select a folder from the list or create a new one to assign your announcement to, then select the language version (PL/EN) and upload/record your file
- **exact words from recording or description of inarticulate sound** - transcript of the announcement
- **recording source** - upload file or record using the phone
- **recording file** - select the announcement file from your resources (*.wav, *.a-law, *.mp3)

NOTE

Announcement names containing multiple words should use underscores _ instead of spaces between words

11.2.1. Announcement upload procedure via sound manager

Below are the steps required to create your own announcement from a file or recorded with a phone.

The screenshot displays the 'Sound manager' interface. At the top, there's a 'Filter sounds' bar. Below it, the 'Sound manager' section includes 'Add sound' and 'Delete' buttons. A table lists sounds with columns: 'Time', 'Folder', 'Sound', and 'Script'. Below the table, the 'Add new sound' dialog is open, showing 'Name: DISA' and 'Choose folder: /test1'. Below this, the 'Modify sound' dialog is open, showing 'Language: en', 'Folder: /test1', 'Sound name: test_sound', and 'Sound id: /test1/test_sound'. The 'Sound source' dropdown is set to 'Upload file'. The 'Allowed audio file formats' section lists: Microsoft wave (*.wav), Raw G.711 (a-law) without wave header (*.alaw), and MPEG-2 Audio Layer III (*.mp3). The 'Sound file' section has a 'Wybierz plik' button and the text 'Nie wybrano pliku'.

For the purposes of verification, you can check your announcement by playing it on a selected internal number or download a file from the PBX.

11.2.2. Uploading announcements to queues

When uploading custom announcements for queue handling, remember that announcements with additional information about position in the queue should include the following parts:

- first in queue, e.g. ***All lines are busy, your call is in position one***
- position in queue, e.g. ***All lines are busy, your call is in position...***
- a numeral, e.g. ***two*** - replace the system announcement on numerals here
 - system announcements should be placed in the appropriate folder (for numerals, it is the folder: digits)
- on hold, e.g. ***...position...***
- thank you, e.g. ***...please call later or wait for operator to sign in***

11.2.3. Uploading announcements using Text2speech

In PBX it is possible to generate announcements from a text form using the text2speech service. The advantage of this form of announcement is their compatibility with other system announcements. The Text2speech service is a paid service and you must buy an announcement package to use it. Packages of 100 and 1000 announcements are available. The service together with the purchased package is active for a period of 1 year. After this period, the service is deactivated and the available generation quantities are reset. If any announcement package is purchased before the end of the 1 year period, the service activity period is extended for the next 12 months from the date of purchase of a new package for all previously purchased and unused announcements. When purchasing a license to update the firmware, we get the opportunity to generate 10 announcements for use for a period of 1 year. In Configweb, after entering the / Media / Text2speech option, we obtain information about the purchased license packages and the quantity and expiry date of the remaining announcements. To generate an announcement in the Text2speech system, we enter the edition of the announcement we are interested in and in the Script window, enter the exact content of the announcement being prepared, remembering that it should be recorded "phonetically", i.e. how it should sound. Then press the Text2speech button and confirm. After confirmation, the announcement will be generated and the number of remaining available generations will be reduced. It should be remembered that the very act of generating an announcement is important, and not e.g. downloading an announcement. Each subsequent attempt reduces the number of available generations. To use the Text2speech service, you must have PBX Internet access.

12. Diagnostics

A set of useful tools concerning current PBX statistics, i.e.: PBX type, firmware version, system clock, hardware statistics, system logs. Useful for assessing any potential issues and analysing traffic using logs.

12.1. Summary information

Collective information is main information of a working system, collected in a table. The table contains PBX data: notifications, hardware statistics, information on numbers of internal equipment modules and numbers of linked exchanges, as well as licences held.

12.2. System alarm

In the option you can see system alarms and descriptions of actions to be taken to eliminate them, as well as links to the configuration of alarming elements.

