



Office IP PBXs

SMG-200

SMG-500

Operation Manual

Firmware version: 3.14.0

SMG-200 firmware version: V. 3.14.0			
SIP adapter version: 3.14.0			
Document version	Firmware version	Issue date	Revisions
Version 2.1	V.3.14.0	07/12/2018	<p>Added:</p> <ul style="list-style-type: none"> - VAS: 'Conference with sequential collection' - VAS: 'Do not disturb' - VAS: 'Black list' - Public IP support; - STUN support; - FXS port emergency locks; - The access point detection - Disabling the FXS port; - Battery status indication; - NAT comedia support; - Group editing of FXS-/FXO ports; - Automatic detection of type and version of FXS/FXO submodules; - Monitoring the total number of calls; - Voice gain control for receiving/transferring on FXS ports; - Web/telnet/SSH user authorization via RADIUS; - Transmitting the received SIP header X-UniqueTag or forming it from the RADIUS Acct-Session-Id; - SNMP OID of SIP trunk availability; - The possibility of enabling call traces by the trunk group or the telephone number; - Transmission of the Connected Name for SIP subscribers - Device-side ring-off mark in CDR; <p>Changed:</p> <ul style="list-style-type: none"> - Queue limit from 5-30 to 1-30 participants.
Version 2.0	V.3.14.0	12/11/2018	<p>Changed:</p> <ul style="list-style-type: none"> 1.5 Main Specifications 1.7 Light indication 3.1.24 Control Menu 3.3 SMG Configuration via Telnet, SSH, or RS-232 3.3.1 List of CLI commands <p>Added:</p> <ul style="list-style-type: none"> 3.1.5.2.1 "Name delivery settings" tab 3.1.5.2.2 "Channel usage" tab 3.1.17.4 PRI subscribers
Version 1.1	V.3.11.2	31/05/2018	<p>Changed:</p> <ul style="list-style-type: none"> 3.1.2.9 Active Calls Monitoring 3.1.7.1 Trunk Groups <p>Added:</p> <ul style="list-style-type: none"> 3.1.2.3 E1 stream monitoring (for SMG-500 only) 3.1.2.4 E1 channel monitoring (for SMG-500 only) 3.1.3 Synchronization source (for SMG-500 only) 3.1.5 E1 Streams(for SMG-500 only) 3.1.7.2 SS7 link sets (for SMG-500 only)
Version 1.0	V.3.11.1	16/04/2018	<p>Changed:</p> <ul style="list-style-type: none"> 3.1.1 System Specifications 3.1.5.2 SIP/SIP-T/SIP-I Interfaces, SIP Profiles

			Added: 3.1.2.7 Monitoring Active Calls 3.1.5.3 H323 Interfaces 3.1.6.5 FXO Profiles Appendix B. Calculation of the Telephone Line Length
Version 1.0	V.3.11.0	12/02/2018	First issue

EXPLANATION OF THE SYMBOLS USED

Symbol	Description
Calibri	Notes, warnings, chapter headings, titles, and table titles are written in bold.
<i>Calibri</i>	Italic denotes important information that requires special attention.
Courier New	Courier New is used for command entry examples, command execution results, and program output data.
<KEY>	Keyboard keys are written in upper-case and enclosed in angle brackets.

NOTES AND WARNINGS



Notes contain important information, tips, or recommendations on device operation and setup.



Warnings inform users about hazardous conditions, which may cause injuries or device damage and may lead to the device malfunctioning or data loss.

TARGET AUDIENCE

This operation manual is intended for technical personnel in charge of gateway configuration and monitoring using the web configurator, as well as of installation and maintenance. Qualified technical personnel should be familiar with the operation basics of the TCP/IP & UDP/IP protocol stacks and Ethernet networks design concepts.

TABLE OF CONTENTS

EXPLANATION OF THE SYMBOLS USED	4
NOTES AND WARNINGS.....	4
TARGET AUDIENCE.....	5
INTRODUCTION.....	8
1 DEVICE DESCRIPTION	9
1.1 Application	9
1.2 SMG Main Specifications	9
1.3 Typical Applications.....	11
1.4 Device Design and Operating Principle	12
1.4.1 SMG-200 Design	12
1.4.2 Structure of SMG-500.....	13
1.4.3 SMG-200 Operating Principle.....	14
1.4.4 SMG-500 Operating Principle.....	14
1.5 Main Specifications	15
1.6 Design.....	17
1.7 LED Indication	18
1.8 The <i>F</i> Function Button.....	19
1.8.1 LED Indication During Device Startup and Reset to Factory Defaults.....	19
1.9 Saving Factory Configuration	20
1.10 Password Recovery	20
1.10.1 CLI Password Recovery.....	20
1.10.2 WEB password recovery.....	21
1.11 Delivery Package	22
1.12 Safety Instructions	22
1.12.1 General Guidelines	22
1.12.2 Electrical Safety Requirements	22
1.12.3 Electrostatic Discharge Safety Measures	23
1.13 Installation.....	23
1.13.1 Startup Procedure	23
1.13.2 Support Brackets Mounting	24
1.13.3 Device Rack Installation	24
1.13.4 Opening the Case	25
1.13.5 Installation of Submodules.....	26
1.13.6 RTC Battery Replacement	27
1.13.7 Accumulator battery connection	28
2 GENERAL GUIDELINES FOR GATEWAY OPERATION.....	30
3 DEVICE CONFIGURATION.....	31
3.1 SMG Configuration via Web Configurator	31
3.1.1 System settings.....	34
3.1.2 Monitoring.....	37
3.1.3 Synchronization source	49
3.1.4 CDR	50
3.1.5 E1 streams (for SMG-500 only)	59
3.1.6 Numbering Schedule	65
3.1.7 Routing	73
3.1.8 Internal Resources.....	105
3.1.9 IVR	126
3.1.10 TCP/IP Settings	135
3.1.11 Network Services.....	138
3.1.12 Security.....	143
3.1.13 Network Utilities	151
3.1.14 RADIUS Configuration	154

3.1.15	Tracing	165
3.1.16	Conversation Recording	173
3.1.17	Subscribers	182
3.1.18	Working with Objects and the Objects Menu	206
3.1.19	Saving Configuration and the Service Menu	206
3.1.20	Date and Time Settings	207
3.1.21	Firmware Update via Web Configurator	207
3.1.22	Licenses	207
3.1.23	Help Menu	207
3.1.24	Password Configuration for Web Configurator Access	208
3.1.25	View Factory Settings and System Information	209
3.1.26	Configurator Exit	209
3.2	Command Line, List of Supported Commands and Keys	209
3.2.1	Tracing Commands Available Through the Debug Port	211
3.3	SMG Configuration via Telnet, SSH, or RS-232	212
3.3.1	List of CLI Commands	212
3.3.2	Changing Device Access Password via CLI	214
	APPENDIX A. CABLE CONTACT PIN ASSIGNMENT	215
	APPENDIX B. ALTERNATIVE FIRMWARE UPDATE METHOD	216
	APPENDIX C. CALCULATION OF TELEPHONE LINE LENGTH	218
	APPENDIX D. TRANSMISSION OF VAS SETTINGS FROM THE RADIUS SERVER FOR DYNAMIC SUBSCRIBERS	220
	APPENDIX F. CORRELATION BETWEEN ROUTING, SUBSCRIBERS, AND SIGNAL LINK PARAMETERS	222
	APPENDIX G. GUIDELINES FOR SMG OPERATION IN A PUBLIC NETWORK	223
	APPENDIX H. VOICE MESSAGES AND MUSIC ON HOLD (MOH)	224
	APPENDIX K. WORKING WITH VAS SERVICES	225
	APPENDIX L. RADIUS CALL MANAGEMENT SERVICE	234
	APPENDIX M. MANAGEMANT AND MONITORING VIA SNMP	239
	TECHNICAL SUPPORT	269

INTRODUCTION

Office IP SMG-200 and SMG-500 PBXs are designed to provide communication in small, medium and large enterprises.

SMG-200 and SMG-500 PBXs allow companies to connect remote offices into a single network and create remote workplaces, thus reducing the cost of long-distance and international communication. In case of office relocation, telephone numbers remain the same, which allows the company to always stay in touch with its customers.

A state-of-the-art hardware platform, support for G.711, G.729 audio codecs, functions of echo cancellation, silence detector, comfort noise generator, and traffic prioritization mechanisms ensure that office IP SMG-200 and SMG-500 PBXs provide high quality voice communication.

This operation manual details main features of SMG-200 and SMG-500. The document contains technical specifications of these devices and their components. Also, it provides an overview of software-based operation and maintenance procedures.

1 DEVICE DESCRIPTION

1.1 Application

Office IP SMG-200/SMG-500 PBXs are designed to provide telephone communication inside the enterprise.

Office IP SMG-200 PBX is designed for 100 SIP subscribers in its basic configuration and can be expanded up to 200 subscribers if respective software is purchased. The SMG-500 PBX is designed for 250 subscribers in the basic configuration, with possible extension up to 500 subscribers.

SMG-200

16 RJ-11 ports can be used to connect analogue telephones and/or PSTN subscriber lines from PBX. LAN ports provide connection to Telecom operators networks via SIP trunks, as well as to VoIP gateways (for example, TAU-24 with 24 FXS ports), in order to increase the number of FXS/FXO ports.

SMG-500

PSTN connection can be made via E1 ports and SIP trunks. Analogue telephones can be connected to SMG-500 through the subscriber's VoIP gateways, while IP telephones – directly through the data network.

SMG-200/SMG-500 PBXs are able to store recorded conversations and CDR files to SD cards or USB drives. It is also possible to automatically upload files to external media or FTP server.

1.2 SMG Main Specifications

Interfaces:

SMG-200

- 16 x FXS/FXO (RJ-11) ports
- 4 x Ethernet 10/100/1000Base-T (RJ-45) ports
- 1 x USB2.0, 1 x USB3.0
- 1 x SD card slot
- 1 x COM port (RS-232, RJ-45)

SMG-500

- 4 x E1 (RJ-48) ports
- 4 x Ethernet 10/100/1000Base-T (RJ-45) ports
- 1 x USB2.0, 1 x USB3.0
- 1 x SD card slot
- 1 x COM port (RS-232, RJ-45)

Features:

- SMG-200: up to 100 subscribers in the basic configuration with possible extension up to 200 subscribers
- SMG-500: up to 250 subscribers in the basic configuration with possible extension up to 500 subscribers
- Static address and DHCP support
- IP telephony protocols: SIP, SIP-T, SIP-I, H.323
- DTMF transmission (SIP INFO, RFC2833, in-band, SIP NOTIFY)
- Echo cancellation (G.168 recommendation)
- Voice activity detector (VAD)
- Comfortable noise generator (CNG)
- NTP support
- DNS support
- SNMP support
- ToS and CoS for signalling
- VLAN for RTP signalling and management
- Firmware update: via the web configurator, CLI¹ (Telnet, SSH, console (RS-232))
- Configuration and setup (also remotely):
 - web configurator;
 - CLI¹ (Telnet, SSH, console (RS-232))
 - Remote monitoring:
 - web configurator
 - SNMP

SIP/SIP-T/SIP-I Functions

- RFC 2976 SIP INFO (for DTMF transmission);
- RFC 3204 MIME Media Types for ISUP and QSIG (ISUP support);
- RFC 3261 SIP;
- RFC 3262 Reliability of Provisional Responses in SIP (PRACK);
- RFC 3263 Locating SIP servers for DNS;
- RFC 3264 SDP Offer/Answer Model;
- RFC 3265 SIP Notify
- RFC 3311 SIP Update;
- RFC 3323 Privacy Header
- RFC 3325 P-Asserted-Identity
- RFC 3326 SIP Reason Header;
- RFC 3372 SIP for Telephones (SIP-T);
- RFC 3515 SIP REFER;
- RFC 3581 An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing;
- RFC 3665 Basic Call Flow Examples;
- RFC 3891 SIP Replaces Header;
- RFC 3892 SIP Referred-By Mechanism;
- RFC 4028 SIP Session Timer;
- RFC 4566 Session Description Protocol (SDP);
- RFC 5009 P-Header;
- RFC 5373 Requesting Answering Modes for the Session Initiation Protocol;
- RFC 5806 SIP Diversion Header;

¹ Not supported in the current firmware version 3.14.0

- RFC 6432;
- Q1912.5 SIP-I;
- SIP/SIP-T/SIP-I interaction;
- SIP Enable/Disable 302 Responses;
- Delay offer;
- SIP OPTIONS Keep-Alive (SIP Busy Out);
- SIP registrar.

1.3 Typical Applications

The SMG-200/SMG-500 PBXs are designed to register SIP subscribers and connect to a PSTN network via FXO port (SMG-200), or E1 stream (SMG-500), SIP-t/SIP-T/SIP-I trunk, or H. 323 protocol.

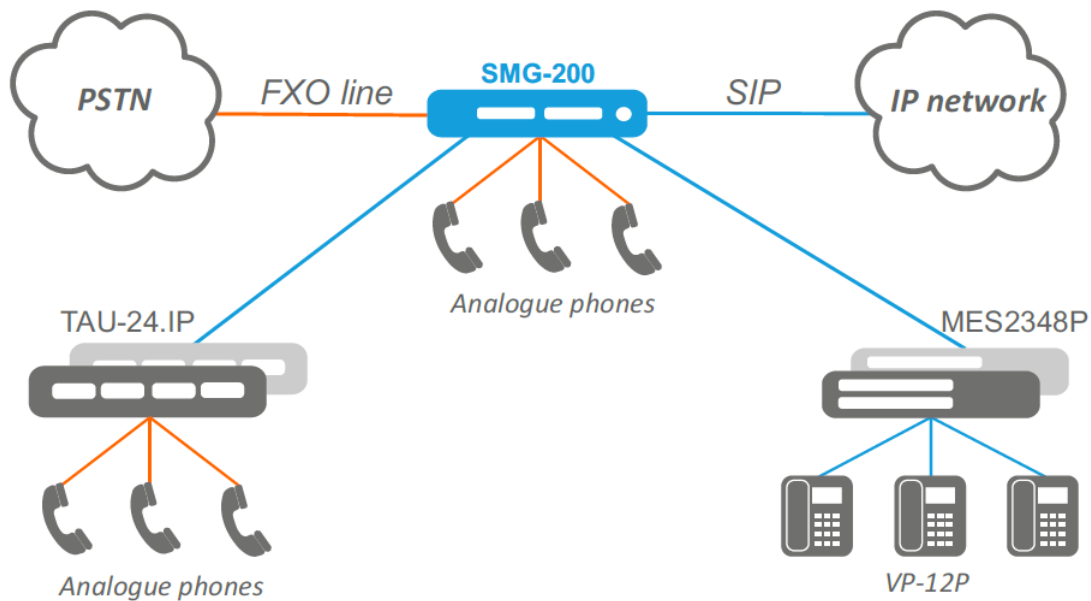


Fig. 1 – Office IP PBX based on SMG-200

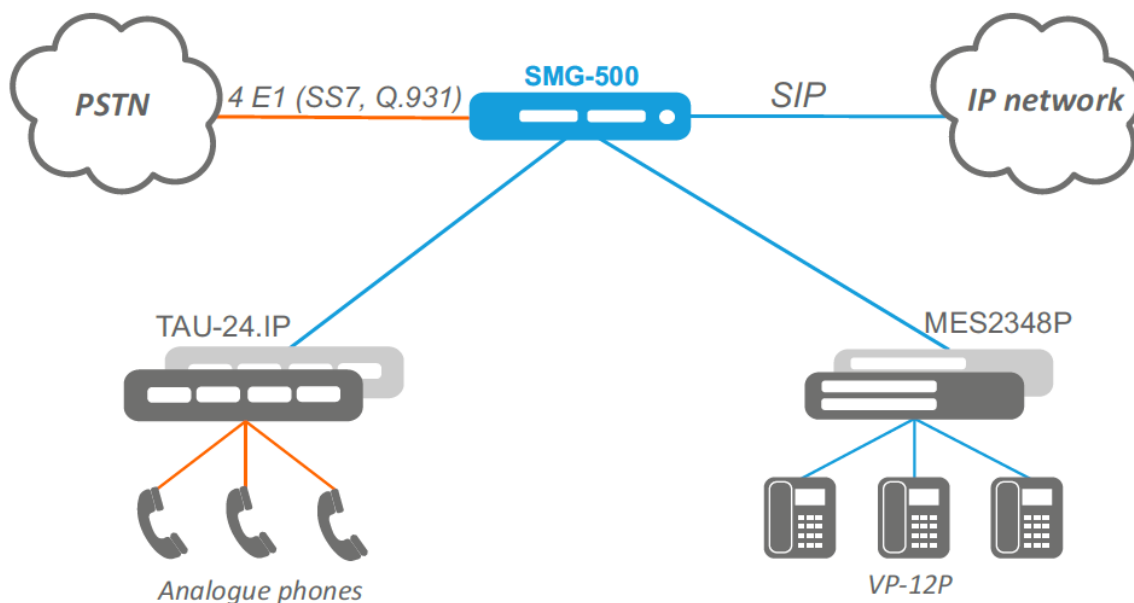


Fig. 2 – Office IP PBX based on SMG-500

1.4 Device Design and Operating Principle

1.4.1 SMG-200 Design

SMG-200 has a submodule architecture and contains the following elements:

- A controller featuring:
 - a controlling CPU,
 - 4 GB flash memory,
 - 2 GB RAM,
- up to 2 analogue FXS port submodules,
- up to 2 analogue FXO termination submodules,
- 4-port 10/100/1000BASE-T L2 Ethernet switch.

See the SMG-200 functional chart in Figure below.

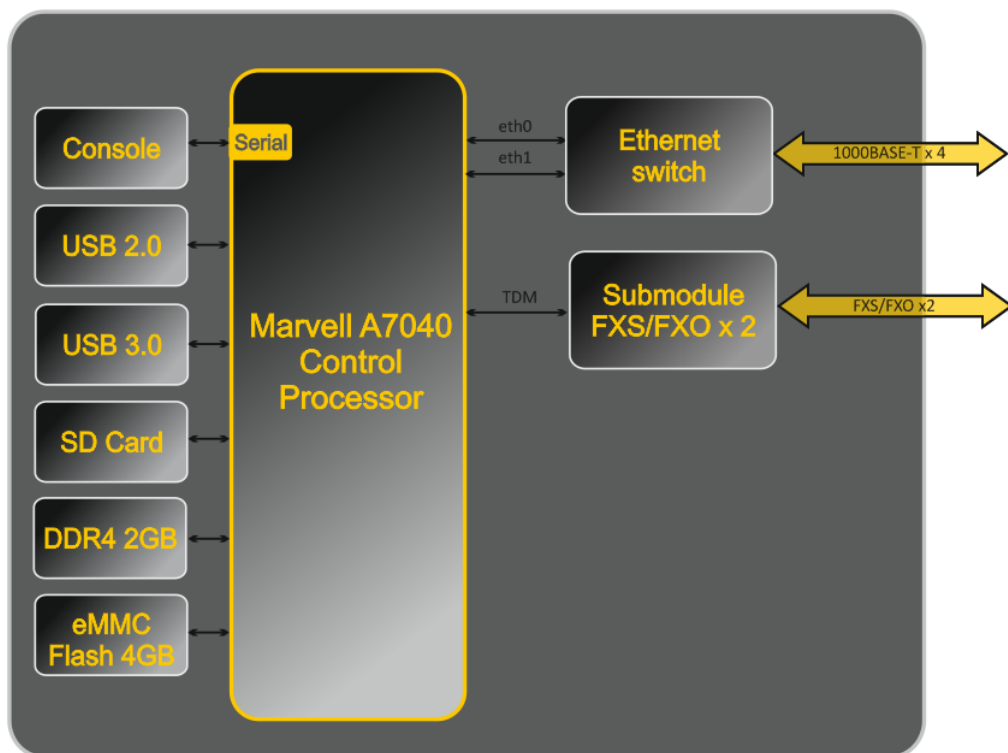


Fig. 3 – SMG-200 Functional Chart

1.4.2 Structure of SMG-500

SMG-500 has a submodule architecture and contains the following elements:

- A controller featuring:
 - a controlling CPU,
 - 4 GB flash memory,
 - 2 GB RAM,
- E1 stream submodule *C4E1*,
- IP submodule *SM-VP-M300*,
- 4-port 10/100/1000BASE-T L2 Ethernet switch.

Figure below shows SMG-500 functional chart.

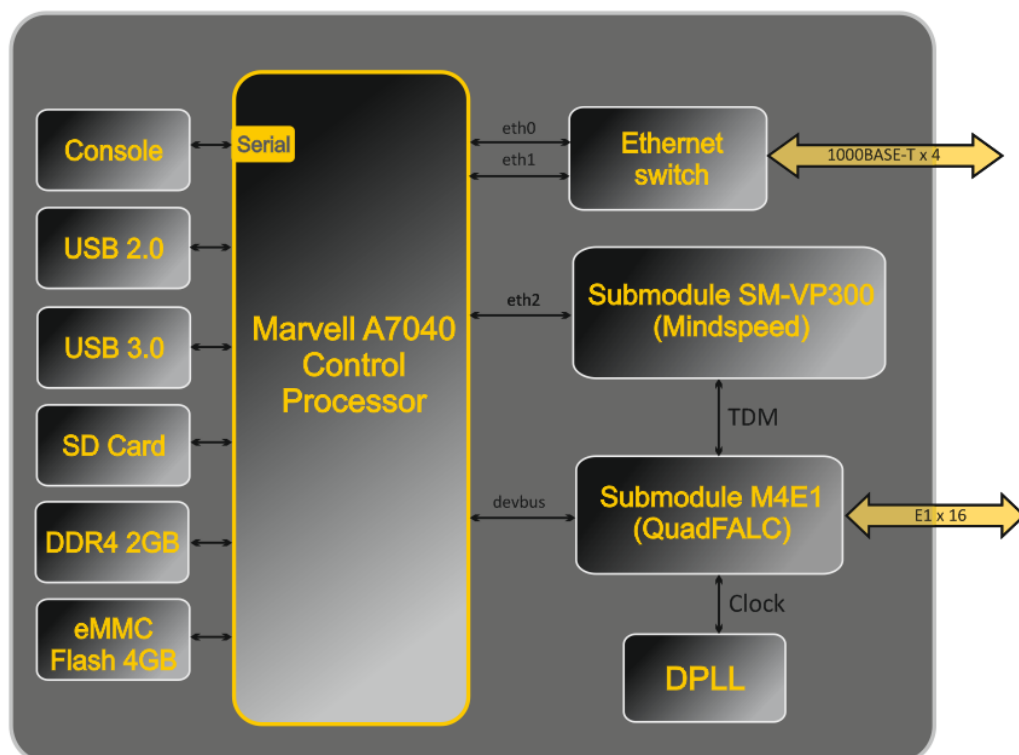


Fig. 4 – SMG-500 Functional Chart

1.4.3 SMG-200 Operating Principle

In the PSTN-to-IP direction, the signal from the FXS/FXO ports is sent for processing to the CPU through the internal TDM trunk, then encoded using one of the selected standards and transmitted in the form of digital packets to the Ethernet switch. In the IP-to-PSTN direction, digital packets from the Ethernet switch are sent for processing to the CPU, decoded, and transmitted over the internal TDM trunk to the FXS/FXO ports.

1.4.4 SMG-500 Operating Principle

In the PSTN-to-IP direction, the signal coming to the E1 streams is sent to the audio codecs of the VoIP submodules via the internal trunk, where it is encoded using one of the selected standards, sent in the form of digital packets to the CPU for processing, and then transmitted to the Ethernet switch. In the IP-to-PSTN direction, digital packets from the Ethernet switch are sent for processing to the CPU and further to the VoIP modules, decoded, and transmitted over the internal TDM trunk to the E1 streams.

External 2 Mbps E1 streams are transmitted to framers through matching transformers. At that, synchronisation signal is extracted from the stream and sent to the common synchronisation line of the device. Synchronisation line priority is managed at the software level according to the defined algorithm.

See Fig. 5 for the device firmware architecture.

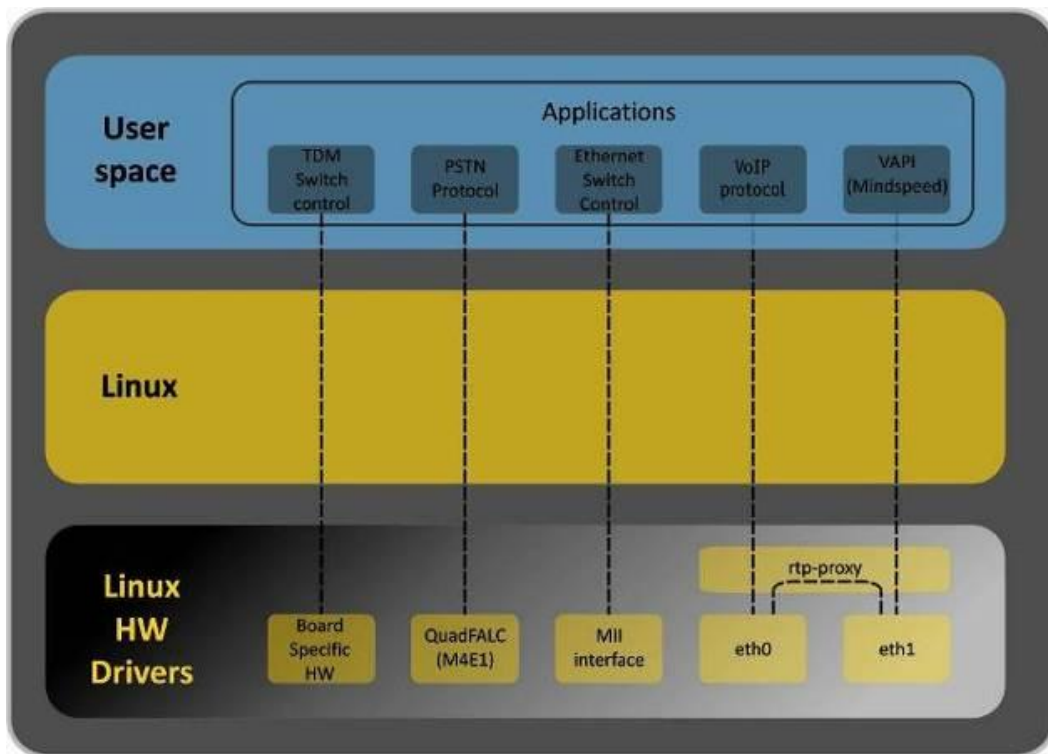


Fig. 5 – SMG firmware architecture

1.5 Main Specifications

Table below lists the main specifications of the system.

Table 1 – Main Specifications

VoIP Protocols

Supported protocols	SIP-T/SIP-I SIP H.323
---------------------	-----------------------------

Audio Codecs

Codecs	G.711 (A/U) G.729 (A/B) OPUS ¹ AMR ¹
--------	---


Electrical Ethernet Interface Specifications

No. of interfaces	4
Electric port	RJ-45
Data transfer rate, Mbps	Auto detection, 10/100/1000 Mbps, duplex
Supported standards	10/100/1000Base-T

Console Parameters

RS-232 serial port	
Data transfer rate, bps	115200
Electric signal parameters	Acc. to ITU-T V.28 guidelines

FXS interface parameters (only for SMG-200)

Number of ports	16
Loop resistance	Up to 3.4 k Ω
Dial support	Pulse dialling / DTMF
Caller ID	FSK (ITU-T V.23, Bell 202), DTMF, Russian Caller ID
Subscriber terminal protection	Current/voltage protection.  To protect the subscriber devices from overvoltage, the linear side of the distribution cross should be equipped with MKZ 3-K cross protection modules with 400 V pick-up voltage.
Possibility of remote measurement for subscriber line parameters	Yes
System parameters	Programmable

E1S interface parameters (only for SMG-500)

No. of channels	Acc. to ITU-T G.703 and G.704 guidelines
Line data transfer rate	2,048 Mbps
Line code	HDB3, AMI
Output signal to the line	3.0 V peak for 120 Ω load 2.37 V peak for 75 Ω load (acc. to CCITT G.703 guidelines)
Input signal from the line	From 0 to -6 dB in relation to the standard output impulse
Elastic buffer	2 frame capacity
Signalling protocols	ISDN PRI (Q.931), QSIG and CORNET to transmit user name, SS-7.

¹ Not supported in the current firmware version 3.14.0

General Parameters

Operating temperature range	0 to +40° C	
Relative humidity	Up to 80%	
Power voltage	AC: 220V+/-20%, 50 Hz Lead-acid battery 12V <ul style="list-style-type: none"> - Battery charge current – 1.6 + -0.1 A, - low battery voltage threshold indication – 11V, - threshold pick-up voltage for battery deep discharge protection – 10-10.5 V 	
Power consumption	Max. 40 W during battery charge, max. 20 W without battery charge	
Dimensions (W x H x D)	SMG-200	SMG-500
	430x43.6x203.2 mm	430x43.6x203.2 mm
Form-factor	19" form-factor, 1U size	

1.6 Design

The SMG-200/SMG-500 digital gateways have a metal case and can be installed in a 19" 1U rack mount.

The front panels of the devices are depicted in the figures below.

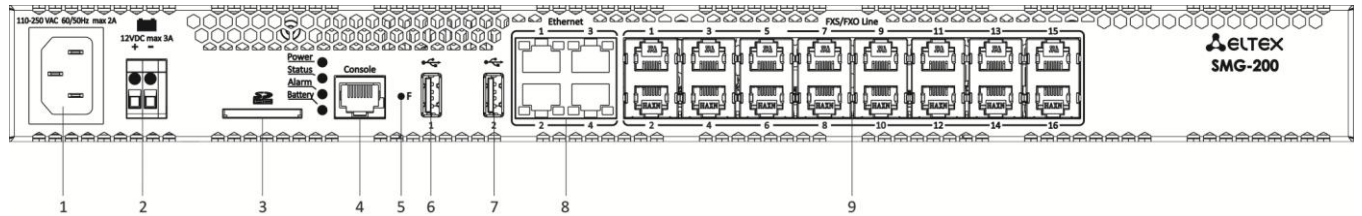


Fig. 6 – SMG-200 Front Panel

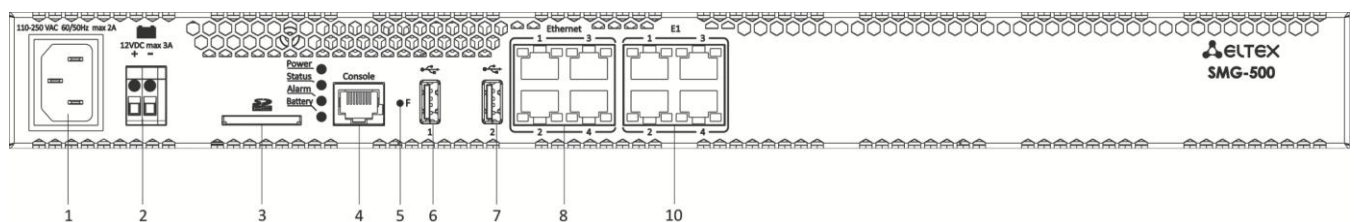


Fig. 7 – SMG-500 Front Panel

For ports, LEDs, and controls located on the front panels of the devices, see Table 2.

Table 2 – Description of Ports, LEDs, and Controls Located on the Front Panel

No.	Front Panel Element	Description
1	Power Connectors	Connector for 220 V power supply
2	Battery connector	Connector for accumulator battery
3	SD	SD card slot
4	Console	RS-232 console port for local device administration (for connector wiring, see Appendix A)
5	F	Function button
6	USB 1	USB 2.0 port for external storage device
7	USB 2	USB 3.0 port for external storage device
8	Ethernet 1..4	4 x RJ-45 ports for Ethernet 10/100/1000 Base-T interface
9	FXS/FXO Line	16 x RJ-11 ports for FXS/FXO line connection
10	E1	4 x RJ-48 ports for E1 streams

The device rear panel is depicted in Fig. 8

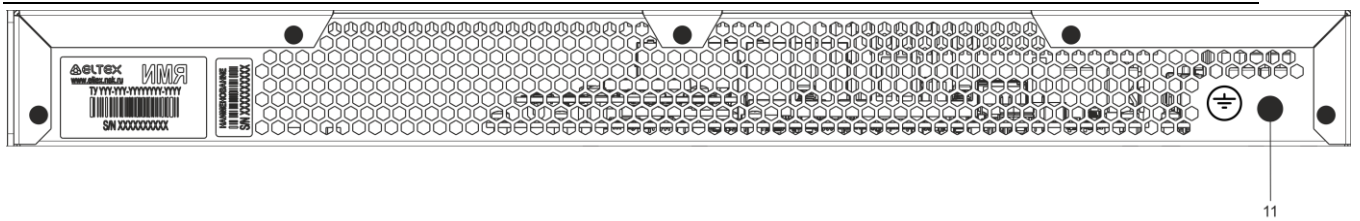



Fig. 8 – SMG-200/500 Rear Panel

Table below lists the rear panel connectors of the switch.

Table 3 – Description of Switch Rear Panel Connectors

No.	Rear Panel Element	Description
11	Earth bonding  point	Earth bonding point of the device.

1.7 LED Indication

The LED indicators located on the front panel show the current device status.

LED indication of the device in operation is described in Table below.

Table 4 – LED Indication of the Device Status in Operation

LED	LED Status	Device Status
<i>Power</i>	Off	Device power lost
	Solid green	Device power normal
	Solid red	Fault in the device power supply circuit
<i>Alarm</i>	Blinking red	Critical device failure
	Solid red	Non-critical device failure
	Solid green	No faults, normal operation. Non-critical problems may be present.
	Flashes green	Warning
<i>Status</i>	Solid green	Normal operation
	Off	Firmware error
<i>Battery</i>	Solid green	Battery is connected, proper operation
	Flashes green	Battery is charging
	Alternating red and green	Primary power supply is disabled, battery runs down
	Solid red	battery low
	Off	Battery is disabled
	Flashes red	Battery circuit-breaker failure

Ethernet interface status is also shown by LED indicators built in the 1000/100 connector, as described in the table below.

Table 5 – LED Indication for Ethernet 1000/100 Interfaces

Device Status	LED/Status	
	Yellow LED 1000/100	Green LED 1000/100
The port is in the 1000Base-T mode, no data transfer	Solid on	Solid on
The port is in the 1000Base-T mode, data transfer	Solid on	Blinking
The port is in the 10/100Base-TX mode, no data transfer	Off	Solid on
The port is in the 10/100Base-TX mode, data transfer	Off	Blinking

Table 6 – E1 stream state indication

Indication (time of LED blinking)		E1 stream states (ports 1-4, RJ-48)
Yellow	Green	
On	On	Status
Off	Off	E1 is disabled in gateway configuration
Flashes (200 ms)	Off	E1stream failure state
On	Off	Loss of Signal (LoS)
Flashes (200 ms) and lights off (1500 ms)	Off	AIS (Alarm Indication System) failure
Flashes (1500 ms)	Off	LOF (Loss of Signal) failur
Flashes (1500 ms)	Off	LOFM failure
Off	On	Normal operation of E1 stream
Flashes (200 ms)	Flashes (200 ms)	RAI failure
Flashes (300 ms)	Flashes (1500 ms)	E1 stream is in operation, the stream has SLIPs
On	Flashes (200 ms)	E1stream test is in progress

1.8 The F Function Button

The *F* button allows device reboot, restoration to factory configuration, and recovery of forgotten password.

For instructions on how to reset the operating device to factory defaults, see section 1.8.1, Table 7.

When the factory configuration is restored, the device can be accessed by IP address 192.168.1.2 (mask 255.255.255.0):

- via telnet or console: login: **admin**, password: **rootpasswd**;
- via the web-configurator: login: **admin**, password: **rootpasswd**.

After that, saving the factory configuration, restoring a password, or rebooting the device can be performed.

1.8.1 LED Indication During Device Startup and Reset to Factory Defaults

LED indication during the device startup and reset to factory defaults is described in Table below.

Table 7 – LED Indication During Device Startup and Reset to Factory Defaults

No	LED				Reset to Factory Defaults (Device Is On)
	Power	Status	Alarm	Battery	
1	Green	Red	Red	-	To reset the device, press the F button and hold it down until all the indicators light up as indicated to the left, then release the button.
2	Green	Off	Off	-	The boot process starts. Hold F pressed.
3	Green	Red	Red	-	Hold F until the indicators light up as indicated to the left.

					Release the F button.
4	Green	Green	Green	Green	Wait for the device to boot.

1.9 Saving Factory Configuration

To save the factory configuration:

- reset the device to the factory settings (section 1.8.1);
- connect via telnet or console, with **admin** as the user name and **rootpasswd** as the password;
- enter the **sh** command (the device changes CLI mode to SHELL mode);
- Enter the **save** command;
- Reboot the device with the **reboot** command.

The gateway will be restarted with the factory configuration.

```

*****
*           Welcome to SMG-200           *
*****

smg login: admin
Password: rootpasswd

*****
*           Welcome to SMG-200           *
*****

Welcome! It is Wed Mar 11 08:45:20 NOVT 2015
SMG> save
tar: removing leading '/' from member names
save: done
SMG> reboot yes

```

1.10 Password Recovery

1.10.1 CLI Password Recovery

To recover a password:

- reset the device to the factory settings (section 1.8.1);
- connect via Telnet, SSH or Console;
- enter the **sh** command (the device will change CLI mode to SHELL mode);
- enter the **restore** command (the current configuration will be restored);
- enter the **password** command (the device will prompt for the new password and its confirmation);
- Enter the **save** command;
- Reboot the device with the **reboot** command.

The gateway will be restarted with the current configuration and the new password.

If the device is rebooted without any additional operations, the current configuration will be restored on the device without password recovery. The gateway will be restarted with the current configuration and the old password.

```

*****
*           Welcome to SMG-200           *
*****

```

```

smg login: admin
Password: rootpasswd

*****
*           Welcome to SMG-200           *
*****
Welcome! It is Fri Jul  2 12:57:56 UTC 2010
SMG> restore
restore: successful
SMG> password
Changing password for admin
New password: 1q2w3e4r5t6y
Retype password: 1q2w3e4r5t6y
Password for admin changed by root
SMG> save
tar: removing leading '/' from member names
save: done
SMG> reboot yes

```

1.10.2 WEB password recovery

To recover a password:

- Reset the device to the factory settings (see section 1.8.10);
- Connect via Telnet, SSH, or Console;
- Enter the **sh** command (the device will change CLI mode to SHELL mode);
- Enter the **restore** command (the current configuration will be restored);
- Connect to the web interface via address 192.168.1.2;
- Go to the “User - Management” tab;
- Change password for *admin* user;
- Enter the **save** command in console;
- Reboot the device by the **reboot** command.



It is not recommended to save configuration from WEB interface. It may lead to loss of the saved gateway configuration. Use the *save* command from the SHELL mode.

The gateway will be restarted with the current configuration and new password.

If the device is rebooted without any further action, the current configuration will be restored without password recovery. The gateway will be restarted with the current configuration and an old password.

```

*****
*           Welcome to SMG-1016M        *
*****

smg login: admin
Password: rootpasswd

*****
*           Welcome to SMG-1016M        *
*****

Welcome! It is Fri Jul  2 12:57:56 UTC 2010
SMG> sh
/home/admin # restore
New image 1
Restored successful

```

You can change password via web interface on this step

```
/home/admin # save
tar: removing leading '/' from member names
*****
*****
***Saved successful
New image 0
Restored successful
# reboot
```

1.11 Delivery Package

The SMG-200/500 standard delivery package includes:

- Office IP SMG-200/SMG-500 PBX;
- Power cord;
- Operation Manual (provided on CD disc)
- Device Certificate.

1.12 Safety Instructions

1.12.1 General Guidelines

Any operations with the equipment should comply with the Safety Rules for Operation of Customers' Electrical Installations.



Operations with the equipment should be carried out only by personnel authorised in accordance with the safety requirements.

Before operating the device, all engineers should undergo special training.

The device should only be connected to properly functioning supplementary equipment.

The SMG-200/SMG-500 PBXs can be operated 24/7 provided the following requirements are met:

- Ambient temperature from 0 to +40°C.
- Relative humidity up to 80% at +25°C.
- Atmospheric pressure from 6.0×10^4 to 10.7×10^4 Pa (450–800 mm Hg).

The device should not be exposed to mechanical shock, vibration, smoke, dust, water, and chemicals.

To avoid components overheating, which may result in device malfunction, do not block air vents or place objects on the equipment.

1.12.2 Electrical Safety Requirements

Prior to connecting the device to a power source, ensure that its case is grounded with an earth bonding point. The earthing wire should be securely connected to the earth bonding point. The resistance between the earth bonding point and the earthing busbar should be less than 0.1 Ohm.

PC and measurement instruments shall be grounded prior to connection to the device. The potential difference between the equipment and instrument cases must not exceed 1 V.

Prior to turning the device on, check that all cables are undamaged and securely connected.

Make sure the device is off, when installing or removing the housing.

Submodules should be installed and removed only when the power is off, according to the instructions in section 1.13.4.

1.12.3 Electrostatic Discharge Safety Measures

In order to avoid failures caused by electrostatic discharge, we strongly recommend wearing a special belt, shoes or wrist strap to prevent electrostatic charge accumulation (if the wrist strap is used, make sure it fits tightly against the skin), and to ground the cord before operating the equipment.

1.13 Installation

Check the device for visible mechanical damage before installing and turning it on. In case of any damage, stop the installation, fill in the corresponding document, and contact your supplier.

The device should be installed on premises with access restricted only to service personnel.

If the device has been exposed to low temperatures for a long time before installation, leave it for 2 hours at ambient temperature prior to operation. If the device has been exposed to high humidity for a long time, leave it for at least 12 hours in normal conditions prior to turning it on.

Assemble the device. The device can be mounted on a 19" rack, using the mounting kit, or on a horizontal perforated shelf.

Once the device has been installed, its case must be earthed. This should be done prior to connecting the device to power supply. An insulated multiconductor wire should be used for earthing. The device grounding and the earthing wire section should comply with the Electric Installation Code. The earth bonding point is located in the lower right corner of the rear panel, Fig. 8.

1.13.1 Startup Procedure

1. Connect FXS/FXO lines (for SNG-200), E1 streams (for SMG 500) and Ethernet cables to corresponding gateway connectors.
2. Connect the power supply cable to the device.
3. If you plan to connect the computer to the SMG console port, connect the SMG console port to the PC COM port, and ensure the PC is turned off and grounded at the same point as the device.
4. Ensure that all cables are not damaged and securely connected.
5. Turn the device on and check the front panel LEDs to make sure the terminal is in normal operating conditions.

1.13.2 Support Brackets Mounting

The delivery package includes support brackets for rack installation and mounting screws to fix the device case on the brackets.

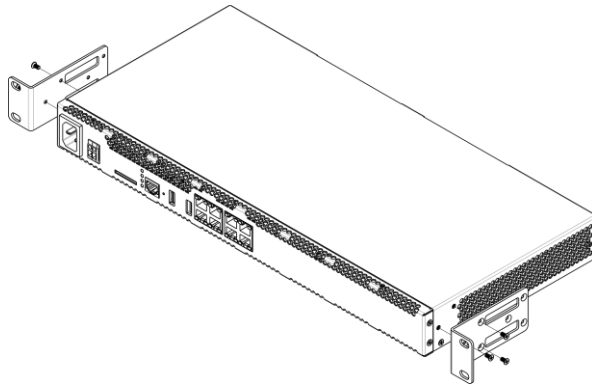


Fig. 9 – Support Brackets Mounting

To install the support brackets:

1. Align three mounting holes in the support bracket with the corresponding holes in the side panel of the device, Fig. 9.
2. Use a screwdriver to screw the support bracket to the case.

Repeat steps 1 and 2 for the second support bracket.

1.13.3 Device Rack Installation

To install the device to the rack:

1. Attach the device to the vertical guides of the rack.
2. Align mounting holes in the support bracket with the corresponding holes in the rack guides. Use the holes of the same level on both sides of the guides to ensure horizontal installation of the device.
3. Use a screwdriver to screw the device into the rack.

To remove the device, disconnect the connected cables and bracket screws from the rack, and remove the device from the rack.

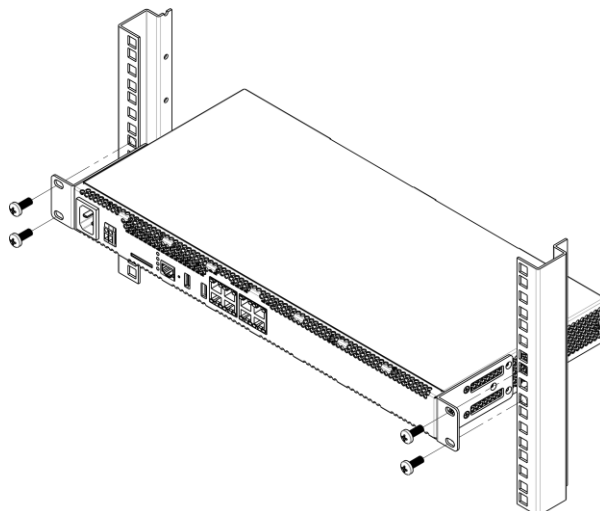


Fig. 10 – Device Rack Installation

1.13.4 Opening the Case

First, disconnect SMG from the power supply, disconnect all the cables and, if necessary, remove the device from the rack (see section 1.13.3).

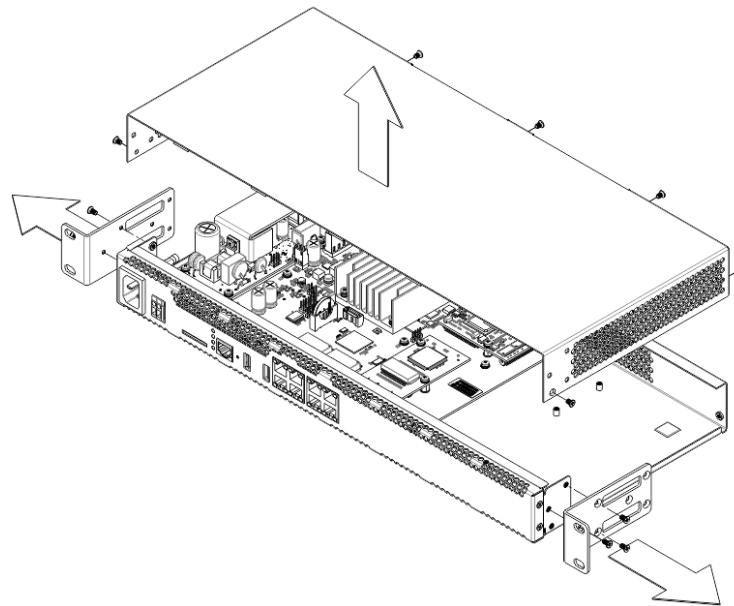


Fig. 11 – Opening the Case

1. Using a screwdriver, disconnect the brackets from the device case.
2. Unscrew the front panel locking screws, and then pull the front panel away from the top and side panels (Fig. 11).
3. Unscrew the screws on the top of the device.
4. Pull the top panel (cover) of the device to remove it.

To assemble the device, repeat all the steps above in the reverse order.

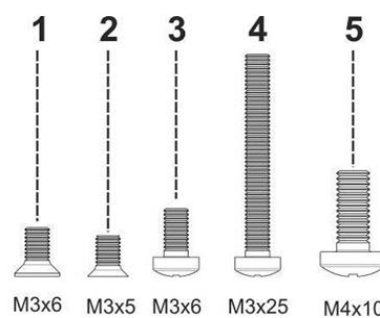


Fig. 12 – Types of Bolts for SMG Assembly

Fig. above shows the types of bolts used to assemble the device into the case:

1. Bracket mounting for rack installation.
2. Mounting of the case parts.
3. Mounting of the boards, ventilation units, plugs, guides.
4. Fan mounting screw.
5. Earthing screw.



When assembling the device, never use inappropriate screw type for the specified operations. Changing the screw type may cause the device failure.

1.13.5 Installation of Submodules

The SMG-200/SMG-500 PBXs have a modular design and may accommodate up to 2 submodules. SMG-200 supports the FXS/FXO submodules (M8S and M8O respectively), while SMG-500 supports the C4E1 and SM-VP-300 submodules. The location of the submodules in the devices is shown in Fig. 13 and Fig. 14.

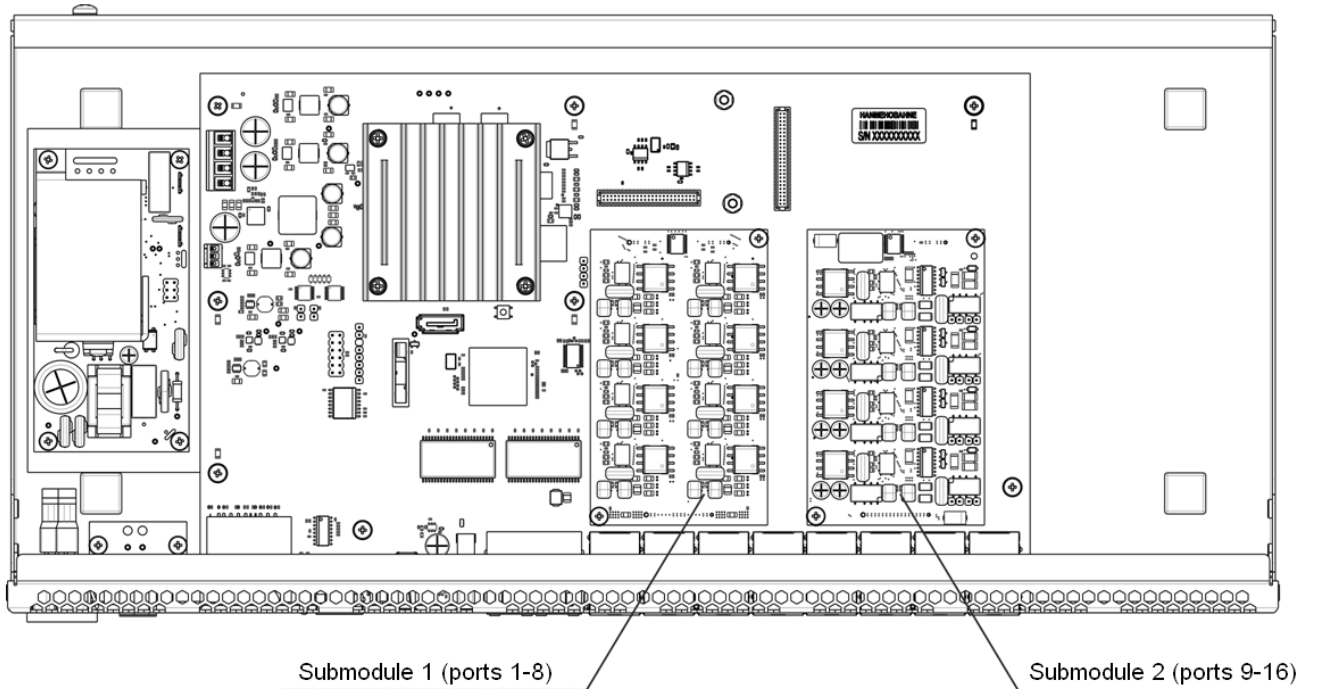


Fig. 13 – Location of the Submodules in SMG-200

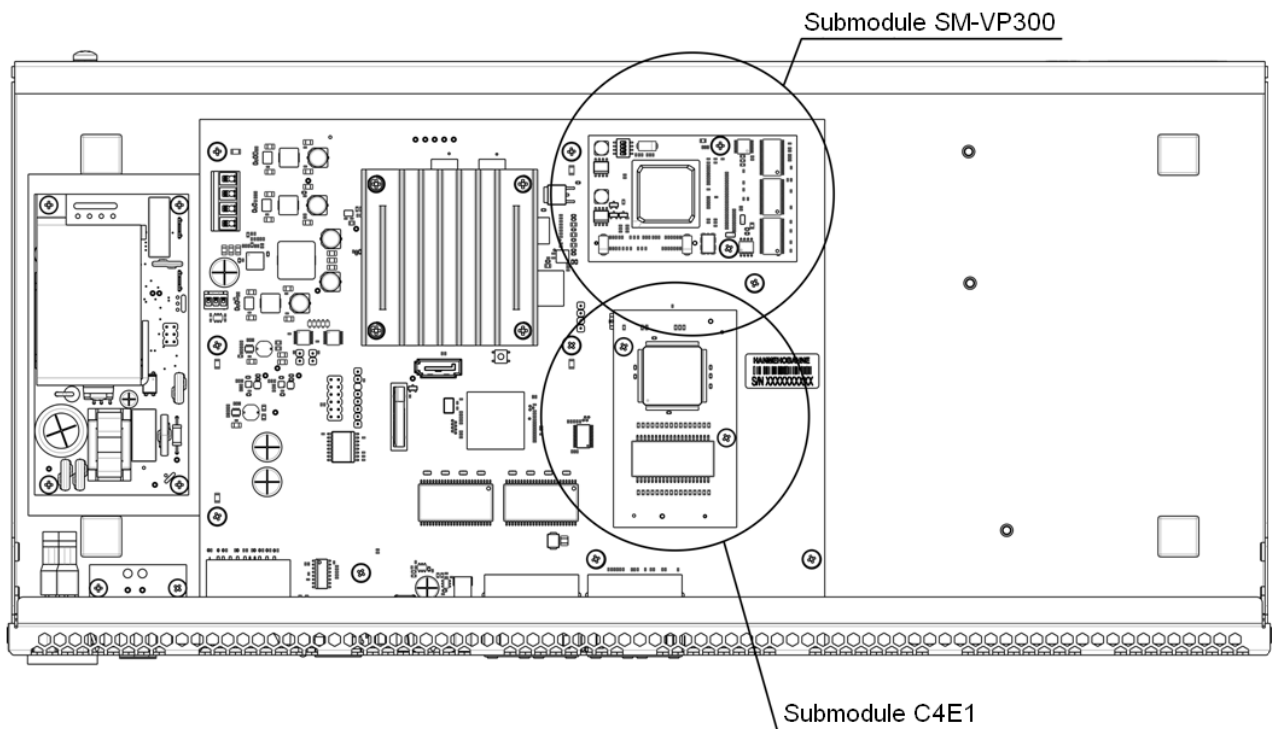


Fig. 14 – Location of the Submodules in SMG-500

Installation of the submodules in SMG:

1. Check if the device is energised.

2. If the voltage is present, disconnect the power supply.
3. Remove the device from the rack, if necessary (see section 1.13.3).
4. Open the device case (see section 1.13.4).
5. Remove screws holding submodules.
6. Install the submodules as shown in Fig. 13 and Fig. 14.
7. Screw submodules with less effort.
8. Assemble the case and install the device in a rack (if required).

1.13.6 RTC Battery Replacement

RTC (an electric circuit designed for independent chronometric data metering – current time, date, day of the week, etc.) installed on the device plate has a battery with specifications described in the table below:

Table 8 – RTC Battery Specifications

Battery type	Lithium
Form-factor	CR2032 (CR2024 option is possible)
Voltage	3 V
Capacity	225 mA
Diameter	20 mm
Thickness	3.2 mm
Battery life / expiration date	5 years
Storage conditions	-20 to +35 °C

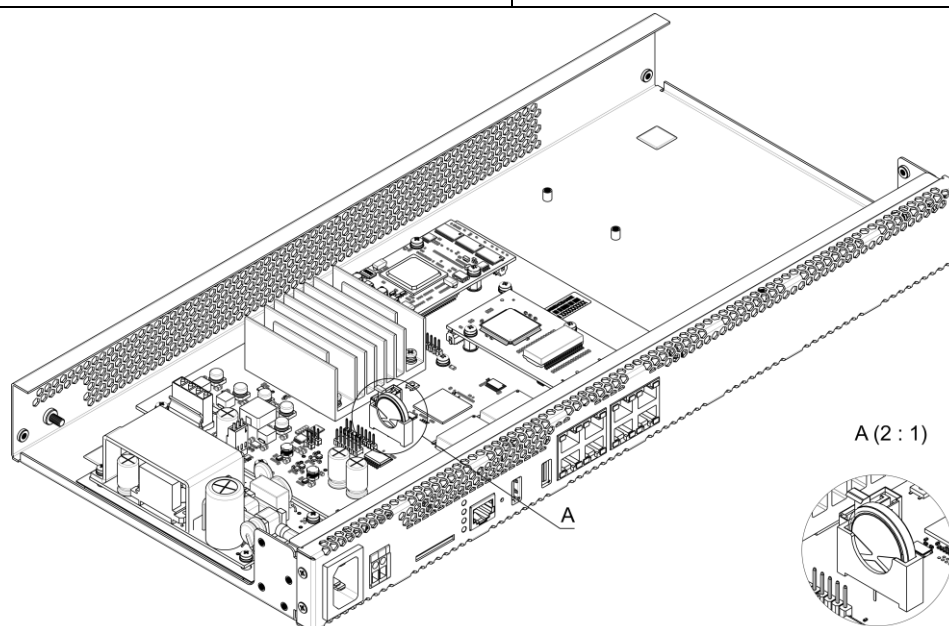


Fig. 15 – Battery Location in RTC

If battery life expires, replace the battery with a new one to ensure correct and continuous operation of the equipment. The replacement procedure is as follows:

1. Check if the device is energised.
2. If the voltage is present, disconnect the power supply.
3. If needed, remove the device from the rack (see section 1.13.3).
4. Open the device case (see section 1.13.4).
5. Remove the exhausted battery (Fig. 15) and install a new one in the same position.

To assemble the device, repeat all the steps above in the reverse order.



If NTP synchronisation is disabled, the system date and time will require adjustment after RTC battery replacement.



Used batteries should be recycled according to requirements.

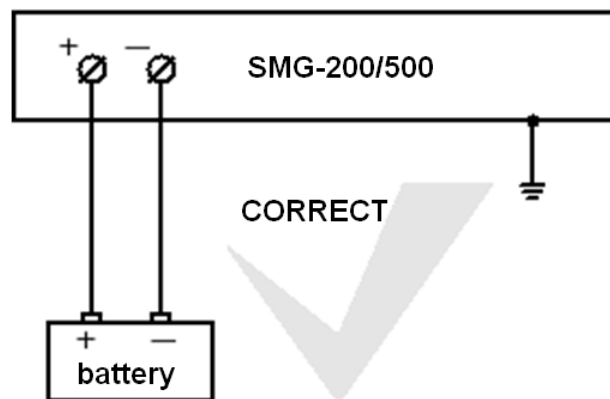
1.13.7 Accumulator battery connection

SMG-200 and SMG-500 devices are equipped with ports for accumulator battery connection with nominal voltage of 12V and charging current up to 3A.

For avoiding parasitic transition effects during switching battery supply cables and AC cables, it is recommended to observe the cable connection procedure. If AC supply is used, the next procedure of cable connection is recommended:



Make sure that the current-carrying free parts of the cable were isolated from each other to avoid short-circuit contact of accumulator battery or power supply unit.

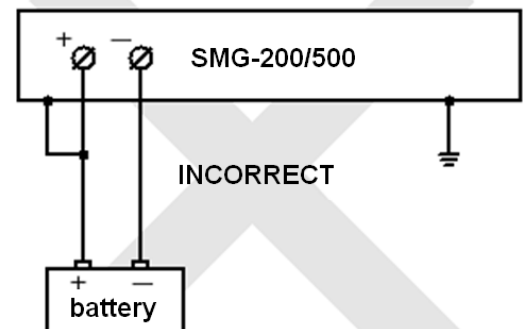
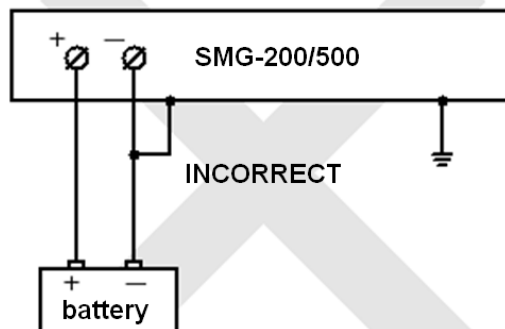


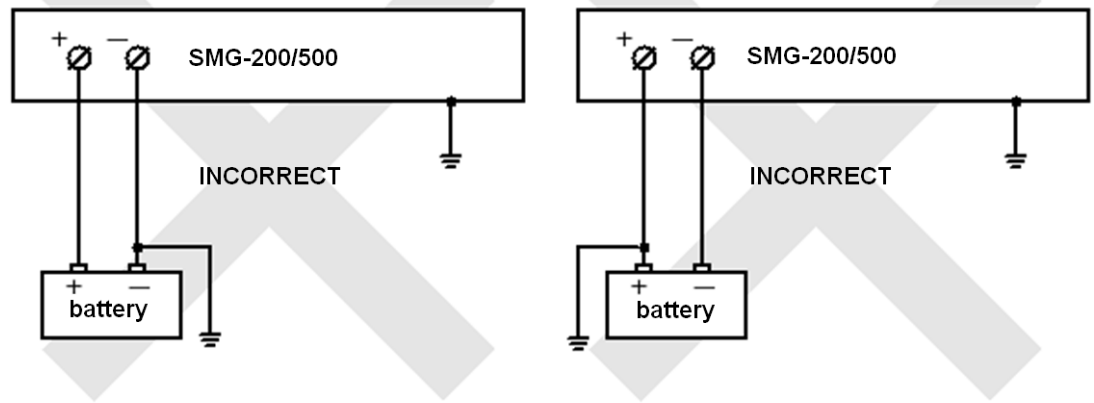
Accumulator battery is connected to the device by D-cable as shown below:



You must use only '+' and '-' battery terminals to connect accumulator! Accumulator cable connection to the case is forbidden! Do not allow accumulator cable to connect or to contact with the device case!

Do not ground accumulator terminals!





Connection of 12V accumulator battery:

1. Connect cable to the port with screw terminal on the device front panel;
2. Connect terminals to the accumulator battery, observing the polarities.

Disconnection of 12V accumulator battery:

1. Disconnect terminals from accumulator battery;
2. Release the port screws on the face panel of the device and remove cable from the port.

The recommended switch procedure of AC feeding when the system is powered by an accumulator battery:

AC supply connection (~220V):

1. Connect the power cable to the device;
2. Plug the power cable to the electrical outlet.

AC supply disconnection (~220V):

1. Unplug the power cable from the electrical outlet;
2. Unplug the power cable from the device.

2 GENERAL GUIDELINES FOR GATEWAY OPERATION

The easiest way to configure and monitor your device is to use the web configurator.

In order to prevent unauthorized access to the device, we recommend changing the password for telnet and console access (default username: *admin*, password: *rootpasswd*) and the administrator password for web configurator access. For setting password for telnet and console access, see section **3.3.2 Changing Password for CLI Access to the Device**. For setting password for the web configurator access, see section **3.1.24 Password Configuration for Web Configurator Access**. It is recommended to write down and store the configured passwords in a safe place, inaccessible for intruders.

In order to prevent the loss of device configuration data, e. g. after reset to factory defaults, it is recommended to make configuration backups and save them on a PC each time significant changes are made.

3 DEVICE CONFIGURATION

The device provides 4 connection options: the web configurator, the Telnet protocol, SSH, or RS-232 cable connection (for access via RS-232, SSH, or Telnet, use CLI).



All settings will take effect without gateway restart. To save configuration changes into the non-volatile memory, use the *Service/Save Configuration into Flash* menu in the web configurator or the `copy running_to_startup` command in CLI.

3.1 SMG Configuration via Web Configurator

To configure the device, establish a connection to the device in a *web browser* (hypertext document viewer), such as Firefox, Opera, Internet Explorer. Enter the IP address of the device in the browser address bar.



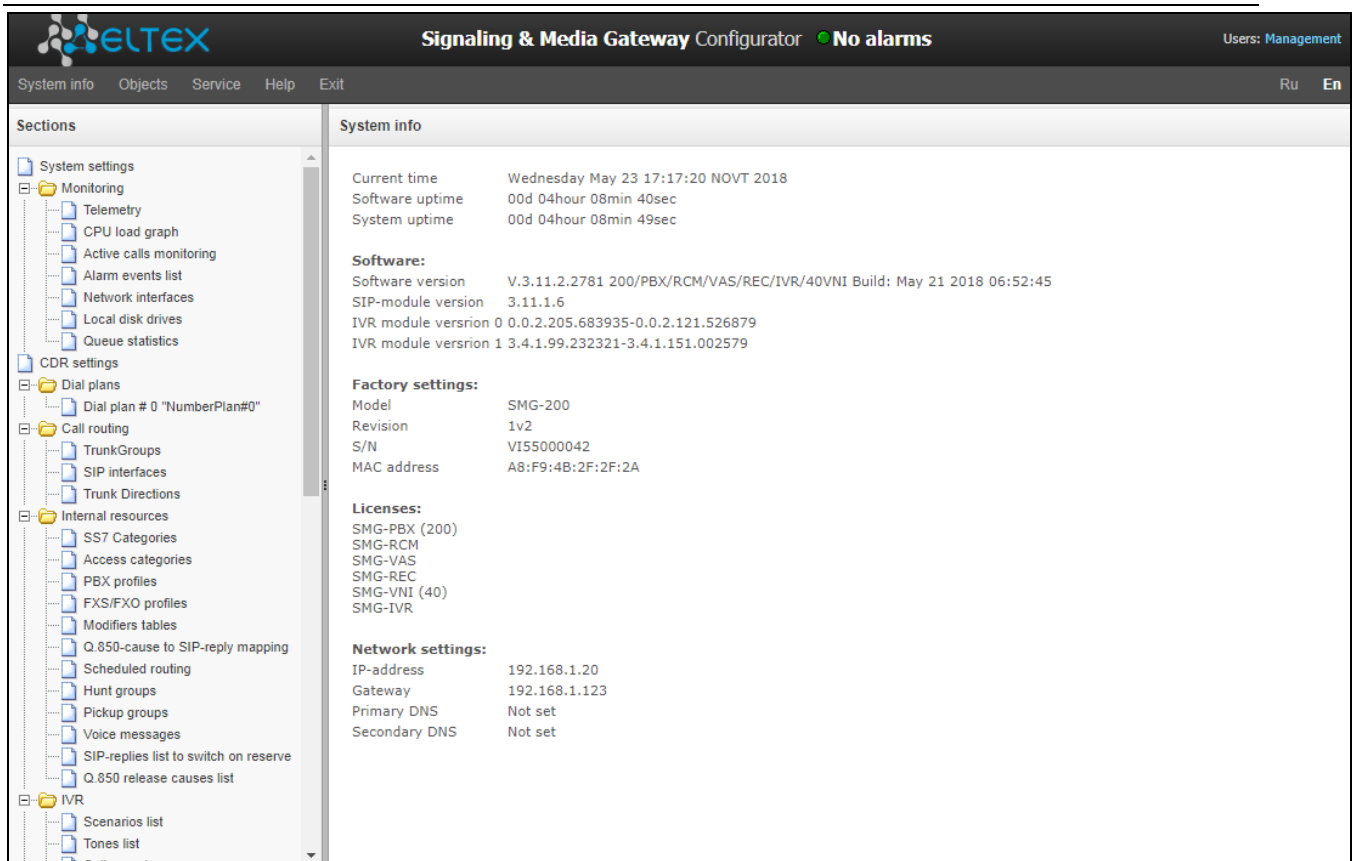
SMG factory default IP address: **192.168.1.2**, network mask: **255.255.255.0**.

As soon as the IP address is entered, the device will request username and password. You can also select the language to be used in the interface.




Initial startup username: **admin**, password: **rootpasswd**.

When the web configurator access is established, the *System Information* page opens.



The figures below illustrate navigation in the web configurator.

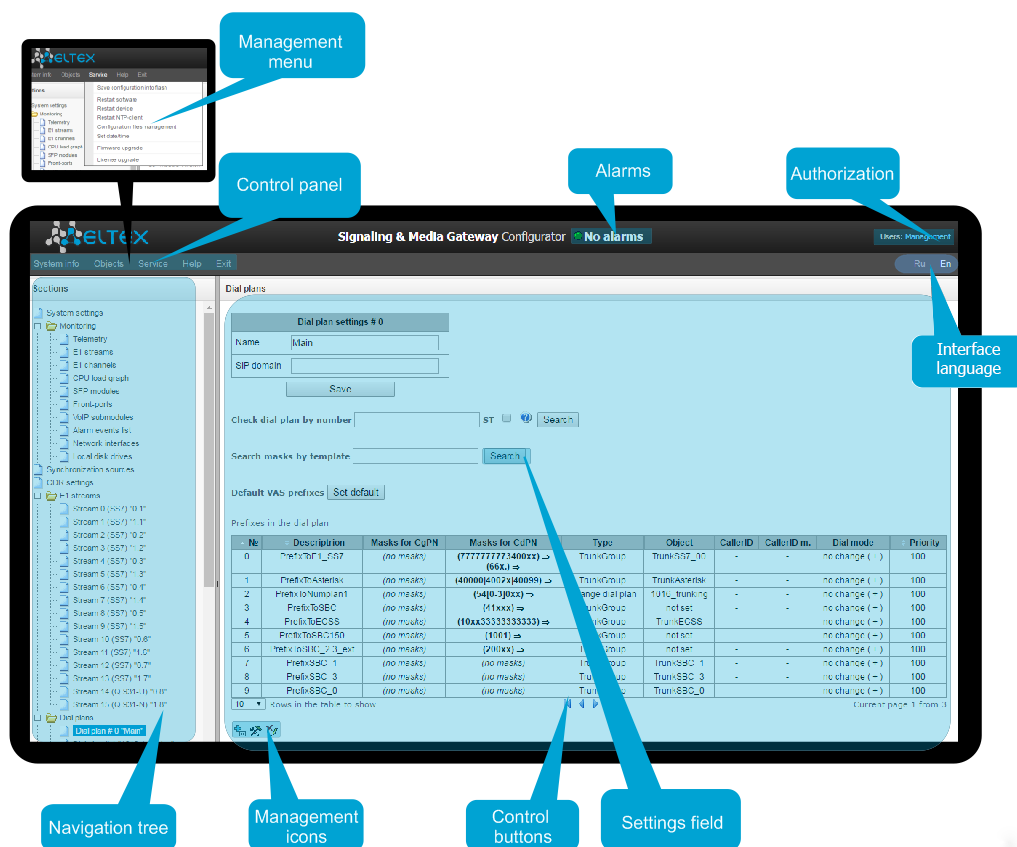






Fig. 16 – Navigation in the Web Configurator

The user interface window is divided into several areas.

