Enterprise IP PBX

SMG-200, SMG-500

Operation manual, firmware version 3.20.3

SMG-200 firmware version: V. 3.20.3
SMG-500 firmware version: V. 3.20.3

Document version	Firmware version	Issue date	Revisions
Version 3.5	V.3.20.3	14 November 2022	Added: – ‘Direction of Echo Cancellation’ option for fxs/fxo ports – ‘Notify call completion in (sec) before’ option on the prefix in the dial plan – Ability to upload cdr files via SCP protocol – SD card monitoring via SNMP – ‘Replace symbol ‘?’ by ‘D’ in CgPN’ option for Q.931 protocol – ‘DSCP for RTP’ option for SIP interfaces – ‘CISCO 1700 Adaptation’ option for H.323 interfaces Changed: – ‘VAS: Reset timeout’ option for dynamic subscribers has been removed
Version 3.4	V.3.20.0	31 July 2022	Added: – VAS: ‘One Touch Record’ – ‘Silent’ clear mode for hunt groups – Disk monitoring via SNMP – RedirPN modification for RADIUS – ‘AND’ logic in the dial plan – Name transferring method for H323 interfaces – Ability to clear queue statistics – ‘Recall declined’ option in hunt group; – ‘Enable inband DTMF’ option – ‘SLC engagement order’ option – SNMP request for obtaining IP address value from network interface – Ring-back tone settings for a hunt group when using a queue – Ability to monitor active web interface sessions – ‘Notify about the start of intervention’ option – Modifiers of outgoing communication to PRI profile – VAS: ‘Speed dialing’ (FXS) – DHCP server – Signal gain/decay options on FXO/FXS ports – Unconditional use of hair-pinning echo cancellation method for E1-E1 calls Changed: – Logging has been reworked – Number of consecutive redirects has been increased to 10
Version 3.3	V.3.19.0	15 July 2020	Added: – Multiple registration (SIP forking) – Routing by access category – ‘Real IP’ sending into RADIUS-Accounting – Radius request statistics via SNMP – Listening to call recordings without the possibility of downloading – Automatic enabling of logging after restarting the

			gateway – Sending a Display name when calling through a hunt group – Voice mail. Playing message details – Access category for Dial block in IVR Changed: – When using VAS DND, response from 502 to 486 busy here has been changed – Transport mode operation on SIP interfaces (one mode is allowed per port)
Version 3.2	V.3.18.0	3 July 2020	Added: – VAS: Call intervention – Detecting the subscriber phone on the FXS line – Hotline for FXS – SIP subscriber registration from an arbitrary network interface – Routing by TO instead of RURI (optional); – 'SIP Header Transit' option for SIP profile – Voice mail – Optional CPC defining on FXO – Command Line Interface (CLI) Changed: – Call group member number has been added to the call record – List of active alarm events has been added – Transport protocol setting is now on every SIP-interface
Version 3.1	V.3.17.4	16 December 2019	Synchronized with firmware version 3.17.4
Version 3.0	V.3.17.0	6 December 2019	Added: – Support for operation with a remote LDAP server – Local LDAP server – VAS: 'Call Parking' – Advanced sip profile settings – Ability to use Login as User-Name when authorization/accounting via Radius – Defining call group number in a call record if the call was established through the group to a certain subscriber – Dial sequence for FXO support – Offroad mode video support – 'Display Name' for FXS port support Changed: – Changing settings in web-interface has been changed from drop-down list to tabs for convenience – Broadcast address setting on network interfaces has been removed (automatic filling) – Playing time and position in a queue have been moved to two different functions (hunt group) – 'Modifier' prefix type has been renamed to 'Subscriber capacity' – 'Direct prefix availability control' has been renamed to 'Block if direct prefix is unavailable' (SMG-500) – 'Hotline' has been renamed to 'Hotline (incoming calls)'

			(SMG-200) – 'PSTN Hotline' to 'Hotline (outgoing calls)' (SMG-200)
Version 3.0	V.3.16.0	15 July 2019	Added: — Playing audio files as ringback tones — PRI subscribers (SMG-500): - PRI profile has been added - Multiple E1 streams support - Limited quantity of lines - Using different dial plans - Added call categories — Echo cancellation for SIP subscribers and trunks — Echo cancellation on FXS and FXO ports — Enhanced reception and transmission on FXO ports — FXS lines testing — AutoCLIP feature for FXO ports — Trunk group with FXO ports support — 'Handset is replaced' signal for FXS ports — Subscription (BLF) to FXS subscriber status — Monitoring and configuring FXS/FXO subscribers via SNMP — SNMP trap on E1 stream synchronization source change — SNMP OID including E1 stream name — Call forwarding on time and day of the week — External storage names are attached to interface ports — Blocking trunk when direct prefix is not available (SMG-500) — VAS: Intercom Changed: — Pickup group size has been increased to 60 participants; — Upper timeout limit in a hunt group has been increased to 3600 seconds; — Settings in the WEB have been sorted – the most used functions have been relocated to the top and logically grouped
Version 2.1	V.3.14.0	7 December 2018	Added: — VAS: 'Add-on conference' — VAS: 'Do not disturb' — VAS: 'Black list' — Public IP support — STUN support — FXS ports emergency blocks — Subscriber phone detection — Disabling FXS port — Battery status indication — NAT comedia support — Group editing of FXS/FXO ports — Automatic detection of FXS/FXO submodules type and version — Total number of calls monitoring — Voice gain control for receiving/transferring on FXS

			ports —WEB/telnet/SSH user authorization via RADIUS —Transmitting the received X-UniqueTag SIP header or generating it from a RADIUS Acct-Session-Id value —SNMP OID of SIP trunk availability —Ability to enable call traces by trunk group or phone number —Transmission of the Connected Name for SIP subscribers —Device-side release mark in CDR Changed: — Queue limit has been changed from 5–30 participants to 1–30 participants
Version 2.0	V.3.14.0	12 November 2018	Changed: 1.5 Main Specifications 1.7 Light indication 3.1.24 'Management' Menu 3.3 SMG configuration via Telnet, SSH or RS-232 3.3.1 List of CLI commands Added: 3.1.5.2.1 'Name transfer settings' tab 3.1.5.22 'Channel usage' tab 3.1.17.4 PRI subscribers
Version 1.1	V.3.11.2	31 May 2018	Changed: 3.1.2.9 Active Calls Monitoring 3.1.7.1 Trunk Groups Added: 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 sources (for SMG-500 only) 3.1.5 E1 streams 3.1.7.2 SS7 Linksets (for SMG-500 only)
Version 1.0	V.3.11.1	16 April 2018	Changed: 3.1.1 System Specifications 3.1.5.2 SIP/SIP-T/SIP-I interfaces, SIP profiles Added: 3.1.2.7 Active Calls Monitoring 3.1.5.3 H323 Interfaces 3.1.6.5 FXO Profiles Appendix B. Telephone line length calculation
Version 1.0	V.3.11.0	12 February 2018	First issue

EXPLANATION OF THE SYMBOLS USED

Symbol	Description
`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.

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 CONTENT

INTRODUCTION

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

The SMG-200 and SMG-500 PBXes allow connecting remote offices into a single network and creating remote workplaces, thus reducing the cost of intercity and international calls. In case of office relocation, telephone numbers will be preserved, which allows the company to always stay in touch with customers.

The high quality of voice processing by the enterprise IP PBXes SMG-200 and SMG-500 is provided by the up-to-date hardware platform, support for main audio codecs – G.711, G.729, echo cancellation, silence detector, comfort noise generator, as well as traffic prioritization mechanisms.

This operation manual presents 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 firmware-based operation and maintenance procedures.

1 PRODUCT DESCRIPTION

1.1 Purpose

Enterprise IP PBXes SMG-200 and SMG-500 are designed to organize telephone communication within the enterprise.

The basic configuration of the enterprise IP PBX SMG-200 is designed to connect up to 100 SIP subscribers and can be extended to connect up to 200 subscribers when purchasing the appropriate firmware. The basic configuration of SMG-500 is designed to connect up to 250 subscribers and can be extended to connect up to 500 subscribers.

SMG-200

16 RJ-11 ports can be used to connect analogue phones 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

The E1 ports and SIP trunks can be used for connection to PSTN. Analogue phones are connected to SMG-500 via subscriber VoIP gateways, while IP phones – directly via the data network.

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

1.2 SMG Main Specifications

Interfaces:

SMG-200

- 16 × FXS/FXO (RJ-11) ports;
- 4 × Ethernet 10/100/1000BASE-T (RJ-45) ports;
- 1 × USB 2.0, 1 × USB 3.0;
- 1 × SD card slot;
- 1 × COM port (RS-232, RJ-45).

SMG-500

- 4 × E1 (RJ-48) ports;
- 4 × Ethernet 10/100/1000BASE-T (RJ-45) ports;
- 1 × USB 2.0, 1 × USB 3.0;
- 1 × SD card slot;
- 1 × COM port (RS-232, RJ-45).

Features:

- SMG-200: up to 100 subscribers in the basic configuration with possible extension of up to 200 subscribers;
- SMG-500: up to 250 subscribers in the basic configuration with possible extension of up to 500 subscribers;
- Static address and DHCP support;
- IP telephone protocols: SIP, SIP-T, SIP-I, H.323;
- DTMF transmission (SIP INFO, RFC2833, in-band, SIP NOTIFY);
- SMG-500:
  - 4 × E1 Interfaces;
  - TDM protocols (SMG-500): DSS1/EDSS1 (ISDN PRI Q.931), QSIG and CORNET for subscriber ID transmission, SS7 (operation in associated and quasi-associated modes);
- Q.699 standard support — EDSS1 and SS7 interaction;
- SMG-200:
  - up to 16 FXS ports (increment value — 8);
  - up to 16 FXO ports (increment value — 8);
- Echo Cancellation (G.168 recommendation);
- Voice Activity Detector (VAD);
- Comfort Noise Generation (CNG);
- NTP support;
- DNS support;
- SNMP support;
- ToS and CoS for signaling;
- VLAN for RTP, signaling and management;
- Firmware update: via the web configurator, CLI (Telnet, SSH, console (RS-232));
- Configuration and setup (also remotely):
  - web configurator;
  - CLI (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;
- RFC 6432;
- Q1912.5 SIP-I;
- Interaction of SIP and SIP-T/SIP-I;
- SIP Enable/Disable 302 Responses;
- Delay offer;
- SIP OPTIONS Keep-Alive (SIP Busy Out);
- SIP registrar.

1.3 Use case

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

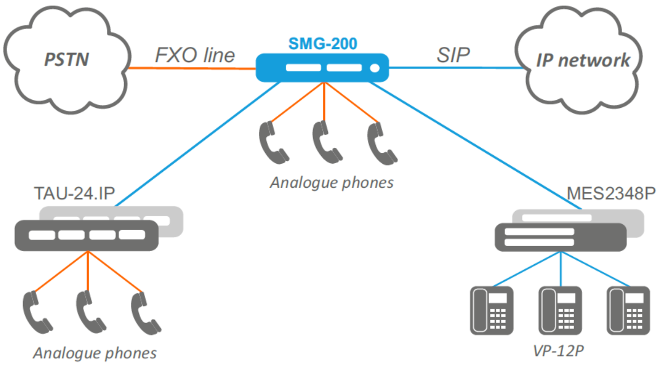


Fig. 1 – Enterprise IP PBX based on SMG-200

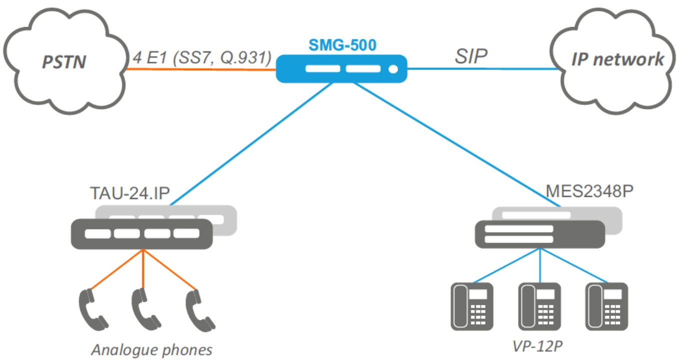


Fig. 2 – Enterprise IP PBX based on SMG-500

1.4 Device Design and Operating Principle

1.4.1 Structure of SMG-200

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

- A controller including the following:
  - a control processor;
  - 4 GB flash memory;
  - 2 GB RAM.
- up to 2 FXS analogue ports submodules;
- up to 2 FXO analog termination submodules;
- 4-port 10/100/1000BASE-T Ethernet switch (L2).

See the SMG-200 functional diagram in the figure below.

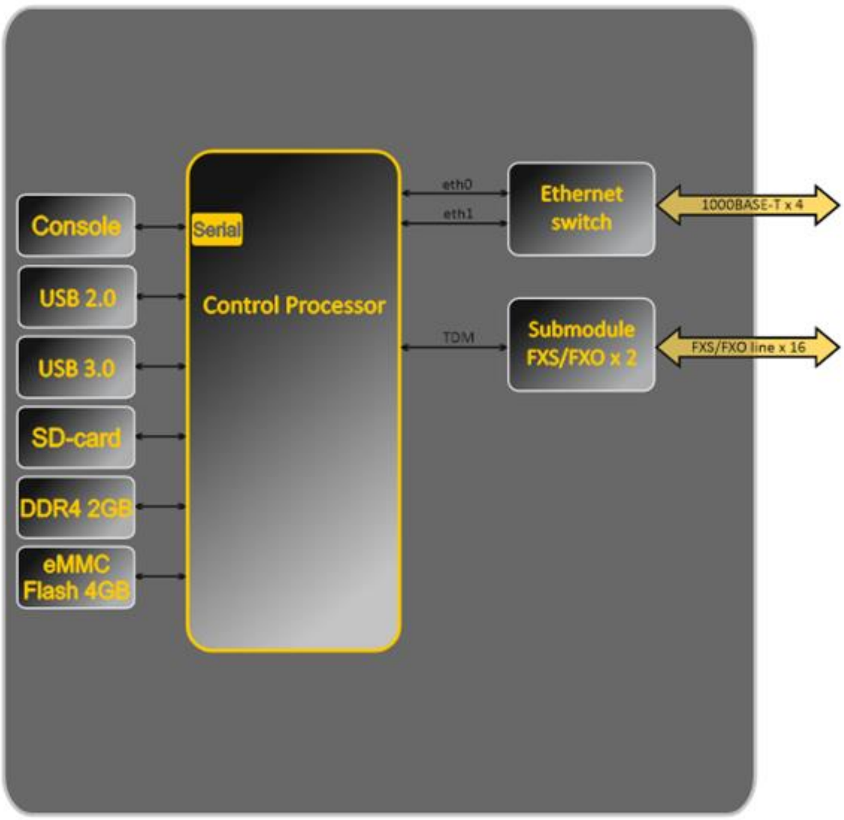


Fig. 3 – SMG-200 Functional Diagram

1.4.2 Structure of SMG-500

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

- A controller including the following:
  - A control processor;
  - 4 GB flash memory;
  - 2 GB RAM.
- E1 stream submodule C4E1;
- IP submodule SM-VP-M300;
- 4-port 10/100/1000BASE-T Ethernet switch (L2).

See the SMG-500 functional diagram in the figure below.

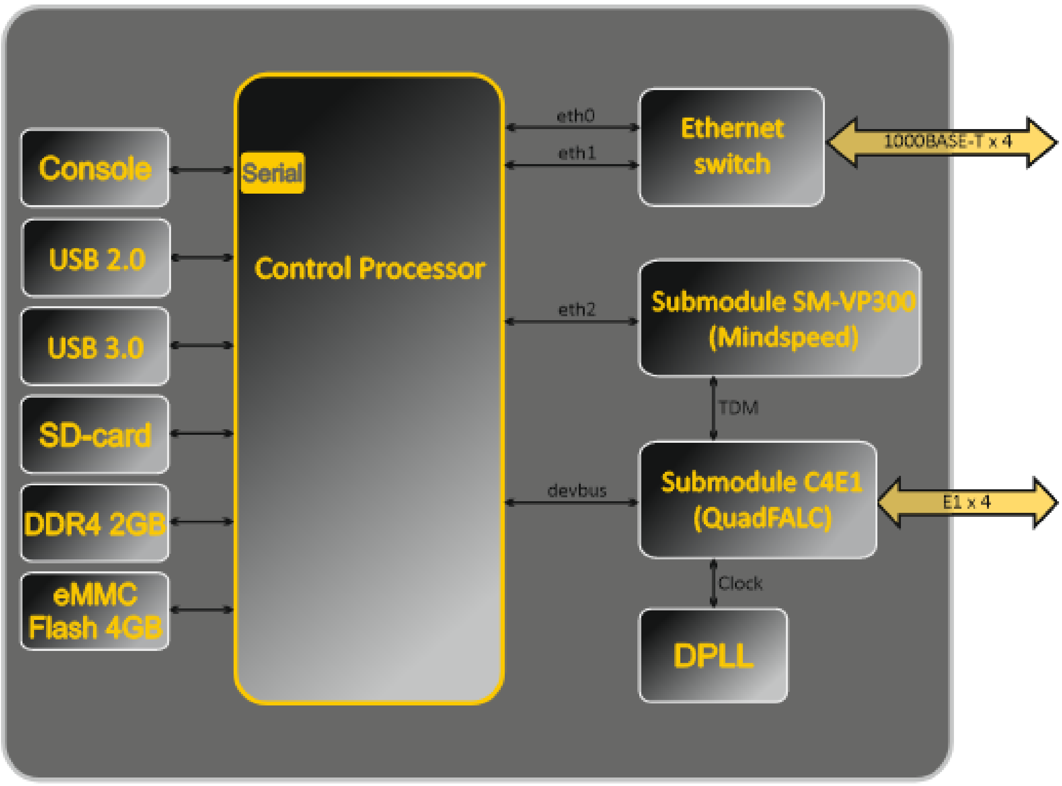


Fig. 4 – SMG-500 Functional Diagram

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 via the internal TDM trunk, then encoded with 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 device CPU, then decoded and transmitted via the internal TDM trunk to the FXS/FXO ports.

1.4.4 SMG-500 Operating Principle

In the 'TDM-to-IP' direction, the signal coming to the E1 streams is sent to the VoIP submodule via the internal trunk, then sent in the form of digital packets to the device CPU for processing, encoded with one of the selected standards, and transmitted to the Ethernet switch. In the 'IP-to-TDM' direction, digital packets from the Ethernet switch are sent for processing to the device CPU, decoded and then transmitted to the VoIP submodule and then transmitted via the internal trunk to the E1 streams.

It is required to install both submodules, the SM-VP and the C4E1, for E1 streams to operate on the SMG-500.

External 2 Mbps E1 streams are transmitted to framers via matching transformers. At that, synchronization signal is extracted from the stream and sent to the common synchronization line of the device. Synchronization line priority is managed at the firmware level according to the predefined algorithm.

See Fig. 5 for the device firmware architecture.

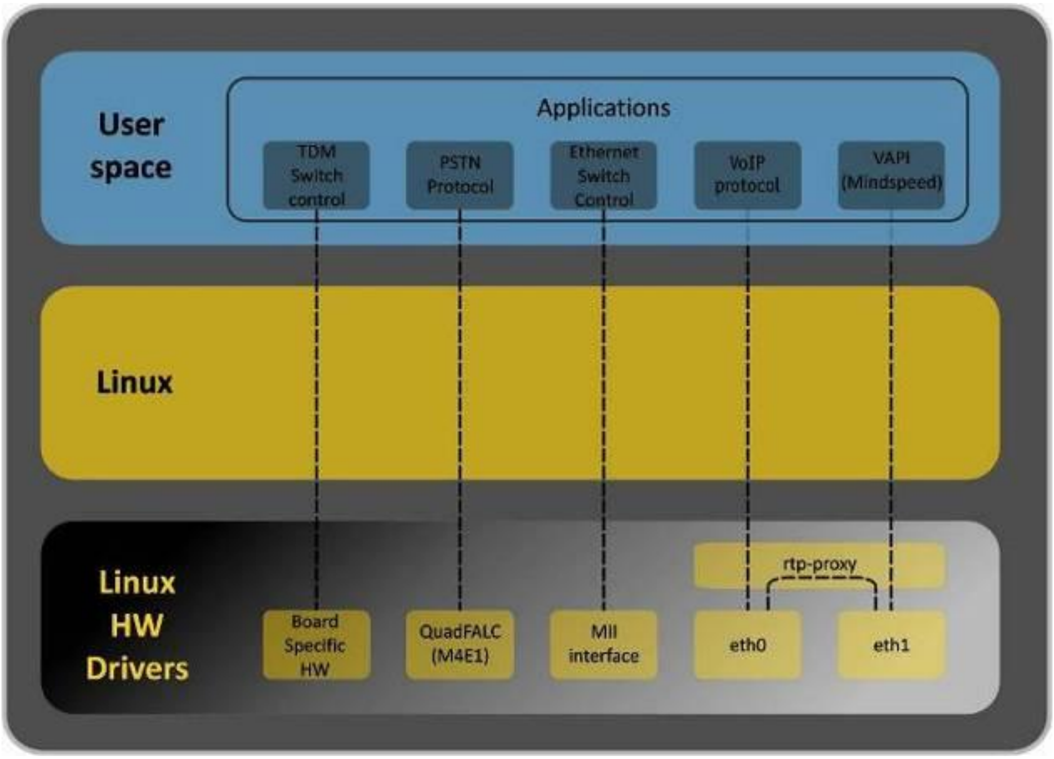


Fig. 5 – SMG firmware architecture

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-law (hereinafter — G.711A) G.711 μ-law (hereinafter — G.711U) G.729 (A/B) OPUS[1] AMR[1]

Number of simultaneous calls

SMG-200	50 (100 VoIP channels)
SMG-500	100 (200 VoIP channels)

Electrical Ethernet Interface Specifications

Number of interfaces	4
Electric connector	RJ-45
Data transfer rate	Autodetection, 10/100/1000 Mbps, duplex
Supported standards	10/100/1000BASE-T

Console parameters

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

FXS interface parameters (for SMG-200 only)

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

E1 interface parameters (for SMG-500 only)

Number 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

[1] Not supported in the current firmware version 3.20.3.

Elastic buffer	2 frame capacity
Signaling protocols	DSS1/EDSS1 (ISDN PRI Q.931), QSIG and CORNET for subscriber ID transmission, SS7

Number of conference participants

SMG-200/500	Maximum number of participants — 40

Supported file systems for external storages

SMG-200/500	MBR	USB flash — FAT32, ext2, ext3, ext4 USB HDD — ext2, ext3, ext4 SD card — FAT32, ext2, ext3, ext4
	GPT	USB flash — FAT32, ext2, ext3, ext4 USB HDD — ext2, ext3, ext4 SD card — FAT32, ext2, ext3, ext4

General Parameters

Operating temperature	From 0 to +40 °C	
Relative humidity	Up to 80 %	
Power supply	AC: 220 V+-20%, 50 Hz Lead-acid battery, 12 V • battery charge current: 1.6+-0.1 A, • low battery voltage threshold indication: 11 V, • voltage threshold for battery deep discharge protection: 10–10.5 V.	
Power consumption	No more than 40 W during battery charge, no more than 20 W without battery charge	
Dimensions (W × H × D)	SMG-200	SMG-500
	430 × 43.6 × 203.2 mm	430 × 43.6 × 203.2 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 shown in the figures below.

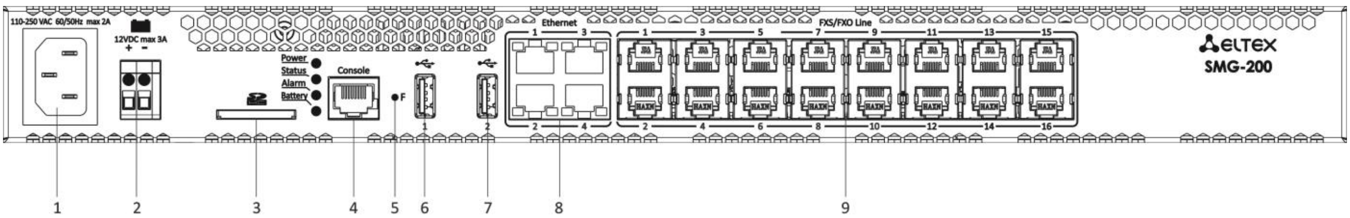


Fig. 6 – SMG-200 Front Panel

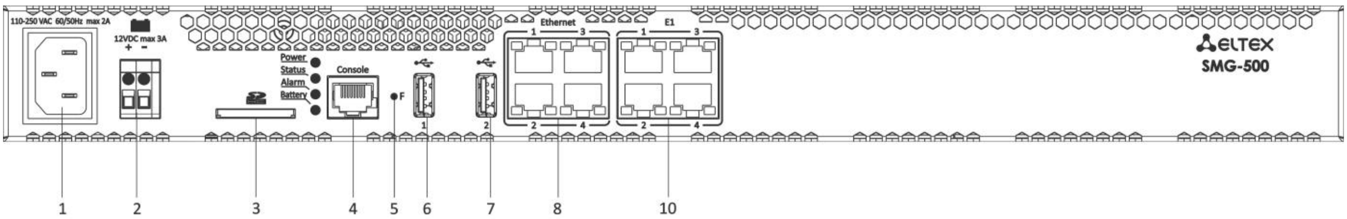


Fig. 7 – SMG-500 Front Panel

Connectors, LEDs, and controls located on the front panel of the devices are listed in the 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 control (see APPENDIX A. CABLE CONTACT PIN ASSIGNMENT for connector wiring)
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 × RJ-45 ports for Ethernet 10/100/1000 BASE-T interface
9	***FXS/FXO Line***	16 × RJ-11 ports for FXS/FXO line connection
10	***E1***	4 × RJ-48 ports for E1 streams

The device rear panel is shown in the Fig. 8

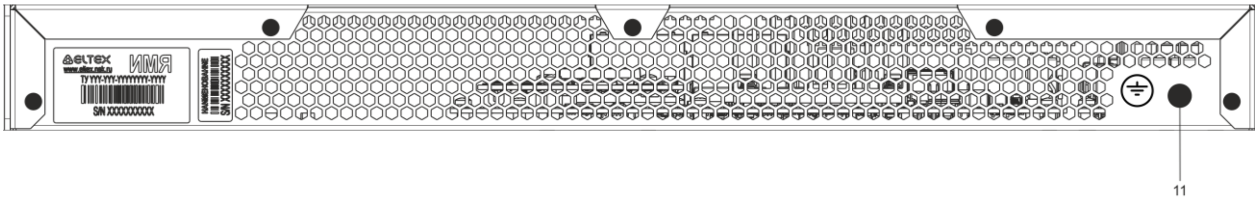


Fig. 8 – SMG-200/500 Rear Panel

Table below lists the rear panel connectors of the switch.

Table 3 – Description of Switch Rear Panel Connectors

No.	Rear Panel Element	Description
11	Ground connection point ⏚	Ground connection 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
Power	Off	Device power lost
	Solid green	Device power normal
	Solid red	Fault in the device power supply circuit
Alarm	Blinking red	Device critical failure
	Solid red	Device non-critical failure
	Solid green	No faults, normal operation. Non-critical problems may be present
	Blinking green	Warning
Status	Solid green	Normal operation
	Off	Firmware error
Battery	Solid green	Battery is connected, normal power supply
	Blinking green	Battery is charging
	Blinking red and green	Primary power is disabled, battery is discharging
	Solid red	Battery low
	Off	Battery is disconnected
	Blinking 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**	
Yellow	Green	Status
Off	Off	E1 is disabled in gateway configuration
Blinking (200 ms)	Off	E1 stream failure state
On	Off	Loss of Signal (LoS)
Blinking (200 ms) and off (1500 ms)	Off	Alarm (AIS)
Blinking (1500 ms)	Off	LOF failure
Blinking (1500 ms)	Off	LOFM failure

Off	On	E1 stream normal operation
Blinking (200 ms)	Blinking (200 ms)	RAI failure (a failure at the remote side)
Blinking (300 ms)	Blinking (1500 ms)	E1 stream is in operation and has SLIPs
On	Blinking (200 ms)	E1 stream test is in progress

1.8 Function Button ‘F’

The ‘F’ button is used to reboot the device, to restore factory configuration, and to recover forgotten password.

For instructions on how to reset the operating device to factory configuration, 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).

– 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 described on the left, then release the button.
2	Green	Off	Off	–	The boot process starts. Hold the ‘F’ button pressed.
3	Green	Red	Red	–	Press the ‘F’ button until the indicators light up as described on 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 1.8.1);
- 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);
- connect to the web interface via address 192.168.1.2;
- go to the 'Users: 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-200            *
*********************************************

smg login: admin
Password: rootpasswd

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


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

The password can be changed 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:

- Enterprise IP PBX SMG-200/500;
- PVC cord, 2 × 1.5, 2 m;
- C13 Europlug power cord, 1.8 m;
- User Manual on a CD (optional);
- Passport.

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 authorized in accordance with the safety requirements.

Before operating the device, all engineering and technical personnel should undergo special training.

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

The SMG-200/SMG-500 devices can be operated 24/7 if 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, ensure that all cables are undamaged and securely connected.

Make sure the power supply of 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, draw up the corresponding report, and contact your supplier.

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

If the device has been exposed to the cold for a long period of time, let it warm up at room temperature for two hours before starting work. If the device has been exposed to high humidity for a long period of time, let it stay under normal conditions for at least 12 hours before turning it on.

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

Once the device has been installed, its case should be grounded. This should be done prior to connecting the device to power supply. An insulated multiconductor wire should be used for grounding. The rules for device grounding and the grounding conductor should comply with the Electrical Installation Code. The ground connection 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 SMG-200), E1 streams (for SMG-500) and Ethernet cables to corresponding gateway connectors.
2. Connect the power cord 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 undamaged 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 brackets to the device case.

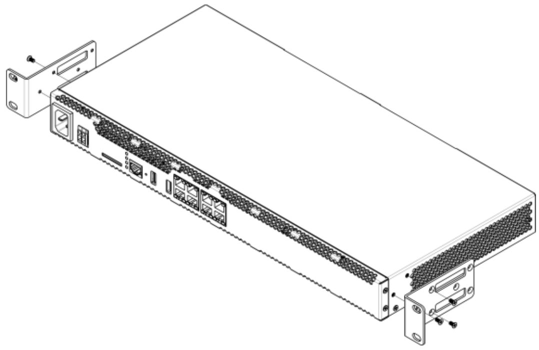


Fig. 9 – Support Brackets Mounting

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 in a rack:

1. Put the device to the vertical guides of the rack.
2. Align mounting holes in the support bracket with the corresponding holes in the rack guide frames. Use the guide frame holes located on the same level of the both sides of the rack to ensure horizontal position of the device.
3. Use a screwdriver to fix the device in the rack.

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

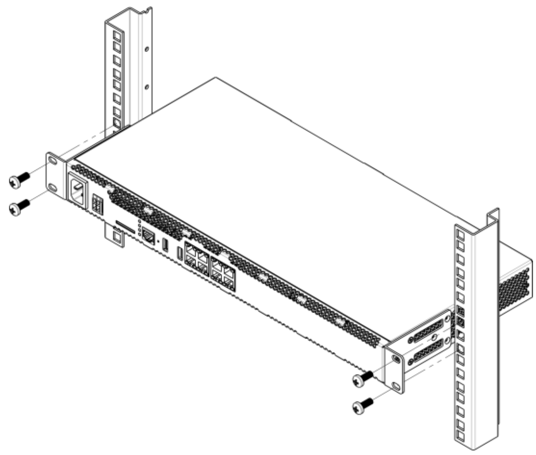


Fig. 10 – Device Rack Installation

1.13.4 *Opening the Case*

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

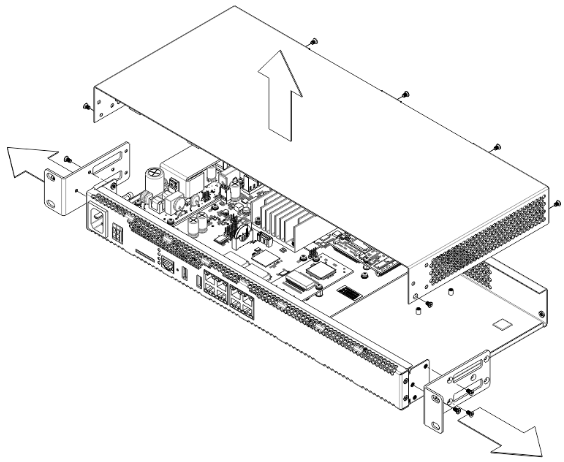


Fig. 11 – Opening the Case

1. Use a screwdriver to disconnect the brackets from the device case.
2. Unscrew the front panel locking screws, and then pull the front panel until it detaches from the top and side panels (Fig. 11).
3. Unscrew the screws on the top panel 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.

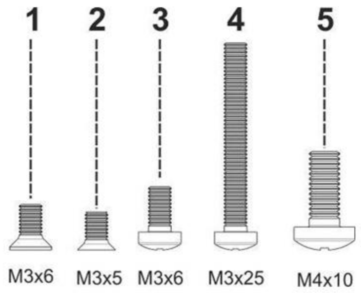


Fig. 12 – Types of Screws for SMG Assembly

Figure above shows the types of screws used to assemble the device into the case:

1. Bracket mounting for rack installation.
2. Mounting of case parts.
3. Mounting of boards.
4. 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 PBXes 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.

For the functioning of E1 streams on SMG-500, both submodules, C4E1 and SM-VP-M300, should be installed. When using SMG-500 without E1 streams, SM-VP-M300 submodule is not required. SM-VP-M300 submodule is used only for processing sound from E1 streams and operates together with C4E1.

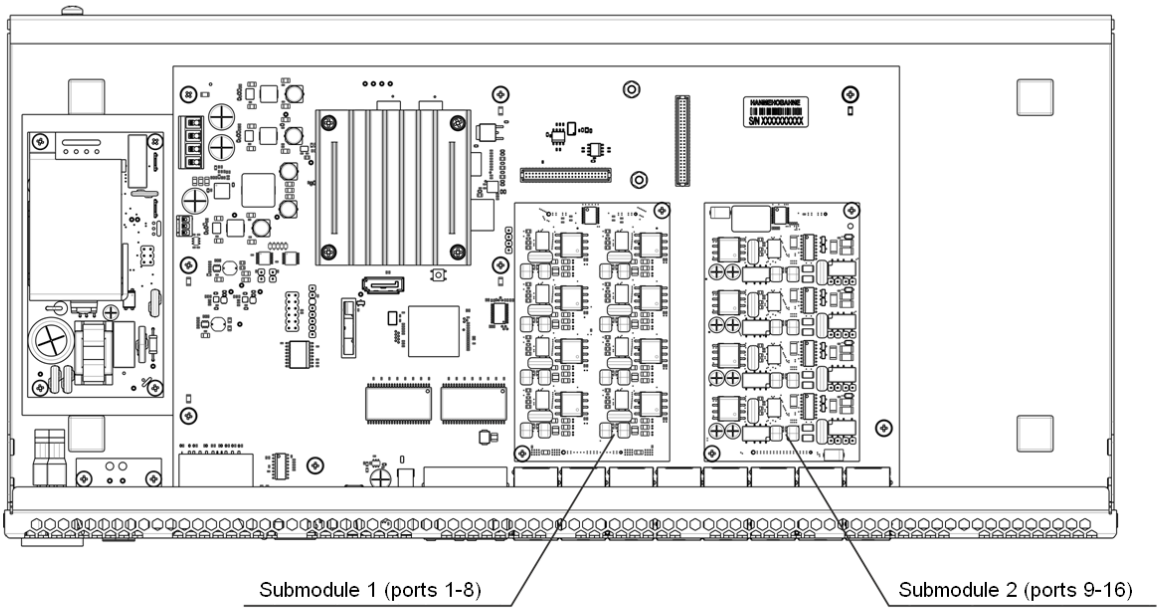


Fig. 13 – Location of the Submodules in SMG-200

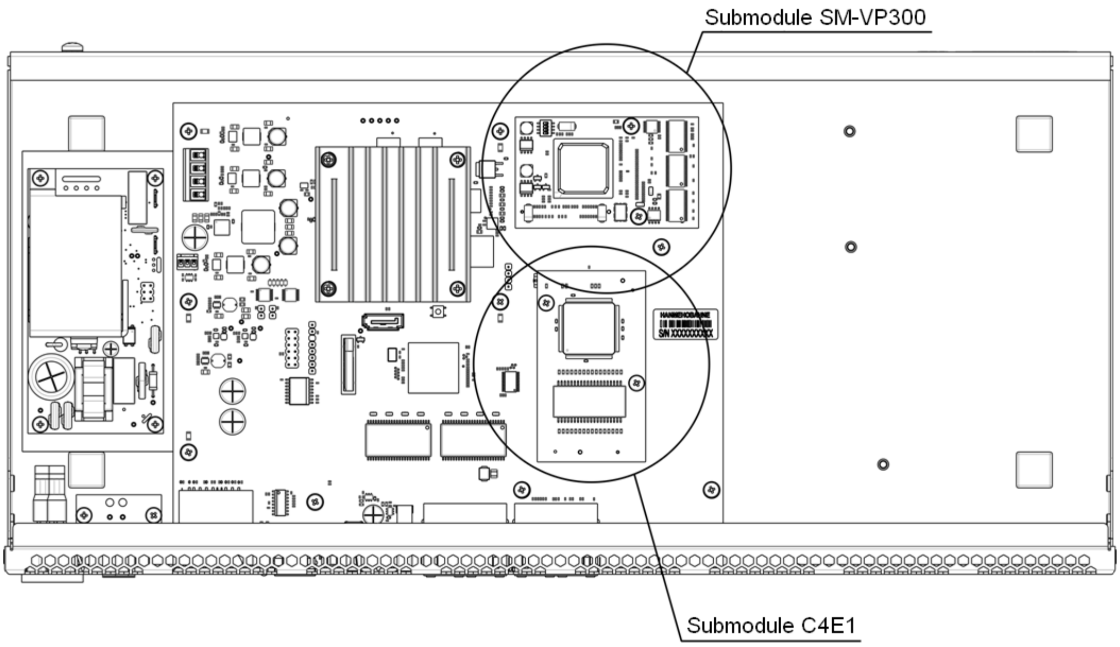


Fig. 14 – Location of the Submodules in SMG-500

Installation of the submodules in SMG:

1. Check if the device is powered on.
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	From -20 to +35 °C

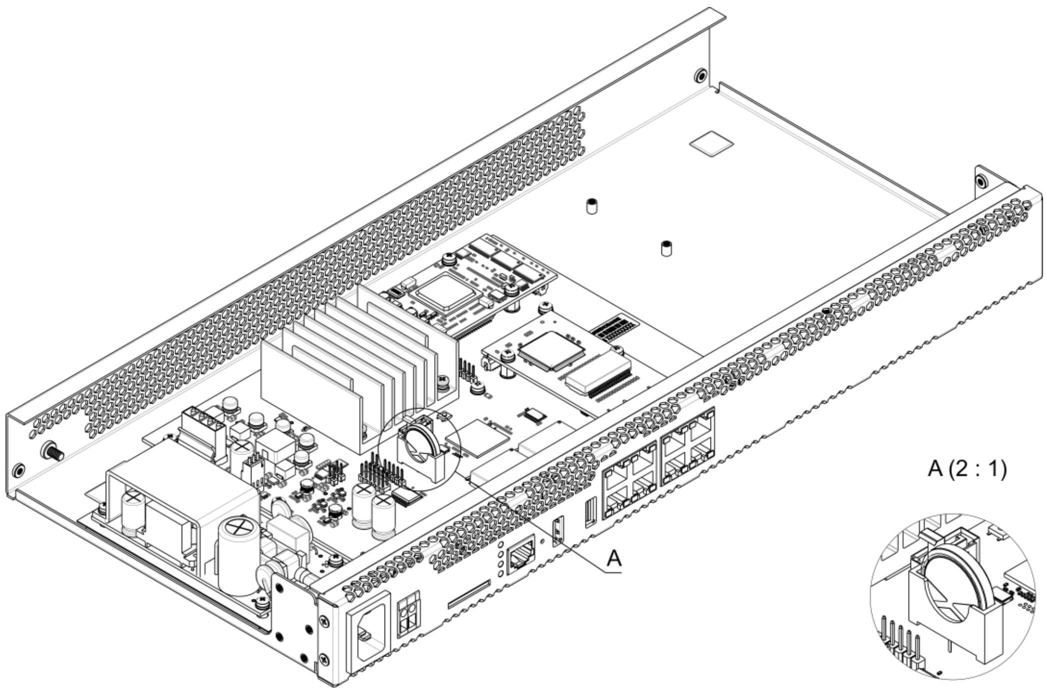


Fig. 15 – Battery Location in RTC

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 powered on.
2. If the voltage is present, disconnect the power supply.
3. If required, remove the device from the rack (see section 1.13.3).
4. Open the device case (see section 1.13.4).
5. Remove the used battery (

6. 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 synchronization is disabled, the system date and time will require adjustment after RTC battery replacement.

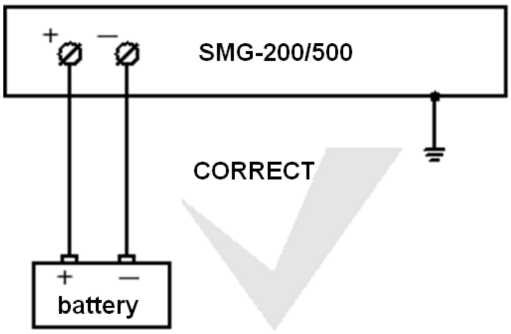
Used batteries are subject to special disposal.

1.13.7 Accumulator battery connection

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

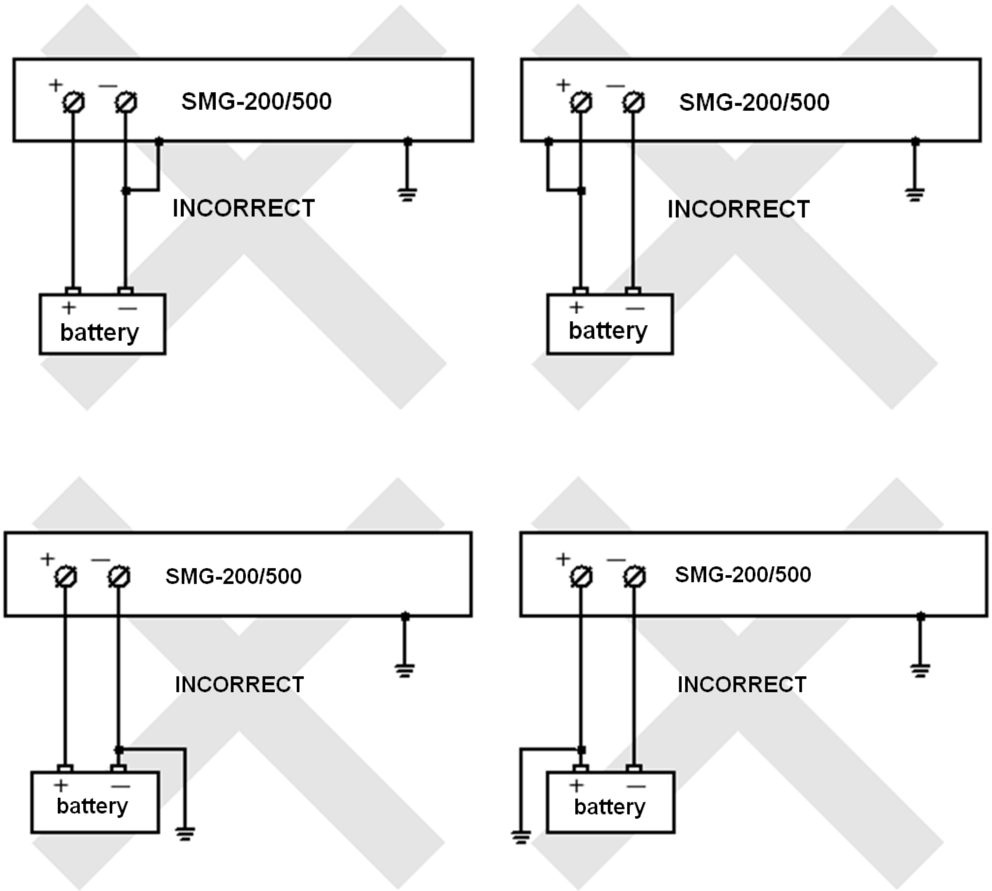
To avoid parasitic transition effects during switching accumulator battery supply cables and AC cables, it is recommended to observe the cable connection procedure. If AC supply is used, the next procedure of cable connection is recommended:

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



The battery is connected to the device with a two-wire cable, as shown in the figure below:

Use ONLY ‘+’ and ‘-’ terminals to connect an accumulator battery.
Do not connect accumulator battery cables to the case of the device.
Do not allow accumulator battery cable to connect to the device case or to contact with it.
Do not ground accumulator battery terminals.



Connection of 12V accumulator battery:

1. Connect the cable to the connector with screw clamps on the front of the device, and tighten the screws of the connector;
2. Connect the terminals to the accumulator battery, observing the polarities.

Disconnection of 12V accumulator battery:

1. Disconnect the terminals from the accumulator battery;
2. Loose the connector screws on the front of the device and remove the cable from the connector.

The recommended procedure for switching the AC power 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 for configuring and monitoring the device is to use the web configurator.

To prevent unauthorized access to the device, it is recommended to change the password for access to telnet and console (default username: ***admin***, password: ***rootpasswd***) and the administrator password for access to the web configurator. For setting password for access via telnet and console, see section 3.3.2 Changing Device Access Password via CLI. For setting password for access via the web configurator, see section 3.1.25 Management menu. It is recommended to write down and store the set passwords in a safe place which is inaccessible for intruders.

To prevent the device configuration data loss, 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 are applied without rebooting the gateway. To save configuration changes into the non-volatile memory, use the *'Service/Save Configuration into Flash'* menu in the web configurator.

3.1 SMG Configuration via web configurator

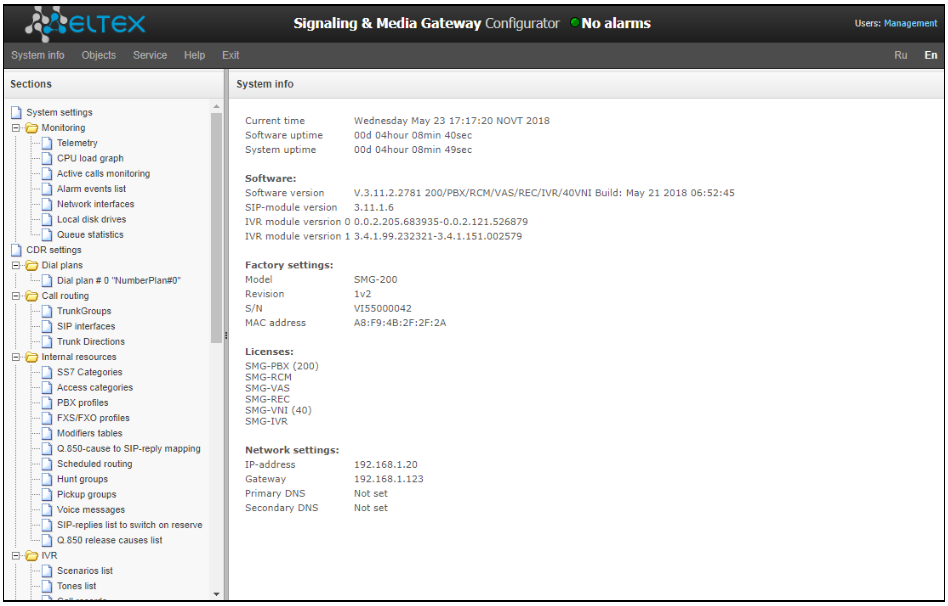
To configure the device, establish a connection to the device in a web browser (hypertext document viewer), such as Firefox, Opera, Internet Explorer. Enter the IP address of the device in the browser address bar.

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. The language to be used in the interface can be also selected here.

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.

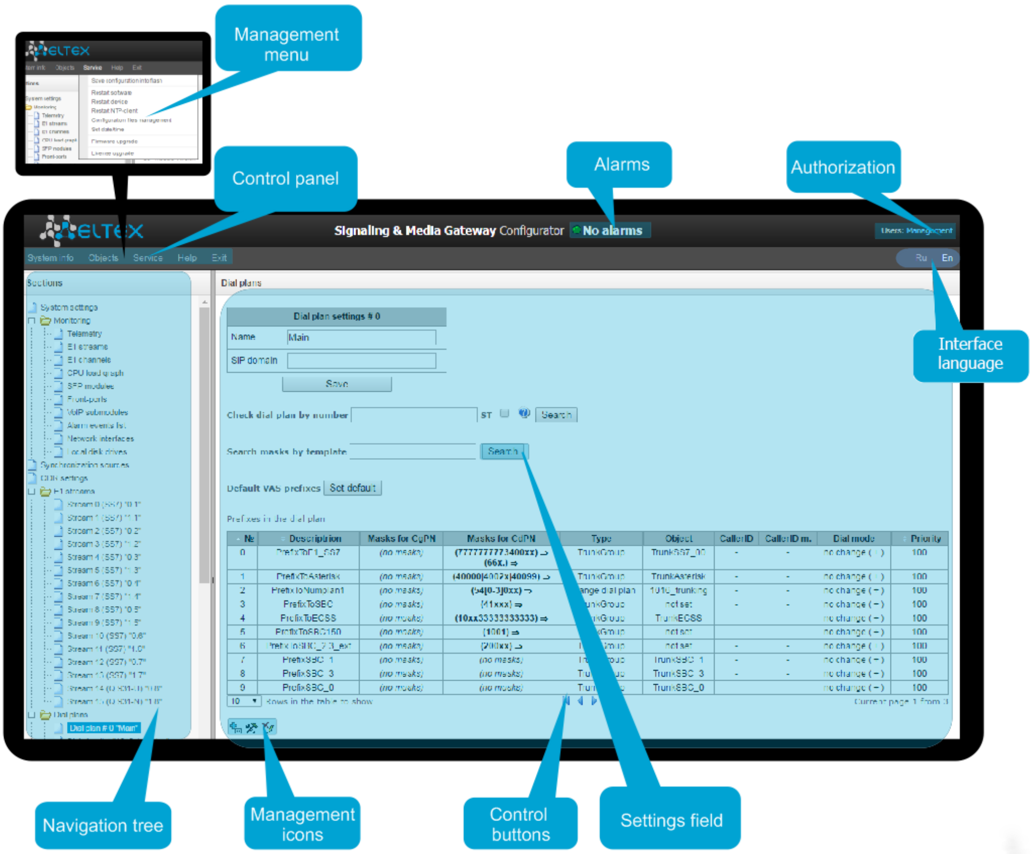


Fig. 16 – Navigation in the Web Configurator

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.
- *Authorization* – 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.

- *Management icons* – controls to work with objects in the settings field; the icons duplicate the Objects menu of the control panel:

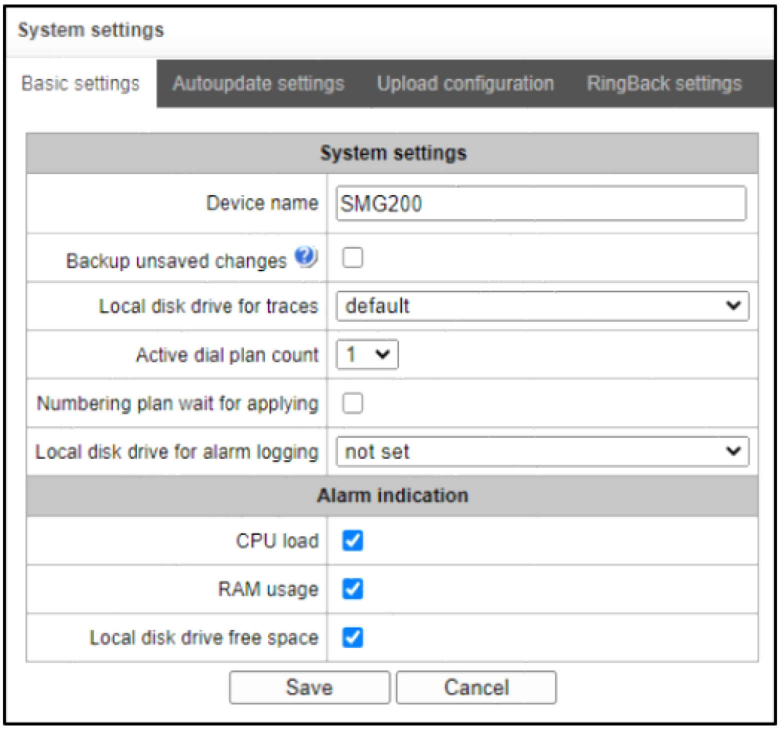
  — Add Object;
  — Edit Object;
  — Remove Object;
  — View Object.

- Control buttons – controls to work with the settings field.

To prevent unauthorized access to the device in the future, it is recommended to change the password (see section 3.1.25 Management menu).

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

3.1.1 System settings



- *Device name* – the device name. This name is used in the header of the device web configurator;

- *Backup unsaved changes* – if this option is enabled, the device creates a backup copy of unsaved configuration changes every 60 seconds with the possibility of their further restoration. For example, there were some unsaved changes on the device, and then a power cut occurred. If the option was enabled after the device started, the web interface would display a window suggesting to restore unsaved changes;

- *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; it 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.

- *Active dial plan count* – the quantity of simultaneously active dial plans (dial plans); up to 16 independent dial plans can be configured with a possibility to add subscribers and create a customized call routing table;

- *Numbering plan wait for applying* – 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 dial plans, since it helps to avoid long processing after each change of settings;

- *Local disk drive for alarm logging* – selects 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

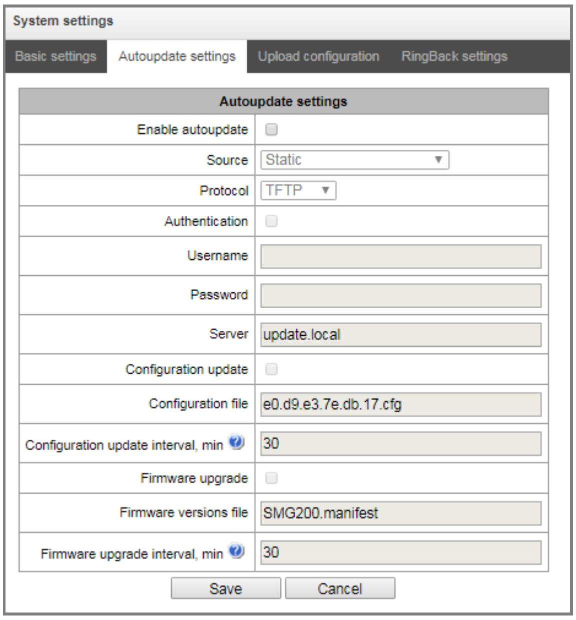
Alarm Message	Meaning
Configuration error	Configuration file error
SIPT-module lost	Failure of a firmware module responsible for VoIP operation
Linkset down	SS7 linkset failure
E1-Line alarmed	E1 stream failure
SS7-Link alarmed	SS7 signal channel failure
Sync from local source, but sync source table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

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

Alarm indication

- *CPU load* — when this option is active, a high CPU load results in fault indication (the ALARM LED turns on and the alarm is registered in the alarm log);
- *RAM usage* — when this option is active, usage of over 75% of RAM results in fault indication (the ALARM LED turns on and the alarm is registered in the alarm log);
- *Local disk drive free space* — when this option is active, if one of the external drives with capacity less than 5 GB is more than 80 % full (or there is less than 1024 MB of free space on an external storage device with capacity exceeding 5 GB), there will be an indication of an accident (the ALARM LED turns on and the alarm is registered in the alarm log).

Autoupdate settings



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, one can specify the time allowed for the update. The file format should be as follows:

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

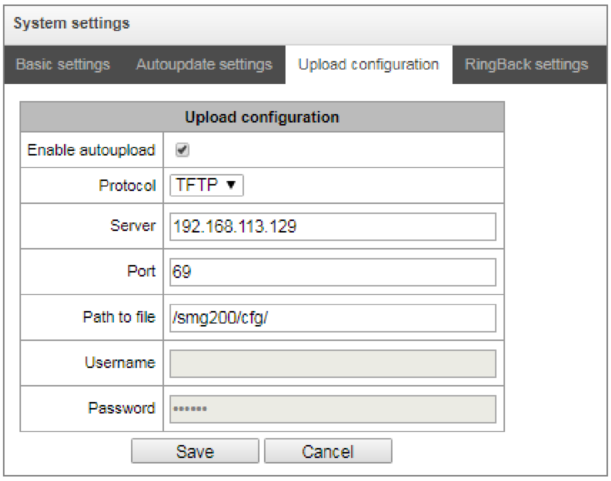
- The firmware version is specified completely before the build version;
- The firmware file name should have a .bin extension;
- The allowed update time may be absent. In this case, SMG will be updated shortly, when there are no active calls. If the allowed update time is specified, SMG will only be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

Example of a firmware version file:

3.14.0.3057;smg500_firmware_3.14.0.3057.bin
3.16.0.3247;smg500_firmware_3.16.0.3247.bin;9-13

- *Enable autoupdate* – enables automatic updates of configuration and firmware files;
- *Source* – selects 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* – selects the server connection protocol;
- *Authentication* – uses authentication to access the server (for FTP, HTTP, HTTPS);
- *Username* – a 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;
- *Configuration update* – allows configuration updates from the server;
- *Configuration file* – 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;
- *Firmware upgrade* – allows firmware updates from the server;
- *Firmware versions file* – the name of the firmware version file. The file name should have a .manifest extension and not exceed 64 characters in length;
- *Firmware upgrade interval, min* – how often the server is checked for the presence of a new firmware version.

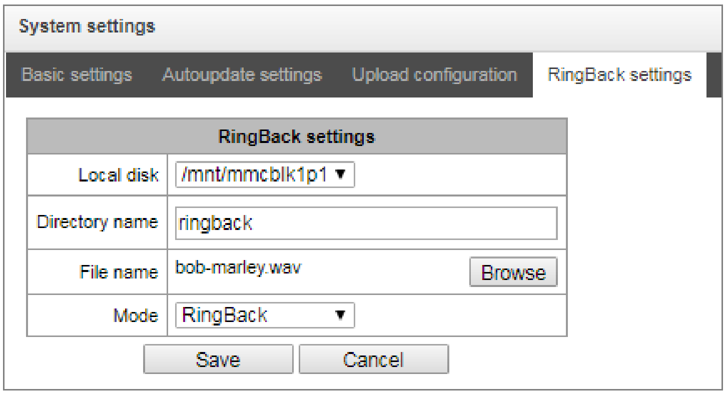
Upload configuration



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

- *Enable autoupload* – enables the configuration upload function;
- *Protocol* – selects the protocol for uploading. FTP, TFTP, and SCP 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 file* – the directory on the server to which the configuration file will be saved;
- *Username* – the authentication user name when using FTP;
- *Password* – the authentication password when using FTP.

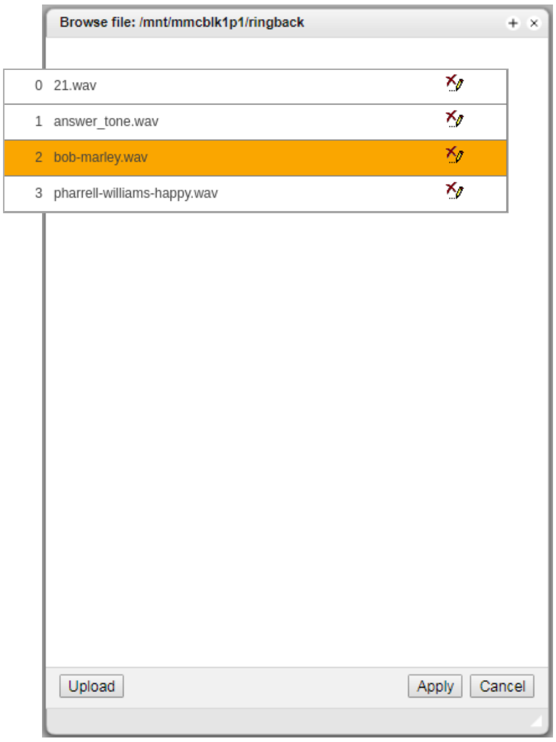
RingBack settings



'*RingBack settings*' allow changing standard ringback tone, work as 'Change Ringback tone' feature.

- *Local disk* — a path to an external storage where audio files will be kept;
- *Directory name* — a name of the directory on the external storage where audio files are kept;
- *File name* — selects file for playback as a ringback tone;
- *Mode*:
    - *RingBack* — standard ringback tone;
    - *Audio file* — selected file to playback as a ringback tone.

The ‘*Browse’* submenu allows the user to load, select and delete audio files as ringback tones:



Audio files should be in WAV format, codec G.711a, 8 bit, 8 kHz, mono.

- *Upload* — upload an audio file of the certain format;
- *Apply* — select needed audio file;
- *Cancel* — exit from the ‘Browse’ submenu.

When configuring ringback tone in ‘System settings’, a selected audio file is applied to all subscribers and trunk groups of the system.

There are several levels of settings: more detailed level has a higher priority.

1. System settings of ringback tone.
2. Ringback tone settings for trunk groups and PBX profiles.
3. Ringback tones settings for subscribers.

3.1.2 Monitoring

3.1.2.1 Telemetry

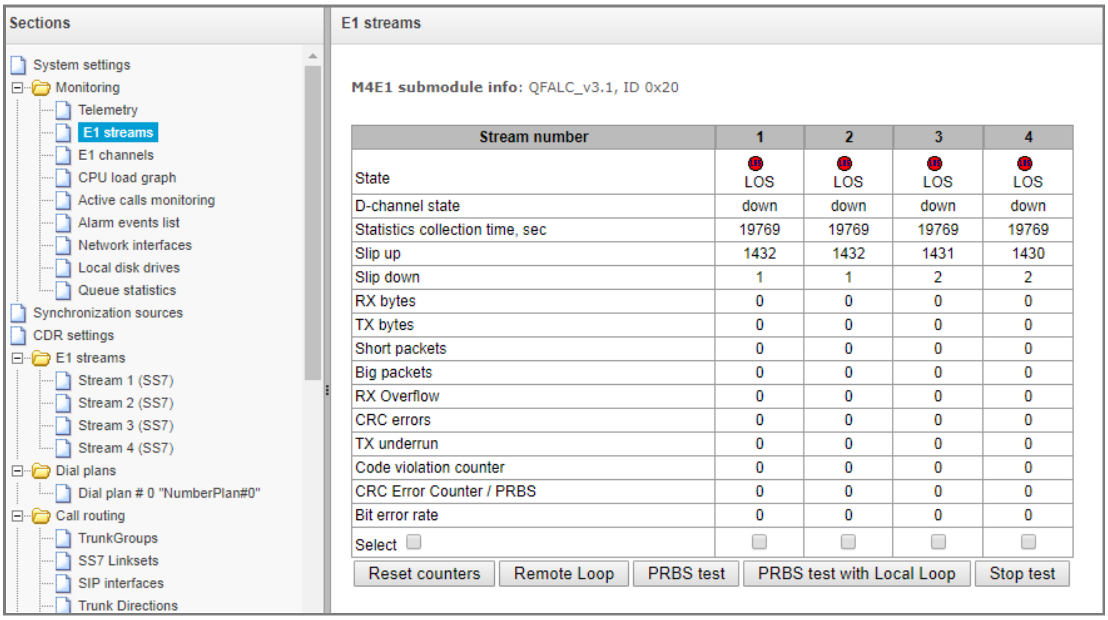
This section describes the readings of the telemetry system sensors installed on the device.

CPU load

- *USR* – percentage of CPU time utilization by user applications;
- *SYS* – percentage of CPU time utilization by core processes;
- *NIC* – percentage of CPU time utilization 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 E1 stream monitoring (for SMG-500 only)

This section of the menu displays information about the installed chip on the C4E1 (M4E1) submodule, as well as monitoring and statistics of E1 streams.



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				

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 received packets 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;
- *TXunderrun* – stream transmission failure counter;
- *Code violation 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.

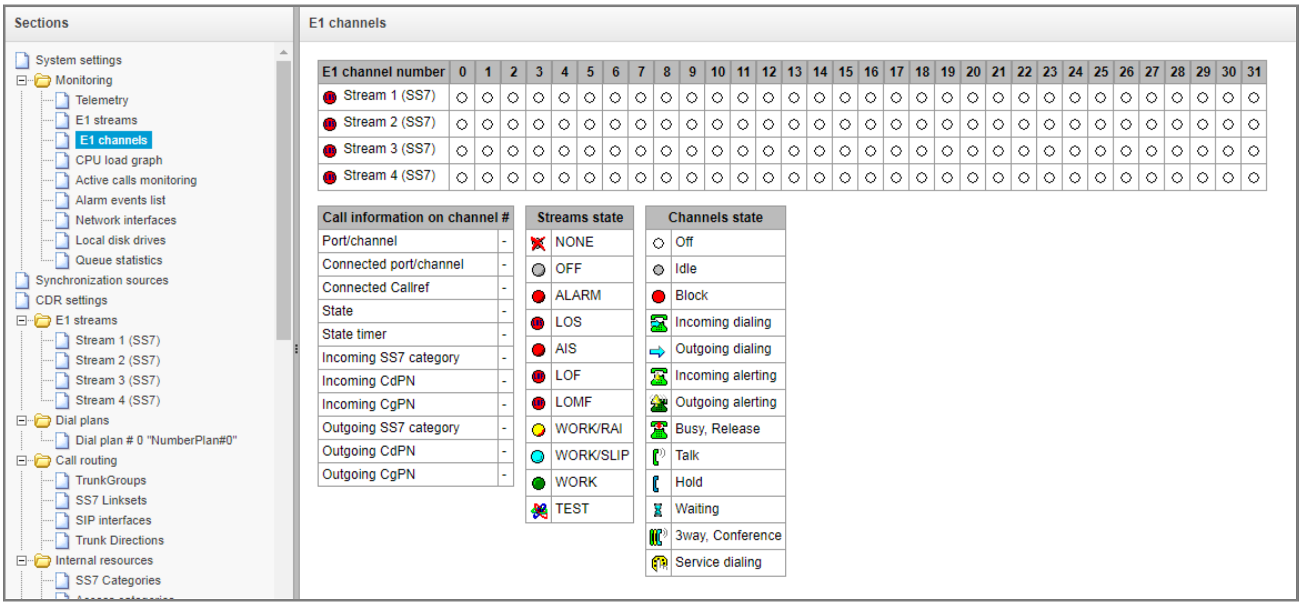
The following buttons are located under the table of E1 channel parameters:

- *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* – disables test mode.