12.3. Connection Monitor

A comprehensive call screen, divided into:

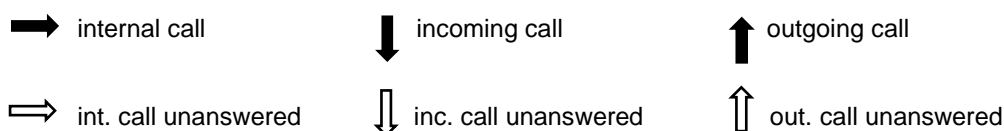
- active calls with statistics: calls answered, on hold, longest

- calls finished: with detailed information on the call flow

The list of active calls in live view is refreshed every 2 seconds.

When a call is routed, for example, to a group or queue, or is transferred, then the record of such an event is more complex and marked with an identifier. Clicking individual identifiers (e.g. [#1](#)) expands individual components of the given call record. Components of complex records enable you to follow the call flow. Each record is additionally marked with an icon indicating the call type, duration and reason for ending.

Call type key:



Call duration key:



The maximum number of visible records is 100 (including complex ones).

In ongoing and terminated connections, the "More" link is visible, under which information about the course of a given connection is hidden, by which traffic, presentation and authorization rules have been combined, or if there were no rules, which rules blocked them.

12.4. Status

A menu in the form of tabs with information on equipment status broken down into:

12.4.1. Providers

VoIP operators

- **type** - protocol type: SIP, ESSL
- **name** - of the configured VoIP translation
- **user** - VoIP/eSSL account name
- **address** - of the VoIP server
- **dynamic** - host type (dynamic IP address)
- **NAT** - routing information
- **secure** - signalling encryption settings (SIP, RTP)
- **latency** - time of server (VoIP) response to client side query
- **connection status** - information about registering and monitoring
- **registration status** - information about registration status
- **device status** - information about line load

TDM operators

- **port** - physical port number
- **port type** - type of TDM module (ISDN, GSM)
- **TDM operator** - assigned TDM operator name
- **port status** - current information about physical status of the port (e.g. in ISDN, information about layer status)
- **device status** - information about device load

12.4.2. Extensions

SIP extensions status

- **type** - protocol type: SIP
- **internal** - assigned internal number
- **name** - description of internal number
- **address** - of the registered VoIP device
- **dynamic** - host type (dynamic IP address)
- **NAT** - routing information
- **secure** - signalling encryption settings (SIP, RTP)
- **latency** - time of server (VoIP) response to client side query
- **connection status** - information about registering and monitoring
- **device status** - information about device load
- **client** - type of registered terminal (information sent in the UAC field of SIP signalling)

Phone extensions status

- **port** - physical port number
- **port type** - equipment type (CTS, CTS.IP, FXS)
- **internal** - assigned internal number
- **name** - number description
- **port status** - current information on physical port status (for digital ports, additional information about the terminal)
- **device status** - information about device load

eSSL internal numbers

- **eSSL device** - name of the connected eSSL server
- **type** - type of synchronised equipment (CTS, CTS.IP, FXS, SIP)
- **internal** - assigned internal eSSL subscriber number
- **name** - number description
- **device status** - information about device load

Virtual extensions status

- **internal** - assigned internal number
- **name** - number description
- **device** - indicates the type of device on which the account is logged in
- **device status** - information about device load
- **other services** - information about enabled services

In this option, by clicking on the restart link, we force the reset of a given PBX port and for sip phones we have the option of clicking on the configuration link to connect to the phone and launch the phone's web interface.

12.4.3. Services

A view of services active on internal numbers or sets. A built-in filter enables selecting services from a drop-down list showing their status.

12.4.4. CTI applications

Viewing the status of MessengerCTI.Desktop and MessengerCTI.Mobile applications and access to the application system log.

Application Status

- **type** - port type
- **extension** - assigned extension number
- **name** - description of internal number
- **condition** - subscriber status - free, busy, damaged
- **applications name** - application name
- **applications** - application login status
- **IP address** - the IP address from which the application is or was logged in
- **restart** - allows you to restart the port
- **event logs** - view the system log with events related to a given application port

12.5. Logs

Logs are a record of PBX events grouped into categories. An additional filter provides the ability to view events selectively.