-
- *Navigation tree* – enables management of the settings field. The navigation tree represents a hierarchy of management sections and nested menus.
 - *Settings field* – is defined by user selections. Allows user to view device settings and enter configuration data.
 - *Control panel* – a panel to control the settings field and firmware status.
 - *Control menus* – drop-down menus in the control panel for the settings field and firmware status.
 - *Alarms* – displays the current highest-priority fault and serves as a link to work with the fault events log.
 - *Authorisation* – a link to work with passwords that are used to access the device via web configurator.
 - *Interface language* – the buttons to switch the interface language.
 - *Control icons* – controls to work with objects in the settings field; the icons duplicate the Objects menu of the control panel:
 -  Add Object;
 -  Edit Object;
 -  Remove Object;
 -  View Object.
 - *Control buttons* – controls to work with the settings field.

To prevent unauthorised access to the device in the future, it is recommended to change the password (see section 3.1.24 Password Configuration for Web Configurator Access).



The  button (Hint) located next to the editing element provides an explanation for a particular parameter.

3.1.1 System settings

System settings	
System settings	
Device name (for web-page only)	SMG200
Local disk drive for traces	default
Active dial plan count	1
Numbering plan wait for applying	<input type="checkbox"/>
Local disk drive for alarm logging	not set
Alarm indication	
CPU load	<input checked="" type="checkbox"/>
RAM usage	<input checked="" type="checkbox"/>
Local disk drive free space	<input checked="" type="checkbox"/>
Autoupdate settings	
Enable autoupdate	<input type="checkbox"/>
Source	Static
Protocol	TFTP
Authentication	<input type="checkbox"/>
Username	
Password	
Server	update.local
Configuration update	<input type="checkbox"/>
Configuration file	a8.f9.4b.2d.fc.03.cfg
Configuration update interval, min	30
Firmware upgrade	<input type="checkbox"/>
Firmware versions file	SMG1016M.manifest
Firmware upgrade interval, min	30
Upload configuration	
Enable autoupload	<input type="checkbox"/>
Protocol	TFTP
Server	
Port	69
Path to file	
Username	
Password	*****
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- *Device name (for web page only)* – name of the device. This name is used in the header of the device web configurator;
- *Local disk drive for traces* – the device can save the debug information (tracing) to random-access memory (RAM) or to the drive installed:
 - *default* – debug information is stored to the random-access memory;
 - */mnt/sdX* – the path to the local drive; is displayed when the drive is installed. If the drive option is selected, the *logs* directory will be created on the *drive* to store tracing files;

- *Quantity of active numbering schedules* – the quantity of simultaneously active numbering schedules; up to 16 independent numbering schedules can be configured with a possibility to add subscribers and create a customised call routing table.
- *Deferred application of the numbering schedule* – when this option is checked, SMG will not apply changes in dial plan until a special confirmation. This option can be useful when working with large numbering schedules, since it helps to avoid long processing after each change of settings;
- *Failure logging device* – select the drive to write down critical alarm messages into the non-volatile memory. This option can be used when determining the cause for the equipment restart or failure;
 - */mnt/sdX* – select the path to the local drive. When this option is checked, the system creates an alarm.txt file that contains details of failures.
- *Using VoIP submodules* – option is used for enabling SM-VP submodules of SMG-500.

Example of alarm.txt file

0. 24/09/13 20:03:22. Software started.
1. 24/09/13 20:03:22. state ALARM. Sync from local source, but sync source table not empty
 2. 24/09/13 20:03:22. state OK. PowerModule#1. Unit ok! or absent
 3. 24/09/13 20:03:31. state OK. MSP-module lost: 1
 4. 24/09/13 20:03:34. state OK. MSP-module lost: 2
 5. 24/09/13 20:03:38. state OK. MSP-module lost: 3
 6. 24/09/13 20:03:42. state OK. MSP-module lost: 4

File format description:

- *0, 1, 2...* – event sequence number;
- *24/09/13...* – event occurrence date;
- *20:03:22* – event occurrence time;
- *ALARM/OK* – current status of the event (OK – the fault is resolved, ALARM – the fault is active).

Table 9 – Alarm Message Examples

Alarm Message	Meaning
Configuration error	Configuration file error
SIPT-module lost	Failure of a software module responsible for VoIP operation
Linkset down	SS7 link set failure
E1-Line alarmed	E1 stream failure
SS7-Link alarmed	SS7 signal channel failure
Sync from local source, but sync source table not empty	Synchronisation source is lost
E1-Line Remote-alarm	E1 stream remote fault
Sync from not most priority source	Primary synchronisation source is lost, the current source has a lower priority
FTP error. CDR-send failed	Failure to send a CDR file to FTP server
Software started	The device software has been started

- *Use of VoIP submodules* – select the SM-VP submodules to be used.

Fault Indication

- *CPU utilisation* – when this option is checked, a high CPU utilisation results in fault indication (the ALARM LED turns on and the alarm is registered in the alarm log).
- *RAM usage* – when this option is checked, usage of over 75% of RAM results in fault indication (the ALARM LED turns on and the alarm is registered in the alarm log).
- *External storage devices are full* – when this option is checked, fault indication will appear if the utilisation of a single external storage device with capacity less than 5 GB exceeds 80% (or there is less than 1024 MB of free space on an external storage device with capacity exceeding 5Gb) (the ALARM LED turns on and the alarm is registered in the alarm log).

Automatic Configuration

SMG can automatically receive configuration and firmware version files from the autoconfiguration server (hereinafter referred to as the server) at specified intervals.

After downloading the configuration, SMG will wait for all active calls to be completed, and then apply a new configuration. Or, the configuration will be applied during the reboot, together with the new firmware version.

The firmware version file contains details of the firmware available on the server: versions and file names. In the same place, you can specify the time allowed for the update. The file format should be as follows:

<firmware version number>; <firmware file name>; <allowed update time, hour>

- The firmware version number is specified completely before the build version;
- The firmware file name should have a .bin extension;
- The allowed update time may be absent. In this case, SMG will be updated shortly, when there are no active calls. If the allowed update time is specified, SMG will only be updated at the specified time interval.

Example of a firmware version file:

```
3.7.0.1944;smg1016m_firmware_3.7.0.1944.bin
3.8.0.2050;smg1016m_firmware_3.8.0.2050.bin;9-13
```

- *Enable automatic updates* – enable automatic updates of configuration and firmware files;
- *Source* – select the source of server information;
- *Static* – the server information is written down and stored at the SMG PBX in the corresponding field;
- *DHCP* (interface name) – the server information will be obtained by the selected DHCP interface from option 66; information about the version file name and the configuration file will be obtained from option 67;
- *Protocol* – select the server connection protocol;
- *Authentication* – use authentication to access the server (for FTP, HTTP, HTTPS);
- *Name* – the user name (login) to access the server;

-
- *Password* – a password to access the server;
 - *Server* – IP address or domain name of the server It is used when the Static source is selected;
 - *Update configuration* – allows configuration updates from the server;
 - *Configuration file name* – name of the configuration file. The file name should have a .cfg extension and not exceed 64 characters in length;
 - *Configuration update interval, min* – how often the server is checked for the presence of a new configuration;
 - *Update firmware* – allows firmware updates from the server;
 - *Firmware version file name* – the name of the firmware version file. The file name should have a .manifest extension and not exceed 64 characters in length;
 - *Firmware update interval, min* – how often the server is checked for the presence of a new firmware version;

Uploading Configurations

SMG PBX can automatically upload its configuration to an external FTP/TFTP server each time it is saved to non-volatile memory.

- *Enable automatic uploading* – enables the configuration upload function;
- *Protocol* – select the protocol for uploading. FTP and TFTP are supported;
- *Server* – IP address of the server to which the file is uploaded;
- *Port* – the server port to which the file is uploaded;
- *Path to the file* – the directory on the server to which the configuration file will be saved;
- *Name* – the authentication user name when using FTP;
- *Password* – the authentication password when using FTP.

3.1.2 Monitoring

3.1.2.1 Telemetry

This section describes the readings of the telemetry system sensors installed on the device.

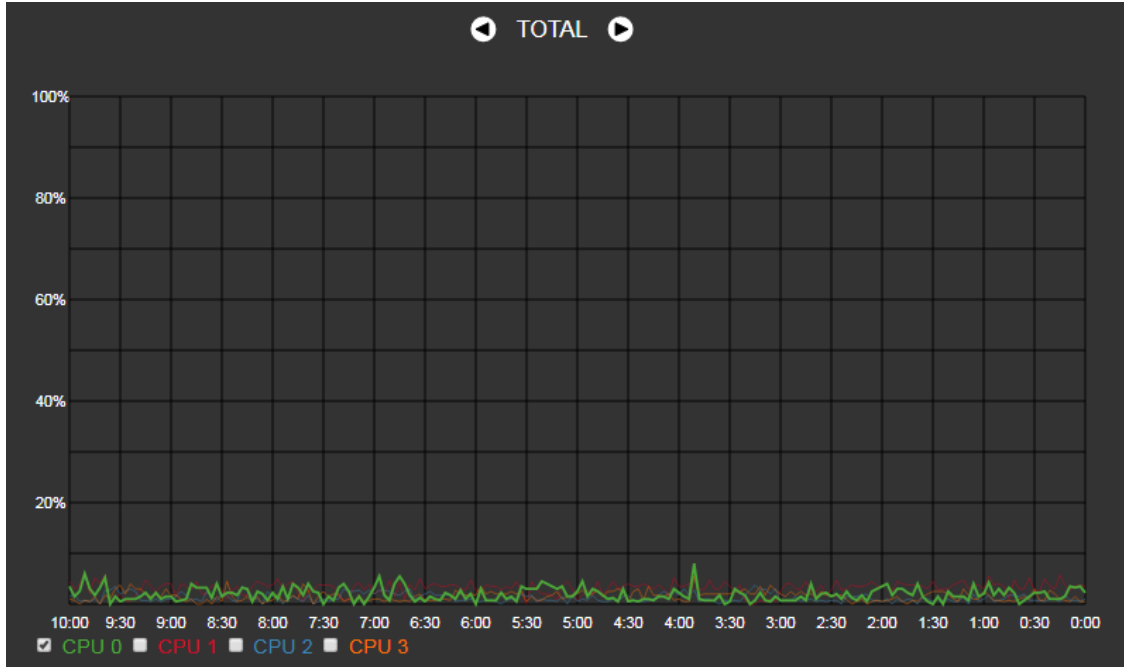
Current CPU Utilisation



- *USR* – percentage of CPU time utilisation by user applications;
- *SYS* – percentage of CPU time utilisation by core processes;
- *NIC* – percentage of CPU time utilisation by applications with a modified priority;
- *IDLE* – percentage of unused CPU resources;
- *IO* – percentage of CPU time spent on I/O operations;
- *IRQ* – percentage of CPU time spent on processing of hardware interruptions;

- *SIRQ* – percentage of CPU time spent on processing of software interruptions.

3.1.2.2 CPU Utilisation Chart

This section contains information on CPU utilisation in real time (10-minute interval). Statistics charts are based on average data for each 3-second device operation interval.



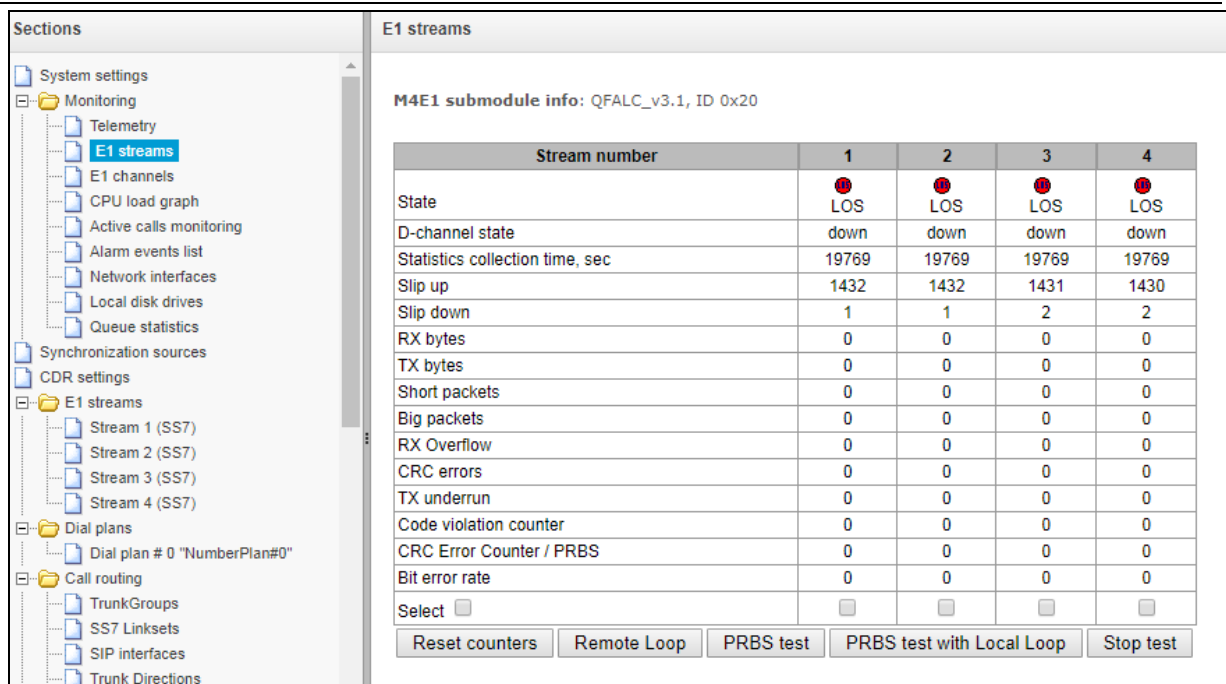
To navigate between specific parameters in monitoring charts, use the  and  buttons. To enhance visual identification, all charts have different colours.

- *TOTAL* – total percentage of CPU utilisation;
- *IO* – percentage of CPU time spent on I/O operations;
- *IRQ* – percentage of CPU time spent on processing of hardware interruptions;
- *SIRQ* – percentage of CPU time spent on processing of software interruptions;
- *USR* – percentage of CPU time utilisation by user applications;
- *SYS* – percentage of CPU time utilisation by core processes;
- *NIC* – percentage of CPU time utilisation by applications with a modified priority.

CPU 0..3 – view the utilisation of each CPU core separately.

3.1.2.3 E1 stream monitoring (for SMG-500 only)

This section contains information on E1 stream monitoring and statistics as well as C4E1 (M4E1) submodule chips installed.



Stream number	1	2	3	4
State	LOS	LOS	LOS	LOS
D-channel state	down	down	down	down
Statistics collection time, sec	19769	19769	19769	19769
Slip up	1432	1432	1431	1430
Slip down	1	1	2	2
RX bytes	0	0	0	0
TX bytes	0	0	0	0
Short packets	0	0	0	0
Big packets	0	0	0	0
RX Overflow	0	0	0	0
CRC errors	0	0	0	0
TX underrun	0	0	0	0
Code violation counter	0	0	0	0
CRC Error Counter / PRBS	0	0	0	0
Bit error rate	0	0	0	0
Select	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

For E1 chips, the table lists installation position number (see section 1.13.5 Installation of Submodules), chip name and identifier.

Stream parameters:

- *State* – data flow state:
 - *WORK* – data stream is in operation;
 - *LOS* – loss of signal;
 - *OFF* – data stream is disabled in configuration;
 - *NONE* – submodule is not installed;
 - *AIS* – alarm indication signal (signal that contains all ONEs);
 - *LOMF* – multi-frame alarm indication signal (loss of multiframe);
 - *RAI* – remote alarm indication;
 - *TEST* – data stream test indication (PRBS test, local or remote loop);
- *D-channel state* – D-channel state, service management channel;
 - *up* – D-channel is active;
 - *down* – D-channel is inactive;
 - *no* – there is no management channel for data stream;
 - *off* – stream signaling is disabled;
- *Statistics collection time, sec* – statistics collection period, in seconds;
- *Slip up* – number of positive bit slips for the stream;
- *Slip down* – number of negative bit slips for the stream;
- *Rx bytes* – number of bytes received from the stream;
- *Tx bytes* – number of bytes sent to the stream;
- *Short packets* – number of packets received which size is less than standard;
- *Big packets* – number of packets which size is bigger than standard;
- *Rx Overflow* – buffer overrun error / counter;

- *CRC errors* – CRC error counter;
- *Tx underrun* – stream transmission failure counter;
- *Code violations counter* – signal code sequence failure counter;
- *CRC Error Counter / PRBS* – CRC error quantity (in 'PRBS test' mode);
- *Bit error rate* – number of bit errors for the stream.

The following buttons are located under the table of E1 channel parameters:

- *Reset counters* – when checked, click 'Reset' button to reset the collected statistics for the selected stream;
- *Remote loop* – E1 path test mode under which signal received through the connected E1 stream is transmitted back into the same stream;
- *PRBS test* – enables pseudorandom sequence output to the output port of the unit (transmitted through the connected E1 stream); at that, error detection mode will be enabled at the unit input port (E1 stream reception) for this sequence in order to evaluate the signal transmission quality. Number of errors and analysis time counter will be displayed in the stream information window;
- *PRBS test with local loop* – E1 path test mode, where external line is disabled and the signal transferred by the unit is transmitted into the input of the same unit. Pseudorandom sequence output will be enabled to the unit output port; input port will operate in the error detection mode;
- *Stop test* – disable test mode.

3.1.2.4 E1 channel monitoring (for SMG-500 only)

This section contains information on E1 stream channel status. In the upper part of the field, there is E1 stream channel matrix, where channel numbers are defined in rows and stream numbers are defined in columns (their assigned signalling protocol listed in parentheses). In the lower part of the field, there are information tables and the management table.

Information tables

E1 channel number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Stream 1 (SS7)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Stream 2 (SS7)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Stream 3 (SS7)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Stream 4 (SS7)	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Call information on channel #	Streams state	Channels state
Port/channel	✗ NONE	○ Off
Connected port/channel	○ OFF	○ Idle
Connected Callref	● ALARM	● Block
State	● LOS	📞 Incoming dialing
State timer	● AIS	➡ Outgoing dialing
Incoming SS7 category	● LOF	📞 Incoming alerting
Incoming CdPN	● LOMF	📞 Outgoing alerting
Incoming CgPN	● WORK/RAI	📞 Busy, Release
Outgoing SS7 category	● WORK/SLIP	📞 Talk
Outgoing CdPN	● WORK	📞 Hold
Outgoing CgPN	🚧 TEST	📞 Waiting
		📞 3way, Conference
		📞 Service dialing

Connection information on channel #:

- *Port/channel* – this section is divided into two parts:
 - Signalling protocol (PRI/SS7);
 - Port location: Stream #:, channel #.
- *Connected port/channel* – this section is divided into two parts:
 - Linked port signalling protocol (PRI/SS7/VoIP);
 - Linked port location: *Stream #: Channel # for PRI/SS7 or VoIP submodules #: VoIP channel #.*
- *Connected Callref* – call identifier for linked channel;
- *State* – channel state:
 - *Off* – channel is disabled;
 - *Block* – port is blocked;
 - *Init* – channel initialization;
 - *Idle* – channel is in initial state;
 - *In-Dial/ Out-Dial* – inward/outward dialing;
 - *In-Call/ Out-Call* – incoming/outgoing occupation;
 - *In-Busy/ Out-Busy* – busy tone generation;
 - *Talk* – channel is in speech condition;
 - *Release* – channel release;
 - *Wait-Ack* – waiting for acknowledgement;
 - *Wait-CID* – waiting for CgPN (Caller ID);
 - *Wait-Num* – waiting for dialling;

– *Hold* – subscriber is on hold.

- *State timer* – channel last known state duration;
- *Incoming SS7 category* – SS7 category of an incoming call before modification;
- *Incoming CdPN* – callee number before modification;
- *Incoming CgPN* – caller number before modification;
- *Outgoing SS7 category* – SS7 category of an incoming call after modification;
- *Outgoing CdPN* – callee number after modification;
- *Outgoing CgPN* – caller number after modification.

Streams state – information table with matrix symbol interpretations:

State – stream state:

- *NONE* – C4E1 submodule is not available;
- *OFF* – stream is disabled in configuration;
- *ALARM* – C4E1 submodule initialization error;
- *LOS* – signal is lost;
- *AIS* – alarm indication signal (signal that contains all ONES);
- *LOMF* – multi-frame alarm indication signal (loss of multiframe);
- *WORK/RAI* – remote alarm indication;
- *WORK/SLIP* – SLIP indication for a data stream;
- *WORK* – data stream is in operation;
- *TEST* – data stream test indication (PRBS test, local or remote loop)

Channels state – information table with matrix symbol interpretation:

State – channel state:

- *Off* – channel is disabled in the configuration;
- *Idle* – channel is in initial state;
- *Block* – channel is blocked;
- *Incoming dialing* – incoming call dialing;
- *Outgoing dialing* – outgoing call dialing;
- *Incoming alerting* – incoming occupation, callee is disengaged;
- *Outgoing alerting* – outgoing occupation, caller is disengaged;
- *Busy, Release* – channel release, “busy” tone generation;
- *Talk, Hold* – channel is in call state, on hold;
- *Waiting* – waiting for a response from the opposite party (waiting for occupation acknowledgement, caller ID, and dialing number);
- *3way, Conference* – conference mode (3-WAY or Add on conference);
- *Service dialing* – call by VAD numbers.

If one of the C4E1 submodules is not accessible, '*C4E1 submodule is not installed, channel monitoring is unavailable*' will be generated.

Channel state updates in 5 seconds interval.

Link management

To enable stream management, left-click the stream name. The field will become highlighted, for example, the screenshot below shows the information for Stream 1 (SS7). Next, in 'SS7 link management' table, select the field with the required action and left-click it. Pop-up informational message about the command execution will be shown on screen.

SS7 link management – SS7 signal link management table:

- *Send LUN* – send link uninhibit signal;
- *Send LIN* – send link inhibit signal;
- *Send LFU* – send link forced uninhibit signal;
- *Set congestion state* – set signal link overload state;
- Clear congestion state – cancel signal link overload state;
- Set local processor outage;
- Clear local processor outage;
- Invoke normal link restart;
- Invoke emergency link restart;
- Stop link.

SS7 channel management

To enable management for a channel in a stream, left-click its icon. The field will become highlighted, for example, the screenshot below shows the information for Channel 18 in Stream 1 (SS7). Next, in 'SS7 channel management' table, select the field with the required action and left-click it. Pop-up informational message about the command execution will be shown on screen.



You may perform group operations for channels in a stream. To do this, select the range of channels while holding <SHIFT> key.

SS7 channel management – SS7 (CIC) channel management:

- *Block channel (send BLO)* – send BLO message to block channel;
- *Unblock channel (send UBL)* – send UBL message to unblock channel;
- *Reset channel to initial state (send GRS)* – send RSC message;
- *Local block* – block channel locally without sending BLO message;
- *Local unblock* – cancel local block;
- *Release (send REL)* – send REL message;
- *Release confirmation (send RLC)* – send RLC message;
- *Run continuous-check test (send CCR)* – run continuous-check test by sending CCR message;
- *Stop continuous-check test* – forcibly terminate channel continuity test;
- *Show continuous-check test* – show the current channel continuity test state.

3.1.2.5 Fault Alarms Fault Events Log

When a failure occurs, all related information containing the fault stream number, SS-7 line group, signal link, or faulty module is displayed in the header of web configurator. If there are multiple active failures, the header of web configurator will alert about the current most critical one.

When there are no alarms, the message *No alarms* will be displayed.

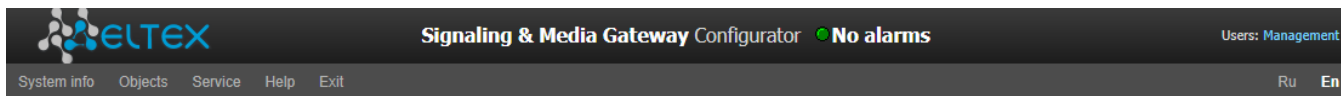


Table 10 – Alarm Message Examples

Alarm Message	Meaning
Configuration has not been read	Configuration file error
No communication with SIP module	Failure of a software module responsible for SIP operation
Failed to send CDR files via FTP	Failure to send a CDR file to FTP server
No communication with the VoIP submodule	No communication with the SM-VP submodule
Running out of operating memory	Alarm about high usage of memory resources
No communication with the H323 module	Failure of a firmware module responsible for H.323 operation
High CPU temperature	Temperature has reached 70°C – warning; 85°C – failure; 100°C – critical failure;
SIP interface does not respond to OPTIONS requests	One of SIP interfaces is unavailable
High CPU utilisation"	Utilisation above 90% – warning; Over 95% – failure.
Low free space on the disk	Free space on one of the external storage devices is running out.
CPS threshold is exceeded for the TrunkGroupName trunk group	One of the trunk groups receives more calls per second than defined in the <i>CPS alarm threshold</i> setting

The *Fault Events Log* menu contains a list of alarm events arranged by time and date. There is also the "Clear" button, which removes all information messages and resolved faults from the current log file.

Alarm events list					
Local alarm-events list					
<input type="button" value="Clear"/> Clear the alarm events list					
No	Time	Date	Type	State	Parameters
4	13:09:04	23/05/18	SIPT-MODULE	OK	SIP-module connection error
3	13:08:59	23/05/18	SIPT-MODULE	Critical alarm	SIP-module connection error
2	13:08:59	23/05/18	Configuration is not read	OK	
1	13:08:59	23/05/18	Software start V.3.11.2.2781	OK	
0	13:08:49	23/05/18	Configuration is not read	Critical alarm	

Alarm Table:

Clear – delete the existing fault events table;

- # – fault sequential number;
- *Time* – fault occurrence time (HH:MM:SS);

- *Date* – fault occurrence date (DD/MM/YY);
- *Type* – a fault type:
 - *CONFIG* – a critical fault, a configuration file fault;
 - *SIPT-MODULE* – a critical fault, a failure of a program module responsible for VoIP operation;
 - *CDR-FTP* – a fault or a warning, a failure to send a CDR file to the FTP server;
 - *TRUNK-CPS* – the number of allowed calls per second for the trunk group is exceeded;
- *State* – a fault state status:
 - *critical fault, LED blinking red* – the fault requires immediate intervention of the service personnel and affects device operation and provisioning of communication services;
 - *fault, red LED* – non-critical fault, intervention of the service personnel is also required;
 - *warning and OK, green LED* – the fault is resolved;
- *Parameters* – textual description of the failure details. Depending on the failure type, it has the following form:
 - *CONFIG*;
 - *SIPT-MODULE* – no communication with SIP module;
 - *TRUNK-CPS* – CPS threshold is exceeded for XX trunk group, where XX – the trunk group name;

3.1.2.6 Interface Monitoring

This section describes monitoring the status of network interfaces (tagged/untagged)

Network interfaces							
No	Ethernet	Network name	VLAN ID	DHCP	IP address	Broadcast	Network mask
0	eth0	eth1	-	-	192.168.1.20	192.168.1.255	255.255.255.0
1	eth0:1	0.20	-	-	192.168.0.20	192.168.0.255	255.255.255.0

- *Ethernet* – Ethernet interface name;
- *Network name* – the network name with which the specified network settings are associated;
- *VLAN ID* – virtual network identifier (for the tagged interface);
- *DHCP* – indicates the usage of DHCP to obtain network settings automatically (requires a DHCP server in the operator's network);
- *IP address, Broadcast, Network mask* – network interface settings (if not using DHCP).

3.1.2.7 Storage Devices Information

This section contains information about external storage devices connected to the device.

Local disk drives
No connected drives

- *Extract* – clicking on the link will safely extract the drive.

3.1.2.8 Queues Statistics

This section contains the queues operation statistics.

Queue statistics							
ID queue	Total calls	Answered	Unanswered	Average queue length	Callback failure	Queue overflow	Waiting time
0	0	0	0	0 / 0 / 0	0	0	0
1	0	0	0	0 / 0 / 0	0	0	0

- *Queue ID* – the queue identifier.
- *Total of incoming calls* – the total number of incoming calls in the queue.
- *Answered* – the number of successful calls completed by the operator's response.
- *Not answered* – the number of calls dropped by the caller before the operator's response.
- *Average queue length (hour/day/workday)* – the maximum queue length for the last hour/day/working day. The last hour/day – a periodic interval of time repeated every hour/24 hours respectively, where the first interval starts at the firmware start time. The time intervals of the workday are set in the call group settings.
- *Unsuccessful callback attempts* – the number of unsuccessful attempts to call back to the subscriber, when using the callback option¹.
- *Queue overflows* – the number of calls failed due to the queue size overflow.
- *Average waiting time* – the average waiting time for the operator to respond; based on this value, the response is generated.

3.1.2.9 Active Calls Monitoring

The 'VoIP submodules load' window displays sound mixer channel occupancy, and the state of SM-VP-M300 submodule installed on SMG-500.

VoIP submodule load			
Type	State	Active count	Payload
M82359	Work	0	0.0%



The SM-VP submodule of SMG-500 is designed for converting media traffic in the E1-VoIP direction. The submodule is not involved for processing media traffic and calls in the VoIP – VoIP direction.

¹ Not supported in the current firmware version 3.14.0

Sections

- System settings
- Monitoring
 - Telemetry
 - E1 streams
 - E1 channels
 - CPU load graph
 - Active calls monitoring
 - Alarm events list
 - Network interfaces
 - Local disk drives
 - Queue statistics
- Synchronization sources
- CDR settings
- E1 streams
 - Stream 1 (SS7)
 - Stream 2 (SS7)
 - Stream 3 (SS7)
 - Stream 4 (SS7)
- Dial plans
 - Dial plan # 0 "NumberPlan#0"
- Call routing
 - TrunkGroups
 - SS7 Linksets
 - SIP interfaces
 - Trunk Directions
- Internal resources
 - SS7 Categories
 - Access categories
 - PBX profiles
 - Modifiers tables
 - Q.931 timers
 - SS7 timers
 - Q.850-cause to SIP-reply mapping
 - Scheduled routing
 - Hunt groups
 - Pickup groups
 - Voice messages
 - SIP replies list to switch on response

Active calls monitoring

VoIP submodule load			
Type	State	Active count	Payload
M82359	Work	0	0.0%

Active calls monitoring																															
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

Channel info #	Channel states
State -	Idle
State timer -	Incoming dialling
Incoming SS7 category -	Outgoing dialling
Incoming CdPN -	Incoming alerting
Incoming CgPN -	Outgoing alerting
Outgoing SS7 category -	Busy, Release
Outgoing CdPN -	Talk
Outgoing CgPN -	Hold
	Waiting, Wait CID
	3way, Conference

Active calls monitoring window displays state indicators for each port. **Channel state** window shows indication description, see below.

Channel Status

- *Idle* (grey) – initial state, the channel is ready to serve a call;
- *Incoming dialling* – incoming call;
- *Outgoing dialling* – outgoing call;
- *Incoming alerting* – incoming alert message;
- *Outgoing alerting* – outgoing alert message;
- *Busy, Release* – line is busy;
- *Talk* – conversation;
- *Hold* – on hold;
- *Waiting, Wait CID* – waiting, waiting for CallerID;
- *3way, Conference* – participates in the conference.

To get additional information on channel state, select the required channel in **Active calls monitoring** window. Information on connection via channel # displays information on channel.

Channel Connection Information

- *Status* – channel status:

- Off – channel is disabled;
 - Block – port is blocked;
 - Init – channel initialisation;
 - Idle – channel is in initial state;
 - In-Dial/Out-Dial – incoming/outgoing call dial;
 - In-Call/Out-Call – incoming or outgoing engagement;
 - In-Busy/Out-Busy – sending the busy tone;
 - Talk – channel is in call state;
 - Release – channel release;
 - Wait-Ack – waiting for acknowledgement;
 - Wait-CID – waiting for Caller ID (CLI);
 - Wait-Num – waiting for call dial;
 - Hold – subscriber is on hold;
- *Status timer* – channel last known status duration.
 - *Incoming SS7 category* – SS7 category of an incoming call before modification.
 - *CdPN incoming number* – callee number before modification.
 - *CgPN incoming number* – caller number before modification.
 - *Outgoing SS7 category* – SS7 category of an incoming call after modification.
 - *CdPN outgoing number* – callee number after modification.
 - *CgPN outgoing number* – caller number after modification.

3.1.3 Synchronization source

To synchronize device with multiple sources, priority list algorithm has been implemented. Its meaning is as follows: when sync signal from the current source is lost, the list lookup is performed to identify active signals from the lower priority sources. When the higher priority signal is restored, the system will switch to that signal. Also, you may use multiple sources with the same priority; at that, when the same priority signal is restored, the system will not switch to that signal

You may specify up to 4 synchronization sources (from each of 4 E1 streams).


To generate the list, use the following buttons:



– Add source;



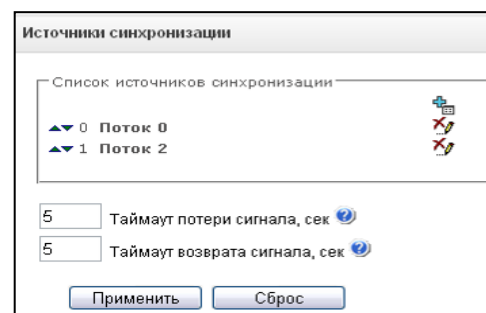
– Delete.

To change the source priority, use  'Up/Down' buttons located next to each source. The highest priority value is 0, the lowest priority value is 14.

- *Signal loss timeout* – time interval that should pass before the system switches to the lower priority synchronization source when the signal is lost. If the signal is restored during this interval, there will be no switching.
- *Return timeout* – time interval of the restored higher priority synchronization signal activity that should pass before the system switches to that signal.




If D-channel is configured for the stream originating the synchronization signal (for SS7 or PRI protocol), make sure that D-channel is in operation, otherwise the synchronization signal will not be captured from the stream that will cause slips.



3.1.4 CDR

This section describes parameters configuration to save call detail records.

CDR is a call detail record, which allows the system to save the history of calls performed through SMG.

CDR settings	
CDR settings	
Enable CDR	<input checked="" type="checkbox"/>
CDR files settings	
Create files	periodically ▾
Hours	1 ▾
Minutes	0 ▾
Add header	<input type="checkbox"/>
Signature	<input type="text"/>
Local storage settings	
Store files on local disk drive	<input type="checkbox"/>
Path to local disk drive	<input type="text"/>
Directory usage	by date ▾
Keep files for: Days	30 ▾
Hours	0 ▾
Minutes	0 ▾
FTP server settings	
Store files on FTP	<input type="checkbox"/>
Server address/hostname	<input type="text"/>
Server port	21
Path on server	<input type="text"/>
Login	<input type="text"/>
Password	*****
Reserve FTP server settings	
Store files on FTP	<input type="checkbox"/>
Only if primary FTP failed	<input type="checkbox"/>
Server address/hostname	<input type="text"/>
Server port	21
Path on server	<input type="text"/>
Login	<input type="text"/>
Password	*****
Other settings	
Save unsuccessfull calls	<input type="checkbox"/>
Save empty files	<input type="checkbox"/>
Write redirected call duration	<input type="checkbox"/>
Swap Redirecting number and CgPN 	<input type="checkbox"/>
Round duration	upwards ▾
Modifiers for incoming numbers	
CdPN	[3] format_CDR ▾
CgPN	not used ▾
RedirPN	not used ▾
Modifiers for outgoing numbers	
CdPN	not used ▾
CgPN	not used ▾
RedirPN	not used ▾
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

CDR Saving Parameters

- *Enable saving CDR* – when this option is checked, the gateway will generate CDRs.

CDR Files Creation Settings

- *Create mode* – select the mode to create CDR files:
 - *After the specified period* – CDR file is created after the specified period has elapsed since the device boot;
 - *Once a day* – CDR file is created once a day at the specified time;
 - *Once an hour* – CDR file is created once an hour at the specified time;
- *Saving period: Days, Hours, Minutes* – time period for CDR generation and saving in the device RAM;
- *Add header* – when this option is checked, the following header will be written at the beginning of the CDR file: SMG200. CDR. File started at “YYYYMMDDhhmmss”, where “YYYYMMDDhhmmss” is the records saving start time.
- *Discriminant* – specifies a distinctive feature to identify the device, which created the record.

Local Storage Settings

- *Save to local drive* – when this option is checked, save CDRs onto the local drive;
- *Local drive path* – the path to the local drive. If the local drive path is selected, the menu displays the list of folders and files on that drive. To download data to your computer, select the checkbox for the required records and click *Download*. The folder with records will be moved to the archive, which is recommended to delete after the boot to avoid the disk overflow. To remove the outdated data from your computer, select the checkbox for the required records and click *Remove*.

Local storage settings	
Store files on local disk drive	<input type="checkbox"/>
Path to local disk drive	<input type="text"/>
Directory usage	by date ▾
Keep files for: Days	30 ▾
Hours	0 ▾
Minutes	0 ▾

- *Directory utilisation* – select the directories for CDR data storage;
 - *Directories by date* – CDRs are saved into separate directories, where the directory name corresponds to the CDR file creation date and the name format is “cdryyyymmdd”, for example, cdr20150818;
 - *Single directory* – all CDRs are saved into a single cdr_all directory located on the selected drive.
- *Data storage time: Days, Hours, Minutes* – the period to keep CDRs on the local drive.



-  **When the FTP server is not available, CDRs will be saved to the device RAM. When the memory is full, a warning message will be generated, followed by a failure alarm. For CDR file saving indication, see section 1.7. The thresholds for warning and failure alarms are described in the table of memory thresholds for CDRs saving.**
-  **When the failure status is activated, the corresponding SNMP trap is sent.**

Table of memory thresholds for CDR saving

A certain amount of RAM is allocated for the temporary storage of CDR on the device, in case it is impossible to save data to the FTP server for some reason. When this amount is filled, a warning or failure alarm is displayed.

	SMG-200/500
Total memory allocated:	30 MB
Memory thresholds for alarm messages:	
- warning	512 KB
- failure	5 MB
- critical failure	15 MB

One CDR takes from 200 to 400 bytes. Thus, 1 MB of memory can store from 2,600 to 5,200 records.

FTP Server Settings

- *Save to FTP* – when this option is checked, CDRs will be transferred to a FTP server;
- *FTP Server* – IP address of the FTP server;
- *FTP Port* – TCP port of the FTP server;
- *Path to file* – a path to the FTP server directory to store CDRs;
- *FTP login* – username for access to the FTP server;
- *FTP password* – user password for access to the FTP server.

Settings of Redundant FTP Server

In case the primary FTP server is unavailable, CDRs will be sent to the redundant server (if configured), until communication with the primary FTP server is restored.

- *Save to FTP* – when this option is checked, CDRs will be transferred to a redundant FTP server;
- *FTP Server* – IP address of the redundant FTP server;
- *FTP Port* – TCP port of the redundant FTP server;
- *Path to file* – a path to the redundant FTP server directory to store CDRs;
- *FTP login* – username for access to the redundant FTP server;
- *FTP password* – user password for access to the redundant FTP server.

Miscellaneous Settings

- *Save unsuccessful calls* – when this option is checked, stores unsuccessful calls (not resulted in conversation) into CDR files;
- *Save empty files* – when this option is checked, saves CDR files containing no records;
- *Redirected call duration* – when this option is checked, the CDR for a call redirected from “discinfo: redirected call;”, will contain actual call duration; when unchecked, the duration will be set to zero;
- *Replace CgPN with Redirecting number* – the option applies to calls redirected in case the CgPN and the Redirecting number fields in the CDR are used simultaneously. If there is no Redirecting number field in the CDR, the CgPN value is automatically replaced with Redirecting number value for redirected calls;
- *Duration rounding* – this option specifies the rounding mode for the call duration in CDRs:
 - *Rounding up* – call duration rounding mode; the call duration is rounded up if it exceeds 330 ms;
 - *Rounding down* – call duration rounding mode; the call duration is rounded down if it exceeds 850 ms;
 - *No rounding (ms counted)* – in this mode, the call duration is not rounded up or down, and is recorded to the nearest millisecond.

Incoming Number Modifiers

Incoming number modifiers are the modifiers that modify any CDR fields containing subscriber numbers and apply to these fields before a call proceeds through a numbering schedule.

- *CdPN* – intended for modifications based on the analysis of the callee number received from the incoming channel;
- *CgPN* – intended for modifications based on the analysis of the caller number received from the incoming channel;
- *RedirPN* – intended for modifications based on the analysis of the number of the subscriber that redirected the call received from the incoming channel.

Outgoing Number Modifiers

Outgoing number modifiers are the modifiers that modify any CDR fields containing subscriber numbers and apply to these fields after a call proceeds through a numbering schedule.

- *CdPN* – intended for modifications based on the analysis of the callee number sent to the outgoing channel;
- *CgPN* – intended for modifications based on the analysis of the caller number sent to the outgoing channel;
- *RedirPN* – intended for modifications based on the analysis of the number of the subscriber that redirected the call sent to the outgoing channel.

3.1.4.1 List of Available CDR Fields

You can select the fields to be written to CDR files and configure their order. The *Available* column displays all the fields available for adding; the *Added* column displays the fields in the order they will be written to CDR files.

The following buttons are located under the list:

- *Add all* – relocate all available fields to the *Added* column;
- *Remove all* – remove all fields from the *Added* column;
- *Default* – the basic set of fields remains in the *Added* column (see the list of fields in section 3.1.4.2).

You can add or remove the desired fields by dragging them to the corresponding column with the left mouse button. The *Added* column is numbered according to the sequence number of the field in the CDR file.

3.1.4.2 Default CDR Format

- First line – a general header for an entire CDR file (this parameter is displayed if the corresponding setting is selected);
- Next lines – CDRs in the form of fields separated by semicolons “;”. The basic set of fields is as follows:

- discriminant;
- connection establishment time in the YYYY-MM-DD hh:mm:ss format (in case of unsuccessful calls, this parameter is equal to the disconnection time);
- call duration, seconds;
- cause of disconnection according to ITU-T Q.850;
- call status in case of disconnection;

- Caller information:

- IP address;
- source type;
- description – subscriber/trunk name (TG);
- caller number on input;
- caller number on output.

- Callee information:

- IP address;
- destination type;
- description – subscriber/trunk name (TG);

List of fields CDR used	
Added	Available
1. Device Sign	Redirecting mark
2. Connect time	Pickup mark
3. Duration	Release side mark
4. Release cause	Incoming SIP Call-ID
5. Call release info	Outgoing SIP Call-ID
6. Incoming IP-address	Incoming SS7 category
7. Incoming type	Incoming Calling party category (RUS)
8. Incoming description	Outgoing SS7 category
9. Incoming CgPN	Outgoing Calling party category (RUS)
10. Outgoing CgPN	Sequence number
11. Outgoing IP-address	Incoming redirecting number
12. Outgoing type	Outgoing redirecting number
13. Outgoing description	RADIUS Accounting-Session-Id
14. Incoming CdPN	Global Callref
15. Outgoing CdPN	Incoming numplan
16. Setup time	
17. Disconnect time	

-
- callee number on input;
 - callee number on output;
 - call received time in the format: YYYY-MM-DD hh:mm:ss;
 - connection termination time in the format: YYYY-MM-DD hh:mm:ss.

3.1.4.3 Description of CDR Fields

Discriminant – a user-configurable string that identifies the device;

Call received time, call response time, disconnect time – time of the corresponding event in the following format: “YYYY-MM-DD HH:MM: SS.MSEC”;

Call duration – counted in seconds “SS”; if the rounding method is set to “no rounding”; milliseconds are sent after the separating point: “SS.MSEC”;

Q.850 disconnect cause – numeric disconnect code, as recommended by ITU-T Q.850;

Call statuses in case of disconnection:

- user answer – successful call;
- user called, but unanswer – unsuccessful call, no response from subscriber;
- unassigned number – unsuccessful call, the number is not assigned;
- user busy – unsuccessful call, the user is busy;
- uncomplete number – unsuccessful call, the number is not complete;
- out of order – unsuccessful call, the terminal equipment is not available;
- unavailable trunk line – unsuccessful call, the trunk is not available;
- unavailable voice-chan – unsuccessful call, no free voice links available;
- access denied – unsuccessful call, access denied;
- RADIUS-response not received – unsuccessful call, no response from the RADIUS server;
- unspecified – unsuccessful call, another cause.

IP address of the caller/callee – IP address, if the call is made by SIP/H. 323 protocols. If the call is made not over the IP network, the value 0.0.0.0 will be written into the field.

Source and Destination Types

- SIP-user – SIP subscriber;
- fxs-port/fxo-port;
- user-service – use of VAS, only for the source type;
- trunk-SIP – SIP trunk;
- trunk-SS7 – SS-7 trunk;
- trunk-Q931 – ISDN PRI trunk.
- trunk-H.323 – H.323 trunk.

Caller description – contains the text name of the trunk through which the call was made, or the caller’s name. If the call is initiated by VAS, the description can take the following values:

- *Redirection* – call forwarding;
- *CallTransfer* – call transfer;
- *CallPickup* – call pickup;
- *ServiceManagement* – management of VAS;
- *Conference* – ad-hoc conference;
- *IVR* – call from IVR system;

-
- *3way* – three-way conference;

Incoming/outgoing number of the caller – the caller’s number at the input (before modification in the incoming TG) or at the output (after all modifications in the incoming and outgoing TGs);

Incoming/outgoing number of the callee – the callee’s number at the input (before modification in the incoming TG) or at the output (after all modifications in the incoming and outgoing TGs);

Forwarding Tag:

- *normal* – the call w/o forwarding;
- *redirecting* – the caller has redirected the call to the callee;
- *redirected* – the call initiated by the caller has been redirected to another subscriber.

Interception tag:

- *normal* – the call passed without interception;
- *pickup* – the call was intercepted.

Disconnect initiator tag:

- *originate* – call ended by the caller;
- *originate* – call ended by the callee.
- *internal* – call ended by the device (SMG).

Incoming/outgoing SS7 CIC – CIC number for the incoming/outgoing call. If the call was made not through the SS7 interface, the field will be empty;

Incoming/outgoing Call-ID – Call-ID for the incoming/outgoing call. If the call was made not through the SIP interface, the field will be empty;

Incoming/outgoing SS7 category – the caller category in SS7 line at the input (before modification in the incoming TG) or at the output (after all modifications in the incoming and outgoing TGs);

Incoming/outgoing Caller ID category – the Caller ID category at the input (before modification in the incoming TG) or at the output (after all modifications in the incoming and outgoing TGs);

Incoming/outgoing E1 stream – number of the incoming/outgoing E1 stream. If the call was made not through E1 stream, the field will be empty;

Incoming/outgoing E1 channel – number of the incoming/outgoing E1 channel. If the call was made not through E1, the field will be empty;

Sequential record number – two numbers separated by a hyphen. The first number is the timestamp generated when the device starts, the second is the CDR record sequential number;

Incoming/outgoing redirecting number – the redirecting number at the input (before modification in the incoming TG) or at the output (after all modifications in the incoming and outgoing TGs);

RADIUS Accounting-Session-Id – the Acct-Session-Id attribute value sent to RADIUS;

Global Callref – Global Call Reference field, which is formed as follows:
“|XX.XX.XX|YY.YY.YY.YY.YY”, where:

XX.XX.XX – own point code (OPC) in little-endian HEX format;

YY.YY.YY.YY.YY – sequential call number in little-endian HEX format;

Incoming/outgoing numbering schedule – the number of the numbering schedule in which the call arrived and left.

3.1.4.4 CDR File Example

An example CDR file containing four entries. The file header is enabled and the following fields are selected:

1. sequential record number;
2. discriminant;
3. call received time;
4. call response time;
5. call disconnect time;
6. call duration;
7. disconnect cause Q.850;
8. call status in case of disconnection;
9. disconnect initiator tag;
10. forwarding tag;
11. pickup tag;
12. caller type;
13. caller description;
14. incoming E1 stream;
15. caller IP address;
16. incoming number of the caller;
17. outgoing number of the caller;
18. callee type;
19. callee description;
20. outgoing E1 stream;
21. callee IP address;
22. incoming number of the callee;
23. outgoing number of the callee.

RADIUS Accounting-Session-Id
SMG200. CDR. File started at '20161213115258'

20161210124301-00000;SMG 200 ELTZ;2016-12-13 11:52:58.126;2016-12-13 11:52:58.465;2016-12-13 11:52:58.479;0.014;16;user answer;originate;normal;normal;trunk-SIP;sipp_in;;192.168.0.123;20001;20001;trunk-SS7;TrunkSS7_00;0;0.0.0.0;10001;10001;11000321584f7eaa 65a813f9 53681e51;

20161210124301-00001;SMG 2016 ELTZ;2016-12-13 11:52:58.134;2016-12-13 11:52:58.462;2016-12-13 11:52:58.483;0.021;16;user answer;originate;normal;normal;trunk-SS7;TrunkSS7_01;1;0.0.0.0;20001;20001;trunk-SIP;sipp_out;;192.168.1.123;10001;10001;06000106584f7eaa 59a880c4 5b369253;

20161210124301-00002;SMG 200 ELTZ;2016-12-13 11:52:58.026;2016-12-13 11:53:00.049;2016-12-13 11:53:00.062;0.013;16;user answer;originate;normal;normal;trunk-SIP;sipp_in;;192.168.0.123;20000;20000;trunk-SS7;TrunkSS7_00;0;0.0.0.0;10000;10000;11000043584f7ea9 5068f1a1 418fbc82;

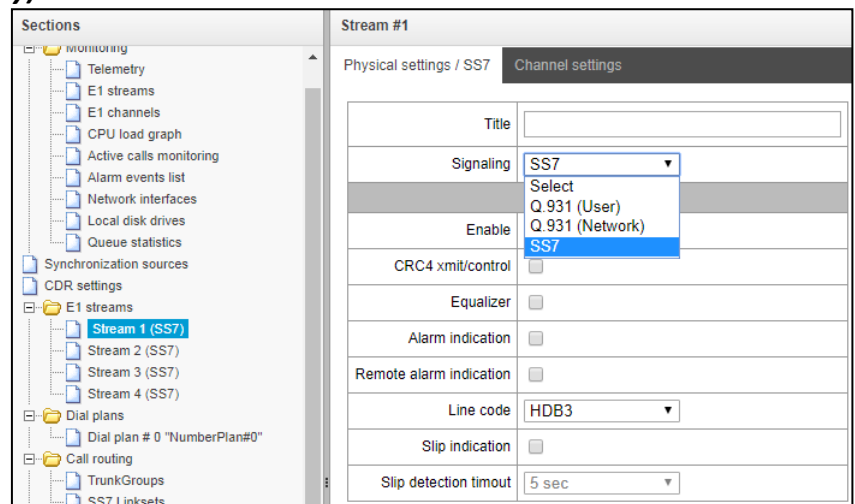
20161210124301-00003;SMG 200 ELTZ;2016-12-13 11:52:58.034;2016-12-13 11:53:00.046;2016-12-13 11:53:00.066;0.020;16;user answer;originate;normal;normal;trunk-SS7;TrunkSS7_01;1;0.0.0.0;20000;20000;trunk-SIP;TrunkAsterisk;;192.168.69.123;10000;10000;06000105 584f7eaa 7f14fecf 2a88c6d7.

3.1.5 E1 streams (for SMG-500 only)

To select signaling protocol for a stream, use the 'Signaling protocol' drop-down list.

The device supports the following signaling protocols:

- Q.931 (User);
- Q.931 (Network);
- SS7.



3.1.5.1 Configuring physical settings

Physical settings:

- *Name* – E1 stream name;
- *Enable* – physically enable stream;
- *CRC4 xmit/control* – CRC4 check sum generation at transmission and control at the reception;
- *Equalizer* – when checked, transmitted signal will be amplified;
- *Alarm indication* – when checked, fault indication will appear in case of local stream fault (ALARM LED will light up, alarm will be recorded to alarm log);
- *Remote alarm indication* – when checked, fault indication will appear in case of remote stream fault (ALARM LED will light up, alarm will be recorded to alarm log);
- *Line code* – type of information encoding in a channel (HDB3, AMI);
- *Slip indication* – when checked, fault indication will appear when slips are identified in the reception path;
- *Slip detection timeout* – stream parameter polling frequency; if the slip is detected in that stream, the gateway will indicate an alarm for the duration of this timeout.

3.1.5.2 Q.931 signalling protocol configuration

'Physical settings/Q.931' tab

Stream #1	
Physical settings / Q.931 Calling name translation settings Channel settings	
Title	<input type="text"/>
Signaling	Q.931 (User) ▼
Physical settings	
Enable	<input checked="" type="checkbox"/>
CRC4 xmit/control	<input type="checkbox"/>
Equalizer	<input type="checkbox"/>
Alarm indication	<input type="checkbox"/>
Remote alarm indication	<input type="checkbox"/>
Line code	HDB3 ▼
Slip indication	<input type="checkbox"/>
Slip detection timeout	5 sec ▼
Q.931 LAPD	
T200, x100 ms ⓘ	<input type="text" value="10"/>
T203, x100 ms ⓘ	<input type="text" value="100"/>
N200 ⓘ	<input type="text" value="3"/>
Q.931 settings	
TrunkGroup	not set ▼
Scheduled routing profile	not set ▼
Access category	[0] AccessCat#0 ▼
Dial plan	[0] NumberPlan#0 ▼
Numbering plan type	Unknown ▼
Calling party category (RUS)	1 ▼
Send calling party category (RUS)	<input type="checkbox"/>
'End-of-dial' message	<input type="checkbox"/>
Do not send RESTART for interface	<input type="checkbox"/>
Do not send RESTART for channel	<input type="checkbox"/>
Channels selection order	Successive forward ▼
DialTone for incoming overlap-seize	<input type="checkbox"/>
Process PI 'In-band' in DISCONNECT	<input type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Q.931 LAPD – LAPD channel level settings of Q.931 protocol

- *T200* – transmission timer. This timer defines time period for frame response reception that will enable the following frames' transmission. This time period should be greater than the time required for frame transmission and its acknowledgement reception.
- *T203* – maximum time during which the device may not exchange frames with the opposite device.

- *N200* – quantity of frame retransmission attempts.

Q.931 settings

- *Trunk group* – name of a trunk group, that E1 stream ;
- *Scheduled routing profile* – select scheduled routing profile from the list of existing profiles;
- *Access category* – select access category;
- *Dial plan* – define dial plan that will be used for routing of the call received from this port (necessary for dial plan negotiation);
- *Numbering plan type* – define ISDN dial plan type. To use common dial plan E.164, select 'ISDN/telephony';
- *Calling category for incoming calls* – Caller ID category assigned to calls received from this port;
- *Send calling category* – enable Caller ID category transmission as the first digit of a number in CgPN information element of the SETUP message.



For proper operation, it is required to support this setting on the opposite party.

- *'End of dial' message* – produce 'Sending Complete' informational element upon 'End of dial' event (such event arrives from the linked channel side, achieved maximum quantity of digits according to prefix, dialing timeout for the next digit);
- *Do not send RESTART for interface* – when checked, gateway will not send RESTART message into the line when the stream is restored (channel level LAPD is established);
- *Do not send RESTART for channel* – when checked, gateway will not send RESTART message upon the expiration of T308 timer. This timer activates when RELEASE message is sent into the channel and resets when it receives RELEASE COMPLETE message as a response. If RELEASE COMPLETE message is not received during T308 timer active state, RESTART message is transmitted in order to release the channel.
- *Capturing a channel* – defines the order of the physical channel provisioning when performing outgoing call. You may select one of four types: sequential forward, sequential back, from the first and forward, from the last and back. To minimize conflicts during communication with neighboring PBXes, we recommend to set inverse channel engagement types.
- *DialTone for incoming overlap seize* – when checked, gateway will send DialTone into the line during incoming overlap seize ('PBX response' ready signal). In this case, overlap seize is a reception of SETUP message without 'sending complete' indication;
- *Process PI In-Band in DISCONNECT* – when checked, field PI In-Band contained in DISCONNECT message will be processed for call release voice message transmission, otherwise this field is ignored.

3.1.5.2.1 "Name delivery settings" tab

Stream #1

Physical settings / Q.931
Calling name translation settings
Channel settings

Calling name translation settings

Name transmission	not set ▼
Name coding	Transit ▼

Use the tab to configure the way of name reception/transmission and coding of received/transmitted name.

- Name delivery method:
 - *None* – name delivery is disabled;
 - *Q.931 DISPLAY* – transmission by using Q.931 Display element with Codeset 5;
 - *QSIG-NA* – transmission via QSIG-NA (ECMA-164) protocol;
 - *CORNET* – transmission via Siemens CorNet protocol;
 - *CORNET HICOM-350* – transmission via Siemens CorNet protocol with additional info for Hicom PBX;
 - *AVAYA DISPLAY* – transmission in Q.931 Display element with Codeset 6.

- Name coding method:
 - *Transit* – recoding is not available (name format is UTF-8 by default);
 - *CP 1251* – code of Windows-1251;
 - *Siemens adaptation* – code of Siemens PBX;
 - *AVAYA adaptation* – code of AVAYA PBX;
 - *Transliteration into latin script* – Russian names will be transliterated into Latin script.

Method is selected for name reception/transmission and coding work only in a configurable E1 stream. Transmission between streams differing by the settings of name delivery parameters is possible. In case of such transmission, the SMG will be decoded automatically to synchronize the sides.

3.1.5.2.2 “Channel usage” tab

You may enable/disable E1 stream channel in this menu. To do that, select/deselect checkbox against the corresponding channel. “Trunk group” column displays number of group where these channels are configured (used only when trunk group is assigned to channels, not to the whole stream).

The screenshot shows the ELTEX software interface. On the left is a sidebar with a tree view of system settings. The main window has three tabs: "Physical settings / Q.931", "Calling name translation settings", and "Channel settings". The "Channel settings" tab is active, displaying a table of channel configurations for Stream #1. The table has columns for "№", "Enable", and "TrunkGroup" for channels 0 through 31. Channels 1 through 31 are all checked in the "Enable" column and have "not set" in the "TrunkGroup" column. Channel 0 is disabled and has a "—" in the "TrunkGroup" column. Below the table are "Apply" and "Cancel" buttons.

№	Enable	TrunkGroup	№	Enable	TrunkGroup
0	<input type="checkbox"/>	—	16	<input type="checkbox"/>	—
1	<input checked="" type="checkbox"/>	not set	17	<input checked="" type="checkbox"/>	not set
2	<input checked="" type="checkbox"/>	not set	18	<input checked="" type="checkbox"/>	not set
3	<input checked="" type="checkbox"/>	not set	19	<input checked="" type="checkbox"/>	not set
4	<input checked="" type="checkbox"/>	not set	20	<input checked="" type="checkbox"/>	not set
5	<input checked="" type="checkbox"/>	not set	21	<input checked="" type="checkbox"/>	not set
6	<input checked="" type="checkbox"/>	not set	22	<input checked="" type="checkbox"/>	not set
7	<input checked="" type="checkbox"/>	not set	23	<input checked="" type="checkbox"/>	not set
8	<input checked="" type="checkbox"/>	not set	24	<input checked="" type="checkbox"/>	not set
9	<input checked="" type="checkbox"/>	not set	25	<input checked="" type="checkbox"/>	not set
10	<input checked="" type="checkbox"/>	not set	26	<input checked="" type="checkbox"/>	not set
11	<input checked="" type="checkbox"/>	not set	27	<input checked="" type="checkbox"/>	not set
12	<input checked="" type="checkbox"/>	not set	28	<input checked="" type="checkbox"/>	not set
13	<input checked="" type="checkbox"/>	not set	29	<input checked="" type="checkbox"/>	not set
14	<input checked="" type="checkbox"/>	not set	30	<input checked="" type="checkbox"/>	not set
15	<input checked="" type="checkbox"/>	not set	31	<input checked="" type="checkbox"/>	not set

3.1.5.3 SS7 protocol configuration

'Physical settings/SS7' tab

SS7 settings:

- *SS7 Linkset* – link set selection (SS7 link set);
- *Channel ID (SLC)* – signal line identifier in SS7 link set;
- *DPC-MTP3* – destination point code of the signalling transition point (STP). Used during SMG operation in quasi-associated mode. If quasi-associated mode is not required, set value 0. At that, MTP3 opposite code is equal to DPC-ISUP value defined in configuration (Section 3.1.7.2 SS7 link sets (for SMG-500 only));
- *D-channel* – number of the channel timeslot that will be used for signaling transmission;



Move to 'channel settings' tab after changing the number of D channel on a stream with SS7 and set the appropriate CIC for the same channel timeslot that you have already set for D channel.

- *Bit D in LSU* – set value 1 for bit D in status field (SF) of a signal unit LSSU (bits D-F in status field SF are reserved).

3.1.6 Numbering Schedule

This section describes how to configure the numbering schedule of the device.

The device features up to 16 independent numbering schedules. Every numbering schedule may have its own subscribers and prefixes. To set the number of active schedules, see section 3.1.1.

The device routes calls using 3 criteria:

- search by caller number – CgPN (Calling Party Number);
- search by callee number – CdPN (Called Party Number);
- search by the database of subscribers configured on the device.

When a call arrives to a numbering schedule, its routing begins. First, a search for matches to CgPN number masks is performed, then a search by the database of subscribers configured on the device is done. If a match against any of this parameters is found, the call is routed and further search is stopped.

Search and call routing using the configured subscriber database is performed even when there is a match between call parameters and CgPN number mask.

When call parameters do not match CgPN masks and the subscriber number, a search by all CdPN masks configured in the numbering schedule is performed.



If both CgPN and CdPN number masks are configured in prefix parameters, this rule uses OR logic, i. e. the call is not analysed for CgPN and CdPN numbers simultaneously.

Dial plans

Dial plan settings # 0

Name

Check dial plan by number ST

Search masks by template

Default VAS prefixes

Prefixes in the dial plan

No	Description	Masks for CgPN	Masks for CdPN	Type	Object	Dial mode	Priority	
0	2016	(no masks)	(x.[46xxx]543210) ⇒	TrunkGroup	trunk2016	no change (+)	100	<input type="checkbox"/>
1	OUT	(no masks)	(1234567890[134]xxxx) ⇒	TrunkGroup	out	no change (+)	100	<input type="checkbox"/>
2	IN	(no masks)	(42xxxx) ⇒	TrunkGroup	in	no change (+)	100	<input type="checkbox"/>
3	Prefix#03	(no masks)	(no masks)	IVR scenario	not set	no change (+)	100	<input type="checkbox"/>

10 Rows in the table to show Current page 1 from 1

Numbering Schedule Parameters

- *Name* – name of the numbering schedule.

Numbering check by number – checks if routing is possible for the number entered into this field.

The check is performed by the caller and callee masks and also in the configured SIP subscriber database.

- *ST* – when this option is checked, the search recognises the end dial marker.


Wildcard masks search – searches a prefix by the number template.
The check provides information on routing capability for this number:

- *calling-table* – routing by the caller table;
- *called-table* – routing by the callee table;
- *NOT found in* – routing by this table is not possible;
- *found in* – routing by this table is possible;
- *Abonent 'SIP' idx[4]* – SIP subscriber [entry number for this subscriber in the database];
- *FXS port [1].* – FXS subscriber [subscriber's port number];
- *Prefix [6]* – routing by a prefix [the prefix number in the list].

Copying Prefixes to Another Numbering Schedule

- *Copy selected prefixes to numbering schedule* – this option allows you to copy the selected prefixes to another numbering schedule. To do this, select the prefixes and the target numbering schedule, and click the “Copy” button;
- *Copy all prefixes to numbering schedule* – this option allows you to copy all prefixes in the current numbering schedule to another numbering schedule. It works in the same way as copying selected prefixes, but does not require selection of prefixes.

3.1.6.1 Creating a Prefix in the Numbering Schedule

To create a new prefix, open the *Objects* menu and click *Add Object* or click the  button located below the list and enter prefix parameters in the opened form:

Dial plans

Common prefix settings 1	
Title	OUT
Dial plan	[0] NumberPlan#0
Access category	[0] AccessCat#0
Check access category	<input type="checkbox"/>
Prefix type	TrunkGroup
TrunkGroup	[1] out
Direction	local network
Dial mode	unchanged
Do not send end-of-dial (ST)	<input type="checkbox"/>
Priority	100
Max session time (sec)	0
CdPN settings	
Number type	unchanged
Numbering plan type	isdn/telephony
Direct route timers	
Short timer	5
Duration	30
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Main Prefix Parameters

- *Name* – name of the numbering schedule;
- *Numbering schedule* – select the numbering schedule;
- *Access category* – select an access category;
- *Check access category* – when this option is checked, it checks the possibility of call routing by the prefix based on the rules determined by access categories;
- *Prefix type* – select the prefix type:
 - *trunk group* – transition to a trunk group;
 - *trunk direction* – transition to a trunk direction;
 - *change numbering schedule* – this option allows you to enter another numbering schedule when this prefix is dialled. When this prefix type is selected, the *New Numbering Schedule* option becomes available, where you should specify the numbering schedule for transition;
 - *modifier* – enables setting the subscriber capacity of the device. If the number is present in the subscriber capacity but not yet assigned to any subscriber, a call to such a number will trigger a clearback message with the cause code: 1 – Unallocated (unassigned) number;
 - *VAS prefix* is used to manage VAS services from the telephone set;
 - *interception group* is used to configure the interception group transition prefix;
 - *IVR script* is used to configure the IVR script pickup group transition prefix.

Parameters of the “Trunk Group and Trunk Direction” Prefix

Main Prefix Parameters:

- *Trunk group* – the trunk group to which the call will be routed by this prefix.
- *Direction* – the trunk group access type: local, emergency, zone, private, long-distance, international. The prefix is used when enabling SORM function in the network, as well as to restrict a connection if a failure occurs during the data exchange with the RADIUS server (see section 3.1.14 RADIUS Configuration);
- *Dial mode* – the method of number transmission:
 - *enblock* – wait for collection of the entire address information;
 - *overlap* – do not wait for collection of the entire address information.
- *Do not send end dial (ST)* – when this option is checked, the end dial marker is not sent (ST in SS or *sending complete* in PRI);
- *Priority* – if there are some overlapping masks in the numbering schedule, the call will be made into the prefix with a higher priority. The value 0 is the highest priority, 100 – the lowest priority;
- *Call duration limitation (sec)* – limit duration of calls passed through this prefix.

CdPN Parameters

- *Number type* – the callee number type: unknown, subscriber number, national number, international number, no change. The selected number type will be sent in SS-7, ISDN PRI, SIP-I/T signalling messages during an outgoing call by a prefix (*no change* means that the number type will not be converted, i. e. it will be sent in the form it has been received from the incoming channel).

- *Numbering schedule type* – the callee's numbering schedule type; may take the following values: unknown, isdn/telephony, national, private, no change. The selected numbering schedule type will be sent in ISDN PRI signalling messages during outgoing call by a prefix (*no change* means that the number type will not be converted, i. e. it will be sent in the form it has been received from the incoming channel).

Timers for direct out (used when trunk groups are directly connected without prefix mask analysis – the *Direct Prefix* function in trunk group settings).

These timers work only when dialling in the **overlap** mode:

- *Short timer* – the time interval in seconds when the digital gateway will wait for further dialling if a part of address information has already been received. The default value: 5 seconds.
- *Duration* – the timer for number dialling duration. The default value: 30 seconds.

Parameters of the “Change Numbering Schedule” Prefix

- *New numbering schedule* – the numbering schedule to which the call will be transferred;
- *New access category* – the category assigned to the caller after switching to another numbering schedule;
- *Priority* – if there are some overlapping masks in the numbering schedule, the call will be made into the prefix with a higher priority. The value 0 is the highest priority, 100 – the lowest priority;
- *Call duration limitation (sec)* – limit duration of calls passed through this prefix;
- *Modifiers for changing a numbering schedule:*
 - *CdPN modifiers* – intended for modifications based on the analysis of the callee number;
 - *CgPN modifiers* – intended for modifications based on the analysis of the caller number.

Parameters of the “VAS Prefix”

- *VAS service type* – select the VAS service type to manage it from the subscriber's telephone set:
 - *CFU* – Call Forwarding Unconditional;
 - *CFB* – Call Forwarding Busy;
 - *CFNR* – Call Forwarding No Reply;
 - *CFOS* – Call Forwarding Out of Service;
 - *Call pickup* – call pickup;
 - *Conference* – conference call;
 - *Clear All* – cancel all services;
 - *Intercom* – intercom call (with an automatic answer from party B);
 - *Paging* – similar to Intercom, but with a call to conference numbers;
 - *Password* – password setting;
 - *Password once* – access by password;
 - *Password access* – password activation;
 - *Restrict out* – restriction of outgoing communication;
 - *Follow me* – managed forwarding “Follow me”;

-
- *Follow me (no response)* – managed “Follow Me” forwarding when there is no answer.
 - *Action* – select an action for the service:
 - *Enable* – enable VAS service;
 - *Cancel* – cancellation of VAS service;
 - *Control* – VAS service activity control.

Parameters of the “Interception Group” Prefix

- *Interception group* is a group in which a call is intercepted when this prefix is dialled. When you select the “Any” group, interception will be performed in all groups;
- *Priority* – sets the prefix priority within the range from 0 to 100. A prefix with a smaller value has a higher priority (0 is the highest priority, 100 is the lowest).
- *Call duration limitation (sec)* – limit duration of calls passed through this prefix.

Timers for direct out (used when trunk groups are directly connected without prefix mask analysis – the *Direct Prefix* function in trunk group settings).

These timers work only when dialling in the **overlap** mode:

- *Short timer* – the time interval in seconds when the digital gateway will wait for further dialling if the dialled number already matches a sample in the numbering schedule, but additional digits may be also dialled, which will result in a match to another sample. The default value: 5 seconds.
- *Duration* – the timer for number dialling duration. The default value: 30 seconds.

Parameters of the “IVR Script” Prefix

- *IVR script* is an IVR script to which a call will be routed by this prefix.
- *Priority* – sets the prefix priority within the range from 0 to 100. A prefix with a smaller value has a higher priority (0 is the highest priority, 100 is the lowest).
- *Call duration limitation (sec)* – limit duration of calls passed through this prefix.

Timers for direct out (used when trunk groups are directly connected without prefix mask analysis – the *Direct Prefix* function in trunk group settings).

These timers work only when dialling in the **overlap** mode:

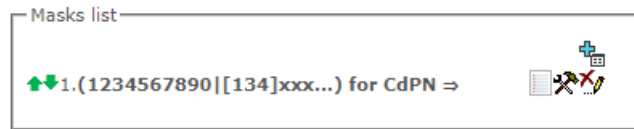
- *Short timer* – the time interval in seconds when the digital gateway will wait for further dialling if the dialled number already matches a sample in the numbering schedule, but additional digits may be also dialled, which will result in a match to another sample. The default value: 5 seconds.
- *Duration* – the timer for number dialling duration. The default value: 30 seconds.

Mask List

For created numbering schedules, the *Mask List* section allows you to configure the number masks for routing by this prefix.

To generate the list, use the following buttons:

- *add Mask*;
- *edit Mask*;
- *remove Mask*;
- *view Mask*.