3.1.2.3 *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



Call 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:
  - Connected port signalling protocol (PRI/SS7/VoIP);
  - Connected 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 engagement;
  - *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* – called number before modification;
- *Incoming CgPN* – calling number before modification;
- *Outgoing SS7 category* – SS7 category of an incoming call after modification;
- *Outgoing CdPN* – called number after modification;
- *Outgoing CgPN* – calling 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);
- *LOF* – loss of frame;
- *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:

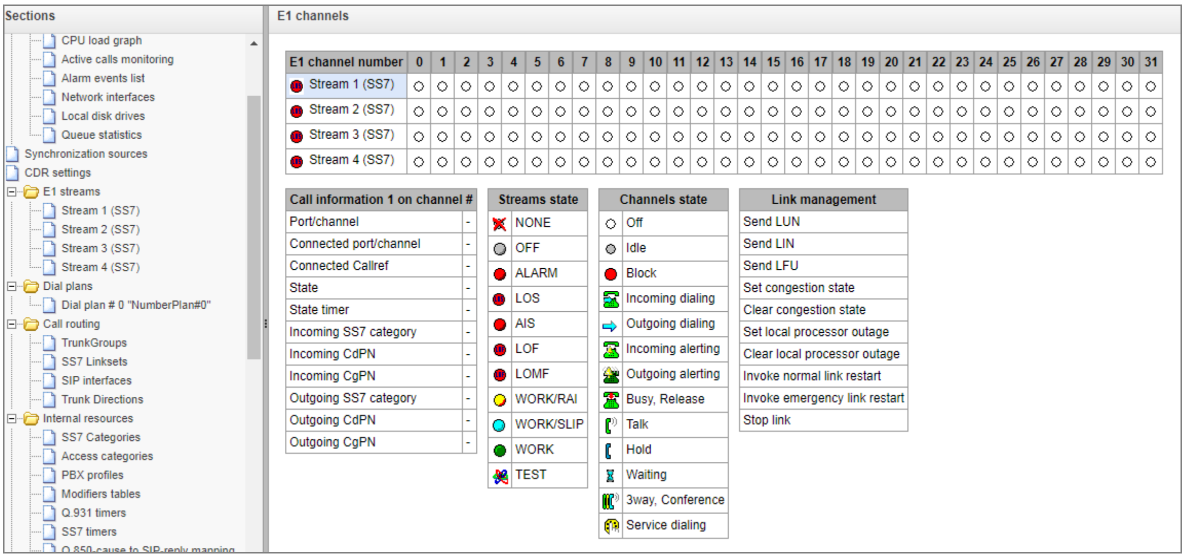
- *Off* – channel is disabled in the configuration;
- *Idle* – channel is in initial state;
- *Block* – channel is blocked;
- *Incoming dialing* – incoming call dialing;
- *Outgoing dialing* – outgoing call dialing;
- *Incoming alerting* – incoming engagement, calling is free;
- *Outgoing alerting* – outgoing engagement, called is free;
- *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 engagement acknowledgement, caller ID, and dialing number);
- *3way, Conference* – conference mode (3-WAY or Add on conference);
- *Service dialing* – call service numbers of VAS.

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

Channel state updates in 5 seconds interval.

Link management

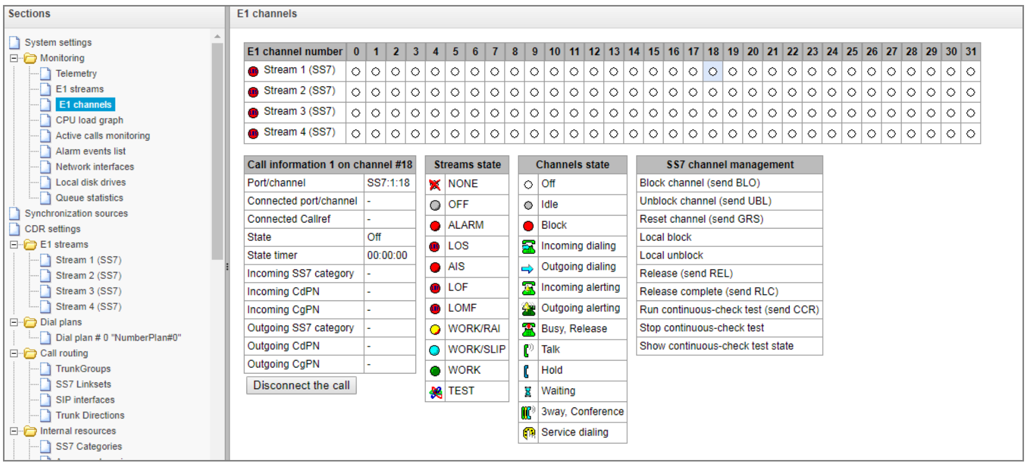
To enable stream management, left-click the stream name. The field will become highlighted, for example, the screenshot below shows the information for Stream 1 (SS7). Next, in '*SS7 link management*' table, select the field with the required action and left-click it. Pop-up informational message on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

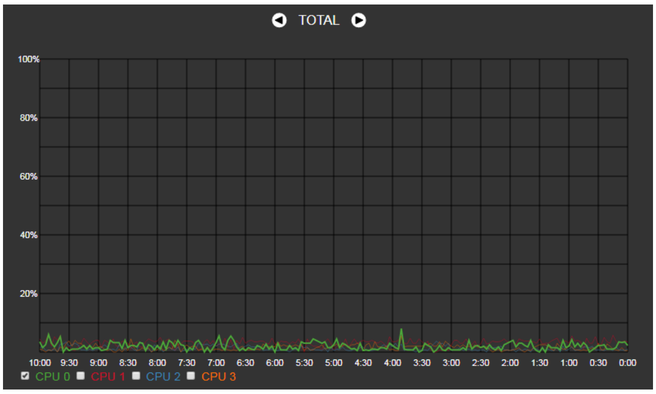
It is possible to perform group operations for channels in a stream. To do this, select the range of channels while holding <SHIFT> key.

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 (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 complete (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 state* – show the current channel continuity test state.

3.1.2.4 CPU load graph

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



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

- *TOTAL* – total percentage of CPU load;
- *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 utilization by user applications;
- *SYS* – percentage of CPU time utilization by core processes;
- *NIC* – percentage of CPU time utilization by applications with a modified priority;
- *CPU 0..3* – view the load of each CPU core separately.

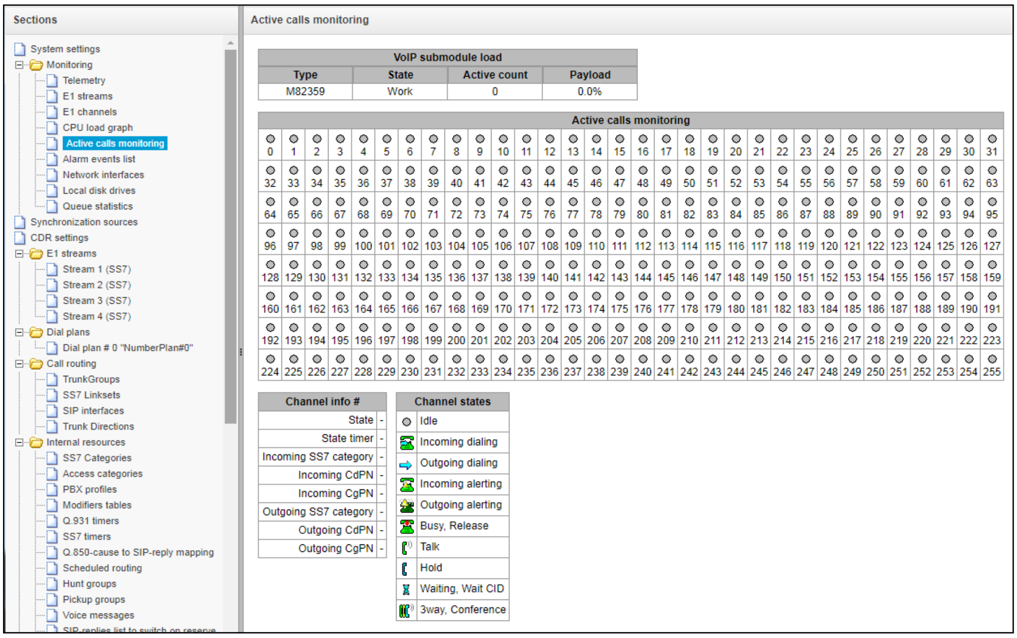
3.1.2.5 Active Calls Monitoring

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 in the VoIP — VoIP direction.

The ‘*Active Calls Monitoring*’ window displays state indicators for each port. The ‘*Channel states*’ window shows indication description, see below.



Channel states

- *Idle* (grey) – initial state, the channel is ready to serve a call;
- *Incoming dialing* – incoming call;
- *Outgoing dialing* – 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 the ‘*Active Calls Monitoring*’ window. The ‘*Channel info #*’ window displays information on the channel.

Channel Connection Information

- *State* – channel status:
  - *Off* – channel is disabled;
  - *Block* – port is blocked;
  - *Init* – channel initialization;
  - *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 (AON);
  - *Wait-Num* – waiting for call dial;
  - *Hold* – subscriber is on hold.
- *State timer* – channel last known status duration;
- *Incoming SS7 category* – SS7 category of an incoming call before modification;
- *Incoming CdPN* – called number before modification;
- *Incoming CgPN* – calling number before modification;
- *Outgoing SS7 category* – SS7 category of an incoming call after modification;
- *Outgoing CdPN* – called number after modification;
- *Outgoing CgPN* – calling number after modification.

3.1.2.6 Fault alarms. Alarm events list

When a failure occurs, all related information containing the fault stream number, SS7 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 on the current most critical one.

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

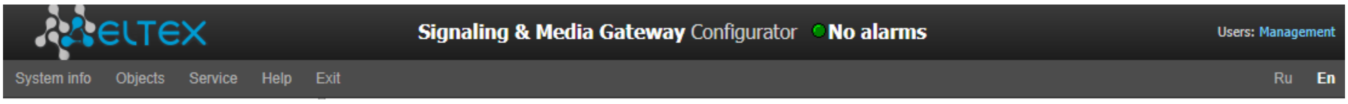
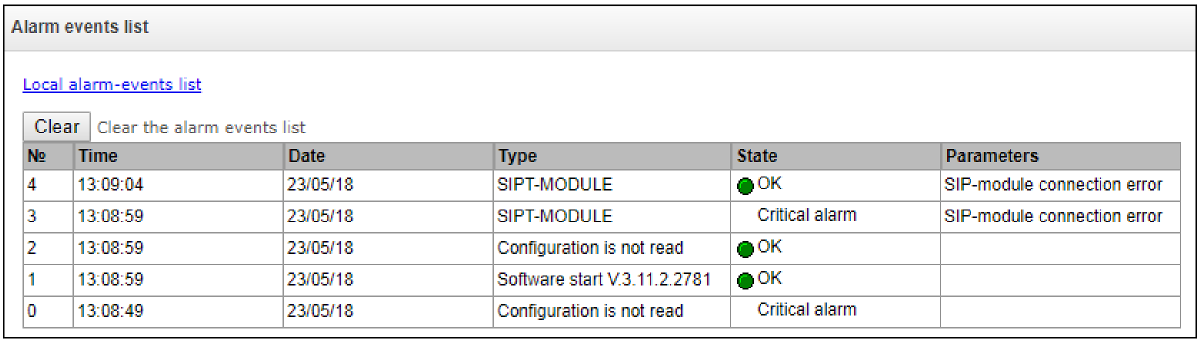


Table 10 – Alarm Message Examples

Alarm Message	Meaning
Configuration is not read	Configuration file error
SIP-module connection error	Failure of a software module responsible for SIP operation
Failed to send CDR files to the external storage	Failure to send a CDR file to the external storage
VoIP-submodule 0 connection error	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 utilization	Utilization over 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 *CPS alarm threshold* setting

The *Alarm events list* 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

Clear | Clear the alarm events list

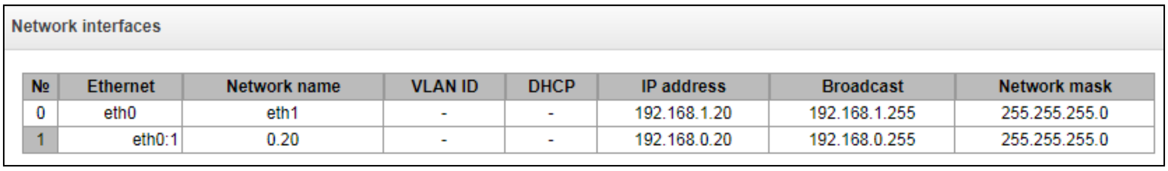
№	Time	Date	Type	State	Parameters
4	13:09:04	23/05/18	SIPT-MODULE	OK	SIP-module connection error
3	13:08:59	23/05/18	SIPT-MODULE	Critical alarm	SIP-module connection error
2	13:08:59	23/05/18	Configuration is not read	OK	
1	13:08:59	23/05/18	Software start V.3.11.2.2781	OK	
0	13:08:49	23/05/18	Configuration 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 failure, a configuration file failure;
  - *SIPT-MODULE* – a critical failure, a failure of a program module responsible for VoIP operation;
  - *CDR-UPSERVER* – a failure or a warning, a failure to send a CDR file to external drive;
  - *TRUNK-CPS* – a number of allowed calls per second for the trunk group is exceeded.
- *State* – a failure state status:
  - *critical alarm, LED blinking red* – the failure requires immediate intervention of the service personnel and affects device operation and provisioning of communication services;
  - *alarm, red LED* – non-critical failure, intervention of the service personnel is also required;
  - *warning and OK, green LED* – the failure 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.

3.1.2.7 Interface Monitoring

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

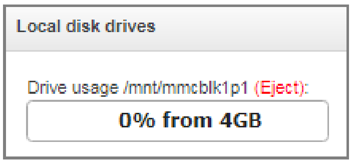

Network interfaces

№	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).

3.1.2.8 Storage Devices Information

This section contains information on external storage drives connected to the device.



- *Eject* – clicking the link allows extracting the drive safely.

Names of the external drives are attached to the interfaces.

SMG200/500	
USB1	/dev/sda1
USB2	/dev/sdb1
SD	/dev/mmcblk1p1

3.1.2.9 Queues Statistics

This section contains the queues operation statistics.

Queue statistics

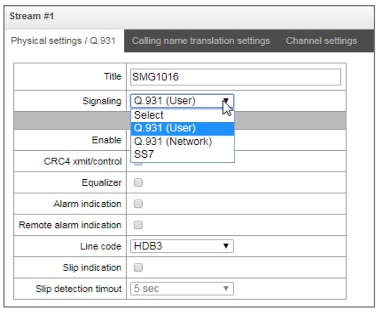
ID queue	Total calls	Answered	Unanswered	Maximum queue length (hour/day/workday)	Callback failure	Queue overflow	Waiting time
0	0	0	0	0 / 0 / 0	0	0	0
1	0	0	0	0 / 0 / 0	0	0	0

- *ID queue* – the queue identifier;
- *Total calls* – the total number of incoming calls in the queue;
- *Answered* – the number of successful calls completed by the operator's response;
- *Unanswered* – the number of calls dropped by the caller before the operator's response;
- *Maximum 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;
- *Callback failure* – the number of unsuccessful attempts to call back to the subscriber, when using the callback option[1];
- *Queue overflow* – the number of calls failed due to the queue size overflow;
- *Waiting time* – the average waiting time for the operator to respond; based on this value, the response is generated.

To clear queue statistics, check the '*Select*' flag next to the queues which statistics are to be cleared, and then click the '*Clear Selected*' button that will be displayed.

3.1.3 E1 streams (only for SMG-500)

You can select a signaling protocol in a drop-down list of 'Signaling'.



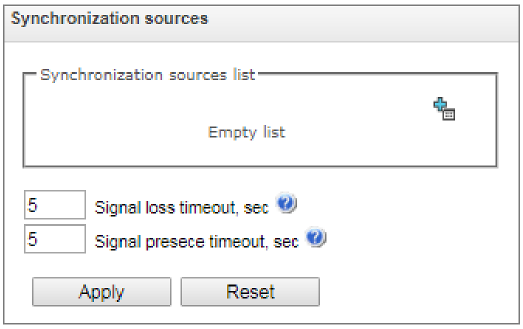
The device supports the following signaling protocols:

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

[1] Not supported in the current firmware version 3.20.3

3.1.3.1 Synchronization source

To synchronize device with multiple sources, a priority list algorithm is used. Its meaning is as follows: when sync signal from the current source is lost, the list is examined to identify active signals from the lower priority sources. When the higher priority signal is restored, the system switches to that signal. Also, it is possible to use multiple sources with the same priority; at that, when the same priority signal is restored, the system does not switch to that signal. Up to 4 synchronization sources (from each of 4 E1 streams) may be set.



To generate a 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, sec* – 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;
- *Signal presence timeout, sec* – time interval during which the restored synchronization signal from a higher priority source should be active before the system switches to the signal.

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

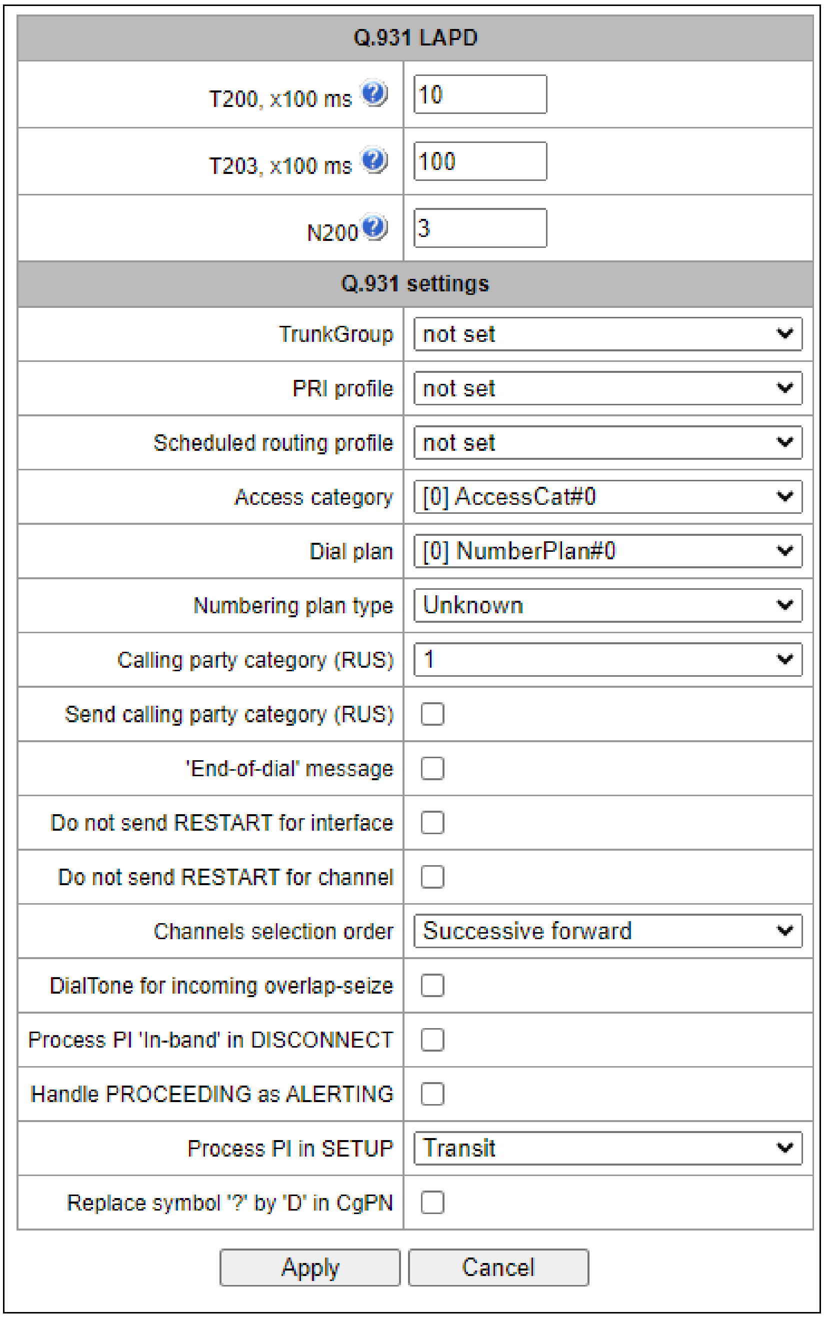
3.1.3.2 Configuring physical settings

3.1.3.2.1 Physical settings:

- *Title* – E1 stream name;
- *Signaling* – physically enable stream;
- *Framing*:
    - *doubleframe* – CRC4 disabled;
    - *CRC multiframe* – 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.

3.1.3.3 DSS1/EDSS1 signaling protocol configuration (ISDN PRI Q.931)

3.1.3.3.1 ‘Physical settings/Q.931’ tab



Q.931 LAPD	
T200, x100 ms	10
T203, x100 ms	100
N200	3
Q.931 settings	
TrunkGroup	not set
PRI profile	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)	☐
'End-of-dial' message	☐
Do not send RESTART for interface	☐
Do not send RESTART for channel	☐
Channels selection order	Successive forward
DialTone for incoming overlap-seize	☐
Process PI 'In-band' in DISCONNECT	☐
Handle PROCEEDING as ALERTING	☐
Process PI in SETUP	Transit
Replace symbol '?' by 'D' in CgPN	☐

Apply Cancel

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

- *T200, x100 ms* – 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, x100 ms* – maximum time during which the device may not exchange frames with the opposite device;
- *N200* – quantity of frame retransmission attempts.

Q.931 settings

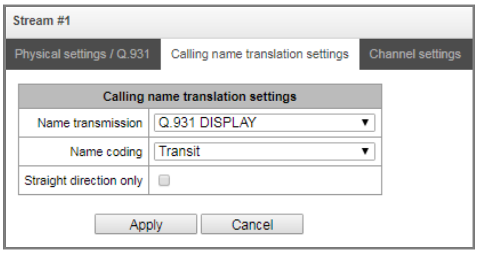
- *Trunk group* – name of a trunk group, that includes the E1 stream;
- *PRI profile* – selects a PRI profile for servicing PRI subscribers;
- *Scheduled routing profile* – selects scheduled routing profile from the list of existing profiles;
- *Access category* – selects access category;
- *Dial plan* – defines dial plan that will be used for routing of the call received from this port (necessary for dial plan negotiation);
- *Numbering plan type* – defines ISDN dial plan type. To use common dial plan E.164, select 'ISDN/telephony';
- *Calling party category* – Caller ID category assigned to calls received from this port;
- *Send calling part category* – enables 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* – produces *'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;
- *Channels selection order* – 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;
- *Handle PROCEEDING as ALERTING* – when checked, upon receiving a PROCEEDING message, it will be processed as an ALERTING and a RBT will be issued;

- *Process PI in SETUP* – when checked, adds the ability to change the Progress Indicator in a SETUP message. It is possible to change to:
  - *Transit* – transmit without change;
  - *1* – Not end-to-end ISDN;
  - *2* – Dest addr is non ISDN;
  - *3* – Orig addr is non ISDN;
  - *4* – Return to ISDN;
  - *5* – Interworking occurred;
  - *8* – In-band information.
- *Replace symbol '?' by 'D' in CgPN* – when checked, if a received SETUP message in CgPN receives a '?', it will be replaced by 'D'.

3.1.3.3.2 'Calling name translation settings' tab



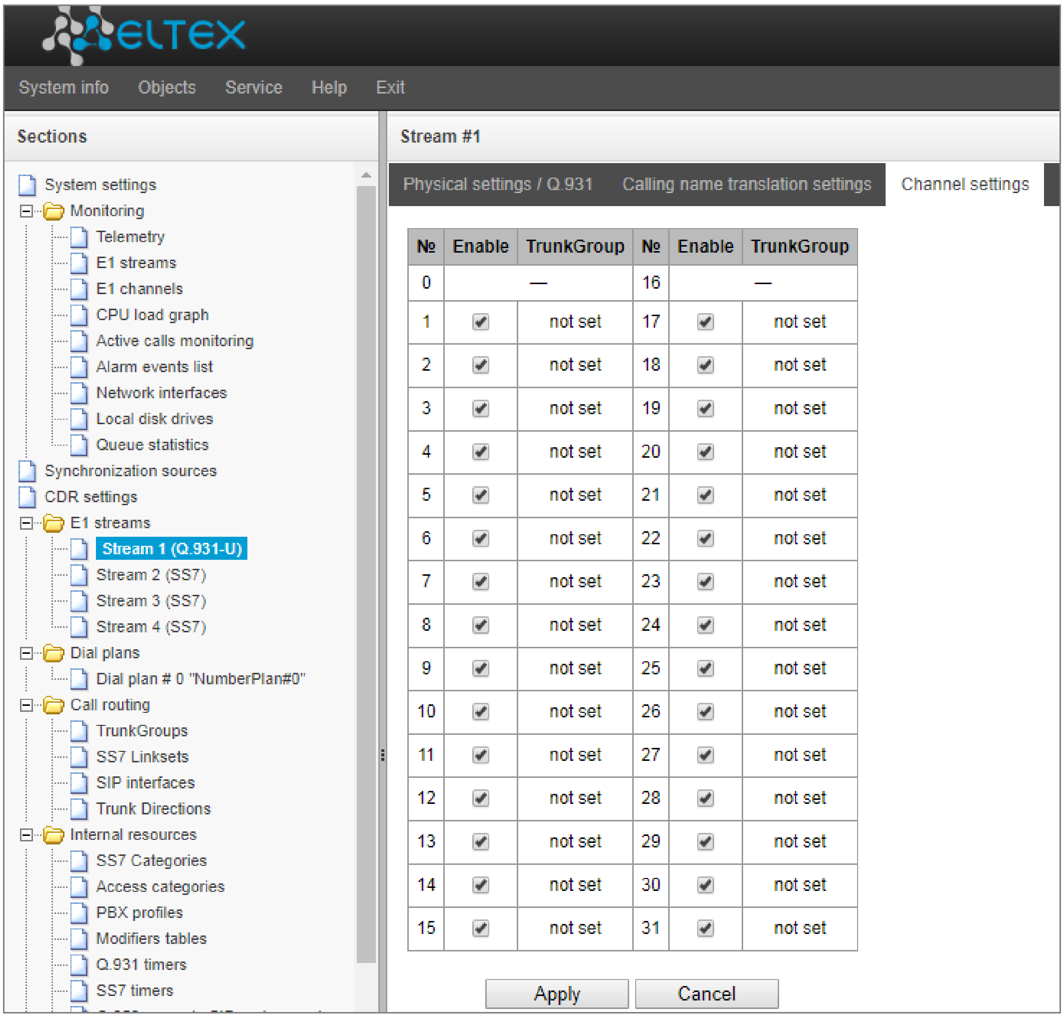
Use the tab to configure the way of name reception/transmission and coding of received/transmitted name.

- Name transmission:
  - *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:
  - *Transit* – recoding is not available (name format is UTF-8 bit 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;
- *Straight direction only* — send subscriber name only in forward direction messages.

The method selected for name reception/transmission and coding of received/transmitted name works only in a configurable E1 stream. Transmission between streams differing by the settings of name transmission parameters is possible. In case of such transmission, the SMG performs recoding by itself to harmonize the sides.

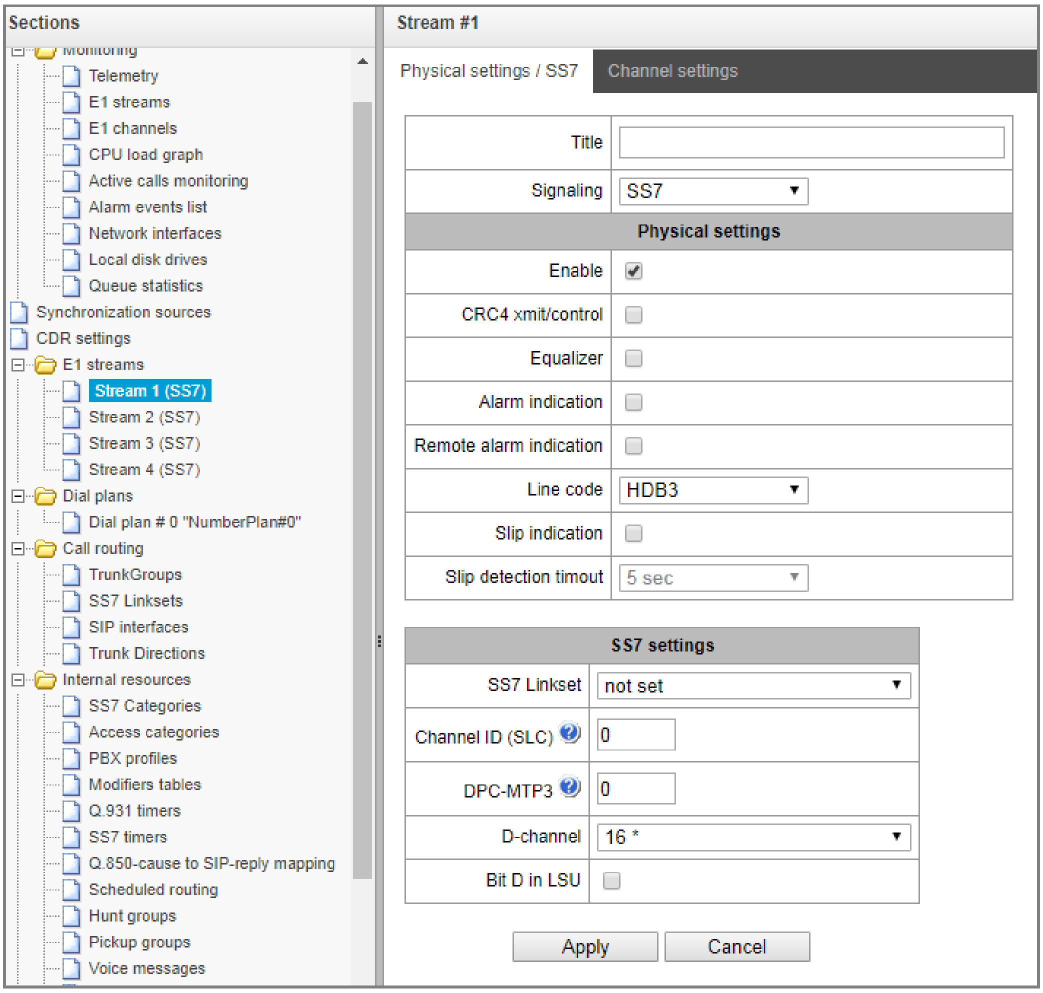
3.1.3.3.3 'Channel settings' tab

Use this menu to enable/disable E1 stream channel. To do that, select/clear 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).



3.1.3.4 SS7 protocol configuration

3.1.3.4.1 'Physical settings/SS7' tab



SS7 settings:

- *SS7 Linkset* – linkset selection (SS7 linkset);
- *Channel ID (SLC)* – signal line identifier in SS7 linkset;
- *DPC-MTP3* – destination point code of the signaling 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 3.1.5.2 SS7 Linksets (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).

3.1.4 Dial plan

This section describes how to configure the dial plan of the device.

The device features up to 16 independent dial plans. Every dial plan may have its own subscribers and prefixes. To set the number of active dial plans, see section 3.1.1 System settings.

The device routes calls using 4 criteria:

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

When a call arrives to a dial plan, its routing begins. First, search for matches to CgPN number masks is performed. If there is a prefix with 'AND' logic (masks for CgPN and CdPN are set, and there is a match for both parameters) and there is a prefix with the same mask for CgPN, then when 'Priority' parameter is equal, the call will go to the prefix with 'AND' logic, since it is considered that its mask is more precise. If the prefix with 'AND' has less priority, the call goes to the prefix with 'OR'.

If a CgPN search finds two prefixes with 'AND' logic, and the CgPN mask is the same, then CdPN is compared and the call is routed to the prefix with the more precise mask.

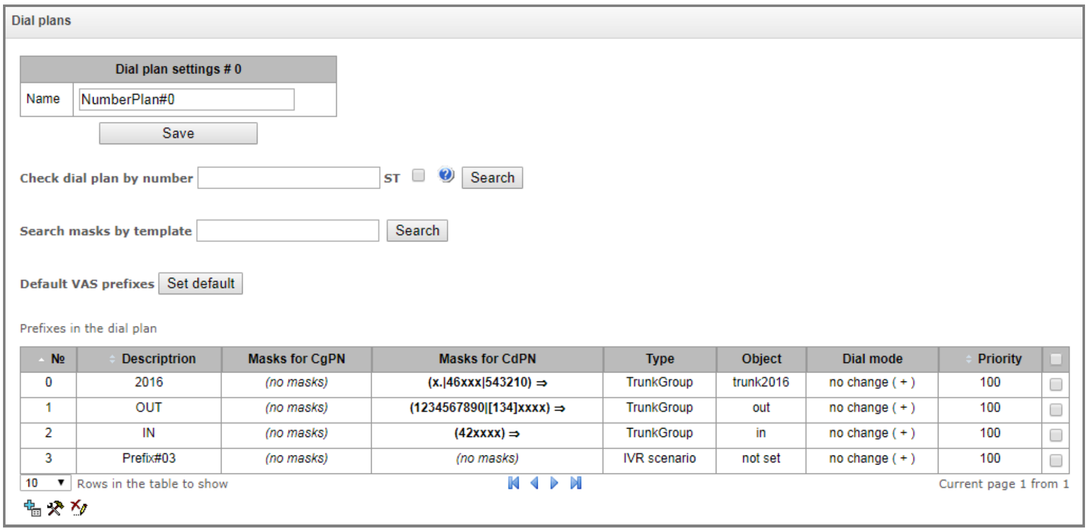
Then the search in the database of subscribers configured on the device is performed. If a match by any of this parameters is found, the call is routed and further search is stopped.

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

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

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

If both CgPN and CdPN number masks are configured in prefix parameters and AND logic operator is set, this rule uses AND logic, i. e. for routing a call via this prefix, matching with CgPN and CdPN masks is required.



Dial plan settings

- *Name* – name of the dial plan.

Check dial plan by number – checks if routing is possible for the number entered into this field.

The check is performed by calling and called masks and the system also checks in the configured SIP subscriber database.

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

Search masks by template – searches for a prefix by the number template, name, direction, prefix type, trunk direction, trunk group.

The check provides information on routing capability for this number:

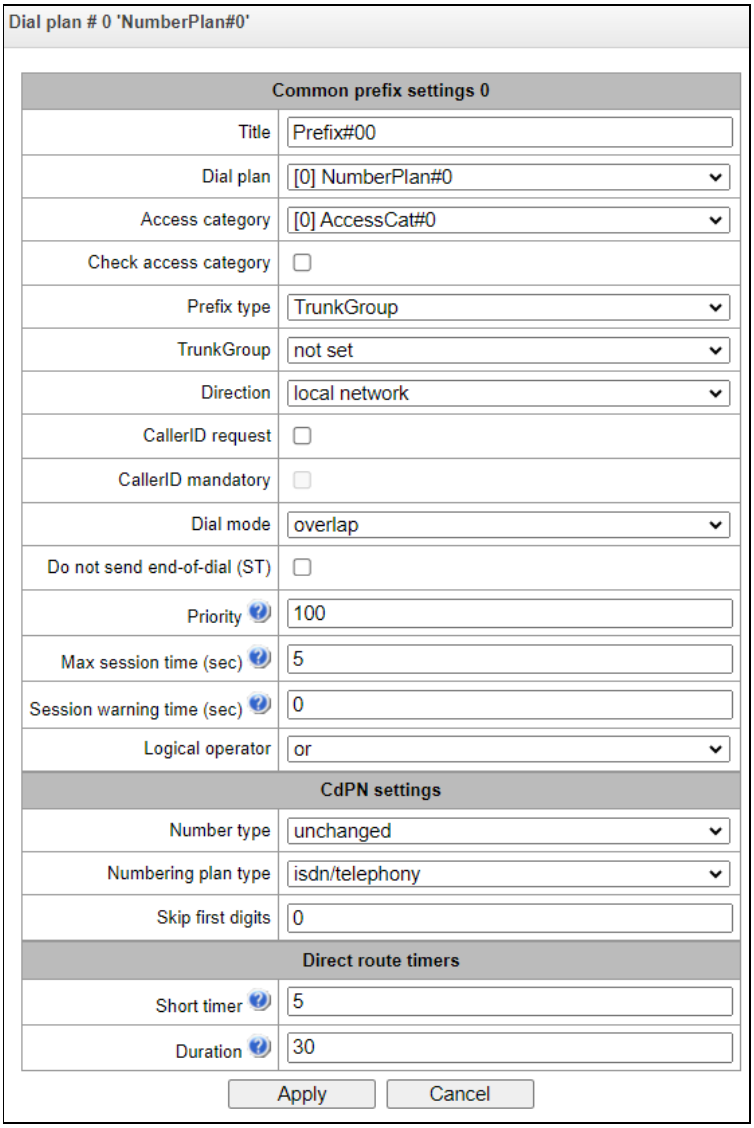
- *calling-table* – routing by the calling table;
- *called-table* – routing by the called table;
- *NOT found in* – routing by this table is not possible;
- *found in* – routing by this table is possible;
- *Abonent 'SIP' idx[4]* – SIP subscriber [entry number for this subscriber in the database];
-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

Copying prefixes to another dial plan

- *Copy selected prefixes to the dial plan* – this option allows copying the selected prefixes to another dial plan. To do this, select the prefixes and the target dial plan, and click the 'Copy' button.

3.1.4.1 Creating a dial plan prefix

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



Dial plan # 0 'NumberPlan#0'

Common prefix settings 0	
Title	Prefix#00
Dial plan	[0] NumberPlan#0
Access category	[0] AccessCat#0
Check access category	☐
Prefix type	TrunkGroup
TrunkGroup	not set
Direction	local network
CallerID request	☐
CallerID mandatory	☐
Dial mode	overlap
Do not send end-of-dial (ST)	☐
Priority	100
Max session time (sec)	5
Session warning time (sec)	0
Logical operator	or
CdPN settings	
Number type	unchanged
Numbering plan type	isdn/telephony
Skip first digits	0
Direct route timers	
Short timer	5
Duration	30

Apply Cancel

Common Prefix settings

- *Title* – name of the prefix;
- *Dial plan* – selects a dial plan;
- *Access category* – selects 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* – selects the prefix type:
    - *TrunkGroup* – transition to a trunk group;
    - *Trunk Direction* – transition to a trunk direction;
    - *Change dial plan* – this option allows you to enter another dial plan when this prefix is dialed. When this prefix type is selected, the *New Dial plan* option becomes available, where you should specify the dial plan for transition;
    - *Subscriber pool* – 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;
- *Pickup group* is used to configure the interception group transition prefix;
- *IVR scenario* is used to configure the IVR script pickup group transition prefix.

Parameters of the 'Trunk Group and Trunk Direction' Prefix

Main Prefix Parameters:

- *TrunkGroup* – a trunk group to which the call will be routed by this prefix;
- *Direction* – a 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 3.1.17 RADIUS Configuration);
- *Dial mode* – a method of number transmission:
  - *enblock* – after collection of all address information;
  - *overlap* – without waiting for collection of all address information.
- *Do not send end-of-dial (ST)* – when this option is active, the end dial marker is not sent (ST in SS or sending complete in PRI);
- *Priority* – if there are some overlapping masks in the dial plan, the call will be made into the prefix with a higher priority. The value of 0 is the highest priority, 100 – the lowest priority;
- *Max session time (sec)* – limit duration of calls passed through this prefix;
- *Session warning time (sec)* – activates when using the option 'Max session time (sec)', an audible signal is issued, which warns about the end of the call for a specified number of seconds before the end of the call. If the specified time is more than 60 seconds, an additional warning signal will sound 5 seconds before the end of the call. If the specified time is less than 60 seconds, there will be no additional signal;
- *Logical operator:*
  - *OR* – if CgPN and CdPN masks are present on the prefix, there is no simultaneous analysis by CgPN and CdPN number;
  - *AND* – simultaneous analysis by CgPN and CdPN number is performed.

For correct operation of prefixes with the logical operator 'AND', it is necessary to configure a mask for CgPN and CdPN. If one of the masks is missing, the prefix does not work.

CdPN Settings:

- *Number type* – a called number type: unknown, subscriber number, national number, international number, no change. The selected number type will be sent in SS7, ISDN PRI, SIP-I/T signaling 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 plan type* – a called dial plan type; it may take the following values: unknown, isdn/telephony, national, private, no change. The selected dial plan type will be sent in IDSN PRI signaling 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).

- *Skip first digits* – the number of digits removed from the called subscriber number, starting from the first.

Direct route timers (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 waits for further dialing if a part of address information has already been received. Default value: 5 seconds;
- *Duration* – a timer for number dialing duration. Default value: 30 seconds.

Parameters of the 'Change dial plan' Prefix

- *New dial plan* – a dial plan to which a call will be transferred;
- *New access category* – a category assigned to the caller after switching to another dial plan;
- *Priority* – if there are some overlapping masks in the dial plan, the call will be made into the prefix with a higher priority. The value of 0 is the highest priority, 100 – the lowest priority;
- *Max session time (sec)* – limit duration of calls passed through this prefix;
- *Notify call completion in (sec) before* – activates when using the option 'Max session time (sec)', an audible signal is issued, which warns about the end of the call for a specified number of seconds before the end of the call. If the specified time is more than 60 seconds, an additional warning signal will sound 5 seconds before the end of the call. If the specified time is less than 60 seconds, there will be no additional signal;
- *Logic operator:*
  - *OR* – if CgPN and CdPN masks are present on the prefix, there is no simultaneous analysis by CgPN and CdPN number;
  - *AND* – simultaneous analysis by CgPN and CdPN number is performed.

  For correct operation of prefixes with the logical operator 'AND', it is necessary to configure a mask for CgPN and CdPN. If one of the masks is missing, the prefix does not work.

Modifiers when changing the dial plan:

- *CdPN modifiers* – intended for modifications based on the analysis of the called number;
- *CgPN modifiers* – intended for modifications based on the analysis of the calling number.

Parameters of the 'VAS Prefix'

Number masks for VAS prefix always must be ended with # symbol.

- *VAS type* – selecting the Supplementary Service type to manage it from the subscriber's telephone:
  - *CFU* – Call Forwarding Unconditional;
  - *CFB* – Call Forwarding Busy;
  - *CFNR* – Call Forwarding No Reply;
  - *CFOS* – Call Forwarding Out of Service;
  - *CFT* – Call Forwarding on schedule (Time);
  - *Call pickup* – call pickup;
  - *Conference* – conference call;
  - *Clear All* – canceling all services;
  - *Intercom* – intercom call (with an automatic answer from party B);
  - *Paging* – similar to Intercom, but with a call to conference numbers;
  - *Password* – setting a password;
  - *Password once* – access by password;
  - *Password access* – password activation;

  - *Restrict out* – restriction of outgoing communication;
  - *Follow me* – managed ‘*Follow me*’ forwarding;
  - *Follow me (no response)* – managed ‘*Follow Me*’ forwarding when there is no answer.
  - *DND – Do Not Disturb* feature;
  - *Blacklist* – black list;
  - *Call Park Set* – setting a subscriber to call parking slot;
  - *Call Park Get* – retrieving a subscriber from call parking slot;
  - *Voice Mail Local* – accessing your voice mail from your telephone;
  - *Voice Mail Remote* – accessing your voice mail from someone else's telephone;
  - *Intervention* – intervention;
  - *Speed Dial* – speed dial.
- *Action* – selecting an action for the service:
  - *Configure* – enabling a Supplementary Service;
  - *Cancel* – canceling a Supplementary Service;
  - *Control* – a Supplementary Service activity control;
  - *Add number* – add a number;
  - *Del number* – delete a number.

Parameters of the ‘Pickup Group’ Prefix

- *Pickup group* — a pickup group in which a call pickup is performed when this prefix is dialed. If you choose ‘Any’, pickup will be enabled for all groups;
- *CallerID request* – defining the Caller ID information necessity (caller number and category) for transition to the trunk group specified in ‘Trunk group’ field. When a call arrives from the communication node and the Caller ID information is missing in that call, Caller ID request will be directed to that node (INR message from SS7 signaling);
- *CallerID mandatory* – indicating that Caller ID information is mandatory during the direction transition. If Caller ID information cannot be received from the calling party, connection establishment process is interrupted;
- *Priority* — configuring prefix priority in the range from 0 to 100. Prefix which parameter value is lower has a greater priority (0 — the highest priority, 100 — the lowest priority);
- *Max session time (sec)* – limit duration of calls passed through this prefix;
- *Notify call completion in (sec) before* – activates when using the option ‘Max session time (sec)’, an audible signal is issued, which warns about the end of the call for a specified number of seconds before the end of the call. If the specified time is more than 60 seconds, an additional warning signal will sound 5 seconds before the end of the call. If the specified time is less than 60 seconds, there will be no additional signal;
- *Logical operator:*
  - *OR* – if CgPN and CdPN masks are present on the prefix, there is no simultaneous analysis by CgPN and CdPN number;
  - *AND* – simultaneous analysis by CgPN and CdPN number is performed.
- For correct operation of prefixes with the logical operator “AND”, it is necessary to configure a mask for CgPN and CdPN. If one of the masks is missing, the prefix does not work.

Direct route timers (this parameter is used when trunk groups are directly switched 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 dialed number already matches a sample in the dial plan, but additional digits may be also dialed, 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 Scenario' Prefix

- *IVR scenario* – an IVR scenario to which a call will be routed to on the basis of this prefix;
- *Priority* – configuring prefix priority in the range from 0 to 100. Prefix which parameter value is lower has a greater priority (0 —the highest priority, 100 —the lowest priority);
- *Max session time (sec)* – limit duration of calls passed through this prefix;
- *Notify call completion in (sec) before* – activates when using the option 'Max session time (sec)', an audible signal is issued, which warns about the end of the call for a specified number of seconds before the end of the call. If the specified time is more than 60 seconds, an additional warning signal will sound 5 seconds before the end of the call. If the specified time is less than 60 seconds, there will be no additional signal;
- *Logical operator:*
  - *OR* – if CgPN and CdPN masks are present on the prefix, there is no simultaneous analysis by CgPN and CdPN number;
  - *AND* – simultaneous analysis by CgPN and CdPN number is performed.

For correct operation of prefixes with the logical operator 'AND', it is necessary to configure a mask for CgPN and CdPN. If one of the masks is missing, the prefix does not work.

Direct route timers (this parameter is used when trunk groups are directly switched without prefix mask analysis – the *Direct Prefix* function in trunk group settings).

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

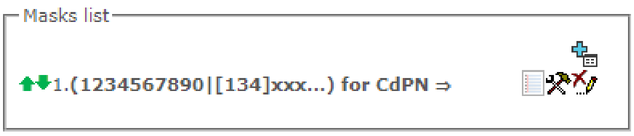
- *Short timer* – a time interval in seconds when the digital gateway waits for further dialing if the dialed number already matches with a sample in the dial plan, but additional digits may be also dialed, which will result in a match with another sample. Default value: 5 seconds;
- *Duration* – a timer for number dialing duration. Default value: 30 seconds.

Mask List

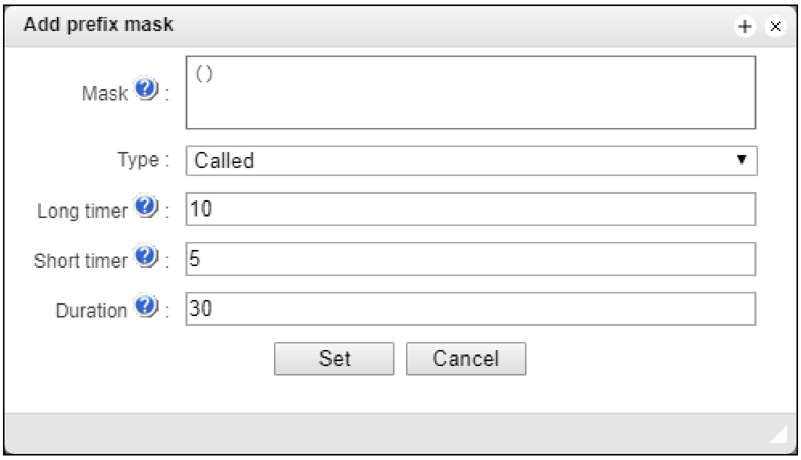
For created dial plans, the '*Mask List*' section allows configuring the masks of numbers for routing by this prefix.

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, the entries can be moved in the table by prioritizing them.



- *Mask* – a template or a set of templates, which is compared to the calling or called number received from the incoming channel. It is used for further call routing (for mask syntax, see section 3.1.5.2);
- *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 dial plan 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 dialed number already matches a sample in the dial plan, but additional digits may be also dialed, 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'*.

3.1.4.2 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 sign of the followings: 0-9*#;

***** – an asterisk (*);

– a pound key (#);

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

Prefix 1: (2xxxx)
Prefix 2: (23xxx)
When the number '23456' arrives to the dial plan, 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 a certain number of characters, e. g.:

Prefix 1: (2x{4,7})
Prefix 2: (23xxx)
When the number '23456' arrives to the dial plan, 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 dial plan, it will be processed with prefix 2.

3.1.4.3 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#** – dialling a 4-character 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 * and #.
   In general, this template disables VAS utilization using a phone unit.
2. ***#XX#** – dialling a 5-character 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 * and #.
   In general, this template is used to control VAS utilization from the phone unit.
3. ***XX*X.#** – dialling an N-character number which begins with * followed by two arbitrary characters (digits from 0 to 9, as well as * and # characters), then followed by *, and then by any number of characters (digits from 0 to 9, or *) until **#** is met.
   In general, this template is used to order VAS using a 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 dial plan 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

It is required 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)**

3.1.4.4 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 matches to 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.

3.1.4.5 Configuration example of prefix with 'subscribers pool' type

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 release cause ***3 – No route to destination***. But since this numbering is local to the gateway, it should have sent release cause ***1 – Unallocated (unassigned) number***.

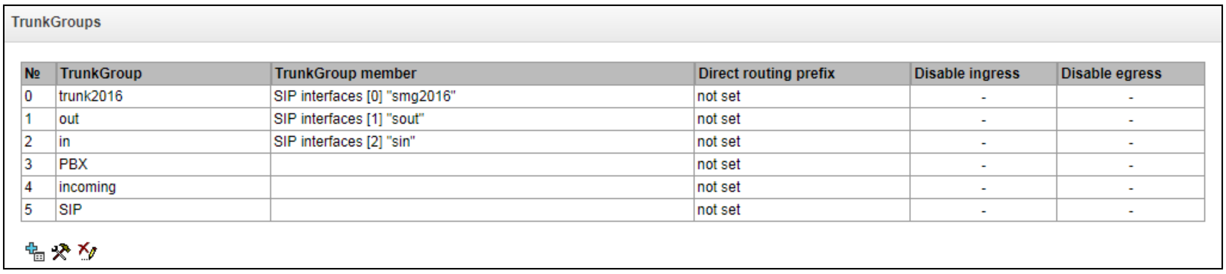
Solution

For correct clearback cause transmission, you should create local numbering – configure a 'subscribers pool' type prefix.

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

3.1.5 Call routing

3.1.5.1 Trunk Groups


TrunkGroups

№	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	-	-

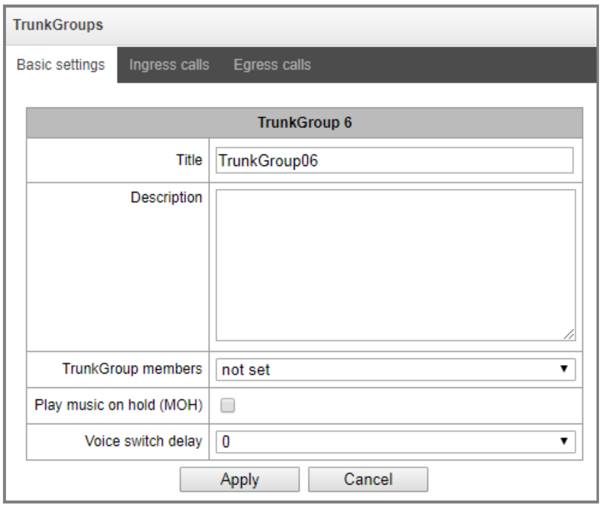
A trunk group is a set of connection lines (trunks), including the channels of E1 stream and data transmission bandwidth (IP channels). E1 stream channels are used for Q.931 and SS7. IP channel interfaces are SIP/SIP-T/SIP-I/H.323. To *edit a trunk group* double-click the corresponding row in the group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

<u>*'Basic Settings' Tab*</u>

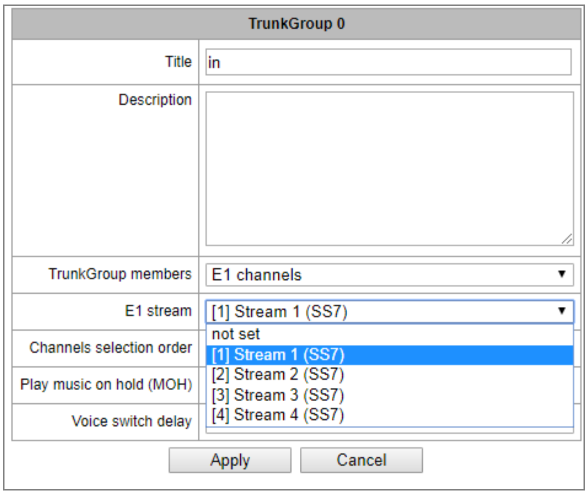


To access a trunk group, the device configuration should include prefixes that perform transition to this group.

- *Title* – trunk group name;
- *Description* – trunk group description;
- *TrunkGroup members* – trunk group members:
  - *Stream with Q.931 signaling, SS linkset or SIP interface;*
  - *E1 channels* – E1 stream channels with Q.931, SS7 signalling protocols;

- *SS7 Linkset lines;*
- *FXO lines;*
- *H323 Interface.*

- *E1 Stream* – selects E1 stream for trunk group assignment to E1 stream channels. This menu is active only when '*E1 channels*' value is selected for '*TrunkGroup members'* field.



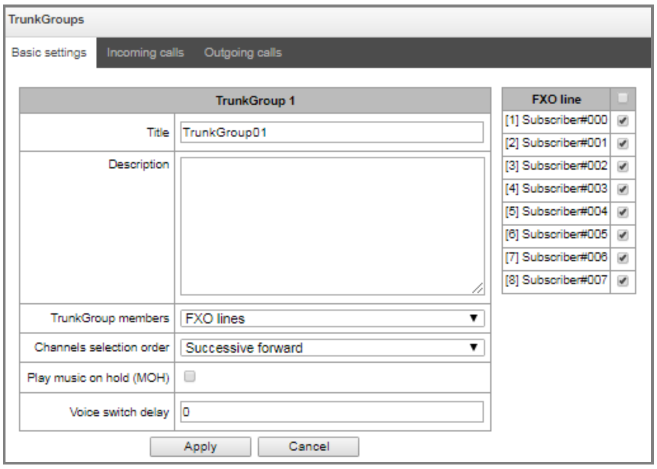
A single trunk group may be assigned to channels only within a single E1 stream.

- *SS7 Linkset* – SS7 link set for selecting E1 streams. This menu is available only when you choose 'SS7 Linkset lines' in 'TrunkGroup members' menu.
- *Channels selection order* – channel selection order in E1 streams. This menu is available only when you chose "SS7 Linkset lines" in "TrunkGroup members" menu;
- *Play music on hold (MOH)* – enabling *Music On Hold* option;
- *Voice switch delay* – forced voice frequency path delay after the subscriber's answer.

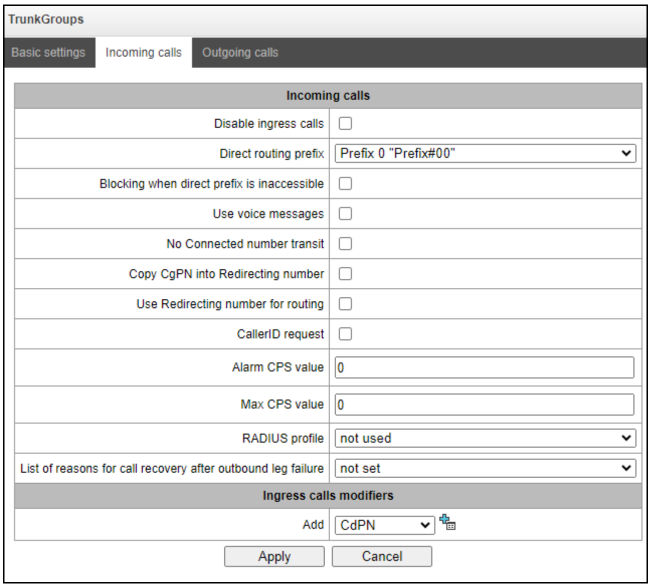
It is impossible to set trunk group with SS7 Linkset and trunk group with E1 streams from the same SS7 Linkset simultaneously.

FXO lines (only for SMG-200):

When FXO lines are selected as TrunkGroup members, the window with FXO lines to be selected for interaction in the Trunk group is opened.



<u>'Incoming calls' tab</u>



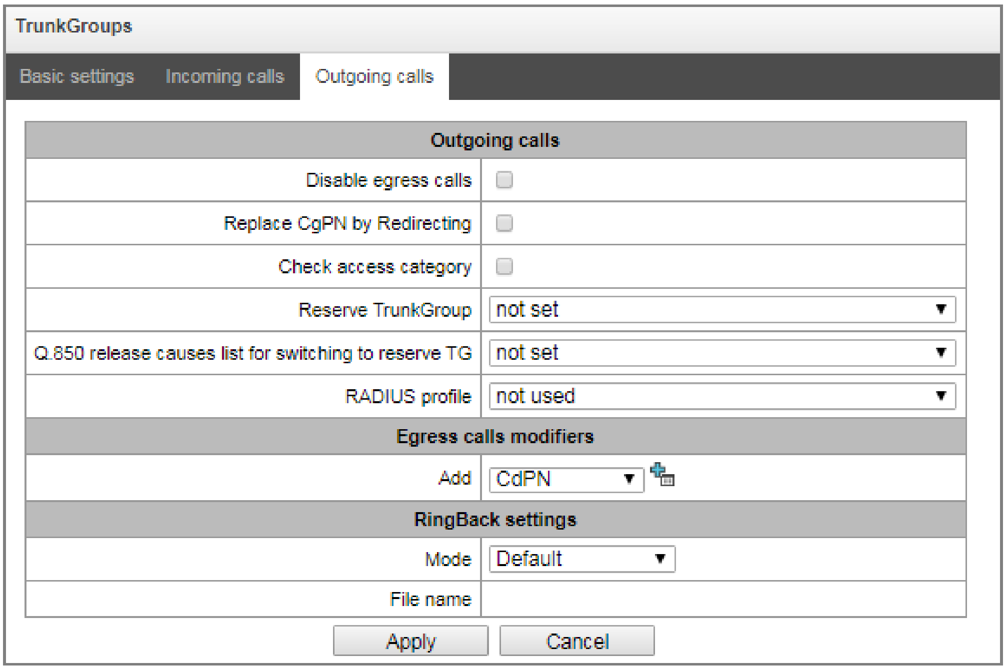
- *Disable ingress calls* – when this option is checked, the incoming calls are prohibited. Setting the call prohibition does not terminate any of the established connections;
- *Direct routing prefix* – the prefix will be used without caller or callee number analysis. It enables switching of all calls 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;
- *Blocking when direct prefix is inaccessible (SMG-500)* – the option is available only when E1 streams are in the trunk group and direct routing prefix is selected. When the option is enabled, then if the remote side (to which the direct prefix is routed) fails, the E1 stream from which the initializing call came is switched off. Thus, initializing side understands that the E1 stream is disabled and uses redundancy on the carrier side which initialize the call via the E1 stream;

- *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 G. VOICE MESSAGES AND MUSIC ON HOLD (MOH);
- *No Connected number transit* – disable the transmission of the Connected number field;
- *Copy CgPN into Redirecting number* – 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 number for routing* – when this option is checked, the SIP *diversion* field is used to route the incoming call in the dial plan using CgPN number masks;
- *CallerID request (SMG-500)* – specify the need of a caller's information (number and category) to call the trunk group. If a call is received from an interacting node and do not contain CallerID information, the CallerID request will be sent to the calling node (INR messages via SS7);
- *Alarm CPS value* – 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;
- *Max CPS value* – the maximum number of calls per second that can be received by a trunk group. ‘0’ value – turning off the CPS limit. 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* – selecting the RADIUS profile to use (profiles are configured in the RADIUS Configuration/Profile List menu, in section 3.1.17.2);
- *List of reasons for call recovery after outbound leg failure* – selecting the ‘List of reasons to restore the Q.850’ table to configure the reasons for the Q.850 release to restore the call in case of failure of the outgoing leg. If a call received through the trunk group with the enabled option was released not from an incoming side and the cause of the release is present in the selected table, then SMG will try to recover the connection without interrupting the conversation on the A call leg using recall or alternative routes if the main is not unavailable.

Ingress calls modifiers

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

'Outgoing calls' tab



- *Disable egress calls* – when this option is active, transmitting outgoing calls is forbidden. Setting the call prohibition does not terminate any of the established connections;
- *Replace CgPN by Redirecting* – when this option is active, the CgPN number is replaced with Redirecting;
- *Check access category* – when this option is active, it checks the possibility of call routing based on the rights determined by access categories;
- *Reserve TrunkGroup* – specifying a trunk group to which a call will be routed when routing to the current trunk group is not possible (all channels are engaged or inoperable);
- *Q.850 release causes list for switching to reserve TG* – selecting the *Q.850 release causes* table to configure the Q.850 release causes for switching to the redundant trunk group;
- *RADIUS profile* – selecting the RADIUS profile to use (profiles are configured in the *RADIUS Configuration/Profile List* menu, in section 3.1.17.2).

Egress calls 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*' and '*Objects*' — '*Remove object*' menus and the following buttons:

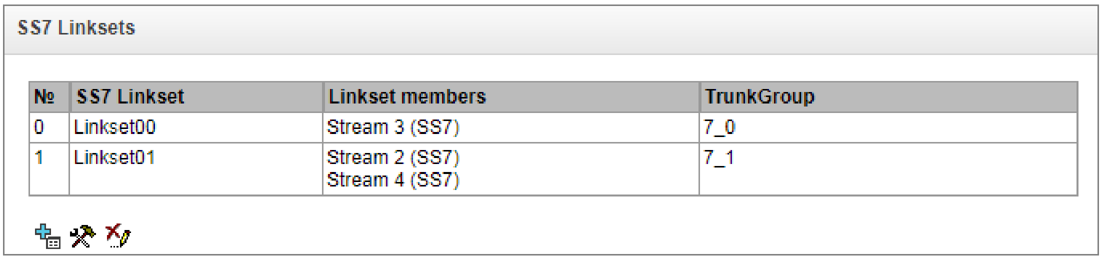
– Add trunk group;
– Edit trunk group parameters;
– Remove trunk group.

RingBack settings

Mode:

- *Default* — the option corresponds to the default settings;
- *RingBack* — play the standard ringback tone, ignore the default settings;
- *Audio file* — change the standard ringback tone to a chosen one which has been downloaded in *System settings* (an individual sound for the direction).

3.1.5.2 SS7 Linksets (for SMG-500 only)



SS7 Linksets

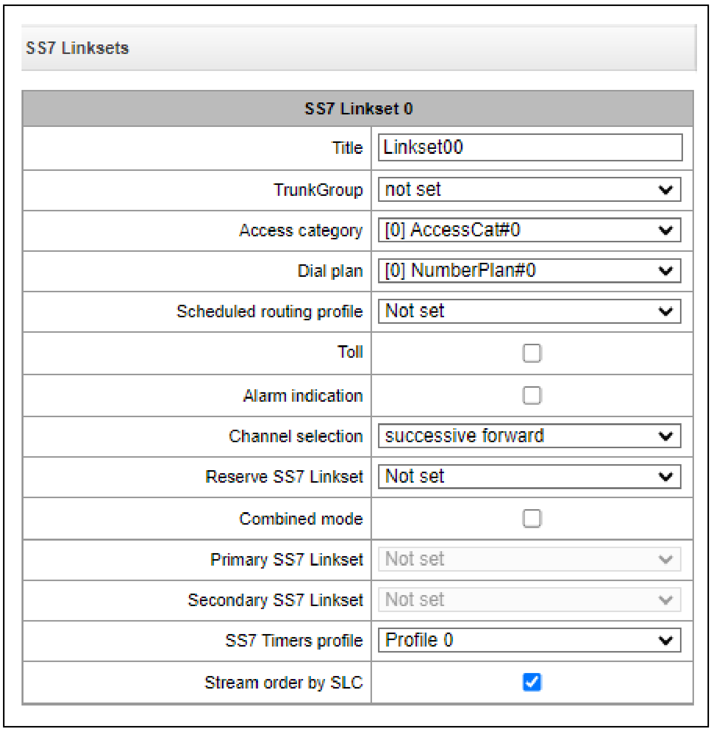
№	SS7 Linkset	Linkset members	TrunkGroup
0	Linkset00	Stream 3 (SS7)	7_0
1	Linkset01	Stream 2 (SS7) Stream 4 (SS7)	7_1

For SS7 protocol configuration, see *E1 streams* (section 3.1.3.4).

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

– Add SS7 linkset;
– Edit SS7 linkset;
– Delete SS7 linkset.