12.5.1. Calls log

The call log is nothing else than a billing record of calls, broken down into incoming, outgoing and internal traffic.

Simple view

Basic call information with data on:

- dialled number
- calling number
- duration

Advanced view

In this view, the scope of information is expanded with additional data:

- call duration
- waiting time
- operator of origin
- dialled number
- number reached
- destination number
- disconnect type

The PBX enables this data to be exported to a formatted **.csv** file.

From version 1.12, access to statistics of Call Center queue agents has been moved to the CallCenterMAN application

12.5.2. SMS log

Information about text messages sent from the PBX, with data on: sender, recipient and operator. This data can also be exported to a **.csv** file.

12.5.3. Service states log

Information concerning services executed, including: date, internal number, event, status, source.

12.5.4. Event logs

The tab stores the logs of events occurring in the control panel, which enable the system diagnostics to be performed

Notification

System notifications concerning: reboots, module alarms, network or power supply failures. Ability to filter notifications, broken down into categories and filtered by event date.

System

System logs contain information concerning, for example:

- SIP account registration
- eSSL message
- handling incoming/outgoing traffic
- services executed

Detailed

The tab stores detailed logs related to making connections and system operation.

12.6. Statistics

Visualization of call statistics and IVR hotline reports.

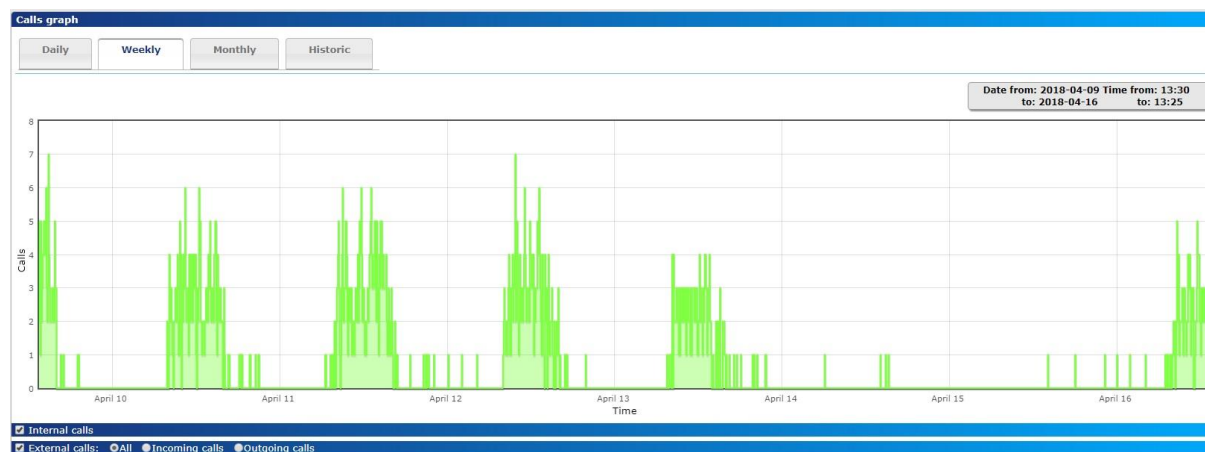
12.6.1. IVR statistics

The report includes statistics of calls going through the IVR helplines, where the percentage and quantity of customer choices at different levels of the helpline and the dialed extensions are shown

IVR report							
		From: 2020-09-08		To: 2020-10-08			
IVR	Number of connections	Dialed digits			Dialed extensions	No dialed	Abandoned
		Digit	Directed to	Quantity			
6663 IVR_Serwis	178	7	None	1	0 (0%)	173 (97%)	5 (3%)
6670 tryb_DWT spotkanie	31				0 (0%)	0 (0%)	30 (97%)
6660 IVR_Infolinia główna	223	4	6661 IVR_Książka_telefoniczna	84 (38%)	0 (0%)	41 (18%)	46 (21%)
		0	6647 Kolejka Sekret + Market	39 (17%)			
		5	6661 IVR_Książka_telefoniczna	10 (4%)			
		3	178 Szczeszak-Kielpińska Magda	2 (1%)			
		9	213 Fax Sekretariat	1 (0%)			
6661 IVR_Książka_telefoniczna	155	7	6662 IVR_DWT_API	59 (38%)	0 (0%)	6 (4%)	10 (6%)
		3	131 Handel Cykliczna	30 (19%)			
		0	6647 Kolejka Sekret + Market	21 (14%)			
		5	6663 IVR_Serwis	15 (10%)			
		4	114 Grupa Marketing	9 (6%)			
		6	116 Zaopatrzenie	5 (3%)			
		*	None	2			
		1	None	1			
		8	None	1			