Using green arrows to the left of the created mask, you can move the entries in the table by prioritising them.

- *Mask* – a template or a set of templates, which is compared to the caller or callee number received from the incoming channel. It is used for further call routing (for mask syntax, see section 3.1.3.1).
 - *Type* – mask type. Defines the number for the call routing – caller number (calling) or callee number (called).
 - *Long timer* – the time interval in seconds when the digital gateway will wait for the next digit dialling until a match to a sample from the numbering schedule is established. The default value: 10 seconds.
 - *Short timer* – the time interval in seconds when the digital gateway will wait for further dialling if the dialled number already matches a sample in the numbering schedule, but additional digits may be also dialled, which will result in a match to another sample. The default value: 5 seconds.
 - *Duration* – the timer for number dialling duration. The default value: 30 seconds.

To *edit a prefix*, double-click the prefix row in the prefix table with the left button or select the prefix and click the button below the list.

To *delete a prefix*, select the prefix and click the button below the list or open the *Objects* menu and select *Remove Object*.

3.1.6.2 Description of Number Mask and Its Syntax

Number mask is a set of *templ* templates delimited by the special character '|'. The mask should be enclosed into parentheses. (templ) is equal to (templ1|templ2|...|templN).

Syntax:

- **X** or **x** – any digit;

- * – an asterisk (*);
- # – a sharp (#);
- 0–9 – digits from 0 to 9;
- D – character D.
- . – the *dot* is a special symbol which means that the preceding character may be repeated any number of times (30 characters max. for one number), e. g.:
- (34x.) – all possible number combinations that begin with “34”.
- [] – defines a range (with a hyphen) or an enumeration (w/o spaces, commas, and other characters between the digits) of prefixes, e. g.:
 - the range ([1–5]XXX) – all 4-digit numbers that begin with 1, 2, 3, 4, or 5.
 - the enumeration ([138]xx) – all 3-digit numbers that begin with 1, 3, or 8.
- {min, max} – defines the number of repetitions for the character outside the parentheses, e. g.:
 - (1x{3,5}) – means that there may be from 3 to 5 arbitrary digits (x) and it corresponds to the mask (1xxx|1xxxx|1xxxxx).
- | – vertical bar. Logical **OR** – separates templates in a mask;
- ! – exclamation mark. When used before a template, it indicates a negation, that is a mismatch between the number and the template;
- (-) – the mask used only in CgPN number modifier tables for calls without caller number. Allows the caller number to be added if it was missing and also specifies indicators for that number.



If a numbering schedule contains overlapping prefixes, then the prefix with the most accurate mask for a specific number will have a higher priority during the number processing in the numbering schedule, e. g.:

Prefix 1: (2xxxx)

Prefix 2: (23xxx)

When the number “23456” arrives to the numbering schedule, it will be processed with prefix 2.

Also, the masks containing an arbitrary number of repetitions (x.) or a range of repetitions {min, max} have a lower priority than the masks with an accurate number of characters, e. g.:

Prefix 1: (2x{4,7})

Prefix 2: (23xxx)

When the number “23456” arrives to the numbering schedule, it will be processed with prefix 2.

The masks with a specified range of repetitions {min, max} have a higher priority than the masks with an arbitrary number of repetitions (x.), e. g.:

Prefix 1: (2x.)

Prefix 2: (2x{4,7})

When the number “23456” arrives to the numbering schedule, it will be processed with prefix 2.

3.1.6.3 Mask Operation Examples

Example 1

(#XX#|*#XX#|*XX*X.#|112|011|0[1-4]|6[2-9]XXX|5[24]XXXXX|810X{11, 15})

The mask contains 9 templates:

1. **#XX#** – any 4-digit number that begins and ends with #; the 2nd and the 3rd digits of the number may take any values from 0 to 9, as well as * or #.
In general, this template disables VAS utilisation from the phone unit.
2. ***#XX#** – any 5-digit number that begins with *# and ends with #, the 3rd and the 4th digits of the number may take any values from 0 to 9, as well as * or #.
In general, this template is used to control VAS utilisation from the phone unit.
3. ***XX*X.#** – an N-digit number which begins with * followed by two arbitrary digits (from 0 to 9, as well as * and #), then by *, and then by any number of any digits (from 0 to 9, *) until # is met.
In general, this template is used to order VAS utilisation from the phone unit.
4. **112** – dialling the specific 3-digit number (112).
5. **011** – dialling the specific 3-digit number (011).
6. **0[1-4]** – a 2-digit number that begins with 0 and ends with 1, 2, 3, or 4, i. e. 01, 02, 03, or 04.
7. **6[2-9]XXX** – a 5-digit number that begins with 6, with the second digit of the number being any digit from 2 to 9, and the last three digits being any digits from 0 to 9, as well as * and #.
8. **5[24]XXXXX** – a 7-digit number that begins with 5, with the second digit of the number being 2 or 4, and the last five digits being any digits from 0 to 9, as well as * and #.
9. **810X{11, 15}** – a number that begins with 810 followed by 11 to 15 arbitrary digits from 0 to 9, as well as * and #. Taking into account the first three digits, the length of the number according to this rule is from 14 to 18 digits.

Example 2

A numbering schedule configuration is required to allow all numbers that begin with 1 and have the length of 3, to be routed to Trunk0, and number 117 to be individually routed to Trunk1.

To solve this task, configure the following prefixes:

1. Route the first prefix with the mask **(117)** to Trunk1;
2. Route the second prefix with the mask **(11[0-689]|1[02-9]x)** to Trunk0.

Templates of the second prefix overlap all “1xx” numbers except for 117.

Example 3

You want to configure a dial plan by deleting a few numbers from the group. Number group: 2340000-2349999, excluded numbers: 2341111, 2341112, 2341113, 2341114, 2341115, 2341234.

Such mask is set as follows: **(234xxxx|!234111[1-5]|!2341234)**

3.1.6.4 Timer Operation Examples

Consider an example of timer operation for dialling with 011 number overlap (example 1 from the previous section). Let us assume that the timer has the following values set:

- L = 10 seconds.
- S = 5 seconds.

Receiving the first digit – 0. A mask for such a dial includes 2 rules: 011 and 0[1-4]. The first received digit does not provide any complete match to any of the rules, therefore the L-timer is activated (10 seconds) to wait for the next digit. If the next digit does not come in 10 seconds, a timeout will be registered. Since there are no matches to the rules, the timeout will result in dial error.

Receiving the second digit – 1. Receiving the second digit results in a match to rule 6: 0[1-4] (prefix 01). Since the match is found, but there may also be a further match to rule 5 (that is 011), the S-timer is activated (5 seconds) to wait for the next digit. If the next digit does not come in 5 seconds, a timeout will be registered. Since there is a match to a rule, the call will be successfully directed according to this mask.

Receiving the third digit – 1. There is no match to rule 6 anymore, but the number matches rule 5 now. This match is final, since the mask has no more rules for further matches. The call is immediately routed according to rule 5.

3.1.6.5 Configuration example of a modifier type prefix

Objective

The following range of numbers is allocated to SMG: 26000 – 26199. However, not all numbers can be assigned to subscribers immediately. When an unassigned call arrives to a number in this range, SMG will reject it with cause of disconnection **3 – No route to destination**. But since this numbering is local to the gateway, it should have sent cause of disconnection **1 – Unallocated (unassigned) number**.

Solution


For correct clearback cause transmission, you should create local numbering – configure a “Modifier” type prefix.


To do this, in the **Numbering Schedule** section, add a new prefix with *Modifier* as the **Prefix Type** parameter value. In the prefix settings, add a list of prefix masks of the *Called* type. For the number range 26000-26199 specified in the objective, the mask will be as follows: **(26[0-1]xx)**.

3.1.7 Routing

3.1.7.1 Trunk Groups

TrunkGroups					
No	TrunkGroup	TrunkGroup member	Direct routing prefix	Disable ingress	Disable egress
0	trunk2016	SIP interfaces [0] "smg2016"	not set	-	-
1	out	SIP interfaces [1] "sout"	not set	-	-
2	in	SIP interfaces [2] "sin"	not set	-	-
3	PBX		not set	-	-
4	incoming		not set	-	-
5	SIP		not set	-	-

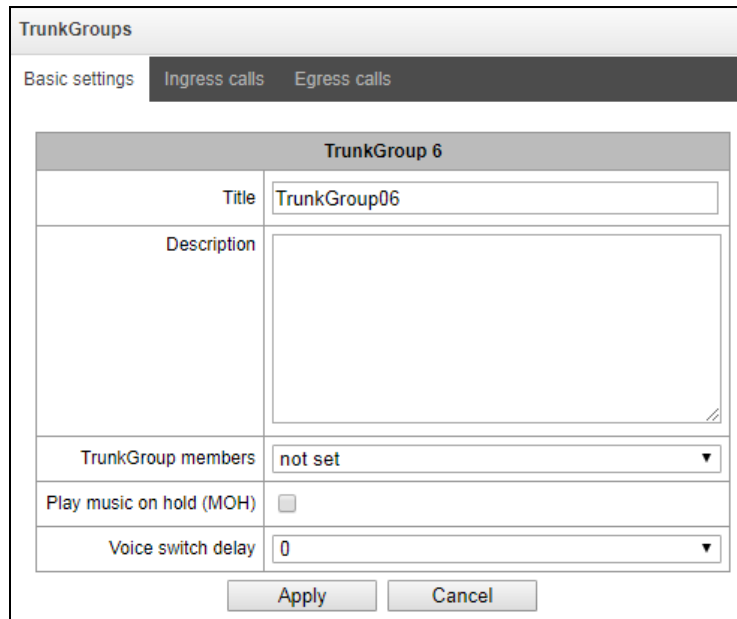
A trunk group is a set of connection lines (trunks), including the channels of E1 flow and data transmission bandwidth (IP channels). E1 flow channels are used for Q.931 and SS7. IP channel interfaces are SIP/SIP-T/SIP-I/H.323. To *edit a trunk group* double-click the corresponding row in the group table with the left mouse button or select the group and click the  button below the list.

To *delete a trunk group*, select the group and click the  button below the list or open the *Objects* menu and select *Remove Object*.

Up to 255 trunk groups are supported.

Trunk Group Creation

Basic Settings Tab



The screenshot shows the 'TrunkGroups' configuration window with the 'Basic settings' tab selected. The window title is 'TrunkGroup 6'. The fields are as follows:

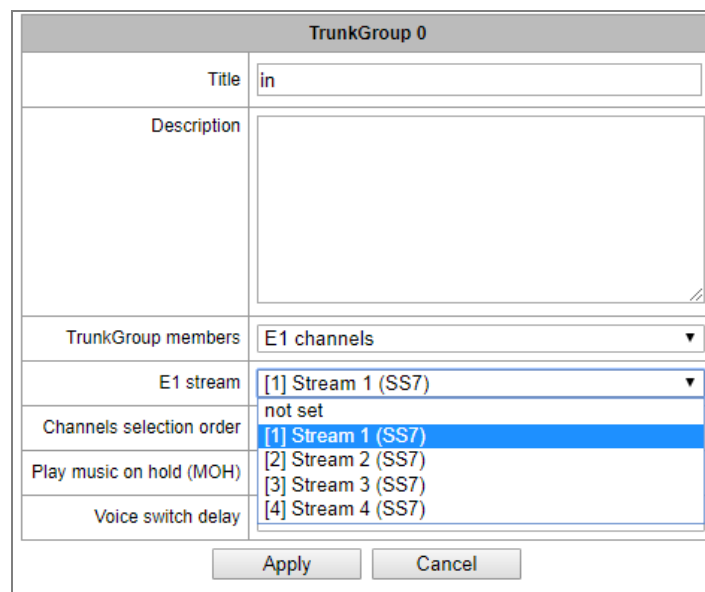
Title	TrunkGroup06
Description	
TrunkGroup members	not set
Play music on hold (MOH)	<input type="checkbox"/>
Voice switch delay	0

Buttons: Apply, Cancel



To access a trunk group, the device configuration should include prefixes that perform transition to this group.

- *Name and description* – the trunk group name and its description;
- *Group members* – trunk group members:
 - *Stream with Q.931 signaling, SS link set or SIP interface;*
 - *E1 stream channels* – E1 stream channels with Q.931, SS7 signalling protocols;
 - *E1 stream of SS7 link set.*
- *E1 Stream* – select E1 stream for trunk group assignment to E1 stream channels. This menu is active only when 'E1 stream channels' value is selected for 'Group contents'.



The screenshot shows the 'TrunkGroup 0' configuration window with the 'Basic settings' tab selected. The fields are as follows:

Title	in
Description	
TrunkGroup members	E1 channels
E1 stream	[1] Stream 1 (SS7)
Channels selection order	[1] Stream 1 (SS7)
Play music on hold (MOH)	<input type="checkbox"/>
Voice switch delay	0

Buttons: Apply, Cancel




A single trunk group may be assigned to channels only within a single E1 stream.

- *SS7 link set* – SS7 link set for selecting E1 streams. This menu is available only when you chose ‘E1 streams from SS7 link set’ in ‘Group membership’ menu.
- *Channel selection order* – channel selection order in E1 streams. This menu is available only when you chose ‘E1 stream from SS7 link set’ in ‘Group membership’ menu



You cannot set trunk group with SS7 Linkset and trunk group with E1 streams from the same SS7 Linkset simultaneously.

Incoming Communication Tab

TrunkGroups	
Basic settings	Ingress calls
Ingress calls	
Disable ingress calls	<input type="checkbox"/>
Direct routing prefix	not set
Use voice messages	<input type="checkbox"/>
No Connected number transit	<input type="checkbox"/>
Copy CgPN into Redirecting number	<input type="checkbox"/>
Use Redirecting number for routing	<input type="checkbox"/>
Alarm CPS value	0
Max CPS value	0
RADIUS profile	not used
Ingress calls modifiers	
Add	CdPN 
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	


- *Incoming call barring* – when this option is checked, the incoming calls are barred. Setting the call barring does not terminate any of the established connections;
- *Direct prefix* – the prefix will be used without caller or callee number analysis. It enables switching of all calls in a single trunk group to another group regardless of the dialed number (without mask creation in prefixes). When a number is dialed in the overlap mode, direct dialling timers are used, which are configured in the direct prefix.
- *Use voice messages* – when this option is selected, pre-recorded voice messages stored in the device memory will be played upon the occurrence of specific events. For detailed description, see Appendix I. Voice messages and music on hold (MOH);
- *Block Connected number transmission* – disable the transmission of the *Connected number* field;
- *Copy CgPN to Redirection* – when this option is checked, if there is no *Redirecting number* in the incoming call, it will be generated from the CgPN number;

- *Use Redirecting for routing* – when this option is checked, the SIP *diversion* field is used to route the incoming call in the numbering schedule using CgPN number masks;
- *Failure value of CPS* – the number of calls per second after which a failure will be indicated in the log. “0” value – the fault indication is turned off. Fault indication time – 5 minutes after exceeding the specified threshold of CPS;
- *CPS limit* – the maximum number of calls per second that can be received by a trunk group. “0” value – the CPS limit is turned off. The CPS value is calculated as the moving average for the last 3 seconds. For example, if 3xCPS calls arrive within the first second, they will be accepted, but if there are any additional calls within the next two seconds, they will be rejected;
- *RADIUS profile* – select the RADIUS profile to use (you can configure profiles in the *RADIUS Configuration/Profile List* menu, in section 3.1.14.2).

Incoming Communication Modifiers

- *CdPN modifiers* – intended for modifications based on the analysis of the callee number received from the incoming channel;
- *CgPN modifiers* – intended for modifications based on the analysis of the caller number received from the incoming channel.

Outgoing Communication Tab

TrunkGroups		
Basic settings	Ingress calls	Egress calls
Egress calls		
Disable egress calls	<input type="checkbox"/>	
Replace CgPN by Redirecting	<input type="checkbox"/>	
Check access category	<input type="checkbox"/>	
Reserve TrunkGroup	not set ▼	
Q.850 release cause list for reserve	not set ▼	
RADIUS profile	not used ▼	
Egress calls modifiers		
Add	CdPN ▼ 	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		




- *Outgoing call barring* – when this option is checked, the outgoing calls are barred. Setting the call barring does not terminate any of the established connections;
- *Replace CgPN with Redirecting* – when this option is checked, the CgPN number is replaced with Redirecting;
- *Check access category* – when this option is checked, it checks the possibility of call routing based on the rules determined by access categories;
- *Redundant trunk group* – specifies the trunk group a call will be routed to when routing to the current trunk group is not possible (all channels are engaged or inoperable).

- *Q.850 disconnect causes for transfer to reserve* – select the *List of Q.850 Disconnect Causes table* to configure the Q.850 disconnect causes initiating transfer to the reserve trunk group.
- *RADIUS profile* – select the RADIUS profile to use (you can configure profiles in the *RADIUS Configuration/Profile List* menu, in section 3.1.14.2).

Outgoing Communication Modifiers




- *CdPN modifiers* – intended for modifications based on the analysis of the callee number sent to the outgoing channel;
- *CgPN modifiers* – intended for modifications based on the analysis of the caller number sent to the outgoing channel;
- *Original CdPN modifiers* – intended for modifications based on the analysis of the original callee number sent to the outgoing channel;
- *RedirPN modifier* – intended for modifications based on the analysis of the redirecting number sent to the outgoing channel;
- *GenericPN modifiers* – intended for modifications based on the analysis of the generic number sent to the outgoing channel;
- *LocationNumber modifiers* – intended for modifications based on the analysis of the location number sent to the outgoing channel.

To create, edit, or remove groups (as well as other objects), use the *Objects – Add Object*, *Objects – Edit Object*, or *Objects – Remove Object* menus and the following buttons:

-  – Add Trunk Group;
-  – Edit Trunk Group Parameters;
-  – Remove Trunk Group.

3.1.7.2 SS7 link sets (for SMG-500 only)




SS7 Linksets			
No	SS7 Linkset	Linkset members	TrunkGroup
0	Linkset00	Stream 3 (SS7)	7_0
1	Linkset01	Stream 2 (SS7) Stream 4 (SS7)	7_1



For SS7 protocol configuration, see 'E1 streams' (section 3.1.5.3).

SS7 protocol is a set of signal links of a single direction. To create, edit or remove link sets, use '*Objects*' – '*Add object*', '*Objects*' – '*Edit object*' and '*Objects*' – '*Remove object*' menus and the following buttons:

-  – add SS7 link set;
-  – edit SS7 link set;
-  – delete SS7 link set.

SS7 Linksets	
SS7 Linkset 0	
Title	Linkset00
TrunkGroup	[2] 7_0
Access category	[0] AccessCat#0
Dial plan	[0] NumberPlan#0
Scheduled routing profile	Not set
Toll	<input type="checkbox"/>
Alarm indication	<input type="checkbox"/>
Channel selection	from first forward
Reserve SS7 Linkset	Not set
Combined mode	<input type="checkbox"/>
Primary SS7 Linkset	Not set
Secondary SS7 Linkset	Not set
SS7 Timers profile	Profile 0
MTP2 layer settings	
Emergency alignment for a single link	<input type="checkbox"/>
Service information (SIO)	
Network ID	00 - international network (DEC=
Routing label	
OPC	0
DPC-ISUP	1
ISUP subsystem	
Channels initialization mode	individual unblock
Send REL on receiving SUS	<input type="checkbox"/>
Add a digit in IAM for overlap	<input type="checkbox"/>
Restrict CdPN in IAM to 15 digits	<input type="checkbox"/>
Control receiving Redirecting/Original Called for incoming redirection	<input checked="" type="checkbox"/>
Transmit Global Callref	<input type="checkbox"/>
Hop counter	Decrement 1
IAM indicators	
Transmission medium requirements	transit
Forward call indications	
ISUP preference	unchanged
Interworking indicator	unchanged
Call type indicator	unchanged
Connect type indicators	
Satellite indicator	change to 'no satellite'
Enable continuity check	<input type="checkbox"/>
Continuity check frequency	0
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

SS7 link set settings:

- *Name* – SS7 link set name;
- *Trunk group* – name of a trunk group that SS7 link set operates with;
- *Access category* – select access category;
- *Dial plan* – defines dial plan that will be used for routing in this group (necessary for dial plan negotiation);
- *Scheduled routing profile* – select 'scheduled routing' service profile, configured in the 'Internal resources' section;
- *Toll* – means that the signal link is connected to ALDE. This parameter allows for the correct operation with the long-distance type calls (used for CAS transits);
- *Alarm indication* – when checked, fault indication will appear in case of SS7 signal link fault (ALARM LED will light up, alarm will be added to alarm log);
- *Channel selection* – channel engagement order for the outgoing calls. Available options:
 - Successive forward;
 - Successive backward;
 - From first forward;
 - From last backward;
 - Successive forward (even);
 - Successive back (even);
 - Successive forward (odd);
 - Successive back (odd).



To minimize conflicts during communication with neighboring PBXes, we recommend to set inverse channel engagement types.

- *Reserve SS7 Linkset* – redundant SS7 link set selection. When the main SS7 link set is not available, the whole signalling message exchange will be performed through the redundant SS7 link set;
- *Combined mode* – Combined Linkset mode that will enable the exclusive utilization of voice streams in the current SS7 link set and signalling transfer through the signal channels of SS7 primary and secondary groups;
- *Primary SS7 link set* – select SS7 link set, that will perform the exchange of signalling messages related to this particular SS7 link set, by the signal D-channels;
- *Secondary SS7 link set* – select the second SS7 link set, that will perform the exchange of signalling messages related to this particular SS7 link set, by the signal D-channels;



In the combined mode operation, the signalling payload will be distributed evenly (50/50) between the primary and secondary SS7 link sets.

- *SS7 timer profile* – select the timer profile that will be used for the current SS7 link set.

MTP2 level

- *Emergency alignment for a single link* – enables emergency phasing procedure during SS7 link set commissioning, if this SS7 link set has a single signal link;

Service information (SIO)

- *Network ID* – indicates the network type: international, national, local network or reserve;

Routing label

- OPC – own point code;
- DPC ISUP – destination point code of the ISUP;

ISUP

- *Initialization* – device operations during stream recovery:
 - *Remain in block* – channels will remain blocked (BLO);
 - *Individual unblock* – sends unblock command (UBL) for each channel;
 - *Group unblock* – sends channel group unblock command (CGU);
 - *Group reset* – group reset command (GRS).
- *Send REL in response to SUS* – sends Release message in response to Suspend message;
- *Add a digit in IAM for overlap* – sends a single digits to Called Party number of IAM message if overlap dialing method is used;
- *Restrict CdPN in IAM to 15 digits* – when checked, up to 15 digits of CdPN number will be sent in IAM message, other digits will be sent in SAM message;
- *Control receiving Redirecting/Original Called for incoming redirection* – checkbox that enables checking the presence of Redirecting/Original Called fields with redirection information in incoming IAM message; when checked, the call will be rejected if these fields are absent.
- *Transmit Global Callrefs* – when there is no Global Call Reference (GCR) field in an incoming leg, SMG will form it automatically;
- *Hop counter* – sets rules for operation with hop counter field:
 - *Decrement* – transmission with decreasing value;
 - *No change* – transmission without any changes;
 - *Value* – transmission with pre-assigned value;
 - *Don't send* – disable hop counting.

IAM

- *Transmission medium requirements* – indicates the information type that should be transmitted via transmission medium; when '*transit*' type is selected, value will be taken from the incoming connection branch. If this field is missing from the incoming connection branch, default value '*3.1 kHz audio*' will be taken;

Forward call indicators

- *ISUP preference* – rule that governs 'ISUP preference indicator' modification. In a standard situation, these bits should not be changed;
- *Interworking indicator* – defines whether the interaction indicator should be modified or not (defines whether the interaction with non-ISDN network has occurred);
- *Call type indicator* – 'National/international call indicator' parameter modifications in FCI.

Connect type indicators

- *Satellite indicator* – identifies the presence of the satellite channel.
 - *Change to “no satellite”* – change identifier value to 'no satellite' regardless of the value received from the incoming channel;
 - *Unchanged* – keep the indicator value unchanged;
 - *Add one satellite* – this setting is used, if the signal link operates via satellite channel. In this case, satellite channel parameter transmitted in the 'nature of connection' indicators will be increased by 1;
- *Enable continuity check* – enables integrity check support in the SS7 link set. During the outgoing call, the called party establishes a remote loop in the stream, SMG sends the frequency to the channel that will be detected on reception after transmission through the channel. If the frequency is detected, the call will be served through this channel; if it is not detected, the similar attempt will be performed at the next channel. After 3 unsuccessful attempts (for three different channels), call serving will stop;
- *Continuity check frequency* – defines the frequency of channel integrity checks during outgoing calls performed through the SS7 link set. For example, value 3 means that each third outgoing call will be performed with the channel integrity check;

For the gateway, you may assign the correspondence of SS categories to Caller ID categories. For configuration, see Section 3.1.8.1 SS.

Examples

SMG connection method example for operation in SS7 quasi-associated mode via signalling transition points (STP):

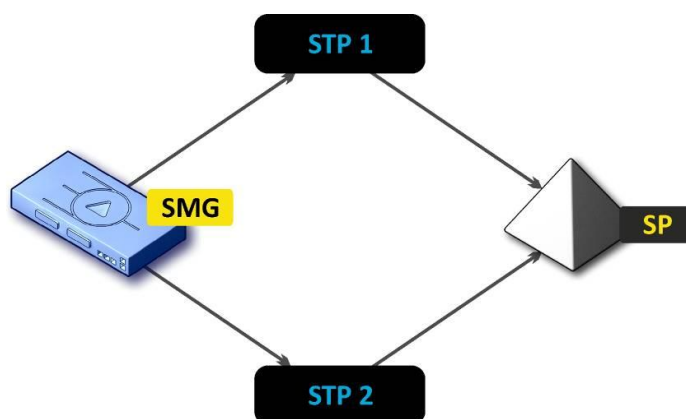


Figure 17 – SMG connection method for operation in SS7 quasi-associated mode via STP

Objective

You have to provide the SMG connection to the opposite signalling point (SP) using two signal links. The first signal link should pass through the signalling transition point STP 1 and the second signal link should pass through the STP 2.

Point code: SMG = 22, STP 1 = 155, STP 2 = 166, SP = 23.

Solution

In addition to the basic settings, set the 'origination code (OPC) = **22** and ISUP destination code (DPC-ISUP) = **23** in 'SS7 link set' menu.

Let us assume that stream 0 is connected to STP1 and stream 1 to STP 2. In the stream settings, you should specify: SS7 'Signalling protocol', configure CIC numbering correctly and select the required E1 stream time slot for signalling D-channel, select the pre-created SS7 link set in 'SS7 link set' settings and define the parameter 'MTP3 destination code (DPC-MTP3)' equal to **155** for stream 0, and **166** for stream 1.

SMG connection method example for operation in SS7 quasi-associated mode via PBX with STP features:

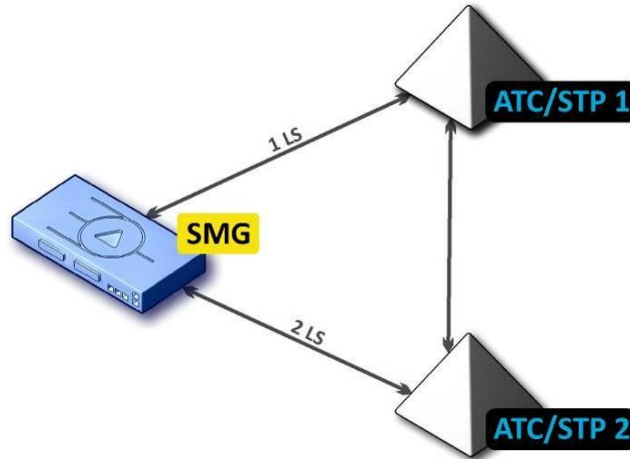


Figure 18 – SMG connection method for operation in SS7 quasi-associated mode via PBX with STP

LS – SS7 Link Set

Objective

You have to provide SMG connection to a couple of PBX with STP features (PBX/STP); when the failure occurs in the main circuit group 1LS between SMG and PBX/STP 1, signalling messages should be sent via 2LS.

Solution

Let us assume that SMG stream 0 is connected to PBX/STP 1 and used for the first SS7 link set configuration, stream 1 is connected to PBX/STP 2 and used for the second SS7 link set configuration. In the stream settings, you should specify: SS7'Signalling protocol', configure CIC numbering correctly and select the required E1 stream time slot for signalling D-channel, select the second SS7 link set in the 'Redundant SS7 link set' setting in the first SS7 link set configuration.

SMG connection method example for operation in combined mode:

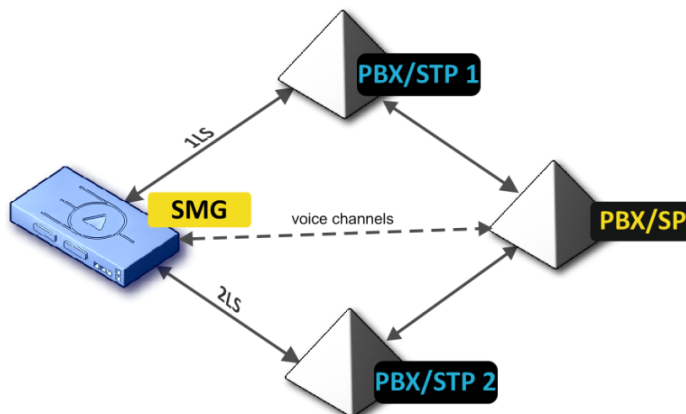


Figure 19 – SMG connection method for operation in combined mode

Objective

Only the voice channels exist between SMG and PBX/SP, signalling traffic should be transferred via PBX/STP 1 and PBX/STP 2.

Solution

Let us assume that SMG stream 0 is connected to PBX/STP 1 and used for the first SS7 link set configuration, stream 1 is connected to PBX/STP 2 and used for the second SS7 link set configuration, SMG stream 2 is connected to PBX/SP and used for the third SS7 link set configuration. In the stream settings, you should specify: **SS7** 'Signalling protocol', configure CIC numbering correctly and for streams 0 and 1 select the required E1 stream time slot for signalling D-channel, select the **first** SS7 link set in the 'Primary SS7 link set' setting and the **second** SS7 link set in the 'Secondary SS7 link set' setting in the third SS7 link set configuration.

3.1.7.3 SIP/SIP-T/SIP-I Interfaces, SIP Profiles

Configuration

This section describes configuration of general parameters for SIP stack, custom settings for each direction operating via SIP/SIP-T/SIP-I protocols, and SIP subscriber profiles.

SIP (Session Initiation Protocol) is a signalling protocol, which used in IP telephony. It facilitates basic call management tasks such as session start and termination.

SIP network addressing is based on the SIP URI scheme:

sip:user@host:port;uri-parameters

user – the number of a SIP subscriber;

@ – a separator located between the number and domain of the SIP subscriber;

host – domain or IP address of the SIP subscriber;

port – the UDP port used for subscriber's SIP service operation;

uri-parameters – additional parameters.

One of the additional SIP URI parameters is user=phone. If this parameter is specified, the syntax of the SIP subscriber number (in the user part) should match the TEL URI syntax described in RFC 3966. In this case, SMG PBX will process requests that contain "+", ";", "=", "?" in the SIP subscriber number, and will automatically add "+" before the callee number for international calls using the SIP-T protocol.

SIP interfaces

Settings

No	SIP interface	Mode	TrunkGroup	Hostame / IP-address:port	Codecs	DTMF mode	
0	smg2016	SIP	trunk2016	192.168.1.22:5020	G.711A G.711U	Inband	<input type="checkbox"/>
1	sout	SIP	out	192.168.1.123:5065	G.711A G.711U	Inband	<input type="checkbox"/>
2	sin	SIP	in	192.168.0.123:5064	G.711A G.711U	Inband	<input type="checkbox"/>
3	SIP-profile	SIP profile	-	-	G.711A G.711U	Inband	<input type="checkbox"/>

Swap selected

Common SIP settings

Local SIP port	<input type="text" value="5060"/>
Transport	<input type="text" value="UDP-only"/>
(x100 ms) T1 timer	<input type="text" value="5"/>
(x100 ms) T2 timer	<input type="text" value="40"/>
(x100 ms) T4 timer	<input type="text" value="50"/>
Ringing timeout (sec)	<input type="text" value="120"/>
Enable Q.850 cause header for all SIP-replies (RFC 6432)	<input type="checkbox"/>
Ignore address from R-URI	<input checked="" type="checkbox"/>
Enable KZ SIP specification	<input type="checkbox"/>
Save subscribers DB	<input type="checkbox"/>
Subscribers DB save period	<input type="text" value="1 hour"/>
Dynamic routing SIP profile	<input type="text" value="not set"/>




SIP General Parameters

- *Port for SIP signalling reception* – the UDP port for sending and receiving SIP messages;
- *Transport* – select a transport protocol for sending and receiving SIP messages:
 - *TCP-prefer* – the messages are received via UDP and TCP, and sent via TCP. If failed to establish a TCP connection, the messages are sent via UDP;
 - *UDP-prefer* – the messages are received via UDP and TCP. The packets smaller than 1,300 bytes are sent via TCP, while the ones larger than 1,300 bytes – via UDP;
 - *UDP-only* – use the UDP protocol only;
 - *TCP-only* – use the TCP protocol only;
- *T1 timer* – timeout for a request; upon expiration, the request is re-sent. The maximum retranslation interval for the INVITE requests is equal to 64*T1;
- *T2 timer* – the maximum retranslation interval for responses to the INVITE request and for all requests except for the INVITE ones;
- *T4 timer* – the maximum time allotted for all retranslations of the final response;
- *Ringing timeout, sec* – pre-answering state timeout of the call after reception of 18X message, during which the ringback tone or IVR message is played to the subscriber.
- *Use Q.850 cause header for all response SIP codes (RFC 6432)* – when this option is checked, the device analyses the Q. 850 cause field in all final SIP messages. If the option is not checked, the Q. 850 cause field is analysed in BYE and CANCEL messages only;

- *Ignore address in R-URI* – when this option is checked, address information after the “@” separator in Request-URI is ignored. Otherwise, the gateway checks if the address information matches the device IP address and host name; if there is no match, the call is rejected;
- *Enable/disable the specification in accordance with the requirements of the Republic of Kazakhstan*;
- *Store a subscriber database* – when this option is checked, save details of registered subscribers to the non-volatile memory of the gateway. The option is required to save the database of registered subscribers in case of device reboot due to power loss or failure. If the gateway is rebooted from WEB or CLI, the current database will be saved to non-volatile memory regardless of this setting;
- *Database update period* – set the data update period in the archive database (from 1 to 16 hours);

The SIP protocol defines two types of responses to connection initiating requests (INVITE) – provisional and final. 2xx, 3xx, 4xx, 5xx and 6xx-class responses are final, their transfer is reliable and confirmed by the ACK message. 1xx-class responses, except for the *100 Trying* response, are provisional and do not have a confirmation (rfc3261). These responses contain information on the current INVITE request processing step; in SIP-T/SIP-I protocols, SS-7 messages are encapsulated into 1xx class responses, therefore the loss of these responses is unacceptable. Utilisation of reliable provisional responses is also realised in the SIP protocol (rfc3262) and is defined by the *100rel* tag in the initiating request. In this case, provisional responses are confirmed by a PRACK message.

Up to 255 interfaces are supported. To create, edit, or remove SIP/SIP-T interfaces, use the *Objects – Add Object*, *Objects – Edit Object*, or *Objects – Remove Object* menus and the following buttons:

-  – *add Interface*;
-  – *edit Interface Parameters*;
-  – *remove Interface*.

The signal processor of the gateway encodes analogue voice traffic and fax/modem data into digital signals and performs its reverse decoding. The gateway supports the following codecs: G.711 (A/U), G.729 (A/B), OPUS¹ and AMR¹.

G.711 is a PCM codec without compression of voice data. To ensure correct operation, this codec should be supported by all manufacturers of VoIP equipment. G.711A and G.711U codecs differ from each other in encoding law (A-law is a linear encoding and U-law is a non-linear). The U-law encoding is used in North America, and the A-law encoding – in Europe.

G.729 – speech compression codec with a bit rate of 8 Kbps, supports detection of speech activity and generation of comfort noise (Annex B).

¹ Not supported in the current firmware version 3.14.0

SIP Interface Configuration Tab

SIP interfaces			
SIP interface settings	SIP protocol settings	Codecs/RTP settings	Extended SIP settings
Index [4]			
Title	SIP-interface04		
Mode	SIP ▼		
TrunkGroup	not set ▼		
Access category	[0] AccessCat#0 ▼		
Dial plan	[0] NumberPlan#0 ▼		
Hostname / IP-address			
Subnet mask for incoming calls	0.0.0.0		
Remote SIP port	0		
Local SIP port	0		
SIP domain			
Ignore source port for incoming calls	<input checked="" type="checkbox"/>		
Trusted network	<input type="checkbox"/>		
Alarm indication	<input type="checkbox"/>		
Network interface for SIP	eth1 (eth0 192.168.1.20) ▼		
Network interface for RTP	eth1 (eth0 192.168.1.20) ▼		
Q.850-cause and SIP-reply mapping table	not set ▼		
SIP-replies list for switching on reserve TG	not set ▼		
Scheduled routing profile	Not selected ▼		
Max active calls	0		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- **Name** – the interface name;
- **Mode** – select the interface protocol (*SIP/SIP-T/SIP-I/SIP Profile*);
- **Incoming RADIUS Profile** – select the RADIUS profile for the *SIP Profile* interface for incoming communication (for other interfaces, the RADIUS profile is assigned in the trunk group);
- **Outgoing RADIUS Profile** – select the RADIUS profile for the *SIP Profile* interface for outgoing communication (for other interfaces, the RADIUS profile is assigned in the trunk group);
- **Trunk group**¹ – name of the trunk group to which the interface belongs;
- **Access category** – select an access category;
- **Numbering schedule** – define the numbering schedule that will be used for dialling from this port (required for coordination of numbering schedules);

Mode	SIP profile ▼
Ingress RADIUS profile	not set ▼
Egress RADIUS profile	not set ▼

¹ The field is disabled in the SIP profile mode.

-
- *Host name/IP address* – IP address or name of the host communicating via the gateway's SIP/SIP-T protocol;
 - *Subnet mask for incoming calls* – if the mask is set, SMG will receive calls from the subnet holding the connecting host, specified in the “Host name/IP address” field. Note that when using the masks 0.0.0.0 (/0), 255.255.255.255 (/32) or 255.255.255.254 (/31), SMG will only accept calls from the IP address indicated in the “Host name/IP address” field, rather than from the subnet;
 - *SIP signalling destination port* – a UDP/TCP port of the communicating gateway that is used to receive SIP/SIP-T signalling;
 - *Port for SIP signalling reception* – a local UDP/TCP port of the device used to receive SIP/SIP-T signalling from the device communicating via this interface;
 - *SIP domain* – a domain that is placed into the *from* field when an outgoing call is made through the SIP interface; is used in the SIP interface registration;
 - *Ignore the source port during incoming calls* – when this option is checked, the signalling transmission UDP port of the communicating gateway that is specified in the *Port for SIP Signalling Reception* parameter is not checked; otherwise, the port is checked and the call is cleared back if the INVITE request is received from another port. If the INVITE request is received via TCP, the port is not checked regardless of the parameter value;
 - *Trusted network* – means that the interface is connected to a trusted network. This option defines generation of the INVITE request fields for calls with hidden caller number (presentation restricted). When this option is checked, the caller number information is transmitted in the *from* and *P-Asserted-identity* fields together with the information on its hidden state in the *Privacy: id* field; otherwise, the caller number information is not transmitted in any fields;
 - *Fault indication* – when this option is checked, SMG will indicate a fault when connection to the opposite device is lost. For correct operation of this feature, check the *Opposite party availability control using OPTIONS messages* checkbox in SIP settings;
 - *Signalling network interface* – the network interface selected to receive and transmit signalling SIP messages;
 - *RTP network interface* – select a network interface to receive and transmit voice traffic;
 - *Q.850-cause and SIP-reply correspondence table* – the selected table of correspondence between Q.850-cause and SIP-reply codes. To configure correspondence tables, use the *Internal Resources* menu.
 - *List of SIP replies for transition to redundant TG* – select the reply table for SIP 4XX – 6XX classes for transition to a redundant trunk group. The reply list table is configured in section 3.1.8 Internal Resources;
 - *Scheduled routing profile* – select a profile for the *Scheduled Routing* service configured in the Internal Resources section;
 - *Active connections* – the maximum number of simultaneous (incoming and outgoing) connections through this interface.

STUN server and Public IP settings:

STUN network protocol (RFC 5389) allows applications located behind a network address translation server (NAT) to discover their external IP address and port mapped to an internal port. Used

when SMG is located behind a NAT. To identify external device address you can use STUN or Public IP (used separately).

- *Use STUN* – when checked, use STUN server, otherwise use a specified public IP address;
- *STUN server IP* – IP address of STUN server;
- *STUN server port* – server port for request transmission (default value is 3478);
- *Request period* – time interval between requests (10–1800 seconds);
- *Public IP address* – sets public (external) address of NAT WAN interface to insert in SIP messages.

Before signalling message transmission, the request (Binding Request) has been sent to the STUN server from the interface; in the response (Binding Response) message, STUN server communicates device IP address and port (udp) that are used by SMG in signalling message generation.

Requests to STUN server has been generated before each SIP signalling message transmission, but not more often than the configured request period time.

Public IP setting is not used in the 'SIP profile' interface mode.

SIP Protocol Configuration Tab

SIP interfaces			
SIP interface settings	SIP protocol settings	Codecs/RTP settings	Extended SIP settings
Options			
Keep-alive control	<input type="checkbox"/>	0	
Keep-alive mode		SIP-OPTIONS	
Always transmit SDP in provisional responses	<input type="checkbox"/>		
'In-band signal' with 183+SDP transmission	<input type="checkbox"/>		
Local ring-back instead of early-media	<input type="checkbox"/>		
Enable P-Early-Media (RFC5009)	<input type="checkbox"/>		
Fill empty Display-Name	<input type="checkbox"/>		
Ignore RURI and To difference	<input type="checkbox"/>		
Do not use plus sign in CdPN and Diversion	<input type="checkbox"/>		
Diversion header with SIP URI	<input type="checkbox"/>		
Enable redirection (302) processing	<input type="checkbox"/>		
Redirection server direction	<input type="checkbox"/>		
Enable REFER processing	<input type="checkbox"/>		
Enable Re-INVITE with a=sendonly processing	<input type="checkbox"/>		
Send calling category		off	
Reliable provisional responses (1xx)	<input type="checkbox"/>	off	
DSCP for signaling	<input type="checkbox"/>	0	
Transit SIP header	<input type="checkbox"/>		
SIP-session timers (RFC 4028)			
Enable	<input type="checkbox"/>		
Session Expires	<input type="checkbox"/>	0	
Min SE	<input type="checkbox"/>	0	
Refresher side		Client	
Registration settings			
Upper registration		no registration	
Login			
Password			
Username/Number			
Default CdPN			
Replace CgPN on egress call	<input type="checkbox"/>		
Registration period (sec)		1800	
Registration requests interval (ms)		1000	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

SIP/SIP-T/SIP-I Options Configuration

- *Opposite party availability control* – a function that controls direction availability by sending OPTIONS requests; when a direction is not available, the redundant trunk group is used for the call. This function also analyses the received OPTIONS response that allows avoiding the use of the *100rel*, *replaces*, and *timer* features configured in this direction, unless the opposite party supports them. The parameter defines the request transmission period and may take values in the range of 30–3,600 seconds.

- *Availability control mode for the opposite party:*
 - *SIP-OPTIONS* – at specified opposite party control intervals, the device will send the OPTIONS control message. This message should receive a response from the opposite party; if no response is received, the direction is considered unavailable, and the failure status is registered in the device;
 - *SIP-NOTIFY* – the device will send the NOTIFY control message at specified opposite party control intervals. This message should receive a response from the opposite party; if no response is received, the direction is considered unavailable, and the failure status is registered in the device;
 - *UDP-CRLF* – device will send an empty UDP packet at specified opposite party control intervals; the opposite party response to an empty UDP packet is not applicable; consequently, the failure status will not be initiated on the device.



These methods are also used to maintain the NAT connection

- *Always send SDP in provisional replies* – allows early forwarding of the voice frequency path. For example, when this option is not checked, SMG sends reply 180 without SDP session description; according to this reply, the outgoing party plays the ringback tone; when this option is checked, SMG sends reply 180 with SDP session description and the ringback is played by the incoming party;
- *In-band signal with 183+SDP transmission* – issues SIP-reply 183 with SDP session description for voice frequency path forwarding upon receipt of the CALL PROCEEDING or PROGRESS messages from ISDN PRI that contain the progress indicator = 8 (in-band signal);
- *Local ringback instead of early-media* – when the early media marker is received from the outgoing connection branch, ringback tone will be played to the caller instead of the inband voice message;
- *Use P-Early-Media (RFC5009)* – use the P-Early-Media header described in RFC 5009. With outgoing call, the device will transmit the P-Early-Media header in an INVITE request: supported. When an INVITE request with P-Early-Media: supported marker is received, the response 18X messages will contain the P-Early-Media header: sendrecv;
- *Fill in Display-Name empty field* – when this option is checked, if a call with the missing display-name is received, SMG will fill it with the user name (number) taken from the URI;
- *Ignore RURI and To difference* – disable the Redirecting and Original Called numbers in SS7 calls when the values in *SIP RURI* and *To* fields are different;
- *Do not use "+" in Cdpn and Diversion* – disable addition of "+" to a number, for International number type;
- *SIP URI in Diversion header* – use SIP URI in the Diversion header instead of TEL URI;
- *Enable integrity checking* – for SIP-I/T, enable transmission of IAM with a Continuity check indication value of 2. **The option is available only for SIP-T and SIP-I protocols;**
- *Enable forwarding (302)* – when this option is checked, the gateway is allowed to perform forwarding upon receipt of reply 302 from this interface. When unchecked and reply 302 is received, the gateway will reject the call and perform forwarding;
- *Forward to forwarding server* – this option is available when the reply 302 processing is enabled (the *Enable forwarding (302)* parameter). This enables forwarding of the call, which was sent using a public address, to the subscriber's private address received in

reply 302 without numbering schedule routing. The call is routed directly to the address specified in the “contact” header of reply 302 received from the forwarding server.

- *Enable processing of REFER messages* – a REFER request is sent by the communicating gateway to enable the *Call Transfer* service. When this option is checked, the gateway is allowed to process REFER requests received from this interface. When unchecked, the gateway clears back the call upon receipt of a REFER request and does not provide the *Call Transfer* service.
- *Enable processing of Re-INVITE with a=sendonly* – when this option is checked, it allows a call to be put on hold when the Re-INVITE message is received with a=sendonly marker in SDP;
- *Caller category transmission* – select a method of caller category transmission through SIP. The following methods are implemented:
 - *off* – sending and receiving of Caller ID category are disabled;
 - *category* – the caller category is sent/received in a separate *category* field in the INVITE message; in this case, the SS7 category with values 0 – 255 is sent;
 - *cpc* – the caller category is sent/received via the “cpc=” tag transmitted in the *from* field, in this case, the Caller ID category with values 1 – 10 is sent;
 - *cpc-rus* – the caller category is sent/received via the “cpc-rus=” tag transmitted in the *from* field; in this case, the Caller ID category with values 1 – 10 is sent;
- *Reliable delivery of provisional responses (1xx)* – when this option is checked, the INVITE request and 1xx class provisional responses will contain the *require: 100rel* option, which requires assured confirmation of provisional responses;
 - *off* – reliable delivery of provisional responses is disabled;
 - *support* – the INVITE request and 1xx class provisional responses will contain the *support: 100rel* option;
 - *support+* – duplicate SDP in 200 OK message when using support: 100rel;
 - *require* – the INVITE request and 1xx class provisional responses will contain the *require: 100rel* option, which requires assured confirmation of provisional responses;
 - *support+* – duplicate SDP in 200 OK message when using require: 100rel.
- *DSCP for Signalling* – a service type (DSCP) for SIP signalling traffic;
- *SIP headers transit* – enables transit of the received SIP headers into the outgoing branch.

NAT options

- *NAT (comedia mode)* – option required for correct operation of SIP through NAT (Network Address Translation) when SMG is used in a public network. Verifies source data in the incoming RTP stream and translate the outgoing stream to IP address and UDP port that the media stream is coming from.
- *Send SDP in 18x messages* – translate SDP attachment in 18x provisional replies when NAT option is enabled (comedia mode). Allows performing an early forwarding of voice frequency path (before the subscriber answers) and early source data verification in the incoming RTP stream;
- *VIA and IP address match control* – NAT traversal support option. When enabled, VIA address and request originator IP address will be analyzed. When they match, SMG will assume that the device is located outside the NAT.








SIP Session Timers (RFC 4028):

- *Enable timer support* – when this option is checked, enables support of SIP session timers (RFC 4028). A session is renewed by re-INVITE requests sent during the session;
- *Session Expires* – a period of time in seconds before a forced session termination if the session is not renewed in time (from 90 to 64,800 seconds; 1,800 seconds is recommended);
- *Minimum session expiration (Min SE)* – the minimal time interval for connection health checks (from 90 to 32,000 seconds). This value should not exceed the *Sessions Expires* forced termination timeout.
- *Session renewal party* – defines the party to renew the session (client (uac) – client (caller) party, server (uas) – server (callee) party).

Registration Parameters:

- *Registration on upstream server* – the selected type of registration on an upstream server:
 - *No registration* – do not perform registration on the upstream server;
 - *Trunk registration* – registration on the upstream server using parameters specified in this section;
- *Login* – the name used for authentication;
- *Password* – the password used for authentication;
- *Username/Number* – the user number which is used as a caller number for outgoing trunk calls;
- *Default CdPN* – the default CdPN number that will be used for all calls via this SIP interface;
- *CgPN substitution in outgoing call* – when this option is checked, the caller number (CgPN) is taken from the *Username/Number* parameter; otherwise, the CgPN number received in the incoming call is used;
- *Registration time* – the time interval for registration renewal;
- *Registration request interval (ms)* – the minimum interval between the Register messages that is used to protect from high traffic caused by simultaneous registration of a large number of subscribers.

Configuration of Options for SIP Profile Mode:

SIP interfaces	
SIP interface settings	SIP protocol settings
Options	
Keep-alive control 	<input type="checkbox"/> 30
Keep-alive mode	SIP-OPTIONS ▼
Register expires, min 	300
Register expires, max 	3600
Always transmit SDP in provisional responses	<input type="checkbox"/>
'In-band signal' with 183+SDP transmission	<input type="checkbox"/>
Local ring-back instead of early-media	<input type="checkbox"/>
Enable P-Early-Media (RFC5009)	<input type="checkbox"/>
Fill empty Display-Name	<input type="checkbox"/>
Ignore RURI and To difference	<input type="checkbox"/>
Do not use plus sign in CdPN and Diversion	<input type="checkbox"/>
Diversion header with SIP URI	<input type="checkbox"/>
Enable redirection (302) processing	<input type="checkbox"/>
Enable REFER processing	<input type="checkbox"/>
Enable Re-INVITE with a=sendonly processing	<input type="checkbox"/>
Reliable provisional responses (1xx) 	off ▼
DSCP for signaling 	0
SIP-session timers (RFC 4028)	
Enable	<input type="checkbox"/>
Session Expires 	0
Min SE 	0
Refresher side	Client ▼
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- *Opposite party availability control* – function to control the direction availability (NAT keep-alive) using SIP-OPTIONS, SIP-NOTIFY methods or empty UDP. The parameter defines the request transmission period and may take values in the range of 30–3,600 seconds.
- *Availability control mode for the opposite party:*
 - *SIP-OPTIONS* – at specified opposite party control intervals, the device will send the OPTIONS control message. This message should receive a response from the opposite party; if no response is received, the direction is considered unavailable, and the failure status is registered in the device;
 - *SIP-NOTIFY* – the device will send the NOTIFY control message at specified opposite party control intervals. This message should receive a response from the opposite party; if no response is received, the direction is considered unavailable, and the failure status is registered in the device;
 - *UDP-CRLF* – device will send an empty UDP packet at specified opposite party control intervals; the opposite party response to an empty UDP packet is not applicable; consequently, the failure status will not be initiated on the device.



These methods are also used to maintain the NAT connection

- *Register expires, min* – the minimum value of “expires” registration time;
- *Register expires, max* – the maximum value of “expires” registration time;
- *Always send SDP in provisional replies* – allows early forwarding of the voice frequency path. For example, when this option is not checked, SMG sends reply 180 without SDP session description; according to this reply, the outgoing party plays the ringback tone; when this option is checked, SMG sends reply 180 with SDP session description and the ringback is played by the incoming party;
- *In-band signal with 183+SDP transmission* – issues SIP-reply 183 with SDP session description for voice frequency path forwarding upon receipt of the CALL PROCEEDING or PROGRESS messages from ISDN PRI that contain the progress indicator = 8 (in-band signal);
- *Local ringback instead of early-media* – when the early media marker is received from the outgoing connection branch, ringback tone will be played to the caller instead of the inband voice message;
- *Use P-Early-Media (RFC5009)* – use the P-Early-Media header described in RFC 5009. With outgoing call, the device will transmit the P-Early-Media header in an INVITE request: supported. When an INVITE request with P-Early-Media: supported marker is received, the response 18X messages will contain the P-Early-Media header: sendrecv;
- *Fill in Display-Name empty field* – when this option is checked, if a call with the missing display-name is received, SMG will fill it with the user name (number) taken from the URI;
- *Ignore RURI and To difference* – disable the Redirecting and Original Called numbers in SS7 calls when the values in SIP RURI and To fields are different;
- *Do not use “+” in CdPN and Diversion* – disable addition of “+” to a number, for International number type;
- *SIP URI in Diversion header* – use SIP URI in the Diversion header instead of TEL URI;
- *Enable forwarding (302)* – when this option is checked, the gateway is allowed to perform forwarding upon receipt of reply 302 from this interface. When unchecked and reply 302 is received, the gateway will reject the call and perform forwarding;
- *Enable processing of REFER messages* – a REFER request is sent by the communicating gateway to enable the *Call Transfer* service. When this option is checked, the gateway is allowed to process REFER requests received from this interface. When this option is unchecked, the gateway rejects the call upon receipt of a REFER request and does not provide the *Call Transfer* service;
- *Enable processing of Re-INVITE with a=sendonly* – when this option is checked, it allows a call to be placed on hold when receiving a Re-INVITE message with a=sendonly attribute in SDP.
- *Reliable delivery of provisional responses (1xx)* – when this option is checked, the INVITE request and 1xx class provisional responses will contain the *require: 100rel* option, which requires assured confirmation of provisional responses;
 - *off* – reliable delivery of provisional responses is disabled;

- *support* – the INVITE request and 1xx class provisional responses will contain the *support: 100rel*;
 - *support+* – duplicate SDP in 200 OK message when using *support: 100rel*;
 - *require* – the INVITE request and 1xx class provisional responses will contain the *require: 100rel* option, which requires assured confirmation of provisional responses;
 - *support+* – duplicate SDP in 200 OK message when using *require: 100rel*.
- *DSCP for Signalling* – a service type (DSCP) for SIP signalling traffic;

SIP Session Timers (RFC 4028):

- *Enable timer support* – when this option is checked, enables support of SIP session timers (RFC 4028). A session is renewed by re-INVITE requests sent during the session;
- *Session Expires* – a period of time in seconds before a forced session termination if the session is not renewed in time (from 90 to 64,800 seconds; 1,800 seconds is recommended);
- *Minimum session expiration (Min SE)* – the minimal time interval for connection health checks (from 90 to 32,000 seconds). This value should not exceed the *Sessions Expires* forced termination timeout.
- *Session renewal party* – defines the party to renew the session (client (uac) – client (caller) party, server (uas) – server (callee) party).

RTP Codec Configuration Tab

SIP interfaces																							
SIP interface settings	SIP protocol settings	Codecs/RTP settings																					
Options VAD / CNG <input type="checkbox"/> Echo-cancellation <input type="text" value="off"/>		<table border="1"> <thead> <tr> <th>On</th> <th>Codec</th> <th>PType</th> <th>PTE</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>G.711A</td> <td>8</td> <td>20</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>G.711U</td> <td>0</td> <td>20</td> </tr> <tr> <td><input type="checkbox"/></td> <td>G.729</td> <td>18</td> <td>20</td> </tr> <tr> <td><input type="checkbox"/></td> <td>G.726-32</td> <td>102</td> <td>20</td> </tr> </tbody> </table>		On	Codec	PType	PTE	<input checked="" type="checkbox"/>	G.711A	8	20	<input checked="" type="checkbox"/>	G.711U	0	20	<input type="checkbox"/>	G.729	18	20	<input type="checkbox"/>	G.726-32	102	20
On	Codec	PType	PTE																				
<input checked="" type="checkbox"/>	G.711A	8	20																				
<input checked="" type="checkbox"/>	G.711U	0	20																				
<input type="checkbox"/>	G.729	18	20																				
<input type="checkbox"/>	G.726-32	102	20																				
Dual-Tone Multi-Frequency signaling settings DTMF transport <input type="text" value="inband"/> Flash signal processing (RFC2833) <input type="checkbox"/> HOLD set/remove by <input type="text" value="flash"/> RFC2833 PT <input type="text" value="101"/> RFC2833: same PT <input type="checkbox"/> DTMF MIME Type <input type="text" value="application/dtmf"/>																							
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>																							

Options

- *Voice activity detector / Comfort noise generator (VAD/CNG)* – when this option is checked, enables a silence detector and a comfort noise generator. The voice activity detector allows transmission of RTP packets to be disabled during periods of silence, thus reducing the load in data networks;
- *Echo cancellation* – the echo cancellation mode:
 - *on* – echo cancellation enabled;

- *off* – echo cancellation is disabled (this mode is set by default).

DTMF Signals Acceptance | Transmission:

- *DTMF transmission method* – the method of DTMF transmission via IP network;
 - *inband* – in RTP packets, in-band;
 - *RFC2833* – in RTP packets according to rfc2833 recommendations;
 - *SIP-INFO* – out-of-band, via SIP protocol using INFO messages; the type of DTMF signals transferred depends on the MIME extension type in this case.
 - *SIP-NOTIFY* – out-of-band, via SIP protocol using NOTIFY messages. This DTMF transmission is an implementation of the method used in Cisco hardware.





In order to be able to use extension dialling during a call, make sure the similar DTMF tone transmission method is configured in the opposite gateway.

- *Flash signal processing (RFC2833)* – when this option is checked, activates FLASH signal processing by INFO, rfc2833 and re-invite methods for the VAS *Call Transfer* service.
- *RFC2833 PT* – the type of dynamic load used to transfer DTMF packets via RFC2833. The range of permitted values is from 96 to 127. RFC2833 recommendation defines the transmission of DTMF via the RTP protocol. This parameter should conform to the similar parameter of the communicating gateway (the most frequently used values are 96, 101).
- *Same RFC2833 PT* – when this option is checked, if SMG is the party which sends *offer SDP*, RFC2833 packets are expected for reception with a PT value sent in *answer SDP*; otherwise, RFC2833 packets are expected for reception with the same PT value as sent by SMG to *offer SDP*.
- *DTMF MIME Type* – the load type used for DTMF transmission in SIP protocol INFO packets:
 - *application/dtmf-relay* – in SIP INFO application/dtmf-relay packets ("*" and "#" are sent as symbols "*" and "#");
 - *application/dtmf* – in SIP INFO application/dtmf packets ("*" and "#" are sent as digits 10 and 11).

Codecs:

In this section, you can select the interface codecs and the order in which they will be used when establishing the connection. The codec with the highest priority should be placed in the top position.

Left-clicking highlights a row with the selected codec. To change the codec priority, use the arrows   (up, down).

- *Enable* – when this option is checked, use the codec specified in the opposite field.
- *Codec* – set the codec to be used for voice data transmission. Supported codecs: G.711 (A/U), G.729 (A/B), G.726-32.

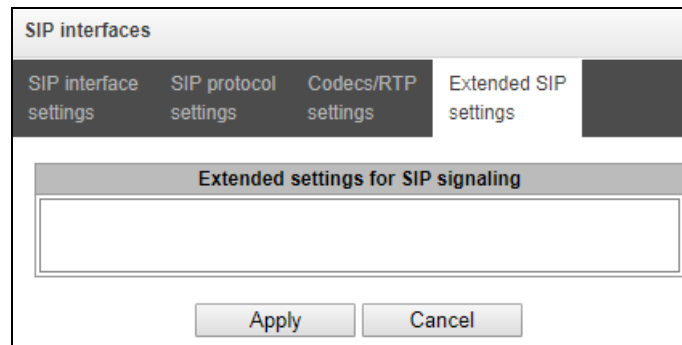


With VAD/CNG functions enabled, G.729 codec works as G.729B, otherwise as G729A.

- *PType* – load type for the codec. Assigned automatically.
- *PTE* – packetisation time – the number of milliseconds (ms) of speech transmitted in a single packet.

Advanced Settings Tab

The tab contains the advanced settings for SIP protocol. Using these settings, the fields of SIP messages can be adjusted according to the specified rules.



Field Format

[sipheader:HEADER_NAME=operation],[sipheader:...],...

where:

- *Operations* – disable, insert, or modification rule;
- *HEADER_NAME* – case-insensitive parameter, for example Accept = accept = ACCEPT. Other parameters are case-sensitive.

Modification Rules

Modification rules use the following characters:

- \$ – keep the rest of the text;
- ! – delete the rest of the text;
- +(AБB) – add the specified text;
- -(AБB) – delete the specified text;

Examples of implemented operation rules are given in Table 11.



To transit the SIP headers, select the *SIP Headers Transit* option in the SIP interface where you will select the headers.

Table 11 – Operation Rules Examples

Operation	Original header	Rule	Result
Do not transit the header	Accept: application/SDP	[sipheader:accept=disable]	
Transit the header from the first branch without changes	Additional headers in the first branch: P-Asserted-Identity: <u>username@domain</u> Subject: Test call	[sipheader:[MESSAGE_LIST]: [HEADER_MASK]=transit] [sipheader:[HEADER_MASK]=transit] In INVITE and 200 messages: [sipheader:INVITE,200:Subject=transit] In any messages: [sipheader:Subject=transit]	This header will appear in the second branch: Subject: Test call
Transit the	Additional headers in the	[sipheader:P-*=transit]	These headers will appear

header group from the first branch without changes	<p>first branch:</p> <p>P-Asserted-Identity: sip:<u>username@domain</u></p> <p>P-Called-Party-ID: sip:<u>username@domain</u></p> <p>Privacy: id</p> <p>Subject: Test call</p>	Note that the rule: [sipheader:*=transit] will not work, as the * character can only replace part of the name.	<p>in the second branch:</p> <p>P-Asserted-Identity: sip:<u>username@domain</u></p> <p>P-Called-Party-ID: sip:<u>username@domain</u></p>
Insert header		<p>[sipheader:insert[HEADERS_LIST]:Remotelp=+(TEXT)]</p> <p>In all requests: [sipheader:insert:Remotelp=+(example.SMG)]</p> <p>Only in INVITE request: [sipheader:insert,INVITE:Remotelp=+(example.SMG)]</p> <p>Only in specified requests (for example, INVITE and ACK): [sipheader:insert,INVITE,ACK:Remotelp=+(example.SMG)]</p>	Remotelp:example.SMG
Add text to the beginning	Accept: application/SDP	[sipheader:accept=+(application/ISUP,)\$]	Accept: application/ISUP,application/SDP
Add text to the end	Accept: application/SDP	[sipheader:accept=\$+(,application/ISUP)]	Accept: application/SDP,application/ISUP
Delete text	Accept: application/SDP,application/ISUP	[sipheader:accept=- (application/SDP,)\$]	Accept: application/ISUP
Delete, starting from the specified text	Accept: application/SDP,text/plain	[sipheader:accept=- (text)!]	Accept: application/SDP
Replace text completely	Accept: application/SDP	[sipheader:accept=+(application/ISUP)!]	Accept: application/ISUP
Replace text	Accept: application/SDP,text/plain	[sipheader:accept=- (SDP)+(ISUP)\$]	Accept: application/ISUP,text/plain
Replace text by dropping the data at the end	Accept: application/SDP,text/plain	[sipheader:accept=- (SDP)+(ISUP)!]	Accept: application/ISUP
Example of complex modification	From: <sip:who@host>;tag=aBc	[sipheader:from=+(DISPLAY)-(who)+(12345)-(>)+(;user=phone>)\$+ (;line=abc)]	From: DISPLAY <sip:12345@host;user=phone>;tag=aBc;line=abc
Not to transfer X-UniqueTag	X-UniqueTag: 12345678 90abcdef 12345678 90abcdef	unique-tag=disable	X-UniqueTag header is not transmitted.
Transfer X-UniqueTag content in another header	X-UniqueTag: 12345678 90abcdef 12345678 90abcdef	unique-tag=NewHeader-Name	NewHeader-Name: 12345678 90abcdef 12345678 90abcdef

Example

```
[sipheader:Accept=disable],[sipheader:user-agent=disable]
```

In this example, all SIP messages sent by the device through this SIP interface will not contain *Accept* and *user-agent* fields.

List of required SIP message fields that will not be subject to this restriction: *via*, *from*, *to*, *call-id*, *cseq*, *contact*, *content-type*, *content-length*.

3.1.7.4 H323 Interfaces

In this section you can configure general configuration settings for H.323 stack¹ and individual settings for each direction using H.323 protocol.

H.323 protocol is a signalling protocol used in IP telephony for multimedia data transmission via **packet networks**. The protocol facilitates the basic call management tasks such as starting and finishing a session.

H.323 signalling is a stack of protocols based on **Q.931** recommendation used in **ISDN**. The gateway uses the following recommendations: **H.225.0** and **H.245**.

SMG PBXs can be used in configurations both with **Gatekeeper** and without it. After purchasing a separate license, the SMG gateway can act as a gatekeeper or interact with the Directory gatekeeper to localise the subscriber.

General Configuration of H.323

H.323 interfaces

№	Name	Mode	TrunkGroup	Hostname / IP-address	Codecs	DTMF Type
<div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;"> <p style="text-align: center; margin: 0;">Common H323 settings</p> <p>Device ID (H323 alias) <input style="width: 80%;" type="text" value="SMG500"/></p> <p>Network interface for signaling <input style="width: 80%;" type="text" value="1.25 (eth0 192.168.1.25)"/></p> <p>Port for signaling <input style="width: 80%;" type="text" value="1720"/></p> </div> <div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;"> <p style="text-align: center; margin: 0;">GateKeeper settings</p> <p>GateKeeper <input style="width: 80%;" type="text" value="not used"/></p> </div> <p style="margin: 0;"><input type="button" value="Apply"/></p>						

- *Device ID (Alias)* – the gateway name during the registration at the Gatekeeper;
- *Signalling network interface* – select the network interface for H.323 signalling;
- *Signalling reception port* – local TCP port for receiving H. 323 signalling messages;
- *Use GateKeeper* – sets the operation mode as **Gatekeeper**. In the “remote” mode, SMG will interact with an external gatekeeper, while in the “local” mode the gateway will act as a gatekeeper itself.

“Remote” mode settings:

¹ The menu is available only in a version with H. 323 license. For more information about the licenses, see section 3.1.22 Licenses

Common H323 settings	
Device ID (H323 alias)	SMG500
Network interface for signaling	1.25 (eth0 192.168.1.25)
Port for signaling	1720
GateKeeper settings	
GateKeeper	remote
Search GateKeeper	<input type="checkbox"/>
GateKeeper IP	0.0.0.0
GateKeeper Port	1719
Registration time	300
Keep-alive timeout	20
Apply	

- *Search GateKeeper* – when this option is checked, the Gatekeeper is detected automatically by using IP multicast address 224.0.1.41 and UDP port 1718; otherwise this method is not used and the Gatekeeper has a specific IP address;
- *GateKeeper IP* – detecting the Gatekeeper at specific IP;
- *GateKeeper Port* – Gatekeeper UDP port (port 1719 is used by most Gatekeepers by default);
- *Time To Live* – the time frame (in seconds) for the device to register at the Gatekeeper;
- *Keep Alive Time* – the time frame (in seconds) for the device to re-register at the Gatekeeper;



For reliable re-registration of the device at the gatekeeper, the value of the *Keep Alive Time* should be set as 2/3 of the *Time To Live* registration period. We recommend setting the *Time To Live* parameter the same as that on the gatekeeper, so that the *Keep Alive Time* of the gateway re-registration is always less than the *Time To Live* value transmitted in the gatekeeper's responses. Otherwise, an incorrect setting may cause the gatekeeper to unregister the gateway before the gateway re-registers, which in turn will destroy all active connections established through the gatekeeper.



When applying the settings in this section, the H323 module is restarted and all established conversations over H. 323 protocol are forcibly completed. The “H323-MODULE LOST” failure may occur for a short time.

3.1.7.5 H.323 Interface Configuration Tab

H.323 interfaces	
H323 interface settings	H323 protocol settings
Index [0]	
Name	H323-interface00
TrunkGroup	not set
Access category	[0] AccessCat#0
Dial plan	[0] NumberPlan#0
Use GateKeeper	<input type="checkbox"/>
Hostname / IP-address	
Port for signaling	1720
Network interface for RTP	1.25 (eth0 192.168.1.25)
Scheduled routing profile	Not selected
Max active calls	0
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- *Name* – the interface name;
- *Trunk group* – name of the trunk group that includes this interface;
- *Access category* – select an access category;
- *Numbering schedule* – defines the numbering schedule that will be used for dialling from this interface (required for coordination of numbering schedules);
- *Use GateKeeper* – when this option is checked, the interface communicates via GateKeeper, settings of which are selected in the “H323 General Configuration” section;
- *Host name/IP address* – IP address or name of the host communicating via the gateway's H.323 protocol;
- *H323 signalling destination port* – a signalling TCP port of the communicating gateway used to receive H323 signalling;
- *RTP network interface* – select a network interface to receive and transmit voice traffic;
- *Scheduled routing profile* – select a profile for the *Scheduled Routing* service configured in the Internal Resources section;
- *Active connections* – the maximum number of simultaneous (incoming and outgoing) connections through this interface.

3.1.7.6 H.323 Protocol Configuration Tab

- *Device ID (Alias)* – the gateway name during the registration at the Gatekeeper;
- *Fast start* – when this option is checked, the quick start function is enabled; otherwise it is disabled. When using the option, session description for establishing a media channel is sent via H.225 protocol, otherwise – via H.245 protocol;
- *H245 tunnel* – when this option is checked, H. 245 tunnelling through Q. 931 signal channels is enabled; otherwise it is disabled;
- *DSCP for signalling* – a service type (DSCP) for SIP signalling traffic (H.323).
- *Number prefixes (Prefix 1, Prefix 2, Prefix 3)* – numbers registered by SMG at the gatekeeper, local or external, depending on the settings. The table includes the numbers or the initial digits of the numbers of SIP subscribers registered with SMG, so that the Gatekeeper can route the calls addressed to SIP subscribers to SMG (for example, one common prefix 10010 can be specified for 100101 and 100102 subscribers).