SS7 link set settings:



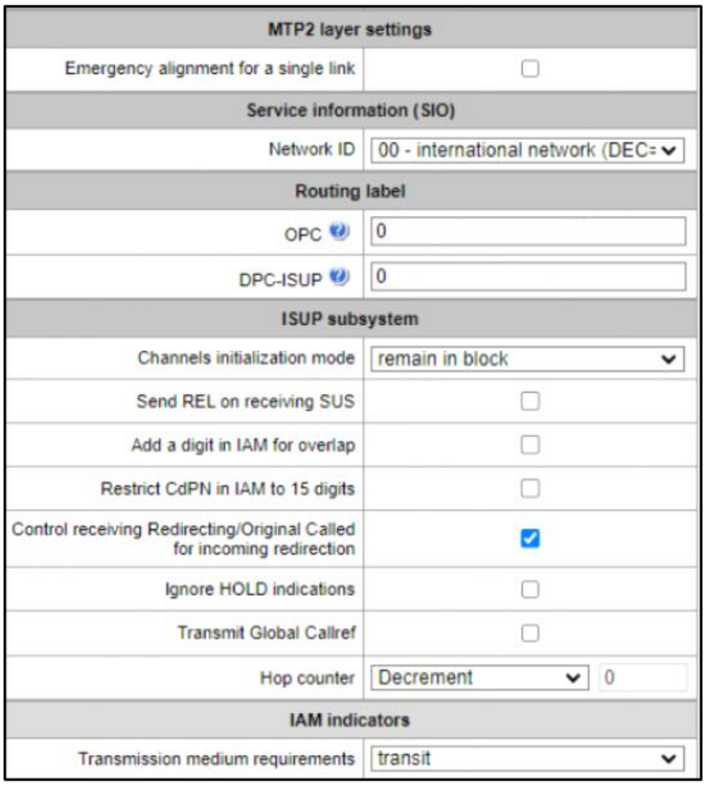
- *Title* – SS7 linkset name*;*
- *Trunk group* – name of a trunk group that SS7 linkset operates with;
- *Access category* – selects access category;
- *Dial plan* – defines dial plan that will be used for routing in this group (necessary for dial plan negotiation);
- *Scheduled routing profile* – selects '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, it is recommended to set inverse channel engagement types.

- *Reserve SS7 Linkset* – redundant SS7 linkset selection. When the main SS7 linkset is not available, the whole signalling message exchange will be performed through the redundant SS7 linkset;
- *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 Linkset* – selects 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 Linkset* – selects 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 linksets.

- *SS7 Timers profile* – selects the timer profile that will be used for the current SS7 linkset;
- *Stream order by SLC* – affects the operation of the *Order of channel engagement* setting. With this option enabled, the order of engaged E1 streams is determined by the SLC number (sorted from a smaller SLC to a larger one), with this option disabled the order is determined by the E1 stream index.



MTP2 level

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

Service information (SIO)

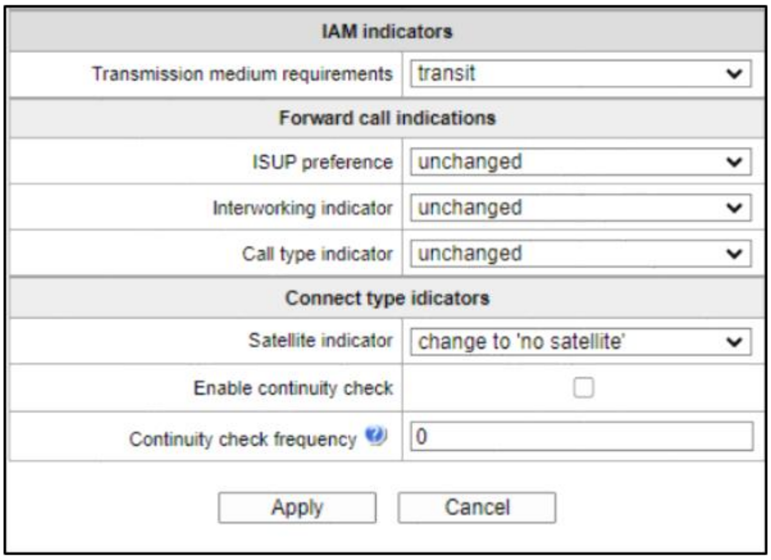
- *Network ID* – indicates the network type: international, national, local network or reserve.

Routing label

- *OPC* – own code of the signaling point;
- *DPC ISUP* – destination point code of the ISUP subsystem.

ISUP subsystem

- *Channels initialization mode* – device operations during stream recovery:
  - *Remain in block* – channels remain blocked (BLO);
  - *Individual unblock* – sending unblock command (UBL) for each channel;
  - *Group unblock* – sending channel group unblock command (CGU);
  - *Group reset* – group reset command (GRS).
- *Send REL on receiving SUS* – sending *Release* message in response to *Suspend* message;
- *Add a digit in IAM for overlap* – sending a single digit of the number to *Called Party number* of IAM message if overlap dialing method is used;
- *Restrict CdPN in IAM to 15 digits* – when active, 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* – this checkbox enables controlling the presence of *Redirecting/Original Called* fields with redirection information in incoming IAM message; when this option is active, the call will be rejected if these fields are absent;
- *Ignore HOLD indication* – when checked, SMG will ignore the CPG messages with *remote hold* or *remote retrieval* signs;
- *Transmit Global Callref* – when there is no *Global Call Reference (GCR)* field in an incoming leg, SMG forms it automatically;
- *Hop counter* – setting rules for operation with hop counter field:
  - *Decrement* – transmission with decreasing value;
  - *No change* – transmission without any changes;
  - *Preset* – transmission with pre-assigned value;
  - *Don’t send* – disabling hop counting.



IAM messages indicators

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

Forward call indicators

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

Connect type indicators

- *Satellite indicator* – identifies the presence of a satellite channel:
  - *Change to 'no satellite'* — changing identifier value to *no satellite* regardless of the value received from the incoming channel;
  - *Unchanged* – keeping the indicator value unchanged;
  - *Add one satellite* – this setting is used if the signal link operates via satellite channel. In this case, a 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. The SMG sends the frequency value to the channel and then detects it on reception after transmission through the channel. If the frequency is detected, the call will be served at 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 continuity checks during outgoing calls performed via 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 3.1.8.2 SS7 Categories.

Examples

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

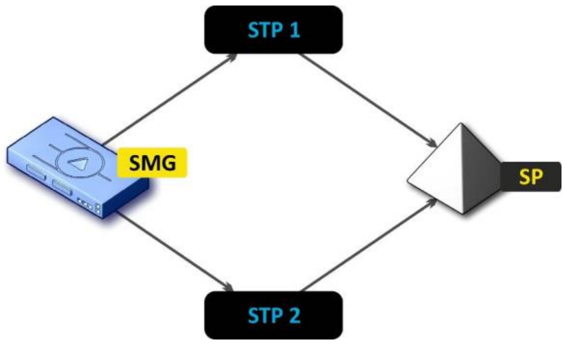


Fig. 17 – SMG connection method for operation in SS7 quasi-associated mode via STP

Objective

It is necessary 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, one 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:

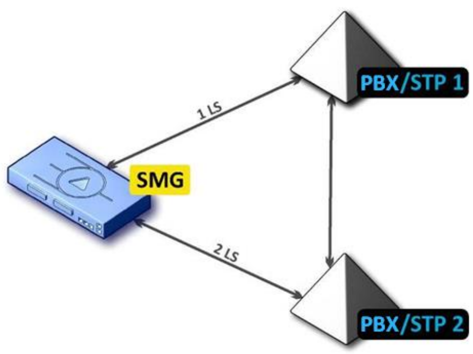


Fig. 18 – SMG connection method for operation in SS7 quasi-associated mode via PBX with STP
(*LS – SS7 Link Set)*

Objective

It is necessary to provide SMG connection to a couple of PBXes 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 'Reserve SS7 Linkset' setting in the first SS7 link set configuration.

SMG connection method example for operation in combined mode:

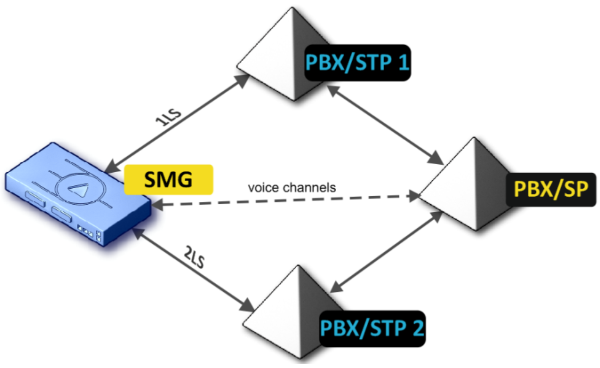


Fig. 19 – SMG connection method for operation in combined mode

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 linkset configuration, SMG stream 1 is connected to PBX/STP 2 and used for the second SS7 linkset configuration, SMG stream 2 is connected to PBX/SP and used for the third SS7 linkset 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 linkset in the *'Primary SS7 Linkset'* setting and the **second** SS7 linkset in the *'Secondary SS7 link set'* setting in the third SS7 link set configuration.

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

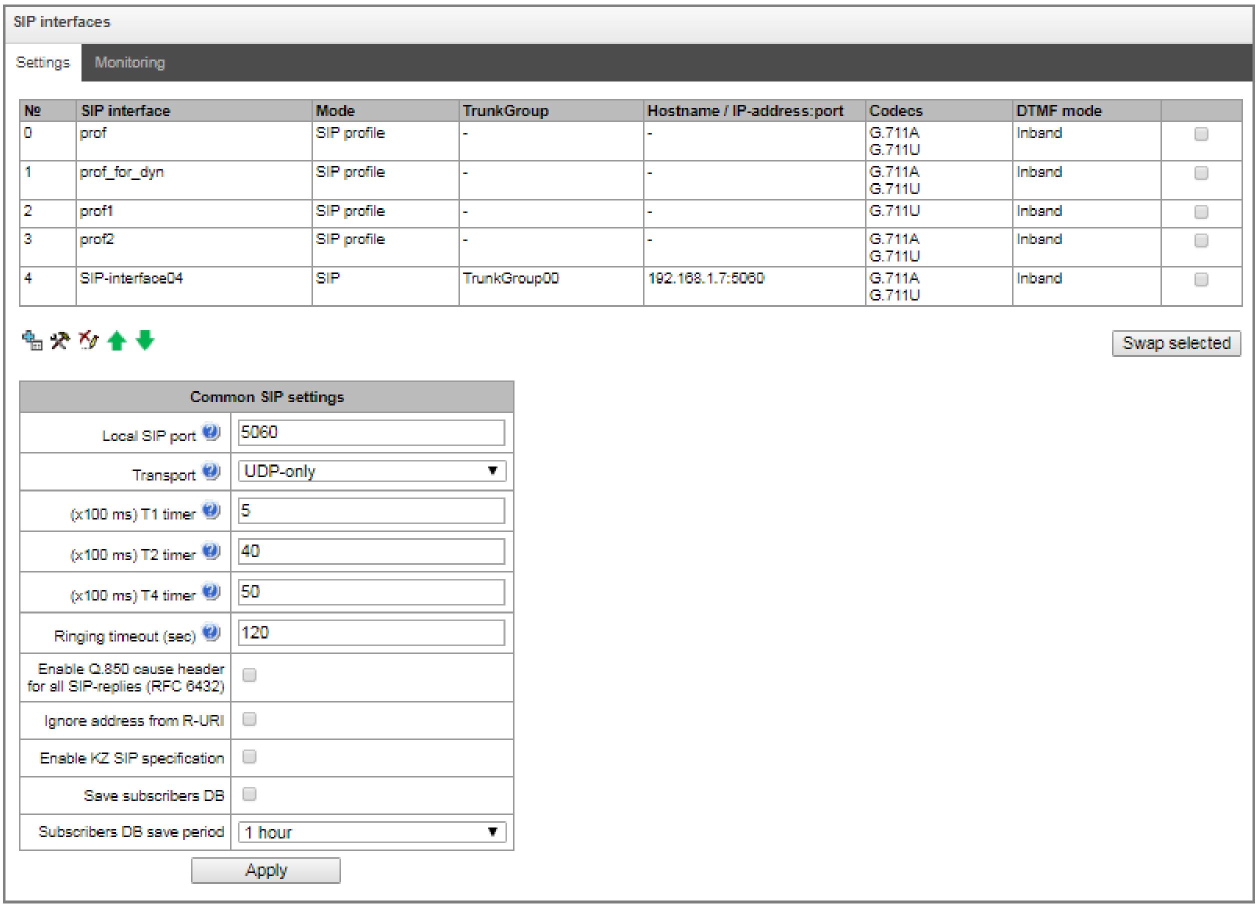
Configuration

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 called number for international calls using the SIP-T protocol.



Common SIP settings

- *T1 timer* – timeout for a response to the request, after which the request will be sent again. The maximum retranslation interval for INVITE requests is 64*T1;
- *T2 timer* – the maximum retranslation interval for responses to the INVITE request and for all requests except for the INVITE requests;
- *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.
- *Enable Q.850 cause header for all SIP codes of a reply (RFC 6432)* – when this option is active, the device analyses the Q.850 cause field in all final SIP messages. If the option is not active, the Q.850 cause field is only analyzed in BYE and CANCEL messages;

- *Ignore address from R-URI* – when this option is active, address information after the '@' separator in Request-URI is ignored. Otherwise, the gateway checks if the address information matches the device's IP address and host name; if there is no match, the call is rejected;
- *Enable KZ SIP specification* — setting a specification in accordance with the requirements of the Republic of Kazakhstan;
- *Save subscribers DB* – when this option is active, saving 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;
- *Subscriber DB save period* – setting 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.

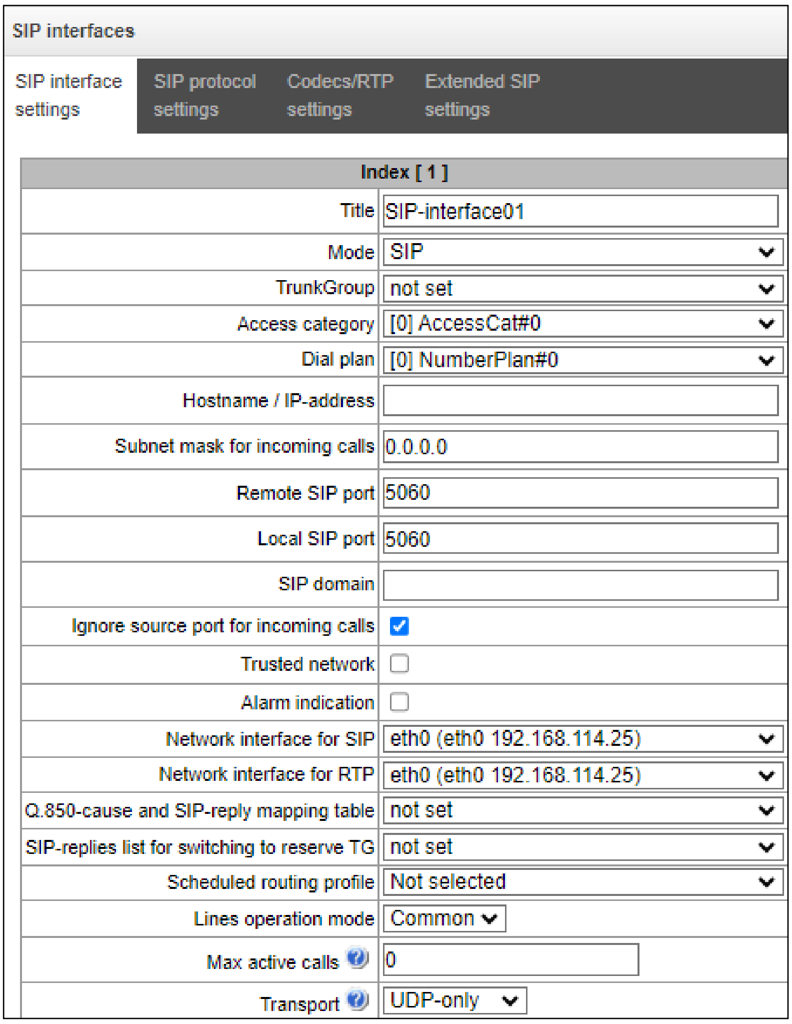
The signal processor of the gateway encodes analogue voice traffic and fax/modem data into digital signals and performs its reverse decoding. The gateway supports the following codecs: G.711 (A/U), G.729 (A/B), OPUS[1] and AMR[1].

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 3.20.3.

'SIP Interface settings' tab



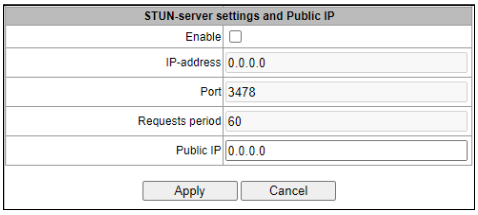
- *Title* – the interface name;
- *Mode* – selects the interface protocol (*SIP/SIP-T/SIP-I/SIP Profile*);
- *Ingress RADIUS profile* – selects the RADIUS profile for the *SIP* Profile interface for incoming communication (for other interfaces, the RADIUS profile is assigned in the trunk group);
- *Egress RADIUS profile* – selects 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* – selects an access category;
- *Dial plan* – defines the dial plan that will be used for dialling from this port (required for coordination of dial plans);
- *Hostname/IP-address* – IP address or name of the host communicating via the gateway's SIP/SIP-T protocol;

[1] The field is disabled in the SIP profile mode.

- *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;
- *Remote SIP port* – a UDP/TCP port of the communicating gateway that is used to receive SIP/SIP-T signalling;
- *Local SIP port* – 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 source port for 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;
- *Alarm 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;
- *Network interface for SIP* – the network interface selected to receive and transmit signalling SIP messages;
- *Network interface for RTP* – selects a network interface to receive and transmit voice traffic;
- *Q.850-cause and SIP-reply mapping table* – the selected table of correspondence between Q.850-cause and SIP-reply codes. To configure correspondence tables, use the *Internal Resources* menu.
- *SIP-replies list for switching to reserve TG* – selects 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* – selects a profile for the *Scheduled Routing* service configured in the Internal Resources section;
- *Lines operation mode* – setting lines operation mode to limit the number of simultaneous calls via this interface:
  - *Common* – considering the total number of simultaneous calls (incoming and outgoing) via this interface;
  - *Separate* – incoming and outgoing calls are counted separately;
- *Max active calls* – maximum number of simultaneous (incoming and outgoing) connections via this interface. The field is displayed if *Common* operation mode is selected;

- *Number of incoming lines* – number of simultaneous incoming calls via this SIP interface. The field is displayed if *Separate* operation mode is selected;
- *Number of outgoing lines* – number of simultaneous outgoing calls via this SIP interface. The field is displayed if *Separate* operation mode is selected;
- *Transport* – selecting a transport level protocol using for reception and transmission of SIP messages:
    - *TCP-prefer* – receiving by UDP and TCP. Sending via TCP. If not connected by TCP, make attempt by UDP;
    - *UDP-prefer* – receiving by UDP and TCP. Transmitting by TCP whenever packet is greater than 1300 bytes, otherwise by UDP;
    - *UDP-only* – receiving and transmitting only by UDP;
    - *TCP-only* – receiving and transmitting only by TCP.
- *Global Callref generation* – if there is no GCR in a call, it will be generated locally. If there is GCR in a call, it will be transmitted further without generating a new one. *The option is only enable for SIP-I*;
- *Node ID* – an identifier used for generating a global Callref. The range of allowed values is [0;255]. *The option is only enable for SIP-I.*

STUN server settings and Public IP:



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, use STUN or Public IP (used separately).

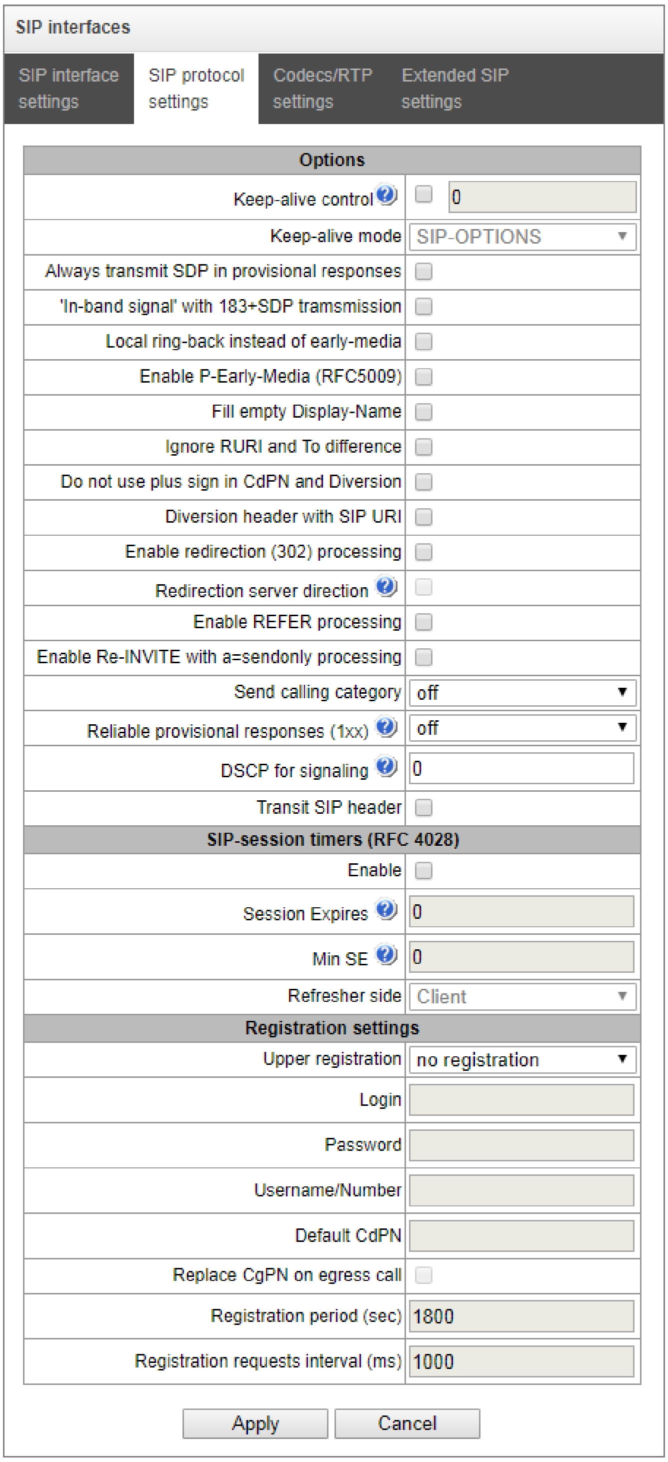
- *Enable* – when checked, use STUN server, otherwise use a specified public IP address;
- *IP-address* – IP address of STUN server;
- *Port* – server port for request transmission (default value is 3478);
- *Requests period* – time interval between requests (10–1800 seconds);
- *Public IP* – sets public (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 settings' tab



SIP/SIP-T/SIP-I Options Configuration:

- *Keep-alive control* – a function that controls direction availability by sending OPTIONS requ-ests; 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;

- *Keep-alive mode:*
    - *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 oppo-site 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 transmit SDP in provisional responses* – allows early forwarding of the voice frequ-ency 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 descript-tion 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;

- *Enable P-Early-Media (RFC5009)* – uses 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 empty Display-Name* – 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* – disables the Redirecting and Original Called numbers in SS7 calls when the values in *SIP RURI* and *To* fields are different;

- *Do not use plus sign in CdPN and Diversion* – disables addition of ‘+’ to a number, for International number type;

- *Diversion header with SIP URI* – uses SIP URI in the Diversion header instead of TEL URI;

- *Enable CCI* – 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 redirection (302) processing* – 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;

- *Redirection server direction* – this option is available when the redirection 302 processing is enabled. This enables forwarding of the call, which was sent using a public address, to the subscriber's private address received in reply 302 without dial plan routing. The call is routed directly to the address specified in the 'contact' header of reply 302 received from the forwarding server;

- *Enable REFER processing* – 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 Re-INVITE with a=sendonly processing* – 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;

- *Send calling category* – 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 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;
  - *require+* – duplicating SDP in 200 OK message when using *require: 100rel.*

- *DSCP for signaling* – a service type (DSCP) for SIP signalling traffic;

- *Transit SIP header* – enables transit of the received SIP headers into the outbound leg.

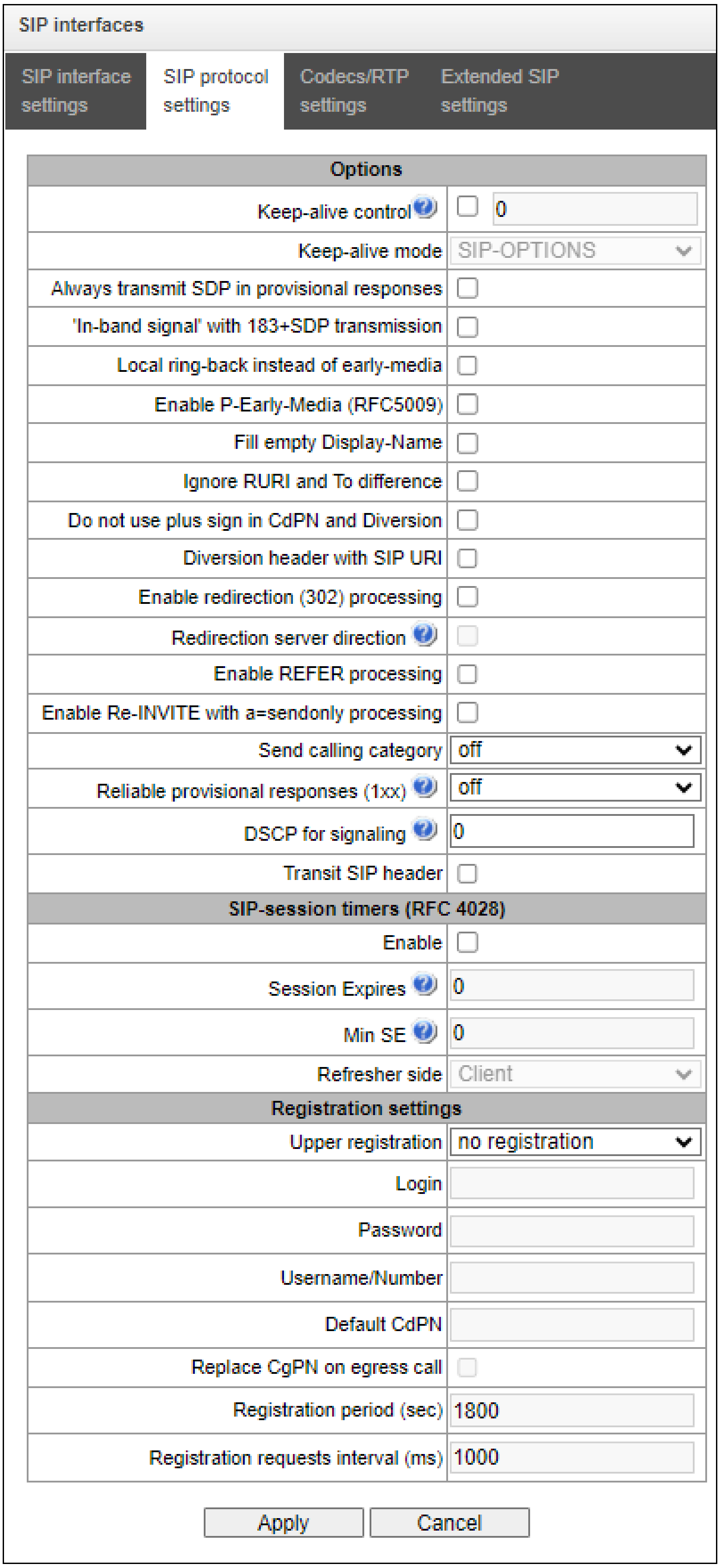
SIP-session timers (RFC 4028):

- *Enable* – 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);
- *Min SE (Minimum session expiration)* – 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;
- *Refresher side* – defines the party to renew the session (client (uac) – client (calling) party, server (uas) – server (called) party).

Registration settings (only for SIP mode):

- *Upper registration* – 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;
    - *User registration* – registration on the upstream server using parameters specified on the 'registration' tab. This registration type allows to define the list of subscribers with enabled access via this interface;
    - *Upper registration* – transit registration of device subscribers on the upstream server; when this option is selected, SMG will transfer subscribers' SIP messages via this SIP interface. When transit registration is selected, you should specify this SIP interface in the settings of SIP profile that requires transit registration.
- *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;
- *Replace CgPN on egress 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 period (sec)* – the time interval for registration renewal;
- *Registration requests 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:



- *Keep-alive 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.
- *Keep-alive mode:*
  - *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 (for SIP profile);
- *Register expires, max* – the maximum value of “expires” registration time (for SIP profile);
- *Always transmit SDP in provisional responses* – 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 ring-back 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;
- *Enable 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 empty Display-Name* – 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 plus sign in CdPN and Diversion* – disable addition of ‘+’ to a number, for International number type;
- *Diversion header with SIP URI* – use SIP URI in the Diversion header instead of TEL URI;
- *Enable redirection (302) processing* – 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 REFER processing* – 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 Re-INVITE with a=sendonly processing* – 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 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;
  - *require +* – duplicate SDP in 200 OK message when using require: 100rel.
- *DSCP for signaling* – a service type (DSCP) for SIP signalling traffic;
- *Transit SIP header* – allows transit of received SIP headers to the outbound leg;
- *Maximum number of redirects between subscribers* – the maximum possible number of consecutive redirects between subscribers, by default: 5.

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)

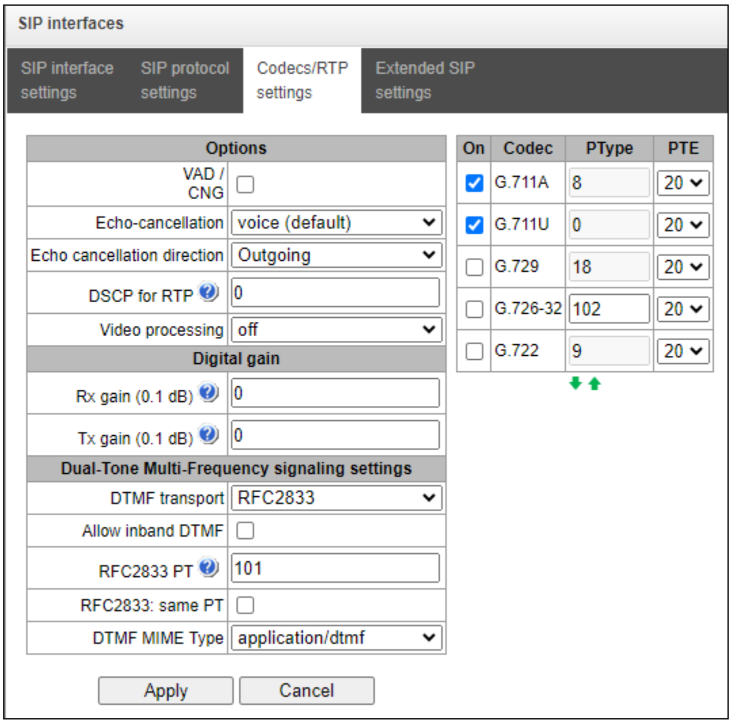
- *Enable* – when this option is checked, enables support of SIP session timers (RFC 4028). A session is renewed by re-INVITE requests sent during the session;
- *Session Expires* – a period of time in seconds before a forced session termination if the session is not renewed in time (from 90 to 64,800 seconds; 1,800 seconds is recommended);
- *Min SE* (Minimum session expiration) – 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;

- *Refresher side* – defines the party to renew the session (client (uac) – client (caller) party, server (uas) – server (callee) party).

***Upper registration settings*[1]**

- *Upper registration interface* – select SIP interface for transit registration.

<u>'Codecs/ RTP settings' tab</u>



Options

- *VAD/CNG (Voice activity detector / Comfort noise generator)* – 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:
  - *voice (default)* – echo cancellation is enabled in voice transmission mode;
  - *voice nlp-off* – echo cancellation is enabled in voice mode, non-linear processor (NLP) is disabled. If transmission and reception signal levels are very different, a weak signal might be suppressed by NLP. To prevent such suppression, this mode is used;
  - *speex algorithm;*
  - *off* – echo cancellation is disabled (this mode is set by default).

[1] The parameter block is only available for *SIP-profile* mode.

- *Echo cancellation direction:*
    - *Incoming* – the echo from the caller is suppressed;
    - *Outgoing* – the echo towards the subscriber is suppressed.
- *DSCP for RTP* – type of service (DSCP) for RTP;
- *Video processing* – activation of video connection in Offroad mode.

Digital gain

- *Rx gain (0.1 dB)* – received signal volume, amplification/attenuation of signal level received from the interacting gateway;

- *Tx gain (0.1 dB)* – transmitted signal volume, amplification/attenuation of signal level transmitted to the interacting gateway.

Dual-Tone Multi-Frequency signaling settings

- *DTMF transport* – 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.

- *Allow inband DTMF* – this option appears for all DTMF transmission methods except inband. With this option disabled, if SMG receives DTMF in two formats, e.g. RFC2833 and inband, then inband will be ignored and only RFC2833 will be processed;

- *Flash signal processing (RFC2833)* – when this option is checked, activates FLASH signal processing by INFO, frc2833 and re-invite methods for the VAS '*Call Transfer*' service. The option is available only for SIP profile;

- HOLD set/remove by:

    - Flash/* – HOLD by pressing Flash or '*' on a phone;
    - Flash/# – HOLD by pressing Flash or '#' on a phone;
    - Flash/*/# – HOLD by pressing Flash or '*' or '#' on a phone.

  The option is available only for SIP profile.

- *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);

- *RFC2833: same 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, the interface codecs and the order in which they will be used when establishing the connection will be selected. 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).

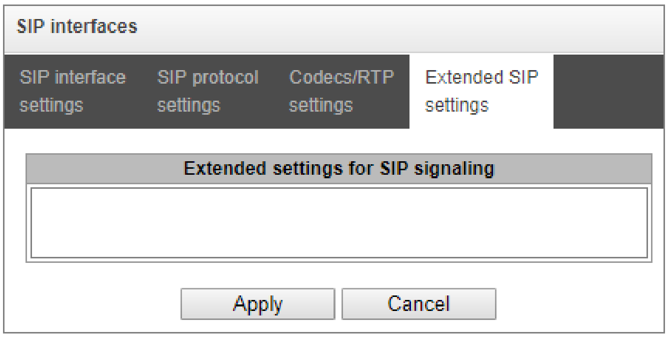
- *On* – when this option is checked, use the codec specified in the opposite field;
- *Codec* – set the codec to be used for voice data transmission. Supported codecs: G.711 (A/U), G.729 (A/B), G.726-32;

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

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

'Extended SIP 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;
- +(ABC) – add the specified text;
- -(ABC) – delete the specified text.

Examples of implemented operation rules are given in Table 11.

To transit the SIP headers, select the *Transit SIP Headers* 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 call leg without changes	Additional headers in the first call leg: P-Asserted-Identity: username@domain 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 leg: Subject: Test call
Transit the header group from the first call leg without changes	Additional headers in the first call leg: P-Asserted-Identity: sip:username@domain P-Called-Party-ID: sip:username@domain Privacy: id Subject: Test call	[sipheader:P-*=transit] Note that the rule: [sipheader:*=transit] will not work, as the * character can only replace part of the name.	These headers will appear in the second leg: P-Asserted-Identity: sip:username@domain P-Called-Party-ID: sip:username@domain
Insert header		[sipheader:insert[HEADERS_LIST]:RemoteIp=+(TEXT)] In all requests: [sipheader:insert:RemoteIp=+(example.SMG)] Only in INVITE request: [sipheader:insert,INVITE:RemoteIp=+(example.SMG)] Only in specified requests (for example, INVITE and ACK): [sipheader:insert,INVITE,ACK:RemoteIp=+(example.SMG)]	RemoteIp: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
Supplement text	To: "Ivanov A.A." <sip:123@eltex>	[sipheader:to=-(eltex)+(eltexdomain.loc)$]	To: "Ivanov A.A." <sip:123@eltexdomain.loc>
Example of complex modification	From: <sip:who@host>;tag=aBc	[sipheader:from=+(DISPLAY)-(who)+(12345)-(>)+(;user=phone>)$+(;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

The option allows to use TO instead of RURI for routing	We receive:
	`Request-Line: INVITE sip:558018@10.22.128.36:5060 SIP/2.0`
	`...`
	`To: <sip:73852245673@10.22.1.50;user=phone>`
		[siprequest:cdpn=to]	We send:
			`Request-Line: INVITE sip:73852245673@10.22.120.40:5060 SIP/2.0`
			`...`
			`To: <sip:73852245673@10.22.120.40;user=phone>`

Activate history-info sending in a forwarded call		[siprequest:history=true]	

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

<u>Acquiring a Display Name from a remote server via LDAP</u>

To configure obtaining Display Name from a remote server, add the configuration line to the 'Extended settings for SIP signaling' field.

SMG interrogates servers in certain interval of time and keeps an up-to-date name. When there is a call, names of an initiator and a destination is requested. If the base does not contain up-to-date names, the default names (configured in sip subscriber settings) are used.

Configuration string format:

```
STRING::
ldap:ID:display:INTERVAL:DIRECTION:IP:PORT:LOGIN:PASSWORD:BASE[:ATTRPHONE:ATTRDISPLAY]
```

- *ID* – an entry identifier. There might be the same description for several interfaces, in this case the IDs must be the same too. It solves the problem with duplicating of records for SIP profiles (when all the profile users have the same record);
- *INTERVAL* – base update interval (in minutes);
- *DIRECTION* – type of a subscriber which the option is applied to:
    - *sip* – From value for calling from SIP and To towards SIP;
    - *exchange* –To value for calling from SIP and From towards SIP;
    - * – both names are requested in the same section.
- *IP* – LDAP server address;
- *PORT* – LDAP server port;
    - * – specifies the default port 389.
- *LOGIN* – base user name;
- *PASSWORD* – base user password;
- *BASE* – path to the subscriber base server;
- *ATTRPHONE* – an attribute which describes Number (which will be used in the search of a name) in the base. The parameter is optional, you may not specify it, the default value is telephoneNumber;
- *ATTRDISPLAY* – an attribute which describes DisplayName. The parameter is optional, you may not specify it, the default value is displayName.

Configuration string example:

Full string:

[ldap:L1:display:30:sip:192.168.23.187:389:cn=user,dc=smg,dc=com:userpassword:dc=smg,dc=com:telephoneNumber:displayName]

Short string:

[ldap:L1:display:30:*:192.168.23.187:*:cn=user,dc=smg,dc=com:userpassword:dc=smg,dc=com]

3.1.5.4 H323 Interfaces

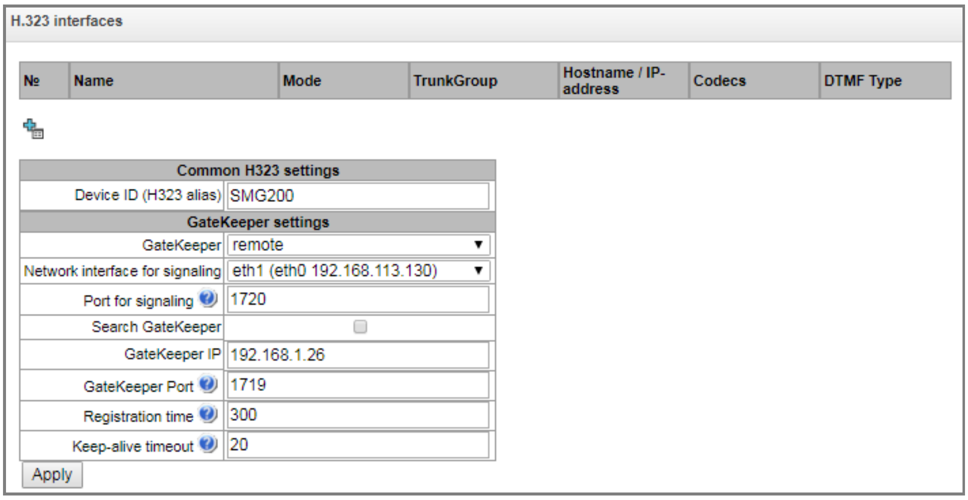
In this section you can configure general configuration settings for H.323 stack[1] and individual settings for each direction using H.323 protocol.

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 PBXes 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 localize the subscriber.

General Configuration of H.323



- *Device ID (Alias)* – the gateway name during the registration at the Gatekeeper.

GateKeeper settings

- *GateKeeper* – in the *'remote'* mode, SMG will interact with an external gatekeeper;
- *Network interface for signaling* – selects the network interface for H.323 signalling;
- *Port for signaling* – local TCP port for receiving H. 323 signalling messages;

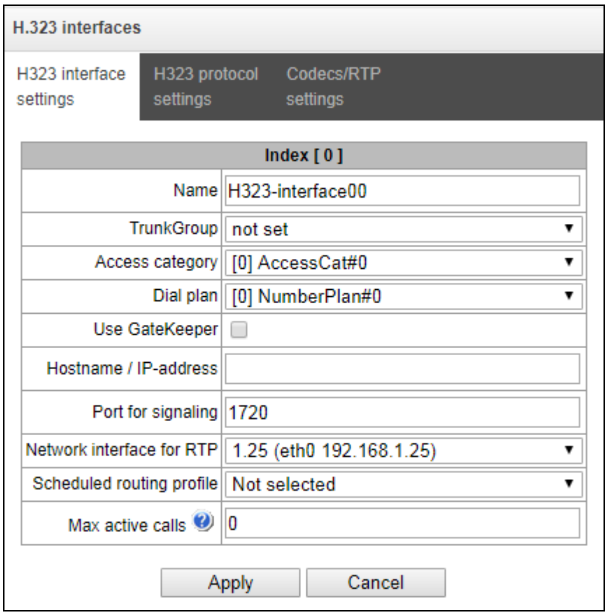
[1] The menu is only available in the software version with an H.323 license, for more information about licenses see 3.1.23 Licenses.

- *Search GateKeeper* – when this option is checked, the Gatekeeper is detected auto-matically 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);
- *Registration time* – the time frame (in seconds) for the device to register at the Gatekeeper;
- *Keep-alive timeout* – 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.

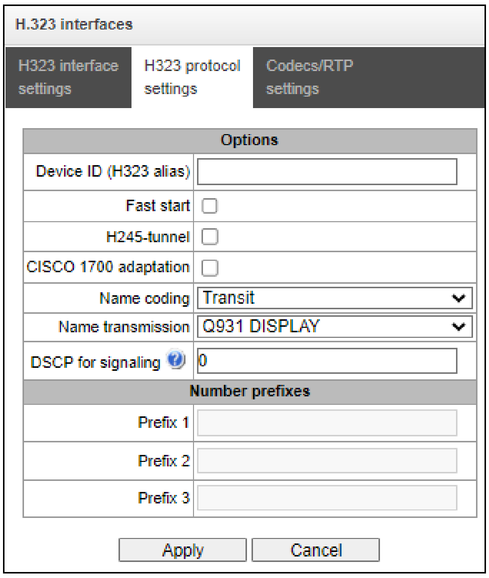
3.1.5.5 'H.323 Interface settings' tab



- *Name* – the interface name;
- *TrunkGroup* – name of the trunk group that includes this interface;
- *Access category* – select an access category;
- *Dial plan* – defines the dial plan that will be used for dialling from this interface (required for coordination of dial plans);
- *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;
- *Port for signaling* – a signalling TCP port of the communicating gateway used to receive H323 signalling;

- *Network interface for RTP* – selects a network interface to receive and transmit voice traffic;
- *Scheduled routing profile* – selects a profile for the *Scheduled Routing* service configured in the Internal Resources section;
- *Max active calls* – the maximum number of simultaneous (incoming and outgoing) connections through this interface.

3.1.5.6 'H.323 Protocol settings' tab



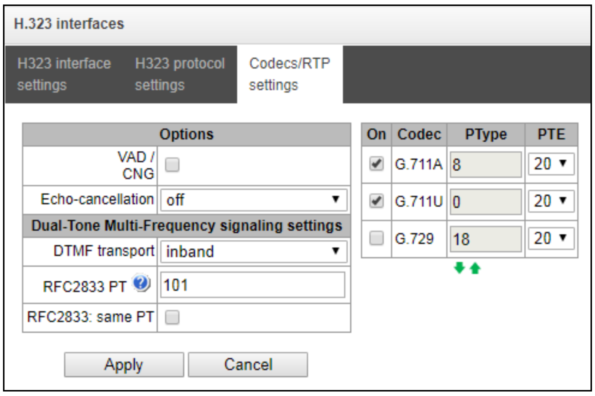
- *Device ID (H323 alias)* – the gateway name during the registration at the Gatekeeper;
- *Fast start* – when this option is checked, the quick start function is enabled; otherwise it is disabled. When using the option, session description for establishing a media channel is sent via H.225 protocol, otherwise – via H.245 protocol;
- *H245-tunnel* – when this option is checked, H. 245 tunneling through Q. 931 signal channels is enabled; otherwise it is disabled;
- *CISCO 1700 Adaptation* – when this option is active, it works as follows:
    - *Bandwidth* for Admission Request is set to 64000.
    - The following is added during the outgoing call:
        - *Remote alias* with CgPN value
        - *Local alias* with CdPN value
        - *Remote alias* with *H.323 ID Primary Directory Gatekeeper* value
        - *Local alias* with the *Device ID (Alias)* value from the general H.323 configuration
    - A search for an alternate H.323 interface is not performed during an incoming call.
- *Name coding:*
    - *Transit* – coding is not performed (by default, name is considered to be in UTF-8);
    - *CP 1251* – Windows-1251 coding;
    - *Siemens adaptation* – PBX Siemens coding;
    - *AVAYA adaptation* – PBX AVAYA coding;
    - *Latin transliteration* – Russian names will be transliterated with Latin letters.
- *Name transmission method:*
    - *Q931 DISPLAY* – transmission in Q.931 Display element with Codeset 5;
    - *AVAYA DISPLAY* – transmission in Q.931 Display element with Codeset 6;
    - *QSIG-NA* – transmission via QSIG-NA (ECMA-164).

- *DSCP for signalling* – a service type (DSCP) for signalling traffic (H.323);

Number prefixes

- *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).

3.1.5.7 'Codecs/ RTP settings' Tab



Options:

- *VAD/CNG (Voice activity detector / Comfort noise generator)* – this option 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 disabled.
- *Echo cancellation direction:*
  - *Incoming* – the echo from the subscriber is suppressed;
  - *Outgoing* – the echo towards the subscriber is suppressed.

Dual-Tone Multi-Frequency signaling settings

- *DTMF transport* – 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);

- *RFC2833: same 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*.

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).

- *On* – when this option is checked, use the codec specified in the opposite field;
- *Codec* – sets 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* – packetization time – the number of milliseconds (ms) of speech transmitted in a single packet.

3.1.5.8 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.

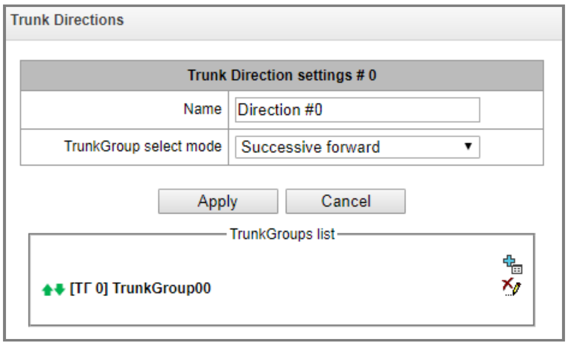
Trunk Directions

№	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:

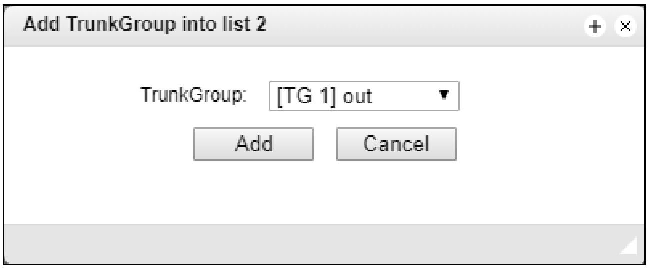
– Add direction;
– Edit direction parameters;
– Remove direction.

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



- *Name* – name of the trunk direction;
- *TrunkGroup select mode* – order of trunk group selection in the direction:
    - *Successive 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;
    - *Successive backward* – 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;
    - *Starting from first 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;
    - *Starting from last backward* – 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.

A list of trunk groups in the direction:



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

– Add;
– Remove.

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

3.1.6 Registration

3.1.6.1 Configuration

Configuring subscriber registration and authentication parameters for interfaces with a subscriber registration type.

Registration parameters:

- *Login* – name used for authentication;
- *Password* – password used for authentication;
- *User name/numbe*r – user number registered in the SIP domain;
- *SIP domain* – domain in which the subscriber is registered on the upstream server.

A registration binding to a particular SIP-interface is assigned/removed in the list of SIP interfaces. This allows to define a list of subscribers who are allowed to make calls via this interface.

3.1.6.2 Monitoring

When *Monitoring* is selected from the drop-down list, the table for monitoring subscriber registration on the upstream server is displayed.

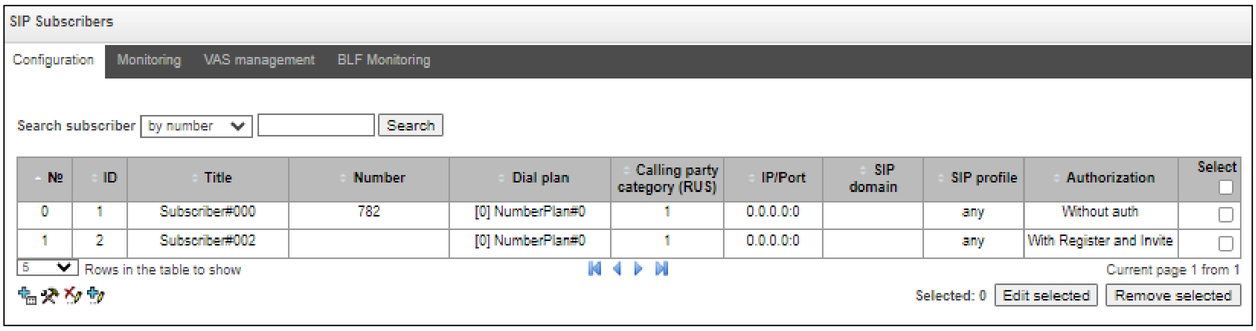
- *Login* – name used for authentication;
- *User Number/Number* – number of the user registered in the SIP domain;
- *List of SIP interfaces* – list of interfaces via which the subscriber is allowed to access;
- *Status* – subscriber registration status (registered, not registered, registration expired);
- *Reason* – possible reason for the lack of registration;
- *Registration expires* – time remaining until the registration expires.

3.1.7 Subscribers

The menu can be used to configure the parameters of SIP subscribers [1].

3.1.7.1 SIP Subscribers

3.1.7.1.1 Subscriber Configuration



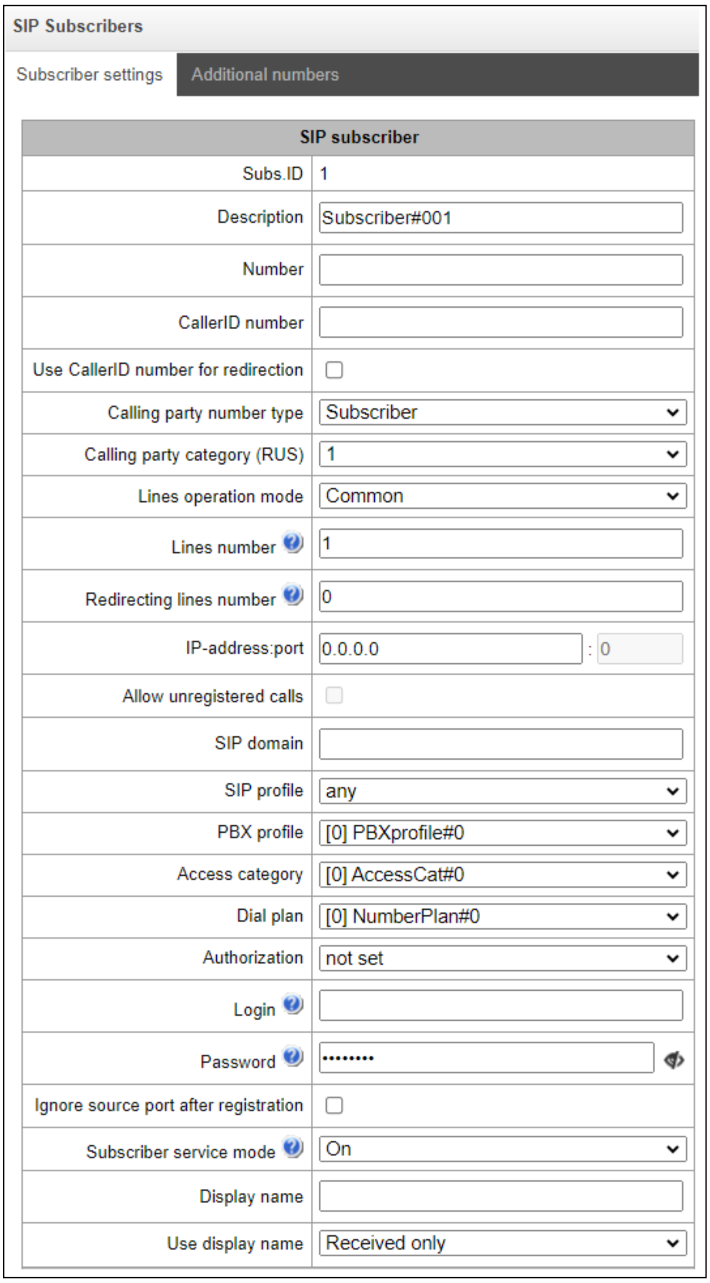
- *Search subscriber* – checking whether the specified subscriber number is available in the database of configured SIP subscribers; it can be checked by name, number, Caller ID, IP address: Port, SIP domain, SIP profile, PBX profile and dial plans;
- *Edit selected* – click this button to enter the 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 3.1.23 Licenses.

Subscriber Settings tab



- *Subs. ID* – unique subscriber identifier;
- *Description* – an arbitrary text description of subscribers;
- *Number* – subscriber's number. For a group of subscribers, the number of each following subscriber will be increased by 1;
- *CallerID number* – subscriber's Caller ID number. For a group of subscribers, number of each following subscriber will be increased by 1;
- *Use CallerID number for redirection*;
- *Calling party number type* – type of the subscriber number;

- *Calling party category (RUS)* – subscriber's Caller ID category;
- *Lines operation mode* – setting limits on the number of simultaneous calls. Can take two values: Common 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;
- *Lines number* – the number of simultaneous calls in which the subscriber can take part. The field appears if the *Line operation mode* is set to *Common*. The range of possible values is [1;255] or 0 – no limits;
- *Ingress lines number*[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;
- *Egress lines number*[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;
- *Redirecting lines number* – number of simultaneous calls for redirection. Valid range [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 unregistered calls* – 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* – selects the SIP profile. The SIP profile defines most of the subscriber settings (see section 3.1.5.2);
- *PBX profile* – selects the PBX profile (see section 3.1.7.5 PBX Profiles);
- *Access category* – selects an access category;
- *Dial plan* – define a dial plan for the subscriber;
- *Authorization* – defines the authentication mode for the device*:*
  - *not set* – authentication is disabled;
  - *with REGISTER* – authentication is performed only during the registration, using the REGISTER request;
  - *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 source port after registration* – after registration, messages from subscribers can arrive from any port of the registered address;

[1] These settings are displayed if the separate line mode is selected.

- *Subscriber service mode* – set a limit on the incoming and outgoing communication for the subscriber:

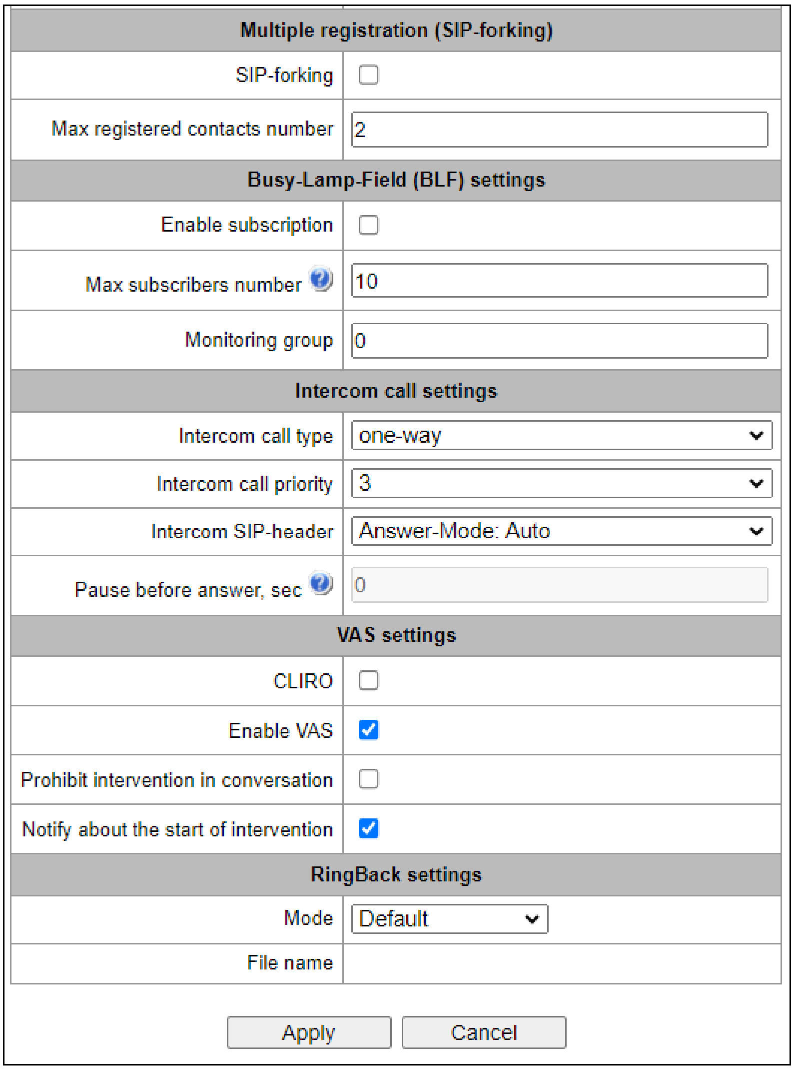
  - *off:* out of service. The subscriber number is present in the dial plan, but the subscriber terminal cannot be registered. Therefore, incoming calls will be rejected with the *out of order* cause; outgoing calls cannot be initiated;
  - *on:* all types of communication are available;
  - *off 1:* incoming communication is enabled; outgoing communication is to special services only;
  - *off 2:* incoming communication is disabled; outgoing communication is to special services only;
  - *denied 1:* full prohibition for incoming and outgoing calls. Calls will be routed according to the dial plan, but be rejected;
  - *denied 2:* full prohibition for incoming and outgoing calls, except for special services;
  - *denied 3:* incoming calls are prohibited, outgoing calls are allowed;
  - *denied 4:* incoming calls are prohibited, outgoing calls are allowed only for local and private communication;
  - *denied 5:* incoming calls are allowed, outgoing calls are fully prohibited;
  - *denied 6:* incoming calls are allowed, outgoing calls are allowed only for special services;
  - *denied 7:* incoming calls are allowed, outgoing calls are allowed only for local and private communication;
  - *denied 8:* incoming calls are allowed, outgoing calls are allowed only for local and private and zone communication;
  - *ignore:* excluded from the dial plan. The number is completely excluded from the subscriber number list of the dial plan. 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 dial plan.

- *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;

- *Use display name*– the display name usage mode (SIP display-name). Can take the values:

  - *Received only* – the *Display name* setting will not be used and the display-name parameter will always take the value indicated in the initiating INVITE request;
  - *Received prefer* – 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;
  - *Configured only* – regardless of the display-name indicated in the subscriber's request, the display-name configured on SMG will be used.

Multiple registration (SIP forking)



Multiple registration of up to five clients on one account is allowed. The registration is possible on the same or on different network interfaces. A call goes to all registered contacts simultaneously. Work with priorities (q-parameter) will be implemented in future versions.

- *SIP-forking* – enables multiple registration on a subscriber;
- *Number of registered contacts* – allowed acceptable range of registration per subscriber (the range of allowed values is [2; 5]).

Busy lamp field (BLF) settings

- *Enable subscription* – enable subscription to BLF events of other subscribers;
- *Max subscribers number* – 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 dial plan.

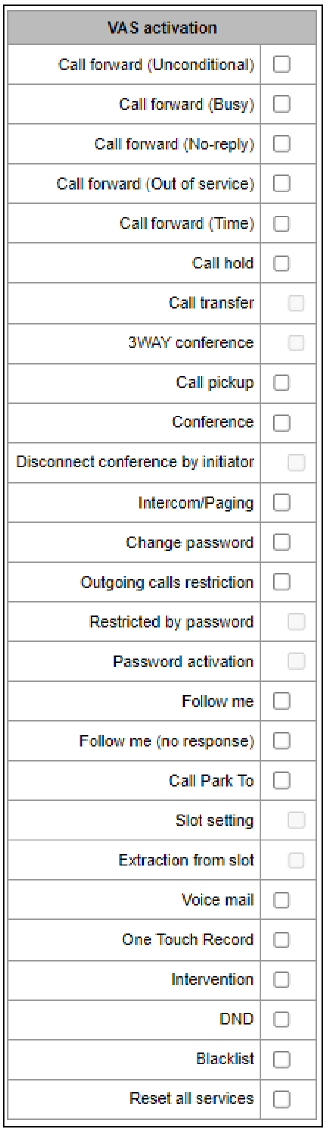
Intercom call settings

- *Intercom call type* – type of incoming intercom calls (call with auto-replay from 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;
  - *Ordinary call* – the incoming intercom call will be made as a normal call with no auto-reply from party B;
  - *Ignore* – the incoming intercom call will be rejected.
- *Intercom call priority* – the priority of the incoming intercom call over all other calls:
  - If subscriber A with priority 1 calls an already busy subscriber B (with one line and any priority), then subscriber A will be rejected;
  - If subscriber A with priority 2 calls an already busy subscriber B (with one line and any priority), then subscriber A will interrupt an already busy regular call;
  - If subscriber A with priority 2 calls an already busy subscriber B (with one line and any priority), but subscriber B is already busy with subscriber C (with priority 3), then subscriber A will be rejected;
  - Notification of subscriber A should pass in any case, with unconditionally higher priority.
- *Intercom SIP header* – selecting a SIP header that will be sent to the subscriber in the INVITE message during the 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 answer (sec)* – transmitting the pause time before the answer to the intercom/paging call in the '*answer-after'* parameter.

VAS Configuration

- *CLIRO* – a service for overriding the prohibition on caller number identification;
- *Enable VAS* – enabling Supplementary Services. When this option is active, the *VAS Activation Table* becomes available;
- *Prohibit intervention in conversation* – prohibiting the subscriber from interfering with the conversation;
- *Notify about the start of intervention* – if the call is interfered with, the subscriber will hear a sound signal; this option is active by default.

VAS Activation



- *Call forward (Unconditional)* – enables the Call Forwarding Unconditional (CF Unconditional) service;
- *Call forward (Busy)* – enables the Call Forwarding Busy (CF Busy) service;
- *Call forwarding (No-reply)* – enables the Call Forwarding No Reply (CF No Reply) service;
- *Call Forward (Out of Service)* – enables the Call Forwarding Out of Service (CF Out Of Service);
- *Call Forward (Time)* – enables the service of call forwarding depending on time;
- *Call hold* – enables the Call Hold service;
- *Call transfer* – enables the Call Transfer service;
- *3WAY conference* – enables the 3WAY conference service;
- *Call pickup* – enables the Call Pickup service;
- *Conference* with consequent assembly;

- *Disconnect conference by initiator* – 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;
- *Intercom/Paging* – activates access to the intercom and paging service (call with auto-reply from B side);
- *Change password* – changes the password to restrict the outgoing communication;
- *Outgoing calls restriction* – uses the outgoing calls restriction by password service;
- *Restricted 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* – activates the follow me service;
- *Follow me (no response)* – activates the follow me service;
- *Call Park To* – enables Call Park service;
- *Slot setting* – allows to put a subscriber to a slot within Call Park service;
- *Extraction from slot* – allows to retrieve a subscriber from a slot within Call Park service;
- *Voice mail* – enables the voice mail service;
- *One touch record* – enables the call recording service on demand;
- *Intervention* – enables the call intervention service;
- *DND (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;
- *Blacklist* – allows subscriber to include phone numbers in the black list for blocking calls from these numbers;
- *Reset all services* – cancels all numbers configured for forwarding by clicking a service prefix set in the dial plan.

For a detailed description of VAS, see APPENDIX H. WORKING WITH VAS SERVICES.

RingBack settings

RingBack settings allows to set up a ring back tone for each subscriber individually.

- Mode:
  - *Default* — the option corresponds to the default settings;
  - *RingBack* — plays the standard ringback tone, ignore the default settings;
  - *Audio file* — changes the standard ringback tone to a chosen one which has been downloaded in "System settings" (an individual sound for the direction).

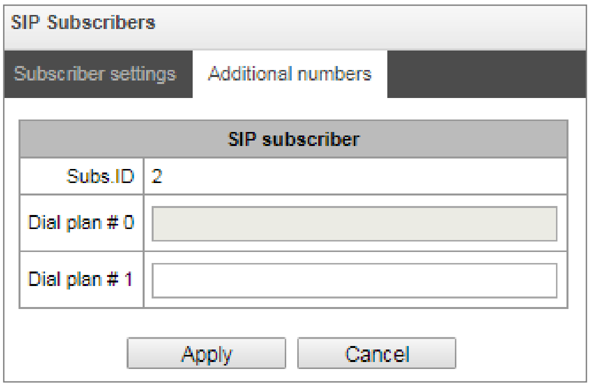
'Additional Numbers' Tab

A subscriber can have different numbers in different dial plans. So that, when a call passes through the prefix of dial plan changing, the subscriber's CgPN number is automatically replaced with the number in the corresponding dial plan.