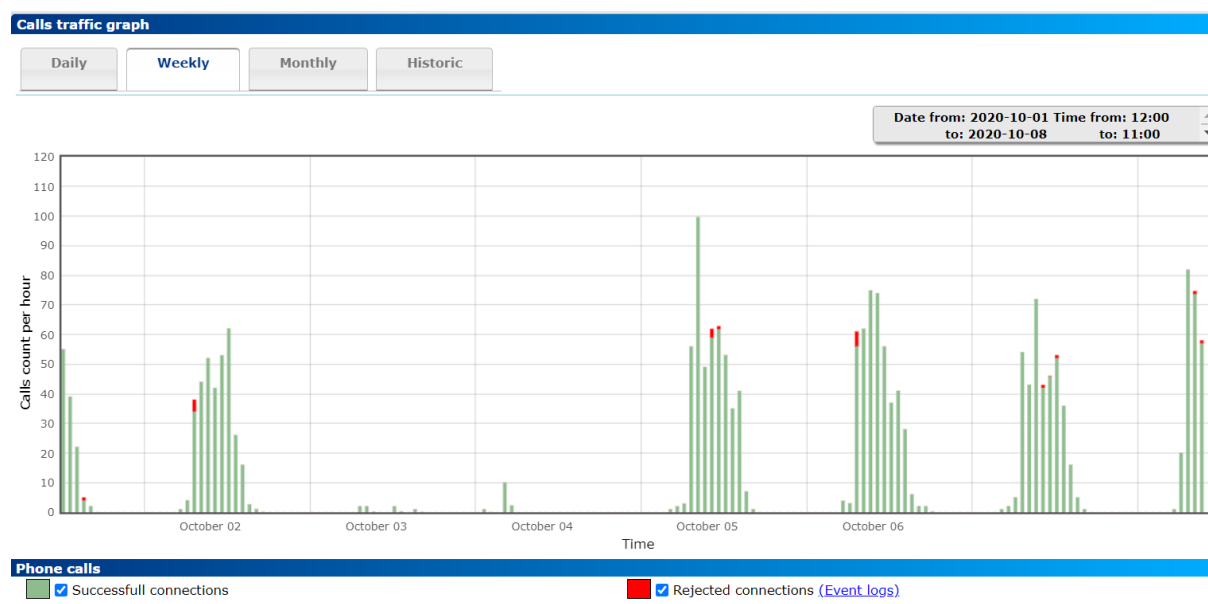
12.6.2 Calls statistics graph

Graph of simultaneous connections (outgoing/incoming/internal) in graphical form with time distribution: daily, weekly, monthly, historical. An additional filter provides the ability to accurately specify the time period of interest.



12.6.3 Calls Traffic graph

Graph of telephone traffic measured in the number of calls handled / rejected by the exchange per hour (BHCA) (outgoing / incoming / internal) in a graphical form with a time division: daily, weekly, monthly, historical and with the separation of answered and rejected calls. An additional filter that allows you to accurately determine the time period you are interested in.



After clicking the Event Logs link with rejected connections, we will be transferred to the system log, with filtered information about the reasons for the disconnection.

12.7. Tools

The tab provides access to tools enabling control panel operation, network traffic and ISDN signaling dumps, and access to console commands.

12.7.1. Calls simulator

An integrated test call simulator for inspecting whether outgoing calls function properly. Select a specific internal number and indicate the destination number (to be called). Then choose the number of calls to be generated and the duration of the test and the type of action to answer the call: echo test, music playback. The simulator can also be used to check the behavior of other PBXs for higher inbound traffic.