3.1.7.7 RTP/Codec Configuration Tab

On	Codec	PType	PTE
<input checked="" type="checkbox"/>	G.711A	8	20
<input checked="" type="checkbox"/>	G.711U	0	20
<input type="checkbox"/>	G.729	18	20

Options:

- *Voice activity detector / Comfort noise generator (VAD/CNG)* – when this option is checked, enables a silence detector and a comfort noise generator. The voice activity detector allows transmission of RTP packets to be disabled during periods of silence, thus reducing the load in data networks;

- *RTP source IP:Port control* – when this option is checked, it controls media traffic received from the IP address and UDP port specified in the SDP communication session description; otherwise, it accepts traffic from any IP address and UDP port;
- *Echo cancellation* – the echo cancellation mode:
 - *on* – echo cancellation enabled;
 - *off* – echo cancellation disabled.

DTMF Transmission

- *DTMF transmission method* – the method of DTMF transmission via IP network;
 - *inband* – inside the band, in RTP voice packets;
 - *RFC2833* – according to RFC2833 recommendations, as a dedicated load in RTP voice packets;
 - *H.245 Alphanumeric* – out-of-band, in userInput messages of the H.245 protocol; the basicstring compatibility is used for the transmission of DTMF signals;
 - *H.245 Signal* – out-of-band, in userInput messages of the H.245 protocol; the dtmf compatibility is used for the transmission of DTMF signals;
 - *Q931 Keypad IE* – out-of-band, the Keypad element in INFORMATION message of Q.931 protocol is used for transmission of DTMF signals;





In order to be able to use extension dialling during a call, make sure the similar DTMF tone transmission method is configured in the opposite gateway.

- *RFC2833 PT* – the type of dynamic load used to transfer DTMF packets via RFC2833. The range of permitted values is from 96 to 127. RFC2833 recommendation defines the transmission of DTMF via the RTP protocol. This parameter should conform to the similar parameter of the communicating gateway (the most frequently used values are 96, 101).

Codecs:

In this section, you can select the interface codecs and the order in which they will be used when establishing the connection. The codec with the highest priority should be placed in the top position.

Left-clicking highlights a row with the selected codec. To change the codec priority, use the arrows   (up, down).

- *Enable* – when this option is checked, use the codec specified in the opposite field;
- *Codec* – set the codec to be used for voice data transmission. Supported codecs: G.711 (A/U), G.729 (A/B).



With VAD/CNG functions enabled, G.729 codec works as G.729B, otherwise as G729A.




- *PType* – load type for the codec. Assigned automatically.
- *PTE* – packetisation time – the number of milliseconds (ms) of speech transmitted in a single packet.

3.1.7.8 Trunk Directions

A trunk direction is a set of trunk groups. When a call is performed to a trunk direction, the order of selection of the trunk groups in this direction can be chosen.

Trunk Directions			
No	Name	TrunkGroup list	TrunkGroup selection order
0	Direction #0	TrunkGroup00	Successive forward
1	Direction #1	TrunkGroup00	Starting from first forward

To create, edit, or remove trunk directions, use the *Objects – Add Object*, *Objects – Edit Object*, or *Objects – Remove Object* menus and the following buttons:

-  – add direction;
-  – edit direction parameters;
-  – remove direction.



To access a trunk direction, the device configuration should include prefixes which perform transition to this direction.

Trunk Directions

Trunk Direction settings # 0

Name

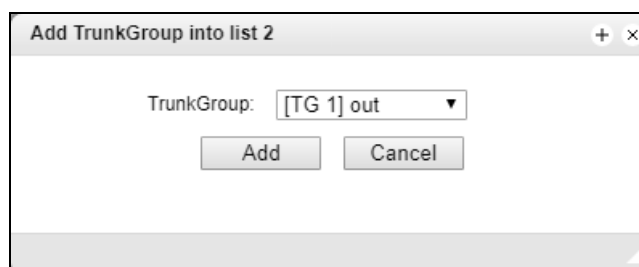
TrunkGroup select mode

TrunkGroups list

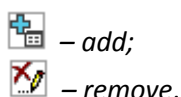
↕ [TF 0] TrunkGroup00

- *Name* – name of the trunk direction;
- *Trunk group selection mode* – order of trunk group selection in the direction:
 - *Sequential forward* – all trunk groups of the direction are selected in turns beginning from the first one in the list. It means that the first call will be sent to the first trunk group, the second - in the second and so on.
 - *Sequential back* – all trunk groups of the direction are selected in turns beginning from the last one in the list. It means that the first call will be sent to the last trunk group, the second - in the next to last and so on. Then the cycle repeats.
 - *From the first and forward* – the first free trunk group of the direction is selected beginning from the first one in the list. The search starts from the top of list.
 - *From the last and back* – the first free trunk group of the direction is selected beginning from the last one in the list. The search starts from the top of list.
- *Local direction* – when this option is checked, subscribers of this direction are considered as local. Subscribers of this direction are subjected to SORM control, with the number type and attribute as “subscriber of this station”.

A list of trunk groups in the direction:



To add or remove trunk groups, use the following buttons:



Use the arrow buttons (up, down) to change the trunk group order in the list.

3.1.8 Internal Resources

3.1.8.1 SS7 Categories

In this section, you can specify the corresponding Caller ID and SS7 categories, when using SIP-T/SIP-I protocols.

The generally accepted correspondence between SS-7 categories and Caller ID categories is provided below.

- SS7 category 10 – Caller ID category 1
- SS7 category 11 – Caller ID category 4
- SS7 category 12 – Caller ID category 8
- SS7 category 15 – Caller ID category 6
- SS7 category 224 – Caller ID category 0
- SS7 category 225 – Caller ID category 2
- SS7 category 226 – Caller ID category 5
- SS7 category 227 – Caller ID category 7
- SS7 category 228 – Caller ID category 3
- SS7 category 229 – Caller ID category 9

SS7 Categories		
SS7 categories		
No	Calling party category (RUS)	SS7 category
0	1	10
1	2	225
2	3	228
3	4	11
4	5	226
5	6	15
6	7	227
7	8	12
8	9	229
9	10	224
10	7	0
11	7	240
12	1	10
13	1	10
14	1	10
15	1	10

Apply

3.1.8.2 Access Categories

Access categories are used to define access privileges for subscribers, trunk groups, and other objects. The categories enable calls from the incoming channel to the outgoing channel.

To restrict access to an object, assign the corresponding category. For other categories, this menu defines accessibility to a category assigned to an object (to disable access, uncheck the checkbox for the corresponding category; to enable access, check the checkbox next to the corresponding category).

In total, up to 128 access categories can be configured. Access to the first 16 categories is provided by default in each of the access categories.

To configure and edit a selected category, click the button.

Access categories		
No	Category	Access to categories
0	AccessCat#0	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
1	AccessCat#1	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
2	AccessCat#2	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
3	AccessCat#3	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
4	AccessCat#4	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
5	AccessCat#5	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
6	AccessCat#6	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
7	AccessCat#7	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
8	AccessCat#8	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
9	AccessCat#9	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
10	AccessCat#10	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
11	AccessCat#11	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
12	AccessCat#12	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
13	AccessCat#13	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
14	AccessCat#14	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
15	AccessCat#15	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
16	AccessCat#16	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
17	AccessCat#17	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
18	AccessCat#18	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
19	AccessCat#19	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
20	AccessCat#20	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
21	AccessCat#21	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
22	AccessCat#22	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
23	AccessCat#23	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
24	AccessCat#24	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
25	AccessCat#25	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
26	AccessCat#26	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
27	AccessCat#27	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
28	AccessCat#28	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
29	AccessCat#29	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
30	AccessCat#30	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
31	AccessCat#31	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
32	AccessCat#32	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
33	AccessCat#33	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
34	AccessCat#34	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
35	AccessCat#35	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
36	AccessCat#36	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
37	AccessCat#37	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
38	AccessCat#38	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
39	AccessCat#39	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15

Example of access restriction configuration

To restrict access to long-distance communication, proceed as follows:

1. Select the access category for long-distance communication. For convenience, you can specify the name *Long-distance* or *Transition to 8*.

2. Assign 2 categories for subscribers: *LD Subscriber* and *Non LD Subscriber*, for which you can respectively allow/deny access to the *Long-distance* category (select/deselect the checkbox next to the *Long-distance*).

3. In the “Numbering schedule” section: for *Transition to 8* prefix, select *Long-distance* and *Check access category*.

Dial plans

Common prefix settings 29

Title: to 8

Dial plan: [0] NumberPlan#0

Access category: [0] Long-distance

Check access category:

Prefix type: TrunkGroup

TrunkGroup: [0] TrunkGroup00

Direction: national network

CallerID request:

CallerID mandatory:

Dial mode: unchanged

Do not send end-of-dial (ST):

Priority: 100

Max session time (sec): 0

CdPN settings

Number type: unchanged

Numbering plan type: isdn/telephony

Direct route timers

Short timer: 5

Duration: 30

Next Cancel

4. For subscribers with access to long-distance communication, assign the *LD Subscriber* category.
5. For subscribers without access to long-distance communication, assign the *Non LD Subscriber* category.



Steps 4 and 5 can be made using group editing of subscribers:

- Check *Select* next to the required subscribers;
- Click the *Edit selected* button;
- Select the parameter you want to edit by checking the corresponding checkboxes.

3.1.8.3 PBX Profiles

PBX profiles are used to assign additional parameters to SIP subscribers.

PBX profiles			
No	Description	Station prefix	Direct routing prefix
0	PBXprofile#0		not set

To create, edit, or remove a PBX profile, use the *Objects – Add Object*, *Objects – Edit Object*, or *Objects – Remove Object* menus and the following buttons:

- add profile;
- edit profile parameters;
- remove profile.

PBX profiles	
PBX profile 1	
Description	PBX_Profile01
Station prefix	
Direct routing prefix	no prefix ▼
Scheduled routing profile	Not selected ▼
Ingress calls	
Use voice messages	<input type="checkbox"/>
No Connected number transit	<input type="checkbox"/>
Copy CgPN into Redirecting number	<input type="checkbox"/>
Use Redirecting number for routing	<input type="checkbox"/>
CdPN modifiers	not used ▼
CgPN modifiers	not used ▼
Egress calls	
CdPN modifiers	not used ▼
CgPN modifiers	not used ▼
First digit timeout, sec	15
Next digit timeout, sec	5
Busy-tone timeout, sec	60
VAS timeouts	
CFNR timeout, sec	10
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

PBX Profile:

- *Profile name* – the profile name;
- *Station prefix* – prefix to be added to the beginning of SIP/FXS subscriber number (CgPN);
- *Direct prefix* – the prefix will be used without caller or callee number analysis. If the direct prefix is specified, all calls from a SIP subscriber will be directed to the trunk group specified in that prefix, regardless of the dialed number (without creating masks in prefixes).
- *Scheduled routing profile* – select a profile for the *Scheduled Routing* service, which is configured in the *Internal Resources* section.

Incoming Communication:

- *Use voice messages* – when this option is checked, specific events will trigger transmission of the voice messages recorded on the device. For detailed description, see Appendix I. Voice messages and music on hold (MOH);
- *Block Connected number transmission* – disable the transmission of the *Connected number* field;
- *Copy CgPN to Redirecting* – when this option is checked and there is no *Redirecting number* in the incoming call, it will be generated from the CgPN number;
- *Use Redirecting for routing* – when this option is checked, the *Redirecting number* field (SS7 or Q.931 signalling protocols), or the *diversion* field of the SIP protocol is used to route the incoming call in the numbering schedule by the CgPN number masks;

- *CdPN modifiers* – intended for modifications based on the analysis of the callee number received from the incoming channel;
- *CgPN modifiers* – intended for modifications based on the analysis of the caller number received from the incoming channel.

Outgoing Communication:

- *CdPN modifiers* – intended for modifications based on the analysis of the callee number before sending it to the outgoing channel.
- *CgPN modifiers* – intended for modifications based on the analysis of the caller number before sending it to the outgoing channel.

Timers:

- *First digit dialling timeout, sec* – the timeout for waiting for the first digit, after the subscriber presses the FLASH key when using the “Call Transfer” service. When the timeout expires, the subscriber receives a busy signal. Possible values are 5-20 seconds;
- *Next digit dialling timeout, sec* – the timeout for waiting for the next digit after dialling the first one when using the “Call Transfer” service. When the timeout expires, the dialling will be stopped and the call will be routed. Possible values are 5-20 seconds;
- *Busy signal timeout, sec* – timeout for generation of a busy signal in case of unsuccessful dialling of the subscriber when using the “Call Transfer” service. When this timeout expires, the call will be switched to the subscriber who is put on-hold;
- *Call response timeout, sec (for FXS/FXO subscribers)* – timeout for the subscriber response to the incoming call; when the time expires, the caller is disconnected;
- *On hold timeout, sec (for FXS/FXO subscribers)* – timeout for putting the subscriber on hold.


VAS Timers:

- *Call Forwarding No Reply timeout (CFNR), sec* – when this timeout expires, the incoming call will be forwarded by the “Call Forwarding No Reply” VAS service. Possible values are 5-60 seconds.




3.1.8.4 FXS Profiles (for SMG-200 only)

FXS profiles are used to assign additional parameters to FXS subscribers.

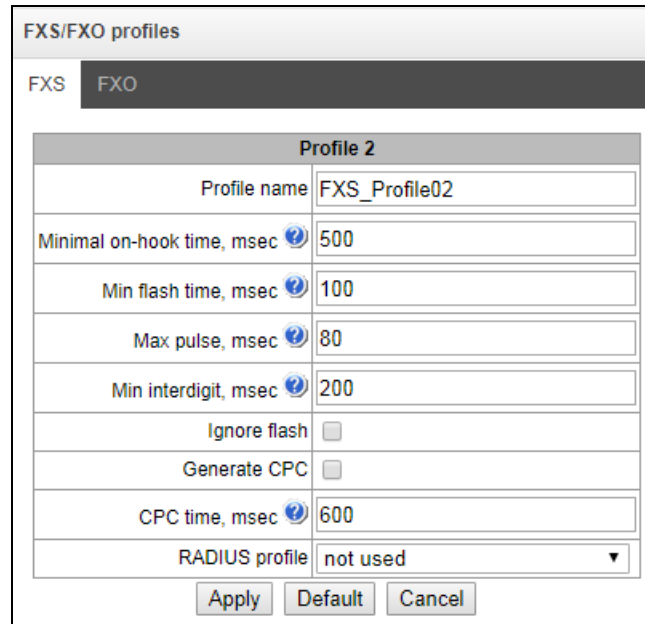
FXS/FXO profiles	
No	Profile name
0	hotline FXO
1	collect FXO



To create, edit, or remove FXS profile, use the *Objects – Add Object*, *Objects – Edit Object*, or *Objects – Remove Object* menus and the following buttons:

-  – add profile;
-  – edit profile parameters;
-  – remove profile.

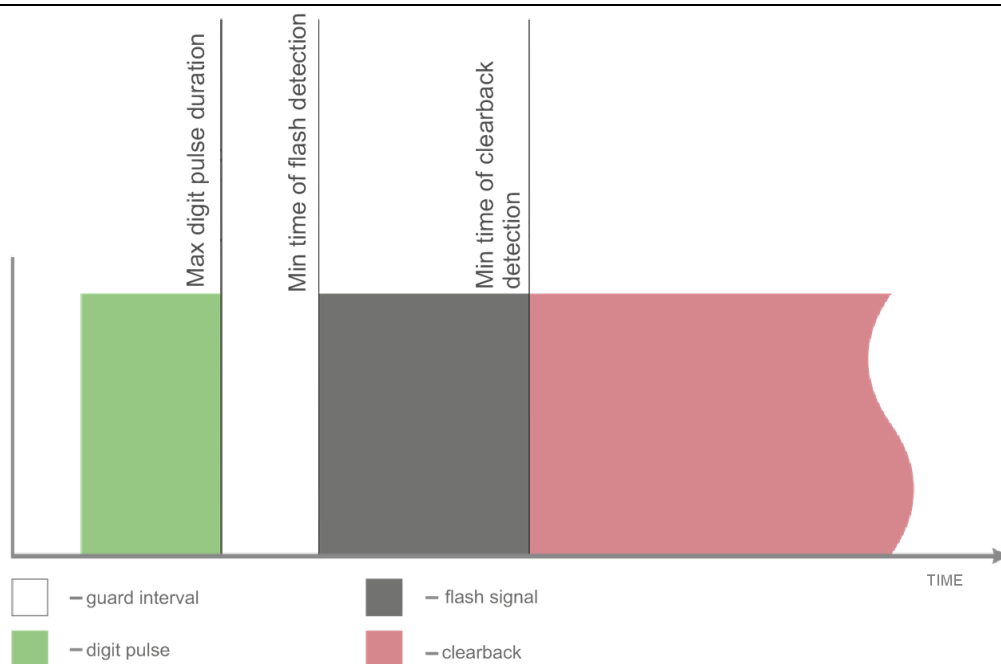
FXS Profile:



Profile 2	
Profile name	FXS_Profile02
Minimal on-hook time, msec	500
Min flash time, msec	100
Max pulse, msec	80
Min interdigit, msec	200
Ignore flash	<input type="checkbox"/>
Generate CPC	<input type="checkbox"/>
CPC time, msec	600
RADIUS profile	not used

- *Profile name* – name of the FXS profile
- *Minimum time to detect clearback, ms* – the time to disconnect the loop, after which the clearback signal will be detected.
- *Minimum time to detect flash, ms* – the time to disconnect the loop, after which the flash signal can be detected, provided that the loop disconnection time does not exceed the minimum time to detect clearback.
- *Maximum time to detect flash, ms* – the loop disconnection time, after which it will be possible to detect the pulse of digit in case of decadic dialling, provided that the loop disconnection time is 10 ms shorter than the minimum time to detect flash.
- *Minimum interdigit delay, ms* – the minimum time interval between digits for pulse dialling.
- *Ignore flash* – when this option is checked, flash signal detection is disabled.

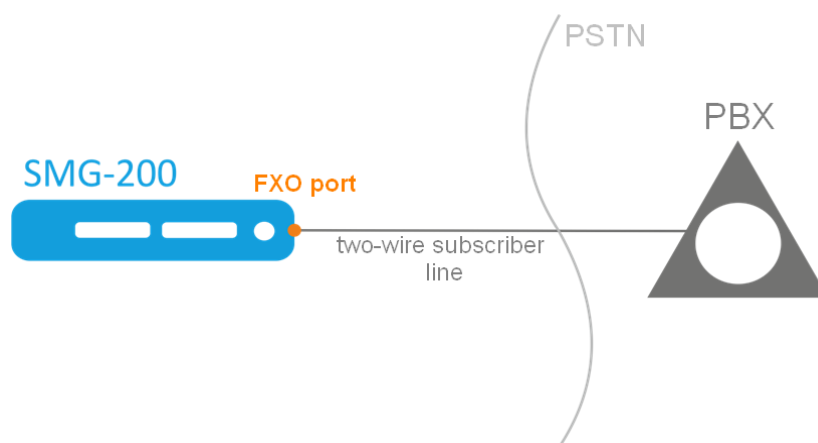
The dialling pulse, flash signal and clearback signal are the signals generated by the loop disconnection with different time intervals. The time intervals of these signals are presented in a graph below.



- *Generate CPC* – when checked, carry out short-time break of a subscriber loop when clearback from the side of communicating device;
- *Duration CPC, ms* – duration of the short-time subscriber loop break ;
- *RADIUS profile* – RADIUS profile used for incoming call authentication,.

3.1.8.5 FXO Profiles (for SMG-200 only)

This section describes how to configure call processing rules for the calls passing through the FXO port. Calls coming to the FXO port from the public switched telephone network (PSTN) over a two-wire subscriber line are configured in the Incoming Communication section. Calls that are to be transmitted to PSTN, are configured in the Outgoing Communication section.



FXO Profile:

FXS/FXO profiles	
FXS	FXO
Ingress calls	
Seize mode	with CallerID
Dial mode	Hotline
Off-hook on	seize
RADIUS profile	not used
Egress calls	
Dial trigger	Pause
Dial pause, sec	2
Dial mode	DTMF
Number dialing	PSTN hotline
Send answer on	seize
Tone detect parameters Show help	
Dialtone detection parameters	425;0(1000/0)
Busytone detection parameters	425;1(330/330)
Ringback tone detection parameters	425;0(1000/4000)
Disconnect tone	425;1(330/330)
<input type="button" value="Apply"/> <input type="button" value="Default"/> <input type="button" value="Cancel"/>	

Incoming Communication

- *Engagement detection* – the parameter indicating when processing begins for a call received to the FXO port from the PSTN.
 - *After Caller ID receipt* – the option enables receipt of the CallerID, which is sent between the first and second ringing. If the Caller ID has not been received, the engagement is determined when the second ringing begins. Caller ID can be received in FSK V23 and FSK BELL202 formats. If the Caller ID is successfully detected, the received number is used as the number of subscriber A (CgPN); otherwise the number specified in the FXO port settings is used as CgPN.
 - *After the first ringing finished* – when this option is checked, the engagement will be determined after the end of the first ringing.
 - *When the first ringing begins* – when this option is checked, the engagement will be determined when the first ringing begins.
- *Dialling mode* – select the method for further processing of the call after the engagement.
 - *Hotline* – the number specified in the “hotline” setting on the FXO port will be used for further routing.
 - *Extension dialling* – after detecting the engagement by PSTN, the device will issue a station response signal to the caller and will be ready to accept dialling in DTMF format.
- *Response at* – this option determines at what time to initiate the response (close the loop). The option is only available for the “hotline” dialling mode, while in the “extension dialling” mode the response (loop closure) will be sent immediately after the engagement.
 - *Engagement* – the response (loop closure) will be sent immediately after the engagement is detected.

- *Call to the remote party* – the response (loop closure) will be sent after the call is routed to the number specified in the “hotline” setting on the FXO port.
- *Response of the remote party* – the response (loop closure) will be sent after the subscriber number specified in the “hotline” setting on the FXO port has answered.
- *RADIUS profile* – RADIUS profile used for incoming call authentication.

Outgoing Communication

- *Start dialling after* – this option determines at what point in time the dialling will be performed after the loop closure when making outgoing calls to PSTN.
 - *Pause* – after the loop is closed, the dialling will be performed after the specified pause.
 - *Station response* – when this option is checked, dialling will be performed after detecting the “station response” signal according to the parameters specified below in the “Parameters of Detected Signals” section.
- *Pause before dialling, s* – the field is active only when ‘Start work after pause’ option is selected;
- *Dialling mode* – select the dialling method.
 - *Tone* – dialling will be done in the tone mode (DTMF).
 - *Pulse* – the number will be dialled in the pulse mode.
 - *Interdigit delay, ms* – the time interval between digits for the pulse mode.
 - *Pulse duration, ms* – duration of a digit pulse for the pulse mode.
 - *Pause duration, ms* – duration of a digit pulse pause for the pulse mode.
- *Dialling* – select the callee number generation mode, for further dialling to PSTN.
 - *PSTN hotline* – the number specified in the “PSTN Hotline” setting in the FXO port parameters will be dialled.
 - *Extension dialling* – when this option is checked, the number received from the caller will be dialled to PSTN using the extension dialling method, after establishing a connection with the FXO port.

Example:
In the FXO port configuration, the “Number” is set to 300. When a call is received to the number 300, it is routed to the FXO port. Next, the FXO port closes the loop and SMG-200 PBX sends the “station response” signal. Then the caller can dial the callee number.
 - *Full number* – when this option is checked, the number dialled to PSTN will be equal to the FXO port number and all digits that follow after the FXO port number.

Example:
In the FXO port configuration, the “Number” is set to 8499. When a call is made to the number 84993668877, the system, based on prefix 8499, will route the call to the corresponding FXO port, and the number 84993668877 will be dialled to PSTN.
 - *No prefix* – when this option is checked, the number that follows the port number specified in the FXO port configuration will be dialled to PSTN.

Example:

In the FXO port configuration, the “Number” is set to 300. When a call is made to the number 30084993668877, the system, based on prefix 300, will route the call to the corresponding FXO port, and the number 84993668877 (not including the FXO port number) will be dialled to PSTN.

Parameters of Detected Signals:

Format of values:

X;Z(A/B),
X,Y;Z(A/B),

where:

X – frequency component 1 (Hz). The range of possible values is [300; 3400].

X – frequency component 2 (Hz). The range of possible values is [300; 3400].

Z – number of repetitions. Maximum 3. For the “Ringing control” signal, “0” means that the voice channel will be connected when no further repetitions of the signal are detected.

A – the tone duration (ms). The range of possible values is [100; 30,000].

B – the pause duration (ms). The range of possible values is [100; 30,000].

3.1.8.6 Modifier Tables

Modifiers tables						
No	Name	TrunkGroups	PBX profiles	RADIUS profiles	CDR settings	Prefixes
0	format_e164	incoming				
1	from_SIP_cdpn	SIP				
2	to_PBX	PBX				
3	format_CDR				CDR settings	
4	to_RADIUS			RADIUS_Profile00		

[Check number](#)

This table contains all created modifiers and the objects they are assigned to.

To create, edit, or remove a modifier, use the *Objects – Add Object*, *Objects – Edit Object*, or *Objects – Remove Object* menus and the following buttons:

- add modifier;
- edit modifier parameters;
- remove modifier;
- add modifier by copying.

Modifiers tables

Modifiers table 5	
Name	ModTable#05
Long timer	7
Short timer	3

Modifiers

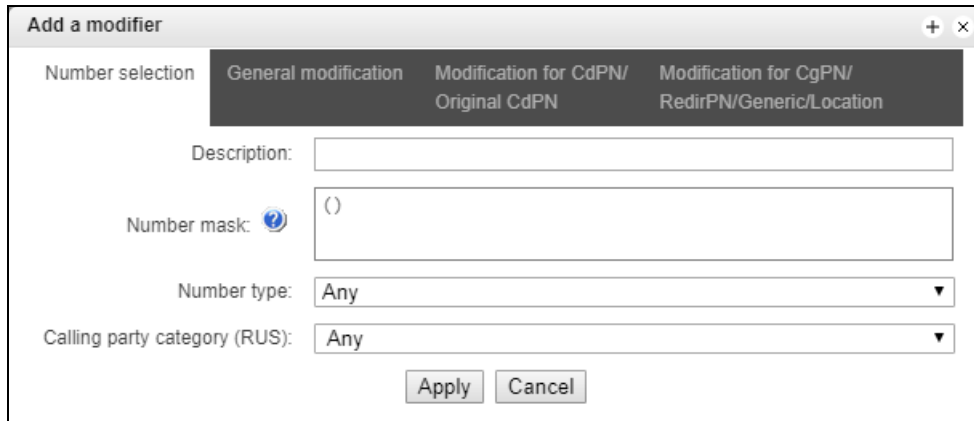
Empty list

To assign or edit parameters of a created modifier, select the corresponding row and click .

To confirm changes in modifier parameters, click the *Set* button, or click the *Cancel* to exit without saving.

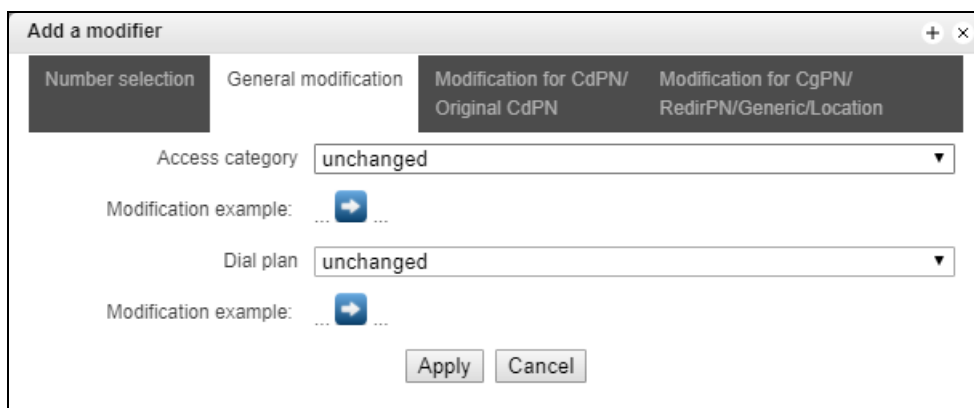
To check the modifier operation, you can click the *Check number* link below the modifier table. For the checking procedure, see section *Checking Modifiers Operation*


Number Selection Tab



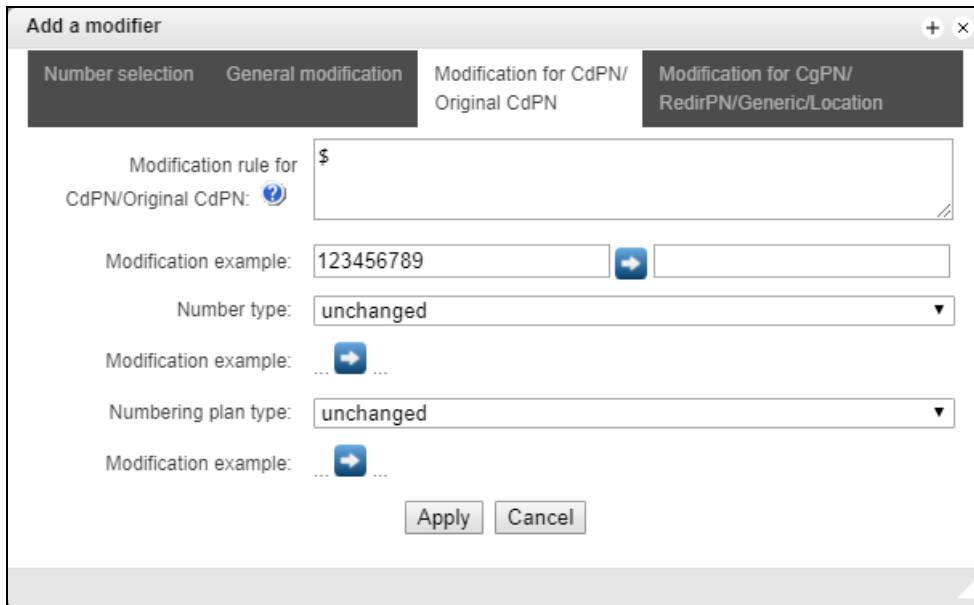
- *Description* – description of the modifier;
- *Number mask* – a template or a set of templates which is compared to the subscriber number (for mask syntax, see section 3.1.6.2);
- *Number type* – type of the subscriber number:
 - *Subscriber* – subscriber number (SN) in E.164 format;
 - *National* – national number. Format: NDC + SN, where NDC – a geographical area code;
 - *International* – international number. Format: CC + NDC + SN, where CC – a country code;
 - *Network specific* – specific network number;
 - *Unknown* – unknown type of the number;
 - *Any* – modification will be performed for any number type;
- *Caller ID category* – subscriber's Caller ID category.


General Modification Tab



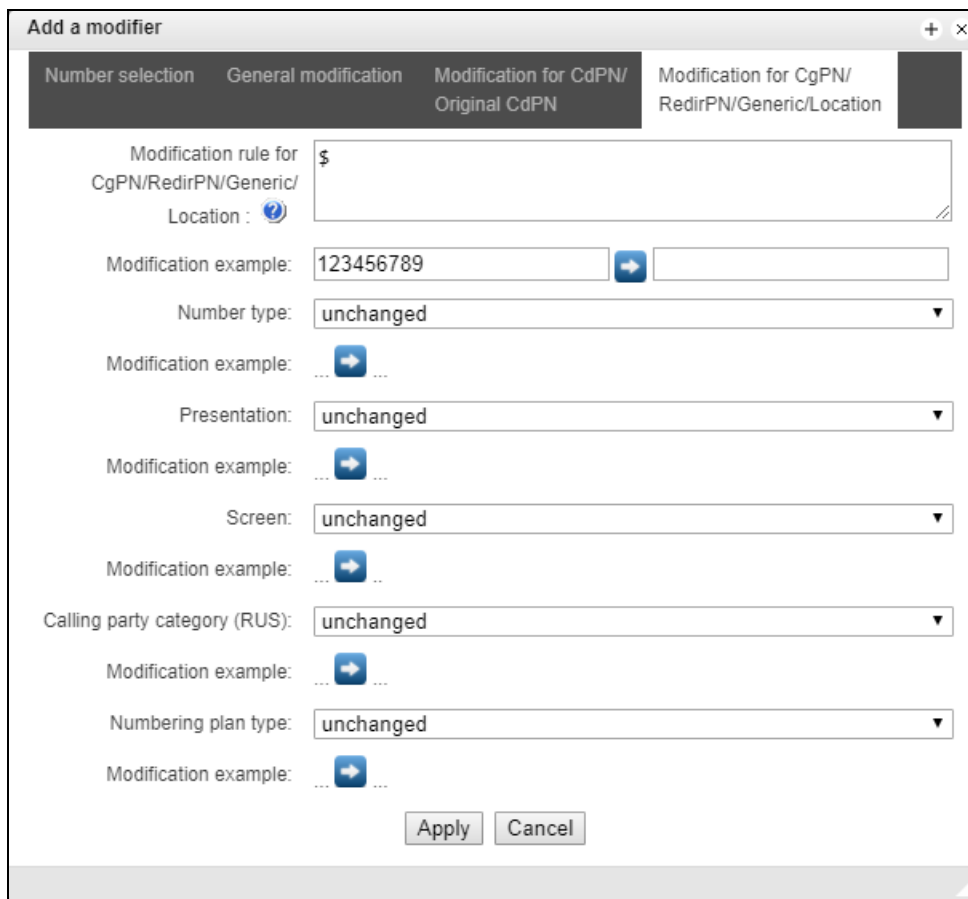
- *Modification example* – click the  button to view modification summary after application of the specified modification rules;
- *Access category* – allows modification of access categories;
- *Numbering schedule* – allows modification of the numbering schedule to be used for further routing (required for coordination of numbering schedules).


CdPN/Original CdPN Modification Tab



- *Modification example* – click the  button to view modification summary after application of the specified modification rules; It is recommended to define a number to be modified instead of number 123456789, which is entered in the rule check example;
- *CdPN/Original CdPN modification rule* – callee number modification rule. For syntax, see section 0; for examples, see Appendix C. This rule also applies to modification of the callee original number (original Called party number) when this modifier table is chosen in the *Trunk Group* section for *Original CdPN* modification;
- *Number type* – modification rule for the callee number type;
- *Numbering schedule type* – modification rule for the numbering schedule type.

CgPN/RedirPN/Generic/Location Modification Tab



- *CgPN/RedirPN/Generic/Location modification rule* – the callee number modification rule. The syntax used is described in section 0. Some examples are given in Appendix C. This rule also applies to the redirecting number modification (if this modifier table is selected in the group trunk section for the RedirPN modification); to the Generic Number modification (if selected in the GenericPN modifications section); or to the Location Number modification (if selected in the LocationNumber modifications section);
- *Modification example* – click the  button to view modification summary after application of the specified modification rules. It is recommended to define a number to be modified instead of number 123456789, which is entered in the rule check example;
- *Number type* – modification rule for the caller number type;
- *Presentation* – modification rule for the caller presentation;
- *Screen* – modification rule for the caller screen indicator;
- *Caller ID category* – modification rule for the caller category;
- *Numbering schedule type* – modification rule for the numbering schedule type.

Modification Rule Syntax

Modification rule is a set of special characters that govern number modifications:

- '.' and '!': special characters indicating that a digit is removed in the current position and other digits that follow the removed one are shifted to its position;

- 'X', 'x': special characters indicating that a digit in the current position remains unchanged (the position must contain a digit).
- '?': a special character indicating that a digit in the current position remains unchanged (the position may contain no digits);
- '+': a special character indicating that all characters located between the current position and the next special character (or the end of the sequence) are inserted at the specified location of the number;
- '!': a special character indicating a breakdown finish; all other digits of the number are truncated;
- '\$': a special character indicating a breakdown finish; all other digits of the number remain unchanged;
- **0–9, D, #, and *** (not preceded by +): informational characters that substitute a digit in the specified position of the number.

Modification examples:

Add city code 383 to number 2220123

Modifier: **+383**

Result: **38322201234**

Replace country code with 7 in number 83832220123

Modifier: **7**

Result: **738322201234**

Replace the third digit with 6 in number 2220123

Modifier: **xx6\$ or XX6\$**

Result: **22601234**

Remove prefix 99# from number 99#2220123

Modifier: **---\$**

Result: **2220123**

Remove the last four digits from number 22201239876

Modifier: **\$----**

Result: **2220123**

Select the first seven digits of number 222012349876

Modifier: **xxxxxxx!**

Result: **2220123**

Delete the last two digits, replace the third digit with 6 and add the city code 383 to number 222012398

Modifier: **+383xx6\$--**

Result: **3832260123**

– *Checking Modifiers Operation*

The *Check number* link under the modifier table allows you to check the modifiers for the number with specified parameters.

To perform the check, you need to set the CdPN and CgPN numbers, fill in the following fields: Number type, Numbering Schedule Type, Presentation, Screen, and Caller ID Category. Then select the desired CdPN and CgPN modification tables and click the Check button. Next to the populated fields, the blue arrows will show the values that will be assigned to the number as a result of the modification. Below you will see the number masks that contain the numbers being checked, and the descriptions of the modifiers included in the modification table.

3.1.8.7 Q.850-Cause and SIP-Reply Code Correspondence Table

This section establishes correspondence between clearback reasons described in Q.850 recommendations for the SS-7 protocols (SIP-T/SIP-I) and 4xx, 5xx, 6xx class SIP replies.

The correspondence described in the Order No. 10 as of January 27, 2009, issued by the Ministry of Communications and Mass Media (MinComSvyaz) of the Russian Federation is used by default; for the causes not described in this Order, the correspondence described in Q.1912.5 recommendation for SIP-I and in RFC3398 for SIP/SIP-T is used.

To create, edit, or remove rules in correspondence tables, use the following buttons:

- *add rule;*
- *edit rule parameters;*
- *remove rule.*

- Name – name of the Q.850-cause and SIP-reply correspondence table.

Profile Settings

- Direction:

Q.850-cause and SIP-reply mapping table

№	Name
0	Profile #0

Q.850-cause and SIP-reply mapping table

Profile 0

Name: Profile #0

Save Cancel

Q.850-cause to SIP-reply mapping table

№	Cause	Reply

SIP-reply to Q.850-cause mapping table

№	Reply	Cause

- SIP reply -> Q.850 cause – direction from SIP to Q.850;
- Q.850 cause -> SIP reply – direction from Q.850 to SIP;
- Q.850 cause – value of a Q.850 cause;
- SIP-reply – value of a 4xx, 5xx, 6xx class SIP reply.

Q.850-cause and SIP-reply mapping table

Mapping	
Direction	SIP-reply -> Q.850-cause
Q.850-cause	
SIP-reply	

Save Cancel

3.1.8.8 Scheduled Routing

This section configures scheduled routing that allows the use of different numbering schedules depending on the time and day of the week.

Scheduled routing

Profile 0

Name Profile #0

Save Cancel

Call routing rules

No	Begin	Duration (days)	Dial plan
0	31.05.2018	0	[0] NumberPlan#0

+ - -

To create, edit, or remove rules, use the following buttons:

- add rule;
- edit rule parameters;
- remove rule.

Routing Rule

- Operation period start date – select start date for the scheduled routing rule operation;
- Operation duration (days) – duration of the scheduled routing rule operation;
- Repeat every month – allows monthly repetition of the routing rule;
- Days of the week – select days of the week for the scheduled routing rule operation;
- Hours of operation – select hours of the scheduled routing rule operation;
- Numbering schedule – select a numbering schedule that will be used during the scheduled routing rule operation.

Scheduled routing

Route rule

May 2018

Mon	Tue	Wed	Thu	Fri	Sat	Sun
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

Start date

Active days 0

Repeat monthly

Week days

Mon	Tue	Wed	Thu	Fri	Sat	Sun
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Active hours (0:00-11:59)

(12:00-23:59)

Dial plan [0] NumberPlan#0

Save Cancel

3.1.8.9 Hunt Groups

Call group¹ – a group of numbers to which the device can initiate calls using different dialling types for these numbers when a call arrives at the call group prefix.

The call group is designed for call centres or connection of offices with simultaneous or successive dialling for employees from the same call group.

In total, you can create up to 1000 call groups.




No	Name	Masks for CdPN	Calling mode	Group members	Выделить
0	HuntGroup00	40299	sequential from first	40221 40222 40223	<input type="checkbox"/>
1	HuntGroup01	12000	simultaneous call	20000 20001 20002 20003	<input type="checkbox"/>

10 Rows in the table to show

Current page 1 from 1

Remove selected

To create, edit, or remove entries in the table, use the following buttons:

-  – add entry;
-  – edit entry parameters;
-  – remove entry.

A call group can include both numbers of device subscribers and external numbers.

Hunt groups

Hunt group 2

Name	HuntGroup02
Dial plan	[0] NumberPlan#0
Masks for CdPN	
Calling mode	simultaneous call
Participant ringing timeout, sec	5
Group ringing timeout, sec	30
Queue settings	
Queue size	15
Sound path	off
Sound path	
Music on hold	<input checked="" type="checkbox"/>
Advertise	<input type="checkbox"/>
Advertise timeout, sec	15
Play queue position	<input checked="" type="checkbox"/>
Position timeout, sec	30
First position timeout, sec	2
Persian numbers	<input type="checkbox"/>
Answer tone	<input type="checkbox"/>
Cache calls	None
Work day time	09:00 - 18:00
Group members	
<input type="button" value="Add"/>	

¹ This option is available only if you have an SMG-VAS license. For more information about the licenses, see section 3.1.22 Licenses

-
- *Name* – name of a call group
 - *Numbering schedule* – select a numbering schedule that the call group will belong to;
 - *CdPN masks* – the callee number mask to call the group from the numbering schedule tied to the group (the mask syntax is described in section 3.1.6.2);
 - *Operation mode* – the method of dialling to members of a call group:
 - *simultaneous call* – calls to all members of a call group are made at the same time.
 - *from the first, one by one* – method that always dials the first number in the call group number list when a new call comes to this group. After the Stimer expires, the call to a member of this group is cancelled and a call to the next member of the group is initiated;
 - *sequentially, one by one* – group numbers are called one by one, starting from the number of a member who has ended a conversation in the previous call to this call group. This method is required to balance the load between the group members. After the Stimer expires, the call to a member of this group is cancelled and a call to the next member of the group is initiated;
 - *from the first, adding the next* – method that always dials the first number in the call group number list when a new call comes to this group. After the Stimer expires, the call to a member of this group is not cancelled and a call to the next member of the group is initiated;
 - *sequentially, adding the next* – group numbers are called one by one, starting from the number of a member who has ended a conversation in the previous call to this call group. This method is required to balance the load between members. After the Stimer expires, the call to a member of this group is not cancelled and a call to the next member of the group is initiated;
 - *serial search (from the first)* – the method that searches for the first available subscriber from the beginning of the list; this group can include only subscribers of this gateway;
 - *serial search (from the last)* – the method that searches for the first available subscriber from the end of the list; this group can include only subscribers of this gateway;
 - *Conference number* – when this number is dialled after the Conference VAS prefix, all members of this call group will be included into a conference call.
 - *Member call timeout, sec* – the call timeout for one member of a call group;
 - *Group call timeout, sec* – the general call timeout for the entire call group.

The queue functionality is available for the following modes: “simultaneous call”, “from the first one by one”, “sequentially one by one”, “from the first, adding the next”, and “sequentially, adding the next”.

The queue functionality is required for call centres.

- *Queue size* – the maximum number of members waiting in the queue for the operator’s answer. When the specified number is exceeded, new calls will be rejected.
- *Drive path* – when “off” is selected, the system audio files, located in the file system of the device, will be used for the queue. If needed, you can record your audio files to an external drive and indicate the path to the drive with the audio files. The files should have specific names, as shown in the table below.

- *Audio files directory* – the directory name on the external drive where the audio files for the queue are stored.



Audio files should have the following parameters: WAV format, codec G.711a, 8 bit, 8 kHz, mono.

File name	Value	By default
queue_position.wav	“Your position in the queue”	yes
answer_tone.wav	Sound\melody to be played with the operator answer	no
callback.wav	Phrase played to the operator before a subscriber is called back	no
advertise	Directory with advertising files	no
not_more_2m.wav	“Maximum waiting time: 2 minutes”	yes
not_more_3m.wav	“Maximum waiting time: 3 minutes”	yes
not_more_4m.wav	“Maximum waiting time: 4 minutes”	yes
not_more_5m.wav	“Maximum waiting time: 5 minutes”	yes
more_than_5m.wav	“Waiting time: more than 5 minutes”	yes
1-20.wav, 30.wav	Number in the queue	yes
callback_operator.wav	Phrase played to the operator before a subscriber is called back	no
callback_abonent.wav	Phrase played to the subscriber when the callback option is enabled	no

- *MoH instead of ringback* – “music on hold” instead of ringback tones when waiting for the operator's answer.
- *Advertise* – when this option is checked, audio files from the advertise directory will be played to the caller waiting for the operator's answer (with the specified advertising timeout).



Only the first 5 files in the advertise directory will be used. This option is only available when the audio files for the queue are stored on an external drive.

- *Advertising timeout, sec* – the period during which advertising will be played.
- *To play the queue position* – when this option is checked, the caller will be informed of their position in the queue.
- *Queue position timeout, sec* – the interval at which the subscriber will be informed of their position in the queue; the interval starts when the last playback of the position ends.
- *First playback timeout, sec* – time after which the subscriber's queue position will be played for the first time.
- *Persian numerals* – SMG200/SMG-500 devices support playback of composite Persian numerals. To reproduce numbers greater than 20, three parts of a numeral, including a connecting word, are used.
- *Notification at reply* – when this option is checked, the answerer_tone.wav audio file will be played to the caller and operator after the operator responds.

- *Call caching* – this option is used to store an operator who has spoken with the caller last time. Ensures that in case of calling back, the caller immediately gets to the operator to whom they were talking last time.
 - *Disabled* – caching is disabled.
 - *Strict* – if the operator is busy, the call will not be forwarded to other operators but will wait for the specified operator to get free.
 - *Not strict* – if the required operator is busy, the call will be distributed among other operators in accordance with the accepted operation mode.
- *Working hours* – sets the working hours to calculate the statistics of a call group.

Group members – the list of operators who are members of a call group.

3.1.8.10 Interception Groups

Interception group¹ – a group of device subscribers: when a call comes to a subscriber of this group, another group member can intercept this call by dialling an exit prefix for this call group.

No	Name	Numbers list	Select
0	PickupGroup00	345771 Ordinary	<input checked="" type="checkbox"/>

To create, edit, or remove entries in the table, use the following buttons:

- Add Entry;
- Edit Entry Parameters;
- Remove Entry.

Only subscribers of this device can be members of this group.

- *Name* – name of the interception group;
- *Number list* – members of the interception group.

Interception group member type:

- *Restricted* – cannot intercept, but calls to this member can be intercepted by another member of the group;

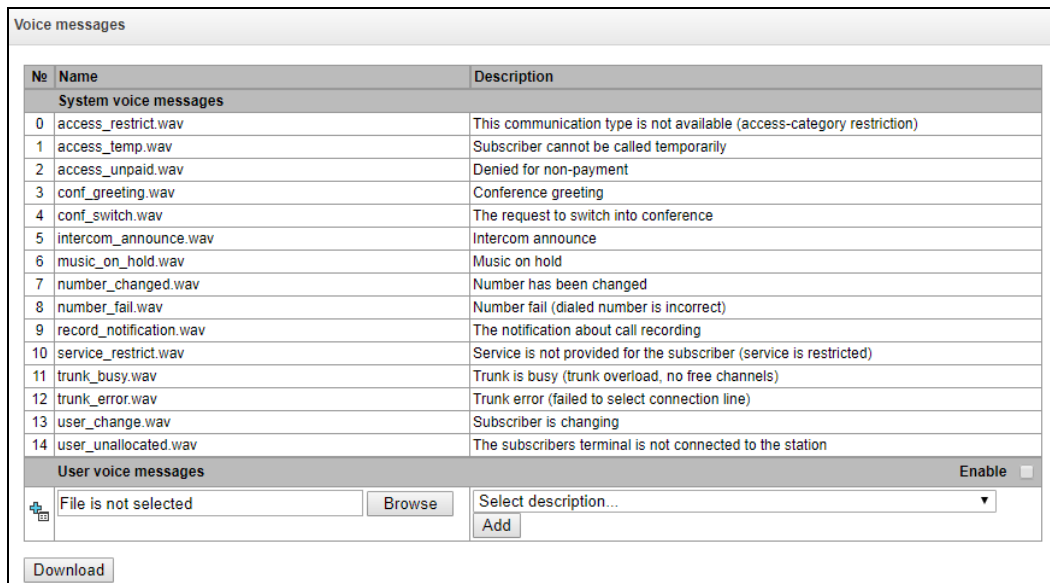
¹ This option is available only if you have an SMG-VAS license. For more information about the licenses, see section **3.1.22 Licenses**

- *Common* – can intercept calls to common and restricted group members, but cannot intercept calls to a privileged group member;
- *Privileged* – can intercept calls to any member of the interception group.

3.1.8.11 Voice Messages

There are 11 standard phrases of voice messages on the device, which are used to inform subscribers. In this section, you can upload custom voice message files.

A file should be in WAV format compressed using codec G.711a, 8bit, 8khz mono. File size should not exceed 2 MB.



No	Name	Description
System voice messages		
0	access_restrict.wav	This communication type is not available (access-category restriction)
1	access_temp.wav	Subscriber cannot be called temporarily
2	access_unpaid.wav	Denied for non-payment
3	conf_greeting.wav	Conference greeting
4	conf_switch.wav	The request to switch into conference
5	intercom_announce.wav	Intercom announce
6	music_on_hold.wav	Music on hold
7	number_changed.wav	Number has been changed
8	number_fail.wav	Number fail (dialed number is incorrect)
9	record_notification.wav	The notification about call recording
10	service_restrict.wav	Service is not provided for the subscriber (service is restricted)
11	trunk_busy.wav	Trunk is busy (trunk overload, no free channels)
12	trunk_error.wav	Trunk error (failed to select connection line)
13	user_change.wav	Subscriber is changing
14	user_unallocated.wav	The subscribers terminal is not connected to the station
User voice messages		
File is not selected		Enable <input type="checkbox"/>
Browse		Select description... <input type="text"/>
		Add
Download		

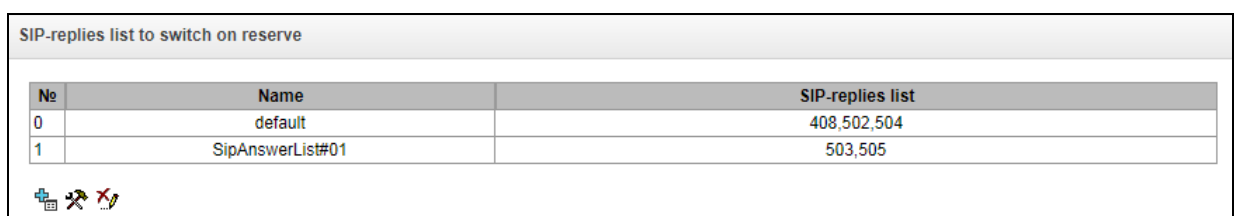
- *No.* – sequential number of a voice message file;
- *Name* – name of a voice message file;
- *Description* – description of a voice message file.

To add your own file and select description of an event for this file to be played, click the *Select file* and *Add* buttons.

- *Enable* – enables playback of a voice message file.

3.1.8.12 List of SIP Replies for Transition to a Redundant Trunk Group

In this section, you can configure the list of SIP responses of 4XX – 6XX class that will be used for transition to the redundant trunk group or to the next trunk in the trunk direction.



No	Name	SIP-replies list
0	default	408,502,504
1	SipAnswerList#01	503,505

To create, edit, or remove the list, use the *Objects – Add Object*, *Objects – Edit Object* or *Objects – Remove Object* menus and the following buttons:

- Add the reply list;
- Edit the reply list;
- Remove the reply list.

The screenshot shows a dialog box titled "SIP-replies list to switch on reserve". Inside, there is a sub-dialog titled "SIP-replies list 1". It contains a table with the following data:

SIP-replies list 1	
Name	SipAnswerList#01
1	503
2	505

Below the table are "Add", "Apply", and "Cancel" buttons.

You should specify the list name and generate it by clicking the *Add* and (*Remove*) buttons.

3.1.8.13 List of Q.850 Clearback Causes

In this section, you can configure the list of Q.850 clearback causes for SS7 and Q.931 protocols that will be used for transition to the redundant trunk group or to the next trunk in the trunk direction.

The screenshot shows a table titled "Q.850 release causes list".

No	Name	Q.850 release codes
0	Release causes #00	41

Below the table are icons for Add, Edit, and Remove.

To create, edit, or remove the list, use the *Objects – Add Object*, *Objects – Edit Object* or *Objects – Remove Object* menus and the following buttons:

- Add the reply list;
- Edit the reply list;
- Remove the reply list.

The screenshot shows a dialog box titled "Q.850 release causes list". Inside, there is a sub-dialog titled "Q.850 release codes 0". It contains a table with the following data:

Q.850 release codes 0	
Name	Release causes #00
1	41

Below the table are "Add", "Apply", and "Cancel" buttons.

You should specify the list name and generate it by clicking the *Add* and (*Remove*) buttons.

3.1.9 IVR

IVR (Interactive Voice Response) – a smart call routing system based on the information entered by the client using the telephone keypad and tone dialling, current time and day of the week, caller number and callee




number; it enables voice notification of subscribers using audio files uploaded to the device. This function is required for call centres, taxi services, technical support, etc.

In this section, you can configure lists of IVR scripts and sounds, as well as manage recorded conversations files.

3.1.9.1 List of Scripts




In this section, you can create the IVR operation scripts¹.

To create, edit, or remove entries in the tables, use the following buttons:

-  – Add Entry;
-  – Edit Entry Parameters;
-  – Remove Entry.

The **List of Scripts** table – this table displays all created IVR scripts.

Scenarios list		
No	Name	Filename
0	IVRScenario_00	

- *Name* – IVR script name;
- *File name* – select an IVR script file from the list of files created on the device.


The **System Parameters** table – this table contains the *Path to a drive for IVR scripts* setting, which specifies a drive to store the script files.

Files list		
No	Filename	Delete
		<input type="checkbox"/>



The **List of Files** table – this table displays all created IVR script files.

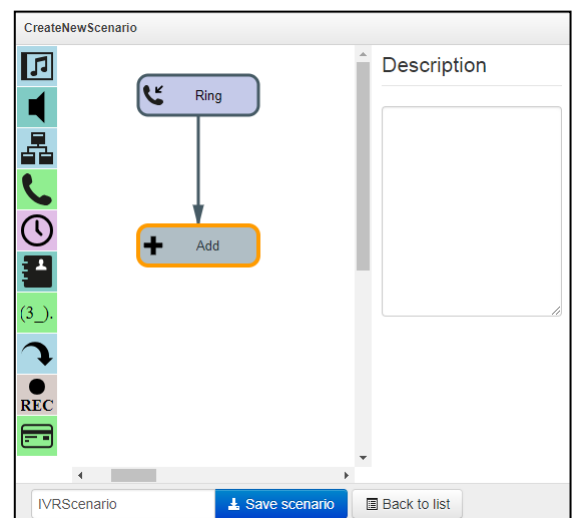
The **List of Common Scripts** table – this table contains files of common IVR scripts that can be edited.

-  *Download script* – download the scripts selected in the table to the user PC.

The script creation and editing menu provides a design view: the IVR script flowchart is generated in the central field; on the left side there are common blocks; on the right side there is a list of configurable parameters for the current block.

To select a block in the chart, left-click it. Borders of the selected block turn orange.

To add a block, select the *Add* empty block and then



¹ This option is available only if you have an SMG-IVR license. For more information about the licenses, see section **3.1.22 Licenses**

select the desired action from the set of common blocks by left-clicking it. In the field on the right, configure the parameters for the created block. Logical links for a newly created item will be added automatically. The logical link for the *Goto* block is set manually; to do this, click the *Select block on chart* button in the block parameters and select the desired block. The logical link for the *Goto* is represented by the dashed line.

When the selected block has been configured, you should save the changes by clicking the *Save* button or click *Cancel* to cancel them.

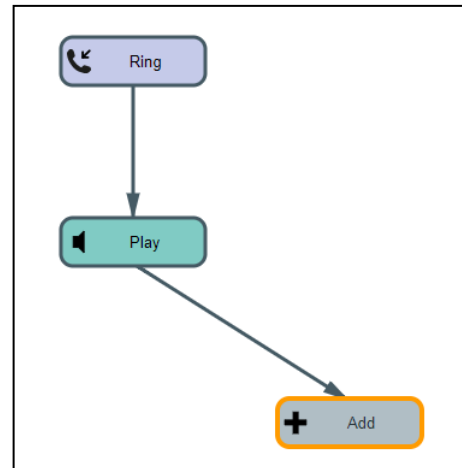
To remove the selected block from the chart, click the *Remove block* button. If this block has any lower-level logical links, the **entire branch** of these lower-level objects will be removed.

You can move the blocks across the field; to do this, select the desired block and move it to the desired place while holding the left mouse button. At that, all existing logical links will remain intact.

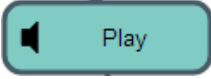

You can also modify the form of a logical link between the blocks by left-clicking it. The selected line turns orange and has three points to edit: to set the output point from the block, the input point to the block, and the line curvature.



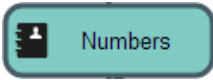
For IVR block description, see Table 12


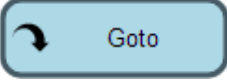

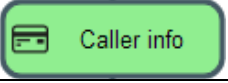
Table 12 – IVR Block Description



Symbol	Name	Description
	Add	An empty unit designed for block addition.
	Ring	<p>This block enables ringback tone playback for the subscriber; it is always the first one in the list of scripts. When a call arrives to the RING block, the call status does not change.</p> <p>Parameters</p> <p><i>Ringback playback duration, sec</i> – select duration of the ringback tone playback or disable it.</p> <p>Links</p> <p><i>Input</i> – beginning of the call to IVR.</p> <p><i>Output</i> – a single output containing information about the incoming call parameters (number A, number B).</p> <p>Features</p> <p>The block does not change the call status.</p>
	Info	<p>The block is required for playback of a single or multiple voice messages to the caller in the preanswering state (without taking a call by subscriber B). In other words, while this block is being played, no connection fee is charged. This block can be placed in the script after the blocks that do not change the call status, and if there was no previous transition to the answering state. The block is useful to inform the callee with service information until the resource that is able to handle the call becomes free.</p> <p>Parameters</p> <p><i>Messages for playback until the subscriber answers</i> – select a single or multiple voice messages for playback to the caller. For voice message management, see section 3.1.8.11 Voice Messages. A drive for storing the files can be specified in section 3.1.1 System settings.</p>

		<p><i>Loop playback</i> – select the number of message playback loops; they are played one by one, starting from the first message.</p> <p>Links</p> <p><i>Input</i> – an incoming call in the preanswering state.</p> <p><i>Output</i> – end the playback of the selected files.</p> <p>Features</p> <p>The Info block may be preceded only by blocks that do not affect the call status (Ring, Info, Digitsmap, Time, Goto).</p>
	<p>Play</p>	<p>The block is required for playback of a single or multiple voice messages to the caller in the answer state (after subscriber B answers). The block is used to inform subscriber A.</p> <p>Parameters</p> <p><i>Messages for playback until the subscriber answers</i> – select a single or multiple voice messages for playback to the caller. For voice message management, see section 3.1.8.11 Voice Messages. A drive for storing the files can be specified in section 3.1.1 System settings.</p> <p><i>Loop playback</i> – select the number of playback cycles. The messages are played one by one, starting from the first message.</p> <p>Links</p> <p><i>Input</i> – an incoming call in the preanswering or answer state.</p> <p><i>Output</i> – end the playback of the selected files.</p>
	<p>IVR</p>	<p>The block is required to implement the interactive voice menu function. In this block, you can select the logical path of the call by clicking certain combinations of digits, extension dialling of the subscriber number according to the internal numbering schedule and playback of audio files, system sounds (ringback tones, ringing tone, a busy signal) and DTMF digits to notify the subscriber.</p> <p>Parameters</p> <p><i>Type</i> – the type of audio file to be played.</p> <p><i>File</i> – an audio file uploaded to the device. The list of IVR sounds is configured in section 3.1.9.2 IVR Audio List).</p> <p><i>Tone</i> – select a system sound to be played (DTMF digit, dialtone, busy, ringback).</p> <p><i>Subscriber selection</i> – configure the logic for further call path. When you click on the configured combination of digits, the device identifies the outgoing branch of the IVR block. If the subscriber has not clicked anything, “No Match” branch is selected.</p> <p><i>Subscriber selection timeout, sec</i> – extension number dialling timer; when this timer expires, the outgoing IVR branch is selected.</p> <p><i>Enable extension dialling</i> – enable extension dialling, which is followed by the device numbering schedule routing, e. g. internal subscriber number can be dialled.</p> <p><i>Access category</i> – select an access category. Access category allows you to define call barring for the number dialled by the subscriber in the IVR block.</p> <p><i>Number of digits for extension dialling</i> – the maximum number of digits that can be dialled using the extension dialling.</p>

		<p><i>Interdigit delay, sec</i> – interdigit delay for the extension number.</p> <p>Links</p> <p><i>Input</i> – an incoming call in the preanswering state or active call phase.</p> <p><i>Output</i> – the number of outputs can be configured, extension dialling can also be one of the outputs.</p> <p>Features</p> <p>If the call entering the block is in the preanswering state, the block automatically changes it into the active state (sends a reply to the caller), followed by the further execution of the block logic.</p>
	<p>Dial</p>	<p>The block is required to dial the specified number, which is further routed according to the numbering schedule of the device.</p> <p>Parameters</p> <p><i>Number</i> – the specified number.</p> <p>Numbering Schedule</p> <p><i>Transit</i> – the numbering schedule is not changed.</p> <p>Links</p> <p><i>Input</i> – an incoming call in the preanswering state or active call phase.</p> <p><i>Output</i> – exit from the block if the dial is unsuccessful.</p> <p>Features</p> <p>Finishes the script branch.</p>
	<p>Time</p>	<p>The block is required to select the call path logic according to the current time and day of the week.</p> <p>Parameters</p> <p><i>Time</i> – select a template for time and day of the week. The time is set in 24-hour format.</p> <p>Links</p> <p><i>Input</i> – an incoming call in the preanswering state or active call phase.</p> <p><i>Output</i> – the block has 2 outputs: the first one is used when the time matches the specified template (“yes” output), the second – if no match is detected (“no” output).</p> <p>Features</p> <p>The block does not change the call status.</p>
	<p>Numbers</p>	<p>The block is required to select the call path logic depending on the caller number.</p> <p>Parameters</p> <p><i>Number</i> – the caller number template.</p> <p>Links</p> <p><i>Input</i> – an incoming call in the preanswering state or active call phase.</p> <p><i>Output</i> – the block has 2 outputs: the first one is used when the caller number matches the specified template (“yes” output), the second – if no match is</p>

		<p>detected (“no” output).</p> <p>Features</p> <p>The block does not change the call status.</p>
	Digitmap	<p>The block is required to select the call path logic depending on the callee number. The callee number is verified at the entry to the digitmap block.</p> <p>Parameters</p> <p><i>Mask</i> – the callee number template.</p> <p>Links</p> <p><i>Input</i> – an incoming call in the preanswering state or active call phase.</p> <p><i>Output</i> – the block has 2 outputs: the first one is used when the callee number matches the specified template (“yes” output), the second – if no match is detected (“no” output).</p> <p>Features</p> <p>The block does not change the call status.</p>
	Goto	<p>The block is required to transfer a call to another arbitrary script block.</p> <p>Parameters</p> <p><i>Select block in the chart</i> – click this button to select a block in the chart to which the transition will be made.</p> <p><i>Maximum number of actuations</i> – select the number of passes for a call through this block to ensure the call looping protection.</p> <p>Links</p> <p><i>Input</i> – an incoming call in the preanswering state or active call phase.</p> <p><i>Output</i> – a single output to the block to which the transition is made.</p> <p>Features</p> <p>The block does not change the call status.</p>
	REC	<p>The block is required to start conversation recording; as soon as the call logic has passed through the block, the subscriber conversation is recorded into a file.</p> <p>Links</p> <p><i>Input</i> – an incoming call in the active call phase.</p> <p><i>Output</i> – the block has a single output.</p> <p>Features</p> <p>The block does not change the call status. The conversation recording is stopped only after disconnection. In order to configure a directory for saving IVR call record files, see section 3.1.16.1 Recording Parameters, in the “Folder name for IVR conversation recording” parameter. For management of the records, see section 3.1.9.3 Conversation Recording.</p>
	Caller Info	<p>The block allows you to change the caller name, which will be displayed on the callee's phone. The block allows you to display the caller name, company name and other data on the callee's phone.</p>

		<p>Parameters:</p> <p><i>Number mask</i> – the caller number template.</p> <p><i>Subscriber name</i> – new subscriber name.</p> <p>Links</p> <p><i>Input</i> – an incoming call in the preanswering state or active call phase.</p> <p><i>Output</i> – the block has a single output.</p> <p>Features</p> <p>The block does not change the call status.</p>
--	--	--

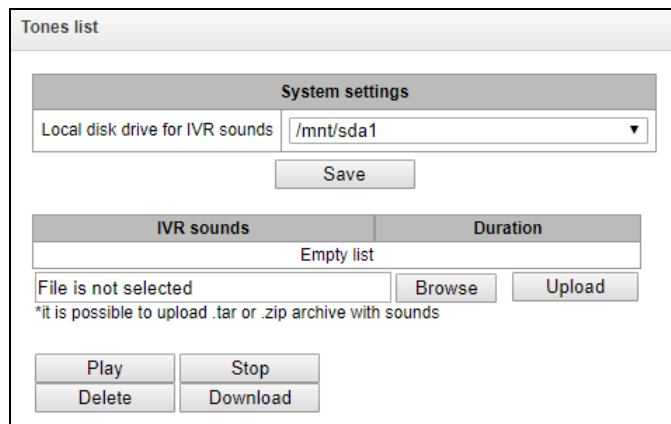
After you create the script flowchart, specify its name and save it by clicking the *Save script* button. Click the *Back to list* button to exit the design view without saving any changes.

3.1.9.2 IVR Audio List

In this section, you can manage the audio files required for IVR operation.

Audio file format: WAV, codec G. 711A, 8 bit, 8 KHz, mono.

The **System Parameters** table contains the “Path to IVR audio drive” setting that specifies a drive to store IVR conversation record files.



- *IVR audio* – the list of uploaded files;
- *Duration* – uploaded file length;
- *Browse* – select an audio file to be uploaded to your device;
- *Upload* – command to upload the selected file.



You can upload a tar or zip archive file containing multiple audio files; audio files should be in the root directory of the archive.

- *Play* – play the selected file;
- *Stop* – stop playing the file;
- *Delete* – delete the selected file;

- *Download* – download the selected file from the device.

3.1.9.3 Conversation Recording (IVR)

In this section, you can manage IVR conversation record files. If there is a **REC** block in the IVR script, all recorded conversations will be displayed in the table.

- *Total number of records* – total number of conversation record files in the selected directory;
- *Drive utilisation* – display the used space on the drive selected to store the conversation record files;
- *Select the date* – select the date to display conversation record files;
- *Time interval* – select the interval to display conversation record files;
- *Search details* – search for conversation record files; the search function uses any match of the entered value against the name of a conversation record file.

The record control buttons are described in the table below.

Table 13 – Record Control Buttons

Button	Function
	previous record
	start playback
	stop playback
	next record
	repeated record playback
	save record
	delete record

Format of a conversation record file

1. A common call without call forwarding or transfer

YYYY-MM-DD_hh-mm_ss-CgPN-CdPN.wav

where

- **YYYY-MM-DD** – file creation date, YYYY – year, MM – month, DD – day;
- **Hh-MM_SS** – file creation time, hh – hours, mm – minutes, ss – seconds;
- **CgPN** – the caller number, if absent, set to none;
- **CdPN** – the callee number.

Example:

Subscriber 7111 calls to subscriber 7222. The file will look as follows:

2014-05-20_12-05-35_7111_7222.wav

2. Making a call when the call forwarding service is used

YYYY-MM-DD_hh-mm_ss-CgPN- RdNum cf CdPN.wav

where:

- **YYYY-MM-DD** – file creation date, YYYY – year, MM – month, DD – day;
- **Hh-MM_SS** – file creation time, hh – hours, mm – minutes, ss – seconds;
- **CgPN** – the caller number, if absent, set to none;
- **RdNum** – redirecting number – the number with a configured call forwarding service.
- **Cf** – a label indicating that the call forwarding service was used;
- **CdPN** – the callee number – the number that actually receives the call.

Example:

Subscriber 7111 calls to subscriber 7222 who redirects the call to subscriber 7333.

2014-05-20_12-05-35_7111_7222cf7333.wav

3. Making a call when the call transfer service is used

The use of the call transfer service involves 3 subscribers – initiator of the call (subscriber A), subscriber implementing the call transfer (subscriber B), and subscriber receiving the transferred call (subscriber C).

When transferring a call, 3 conversation record files are created:

- Conversation between subscribers A – B;
- Conversation between subscribers B – C;
- Conversation between subscribers A – C after the call transfer.

Example:

Subscriber 7111 calls to subscriber 7333, which transfers the call to subscriber 7333.

The following files are generated:

2014-05-20_12-05-35_7111_7222.wav – conversation of subscribers A and B.

2014-05-20_12-06-36_7222_7333.wav – conversation of subscribers B and C, after the subscriber B has put the subscriber A on hold.

2014-05-20_12-05-35_7111_7222ct7333.wav – conversation of subscribers A and C after the call was transferred by subscriber B, where *ct* in the file name is the label indicating that was the call transfer was made.

3.1.10 TCP/IP Settings

This section configures device network settings and IP packet routing rules.