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 the prefix 9.

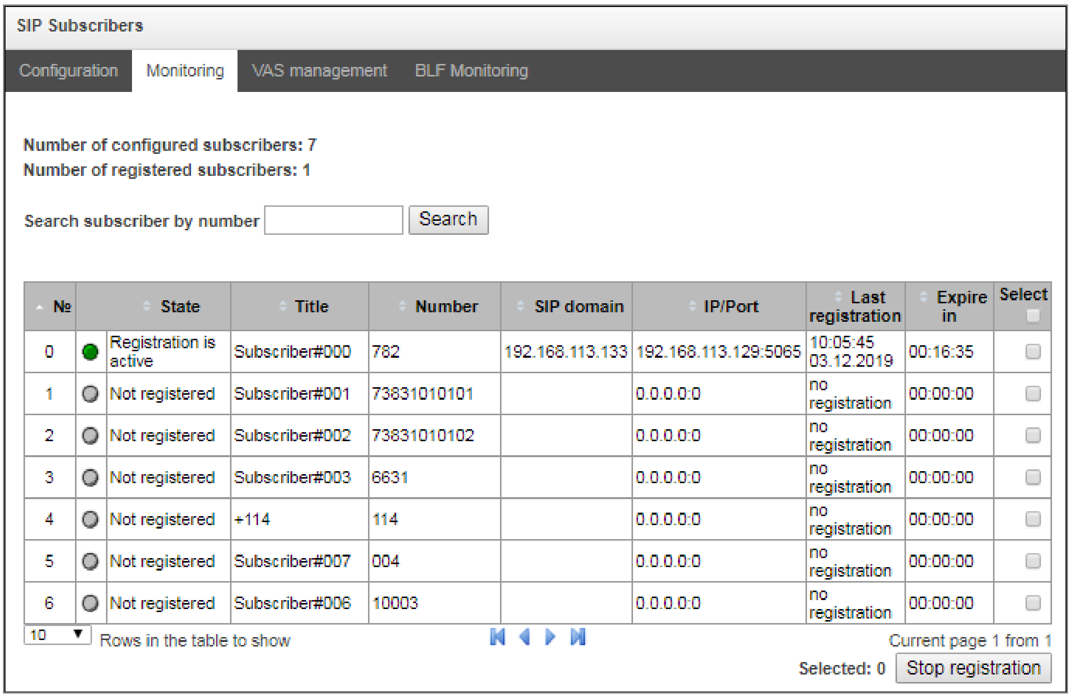
To solve this task, it is necessary to activate two dial plans in the *System settings* section, create a list of subscribers with short numbering at the gateway, and specify an external number for each subscriber in the *Additional numbers* tab in the *Dial plan # 1* field. In the *Dial plan # 1*, create the prefix of transition to the external network, while in the *Dial plan # 0*, create a prefix *(9x.)* Having *Change dial plan* type that will transfer the calls to the *Dial plan # 1*. When the subscriber dials a full number starting from 9, the call will be transferred to the *Change dial plan* prefix; when the call gets into the *Dial plan # 1*, the subscriber's CgPN number will automatically be replaced with their external number.



Dial plan # 0–16 – additional subscriber number in the corresponding dial plan.

3.1.7.1.2 Subscriber Monitoring

Upon selecting the '*Monitoring*' tab, a subscriber status table is displayed.


SIP Subscribers

Configuration | Monitoring | VAS management | BLF Monitoring

Number of configured subscribers: 7
Number of registered subscribers: 1

Search subscriber by number [ ] Search

№	State	Title	Number	SIP domain	IP/Port	Last registration	Expire in	Select
0	Registration is active	Subscriber#000	782	192.168.113.133	192.168.113.129:5065	10:05:45 03.12.2019	00:16:35	
1	Not registered	Subscriber#001	73831010101		0.0.0.0:0	no registration	00:00:00	
2	Not registered	Subscriber#002	73831010102		0.0.0.0:0	no registration	00:00:00	
3	Not registered	Subscriber#003	6631		0.0.0.0:0	no registration	00:00:00	
4	Not registered	+114	114		0.0.0.0:0	no registration	00:00:00	
5	Not registered	Subscriber#007	004		0.0.0.0:0	no registration	00:00:00	
6	Not registered	Subscriber#006	10003		0.0.0.0:0	no registration	00:00:00	

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

Selected: 0 Stop registration

- *Search subscriber by number* – checking the database of configured SIP subscribers, you can check by name, number, status, SIP domain, IP address:Port;
- *State* – subscriber registration status (registration is avtive, not registered, registration expired);
- *Title* – 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;
- *Expire in* – the time remaining before the registration expiration.

Click the *Stop registration* button to forcibly reset the registration for selected subscribers.

3.1.7.1.3 VAS Management

In this section, VAS settings for subscribers can be configured.

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, check the *Enable VAS* and select necessary VAS in the opened section, see 3.1.7.1.1 Subscriber Configuration.

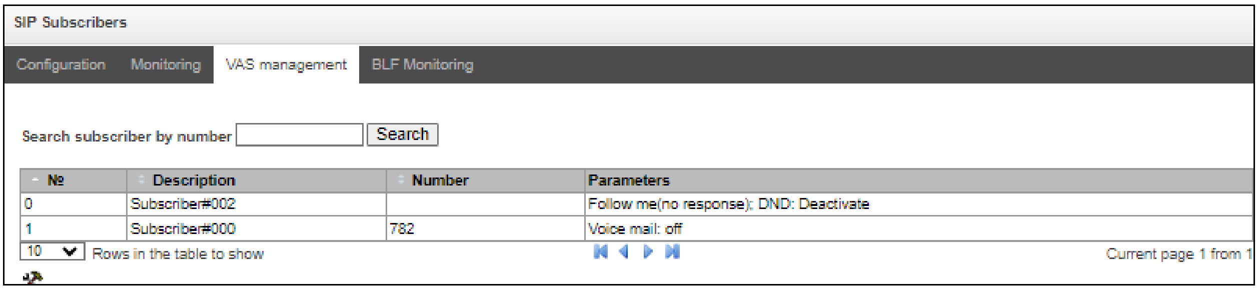
Subscribers can manage the status of VAS services from their telephone set. The following options are available:

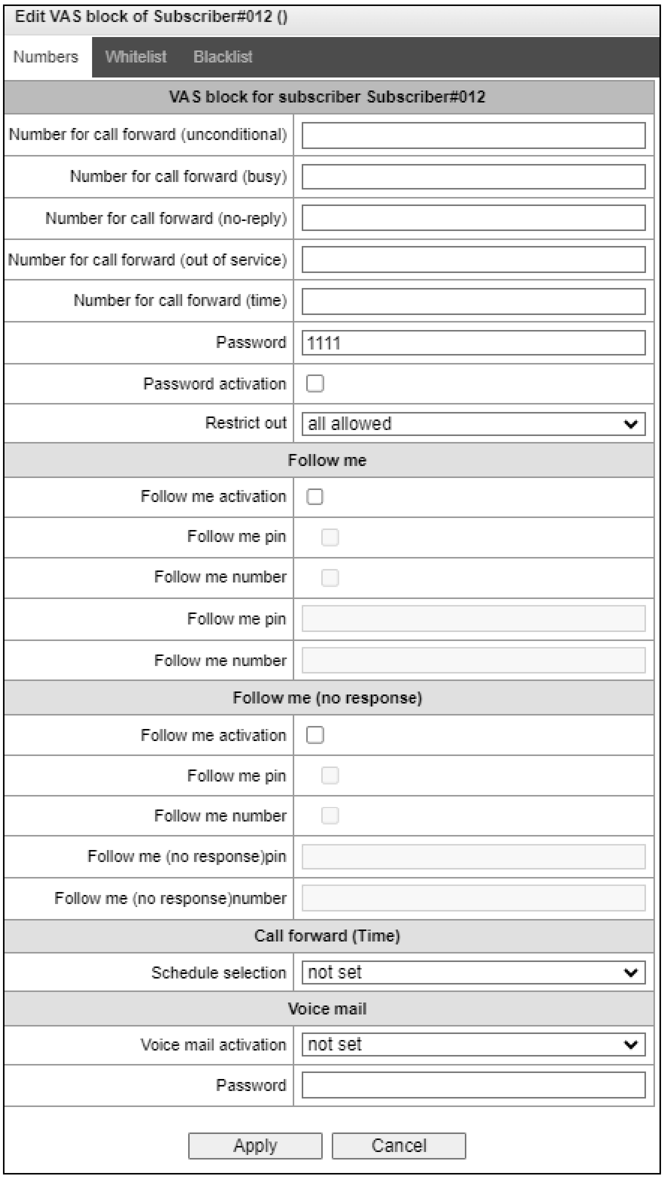
- *service activation* – activates the service and enter additional data;
- *service verification*;
- *cancel service* – disables the service.

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 *Enable VAS* checkbox is selected in the configuration menu (section 3.1.7.1.1 Subscriber Configuration).





- *Number for call forward (unconditional)* – phone number for the Call Forwarding Unconditional service;
- *Number for call forward (busy)* – phone number for the Call Forwarding Busy service;
- *Number for call forward (no-reply)* – phone number for the Call Forwarding No Reply service;
- *Number for call forward (out of service)* – phone number for the Call Forwarding Out of Service;
- *Number for call forward (time)* – phone number for the Call Forwarding by schedule;
- *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 out* – 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.

Follow me

- *Follow me activation* — enables the service;
- *Follow me pin* — activates the function of disabling the service by using a PIN code;
- *Follow me number* — activates the function of using number for redirection;
- *Follow me pin* — sets a PIN code which will be used to activate the service;
- *Follow me number* — a number for redirection.

Follow me (no response)

- *Follow me activation* — enables the service;
- *Follow me pin* — activates the function of disabling the service by using a PIN code;
- *Follow me number* — activates the function of using number for redirection;
- *Follow me (no response)pin* — sets a PIN code which will be used to activate the service;
- *Follow me (no response)number* — a number for redirection.

Call forward (Time) — selects a schedule for forwarding.

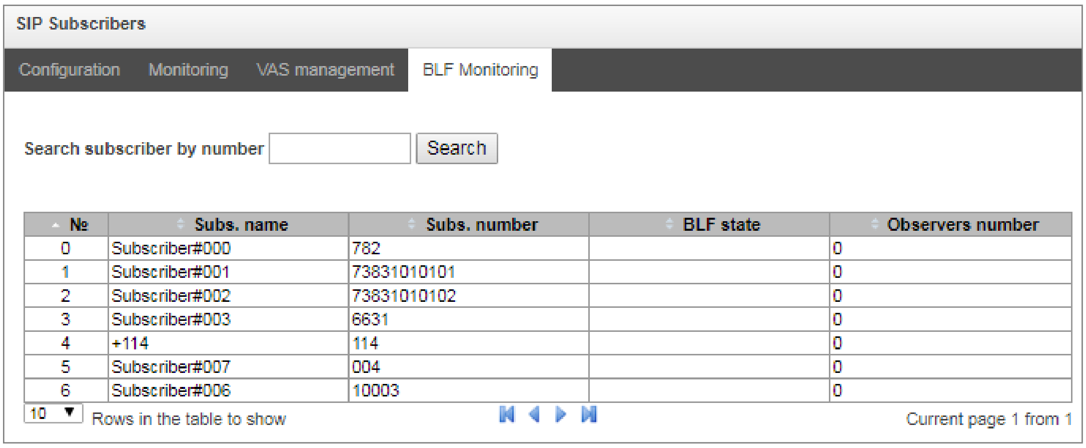
Voice mail – enabling voice mail service.

'*Whitelist'* 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.

'*Blacklist'* tab – you may activate the *black list* service and set black list of numbers which cannot call the subscriber.

For a detailed description of VAS, see APPENDIX H. WORKING WITH VAS SERVICES.

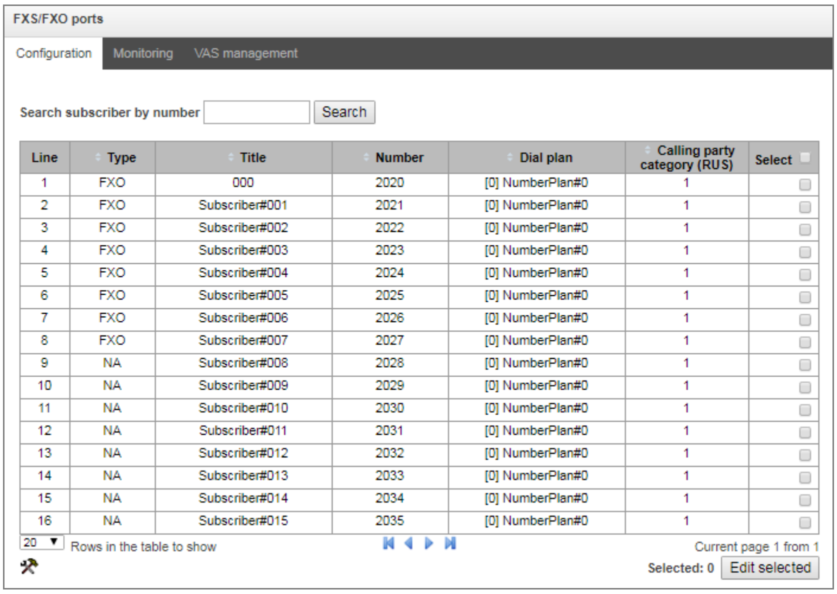
3.1.7.1.4 BLF Monitoring



№	Subs. name	Subs. number	BLF state	Observers number
0	Subscriber#000	782		0
1	Subscriber#001	73831010101		0
2	Subscriber#002	73831010102		0
3	Subscriber#003	6631		0
4	+114	114		0
5	Subscriber#007	004		0
6	Subscriber#006	10003		0

- *Subs. name* – displays the subscriber name;
- *Subs. number* – displays the subscriber number;
- *BLF state* – displays the BLF status;
- *Observers number* – the number of contacts who monitor the subscriber.

3.1.7.2 FXS/FXO Ports

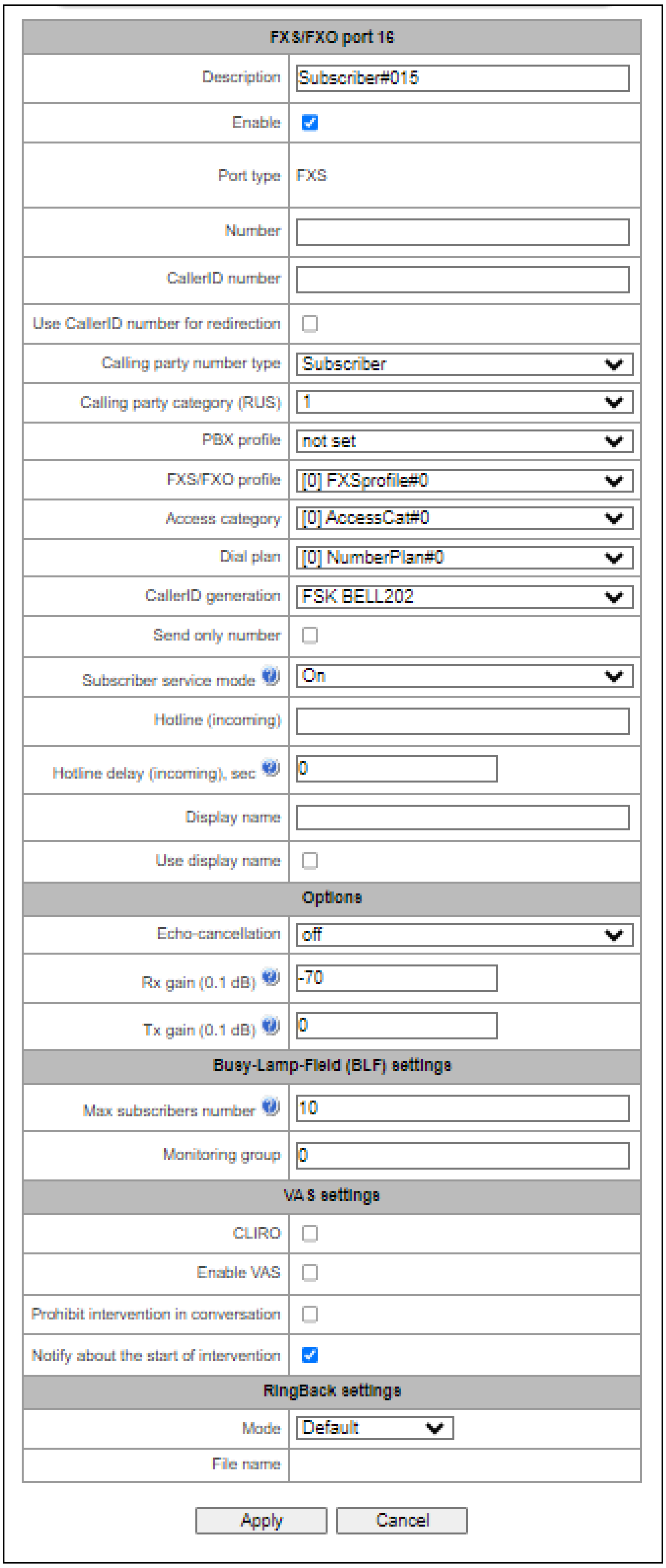


Line	Type	Title	Number	Dial plan	Calling party category (RUS)	Select
1	FXO	000	2020	[0] NumberPlan#0	1	
2	FXO	Subscriber#001	2021	[0] NumberPlan#0	1	
3	FXO	Subscriber#002	2022	[0] NumberPlan#0	1	
4	FXO	Subscriber#003	2023	[0] NumberPlan#0	1	
5	FXO	Subscriber#004	2024	[0] NumberPlan#0	1	
6	FXO	Subscriber#005	2025	[0] NumberPlan#0	1	
7	FXO	Subscriber#006	2026	[0] NumberPlan#0	1	
8	FXO	Subscriber#007	2027	[0] NumberPlan#0	1	
9	NA	Subscriber#008	2028	[0] NumberPlan#0	1	
10	NA	Subscriber#009	2029	[0] NumberPlan#0	1	
11	NA	Subscriber#010	2030	[0] NumberPlan#0	1	
12	NA	Subscriber#011	2031	[0] NumberPlan#0	1	
13	NA	Subscriber#012	2032	[0] NumberPlan#0	1	
14	NA	Subscriber#013	2033	[0] NumberPlan#0	1	
15	NA	Subscriber#014	2034	[0] NumberPlan#0	1	
16	NA	Subscriber#015	2035	[0] NumberPlan#0	1	

- *Search 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.

3.1.7.2.1 FXS port parameters



- *Description* – arbitrary text description of a subscriber;
- *Enable* – checkbox for enabling/disabling port operation;
- *Port type* – information field displaying port type (FXS, FXO or “unavailable” type if submodule is not installed or initialized);
- *Number* – the phone number of the FXS port for making a call to this port;

- *CallerID number* – the phone number of the FXS port for making a call from this port;
- *Use CallerID number for redirection* – uses the number specified in the *Caller ID Number* field when performing the call forwarding service;
- *Calling party number type* – type of the subscriber number;
- *Calling party category (RUS)* – subscriber's Caller ID category;
- *PBX profile* – selects the PBX profile (see section 3.1.7.5 PBX Profiles);
- *FXS/FXO profile* – selects the FSX/FXO profile for the subscriber;
- *Access category* – selects an access category;
- *Dial plan* – defines the dial plan for the subscriber;
- *CallerID generation* – selects the Caller ID display format. Available values: disabled, Caller ID, Caller ID (w/o waiting 500 Hz), DTMF, FSK BELL202, FSK V.23;
- *Send only number* – if this option is checked, only the caller number (without name) is displayed;
- *Subscriber service mode* – sets a limit on the incoming and outgoing communication for the subscriber:
    - *off:* out of service. The subscriber number is present in the dial plan, but the subscriber terminal cannot be registered. Therefore, incoming calls will be rejected with the *out of order* cause; outgoing calls cannot be initiated;
    - *on:* all types of communication are available;
    - *off 1:* incoming communication is enabled; outgoing communication is to special services only;
    - *off 2:* incoming communication is disabled; outgoing communication is to special services only;
    - *denied 1:* full prohibition for incoming and outgoing calls. Calls will be routed according to the dial plan, but be rejected;
    - *denied 2:* full prohibition for incoming and outgoing calls, except for special services;
    - *denied 3:* incoming calls are prohibited, outgoing calls are allowed;
    - *denied 4:* incoming calls are prohibited, outgoing calls are allowed only for local and private communication;
    - *denied 5:* incoming calls are allowed, outgoing calls are fully prohibited;
    - *denied 6:* incoming calls are allowed, outgoing calls are allowed only for special services;
    - *denied 7:* incoming calls are allowed, outgoing calls are allowed only for local and private communication;
    - *denied 8:* incoming calls are allowed, outgoing calls are allowed only for local and private and zone communication;
    - *ignore:* excluded from the dial plan. The number is completely excluded from the subscriber number list of the dial plan. 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 dial plan.
- *Hotline (incoming)* – a number used to call in hotline mode;
- *Hotline delay (incoming), sec* – pause in seconds before the automatic dialing of the number that is specified in the *Hotline (incoming call)* field;
- *Display name* — a name which will be transmitted in *display-name.* Also, the parameter will influence on using *display-name* as *Connected Name* in responses on calls directed to the subscriber;
- *Use display name* – enable using Display.

Options

- *Echo-cancellation* — echo-cancellation mode:
  - *voice(default)* – echo cancellators are enabled in voice transmission mode;
  - *voice nlp-off* – echo cancellators are enabled in voice transmission mode, non-linear processor (NLP) is disabled. When the signal levels on transmission and receiving are very different, a weak signal might be suppressed by NLP. Use this mode to prevent such situations;
  - *off* – do not use echo-cancellation (the mode is set by default);
  - *speex algorithm*.
- *Echo cancellation direction:*
  - *Incoming* – the echo from the caller is suppressed;
  - *Outgoing* – the echo towards the subscriber is suppressed.
- *Rx gain (0.1 dB)* – volume of the received signal (amplification/attenuation of the signal level);
- *Tx gain (0.1 dB)* – volume of signal transmitted, gain/loss of the signal transmitted to the communicating device direction.

AGC (Auto Gain Control)

The settings block becomes available when the *speex algorithm echo cancellation* mode is enabled.

- *Enable/Disable AGC for Speex* – enabling/disabling AGC;
- *Target volume level* – frequency that AGC will try to hold;
- *Max gain increment, dB/sec* – maximum allowable value of gain increase rate of the original signal;
- *Max gain decrement, dB/sec* – maximum allowed value of gain reduction rate of the initial signal;
- *Max gain* – maximum allowable value of amplification of the original signal.

Busy-Lamp-Field (BLF) settings

- *Max subscribers number* – the maximum number of subscribers capable to monitor the line state;
- *Monitoring group* – BLF monitoring group, BLF monitoring is available for subscribers who are in the same monitoring group.

VAS settings

- *CLIRO* – a service for overriding the prohibition on caller number identification;
- *Enable VAS* – enables VAS services. When this option is checked, the *VAS Activation* table becomes available;
- *Prohibit intervention in conversation* – prohibits the subscriber to interfer in the conversation;
- *Notify about the start of intervention* – when interfering in a conversation, a sound signal will be played to the subscriber, by default the option is enabled.

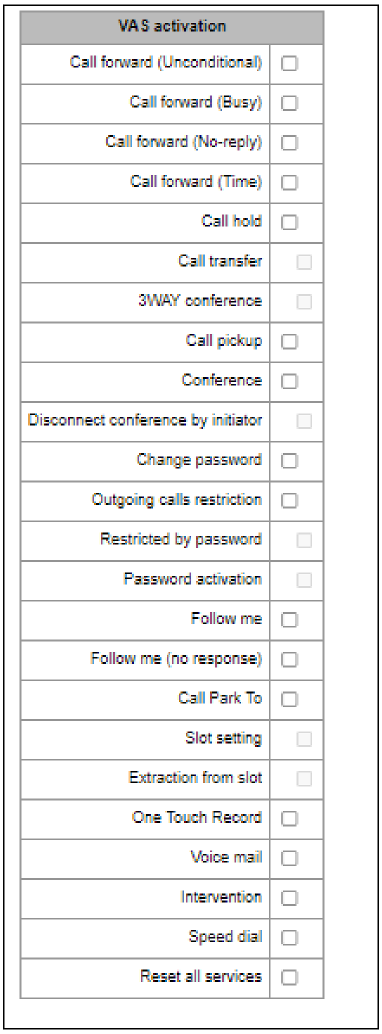
RingBack settings

RingBack settings allows to set up a ring back tone for each subscriber individually.

Mode:

- *Default* – the option corresponds to the default system settings;
- *RingBack* – playing the standard ringback tone, ignoring the default system settings;
- *Audo file* – changing the standard ringback tone to a chosen one which has been downloaded in *System settings* menu option (an individual sound for a subscriber).

VAS Activation

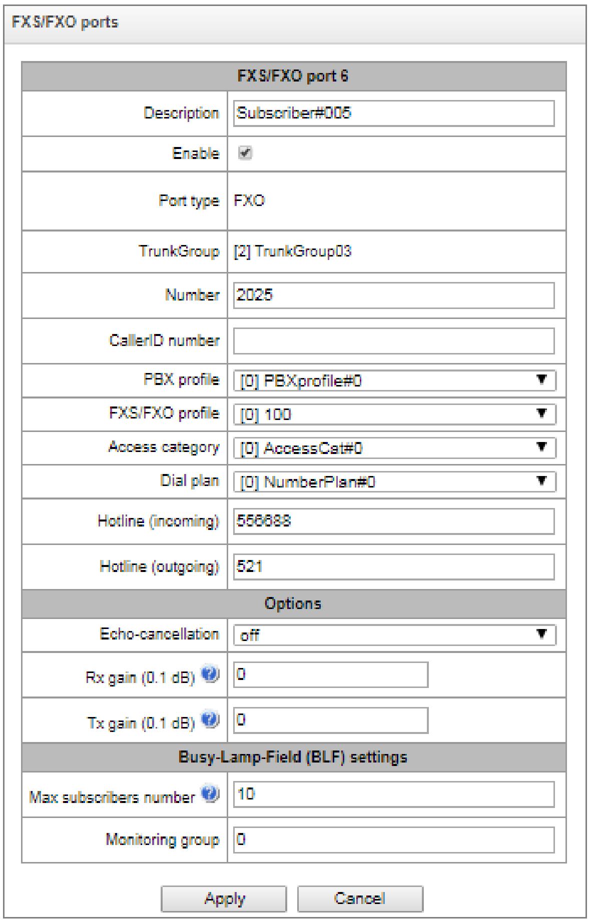


- *Call forward (Unconditional)* – enables the Call Forwarding Unconditional (CF Unconditional) service;
- *Call forward (Busy)* – enables the Call Forwarding Busy (CF Busy) service;
- *Call forward (No-reply)* – enables the Call Forwarding No Reply (CF No Reply) service;
- *Call forward (Time)* – enables service for Call Forwarding by Schedule;
- *Call hold* – enables the Call Hold service;
- *Call transfer* – enables the Call Transfer service;

- *3WAY conference* – enables the 3WAY conference service;
- *Call pickup* – enables the Call Pickup service;
- *Conference* – activates 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 quiting and will be over only when all the participants leave the conference;
- *Change password* – changes the password to restrict the outgoing communication;
- *Outgoing calls restriction* – uses the Restrict outgoing communication by password service;
- *Restricted 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* – activates the follow me service.
- *Follow me (no response)* – activates the follow me service.
- *Call Park To* – enables Call Park service;
- *Slot setting* – allows to put a subscriber to a slot within Call Park service;
- *Extraction from slot* – allows to retrieve a subscriber from a slot within Call Park service;
- *One touch record* – enables the Call recording service on demand;
- *Voice mail* – enables the Voice mail service;
- *Intervention* – enables the Call intervention service;
- *Speed dial* – enables the Speed dial service;
- *Reset all services* – cancels all numbers configured for forwarding by clicking a service prefix set in the dial plan.

For a detailed description of VAS, see APPENDIX H. WORKING WITH VAS SERVICES.

3.1.7.2.2 FXO port settings



- *Description* – arbitrary text 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 initialized);
- *Trunkroup* – shows a trunk group which includes this FXO port;
- *Number* – FXS port number used for calling to this port;
- *CallerID number* – phone number of FXS port that will be used for calling from this port;
- *PBX profile* – selects PBX profile (see section 3.1.7.5 PBX Profiles);
- *FXS/FXO profile* – selects FXS/FXO profile for subscriber;
- *Access category* – selects access category;
- *Dial plan* — defines the dial plan that the subscriber will belong to;
- *Hotline (incoming)* — the hotline number used for incoming calls to the port;
- *Hotline delay (incoming), sec* – pause in seconds before the automatic dialing of the number that is specified in the *Hotline (incoming call)* field;
- *Hotline (outgoing)* — the hotline number used for outgoing calls from the port.

Options

- *Echo-cancellation* — echo-cancellation mode:
  - *voice(default)* – echo cancellators are enabled in voice transmission mode;
  - *voice nlp-off* – echo cancellators are enabled in voice transmission mode, non-linear processor (NLP) is disabled. When the signal levels on transmission and receiving are very different, a weak signal might be suppressed by NLP. Use this mode to prevent such situations;
  - *off* – do not use echo-cancellation (the mode is set by default);
  - *speex algorithm*.
- *Echo cancellation direction:*
  - *Incoming* – the echo from the caller is suppressed;
  - *Outgoing* – the echo towards the subscriber is suppressed.
- *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.

AGC (Auto Gain Control)

The settings block becomes available when the *speex algorithm echo cancellation* mode is enabled.

- *Enable/Disable AGC for Speex* – enabling/disabling AGC;
- *Target volume level* – frequency that AGC will try to hold;
- *Max gain increment, dB/sec* – maximum allowable value of gain increase rate of the original signal;
- *Max gain decrement, dB/sec* – maximum allowed value of gain reduction rate of the initial signal;
- *Max gain* – maximum allowable value of amplification of the original signal.

Busy-Lamp-Field (BLF) settings

- *Max subscribers number* – the maximum number of subscribers capable to monitor the line state;
- *Monitoring group* – BLF monitoring group, BLF monitoring is available for subscribers who are in the same monitoring group.

3.1.7.2.3 VAS Management

In this section, VAS settings for subscribers can be configured.

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 *Enable VAS* checkbox and other checkboxes for required VAS functions in the section 3.1.7.1.1 Subscriber Configuration.

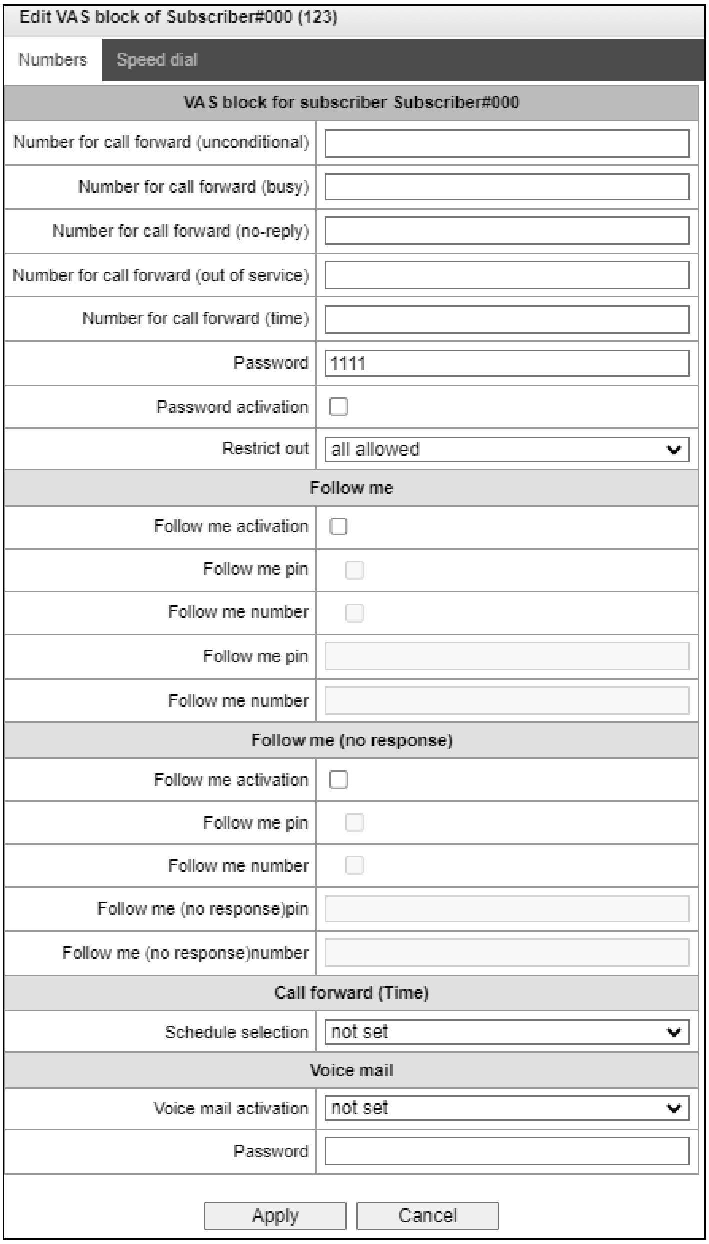
Subscribers can manage the status of VAS services from their telephone set. The following options are available:

- *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 *Enable VAS* checkbox is selected in the configuration menu (section 3.1.7.1.1 Subscriber Configuration).



- *Number for call forward (unconditional)* – phone number for the Call Forwarding Unconditional service;
- *Number for call forward (busy)* – phone number for the Call Forwarding Busy service;
- *Number for call forward (no-reply)* – phone number for the Call Forwarding No Reply service;
- *Number for call forward (out of service)* – phone number for Call Forwarding Out of Service;
- *Number for call forward (time)* – phone number for the Call Forwarding by schedule;
- *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 out* – 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.

Follow me

- *Follow me activation* — enables the service;
- *Follow me pin* — activates the function of disabling the service by using a PIN code;
- *Follow me number* — activates the function of using number for redirection;
- *Follow me pin* — sets a PIN code which will be used to activate the service;
- *Follow me number* — a number for redirection.

Follow me (no response)

- *Follow me activation* — enables the service;
- *Follow me pin* — activates the function of disabling the service by using a PIN code;
- *Follow me number* — activates the function of using number for redirection;
- *Follow me (no response)pin* — sets a PIN code which will be used to activate the service;
- Follow me (no response)number — a number for redirection.

Call forward (Time) — select a schedule for forwarding.

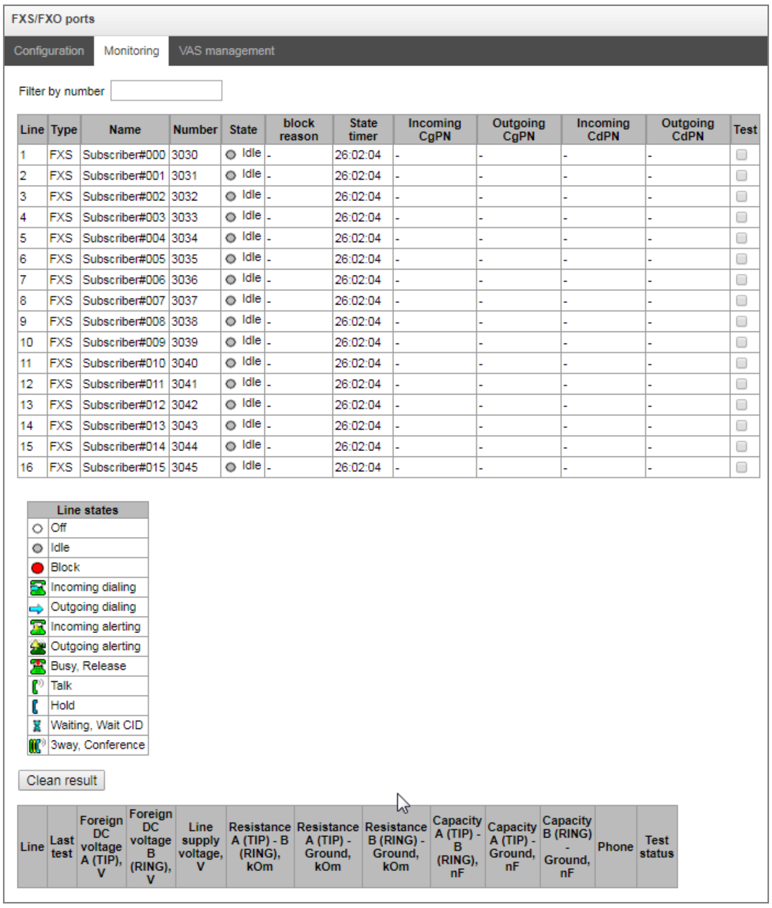
'Whitelist' tab – you may activate the 'do not disturb' service and define white number list containing the numbers which can call the subscriber even in 'do not disturb' mode.

'Blacklist' tab – you may activate the 'black list' service and set black list of numbers which cannot call the subscriber.

For a detailed description of VAS, see APPENDIX H. WORKING WITH VAS SERVICES.

3.1.7.2.4 Monitoring

Upon selecting the *'Monitoring'* tab, a subscriber status table will be shown.



- *Line* – port sequence number;
- *Type* – FXO or FXS port type;
- *Name* – arbitrary subscriber text description;
- *Number* – subscriber's number;
- *State* – the current status of the port. The available states are in the legend located under the ports table:
  - *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.

<u>*Testing ports*</u>

By selecting the necessary ports for testing opposite each port and clicking the '*Test'* button, one can test the parameters of the subscriber line corresponding to this port. At the end of the test, it is possible to view the test results by clicking on the '*Show test results*' button:

Line	Last test	Foreign DC voltage A (TIP), V	Foreign DC voltage B (RING), V	Line supply voltage, V	Resistance A (TIP) - B (RING), kOm	Resistance A (TIP) - Ground, kOm	Resistance B (RING) - Ground, kOm	Capacity A (TIP) - B (RING), nF	Capacity A (TIP) - Ground, nF	Capacity B (RING) - Ground, nF	Phone	Test status

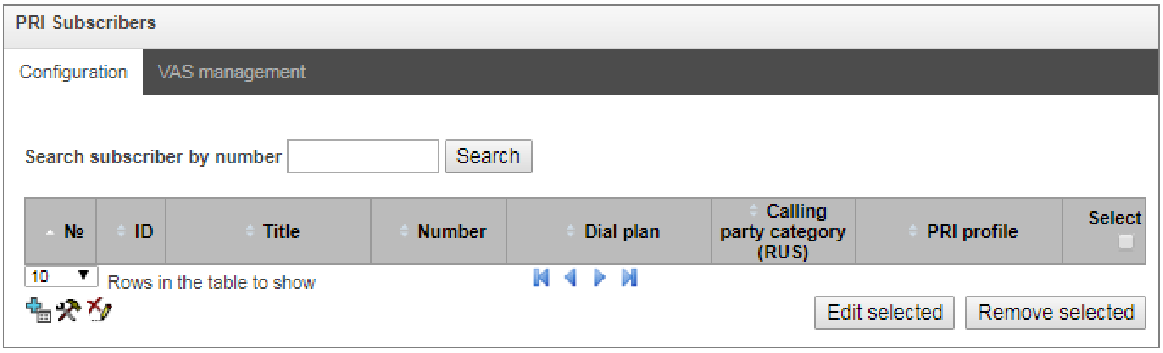
- Foreign DC voltage B (RING), V
- Foreign DC voltage A (TIP), V
- Line supply voltage, V
- Resistance A (TIP) – B (RING), kOm
- Resistance A (TIP) – GND, kOm
- Resistance B (RING) – GND, kOm
- Capacity A (TIP) – B (RING), mkF
- Capacity A (TIP) – GND, mkF
- Capacity B (RING) – GND, mkF
- Phone – displays TA connection to FXS port:
    - Not connected;
    - Connected.
- Test status.

3.1.7.3 *PRI subscribers*

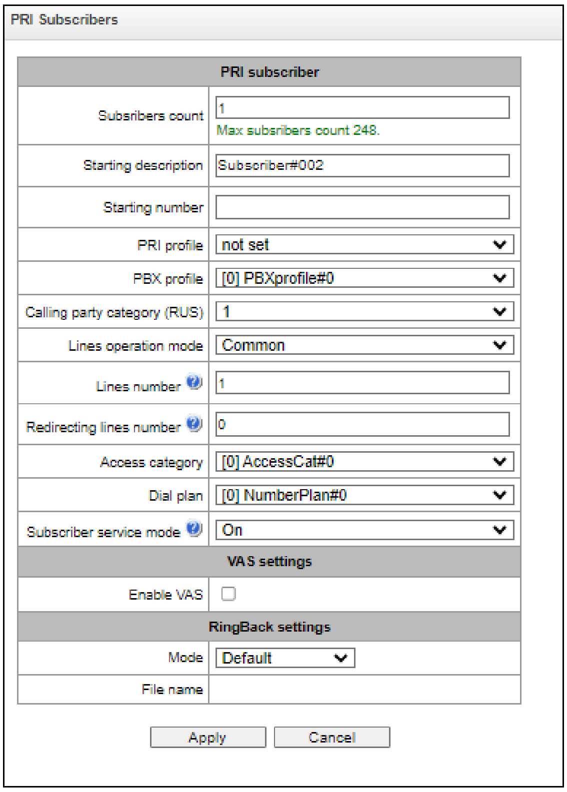
PRI subscribers are numbers located behind PRI trunk (E1 stream with Q.931 signalling). PRI subscribers are identified by SMG as local subscribers with several subscriber services. Routing for such subscribers are performed without creating additional rules in the dial plan.

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.

Search subscriber – checking the presence of a subscriber in the database of configured PRI subscribers; the check can be performed by name, number, PRI profile, PBX profile, dial plans.



3.1.7.3.1 PRI Subscribers Configuration



- *Subscribers count* – number of the subscribers;
- *Starting description* – arbitrary subscriber text description;
- *Starting number* – subscriber number for a group of subscribers. The next subscriber will have the number increased by one.
- *PRI profile* – selects PRI profile;
- *PBX profile* – selects PBX profile (see section 3.1.7.5 PBX Profiles);
- *Calling party category (RUS)* – CallerID category;
- *Lines operation mode* – setting limits on the number of simultaneous calls. Can take two values: Common and Separate. The common mode takes into account the total number of simultaneous calls in which the subscriber can take part; in the separate mode, incoming and outgoing calls are counted separately;
- *Lines number* – the number of simultaneous calls in which the subscriber can take part. The field appears if the line mode is set to *Common*. The range of possible values is [1;255] or 0 – no limits; If *Separate* mode has been selected, the quantity of calls is selected separately for incoming and outgoing directions;
- *Ingress lines number*[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;
- *Egress lines number*[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;
- *Redirecting lines number* – number of simultaneous calls for redirection. Valid range [1;255] or 0 — no limits;

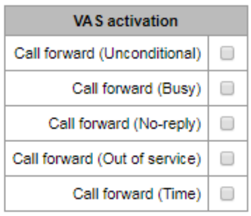
[1] These settings are displayed if the separate line mode is selected.

- *Access category* – select access category;
- *Dial plan* – define a dial plan for the subscriber;
- *Subscriber service mode*— defines restrictions on incoming and outgoing communication for the subscriber:
  - *Off* – out off 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 dial plan 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 prohibited, 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 management

- *Enable VAS* – VAS connection for a subscriber. When this item is selected, 'VAS activation' table will become available.

VAS activation



- *Call forward (Unconditional)* — activate call forward unconditional (CF Unconditional) service;
- *Call forward (Busy)*— activate call forward on busy (CF Busy) service;
- *Call forward (No-reply)* — activate call forward on no reply (CF No reply) service;
- *Call forward (Out-of service)* — activate call forwarding on out of service (CF Out of Service);
- *Call forward (Time)* – activate call forwarding by schedule (CF (Time)).

For a detailed description of VAS, see APPENDIX H. WORKING WITH VAS SERVICES.

RingBack settings

RingBack settings allows to configure a ring back tone for each subscriber individually.

Mode:

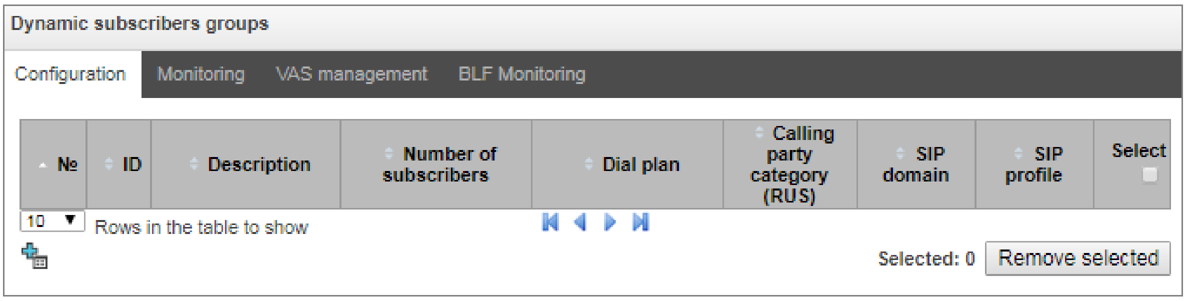
- *Default* — the option corresponds to the default system settings;
- *RingBack* — playing the standard ringback tone, ignoring the default system settings;
- *Audio file* — changing the standard ringback tone to a chosen one which has been downloaded in *System settings* menu option (an individual sound for a subscriber).

3.1.7.4 Dynamic Subscriber Groups

3.1.7.4.1 Configuration of Dynamic Subscriber Groups

In this section, the dynamic subscriber groups can be configured.

Dynamic *registration* uses digest authentication of subscribers on the RADIUS server (rfc 5090, rfc5090-no-challenge, draft-sterman).

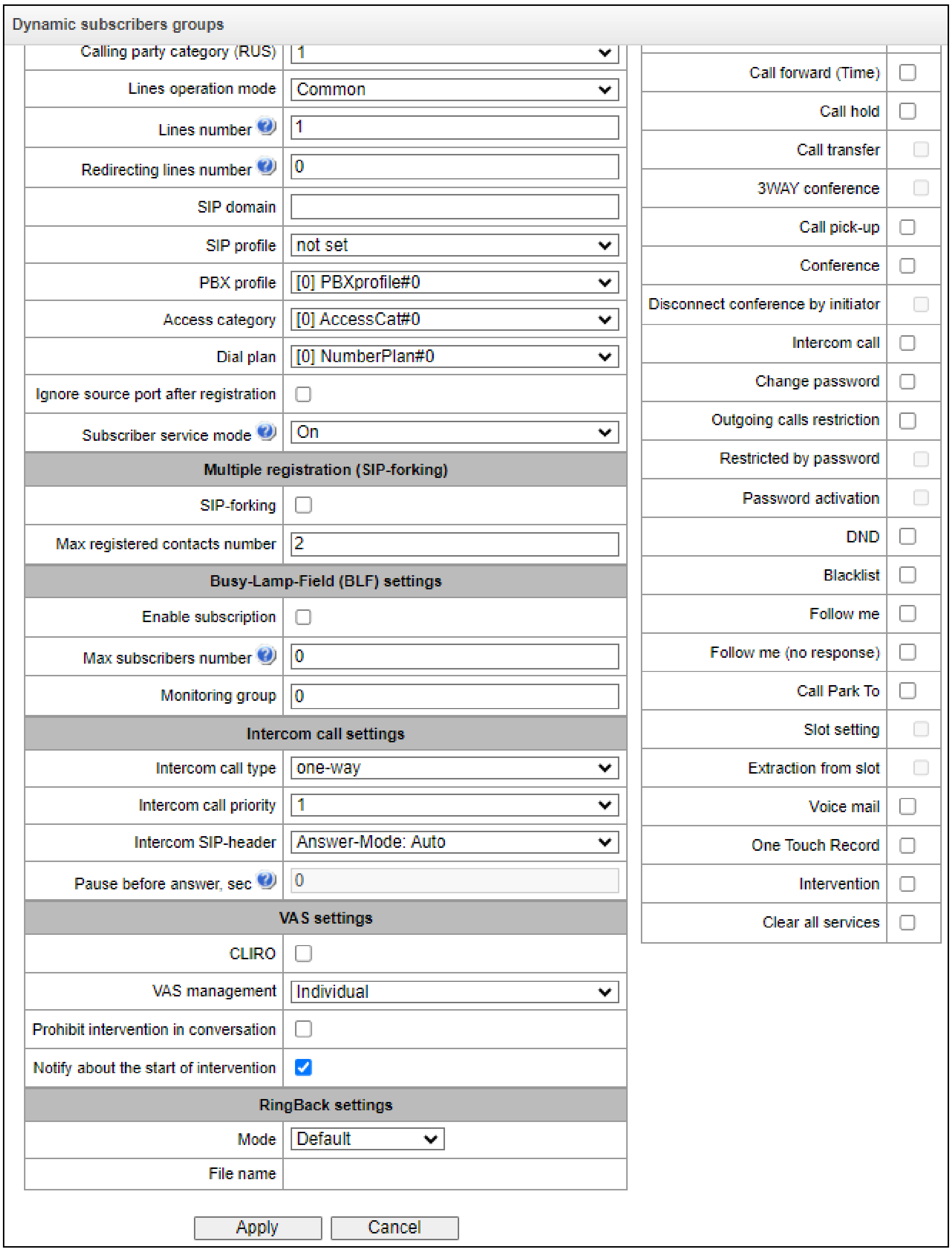


To create, edit, or remove an entry, use the *Objects – Add Object, Objects – Edit Object* or *Objects – Remove Object* menus and the following buttons:

– Add subscribers;

– Edit subscriber parameters;

– Remove subscriber.



Dynamic Subscribers Group

- *Subscribers number* – the number of subscribers in the group;
- *Description* – name of the dynamic subscriber group;
- *Calling party number type* – type of the subscriber number;
- *Calling party category (RUS)* – subscriber's Caller ID category;
- *Lines operation mode* – setting limits on the number of simultaneous calls. Can take two values: Common and Separate. The Common mode takes into account the total number of simultaneous calls in which the subscriber can take part; in the Separate mode, incoming and outgoing calls are counted separately;
- *Lines number* – the number of simultaneous calls in which the subscriber can take part. The field appears if the line mode is set to *Common*. The range of possible values is [1;255] or 0 – no limits;

- *Ingress lines number* [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;
- *Egress lines number*[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;
- *Redirecting lines number* – number of simultaneous calls for redirection. Valid range [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 3.1.4.4);
- *SIP profile* – select the SIP profile. The SIP profile defines the most of the subscriber settings. Selecting "Any" profile makes it possible to register a sip subscriber on any of the available sip profiles in the system (see section 3.1.5.2 for SIP/ SIP-T/ SIP-I interfaces, SIP profiles);
- *PBX profile* – select the PBX profile (see section 3.1.7.5);
- *Access category* – select an access category;
- *Dial plan* – define the dial plan for the subscriber;
- *Ignore 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:
  - *off* – the port is out of service. The subscriber number is present in the dial plan, but the subscriber terminal cannot be registered. Therefore, incoming calls will be rejected with the *out of order* cause; outgoing calls cannot be initiated;
  - *on* – all types of communication are available;
  - *off 1* – incoming communication is enabled; outgoing communication is to special services only;
  - *off 2* – incoming communication is disabled; outgoing communication is to special services only;
  - *denied 1* – full prohibition for incoming and outgoing calls. Calls will be routed according to the dial plan, but be rejected;
  - *denied 2* – full prohibition for incoming and outgoing calls, except for special services;
  - *denied 3* – incoming calls are prohibited, outgoing calls are allowed;
  - *denied 4* – incoming calls are prohibited, outgoing calls are allowed only for local and private communication;
  - *denied 5* – incoming calls are allowed, outgoing calls are fully prohibited;
  - *denied 6* – incoming calls are allowed, outgoing calls are allowed only for special services;
  - *denied 6* – incoming calls are prohibited, outgoing calls are allowed only for local and private communication;
  - *denied 8* – incoming calls are allowed, outgoing calls are allowed only for local and private and zone communication;
  - *ignore* – the number is excluded from the dial plan. The number is completely excluded from the subscriber number list of the dial plan. 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 dial plan.

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 dial plan.

[1] These settings are displayed if the separate line mode is selected.

Multiple registration (SIP forking);

Multiple registration of up to five clients on one account is allowed. The registration is possible on the same or on different network interfaces. A call goes to all registered contacts simultaneously. Work with priorities (q-parameter) will be implemented in future versions.

- *SIP-forking* – enables multiple registration on a subscriber;
- *Max registered contacts number* – allowed acceptable range of registration per subscriber (The range of allowed values is [2; 5]).

Busy-Lamp-Field (BLF) settings

- *Enable subscription* – the BLF (*Busy Lamp Field*) function allows monitoring the current status of other subscriber lines in real time;
- *Max subscribers number* – 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 call settings

- *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;
    - *Ordinary call* – an incoming intercom call is made as a normal call, without an automatic answer of subscriber B;
    - *Ignore* – an incoming intercom call will be rejected;
- *Intercom call priority* – the priority of an incoming intercom call over other calls;
- *Intercom SIP-header* – 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 answer, sec* – the pause duration before answering an intercom/paging call, which can be transmitted in the ‘answer-after’ header.

VAS settings

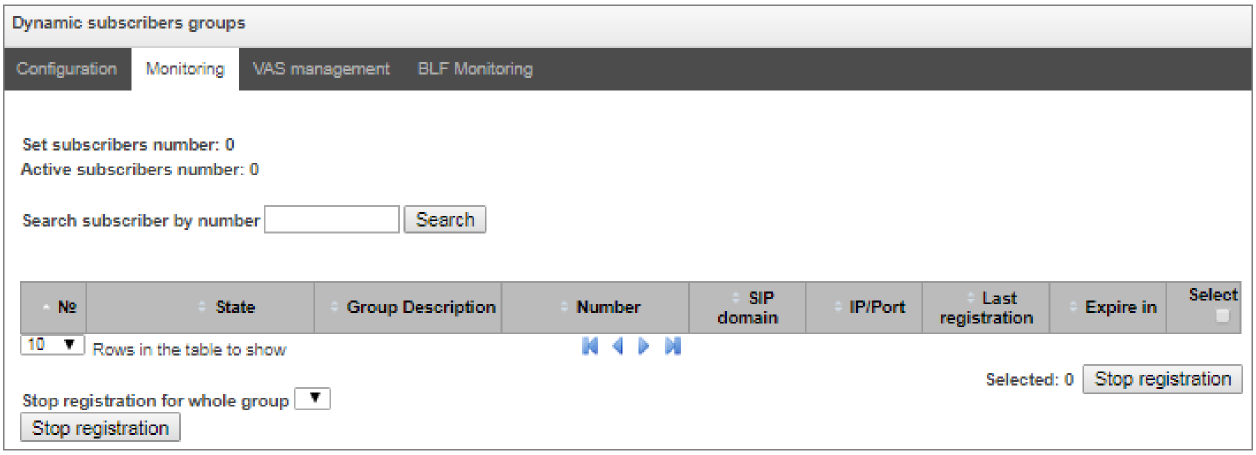
- *CLIRO* – a service for overriding the prohibition on caller number identification;
- *VAS management* – selects how VAS services will be activated for dynamic subscribers.
    - *Do not activate* – do not enable VAS services for dynamic subscribers;
    - *Individual selection* – VAS services can be configured for each subscriber individually via the gateway configurator. If this option is selected, the *VAS Activation* table will become available (see section 3.1.7.1.1);
    - *From RADIUS* – for dynamic subscribers, VAS settings will be sent in the RADIUS server responses. For details, see APPENDIX D. TRANSMISSION OF VAS SETTINGS FROM RADIUS SERVER FOR DYNAMIC SUBSCRIBERS.
- *Prohibit intervention in conversatioin* – prohibiting the subscriber from interfering with the conversation;
- *Notify about the start of intervention* – if the call is interfered with, the subscriber will hear a sound signal; this option is active by default.

RingBack settings

RingBack settings allow to configure a ring back tone for each subscriber individually.

- Mode:
    - *Default* — the option corresponds to the default settings;
    - *RingBack* — play the standard ringback tone, ignore the default settings;
    - *Audio file* — change the standard ringback tone to a chosen one which has been downloaded in 'System settings' (an individual sound for the direction).

3.1.7.4.2 Monitoring of Dynamic Subscriber Groups

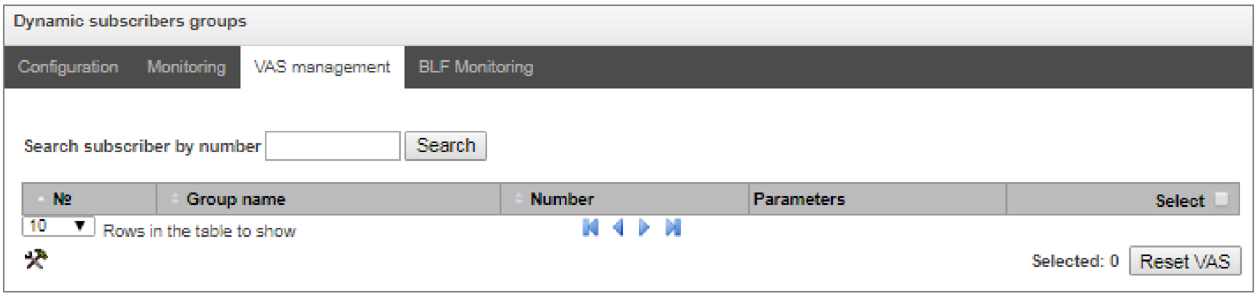


Click the *Search* button to search entries for the subscriber with the specified number.

- *State* – subscriber registration status (registered, not registered, registration expired);
- *Group Description* – 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;
- *Expire in* – 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;
- *Stop registration* – forcibly reset the registration for a selected subscriber.

Click the *Stop registration* button to reset the registration of all subscribers in the specified group. You can select a group from the drop-down list.

3.1.7.4.3 VAS management of Dynamic Subscriber Groups

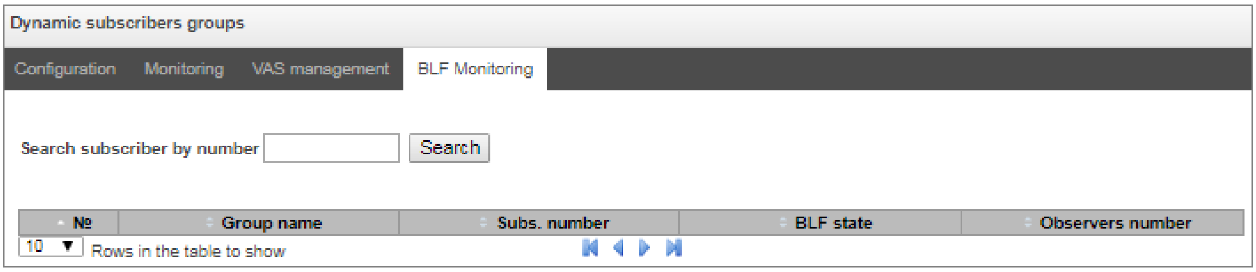


Click the *Search* button to search entries for the subscriber with the specified number.

- *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.

3.1.7.4.4 BLF monitoring of Dynamic Subscriber Groups



Click the *Search* button to search entries for the subscriber with the specified number.

- *Group name* – arbitrary text description of the group;
- *Subs. number* – the subscriber number;
- *BLF state* – the current status of the *busy lamp field* service;
- *Observers number* – the current number of subscribers who monitor the subscriber's line status.

3.1.7.5 PBX Profiles

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

PBX profiles

№	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
Adding participants to the conference	Auto
Ingress calls	
Use voice messages	☐
No Connected number transit	☐
Copy CgPN into Redirecting number	☐
Use Redirecting number for routing	☐
CdPN modifiers	not used
CgPN modifiers	not used
List of reasons for call recovery after outbound leg failure	not set
Egress calls	
CdPN modifiers	not used
CgPN modifiers	not used
RingBack settings	
Mode	Default
File name	
Timeouts	
First digit timeout, sec	15
Next digit timeout, sec	5
Busy-tone timeout, sec	60
Timeout for call answer, sec (for FXS/FXO-abonents)	90
Timeout for call hold, sec (for FXS/FXO-abonents)	60
VAS timeouts	
CFNR timeout, sec	10
Timeout for call park, sec	300
Restriction on directions	
Add	not set

Apply Cancel

PBX Profile

- *Description* – the profile name;
- *Station prefix* – prefix to be added to the beginning of SIP/FXS subscriber number (CgPN);
- *Direct routing 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 dialled 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;
- *Adding participants to the conference.*

Ingress calls

- *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 G. VOICE MESSAGES AND MUSIC ON HOLD (MOH);
- *No Connected number transit* – disable the transmission of the Connected number field;
- *Copy CgPN into Redirecting number* – 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 number for routing* – when this options 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 dial plan 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;
- *List of reasons for call recovery after outbound leg failure* – selecting the Q.850 Recovery Reasons List table to configure Q.850 release reasons for call recovery in case of outgoing leg failure. If a call received through a pbx-profile with an activated setting is rejected from the side of the incoming side, and the reason for the release is in the selected table, then the SMG will, without interrupting the conversation on A leg, try to restore communication using a repeated call or alternative routes when the main one is unavailable.

Egress calls

- *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.

RingBack settings

- Mode:
  - *Default* — the option corresponds to the default settings;
  - *RingBack* — play the standard ringback tone, ignore the default settings;
  - *Audio file* — change the standard ringback tone to a chosen one which has been downloaded in 'System settings' (an individual sound for the direction).

- *File name* — select necessary audio file to be played as a ring back tone.

Timeouts

- *First digit 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 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-tone 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;

- *Timeout for call answer, sec (for FXS/FXO-abonents)* – timeout for the subscriber response to the incoming call; when the time expires, the caller is disconnected;

- *Timeout for call hold, sec (for FXS/FXO-abonents)* – timeout for putting the subscriber on hold.

VAS timeouts

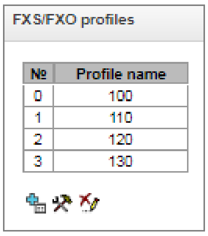
- *CFNR timeout, sec* – when this timeout expires, the incoming call will be forwarded by the "Call Forwarding No Reply" VAS service. Possible values are 5–60 seconds;

- *Timeout for call park, sec* – a timeout for staying in a call parking slot. When this timeout expires, the call back will be performed to a subscriber initiated the call parking. Possible values are 300 – 3,600 seconds.

3.1.7.6 FXS-/FXO profiles

3.1.7.6.1 FXS profiles

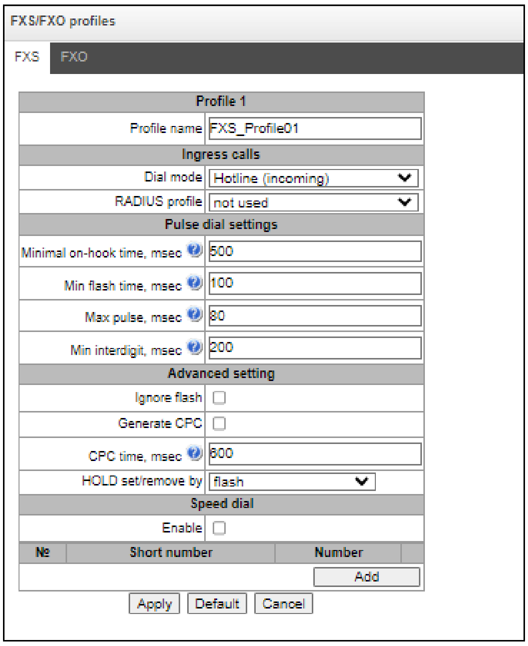
FXS profiles are used to assign additional parameters to FXS subscribers.



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.

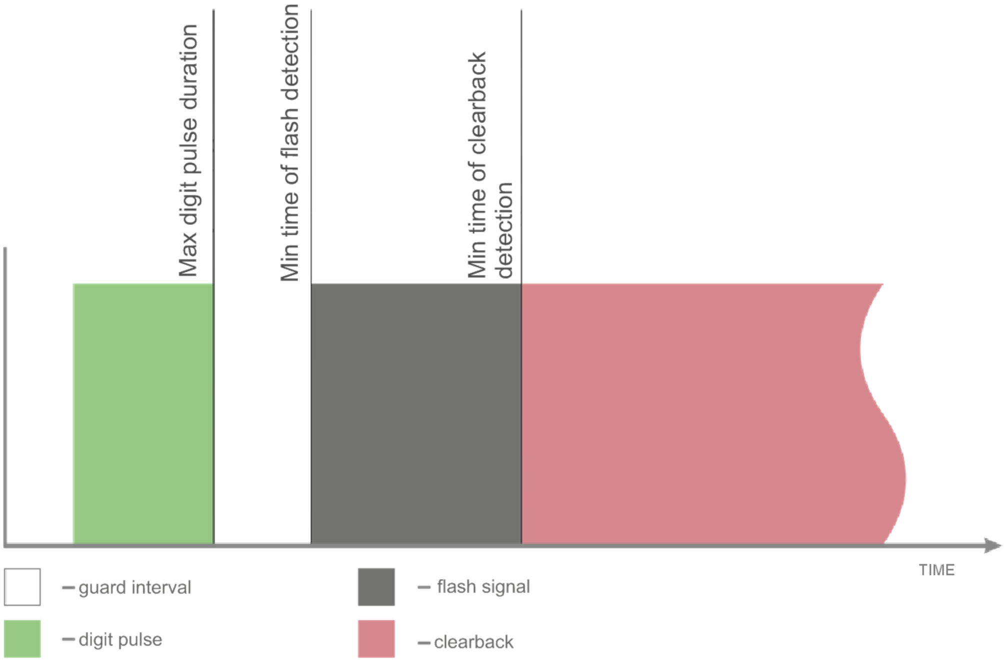
FXS Profile



- *Profile name* – name of the FXS profile;
- *Dial mode:*
  - *Collect* – a standard FXS port operation mode;
  - *Hotline (incoming)* – port operation in hotline mode (automatic dialing).
- *RADIUS Profile* – the RADIUS profile that will be used when authenticating an incoming call;
- *Minimal on-hook time, msec* – the loop disconnection time, after which the clearback signal will be detected;

- *Min flash time, msec* – the loop disconnection time, after which the flash signal can be detected, provided that the loop disconnection time does not exceed the *Minimal on-hook time*;
- *Max pulse, msec* – the loop disconnection time, after which the decade dialing pulse can be detected, provided that the loop disconnection time is 10 ms shorter than the *Min flash time*;
- *Min interdigit, msec* – the minimum time interval between digits for pulse dialing;
- *Ignore flash* – when this option is active, flash signal detection is disabled.