12.8. Network traffic analysis

A tool for network packet capturing for deeper analysis in the event of issues concerning VoIP-based traffic in particular.

Select the interface on which you want to capture network traffic and set the appropriate protocol filter.

VoIP (signalingacoustics) or Slican(XML, HotelIP), and additionally address (IP, MAC). The captured traffic will be saved in a *.pcap file. The maximum file size is 100 MB and after it is reached, older records will be deleted and replaced with new ones. Files can be opened using popular network analysers: **Wireshark** or **Tcpdump**.

Network traffic analyzer	
Network traffic will be written to *.pcap format file. It can be opened with applications like Wireshark or Tcpdump. Maximum size of file is 100MB and if this size will be reached oldest records will be replaced by new ones.	
Network interface	
Interface:	LAN ▾
Protocol filter	
All network traffic:	<input type="checkbox"/>
VoIP signaling (SIP, DNS, ICMP, eSSLv2, CTS.IP):	<input checked="" type="checkbox"/>
VoIP audio (RTP, ICMP):	<input type="checkbox"/>
Slican (XML, HOTELP, CTIP, HTTP, WebAPI, ICMP):	<input checked="" type="checkbox"/>
Address filter	
Address type:	Any address ▾
Address:	<input type="text"/>
Capture network traffic	
<input type="button" value="Start"/>	
Recorded network traffic file	
File name:	LAN.sip.dump.pcap
File size:	91912 KB
Last modification:	2020-10-08 08:00:28
<input type="button" value="Download"/> <input type="button" value="Delete"/>	

12.7.3 ISDN analyzer

The built-in analyzer allows you to dump ISDN signaling logs. After entering the option, we have the option to start the logs with the start button - then the collection of signaling logs on all ISDN ports begins. After stopping, we can download logs from individual ports, or a log containing all signaling.

ISDN analyzer		
Capture ISDN traffic:		<input type="button" value="Start"/>
Recorded ISDN traffic files		
		<input type="button" value="Download all"/>
		Last modification
ISDNLogAll.txt (0.15 KB)	Download	Today, 12:16:38
ISDNLog_1-17.txt (0.15 KB)	Download	Today, 12:16:38
ISDNLog_1-18.txt (0.15 KB)	Download	Today, 12:16:38
ISDNLog_1-21.txt (0.91 KB)	Download	Today, 12:16:38

12.7.4. Console commands

The system console contains a set of practical tools, settings, and network monitoring mechanisms, i.e.:

- ping (network connection diagnostics)
- traceroute (packet route inspection in IP networks)
- ifconfig (network interface configuration)
- route (routing table)
- nslookup (manual execution of DNS queries)
- arp (hardware address table)
- sipping (SIP terminal connection diagnostics)
- dhcpd.leases (information on addresses assigned to GW shelves in INT network)

Console commands	
Command	sipping
SIPping	
Hostname or IP address:	sip.foneo.pl
<input type="button" value="Start"/>	
<pre> Reply from sip.foneo.pl (Kamailio (1.4.4-notls (i386/linux))) in 9.3ms Reply from sip.foneo.pl (Kamailio (1.4.4-notls (i386/linux))) in 7.9ms Reply from sip.foneo.pl (Kamailio (1.4.4-notls (i386/linux))) in 8.7ms Reply from sip.foneo.pl (Kamailio (1.4.4-notls (i386/linux))) in 8.8ms 4 packets transmitted, 4 packets received, 0% packet loss </pre>	

ADDITIONAL INFORMATION

Visit our website: wiki.slican.pl for current information on the latest software versions, additional functions, configuration examples and news on upcoming products.

You can find information on our other products at <http://www.slican.com>. If you have purchased our products through an authorised dealer, contact the dealer directly for immediate support in the event of issues.

Our technical support personnel is trained and ready to answer any questions you may have. To contact Slican technical support, send a report to the e-mail address: support@slican.pl

THE MANUFACTURER RESERVES THE RIGHT TO
MODIFY THE PRODUCT WITHOUT PRIOR NOTICE.



www.slican.com