- **DHCP** is a protocol which allows automatic retrieval of IP address and other settings required for operation in a TCP/IP network. It allows the gateway to obtain all necessary network settings from DHCP server.
- **SNMP** is a simple network management protocol. It allows the gateway to send real-time messages about failures to the controlling SNMP manager. Also, the gateway's SNMP agent supports monitoring of gateway sensors' status on request from the SNMP manager.
- **DNS** is a protocol which is used to retrieve domain information. It allows the gateway to obtain the IP address of the communicating device by its network name (hostname). This may be useful, e. g. when hosts are specified in the routing schedule or when a network name of the SIP server is used as its address.
- **TELNET** is a protocol which is used to establish control over network. Allows remote connection to the gateway from a computer for configuration and management. In case of the TELNET protocol, the data transfer process is not encrypted.
- **SSH** is a protocol which is used to establish control over network. Unlike TELNET, this protocol implies encryption of all data transferred through the network, including passwords.

3.1.10.1 Routing Table

This submenu can be used to configure static routes.




Static routing allows packets to be routed to specified IP networks or IP addresses through the specified gateways. The packets sent to IP addresses, which do not belong to the gateway IP network and are outside the scope of static routing rules, will be sent to the default gateway.

The routing table is separated into 2 parts: configured routes at the top of the table and automatically created ones.

The automatically created routes cannot be changed as they are created automatically when the network and VPN/PPTP interfaces are established. These routes are required for normal operation of the interfaces.

Routing table							
No	Enable	Status	Destination	Mask	Gateway	Interface	Metric
Automatically generated routes							
0	Yes	Active	default	0.0.0.0	192.168.1.123	eth0	0
1	Yes	Active	192.168.0.0	255.255.255.0	*	eth0	0
2	Yes	Active	192.168.1.0	255.255.255.0	*	eth0	0
3	Yes	Active	192.168.69.0	255.255.255.0	*	eth0.609	0

To create, edit, or remove a route, use the *Objects – Add Object*, *Objects – Edit Object* or *Objects – Remove Object* menus and the following buttons:

-  – Add Route;
-  – Edit Route Parameters;
-  – Remove Route.

Route Parameters

- *Enable* – when this option is checked, enables the route;
- *Direction* – IP network;
- *Mask* – specifies a network mask for the defined IP network (use mask 255.255.255.255 for IP address);
- *Interface* – select a network transmission interface;
- *Gateway* – defines an IP address of the route gateway;
- *Metrics* – the route metrics.

Routing table

Route #0	
Enable	<input type="checkbox"/>
Destination	<input type="text"/>
Mask	<input type="text" value="255.255.255.255"/>
Gateway IP-address or *	<input type="text" value="*"/>
Interface	<input type="checkbox"/> eth1 (eth0 192.168.1.20) ▼
Metric	<input type="text" value="0"/>

Network settings

Hostname	<input type="text" value="smg200"/>
Use gateway from	<input type="text" value="eth1 (eth0 192.168.1.20) ▼"/>
Primary DNS	<input type="text" value="0.0.0.0"/>
Secondary DNS	<input type="text" value="0.0.0.0"/>
Port for SSH	<input type="text" value="22"/>
Port for Telnet	<input type="text" value="23"/>

3.1.10.2 Network Settings

This submenu can be used to specify a device name and to change the network gateway address, the DNS server address, and the SSH/Telnet access ports.

- *Hostname* – device network name;
- *Use the gateway interface* – select the network interface to be used as the primary gateway of the device;
- *Primary DNS* – primary DNS server;
- *Secondary DNS* – secondary DNS server;
- *ssh access port* – TCP port for device access via the SSH protocol; the default value is 22;
- *Telnet access port* – TCP port for device access via the Telnet protocol; the default value is 23.

3.1.10.3 Network Interfaces

You can configure 1 main network interface eth0 and up to 9 additional interfaces on the device. These can be VLAN interfaces and alias of the main eth0 interface, or alias of the VLAN interface.

Alias – an optional network interface that is created from an existing primary eth0 interface or from an

existing VLAN interface.

Network interfaces												
No	Interface name	Network label	IP-address	Network mask	DHCP	Management services			Telephony services			Firewall profile
0	eth0	eth1	192.168.1.20	255.255.255.0	-	WEB	TELNET	SSH	SIP	RTP	RADIUS	Not selected
1	eth0:1	0.20	192.168.0.20	255.255.255.0	-				SIP	RTP	RADIUS	Not selected
2	eth0.609	vlan 609	192.168.69.20	255.255.255.0	-					RTP		Not selected

To create, edit, or remove rules for network interfaces, use the following buttons: *Add*, *Edit*, *Remove*.

Network Interface Settings

Basic Settings

- *Network name* – name of the network;
- *Firewall profile* – shows the firewall profile selected for this interface;
- *Type* – interface type (always untagged for eth0 interface);
- *VLAN ID* – VLAN identifier (1–4,095) (only for tagged type interfaces);
- *Enable DHCP* – dynamically obtain the IP address from the DHCP server (Alias is not supported);
- *IP address* – network address of the device;
- *Subnet mask* – the subnet mask of the device;
- *Broadcast* – address for packet broadcasting;
- *Gateway* – network gateway for the interface (Alias is not supported);
- *Obtain DNS automatically* – obtain the IP address of the DNS server dynamically from the DHCP server (Alias is not supported);
- *Obtain NTP automatically* – obtain the IP address of the NTP server dynamically from the DHCP server (Alias is not supported);

Network interfaces

Network interface 3

Network label	<input type="text"/>
Firewall profile	Not selected
Type	Untagged ▼
Enable DHCP	<input type="checkbox"/>
IP-address	<input type="text"/>
Network mask	<input type="text"/>
Broadcast	<input type="text"/>
Gateway	<input type="text"/>
DNS-address by DHCP	<input type="checkbox"/>
NTP-address by DHCP	<input type="checkbox"/>
Services	
Enable Web	<input type="checkbox"/>
Enable Telnet	<input type="checkbox"/>
Enable SSH	<input type="checkbox"/>
Enable SIP signalling	<input type="checkbox"/>
Enable RTP transmission	<input type="checkbox"/>
Enable RADIUS	<input type="checkbox"/>

Services – a configuration menu for the services enabled for this interface:

- *Management via Web* – enables access to the configurator via the interface;
- *Management via Telnet* – enables access via the Telnet protocol;
- *Management via SSH* – enables access via the SSH protocol;
- *SIP signalling* – enables reception and transmission of the SIP signalling information through the network interface configured in this section;

- *Send RTP* – enables reception and transmission of the voice traffic through the network interface configured in this section;
- *Enable RADIUS* – enables the RADIUS protocol.



If an IP address or a network mask has been changed or the web configurator management has been disabled for the network interface, confirm these settings by logging into the web configurator to prevent the loss of access to the device; otherwise, the previous configuration will be restored in two minutes.

3.1.10.4 RTP Port Range

This section allows configuration of a UDP port range for voice RTP packets transmission.

UDP Port Parameters

- *Starting port* – the number of the starting UDP port for voice traffic (RTP) and data transmission via the T.38 protocol;
- *Number of ports* – the number of UDP ports (starting from the first port) used for voice traffic (RTP) and data transmission via the T.38 protocol.



To avoid conflicts, make sure that the ports used for RTP and T.38 transmission do not overlap the ports used for SIP signalling (port 5060 by default).

3.1.11 Network Services

3.1.11.1 NTP

NTP is a protocol for synchronisation of real-time clock of the device. It allows synchronisation of date and time used by the gateway against their reference values.

- *Use NTP* – enables time synchronisation via NTP;
- *Time server (NTP)* – the IP address or host name of the NTP server;
- *Timezone* – configuration of the time zone and GMT (Greenwich Mean Time) offset:

- *Manual mode* – defines the GMT offset;
- *Automatic mode* – this mode allows selection of device location; the GMT offset will be determined automatically. This mode also enables automatic switch to daylight saving time;
- *NTP synchronisation period, minutes* – an interval between synchronisation requests.
- *Save* – saves changes.
- *Discard* – discards changes.

To force time synchronisation with the server, click the *Restart NTP Client* button (the NTP client will be restarted).

3.1.11.2 SNMP setting

SMG software enables to monitor status of the device via SNMP. In SNMP submenu, you can configure settings of the SNMP agent.

SNMP monitoring functions are able to request the following gateway parameters:

- gateway name;
- device type;
- firmware version;
- IP address;
- E1 stream statistics;
- IP submodule statistics;
- Linkset state;
- E1 stream channel state;
- IP channel state (statistics show the current calls by IP).

Statistics of the current calls by IP channels show the next data:

- channel number;
- channel state;
- Call ID;
- Caller MAC address;
- Caller IP address;
- Caller number;
- Callee MAC address;
- Callee IP address;
- Callee number;
- Channel engagement duration.

SNMP settings:

- *Sys Name* – device name;
- *Sys Contact* – contact information;
- *Sys Location* – device location;
- *ro Community* – parameter read password/community;
- *rw Community* – parameter write password/community.

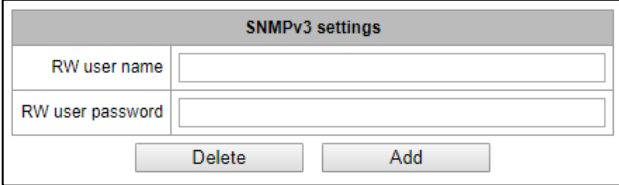
SNMP settings	
Sys Name	SMG500
Sys Contact	Contact
Sys Location	Location
ro Community	public
rw Community	private
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Use "Apply"/"Reset" button to apply/reset the settings.

SNMPv3 configuration:

The system uses a single SNMPv3 user.

- *RW User name* – user name;
- *RW User password* – password (password should contain 8 characters or more);



The image shows a web interface titled "SNMPv3 settings". It contains two input fields: "RW user name" and "RW user password". Below these fields are two buttons: "Delete" and "Add".

To apply SNMPv3 user configuration, click 'Add' button (settings will be applied immediately). To remove a record, click 'Remove' button.

3.1.11.4 *SNMP trap settings*


For detailed monitoring parameters and Traps description, see MIB files on disk shipped with the gateway.

SNMP agent sends SNMPv2-trap messages when the following events occur:

- Configuration error;
- SIP module failure;
- IP submodule failure;
- Linkset failure;
- SS7 signal channel failure;
- Synchronization loss or synchronization from the lower priority source;
- E1 stream failure;
- Remote E1 failure;
- Configuration error is corrected;
- SIP-T module normal operation restored after failure;
- IP submodule normal operation after failure;
- Linkset normal operation restored after failure;
- SS7 channel normal operation restored after failure;
- Synchronization from the priority source is restored;
- No stream fault (after failure or remote failure);
- FTP server is unavailable, utilization of RAM for CDR file storage exceeds 50%(15 – 30 Mb);
- FTP server is unavailable, utilization of RAM for CDR file storage is below - 50% (5 – 15 Mb);
- FTP server is unavailable, utilization of RAM for CDR file storage is full up to 5 Mb;
- External storage has less than 5Mb of free space;
- Software update or configuration file upload/download status.

SNMP traps settings				
No	Type	Community	IP-address	Port
0	trap2sink		0.0.0.0	162

Restart SNMPd

- *Restart SNMPd* – click this button to restart SNMP client;
- *Download MIB files* – download up-to-date MIB files.

To create, edit or remove trap parameters, use the following buttons:

- 'Add';
- 'Edit';
- 'Remove'.

- *Type* – SNMP message type (TRAPv1, TRAPv2, INFORM);
- *Community* – password contained in traps;
- *IP address* – trap receipt IP address;
- *Port* – trap receipt UDP port (default port – 162).

SNMP trap 1	
Type	trapsink ▼
Community	<input type="text"/>
IP-address	0.0.0.0
Port	162

3.1.11.5 FTP Server

This section allows configuration of an integrated FTP server used for provisioning FTP access to the following directories:

- *cdr* – a directory with CDR files;
- *log* – a directory with tracing files and other debug data;
- *mnt* – a directory with files of external storage devices (SSD drives, SATA drives, USB flash drives).

FTP Server Settings

FTP-server settings				
Enable	<input type="checkbox"/>			
Network interface	eth1 (eth0 192.168.1.20) ▼			
Port	21			
Authorization timeout, sec	120			
Idle timeout, sec	180			
Session timeout, sec	600			

User settings:

Name	Directory access			
	log	mnt	CDR	Configuration
ftuser	R	R	R	R

- *Enable* – enables/disables the local FTP server;
- *Network interface* – select a network interface for the FTP server;
- *Port* – select a TCP port for the FTP server;
- *Authorisation timeout, seconds* – a timeout for subscriber authorisation on the FTP server; when the timeout expires, the server forces connection termination;
- *Idle timeout, seconds* – a timeout for user idle status on the FTP server; when the timeout expires, the server forces connection termination;
- *Session timeout, seconds* – duration of a session.

User Configuration:

By default, the device has a subscriber account created with permissions to read all directories (login: **ftpuser**, password: **ftppasswd**).

User settings:

Name	Directory access			
	log	mnt	CDR	Configuration
ftpuser	R	R	R	R

To edit a user, click ; to create a new user, click .

Page for editing/creating a user:

FTP-server

Username 1

Name:

Password:

Access to logs: read; write.

Access to mounts: read; write.

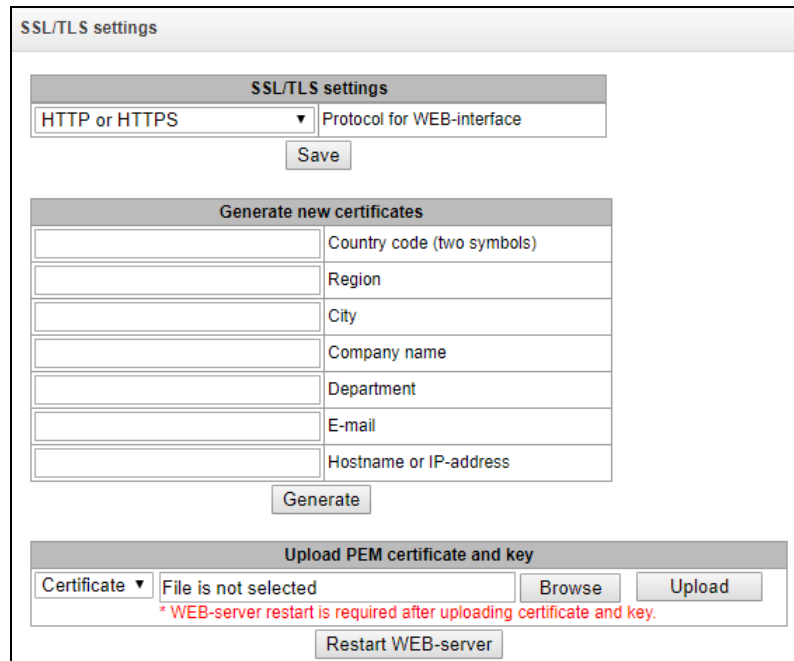
Access to CDR: read; write.

Access to configuration: read; write.

- *Name* – username;
- *Password* – user password;
- *Access to log* – log directory access configuration, read/write;
- *Access to mnt* – mnt directory access configuration, read/write;
- *Access to CDR* – CDR directory access configuration, read/write;
- *Access to Configuration* – /etc/config directory access configuration, read/write.

3.1.12 Security

3.1.12.1 SSL/TLS Configuration



This section is used to obtain a self-signed certificate in order to use an encrypted connection to the gateway via the HTTP protocol and to upload/download configuration files via the FTPS protocol.

- *Web configurator interaction protocol* – web configurator connection mode:
 - *HTTP or HTTPS* – allows both unencrypted (HTTP) and encrypted (HTTPS) connections. HTTPS connection is possible only when a generated certificate is available;
 - *HTTPS only* – enables only encrypted HTTPS connection. HTTPS connection is possible only when a generated certificate is available.

Generate New Certificates



These parameters should be entered in Latin characters.

- *2-digit country code* – country code (RU for Russia);
- *Region* – region name;
- *City* – city name;
- *Organisation* – organisation name;
- *Organisation unit* – name of the organisation unit or division;
- *Contact e-mail* – e-mail address;
- *Device name (or IP address)* – IP address of the gateway.

Upload the PEM Certificate and Key

In this section, you can upload the pre-generated and signed PEM certificate and key. Select the type of file to upload from the drop-down menu. Click the Browse button and select the required file. Then click the Upload button.



After the certificate and key are loaded, the web server should be restarted with the Restart web server button.

3.1.12.2 Dynamic firewall

Dynamic firewall – a utility that monitors for attempts to access various services. When the utility discovers repeated unsuccessful access attempts from the same IP address/host, it blocks all further access attempts from this IP address/host.

The following actions may be identified as an unsuccessful access attempt:

- brute forcing of authentication data for the web configurator or SSH protocol, i. e., attempts to enter the management interface with incorrect login or password.
- Brute forcing authentication data – reception of REGISTER requests from a known IP address but containing wrong authentication data;
- Reception of requests (REGISTER, INVITE, SUBSCRIBE, and others) from an unknown IP address;
- Reception of unknown requests via SIP port.

Dynamic firewall

Settings	SIP	WEB	TELNET	SSH
Enable	<input type="checkbox"/>			
Block time, sec	600	600	600	600
Forgive time, sec	1800	1800	1800	1800
Access attempts before blocking	3	3	3	3
Block attempts before black-listing	4	4	4	4
Progressive block	<input type="checkbox"/>			

White list (Total records: 2)

Add Search Delete

	IP address or IP/mask (last 30 records)
<input type="checkbox"/>	192.162.1.0/24
<input type="checkbox"/>	127.0.0.1

Black list (Total records: 0)

Add Search Delete

	IP address or IP/mask (last 30 records)
The list is empty	

Blocked addresses list (Total records: 0)

Search Delete

	IP address or IP/mask (last 30 records)
The list is empty	

Parameters:

- *Enable* – run the dynamic firewall utility;
- *Ban time, sec* – time in seconds during which access from a suspicious address will be banned;
- *Forgiveness time, sec* – time after which the address initiating the problem query will be forgotten, in case it has never been blocked before;

144

Office IP SMG-200 and SMG-500 PBXs

- *Number of access attempts* – the maximum number of unsuccessful service access attempts before the host is banned by dynamic firewall.
- *Number of temporary bans* – the number of bans after which the problem address will be forcibly blacklisted;
- *Progressive ban* – when this option is checked, each new address ban will be twice as long as the previous one, and the number of access attempts before banning will be half as the previous number of attempts. For example, for the first time the address was banned for 30 seconds after 16 attempts, for the second time – for 60 seconds after 8 attempts, for the third time – for 120 seconds after 4 attempts, and so on..

White list (the last 30 records) – a list of IP addresses or subnets that cannot be banned by a dynamic firewall.



White list doesn't mean that access is allowed. The list doesn't enable any permissive rules. The presence of IP address in this list means the address will not be automatically blocked.

Black list (the last 30 records) – a list of permanently banned addresses or subnets. A total of 8,192 entries can be created on SMG-200/SMG-500. To add, search, or remove an address from the list, select it in the entry field and click the *Add*, *Search*, or *Remove* button.

An IP address or a subnet can be specified.

To enter a subnet, enter the data in the following format:

AAA.BBB.CCC.DDD/mask

Example:

192.168.0.0/24 – this record corresponds to the network address 192.168.0.0 with the mask 255.255.255.0.

- *Download the entire white/black list of IP addresses* – the web configurator interface shows only the last 30 records in the file; click this button to download the entire white or black list to PC.

List of banned addresses – a list of addresses banned by the dynamic firewall. A total of 8,192 entries can be created on SMG-200/SMG-500.

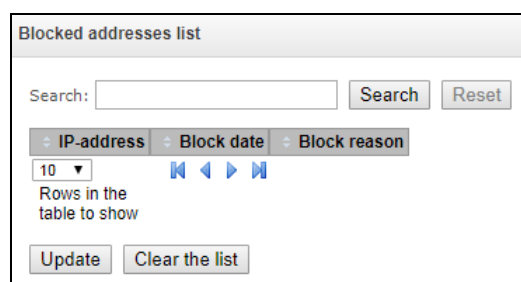
- *Download the entire list of banned IP addresses* – allows download of the entire list of banned addresses to PC.

To update the lists, click the *Refresh* button next to the header.

The dynamic firewall log file is located in the **pbx_sip_bun.log** file.

3.1.12.3 Banned Address Log

This section displays a log of addresses banned by the dynamic firewall, which allows you to analyse when and which addresses have been banned since the gateway was turned on.



- *Search string* – enter an address to search in the table of banned addresses.

MAC address

- *IP address* – IP address that was banned;
- *Ban date* – date and time when the IP address was banned;
- *Ban reason* – explanation which service imposed the ban and why.

Buttons

- *Update* – update the banned address log;
- *Clean the log* – remove all entries from the banned address log.

The table below contains the list of ban messages and their causes.

Table 14 – Ban messages

Message in pbx sip__bun.log	Ban cause	SIP message
Request error: REGISTER failed : Resource limit overflow	Maximum number of registrations of dynamic users is reached	403 response
Request error: REGISTER failed : Unknown user or registration domain	Registration request of an unknown user	403 response
Request error: REGISTER failed : Server doesn't allow a third party registration	Registration request with different to and from headers	403 response
Request error: REGISTER failed : Authentication is wrong	Invalid login/password	403 response
Request error: REGISTER failed : Wrong de-registration	The user attempts to deregister an unregistered contact	200 response
Request error: REGISTER failed : Request from disallowed IP	Attempt to register from an address other than permitted	403 response
Request error: INVITE failed : No registration before	Call attempt from a user who is known but their contact has not been registered	403 response
Request error: INVITE failed : Registration is expired	Call attempt from the user who is known, but their contact registration has expired	403 response
Request error: INVITE failed : Authentication is wrong	Incoming call or registration is not authenticated	403 response
Request error: INVITE failed : Unknown original address	A call from an unknown direction	The call is routed to mgapp, where the decision to pass or reject is taken
Request error: INVITE failed : RURI not for me	Unknown host name or address in RURI	404 response
Request error: BYE failed : Call/Transaction Does Not Exist	No dialogue was found to accept the request	481 response

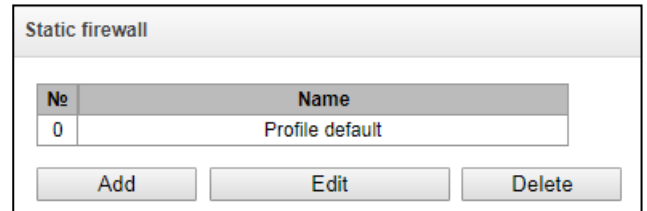
3.1.12.4 Static Firewall

Firewall is a software tools package that allows control and filtration of transmitted network packets in accordance with defined rules to protect the device from unauthorised access.

Firewall Profiles

To create, edit, or remove firewall profiles, use the following buttons:

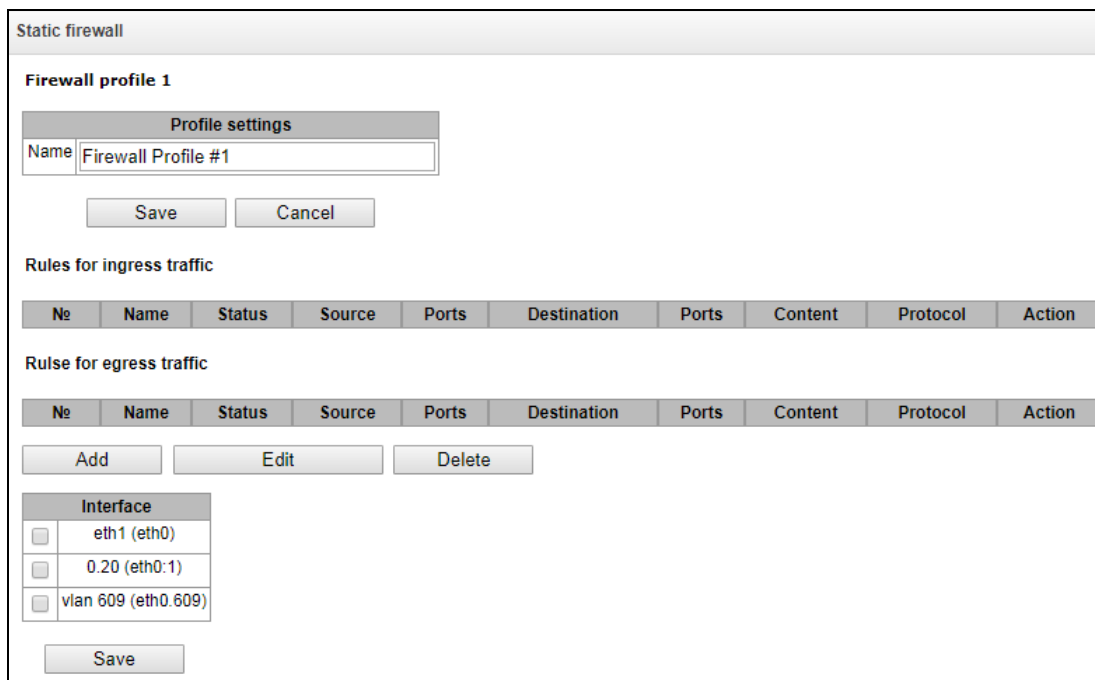
- Add;*
- Edit;*
- Remove.*



No	Name
0	Profile default

Buttons: Add, Edit, Delete

The software allows configuration of firewall rules for incoming, outgoing and transit traffic, as well as for specific network interfaces.



Static firewall

Firewall profile 1

Profile settings

Name: Firewall Profile #1

Buttons: Save, Cancel

Rules for ingress traffic

No	Name	Status	Source	Ports	Destination	Ports	Content	Protocol	Action
----	------	--------	--------	-------	-------------	-------	---------	----------	--------

Rules for egress traffic

No	Name	Status	Source	Ports	Destination	Ports	Content	Protocol	Action
----	------	--------	--------	-------	-------------	-------	---------	----------	--------

Buttons: Add, Edit, Delete

Interface

<input type="checkbox"/>	eth1 (eth0)
<input type="checkbox"/>	0.20 (eth0:1)
<input type="checkbox"/>	vlan 609 (eth0.609)

Button: Save

When a rule is created, the following parameters are configured:

Static firewall

Firewall rule	
Name	Firewall rule 0
Enable	<input type="checkbox"/>
Traffic type	Ingress
Rule type	General
Packet source	<input checked="" type="checkbox"/> Any
IP-address/mask	0.0.0.0
Source ports	0
Destination address	<input checked="" type="checkbox"/> Any
IP-address/mask	0.0.0.0
Destination ports	0
Protocol	Any
ICMP message type	any
Action	Accept

Save Cancel

Static firewall

Firewall rule	
Name	Firewall rule 1
Enable	<input type="checkbox"/>
Traffic type	Ingress
Rule type	String
Content	
Packet source	<input checked="" type="checkbox"/> Any
IP-address/mask	0.0.0.0
Source ports	0
Destination address	<input checked="" type="checkbox"/> Any
IP-address/mask	0.0.0.0
Destination ports	0
Protocol	Any
ICMP message type	any
Action	Accept

Save Cancel

Static firewall

Firewall rule	
Name	Firewall rule 1
Enable	<input type="checkbox"/>
Traffic type	Ingress
Rule type	GeoIP
Country	Afghanistan (AF)
Source ports	0
Destination ports	0
Protocol	Any
ICMP message type	any
Action	Accept

Save Cancel

- *Name* – rule name;
- *Enable* – defines whether the rule is used; When this option is unchecked, the rule is inactive;
- *Traffic type* – type of traffic for the rule being created:
 - *incoming* – intended for SMG;
 - *outgoing* – sent by SMG;
- *Rule type* – can take values:
 - *Normal* – with checking the IP addresses and ports;
 - *GeoIP* – with checking the address against the GeoIP database;
 - *String* – with checking the presence of a string in the packet.

- *Packet source* – define the network address of the packet source either for all addresses or for a particular IP address or network:
 - *any* – for all addresses (the checkbox is checked);
 - *IP address/mask* – for a particular IP address or network. The field is active when the *any* checkbox is unchecked. The mask is mandatory for a network, but optional for an IP address.
- *Source ports* – a TCP/UDP port or port range (defined with a hyphen “-”) of the packet source. This parameter is used for TCP and UDP only; thus, select UDP, TCP, or TCP/UDP in this field to make it active;
- *Destination address* – define the network address of the packet recipient either for all addresses or for a particular IP address or network:
 - *any* – for all addresses (the checkbox is checked);
 - *IP address/mask* – for a particular IP address or network. The field is active when the *any* checkbox is unchecked. The mask is mandatory for a network, but optional for an IP address.
- *Destination ports* – a TCP/UDP port or port range (defined with a hyphen “-”) of the packet recipient. This parameter is used for TCP and UDP only; thus, select UDP, TCP, or TCP/UDP in this field to make it active;
- *Protocol* – the protocol for which the rule will be used: UDP, TCP, ICMP, or TCP/UDP.
- *Message type (ICMP)* – the ICMP message type for which the rule will be used. This field is active when ICMP is selected in the *Protocol* field;
- *Action* – an action executed by the rule:
 - *ACCEPT* – the packets corresponding to this rule will be accepted by the firewall;
 - *DROP* – the packets corresponding to this rule will be rejected by the firewall without informing the party that has sent them;
 - *REJECT* – the packets corresponding to this rule will be rejected by the firewall. The party that has sent the packet will receive either a TCP RST packet or *ICMP destination unreachable*.
- *Country* – select the country to which the address belongs. The field is displayed only for the GeolP rule type;
- *Content* – the string that must be contained in the packet. A case-sensitive search will be done across the entire packet. The field is displayed only for the String rule type;

A created rule is placed into the corresponding section: “Incoming traffic rules”, “Outgoing traffic rules” or “Transit traffic rules”.

Also, in the *firewall profile*, you can specify network interfaces that these profile rules will be applied to.

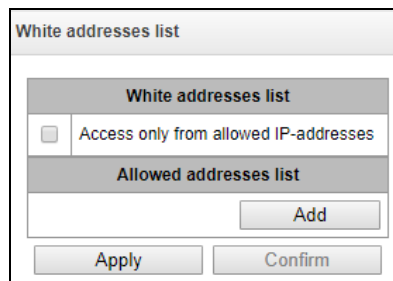


Every network interface can be used only in a single firewall profile at a time. As soon as a network interface is assigned to a new profile, it is removed from the old one.

To apply the rules, click the *Apply* button that appears when changes are made into the firewall settings.

3.1.12.5 List of Allowed IP Addresses

In this section, you can configure the list of allowed IP addresses that the administrator can use for connection to the device via web configurator or Telnet/SSH protocol. By default, all addresses are allowed.





- *Access for allowed IP addresses only* – when this option is checked, the list of allowed IP addresses is used; otherwise, access is allowed from any address.

You can enable access for subnets by setting an IP/mask address, for example: 192.168.0.0/24.

- *Apply* – apply changes;
- *Commit* – confirm changes.

To create, edit or remove a list of allowed addresses, use the following buttons:

-  – *Add*;
-  – *Edit*;
-  – *Remove*.

When the address list has been configured, click the *Apply* and *Commit* buttons; if you fail to confirm changes in 60 seconds, previous values will be restored. This allows user protection from loss of access to the device.

3.1.12.6 SMG firewall operation scheme

The next rule processing procedure is used on SMG for dynamic and static firewall, list of prohibited IP addresses, and access limitation from network interfaces:

1. Rule processing of dynamic firewall (see section 3.1.12.2) is performed. On this stage, requests received from IP addresses located on the blacklist will be dropped.
2. Processing of access limitations (see section 3.1.10.3 Network Interfaces -> Services and 3.1.12.5 List of Allowed IP Addresses). The rules allowing access to any IP addresses will be created for each service enabled on network interface. The access for other services will be blocked. If the allowed IP address list is activated, the access rules will be updated by control of source IP addresses (connection will be available only for IP address from the list). For each service that is allowed for working on the network interface, rules allowing to access from any IP address are created. Access to other services will be blocked. When the list of allowed IP addresses is activated, the access rules are supplemented with the control of the source IP address. Connection is allowed only from the addresses specified in the list.
3. Access to network interfaces that is not bound with rules of static firewall is allowed.
4. The static firewall rules (see 3.1.12.4) is being processed on the network interfaces to which they are bound.



If one of the rules from the list is processed, remaining rules will not be applied to a request.

3.1.12.7 Providing SMG firewall tasks

Restriction of WEB/Telnet/SSH/SNMP administration privileges.

To restrict the access to management, use 3.1.10.3 Network Interfaces -> Services and 3.1.12.5 List of Allowed IP Addresses. In the beginning, you should set protocol flags for network interfaces that have to be accessed. Thus, destination address restriction will be applied. After that, the allowed IP address list will be created. This list imposes additional restrictions for source IP addresses in accordance with allowed IP addresses.

To restrict the access to SIP/H.323 interfaces by specific addresses and/or geographic locations, configure a static firewall (see section 3.1.12.4).

The example of configuration with such restrictions shown below:

- Enable the access from Russia;
- Enable the access from subnet 34.192.128.128/28;
- Restrict the access from other addresses.

To do that, create tree rules for static firewall in the next order:

3. The rule for incoming traffic with GeoIP type and "Russian Federation (RU)" country. Action _ Accept.
4. The rule for outgoing traffic with "General" type and IP address/source mask: 34.92.128.128/255.255.255.240. Action – Accept.
5. The rule for incoming traffic with "General" type, packet source – "Any". Action – Drop.

After that, select the required network interfaces from the list and save settings.

Fully-restricted access to SMG from a specific address or subnet.

In order to implement access restriction to SMG from a certain address or subnet, it is necessary to activate the dynamic firewall (see Section 3.1.12.2) and enter address or subnet in the black list. Pay attention, if there are too many addresses, it is better to create static firewall rules (see Section 3.1.12.4) according the next principle: " first of all, allow connection to trusted nodes, and then drop all". Also, use settings for the access restriction by the list of allowed IP addresses (see Section 3.1.12.5).

Automatic blocking of failed requests/authorizations.

The dynamic firewall (see Section 3.1.12.2) automatically blocks failed requests/authorizations. To enable the automatic blocking, you should activate dynamic firewall and configure the trigger conditions. Also, it is recommended to add addresses and subnets that shouldn't fall under the rules of automatic blocking in the white list.

3.1.13 Network Utilities

3.1.13.1 PING

This utility is used to check device network connection (route presence).

PING

IP Probing

...

Periodic ping

Run at startup	<input type="checkbox"/>
Period, min	<input style="width: 80%;" type="text" value="10"/>
Attempts	<input style="width: 80%;" type="text" value="3"/>

Status

Periodical ping is not started!

IP-addresses list

Empty list

IP Probing – used for a single-time check of the device network connection.

To send a ping request (*the ICMP protocol is used*), enter the host IP address or network name in the *IP Probing* field and click the *Ping* button. The result of the command execution will be shown at the bottom of the page. The result contains information on the number of transmitted packets, the number of responses to the packets, the percent of lost packets, and the time of reception/transmission (minimum/average/maximum) in milliseconds.

PING

IP Probing

```

PING 192.168.27.7 (192.168.27.7): 56 data bytes
64 bytes from 192.168.27.7: seq=0 ttl=62 time=1.024 ms
64 bytes from 192.168.27.7: seq=1 ttl=62 time=0.899 ms
64 bytes from 192.168.27.7: seq=2 ttl=62 time=0.918 ms
64 bytes from 192.168.27.7: seq=3 ttl=62 time=0.892 ms
64 bytes from 192.168.27.7: seq=4 ttl=62 time=0.900 ms

--- 192.168.27.7 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.892/0.926/1.024 ms
          
```

Periodic ping – used for periodic check of device network connection.

- *Run at the device startup* – the option enables a periodic ping after restarting the device;
- *Period, minutes* – the time interval between requests in minutes.
- *Attempts count* – the number of attempts to send a request to an address.

State

- *Start* – starts/restarts periodic ping;
- *Stop* – forcedly stops periodic ping;

- *Information* – click this button to view the /tmp/log/hoststest.log log file which contains data on the last attempt of periodic ping request transmission.

Host list – a list of IP addresses to send periodic ping requests to.

To add a new address to the list, select it in the entry field and click the Add button. To remove an address, click the Remove button next to the required address.

3.1.13.2 TRACEROUTE

The TRACEROUTE utility performs the route tracing function and ping tests to monitor the network health. This function allows you to evaluate the connection quality for the tested node.

TRACEROUTE	
<input type="text"/>	Hostname or IP-address to check connection quality
Use options	Description and additional settings
<input type="checkbox"/>	<input type="text"/> Transmitted packets count (default 10)
<input type="checkbox"/>	<input type="text"/> Packet size to send
<input type="checkbox"/>	Show IP address instead of hostnames
<input type="checkbox"/>	<input type="text"/> Delay between ICMP requests (default 1 sec)
<input type="checkbox"/>	Use only IPv4
<input type="checkbox"/>	Use only IPv6
<input type="checkbox"/>	<input type="text"/> Network interface address for send ICMP request
<input type="button" value="Check"/>	

In the Host name/IP address to test connection quality field, enter the IP address of the network device to test the connection quality. To use the options, select the checkboxes in the corresponding line.

Options:

- *The number of transmitted packets* – the number of the ICMP request transfer cycles;
- *Size of packets to send* – the ICMP packet size in bytes;
- *Display IP addresses instead of host names* – do not use DNS. Display the IP address without trying to obtain their network names;
- *Latency between ICMP requests (1 sec by default)* – polling interval;
- *Use IPv4 only* – use only IPv4 protocol;
- *Use IPv6 only* – use only IPv6 protocol;
- *Network interface address to send ICMP requests* – IP address of the network interface from which ICMP requests will be sent.

After you have entered the IP address of the network device for which the connection quality is evaluated, and set the options, click the Check button.

As a result, the utility displays a table containing:

- the node number and its IP address (or network name)
- the percentage of packets lost (Loss%)
- the number of packets sent (Snt)

- the round-trip time of the last packet (Last)
- average round-trip time of the packet (Avg)
- the best round-trip time of the packet (Best)
- the worst time round-trip time of the packet (Wrst)
- the standard deviation of delays for each node (StDev)

HOST	smg2016	Loss%	Snt	Last	Avg	Best	Wrst	StDev
1.--	192.168.18.56	0.0%	10	0.1	0.1	0.1	0.2	0.0

3.1.14 RADIUS Configuration

3.1.14.1 RADIUS Servers

Servers

RADIUS-Authorization servers

	IP-address	Port	Secret-key
1	127.0.0.1	1812	dummy
2	0.0.0.0	0	
3	0.0.0.0	0	
4	0.0.0.0	0	
5	0.0.0.0	0	
6	0.0.0.0	0	
7	0.0.0.0	0	
8	0.0.0.0	0	

RADIUS-Accounting servers

	IP-address	Port	Secret-key
1	127.0.0.1	1813	dummy
2	0.0.0.0	0	
3	0.0.0.0	0	
4	0.0.0.0	0	
5	0.0.0.0	0	
6	0.0.0.0	0	
7	0.0.0.0	0	
8	0.0.0.0	0	

Server reply timeout (x100 ms)

Request sending attempts

Server inactivity timeout after failure (sec)

Network interface

WEB/telnet/ssh users authorization through RADIUS-authorization servers

Allow access when RADIUS-server failure

The device supports up to 8 authorisation servers and up to 8 accounting servers. You can group servers, And then when configuring RADIUS profiles you can select server group that will be used for sending requests. Four groups are available.

- *Server response timeout* – amount of time to wait for a server response.
- *Number of request transmission attempts* – the number of request retries to a server. When all attempts are used, the server will be deemed inactive and the request will be forwarded to another server if it is specified; otherwise, an error will be detected.
- *Server unavailability time during failure* – amount of time when a server is deemed unavailable (requests will not be sent to it).
- *Network interface* for <N> group – select the network interface for the RADIUS protocol;

-
- *Authorisation of WEB/telnet/ssh users via RADIUS-authorisation servers* – when the user logs on via WEB/telnet/ssh, authorisation will be performed on the RADIUS server. First, create local users with appropriate names and configure their access rights (see section 3.1.25 “Password Configuration for Web Configurator Access”);
 - *Permit access if RADIUS server fails* – if the authorisation of users on RADIUS is enabled and no response from the RADIUS server is received, then you can use a locally configured administrator account (admin) to log on.

3.1.14.2 Profile List

Profiles			
No	Name	Authorization	Accounting
0	RADIUS_Profile00	-	+

Profile Parameters

Profiles

RADIUS rule 1	
Name	<input type="text" value="RADIUS_Profile01"/>
Enable RADIUS-Authorization	<input type="checkbox"/>
Enable RADIUS-Accounting	<input type="checkbox"/>
Send SNMP trap	<input type="checkbox"/>
Modifiers settings	
Modifiers for InCdPN	<input type="text" value="not used"/>
InCdPN	<input type="text" value="original"/>
Modifiers for InCgPN	<input type="text" value="not used"/>
InCgPN	<input type="text" value="original"/>
Modifiers for OutCdPN	<input type="text" value="not used"/>
Modifiers for OutCgPN	<input type="text" value="not used"/>
RADIUS-Authorization settings	
Send requests for ingress calls	<input type="checkbox"/> on ingress seize (CgPN only) <input type="checkbox"/> on end-of-dial (CgPN and CdPN) <input type="checkbox"/> on local redirection
Send requests for egress calls	<input type="checkbox"/> on egress seize
Send requests by modifiers	<input type="text" value="Default"/>
Access restriction on server failure	<input type="text" value="no restrictions"/>
User-name field (originate)	<input type="text" value="CgPN"/>
User-name field (answer)	<input type="text" value="CdPN"/>
Redirecting Number	<input type="text" value="replace Calling-Station-Id"/>
User-password field	<input type="text"/>
Individual passwords for SIP-subscribers	<input type="checkbox"/>
DIGEST authorization	<input type="text" value="RFC4590"/>
Session timeout	<input type="text" value="Ignore"/>
Enable emergency call on receiving Reject	<input type="checkbox"/>
NAS-Port-Type	<input type="text" value="Async"/>
Service-Type	<input type="text" value="Not used"/>
Framed-protocol	<input type="text" value="Not used"/>
Class	<input type="text" value="Not used"/>

RADIUS-Accounting settings	
Send requests	<input checked="" type="checkbox"/> accounting-start <input checked="" type="checkbox"/> accounting-stop <input type="checkbox"/> accounting-stop for unsuccessfull calls <input type="checkbox"/> accounting-update with period <input type="text" value="2 minutes"/> <input checked="" type="checkbox"/> accounting for call-origin=originate <input type="checkbox"/> accounting for call-origin=answer
Send requests by modifiers	<input type="text" value="Default"/>
CISCO adaptation	<input type="checkbox"/>
Use UTC timezone	<input type="checkbox"/>
Round duration	<input type="text" value="upwards"/>
Access restriction on server failure	<input type="text" value="no restrictions"/>
User-name field (originate)	<input type="text" value="CgPN"/>
User-name field (answer)	<input type="text" value="CdPN"/>
Redirecting Number	<input type="text" value="replace Calling-Station-Id"/>
CdPN field	<input type="text" value="CdPN-in"/>
CgPN field	<input type="text" value="CgPN-in"/>
Accordance for RADIUS reply and voice messages	
Accordance table for RADIUS reply and voice messages	<input type="text" value="not used"/>
RADIUS reply attribute	<input type="text" value="Reply-Message"/>
VSA settings	
Enable VSA for call management	<input type="checkbox"/>
Full CISCO-VSA fields	<input type="checkbox"/>

- *Name* – profile name;

-
- *Enable RADIUS-Authorisation* – enable/disable the transmission of authentication/authorization (Access Request) messages to the RADIUS server;
 - *Enable RADIUS-Accounting* – enable/disable the transmission of accounting (Accounting Request) messages to the RADIUS server;
 - *Send reports via SNMP* – enable sending SNMP traps every time a RADIUS request is sent.
 - *Group* – group of RADIUS servers used for sending requests.

Modification Parameters:

- *InCdPN modifiers* – select callee (CdPN) number modifier for the incoming connection in relation to the Called-Station-Id, xpgk-dst-number-in fields of RADIUS-Authorisation and RADIUS-Accounting messages;
- *InCdPN number* – select the number to be sent to the xpgk-dst-number-in field in the RADIUS-Authorisation and RADIUS-Accounting messages:
 - *original* – the original number that was received in the CdPN field of the incoming call before its modification.
 - *processed* – CdPN number after its modification.
- *InCgPN modifiers* – select caller (CgPN) number modifier for the incoming connection in relation to the Calling-Station-Id, xpgk-src-number-in fields of RADIUS-Authorisation and RADIUS-Accounting messages;
- *InCgPN number* – select the number to be sent to the xpgk-dst-number-in field in the RADIUS-Authorisation and RADIUS-Accounting messages:
 - *original* – the original number that was received in the CgPN field of the incoming call before its modification;
 - *processed* – CgPN number after its modification.
- *OutCdPN modifiers* – select callee (CdPN) number modifier for the outgoing connection in relation to the xpgk-src-number-out field of RADIUS-Authorisation and RADIUS-Accounting messages.
- *OutCgPN modifiers* – select caller (CgPN) number modifier for the outgoing connection in relation to the xpgk-dst-number-out field of RADIUS-Authorisation and RADIUS-Accounting messages.

RADIUS-Authorisation Parameters:

Authentication/authorisation requests can be transmitted during various call phases:

- during incoming engagement;
- at the end of dial (full number dial reception);
- during local forwarding;
- during outgoing engagement.

You can restrict the call checking function in RADIUS based on the modifier mask. To do this, select one or more modifiers in the *Modification Parameters* section and set the *Send requests based on modifiers* option to *Restricted*. In this case, an authorisation request will be sent to RADIUS only if the number falls under one of the masks in the modifier tables. Modification will be performed as usual, according to the rules in the modifier table.



When you enable the authentication request restrictions based on the modifiers, the calls from numbers that are not included in the mask modifier will be automatically authorised.

In case of a server fault (no response from the server), the outgoing communications can be restricted:

- *no restrictions* – allow all calls;
- *local and zone networks only* – allow calls to special services, private, local and zone network;
- *local network only* – allow calls to special services, private and local network;
- *special services only* – allow calls to special services only;
- *deny all* – deny all calls.

This restriction governs call routing by a prefix controlling the corresponding call type (local, long-distance, etc.).

- *USER-NAME field* – select value of the User-Name attribute in the corresponding Access Request authorisation packet (RADIUS-Authorisation):
 - *CgPN* – use the caller phone number as the value;
 - *CdPN* – use the callee party phone number as the value;
 - *IP or E1-stream* – use the caller party IP address or incoming connection stream number as the value;
 - *Trunk name* – use incoming connection trunk name as the value.
- *Redirecting Number* – Redirection number processing options:
 - *Replace with Calling-station-ID* – in this case, the Redirection number is replaced in the Calling-station-ID field and transmitted as the caller number.
 - *Transmit to h323-redirection-number* – in this case, the Redirection number is transmitted in a separate “h323-redirection-number” field; the caller number remains unchanged.
- *USER-PASSWORD field* – specify the value of the User-Password attribute in the corresponding RADIUS-Authorisation packet.
- *Custom passwords for SIP subscribers* – when this option is checked, custom passwords of SIP subscribers are used for authentication/authorisation, instead of the password configured in the USER-PASSWORD field;
- *DIGEST authorisation* – select the subscriber authorisation algorithm with dynamic registration via the RADIUS server. When digest authentication is used, the password is not sent in a clear text, as in the basic authentication case, but as a hash code, and cannot be picked up during traffic scanning:
 - RFC4590 (full implementation of the RFC4590 recommendation);
 - RFC4590-no-challenge (operation with a server that does not transfer the Access Challenge field);
 - Draft-sterman (NetUp) (operation according to the draft standard, on the basis of which the RFC4590 recommendation was written);
- *Session time* – limits the maximum call duration:
 - *Ignore* – the maximum call duration is not limited;
 - *Use Session-Time* – use the Session-Timeout(27) value to limit the maximum call duration;

- *Use Cisco h323-credit-time* – use the Cisco VSA (9) h323-credit-time(102) value to limit the maximum call duration;
- *Session-Time priority* – if the server response has both parameters specified (session-time and Cisco h323-credit-time), session-time is used and Cisco h323-credit-time is ignored;
- *Cisco h323-credit-time priority* – if the server response has both parameters specified (session-time and Cisco h323-credit-time), Cisco h323-credit-time is used and session-time is ignored.



The SMG gateway can use the *Session-Timeout* or *Cisco VSA h323-credit-time* values from the Access-Accept packet in order to limit the maximum duration of an authorised call.

- *Allow access to special services when connection is rejected by the server* – if the Access-Reject code is received from the server, allow calls to the special service node.

Optional Attributes of Authentication-Request Packets

- *NAS-Port-Type* – NAS physical port type (a server for user authentication), the default value is Async;
- *Service-Type* – type of the service, not used by default (Not Used);
- *Framed-protocol* – the protocol specified for packet access utilisation, not used by default (Not Used);
- *Class* – process the AV-Pair Class field to change the category:
 - *Not used* – do not process the AV-Pair Class field;
 - *SS7 category* – use the received AV-Pair Class field value as the SS-7 category of the caller.

RADIUS-Accounting Parameters

Send Requests

- *accounting-start* – send an *accounting* start packet that notifies the RADIUS server about call start;
- *accounting-stop* – send an *accounting* stop packet that notifies the RADIUS server about call end;
- *accounting-stop for unsuccessful calls* – send information on unsuccessful calls to the RADIUS server;
- *accounting-update with period* – during a call, periodically send an *update* packet to the RADIUS server to notify the RADIUS server about active state of the call;
- *accounting for call-origin=originate* – send the RADIUS-Accounting messages for the incoming connection branch;
- *accounting for call-origin=answer* – send the RADIUS-Accounting messages for the outgoing connection branch.

Sending the billing information to RADIUS can be restricted based on the modifier mask. To do this, select one or more modifiers in the *Modification Parameters* section and set the *Send requests based on modifiers* option to *Restricted*. In this case, the billing information will be sent to RADIUS only if the number falls under one of the masks in the modifier tables. Modification will be performed as usual, according to the rules in the modifier table.



When you enable the request restrictions based on the modifiers, the billing information will not be sent for those calls whose numbers are not included in the mask modifier.

- *Cisco adaptation* – reverse the positions of the originate and answer sides in the accounting messages;
- *Pass time in UTC format* – send the time in the RADIUS-Accounting messages in UTC format;
- *Duration rounding* – select the time rounding method in the RADIUS-Accounting messages. Three options are available – round up, round down, and not to round (to transmit milliseconds).

In case of a server fault (no response from the server), the outgoing communications can be restricted:

- *no restrictions* – allow all calls;
- *local and zone networks only* – allow calls to special services, private, local and zone network;
- *local network only* – allow calls only to special services;
- *deny all* – deny all calls.

This restriction governs call routing by a prefix controlling the corresponding call type (local, long-distance, etc.).

- *USERNAME field* – select User-Name value in an Accounting Request packet (RADIUS-Accounting):
 - *CgPN* – use the caller phone number as the value;
 - *CdPN* – use the callee party phone number as the value;
 - *IP or E1-stream* – use the caller party IP address or incoming connection stream number as the value;
 - *Trunk name* – use incoming connection trunk name as the value.
- *Redirection Number* – transmission mode for RedirPN to RADIUS:
 - *replace the Calling-Station-Id* – RedirPN will be transmitted to the Calling-Station-Id field by rewriting an existing value;
 - *transmit to h323-redirect-number* – RedirPN will be sent separately into the h323-redirect-number field.
- *CdPN field* – select value of the callee number used for RADIUS packet generation for specific Attribute-Value pairs (see section 3.1.14.5):
 - *CdPN-in* – use the callee number prior to modification (the number received in the SETUP/INVITE request);
 - *CdPN-out* – use the callee number after modification.
- *CgPN field* – select value of the caller number to be used for RADIUS packet generation for certain Attribute-Value pairs (see section 3.1.14.5):
 - *CgPN-in* – use the caller number prior to modification (the number received in the SETUP/INVITE request);
 - *CgPN-out* – use the caller number after modification.

Correspondence between RADIUS Responses and Voice Messages

When a Reject message is received from the RADIUS server, the gateway can send a standard voice message in order to inform the subscriber about the connection failure cause. The voice messages are sent based on the analysis of the replay-Message field or the h-323-return-code of the Reject message.

- *RADIUS responses to voice messages correspondence table* – select a table of correspondence between RADIUS-reject responses and voice messages;

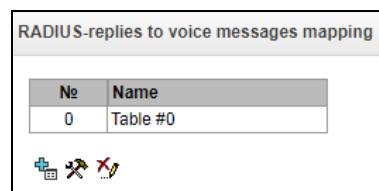
- *RADIUS response attribute* – select an attribute that will be used for the analysis of a RADIUS-reject message.

Eltex-VSA parameters

- *Use Eltex-VSA for call management* – enable the Radius call management service (if you have the RCM license). For the description of the Radius call management service, see Appendix K.
- *Use complete CISCO-VSA value* – transmit full attribute names in the CISCO-VSA fields.

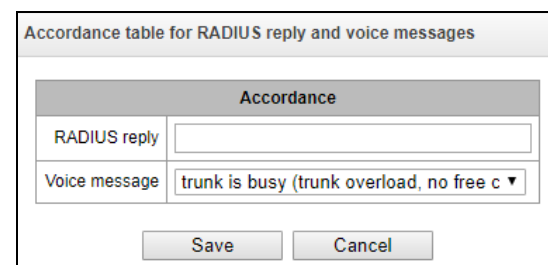
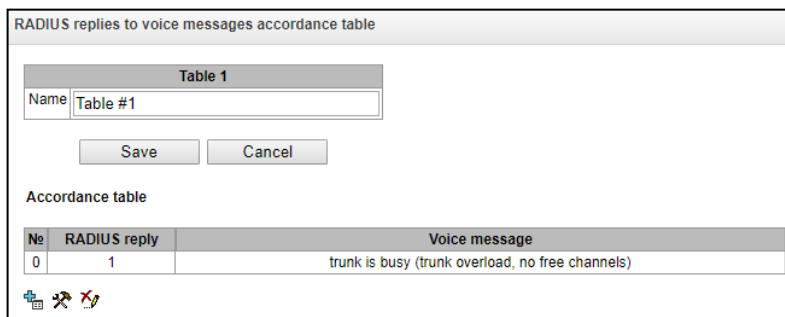
3.1.14.3 Tables of Correspondence between RADIUS Responses and Voice Messages.

In this section, you can configure the correspondence between RADIUS-reject responses and voice messages sent to subscribers.



To create, edit, or remove a table, use the *Objects – Add Object*, *Objects – Edit Object*, or *Objects – Remove Object* menus and the following buttons:

- Add table;
- Edit table;
- Remove table.



- *RADIUS response* – the replay-Message field value or the h-323-return-code value of the Reject message from the RADIUS server;
- *Voice message* – select the voice message to be sent to the subscriber.

3.1.14.4 RADIUS Packet Format

Each packet description includes descriptions of every Attribute-Value pair for this packet type. Attributes may be either standard or vendor specific. If the attribute value is unknown for any reason (e. g. if the outgoing trunk is missing, it is impossible to identify the CdPN_OUT variable value, which is used as a value for some attributes), then the attribute is not included into the message.

Standard attributes have the following description:

Attribute name (attribute number): attribute value

Vendor attributes:

Attribute name (attribute number): vendor name (vendor number): VSA name (VSA number): VSA value

where:

- **Attribute name** – always Vendor-Specific;
- **Attribute number** – always 26;
- **Vendor name** – name of the vendor;
- **Vendor number** – the vendor number assigned by IANA in the PRIVATE ENTERPRISE NUMBERS document (<http://www.iana.org/assignments/enterprise-numbers>);
- **VSA name** – vendor attribute name;
- **VSA value** – vendor attribute value.



<\$NAME> can be used as an attribute value, where NAME is a variable name. For description of variable values, see section 3.1.14.5 Variable Description.

Access-Request Packet

User-Name(1): <\$USER_NAME>
 User-Password(2): is built based on the "eltex" password (without quotes)
 NAS-IP-Address(4): <\$SMG_IP>
 Called-Station-Id(30): <\$CdPN_IN>
 Calling-Station-Id(31): <\$CgPN_IN>
 Acct-Session-Id(44): <\$SESSION_ID>
 NAS-Port(5): <\$NAS_PORT>
 NAS-Port-Type(61): Virtual(5)
 Service-Type(6): Call-Check(10)
 Framed-IP-Address: <\$USER_IP>

Accounting-Request Start Packet

Acct-Status-Type(40) – Start(1)
 User-Name(1): <\$USER_NAME>
 Called-Station-Id(30): <\$CdPN>
 Calling-Station-Id(31): <\$CgPN_IN>
 Acct-Delay-Time(41): according to RFC2866
 Event-Timestamp(55): according to RFC2869
 NAS-IP-Address(4): <\$SMG_IP>
 Acct-Session-Id(44): <\$SESSION_ID>
 Framed-IP-Address: <\$USER_IP>
 Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-src-number-in=<\$CgPN_IN>
 Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-src-number-out=<\$CgPN_OUT>
 Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-dst-number-in=<\$CdPN_IN>
 Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-dst-number-out=<\$CdPN_OUT>
 Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-route-retries=<\$ROUTE_RETRIES>
 Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): h323-remote-id=<\$DST_ID>
 Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): h323-call-id=<\$CALL_ID>
 Vendor-Specific(26): Cisco(9): h323-remote-address(23): h323-remote-address=<\$DST_IP>
 Vendor-Specific(26): Cisco(9): h323-conf-id(24): h323-conf-id=<\$CALL_ID>
 Vendor-Specific(26): Cisco(9): h323-setup-time(25): h323-setup-time=<\$TIME_SETUP>
 Vendor-Specific(26): Cisco(9): h323-call-origin(26): h323-call-origin=originate
 Vendor-Specific(26): Cisco(9): h323-call-type(27): h323-call-type=<\$CALL_TYPE>
 Vendor-Specific(26): Cisco(9): h323-connect-time(28): h323-connect-time=<\$TIME_CONNECT>
 Vendor-Specific(26): Cisco(9): h323-gw-id(33): h323-gw-id=<\$SMG_IP>

Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Incoming-SIP-call-id(2):
 <\$inc_SIP_call_ID>
 Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Outgoing-SIP-call-id(3):
 <\$out_SIP_call_ID>
 Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Incoming-RTP-local-
 address(4): <\$inc_RTP_loc_IP>
 Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Incoming-RTP-remote-
 address(5): <\$inc_RTP_rem_IP>
 Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Outgoing-RTP-local-
 address(6): <\$out_RTP_loc_IP>
 Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Outgoing-RTP-remote-
 address(7): <\$out_RTP_rem_IP>
 Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): call-record-
 file=<\$call_record_file_name>

Accounting-Request Stop Packet

Acct-Status-Type(40) - Stop(2)
 User-Name(1): <\$USER_NAME>
 Called-Station-Id(30): <\$CdPN>
 Calling-Station-Id(31): <\$CgPN_IN>
 Acct-Delay-Time(41): according to RFC2866
 Event-Timestamp(55): according to RFC2869
 NAS-IP-Address(4): <\$SMG_IP>
 Acct-Session-Id(44): <\$SESSION_ID>
 Acct-Session-Time(46): <\$SESSION_TIME>
 Framed-IP-Address: <\$USER_IP>
 Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-src-number-in=<\$CgPN_IN>
 Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-src-number-out=<\$CgPN_OUT>
 Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-dst-number-in=<\$CdPN_IN>
 Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-dst-number-out=<\$CdPN_OUT>
 Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-route-
 retries=<\$ROUTE_RETRIES>
 Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): h323-remote-id=<\$DST_ID>
 Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): h323-call-id=<\$CALL_ID>
 Vendor-Specific(26): Cisco(9): Cisco-AVPair(30): h323-disconnect-
 cause=<\$DISCONNECT_CAUSE>
 Vendor-Specific(26): Cisco(9): Cisco-AVPair(1): xpgk-local-disconnect-
 cause=<\$LOCAL_DISCONNECT_CAUSE>
 Vendor-Specific(26): Cisco(9): h323-remote-address(23): h323-remote-
 address=<\$DST_IP>
 Vendor-Specific(26): Cisco(9): h323-conf-id(24): h323-conf-id=<\$CALL_ID>
 Vendor-Specific(26): Cisco(9): h323-setup-time(25): h323-setup-time=<\$TIME_SETUP>
 Vendor-Specific(26): Cisco(9): h323-call-origin(26): h323-call-origin=originate
 Vendor-Specific(26): Cisco(9): h323-call-type(27): h323-call-type=<\$CALL_TYPE>
 Vendor-Specific(26): Cisco(9): h323-connect-time(28): h323-connect-
 time=<\$TIME_CONNECT>
 Vendor-Specific(26): Cisco(9): h323-disconnect-time(29): h323-disconnect-
 time=<\$TIME_DISCONNECT>
 Vendor-Specific(26): Cisco(9): h323-gw-id(33): h323-gw-id=<\$SMG_IP>
 Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Incoming-SIP-call-id(2):
 <\$inc_SIP_call_ID>
 Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Outgoing-SIP-call-id(3):
 <\$out_SIP_call_ID>
 Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Incoming-RTP-local-
 address(4): <\$inc_RTP_loc_IP>
 Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Incoming-RTP-remote-
 address(5): <\$inc_RTP_rem_IP>
 Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Outgoing-RTP-local-
 address(6): <\$out_RTP_loc_IP>
 Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): Outgoing-RTP-remote-
 address(7): <\$out_RTP_rem_IP>
 Vendor-Specific(26): Eltex Enterprise, Ltd.(35265): call-record-
 file=<\$call_record_file_name>

Access-Accept Packet

When an Access-Accept packet is received from the RADIUS server, the call is considered as authorised. Then, a search for an outgoing trunk is performed and, if successful, an attempt to establish the connection is made.

If the *Session-Time(27)* attribute or the *Cisco VSA (9) h323-credit-time(102)* attribute has been transferred in a packet and the corresponding setting is specified in the RADIUS profile, the attribute value is used to limit the maximum call duration. When this timeout expires, SMG will terminate the connection.

3.1.14.5 Variable Description

Table 15 – Variable Description

Variable	Description and Possible Values
\$CALL_TYPE	Is defined depending on the transmission medium to which the outgoing trunk belongs: <ul style="list-style-type: none"> • <i>Telephony</i>, if the outgoing trunk is PSTN (TDM); • <i>VoIP</i>, if the outgoing trunk is VoIP.
\$CdPN	Is defined based on SMG settings: <ul style="list-style-type: none"> • \$CdPN = \$CdPN_IN [by default]; • \$CdPN = \$CdPN_OUT
\$CdPN_IN	Callee number before modification (received in SETUP/INVITE)
\$CdPN_OUT	Caller number after modification (sent to the called party in SETUP/INVITE)
\$CgPN_IN	Caller number before modification (received in SETUP/INVITE)
\$CgPN_OUT	Caller number after modification (sent to the called party in SETUP/INVITE)
\$DISCONNECT_CAUSE	Q.850 cause for call clearing
\$DST_ID	Outgoing trunk name for this call
\$DST_IP (string)	IP address of the terminating device if the outgoing trunk is VoIP, e. g.: 192.168.0.1
\$USER_IP	IP address of the device that initiated the call, if the incoming call is from VoIP trunk or SIP subscriber
\$LOCAL_DISCONNECT_CAUSE	A local reason for call clearing; values: <ul style="list-style-type: none"> • 1 – connection to the callee has been established (User-Answer); • 2 – wrong or incomplete number format (Incomplete-Number); • 3 – the number does not exist (Unassigned-Number); • 4 – unsuccessful connection attempt, unknown reason (Unsuccessful-Other-Cause); • 5 – the callee is busy (User-Busy); • 6 – equipment fault (Out-of-Order); • 7 – no response from the callee (No-Answer); • 8 – outgoing trunk is unavailable (Unavailable-Trunk); • 9 – RADIUS server authorisation denied (Access-Denied); • 10 – no free channels for connection establishment (Unavailable-Voice-Channel); • 11 – RADIUS server is unavailable (RADIUS-Server-Unavailable).
\$NAS_PORT	(xport.type<<24) + (xport.slot<<16) + (xport.stream<<8) + (xport.cell)

\$ROUTE_RETRIES	The current number of the attempt, the count begins with 1 (for the first attempt, respectively)
\$SESSION_ID	Session identifier
\$SESSION_TIME	Call duration
\$SMG_IP	SMG IP address
\$SRC_ID	Incoming trunk name for this call
\$TIME_SETUP	The time of SETUP/INVITE message arrival in the hh:mm:ss.uuu t www MMM dd yyyy format
\$TIME_CONNECT	The reception time of the CONNECT/200 OK message issued by the callee in the hh:mm:ss.uuu t www MMM dd yyyy format
\$TIME_DISCONNECT	The reception time of the DISCONNECT/BYE message issued by one of the parties in the hh:mm:ss.uuu t www MMM dd yyyy format; if the call is unsuccessful, the time of the message is specified upon reception of which SMG begins the call termination procedure (CANCEL, other)
\$USER_NAME	Determined from incoming trunk settings: <ul style="list-style-type: none"> • <\$CgPN_IN>; • source IP address or E1 stream number [by default]; • incoming trunk name.
<\$inc_SIP_call_ID>	Call-ID field value of SIP messages for the incoming connection branch.
<\$out_SIP_call_ID>	Call-ID field value of SIP messages for the outgoing connection branch.
<\$inc_RTP_loc_IP>	Local IP address of the device to establish the RTP session for the incoming connection branch.
<\$inc_RTP_rem_IP>	Remote IP address of the communicating device to establish the RTP session for the incoming connection branch.
<\$out_RTP_loc_IP>	Local IP address of the device to establish the RTP session for the outgoing connection branch.
<\$out_RTP_rem_IP>	Remote IP address of the communicating device to establish the RTP session for the outgoing connection branch.
<\$call_record_file_name>	Name of the conversation record file. Example: call_records/2016-12-13-0000/2016-12-13_12-41-45_20000-10000.wav

3.1.15 Tracing

3.1.15.1 PCAP Tracings

This menu allows configuration of network traffic analysis and the TDM protocol.

PCAP traces

TCP-dump

Interface: **eth0**

Capture length limit (0 - no limit): **0**

Add filter:

Start **Stop** **Restart**

Available 7.121 GB from 7.123 GB

Files and folders			
	app_log_20180110_074339.log	2.6 kB	10.01.2018 12:29
	app_log_20180112_093654.log	2.8 kB	15.01.2018 06:35
	app_log_20180115_063843.log	1.8 kB	15.01.2018 06:39
	app_log_20180124_155102.log	1.8 kB	25.01.2018 09:15
	app_log_20180125_091605.log	1.8 kB	25.01.2018 09:20
	app_log_20180125_092055.log	1.5 kB	25.01.2018 09:21
	app_log_20180125_092944.log	1.7 kB	25.01.2018 09:40
	cdr.log	1.4 kB	25.01.2018 09:29
	chronica.1	0 B	10.01.2018 07:43
	chronica.idx	18 B	25.01.2018 09:29
	chronica.siz	13 B	25.01.2018 09:29
	dmesg	16.6 kB	24.05.2018 02:07
	hoststest.log	90 B	31.05.2018 15:01
	pbx_ivr.log	26.8 kB	10.01.2018 08:10
	pbx_pstn.log	28.7 kB	10.01.2018 11:32
	pbx_sip.log	27.4 kB	10.01.2018 08:10
	pbx_sip_bun.log	363.3 kB	15.01.2018 08:35
	pbx_siperr.log	722 B	10.01.2018 08:10
	pbx_siptrace.log	293 B	10.01.2018 08:10
	sntp.log	336 B	31.05.2018 14:42
	ssh_log0	0 B	10.01.2018 07:43
	ssh_log3	0 B	10.01.2018 07:43
	sshd_log	2.3 kB	31.05.2018 14:42
	sysmon.1.log	8.0 kB	24.05.2018 02:04
	sysmon.2.log	9.8 kB	24.05.2018 08:16
	sysmon.3.log	331 B	25.01.2018 09:20
	sysmon.4.log	331 B	25.01.2018 09:29
	uauthlog	0 B	10.01.2018 07:43

Download **Delete**

TCPdump – settings of the TCP-dump utility:

TCPdump is a utility designed to pick up and analyse network traffic.

- *Interface* – an interface for network traffic pickup;
- *Packet length limit* – size limit for picked-up packets, bytes;
- *Add filter* – packet filter for the *tcpdump* utility.

Structure of Filter Expressions

Every expression defining a filter includes a single or multiple primitives, which contain a single or multiple object identifiers and preceding qualifiers. An object identifier may be represented by its name or number.

Object Qualifiers:

1. **type** – indicates the object type specified by the identifier. An object type may have the following values:
 - host**,
 - net**,
 - port**.If an object type is not defined, the **host** value is assumed.
2. **dir** – defines the direction towards the object. This may have the following values:
 - src** (object is a source),
 - dst** (object is a destination),
 - src or dst** (source or destination),
 - src and dst** (source and destination).If the dir qualifier is not defined, the **src or dst** value is assumed.
To pick up traffic from the **any** artificial interface, the **inbound** and **outbound** qualifiers can be used.
3. **proto** – defines the protocol to which the packets should belong. This qualifier may have the following values:
 - ether**, **fdi1**, **tr2**, **wlan3**, **ip**, **ip6**, **arp**, **rarp**, **decnet**, **tcp**, and **udp**.If a primitive does not contain a protocol qualifier, it is assumed that all protocols compatible with the object type comply with this filter.

In addition to objects and qualifiers, primitives may contain arithmetic expressions and keywords:

- **gateway**,
- **broadcast**,
- **less**,
- **greater**.

Complex filters may contain a set of primitives connected with logical operators **and**, **or**, and **not**. To reduce the expressions which define filters, lists of identical qualifiers may be omitted.

Filter Examples

- **dst foo** – filters the packets which IPv4/v6 recipient address field contains address of the foo host.
- **src net 128.3.0.0/16** – filters all Ipv4/v6 packets sent from the specified network;
- **ether broadcast** – ensures filtering of all Ethernet broadcasting frames. The *ether* keyword may be omitted;
- **ip6 multicast** – filters packets with IPv6 group addresses.

For detailed information on packet filtering, see specialised resources.

- *Launch* – begin data collection;
- *Finish* – finish data collection;
- *Restart* – restart the utility and begin data collection again.

The **Tracing Directory Files and Folders** block contains a list of tracing files.

To download it to a local PC, check the checkboxes located next to the required filenames and click the *Download* button. To delete the specified files from the directory, click *Delete*.

3.1.15.2 PBX Tracing



Utilisation of PBX SIP tracing leads to delays in device operation. This debug mode is RECOMMENDED only if problems in gateway operation occur and their reason should be identified.