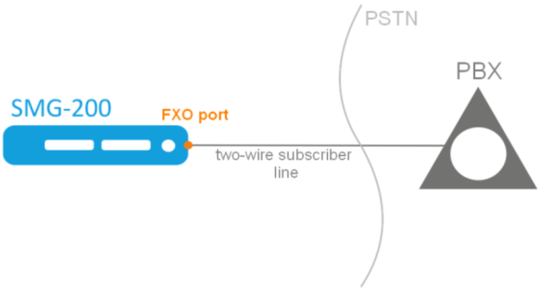
The dialling pulse, flash signal and clearback signal are the signals generated by the loop disconnection with different time intervals. The time intervals of these signals are presented in a graph below.



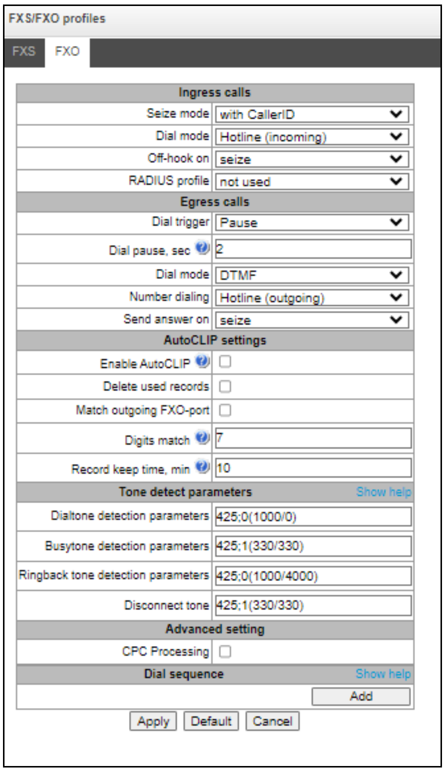
- *Generate CPC* – when checked, carry out short-time break of a subscriber loop when clearback from the side of communicating device;
- *CPC time, msec* – duration of the short-time subscriber loop break;
- *HOLD set/remove by:*
  - Flash/* – put a call on HOLD by pressing Flash or “*” on a phone;
  - Flash/# – put a call on HOLD by pressing Flash or “#” on a phone;
  - Flash/*/# – put a call on HOLD by pressing Flash or “*” or “#” on a phone.

3.1.7.6.2 FXO Profiles

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 'Ingress Calls' section. Calls that are to be transmitted to PSTN, are configured in the 'Egress Calls' section.



FXO Profile:



Ingress calls

- *Seize mode* – the parameter indicating when processing begins for a call received to the FXO port from the PSTN.
  - *with CallerID* – 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 first Ring* – when this option is checked, the engagement will be determined after the end of the first ringing;
- *at first Ring* – when this option is checked, the engagement will be determined when the first ringing begins.

- *Dial mode* – select the method for further processing of the call after the engagement.

  - *Hotline (incoming)* – the number specified in the 'hotline' setting on the FXO port will be used for further routing;
  - *Collect* – 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.

- *Off-hook on* – 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 dialing' mode the response (loop closure) will be sent immediately after the engagement:

  - *seize* – the response (loop closure) will be sent immediately after the engagement is detected;
  - *remote side ringing* – the response (loop closure) will be sent after the call is routed to the number specified in the 'hotline' setting on the FXO port;
  - *remote side answer* – 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.

Egress calls

- *Dial trigger* – 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;
  - *Dial-tone detect* – 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.

- *Dial pause, sec* – the field is active only when 'Start work after pause' option is selected;

- *Dial mode* – select the dialling method:

  - *DTMF* – dialling will be done in the tone mode (DTMF);
  - *Pulse* – the number will be dialed in the pulse mode;

    - *Pulse interdigit, msec* – the time interval between digits for the pulse mode;
    - *Pulse width, msec* – duration of a digit pulse for the pulse mode;
    - *Pause length, msec* – duration of a digit pulse pause for the pulse mode.

- *Number dialing* – select the callee number generation mode, for further dialling to PSTN:

  - *Hotline (outgoing)* – the number specified in the "PSTN Hotline" setting in the FXO port parameters will be dialed;
  - *Extra dialing* – when this option is checked, the number received from the caller will be dialed to PSTN using the extension dialing 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.

- *Stripped number* – when this option is checked, the number that follows the port number specified in the FXO port configuration will be dialed 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 dialed to PSTN.

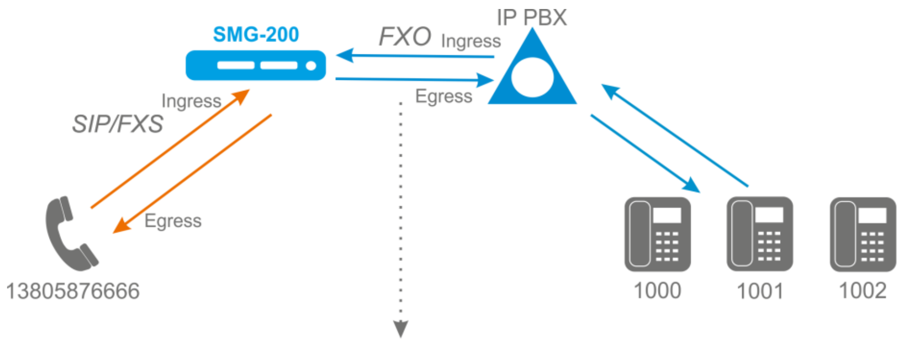
- *Send answer on:*
  - *seize* – the response (loop closure) will be sent immediately after the engagement is detected;
  - *dial tone* — the response will be sent after remote station response (dial tone);
  - *end of dial* — the response will be sent after finishing of the number transmission to FXO;
  - *ringback tone* — the response will be sent after detection of remote station's ringback tone.

AutoCLIP settings

- *Enable AutoCLIP* – activate the service;
- *Delete used records* – after incoming call reception and routing to the subscriber, the record will be deleted from the base and following calls will be routed by a general dial plan;
- *Match outgoing FXO-port* – if the option is checked, then besides Calling and Called numbers, a number of an FXO port will be checked;
- *Digits match* – counting from the end of a number which received via CallerID that enables routing to a subscriber in the base;
- *Record keep time, min* – storage time for records in the base.

The service allows to ‘clip’ a call to a subscriber of the station, if the call is received on FXO port from a remote destination. When the subscriber calls back, the call will be redirected to a number from which the first call was implemented (Subscriber A).

AutoCLIP service is available only for '*with CallerID*' seize mode.



Extension Number	Called Number	Trunk
1002	13805876666	FXO Trunk

The service is dedicated to operate with FXO port.

Operation principles:

- if there is an egress call through an FXO port, SMG saves a record ‘CgPN, CdPN, FXO port index, time of call release’ which is attached to FXO profile of the FXO port;
- if there is an ingress call on an FXO port, SMG compare N last digits of received CallerID with CdPN (if ‘Match outgoing FXO-port' option is enabled, the index of FXO port is also compared). The number of digits compared is set in 'Digits match' field;
- if there is a corresponding record, the call is automatically routed to CgPN. If there are several records matched, the last added is used. If 'Delete used records' is checked, the record will be deleted;
- records are deleted when set 'record keep time' expires.

Tone detect parameters:

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].
Y – 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; 30000].
B – the pause duration (ms). The range of possible values is [100; 30000].

Advanced setting

- CPC processing – enabling CPC signal processing. Calling Party Control (CPC) Signal Detection — tracking the end of connection signal.

Dial sequence

A dial sequence is a number mask with special symbols which define dialing sequence.

Permitted symbols:

0-9 – digits from 0 to 9;

x or X – mask which define any digit from 0 to 9;

p or P – one-second pause. When dialing, there will be a delay before next symbol transmission to a line;

w or W – wait for station response. The station response is waited for 5 seconds. If there is no response in 5 seconds, the call will be released;

. (dot) – repeat digits. The symbol might be located only after 'X' mask in the end of the dial rule.

Example:

Dialing to international direction — 8xxxxxxxxxx.

Transit to FXO port through the prefix 8xxxxxxxxxx, which defines a trunk group with FXO ports included in it.

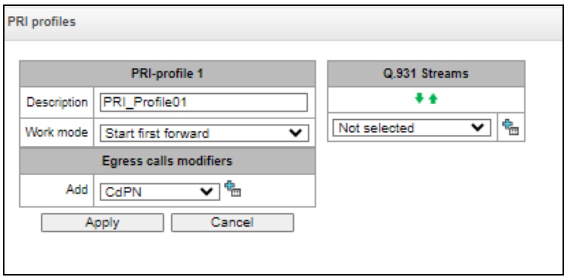
After dialing 8, wait for the station response which may have a delay of 6-7 seconds.

The dialing rule will be as follows:

8xxxxxxxxxx -> 8ppwxxxxxxxxxx – dial 8, make 2 seconds pause, wait for the station response, dial the rest.

3.1.7.7 PRI profiles

PRI profiles are used to configure PRI subscribers:



- *Description* – PRI profile menu;
- *Work mode* – an order of channels seizing:
  - *Start first forward;*
  - *Start last backward.*
- Egress calls modifiers:
  - *CdPN* – intended for modifications based on the analysis of the called number transmitted to the outgoing channel;
  - *CgPN* – intended for modifications based on the analysis of the caller number transmitted to the outgoing channel;
  - *Original CdPN* – intended for modifications based on the analysis of the original called number (original Called party number) transmitted to the outgoing channel;
  - *RedirPN* – intended for modifications based on the analysis of the redirecting number transmitted to the outgoing.

Modifiers of igress/egress calls for PRI subscribers work as follows. For example, on the E1 stream trunk group, to which PRI subscribers are bound, modifiers CgPN (Table1) and CdPN (Table0) are set for incoming communication; on the PBX profile to which PRI subscribers are bound, modifiers CgPN (Table3) and CdPN (Table2) are also set for incoming communication. In all tables, the selection mask is set to (x.)

A call comes in from E1 stream:

1. The rule for CgPN from the modifier table Table1 applies.

2. Checking the CgPN number for the PRI subscriber.

3. If the call is not from a PRI subscriber, the call is treated as from a normal trunk, the remaining modifiers tied to the trunk group on the incoming call will be applied.

If the call is from a PRI subscriber, the remaining modifiers tied to the trunk group and PBX profile will be applied. The order of application of the modifiers is as follows:

- The rule for CgPN from Table3 applies
- The rule for CdPN from Table1 applies
- The rule for CdPN from Table3 applies
- The rule for CgPN from Table0 applies
- The rule for CgPN from Table2 applies
- The rule for CdPN from Table0 applies
- The rule for CdPN from Table2 applies

The egress calls modifiers on a PRI profile are triggered when a call is routed to a PRI subscriber that is bound to this profile.

Q.931 streams

Select streams which will be attached to PRI subscribers.

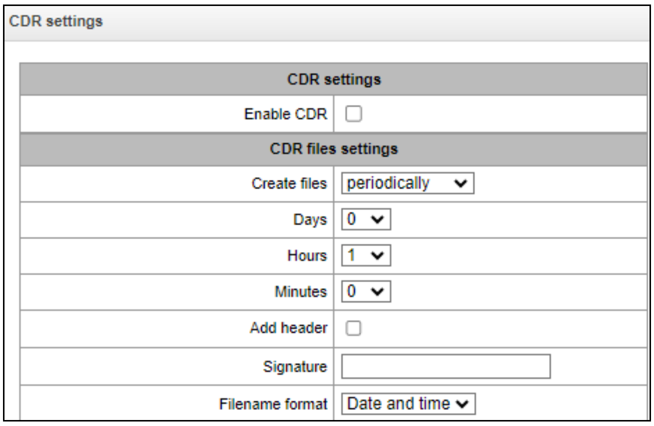
3.1.8 Internal Resources

3.1.8.1 CDR settings

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 gateway.

CDR settings

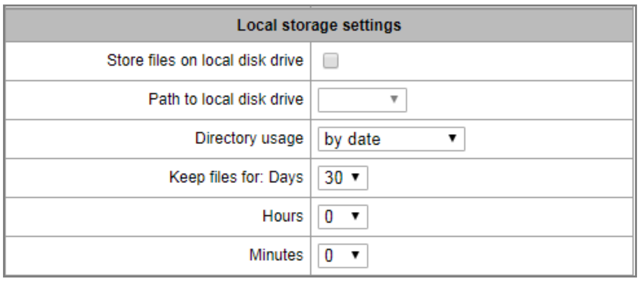


- *Enable CDR* – when this option is checked, the gateway will generate CDRs.

CDR files settings

- *Create files* – select the mode to create CDR files:
    - *periodically* – CDR file is created after the specified period has elapsed since the device boot;
    - *once per day* – CDR file is created once a day at the specified time*;*
    - *once per 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;
- *Signature* – specifies a distinctive feature to identify the device, which created the record;
- *Filename format* – a format of saved CDR file: date and time, only time.

Local Storage Settings



- *Store files on local disk drive* – when this option is checked, save CDRs onto the local drive;
- *Path to local disk drive* – 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*;
- *Directory usage* – select the directories for CDR data storage:
  - *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.
- *Keep files for: Days, Hours, Minutes* – the period to keep CDRs on the local drive.

When the the remote server for CDR storage 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.

<u>*Table of memory thresholds for CDR saving*</u>

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 2600 to 5200 records.

Remote storing settings

Remote storing settings	
Protocol	FTP

- *Protocol* – the protocol by which CDR records will be transmitted to the remote server. FTP and SCP protocols are supported.

Remote storage settings

Remote storage settings	
Store files on server	☐
Server	
Server port	21
Path on server	
Login	
Password	••••••

- *Store files on server* – when this option is checked, CDRs will be transferred to the remote server;
- *Server* – IP address of the server;
- *Server port* – TCP port of the FTP server;
- *Path on server* – a path to the FTP server directory to store CDRs;
- *Login* – username for access to the FTP server;
- *Password* – user password for access to the FTP server.

Remote backup storage settings

Remote backup storage settings	
Store files on server	☐
Only if primary server failed	☐
Server	
Server port	21
Path on server	
Login	
Password	••••••

If the primary server is unavailable, CDR records will be sent to the backup server (if the backup server is configured accordingly) until communication with the primary server is restored.

- *Store files on server* – when this option is checked, CDRs will be transferred to a backup server;
- *Only if primary server failed* – if the option is set, the saving of CDR files on a backup server will be implemented only in case of a failure in recording to a main FTP server. Otherwise, CDR files will be recorded to the primary and backup servers simultaneously;
- *Server* – IP address of the backup server;
- *Server port* – TCP port of the backup server;
- *Path on server* – a path to the backup server directory to store CDRs;
- *Login* – username for access to the backup server;
- *Password* – user password for access to the backup server.

Other settings

Other settings	
Save unsuccessfull calls	☐
Save empty files	☐
Write redirected call duration	☐
Swap Redirecting number and CgPN	☐
Round duration	upwards

- *Save unsuccessful calls* – when this option is checked, unsuccessful calls (not resulted in conversation) will be recorded into CDR files;
- *Save empty files* – when this option is checked, CDR files containing no records are saved;
- *Write 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;
- *Swap Redirecting number and CgPN* – 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;
- *Round duration* – this option specifies the mode for the call duration rounding off in CDRs:
    - *upwards* – call duration rounding mode; the call duration is rounded up if it exceeds 330 ms;
    - *downwards* – call duration rounding mode; the call duration is rounded down if it exceeds 850 ms;
    - *without round (use msec)* – in this mode, the call duration is not rounded up or down, and is recorded to the nearest millisecond.

Modifiers for incoming numbers

Modifiers for incoming numbers	
CdPN	not used
CgPN	not used
RedirPN	not used

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 dial plan.

- *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.

Modifiers for outgoing numbers

Modifiers for outgoing numbers	
CdPN	not used
CgPN	not used
RedirPN	not used

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 dial plan.

- *CdPN* – intended for modifications based on the analysis of the called number sent to the outgoing channel;
- *CgPN* – intended for modifications based on the analysis of the calling 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.

3.1.8.1.1 List of fields of CDR used

Here, the user 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 3.1.8.1.2).

To add or remove the desired fields, drag 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.

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 SS7 CIC
5. Call release info	Incoming SIP Call-ID
6. Incoming IP-address	Outgoing SS7 CIC
7. Incoming type	Outgoing SIP Call-ID
8. Incoming description	Incoming SS7 category
9. Incoming CgPN	Incoming Calling party category (RUS)
10. Outgoing CgPN	Outgoing SS7 category
11. Outgoing IP-address	Outgoing Calling party category (RUS)
12. Outgoing type	Incoming E1 stream
13. Outgoing description	Incoming E1 channel
14. Incoming CdPN	Outgoing E1 stream
15. Outgoing CdPN	Outgoing E1 channel
16. Setup time	Sequence number
17. Disconnect time	Incoming redirecting number
18. Rejecting RADIUS server address	Outgoing redirecting number
	RADIUS Accounting-Session-Id
	Global Callref
	Incoming numplan
	Outgoing numplan
	UniqueTag identifier
	Calling NAI
	Called NAI
	Incoming redirecting NAI
	Outgoing redirecting NAI
	Call transfer mark
	Call record path
	IVR call record path

Add all | Remove all | Default

3.1.8.1.2 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:

- Device sign;
- Setup time in YYYY-MM-DD hh:mm:ss format (for unsuccessful calls, this parameter is equal to the disconnect time);

- Duration, seconds;
- Release cause, according to ITU-T Q.850;
- Call release info.

Information about calling subscriber:

- IP address;
- Source type;
- Description – subscriber/trunk name (TG);
- Caller number on input;
- Caller number on output.

Information about called subscriber:

- IP address;
- Destination type;
- Description – subscriber/trunk name (TG);
- Called number on input;
- Called number on output;
- Connect time in format: YYYY-MM-DD hh:mm:ss;
- Disconnect time in format: YYYY-MM-DD hh:mm:ss.

3.1.8.1.3 Description of CDR Fields

UniqueTag identifier – a user-configurable string that identifies the device;

Connect time, call response time, Disconnect time – time of the corresponding event in the following format: 'YYYY-MM-DD HH:MM: SS.MSEC';

Duration – counted in seconds "SS"; if the rounding method is set to 'no rounding'; milliseconds are sent after the separating point: 'SS.MSEC';

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

Call release info:

- 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.

Incoming/outgoing IP address – 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.

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

Redirecting mark:

- *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.

Pickup mark:

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

Release side mark:

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

Incoming/outgoing SS7 CIC (for SMG-500) – 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 Calling party 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 (for SMG-500) – 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 (for SMG-500) – number of the incoming/outgoing E1 channel. If the call was made not through E1, the field will be empty;

Sequence 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 numplan – the number of the dial plan in which the call arrived and left;

UniqueTag Identifier – an individual call identifier that is received along the entire call transmission path;

NAI caller/called/inc. redirecting/outg. redirecting – indicators of the number's ownership:

- 0 – Spare
- 1 – Subscriber number
- 2 – unknown
- 3 – National (significant) number
- 4 – International number, where:
    - Local – Subscriber
    - International communications – INTERNATIONAL
    - Long-distance communications – NATIONAL
    - Special Services, Zonal and Departmental – unknown

Call Transmission Label – shows the call transmission label:

- <empty>
- transferred (initial call that was subsequently transferred)
- transferring (second call that accepted the transfer)

Blocking RADIUS server address – information about the RADIUS server blocking the call in the following format *IP, PORT, REPLYCODE*, where:

- IP – IP address of the RADIUS server blocking the call;
- PORT – port of the RADIUS server;
- REPLYCODE – RADIUS server response code.

3.1.8.1.4 CDR File Example

Example of CDR file, that contains four entries. Heading adding to a file is enabled, following fields has been chosen:

- Entry sequence number;
- UniqueTag identifier;
- Connect time;
- Setup time;
- Disconnect time;
- Duration;
- Release cause Q.850;
- Call release info;
- Release side mark;
- Redirecting mark;
- Pickup mark;
- Incoming type;
- Incoming description;
- Incoming E1 stream;
- Incoming IP address;
- Incoming CgPN;
- Outgoing CgPN;
- Outgoing type;
- Outgoing description;
- Outgoing E1 stream;
- Outgoing IP address;
- Incoming CdPN;
- Outgoing CdPN.

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;11000321 584f7eaa 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;06000106 584f7eaa 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;11000043 584f7ea9 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.

3.1.8.2 SS7 Categories

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

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		
№	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

3.1.8.3 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.

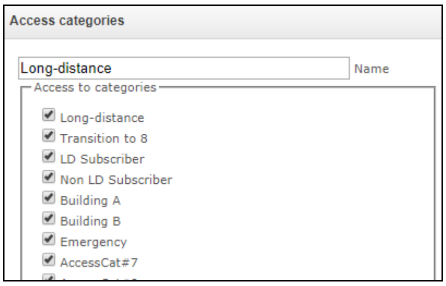
Access categories

№	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

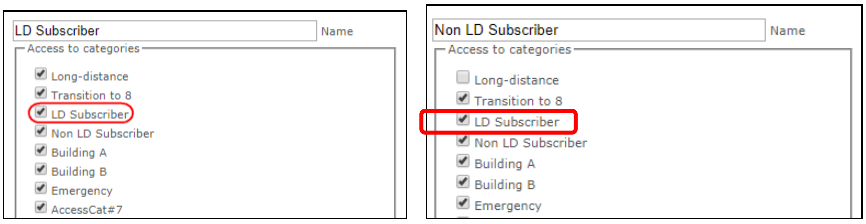
Example of access restriction configuration

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

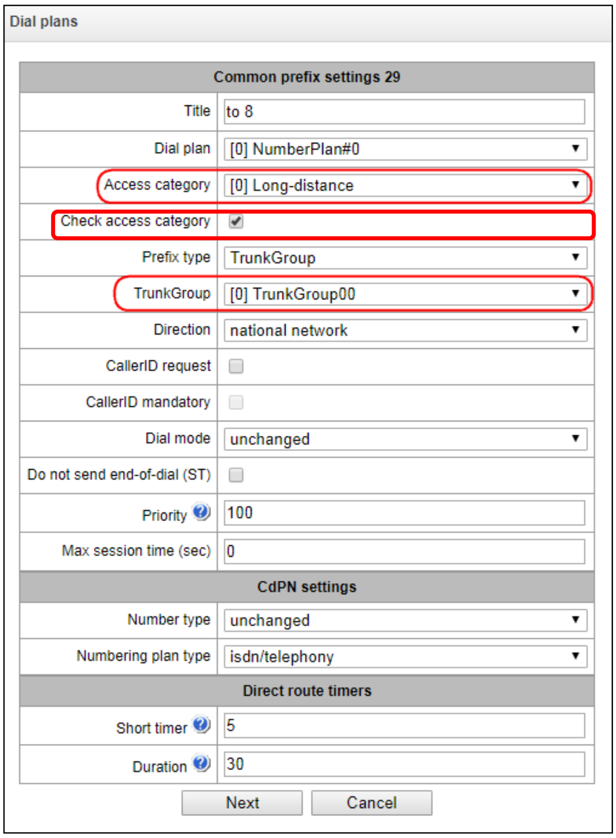
1. Select the access category for long-distance communication. For convenience, you can specify the name *Long-distance* or *Transition to 8.*



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*).

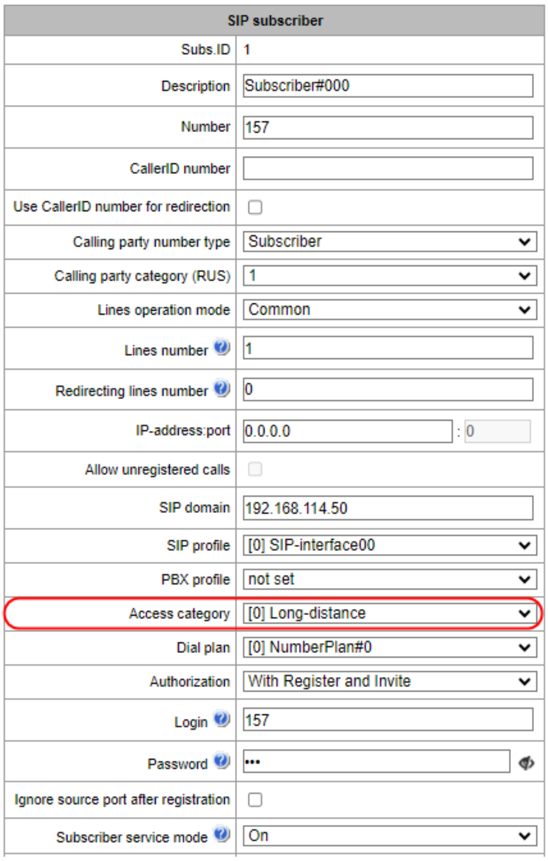


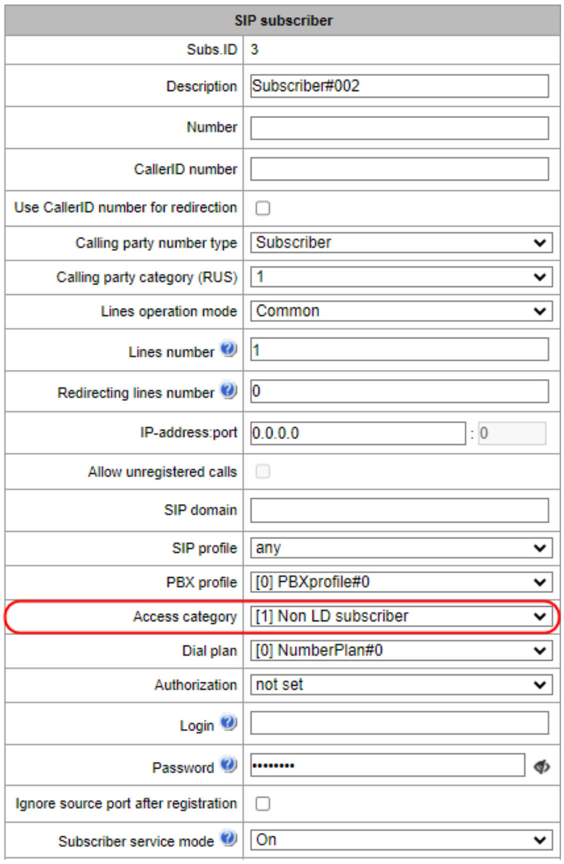
3. In the '*Dial plan*' section: for *Transition to 8 prefix*, select *Long-distance* and *Check access category.*



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.

Routing by access category

When a route is searched by number masks in the numbering plan, there is a check for prefix/call group accessibility by access category. It works optionally based on the *check access category* checkbox in the prefix or call group (the *access category* field is added to the call group).

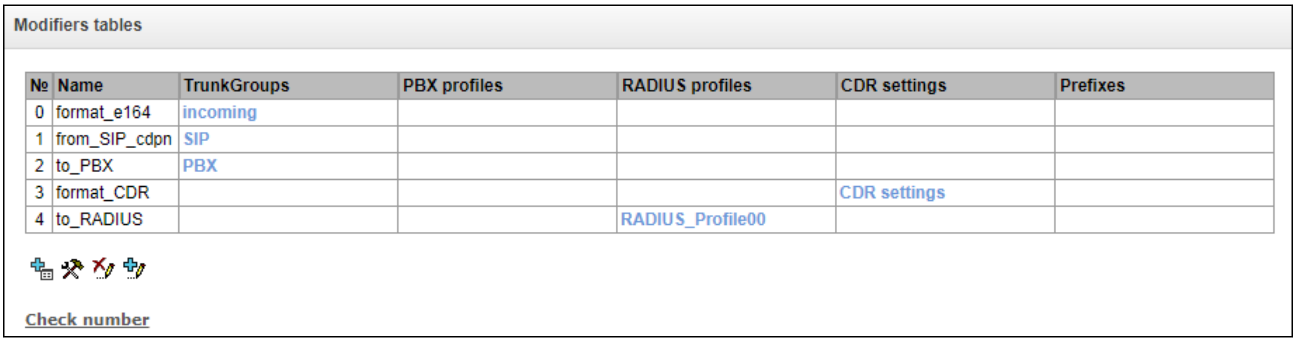
If the *check access category* checkbox is not selected on the prefix/group, the route is considered unconditionally accessible.

Now you can create several completely identical masks leading to different prefixes with different access categories.

In this regard, the procedure of mask analysis now looks as follows:

1. Searching for the masks matching the current number.
2. The masks are checked for accessibility by prefix/call group access category (new mode).
   2.1. All masks not matching the access category are refused service.
   2.2. If only one match is found, available by access category, this mask is used (new mode).
   2.3. If more than one match is found for accessibility by access category, the request is processed according to the old existing algorithm.
3. Checking prefixes priorities (call group has unconditional priority over prefixes).
   3.1. If only one match is found, this mask is used (new mode).
   3.2. If more than one match is found, the request is processed according to the old existing algorithm.
4. Checking the accuracy.
   4.1. Selecting a single mask more suitable to the routing rules.

3.1.8.4 Modifier Tables


Modifiers tables

№	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		

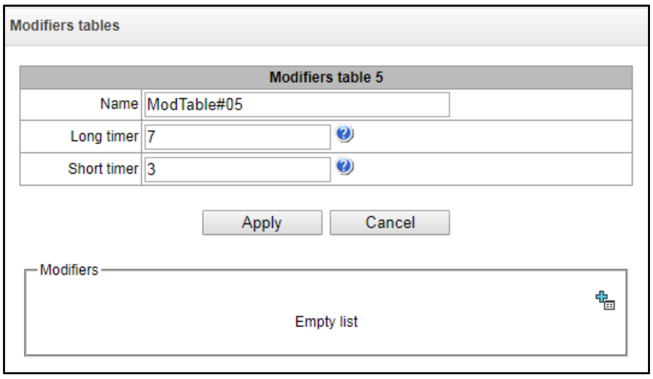
Check number

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.

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

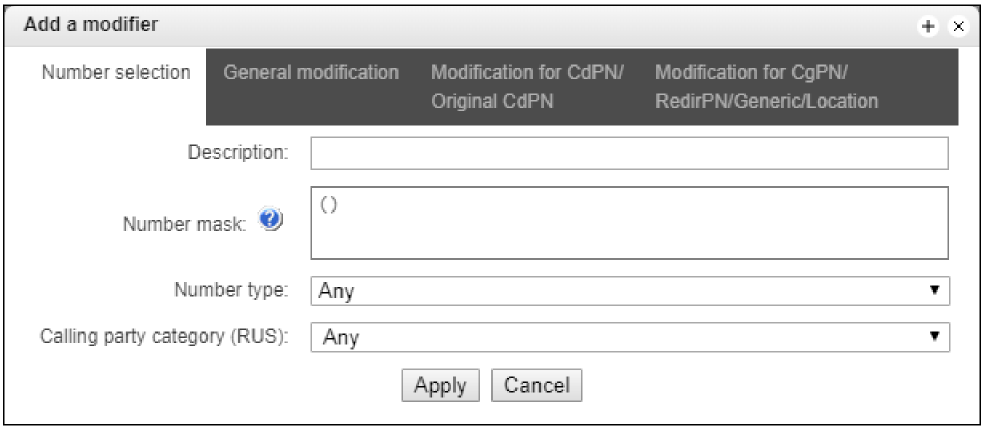


To confirm changes in modifier parameters, click the *Set* button, or click the *Cancel* to exit without saving.

To check the modifier operation, you can click the *Check number* link below the modifier table.

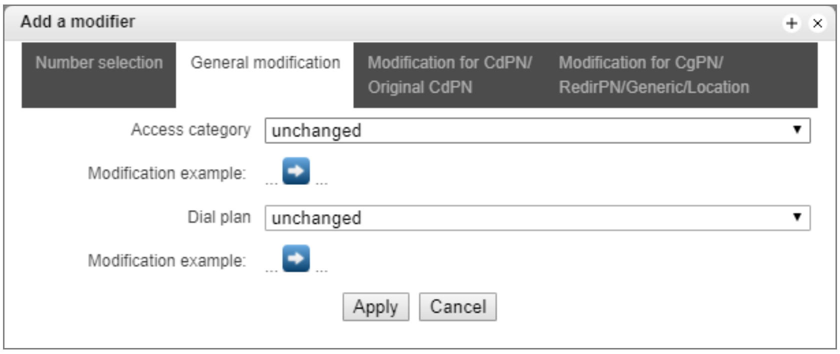
For the checking procedure, see section 3.1.8.4.1 *Checking Modifiers Operation.*

‘Number selection’ tab



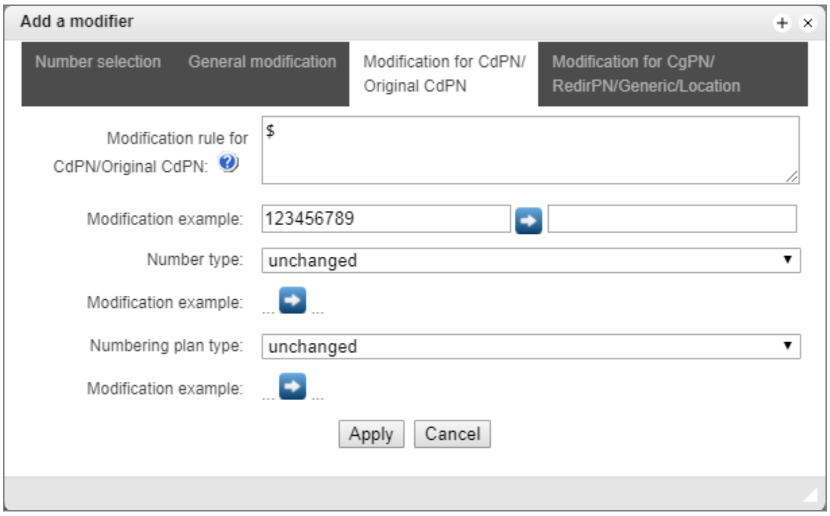
- *Description* – description of the modifier;
- *Number mask* – a template or a set of templates which is compared to the subscriber number (for mask syntax, see section 3.1.4.2);
- *Number type* – type of the subscriber number:
    - *Subscriber* – subscriber number (SN) in E.164 format;
    - *National* – 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;
    - *Unsupported* – number type is not specified in the recommendation.
- *Calling party category (RUS)* – subscriber's Caller ID category.

'General Modification' Tab



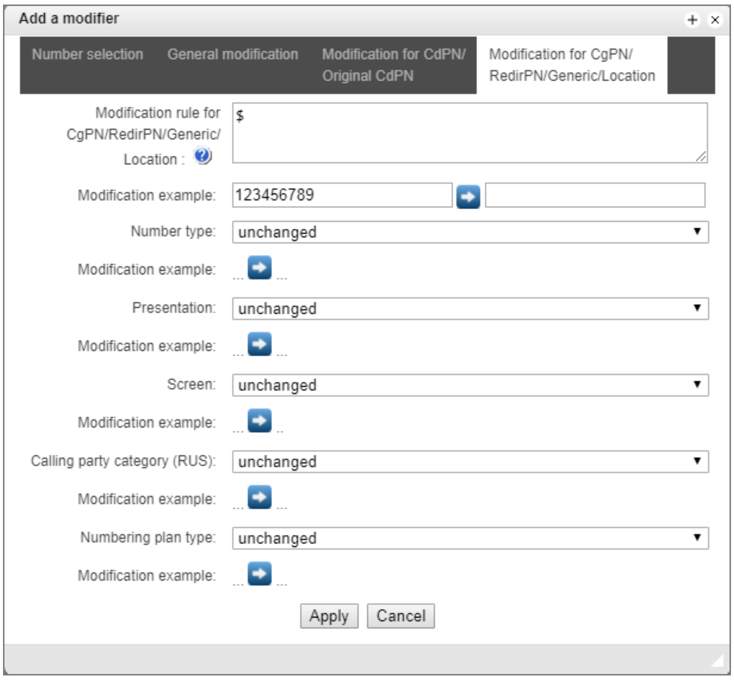
- *Modification example* – click the button to view modification summary after application of the specified modification rules;
- *Access category* – allows modification of access categories;
- *Dial plan* – allows modification of the dial plan to be used for further routing (required for coordination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

'Modification for CdPN/Original CdPN' 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;
- Modification rule for CdPN/Original CdPN – called number modification rule. For syntax, see section Modification Rule Syntax; to get some examples, see APPENDIX I. RADIUS CALL MANAGEMENT SERVICE. 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 plan type* – modification rule for the dial plan type.

‘Modification for CgPN/RedirPN/Generic/Location’ tab



- *Modification rule for CgPN/RedirPN/Generic/Location* – the called number modification rule. For syntax, see section [Modification Rule Syntax;](#) to get some examples, see APPENDIX I. RADIUS CALL MANAGEMENT SERVICE. 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;
- *Calling party category (RUS)* – modification rule for the caller category;
- *Numbering plan type* – modification rule for the dial plan 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**

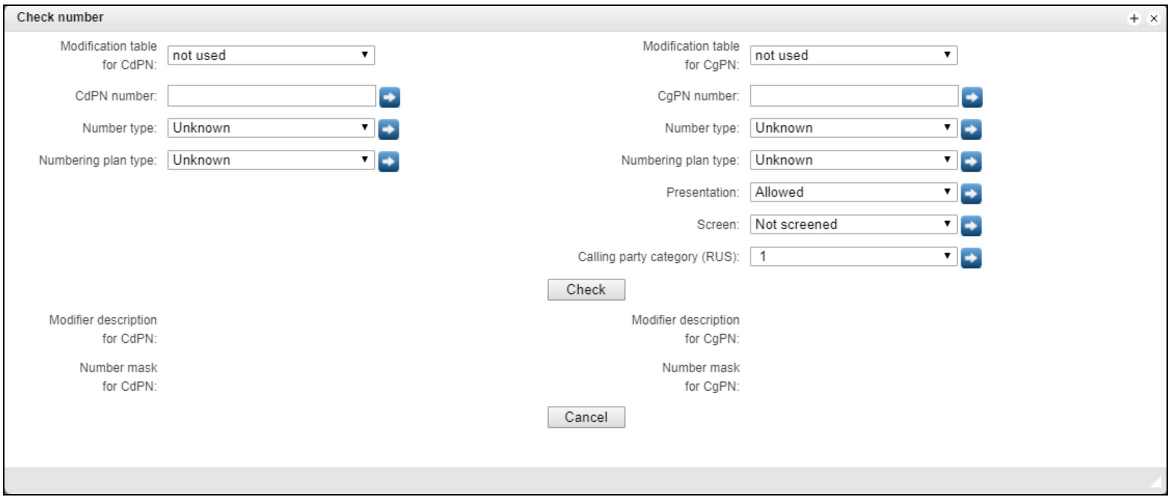
Remove the last four digits from number 22201239876
Modifier: **$----**
Result: **2220123**

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**

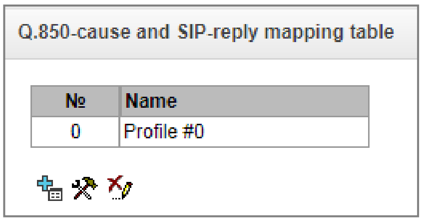
3.1.8.4.1 Checking Modifiers Operation

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 plan type, Presentation, Screen, and Calling party 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.

3.1.8.5 Q.850-Cause and SIP-Reply Mapping Table



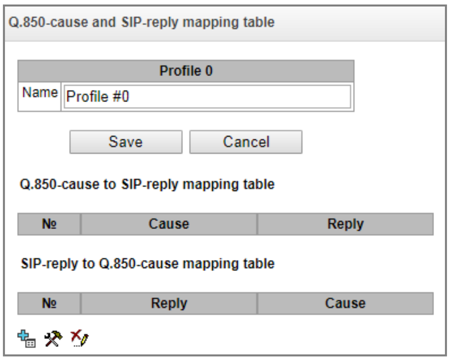
This section establishes correspondence between clearback reasons described in Q.850 recommendations for the SS7 protocols (SIP-T/SIP-I) and 4xx, 5xx, 6xx class SIP replies.

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:

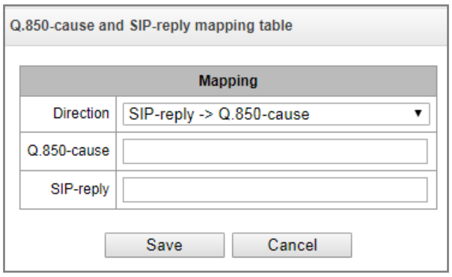
– Add rule;
– Edit rule parameters;
– Remove rule.

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



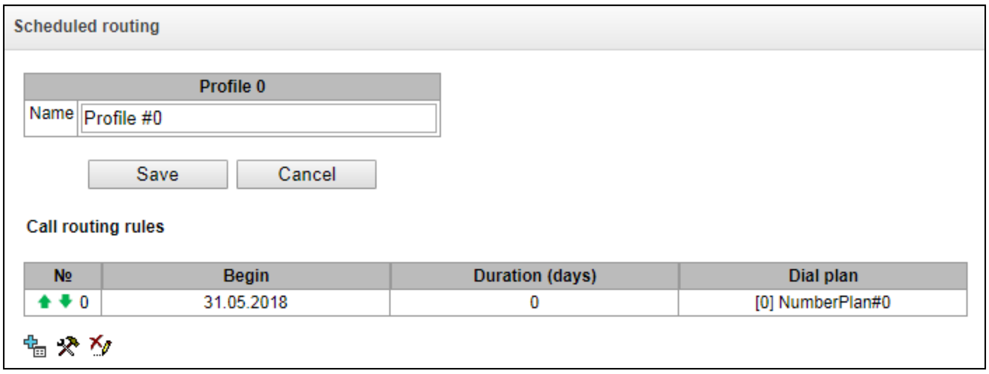
Profile Settings

- Direction:
    - *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.



3.1.8.6 Scheduled Routing

This section configures scheduled routing that allows using different dial plans depending on the time and day of the week.

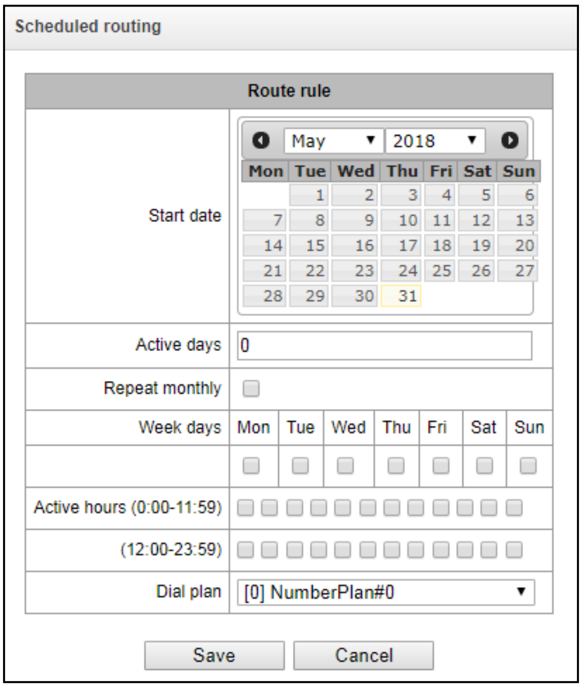


To create, edit, or remove rules, use the following buttons:

– Add rule;
– Edit rule parameters;
– Remove rule.

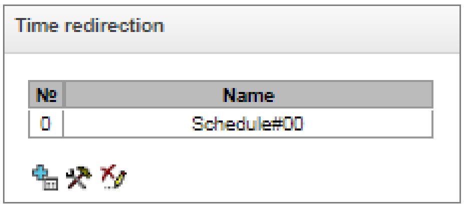
Routing Rule

- *Start date* – select start date for the scheduled routing rule operation;
- *Active days* – duration of the scheduled routing rule operation;
- *Repeat monthly* – allows monthly repetition of the routing rule;
- *Week days* – select days of the week for the scheduled routing rule operation;
- *Active hours* – select hours of the scheduled routing rule operation;
- *Dial plan* – select a dial plan that will be used during the scheduled routing rule operation.

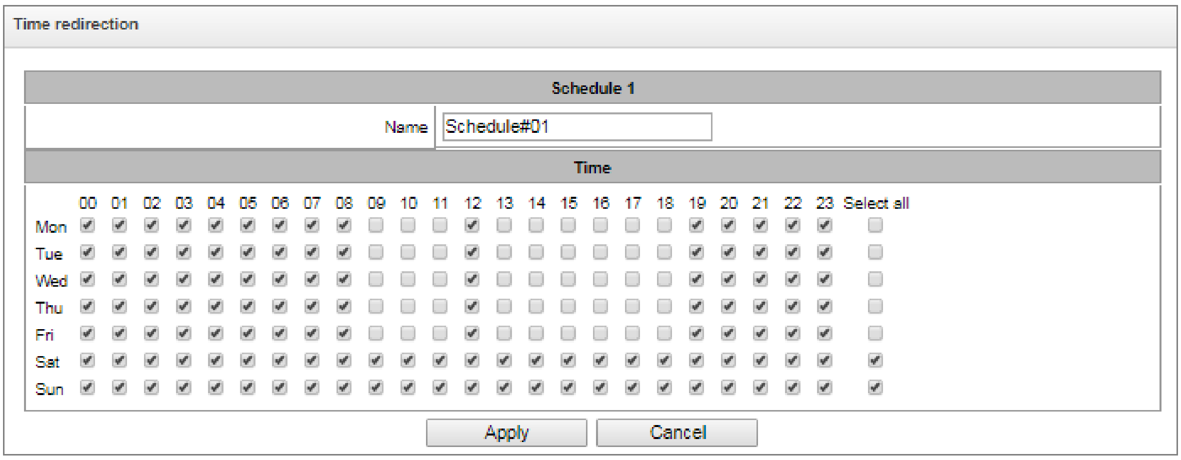


3.1.8.7 Time redirection

To configure time intervals for redirection you need to create a schedule:



Then, you may select time intervals for redirection service.



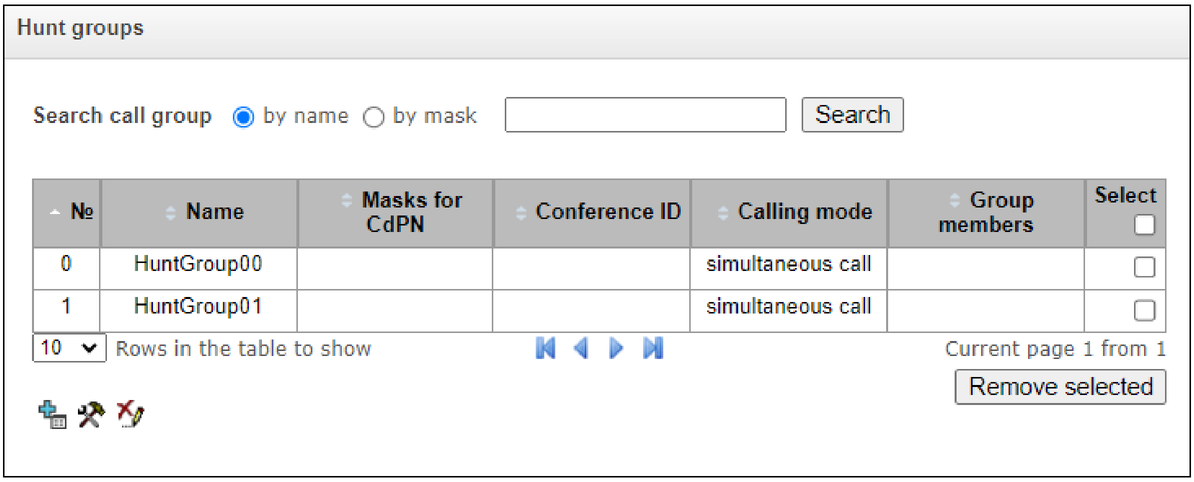
After creating a schedule for redirecting, attach the schedule to a necessary subscriber through VAS management menu (see section 3.1.7.1.3 VAS Management).

3.1.8.8 Hunt Groups (Call group)

Hunt group – 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 hunt group is designed for call centers or connection of offices with simultaneous or successive dialling for employees from the same call group.

In total, up to 1000 hunt groups can be created.

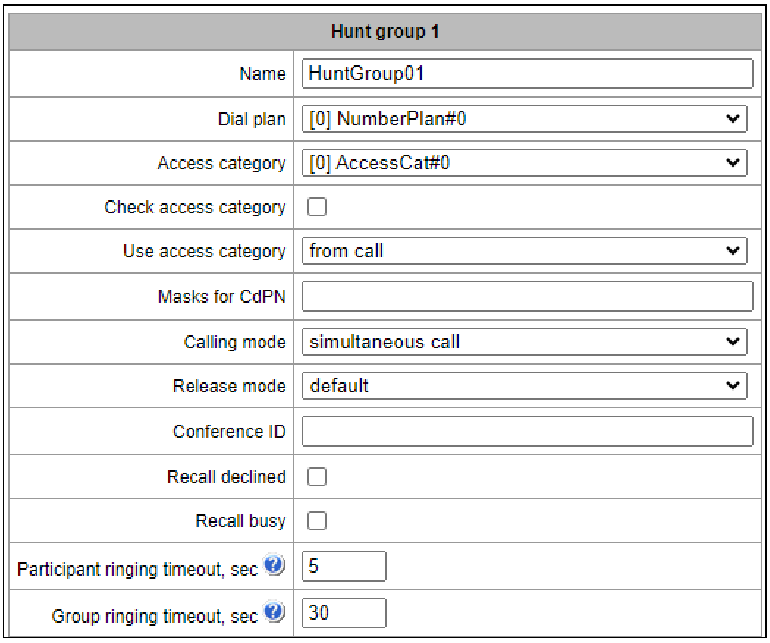


- *Search call group by name* – checking for the presence of a call group by its name;
- *Search call group by mask* – checking for the presence of a call group by mask for CdPN.

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.



- *Name* – name of a call group;
- *Dial plan* – select a dial plan that the call group will belong to;
- *Masks for CdPN* – the called number mask to call the group from the dial plan tied to the group (the mask syntax is described in section 3.1.4.2);
- *Calling mode* – the method of dialling to members of a call group:
  - *simultaneous call* – a simultaneous call to all members of a call group;
  - *sequential from first* – a 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 canceled and a call to the next member of the group is initiated;
  - *sequential from 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 the group members. After the *Stimer* expires, the call to a member of this group is canceled and a call to the next member of the group is initiated;
  - *sequential all from first* – a 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 canceled and a call to the next member of the group is initiated;
  - *sequential all from 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 canceled and a call to the next member of the group is initiated;
  - *serial search from first* – a method that searches for the first available subscriber from the beginning of the list; (the first available subscriber is being called until the caller answers or until the timeout clearback occurs) this group can include only subscribers of this gateway;
  - *serial search from last* – the method that searches for the first available subscriber from the end of the list (the first available subscriber is being called until the caller answers or

until the timeout clearback occurs); this group can include subscribers of this gateway only.

- *Release mode* – a method of releasing members of a call group:
  - *Default* – when one member of a call group answers, a CANCEL message is sent to all other members, resulting in a missed call notification on their telephones;
  - *Silent* – when one member of a call group answers, all other members receive a CANCEL message with the title *Reason:* SIP4 cause=200, as a result, there will be no missed call notification on the telephones of these subscribers.

- *Conference ID* – when this number is dialed after the Conference VAS prefix, all members of this call group will be included into a conference call;

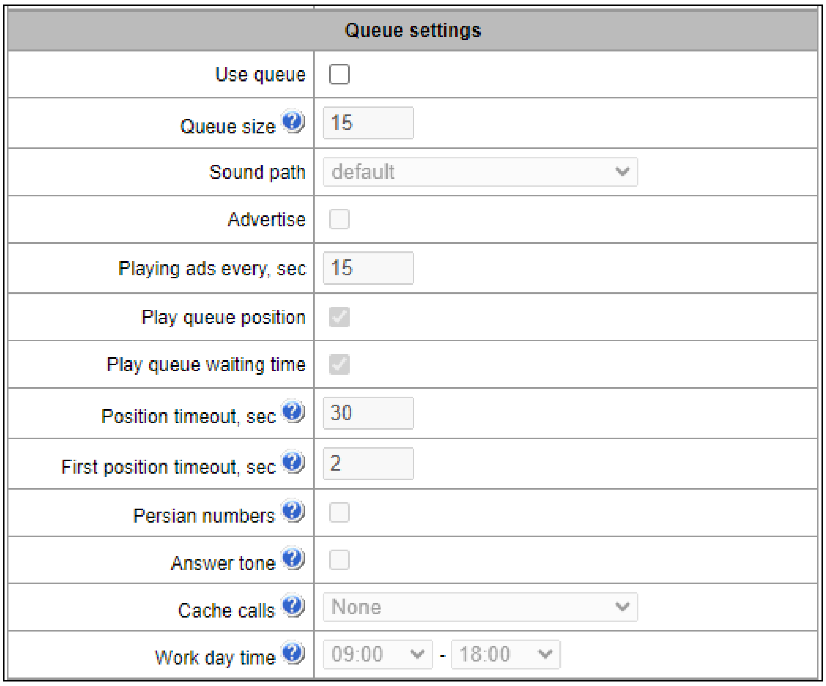
- *Recall declined* – using this option will make repeated attempts to call the group members who rejected the call without picking up the handset. If the called subscriber rejects the call three times, attempts to reach them will stop;

- *Recall busy* – using this option will make repeated attempts to call group members who are busy at the time of the group call (until the group call is answered or the group call timeout expires);

- *Participant ringing timeout, sec* – the call timeout for one member of a call group;

- *Group ringing timeout, sec* – the general call timeout for the entire call group.

The queue functionality is available for the following modes: simultaneous call, sequential from first, sequential from next, sequential all from first, and sequential all from next.



The queue functionality is required for organizing a call center.

- *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;
- *Sound 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

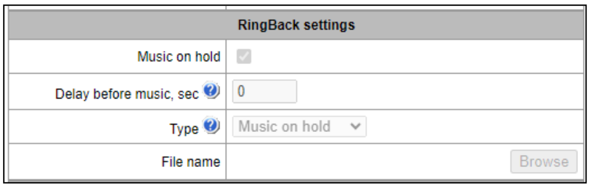
- *Advertise* – when this option is checked, audio files from the advertise directory will be played to the caller waiting for the operator's answer (with the specified advertising timeout);

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.

- *Playing ads every, sec* – the period of time after which the advertisement will be played to the subscriber;
- *Play queue position* – when this option is checked, the caller will be informed on their position in the queue;
- *Play queue waiting time* – when this option is checked, the caller will be informed on the waiting time;

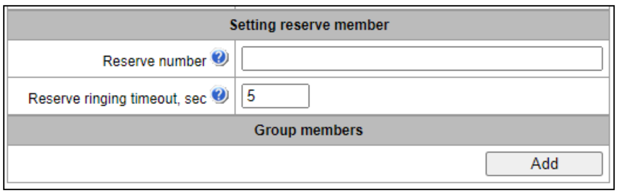
- *Position timeout, sec* – the interval at which the subscribers will be informed of their position in the queue; the interval starts when the last playback of the position ends;
- *First position timeout, sec* – time after which the subscriber's queue position will be played for the first time;
- *Persian numbers* – SMG200/SMG-500 devices support playing composite Persian numbers. To reproduce numbers greater than 20, three parts of a numeral, including a connecting word, are used;
- *Answer tone* – when this option is checked, the answerer_tone.wav audio file will be played to the caller and operator after the operator responds;
- *Cache calls* – 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:
  - *None* – 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;
  - *Non-strict* – if the required operator is busy, the call will be distributed among other operators in accordance with the accepted operation mode.
- *Work day time* – sets the working hours to calculate the statistics of a call group.

RingBack settings



- *Music on hold* – using music on hold instead of the RingBack signal while waiting for an operator response;
- *Delay before music, sec* – the time during which the standard RingBack will be played before the MoH is activated;
- *Type* – selecting the type of MoH:
  - *Music on hold* – when this type is selected, a standard SMG MoH will be played to the subscriber;
  - *Audio file* – by selecting this type it is possible to assign an audio file pre-loaded on the drive for playing. You can select the drive for downloading audio files in *System Settings -> RingBack settings*.
- *File name* – selecting an audio file to be played as a RingBack.

Setting reserve member



- *Reserve number* – a number to which the call will be made after the *group call timeout* is triggered;
- *Reserve ringing timeout, sec* – the timeout responsible for the duration of the call to the reserve number.

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

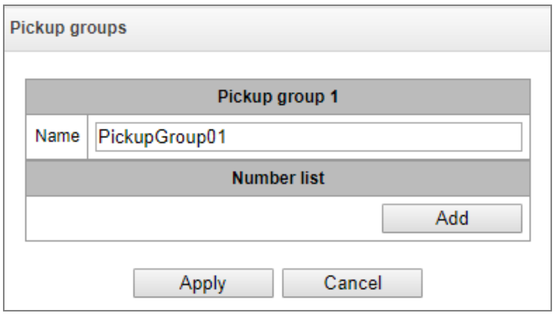
3.1.8.9 Pickup Groups

Pickup group – 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.

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

– Add entry;
– Edit entry parameters;
– Remove selected.

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



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

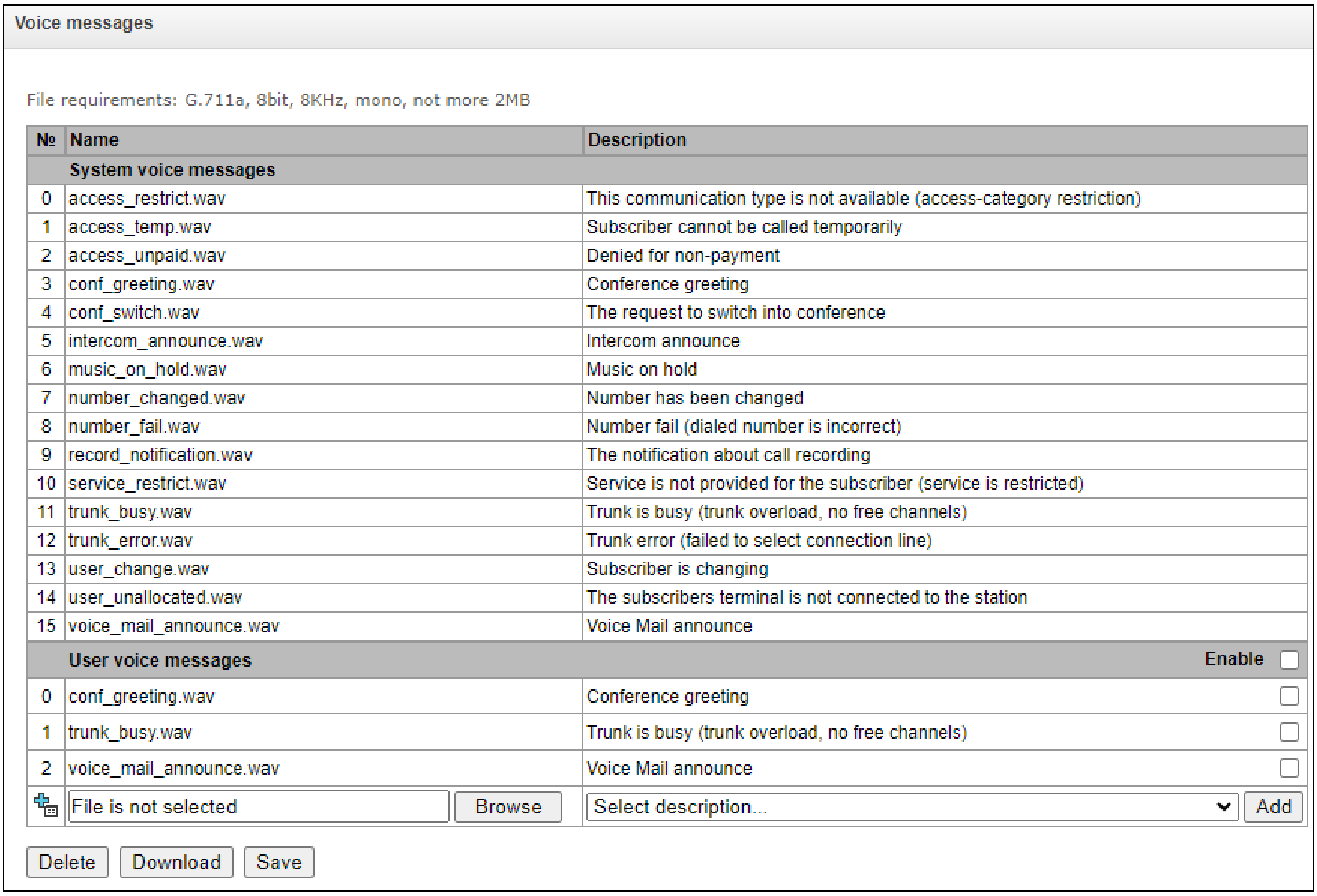
Pickup group member type:

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

3.1.8.10 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.


Voice messages

File requirements: G.711a, 8bit, 8KHz, mono, not more 2MB

№	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	
15	voice_mail_announce.wav	Voice Mail announce	
	User voice messages		**Enable**
0	conf_greeting.wav	Conference greeting	
1	trunk_busy.wav	Trunk is busy (trunk overload, no free channels)	
2	voice_mail_announce.wav	Voice Mail announce	
	File is not selected Browse	Select description...	Add

Delete Download Save

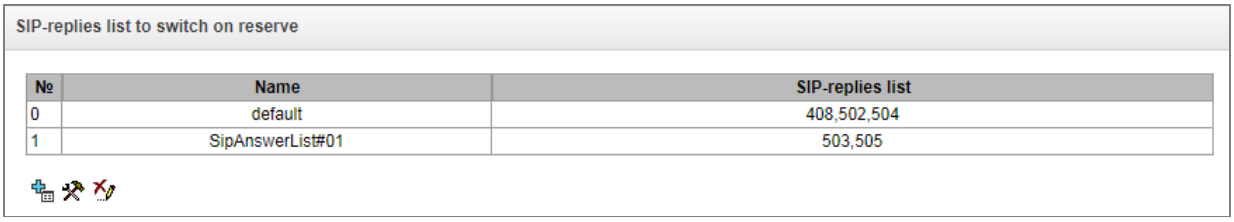
- *No.* – sequential number of a voice message file;
- *Name* – name of a voice message file;
- *Description* – description of a voice message file.

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

- *Enable* – enables playing a voice message file.

3.1.8.11 SIP-replies list to switch on reserve TG

In this section, one 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.

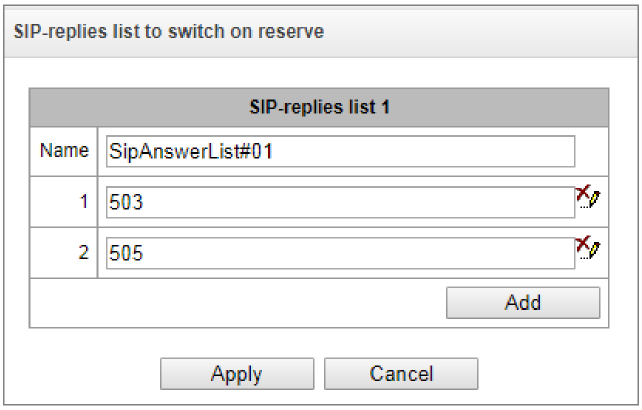


To create, edit, or remove the list, use the *Objects – Add Object, Objects – Edit Object* or *Objects – Remove Object* menus and the following buttons:

– Add the reply list;

– Edit the reply list;

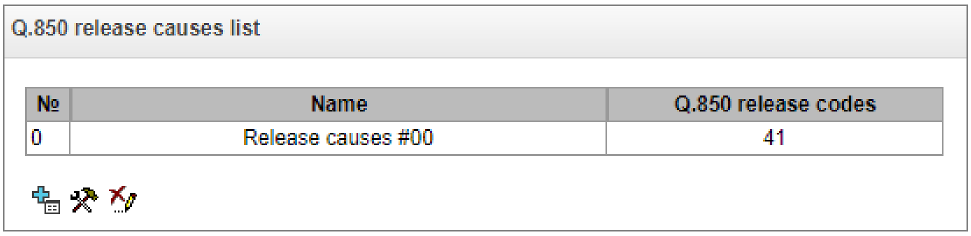
– Remove the reply list.



Specify the list name and generate it by clicking the *Add* and *(Delete)* buttons.

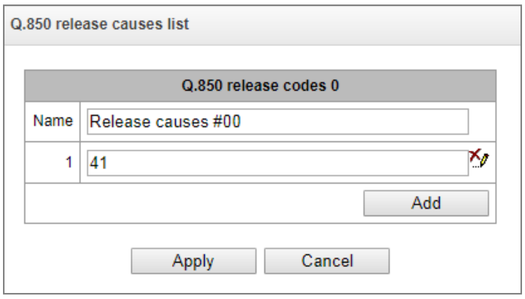
3.1.8.12 Q.850 release causes list

In this section, one can configure the list of Q.850 release 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.



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

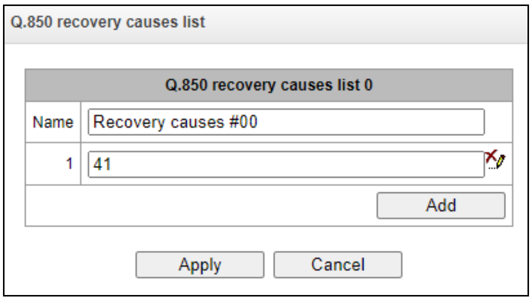
– Add the reply list;
– Edit the reply list;
– Remove the reply list.



Specify the list name and generate it by clicking the *Add* and *(Delete)* buttons.

3.1.8.13 Q.850 recovery causes list

In this section, you can configure the list of Q.850 release causes for SS7 and Q.931 protocols that will be used to recover communication if the call was not released from the incoming party.



To create, edit or remove a list, use *Objects — Add object*, *Objects — Edit object* and *Objects — Remove object* menus and the following buttons:

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

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 centers, 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 Scenarios list (scripts)

In this section, you can create the IVR operation scenario[1].

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

– Add entry;
– Edit entry parameters;
– Remove entry.

The **Scenarios list** table – displays all created IVR scripts.

Scenarios list

№	Name	Filename
0	IVRScenario_00	

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

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

Files list

№	Filename	Delete
0	IVRScenario	

File is not selected Browse Upload

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

The **Typical scenarios list** table contains files of common IVR scripts that can be edited.

Typical scenarios list

№	Filename
0	1_scenario_auto_attendant
1	2_scenario_call_operator
2	3_call_technical_support_department
3	4_call_departament
4	4_call_departament_2
5	4_call_departament_3
6	5_auto_attendant
7	5_auto_attendant_2
8	5_auto_attendant_3
9	5_auto_attendant_4
10	5_auto_attendant_5
11	5_auto_attendant_6

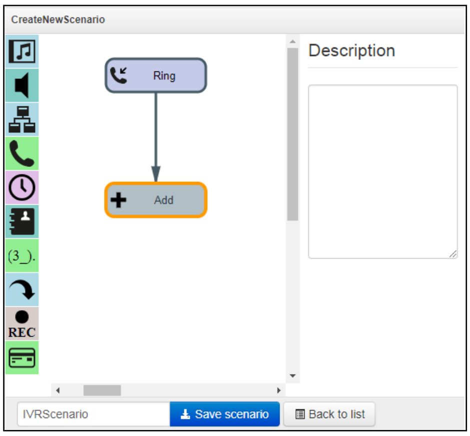
To download the scripts selected in the table to the user PC.

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.

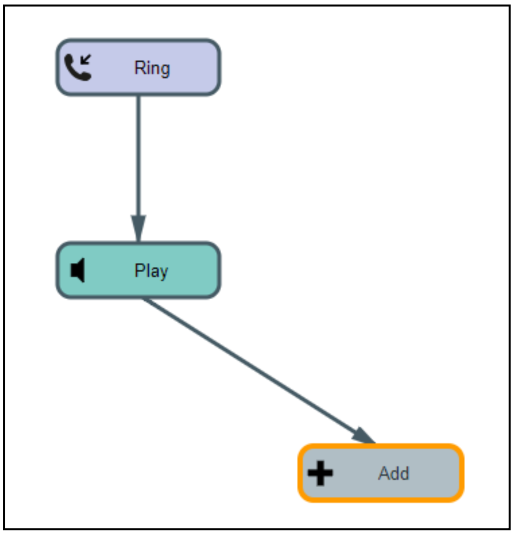
[1] This option is available only if you have an SMG-IVR license. For more information about the licenses, see section 3.1.23 Licenses.

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

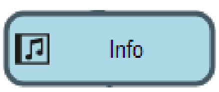


You can move the blocks across the field; to do this, select the desired block and move it to the desired place while holding the left mouse button. At that, all existing logical links will remain intact.

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.

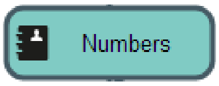
For IVR block description, see Table 12.

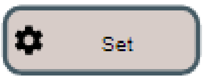
Table 12 – IVR Block Description

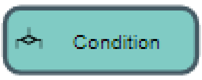
Symbol	Name	Description
	**Add**	An empty unit designed for block addition.
	**Ring**	This block enables ringback tone playback for the subscriber; it is always the first one in the list of scripts. When a call arrives to the RING block, the call status does not change. **Parameters** *Ringback duration, sec* – select duration of the ringback tone playback or disable it. **Links** *Input* – beginning of the call to IVR. *Output* – a single output containing information about the incoming call parameters (number A, number B). **Features** The block does not change the call status.
	**Info**	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.

		Parameters *Messages for playback until the subscriber answers* – select a single or multiple voice messages for playback to the caller. For voice message management, see section 3.1.8.10 Voice Messages. A drive for storing the files can be specified in section 3.1.1 System settings. *Loop playback* – select the number of message playback loops; they are played one by one, starting from the first message. **Links** *Input* – an incoming call in the preanswering state. *Output* – end the playback of the selected files. **Features** The Info block may be preceded only by blocks that do not affect the call status (Ring, Info, Digitmap, Time, Goto).
	**Play**	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. **Parameters** *Messages for playback until the subscriber answers* – select a single or multiple voice messages for playback to the caller. For voice message management, see section 3.1.8.10 Voice Messages. A drive for storing the files can be specified in section 3.1.1 System settings. *Loop playback* – select the number of playback cycles. The messages are played one by one, starting from the first message. **Links** *Input* – an incoming call in the preanswering or answer state. *Output* – end the playback of the selected files.
	**IVR**	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 dial plan and playback of audio files, system sounds (ringback tones, ringing tone, a busy signal) and DTMF digits to notify the subscriber. **Parameters** *Type* – the type of audio file to be played. *File* – an audio file uploaded to the device. The list of IVR sounds is configured in section 3.1.9.2 Tones list. *Tone* – select a system sound to be played (DTMF digit, dialtone, busy, ringback). *Subscriber selection* – 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. *Subscriber selection timeout, sec* – extension number dialling timer; when this timer expires, the outgoing IVR branch is selected. *Enable extension dialling* – enable extension dialling, which is followed by the

		device dial plan routing, e. g. internal subscriber number can be dialled. *Access category* – select an access category. Access category allows you to define call prohibition for the number dialled by the subscriber in the IVR block. *Max dialing digits* – the maximum number of digits that can be dialled using the extension dialling. *Interdigit timeout, sec* – interdigit delay for the extension number. **Links** *Input* – an incoming call in the preanswering state or active call phase. *Output* – the number of outputs can be configured, extension dialling can also be one of the outputs. **Features** 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.
	**Dial**	The block is required to dial the specified number, which is further routed according to the dial plan of the device. **Parameters** *Number* – the specified number. Dial plan: *Transit* – the dial plan is not changed. *Access category* – sets the access category that will be used after passing the Dial block: *Transit* – the access category is not changed. **Links** *Input* – an incoming call in the preanswering state or active call phase. *Output* – exit from the block if the dial is unsuccessful. **Features** Finishes the script branch.
	**Time**	The block is required to select the call path logic according to the current time and day of the week. **Parameters** *Time* – select a template for time and day of the week. The time is set in 24-hour format. **Links** *Input* – an incoming call in the preanswering state or active call phase. *Output* – 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). **Features** The block does not change the call status.

	**Numbers**	The block is required to select the call path logic depending on the caller number. **Parameters** *Number* – the calling number template. **Links** *Input* – an incoming call in the preanswering state or active call phase. *Output* – 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 detected (“no” output). **Features** The block does not change the call status.
	**Digitmap**	The block is required to select the call path logic depending on the called number. The called number is verified at the entry to the digitmap block. **Parameters** *Mask* – the called number template. **Links** *Input* – an incoming call in the preanswering state or active call phase. *Output* – 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). **Features** The block does not change the call status.
	**Goto**	The block is required to transfer a call to another arbitrary script block. **Parameters** *Select block* – click this button to select a block in the chart to which the transition will be made. *Max hops* – select the number of passes for a call through this block to ensure the call looping protection. **Links** *Input* – an incoming call in the preanswering state or active call phase. *Output* – a single output to the block to which the transition is made. **Features** The block does not change the call status.
	**REC**	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. **Links** *Input* – an incoming call in the active call phase. *Output* – the block has a single output.

		Features 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 3.1.12.1 Call recording settings, in the 'Folder name for IVR conversation recording' parameter. For management of the records, see section 3.1.9.3 Call records.
	**Caller Info**	The block allows 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. **Parameters:** *Number mask* – the caller number template. *Subscriber name* – new subscriber name. **Links** *Input* – an incoming call in the preanswering state or active call phase. *Output* – the block has a single output. **Features** The block does not change the call status.
	**Set**	The block allows to dertermine the variable for IVR script: **Parameters:** *Key* – the name of the variable by which you can refer to it in other blocks; *Value* – variable value.

	**Condition**	The condition block is designed to test Boolean conditions composed of variables and strings. All operations are performed over **strings**. Up to 10 conditions can be set in a block. Each condition is assigned a corresponding exit branch (from 0 to 9) from a block to another block. In the Condition block, the transition is carried out along the branch of the first true condition (if there are several true conditions, the first one is selected). If none of the conditions in the Condition block turned out to be true, then the transition along the False branch will be performed.
		
		The following operators are avaible to form conditions:
		Logical operators:
		`!, not – logical NO;`
		`&&, and – logical AND;`
		`||, or – logical OR.`
		Comparison operators:
		`< – less;`
		`<= – less or equal;`
		`= – equal;`
		`> – more;`
		`>= – more or equal;`
		`<> – not equal.`
		
		Logical operators: since the comparison is performed on strings, the comparison is performed **character by character.**
		Examples of comparing strings of digits of equal length:
		
		`"101" < "102" = true`
		`"101" =< "102" = true`

		“101” > “102” = false “101” >= “102” = false Examples of comparing strings of digits of unequal length: “101” < “1102” = true “101” =< “1102” = true “101” > “1102” = false “101” >= “1102” = false Examples of comparing strings of numbers and letters of equal length: “A01” < “102” = false “A01” =< “102” = false “A01” > “102” = true “A01” >= “102” = true “A01” < “102” = false, since the strings are compared character by character, namely the character code A in the ASCI table is greater than the character code 1. Entry operator in – operator for entering a variable into a list (eg., %%CGPN%% in (710, 711, 712)). Variables: A string enclosed in percent symbols (%). The variable name can contain characters: [A- Za-z 0-9]. Constants: Any characters enclosed in single (‘) or double (“) quotes. The slash character (/) is used for escaping. Or any sequence of non-whitespace characters that do not start with a percent sign does not contain single or double quote characters. Predefined variables: CGPN – calling number; CDPN – called number; YEAR_LOCAL, MONTH_LOCAL, DAY_LOCAL, HOUR_LOCAL, MINUTE_LOCAL, SECOND_LOCAL – date and time of script execution (local time from the device is used).
	**RPC**	Block for interacting with an external HTTP server HTTP request settings: • *URL* – the full URL of the request to the http server. If necessary, you can use the variables of the current IVR scenario in the URL; Example: http://infoUserServer.co/shirts?style=%CDPN% • *Method* – HTTP request method (GET, POST, PUT, TRACE, OPTIONS, DELETE, HEAD); • *Request timeout* – time to attempt a request to the HTTP server in milliseconds; • *Content type* – the type of data contained in the request body; • *Body content* – request body (a string with the possible presence of macro variables); • *Headers* – HTTP request header; • *Key* – http header key;

		• *Value* – a string with a possible value of macro variables; • *Response type* – the type of data contained in the response body; • *icon* – when this type is selected, if the response body receives data “key:value”, then SMG writes this data as variables that can be used later; **If the key in the response body is written in small letters, for example var, then in order to later access this variable, it must be written in capital letters % VAR%.** • *regexp* – when this type is selected, the ‘Regular expression’ window appears, in which you can write a regexp expression for parsing a response from an HTTP server with the ability to write the parsed data to IVR variables and use them later. Example: Reply in the message body: Hello world The string in the field “Regular expression”: Hello (?<var>.*) As a result, a variable will be created within the IVR script VAR1=world • *Max bytes* – maximum response size; • *Expected encoding* – encodings supported in the response; • *Codes* – expected HTTP server response codes.

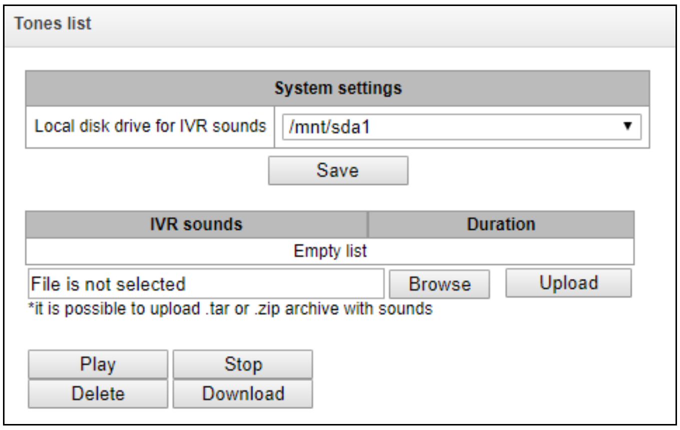
Having created a script flowchart, specify its name and save it by clicking the *Save script* button. Click the *Back to list* button to exit the design view without saving any changes.

3.1.9.2 Tones list

In this section, the audio files required for IVR operation can be managed.

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

The **System Settings** table contains the ‘Local disk drive for IVR sounds’ setting that specifies a drive to store IVR conversation record files.



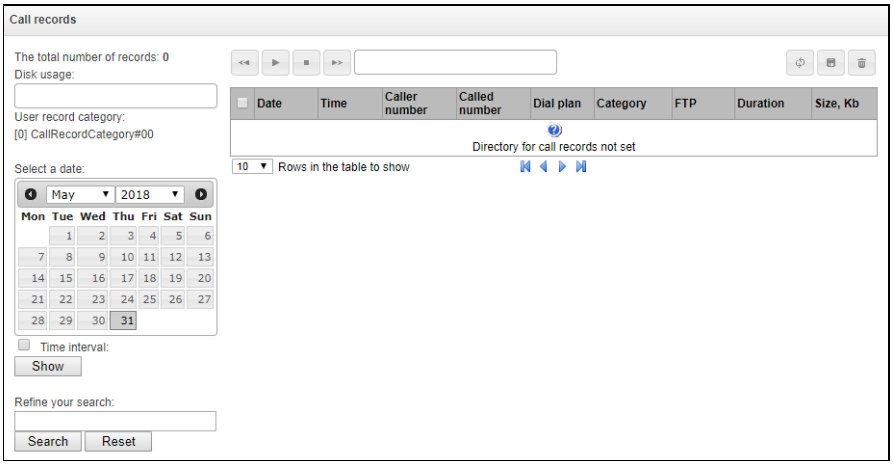
- *IVR sounds* – the list of uploaded files;
- *Duration* – uploaded file length;
- *Browse* – select an audio file to be uploaded to your device;
- *Upload* – command to upload the selected file.

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 Call records (IVR)

In this section, IVR conversation record files can be managed. 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;
- *Disk usage* – display the used space on the drive selected to store the conversation record files;
- *Select a date* – select the date to display conversation record files;
- *Time interval* – select the interval to display conversation record files;
- *Refine your search* – 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

Description of the records table columns

- *Date/time* – date and time of starting a record;
- *Caller/called number* – numbers of subscribers participating in the conversation*;*
- *Called number from the hunt group* – number of the subscriber who answered after passing through the call group;
- *Dial plan* – dial plan, in which the entry was made;
- *Category* – conversation recording category;
- *FTP* – whether uploading to FTP was performed;
- *Duration* – conversation duration;
- *Size*, *kB* – record size in kilobytes.

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 – caller number, if absent, set to none;

   CdPN – called 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 – 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 – called 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 A – B subscribers;

   Conversation between B – C subscribers;

   Conversation between A – C subscribers after the call transfer.

4. Making a call from the 'Hunt group'

   If the call to the subscriber comes after the call group, then an additional field is added to the record file with the information about the group through which the call to a member of this group was made.

   YYYY-MM-DD_HH-MM-SS_ CgPN - CdPN -CALLEDHG_nPLAN_cCATEGORY.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 – caller number, if absent, set to none;

   CdPN – called number – the number that actually receives the call.

   CALLEDHG – hunt group number;

   nPLAN – dial plan;

   cCATEGORY – call recording category.

5. Calling a subscriber through the 'Hunt group'

   YYYY-MM-DD_hh-mm_ss-CgPN-CdPN-hgPN_numplan_category.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 – caller number, if absent, set to none;

   CdPN – called number – the number that actually receives the call;

   hgPN – number of the subscriber who answered after passing through the hunt group;

   numplan – dial plan;

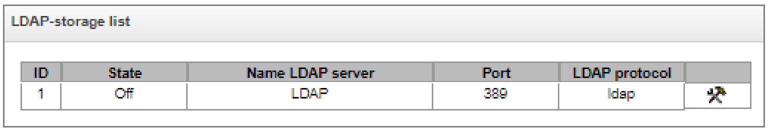
   category – call recording category.

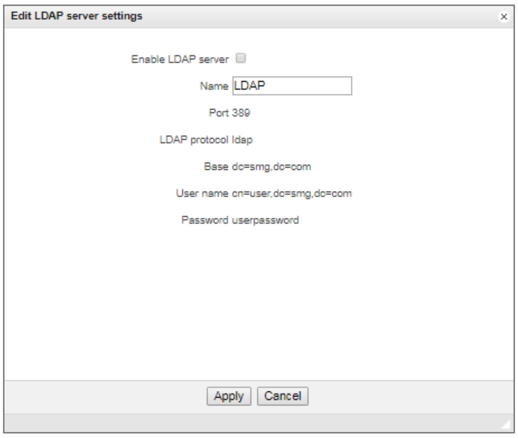
   Example:
   Subscriber 7111 is calling Subscriber 7222, who redirects the call to the subscriber 7333.
   The following files are generated:
   2014-05-20_12-05-35_7111_7222.wav – conversation of A and B subscribers.
   2014-05-20_12-06-36_7222_7333.wav – conversation of B and C subsribers, after subscriber B has put subscriber A on hold.
   2014-05-20_12-05-35_7111_7222ct7333.wav – conversation of A and C subscribers, after the subscriber B has redirected the call, ct in the file name is a label that the call was transferred.

3.1.10 LDAP

3.1.10.1 LDAP-storage list

This section allows configuring local LDAP server operation.





LDAP storage forms on the basis of station capacity (quantity of FXS, SIP subscribers).

Displayname = display name. If this field is empty in settings, ‘no_name’ value is displayed.

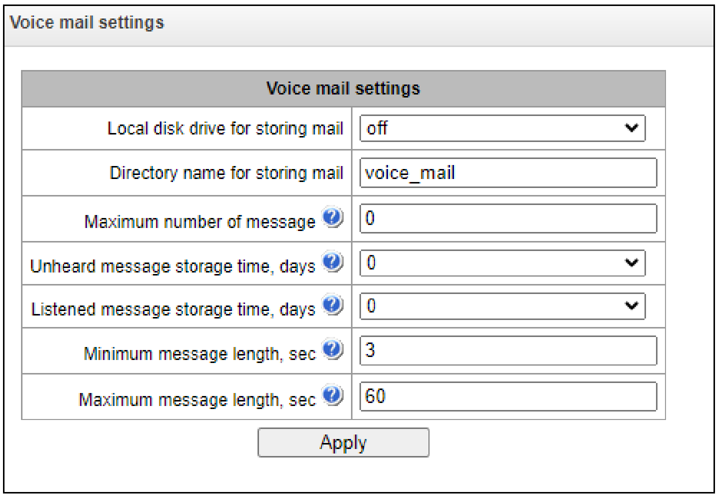
Uid = name
Cn = subscriber ID
Sn = displayed name
telephoneNumber = subscriber phone number

To connect to a local LDAP server, the following parameters are used:

Protocol Version = 3
Port: 389
LDAP protocol: ldap
Base: ou=phonebook,dc=smg,dc=com
User name: cn=user,dc=smg,dc=com
Password: userpassword

3.1.11 Voice mail

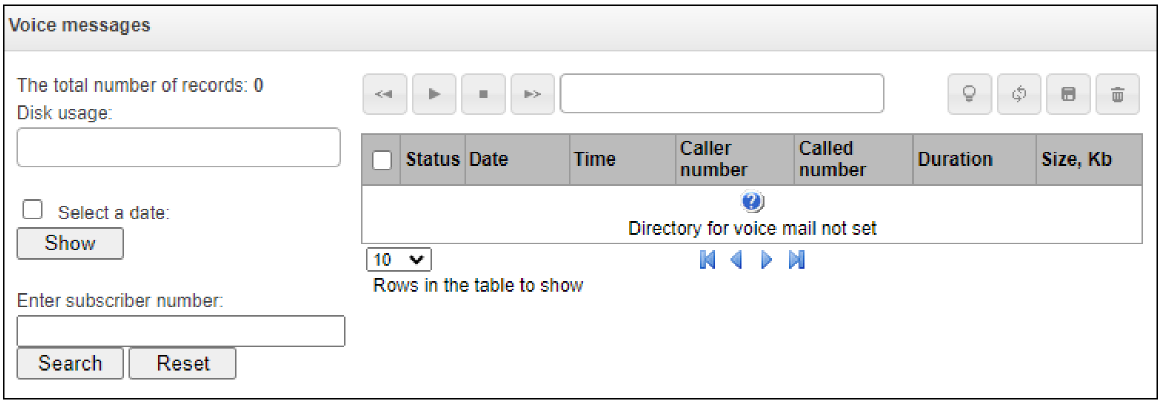
3.1.11.1 Voice mail settings



- *Local disk drive for storing mail* – specify an external storage medium for storing voice messages;
- *Directory name for storing mail* – specify the name of the folder where the voice messages will be stored;
- *Maximum number of messages* – maximum number of messages for one subscriber (range of valid values [0; 200] 0 – No restrictions);
- *Unheard message storage time, days* – storage time for unheard messages, after which the message will be deleted from the voice mailbox;
- *Listened message storage time, days* – storage time for listened messages, after which the message will be deleted from the voice mailbox;
- *Minimum message length, sec* – minimum duration of a message from a subscriber that can get into voice mail (if the record is shorter, the message will not be saved);
- *Maximum message length, sec* – maximum duration of a message from a subscriber that can get into voice mail (if the record is larger, the connection will be broken and only the recorded part will be saved).

3.1.11.2 Voice messages

In this section, it is possible to listen, download, delete, change the status of voice messages. Messages are grouped by the number on which the Voice Mail service is enabled.



- *Status* – indicates the message status:
  - – message is unheard;
  - – message is listened.
- *Date* – date of receiving a voice message;
- *Time* – time of receiving a voice message;
- *Caller number* – the subscriber who made the call to voicemail;
- *Called number* – subscriber number for which the ‘Voice mail’ service is enabled;
- *Duration* – voice message duration;
- *Size, Kb* – voice message recording file size.

Select message for change status – changes status from ‘Listen’ to ‘Unheard’ and vice versa;

Refresh table – updates the table with voice messages;

Download selected – downloads selected voice messages;

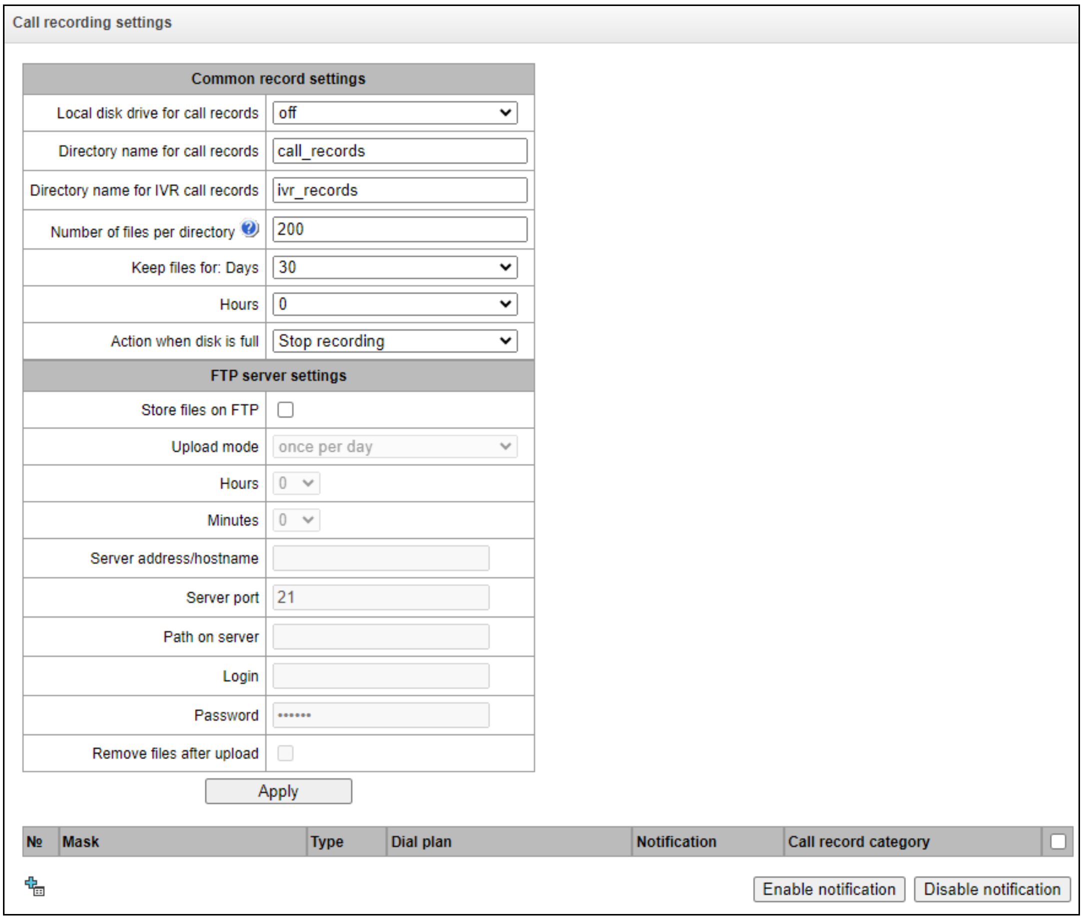
Delete selected – deletes the selected voice messages.

3.1.12 Call recording settings

Conversation recording settings menu[1].

The digital gateways SMG-200 and SMG-500 do not belong to special technical means designed to secretly obtain information.

3.1.12.1 Call recording settings



Common record settings:

- *Local disk drive for call records* – selects the available drive for saving conversation records;
- *Directory name for call 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;
- *Directory name for IVR call 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.

[1] The menu is available only in a firmware version with the Call-record license. For more information about the licenses, see section 3.1.23 Licenses.

In the conversation record directory, a new subdirectory is created for each day of recording under the following name:

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

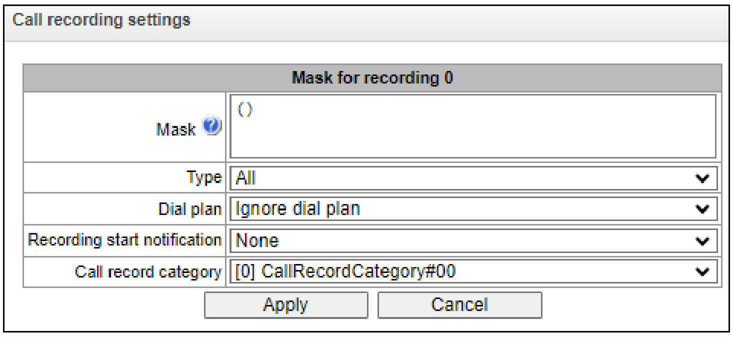
- *Keep files for* (days/hours) – the time period during which conversation record files will be stored on the drive; after this time period expires, old files will be deleted;
- *Action when disk is full* – select an action to be applied to conversation record files when the drive is full:
  - *Stop recording* – stop recording new conversations when the drive is full;
  - *Remove old records* – delete old conversation records when the drive is full.

FTP Server Settings:

- *Store files on FTP* – when this option is checked, conversation records will automatically be uploaded to the FTP server, according to the selected upload mode;
- *Upload mode* – determines how often the records will be uploaded to FTP:
  - once per day – uploading once a day at a given time;
  - once per hour – uploading every hour;
  - once per 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;
- *Server address/hostname* – the IP address or domain name of the FTP server to which conversation records will be uploaded;
- *Server port* – the FTP server port;
- *Path on server* – the path for saving files on the FTP server;
- *Login* – login for authorization;
- *Password* – password for authorization;
- *Remove files after upload* – 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 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 3.1.4.2 Description of Number Mask and Its Syntax;
- *Type* – search for a mask match by CdPN or CgPN number;

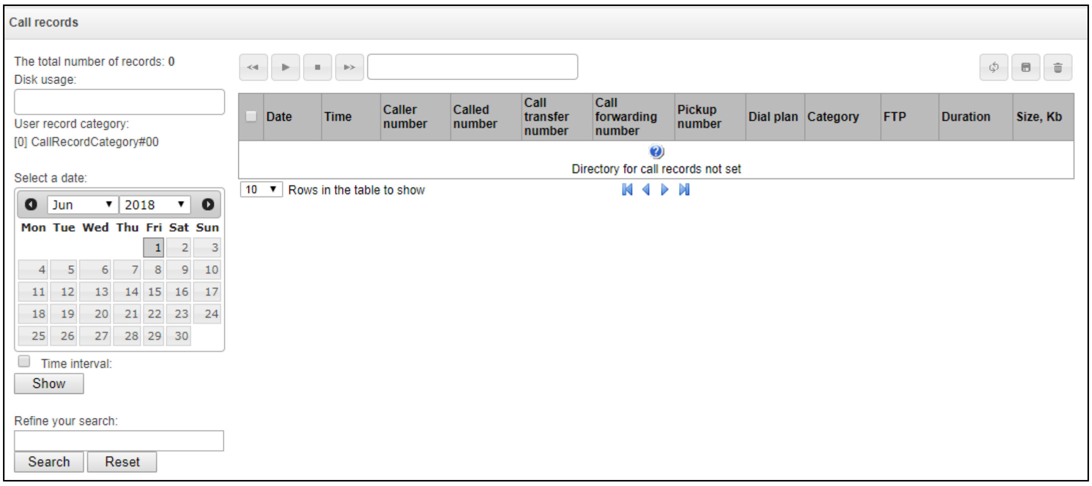
Please note that this setting uses OR logic, i. e. either CgPN or CdPN match is sufficient for the record identification.

  - *All* – search by CgPN and CdPN numbers;
  - *Calling* – search only by CgPN number;
  - *Called* – search only by CdPN number.

- *Dial plan* – specify the dial plan in which the call recording mask will work. If to select *Ignore dial plan*, a search will be done across all active dial plans;
- *Recording start notification* – notify the callee that the conversation will be recorded:
  - *None* – disable notification of recording start;
  - *Voice message* – voice notification of recording start.
- *Call record category* – a category assigned to the record for the specified mask.

3.1.12.2 Call records

In this section, conversation record files can be managed.



- *The total number of records* – total number of conversation record files in the selected directory;
- *Disk usage* – display the used space on the drive selected to store the conversation record files;
- *User record category* – display the conversation record category assigned to the current user of the web interface;
- *Select a date* – select the date to display conversation record files;
- *Time interval* – select the interval to display conversation record files;
- *Refine your search* – 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 14 – 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 called number;
   nX – the number of the dial plan 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 called 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 dial plan 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 A – B subscribers;
- Conversation between B – C subscribers;
- Conversation between A – C subscribers 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 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.

4. Making a call from ‘Call group’ (Hunt group)

If there is a call to a subscriber through a hunt group, the call record will have an additional filed — name of a call group which the call was established through.

YYYY-MM-DD_HH-MM-SS_ CgPN - CdPN -CALLEDHG_nPLAN_cCATEGORY.wav

YYYY-MM-DD – date of the record creation, YYYY – year, MM – month, DD – day;
hh-mm_ss – time of the record creation, hh – hour, mm – minutes, ss – seconds;
CgPN – calling party phone number, if there is no CgPN the field takes 'none' value;
CdPN – called party phone number – number which a call is actually directed;
CALLEDHG – call group number;
nPLAN – dial plan;
cCATEGORY – call record category.

3.1.12.3 Call record categories

Call record categories

№	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

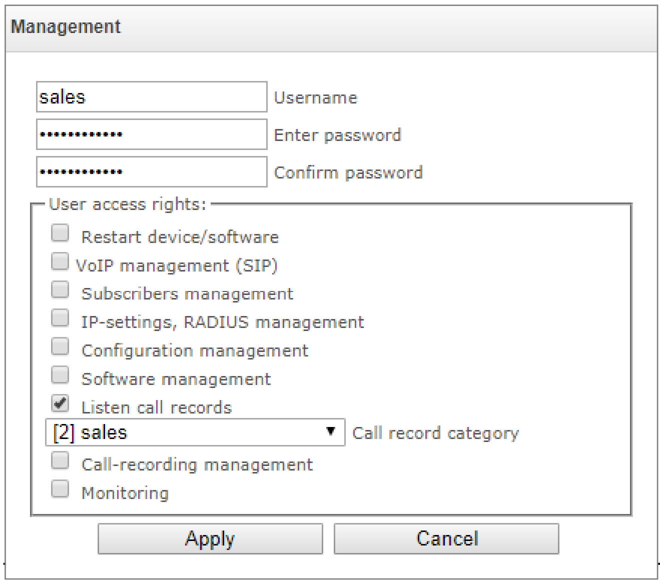
Consider an example when it is necessary to distinguish between access to the conversation records of the production department ("production user") and those of the sales department ("sales user"). Each user should be able to listen only to conversations of their relevant department. To restrict access, proceed as follows:

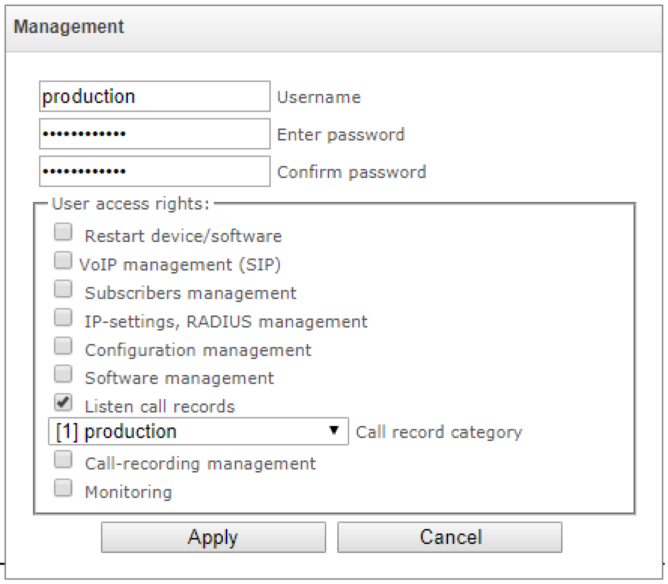
1. Select the access category for records. You can specify a convenient name, for example, *Production* or *Sales.* For each category, set access only to itself:

Call record categories

№	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	

Log in to the user account management interface (see section 3.1.25 Management Menu). 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*:





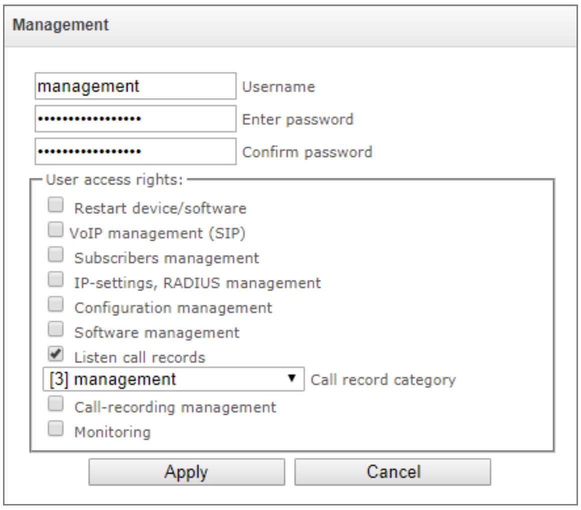
2. In the *Call recording settings* section, add the recording number masks for the production and sales departments, and assign the relevant recording categories to them.

№	Mask	Type	Dial plan	Notification	Call record category
0	(4xxx)	All	Ignore dial plan	None	[0] production
1	(3xxx)	All	Ignore dial plan	None	[1] sales

Enable notification Disable notification

3. Now, if the users enter the *Conversation Recording* section, they will only see records of the categories to which they have access.

4. 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.



As a result of these settings, the table of access restriction to conversation calls will look as follows:

Call record categories

№	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	

3.1.13 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.

3.1.13.1 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

№	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:

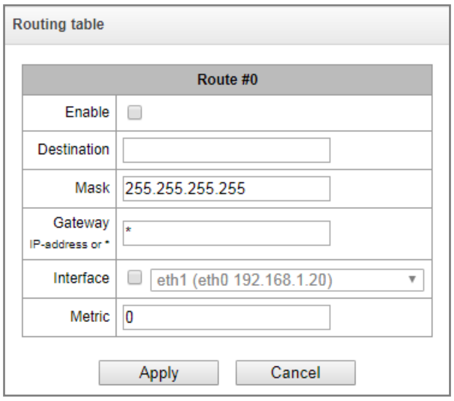
– Add route;

– Edit route parameters;

– Remove route.

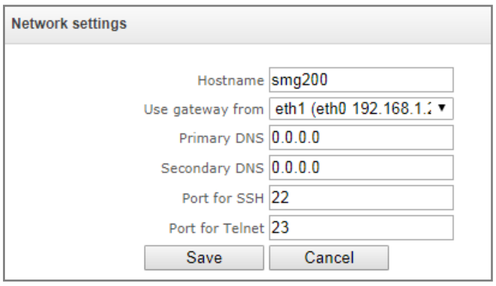
Route Parameters

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



3.1.13.2 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.

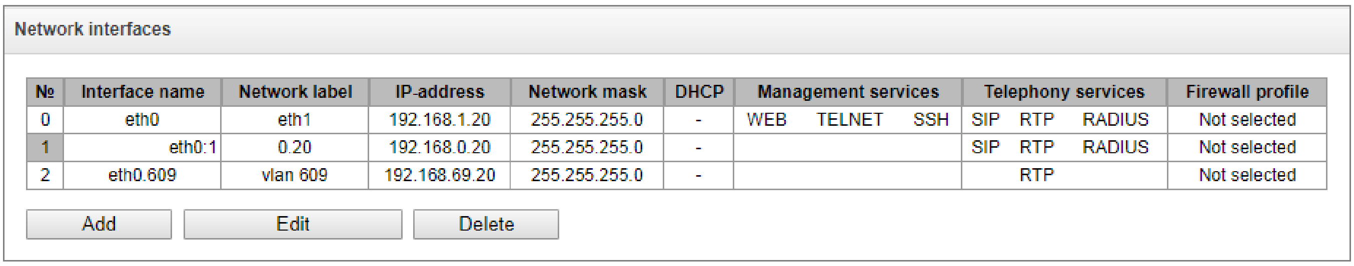


- *Hostname* – device network name;
- *Use gateway from* – selects the network interface to be used as the primary gateway of the device;
- *Primary DNS* – primary DNS server;
- *Secondary DNS* – secondary DNS server;
- *Port for SSH* – TCP port for device access via the SSH protocol; the default value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

3.1.13.3 Network Interfaces

It is possible to configure 1 primary network interface eth0 and up to 9 additional interfaces on the device. These can be VLAN interfaces and alias of the primary eth0 interface, or alias of the VLAN interface.

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



Network interfaces

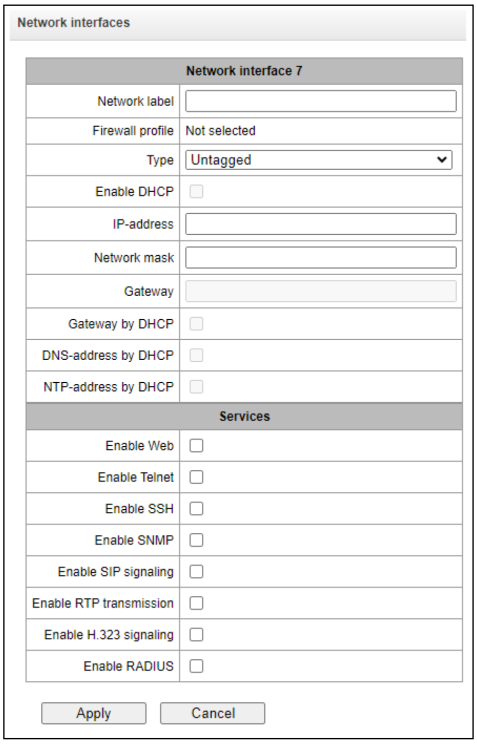
№	Interface name	Network label	IP-address	Network mask	DHCP	Management services	Telephony services	Firewall profile
0	eth0	eth1	192.168.1.20	255.255.255.0	-	WEB TELNET SSH	SIP RTP RADIUS	Not selected
1	eth0:1	0.20	192.168.0.20	255.255.255.0	-		SIP RTP RADIUS	Not selected
2	eth0.609	vlan 609	192.168.69.20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

Add Edit Delete

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

Network Interface Settings

Basic Settings



- *Network label* – name of the network;
- *Firewall profile* – show the firewall profile selected for this interface;
- *Type* – interface type (always untagged for eth0 interface);
- *VLAN ID* – VLAN identifier (1–4095) (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;
- *Network mask* – the subnet mask of the device;
- *Gateway* – network gateway for the interface (Alias is not supported);
- *Gateway by DHCP* – obtain the IP address of the gateway dynamically from the DHCP server (Alias is not supported);
- *DNS-address by DHCP* – obtain the IP address of the DNS server dynamically from the DHCP server (Alias is not supported);
- *NTP-address by DHCP* – obtain the IP address of the NTP server dynamically from the DHCP server (Alias is not supported).

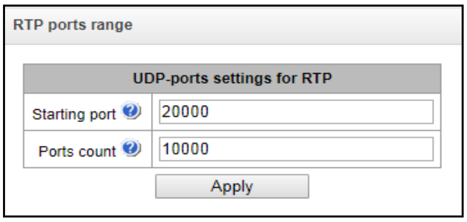
Services – a configuration menu for the services enabled for this interface:

- *Enable Web* – enables access to the configurator via the interface;
- *Enable Telnet* – enables access via the Telnet protocol;
- *Enable SSH* – enables access via the SSH protocol;
- *Enable SNMP* — enables access via the SNMP protocol*;*
- *Enable SIP signalling* – enables reception and transmission of the SIP signalling information through the network interface configured in this section;
- *Enable RTP transmission* – enables reception and transmission of the voice traffic through the network interface configured in this section;
- *Enable H.323 signaling* – enables reception and transmission of H.323 signalling data 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.

3.1.13.4 RTP Ports Range

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



UDP Port Parameters

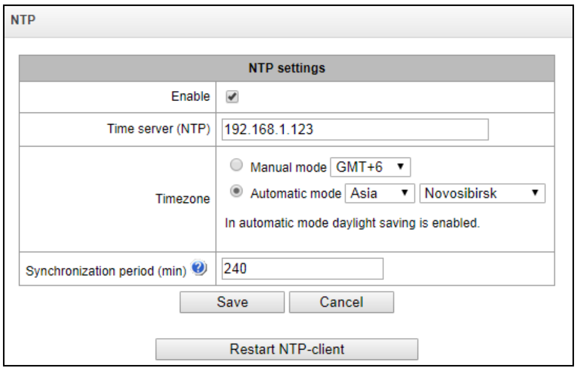
- *Starting port* – the number of the starting UDP port for voice traffic (RTP) and data transmission via the T.38 protocol;
- *Ports count* – the quantity of UDP ports (from the strating port) used for voice traffic (RTP) and data transmission via the T.38 protocol.

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).

3.1.14 Network Services

3.1.14.1 NTP

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



- *Enable* – enables time synchronization 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.
- *Synchronization period (min)* – an interval between synchronisation requests;
- *Save* – saves changes;
- *Cancel* – discards changes.

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

3.1.14.2 SNMP setting

SMG software enables to monitor status of the device via SNMP. In *SNMP* submenu, the settings of the SNMP agent can be configured.

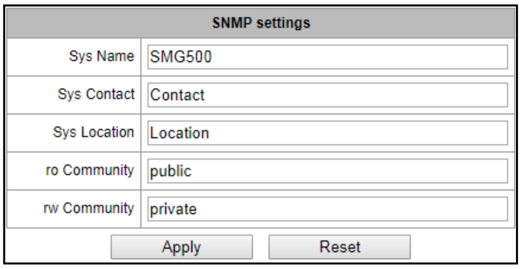
SNMP monitoring functions are able to request the following gateway parameters:

- 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;
- Called MAC address;
- Called IP address;
- Called number;
- Channel engagement duration.

SNMP settings:



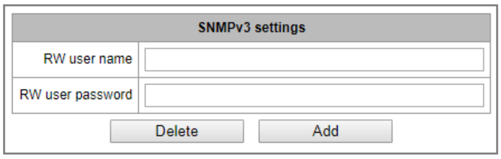
- *Sys Name* – device name;
- *Sys Contact* – contact information;
- *Sys Location* – device location;
- *ro Community* – parameter read password/community;
- *rw Community* – parameter write password/community.

Use *'Apply'/'Reset'* button to apply/reset the settings.

3.1.14.3 SNMPv3

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).

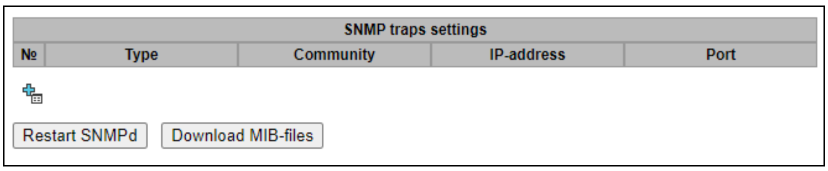
To apply SNMPv3 user configuration, click *'Add'* button (settings will be applied immediately). To remove a record, click *'Remove'* button.

3.1.14.4 SNMP trap settings

For detailed information about the monitoring parameters and Traps, see MIB files.

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

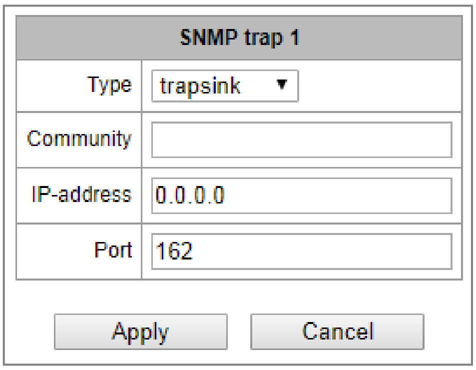
- Configuration error;
- SIP module failure;
- IP submodule failure;
- Linkset failure;
- SS7 signal channel failure;
- Synchronization loss or synchronization from the lower priority source;
- E1 stream failure;
- Remote E1 failure;
- Configuration error is corrected;
- SIP-T module normal operation 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.



- *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:

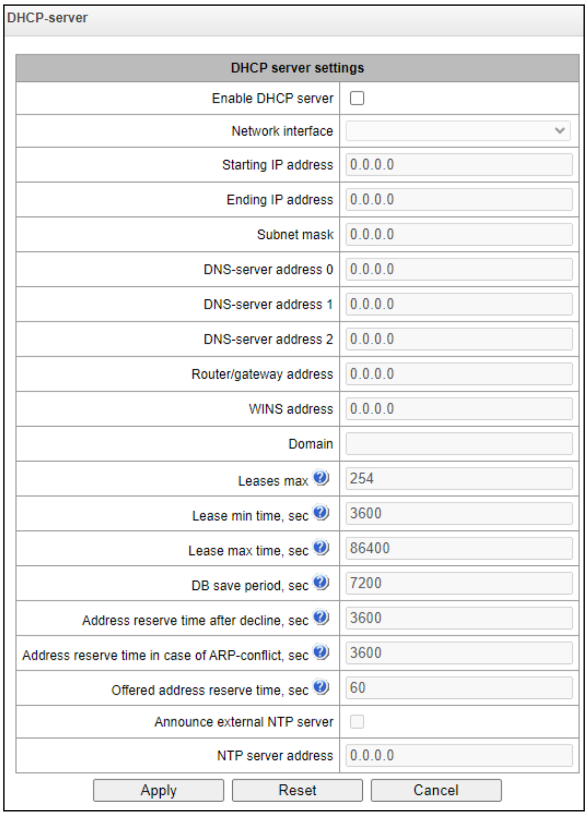
– Add;
– Edit;
– Remove.



- *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).

3.1.14.5 DHCP server

The Dynamic Host Configuration Protocol (DHCP) host configuration protocol automatically assigns IP addresses to network devices. Upon receiving a request, the DHCP server chooses an IP address from a pool of addresses in its database and offers it to the DHCP client. If DHCP client accepts the offer, then the network settings, i.e. IP-address, mask and other parameters are leased to the client for a certain period.



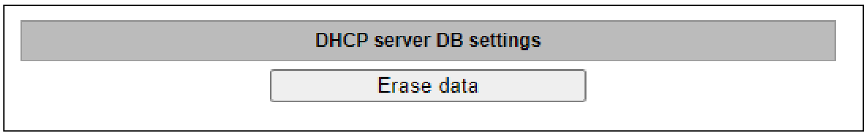
DHCP server settings:

- *Enable DHCP server* – if this checkbox is set, the DHCP server is started at the gateway startup;
- *Network interface* – selects a network interface for a DHCP server;
- *Starting IP address* – the starting address of assigned IP address range;
- *Ending IP address* – the ending address of assigned IP address range;
- *Subnet mask* – subnet mask;
- *DNS-server address 0/1/2/3* – addresses of DNS servers in the operator's network;
- *Router/gateway address* – router/gateway address;
- *WINS address* – IP address of the WINS server in the operator's network;
- *Domain* – network domain name;
- *Leases, max* – setting a limit on the number of simultaneously leased addresses;
- *Lease min time, sec* – setting the minimum time for the client to use the IP address assigned by the DHCP server, at least 10 seconds;
- *Lease max time, sec* – setting the maximum time for the client to use the IP address assigned by the DHCP server, from 10 to 10 000 000 seconds;

- *DB save period, sec* – the period of time after which the device will save information about leased addresses to the dhcpd.leases file. Use ‘off’ so that not to store information about leased addresses;
- *Address reserve time after decline, sec* – the period of time for which the IP address will be reserved for the client in case of receiving a rejection message (DHCP decline), at least 10 seconds;
- *Address reserve time in case of ARP-conflict, sec* – the period of time for which the IP address will be reserved for the client in case of a MAC address conflict, at least 10 seconds;
- *Offered address reserve time, sec* – the period of time for which the IP address requested by the client will be reserved, at least 10 seconds;
- *Announce external NTP server* – when this option is enabled, the DHCP server will announce in option 42 server addresses specified in the ‘*NTP server address’* option;
- *NTP server address* – the address of the NTP server that the SMG will advertise in option 42 if the ‘*Announce arbitrary NTP server*’ option is enabled.

DHCP server management:

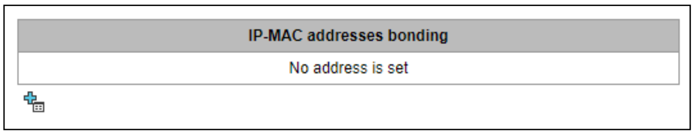
- *Start server* – to start DHCP server;
- *Stop server* – to stop DHCP server;
- *Erase data* – to delete established IP-MAC mappings in the DHCP server memory.

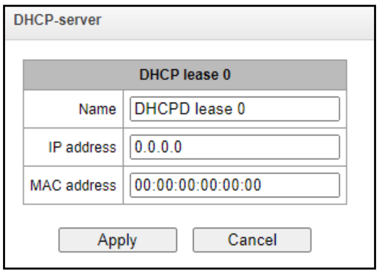


IP-MAC addresses bonding – assignment of static mappings of IP and MAC addresses.

To assign a new correspondence to editing and deleting parameters, use the buttons:

- *Add*;
- *Edit*;
- *Delete*.

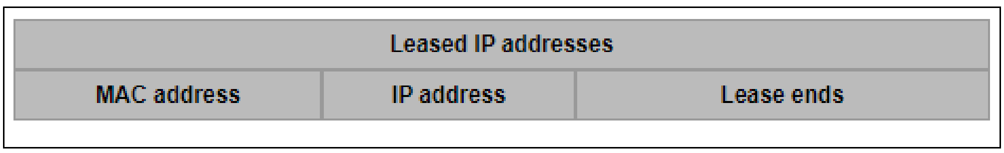




- *Name* – correspondence name;
- *IP address* – client’s IP address;
- *MAC address* – client’s MAC address.

Leased IP address:

- *MAC address* – client’s MAC address;
- *IP address* – an address issued from a pool of IP addresses;
- *Lease ends* – the time after which the lease of this address expires.
  - *Expired* – address lease has expired.

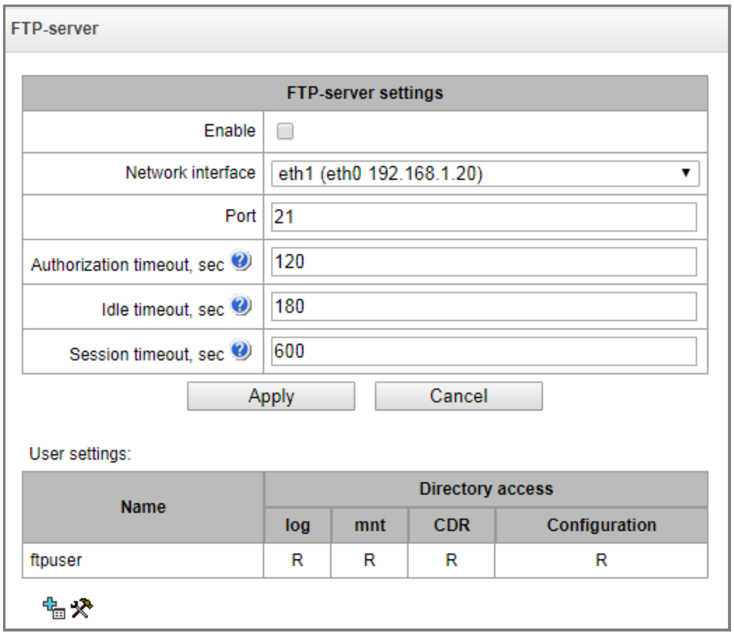


3.1.14.6 FTP Server

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).

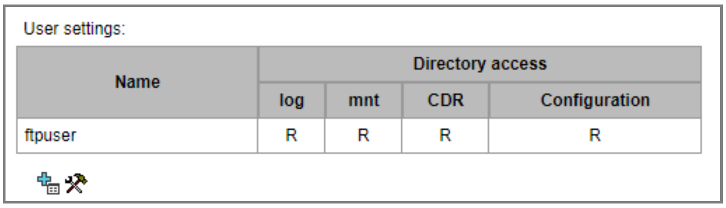
FTP Server Settings



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

User Settings

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

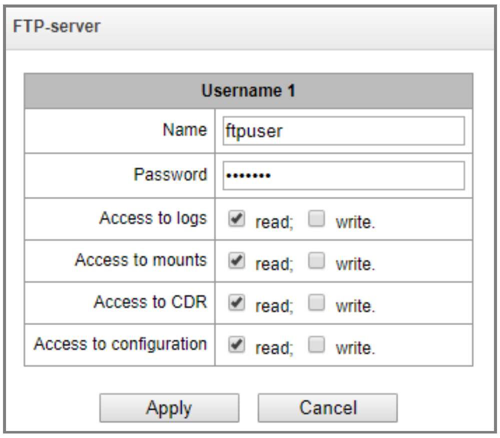


User settings:

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:

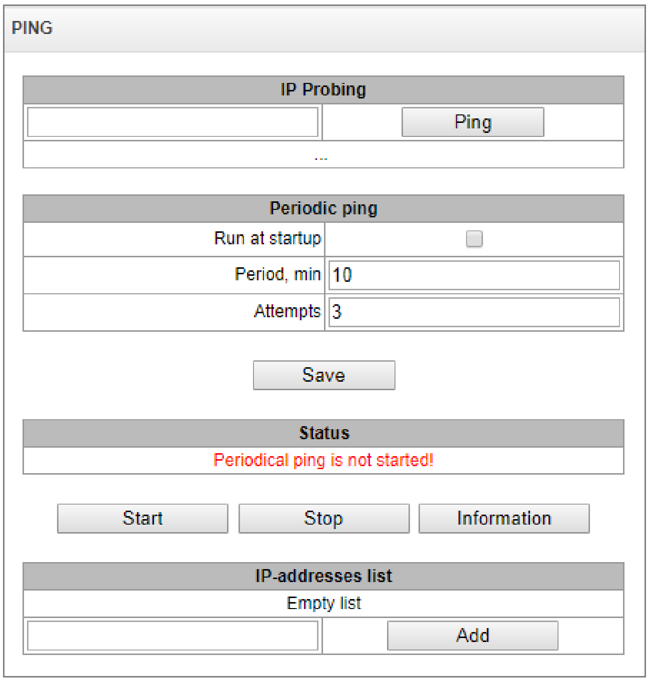


- *Name* – username;
- *Password* – user password;
- *Access to logs* – log directory access configuration, read/write;
- *Access to mounts* – mnt directory access configuration, read/write;
- *Access to CDR* – CDR directory access configuration, read/write;
- *Access to configuration* – /etc/config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

3.1.15 Network Utilities

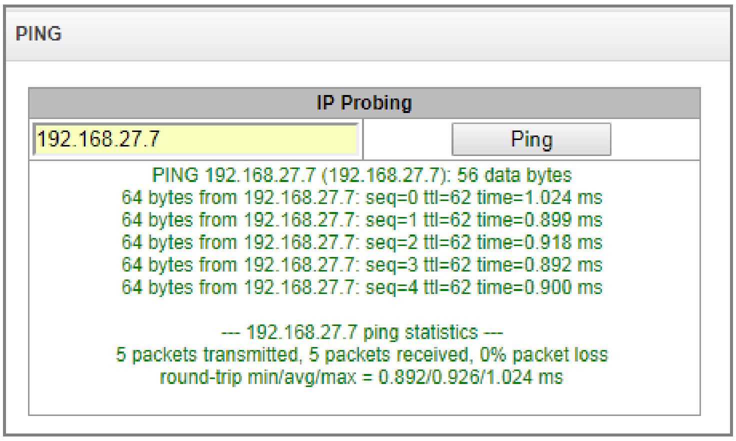
3.1.15.1 PING

This utility is used to check device network connection (route presence).



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.



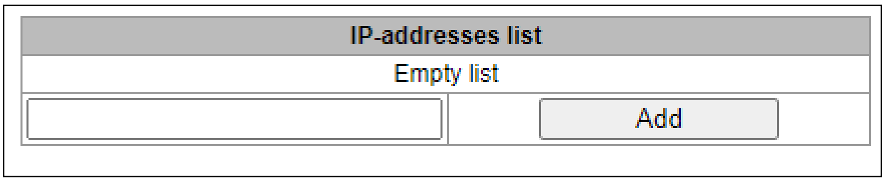
Periodic ping – used for periodic check of device network connection.

- *Run at startup* – the option enables a periodic ping after restarting the device;
- *Period, min* – the time interval between requests in minutes.
- *Attempts* – the number of attempts to send a request to an address.

Status

- *Start* – starts/restarts periodic ping;
- *Stop* – forcibly stops periodic ping;
- *Information* – click this button to view the '/tmp/log/hosttest.log' log file which contains data on the last attempt of periodic ping request transmission.

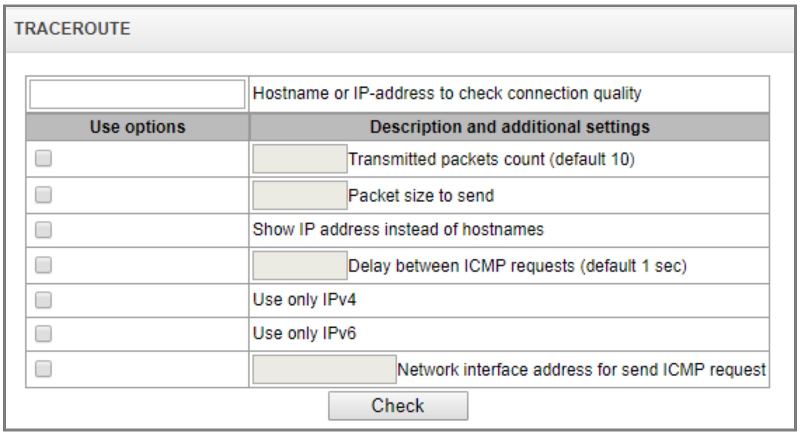
IP addresses list – a list of IP addresses to send periodic ping requests to.



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.

3.1.15.2 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.



In the '*Hostname or IP address to check 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:

- *Transmitted packets count (default 10)* – the number of the ICMP request transfer cycles;
- *Packet size to send* – the ICMP packet size in bytes;
- *Show IP address instead of hostnames* – do not use DNS. Display the IP address without trying to obtain their network names;
- *Delay between ICMP requests (default 1 sec)* – polling interval;
- *Use only IPv4*– use only IPv4 protocol;
- *Use only IPv6*– use only IPv6 protocol;
- *Network interface address for send ICMP request* – IP address of the network interface from which ICMP requests will be sent.

Having entered the IP address of the network device for which the connection quality is evaluated, set the options and click the *'Check'* button.

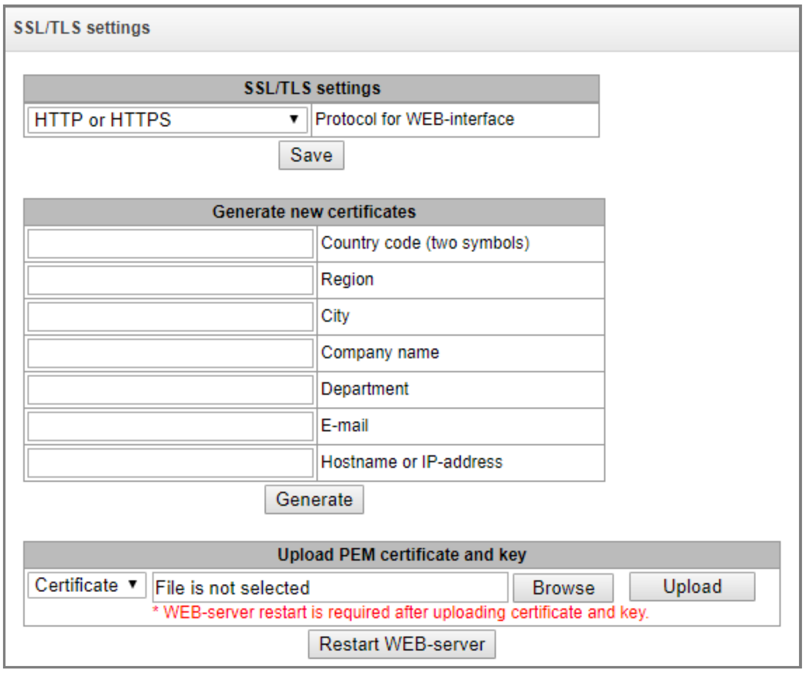
As a result, the utility displays a table containing:

- 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

3.1.16 Security

3.1.16.1 SSL/TLS settings



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.

- *Protocol for WEB-interface* – 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.

- *Country code (two symbols)* – country code (RU for Russia);
- *Region* – region name;
- *City* – city name;
- *Company name* – organization name;
- *Department* – name of the organization unit or division;
- *E-mail* – e-mail address;
- *Hostname or IP address* – IP address of the gateway.

Upload PEM Certificate and Key

In this section, the pre-generated and signed PEM certificate and key can be uploaded. 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.

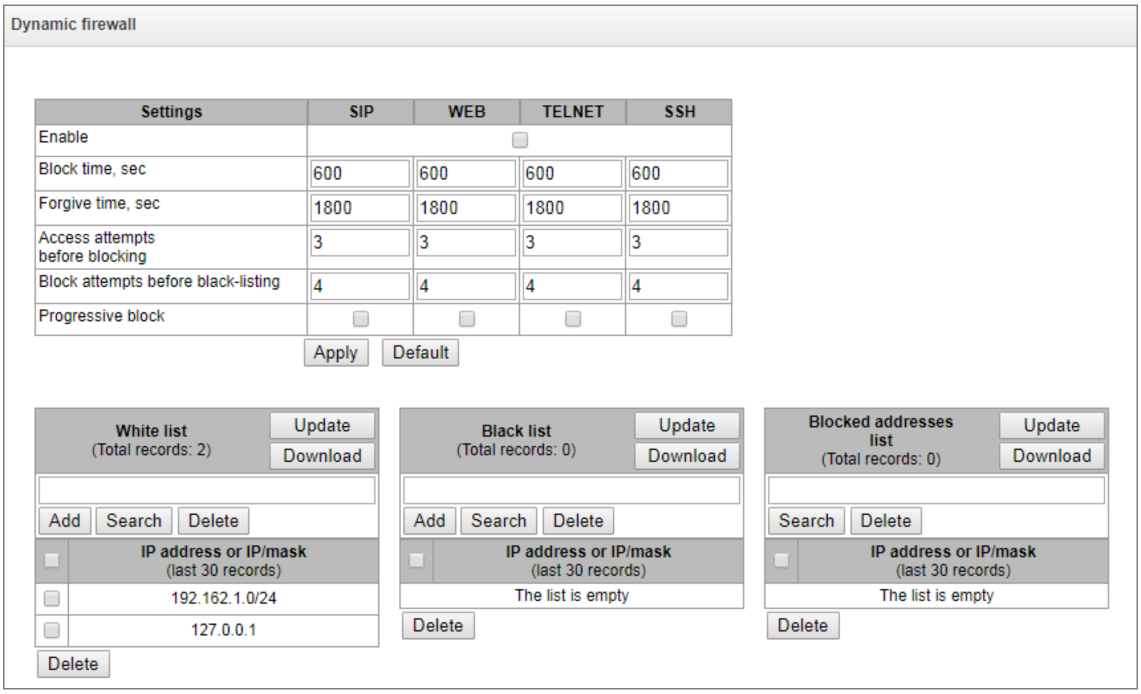
After the certificate and key are loaded, the web server should be restarted with the '*Restart Web-server*' button.

3.1.16.2 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.