PBX traces

PBX PSTN

PBX PSTN trace is finished!
[Download pbx_pstn.log](#)

Trace level

alarms

calls

FXS

SIP

RTP-connections

RADIUS

IVR

[Start](#) [Stop](#) [Restart](#)

Available 7.121 GB from 7.123 GB

Files and folders			
<input type="checkbox"/>	app_log_20180110_074339.log	2.6 kB	10.01.2018 12:29
<input type="checkbox"/>	app_log_20180112_093654.log	2.8 kB	15.01.2018 06:35
<input type="checkbox"/>	app_log_20180115_063843.log	1.8 kB	15.01.2018 06:39
<input type="checkbox"/>	app_log_20180124_155102.log	1.8 kB	25.01.2018 09:15
<input type="checkbox"/>	app_log_20180125_091605.log	1.8 kB	25.01.2018 09:20
<input type="checkbox"/>	app_log_20180125_092055.log	1.5 kB	25.01.2018 09:21
<input type="checkbox"/>	app_log_20180125_092944.log	1.7 kB	25.01.2018 09:40
<input type="checkbox"/>	cdr.log	1.4 kB	25.01.2018 09:29
<input type="checkbox"/>	chronica.1	0 B	10.01.2018 07:43
<input type="checkbox"/>	chronica.idx	18 B	25.01.2018 09:29
<input type="checkbox"/>	chronica.siz	13 B	25.01.2018 09:29
<input type="checkbox"/>	dmesg	16.6 kB	24.05.2018 02:07
<input type="checkbox"/>	hoststest.log	90 B	31.05.2018 15:01
<input type="checkbox"/>	sip_info_20180524_081524_wrk.log	20 B	24.05.2018 02:15
<input type="checkbox"/>	sip_info_20180524_141648_disp.log	0 B	24.05.2018 08:16
<input type="checkbox"/>	sip_info_20180524_141648_mngr.log	0 B	24.05.2018 08:16
<input type="checkbox"/>	sip_info_20180524_141648_wrk.log	20 B	24.05.2018 08:16
<input type="checkbox"/>	snmpd	968 B	24.05.2018 02:08
<input type="checkbox"/>	sntp.log	336 B	31.05.2018 14:42
<input type="checkbox"/>	ssh_log0	0 B	10.01.2018 07:43
<input type="checkbox"/>	ssh_log3	0 B	10.01.2018 07:43
<input type="checkbox"/>	sshd_log	2.3 kB	31.05.2018 14:42
<input type="checkbox"/>	sysmon.1.log	8.0 kB	24.05.2018 02:04
<input type="checkbox"/>	sysmon.2.log	9.8 kB	24.05.2018 08:16
<input type="checkbox"/>	sysmon.3.log	331 B	25.01.2018 09:20
<input type="checkbox"/>	sysmon.4.log	331 B	25.01.2018 09:29
<input type="checkbox"/>	uauthlog	0 B	10.01.2018 07:43

[Download](#) [Delete](#)

The **PBX PSTN** block registers operations and interaction in a log, as well as message exchange via various protocols. PBX PSTN parameters allow configuration of tracing levels for various events and protocols.

To collect data, you need to set a non-zero tracing level for protocols and subsystems required, and then click 'Start' button.

To stop data collecting, click 'Stop' button.

Also, when data collecting, you may change settings and restart data selection by clicking 'Restart' button.

The **PBX SIP** block registers SIP errors and messages tracing:

- *Launch* – begin data collection;
- *Finish* – finish data collection;
- *Restart* – restart tracing and begin data collection again.

The **PBX H323** block is used to deactivate tracing of H.323 errors and messages¹.

- *Launch* – begin data collection;
- *Finish* – finish data collection;
- *Restart* – restart and begin data collection again.



When data collection is stopped, buttons are displayed; they allow tracing files to be downloaded to a local PC.

In the **Tracing Directory Files and Folders** block, you can download a set of recorded tracing files.

To download it to a local PC, check the checkboxes located next to the required filenames and click the *Download* button. To delete the specified files from the directory, click *Delete*.

¹ Not supported in the current firmware version 3.11.0

'By Trunk Group' tab

The screenshot shows the 'PBX traces' configuration in the 'By TrunkGroup' tab. The 'PBX PSTN' section has the following settings:

- Trace level: alarms calls SS7-ISUP SIP Q.931
- RTP-connections:
- SM-VP commands:
- RADIUS:
- IVR:

The 'PBX SIP' section has the following settings:

-

The 'Files and folders' table shows the following files:

File name	Size	Created	Actions
app_log_20180601_072532.log	3.4 kB	01.06.2018 07:26	<input type="checkbox"/>
app_log_20180601_072629.log	3.1 kB	01.06.2018 07:27	<input type="checkbox"/>
app_log_20180601_072721.log	3.1 kB	01.06.2018 07:28	<input type="checkbox"/>
app_log_20190129_102515.log	2.3 kB	29.01.2019 10:25	<input type="checkbox"/>
chronica.1	0 B	29.01.2019 10:25	<input type="checkbox"/>
chronica.idx	18 B	29.01.2019 10:25	<input type="checkbox"/>
chronica.siz	13 B	29.01.2019 10:25	<input type="checkbox"/>
hosttest.log	91 B	29.01.2019 10:25	<input type="checkbox"/>
lastlog	296 B	31.01.2019 10:55	<input type="checkbox"/>
messages	0 B	29.01.2019 10:25	<input type="checkbox"/>
networkd.1.log	38.7 kB	08.02.2019 17:31	<input type="checkbox"/>
pa_h323.1.log	877 B	29.01.2019 10:25	<input type="checkbox"/>
pbx_sip_bun.log	0 B	29.01.2019 10:25	<input type="checkbox"/>
smg_logs_dump.tar.gz	2.3 kB	29.01.2019 10:25	<input type="checkbox"/>
snmpd	968 B	29.01.2019 10:25	<input type="checkbox"/>
ssh_log0	0 B	29.01.2019 10:25	<input type="checkbox"/>
ssh_log3	0 B	29.01.2019 10:25	<input type="checkbox"/>
sshd_log	263 B	31.01.2019 10:55	<input type="checkbox"/>
sysmon.1.log	381 B	29.01.2019 10:25	<input type="checkbox"/>
uauthlog	0 B	26.01.1970 03:55	<input type="checkbox"/>

Use the menu to start PBX PSTN log collecting on selected trunk group. Tracing levels works similar with PBX PSTN tracing levels (see 'Common settings' tab) and differ only by the fact that all protocols have the same specified logging level.

To start data collecting, it is necessary to set nonezero tracing level for required trunk groups, and then click 'Start' button.

To stop data collecting, click 'Stop' button.

Also, when tracing, you can change the settings and restart data collecting by clicking 'Restart' button.

'By phone number' tab

The screenshot shows the 'PBX traces' configuration window in the ELTEX Signaling & Media Gateway Configurator. The 'By telephone number' tab is selected. The interface includes a 'Trace level' input field set to 0, a 'Numbers list' with an 'Add' button, and 'Start', 'Stop', and 'Restart' buttons. On the right, a table lists files and folders with columns for file name, size, and date. The table is as follows:

Files and folders			
app_log_20180601_072532.log	3.4 kB	01.06.2018 07:26	<input type="checkbox"/>
app_log_20180601_072629.log	3.1 kB	01.06.2018 07:27	<input type="checkbox"/>
app_log_20180601_072721.log	3.1 kB	01.06.2018 07:28	<input type="checkbox"/>
app_log_20190129_102515.log	2.3 kB	29.01.2019 10:25	<input type="checkbox"/>
chronica.1	0 B	29.01.2019 10:25	<input type="checkbox"/>
chronica.idx	18 B	29.01.2019 10:25	<input type="checkbox"/>
chronica.siz	13 B	29.01.2019 10:25	<input type="checkbox"/>
hoststest.log	91 B	29.01.2019 10:25	<input type="checkbox"/>
lastlog	296 B	31.01.2019 10:55	<input type="checkbox"/>
messages	0 B	29.01.2019 10:25	<input type="checkbox"/>
networkd.1.log	38.7 kB	08.02.2019 17:31	<input type="checkbox"/>
pa_h323.1.log	877 B	29.01.2019 10:25	<input type="checkbox"/>
pbx_sip_bun.log	0 B	29.01.2019 10:25	<input type="checkbox"/>
smg_logs_dump.tar.gz	2.3 kB	29.01.2019 10:25	<input type="checkbox"/>
snmpd	968 B	29.01.2019 10:25	<input type="checkbox"/>
ssh_log0	0 B	29.01.2019 10:25	<input type="checkbox"/>
ssh_log3	0 B	29.01.2019 10:25	<input type="checkbox"/>
sshd_log	263 B	31.01.2019 10:55	<input type="checkbox"/>
sysmon.1.log	381 B	29.01.2019 10:25	<input type="checkbox"/>
uauthlog	0 B	26.01.1970 03:55	<input type="checkbox"/>

At the bottom of the table are 'Download' and 'Delete' buttons. The left sidebar shows a tree view of system sections, with 'PBX traces' selected under the 'Traces' category.

Use the menu to start PBX PSTN log collecting on selected phone number. Collection is performed by CdPN as well as CgPN. Tracing levels work similar with PBX PSTN tracing levels (see 'Common settings' tab) and differ only by the fact that all protocols have the same specified logging level.

To start data collecting, add phone number in the phone number list, set tracing level, and then click 'Start' button.

To stop data collecting, click 'Stop' button. Also, when tracing, you can change the settings and restart data collecting by clicking 'Restart' button.

3.1.15.3 Syslog Settings

The **SYSLOG** menu allows configuration of system log settings.

SYSLOG is a protocol designed for the transmission of messages on current system events. The gateway firmware generates system data logs on operation of system applications and signalling protocols, as well as occurred failures, and sends them to the SYSLOG server.



**High debug levels may cause delays in device operation.
IT IS NOT RECOMMENDED to use the system log without a due reason.**



The system log should be used only when problems in gateway operation occur and their reason should be identified. To determine the necessary debug levels, please contact ELTEX Service Centre.

Tracings are used to save the operation and interaction log for the device components, as well as to exchange messages through various protocols.

Tracing parameters allow you to configure tracing levels for various events and protocols. Possible levels are as follows: 0 – disabled, 1–99 – enabled; 1 – minimum debug level, 99 – maximum debug level.

- *Server IP address* – the server address to which the tracing will be sent;
- *Server port* – the server port to which the tracing will be sent;

Output the history of entered commands – save the history of changes in gateway settings.

- *Server IP address* – the server address to which the entered commands log will be sent;
- *Server port* – the server port to which the entered commands log will be sent;
- *Verbosity level* – verbosity level of the entered commands log:
 - *Disable logs* – disable the generation of the entered commands log.
 - *Standard* – messages contain the name of the modified parameter;
 - *Full* – messages contain the name of the modified parameter as well as parameter values before and after modification.

System log configuration – configuration settings for the system log that records the device access events.


- *Enable logging* – when this option is checked, the device access events history is saved; when unchecked, logging is disabled;
- *Send to server* – when this option is checked, the system log is stored on a server at the specified address;
- *Server IP address* – address of the server where the system log is stored;
- *Server port* – the server port to which the system log will be sent.

3.1.16 Conversation Recording


Conversation recording settings menu¹.

3.1.16.1 Recording Parameters

Call recording settings

Common record settings	
Local disk drive for call records	off ▼
Directory name for call records	call_records
Directory name for IVR call records	ivr_records
Number of files per directory 	200
Keep files for: Days	30 ▼
Hours	0 ▼
Action when disk is full	Stop recording ▼
FTP server settings	
Store files on FTP	<input type="checkbox"/>
Upload mode	once per day ▼
Hours	0 ▼
Minutes	0 ▼
Server address/hostname	
Server port	21
Path on server	
Login	
Password	*****
Remove files after upload	<input type="checkbox"/>

Apply

No	Mask	Type	Dial plan	Call record category
				

General Recording Parameters:

- *Path to call recording drive* – select the available drive for saving conversation records;
- *Folder name for conversation records* – the name of directory for saving conversation records; if the folder name is not specified, conversation records will be saved to the root directory of the drive;
- *Folder name for IVR conversation records* – the name of directory name for saving conversation records when a call comes to the REC block in the IVR script;
- *Number of files per directory* – the maximum number of conversation record files in a single directory; if the maximum number of files is reached, a new directory will be created;

In the conversation record directory, a new subdirectory is created for each day of recording under the following name:

¹ The menu is available only in a firmware version with the Call-record license. For more information about the licenses, see section **3.1.222 Licenses**

YYYY-MM-DD-NNNN,

where:

- **YYYY** – 4 characters – the current year;
- **MM** – 2 characters – the current month;
- **DD** – 2 characters – the current date;
- **NNNN** – 4 characters – number of a directory containing conversation records for the current date.

If the *Number of files per directory* value is reached, the device will create a new directory with the value **####** increased by one.

Example of directories created on 2014-02-27:

2014-02-27-0000

2014-02-27-0001

2014-02-27-0002

2014-02-27-0003



- *Data storage time (days/hours)* – the time period during which conversation record files will be stored on the drive; after this time period expires, old files will be deleted.
- *Action for a full drive* – select an action to be applied to conversation record files when the drive is full:
 - *Stop recording* – stop recording new conversations when the drive is full.
 - *Delete old records* – delete old conversation records when the drive is full.

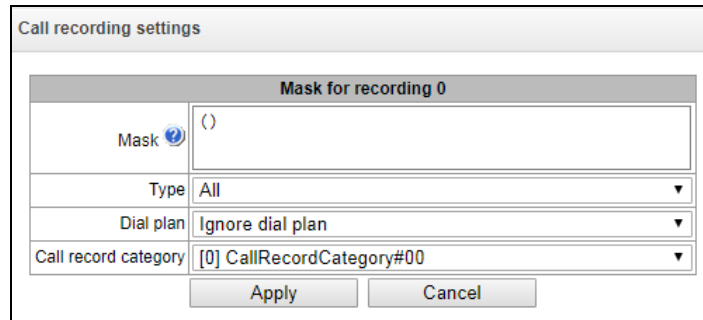
FTP Server Settings:

- *Save to FTP* – when this option is checked, conversation records will automatically be uploaded to the FTP server, according to the selected upload mode;
- *Uploading mode* – determines how often the records will be uploaded to FTP:
 - once a day – uploading once a day at a given time;
 - once an hour – uploading every hour;
 - once a minute – uploading every minute.
- *Hours* – available in the *once a day* uploading mode. Here you can specify the hour for uploading;
- *Minutes* – available in the *once a day* and *once an hour* uploading modes. Here you can specify the minutes for uploading;
- *FTP server* – the IP address or domain name of the FTP server to which conversation records will be uploaded;
- *FTP port* – the FTP server port
- *File path* – the path for saving files on the FTP server;
- *Login for FTP* – login for authorisation;

- *Password for FTP* – password for authorisation;
- *Delete files after uploading* – if this option is checked, record files will be deleted from the local SMG storage after uploading.

Filter Masks for Conversation Records:

Click the *Create*  button to create a new recording mask or click the *Edit*  button to edit the existing one.



The device determines whether a conversation should be recorded for CgPN and CdPN numbers.

- *Mask* – the number filter mask. For mask syntax, see section 3.1.6.2 Description of Number Mask and Its Syntax;
- *Type* – search for a mask match by CdPN or CgPN number;

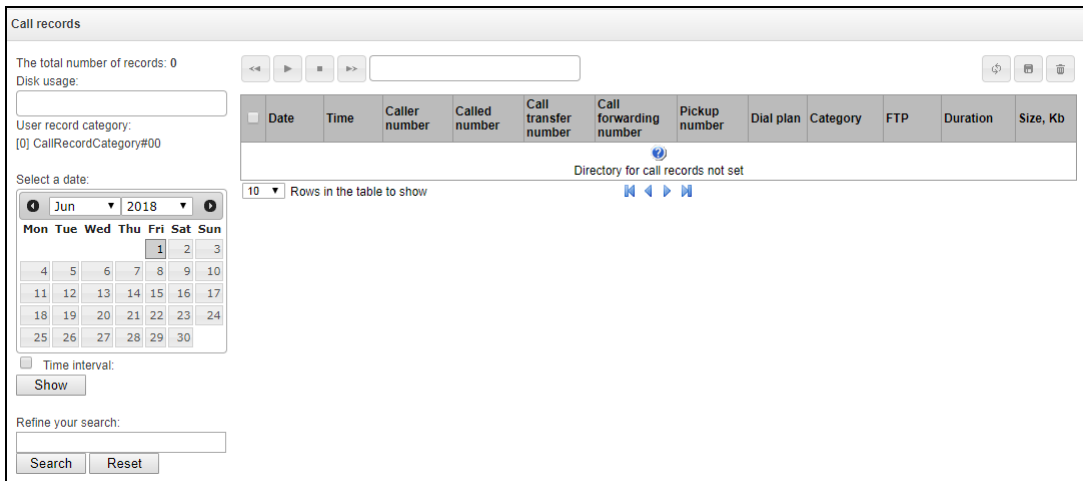


Please note that this setting uses OR logic is used in the setting, i. e. either CgPN or CdPN match is sufficient for the record identification.

- *All* – search by CgPN and CdPN numbers;
- *Calling* – search only by CgPN number;
- *Called* – search only by CdPN number.
- *Numbering schedule* – specify the numbering schedule in which the call recording mask will work. If you select *Ignore numbering schedule*, a search will be done across all active numbering schedules;
- *Notification of recording start* – notify the callee that the conversation will be recorded:
 - *Do not notify* – disable notification of recording start;
 - *Voice message* – voice notification of recording start.
- *Conversation record category* – a category assigned to the record for the specified mask.

3.1.16.2 Conversation Recording

In this section, you can manage conversation record files.



- *Total number of records* – total number of conversation record files in the selected directory;
- *Drive utilisation* – display the used space on the drive selected to store the conversation record files;
- *User category* – displays the conversation record category assigned to the current user of the web interface;
- *Select the date* – select the date to display conversation record files;
- *Time interval* – select the interval to display conversation record files;
- *Search details* – search for conversation record files; the search function uses any match of the entered value against the name of a conversation record file.

The record control buttons are described in the table below.

Table 16 – Record Control Buttons

Button	Function
	previous record
	start playback
	stop playback
	next record
	repeated record playback
	save record
	delete record

Format of a conversation record file

1. A common call without call forwarding or transfer

YYYY-MM-DD_hh-mm-ss_CgPN-CdPN_nX_cY.wav

where:

- **YYYY-MM-DD** – file creation date, YYYY – year, MM – month, DD – day;
- **hh-mm-ss** – file creation time, hh – hours, mm – minutes, ss – seconds;
- **CgPN** – the caller number, if absent, set to none;
- **CdPN** – the callee number;
- **nX** – the number of the numbering schedule in which the record was made;
- **cX** – the record category.

Example:

Subscriber 40010 calls to subscriber 40012, the file will look as follows:

2017-10-23_09-27-26_40010-40012_n0_c0.wav

2. Making a call when the call forwarding service is used

YYYY-MM-DD_hh-mm-ss_CgPN-CdPN_Srv_SrvNum_nX_cY.wav

where:

- **YYYY-MM-DD** – file creation date, YYYY – year, MM – month, DD – day;
- **hh-mm-ss** – file creation time, hh – hours, mm – minutes, ss – seconds;
- **CgPN** – the caller number, if absent, set to none;
- **CdPN** – the callee number – the number that actually receives the call.
- **Srv** – a label indicating that an additional service was used. The label values:
 - **cf** – the call was forwarded;
 - **ct** – the call was transferred;
 - **cp** – the call was picked up;
- **SrvNum** – the number of the service that provided the additional service. Depending on the label value, **Srv** is the number, which has received a redirected or transferred call, or the number from which the call has been picked up;
- **nX** – the number of the numbering schedule in which the record was made;
- **cX** – the record category.

Example:

Subscriber 40010 calls to subscriber 40011 who redirects the call to subscriber 40012.

2017-10-23_09-28-04_40010-40011_cf_40012_n0_c0.wav

3. Making a call when the call transfer service is used

The use of the call transfer service involves 3 subscribers – initiator of the call (subscriber A), subscriber implementing the call transfer (subscriber B), and subscriber receiving the transferred call (subscriber C).

When transferring a call, 3 conversation record files are created:

- Conversation between subscribers A – B;
- Conversation between subscribers B – C;
- Conversation between subscribers A – C after the call transfer.

Example:

Subscriber 40012 calls to subscriber 40010, which transfers the call to subscriber 40000.

The following files are generated:

2017-10-23_10-15-19_40012-40010_n0_c0.wav – conversation of subscribers A and B;

2017-10-23_10-15-31_40010-40000_n0_c0.wav – conversation of subscribers B and C, after the subscriber B has put on hold the subscriber A;

2017-10-23_10-15-19_40012-40010_ct_40000_n0_c0.wav – conversation of subscribers A and C after the call was transferred by subscriber B, where *ct* in the file name is the label indicating that the call transfer was made.

3.1.16.3 Conversation Record Categories

Call record categories		
No	Name	Access to categories
0	CallRecordCategory#00	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31
1	CallRecordCategory#01	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
2	CallRecordCategory#02	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
3	CallRecordCategory#03	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
4	CallRecordCategory#04	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
5	CallRecordCategory#05	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
6	CallRecordCategory#06	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
7	CallRecordCategory#07	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
8	CallRecordCategory#08	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
9	CallRecordCategory#09	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
10	CallRecordCategory#10	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
11	CallRecordCategory#11	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
12	CallRecordCategory#12	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
13	CallRecordCategory#13	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
14	CallRecordCategory#14	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
15	CallRecordCategory#15	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
16	CallRecordCategory#16	
17	CallRecordCategory#17	
18	CallRecordCategory#18	
19	CallRecordCategory#19	
20	CallRecordCategory#20	
21	CallRecordCategory#21	
22	CallRecordCategory#22	
23	CallRecordCategory#23	
24	CallRecordCategory#24	
25	CallRecordCategory#25	
26	CallRecordCategory#26	
27	CallRecordCategory#27	
28	CallRecordCategory#28	
29	CallRecordCategory#29	
30	CallRecordCategory#30	
31	CallRecordCategory#31	

Conversation record categories are used to define the user access rights for recorded conversations.

To restrict access to records, assign the corresponding category. For other categories, this menu defines accessibility to a category assigned to an object (to disable access, uncheck the checkbox next to the corresponding category; to enable access, check the checkbox next to the corresponding category).

In total, up to 32 record categories can be configured. By default, “Category 0” has a permanent access to all other categories and is used for the administrator account that provides access to all conversations. Other categories have configurable access. By default, the first 15 of them provide access to the first 16 categories.

To configure and edit a selected category, click the button.

Setup example: restrict access to conversation records

Consider an example when it is necessary to distinguish between access to the conversation records of the production department (“production user”) and those of the sales department (“sales user”). Each user should be able to listen only to conversations of their relevant department. To restrict access, proceed as follows:

1. Select the access category for records. You can specify a convenient name, for example, *Production* or *Sales*. For each category, set access only to itself:

Call record categories		
No	Name	Access to categories
0	Admin	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31
1	production	1
2	sales	2
3	CallRecordCategory#03	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
4	CallRecordCategory#04	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
5	CallRecordCategory#05	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
6	CallRecordCategory#06	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
7	CallRecordCategory#07	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
8	CallRecordCategory#08	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
9	CallRecordCategory#09	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
10	CallRecordCategory#10	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
11	CallRecordCategory#11	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
12	CallRecordCategory#12	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
13	CallRecordCategory#13	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
14	CallRecordCategory#14	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
15	CallRecordCategory#15	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
16	CallRecordCategory#16	
17	CallRecordCategory#17	
18	CallRecordCategory#18	
19	CallRecordCategory#19	
20	CallRecordCategory#20	
21	CallRecordCategory#21	
22	CallRecordCategory#22	
23	CallRecordCategory#23	
24	CallRecordCategory#24	
25	CallRecordCategory#25	
26	CallRecordCategory#26	
27	CallRecordCategory#27	
28	CallRecordCategory#28	
29	CallRecordCategory#29	
30	CallRecordCategory#30	
31	CallRecordCategory#31	

2. Log in to the user account management interface (see section 3.1.25 *Users of the Web Interface*). In the access rights of the production user, select *Listen to recorded conversations* right and set the available category to *Production*. For the sales user, select the *Listen to recorded conversations* and set the category to *Sales*:

Management

production Username

..... Enter password

..... Confirm password

User access rights:

- Restart device/software
- VoIP management (SIP)
- Subscribers management
- IP-settings, RADIUS management
- Configuration management
- Software management
- Listen call records
- [1] production Call record category
- Call-recording management
- Monitoring

Apply Cancel

Management

sales Username

..... Enter password

..... Confirm password

User access rights:

- Restart device/software
- VoIP management (SIP)
- Subscribers management
- IP-settings, RADIUS management
- Configuration management
- Software management
- Listen call records
- [2] sales Call record category
- Call-recording management
- Monitoring

Apply Cancel

- In the Recording Parameters section, add the recording number masks for the production and sales departments, and assign the relevant recording categories to them.

No	Mask	Type	Dial plan	Call record category
0	(4xxx)	All	Ignore dial plan	[1] production
1	(1xxx)	All	Ignore dial plan	[2] sales

- Now, if the user enters the Conversation Recording section, they will only see records of the categories to which they have access.
- In this example, if you need to add a “management user” with the right to listen records of all departments, then, as in step 1, add a new category, for example, “Management” and assign the access rights to the “Production” and “Sales” categories. Then, in the user management section, assign the access to the “Management” category to the management user.

Management

management Username

..... Enter password

..... Confirm password


User access rights:

- Restart device/software
- VoIP management (SIP)
- Subscribers management
- IP-settings, RADIUS management
- Configuration management
- Software management
- Listen call records
- [3] management Call record category
- Call-recording management
- Monitoring

Apply Cancel

As a result of these settings, the table of access restriction to conversation calls will look as follows:

Call record categories		
No	Name	Access to categories
0	Admin	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31
1	production	1
2	sales	2
3	management	1,2
4	CallRecordCategory#04	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
5	CallRecordCategory#05	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
6	CallRecordCategory#06	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
7	CallRecordCategory#07	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
8	CallRecordCategory#08	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
9	CallRecordCategory#09	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
10	CallRecordCategory#10	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
11	CallRecordCategory#11	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
12	CallRecordCategory#12	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
13	CallRecordCategory#13	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
14	CallRecordCategory#14	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
15	CallRecordCategory#15	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
16	CallRecordCategory#16	
17	CallRecordCategory#17	
18	CallRecordCategory#18	
19	CallRecordCategory#19	
20	CallRecordCategory#20	
21	CallRecordCategory#21	
22	CallRecordCategory#22	
23	CallRecordCategory#23	
24	CallRecordCategory#24	
25	CallRecordCategory#25	
26	CallRecordCategory#26	
27	CallRecordCategory#27	
28	CallRecordCategory#28	
29	CallRecordCategory#29	
30	CallRecordCategory#30	
31	CallRecordCategory#31	



3.1.17 Subscribers

The menu can be used to configure the parameters of SIP subscribers ¹.

3.1.17.1 SIP Subscribers

Subscriber Configuration

No	ID	Title	Number	Dial plan	Calling party category (RUS)	IP	SIP domain	SIP profile	Authorization	Select
0	17	40220	40220	[0] NumberPlan#0	1	0.0.0.0		SIP-profile	Without auth	<input type="checkbox"/>
1	18	40221	40221	[0] NumberPlan#0	1	0.0.0.0		SIP-profile	Without auth	<input type="checkbox"/>
2	19	40222	40222	[0] NumberPlan#0	1	0.0.0.0		SIP-profile	Without auth	<input type="checkbox"/>
3	20	40223	40223	[0] NumberPlan#0	1	0.0.0.0		SIP-profile	Without auth	<input type="checkbox"/>





- *Search for subscriber by number* – check whether the specified subscriber number is available in the database of configured SIP subscribers;
- *Edit selected* – click this button to enter the group editing menu for selected subscribers' parameters (with the *Select* checkbox selected next to them). To enable editing, select the *Edit* checkbox for the required parameter. The configuration parameters are described below;
- *Remove selected* – by clicking the button, a group of selected subscribers is deleted.

To create, edit, or remove a subscriber entry, use the *Objects – Add Object*, *Objects – Edit Object* or *Objects – Remove Object* menus and the following buttons:

- add subscribers;
- edit subscriber parameters;
- remove subscriber.

¹ The menu is available only in the firmware version with a SIP registration license. For more information about the licenses, see section **3.1.22 Licenses**

Subscriber Settings tab

SIP-Subscribers	
SIP subscriber	
Subscribers count	1 <small>Max subscribers count 196.</small>
Starting description	Subscriber#020
Starting number	
Starting CallerID number	
Use CallerID number for redirection	<input type="checkbox"/>
Calling party number type	Subscriber ▼
Calling party category (RUS)	1 ▼
Lines operation mode	Common ▼
Lines number 	1
IP-address:port	0.0.0.0 : 0
Allow unregistered calls	<input type="checkbox"/>
SIP domain	
SIP profile	not set ▼
PBX profile	[0] PBXprofile#0 ▼
Access category	[0] AccessCat#0 ▼
Dial plan	[0] NumberPlan#0 ▼
Authorization	not set ▼
Login	
Password	<input type="password"/> 
Ignore source port after registration	<input type="checkbox"/>
Subscriber service mode 	On ▼
Display name	
Use display name	Received only ▼
Busy-Lamp-Field (BLF) settings	
Enable subscription	<input type="checkbox"/>
Max subscribers number 	10
Monitoring group	0
VAS settings	
CLIRO	<input type="checkbox"/>
Enable VAS	<input type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- *Subscriber ID* – unique subscriber identifier;

-
- *Name* – arbitrary text description of subscribers;
 - *Number* – subscriber number; for a group of subscribers, number of each following subscriber will be increased by 1;
 - *Caller ID number* – subscriber's Caller ID number; for a group of subscribers, number of each following subscriber will be increased by 1;
 - *Use Caller ID for call forwarding*
 - *Caller ID type* – type of the subscriber number;
 - *Caller ID category* – subscriber's Caller ID category;
 - *Line mode* – setting limits on the number of simultaneous calls. Can take two values: Combined and Separate. The first mode takes into account the total number of simultaneous calls in which the subscriber can take part; in the second mode, incoming and outgoing calls are counted separately;
 - *Number of lines* – the number of simultaneous calls in which the subscriber can take part. The field appears if the line mode is set to *Combined*. The range of possible values is [1;255] or 0 – no limits;
 - *Number of incoming lines*¹ – the number of simultaneous incoming calls to the subscriber. The field appears if the line mode is set to *Separate*. The range of possible values is [1;255] or 0 – no limits;
 - *Number of outgoing lines*¹ – the number of simultaneous outgoing calls from the subscriber. The field appears if the line mode is set to *Separate*. The range of possible values is [1;255] or 0 – no limits;
 - *IP address: Port* – IP address and port of the subscriber. If the value is set to 0.0.0.0, the subscriber is allowed to register from any IP address. When you set the port value to zero, the port sending the registration request is ignored;
 - *Allow calls without registration* – the option becomes active only if the *IP address: Port* option specifies both the IP address and the port of the subscriber. When this option is checked, the subscriber is allowed to make calls without registration from the specified IP and port;
 - *SIP domain* – identifies the domain to which the subscriber belongs. It is sent by the subscriber gateway as the “host” parameter in the SIP URI of the *from* and *to* fields;
 - *SIP profile* – select the SIP profile. The SIP profile defines most of the subscriber settings (see section 3.1.7.3);
 - *PBX profile* – select the PBX profile (see section 3.1.8.3 PBX Profiles);
 - *Access category* – select an access category;
 - *Numbering schedule* – define the numbering schedule for the subscriber;
 - *Authorisation* – define the authentication mode for the device:
 - *None* – authentication is disabled;
 - *With REGISTER* – authentication is performed only during the registration, using the REGISTER request;

¹ These settings appear if the separate line mode is selected

-
- *With REGISTER and INVITE* – authentication is performed both during the registration and when making outgoing calls, using REGISTER and INVITE requests;
 - *Login* – the user name for authentication;
 - *Password* – password for authentication;
 - *Ignore the source port after registration* – after registration, messages from subscribers can arrive from any port of the registered address;
 - *Subscriber service mode* – set a limit on the incoming and outgoing communication for the subscriber:
 - *disabled*: out of service. The subscriber number is present in the numbering schedule, but the subscriber terminal cannot be registered. Therefore, incoming calls will be rejected with the *out of order* cause; outgoing calls cannot be initiated;
 - *enabled*: all types of communication are available;
 - *disabled 1*: incoming communication is enabled; outgoing communication is to special services only;
 - *disabled 2*: incoming communication is disabled; outgoing communication is to special services only;
 - *barring 1*: full barring for incoming and outgoing calls. Calls will be routed according to the numbering schedule, but be rejected;
 - *barring 2*: full barring for incoming and outgoing calls, except for special services;
 - *barring 3*: incoming calls are barred, outgoing calls are allowed;
 - *barring 4*: incoming calls are barred, outgoing calls are allowed only for local and private communication;
 - *barring 5*: incoming calls are allowed, outgoing calls are fully barred;
 - *barring 6*: incoming calls are allowed, outgoing calls are allowed only for special services;
 - *barring 7*: incoming calls are allowed, outgoing calls are allowed only for local and private communication;
 - *barring 8*: incoming calls are allowed, outgoing calls are allowed only for local and private and zone communication;
 - *excluded*: excluded from the numbering schedule. The number is completely excluded from the subscriber number list of the numbering schedule. If this number is called, the call will be rejected with the *no route to destination* cause, or it will be routed to the appropriate prefix in the numbering schedule.
 - *Display name* – the name to be transferred to the display-name parameter. The parameter affects on usage of display-name as Connected Name in call reply in the direction of subscriber;
 - *Display name usage* – the display name usage mode (SIP display-name). Can take the values:
 - *Never* – the *Display name* setting will not be used and the display-name parameter will always take the value indicated in the initiating INVITE request;
 - *If not specified* – if a call initiation request received from the subscriber does not specify the display-name, then the display-name is substituted with the value configured on SMG. Otherwise, the specified display-name will be used;
 - *Always* – regardless of the display-name indicated in the subscriber's request, the display-name configured on SMG will be used.

Busy lamp field (BLF) settings

- *Allow event subscription* – enable subscription to BLF events of other subscribers;
- *Number of subscribers* – the amount of monitored numbers with the activated BLF service;

- *Monitoring group* – the BLF monitoring group; BLF monitoring is allowed only between the subscribers belonging to the same monitoring group.



Directions (*local network, special service, zone network, private network, long-distance communication, international communication*) are specified when configuring the prefix in the **Direction** field of the numbering schedule.

VAS Configuration

- *CLIRO* – a service for overriding the prohibition on caller number identification;
- *Use VAS¹* – enable VAS services. When this option is checked, the *VAS Activation* table becomes available:

VAS Activation

VAS activation	
Unconditional redirection	<input type="checkbox"/>
Busy redirection	<input type="checkbox"/>
No-reply redirection	<input type="checkbox"/>
Out-of-service redirection	<input type="checkbox"/>
Call hold	<input type="checkbox"/>
Call transfer	<input type="checkbox"/>
3WAY conference	<input type="checkbox"/>
Call pickup	<input type="checkbox"/>
Change password	<input type="checkbox"/>
Outgoing calls restriction	<input type="checkbox"/>
Restricted by password	<input type="checkbox"/>
Password activation	<input type="checkbox"/>
Follow me	<input type="checkbox"/>
Follow me (no response)	<input type="checkbox"/>
Reset all services	<input type="checkbox"/>

- *Call Forwarding Unconditional* – enable the Call Forwarding Unconditional (CF Unconditional) service;
- *Call Forwarding Busy* – enable the Call Forwarding Busy (CF Busy) service;
- *Call Forwarding No Reply* – enable the Call Forwarding No Reply (CF No Reply) service;
- *Call Forwarding Out of Service* – enable the Call Forwarding Out of Service (CF Out Of Service);
- *Call hold* – enable the Call Hold service;
- *Call transfer* – enable the Call Transfer service;
- *3-way conference* – enable the 3WAY conference service;
- *Call pickup* – enable the Call Pickup service;
- *Conference with consequent assembly* ;

¹ The menu is available only in the firmware version with an SMG-VAS license. For more information about the licenses, see section **3.1.22 Licenses**

- *Disable conference when an initiator leaves the conference* – when checked, the conference will be disabled when an initiator leaves the conference. Otherwise, the conference will be saved even when the initiator leaves and will be over only when all the participants leave;
- *Password change* – change the password to restrict the outgoing communication;
- *Restrict outgoing communication* – use the *Restrict outgoing communication by password* service;
- *Outgoing communication by password* – allows the subscriber to make a call once without communication restriction by entering the VAS password;
- *Password activation* – allows the subscriber to enter a password once to remove the outgoing communication restriction. Re-entering the password sets the restriction again;
- *Follow me* – activate the *follow me* service.
- *Follow me (no response)* – activate the *follow me* service.
- *Do not disturb* – allows subscriber to set the ‘Do not Disturb’ mode and to specify several numbers, that can call this subscriber, from the white list.
- *Black list* – allows subscriber to include phone numbers in the black list for blocking calls from these numbers;
- *Cancel all services* – cancel all numbers configured for forwarding by clicking a service prefix set in the numbering schedule.

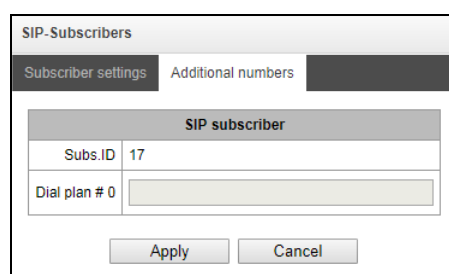
For a detailed description of VAS, see APPENDIX K. WORKING WITH VAS SERVICES

Additional Numbers Tab

A subscriber can have different numbers in different numbering schedules. At that, when a call passes through the numbering schedule change prefix, the subscriber's CgPN number is automatically replaced with their number in the corresponding numbering schedule. For example:

a subscriber has an internal short number and, therefore, registers at the gateway with the short number. When connecting to an external network, the subscriber should replace CgPN with their number in the international format. The transition to an external network is performed through prefix 9.

To solve this task, you need to activate two numbering schedules in the *System Parameters* section, create a list of subscribers with short numbering at the gateway, and specify an external number for each subscriber in the *Additional numbers* setting of the *Numbering schedule 1* field. In the *Numbering schedule 1*, create the prefix of transition to the external network, while in the *Numbering schedule 0*, create a prefix (*9x.*) of the *Numbering schedule change* type that will transfer the calls to the *Numbering schedule 1*. When the subscriber dials a full number starting from 9, the call will be transferred to the *Numbering schedule change* prefix; when the call gets into the numbering schedule 1, the subscriber's CgPN number will automatically be replaced with their external number.



SIP subscriber	
Subs.ID	17
Dial plan # 0	

Apply Cancel

Numbering schedule # 0–16 – additional subscriber number in the corresponding numbering schedule.

VAS Management

In this section, you can configure VAS settings for subscribers.

VAS services are provided to each subscriber, but in order to use a particular service, it must be enabled by the operator. The operator can create a service plan from multiple VAS functions. To do this, select the *Use VAS* checkbox and other checkboxes for required VAS functions in the section Subscriber Configuration.

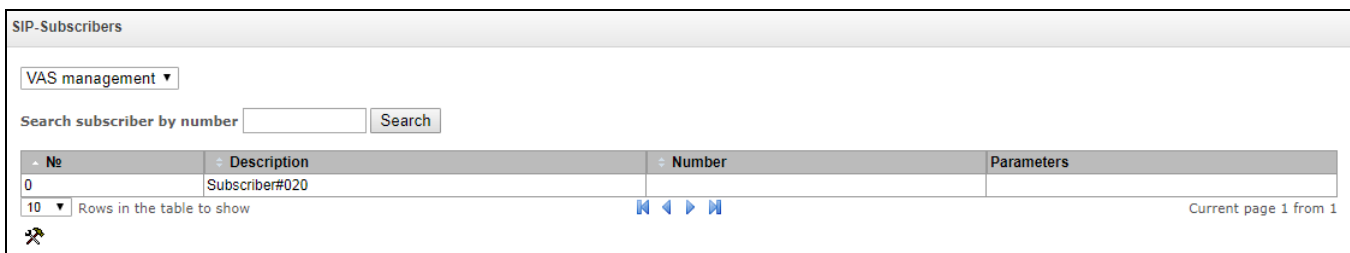
Subscribers can manage the status of VAS services from their telephone set. The following options are available:

- *service activation* – activate the service and enter additional data;
- *service verification*;
- *cancel service* – disable the service;

When the activation code is entered or the service is cancelled, subscribers may hear either a *Confirmation* signal (3 short tones) or a *Busy* signal (intermittent tone with tone/pause duration – 0.35/0.35 sec). The *Confirmation* signal indicates that the service has been successfully activated or cancelled; the *Busy* signal indicates that this service is not activated for the subscriber.

After entering the service verification code, the subscriber may hear either the *Station Response* signal (continuous tone) or the *Busy* signal. The *Station Response* signal indicates that the service has been successfully enabled and activated for the subscriber; the *Busy* signal indicates that the service is disabled or not activated for the subscriber.

The menu displays only those numbers for which the *Use VAS* checkbox is selected in the configuration menu (section 0 Subscriber Configuration).



No	Description	Number	Parameters
0	Subscriber#020		

- *Number for Call Forwarding Unconditional* – phone number for the Call Forwarding Unconditional service;

Numbers [redacted]

VAS block for subscriber Subscriber#020

Number for unconditional redirection	<input type="text"/>
Number for busy redirection	<input type="text"/>
Number for no-reply redirection	<input type="text"/>
Number for out-of-service redirection	<input type="text"/>
Password	<input type="text" value="1111"/>
Password activation	<input type="checkbox"/>
Restrict out	<input type="text" value="all allowed"/>
Follow me	
Follow me activation	<input type="checkbox"/>
Follow me pin	<input type="checkbox"/>
Follow me number	<input type="checkbox"/>
Follow me pin	<input type="text"/>
Follow me number	<input type="text"/>
Follow me (no response)	
Follow me activation	<input type="checkbox"/>
Follow me pin	<input type="checkbox"/>
Follow me number	<input type="checkbox"/>
Follow me (no response)pin	<input type="text"/>
Follow me (no response)number	<input type="text"/>

Apply Cancel

- *Number for Call Forwarding Busy* – phone number for the Call Forwarding Busy service;
- *Number for Call Forwarding No Reply* – phone number for the Call Forwarding No Reply service;
- *Number for Call Forwarding Out of Service* – phone number for the Call Forwarding Out of Service;
- *Password* – a 4–8 digit password to access the outgoing communication restriction service by password;
- *Password activation* – when this option is checked, the password is activated and the outgoing communication restrictions are removed;
- *Restrict outgoing communication* – specifies that outgoing communication is not allowed for certain types of directions when the password is inactive.
 - *all allowed* – all the restrictions are not valid, restriction code – 0;
 - *only to emergency* – egress communication is restricted, only emergency calls are available, restriction code – 1;
 - *only local and department network* – egress communication is restricted, it is available to call only to local numbers and departmental numbers, restriction code – 2;
 - *only local, department and zone network* – egress communication is restricted, it is available to call only to local and zone numbers and departmental numbers, restriction code – 3.
- *“White list” tab* – you may activate the "do not disturb" service and define white number list containing the numbers which can call the subscriber even in "do not disturb" mode.
- *“Black list” tab* – you may activate the "black list" service and set black list of numbers which can not call the subscriber.

The operation and configuration of the VAS services are detailed in APPENDIX K. WORKING WITH VAS SERVICES

Subscriber Monitoring

When you select the *Monitoring* command from the drop-down list, a subscriber status table is displayed.

SIP-Subscribers

Monitoring ▾

Number of configured subscribers: 5
Number of registered subscribers: 0

Search subscriber by number

No	State	Title	Number	SIP domain	IP/Port	Last registration	Expire in	Select
0	Registration is expired	40220	40220	192.168.1.20	192.168.1.12:5060	13:50:24 31.05.2018	00:00:00	<input type="checkbox"/>
1	Not registered	40221	40221		0.0.0.0:0	no registration	00:00:00	<input type="checkbox"/>
2	Not registered	40222	40222		0.0.0.0:0	no registration	00:00:00	<input type="checkbox"/>
3	Not registered	40223	40223		0.0.0.0:0	no registration	00:00:00	<input type="checkbox"/>
4	Not registered	Subscriber#020			0.0.0.0:0	no registration	00:00:00	<input type="checkbox"/>

10 ▾ Rows in the table to show Current page 1 from 1

Selected: 0

- *Status* – subscriber registration status (registered, not registered, registration expired);
- *Name* – arbitrary text description of a subscriber;
- *Number* – the subscriber number;
- *SIP domain* – the domain to which the subscriber belongs;
- *IP/Port* – IP address and port of the subscriber;
- *Last registration* – the time of the last registration;
- *Registration expires* – the time remaining before the registration expiration.

Click the *Reset registration* button to forcedly reset the registration for selected subscribers.

BLF Monitoring

SIP-Subscribers

BLF Monitoring ▾

Search subscriber by number Search

№	Subs. name	Subs. number	BLF state	Observers number
0	40220	40220		0
1	40221	40221		0
2	40222	40222		0
3	40223	40223		0
4	Subscriber#020			0

10 ▾ Rows in the table to show Current page 1 from 1

- *Subscriber name* – display the subscriber name;
- *Number* – display the subscriber number;
- *BLF status* – display the BLF status;
- *Number of observers* – the number of contacts who monitor the subscriber.

3.1.17.2 FXS/FXO Ports

FXS/FXO ports

Configuration ▾

Search subscriber by number Search

Line	Type	Title	Number	Dial plan	Calling party category (RUS)	Select
1	FXO	Subscriber#000	10000	[0] NumberPlan#0	1	<input type="checkbox"/>
2	FXO	Subscriber#001	10001	[0] NumberPlan#0	1	<input type="checkbox"/>
3	FXO	Subscriber#002	10002	[0] NumberPlan#0	1	<input type="checkbox"/>
4	FXO	Subscriber#003	10003	[0] NumberPlan#0	1	<input type="checkbox"/>
5	FXO	Subscriber#004	10004	[0] NumberPlan#0	1	<input type="checkbox"/>
6	FXO	Subscriber#005	10005	[0] NumberPlan#0	1	<input type="checkbox"/>
7	FXO	Subscriber#006	10006	[0] NumberPlan#0	1	<input type="checkbox"/>
8	FXO	Subscriber#007	10007	[0] NumberPlan#0	1	<input type="checkbox"/>
9	FXS	Subscriber#008	10008	[0] NumberPlan#0	1	<input type="checkbox"/>
10	FXS	Subscriber#009	10009	[0] NumberPlan#0	1	<input type="checkbox"/>
11	FXS	Subscriber#010	10010	[0] NumberPlan#0	1	<input type="checkbox"/>
12	FXS	Subscriber#011	10011	[0] NumberPlan#0	1	<input type="checkbox"/>
13	FXS	Subscriber#012	10012	[0] NumberPlan#0	1	<input type="checkbox"/>
14	FXS	Subscriber#013	10013	[0] NumberPlan#0	1	<input type="checkbox"/>
15	FXS	Subscriber#014	10014	[0] NumberPlan#0	1	<input type="checkbox"/>
16	FXS	Subscriber#015	10015	[0] NumberPlan#0	1	<input type="checkbox"/>

20 ▾ Rows in the table to show Current page 1 from 1

Selected: 0

- *Search for subscriber by number* – check whether the specified subscriber number is available in the database of configured SIP subscribers;
- *Edit selected* – click this button to enter the group editing menu for selected subscribers' parameters (with the *Select* checkbox selected next to them). To enable editing, select the *Edit* checkbox for the required parameter. The configuration parameters are described below;

To edit the selected objects, click the button.

FXS/FXO ports	
FXS/FXO port 9	
Description	Subscriber#008
Port type	<input checked="" type="radio"/> FXS <input type="radio"/> FXO
Number	10008
CallerID number	10008
Use CallerID number for redirection	<input type="checkbox"/>
Calling party number type	Subscriber
Calling party category (RUS)	1
PBX profile	[0] PBXprofile#0
FXS/FXO profile	[0] hotline FXO
Access category	[0] AccessCat#0
Dial plan	[0] NumberPlan#0
CallerID generation	FSK BELL202
Send only number	<input type="checkbox"/>
Subscriber service mode	On
VAS settings	
CLIRO	<input type="checkbox"/>
Enable VAS	<input type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- *Name* – arbitrary text description of a subscriber;
- *Enable VAS* – checkbox for enabling/disabling port operation;
- *Port type* – information field displaying port type (FXS, FXO or “inavalable” type if submodule is not installed or initialized);
- *Number* – the phone number of the FXS port for making a call to this port;
- *Caller ID number* – the phone number of the FXS port for making a call from this port;
- *Use Caller ID number for call forwarding* – use the number specified in the *Caller ID Number* field when performing the call forwarding service;
- *Caller ID type* – type of the subscriber number;
- *Caller ID category* – subscriber's Caller ID category;
- *PBX profile* – select the PBX profile (see section 3.1.8.3 PBX Profiles);
- *FXS/FXO profile* – select the FSX/FXO profile for the subscriber;
- *Access category* – select an access category;
- *Numbering schedule* – define the numbering schedule for the subscriber;

- *Caller ID display* – select the Caller ID display format. Available values: disabled, Caller ID, Caller ID (w/o waiting 500 Hz), DTMF, FSK BELL202, FSK V.23;
- *Display number only* – if this option is checked, only the caller number (without name) is displayed;
- *Subscriber service mode* – set a limit on the incoming and outgoing communication for the subscriber:
 - *disabled*: out of service. The subscriber number is present in the numbering schedule, but the subscriber terminal cannot be registered. Therefore, incoming calls will be rejected with the *out of order* cause; outgoing calls cannot be initiated;
 - *enabled*: all types of communication are available;
 - *disabled 1*: incoming communication is enabled; outgoing communication is to special services only;
 - *disabled 2*: incoming communication is disabled; outgoing communication is to special services only;
 - *barring 1*: full barring for incoming and outgoing calls. Calls will be routed according to the numbering schedule, but be rejected;
 - *barring 2*: full barring for incoming and outgoing calls, except for special services;
 - *barring 3*: incoming calls are barred, outgoing calls are allowed;
 - *barring 4*: incoming calls are barred, outgoing calls are allowed only for local and private communication;
 - *barring 5*: incoming calls are allowed, outgoing calls are fully barred;
 - *barring 6*: incoming calls are allowed, outgoing calls are allowed only for special services;
 - *barring 7*: incoming calls are allowed, outgoing calls are allowed only for local and private communication;
 - *barring 8*: incoming calls are allowed, outgoing calls are allowed only for local and private and zone communication;
 - *excluded*: excluded from the numbering schedule. The number is completely excluded from the subscriber number list of the numbering schedule. If this number is called, the call will be rejected with the *no route to destination* cause, or it will be routed to the appropriate prefix in the numbering schedule.
- *Receive side signal amplification (Gain receive)* – volume of the received signal (amplification/attenuation of the signal level)
- *Gain transmit (0.1 dB)*— volume of signal transmitted, gain/loss of the signal transmitted to the communicating device direction.

VAS Configuration

- *CLIRO* – a service for overriding the prohibition on caller number identification;
- *Use VAS¹* – enable VAS services. When this option is checked, the *VAS Activation* table becomes available:

¹ The menu is available only in the firmware version with an SMG-VAS license. For more information about the licenses, see section **3.1.22** Licenses

VAS Activation

VAS activation	
Unconditional redirection	<input type="checkbox"/>
Busy redirection	<input type="checkbox"/>
No-reply redirection	<input type="checkbox"/>
Call hold	<input checked="" type="checkbox"/>
Call transfer	<input type="checkbox"/>
3WAY conference	<input type="checkbox"/>
Call pickup	<input type="checkbox"/>
Change password	<input type="checkbox"/>
Outgoing calls restriction	<input type="checkbox"/>
Restricted by password	<input type="checkbox"/>
Password activation	<input type="checkbox"/>
Follow me	<input type="checkbox"/>
Follow me (no response)	<input type="checkbox"/>
Reset all services	<input type="checkbox"/>

- *Unconditional redirection* – enable the Call Forwarding Unconditional (CF Unconditional) service;
- *Busy redirection* – enable the Call Forwarding Busy (CF Busy) service;
- *No-reply redirection* – enable the Call Forwarding No Reply (CF No Reply) service;
- *Call hold* – enable the Call Hold service;
- *Call transfer* – enable the Call Transfer service;
- *3WAY conference* – enable the 3WAY conference service;
- *Call pickup* – enable the Call Pickup service;
- *Conference* – activate a conference with consequent participant collection;
- *Disconnect conference by initiator* – when checked, a conference will be over when an initiator leaves it. Otherwise, the conference will be saved after the initiator quitting and will be over only when all the participants leave the conference;
- *Password change* – change the password to restrict the outgoing communication;
- *Restrict outgoing communication* – use the *Restrict outgoing communication by password* service;
- *Outgoing communication by password* – allows the subscriber to make a call once without communication restriction by entering the VAS password;
- *Password activation* – allows the subscriber to enter a password once to remove the outgoing communication restriction. Re-entering the password sets the restriction again;
- *Follow me* – activate the *follow me* service.
- *Follow me (no response)* – activate the *follow me* service.

- *Do not disturb* – allows a subscriber to set the ‘Do not disturb’ and define several numbers from white list which were able to call the subscriber.
- *Black list* – allows a subscriber to add numbers to a black list to block calls from these numbers.
- *Reset all services* – cancel all numbers configured for forwarding by clicking a service prefix set in the numbering schedule.

For a detailed description of VAS, see APPENDIX K. WORKING WITH VAS SERVICES

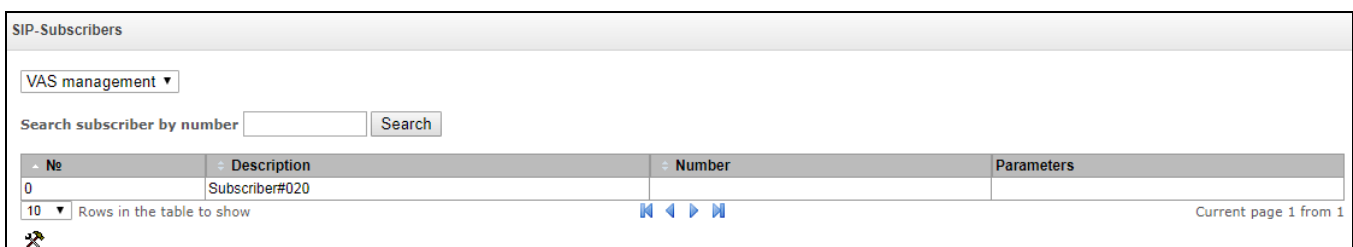
FXO port settings

FXS/FXO ports	
FXS/FXO port 10	
Description	Subscriber#009
Enable	<input checked="" type="checkbox"/>
Port type	FXS
Number	10000
CallerID number	
Use CallerID number for redirection	<input type="checkbox"/>
Calling party number type	Subscriber
Calling party category (RUS)	1
PBX profile	[0] PBXprofile#0
FXS/FXO profile	[0] FXSprofile#0
Access category	[0] AccessCat#0
Dial plan	[0] NumberPlan#0
CallerID generation	FSK V.23
Send only number	<input type="checkbox"/>
Subscriber service mode	On
Rx gain (0.1 dB)	0
Tx gain (0.1 dB)	0
VAS settings	
CLIRO	<input type="checkbox"/>
Enable VAS	<input checked="" type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- *Description* – arbitrary textual description of the subscriber;
- *Enable* – on/off port operation ;
- *Port type* – information field displaying port type (FXS, FXO or unavailable if the submodule is not installed or initialised);
- *Number* – FXS port number used for calling to this port;
- *Caller ID number* – phone number of FXS port that will be used for calling from this port;

- *PBX profile* – select PBX profile (see Section 3.1.8.3 PBX Profiles);
- *FXS/FXO profile* – select FXS/FXO profile for subscriber;
- *Access category* – select access category;
- *Dial plan* – defines the numbering schedule that the subscriber will belong to;
- *Hotline* – the hotline number used for incoming calls to the port;
- *PSTN hotline* – the hotline number used for outgoing calls from the port;
- *Rx gain (0.1 dB)* – volume of signal received, gain/loss of the signal received from the communicating device.
- *Tx gain (0.1 dB)* – volume of signal transmitted, gain/loss of the signal transmitted to the communicating device direction.

VAS Management



No	Description	Number	Parameters
0	Subscriber#020		

In this section, you can configure VAS settings for subscribers.

VAS services are provided to each subscriber, but in order to use a particular service, it must be enabled by the operator. The operator can create a service plan from several VAS functions. To enable this, select the *Use VAS* checkbox and other checkboxes for required VAS functions in the section *Subscriber Configuration*.

Subscribers can manage the status of VAS services from their telephone set. The following options are available:

- *service activation* – activate the service and enter additional data;
- *service verification*;
- *cancel service* – disable the service;

When the activation code is entered or the service is cancelled, subscribers may hear either a *Confirmation* signal (3 short tones) or a *Busy* signal (intermittent tone with tone/pause duration – 0.35/0.35 sec). The *Confirmation* signal indicates that the service has been successfully activated or cancelled; the *Busy* signal indicates that this service is not activated for the subscriber.

After entering the service verification code, the subscriber may hear either the *Station Response* signal (continuous tone) or the *Busy* signal. The *Station Response* signal indicates that the service has been successfully enabled and activated for the subscriber; the *Busy* signal indicates that the service is disabled or not activated for the subscriber.

The menu displays only those numbers for which the *Use VAS* checkbox is selected in the configuration menu (section *Subscriber Configuration*).

-
- *Number for Call Forwarding Unconditional* – phone number for the Call Forwarding Unconditional service;
 - *Number for Call Forwarding Busy* – phone number for the Call Forwarding Busy service;
 - *Number for Call Forwarding No Reply* – phone number for the Call Forwarding No Reply service;
 - *Number for Call Forwarding Out of Service* – phone number for Call Forwarding Out of Service;
 - *Password* – a 4–8 digit password to access the outgoing communication restriction service by password;
 - *Password activation* – when this option is checked, the password is activated and the outgoing communication restrictions are removed;
 - *Restrict outgoing communication* – specifies that outgoing communication is not allowed for certain types of directions when the password is inactive.
 - *all allowed* – all the restrictions for outgoing traffic are not valid, restriction code – 0;
 - *only to emergency* – egress communication is restricted, only emergency calls are available, restriction code – 1;
 - *only local or department network*– egress communication is restricted, it is available to call only to local numbers and departmental numbers, restriction code – 2;
 - *only local, department and zone network* – egress communication is restricted, it is available to call only to local and zone numbers and departmental numbers, restriction code – 3.
 - *“White list” tab* – you may activate the "do not disturb" service and define white number list containing the numbers which can call the subscriber even in "do not disturb" mode.
 - *“Black list” tab*– you may activate the "black list" service and set black list of numbers which can not call the subscriber.

The operation and configuration of the VAS services are detailed in APPENDIX K. WORKING WITH VAS SERVICES.

Subscriber Monitoring

When you choose 'Monitoring' item from the drop down list, a subscriber status table will be shown.

ELTEX Signaling & Media Gateway Configurator ● No alarms Users: Management

System info Objects Service Help Exit Ru En

Sections

- ▶ Voice messages
 - ▶ SIP-replies list to switch on reserve
 - ▶ Q.850 release causes list
- ▶ IVR
 - ▶ Scenarios list
 - ▶ Tones list
 - ▶ Call records
- ▶ TCP/IP settings
 - ▶ Routing table
 - ▶ Network settings
 - ▶ Network interfaces
 - ▶ RTP ports range
- ▶ Network services
 - ▶ NTP
 - ▶ SNMP
 - ▶ FTP-server
- ▶ Security
 - ▶ SSL/TLS settings
 - ▶ Dynamic firewall
 - ▶ Blocked addresses list
 - ▶ Static firewall
 - ▶ White addresses list
- ▶ Network utilities
 - ▶ PING
 - ▶ TRACEROUTE
- ▶ RADIUS settings
 - ▶ Servers
 - ▶ Profiles
 - ▶ RADIUS-replies to voice messages r
- ▶ Traces
 - ▶ PCAP traces
 - ▶ PBX traces
 - ▶ SYSLOG
- ▶ Call recording
 - ▶ Call recording settings
 - ▶ Call records
 - ▶ Call record categories
- ▶ Subscribers
 - ▶ SIP-Subscribers
 - ▶ FXS/FXO ports
 - ▶ PRI-Subscribers
 - ▶ Dynamic subscribers groups

FXS/FXO ports

Monitoring ▾

Filter by number

Line	Type	Name	Number	State	block reason	State timer	Incoming CgPN	Outgoing CgPN	Incoming CdPN	Outgoing CdPN	Line states
1	FXO	Subscriber#000		Idle	-	1036:49:40	-	-	-	-	Off
2	FXO	Subscriber#001	10001	Idle	-	1036:49:40	-	-	-	-	Idle
3	FXO	Subscriber#002		Idle	-	1036:49:40	-	-	-	-	Block
4	FXO	Subscriber#003		Idle	-	1036:49:40	-	-	-	-	Incoming dialing
5	FXO	Subscriber#004		Idle	-	1036:49:40	-	-	-	-	Outgoing dialing
6	FXO	Subscriber#005		Idle	-	1036:49:40	-	-	-	-	Incoming alerting
7	FXO	Subscriber#006		Idle	-	1036:49:40	-	-	-	-	Outgoing alerting
8	FXO	Subscriber#007		Idle	-	1036:49:40	-	-	-	-	Busy, Release
9	FXS	Subscriber#008	10004	Idle	-	1036:49:40	-	-	-	-	Talk
10	FXS	Subscriber#009	10000	Idle	-	503:35:47	-	-	-	-	Hold
11	FXS	Subscriber#010	10002	Idle	-	503:35:47	-	-	-	-	Waiting, Wait CID
12	FXS	Subscriber#011	10003	Idle	-	1036:49:40	-	-	-	-	3way, Conference
13	FXS	Subscriber#012		Idle	-	1036:49:40	-	-	-	-	
14	FXS	Subscriber#013		Idle	-	1036:49:40	-	-	-	-	
15	FXS	Subscriber#014		Idle	-	1036:49:40	-	-	-	-	
16	FXS	Subscriber#015		Idle	-	1036:49:40	-	-	-	-	

- *Line* – port sequence number;
- *Type* – FXO or FXS port type;
- *Name* – arbitrary subscriber text description.
- *Number* – subscriber's number.
- *Status* – the current status of the port. The available states are in the legend located under the ports table.
 - Description of states:
 - *OFF*—channel is disabled in configuration;
 - *Idle*—channel is in initial state;
 - *Block*—port is blocked;
 - *Incoming dialing*—incoming call dialling;
 - *Outgoing dialing*—outgoing call dialling;
 - *Incoming alerting*—incoming occupation, callee is disengaged;
 - *Outgoing alerting*—outgoing occupation, callee is disengaged;
 - *Busy, Release*—channel release, sending 'busy' tone;
 - *Talk, Hold*—channel is in call state, on hold;
 - *Waiting, Waiting CID* –waiting for response from the opposite party (waiting for occupation acknowledgement, waiting for Caller ID, waiting for call dialling);
 - *3way, Conference* – conference mode (three-way or sequential collection).
- *Block reason* – port block reason. The following reasons are possible:

- The leakage current exceeds permissible value;
 - Temperature exceeds permissible value;
 - Power dissipation exceeds the permissible value;
 - Hardware problem;
 - Line reinitialization (after enabling the port, it is blocked. The reason of blocking will be reinitialization because the port will be completely reinitialized);
 - Offhook condition (doesn't appear in the list of accidents and doesn't send traps);
 - Unknown reason;
- *State timer* – timer showing how long the port is in the current state;
 - *Incoming CgPN* – incoming A-number;
 - *Outgoing CgPN* – outgoing A-number;
 - *Incoming CdPN* – incoming B-number;
 - *Outgoing CdPN* – outgoing B-number.

3.1.17.3 Dynamic Subscriber Groups

Configuration of Dynamic Subscriber Groups

In this section, you can configure dynamic subscriber groups.

Dynamic *registration* uses digest authentication of subscribers on the RADIUS server (rfc 4590, rfc4590-no-challenge, draft-sterman).




Dynamic subscribers groups								
Configuration								
No	ID	Description	Number of subscribers	Dial plan	Calling party category (RUS)	SIP domain	SIP profile	Select
0	1	SubscriberGroup#000	1	[0] NumberPlan#0	1		het	<input type="checkbox"/>





10 Rows in the table to show

Current page 1 from 1

Selected: 0

To create, edit, or remove an entry, use the *Objects – Add Object*, *Objects – Edit Object* or *Objects – Remove Object* menus and the following buttons:

-  – add subscribers;
-  – edit subscriber parameters;
-  – remove subscriber.

Dynamic subscribers groups	
Dynamic Subscribers Group 1	
Group ID	1
Subscribers number	1 <small>Maximum available subscribers count is 195.</small>
Description	SubscriberGroup#000
Calling party number type	Subscriber
Calling party category (RUS)	1
Lines operation mode	Common
Lines number 	1
SIP domain	
SIP profile	not set
PBX profile	[0] PBXprofile#0
Access category	[0] AccessCat#0
Dial plan	[0] NumberPlan#0
Ignore source port after registration	<input type="checkbox"/>
Subscriber service mode 	On
Busy-Lamp-Field (BLF) settings	
Enable subscription	<input type="checkbox"/>
Max subscribers number 	0
Monitoring group	0
VAS settings	
CLIRO	<input type="checkbox"/>
VAS management	not used
Timeout for VAS block reset, days 	0
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Dynamic Subscriber Group

- *Number of subscribers* – the number of subscribers in the group;
- *Name* – name of the dynamic subscriber group;
- *Caller ID type* – type of the subscriber number;
- *Caller ID category* – subscriber's Caller ID category;
- *Line mode* – setting limits on the number of simultaneous calls. Can take two values: Combined and Separate. The first mode takes into account the total number of simultaneous calls in which the subscriber can take part; in the second mode, incoming and outgoing calls are counted separately;
- *Number of lines* – the number of simultaneous calls in which the subscriber can take part. The field appears if the line mode is set to *Combined*. The range of possible values is [1;255] or 0 – no limits;
- *Number of incoming lines¹* – the number of simultaneous incoming calls to the subscriber. The field appears if the line mode is set to *Separate*. The range of possible values is [1;255] or 0 – no limits;

¹ These settings appear if the separate line mode is selected

- *Number of outgoing lines*¹ – the number of simultaneous outgoing calls from the subscriber. The field appears if the line mode is set to *Separate*. The range of possible values is [1;255] or 0 – no limits;
- *SIP domain* – identifies the domain to which the subscriber belongs. It is sent by the subscriber gateway as the “host” parameter in the SIP URI of the *from* and *to* fields (see section 3.1.6.4);
- *SIP profile* – select the SIP profile. The SIP profile defines the most of the subscriber settings (see section 3.1.7.3 for SIP/ SIP-T/ SIP-I interfaces, SIP profiles);
- *PBX profile* – select the PBX profile (see section 3.1.8.3);
- *Access category* – select an access category;
- *Numbering schedule* – define the numbering schedule for the subscriber;
- *Ignore the source port after registration* – after registration, messages from subscribers can arrive from any port;
- *Subscriber service mode* – set a limit on the incoming and outgoing communication for the subscriber:
 - *disabled* – the port is out of service. The subscriber number is present in the numbering schedule, but the subscriber terminal cannot be registered. Therefore, incoming calls will be rejected with the *out of order* cause; outgoing calls cannot be initiated;
 - *enabled* – all types of communication are available;
 - *disabled 1* – incoming communication is enabled; outgoing communication is to special services only;
 - *disabled 2* – incoming communication is disabled; outgoing communication is to special services only;
 - *barring 1* – full barring for incoming and outgoing calls. Calls will be routed according to the numbering schedule, but be rejected;
 - *barring 2* – full barring for incoming and outgoing calls, except for special services;
 - *barring 3* – incoming calls are barred, outgoing calls are allowed;
 - *barring 4* – incoming calls are barred, outgoing calls are allowed only for local and private communication;
 - *barring 5* – incoming calls are allowed, outgoing calls are fully barred;
 - *barring 6* – incoming calls are allowed, outgoing calls are allowed only for special services;
 - *barring 6* – incoming calls are barred, outgoing calls are allowed only for local and private communication;
 - *barring 8* – incoming calls are allowed, outgoing calls are allowed only for local and private and zone communication;
 - *excluded* – the number is excluded from the numbering schedule. The number is completely excluded from the subscriber number list of the numbering schedule. If this number is called, the call will be rejected with the *no route to destination* cause, or it will be routed to the appropriate prefix in the numbering schedule.



Directions (*local network, special service, zone network, private network, long-distance communication, international communication*) are specified when configuring the prefix in the *Direction* field of the numbering schedule.

Busy lamp field settings (BLF)

- *Allow event subscription* – the BLF (*Busy Lamp Field*) function allows you to monitor the current status of other subscriber lines in real time;
- *Number of subscribers* – the number of subscribers who can monitor the subscriber line status;
- *Monitoring group* – the BLF monitoring group; BLF monitoring is allowed only between the subscribers belonging to the same monitoring group.

Intercom configuration

- *Intercom call type* – the incoming intercom call type (a call with an automatic answer of subscriber B):
 - *One-way* – with an incoming intercom call, subscriber B will hear subscriber A, but subscriber A will not hear subscriber B (one-way notification);
 - *Two-way* – with an incoming intercom call, both subscribers will hear each other;
 - *Normal call* – an incoming intercom call is made as a normal call, without an automatic answer of subscriber B;
 - *Reject* – an incoming intercom call will be rejected;
- *Priority of intercom call* – the priority of an incoming intercom call over other calls;
- *SIP header for intercom* – select a SIP header to be sent to the callee in the INVITE message during an intercom/paging call:
 - Answer-Mode: Auto;
 - Alert-Info: Auto Answer;
 - Alert-Info: info=alert-autoanswer;
 - Alert-Info: Ring Answer;
 - Alert-Info: info=RingAnswer;
 - Alert-Info: Intercom;
 - Alert-Info: info=intercom;
 - Call-Info: =\;answer-after=0;
 - Call-Info: \;answer-after=0;
 - Call-Info: ;answer-after=0;
- *Pause before answering (sec)* – the pause duration before answering an intercom/paging call, which can be transmitted in the "answer-after" header.

VAS Configuration:

- *CLIRO* – a service for overriding the prohibition on caller number identification;
- *VAS activation* – select how VAS services will be activated for dynamic subscribers.
 - *Do not activate* – do not enable VAS services for dynamic subscribers;
 - *Individual selection* – VAS services can be configured for each subscriber individually via the gateway configurator. If this option is selected, the *VAS Activation* table will become available (see section *Subscriber Settings* tab);
 - *Through RADIUS* – for dynamic subscribers, VAS settings will be sent in the RADIUS server responses. For details, see APPENDIX D. TRANSMISSION OF VAS SETTINGS FROM THE RADIUS SERVER FOR DYNAMIC SUBSCRIBERS.