Parameters:

- *Enable* – start the dynamic firewall utility;
- *Block time, sec* – time in seconds during which access from a suspicious address will be banned;
- *Forgive time, sec* – time after which the address initiating the problem query will be forgotten, in case it has never been blocked before;
- *Access attempts before blocking* – the maximum number of unsuccessful service access attempts before the host is banned by dynamic firewall;
- *Block attempts before black-listing* – the number of bans after which the problem address will be forcibly blacklisted;
- *Progressive block* – when this option is checked, each new address ban will be twice 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 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.

Blocked addresses list – a list of addresses banned by the dynamic firewall. A total of 8192 entries can be created on SMG-200/SMG-500.

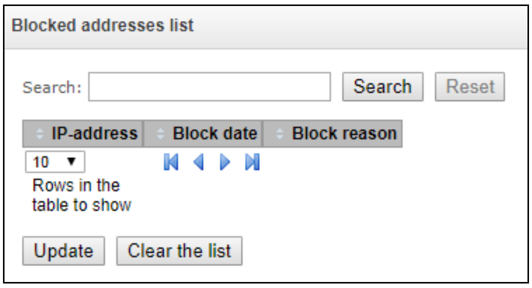
- *Download* – allows download of the entire list of banned addresses to PC.

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

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

3.1.16.3 Blocked addresses list

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



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

Table

- *IP-address* – IP address that was blocked;
- *Block date* – date and time when the IP address was blocked;
- *Block reason* – explanation which service imposed the block and why.

Buttons

- *Update* – update the banned address log;
- *Clear the list* – remove all entries from the blocked addresses list.

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

Table 15 – Blocked 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 where To and From headers are different	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 fail authentication	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

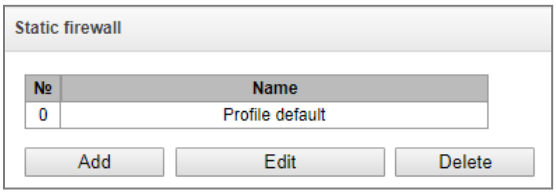
3.1.16.4 Static Firewall

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 unauthorized access.

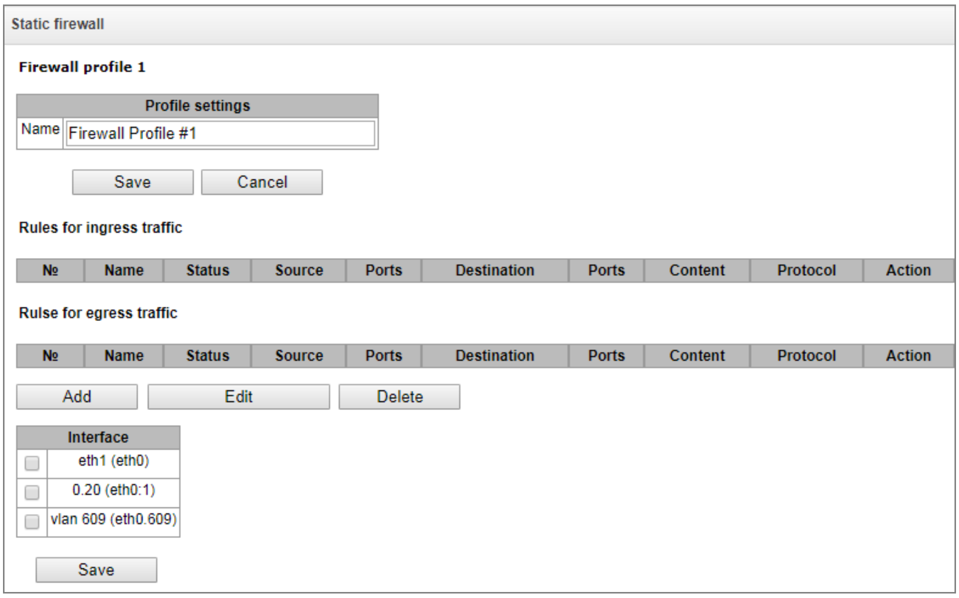
Firewall Profiles

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

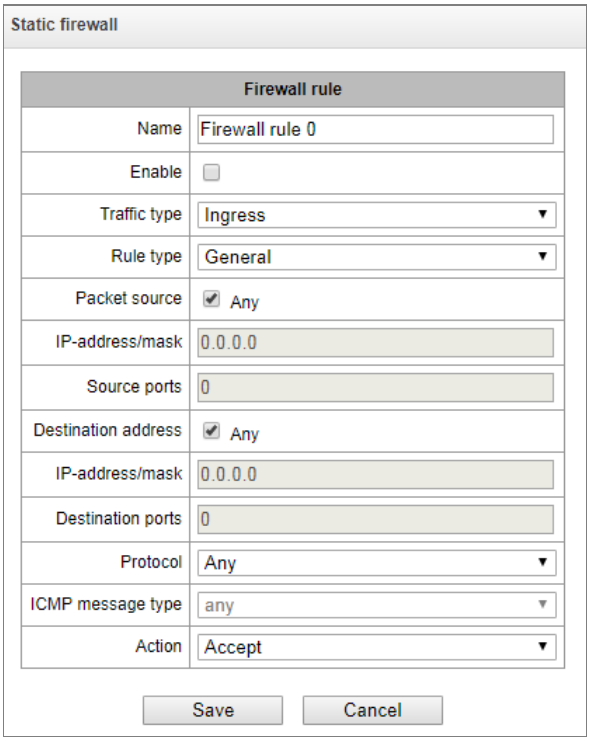
- *Add*;
- *Edit*;
- *Remove*.

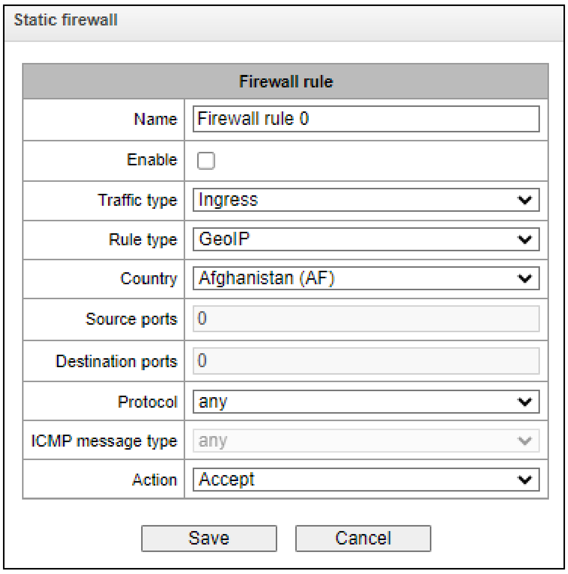


The software allows configuration of firewall rules for incoming, outgoing and transit traffic, as well as for specific network interfaces.



When a rule is created, the following parameters are configured:





- *Name* – rule name;
- *Enable* – defines whether the rule is used; цhen this option is unchecked; the rule is inactive;
- *Traffic type* – type of traffic for the rule being created:
  - *ingress* – intended for SMG;
  - *egress* – sent by SMG.
- *Rule type* – can take values:
  - *General* – 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* – defines 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* – defines 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;

- *ICMP Message type* – 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* – selects the country to which the address belongs. The field is displayed only for the GeoIP 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*'.

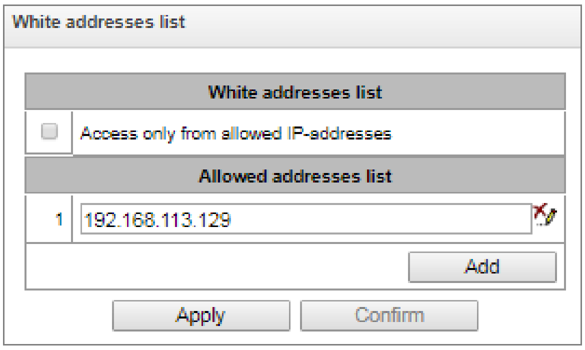
Also, in the *firewall* profile, one can specify network interfaces that these profile rules will be applied to.

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.

3.1.16.5 White addresses list

In this section, one 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 only from allowed IP addresses* – when this option is checked, the list of allowed IP addresses is used; otherwise, access is allowed from any address.

It is possible to enable access for subnets by setting an IP/mask address, for example: 192.168.0.0/24.

- *Apply* – apply changes;

- *Confirm* – 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 *'Confirm'* 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.

3.1.16.6 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 3.1.16.2) is performed. On this stage, requests received from IP addresses located on the blacklist will be dropped.

2. Processing of access limitations (see section 3.1.13.3 Network Interfaces -> Services and 3.1.16.5 White addresses list).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 3.1.16.4) 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.

3.1.16.7 Providing SMG firewall tasks

Restriction of WEB/Telnet/SSH/SNMP administration privileges.

To restrict the access to management, use 3.1.13.3 Network Interfaces -> Services and 3.1.16.5 White addresses list. 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 3.1.16.4).

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:

1. The rule for incoming traffic with ‘GeoIP’ type and ‘Russian Federation (RU)’ country. Action _ Accept.
2. The rule for outgoing traffic with ‘General’ type and IP address/source mask: 34.92.128.128/255.255.255.240. Action – Accept.
3. 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.

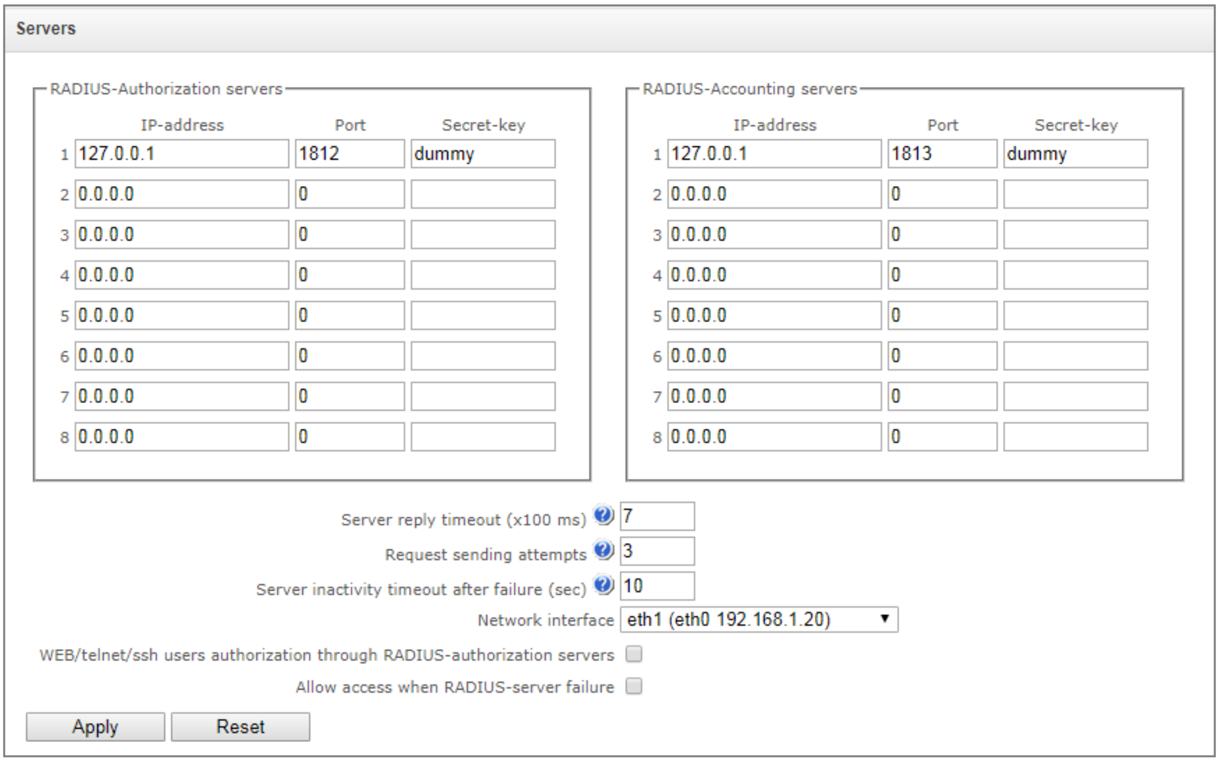
In order to implement access restriction to SMG from a certain address or subnet, it is necessary to activate the dynamic firewall (see section 3.1.16.2) and enter address or subnet in the black list. Pay attention, if there are too many addresses, it is better to create static firewall rules (see section 3.1.16.4) 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 3.1.16.5).

Automatic blocking of failed requests/authorizations.

The dynamic firewall (see section 3.1.16.2) 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.

3.1.17 RADIUS Configuration

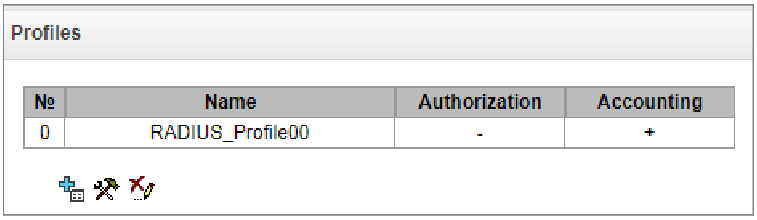
3.1.17.1 RADIUS Servers



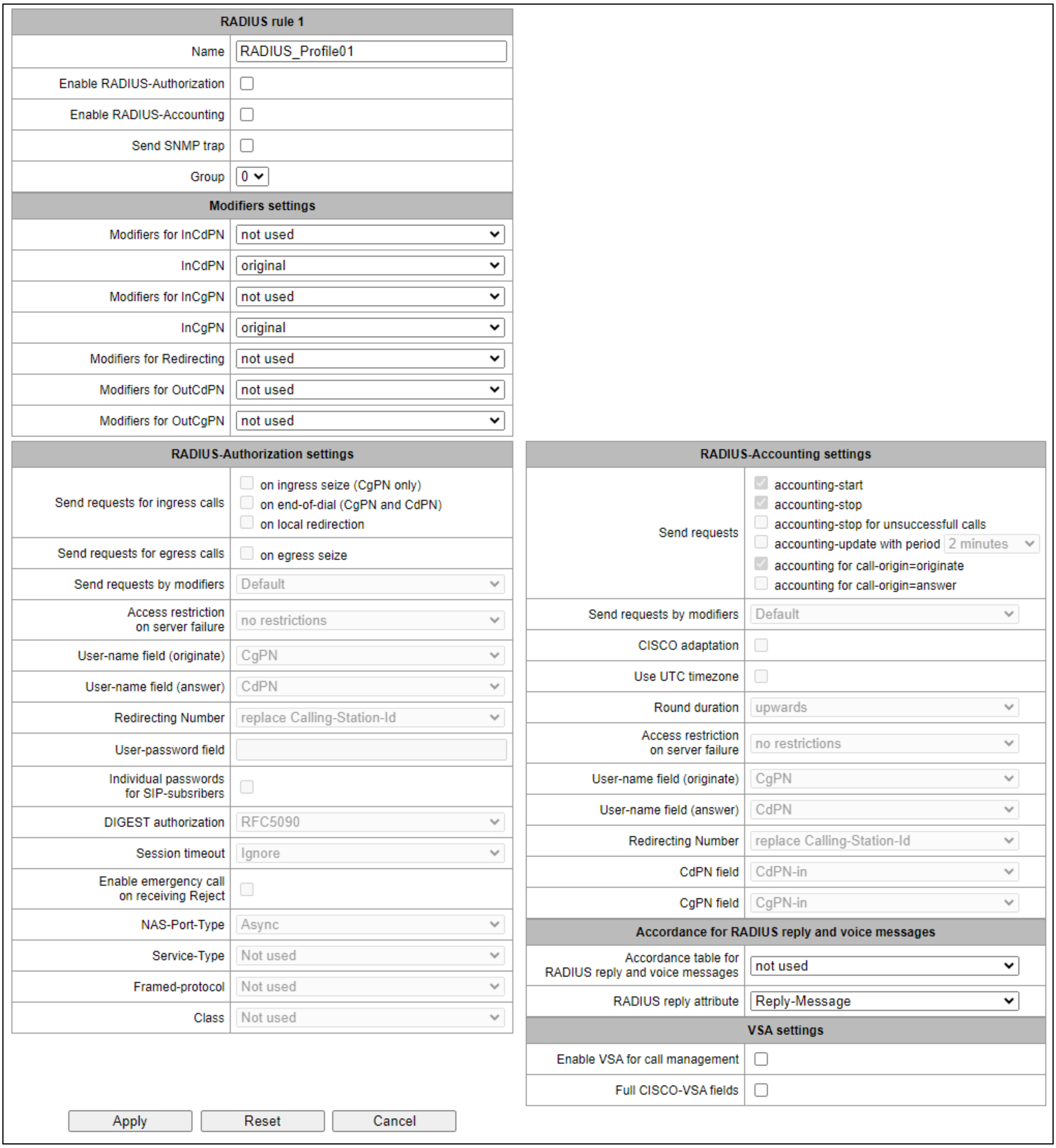
The device supports up to 8 authorization servers and up to 8 accounting servers. The servers can be grouped, and then when configuring RADIUS profiles it is possible to select server group that will be used for sending requests. Four groups are available.

- *Server reply timeout (x100 ms)* – amount of time to wait for a server response;
- *Request sending 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 inactivity timeout after failure (sec)* – amount of time when a server is deemed unavailable (requests will not be sent to it);
- *Network interface* for *group <N>* – selecting network interface through which RADIUS requests will be sent for the corresponding group;
- *WEB/telnet/ssh users authorization through RADIUS-authorization servers* – when the user logs on via WEB/telnet/ssh, authorization will be performed on the RADIUS server. First, create local users with appropriate names and configure their access rights (see section 3.1.25 Management);
- *Allow access when RADIUS-server failure* – if the authorization 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.

3.1.17.2 Profile List



Profile Parameters



- *Name* – profile name;
- *Enable RADIUS-Authorization* – enables/disables the transmission of authentication/uthorization (Access Request) messages to the RADIUS server;
- *Enable RADIUS-Accounting* – enables/disables the transmission of accounting (Accounting Request) messages to the RADIUS server;
- *Send SNMP trap* – enables sending SNMP traps every time a RADIUS request is sent.
- *Group* – group of RADIUS servers used for sending requests.

Modifiers settings

- *Modifiers for InCdPN* – selects called (CdPN) number modifier for the incoming connection in relation to the Called-Station-Id, xpgk-dst-number-in fields of RADIUS-Authorization and RADIUS-Accounting messages;
- *InCdPN* – selects the number to be sent to the xpgk-dst-number-in field in the RADIUS-Authorization 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.
- *Modifiers for InCgPN* – selects caller (CgPN) number modifier for the incoming connection in relation to the Calling-Station-Id, xpgk-src-number-in fields of RADIUS-Authorization and RADIUS-Accounting messages;
- *InCgPN* – selects the number to be sent to the xpgk-dst-number-in field in the RADIUS-Authorization 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.
- *Modifiers for Redirecting* – selects a redirect number modifier (RedirPN) in the h323-redirect-number field in the RADIUS-Authorization and RADIUS-Accounting messages;
- *Modifiers for OutCdPN* – selects called (CdPN) number modifier for the outgoing connection in relation to the xpgk-src-number-out field of RADIUS-Authorization and RADIUS-Accounting messages;
- *Modifiers for OutCgPN* – selects caller (CgPN) number modifier for the outgoing connection in relation to the xpgk-dst-number-out field of RADIUS-Authorization and RADIUS-Accounting messages.

RADIUS-Authorization settings

Authentication/authorization requests can be transmitted during various call phases:

- on ingress seize (CgPN);
- on end of dialing (getting the full number of the dialing);
- on local redirection;
- on egress seize.

The call checking function in RADIUS can be restricted based on the modifier mask. To do this, select one or more modifiers in the *Modifiers settings* section and set the *Send requests by modifiers* option to *Restrict*. In this case, an authorization 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 the authentication request restrictions based on the modifiers is enabled, the calls from numbers that are not included in the mask modifier will be automatically authorized.

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 network only* – allow calls to special services, private, local and zone network;
- *local network only* – allow calls to special services, private and local network;
- *emergency only* – allow calls to special services only;
- *deny all (disconnect)* – deny all calls.

This restriction governs call routing by a prefix controlling the corresponding call type (local, long-distance, etc.).

- *User-name field (originate)* – select value of the User-Name attribute in the corresponding Access Request authorization packet (RADIUS-Authorization):
  - *CgPN* – use the calling phone number as the value;
  - *CdPN* – use the called 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;
  - *Initial CgPN* – initializing calling party number;
  - *Initial CdPN* – initializing called party number;
  - *Login* – use SIP subscriber authorization login.
- *Redirecting Number* – Redirection number processing options:
  - *Replace Calling-station-ID* – in this case, the Redirection number is replaced in the Calling-station-ID field and transmitted as the caller number;
  - *Send as 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-Authorization packet;
- *Individual passwords for SIP-subscribers* – when this option is checked, custom passwords of SIP subscribers are used for authentication/authorization, instead of the password configured in the USER-PASSWORD field;
- *DIGEST authorization* – select the subscriber authorization 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:
  - *RFC5090* (full implementation of the RFC4590 recommendation);

- *RFC5090-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 RFC5090 recommendation was written);

- *Session timeout* – limits the maximum call duration:
  - *Ignore* – the maximum call duration is not limited;
  - *Consider Session-Time* – use the Session-Timeout(27) value to limit the maximum call duration;
  - *Consider Cisco h323-credit-time* – use the Cisco VSA (9) h323-credit-time(102) value to limit the maximum call duration;
  - *Priority Session-Time* – 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;
  - *Priority Cisco h323-credit-time* – 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 authorized call.

- *Enable emergency call on receiving Reject* – 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 utilization, 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 settings

- 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 RADUIS 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 *Modifiers settings* section and set the *Send requests by modifiers* option to *Restrict*. 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;
- *Use UTC timezone* – send the time in the RADIUS-Accounting messages in UTC format;
- *Round duration* – 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.).

- *User-name field* – select User-Name value in an Accounting Request packet (RADIUS-Accounting):
  - *CgPN* – use the caller phone number as the value;
  - *CdPN* – use the called 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;
  - *Initial CgPN* – initializing calling party phone number;
  - *Initial CdPN* – initializing called party phone number;
  - *Login* – use SIP subscriber authorization login.
- *Redirecting Number* – transmission mode for RedirPN to RADIUS:
  - *replace Calling-Station-Id* – RedirPN will be transmitted to the Calling-Station-Id field by rewriting an existing value;
  - *send as h323-redirect-number* – RedirPN will be sent separately into the h323-redirect-number field.
- *CdPN field* – select value of the called number used for RADIUS packet generation for specific Attribute-Value pairs (see section 3.1.17.5):
  - *CdPN-in* – use the called number prior to modification (the number received in the SETUP/INVITE request);
  - *CdPN-out* – use the called 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 3.1.17.5):

- *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.

Accordance for RADIUS reply 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.

- *Accordance table for RADIUS reply and voice messages* – select a table of correspondence between RADIUS-reject responses and voice messages;

- *RADIUS reply attribute* – select an attribute that will be used for the analysis of a RADIUS-reject message.

VSA settings

- *Enable 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 I. RADIUS CALL MANAGEMENT SERVICE.

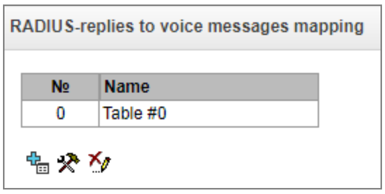
- *Full CISCO-VSA fields* – transmit full attribute names in the CISCO-VSA fields.

Passing 'real ip' to RADIUS-Accounting

Upon receiving real ip parameter in the *INVITE* message in the From field, this field will be transferred to the Framed-Ip-Address (8) RADIUS-Accounting.

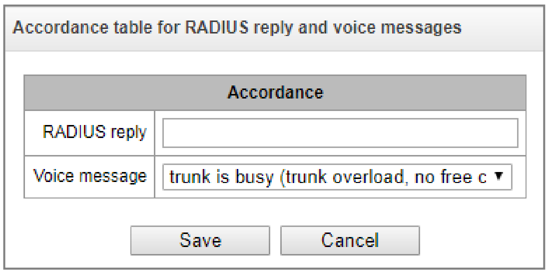
3.1.17.3 RADIUS-replies to voice messages mapping

In this section, the correspondence between RADIUS-reject responses and voice messages sent to subscribers can be configured.



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 reply* – 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.

3.1.17.4 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 3.1.17.5 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.

3.1.17.5 Variable Description

Table 16 – Variable Description

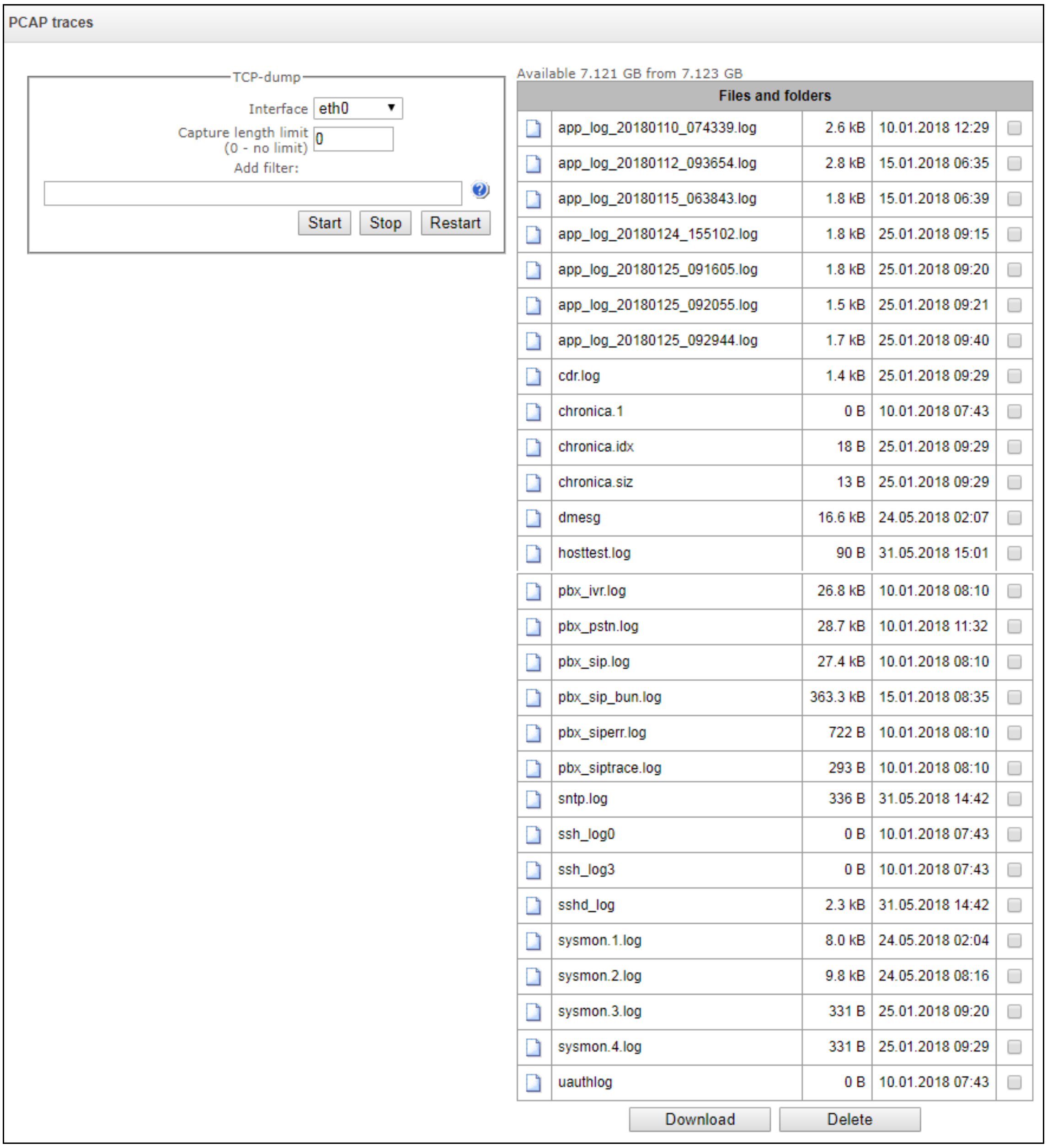
Variable	Description and Possible Values
$CALL_TYPE	Is defined depending on the transmission medium to which the outgoing trunk belongs: • *Telephony*, if the outgoing trunk is PSTN (TDM); • *VoIP*, if the outgoing trunk is VoIP.
$CdPN	Is defined based on SMG settings: • $CdPN = $CdPN_IN [by default]; • $CdPN = $CdPN_OUT
$CdPN_IN	Called 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: • 1 – connection to the called 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 called is busy (User-Busy); • 6 – equipment fault (Out-of-Order); • 7 – no response from the called (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)
$USER_NAME	Determined from incoming trunk settings: • <$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

3.1.18 Tracing

3.1.18.1 PCAP Tracings

This menu allows configuration of network traffic analysis and the TDM protocol.



TCPdump – settings of the TCP–dump utility:

TCPdump is a utility designed to pick up and analyze network traffic.

- *Interface* – an interface for network traffic pickup;
- *Capture 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, **fddi1**, **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 specialized resources.

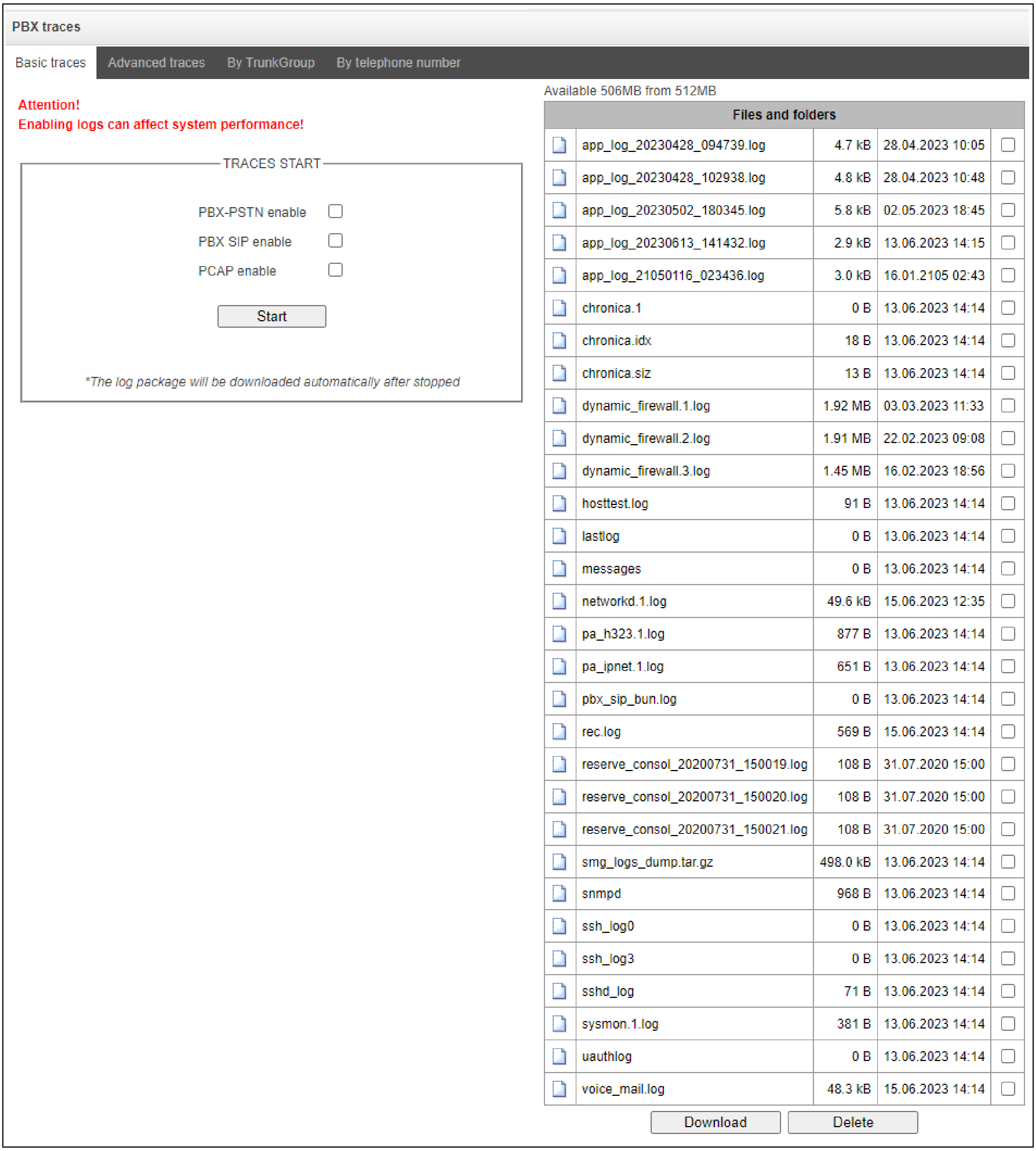
- *Start* – begin data collection;
- *Stop* – finish data collection;
- *Restart* – restart the utility and begin data collection again.

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*.

3.1.18.2 PBX Tracing

Using the 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.



'Basic traces' tab

The following options allow to quickly identify the causes of incorrect operation of the gateway.

- *PBX-PSTN enable* – allows one to run a log of the operation and interaction of the device nodes, as well as message exchange via various protocols. Automatically starts the next level of traces:

  alarms 1
  calls 99
  SIP 99
  SS7-ISUP 99
  Q.931 99
  RTP connections 99
  SM-VP commands 99
  RADIUS 1
  IVR 1

- *PBX SIP enable* – allows to start tracing messages and errors of the SIP protocol;
- *PCAP enable* – allows to run TCP-dump for the main network interface.

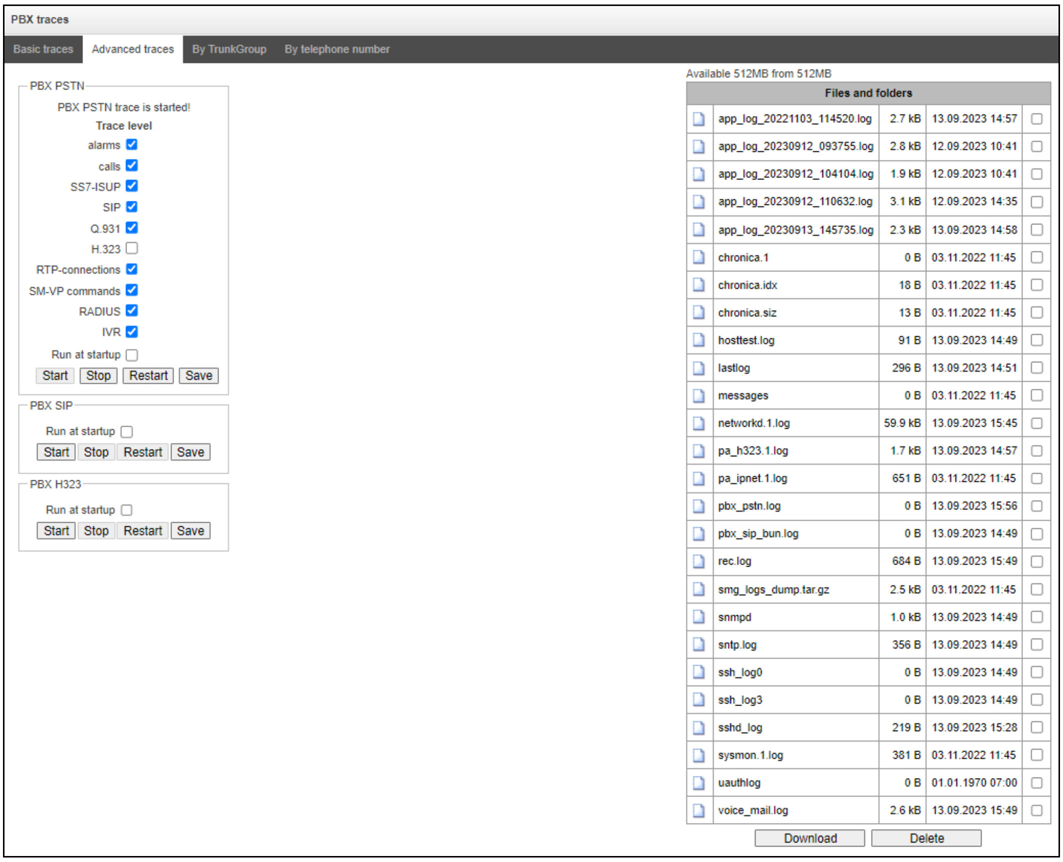
To start the data collection, it is required to enable the required options and click the '*Start*' button. To stop the data collection, use the '*Stop*' button. After stopping data collection, an archive with all taken traces will be automatically generated and downloaded. If all three types of logs were launched, then the following files will be in the archive after the tracing is completed:

  message
  app log *
  gzcore *
  pbx sip *
  pbx pstn *
  .pcap
  /etc/config/cfg*
  /tmp/disk/service.yaml
  /var/run/service.yaml

'Advanced traces' tab

Here, one can run a log on certain protocols and subsystems of the device.

Run at startup – allows to start taking traces immediately after restarting the gateway (Automatically enable logging after restarting the gateway).



The PBX PSTN block registers the operations and interaction of the device nodes in a log, as well as the exchange of messages using various protocols. In the PBX PSTN parameters, it is possible to select the events and protocols for which to get a log.

To start the data collection, select the required protocols and subsystems and click the *Start* button. The enabled option corresponds to the log level 99.

To stop data collecting, click the *'Stop'* button.

Also, when data collecting, one can change settings and restart data selection by clicking the *'Restart'* button.

The **PBX SIP** block registers SIP errors and messages tracing:

- *Start* – begin data collection;
- *Stop* – finish data collection;
- *Restart* – restart tracing and begin data collection again.

The **PBX H323** block is used to register H.323 errors and messages tracing:

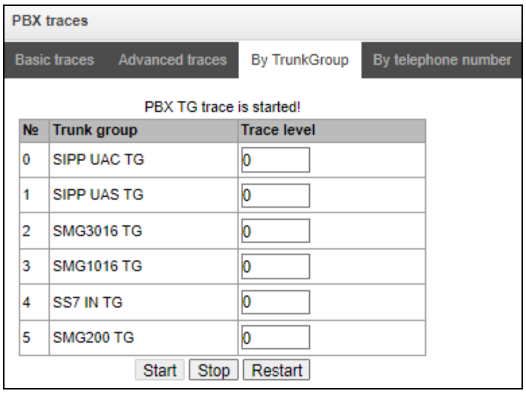
- *Start* – begin data collection;
- *Stop* – finish data collection;
- *Restart* – restart and begin data collection again.

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, one can download a set of recorded tracing files.

To download it to a local PC, check the checkboxes located next to the required file names and click the '*Download*' button. To delete the specified files from the directory, click '*Delete*'.

'By Trunk Group' tab



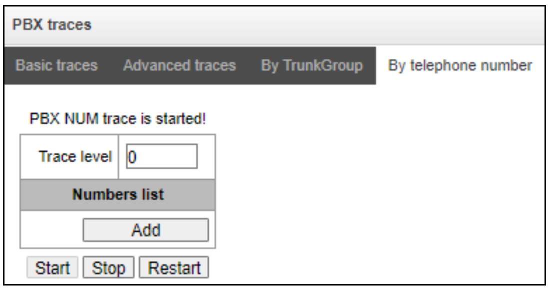
Use the menu to start PBX PSTN log collecting on selected trunk group. Tracing levels work similar to PBX PSTN tracing levels (see '*Common settings*' tab) and differ only by the fact that all protocols have the same specified logging level.

To start the data collection, it is necessary to set non-zero tracing level for required trunk groups, and then click the '*Start'* button.

To stop the data collection, click '*Stop'* button.

Also, when tracing, one can change the settings and restart data collecting by clicking '*Restart'* button.

'By telephone number' tab



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 to PBX PSTN tracing levels (see 'Basic 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.

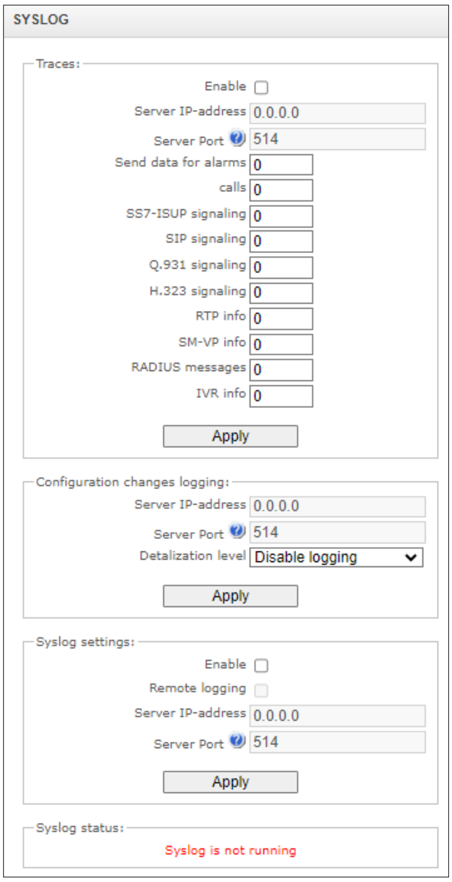
3.1.18.3 Syslog Settings

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 reasons should be identified. To determine the necessary debug levels, please contact ELTEX Service Centre.



Traces 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 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.

- *Enable* – enable syslog;
- *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.

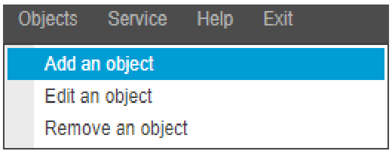
Configuration changes logging – used to save the history of changes in gateway settings.

- *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;
- *Detalization level* – detalization level of the entered commands log:
  - *Disable logging* – disable the generation of the entered commands log;
  - *Standard* – messages contain the name of the modified parameter;
  - *Extended* – messages contain the name of the modified parameter as well as parameter values before and after modification.

Syslog settings – configuration settings for the system log that records the device access events.

- *Enable* – when this option is checked, the device access events history is saved; when unchecked, logging is disabled;
- *Remote logging* – 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.

3.1.19 Working with Objects and the Objects Menu

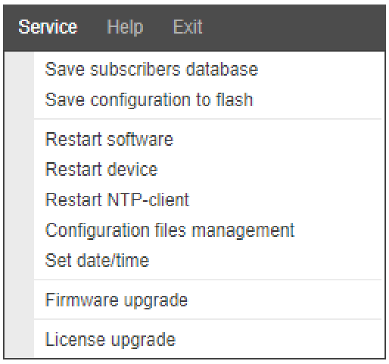


In addition to clicking the create, edit, and remove icons, the corresponding operations with an object can be performed using the *Objects* menu.

3.1.20 Saving Configuration and the Service Menu

To discard all changes, select the *Service – Discard All Changes* menu item.

If you make changes to the configuration without saving to FLASH and then 'cancel all changes', the registration of SIP subscribers fails.



To save the database of registered SIP subscribers, select the *Service – Save subscribers database* menu item.

To write the current configuration into the non-volatile memory of the device, select the *Service – Save Configuration to flash* menu item.

To restart the device firmware, select the *Service – Restart software* menu item.

To restart the device completely, select the *Service – Restart device* menu item.

To perform forced time resynchronization with the NTP server, select the *Service – Restart NTP-client* menu item.

To restart the client SSHD, select the *Service – SSHD Restart* menu item.

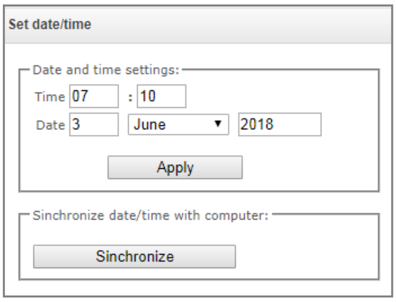
To read/write the main device configuration file, select the *Service – Configuration files management* menu item.

To configure the local date and time manually, select the *Service – Set date/time* menu item; see section 3.1.21.

To update the firmware via web configurator, select the *Service – Firmware upgrade* menu; see section 3.1.22.

To update/add licenses, select the *Service – License Update* menu item; see section 3.1.23.

3.1.21 Date and Time Settings (Service → Set date/time)

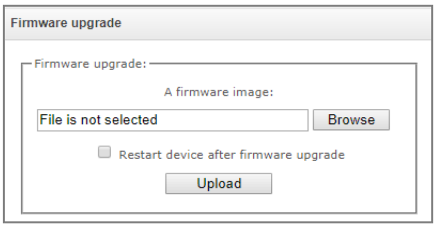


The system time and date can be specified in the respective fields in the HH:MM and DD.month.YYYY formats.

To save settings, use the '*Apply*' button.

Click the '*Sinchronize'* button to synchronize the device system time with the current time on a local PC.

3.1.22 *Firmware upgrade (Service → Firmware upgrade)*



To update the device firmware, use the *Service – Firmware Update* menu item.

The firmware file upload form opens.

- *Upload* – 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.

3.1.23 *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 3.1.26).

SMG-200 Licenses:

SMG-PBX (100) – registration of up to 100 SIP subscribers (set by default);

SMG-PBX (200) – registration of up to 200 SIP subscribers;

SMG-H323 – activation of H.323 protocol functionality;

SMG-RCM – activation of Radius Call Managment;

SMG-VAS – activation of VAS (set by default);

SMG-REC – activation of the call recording functionality;

SMG-VNI (40) – expansion of the number of network interfaces up to 40*;*

SMG-IVR – activation of Interactive Voice Response (set by default).

SMG-500 Licenses:

SMG-PBX (250) – registration of up to 250 SIP subscribers (set by default);

SMG-PBX (500) – registration of up to 500 SIP subscribers;

SMG-H323 – activation of H.323 protocol;

SMG-RCM – activation of Radius Call Managment;

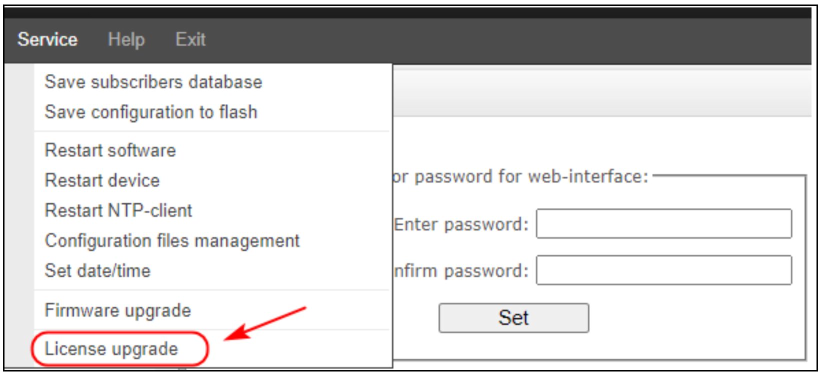
SMG-VAS – activation of VAS (set by default);

SMG-REC – activation of the call recording functionality;

SMG-VNI (40) – expansion of the number of network interfaces up to 40;

SMG-IVR – activation of Interactive Voice Response (set by default).

Next, select the *License upgrade* 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*.

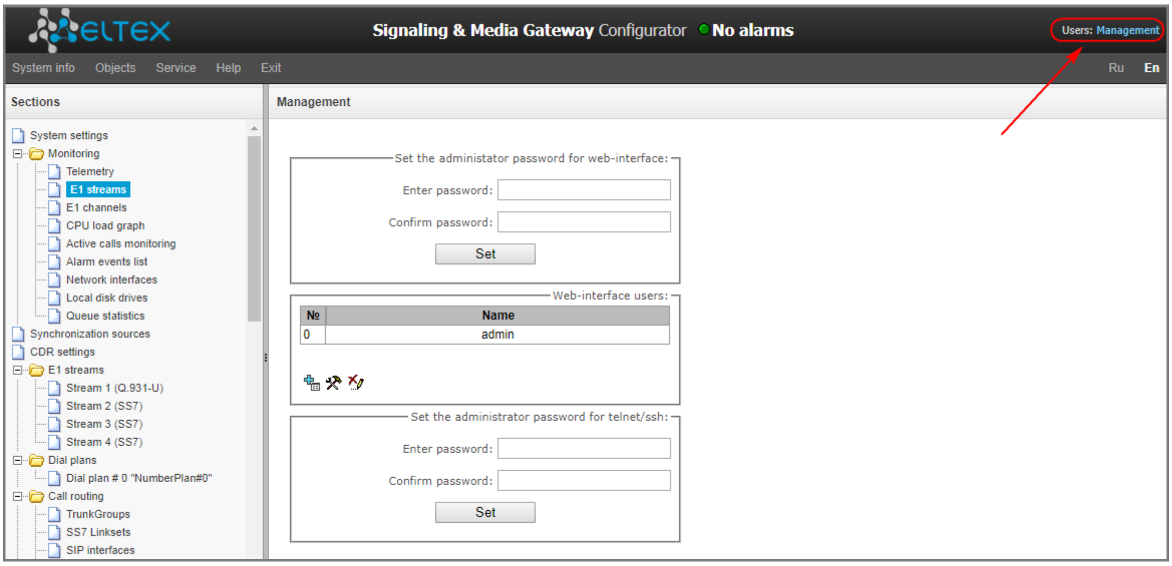
When the operation is complete, the system prompts you to restart the device. This can also be done manually in the *Service – Device Restart* menu.

3.1.24 Help Menu

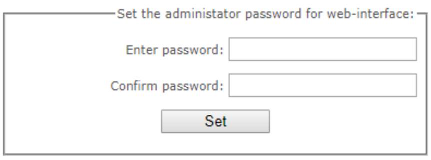
The menu provides information about the current firmware version, factory settings, and other system information.

3.1.25 Management Menu

Use 'Management' menu for work with passwords to access the device via web-configurator, telnet, ssh and user privilege configuration.



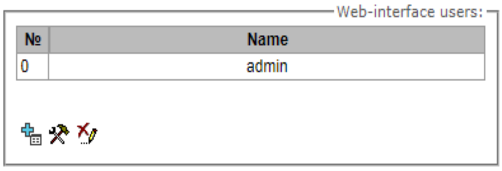
Configure the web interface administrator password:



To change the administrator password, enter a new password in the *Enter Password* field and confirm it in the *Confirmation password* field. To apply the password, click the *Set* button.

To save the configuration, use the *Service – Save Configuration to flash* menu item.

Web Interface Users:

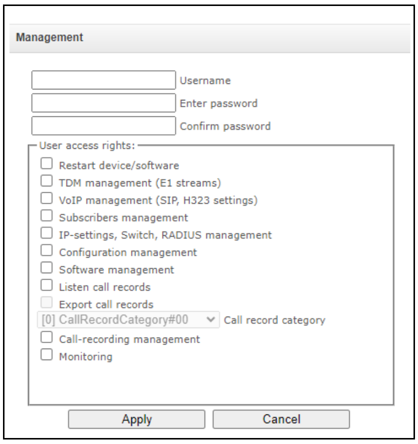


This section allows configuration of web configurator access restrictions for users. A system administrator can always add or remove users and define their access level. To create, edit, or remove users, use the following buttons:

 – Add user;
 – Edit user parameters;
 – Remove user.

The program does not allow changing the administrator's access rights or removing the administrator from the list of users, which ensures guaranteed entry into the system administrator program.

Creating a new user:



To create a new user, fill in the following fields:

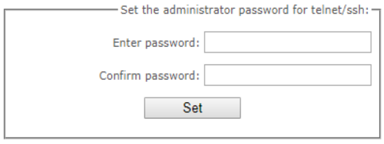
- *Username* – the username to log in the web configurator;
- *Enter password* – the password to access the web configurator;
- *Confirm password* – used to confirm the password to access the web configurator.

User access rights:

- *Restart device/software* — allows you to restart the device and firmware;
- *TDM management (E1 streams)* — allows you to set up E1 streams;
- *VoIP management (SIP, H323 settings)* — allows you to configure SIP and H323 interfaces;
- *Subscribers management* — provides the ability to configure SMG subscribers;
- *IP-settings, Switch, RADIUS management* — allows you to configure settings of switch, TCP/IP, network services and security;
- *Configuration management* — uploading/downloading configuration files;
- *Software management* — updating the device firmware and license;
- *Listen call records* — provides ability to listen recorded calls of the certain category;
- *Export call records* – provides the ability to download recorded conversations (listening to conversation recordings without the possibility of downloading);
- *Call-recording 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 to flash*.

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.

Active sessions list:

Active sessions list:

№	Username	IP address	Request	Previous connection (min:sec)	Forced logout
0	admin	10.13.16.110	/services/users	00:00	Current session
1	admin	10.13.16.116	/jx/alarm	00:03	

This block displays a list of users who are currently connected to the SMG web interface. It is possible for the administrator to forcibly end the session of other users by clicking the '*Forced logout'* button in the line with the user whose session you want to end.

3.1.26 View Factory Settings and System Information

To view factory settings and system information, use the '*Help – System info'* 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.

3.1.27 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)* – designed to configure the device via the CLI command line interface and firmware update;
- *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, *stream* is the stream number (0…15)
e1stat <stream>	Show E1 stream counters
alarm	Show alarm log information
sync	Show information on synchronization sources
syncfreq	Show information on synchronization frequency
setsync	Forced synchronization 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 linkset, <linkset> is the number of SS7 linkset
checknum	Check the number with the dial plan
cfg_read	Apply the current configuration; this command resets and re-initializes E1 streams
callref	Show information on active SIP calls
rtpdebug <level>	Enable switch RTP debugging; <level> is a debug level **This command may cause the switch to become unresponsive under load.**
mspcports	Show RTP port status
mspcshow <device>	Show the signal processor connection statistics
sipstat	Show the SIP call statistics
sipclrstat	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 *unregcon* 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 <POINT>	Command Description	Value <IDX>
hwpkt	Tracing of packet contents at the first level of exchange between the main application and the E1 stream driver	0..3
stream	E1 stream tracing	0..3
port	Application operation tracing	Not used
isup	ISUP subsystem operation tracing in the SS7 protocol	Not used
mtp3	MTP3 level operation tracing in the SS7 protocol for E1 stream	0..3
sipt	SIP/-T/-I protocol operation tracing	Not used
pril3	DSS1 protocol third level operation tracing for E1 stream	0..3
sw	TDM switch network operation tracing	Not used
mspc	IP forwarding tracing	Not used
mspd	Signal processor operation tracing	0..7
net	Tracing of the 2nd layer data network operation	Not used
sync	Tracing of synchronisation source operation	Not used
erl1	Low-level tracing of the system that transfers messages between the application and the SIP module	Not used
erl3	High-level tracing of the system that transfers messages between the application and the SIP module	Not used
snmp	SNMP protocol operation tracing	Not used
np	Numbering (routing) schedule operation tracing	Not used
mod	Modifier operation tracing	Not used
alarm	Gateway fault state tracing	Not used
radius	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***.

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 localization parameters
config			Go to the device parameter configuration mode
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
firmware update tftp	<FILE> <SERVERIP>	firmware file name IP address in the AAA.BBB.CCC.DDD format	Firmware update without automatic gateway restart • *FILE* – firmware file name • *SERVERIP* – 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 • *FILE* – firmware file name • *SERVERIP* – IP address of the FTP server
firmware update usb	<FILE>	firmware file name	Firmware update without automatic gateway restart • *FILE* – 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 • *FILE* – firmware file name • *SERVERIP* – IP address of the TFTP server
firmware update_and_reboot ftp	<FILE> <SERVERIP>	firmware file name IP address in the AAA.BBB.CCC.DDD	Firmware update with automatic gateway restart • *FILE* – firmware file name

		format	• *SERVERIP* – IP address of the FTP server
firmware update_and_reboot usb	<FILE>	firmware file name	Firmware update with automatic gateway restart • *FILE* – firmware file name
history			Show the history of entered commands
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 license
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 called masks and also in the configured SIP, PRI, FXS subscriber database. The check provides information on routing capability for this number in the specified dial plan: • *calling-table* – routing by the caller table; • *called-table* – routing by the called table; • *NOT found in* – routing by this table is not possible; • *found in* – routing by this table is possible; • *SIP/PRI/V5.2 abonent ID[11] index [0]* — SIP/PRI/FXS subscriber [subscriber's ID][entry number for this subscriber in the database]*;* • *Prefix index [6]* – 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
sh			Go to Linux Shell from CLI
tcpdump	<DEVICE> <FILE> <SNAPLEN>	eth0/eth1/local string 0-65535	Capture packets from the Ethernet device • *DEVICE* – an interface for monitoring • *FILE* – a file for packet writing • *SNAPLEN* – 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 *tcpdump* and *pcmdump* 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 unauthorized access.

To do this:

1. Connect to the gateway via CLI, authorize 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 for admin changed by root)
```

4. Save the configuration into Flash:

Go to the configuration mode using the ***config*** command;

Enter ***copy running_to_startup*** *command;*

Press <Enter> key.

3.3.3 Configuration mode of general device parameters

To switch to configuring/monitoring device parameters, execute the ***config*** command.

In each configuration menu, the ***do*** command is available, which allows executing a command from the CLI root menu when you are in any configuration submenu and the ***top*** command to go to the CLI root menu.

```
SMG> config
Entering configuration mode.
SMG-[CONFIG]>
```

Command	Parameter	Value	Action
?			Show the list of available commands
alarm path	<set>	off or /mnt/sd[abc][1-7]*	Select an external storage device for saving alarm messages: *Off* – disable; */mnt/sd[abc][1-7]** – path to the drive for storing traces
access category			Go to the access category configuration mode
cdr			Go to the CDR Parameters Configuration Mode
copy running_to_startup			Write the current configuration to the non-volatile memory of the device (to startup configuration)
copy startup_to_running			Restore current configuration from startup configuration
count linkset			Show a number of SS7 linksets
count trunk			Show a number of trunk groups
count trunk_direction			Show a number of trunk directions
count sipt-interface			Show a number of SIP interfaces

count radius-profile			Show a number of RADIUS profiles
delete modifiers-table			Show a number of modifier table profiles
count sipcause-profile			Show a number of Q.850 conformance profiles and sip-reply
count routing-profile			Show a number of scheduled routing profiles
count h323-interface			Show a number of h.323 profiles
count ss7timers			Show a number of SS7 timer profiles
delete linkset	<OBJECT_INDEX>	existing linkset number	Delete SS7 linkset
delete trunk	<OBJECT_INDEX>	existing trunk group number	Delete a trunk group
delete trunk_direction	<OBJECT_INDEX>	existing trunk direction number	Delete a trunk direction
delete sipt-interface	<OBJECT_INDEX>	existing SIP interface number	Delete SIP interface
delete radius-profile	<OBJECT_INDEX>	existing RADIUS profile number	Delete RADIUS Profile
delete modifiers-table	<OBJECT_INDEX>	existing modifier table number	Delete a modifier table
delete sipcause-profile	<OBJECT_INDEX>	existing number of q.850 and sip-reply conformance table	Delete Q.850 and sip-reply conformance table
delete routing-profile	<OBJECT_INDEX>	existing number of scheduled routing table	Delete a scheduled routing table
delete h323-interface	<OBJECT_INDEX>	existing number of H.323 interface	Delete H.323 interface
delete ss7timers	<OBJECT_INDEX>	existing profile number of SS7 timers	Delete SS7 timer profile
delete hunt-group	<OBJECT_INDEX>	existing hunt group	Delete a hunt group
delete pickup-group	<OBJECT_INDEX>	existing pickup group	Delete a pickup group
e1	<E1_INDEX>	1-4	Go to configuration mode of the selected E1 stream
exit			One menu level up
firewall dynamic			Go to Dynamic Firewall configuration mode
firewall static			Go to Static Firewall configuration mode
ftpd			Go to ftp server configuration mode
fxs/fxo			Go to fxs/fxo line configuration mode
h323 configuration			Go to to H.323 protocol configuration mode
h323 interface	<H323_INDEX>	0-254	Go to the specified interface configuration mode via H.323 protocol
history			View the history of entered commands
hostping			Go to periodic ping configuration mode
hunt-group	<hunt-group_INDEX>	0-31	Go to the operation configuration mode of the specified hunt group
ivr			Go to the ivr setting mode
ldap	<enable> <set name> <show list>	Off/on string no longer than 63 characters	Disable/enable LDAP server LDAP server name Viewing the LDAP Server Setting
log path	<apply> <set> <show>	local /mnt/sd[abc][1-7]*	Apply trace storage path settings Setting the trace storage path: *local* – local storage in RAM; */mnt/sd[abc][1-7]** – path to the drive for storing traces View trace storage path settings
linkset	<LINKSET_INDEX>	0-15	Go to the configuration mode of SS7 linkset

modifiers table	<MODTBL_INDEX>	0-255	Go to the modifier table configuration mode
modtable copy	<MODTBL_INDEX>	0-255	Copy a modifier table
network			Go to the network parameter configuration mode
new linkset			Create a new SS7 linkset
new trunk			Create a new trunk group
new trunk_direction			Create a new trunk direction
new sipt-interface			Create a new SIP-T interface
new radius-profile			Create a new RADIUS profile
new modifiers-table			Create a new modifier table
new sipcause-profile			Create a q.850 and sip-reply mapping table
new routing-profile			Create a scheduled routing table
new h323-interface			Create H.323 interface
new ss7timers			Create a profile of SS7 timers
new hunt-group			Create a hunt group
new pickup-group			Create a pickup group
numplan			Go to the dial plan configuration mode
pbx_profiles			Go to the PBX profile configuration mode
ports range	<RANGE_PORT>	1-65535	Set the range of UDP ports used for the transmission of voice traffic (RTP) and data over the T.38 protocol
ports show			Show UDP port configuration
ports start	<START_PORT>	1024-65535	Set the starting UDP port used for the transmission of conversational traffic (RTP) and data over the T.38 protocol
pri-users			Go to the configuration mode of pri-subscribers
pri_profiles			Go to the configuration mode of pri-profiles
q931-timers			Go to the configuration mode of Q.931 timers
quit			End the current CLI session
radius			Go to the RADIUS configuration mode
record			Go to the call recording configuration mode
route			Go to the static route configuration mode
routing			Go to scheduled routing profile configuration Mode
show running main by_step			Show the running main configuration step by step
show running main whole			Show the whole running main configuration
show running network			Show the running network configuration
show running radius_servers			Show the running configuration of RADIUS servers
show running snmp			Show SNMP running configuration
show startup main by_step			Show startup main configuration step by step
show startup main whole			Show the whole startup main configuration
show startup network			Show the startup network configuration
show startup radius_servers			Show the startup configuration of RADIUS servers
show startup snmp			Show SNMP startup configuration
sip configuration			Go to SIP/SIP-T parameters configuration mode
sip interface	<SIPT_INDEX>	0-63	Go to SIP/SIP-T interface configuration mode
sip users			Go to SIP/SIP-T subscribers configuration mode
ss7cat			Go to the configuration mode of SS7 categories
ss7timers	<SS7_TIMERS_INDEX>	0-15	Go to the configuration mode of SS7 timers

submodule-usage			Go to the SM-VP Submodule Usage Configuration Mode
sync			Go to synchronization settings configuration mode
syslog			Go to syslog configuration mode
trunk	<TRUNK_INDEX>	0-63	Go to trunk groups configuration mode
trunk_direction	<DIRECTION_INDEX>	0-31	Go to trunk directions configuration mode

3.3.4 CDR parameters configuration mode

To enter this mode, it is necessary to run the **cdr** command in the configuration mode.