- *VAS reset timeout (days)* – if the subscriber is lost, i. e. if the subscriber no longer registers at the gateway, the VAS services enabled for this subscriber (for example, call forwarding) will continue to be active during this time period.

Monitoring of the Dynamic Subscriber Group

Dynamic subscribers groups

Monitoring ▾

Set subscribers number: 1
Active subscribers number: 0

Search subscriber by number Search

№	State	Group Description	Number	SIP domain	IP/Port	Last registration	Expire in	Select
0	<input type="radio"/>	SubscriberGroup#000			0.0.0.0:0	never registered	00:00:00	<input type="checkbox"/>

10 ▾ Rows in the table to show Current page 1 from 1

Stop registration for whole group Selected: 0

Click the *Search* button to search entries for the subscriber with the specified number.

- *Status* – subscriber registration status (registered, not registered, registration expired);
- *Group name* – arbitrary text description of the group;
- *Number* – the subscriber number;
- *SIP domain* – the domain to which the subscriber belongs;
- *IP/Port* – IP address and port of the subscriber;
- *Last registration* – the time of the last registration;
- *Registration expires* – the time remaining before the registration expiration;
- *Select* – when this option is checked, this entry in the table will be processed when you click the *Reset registration* button;
- *Reset registration* – forcedly reset the registration for a selected subscriber.

Click the *Reset* button to reset the registration of all subscribers in the specified group. You can select a group from the drop-down list.

Management of Dynamic Subscriber Group VAS

Dynamic subscribers groups

VAS management ▾

Search subscriber by number Search

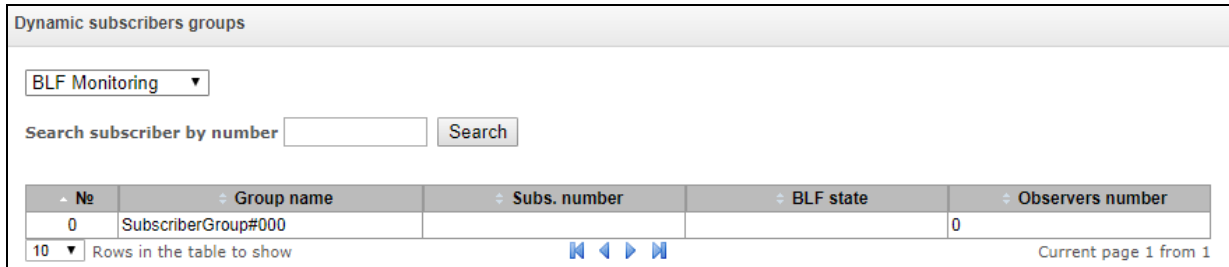
№	Group name	Number	Parameters	Select
10 ▾	Rows in the table to show			Selected: 0 <input type="button" value="Reset VAS"/>

Click the *Search* button to search entries for the subscriber with the specified number.

- *Group name* – arbitrary text description of the group;
- *Number* – the subscriber number;
- *Parameters* – subscriber VAS parameters;
- *Select* – when this option is checked, this entry in the table will be processed when you click the *Reset VAS* button.

Click the *Reset VAS* button to forcibly reset the VAS settings for selected subscribers.

Monitoring of Dynamic Subscriber Group BLF



Click the *Search* button to search entries for the subscriber with the specified number.

- *Group name* – arbitrary text description of the group;
- *Subscriber number*;
- *BLF status* – the current status of the *busy lamp field* service;
- *Number of observers* – the current number of subscribers who monitor the subscriber's line status.

3.1.17.4 PRI subscribers


PRI subscribers are numbers located behind PRI trunk (E1 stream with Q.931 signalling). PRI subscribers are identified by SMG as local subscribers with several subscriber services. Routing for such subscribers are performed without creating additional rules in the numbering plan.

The check of whether the caller is a PRI subscriber or not is carried out by matching of A number and E1 stream Q.931 from which the call was received.



Subscriber settings

- *Subscriber ID* – unique identifier of the subscriber;
- *Name*—arbitrary subscriber text description;
- *Number* – subscriber number for a group of subscribers. The next subscriber will have the number increased by one.
- *E1 stream* – E1 stream, where a call will be routed if the subscriber is called.
- *PBX profile* – select PBX profile (see Section 3.1.8.3 PBX Profiles);
- *Access category* – select access category;
- *Subscriber service mode*— defines restrictions on incoming and outgoing communication for the subscriber:

PRI-Subscribers	
PRI subscriber	
Subscribers count	1 <small>Max subscribers count 199.</small>
Starting description	Subscriber#017
Starting number	
E1 stream	not set
PBX profile	[0] PBXprofile#0
Access category	[0] AccessCat#0
Subscriber service mode 	On
VAS settings	
Enable VAS	<input checked="" type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- Off – out of service. The subscriber number will be in a dial plan, but the subscriber terminal will not be able to register. So, all the incoming calls will be released with "out of order" cause, egress calls will not be initiated.
- ON – enabled, all the types of connections are available.
- Off 1 – ingress communication is enabled, egress communication to the special service only.
- Off 2 – no ingress communication is disabled, egress communication to the special service only.
- denied 1 – ingress and egress communications are prohibited. Calls are routed according to a dialplan but rejected;
- denied 2 – ingress and egress communications are prohibited except for the special services.
- denied 3 – ingress calls are prohibited, egress calls are available;
- denied 4 – ingress calls are barred, egress calls are allowed only within local and departmental communication.
- denied 5 – ingress calls are allowed, egress calls are prohibited.
- denied 6 – ingress calls are allowed, egress calls are allowed only for special services.
- denied 7 – ingress calls are allowed, egress calls are allowed only within local and departmental communication.
- denied 8 – ingress calls are allowed, egress calls are allowed only within local, departmental and zone communication.
- Ignore – excluded from a dial plan. The number is excluded from all the subscriber dial plans. In case of ringing this number, the call will be rejected with "no route destination" cause or will be send to in accordance with prefix in the dial plan.

VAS settings

- Use VAS¹ – VAS connection for a subscriber. When this item is selected, 'VAS activation' table will become available.

¹ This menu is available in the firmware version with SMG-VAS license only, for license details, see Section 3.1.22 Licenses

VAS activation

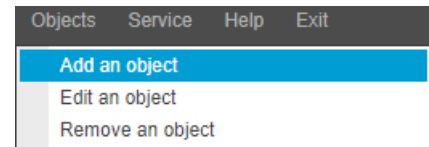
- *Call forward unconditional* — activate call forward unconditional (CF Unconditional) service.
- *Call forward on busy* — activate call forward on busy (CF Busy) service.
- *Call forward on no reply* — activate call forward on no reply (CF No reply) service.
- *Out-of-service redirection* — activate call forwarding on out of service (CF Out Of Service).

VAS activation	
Unconditional redirection	<input type="checkbox"/>
Busy redirection	<input type="checkbox"/>
No-reply redirection	<input type="checkbox"/>
Out-of-service redirection	<input type="checkbox"/>

The detailed description of VAS operation and configuring is presented in APPENDIX K. WORKING WITH VAS SERVICES.

3.1.18 Working with Objects and the Objects Menu

In addition to clicking the create, edit, and remove icons, the corresponding operations with an object can be performed using the *Objects* menu.



3.1.19 Saving Configuration and the Service Menu

To discard all changes, select the *Service – Discard All Changes* menu item.

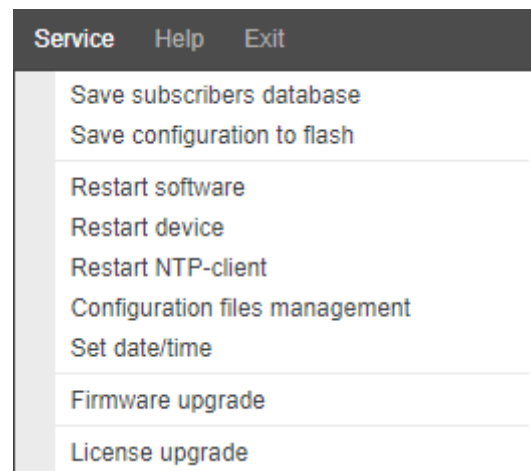
To save the database of registered SIP subscribers, select the *Service – Save subscriber database* menu item.

To write the current configuration into the non-volatile memory of the device, select the *Service – Save Configuration into FLASH* menu item.

To restart the device firmware, select the *Service – Firmware Restart* menu item.

To restart the device completely, select the *Service – Device Restart* menu item.

To perform forced time resynchronisation with the NTP server, select the *Service – NTP Client Restart* menu item.



To restart the client SSHD, select the *Service – SSHD Restart* menu item.

To read/write the main device configuration file, select the *Service – Configuration File Management* menu item.

To configure the local date and time manually, select the *Service – Date and Time Configuration* menu item; see section 3.1.20.

To update the firmware via web configurator, select the *Service – Firmware Update* menu; see section 3.1.21.

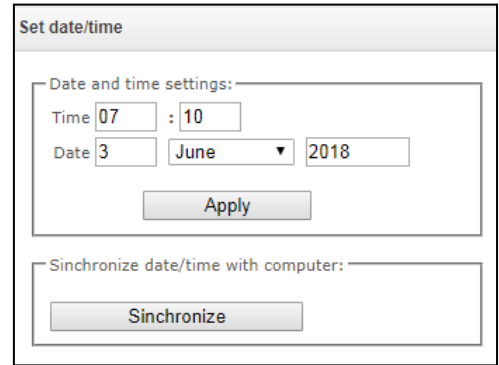
To update/add licenses, select the *Service – License Update* menu item; see section 3.1.22.

3.1.20 Date and Time Settings

The system time and date can be specified in the respective fields in the HH:MM and DD.month.YYYY formats.

To save settings, use the *Apply* button.

Click the *Synchronise* button to synchronise the device system time with the current time on a local PC.



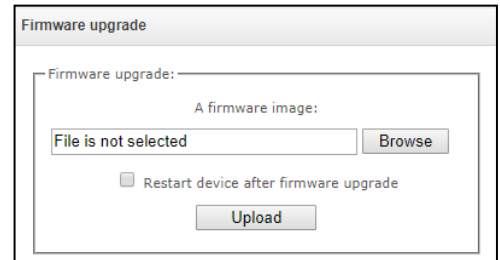
3.1.21 Firmware Update via Web Configurator

To update the device firmware, use the *Service – Firmware Update* menu item.

The firmware file upload form opens.

- *Update Firmware* – updates firmware of the control program and/or Linux kernel.

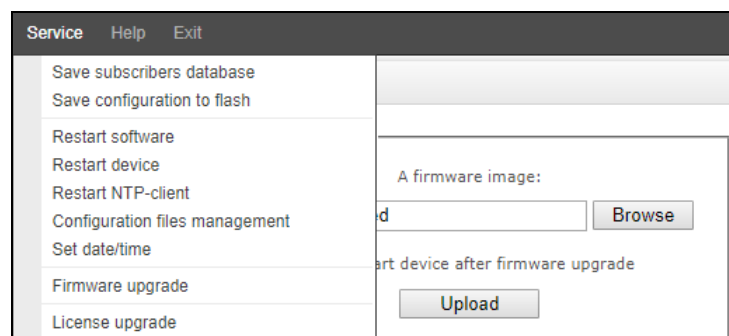
To update the firmware, use the *Browse* button to specify the update file name in the *Firmware File* field and click *Upload*. When the operation is completed, restart the device using the *Service – Device Restart* menu item.



3.1.22 Licenses

To update/add licenses, contact ELTEX Marketing Department by email eltex@eltex-co.ru or phone +7 (383) 274-48-48 to obtain a license file. Specify the serial number and MAC address of your device (see section 3.1.25).

Next, select the *License Update* parameter from the *Service* menu.



Click the *Select File* button to specify the path to the license file obtained from the manufacturer and update it by clicking *Update*.

When the operation is complete, the system prompts you to restart the device. This can also be done manually in the *Service – Device Restart* menu.

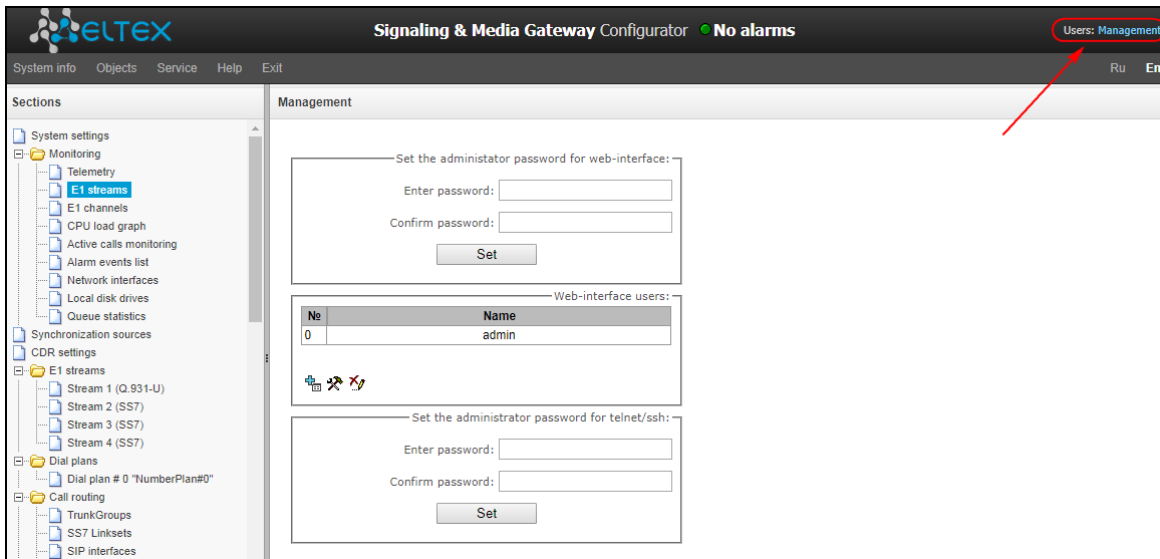
3.1.23 Help Menu

The menu provides information about the current firmware version, factory settings, and other system information.



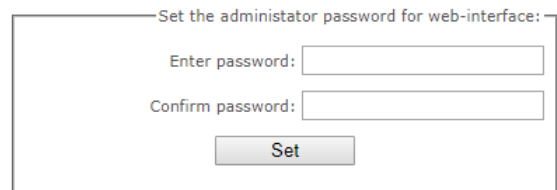
3.1.24 Password Configuration for Web Configurator Access

Use 'Management' menu for work with passwords to access the device via web-configurator, telnet, ssh and user privilege configuration.



Configure the web interface administrator password:

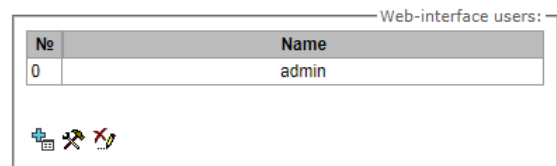
To change the administrator password, enter a new password in the *Enter Password* field and confirm it in the *New Password Confirmation* field. To apply the password, click the *Set* button.



To save the configuration, use the *Service – Save Configuration* menu item.

Web Interface Users:

This section allows configuration of web configurator access restrictions for users. A system administrator can always add or remove users and define their access level. To create, edit, or remove users, use the following buttons:



- Add User;
- Edit User Parameters;
- Remove User.

The program allows neither modification of administrator permissions nor his/her removal from the user list that ensures access to the program for system administrators at any time.

Creating a new user:

- To create a new user, fill in the following fields:
 - user name – the username to log in the web configurator;
 - enter password – the password to access the web configurator;
 - confirm password – used to confirm the password to access the web configurator;

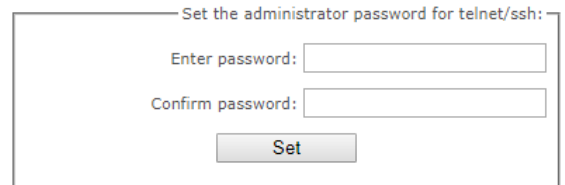
- User rights:
 - Device/Firmware restart — allows you to restart the device and firmware;
 - TDM management (E1 stream) — allows you to set up E1 streams;
 - VoIP management (SIP and H323 interfaces) — allows you to configure SIP and H323 interfaces;
 - Subscriber management - provides the ability to configure SMG subscribers;
 - Management of IP settings, Switch RADIUS — allows you to configure settings of switch, TCP/IP, network services and security;
 - Configuration management — uploading/downloading configuration files;
 - Firmware management — updating the device firmware and license;
 - Recorded calls listening — provides ability to listen recorded calls of the certain category;
 - Call record management — access to call records and to the settings of call recording;
 - Monitoring — access to monitoring sections.

To save the configuration, use the *Service – Save Configuration* menu item.

Configuration of Administrator Password for Telnet and SSH

This section is used to change the password for Telnet, SSH and console access.

To change a password, enter a new password in the *Enter Password* field and confirm it in the *New Password Confirmation* field. To apply the password, click the *Set* button.



3.1.25 View Factory Settings and System Information

To view factory settings and system information, use the *Help – System Information* menu item.

The factory settings are also specified on the label located in the lower part of the device case.



To view the detailed system information (factory settings, SIP adapter version, current date and time, uptime, network settings, internal temperature), click the *Home* link on the control panel.

3.1.26 Configurator Exit

You can exit the Configurator by clicking the *Exit* link.

3.2 Command Line, List of Supported Commands and Keys

SMG features several debug terminals with specific functions:

- *Terminal (com port)* – enable device configuration and firmware update via CLI (command line interface);
- *Telnet port 23* – terminal duplicate (com port);
- *SSH port 22* – terminal duplicate (com port).

System of Commands for SMG Gateway Operation in the Debug Mode

To enter the debug mode, connect to CLI and enter the *tracemode* command.

Table 17 – Debug Mode Commands

help	Show the list of available commands
quit	Exit the debug mode
logout	Exit the debug mode
exit	Exit the debug mode
history	Show the list of previously entered commands
radact [on/off]	Turn RADIUS on/off
radshow	Show the list of requests to the RADIUS server
resolve	Check domain name resolution. Parameter: domain name
rstat	Show the RADIUS protocol operation statistics
q931timers	Show Q.931 timer values
mspping [on/off] <idx>	Enable/disable signal processor querying; idx – signal processor number – 0–5
stream [stream]	Show the status of E1 streams or a specific stream, <i>stream</i> is the stream number (0–15)
e1stat <stream>	Show E1 stream counters
alarm	Show alarm log information
sync	Show information on synchronisation sources
syncfreq	Show information on synchronisation frequency
setsync	Forced synchronisation source change. Parameter: <stream number>
checkmod	Check the number modifier operation for a specific number. Parameters: <modifier table> <the phone number to be checked>
frmtrace	Enable low-level tracing for E1 signal streams. Parameters: <level> <stream number> <usage> – level: l1, l2, l3; – usage: 1 – enabled, 0 – disabled.
cic <linkset>	Show the status of channels in the line group, <linkset> is the number of SS-7 line group
checknum	Check the number with the numbering schedule
cfg_read	Apply the current configuration; this command resets and re-initialises E1 streams
callref	Show information on active SIP calls
rtpdebug <level>	Enable switch RTP debugging; <level> is a debug level WARNING! This command may cause the switch to become unresponsive under load
msscports	Show RTP port status
msscshow <device>	Show the signal processor connection statistics
sipstat	Show the SIP call statistics
sipclrst	Reset the SIP statistics counters
sipreg	Show information about the subscriber/trunk registration. Parameters: <user>, <trunk <self user>>
sipreg user	Show the list of registered subscribers (similar to the reginfo command)
sipreg trunk self	Show information about the SIP trunk registration on the upstream server
sipreg trunk user	Show information about the subscriber registration of SIP interfaces on the upstream server
route	Show information on network routes processed by telephony
showcall	Show information on currently active calls
license	Show information on currently active licenses
mspreglog	Enable the signal processor command tracing
mspunreglog	Disable the signal processor command tracing

talk	Show call statistics
trunk cps	Information on the current number of calls passing through the trunk group per second. Parameters: <idx> – the trunk group number
trunk stat	Information on the current calls passing through the trunk group. Parameters: <idx> – the trunk group number
sys	Show system information, firmware version
hwreboot	Reboot the device
trace	Tracing functions
reginfo	Enter information about registered subscribers
regcon	This command returns to normal operation after the <i>unregcon</i> command (if the application has not terminated abnormally)
unregcon	This command is used in extreme cases to identify the accurate location of the application abnormal termination
stop	Restart the firmware

3.2.1 Tracing Commands Available Through the Debug Port

3.2.1.1 Enable Debugging Globally

Command syntax: **trace start**

3.2.1.2 Disable Debugging Globally

Command syntax: **trace stop**

3.2.1.3 Enable/Disable Debugging for Specific Arguments

Command syntax: **trace <POINT> on/off <IDX> <LEVEL>**

Parameters:

<POINT> argument;
 <IDX> numeric parameter;
 <LEVEL> debug level.

Table 18 – Acceptable Arguments (<POINT>)

Value	Command Description	Value
<i>hwpkt</i>	Tracing of packet contents at the first level of exchange between the main application and the E1 stream driver	0..3
<i>stream</i>	E1 stream tracing	0..3
<i>port</i>	Application operation tracing	Not used.
<i>isup</i>	ISUP subsystem operation tracing in the SS-7 protocol	Not used.
<i>mtp3</i>	MTP3 level operation tracing in the SS-7 protocol for E1 stream	0..3
<i>sipt</i>	SIP/-T/-I protocol operation tracing	Not used.
<i>pril3</i>	DSS1 protocol third level operation tracing for E1 stream	0..3
<i>sw</i>	TDM switch network operation tracing	Not used.
<i>mshpc</i>	IP forwarding tracing	Not used.
<i>mshpd</i>	Signal processor operation tracing	0..7
<i>net</i>	Tracing of the 2 nd layer data network operation	Not used.
<i>sync</i>	Tracing of synchronisation source operation	Not used.
<i>erl1</i>	Low-level tracing of the system that transfers messages between the application and the SIP module	Not used.

<i>erl3</i>	High-level tracing of the system that transfers messages between the application and the SIP module	Not used.
<i>snmp</i>	SNMP protocol operation tracing	Not used.
<i>np</i>	Numbering (routing) schedule operation tracing	Not used.
<i>mod</i>	Modifier operation tracing	Not used.
<i>alarm</i>	Gateway fault state tracing	Not used.
<i>radius</i>	RADIUS protocol operation tracing	Not used.

3.3 SMG Configuration via Telnet, SSH, or RS-232

To configure the device, connect to it via the Telnet or SSH protocol, or by the RS-232 cable (for access via CLI). Factory settings for IP address: **192.168.1.2**; mask: **255.255.255.0**.

Modifications made to configuration via CLI (command line interface) or the web configurator will be applied immediately.

To save the configuration into the non-volatile memory of the device, execute the **copy running_to_startup** command.

Initial startup username: **admin**, password: **rootpasswd**.

Given below is a complete list of commands sorted in the alphabetic order.

3.3.1 List of CLI Commands

Table19 – CLI Commands

Command	Parameter	Value	Action
?			Show the list of available commands
alarm global			Show information on the current faults
alarm list clear			Clear the fault event log
alarm list show			Show the fault event log with fault type and status, occurrence time, and localisation parameters.
CPU load statistic			Show CPU load for the last minute
date	<DAY> <MONTH> <YEAR> <HOURS> <MINS>	1-31 1-12 2011-2037 00-23 00-59	Set the device local date and time
exit			Terminate this CLI session
firmware update tftp	<FILE> <SERVERIP>	firmware file name IP address in the AAA.BBB.CCC.DDD format	Firmware update without automatic gateway restart <i>FILE</i> – firmware file name <i>SERVERIP</i> – IP address of the TFTP server:
firmware update ftp	<FILE> <SERVERIP>	firmware file name IP address in the AAA.BBB.CCC.DDD format	Firmware update without automatic gateway restart <i>FILE</i> – firmware file name <i>SERVERIP</i> – IP address of the FTP server
firmware update usb	<FILE>	firmware file name	Firmware update without automatic gateway restart

			<i>FILE</i> – firmware file name
firmware update_and_reboot tftp	<FILE> <SERVERIP>	firmware file name IP address in the AAA.BBB.CCC.DDD format	Firmware update with automatic gateway restart <i>FILE</i> – firmware file name <i>SERVERIP</i> – IP address of the TFTP server:
firmware update_and_reboot ftp	<FILE> <SERVERIP>	firmware file name IP address in the AAA.BBB.CCC.DDD format	Firmware update with automatic gateway restart <i>FILE</i> – firmware file name <i>SERVERIP</i> – IP address of the FTP server
firmware update_and_reboot usb	<FILE>	firmware file name	Firmware update with automatic gateway restart <i>FILE</i> – firmware file name
history			Show the history of entered commands
license check	<LICENSE>	SMG-PBX-2000/ SMG-SORM/ SIP-PBX-Demo/ SMG-PBX-3000/ SMG-H323/ SMG-RCM/ SMG-VAS-500/ SMG-DEMO	Check the license availability for the device (<i>License installed</i> – license is installed; <i>License NOT installed</i> – license is not installed)
license download	<FILE> <SERVERIP>	License file name Server IP address in the AAA.BBB.CCC.DDD format	Download a license file from the specified address
license update			Update the licence
license reset	no/yes		Delete all installed licenses
number check	<NUMPLAN> <NUMBER> <COMPLETE>	0-15/0-255 String, 31 characters max. yes/no	Check routing capability for this number The check is performed by the caller and callee masks and also in the configured SIP and PRI subscriber database. The check provides information on routing capability for this number in the specified numbering schedule: <i>calling-table</i> – routing by the caller table; <i>called-table</i> – routing by the callee table; <i>NOT found in</i> – routing by this table is not possible; <i>found in</i> – routing by this table is possible; <i>SIP/PRI abonent ID[11] index [0]</i> – SIP/PIR subscriber [subscriber's ID][entry number for this subscriber in the database]; <i>FXS port [10]</i> – FXS subscriber [FXS port number] <i>Prefix index [6]</i> – routing by a prefix [the prefix number in the list].
password			Change access password via CLI
quit			Terminate this CLI session
reboot	<YES_NO>	yes/no	Reboot the device
save			Write the current configuration into the non-volatile memory of the device

sh			Go to Linux Shell from CLI
sntp retry			Send an SNTP request to the server for time synchronisation
tcpdump	<DEVICE> <FILE> <SNAPLEN>	eth0/eth1/local string 0-65535	Capture packets from the Ethernet device <i>DEVICE</i> – an interface for monitoring <i>FILE</i> – a file for packet writing <i>SNAPLEN</i> – the number of bytes captured from each packet (0 – the entire packet is captured).
tftp put	<LOCAL_FILE> <REMOTE_FILE> <SERVERIP>	string string IP address in the AAA.BBB.CCC.DDD format	Get a file via TFTP. This command is used to download the tracings made by the <i>tcpdump</i> and <i>pcmdump</i> commands
tracemode			Enter the tracing mode

3.3.2 Changing Device Access Password via CLI

Since the gateway allows remote connection via Telnet, it is recommended to change the **admin** password to avoid unauthorised access.

To do this:

1. Connect to the gateway via CLI, authorise using login/password, enter the *password* command, and press <Enter>.
2. Enter a new password:

New password:

3. Confirm the entered password:

Retype password:

Password changed (Password for admin changed by root)

4. Save the configuration into Flash: enter the *save* command and press <Enter>.

4.1 Go to the configuration mode using the **config** command.

4.2 Enter **"copy running_to_startup"** command

4.3 Press <Enter> key

APPENDIX A. CABLE CONTACT PIN ASSIGNMENT

For SMG-200:

Table A1 – Assignment of **RJ-11** Connector Pins for the FXS Port

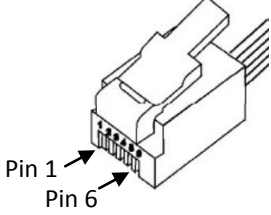
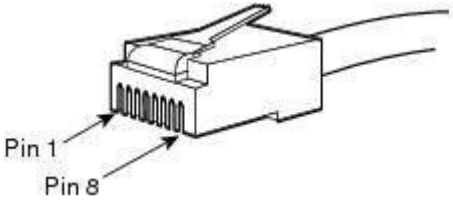
Contact Pin No. (Pin)	Assignment	Contact Pin Numbering
1	Not used	
2	Not used	
3	to connect FXS/FXO	
4	to connect FXS/FXO	
5	Not used	
6	Not used	

Table A2 – Assignment of **RJ-45** Connector Pins for the Console Port

Contact Pin No. (Pin)	Assignment	Contact Pin Numbering
1	Not used	
2	Not used	
3	TX	
4	Not used	
5	GND	
6	RX	
7	Not used	
8	Not used	

APPENDIX B. ALTERNATIVE FIRMWARE UPDATE METHOD

1. Running backup firmware on the device via RS-232 and TFTP

If the device does not start correctly, you can start the backup firmware over the network via TFTP by sending commands to the device over the RS-232 interface.

This requires the following tools:

- Terminal program (for example, TERATERM);
- TFTP server program.

To run the backup firmware on the device, make the following steps:

1. Connect to the Ethernet port of the device;
2. Connect the PC COM port to the device console port using a crossed cable;
3. Run the terminal program;
4. Configure data transmission rate: 115200, data format: 8 bit w/o parity, 1 stop bit, w/o flow control;
5. Run the *tftp* server program on the PC and specify the path to the *smg200_files* folder. Create the *smg200* subfolder in the folder and place there the *smg200_kernel*, *smg200_initrd* files (the computer that runs the TFTP server and the device should be located in the same network);



For SMG-500, the file names will be *smg500_kernel*, *smg500_initrd*, *smg500_devtree*, respectively.

6. Turn the device on and, when the *Autoboot in 3 seconds* message appears in the terminal program window, stop the startup sequence by entering the *stop* command:

```
UU-Boot 2017.03-armada-17.06.3-gbddd5b3 (Dec 12 2017 - 14:43:45 +0700)

Model: Eltex Ltd SMG-200 board
Clock: CPU      1200 [MHz]
      DDR       800  [MHz]
      FABRIC    800  [MHz]
      MSS       200  [MHz]
DRAM:  2 GiB
U-Boot DT blob at : 000000007faee7d8
Comphy-0: SATA1      5 Gbps
Comphy-1: SGMII2     1.25 Gbps
Comphy-2: SGMII0     1.25 Gbps
Comphy-3: SGMII1     1.25 Gbps
Comphy-4: IGNORE
Comphy-5: IGNORE
UTMI PHY 0 initialized to USB Host0
UTMI PHY 1 initialized to USB Host1
NAND:  0 MiB
MMC:   sdhci@6e0000: 0, sdhci@780000: 1

Net:   eth0: mvpp2-0, eth1: mvpp2-1 [PRIME], eth2: mvpp2-2
Autoboot          in              3              seconds
stop
smg200>>
```

7. Enter *set ipaddr <device IP address> <ENTER>*;
8. Enter *set netmask <device network mask> <ENTER>*;
9. Enter *set serverip <IP address of the computer which runs the TFTP server> <ENTER>*;

```
smg200>> setenv ipaddr 192.168.2.2
```



```
smg200>> setenv netmask 255.255.255.0
smg200>> setenv serverip 192.168.2.5
```

10. Startup the device using the *run netboot* command:

```
smg200>> run netboot
TFTP from server 192.168.2.5; our IP address is 192.168.2.2
Filename 'smg200/smg200_kernel'.
Load address: 0x5000000
Loading: #####
...

TFTP from server 192.168.2.5; our IP address is 192.168.2.2
Filename 'smg200/smg200_devtree'.
Load address: 0x4f00000
Loading: #####

...

TFTP from server 192.168.2.5; our IP address is 192.168.2.2
Filename 'smg200/smg200_initrd'.
Load address: 0x8000000
Loading: #####
...

## Loading init Ramdisk from Legacy Image at 08000000 ...
Image Name: smg200 Ramdisk
Image Type: AArch64 Linux RAMDisk Image (gzip compressed)
Data Size: 21910437 Bytes = 20.9 MiB
Load Address: 00000000
Entry Point: 00000000
Verifying Checksum ... OK
## Flattened Device Tree blob at 04f00000
Booting using the fdt blob at 0x4f00000
Loading Ramdisk to 7e607000, end 7faec3a5 ... OK
Using Device Tree in place at 0000000004f00000, end 0000000004f09b72

Starting kernel ...
```

11. After starting the device, you can update the firmware as described in section 3.1.21.

APPENDIX C. CALCULATION OF TELEPHONE LINE LENGTH

Table C1– DC resistance of subscriber’s cable lines depending on the cable type, at 20°C ambient temperature, per km of cable line¹

Cable brand for SL UTN (subscriber lines of urban telephone network)	Core diameter , mm	Electrical resistance per km of the line, Ω, max	Line length (other telephone sets) with the extended range mode on, km	Line length (other telephone sets) with the extended range mode off, km
ТПП, ТППэн, ТППЗ, ТППэнЗ, ТППБ, ТПП энБ, ТППЗБ, ТППБГ, ТППэнБГ, ТППББШп, ТППэнББШп, ТППЗББШп, ТППЗэнББШп, ТППт	0.32	458.0	1.638	0.983
	0.40	296.0	2.534	1.520
	0.50	192.0	3.906	2.344
	0.64	116.0	6.466	3.879
	0.70	96.0	7.813	4.688
ТПВ, ТПЗБГ	0.32	458.0	1.638	0.983
	0.40	296.0	2.534	1.520
	0.50	192.0	3.906	2.344
	0.64	116.0	6.466	3.879
	0.70	96.0	7.813	4.688
ТГ, ТБ, ТБГ, ТК	0.40	296.0	2.534	1.520
	0.50	192.0	3.906	2.344
	0.64	116.0	6.466	3.879
	0.70	96.0	7.813	4.688
ТСтШп, ТАШп	0.50	192.0	3.906	2.344
	0.70	96.0	7.813	4.688
ТСВ	0.40	296.0	2.534	1.520
	0.50	192.0	3.906	2.344
КСПЗП	0.64	116.0	6.466	3.879
КСПП, КСПЗП, КСППБ, КСПЗПБ, КСППт, КСПЗПт, КСПЗПК	0.90	56.8	13.204	7.923

Calculation of the telephone line length for different cable types²:

- 1 Cable resistance at 20°C

$$R_{cab} = L_{cab} * R_{sp20};$$

where:

R_{sp20} [Ω/km] – DC specific resistance of the cable at 20°C; see the table in APPENDIX C. CALCULATION OF TELEPHONE LINE LENGTH).

- 2 Cable length

$$L_{cab} = R_{cab} / R_{sp20} \text{ [km]}$$

- 3 Loop resistance at 20°C

¹ Line length values for the RUS telephone set will be lower that those indicated in the table

² Taken from the website <http://izmer-ls.ru/shle.html>

$$L_{lp} = 2 * L_{cab}$$

$$R_{lp} = L_{lp} * R_{sp20} = 2 * L_{cab} * R_{sp20};$$

$$L_{lp} = R_{lp} / R_{sp20}.$$

For telephone lines, the loop resistance takes into account the telephone set resistance: 600 Ω .

APPENDIX D. TRANSMISSION OF VAS SETTINGS FROM THE RADIUS SERVER FOR DYNAMIC SUBSCRIBERS

The gateway can transmit the VAS settings to dynamic subscribers using the RADIUS server commands in response to RADIUS-Authorisation requests during the registration. The commands are sent in the text format using the Vendor-Specific attribute (see section 3.1.14.3), with the ELTEX vendor number set to 35265 and the Eltex-AVPair attribute name set to 1.

In general, the Eltex-AVPair attribute format is as follows:

```
Vendor-Specific(26) : Eltex(35265) : Eltex-AVPair(1) : <$COMMAND-STRING>
```

Using various commands in the \$ COMMAND-STRING string, you can send the following parameters:

- enable/disable VAS for dynamic subscribers;
- settings for activated services (numbers for call forwarding, the number of BLF subscribers);
- disable all VAS for a subscriber.

Requests Syntax

The command consists of an initial text command identifier, a VAS activation/deactivation identifier for configuration, and a configuration command.

- "UserService:" – a text identifier specifying that this attribute contains a VAS management command.
- "CFU=", "CFB=", "CFNR=", "CFOS=", "CT", "CallPickup=", "BLF=", "Intercom=", "Conf=", "3PTY=", "ClearAll=" – the identifier of enabled/disabled VAS, may take yes/no values to enable/disable VAS respectively.
 - CFU – Call Forwarding Unconditional;
 - CFB – Call Forwarding Busy;
 - CFNR – Call Forwarding No Reply;
 - CFOS – Call Forwarding Out of Service;
 - CT – call transfer;
 - CallPickup – call pickup;
 - BLF – Busy Lamp Field (BLF);
 - Intercom – access to intercom and paging calls;
 - Conf – ad-hoc conference;
 - 3PTY – three-way conference;
 - ClearAll – access to *Cancel all services*.
- "numCFU=", "numCFB=", "numCFNR=", "numCFOS=" – the *Call Forwarding* VAS configuration commands, subscriber's listed phone number used for call forwarding may be sent as a value.
- "limitBLF=" – the *Busy lamp field (BLF)* VAS configuration command; the number of subscribers can be sent as a value.
- "CT=", "CallPickup=", "Intercom=", "Conf=", "3PTY=", "ClearAll=" – these commands do not have any additional settings.
- "UserService: none" – disable VAS for a subscriber.



If some VAS service has been activated for the subscriber, i. e. the VAS activation/deactivation ID with the “yes” value has been sent, then this service can be deactivated only by sending the “no” value for this subscriber. If some VAS service has been activated, but subsequent messages from the RADIUS server do not contain information about the activated VAS, the service is considered active until the “no” value is sent.

If some VAS services have been activated for a subscriber and after some time the subscriber becomes inactive (the device registration timeout has expired), their VAS are considered active until the “UserService:none” value is sent for the subscriber.

After the device reboot, VAS activated for the subscriber remain active.

Examples of service activation

Objective 1

Activate the following services for a subscriber: *Call Forwarding Unconditional* to number 12345, *Call Forwarding No Reply* to number 56789, and *Call Pickup*.

Actions

You need to submit the following request:

```
UserService:CFU=yes;numCFU=12345;CFNR=yes;numCFNR=56789;CallPickup=yes"
```

Objective 2

Deactivate the *Call Forwarding Unconditional* and *Call Pickup* services, and activate the *BLF for 10 subscribers* and *Call Transfer* services for a subscriber.

Actions

You need to submit the following request:

```
UserService:CFU=no;CallPickup=no;CT=yes;BLF=yes;limitBLF=5;
```

APPENDIX F. CORRELATION BETWEEN ROUTING, SUBSCRIBERS, AND SIGNAL LINK PARAMETERS

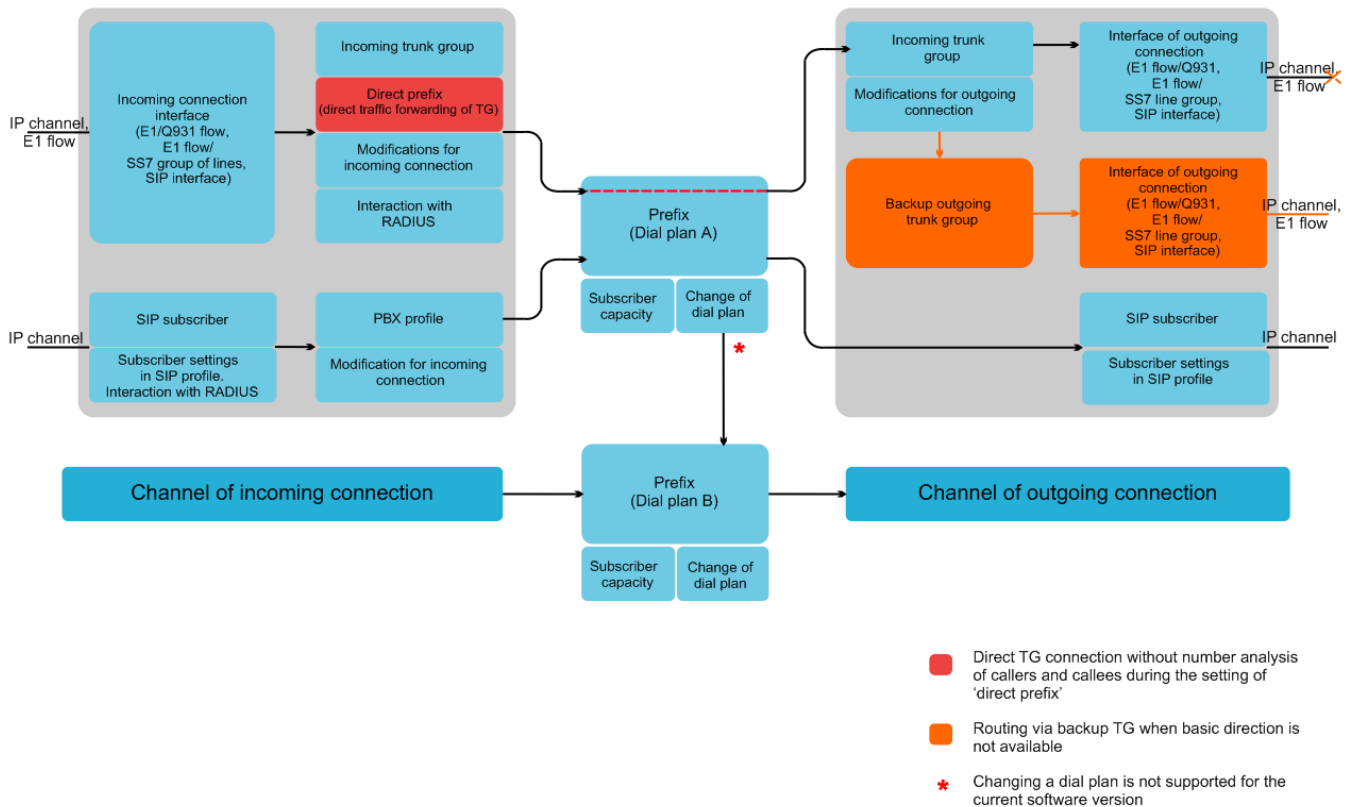


Fig. 20 – Correlation between routing, subscribers and signal link parameters

An incoming call from an IP or TDM channel arrives to the incoming interface, then the further call routing is determined in a trunk group (TG) using the RADIUS protocol (if applicable). In TG, number modifications for incoming communication are performed. After that, the call is routed by prefix into the outgoing channel or to a SIP subscriber. If a “direct prefix” is configured in the incoming TG, the call is routed to the outgoing TG configured in the prefix parameters without caller and callee number analysis. In the outgoing TG, the number modifications are performed. After that, the call arrives to the outgoing interface/channel. If the outgoing direction is not available, the call will be directed to the backup direction (if configured).

An incoming call from a SIP subscriber arrives to the inbound SIP interface (SIP profile), and then the possibility of further call routing is determined in the profile using RADIUS protocol (if applicable). The call is routed by prefix into the outgoing channel or to a SIP subscriber through the PBX profile that is used for number modification. In the outgoing TG, the number modifications are performed. After that, the call arrives to the outgoing interface/channel. If the outgoing direction is not available, the call will be directed to the backup direction (if configured).

To set the numbering capacity of the SMG gateway, use the *subscriber capacity* modifier for the prefix. These numbers will belong to the gateway, although they may not be assigned to subscribers.

APPENDIX G. GUIDELINES FOR SMG OPERATION IN A PUBLIC NETWORK

During SMG operation in a public network, you should take all security measures in order to avoid the device password brute forcing, DoS (DDoS) attacks, and other intrusive actions that may lead to unstable operation, subscriber data theft, attempts to perform calls at the expense of other subscribers, and consequently to damages to the service provider as well as subscribers.

Avoid using SMG in a public network without additional protective measures like session border controller (SBC), firewall, etc.

Guidelines for SMG Operation in a Public Network

- Operation in a public network with the default SIP signalling port 5060 is not recommended. To change this, modify the *Port for SIP signalling reception* parameter in the *SIP interfaces* settings in SIP general configuration and SIP interface settings¹. This setting will not ensure complete protection as the signalling port may be discovered during port scanning.

- If IP addresses of all devices communicating with SMG are known, use the built-in firewall (static firewall) to configure the rules allowing access for these addresses and deny the access for all other ones. The allowing rules should be placed first in the list of rules.

You should also configure the dynamic firewall.

The dynamic firewall stores unsuccessful SIP protocol access attempts in a log file (/tmp/log/pbx_sip_bun.log), and if the number of such attempts exceeds a defined value, the IP address that has originated them will be banned for the specified time. The utility also allows generation of lists for trusted and untrusted addresses. For detailed description, see section 3.1.12.2.

¹ The function is available starting from RC14 version.

APPENDIX H. VOICE MESSAGES AND MUSIC ON HOLD (MOH)

The device contains some pre-recorded voice messages and music to be played on hold (MOH). The messages are triggered in response to specific events. The list of messages and corresponding events is presented in the table below.

Table H1 – MOH Messages and Events

Name	Meaning	Event
TRUNK_BUSY	This direction is overloaded	No free channels for the outgoing direction. Outgoing channels are blocked or out of service. When receiving Q.850 cause = 34
NUMBER_FAIL	You have dialled the wrong number	When calling to a non-existent prefix When receiving Q.850 cause = 3,28
ACCS_DENIED_TEMP	The number cannot be called temporarily	When you call to an unregistered subscriber When receiving Q.850 cause = 27
ACCESS_RESTRICT	This type of communication is not enabled for your device	Restriction of incoming calls for the subscriber Restriction of calls by access category When receiving Q.850 cause = 21
USER_UNALLOCATED	The subscriber's device is not connected to the station	When calling to a "modifier" type prefix When receiving Q.850 cause = 1
USER_CHANGE	The subscriber has changed the number	When receiving Q.850 cause = 22
MOH	Music on hold	When putting the subscriber on hold

The voice messages can be managed in the trunk group settings and PBX profile settings for subscribers.

The MOH message is issued unconditionally, regardless of the settings.

APPENDIX K. WORKING WITH VAS SERVICES

Starting from the firmware version 2.15.01, the device supports the following VAS services:

- *Call Forwarding Unconditional* – enable the Call Forwarding Unconditional (CF Unconditional) service;
- *Call Forwarding Busy* – enable the Call Forwarding Busy (CF Busy) service;
- *Call Forwarding No Reply* – enable the Call Forwarding No Reply (CF No Reply) service;
- *Call Forwarding Out of Service* – enable the Call Forwarding Out of Service (CF Out Of Service);
- *Call hold*;
- *Call transfer* – enable the Call Transfer service;
- *3Way conference*.
- *Call pickup*;
- *Conference with consequent assembly (CONF)*.
- *Disconnect conference by initiator* – when check, the conference will be over when the initiator leaves the conference. Otherwise, the conference will be saved after the initiator is hung up and will be over only when the last participant leaves the conference.
- *Password change (PWD)*;
- *Restrict outgoing communication (Out calls restrict)*;
- *Outgoing communication by password (PWD ACT)*;
- *Password activation (RBP)*;
- *Do not disturb (DND)*;
- *Blacklist*;
- *Follow me*
- *Follow me (no response)*
- *Cancel all services*.

VAS functionality becomes available only when the additional SMG-VAS license is installed.

For a subscriber to be able to use the VAS services, select the *Use VAS* checkbox in the subscriber settings.

To enable a particular VAS service, select the checkbox for the needed service in the *VAS Activation* menu.

SIP subscriber		VAS activation	
Subscribers count	1 <small>Max subscribers count 194.</small>	Unconditional redirection	<input type="checkbox"/>
Starting description	Subscriber#021	Busy redirection	<input type="checkbox"/>
Starting number		No-reply redirection	<input type="checkbox"/>
Starting CallerID number		Out-of-service redirection	<input type="checkbox"/>
Use CallerID number for redirection	<input type="checkbox"/>	Call hold	<input type="checkbox"/>
Calling party number type	Subscriber	Call transfer	<input type="checkbox"/>
Calling party category (RUS)	1	3WAY conference	<input type="checkbox"/>
Lines operation mode	Common	Call pickup	<input type="checkbox"/>
Lines number	1	Change password	<input type="checkbox"/>
IP-address:port	0.0.0.0 : 0	Outgoing calls restriction	<input type="checkbox"/>
Allow unregistered calls	<input type="checkbox"/>	Restricted by password	<input type="checkbox"/>
SIP domain		Password activation	<input type="checkbox"/>
SIP profile	not set	Follow me	<input type="checkbox"/>
PBX profile	[0] PBXprofile#0	Follow me (no response)	<input type="checkbox"/>
Access category	[0] AccessCat#0	Reset all services	<input type="checkbox"/>
Dial plan	[0] NumberPlan#0		
Authorization	not set		
Login			
Password			
Ignore source port after registration	<input type="checkbox"/>		
Subscriber service mode	On		
Display name			
Use display name	Received only		
Busy-Lamp-Field (BLF) settings			
Enable subscription	<input type="checkbox"/>		
Max subscribers number	10		
Monitoring group	0		
VAS settings			
CLIRO	<input type="checkbox"/>		
Enable VAS	<input checked="" type="checkbox"/>		

1. Working with *Call Hold*, *Call Transfer* and *Three-way Conference* Services

The *Call transfer* service requires that the subscriber terminal supports FLASH transfer via SIP using SIP-INFO and RFC2833 methods. Also, the subscriber terminal should have the signal transmission function configured using inband, SIP-INFO or RFC2833 DTMF methods. Make sure that the same method is selected in the subscriber SIP profile setting.

Configuration of the Call Transfer service: example

Subscriber A calls to subscriber B. During the call, subscriber B presses FLASH to put subscriber A on hold. During this time on-hold, subscriber A receives the *Music on hold* signal, while subscriber B

hears the *Station response* signal. At that time, the timeouts for dialling the subscriber C are activated, with the values indicated below. After dialling and getting an answer from subscriber C, the following options are available:

While being in a call subscriber A, put him on hold with short clearback flash (R), wait for the *Station response* signal and dial subscriber C number. When Subscriber C answers,, the following operations are possible:

- R 0 – disconnect the subscriber on hold, connect with the subscriber on line;
- R 1 – disconnect the subscriber on line, connect with the subscriber on hold;
- R 2 – switch to another subscriber (change the subscriber);
- R 3 – three-way conference;
- R 4 – call transfer. A voice call connection is established between subscribers A and C;
- Clearback – call transfer; voice call connection is established between subscribers A and C.

Timeout for the *Call Transfer* service – currently, only default values are set; these timeouts will become configurable in the following firmware versions:

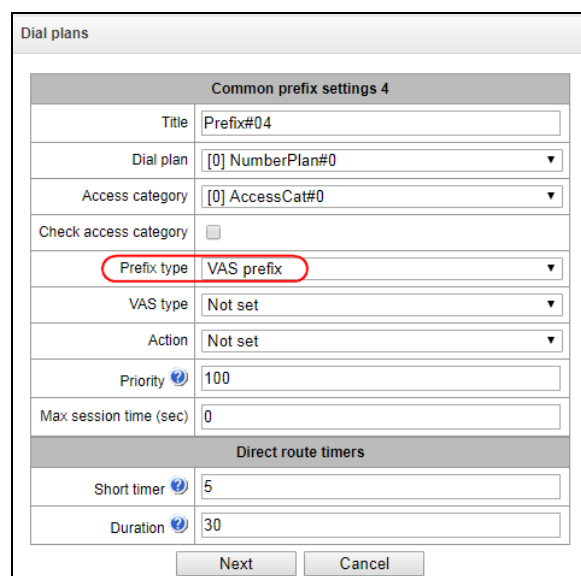
- first digit dial timeout: 15 seconds
- next digit dial timeout: 5 seconds
- busy signal timeout: 60 seconds

2. Working with the Call Forwarding service

The call forwarding service can be configured using the appropriate web-configurator settings in the *SIP Subscribers/VAS Management/Select Subscriber* menus (section 0) or by managing the VAS services from the telephone set (according to RD-45). This method is described below.

VAS configuration from the telephone set (according to RD-45)

The subscriber can enable/disable the service themselves by dialling certain prefixes on their telephone set. The call forwarding service prefixes are configured in the numbering schedule (section 3.1.6 Numbering Schedule). To do this, add a new prefix with the *Prefix Type* value set to *VAS Prefix*.



Common prefix settings 4	
Title	Prefix#04
Dial plan	[0] NumberPlan#0
Access category	[0] AccessCat#0
Check access category	<input type="checkbox"/>
Prefix type	VAS prefix
VAS type	Not set
Action	Not set
Priority	100
Max session time (sec)	0
Direct route timers	
Short timer	5
Duration	30
<input type="button" value="Next"/> <input type="button" value="Cancel"/>	

We recommend using the following prefix values for VAS services:

Call Forwarding Unconditional (CF Unconditional):

- activation (*21* | *21*x.#);
- deactivation (#21#);
- control (*#21* | *#21*x.#).

Call Forwarding Busy (CF Busy):

- activation (*22* | *22*x.#);
- deactivation (#22#);
- control (*#22* | *#22*x.#).

Call Forwarding No Reply (CF No reply).

- activation (*61* | *61*x.#);
- deactivation (#61#);
- control (*#61* | *#61*x.#).

Call Forwarding Out of Service (CF Out Of Service)

- activation (*62* | *62*x.#);
- deactivation (#62#);
- control (*#62* | *#62*x.#).

Digits 21, 22, 61, 62 may take up any value. These examples use the recommended values.



The numbering schedule of the subscriber terminal should contain prefixes for the VAS management. The gateway starts working with VAS services after receiving an INVITE message with the required combination of digits from the subscriber terminal.

Timeouts for the *Call Forwarding* service – currently, only default values are set; these timeouts will become configurable in the following firmware versions:

- Call Forwarding No Reply (CF No Reply) timeout: 10 seconds;
- Call Forwarding Out of Service (CF Out Of Service) timeout: 10 seconds

Example of VAS configuration from the telephone set

Objective

The subscriber needs to assign unconditional forwarding to number 222333444.

Actions

- The subscriber activates the service by dialling *21* and hears the *station response* signal.

- To check the service activation, the subscriber should dial *#21*. If the service is active, the subscriber hears the *station response* signal. If the service is inactive, the subscriber hears the *busy* signal.
- The subscriber defines the call forwarding number by dialling *21* 222333444# and hears the *station response* signal.
- To check whether the service has been activated for the specific number, the subscriber should dial *#21*222333444#. If the service is activated and the dialled number matches the previously defined number, the subscriber will hear the *station response* signal. If the service is not activated or the dialled number does not match the previously defined number, the subscriber will hear the *busy* signal.

To deactivate the service, the subscriber should dial #21#.

3. Conference with consequent participant assembly

This service allows the initiator to establish the conference by consequently adding participants using subscriber hold feature.

Upon the initiator clearback, participants will hear the *busy* tone. Maximum number of conference participants—40.

Access to service is governed by the 'Conference with consequent assembly' VAS category checkbox.

Usage	* 71# <NUMBER 1><CONF> R<NUMBER 2><CONF> ...
-------	--

where:

<NUMBER N>—number of the subscriber participating in a conference.

<CONF>—conference call state

R—short clearback (FLASH).

4. Call pickup

The service allows you to answer the call directed to another subscriber.

The service access is controlled by selecting the checkbox for the *Call Pickup* category.

Use	* 66 * <NUMBER> #
-----	-------------------

<NUMBER> – subscriber number for call pickup.

5. Password activation/deactivation, outgoing communication by password

Using these services, the subscriber can override the service access restrictions, i. e. the restrictions set by the *Restrict outgoing communication* service.

For example, if restrictions on outgoing communication are set, the subscriber, using the *Outgoing communication by password* service can bypass the access restriction only for the next attempt to establish an outgoing connection. The *Password activation/deactivation* service disables/enables the outgoing communication restriction for all subsequent attempt to establish an outgoing connection.

The service access is controlled by the checkbox in the *Password activation/deactivation* VAS category.

To access the *Outgoing communication by password* service, select the checkbox for this VAS service category.

Password code – activation	* 29 * <PASSWORD> #
Password code – deactivation	# 29 #
Outgoing communication by password	* 32 * <PASSWORD> #

<PASSWORD> – a personal password code of the subscriber.

6. Password Change

Using this service, the subscriber can change the password code assigned by the PBX personnel. The service access is controlled by the checkbox for the *Password change* VAS category.

Change	* 30 * <PASSWORD1> * <PASSWORD2> * <PASSWORD2> #
--------	--

<PASSWORD1> – the current password code;

<PASSWORD2> – the new password code, the user needs to dial it twice. The password code should consist of four digits.

7. Do not disturb

The service allows you to prevent ingress calls. However, it is possible to assign a white list of numbers of subscribers who will be able to make a call, even in the "do not disturb" mode.

Access to the service is controlled by the "*do not disturb*" check box of VAS category.

Service order	* 26 #
Service cancellation	# 26 #
Control	* # 26 #
Add number to white list	* 26 * <NUMBER>
To delete a number from white list	# 26 * <NUMBER>

8. Blacklist

The service allows you to prohibit calls to the subscriber from certain numbers.

Access to service is governed by the '*Black list*' category check box.

Service order	* 61 * <PASSWORD> #
Service cancellation	# 61 * <PASSWORD> #
Control	* # 61 * <PASSWORD> #
Add number to blacklist	* 61 * <PASSWORD> * <NUMBER>
Remove number from blacklist	# 61 * <PASSWORD> * <NUMBER>

9. Restrict outgoing communication

The service allows setting access restriction for certain types of outgoing communication from the subscriber's telephone set. To use this service, the following communication groups are defined:

Group 1 – connection only with the special services;

Group 2 – connection with the special services and local communication;

Group 3 – the types of calls defined in groups 1 and 2 and zone calls.

The connection type is specified in the prefix parameters.

To override the restriction set by this service, you can use the *Outgoing communication by password* and the *Password code – Activation* services. To restore the restriction removed by the *Password code – Activation* service, use the *Password code – Deactivation* service.

The service access is controlled by the checkbox for the *Restrict outgoing communication* VAS category.

Ordering the service	* 34 * <PASSWORD> * N #
Cancelling the service	* 34 * <PASSWORD> #
Control	* #34 * <PASSWORD> #

<N> – group number for allowed communication types.

10. Follow Me service

With the *Follow me* service, you can enable call forwarding for all calls from your telephone set to a remote one, using the remote phone. Service use example: a subscriber located outside their workplace wants to activate call forwarding for all calls from their work telephone set to a telephone set which is now “at hand”.

Use

Service activation:

The service involves two telephone sets: local and remote. The subscriber wants to forward all calls from the local telephone set to the remote telephone set. To do this, first of all, the subscriber should activate the service with or without PIN on the local telephone set (i. e. while being in the workplace he should enable the use of the service). After that, the subscriber, using their remote phone, can enable call forwarding from the local telephone set to the remote telephone set (if the service activation involved a PIN code, then you will have to enter the PIN; otherwise, the PIN is not needed).

Service deactivation:

Remote call forwarding can be turned off from both remote and local telephone sets. You can deactivate the service only from the local telephone set, with or without a PIN-code.

Service management from the telephone set:

The service activation with a temporary PIN code is performed on the local number	*23*PIN#
The service activation without a PIN code is performed on the local number	*23#
Call forwarding from the local to the remote telephone set with a temporary PIN is performed on the remote number	* 23 * PIN * LOCAL_PHONE #
Call forwarding from the local to the remote telephone set without a PIN code is performed on the remote number	* 23 ** LOCAL_PHONE#
Cancelling call forwarding from the local to the remote telephone set without a temporary PIN code is performed on the remote number	#23**LOCAL_PHONE#
Cancelling call forwarding from the local to the remote telephone set with a temporary PIN code is performed on the remote	#23*PIN*LOCAL_PHONE#

number	
Deactivation, is performed on the local number	#23#
Status view, is performed on the local number	*#23#

where

- PIN – a secret digital code consisting of 4–12 characters;
- LOCAL_PHONE – the phone number from which the calls will be forwarded.

11. Follow Me (no response) service

Using the *Follow me (no response)* service, you can forward all calls from the local number to the remote number, if a call to the local number has not been answered within the specified time interval.

Use

The service involves two telephone sets: local and remote. The subscriber wants all calls that come to the local phone and have not been answered within the specified time interval, to be forwarded to the remote telephone set. Activation/deactivation of the service is performed only on the local phone number. Request for call forwarding is performed on the remote phone.

Service management from the telephone set:

The service activation with a temporary PIN code is performed on the local number	*25*PIN#
The service activation without a PIN code is performed on the local number	*25#
Call forwarding from the local to the remote telephone set with a temporary PIN is performed on the remote number	* 25 * PIN * LOCAL_PHONE #
Call forwarding from the local to the remote telephone set without a PIN code is performed on the remote number	* 25 ** LOCAL_PHONE#
Cancelling call forwarding from the local to the remote telephone set without a temporary PIN code is performed on the remote number	#25**LOCAL_PHONE#
Cancelling call forwarding from the local to the remote telephone set with a temporary PIN code is performed on the remote number	#25*PIN*LOCAL_PHONE#
Deactivation, is performed on the local number	#25#
Status view, is performed on the local number	*#25#
Checking the non-response timer value (local phone only)	*#125#

where

- PIN – a secret digital code consisting of 4–12 characters;
- LOCAL_PHONE – the phone number from which the calls will be forwarded.
- QTY_BEEPS – the number of beeps (1 beep is equal to 5 seconds) that should be waited before call forwarding. Possible values are 1..9.

12. Cancel all services

This service allows the subscriber to cancel all services ordered from their telephone set by using a single cancellation procedure. The cancellation procedure involves the service code and the password code.

The service access is controlled by the checkbox for the *Cancel all Services* VAS category.

Use	* 50#
-----	-------

APPENDIX L. RADIUS CALL MANAGEMENT SERVICE¹

The gateway can change the passing call parameters using the RADIUS server commands in response to RADIUS-Authorisation requests. The commands are sent in the text format using the Vendor-Specific attribute (see section 3.1.14.3), with the ELTEX vendor number set to 35265 and the Eltex-AVPair attribute name set to 1.

In general, the Eltex-AVPair attribute format is as follows:

Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1):<\$COMMAND-STRING>

Using various commands in the \$ COMMAND-STRING string, you can manage the following parameters:

Modification of CgPN and CdPN numbers:

The numbers modification can be performed at two stages during call processing:

1. for incoming communication, before the call passes through the numbering schedule, i. e. before its routing. For this purpose, the CgPNin and CdPNin values are used for the Calling and Called numbers, respectively.
2. for outgoing communication, after the call passes through the numbering schedule, i. e. after its routing. For this purpose, the CgPNout and CdPNout values are used for the Calling and Called numbers, respectively.

For CgPN numbers, you can modify the following parameters in addition to the number itself:

- *numtype* – CgPN number type;
- *plantype* – CgPN numbering schedule type;
- *presentation* – CgPN presentation field value.

For CdPN numbers, you can modify the following parameters in addition to the number itself:

- *numtype* – CdPN number type;
- *plantype* – CdPN numbering schedule type.

Modification request syntax for CgPN and CdPN numbers

The command consists of a mandatory and an optional part. The mandatory part contains an initial text identifier of the command, modified number identifier and modification mask.

- *“CallManagement:”* – a text identifier specifying that this attribute contains a call management command;
- *“CgPNin=”, “CdPNin=”, “CgPNout=”, “CdPNout=”* – number identifiers indicating the number that the modification should be applied to;
- The *“modification mask”* parameter – modification rule for number digits (may be empty).

The optional part can consist of either a single parameter or multiple parameters separated by a semicolon. The mandatory and optional parts are also separated by a semicolon, if the optional part is present.

¹ Available with an RCM license

Possible parameters of the optional part:

- numtype.
- plantype.
- presentation.

In general, the command format is as follows:

```
CallManagement:CgPNin=<${modifymask}>;numtype=<${numtype}>;plantype=<${plantype}>;presentation=<${presentation}>
```

where

- “CallManagement:CgPNin=<\${modify-mask}>;” – the mandatory part,
- “numtype=<\${numtype}>;plantype=<\${plantype}>;presentation=<\${presentation}>” – the optional part

```
CallManagement:CdPNin=;numtype=<${numtype}>;plantype=<${plantype}>
```

where

- “CallManagement:CgPNin=;” – the mandatory part with a blank modification mask,
- “numtype=<\${numtype}>;plantype=<\${plantype}>” – the optional part.

```
CallManagement:CgPNin=<${modify-mask}>;
```

where

- “CallManagement:CgPNin=<\${modify-mask}>;” – the mandatory part,
- the optional part is missing.

The parameter values used in the commands are as follows:

- *\$modify-mask* – the number modification rule (for the rule modification syntax, see Section Modification Rule Syntax);
- *\$numtype* – one of the values: international, national, network-specific, subscriber, unknown;
- *\$plantype* – one of the values: isdn, national, private, unknown;
- *\$presentation* – one of the values: allowed, restricted, not-available, spare.

The gateway can pass the number modification command parameters in multiple attributes. Thus, a set of commands:

```
«CallManagement:CgPNin=<${modify-mask}>»  
«CallManagement:CgPNin=;numtype=<${numtype}>»  
«CallManagement:CgPNin=;presentation=<${presentation}>»
```

and equivalent to one command:

```
«CallManagement:CgPNin=<${modify-mask}>;numtype=<${numtype}>;presentation=<${presentation}>»
```



If any optional parameter (*numtype*, *platype*, *presentation*) should remain unchanged, do not include it in the request, but you must specify the number type (*CgPNin*, *CdPNin*, *CgPNout*, *CdPNout*) to which the transmitted fields belong.

Example:

For incoming communication, add prefix +7383 to the CgPN number, change its number type to *national* and set *presentation restricted*.

To do this, pass an attribute with the following value in the Access-Accept response from the RADIUS server:

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1):
CallManagement:CgPNin=+7383;numtype=national;presentation=restricted
```

Which is also equivalent to three attributes with the following values:

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1): CallManagement:CgPNin=+7383
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1): CallManagement:CgPNin=;numtype=national
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1): CallManagement:CgPNin=;presentation=restricted
```

Call routing management

Using the commands from the RADIUS server, you can manage the call routing process, i. e., transfer the call to another numbering schedule of the gateway or unconditionally forward it to a prefix created in the configuration (the equivalent of the *direct prefix* parameter described in section 3.1.7.1 Trunk Groups).

The routing management command consists only of the mandatory part:

- *CallManagement*: – a text identifier specifying that this attribute contains a call management command;
- *NumberingPlan* – identifier indicating the change numbering schedule command
- *DirectRoutePrefix* – identifier indicating the direct routing prefix selection command.

In general, the command format is as follows:

```
CallManagement:NumberingPlan=<$numplan_idx>
CallManagement:DirectRoutePrefix=<$prefix_index>
```

where

- *\$numplan_idx* – sequence number of the numbering schedule
- *\$prefix_index* – ID of the prefix created in the numbering schedule.

Example

Change the numbering schedule to the 3rd one.

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1): CallManagement:NumberingPlan=3
```

Call category management

Using commands from the RADIUS server, you can modify the access category and caller ID category of the subscriber (equivalent to calling party category). To do this, use the following fields:

The category change command consists only of the mandatory part:

- *CallManagement*: – a text identifier specifying that this attribute contains a call management command;
- *AccessCategory* – identifier of the access category change command;
- *AONCategory* – identifier of the subscriber category change command (calling party category).

In general, the command format is as follows:

```
CallManagement:AccessCategory=<$category_idx>  
CallManagement:AONCategory=<$category_value>
```

where:

- *\$category_idx* – the access category index.
- *\$category_value* – the Caller ID category index.

The priority of changing the caller ID category depends on the type of subscriber.

Dynamic subscriber:

- Modification via RADIUS;
- Modification through the modification table of incoming leg;
- Modification through the modification table of outgoing leg.

Other subscribers:

- Modification through the modification table of incoming leg;
- Modification via RADIUS;
- Modification through the modification table of outgoing leg.

Example

Set the calling party category to 7.

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1): CallManagement:AONCategory=7
```

Management of subscriber parameters

For a dynamic subscriber, it is possible to set the *Number of lines* parameter and the line operation mode at the subscriber registration stage.

The subscriber parameter management command consists only of the mandatory part:

- *UserManagement*: – a text identifier specifying that this attribute contains a subscriber entry management command;
- *MaxActiveLines* – an identifier indicating the number of active lines available for a given subscriber in the common mode. If this parameter is specified, the line restriction mode is always set to common, even if separate restrictions for incoming/outgoing calls are specified at the same time;
- *MaxEgressLines* – an identifier indicating the number of outgoing lines available for a given subscriber in the separate mode. Can be combined with the *MaxIngressLines* parameter;

- *MaxActiveLines* – an identifier indicating the number of incoming lines available for a given subscriber in the separate mode. Can be combined with the *MaxEgressLines* parameter.

In general, the command format is as follows:

```
"UserManagement:MaxActiveLines=<$line_count>"  
"UserManagement:MaxEgressLines=<$egress>;MaxIngressLines=<$ingress>,"  
"UserManagement:MaxEgressLines=<$egress>"  
"UserManagement:MaxIngressLines=<$ingress>"
```

where

- *\$line_count* – the number of active connections available for the subscriber simultaneously.
- *\$egress* – the number of outgoing connections available for the subscriber;
- *\$ingress* – the number of incoming connections available for the subscriber.

Examples

Set the normal line operation mode and the number of active lines per subscriber to three.

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1): UserManagement:MaxActiveLines=3
```

Set the separate line operation mode, the number of outgoing lines to three and the number of incoming lines to two:

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1): UserManagement:MaxEgressLines=3;MaxIngressLines=2
```

Set the normal line operation mode and the number of active lines per subscriber to two (note that the *MaxActiveLines* parameter has an absolute priority over *MaxEgressLines* and *MaxIngressLines*):

```
Vendor-Specific(26): Eltex(35265): Eltex-AVPair(1):  
UserManagement:MaxEgressLines=6;MaxActiveLines=2;MaxIngressLines=5
```

APPENDIX M. MANAGEMANT AND MONITORING VIA SNMP

The gateway supports monitoring and configuration via **Simple Network Management Protocol (SNMP)**.

Monitoring functions:

- Collection data on device, established sensors and software;
- E1 streams and channels state;
- VoIP submodules and channel state;
- SS7 linksets state;
- SIP interface state.

Management functions:

- Firmware version updating;
- Current configuration saving;
- Device reboot;
- SIP subscriber management;
- Management of dynamic SIP subscriber groups.

The following format of the description will be accepted for the 'Inquiry description' column of OID description tables:

- Get – an object or tree value can be displayed by sending 'GetRequest'.
- Set – an object value can be set by sending 'SetRequest' (Please pay attention if you set value by SET inquiry, you need to specify OID in 'OID.0' form);
- {} – object name or OID;
- N – integer type of numeric parameter is used in the command;
- U – unsigned integer type of numeric partameter is used in the command;
- S – string parameter is used in the command;
- A – IP address is used in the command (Please pay attention, some commands, using IP address as argument, have string type of data – 's').

Table M.1 – Command examples

Request description	Command
Get {}	snmpwalk -v2c -c public -m +ELTEX-SMG \$ip_smg activeCallCount
Get {}.x	snmpwalk -v2c -c public -m +ELTEX-SMG \$ip_smg pmExist.1 snmpwalk -v2c -c public -m +ELTEX-SMG \$ip_smg pmExist.2 etc.
Set {} N	snmpset -v2c -c public -m +ELTEX-SMG \$ip_smg \ smgSyslogTracesCalls.0 i 60
Set {} 1	snmpset -v2c -c private -m +ELTEX-SMG \$ip_smg smgReboot.0 i 1
Set {} U	snmpset -v2c -c public -m +ELTEX-SMG \$ip_smg \ getGroupUserByID.0 u 2
Set {} S	snmpset -v2c -c private -m +ELTEX-SMG \$ip_smg \ smgUpdateFw.0 s "smg1016m_firmware_3.8.0.1966.bin 192.0.2.2"
Set {} "NULL"	snmpset -v2c -c private -m +ELTEX-SMG \$ip_smg \ getUserByNumber.0 s "NULL"
Set {} A	snmpset -v2c -c private -m +ELTEX-SMG \$ip_smg \ smgSyslogTracesAddress.0 a 192.0.2.44

Request execution examples:

The requests shown below are equivalent and are presented by request of the 'activeCallsCount' object , that displays the number of the current calls on SMG. .

```
$ snmpwalk -v2c -c public -m +ELTEX-SMG 192.0.2.1 activeCallCount
ELTEX-SMG::ActiveCallCount.0 = INTEGER: 22
```

```
$ snmpwalk -v2c -c public -m +ELTEX-SMG 192.0.2.1 smg.42.1
ELTEX-SMG::ActiveCallCount.0 = INTEGER: 22
```

```
$ snmpwalk -v2c -c public -m +ELTEX-SMG 192.0.2.1 1.3.6.1.4.1.35265.1.29.42.1
ELTEX-SMG::ActiveCallCount.0 = INTEGER: 22
```

```
$ snmpwalk -v2c -c public 192.0.2.1 1.3.6.1.4.1.35265.1.29.42.1
SNMPv2-SMI::enterprises.35265.1.29.42.1.0 = INTEGER: 22
```

OID descriptions from MIB ELTEX-SMG

Table M.2 – Common information and sensors

Name	OID	Requests	Description
smg	1.3.6.1.4.1.35265.1.29	Get {}	Root object for OID tree
smgDevName	1.3.6.1.4.1.35265.1.29.1	Get {}	Device name
smgDevType	1.3.6.1.4.1.35265.1.29.2	Get {}	Device type (always 29)
smgFwVersion	1.3.6.1.4.1.35265.1.29.3	Get {}	Firmware version
smgEth0	1.3.6.1.4.1.35265.1.29.4	Get {}	IP address of the primary interface
smgUptime	1.3.6.1.4.1.35265.1.29.5	Get {}	Firmware operating time
smgUpdateFw	1.3.6.1.4.1.35265.1.29.25	Set {} S	Firmware updating. Send a Set inquiry with space-separated parameters: - name of firmware w/o space; - TFTP server address
smgReboot	1.3.6.1.4.1.35265.1.29.27	Set {} 1	Reboot of the device
smgSave	1.3.6.1.4.1.35265.1.29.29	Set {} 1	Configuration saving
smgFreeSpace	1.3.6.1.4.1.35265.1.29.32	Get {}	Free space on embedded flash memory
smgFreeRam	1.3.6.1.4.1.35265.1.29.33	Get {}	The value of free RAM
smgMonitoring	1.3.6.1.4.1.35265.1.29.35	Get {}	Display temperature sensors and fan rate, root object
smgTemperature1	1.3.6.1.4.1.35265.1.29.35.1	Get {}	Temperature sensors 1
smgTemperature2	1.3.6.1.4.1.35265.1.29.35.2	Get {}	Temperature sensors 2
smgFan0	1.3.6.1.4.1.35265.1.29.35.3	Get {}	Fan speed sensor 1
smgFan1	1.3.6.1.4.1.35265.1.29.35.4	Get {}	Fan speed sensor 2
smgFan2	1.3.6.1.4.1.35265.1.29.35.5	Get {}	Fan speed sensor 3
smgFan3	1.3.6.1.4.1.35265.1.29.35.6	Get {}	Fan speed sensor 4

Name	OID	Requests	Description
smgPowerModuleTable	1.3.6.1.4.1.35265.1.29.36	Get {}	Information on state of a power supply unit, root object. For subordinate object, 1 or 2 is specified as number of power supply unit.
smgPowerModuleEntry	1.3.6.1.4.1.35265.1.29.36.1	Get {}	See smgPowerModuleTable
pmExist	1.3.6.1.4.1.35265.1.29.36.1.2.x	Get {}.x	Power unit 1 – installed 2 – not installed
pmPower	1.3.6.1.4.1.35265.1.29.36.1.3.x	Get {}.x	Power units are 1 – supplied with electric energy 2 – not supplied with electric energy
pmType	1.3.6.1.4.1.35265.1.29.36.1.4.x	Get {}.x	Type of the installed power supply unit 1 – PM48/12 2 – PM220/12 3 – PM220/12V 4 – PM150-220/12
smgCpuLoadTable	1.3.6.1.4.1.35265.1.29.37	Get {}	CPU load, root object. Shows the CPU load percentage by the task type. For child objects, specify the CPU number (1..4).
smgCpuLoadEntry	1.3.6.1.4.1.35265.1.29.37.1	Get {}	see smgCpuLoadTable
cpuUsr	1.3.6.1.4.1.35265.1.29.37.1.2.x	Get {}.x	% CPU, use application
cpuSys	1.3.6.1.4.1.35265.1.29.37.1.3.x	Get {}.x	% CPU, kernel application
cpuNic	1.3.6.1.4.1.35265.1.29.37.1.4.x	Get {}.x	% CPU, applications with modified priority
cpuidle	1.3.6.1.4.1.35265.1.29.37.1.5.x	Get {}.x	% CPU, idle
cpulo	1.3.6.1.4.1.35265.1.29.37.1.6.x	Get {}.x	% CPU, I/O operations
cpulrq	1.3.6.1.4.1.35265.1.29.37.1.7.x	Get {}.x	% CPU, hardware interrupt request processing
cpuSirq	1.3.6.1.4.1.35265.1.29.37.1.8.x	Get {}.x	% CPU, software interrupt processing
cpuUsage	1.3.6.1.4.1.35265.1.29.37.1.9.x	Get {}.x	% CPU, general utilization
smgSubscribersInfo	1.3.6.1.4.1.35265.1.29.42	Get {}	General information on active calls and registrations
activeCallCount	1.3.6.1.4.1.35265.1.29.42.1	Get {}	Current number of active calls
registrationCount	1.3.6.1.4.1.35265.1.29.42.2	Get {}	Current number of registrations

Table M.3 – Syslog Settings

Name	OID	Requests	Description
smgSyslog	1.3.6.1.4.1.35265.1.29.34	Get {}	Syslog settings, root object

Name	OID	Requests	Description
smgSyslogTraces	1.3.6.1.4.1.35265.1.29.34.1	Get {}	Syslog tracing settings, root object
smgSyslogTracesAddress	1.3.6.1.4.1.35265.1.29.34.1.1	Get {} Set {} S	IP address of syslog for trace receiving
smgSyslogTracesPort	1.3.6.1.4.1.35265.1.29.34.1.2	Get {} Set {} N	Syslog server port for receiving traces
smgSyslogTracesAlarms	1.3.6.1.4.1.35265.1.29.34.1.3	Get {} Set {} N	Alarm trace level 1-99 - enable tracing; 0-disable tracing
smgSyslogTracesCalls	1.3.6.1.4.1.35265.1.29.34.1.4	Get {} Set {} N	Call trace level 1-99 - enable tracing; 0-disable tracing
smgSyslogTracesISUP	1.3.6.1.4.1.35265.1.29.34.1.5	Get {} Set {} N	Trace level SS7/ISUP 1-99 - enable tracing; 0-disable tracing
smgSyslogTracesSIPT	1.3.6.1.4.1.35265.1.29.34.1.6	Get {} Set {} N	SIPT trace level 1-99 - enable tracing; 0-disable tracing
smgSyslogTracesQ931	1.3.6.1.4.1.35265.1.29.34.1.7	Get {} Set {} N	Q.931 trace level 1-99 - enable tracing; 0-disable tracing
smgSyslogTracesRTP	1.3.6.1.4.1.35265.1.29.34.1.8	Get {} Set {} N	RTP trace level 1-99 - enable tracing; 0 - disable tracing
smgSyslogTracesMSP	1.3.6.1.4.1.35265.1.29.34.1.9	Get {} Set {} N	The trace level of the commands of the voice submodules 1-99 - enable tracing; 0-disable tracing
smgSyslogTracesRadius	1.3.6.1.4.1.35265.1.29.34.1.10	Get {} Set {} N	RADIUS trace level 1-99 - enable tracing; 0-disable tracing
smgSyslogTracesRowStat us	1.3.6.1.4.1.35265.1.29.34.1.11	Get {} Set {} i 1	Apply changes in the trace configuration
smgSyslogHistory	1.3.6.1.4.1.35265.1.29.34.2	Get {}	Settings of command history logging in syslog, root object
smgSyslogHistoryAddress	1.3.6.1.4.1.35265.1.29.34.2.1	Get {} Set {} S	IP address of syslog server for command history receiving
smgSyslogHistoryPort	1.3.6.1.4.1.35265.1.29.34.2.2	Get {} Set {} N	Port of syslog server for command history receiving
smgSyslogHistoryLevel	1.3.6.1.4.1.35265.1.29.34.2.3	Get {} Set {} N	Level of log detalization 0-disable logging; 1-standard; 2-complete
smgSyslogHistoryRowSta tus	1.3.6.1.4.1.35265.1.29.34.2.4	Get {} Set {} i 1	Apply changes in command history logging

Name	OID	Requests	Description
smgSyslogConfig	1.3.6.1.4.1.35265.1.29.34.3	Get {}	System log settings
smgSyslogConfigLogsEnabled	1.3.6.1.4.1.35265.1.29.34.3.1	Get {} Set {} N	Enable logging 1– enable; 2 – disable
smgSyslogConfigSendToServer	1.3.6.1.4.1.35265.1.29.34.3.2	Get {} Set {} N	Send messages to syslog server 1– enable; 2 – disable
smgSyslogConfigAddress	1.3.6.1.4.1.35265.1.29.34.3.3	Get {} Set {} S	The IP address of the syslog server
smgSyslogConfigPort	1.3.6.1.4.1.35265.1.29.34.3.4	Get {} Set {} N	Syslog server port
smgSyslogConfigRowStatus	1.3.6.1.4.1.35265.1.29.34.3.5	Get {} Set {} i 1	Apply changes in the system log settings

Table M.4 – E1 stream monitoring (for SMG-500 only)

Name	OID	Requests	Description
smgEOneTable	1.3.6.1.4.1.35265.1.29.7	Get {}	Table with physical states of E1 streams
eOneLineInfoPhyState	1.3.6.1.4.1.35265.1.29.7.1.2 1.3.6.1.4.1.35265.1.29.7.1.2.x	Get {} Get {}x	E1 stream physical state Add a stream number (0..3) to OID for obtaining information on its status. Stream status: 0–the stream is disabled; 1 - ALARM; 2 - LOS; 3 - AIS; 4 - LOM; 5 - LOMF; 6 - stream is in operation; 7 - PRBS test is enabled on the stream
eOneLineInfoRemAlarm	1.3.6.1.4.1.35265.1.29.7.1.3 1.3.6.1.4.1.35265.1.29.7.1.3.x	Get {} Get {}x	The presence of a RAI signal on the stream – an error on the remote side. Add a stream number (0..3) to OID for obtaining information on its status. 0 – normal state; 1 – RAI signal is received
eOneLineInfoRemAlarmTS16	1.3.6.1.4.1.35265.1.29.7.1.4 1.3.6.1.4.1.35265.1.29.7.1.4.x	Get {} Get {}x	Presence of RAI16 signal on the stream – error on the remote side in 16 channels interval. Add a stream number (0..3) to OID for obtaining information on its status. 0 – normal state; 1 – RAI16 signal is received

Name	OID	Requests	Description
eOneLineStateAlarm	1.3.6.1.4.1.35265.1.29.7.1.5 1.3.6.1.4.1.35265.1.29.7.1.5.x	Get {} Get {}.x	The alarm state on the stream. Add a stream number (0..3) to OID for obtaining information on its status. 0 – no alarms or stream is disabled; 1 – critical alarm, the stream is out of work; 2 – alarm, there are errors; 3 – code is not used; 4 – alarm, RAI error
eOneLineStatePhyWork	1.3.6.1.4.1.35265.1.29.7.1.6 1.3.6.1.4.1.35265.1.29.7.1.6.x	Get {} Get {}.x	Physical link state on the stream (signal reception). Add a stream number (0..3) to OID for obtaining information on its status. 0 – no signal; 1 – there is link
eOneLinkState	1.3.6.1.4.1.35265.1.29.7.1.7 1.3.6.1.4.1.35265.1.29.7.1.7.x	Get {} Get {}.x	Common state of the link. Add a stream number (0..3) to OID for obtaining information on its status. 0 – stream is disabled; 1 – stream is in operation;
eOneStatistTimer	1.3.6.1.4.1.35265.1.29.7.1.9 1.3.6.1.4.1.35265.1.29.7.1.9.x	Get {} Get {}.x	Time of statistics gathering, in seconds. Add a stream number (0..3) to OID for obtaining information on its status.
eOneSlipUp	1.3.6.1.4.1.35265.1.29.7.1.10 1.3.6.1.4.1.35265.1.29.7.1.10.x	Get {} Get {}.x	Frame slip (frame repeat). Add a stream number (0..3) to OID for obtaining information on its status.
eOneSlipDown	1.3.6.1.4.1.35265.1.29.7.1.11 1.3.6.1.4.1.35265.1.29.7.1.11.x	Get {} Get {}.x	Frame slip (frame loss). Add a stream number (0..3) to OID for obtaining information on its status.
eOneBERCount	1.3.6.1.4.1.35265.1.29.7.1.12 1.3.6.1.4.1.35265.1.29.7.1.12.x	Get {} Get {}.x	Bit errors. Add a stream number (0..3) to OID for obtaining information on its status.
eOneCVC	1.3.6.1.4.1.35265.1.29.7.1.13 1.3.6.1.4.1.35265.1.29.7.1.13.x	Get {} Get {}.x	Error of a signal failure. Add a stream number (0..3) to OID for obtaining information on its status.
eOneCEC	1.3.6.1.4.1.35265.1.29.7.1.14 1.3.6.1.4.1.35265.1.29.7.1.14.x	Get {} Get {}.x	CRC/PRBS error counter. Add a stream number (0..3) to OID for obtaining information on its status.
eOneRxCount	1.3.6.1.4.1.35265.1.29.7.1.16 1.3.6.1.4.1.35265.1.29.7.1.16.x	Get {} Get {}.x	Bytes received. Add a stream number (0..3) to OID for obtaining

Name	OID	Requests	Description
			information on its status.
eOneTxCount	1.3.6.1.4.1.35265.1.29.7.1.17 1.3.6.1.4.1.35265.1.29.7.1.17.x	Get {} Get {}.x	Bytes transferred. Add a stream number (0..3) to OID for obtaining information on its status.
eOneRxLow	1.3.6.1.4.1.35265.1.29.7.1.18 1.3.6.1.4.1.35265.1.29.7.1.18.x	Get {} Get {}.x	Short packets received. Add a stream number (0..3) to OID for obtaining information on its status.
eOneRxBig	1.3.6.1.4.1.35265.1.29.7.1.19 1.3.6.1.4.1.35265.1.29.7.1.19.x	Get {} Get {}.x	Long packets received. Add a stream number (0..3) to OID for obtaining information on its status.
eOneRxOvfl	1.3.6.1.4.1.35265.1.29.7.1.20 1.3.6.1.4.1.35265.1.29.7.1.20.x	Get {} Get {}.x	Overload of receiving. Add a stream number (0..3) to OID for obtaining information on its status.
eOneRxCRC	1.3.6.1.4.1.35265.1.29.7.1.21	Get {} Get {}.x	CRC errors Add a stream number (0..3) to OID for obtaining information on its status.
eOneTxUrun	1.3.6.1.4.1.35265.1.29.7.1.22	Get {} Get {}.x	Transmission failures. Add a stream number (0..3) to OID for obtaining information on its status.
smgEOneChannelTable	1.3.6.1.4.1.35265.1.29.13	Get {}	Table of E1 channels states, root object.
smgEOneChannelEntry	1.3.6.1.4.1.35265.1.29.13.1	Get {}	see smgEOneChannelTable
channelEOneState	1.3.6.1.4.1.35265.1.29.13.1.2 1.3.6.1.4.1.35265.1.29.13.1.2.x 1.3.6.1.4.1.35265.1.29.13.1.2.x.x	Get {} Get {}.x Get {}.x.x	E1 stream channel state Add a stream number (0..3) to OID for obtaining information on its status. Add a stream number (0..3) and channel number (0..31) to OID for obtaining information on its status.
smgEOneBusyChannelsCounters	1.3.6.1.4.1.35265.1.29.31	Get {}	Quantity of busy E1 channels, root object.
smgEOneInstantCounters	1.3.6.1.4.1.35265.1.29.31.1	Get {}	see smgEOneBusyChannelsCounters
smgEOneStream0BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.0	Get {}	Quantity of busy E1 channels - 0
smgEOneStream1BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.1	Get {}	The number of occupied stream channels E1 - 1
smgEOneStream2BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.2	Get {}	Quantity of busy E1 channels - 2
smgEOneStream3BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.3	Get {}	Quantity of busy E1 channels - 3

Name	OID	Requests	Description
smgEOnePeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2	Get {}	Quantity of busy E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream0BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.0	Get {}	Quantity of busy 0 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream1BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.1	Get {}	Quantity of busy 1 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream2BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.2	Get {}	Quantity of busy 2 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream3BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.3	Get {}	Quantity of busy 3 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneCounterPeriod	1.3.6.1.4.1.35265.1.29.31.2.16	Get {} Set {} N	Frequency (period) of statistics collection, in minutes. Statistics will accumulate in periodic counters, while the counter will display the value for the previous period.
smgChannelsE1free	1.3.6.1.4.1.35265.1.29.41	Get {}	Quantity of free E1 channels, root object.
e1freeS0channels	1.3.6.1.4.1.35265.1.29.41.1	Get {}	Quantity of free 0 E1 channels
e1freeS1channels	1.3.6.1.4.1.35265.1.29.41.2	Get {}	Quantity of free 1 E1 channels
e1freeS2channels	1.3.6.1.4.1.35265.1.29.41.3	Get {}	Quantity of free 2 E1 channels
e1freeS3channels	1.3.6.1.4.1.35265.1.29.41.4	Get {}	Quantity of free 3 E1 channels

Table M.5 – SS7 Linkset monitoring

Name	OID	Requests	Description
smgLinkSetTable	1.3.6.1.4.1.35265.1.29.11	Get {}	Linkset state, root object
linkSetEntry	1.3.6.1.4.1.35265.1.29.11.1	Get {}	see smgLinkSetTable
linkSetState	1.3.6.1.4.1.35265.1.29.11.1.2	Get {} Get {}.x	Linkset state SS7. Add Linkset's index (0..3) to OID for obtaining information on its status.

Table M.6 – SIP interface Monitoring

Name	OID	Requests	Description
smgSipIntrfCallInfo	1.3.6.1.4.1.35265.1.29.43	Get {}	Information about calls on SIP interfaces, root object
sipIntrfCount	1.3.6.1.4.1.35265.1.29.43.1	Get {}	Number of SIP interfaces

Name	OID	Requests	Description
sipIntrfActiveCallTable	1.3.6.1.4.1.35265.1.29.43.2	Get {}	Call table (when absence of SIP interfaces, call table is not displayed)
sipIntrfActiveCallTableEntry	1.3.6.1.4.1.35265.1.29.43.2.1	Get {}	see sipIntrfActiveCallTable
sipIntrfID	1.3.6.1.4.1.35265.1.29.43.2.1.2 1.3.6.1.4.1.35265.1.29.43.2.1.2.x	Get {} Get {}.x	ID SIP interface. Add interface index to OID to obtain information on it.
sipIntrfName	1.3.6.1.4.1.35265.1.29.43.2.1.3 1.3.6.1.4.1.35265.1.29.43.2.1.3.x	Get {} Get {}.x	SIP interface name. Add interface index to OID to obtain information on it.
sipIntrfMode	1.3.6.1.4.1.35265.1.29.43.2.1.4 1.3.6.1.4.1.35265.1.29.43.2.1.4.x	Get {} Get {}.x	Operation mode Add interface index to OID to obtain information on it. 0 – SIP; 1 – SIP-T; 2 – SIP-I; 3 – SIP-Q; 4 – SIP profile
sipIntrfCallCount	1.3.6.1.4.1.35265.1.29.43.2.1.5 1.3.6.1.4.1.35265.1.29.43.2.1.5.x	Get {} Get {}.x	The number of active calls on the interface. Add interface index to OID to obtain information on it.
sipIntrfMaxCallCount	1.3.6.1.4.1.35265.1.29.43.2.1.6 1.3.6.1.4.1.35265.1.29.43.2.1.6.x	Get {} Get {}.x	The maximum number of calls on the interface. Add interface index to OID to obtain information on it. 0 – no limit; 1..65535 – the limit of calls
sipIntrfAccessible	1.3.6.1.4.1.35265.1.29.43.2.1.6 1.3.6.1.4.1.35265.1.29.43.2.1.6.x	Get {} Get {}.x	SIP interface accessibility (the result of controlling counter-party by using OPTIONS): 1 – available; 2 – not available

Monitoring and configuration of SIP-subscribers (static subscribers)

The commands for SNMP utilities call are represented in description of monitoring and configuration functions as follows:

Swalk script that implements the reading values:

```
#!/bin/bash
/usr/bin/snmpwalk -v2c -c public -m +ELTEX-SMG 192.0.2.1 "$@"
```

Sset script that implements value setting:

```
#!/bin/bash
/usr/bin/snmpset -v2c -c private -m +ELTEX-SMG 192.0.2.1 "$@"
```

Monitoring

You can monitor subscriber or static subscriber groups by using the next ways:

- by index or subscriber ID;
- by numbering plan and full subscriber number;
- by numbering plan and partial subscriber number.

To monitor:

1. Reset the search status;
2. Set the search criteria (optionally);
3. Display information.

Example of the search by index

```
sset staticResetCheck.0 i 1      # reset status of the search
sset getUserByIndex.0 i 4        # set up the search by index 4
swalk tableOfUsers               # query of the table with the subscriber information
```

Result:

```
ELTEX-SMG::StaticResetCheck.0 = INTEGER: 0
ELTEX-SMG::getUserByIndex.0 = INTEGER: 4
ELTEX-SMG::UserID.4 = INTEGER: 5
ELTEX-SMG::RegState.4 = INTEGER: 2
ELTEX-SMG::Numplan.4 = INTEGER: 0
ELTEX-SMG::Number.4 = STRING: 20000
ELTEX-SMG::Ip.4 = IpAddress: 192.0.2.123
ELTEX-SMG::Port.4 = Gauge32: 5063
ELTEX-SMG::Domain.4 = STRING: 192.0.2.1
ELTEX-SMG::MaxActiveLines.4 = INTEGER: 3
ELTEX-SMG::ActiveCallCount.4 = INTEGER: 0
ELTEX-SMG::RegExpires.4 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.12.4 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.13.4 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.14.4 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.15.4 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.16.4 = INTEGER: -1
```

Example of the search by numbering plan and number

```
sset staticResetCheck.0 i 1      # reset status of the search
sset getUserByNumplan.0 i 2      # set up the second numbering plan
sset getUserByNumber.0 s 20001   # set the subscriber number
swalk tableOfUsers               # query of the table with the subscriber information
```

Result:

```
ELTEX-SMG::UserID.9 = INTEGER: 10
ELTEX-SMG::RegState.9 = INTEGER: 0
ELTEX-SMG::Numplan.9 = INTEGER: 2
ELTEX-SMG::Number.9 = STRING: 20001
ELTEX-SMG::Ip.9 = IpAddress: 0.0.0.0
ELTEX-SMG::Port.9 = Gauge32: 0
ELTEX-SMG::Domain.9 = STRING: sipp.domain
ELTEX-SMG::MaxActiveLines.9 = INTEGER: 0
ELTEX-SMG::ActiveCallCount.9 = INTEGER: 0
ELTEX-SMG::RegExpires.9 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.12.9 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.13.9 = INTEGER: -1
```



```
ELTEX-SMG::TableOfUsersEntry.14.9 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.15.9 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.16.9 = INTEGER: -1
```

Example of a search by numbering plan and partial number

```
sset ttaticResetCheck.0 i 1          # reset status of the search
sset getUserByNumplan.0 i 0         # set zero numbering plan
sset getUserBySubNumber.0 s 400     # install part of number
swalk tableOfUsers                  # query of the table with the subscriber information
```

Result:

```
ELTEX-SMG::UserID.0 = INTEGER: 1
ELTEX-SMG::UserID.1 = INTEGER: 2
ELTEX-SMG::UserID.2 = INTEGER: 3
ELTEX-SMG::RegState.0 = INTEGER: 1
ELTEX-SMG::RegState.1 = INTEGER: 1
ELTEX-SMG::RegState.2 = INTEGER: 0
ELTEX-SMG::Numplan.0 = INTEGER: 0
ELTEX-SMG::Numplan.1 = INTEGER: 0
ELTEX-SMG::Numplan.2 = INTEGER: 0
ELTEX-SMG::Number.0 = STRING: 40010
ELTEX-SMG::Number.1 = STRING: 40011
ELTEX-SMG::Number.2 = STRING: 40012
ELTEX-SMG::Ip.0 = IpAddress: 192.0.2.21
ELTEX-SMG::Ip.1 = IpAddress: 192.0.2.21
ELTEX-SMG::Ip.2 = IpAddress: 0.0.0.0
ELTEX-SMG::Port.0 = Gauge32: 23943
ELTEX-SMG::Port.1 = Gauge32: 23943
ELTEX-SMG::Port.2 = Gauge32: 0
ELTEX-SMG::Domain.0 = STRING: 192.0.2.1
ELTEX-SMG::Domain.1 = STRING: 192.0.2.1
ELTEX-SMG::Domain.2 = STRING:
ELTEX-SMG::MaxActiveLines.0 = INTEGER: -1
ELTEX-SMG::MaxActiveLines.1 = INTEGER: 4
ELTEX-SMG::MaxActiveLines.2 = INTEGER: 6
ELTEX-SMG::ActiveCallCount.0 = INTEGER: -1
ELTEX-SMG::ActiveCallCount.1 = INTEGER: 0
ELTEX-SMG::ActiveCallCount.2 = INTEGER: 0
ELTEX-SMG::RegExpires.0 = INTEGER: 118
ELTEX-SMG::RegExpires.1 = INTEGER: 91
ELTEX-SMG::RegExpires.2 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.12.0 = INTEGER: 1
ELTEX-SMG::TableOfUsersEntry.12.1 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.12.2 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.13.0 = INTEGER: 2
ELTEX-SMG::TableOfUsersEntry.13.1 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.13.2 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.14.0 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.14.1 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.14.2 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.15.0 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.15.1 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.15.2 = INTEGER: -1
ELTEX-SMG::TableOfUsersEntry.16.0 = INTEGER: 0
ELTEX-SMG::TableOfUsersEntry.16.1 = INTEGER: -1
```

View information without using search

```
sset staticResetCheck.0 i 1      # reset status of the search
swalk tableOfUsers              # show all subscribers
swalk regState.3                # display the registration status of the subscriber
                                # with index 3
swalk ip.4                      # show subscriber IP address with index 4
swalk activeCallCount           # display quantity of active calls
                                # of all subscribers
```

Configuration

Configuration involves the following operations on subscribers:

- Settings viewing;
- Settings editing;
- Creating a new subscriber;
- Removing.

To view settings:

- Select subscriber through the search;
- Select configuration mode - view;
- Display the necessary

To edit settings:

- Select subscriber through the search;
- Select configuration mode - edit;
- Set the required settings;
- Apply the settings.

To create a new subscriber:

- Select configuration mode - creation;
- Set the required settings of the subscriber (at least number);
- Apply the settings.

To remove a subscriber:

- Select subscriber through the search;
- Select configuration mode - removing;
- Apply the settings.

You can cancel changes that were not applied only in 'Add a new subscriber' and 'Edit a subscriber' modes.



Undo group remove is not possible. Only a complete configuration restore via WEB or CLI is available.

Example of new subscriber creation

```
sset staticResetCheck.0 i 1      # reset status of the search
sset staticSetMode.0 i 3        # set the 'add' mode
sset stSetNumber.0 s 71234567890 # set the subscriber number
sset staticSetApply.0 i 1       # apply the settings
sset staticSetMode.0 i 0        # set the 'none' mode
```

Example of settings viewing

```
sset staticResetCheck.0 i 1      # reset status of the search
```

```

sset getUserByIndex.0 i 4          # set up the search by index 4
sset staticSetMode.0 i 1          # set the 'show' mode
swalk tableOfStSetUser           # view the settings table, or
swalk stSetAuth                  # separate registration mode, or
swalk stSetAccessMode            # separate maintenance mode, etc.

```

Example of settings editing

```

sset staticResetCheck.0 i 1      # reset status of the search
sset getUserByNumplan.0 i 0      # set zero numbering plan
sset getUserByNumber.0 s 71234567890 # set the subscriber number
sset staticSetMode.0 i 2        # set the 'set' mode
sset stSetNumplan.0 i 1         # change the numbering plan to the first one
  sset stSetCliro.0 i 1         # connect the CLIRO service
  sset stSetAONtypeNumber.0 i 2 # set 'National' automatic calling line identification type
sset staticSetApply.0 i 1       # apply the settings
sset staticSetMode.0 i 0        # set the 'none' mode

```

Example of removing of subscriber

```

sset staticResetCheck.0 i 1      # reset status of the search
sset getUserByID.0 i 15          # set search by ID 15
sset staticSetMode.0 i 4        # set the 'del' mode
sset staticSetApply.0 i 1       # apply the settings
                                # 'none' mode does not need to be set manually

```

Table M.7 – Monitoring and configuration of SIP subscribers (static subscribers)

Name	OID	Requests	Description
smgSipUser	1.3.6.1.4.1.35265.1.29.38	Get {}	Static subscribers list, root object
staticCheckStatus	1.3.6.1.4.1.35265.1.29.38.1	Get {}	Status of the search by criteria. None - without a search, display all static subscribers; Find user by index; Find user by ID; Find users by numplan; Find user by numplan and number; Find users by numplan and substring number
staticResetCheck	1.3.6.1.4.1.35265.1.29.38.2	Set {} N	Reset search. Any value sets status of search to 'None'.
numActiveUsers	1.3.6.1.4.1.35265.1.29.38.3	Get {}	Quantity of active (authorized) subscribers.
numAllUsers	1.3.6.1.4.1.35265.1.29.38.4	Get {}	Quantity of subscribers in the system.
getUserByIndex	1.3.6.1.4.1.35265.1.29.38.5	Set {} N Set {} -1	Set subscriber's index for the search. The values in a range of [0:numAllUsers) set search in 'Find user by index' state. The '-1' value corresponds to 'None' state of the search.
getUserByID	1.3.6.1.4.1.35265.1.29.38.6	Set {} N Set {} -1	Set user ID for the search.

Name	OID	Requests	Description
			<p>The values from 1 and further complies 'Find user by ID' mode of search.</p> <p>The '-1' value correspondsto 'None' state of the search.</p>
getUserByNumplan	1.3.6.1.4.1.35265.1.29.38.7	Set {} N Set {} -1	<p>Set a numbering plan for subscribers search.</p> <p>Setting the value to 1. If the search status was "Find users by numplan", "Find user by numplan and number" or "Find users by numplan and substring number", the '-1' value sets "None" status.</p> <p>If the value equals '0' or more, the priority of search mode setting is as follows:</p> <ul style="list-style-type: none"> - If 'getUserByNumber' is defined, the 'Find user by numplan and number' mode will be activated; If 'getUserBySubNumber' is defined, the 'Find users by numplan and substring number' mode will be activated; - If 'getUserByNumber' and 'getUserBySubNumber' are not defined, the 'Find users bynumplan' mode will be activated;
getUserByNumber	1.3.6.1.4.1.35265.1.29.38.8	Set {} S Set {} "NULL"	<p>Set the number to search for a subscriber in conjunction with the numbering plan.</p> <p>Number length should be from 1 to 32 digits.</p> <p>When the numbering plan is set, the status of search will set to 'Find user by numplan and number', otherwise the search status will not change.</p> <p>Set 'NULL' value to reset the number.</p> <p>However, if the search status was "Find user by numplan and number" the search status will be changed to 'None'.</p>
getUserBySubNumber	1.3.6.1.4.1.35265.1.29.38.9	Set {} S Set {} "NULL"	<p>Set a partial number to search for subscribers in conjunction with the numbering plan.</p> <p>Number length should be from 1 to</p>

Name	OID	Requests	Description
			<p>32 digits.</p> <p>When the numbering plan is set, the status of search will be set to 'Find users by numplan and substring number', otherwise the search status will not be changed.</p> <p>Set 'NULL' value to reset the number. However, if the search status was "Find users by numplan and substring number", the search status will be changed to 'None'.</p>
TableOfUsers	1.3.6.1.4.1.35265.1.29.38.10	Get {}	Static subscriber table, root object
tableOfUsersEntry	1.3.6.1.4.1.35265.1.29.38.10.1	Get {}	see TableOfUsers
userID	1.3.6.1.4.1.35265.1.29.38.10.1.2 1.3.6.1.4.1.35265.1.29.38.10.1.2.x	Get {} Get {}.x	Subscriber ID. Add subscriber index to OID to obtain information on the subscriber.
userRegState	1.3.6.1.4.1.35265.1.29.38.10.1.3 1.3.6.1.4.1.35265.1.29.38.10.1.3.x	Get {} Get {}.x	State of subscriber registration. Add subscriber index to OID to obtain information on the subscriber. 0 – not registered; 1 – registered
userNumplan	1.3.6.1.4.1.35265.1.29.38.10.1.4 1.3.6.1.4.1.35265.1.29.38.10.1.4.x	Get {} Get {}.x	Numbering plan of the subscriber. Add subscriber index to OID to obtain information on the subscriber.
userNumber	1.3.6.1.4.1.35265.1.29.38.10.1.5 1.3.6.1.4.1.35265.1.29.38.10.1.5.x	Get {} Get {}.x	Subscriber number Add subscriber index to OID to obtain information on the subscriber.
userIp	1.3.6.1.4.1.35265.1.29.38.10.1.6 1.3.6.1.4.1.35265.1.29.38.10.1.6.x	Get {} Get {}.x	Subscriber IP address. Add subscriber index to OID to obtain information on the subscriber. If the address is unknown, the '0.0.0.0' value will be set.
userPort	1.3.6.1.4.1.35265.1.29.38.10.1.7 1.3.6.1.4.1.35265.1.29.38.10.1.7.x	Get {} Get {}.x	Subscriber port. Add subscriber index to OID to obtain information on the subscriber.
userDomain	1.3.6.1.4.1.35265.1.29.38.10.1.8 1.3.6.1.4.1.35265.1.29.38.10.1.8.x	Get {} Get {}.x	SIP-domain of the subscriber. Add subscriber index to OID to obtain information on the subscriber.
userMaxActiveLines	1.3.6.1.4.1.35265.1.29.38.10.1.9 1.3.6.1.4.1.35265.1.29.38.10.1.9.x	Get {} Get {}.x	The quantity of ingress/egress lines while operation in combined line mode. Add subscriber index to OID to obtain information on the subscriber.

Name	OID	Requests	Description
userActiveCallCount	1.3.6.1.4.1.35265.1.29.38.10.1.10 1.3.6.1.4.1.35265.1.29.38.10.1.10.x	Get {} Get {}.x	The quantity of active calls while operation in combined line mode. Add subscriber index to OID to obtain information on the subscriber.
userRegExpires	1.3.6.1.4.1.35265.1.29.38.10.1.11 1.3.6.1.4.1.35265.1.29.38.10.1.11.x	Get {} Get {}.x	Time to registration expiry, in seconds. Add subscriber index to OID to obtain information on the subscriber.
userLinesMode	1.3.6.1.4.1.35265.1.29.38.10.1.12 1.3.6.1.4.1.35265.1.29.38.10.1.12.x	Get {} Get {}.x	Line operation mode Add subscriber index to OID to obtain information on the subscriber. 0 – combined; 1 – separate.
userMaxIngressLines	1.3.6.1.4.1.35265.1.29.38.10.1.13 1.3.6.1.4.1.35265.1.29.38.10.1.13.x	Get {} Get {}.x	The quantity of ingress lines while operation in separate mode. Add subscriber index to OID to obtain information on the subscriber.
userMaxEgressLines	1.3.6.1.4.1.35265.1.29.38.10.1.14 1.3.6.1.4.1.35265.1.29.38.10.1.14.x	Get {} Get {}.x	The quantity of egress lines while operation in separate mode. Add subscriber index to OID to obtain information on the subscriber.
userActiveIngressCount	1.3.6.1.4.1.35265.1.29.38.10.1.15 1.3.6.1.4.1.35265.1.29.38.10.1.15.x	Get {} Get {}.x	The quantity of active ingress calls while operation in separate mode. Add subscriber index to OID to obtain information on the subscriber.
userActiveEgressCount	1.3.6.1.4.1.35265.1.29.38.10.1.16 1.3.6.1.4.1.35265.1.29.38.10.1.16.x	Get {} Get {}.x	The quantity of active egress calls while operation in separate mode. Add subscriber index to OID to obtain information on the subscriber.
stSetAuthLog	1.3.6.1.4.1.35265.1.29.38.15.1.14	Get {} Set {} S	Login for authorization
staticModeSettings	1.3.6.1.4.1.35265.1.29.38.11	Get {}	Operation mode with subscriber settings. None – operation with subscriber settings is disabled; Show – show the settings; Set – change settings; Add – add a subscriber; Del – delete a subscriber; The 'Show', 'Set', and 'Del' statuses display settings only if the search status does not equal to 'None'

Name	OID	Requests	Description
staticSetMode	1.3.6.1.4.1.35265.1.29.38.12	Set {} N	Set subscriber settings operation mode. 0 – None mode; 1 – Show mode; 2 – Set mode; 3 – Add mode; 4 – Del mode
staticSetReset	1.3.6.1.4.1.35265.1.29.38.13	Set {} N	Reset setting changes (if they have not been applied) in 'Set' and 'Add' modes, in other modes this command is ignored.
staticSetApply	1.3.6.1.4.1.35265.1.29.38.14	Set {} N	Apply settings, add or remove a subscriber. New settings are activated in the 'Set' mode; In the 'Add' mode new subscriber is created and index for subscriber search is set equal to the created subscriber index, status of the search changes to 'Find user by index' and settings operation mode sets to 'Show'. In the 'Del' mode user is deleted, search status and settings operation mode set to 'None'. The inquiry is ignored in 'None' and 'Show' modes.
tableOfStSetUser	1.3.6.1.4.1.35265.1.29.38.15	Get {}	Table of static subscribers settings, root object
tableOfStSetUserEntry	1.3.6.1.4.1.35265.1.29.38.15.1	Get {}	see TableOfStSetUser
stSetId	1.3.6.1.4.1.35265.1.29.38.15.1.2	Get {}	Subscriber ID.
stSetName	1.3.6.1.4.1.35265.1.29.38.15.1.3	Get {} Set {} S	Subscriber display name
stSetIpAddr	1.3.6.1.4.1.35265.1.29.38.15.1.4	Get {} Set {} A	Subscriber's IP address.
stSetSIPdomain	1.3.6.1.4.1.35265.1.29.38.15.1.5	Get {} Set {} S	SIP domain
stSetNumber	1.3.6.1.4.1.35265.1.29.38.15.1.6	Get {} Set {} S	Phone number
stSetNumplan	1.3.6.1.4.1.35265.1.29.38.15.1.7	Get {} Set {} N	Numbering schedule
stSetAONnumber	1.3.6.1.4.1.35265.1.29.38.15.1.8	Get {} Set {} S	Caller ID number
stSetAONtypeNumber	1.3.6.1.4.1.35265.1.29.38.15.1.9	Get {} Set {} N	Type of caller ID number 0 – Unknown; 1 – Subscriber;

Name	OID	Requests	Description
			2 – National; 3 – International; 4 – Network specific; 5 – No change (from call)
stSetProfile	1.3.6.1.4.1.35265.1.29.38.15.1.10	Get {} Set {} N	SIP profile
stSetCategory	1.3.6.1.4.1.35265.1.29.38.15.1.11	Get {} Set {} N	Caller ID Category 0 – No change (from call); 1..10 – select category
stSetAccessCat	1.3.6.1.4.1.35265.1.29.38.15.1.12	Get {} Set {} N	Access category
stSetAuth	1.3.6.1.4.1.35265.1.29.38.15.1.13	Get {} Set {} S	Authorization type none – without authorization; register – REGISTER authorization; register_and_invite – REGISTER and INVITE authorization.
stSetAuthLog	1.3.6.1.4.1.35265.1.29.38.15.1.14	Get {} Set {} S	Login for authorization
stSetAuthPass	1.3.6.1.4.1.35265.1.29.38.15.1.15	Get {} Set {} S	Authorization password
stSetCliro	1.3.6.1.4.1.35265.1.29.38.15.1.16	Get {} Set {} N	CLIRO service 0 – not installed; 1 – installed
stSetPbxProfile	1.3.6.1.4.1.35265.1.29.38.15.1.17	Get {} Set {} N	PBX profile
stSetAccessMode	1.3.6.1.4.1.35265.1.29.38.15.1.18	Get {} Set {} N	Customer service mode 0 – Enabled; 1 – Disabled 1; 2 – Disabled 2; 3 – ban 1; 4 – ban 2; 5 – ban 3; 6 – ban 4; 7 – ban 5; 8 – ban 6; 9 – ban 7; 10 – ban 8; 11 – excluded; 12 – disabled
stSetLines	1.3.6.1.4.1.35265.1.29.38.15.1.19	Get {} Set {} N	The number of lines in combined mode operation
stSetNoSRCportControl	1.3.6.1.4.1.35265.1.29.38.15.1.20	Get {} Set {} N	Do not consider the source port after registration 0 – consider; 1 – do not consider
stSetBLFusage	1.3.6.1.4.1.35265.1.29.38.15.1.21	Get {} Set {} N	Event subscription (BLF) 0 – deny;

Name	OID	Requests	Description
			1 – allow
stSetBLFsubscribers	1.3.6.1.4.1.35265.1.29.38.15.1.22	Get {} Set {} N	The quantity of event subscribers
stSetIntercomMode	1.3.6.1.4.1.35265.1.29.38.15.1.23	Get {} Set {} N	Intercom call type 0 – One-sided; 1 – Two-sided; 2 – Regular call; 3-Reject
stSetIntercomPriority	1.3.6.1.4.1.35265.1.29.38.15.1.24	Get {} Set {} N	Intercom call priority (1..5)
stSetLinesMode	1.3.6.1.4.1.35265.1.29.38.15.1.25	Get {} Set {} N	Line operation mode 0 – Combined; 1 – separate.
stSetIngressLines	1.3.6.1.4.1.35265.1.29.38.15.1.26	Get {} Set {} N	The quantity of ingress lines while operation in separate mode. 0 – unlimited
stSetEgressLines	1.3.6.1.4.1.35265.1.29.38.15.1.27	Get {} Set {} N	The quantity of egress lines while operation in separate mode. 0 – unlimited
stSetMonitoringGroup	1.3.6.1.4.1.35265.1.29.38.15.1.28	Get {} Set {} N	BLF monitoring group
stSetIntercomHeader	1.3.6.1.4.1.35265.1.29.38.15.1.29	Get {} Set {} N	Set SIP-header for intercom: 0 – Answer-Mode: Auto 1 – Alert-Info: Auto Answer 2 – Alert-Info: info=alert-autoanswer 3 – Alert-Info: Ring Answer 4 – Alert-Info: info=RingAnswer 5 – Alert-Info: Intercom 6 – Alert-Info: info=intercom 7 – Call-Info: =\;answer-after=0 8 – Call-Info: \;\;answer-after=0 9 – Call-Info: ;answer-after=0
stSetIntercomTimer	1.3.6.1.4.1.35265.1.29.38.15.1.30	Get {} Set {} N	Set pre-answering pause which will be transmitted in 'answer-after' parameter

Monitoring and configuration of dynamic subscriber groups

The commands for SNMP utilities call are represented in description of monitoring and configuration functions as follows:

Swalk script that implements the reading values:

```
#!/bin/bash
/usr/bin/snmpwalk -v2c -c public -m +ELTEX-SMG 192.0.2.1 "$@"
```

Sset script that implements value setting:

```
#!/bin/bash
/usr/bin/snmpset -v2c -c private -m +ELTEX-SMG 192.0.2.1 "$@"
```

Monitoring



Only authorized subscribers will be displayed while dynamic subscriber search.

You can monitor dynamic subscriber by using the next ways:

- by group or subscriber index;
- by subscriber ID;
- by numbering plan and full subscriber number;
- by numbering plan and partial subscriber number.

To monitor:

- Reset the search status;
- Set the search criteria (optionally);
- Display information.

Example of a search by index

```
sset groupResetCheck.0 i 1           # reset status of the search
sset getGroupByIndex.0 i 0           # select zero group
sset getGroupUserByIndex.0 i 4       # set up the search by index 4
swalk tableOfGroupUsers              # query of the table with the subscriber information
```

Result:

```
ELTEX-SMG::GroupUserID.0.4 = INTEGER: 4
ELTEX-SMG::RegState.0.4 = INTEGER: 1
ELTEX-SMG::Numplan.0.4 = INTEGER: 0
ELTEX-SMG::Number.0.4 = STRING: 240011
ELTEX-SMG::Ip.0.4 = IpAddress: 192.0.2.32
ELTEX-SMG::Port.0.4 = Gauge32: 5060
ELTEX-SMG::Domain.0.4 = STRING: dynsmg
ELTEX-SMG::MaxActiveLines.0.4 = INTEGER: -1
ELTEX-SMG::ActiveCallCount.0.4 = INTEGER: -1
ELTEX-SMG::RegExpires.0.4 = INTEGER: 55
ELTEX-SMG::TableOfGroupUsersEntry.13.0.4 = INTEGER: 1
ELTEX-SMG::TableOfGroupUsersEntry.14.0.4 = INTEGER: 3
ELTEX-SMG::TableOfGroupUsersEntry.15.0.4 = INTEGER: 4
ELTEX-SMG::TableOfGroupUsersEntry.16.0.4 = INTEGER: 0
ELTEX-SMG::TableOfGroupUsersEntry.17.0.4 = INTEGER: 0
```

Example of a search by subscriber ID

```
sset groupResetCheck.0 i 1           # reset status of the search
sset getGroupUserByID.0 i 2          # set subscriber ID
swalk tableOfGroupUsers              # query of the table with the subscriber information
```

Example of a search by numbering plan and partial number

```
sset groupResetCheck.0 i 1           # reset status of the search
sset getGroupUserByNumplan.0 i 0     # set zero numbering plan
sset getGroupUserBySubNumber.0 s 24001 # install part of number
swalk tableOfGroupUsers              # query of the table with the subscriber information
```

Result:

```
ELTEX-SMG::GroupUserID.0.0 = INTEGER: 0
ELTEX-SMG::GroupUserID.0.1 = INTEGER: 1
ELTEX-SMG::RegState.0.0 = INTEGER: 1
```

```
ELTEX-SMG::RegState.0.1 = INTEGER: 1
ELTEX-SMG::Numplan.0.0 = INTEGER: 0
ELTEX-SMG::Numplan.0.1 = INTEGER: 0
ELTEX-SMG::Number.0.0 = STRING: 240015
ELTEX-SMG::Number.0.1 = STRING: 240014
ELTEX-SMG::Ip.0.0 = IpAddress: 192.0.2.32
ELTEX-SMG::Ip.0.1 = IpAddress: 192.0.2.32
ELTEX-SMG::Port.0.0 = Gauge32: 5060
ELTEX-SMG::Port.0.1 = Gauge32: 5060
ELTEX-SMG::Domain.0.0 = STRING: dynsmg
ELTEX-SMG::Domain.0.1 = STRING: dynsmg
ELTEX-SMG::MaxActiveLines.0.0 = INTEGER: -1
ELTEX-SMG::MaxActiveLines.0.1 = INTEGER: -1
ELTEX-SMG::ActiveCallCount.0.0 = INTEGER: -1
ELTEX-SMG::ActiveCallCount.0.1 = INTEGER: -1
ELTEX-SMG::RegExpires.0.0 = INTEGER: 98
ELTEX-SMG::RegExpires.0.1 = INTEGER: 100
ELTEX-SMG::TableOfGroupUsersEntry.13.0.0 = INTEGER: 1
ELTEX-SMG::TableOfGroupUsersEntry.13.0.1 = INTEGER: 1
ELTEX-SMG::TableOfGroupUsersEntry.14.0.0 = INTEGER: 3
ELTEX-SMG::TableOfGroupUsersEntry.14.0.1 = INTEGER: 3
ELTEX-SMG::TableOfGroupUsersEntry.15.0.0 = INTEGER: 4
ELTEX-SMG::TableOfGroupUsersEntry.15.0.1 = INTEGER: 4
ELTEX-SMG::TableOfGroupUsersEntry.16.0.0 = INTEGER: 0
ELTEX-SMG::TableOfGroupUsersEntry.16.0.1 = INTEGER: 0
ELTEX-SMG::TableOfGroupUsersEntry.17.0.0 = INTEGER: 0
ELTEX-SMG::TableOfGroupUsersEntry.17.0.1 = INTEGER: 0
```

View information without using search

```
sset groupResetCheck.0 i 1          # reset status of the search
swalk tableOfGroupUsers             # show all subscribers
```

Configuration

Configuration involves the following operations on dynamic subscribers groups:

- Settings viewing;
- Settings editing;
- Creating a new subscriber;
- Removing.

To view settings:

- Set subscriber group by index or ID;
- Select configuration mode - view;
- Display the necessary

To edit settings:

- Set subscriber group by index or ID;
- Select configuration mode - edit;
- Set the required settings;
- Apply the settings.

To create a new group:

- Select configuration mode - creation;
- Define necessary settings of a new group;
- Apply the settings.

To remove a group:

- Set subscriber group by index or ID;
- Select configuration mode - removing;
- Apply the settings.

You can cancel changes that were not applied only in 'Add new group' and 'Edit a group' mode.



Undo group remove is not possible. Only a complete configuration restore via WEB or CLI is available.

Example of a new group creation

```
sset groupSetMode.0 i 3          # set the 'add' mode
sset groupSetApply.0 i 1        # apply the settings
sset groupSetMode.0 i 0        # set the 'none' mode
```

Example of settings viewing

```
sset groupByIndex.0 i 2        # select group by index - second
sset groupSetMode.0 i 1        # set the 'show' mode
swalk tableOfGroupSet          # view the settings table, or
swalk groupSetMaxReg           # maximum number of subscribers in the group, or
swalk groupSetName             # the name of the group, etc.
```

Example of settings editing

```
sset groupByID.0 i 3           # select group by index - third
sset groupSetMode.0 i 2        # set the 'set' mode
sset groupSetClir.0 i 1        # connect the CLIR service
sset groupSetNumplan.0 i 3     # set the third numbering plan
sset groupSetIntercomMode.0 i 3 # forbid intercom calls
sset groupSetApply.0 i 1       # apply the settings
sset groupSetMode.0 i 0       # set the 'none' mode
```

Example of group removing

```
sset groupByID.0 i 3           # select group by ID - third
sset groupSetMode.0 i 4        # set the 'del' mode
sset groupSetApply.0 i 1       # apply the settings
                                # you do not need to set the 'none' mode manually
```

Table M.8 – Monitoring and configuration of dynamic subscriber groups

Name	OID	Requests	Description
smgSipUserGroup	1.3.6.1.4.1.35265.1.29.39	Get {}	The list of dynamic subscriber groups, root object.
groupCheckStatus	1.3.6.1.4.1.35265.1.29.39.1	Get {}	Status of the search by criteria. None – without a search, displays all dynamic subscribers; Find user by group and user index; Find user by ID; Find user by numplan and number;

Name	OID	Requests	Description
			Find user by numplan and number
groupResetCheck	1.3.6.1.4.1.35265.1.29.39.2	Set {} N	Reset search status to 'None'. Set any value to reset.
numGroups	1.3.6.1.4.1.35265.1.29.39.3	Get {}	Number of subscriber groups
numInGroup	1.3.6.1.4.1.35265.1.29.39.4	Set {} N	The quantity of subscribers in a group. Set a group number, and you will receive the number of subscribers. If you receive '-1' in reply, it means that the group with this number does not exist.
numActiveInGroup	1.3.6.1.4.1.35265.1.29.39.5	Set {} N	The quantity of active (authorized) subscribers in the group. Set a group number, and you will receive the number of subscribers. If you receive '-1' in reply, it means that the group with this number does not exist.
getGroupByIndex	1.3.6.1.4.1.35265.1.29.39.6	Set {} N	Set subscriber index for searching of by group index. The search status will be changed to 'Find user by numplan and number', if you set '1' or greater as a group index. If you set '-1' value, the status of search will be changed to 'None'. If you set group index which does not exist, the status of search will be reset to 'None'.
getGroupUserByIndex	1.3.6.1.4.1.35265.1.29.39.7	Set {} N	Set subscriber index in a group for search by group index. Set index of the group before start. (see GetGroupByIndex). The status of the search will be set to 'Find user by numplan and number'. Setting '-1' value makes search status changed from 'Find user by group and user index' to 'None'.
getGroupUserByID	1.3.6.1.4.1.35265.1.29.39.8	Set {} U	Set ID in order to search a subscriber. Setting '1' and greater numbers makes search status changed to 'Find user by ID'. If you set '0' value, the status will be changed from 'Find user by ID' to 'None'.

Name	OID	Requests	Description
getGroupUserByNumplan	1.3.6.1.4.1.35265.1.29.39.9	Set {} N	Set a dial plan in order to search subscriber by the number and dial plan. If you set '-1' value, the status of search will be changed to 'None'. If the value is greater than 0, the status will be set to 'Find user by numplan and number' (see getGroupUserByNumber). Otherwise, the status of search will not be changed.
getGroupUserByNumber	1.3.6.1.4.1.35265.1.29.39.10	Set {} S Set {} "NULL"	Set a number in order to search subscriber by the number and numbering plan. The length of a number should be from 1 to 32 characters. If you set '0' or greater, the search status will be changed to 'Find user by numplan and number', otherwise, the status will not be changed. Set 'NULL' to reset a number, the search status will be changed to 'None' in this case.
getGroupUserBySubNumber	1.3.6.1.4.1.35265.1.29.39.11	Set {} S	Set part of a number and numbering plan for subscriber search. The length of a number from 1 to 32 characters. If you set '0' or greater, the status of the search will be set to 'Find user by numplan and substring number', otherwise the status will not be changed. Set 'NULL' to reset a number, the search status will be changed to 'None' in this case.
tableOfGroupUsers	1.3.6.1.4.1.35265.1.29.39.12	Get {}	Dynamic subscriber table, root object
tableOfGroupUsersEntry	1.3.6.1.4.1.35265.1.29.39.12.1	Get {}	see TableOfGroupUsers
groupUserID	1.3.6.1.4.1.35265.1.29.39.12.1.3 1.3.6.1.4.1.35265.1.29.39.12.1.3.x.x	Get {} Get {}.x.x	Subscriber ID. Add subscriber index to OID to obtain information on this subscriber.
groupUserRegState	1.3.6.1.4.1.35265.1.29.39.12.1.4 1.3.6.1.4.1.35265.1.29.39.12.1.4.x.x	Get {} Get {}.x.x	State of subscriber registration. Add subscriber index to OID to

Name	OID	Requests	Description
			obtain information on this subscriber. 0 – not registered; 1 – registered
groupUserNumplan	1.3.6.1.4.1.35265.1.29.39.12.1.5 1.3.6.1.4.1.35265.1.29.39.12.1.5.x.x	Get {} Get {}.x.x	Numbering plan of the subscriber. Add subscriber index to OID to obtain information on this subscriber.
groupUserNumber	1.3.6.1.4.1.35265.1.29.39.12.1.6 1.3.6.1.4.1.35265.1.29.39.12.1.6.x.x	Get {} Get {}.x.x	Subscriber number Add subscriber index to OID to obtain information on this subscriber.
groupUserIp	1.3.6.1.4.1.35265.1.29.39.12.1.7 1.3.6.1.4.1.35265.1.29.39.12.1.7.x.x	Get {} Get {}.x.x	Subscriber IP address. Add subscriber index to OID to obtain information on this subscriber. If the address is unknown, the '0.0.0.0' value will be set.
groupUserPort	1.3.6.1.4.1.35265.1.29.39.12.1.8 1.3.6.1.4.1.35265.1.29.39.12.1.8.x.x	Get {} Get {}.x.x	Subscriber port. Add subscriber index to OID to obtain information on this subscriber.
groupUserDomain	1.3.6.1.4.1.35265.1.29.39.12.1.9 1.3.6.1.4.1.35265.1.29.39.12.1.9.x.x	Get {} Get {}.x.x	SIP-domain of the subscriber. Add subscriber index to OID to obtain information on this subscriber.
groupUserMaxActiveLines	1.3.6.1.4.1.35265.1.29.39.12.1.10 1.3.6.1.4.1.35265.1.29.39.12.1.10.x.x	Get {} Get {}.x.x	The quantity of ingress/egress lines while operation in combined line mode. Add subscriber index to OID to obtain information on this subscriber.
groupUserActiveCallCount	1.3.6.1.4.1.35265.1.29.39.12.1.11 1.3.6.1.4.1.35265.1.29.39.12.1.11.x.x	Get {} Get {}.x.x	The quantity of active calls while operation in combined mode. Add subscriber index to OID to obtain information on this subscriber.
groupUserRegExpires	1.3.6.1.4.1.35265.1.29.39.12.1.12 1.3.6.1.4.1.35265.1.29.39.12.1.12.x.x	Get {} Get {}.x.x	Time to registration expiry, in seconds. Add subscriber ID and group index to OID to obtain information on the subscriber.

Name	OID	Requests	Description
groupUserLinesMode	1.3.6.1.4.1.35265.1.29.39.12.1.13 1.3.6.1.4.1.35265.1.29.39.12.1.13.x x	Get {} Get {}.x.x	Line operation mode Add subscriber index to OID to obtain information on this subscriber. 0 – Combined; 1 – separate.
groupUserMaxIngress Lines	1.3.6.1.4.1.35265.1.29.39.12.1.14 1.3.6.1.4.1.35265.1.29.39.12.1.14.x x	Get {} Get {}.x.x	The quantity of ingress lines while operation in separate mode. Add subscriber index to OID to obtain information on this subscriber.
groupUserMaxEgress Lines	1.3.6.1.4.1.35265.1.29.39.12.1.15 1.3.6.1.4.1.35265.1.29.39.12.1.15.x x	Get {} Get {}.x.x	The quantity of egress lines while operation in separate mode. Add subscriber index to OID to obtain information on this subscriber.
groupUserActiveIngressCount	1.3.6.1.4.1.35265.1.29.39.12.1.16 1.3.6.1.4.1.35265.1.29.39.12.1.16.x x	Get {} Get {}.x.x	The quantity of active ingress calls while operation in separate mode. Add subscriber index to OID to obtain information on this subscriber.
groupUserActiveEgressCount	1.3.6.1.4.1.35265.1.29.39.12.1.17 1.3.6.1.4.1.35265.1.29.39.12.1.17.x x	Get {} Get {}.x.x	The quantity of active egress calls while operation in separate mode. Add subscriber index to OID to obtain information on this subscriber.
groupUserGroupModeSettings	1.3.6.1.4.1.35265.1.29.39.13	Get {}	Dynamic subscriber group operation settings modes None – work with settings is disabled; Show – show the group settings; Set – change group settings; Add - add a group; Del - delete a group
groupUserGroupSetMode	1.3.6.1.4.1.35265.1.29.39.14	Set {} N	Set a mode for subscriber group operation 0 - None; 1 - Show; 2 - Set;

Name	OID	Requests	Description
			3 - Add; 4 - Del
groupUserGroupSetReset	1.3.6.1.4.1.35265.1.29.39.15	Set {} N	Reset setting changes (if they have not been applied) in 'Set' and 'Add' modes, in other modes this command is ignored.
groupUserGroupSetApply	1.3.6.1.4.1.35265.1.29.39.16	Set {} N	<p>Apply settings, add or remove groups.</p> <p>New settings are activated in the 'Set' mode;</p> <p>In the 'Add' mode new group is created and index for group search is set equal to the created group index, status of the search changes to 'Find group settings by index' and settings operation mode sets to 'Show'.</p> <p>In 'Del' mode, group is deleted, search status and settings operation mode set to 'None'.</p> <p>The inquiry is ignored in 'None' and 'Show' modes.</p>
groupUserGroupFindStatus	1.3.6.1.4.1.35265.1.29.39.17	Get {}	<p>Status of settings search by criteria:</p> <p>Without search;</p> <p>Find group settings by Index;</p> <p>Find group settings by ID</p>
groupFindStatus	1.3.6.1.4.1.35265.1.29.39.17	Get {}	<p>Status of settings search by criteria:</p> <p>Without search;</p> <p>Find group settings by Index;</p> <p>Find group settings by ID</p>
groupResetFindStatus	1.3.6.1.4.1.35265.1.29.39.18	Set {} N	Reset status of search to 'without search' status. Set any value to reset.
groupByIndex	1.3.6.1.4.1.35265.1.29.39.19	Set {} N	<p>Set group index and status of the search as 'Find group settings by index'.</p> <p>If you set '-1', the status will change from 'Find group settings by index' to 'Without search'.</p>

Name	OID	Requests	Description
groupByID	1.3.6.1.4.1.35265.1.29.39.20	Set {} N	Set the group ID (from 1 and greater) and status of the search as 'Find group settings by ID'. If you set '-1', the status will change from 'Find group settings by ID' to 'Without search'.
tableOfGroupSet	1.3.6.1.4.1.35265.1.29.39.21	Get {}	Table of dynamic subscriber group settings.
tableOfGroupSetEntry	1.3.6.1.4.1.35265.1.29.39.21.1	Get {}	see TableOfGroupSet
groupSetId	1.3.6.1.4.1.35265.1.29.39.21.1.2	Get {}	Group ID
groupSetName	1.3.6.1.4.1.35265.1.29.39.21.1.3	Get {} Set {} S	Group name
groupSetSIPdomain	1.3.6.1.4.1.35265.1.29.39.21.1.4	Get {} Set {} S	SIP domain
groupSetMaxReg	1.3.6.1.4.1.35265.1.29.39.21.1.5	Get {} Set {} N	The maximum number of subscribers in a group
groupSetProfile	1.3.6.1.4.1.35265.1.29.39.21.1.6	Get {} Set {} S	SIP profile
groupSetCategory	1.3.6.1.4.1.35265.1.29.39.21.1.7	Get {} Set {} N	Caller ID Category 0 – No change (from call); 1..10 – select category
groupSetAccessCat	1.3.6.1.4.1.35265.1.29.39.21.1.8	Get {} Set {} N	Access category
groupSetCliro	1.3.6.1.4.1.35265.1.29.39.21.1.9	Get {} Set {} N	CLIRO service 0 – not installed; 1 – installed
groupSetPbxProfile	1.3.6.1.4.1.35265.1.29.39.21.1.10	Get {} Set {} N	PBX profile
groupSetAccessMode	1.3.6.1.4.1.35265.1.29.39.21.1.11	Get {} Set {} N	Customer service mode 0 – Enabled; 1 – Disabled 1; 2 – Disabled 2; 3 – ban 1; 4 – ban 2; 5 – ban 3; 6 – ban 4; 7 – ban 5; 8 – ban 6; 9 – ban 7; 10 – ban 8; 11 – excluded; 12 – disabled

Name	OID	Requests	Description
groupSetLines	1.3.6.1.4.1.35265.1.29.39.21.1.12	Get {} Set {} N	The quantity of lines while operation in combined mode.
groupSetNumplan	1.3.6.1.4.1.35265.1.29.39.21.1.13	Get {} Set {} N	Numbering schedule
groupSetNoSRCportControl	1.3.6.1.4.1.35265.1.29.39.21.1.14	Get {} Set {} N	Do not consider the source port after registration 0 – consider; 1 – do not consider
groupSetBLFusage	1.3.6.1.4.1.35265.1.29.39.21.1.15	Get {} Set {} N	Event subscription (BLF) 0 – deny; 1 – allow
groupSetBLFsubscribers	1.3.6.1.4.1.35265.1.29.39.21.1.16	Get {} Set {} N	The quantity of event subscribers
groupSetIntercomMode	1.3.6.1.4.1.35265.1.29.39.21.1.17	Get {} Set {} N	Intercom call type 0 – One-sided; 1 – Two-sided; 2 – Regular call; 3-Reject
groupSetIntercomPriority	1.3.6.1.4.1.35265.1.29.39.21.1.18	Get {} Set {} N	Intercom call priority (1..5)
groupSetLinesMode	1.3.6.1.4.1.35265.1.29.39.21.1.19	Get {} Set {} N	Line operation mode 0 – Combined; 1 – separate.
groupSetIngressLines	1.3.6.1.4.1.35265.1.29.39.21.1.20	Get {} Set {} N	The quantity of ingress lines while operation in separate mode.
groupSetEgressLines	1.3.6.1.4.1.35265.1.29.39.21.1.21	Get {} Set {} N	The quantity of egress lines while operation in separate mode.
groupSetAONtypeNumber	1.3.6.1.4.1.35265.1.29.39.21.1.22	Get {} Set {} N	Type of caller ID number 0 – Unknown; 1 – Subscriber; 2 – National; 3 – International; 4 – Network specific; 5 – No change (from call)
groupSetMonitoringGroup	1.3.6.1.4.1.35265.1.29.39.21.1.23	Get {} Set {} N	BLF monitoring group
groupSetIntercomHeader	1.3.6.1.4.1.35265.1.29.39.21.1.24	Get {} Set {} N	Set SIP-header for intercom: 0 – Answer-Mode: Auto 1 – Alert-Info: Auto Answer 2 – Alert-Info: info=alert-autoanswer 3 – Alert-Info: Ring Answer 4 – Alert-Info: info=RingAnswer 5 – Alert-Info: Intercom 6 – Alert-Info: info=intercom 7 – Call-Info: =\;answer-after=0 8 – Call-Info: \\;answer-after=0

Name	OID	Requests	Description
			9 – Call-Info: ;answer-after=0
groupSetIntercomTimer	1.3.6.1.4.1.35265.1.29.39.21.1.25	Get {} Set {} N	Set pre-answering pause which will be transmitted in 'answer-after' parameter

Obsolete OIDs

Some OIDs have been changed and old branches can be removed or replaced by new one in the next releases. It is recommended to reconfigure monitoring systems and scripts for using new OIDs.

Table M. 9 – Obsolete OID

Name	OID	Requests	Description
eOneRSV	1.3.6.1.4.1.35265.1.29.7.1.8 1.3.6.1.4.1.35265.1.29.7.1.8.x	Get {} Get {}.x	Not used
eOneRxEqualizer	1.3.6.1.4.1.35265.1.29.7.1.15 1.3.6.1.4.1.35265.1.29.7.1.15.x	Get {} Get {}.x	It is not supported in new firmware versions, always '-1'
smgCpuLoad	1.3.6.1.4.1.35265.1.29.17	Get {}	Replaced by smgCpuLoadTable (1.3.6.1.4.1.35265.1.29.37)
smgTopCpuUsr	1.3.6.1.4.1.35265.1.29.17.1.x	Get {}	Replaced by cpuUsr (1.3.6.1.4.1.35265.1.29.37.1.2.x)
smgTopCpuSys	1.3.6.1.4.1.35265.1.29.17.2.x	Get {}	Replaced by cpuSys (1.3.6.1.4.1.35265.1.29.37.1.3.x)
smgTopCpuNic	1.3.6.1.4.1.35265.1.29.17.3.x	Get {}	Replaced by cpuNic (1.3.6.1.4.1.35265.1.29.37.1.4.x)
smgTopCpuIdle	1.3.6.1.4.1.35265.1.29.17.4.x	Get {}	Replaced by cpuIdle (1.3.6.1.4.1.35265.1.29.37.1.5.x)
smgTopCpuIo	1.3.6.1.4.1.35265.1.29.17.5.x	Get {}	Replaced by cpuIo (1.3.6.1.4.1.35265.1.29.37.1.6.x)
smgTopCpuIrq	1.3.6.1.4.1.35265.1.29.17.6.x	Get {}	Replaced by cpuIrq (1.3.6.1.4.1.35265.1.29.37.1.7.x)
smgTopCpuSirq	1.3.6.1.4.1.35265.1.29.17.7.x	Get {}	Replaced by cpuSirq (1.3.6.1.4.1.35265.1.29.37.1.8.x)
smgTopCpuUsage	1.3.6.1.4.1.35265.1.29.17.8.x	Get {}	Replaced by cpuUsage (1.3.6.1.4.1.35265.1.29.37.1.9.x)

Support for OID MIB-2 (1.3.6.1.2.1)

SMG supports the following MIB-2 branches:

- system (1.3.6.1.2.1.1) – common information on the system;
- interfaces (1.3.6.1.2.1.2) – information on network interfaces;
- snmp (1.3.6.1.2.1.11) – information on SNMP operation.

TECHNICAL SUPPORT

For technical assistance in issues related to handling of ELTEXALATAU Ltd. equipment please address to Service Centre of the company:

Republic of Kazakhstan, 050032, Medeu district, microdistrict Alatau, 9 st. Ibragimova, 9

Phone:

+7(727) 220-76-10

+7(727) 220-76-07

E-mail: post@eltexalatau.kz

In official website of the ELTEXALATAU Ltd. you can find technical documentation and software for products, refer to knowledge base, consult with engineers of Service center in our technical forum:

<http://www.eltexalatau.kz/en/>