```
SMG-[CONFIG]> cdr
Entering CDR-info mode.
SMG-[CONFIG]-[CDR]>
```

Command	Parameter	Value	Action
?			Show list of available commands
archive	<all> <directory>	string no longer than 31 characters String no longer than 31 characters	Archiving CDR data
category	save	yes/no	Save/not save subscriber category in CDR files
config			Return to the Configuration menu
duration count mode	< CDR_COUNT_MODE>	round-up/ round-down/ not-round	Rounding duration up, down, or do not round (write in milliseconds)
emptysave	<CDR_EMPTY>	yes/no	Save/do not save CDR files that do not contain records
enabled	<CDR>	yes/no	Generate/do not generate CDR records
exit			Moving from this configuration submenu to a higher level
fields add <field>			Adds the given field to the end of the field list (see 3.3.5 CDR Field List)
fields default			Sets the base set of fields
fields flush			Clears the list of used fields
fields set <field>	<FIELD_INDEX>	0-39	Replaces the field at the corresponding position with the specified field (see 3.3.5 CDR Field List)
file create mode	<CDR_FILE>	periodically/ once-a-day/ once-an-hour	CDR file creation mode: • *periodically* – with a given period; • *once-a-day* – once a day; • *once-an-hour* – once an hour.
header	<CDR_HEADER>	yes/no	Write / do not write to the beginning of the CDR file the header: SMG. CDR. File started at 'YYYYMMDDhhmmss', where 'YYYYMMDDhhmmss' – start time to save records to file
history			View the history of entered commands
localdisk	<set> <show>	/mnt/sd[abc][1-7]*	Path to store CDR data on local drives; View CDR storage path setting
localkeep period	<day> <hour> < min>	0-30 0-23 0-59	CDR data storage time on local disk
localsave	<no> <yes>		Save CDR data to local drive
period day	<CDR_DAY>	0-30	Set the period for generating CDR records and saving them in the device's RAM, days
period hour	<CDR_HOUR>	0-23	Set the period for generating CDR

			records and saving them in the device's RAM, hours
period min	<CDR_MIN>	0-59	Set the period for generating CDR records and saving them in the device's RAM, minutes
pickup mark	<CDR_ pickup _MARK>	yes/no	Add/do not add an additional field 'pickup mark' to the CDR record
quit			End this CLI session
redirectmark	<CDR_REDIRECT_MARK>	yes/no	Add/do not add an additional field 'redirect mark' to the CDR record
redirectsave	<CDR_REDIRECT>	yes/no	Add an additional Redirecting number field to the CDR records, otherwise the Redirecting number will replace the Calling party number for the redirected call
redirected duration	<CDR_REDIR_DURATION>	yes/no	Specify the duration of the redirected call
release initiator mark	<CDR_RELEASE>	yes/no	Save a release initiator mark
show			Show CDR Settings
show_dirs			Show folder path to access FTP server
signature	<CDR_SIGNATURE>	string no longer than 63 characters	Specify a distinguishing sign by which you can identify the device that created a record
unsuccess	<CDR_UNSUCC>	yes/no	Record/do not record unsuccessful calls (that did not end with a conversation) in CDR files
upload archive ftp/tftp	<ARCHIVE_NAME> <FTP/TFTP_server>	string no longer than 63 characters IP address	Send archive to FTP/TFTP server
upserver enabled	<CDR_UPLOAD>	yes/no	Transfer/do not transfer CDR records to the server
upserver ipaddr	<CDR_SERVER_IPADDR>	string no longer than 63 characters	Set server IP address
upserver login	<CDR_SERVER_LOGIN>	string no longer than 63 characters	Set a username to access the server
upserver passwd	<CDR_SERVER_PASSWD>	string no longer than 63 characters	Set a user password to access the server
upserver path	<CDR_SERVER_PATH>	string no longer than 63 characters	Set the path to the folder on the server where the CDR records will be saved
upserver port	<CDR_SERVER_PORT>	1–65535	Set server TCP port
upserver protocol	<CDR_VIA_PROTO>	FTP/SCP	Set the protocol by which CDRs will be sent to the server
upserver reserve enabled	<CDR_RESERV_ENA>	yes/no	Transfer/do not transfer CDR records to the reserve server
upserver reserve ipaddr	<CDR_RESERV_IPADDR>	string no longer than 63 characters	Set reserve server IP address
upserver reserve login	<CDR_RESERV_LOGIN>	string no longer than 63 characters	Set a username to access the reserve server
upserver reserve only fail	<CDR_RESERV_ONLY_FAIL>	yes/no	Enable/disable saving CDR files to the reserve server only in case of an error while writing to the primary server
upserver reserve passwd	<CDR_RESERV_PASSWD>	string no longer than 63 characters	Set a user password to access the reserve server
upserver reserve path	<CDR_RESERV_PATH>	string no longer than 63 characters	Set the path to the folder on the reserve server where CDR records will be saved
upserver reserve port	<CDR_RESERV_PORT>	1–65535	Set the TCP port of the reserve server

3.3.5 CDR fields list

<field>	Value
acct-session-id	RADIUS Account-Session-Id, Acct-Session-Id field value, sent in a RADIUS accounting packet
called in	Called number at the input (before modifications)
called out	Called number at the output (after modifications)
calling in	Calling number at the input (before modifications)
calling out	Calling number at the output (after modifications)
device sign	Distinguishing sign
disc code	Release code according to Q.850
disc info	Call status while releasing
duration	Call duration
global-callref	Global Call Reference (GCR) field
incoming CID category	Caller ID category at the input (before modifications)
incoming description	Caller Description - Subscriber/Trunk Name (TG)
incoming E1 chan	Incoming E1 channel number
incoming E1 stream	Incoming E1 stream number
incoming ipaddr	IP address of calling subscriber
incoming SIP call id	SIP Call-ID of incoming call
incoming SS7 category	Incoming SS7 category (before modifications)
incoming SS7 CIC	CIC number of incoming call
incoming type	Type of a calling party
mark pickup	Pickup mark
mark redir	Redirect mark
mark release side	Release initiator mark
numplan in	Dial plan through which the call came
numplan out	Dial plan through which the call left
outgoing CID category	Outgoing CID category (after modifications)
outgoing description	Called description - Subscriber/Trunk Name (TG)
outgoing E1 chan	Outgoing E1 channel number
outgoing E1 stream	Outgoing E1 stream number
outgoing ipaddr	IP address of called subscriber
outgoing SIP call id	SIP Call-ID of outgoing call
outgoing SS7 category	Outgoing SS7 category (after modifications)
outgoing SS7 CIC	CIC number of outgoing call
outgoing type	Type of a called party
radius-rejected	Blocking RADIUS server address
redirecting in	Redirecting number at the input (before modifications)
redirecting out	Redirecting number at the output (after modifications)
sequential number	Entry sequential number
time connect	Call answer time
time disconnect	Call release time
time setup	Call arrival time

3.3.6 Access category configuration mode

To enter this mode, it is necessary to run the **access category** command in the configuration mode.

```
SMG-[CONFIG]> access category
Entering Access-Category mode.
SMG-[CONFIG]-[ACCESS-CAT]>
```

Command	Parameter	Value	Action
?			Show list of available commands
config			Return to the Configuration menu
exit			Going from this configuration submenu to a higher level
quit			End this CLI session
set access	<CAT_IDX> <ACCESS_IDX> <ACCESSIBLE>	0-63 0-63 enable/disable	Set access rights of categories in relation to each other: • *CAT_IDX* – custom access category index; • *ACCESS_IDX* – category to which access is configured; • *ACCESSIBLE* – category access status (available, not available)
set name	<CAT_IDX> <NAME>	0-63 access category name, no more than 31 characters (numbers, letters, '_' sign)	Change the access category name • *CAT_IDX* – custom access category index; • *NAME* – access category name
show	<CAT_IDX>	0-63	Show configuration for this access category
showall			Show configuration for all access categories

3.3.7 *E1 stream configuration mode (only SMG-500)*

To enter this mode, in the configuration mode it is necessary to run the **e1** <E1_INDEX> command, where <E1_INDEX> is E1 stream number.

```
SMG-[CONFIG]> e1 1
Entering E1-stream mode.
SMG-[CONFIG]-E1[1]>
```

Command	Parameter	Value	Action
?			Show list of available commands
alarm	<ON_OFF>	on/off	Enable/disable alarm indication for this E1 stream
config			Return to the configuration menu
crc4	<ON_OFF>	on/off	Enable/disable CRC4 control for this E1 stream
disabled			Disable the stream
enabled			Enable the stream
equalizer	<ON_OFF>	on/off	Enable/disable E1 stream signal gain
exit			Going from this configuration submenu to a higher level
history			View the history of entered commands
lapd			Going to the LAPD parameters configuration mode for the current E1 stream
linecode AMI			Set AMI line coding type on the given stream
linecode HDB3			Set HDB3 line coding type on the given stream
name		letter or number or '_', '.', '-'. Max 63 characters	E1 stream name
q931			Going to Q931 signaling configuration mode for the current E1 stream
quit			End this CLI session
remalarm	<ON_OFF>	on/off	Enable/disable indication in case of a remote alarm on the given stream
show			Show the configuration of the given stream
signaling	<Signaling type>	Q931_USR Q931_NET SS7	Set signaling type for this stream Possible types of signaling: Q931_USR, Q931_NET, SS7
slipIND	<ON_OFF>	on/off	Display an indication of an accident in the event of a slip in the receiving path
slipTO	<TIMEOUT>	5sec/10sec/ 20sec/30sec/ 45sec/1min/ 2min/3min/ 5min/10min/ 15min/30min/ 1hour/2hour/6hour	Set the frequency of polling the stream parameters from the board; if slip is detected on this stream, then during this timeout the station will signal an accident
ss7			Going to configuration mode of SS7 signaling parameters for the current E1 stream

3.3.7.1 LAPD parameters configuration mode for the current E1 stream

The mode is only available for Q.931 signaling (set by the **signaling** command). To enter this mode, in the E1 stream configuration mode it is necessary to run the **lapd** command.

```
SMG-[CONFIG]-E1[1]> lapd
E1[1]. Signaling is Q931
SMG-[CONFIG]-E1[1]-[LAPD]>
```

Command	Parameter	Value	Action
?			Show list of available commands
config			Return to the configuration menu
exit			Going from this configuration submenu to a higher level
history			View the history of entered commands
N200	<N200>	0-255	Set a number of connection attempts
quit			End this CLI session
show			Show LAPD Configuration
t200	<T200>	0-255	Set timer value T200, x100 ms
t203	<T203>	0-255	Set timer value T203, x100 ms

3.3.7.2 Q931 signaling configuration mode for the current E1 stream

The mode is only available for Q.931 signaling (set by the **signaling** command). To enter this mode, in the E1 stream configuration mode it is necessary to run the **q931** command.

```
SMG-[CONFIG]-E1[0]> q931
E1[0]. Signaling is Q931
SMG-[CONFIG]-E1[0]-[Q931]>
```

Command	Parameter	Value	Action
?			Show list of available commands
access category	<CAT_IDX>	0-31	Set access category for stream
categoryAON	<CAT_AON>	0-10	Set AON category for incoming call
channel	<CHAN_NUM> <on_off>	[0-31] or 'all' on/off	Enable/disable the specified channel
chanorder	<CHAN_ORDER>	up_ring/ down_ring/ up_start/ down_start	Set channel order: • *up_ring* – sequentially forward; • *down_ring* – sequentially backward; • *up_start* – starting from the first forward; • *down_start* – starting from the last backward
config			Return to the configuration menu
exit			Return from this configuration submenu to a higher level
history			View the history of entered commands
InBand in Disconnect	<on_off>	on/off	Enable PI In-Band in DISCONNECT option

numplan	<CLD_PLAN_ID>	unknown/ISDN/ telephony/ National/ Privat	Set the dial plan type. **To use the common E.164 dial plan, select ISDN/telephony**
qsig	<ON_OFF>	on/off	Enable/disable QSIG signaling
quit			End this CLI session
RestartChannel	<SEND>	send/don't_send	Issue/do not issue a RESTART channel
RestartInterface	<SEND>	send/don't_send	Issue/do not issue a RESTART interface
RoutingProfile	<PROF Number>	[0-127] or none	Scheduled Routing Profile Selection
SendCatAON	<ON_OFF>	on/off	Allow/prohibit the transmission of the caller's AON category in the SETUP message as the first digit of the number. **For proper operation, this mode must be supported on the opposite side.**
SendDialTone	<ON_OFF>	on/off	Issue/do not issue a DialTone ready signal to the line during an incoming overlap-session
SendEndOfDial	<ON_OFF>	on/off	Enable/disable the transmission of the 'End of dial' message
show			Show the configuration of a Q931 signaling parameters
trunk	<trunk_index>	0-31	Set trunk group number for this stream

3.3.7.3 Configuration mode of SS7 signaling parameters for the current E1 stream

The mode is only available for SS7 signaling (set by the **signaling** command). To enter this mode, in the E1 stream configuration mode it is necessary to run the **ss7** command.

```
SMG-[CONFIG]-E1[1]> ss7
E1[1]. Signaling is SS7
SMG-[CONFIG]-E1[1]-[SS7]>
```

Command	Parameter	Value	Action
?			Show list of available commands
CIC fill	<CIC> <step>	0-65535 0-255	Set the CIC value for all time slots, starting from zero: • *CIC* – CIC strating number; • *step* – numbering step
CIC set	<TIMESLOT> <CIC>	0-31 0-65535	Set the CIC value for a single timeslot: • *TIMESLOT* – timeslot number; • *CIC* – CIC value
config			Return to the Configuration menu
Dchan	<D_CHAN>	0-31	Set D-channel number for a line: 0 – do not use D-channel (conversational stream)
DPC MTP3		0-16383	Assign DPC MTP3 value for the given stream
exit			Going from this configuration submenu to a higher level
history			View the history of entered

			commands
linkset	<linkset_index>	0-15	Assign SS7 linkset for this stream
quit			End this CLI session
show			Show configuration of SS7 signaling parameters
SLC	<slc>	0-15	Set signaling channel identifier in SS7 linkset

3.3.8 Dynamic firewall parameters configuration mode

To enter this mode, it is necessary to run the **firewall dynamic** command in the configuration mode.

```
SMG-[CONFIG]> firewall dynamic
Entering dynamic firewallmode.
SMG-[CONFIG]-[DYN-FIREWALL ]>
```

Command	Parameter	Value	Action
?			Show list of available commands
blacklist add	<BLACKIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Add an address to the list of blocked addresses
blacklist remove by addr	<BLACKIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Remove an address from the list of blocked addresses
blacklist remove by pos	<POSITION>	0-65635	Remove an address from the list of blocked addresses by its position in the list
blacklist show all			Show list of blocked addresses
blacklist show count			Show a number of entries in the list of addresses blocked by the dynamic firewall
blacklist show address	<BLACKIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Find the specified address in the list of blocked addresses
blacklist show first	<COUNT>	0-4095	Show the specified quantity from the beginning of the list of blocked addresses
blacklist show last	<COUNT>	0-4095	Show the specified quantity from the end of the list of blocked addresses
blacklist show position	<POSITION>	0-65635	Show the entry at the specified position in the list of blocked addresses
block history show all			Show the history of blocked addresses
block show count			Show a number of entries in the log of blocked addresses
block show address	<BLACKIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Find the specified address in the log of blocked addresses
block show first	<COUNT>	0-4095	Show a specified number from the beginning of the blocked addresses log
block show last	<COUNT>	0-4095	Show a specified number from

			the end of the blocked addresses log
block show position	<POSITION>	0-65635	Show an entry at the specified block address log position
blocklist remove by addr	<BLACKIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Remove an address from the list of automatically blocked addresses
blocklist remove by pos	<POSITION>	0-65635	Remove an address from the list of automatically blocked addresses by its position in the list
blocklist show all			Show a list of automatically blocked addresses
blocklist show count			Show a number of entries in the list of automatically blocked addresses
blocklist show address	<BLACKIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Find the specified address in the list of automatically blocked addresses
blocklist show first	<COUNT>	0-4095	Show a specified quantity from the begining of the list of automatically blocked addresses
blocklist show last	<COUNT>	0-4095	Show a specified quantity from the end of the list of automatically blocked addresses
blocklist show position	<POSITION>	0-65635	Show the entry at the specified position in the list of automatically blocked addresses
exit			Going from this configuration submenu to a higher level
history			View the history of entered commands
quit			End this CLI session
set block_time	<SERVICE> <BLCKTIME>	SIP/WEB/TELNET/SSH /OTHER 60-352800	Set the time in seconds for the service during which access from a suspicious address will be blocked
set enable	<ENA>	on/off	Enable/disable Dynamic Firewall
set tries	<SERVICE> <TRIES>	SIP/WEB/TELNET/SSH /OTHER 1-10	Set the maximum number of failed attempts to access a service before the host will be blocked
set forgive_time	<SERVICE> <FORGIVETIME>	SIP/WEB/TELNET/SSH /OTHER 60-352800	Set forgive time for the service
set increment	<SERVICE> <INCREMENT_FLG>	SIP/WEB/TELNET/SSH /OTHER no/yes	Enable progressive blocking for a service
show			Show dynamic firewall settings
whitelist add	<WHITEIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Add an IP address to the list of addresses blocked for automatic blocking
whitelist remove by addr	<WHITEIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Remove an IP address from the list of addresses prohibited for automatic blocking

whitelist remove by pos	<POSITION>	0-65635	Remove an IP address from the list of addresses prohibited for automatic blocking based on its position in the list
whitelist show all			Show a list of addresses prohibited for automatic blocking
whitelist show count			Show a number of entries in the list of addresses prohibited from automatic blocking
whitelist show address	<WHITEIP>	IP address in AAA.BBB.CCC.DDD format or subnet in CIDR notation AAA.BBB.CCC.DDD/FF	Find a specified address in the list of addresses prohibited for automatic blocking
whitelist show first	<COUNT>	0-4095	Show a specified quantity from the beginning of the list of addresses prohibited for automatic blocking
whitelist show last	<COUNT>	0-4095	Show a specified quantity from the end of the list of addresses prohibited for automatic blocking
whitelist show position	<POSITION>	0-65635	Show an entry at the specified position in the list of addresses prohibited for automatic blocking

3.3.9 Static firewall parameters configuration mode

To enter this mode, it is necessary to run the **firewall static** command in the configuration mode.

```
SMG-[CONFIG]> firewall static
Entering static firewall mode
SMG-[CONFIG]-[FIREWALL]>
```

Command	Parameter	Value	Action
?			Show list of available commands
add profile	<PROF_NAME>	allowed to use letters, digits, '_' symbol, maximum 63 characters	Add a firewall profile
add rule	<direction> <ENABLE> <RULE_NAME> <S_IP> <S_MASK> <R_IP> <R_MASK> <PROTO> <S_PORT_START>	forward input output enable/disable Text, max. 63 characters AAA.BBB.CCC.DDD AAA.BBB.CCC.DDD AAA.BBB.CCC.DDD AAA.BBB.CCC.DDD any tcp udp icmp tcp+udp 1-65535	Add a firewall rule Rule direction Enable/disable a rule Rule name Source IP address Source subnet mask Recipient IP address Recipient subnet mask Protocol type Source starting port

	<S_PORT_END> <D_PORT_START> <D_PORT_END> <ICMP_TYPE>	1-65535 1-65535 1-65535 none any echo-reply destination-unreachable network-unreachable host-unreachable protocol-unreachable port-unreachable fragmentation-needed source-route-failed network-unknown host-unknown network-prohibited host-prohibited TOS-network-unreachable TOS-host-unreachable communication-prohibited host-precedence-violation precedence-cutoff source-quench redirect network-redirect host-redirect TOS-network-redirect TOS-host-redirect echo-request router-advertisement router-solicitation time-exceeded ttl-zero-during-transit ttl-zero-during-reassembly parameter-problem ip-header-bad required-option-missing timestamp-request timestamp-reply address-mask-request address-mask-reply	Source ending port Destination starting port Destination ending port ICMP packet type
	<ACTION>	accept, drop, reject	Action – action taken by this rule: • *ACCEPT* – packets matching this rule will be passed by the firewall; • *DROP* – packets matching this rule will be dropped by the firewall without any

			information to the party that transmitted the packet; • *REJECT* – packets matching this rule will be dropped by the firewall, and either a TCP RST packet or an ICMP destination unreachable will be sent to the party that transmitted the packet.
	<P_IDX>	1-65535	Firewall profile number
add rule geoip	<direction> <ENABLE> <RULE_NAME> <COUNTRY> <PROTO> <S_PORT_START> <S_PORT_END> <D_PORT_START> <D_PORT_END> <ICMP_TYPE>	input output enable/disable Text, max. 63 characters Country name any tcp udp icmp tcp+udp 1-65535 1-65535 1-65535 1-65535 none any echo-reply destination-unreachable network-unreachable host-unreachable protocol-unreachable port-unreachable fragmentation-needed source-route-failed network-unknown host-unknown network-prohibited host-prohibited TOS-network-unreachable TOS-host-unreachable communication-prohibited host-precedence-violation precedence-cutoff source-quench redirect	Add a firewall GeoIP-rule Rule direction Enable/disable the rule Rule name Country to which the address belongs Protocol type Source starting port Source ending port Destination starting port Destination ending port ICMP packet type

		network-redirect host-redirect TOS-network-redirect TOS-host-redirect echo-request router-advertisement router-solicitation time-exceeded ttl-zero-during-transit ttl-zero-during-reassembly parameter-problem ip-header-bad required-option-missing timestamp-request timestamp-reply address-mask-request address-mask-reply	
	<ACTION>	accept, drop, reject	Action – action taken by this rule: • *ACCEPT* – packets matching this rule will be passed by the firewall; • *DROP* – packets matching this rule will be dropped by the firewall without any information to the party that transmitted the packet; • *REJECT* – packets matching this rule will be dropped by the firewall, and either a TCP RST packet or an ICMP destination unreachable will be sent to the party that transmitted the packet.
	<P_IDX>	1-65535	Firewall profile number
add rule string	<direction>	input output	Add a firewall rule – strings checking. Rule direction
	<ENABLE>	enable/disable	Enable/disable a rule
	<RULE_NAME>	Text, max. 63 characters	Rule name
	<CONTENT>	Text, max. 127 characters	The text string that should be in the package
	<S_IP>	AAA.BBB.CCC.DDD	Source IP address
	<S_MASK>	AAA.BBB.CCC.DDD AAA.BBB.CCC.DDD	Source subnet mask Recipient IP address

	<R_IP> <R_MASK>	AAA.BBB.CCC.DDD	Recipient subnet mask
	<PROTO>	any tcp udp icmp tcp+udp	Protocol type
	<S_PORT_START>	1-65535	Source starting port
	<S_PORT_END>	1-65535	Source ending port
	<D_PORT_START>	1-65535	Destination starting port
	<D_PORT_END>	1-65535	Destination ending port
	<ICMP_TYPE>	none any echo-reply destination-unreachable network-unreachable host-unreachable protocol-unreachable port-unreachable fragmentation-needed source-route-failed network-unknown host-unknown network-prohibited host-prohibited TOS-network-unreachable TOS-host-unreachable communication-prohibited host-precedence-violation precedence-cutoff source-quench redirect network-redirect host-redirect TOS-network-redirect TOS-host-redirect echo-request router-advertisement router-solicitation time-exceeded ttl-zero-during-transit ttl-zero-during-reassembly parameter-problem ip-header-bad required-option-missing timestamp-request	ICMP packet type

	<ACTION> <P_IDX>	timestamp-reply address-mask-request address-mask-reply accept, drop, reject 1-65535	 Action – action taken by this rule: • *ACCEPT* – packets matching this rule will be passed by the firewall; • *DROP* – packets matching this rule will be dropped by the firewall without any information to the party that transmitted the packet; • *REJECT* – packets matching this rule will be dropped by the firewall, and either a TCP RST packet or an ICMP destination unreachable will be sent to the party that transmitted the packet. Firewall profile number
apply			Apply firewall settings
config			Return to Configuration menu
del profile	<ID>	1-65535	Delete a firewall profile
del rule	<ID>	1-65535	Delete a firewall rule
exit			Exit from this configuration submenu to a higher level
modify profile	<ID> <NAME>	1-65535 allowed to use letters, digits, symbol '_'. Maximum 63 characters	Firewall profile index Entering a new device name
modify rule	<Type> <ID> <param>	action dport_end dport_start enable icmp-type name prof_id proto r_ip r_mask s_ip s_mask sport_end sport_start traffic-type 1-65535 New value according to the given parameter type	Change the specified firewall rule (one of the options)
move down	<ID>	1-65535	Move rule down by one position
move up	<ID>	1-65535	Move rule up by one position
quit			End this CLI session

set eth	<PROFILE ID>	0-65535	Assign a rule to a network interface PROFILE ID = 0 means that the profile is not used
set pptp	<PPP_IDX> <PROFILE ID>	0-5 0-65535	Assign a rule to an interface PROFILE ID = 0 means that the profile is not used
set vlan	<VLAN_IDX> <PROFILE ID>	VLAN1…VLAN8 0-65535	Assign a rule to VLAN PROFILE ID = 0 means that the profile is not used
show config			Show configuration
show interfaces			Show interface options
show system			Show system options

3.3.10 FTP parameters configuration mode

To enter this mode, it is necessary to run the **ftpd** command in the configuration mode.

```
SMG-[CONFIG]> ftpd
Entering ftpd mode.
SMG-[CONFIG]-[FTPd]>
```

Command	Parameter	Value	Action
?			Show list of available commands
config			Return to the configuration menu
exit			Exit from this configuration submenu to a higher level
quit			End this CLI session
set enable	<EN>	on/off	Enable/disable FTP server
set port	<PORT>	1-65535	Assign a port for FTP server
set interface	<IFACE_NAME>	string up to 255 characters	Set network interface for FTP server
set timeout idle	<TIME>	0-600	Set idle timeout, seconds
set timeout login	<TIME>	0-600	Set login timeout, seconds
set timeout session	<TIME>	0-600	Set session timeout, seconds
show config			Show FTP server configuration
show user			Show user configuration
user add	<USER_NAME> <PASSWD> <CDR_ACCESS> <LOG_ACCESS> <MNT_ACCESS> <CFG_ACCESS>	no_access/r/w/r no_access/r/w/r no_access/r/w/r no_access/r/w/r	Add a user Set a username for a new user Set a password for a new user Set access rights to the CDR directory Set access rights to the LOG directory Set access rights to the MNT directory (external drives) Set access rights to the CFG directory (configuration files)
user del	<IDX>	1-4	Delete a user
user modify access	<IDX>	0-4	Modify access rights for the specified user:

	<CDR_ACCESS> <LOG_ACCESS> <MNT_ACCESS> <CFG_ACCESS>	no_access/r/w/r no_access/r/w/r no_access/r/w/r no_access/r/w/r	• Configuring access to the CDR directory, read / write; • Configuring access to the log directory, read / write; • Configuring access to the mnt directory, read / write; • Configuring access to the cfg directory, read / write.
user modify password	<IDX> <PASSWD>	0-4	Modify the password for the specified user

3.3.11 FXS/FXO-lines configuration mode (only SMG-200)

To enter this mode, it is necessary to run the **fxs/fxo** command in the configuration mode.

```
SMG-[CONFIG]> fxs/fxo
Entering FXS mode.
SMG-[CONFIG]-[FXS/FXO]>
```

Command	Parameter	Value	Action
?			Show list of available commands
config			Return to the configuration menu
edit port	<PORT_ID>	1-16	Go to fxs/fxo port settings
exit			Exit from this configuration submenu to a higher level
profile			Go to fxs/fxo profile settings
quit			End this CLI session
show port id	<PORT_ID>	1-16	Show port configuration
show port list			Show configuration of all ports

3.3.12 FXS/FXO parameters configuration mode for the current FXS/FXO line

To enter this mode, it is necessary to run the **edit port** command in the fxs/fxo configuration mode.

```
SMG-[CONFIG]-[FXS/FXO]> edit port 1
SMG-[CONFIG]-[FXS/FXO]-PORT[1]>
```

Command	Parameter	Value	Action
?			Show list of available commands
config			Return to the configuration menu
exit			Exit from this configuration submenu to a higher level
quit			End this CLI session
service			Going to the VAS configuration mode on the fxs port
set access	<CAT_IDX>	0-127	Set access category for FXS/FXO line
set AON number			Set AON number for FXS/FXO line
set blf max_subscribers		0-200	Set a maximum number of subscribers for the FXS/FXO line
set blf monitoring_group		0-15	Set monitoring group number for FXS/FXO line
set echo cancellation direction outgoing			Set outgoing direction of echo cancellation (suppresses echo towards the subscriber)
set echo cancellation direction incoming			Set incoming direction of echo cancellation (suppresses echo from the subscriber)
set echo cancellation voice			Set echo cancellation method to voice

set echo cancellation nlp-off-voice			Set echo cancellation method to nlp-off-voice
set echo cancellation speex-algorithm			Set echo cancellation method to speex-algorithm
set echo cancellation off			Disable echo cancellation
set enable		no/yes	Disable/enable port
set fxo incoming-hotline			Set hotline number (incoming communication) for fxo port
set fxo outgoing-hotline			Set hotline number (outgoing communication) for fxo port
set fxo trunk_group	<TRUNK_INDEX>	0-254	Add fxo line to trunk group
set fxs AON number-for-redirection		off/on	Disable/enable the option to use AON number when redirecting to fxs
set fxs category		0-9, nochange	Set AON category to fxs
set fxs CID generation		Off/CallerID/CallerID_WO_500HZ/DTMF/FSK_BELL202/FSK_V23	Enable AON generating in one of the formats: (CallerID/CallerID_WO_500HZ/DTMF/FSK_BELL202/FSK_V23) or diable(off)
set fxs cliro		on/off	Enable/disable cliro service
set fxs deny_intervention		on/off	Enable/disable the service to deny interference in the conversation
set fxs display_name name		string, max 63 characters	Set the name to be passed to display name
set fxs display_name use		yes/no	Enable/disable display name usage
set fxs incoming-hotline			Set hotline number (incoming communication) for fxs port
set fxs notify_intervention	<ON_OFF>	off/on	Notify about the start of intervention
set fxs RingBack-tone filename			Set file name to be used instead of RingBack-tone
set fxs RingBack-tone mode		system-mode/ringback-tone/specific-file	Set RingBack-tone mode: • *system-mode* – use settings in system options; • *ringback-tone* – playing standard RBT; • *specific-file* – use an uploaded file as RBT
set fxs/fxo profile		0-31	Set fxs/fxo profiles
set gain rx		-230..20	Set gain, rx
set gain tx		-170..60	Set gain, tx
set name		string, max 63 characters	Set port name
set number			Set port phone number
set numplan	<PLAN_IDX>	0-15	Set dial plan for a port
set pbx profile	<PROFILE_IDX>	0-15	Set pbx profile for a port
set speex_AGC enable	<SPEEX_AGC_ENABLE>	no/yes	Enable/disable AGC for Speex
set speex_AGC max_gain	<SPEEX_MAX_GAIN>	0-40	Set maximum AGC gain
set speex_AGC max_gain_decrease	<SPEEX_AGC_DECREMENT>	1-40	Set maximum gain decreasing rate
set speex_AGC max_gain_increase	<SPEEX_AGC_INCREMENT>	1-40	Set maximum gain increasing rate
set speex_AGC target_volume_level	<SPEEX_AGC_LEVEL>	1-32768	Set the frequency that AGC will try to hold
show			Show port configuration

3.3.13 RingBack-tone configuration mode for FXS port

To enter this mode, it is necessary to run the **service** command in the FXS port configuration mode.

```
SMG-[CONFIG]-[FXS/FXO]-PORT[16]> service
Entering User-Service mode.
SMG-[CONFIG]-[FXS/FXO]-PORT[16]-SERVICE>
```

Command	Parameter	Value	Action
?			Show list of available commands
config			Return to the configuration menu
exit			Exit from this configuration submenu to a higher level
quit			End this CLI session
attach service block			Enable VAS for a subscriber
detach service block			Disable VAS for a subscriber
set call park get enable	<ON_OFF>	off/on	Retrieving a subscriber from call parking slot
set call park set enable	<ON_OFF>	off/on	Setting a subscriber to call parking slot
set call-pickup enable	<ON_OFF>	off/on	Enable the 'Call Pickup' service
set cfb enable	<ON_OFF>	off/on	Enable the 'Call Forwarding Busy' (CF Busy) service
set cfb number	<ON_OFF>	number of up to 30 characters or none	Set number for CF Busy service: *none* – disable redirection
set sfnr enable	<ON_OFF>	off/on	Enable the 'Call Forwarding No Reply' service
set sfnr number	<ON_OFF>	number of up to 30 characters or none	Set number for 'CF No Reply' service: *none* – disable redirection
set sft enable	<ON_OFF>	off/on	Enable the 'Call Forwarding by Time'
set sft number	<ON_OFF>	number of up to 30 characters or none	Set number for 'Call Forwarding by Time' service: *none* – disable redirection
set cft schedule	<SCHEDULE_IDX>	0-31	Set schedule index for forwarding by time
set cfu enable	<ON_OFF>	off/on	Enable the 'Unconditional Forwarding' service
set cfu number	<ON_OFF>	number of up to 30 characters or none	Set number for 'Unconditional Forwarding' service: *none* – disable redirection
set clear-all enable	<ON_OFF>	off/on	Enable the 'cancel all services' service
set conf-3way enable	<ON_OFF>	off/on	Enable the 'three-way conference' service. Previously, enable the 'Call hold' service
set conference enable	<ON_OFF>	off/on	Enable the 'Conference with consequent collection' service
set ct enable	<ON_OFF>	off/on	Enable the 'Call transfer' service. Previously, enable the 'Call hold' service
set disconnect_by_initiator enable	<ON_OFF>	off/on	Enable the 'Disconnect conference by initiator' service
set follow me no response active	<ON_OFF>	off/on	Activate the 'Follow me no response' service
set follow me no response enable	<ON_OFF>	off/on	Enable the 'Follow me no response' service

set follow me no response number		number of up to 30 characters or none	Set forwarding number for the 'Follow me no response'
set follow me no response pin		string of up to 4 digits	Set a PIN code to activate the 'Follow me no response' service
set follow me unconditional active	<ON_OFF>	off/on	Activate the 'Follow me' service
set follow me unconditional enable	<ON_OFF>	off/on	Enable the 'Follow me' service
set follow me unconditional number		number of up to 30 characters or none	Set forwarding number for the 'Follow me'
set follow me unconditional pin		string of up to 4 digits	Set a PIN code to activate the 'Follow me' service
set hold enable	<ON_OFF>	off/on	Enable the 'Call hold' service
set intervention enable	<ON_OFF>	off/on	Enable the 'Intervention into conversation' service
set one_touch_record enable	<ON_OFF>	off/on	Eanble the 'One touch record' service
set password change enable	<ON_OFF>	off/on	Enable the 'Password change' service
set password restrict out access active	<ON_OFF>	off/on	Password activation for the 'Password activation' service. The *on* value makes the password active and the communication restriction is removed
set password restrict out access enable	<ON_OFF>	off/on	Enable the 'Password activation' service. Previuosly, activate the service 'restriction of outgoing communication'
set password restrict out once enable	<ON_OFF>	off/on	Enable the 'outgoing communication by password' service. Previuosly, activate the service 'restriction of outgoing communication'
set password value	<VALUE>	string of up to 4 digits	Set a password for the 'restriction of outgoing communication' service
set restrict out enable	<ON_OFF>	off/on	Enable the 'restriction of outgoing communication' service
set restrict out value	<ACCESS_MODE>	On/ Denied_6/ Denied_7/ Denied_8	Restriction of outgoing communication mode: • *On* – everything is allowed; • *Denied_6* – access only to emergency; • *Denied_7* – access only to emergency, local and departmental communications; • *Denied_8* – access only to emergency, local, departmental and zonal communications
set speed_dial add	<SPEED_DIAL_CODE> <SPEED_DIAL_NUMBER>	0-9 number of up to 30 characters	Add a speed dial code
set speed_dial edit	<SPEED_DIAL_CODE> <SPEED_DIAL_NUMBER>	0-9 number of up to 30 characters	Change phone number for speed dial code
set speed_dial enable	<ON_OFF>	off/on	Enable/didable the 'speed dial'
set speed_dial remove	<SPEED_DIAL_CODE>	0-9	Delete code for speed dial

3.3.14 FXS/FXO profiles configuration mode (only SMG-200)

To enter this mode, run the **profile** command in the fxs/fxo configuration mode.

```
SMG-[CONFIG]-[FXS/FXO]> profile
SMG-[CONFIG]-[FXS/FXO]-[PROFILE]>
```

Command	Parameter	Value	Action
?			Show list of available commands
config			Return to the configuration menu
exit			Exit from this configuration submenu to a higher level
quit			End this CLI session
add	<PROFILE_NAME>	String, max 63 characters	Create a new profile
edit	<FXS_FXO_PROFILE_INDEX>	0-31	Going to the settings of the selected fxs/fxo profile
remove	<FXS_FXO_PROFILE_INDEX>	0-31	Delete a profile
show profile index	<FXS_FXO_PROFILE_INDEX>	0-31	Show the profile configuration
show profile list			Show the configuration of all profiles

To enter the mode for configuring the parameters of the current fxs/fxo profile, run the **edit** command in the fxs/fxo profile configuration mode.

```
SMG-[CONFIG]-[FXS/FXO]-[PROFILE]> edit 0
Entering FXS/FXO profile edit mode.
SMG-[CONFIG]-[FXS/FXO]-[PROFILE][0]>
```

Command	Parameter	Value	Action
?			Show list of available commands
config			Return to the configuration menu
exit			Exit from this configuration submenu to a higher level
quit			End this CLI session
default			Set default settings for current fxs/fxo profile
dial_sequence add			Add a dialing rule for fxo
dial_sequence remove	<SEQUENCE_ID>	1-65534	Delete a dialing rule for fxo
set fxo autoclip delete_used_records		yes/no	Enable/disable the option to delete used records
set fxo autoclip digits_match	<DIGITS_MATCH>	1-40	Set a number of matching digits of the number to use the AutoCLIP service
set fxo autoclip enable		yes/no	Enable/disable AutoCLIP
set fxo autoclip match_outgoing_port		yes/no	Enable/disable the option of checking the outgoing FXO port
set fxo autoclip record_keep_time		1-1440	Set record keep time for AutoCLIP
set fxo cpc_processing		yes/no	Enable/disable cpc processing option
set fxo dial_mode_in		hotline/collect	Set dial mode for incoming communication: ● *hotline* — hotline; ● *collect* — extension dialing
set fxo dial_mode_out		DTMF/pulse	Set dial mode for outgoing communication (DTMF/pulse)
set fxo dial_pause		1-10	Set pause time before dialing
set fxo dial_trigger		pause/ dialtone_detect	Set dialing start mode for outgoing calls: ● *pause* – after a pause;

			• *dialtone_detect* – after station answer
`set fxo number_dialing`		`hotline/ full_number/ stripped_number/ extra_dialing`	Set a called subscriber number generation mode for outgoing communication (`hotline/full_number/stripped_number/extra_dialing`)
`set fxo off_hook_on`		`seize/ remote_side_ringing/ remote_side_answer`	Set answer mode for incoming communication: • *seize* – response upon engagement; • *remote_side_ringing* – response when calling the remote side; • *remote_side_answer* – response when the remote side answers. The option is available only in the dialing mode 'hot line (incoming communication)'
`set fxo pulse_interdigit`		`80-2500`	Set the duration of the inter-digit interval for the pulse mode
`set fxo pulse_length`		`50-120`	Set pause duration for digit dialing for pulse mode
`set fxo pulse_width`		`50-120`	Set the pulse duration of the number digit for the pulse mode
`set fxo radius_profile`		`0-31`	Set the radius profile to be used for incoming communication
`set fxo seize_mode`		`with_callerID/ after_first_rin/ at_first_ring`	Set seize detection mode: • *with_callerID* – upon receiving CallerID; • *after_first_ring* – after the end of the first sending of calls; • *at_first_ring* – at the beginning of the first call
`set fxo send_answer_on`		`seize/ dial_tone/ end_of_dial/ ringback_tone`	Set the response mode for outgoing communication: • *seize* – the response will be sent immediately after the engagement is detected; • *dial_tone* – the response will be sent after remote station response; • *end_of_dial* – the response will be sent after finishing the dial; • *ringback_tone* – the response will be sent after detection of remote station's ringback tone
`set fxo tone_detect busytone`			Set the parameters for detecting the 'busy' signal
`set fxo tone_detect dialtone`			Set the parameters for detecting the 'station answer' signal
`set fxo tone_detect disconnect_tone`			Set the parameters for detecting the 'disconnect tone' signal
`set fxo tone_detect ringback_tone`			Set the parameters for detecting the ringback signal
`set fxs cpc_time`		`200-900`	Set the value of the CPC duration parameter for the fxs profile
`set fxs dial_mode`		`hotline/collect`	Set dial mode: • *hotline* — hotline • *collect* — extension dialing
`set fxs generate_cpc`		`yes/no`	Enable/disable the option to generate cpc
`set fxs hold_set_remove_by`		`flash/flash/*/ flash/#/flash/*/`	Set the HOLD mode for set/remove

		#	
set fxs ignore_flash		yes/no	Enable/ disable the option to ignore flash
set fxs max_pulse_time		20-120	Set the value of the maximum pulse duration of a digit
set fxs min_flash_time		70-2000	Set the value of the minimum flash detection time parameter
set fxs min_interdigit_time		100-400	Set the value of the minimum interdigit interval parameter
set fxs min_onhook_time		200-2000	Set the value of the minimum clearback detection time parameter
set fxs radius_profile		0-31	Set radius profile, that will be used for incoming communication
set fxs speed_dial_enable		yes/no	Enable/disable 'speed dial' service
set name		string, max 63 characters	Set fxs/fxo profile name
show			Show current profile configuration
speed dial add	<SPEED DIAL CODE> <SPEED DIAL NUMBER>	0-9 number of up to 30 characters	Add a speed dial code
speed dial edit	<SPEED DIAL CODE> <SPEED DIAL NUMBER>	0-9 number of up to 30 characters	Change phone number for speed dial code
speed dial remove	<SPEED DIAL CODE>	0-9	Delete speed dial code

3.3.15 H.323 protocol parameters configuration mode

To enter this mode, in the configuration mode run the **h323 interface <H323_INDEX>** command, where **<H323_INDEX>** is the the number of the direction operating over H.323 protocol.

```
SMG-[CONFIG]> h323 interface 0
Entering H323-mode.
SMG-[CONFIG]-H323-INTERFACE[0]>
```

Command	Parameter	Value	Action
?			Show list of available commands
access category	<CAT_IDX>	0-31	Assign an access category
alias H323ID clear	<H323ID>	string, max 63 characters	Remove gateway name when registering with Gatekeeper
alias H323ID set	<H323ID>	string, max 63 characters	Add gateway name when registering with Gatekeeper
cisco1700 adaptation	<ON_OFF>	on/off	Enable/disable cisco1700 adaptation
codec disable	<CODEC_IDX>	0-3	Disable the selected codec. Codecs are numbered by priority — from 0 (highest) to 3 (lowest)
codec pte	<CODEC_IDX> <PTE>	0-3 10/20/30/40/50/ 60/70/80/90	Set payload time
codec ptype	<CODEC_IDX> <PTYPE>	0-3 0-127 or static	Set payload type. The value 'static' sets the default value depending on the selected codec
codec set	<CODEC_IDX> <CODEC>	0-3 G.711-U/ G.711-A/ G.729/	Set the used codec
config			Return to the configuration menu
destination clear			Delete destination for an interface
destination set	<HOSTNAME>	string, max 63 characters	Set destination for an interface
DSCP RTP	<DSCP_RTP>	0-63	Set the DSCP identifier for RTP traffic
DSCP SIG	<DSCP_SIG>	0-63	Set the DSCP identifier for SIG traffic
DTMF mode	<DTMF_m>	inband/ RFC2833/	DTMF mode for this interface
DTMF payload	<DTMF_p>	96-127	Set payload type for RFC2833
echo-cancellation direction	<ECAN_DIR>	outgoing/incoming	Set echo-cancellation direction (incoming/outgoing)
echo-cancellation mode	<ECAN_MODE>	voice/ nlp-off-voice/ speex-algorithm/ off	Set echo-cancellation mode: • *Voice* – echo cancellers enabled; • *Nlp-off-voice* – echo cancellers enabled in voice mode, non-linear NLP processor disabled. In the case when the levels of signals at transmission and reception are very different, a weak signal can be suppressed by a non-linear NLP processor. To prevent this from happening, use this mode of operation of echo

			cancellers; • *Speex-algorithm;* • *Off* – do not use echo cancellation (this mode is set by default)
exit			Exit from this configuration submenu to a higher level
faststart	<ON_OFF>	on/off	Enable/disable faststart
gain rx	<GAIN>		Set the volume for voice reception, amplify/attenuate the level of the signal received from the interacting gateway and output to the speaker of the telephone set connected to the SMG gateway
gatekeeper	<ON_OFF>	on/off	Enabling/disabling the use of GK (gatekeeper)
h245tunneling	<ON_OFF>	on/off	Enabling/disabling the use of tunneling
history			View the history of entered commands
interface rtp	<IFACE_NAME>	String, max 255 characters	Selecting a network interface for RTP transmission
max_active	<MAX_ACTIVE>	0-65535	Set the maximum number of active connections for an interface
name	<s_name>	allowed to use letters, digits, '_' symbol, maximum 31	Set a name for H.323 interface
numbering plan	<NUMPLAN>	0-15/0-255	Select a dial plan
port	<PORT>	1-65535	Set a TCP port of interworking gateway on which it receives SIP signaling
quit			End this CLI session
routing_profile	<prof>	0-127	Select a scheduled routing profile
show config			Show the H323 interface information
t38 redundancy	<T38_REDUNDANCY>	off/1/2/3	Use redundant frames for error protection: *off* – do not use
trunk	<TRUNK>	0-31	Set trunk group number for interface
VAD_CNG	< ON_OFF >	on/off	Enable/disable speech activity detector/comfort noise generator for interface

3.3.16 Hunt group configuration mode

To enter this mode, in the configuration mode run the **hunt-group <hunt-group_INDEX>** command, where **<hunt-group _INDEX>** is the the number of the hunt group.

```
SMG-[CONFIG]> hunt-group 0
Entering HuntGroup-mode.
SMG-[CONFIG]-HUNT-GROUP[0]>
```

Command	Parameter	Value	Action
?			Show list of available commands
config			Return to the configuration mode
exit			Going from this configuration submenu to a higher level
history			View the history of entered commands
move number to		end position start	Move the number to the end of the list Move the number to a specific position Move the number to the top of the list
quit			End this CLI session
set conference number		*,#,D,0-9. Or 'none' for blank(delete) number	Set conference number
set ltimer		number in the range 5-255	Set L-timer for a group call
set mode		(all/seqFisrt/ seqNext/ seqAllFirst/ seqAllNextr)	Set group operation mode
set name		letter or number or '_', '.', '-'. Max 63 symbols	Set hunt group name
set number			Set hunt group member number
set stimer		number in the range 5-255	Set S-timer for one group member call
set number-mask		max 255 symbols	Set mask for hunt group
set recall-busy		yes/no	Enable/disable the 'recall busy' option
set recall-declined		yes/no	Enable/disable the 'recall declined' option
set release-mode	<MODE>	yes/no	Set hunt group clear mode – Default/Quiet

3.3.17 SS7 linkset configuration mode (only SMG-500)

To enter this mode, in the configuration mode run the **linkset <LINKSET_INDEX>** command, where **<LINKSET_INDEX>** is the the linkset number.

```
SMG-[CONFIG]> linkset 0
Entering Linkset-mode.
SMG-[CONFIG]-LINKSET[0]>
```

Command	Parameter	Value	Action
?			Show list of available commands
access category	<CAT_IDX>	0-31	Assign an access category for a linkset
alarm_ind	<ON_OFF>	on/off	Enable/disable alarm indication for this SS7 linkset
CCI	<ON_OFF>	on/off	Enable link integrity check support in SS7 linkset
CCI frequency	<FREQ>	0-127	Set the frequency of link integrity checks for outgoing calls via SS7 linkset
cdpn digit in IAM	<ON_OFF>	on/off	Sending the first digit of the CdPN number in the IAM message when dialing using the overlap method
chan_order	<CHAN_SELECT>	up_ring/ down_ring/ up_start/ down_start/ odd_up_ring/ odd_down_ring/ even_up_ring/ even_down_ring	Set the channel engagement order for a given group of SS7 lines: • *up_ring* – sequentially forward; • *down_ring* – sequentially backward; • *up_start* – starting from the first forward; • *down_start* – starting from last backward; • *odd_up_ring* – sequentially forward odd; • *odd_down_ring* – sequentially backward odd; • *even_up_ring* – sequentially forward even; • *even_down_ring* – sequentially backward even
china	<ON_OFF>	on/off	Enable/disable support mode for Chinese SS7 protocol specification
combined	<ON_OFF>	on/off	Enable/disable the use of combined mode
config			Return to the configuration mode
DPC	<DPC_ID>	0-16383	Set the code of the opposite signaling point – DPC
emergency alignment	<ON_OFF>	on/off	Emergency alignment with one signal link in a linkset
exit			Going from this configuration submenu to a higher level
history			View the history of entered commands
ignore hold	<ON_OFF>	off/on	Ignore received CPG with remote hold or remote retrieval attributes
init	<INIT_MODE>	blocked/ individual-ublock/ group-unblock/ group-reset	Set the type of initialization for the given linkset
interworking	<INTERWORK>	no_change/	Set the indicator of the presence of

		no_encountered/ encountered	interaction with other alarm systems: • *no_change* – broadcast the value unchanged from the incoming call; • *no_encountered* – do not report about the interaction with a network that does not support most of the services provided by the ISDN network; • *encountered* – report about the intercation in some areas (ISDN network interworking with a network that does not support most of the services provided by the ISDN network and cannot use the functions that are normally used)
name	<s_name>	allowed to use letters, digits, '_' symbol, maximum 31 characters	Set a name for this linkset
net_ind	<NET_IND>	international/ reserved/federal/ national	Set network identifier: • *international* – international network; • *reserved* – reserve; • *federal* – federal network; • *national* – local network
numbering plan		0-15	Select a dial plan for a LinkSet
OPC	<OPC_ID>	0-16383	Set the code of your own signaling point for this SS7 linkset
primary linkset	<PRI_LINKSET>	0-15	Selection of the primary SS7 linkset, when operating in combined mode
quit			End this CLI session
release on suspend	<ON_OFF>	on/off	Issue/do not issue disconnect messages when a suspend message is received
reserv linkset	<RES_LINKSET>	0-15	Select a reserve SS7 linkset
routing_profile	<prof>	0-127	Select a scheduled routing profile
satellite	<SATELLITE>	override_no_satellite /transit/ add_one	Determine the presence of a satellite channel when working through this SS7 linkset
secondary linkset	<SEC_LINKSET>	0-15	Select the secondary SS7 linkset, when operating in combined mode
show			Show the configuration of this SS7 linkset
ss7timers	<index>	0-15	Select the SS7 timer profile
stream SLC	<ON_OFF>	off/on	Enable/disable the option 'Stream order by SLC'
TMR	<TMR>	speech/ 64kb_unrestricted/ 3.1KHz_audio/ transit	Set the transmission medium requirements for a given group of SS7 linkset
trunk	<trunk_index>	0-31	Set trunk group number for this SS7 linkset

3.3.18 SS7 timers configuration mode

To enter this mode, in the configuration mode run the **ss7timers <SS7_TIMERS_INDEX>** command, where **<SS7_TIMERS_INDEX>** is the profile number.

```
SMG-[CONFIG]> ss7timers 0
Entering SS7Timers-mode.
SMG-[CONFIG]-SS7-TIMERS[0]>
```

Command	Parameter	Value	Action
?			Show list of available commands
config			Return to the configuration menu
exit			Going from this configuration submenu to a higher level
history			View the history of entered commands
quit			End this CLI session
set mtp2 T1	<TIMER>	400-500	Set MTP2 T1 timer (x100ms)
set mtp2 T2	<TIMER>	50-500	Set MTP2 T2 timer (x100ms)
set mtp2 T3	<TIMER>	10-20	Set MTP2 T3 timer (x100ms)
set mtp2 T4 normal	<TIMER>	75-95	Set MTP2 T4 normal timer (x100ms)
set mtp2 T4 emergency	<TIMER>	4-6	Set MTP2 T4 emergency timer (x100ms)
set mtp2 T6	<TIMER>	30-60	Set MTP2 T6 timer (x100ms)
set mtp2 T7 normal	<TIMER>	5-20	Set MTP2 T7 normal timer (x100ms)
set mtp3 T2	<TIMER>	7-20	Set MTP3 T2 timer (x100ms)
set mtp3 T4	<TIMER>	5-12	Set MTP3 T4 timer (x100ms)
set mtp3 T12	<TIMER>	8-15	Set MTP3 T12 timer (x100ms)
set mtp3 T13	<TIMER>	8-15	Set MTP3 T13 timer (x100ms)
set mtp3 T14	<TIMER>	20-30	Set MTP3 T14 timer (x100ms)
set mtp3 T17	<TIMER>	8-15	Set MTP3 T17 timer (x100ms)
set mtp3 T22	<TIMER>	1800-3600	Set MTP3 T22 timer (x100ms)
set mtp3 T23	<TIMER>	1800-3600	Set MTP3 T23 timer (x100ms)
set isup T1	<TIMER>	150-600	Set ISUP T1 timer (x100ms)
set isup T5	<TIMER>	3000-9000	Set ISUP T5 timer (x100ms)
set isup T6	<TIMER>	100-600	Set ISUP T6 timer (x100мс)
set isup T7	<TIMER>	200-300	Set ISUP T7 timer (x100ms)
set isup T8	<TIMER>	150-600	Set ISUP T8 timer (x100ms)
set isup T9	<TIMER>	300-2400	Set ISUP T9 timer (x100ms)
set isup T12	<TIMER>	150-600	Set ISUP T12 timer (x100ms)
set isup T13	<TIMER>	3000-9000	Set ISUP T13 timer (x100ms)
set isup T14	<TIMER>	150-600	Set ISUP T14 timer (x100мс)
set isup T15	<TIMER>	3000-9000	Set ISUP T15 timer (x100ms)
set isup T16	<TIMER>	150-600	Set ISUP T16 timer (x100ms)
set isup T17	<TIMER>	3000-9000	Set ISUP T17 timer (x100ms)
set isup T18	<TIMER>	150-600	Set ISUP T18 timer (x100ms)
set isup T19	<TIMER>	3000-9000	Set ISUP T19 timer (x100ms)
set isup T20	<TIMER>	150-600	Set ISUP T20 timer (x100ms)
set isup T21	<TIMER>	3000-9000	Set ISUP T21 timer (x100ms)
set isup T22	<TIMER>	150-600	Set ISUP T22 timer (x100ms)
set isup T23	<TIMER>	3000-9000	Set ISUP T23 timer (x100мс)
set isup T24	<TIMER>	1-20	Set ISUP T24 timer (x100ms)
set isup T25	<TIMER>	10-100	Set ISUP T25 timer (x100ms)
set isup T26	<TIMER>	600-1800	Set ISUP T26 timer (x100ms)
set isup T33	<TIMER>	120-150	Set ISUP T33 timer (x100ms)
set isup T34	<TIMER>	20-40	Set ISUP T34 (x100ms)
set isup T35	<TIMER>	150-200	Set ISUP T35 timer (x100ms)
show			Show configuration

3.3.19 Modifiers table configuration mode

To enter this mode, in the configuration mode run the **modifiers table < MODTBL_INDEX>** command, where **<MODTBL_INDEX>** is the table number.

```
SMG-[CONFIG]> modifiers table 0
Entering modifiers-table mode.
SMG-[CONFIG]-MODTABLE[0]>
```

Command	Parameter	Value	Action
?			Show list of available commands
add	<MODIFIER_MASK> [CLD_RULE] [CLG_RULE]	modifier mask, maximum 255 characters, must be enclosed in parentheses '(' and ')' modifier rule, maximum 30 characters, should be enclosed in quotes modifier rule, maximum 30 characters, should be enclosed in quotes	Add a modifier: • *MODIFIER_MASK* – modifier mask; • *CLD_RULE* – called number conversion rule; • *CLG_RULE* – calling number conversion rule
change aoncat	<MODIFIER_INDEX> <AONCAT>	0-512 0-9/any	Edit AON category number for a modifier: • *MODIFIER_INDEX* – modifier number; • *AONCAT* – AON category
change called numbering plan type	<MODIFIER_INDEX> <CALLED_NP_TYPE>	0-8191 nochange; unknown; isdn/telephony; national; private	Edit modifier dial plan type for called party number: • *MODIFIER_INDEX* – modifier number; • *CALLED_NP_TYPE* – dail plan type.
change called rule	<MODIFIER_INDEX> <CALLED_RULE>	0-8191 modifier rule, maximum 30 characters, should be enclosed in quotes	Edit call number conversion rule for modifier: • *MODIFIER_INDEX* – modifier number; • *CALLED_RULE* – called number conversion rule.
change called type	<MODIFIER_INDEX> <CALLED_TYPE>	0-8191 unknown/	Edit called number type for modifier: • *MODIFIER_INDEX* – modifier number;

		subscriber/ national/ international/ network_specific/ nochange	• *NUM_TYPE* – subscriber number type: • *Subscriber* – used for servicing local calls and incoming long distance calls; • *National* – used when serving outgoing long distance calls, or local and incoming long distance calls instead of Subscriber; • *International* – used on long-distance lines and CLR trunks when servicing outgoing international calls; • *network_specific* – special network number; • *unknown* – undefined number type; • *nochange* – do not change number type
change calling category	<MODIFIER_INDEX> <CALLING_CAT_AON>	0-8191 0-9/nochange	Edit AON category number of a calling subscriber for modifier
change calling numbering plan type	<MODIFIER_INDEX> <CALLING_NP_TYPE>	0-8191 nochange/ unknown/ isdn/ telephony/ national/ private	Edit modifier dial plan type for caller number: • *MODIFIER_INDEX* – нomodifier number; • *CALLING_NP_TYPE* – dial plan type
change calling presentation	<MODIFIER_INDEX> <CALLING_PRESENT>	0-8191 allowed/ restricted/ not_available/ spare/ nochange	Edit representation transfor-mation rule of a calling subscriber
change calling rule	<MODIFIER_INDEX> <CALLING_RULE>	0-8191 modifier rule, maximum 30 characters, should be enclosed in quotes	Edit number transformation rule of a calling subscriber: • *MODIFIER_INDEX* – modifier number; • *CALLING_RULE* – transfor-mation rule of a calling number
change calling screen	<MODIFIER_INDEX> <CALLING_SCREEN>	0-8191 not_screened/ user_passed/ user_failed/ network/nochange	Edit screen indicator transfor-mation rule of a calling subscriber
change calling type	<MODIFIER_INDEX> <CALLING_TYPE>	0-8191 unknown/ subscriber/ national/	Edit calling number type for modifier: • *MODIFIER_INDEX* – modifier number;

		international/
		network_specific/
		nochange
			• *NUM_TYPE* – subscriber number type:
			  • *Subscriber* – used for servicing local calls and incoming long distance calls;
			  • *National* – used when servicing outgoing long distance calls, or local and incoming long distance calls instead of Subscriber;
			  • *International* – used on long-distance lines and CLR trunks when servicing outgoing international calls;
			  • *network_specific* – special network number;
			  • *unknown* – undefined number type;
			  • *nochange* – do not change number type

change general access-cat	<MODIFIER_INDEX> <ACCESS>	0-8191 0-31/nochange	Edit general modifier access category
change general numplan	<MODIFIER_INDEX> <NUMPLAN>	0-8191 0-15/nochange	Edit general modifier dial plan
change mask	<MODIFIER_INDEX> <MODIFIER_MASK>	0-8191 modifier mask, maximum 255 characters, must be enclosed in parentheses '(' and ')'	Edit modifier mask: • *MODIFIER_INDEX* – modifier number; • *MODIFIER_MASK* – mask
change modtable	<MODIFIER_INDEX> <NEW_MODTBL_INDEX>	0-8191 0-255	Move the modifier to the table with the specified number

change numtype	<MODIFIER_INDEX>
	
	<NUM_TYPE>
		0-8191
		
		unknown/
		subscriber/
		national/
		international/
		network_specific/
		any
			Edit modifier number type:
			• *MODIFIER_INDEX* – modifier number;
			• *NUM_TYPE* – subscriber number type:
			  • *Subscriber* – used for servicing local calls and incoming long distance calls;
			  • *National* – used when servicing outgoing long distance calls, or local and incoming long distance calls instead of Subscriber;
			  • *International* – used on long-distance lines and CLR trunks when servicing outgoing international calls;
			  • *network_specific* – special network number;
			  • *unknown* – undefined number type;
			  • *any* – any number type

exit			Exit from this configuration submenu to a higher level

history			View the history of entered commands
quit			End this CLI session
remove	<MODIFIER_INDEX>	0-8191	Remove the specified modifier
show	<MODIFIER_INDEX>	0-8191	Show modifier configuration

3.3.20 Network parameter configuration modec

To enter this mode, in the configuration mode run the **network** command.

```
SMG-[CONFIG]> network
Entering Network mode.
SMG-[CONFIG]-NETWORK>
```

Command	Parameter	Value	Action
?			Show list of available commands
add interface tagged	dynamic/static <LABEL> <VID> <IPADDR> <NETMASK>	allowed to use letters, digits, '_', '.', '-', ':' symbols, maximum 255 characters 1-4095 IP address in the AAA.BBB.CCC.DDD format Netmask in the AAA.BBB.CCC.DDD format	Add a new network interface • *LABEL* – interface name; • *VID* – VLAN ID; • *IPADDR* – IP address; • *NETMASK* – netmask
add interface untagged	dynamic/static <LABEL> <IPADDR> <NETMASK>	allowed to use letters, digits, '_', '.', '-', ':' symbols, maximum 255 characters IP address in the AAA.BBB.CCC.DDD format Netmask in the AAA.BBB.CCC.DDD format	Add a new network interface • *LABEL* – interface name; • *IPADDR* – IP address; • *NETMASK* – netmask
config			Return to the configuration menu
confirm			Confirm changed network and VLAN settings without rebooting the gateway. If the applied network settings are not confirmed within a minute, their values will return to their original values
dhcp server			Switching to DHCP server settings configuration mode
exit			Exit from this configuration submenu to a higher level
history			View the history of entered commands

ntp			Switching to NTP configuration mode
quit			End this CLI session
remove interface	<NET_IFACE_IDX>	0-39	Delete the specified interface
rollback			Cancel changes
set interface COS	<NET_IFACE_IDX> <COS>	0-39 0-7	Assign 802.1p priority to the specified interface
set interface dhcp	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Receive network settings dynamically from a DHCP server for a specified interface
set interface dhcp_dns	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Obtain DNS server IP address dynamically from DHCP server for specified interface
set interface dhcp_no_gw	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Do not get gateway settings dynamically from DHCP server for specified interface
set interface gateway	<NET_IFACE_IDX> <IPADDR>	0-39 IP address in the AAA.BBB.CCC.DDD format	Set the default gateway for an interface
set interface dhcp_ntp	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Get NTP settings dynamically from a DHCP server for a specified interface
set interface gw_ignore	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Ignore the gateway setting for the specified interface
set interface h323	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Allow H323 signaling exchange for the specified interface
set interface ipaddr	<NET_IFACE_IDX> <IPADDR> <NETMASK>	0-39 IP address in the AAA.BBB.CCC.DDD format Netmask in the AAA.BBB.CCC.DDD format	Set the IP address and netmask for the specified interface
set interface network-label	<NET_IFACE_IDX> <LABEL>	0-39 digits, '_', '.', '-', ':' symbols, maximum 255 charecters	Set a name for this interface
set interface radius	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Allow RADIUS messaging through interface
set Interface rtp	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Allow transmission of RTP packets through the interface
set interface signaling	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Allow SIP messaging through interface
set interface snmp	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Allow transmission of SNMP packets through the interface
set interface ssh	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Allow ssh session through the interface
set interface telnet	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Allow telnet session through the interface
set interface VID	<NET_IFACE_IDX> <VID>	0-39 1-4095	Assign a VID to an interface
set interface web	<NET_IFACE_IDX> <ON_OFF>	0-39 on/off	Allow access via web interface

set settings dns primary	<IPADDR>	IP address in the AAA.BBB.CCC.DDD format	Set the IP address of the primary DNS server
set settings dns secondary	<IPADDR>	IP address in the AAA.BBB.CCC.DDD format	Set the IP address of the reserve DNS server
set settings gateway_iface	<NET_IFACE_NAME>		The name of the interface the gateway of which will be the primary gateway by default
set settings hostname	<HOSTNAME>	allowed to use letters, digits, '_', '.', '-' symbols, maximum 63 characters	Set hostname
set settings ssh	<PORT>	1-65535	Set the TCP port for accessing the device via the SSH protocol, the default is 22
set settings telnet	<PORT>	1-65535	Set the TCP port for accessing the device via the Telnet protocol, the default is 23
set settings web	<PORT>	1-65535	Set TCP port for web configurator, the default is 80
set use_ip_list	<ON_OFF>	on/off	Enable/disable the use of the white IP address list
show interface by_index			Show the settings of the specified network interface
show interface list			Show list of available network interfaces
show settings			Show network parameters
snmp			Switching to SNMP configuration mode
ssh restart			Restarting the SSH process

After changing the IP address, network mask, or when control is disabled via the web configurator on the network interface, you must confirm these settings with the *confirm* command, otherwise, after a two-minute timer, the configuration will be return to the previous one.

3.3.20.1 DHCP server parameter configuration mode

To enter this mode, in the network parameters configuration mode run the **dhcp server** command.

```
SMG-[CONFIG]-NETWORK> dhcp server
Entering NTP mode.
SMG-[CONFIG]-[NETWORK]-NTP>
```

Command	Parameter	Value	Action
?			Show list of available commands
conflicttime	<CONFLICT>	10-10000000	Set the period of time for which the IP address will be reserved if a MAC address conflict is detected, at least 10 seconds
declinetime	<DECLINE>	10-10000000	The period of time for which the IP address will be reserved in case of receiving a DHCP decline message, at least 10 seconds
dhcpd start			Start DHCP Server
dhcpd stop			Stop DHCP Server
dns 0/1/2/3	<DNS>	IP address in the AAA.BBB.CCC.DDD format	Set DNS server addresses from the operator's network
domain	<DOMAIN>	string no longer than 31 characters	Set default domain name for DHCP clients
enabled	<ENABLE>	no/yes	Start / do not start DHCP server at gateway startup
exit			Exit from this configuration submenu to a higher level
gateway	<GW>	IP address in the AAA.BBB.CCC.DDD format	Set the default router or gateway address assigned to DHCP server clients
interface	<IFACE NAME>	string up to 255 characters	Select a network interface for a DHCP server
ipaddr end	<IPADDR>	IP address in the AAA.BBB.CCC.DDD format	Set the ending address of assigned IP address range
ipaddr start	<IPADDR>	IP address in the AAA.BBB.CCC.DDD format	Set the starting address of assigned IP address range
max lease	<MAX LEASE>	10-10000000 sec	Set the maximum time for the device to use the IP address assigned by the DHCP server to at least 10 seconds
maxleases	<MAXLEASES>	1-65535	Set limits on the number of leased addresses
min lease	<MIN LEASE>	10-10000000 sec	Set the minimum time for the device to use the IP address assigned by the DHCP server, at least 10 seconds
netmask	<NETMASK>	IP address in the AAA.BBB.CCC.DDD format	Set netmask
ntp announce external server address	<NTP SERVER>	IP address in the AAA.BBB.CCC.DDD format	Set external NTP server address to announce in option 42
ntp announce external server enable	<ANNOUNCE EXT>	no/yes	Allow to announce external NTP server in option 42
ntp announce local	<ANNOUNCE LOCAL>	no/yes	Allow to announce local NTP server in option 42
offerime	<OFFER>	10-10000000	Set the time period for which

			the requested IP address will be reserved, at least 10 seconds
quit			End this CLI session
savetime	<SAVE>	7200-10000000/off	Set the period of time after which the device will save information about leased addresses to the file dhcpd.leases off – do not save the database
show config			Show DHCP configuration: usage status, address range, netmask, default gateway, domain addresses, Wins servers, number of leased addresses, query times
static lease add 	 <NAME> <IPADDR> <MAC>	 string no longer than 31 characters IP address in the AAA.BBB.CCC.DDD format MAC-address in the XX:XX:XX:XX:XX:XX format	Assign static mappings of IP and MAC addresses: • *NAME* – mapping name; • *IPADDR* – IP address; • *MAC* – MAC address
static lease remove	<INDEX>	0-4095	Delete the specified rule in the table of static IP and MAC addresses
static lease show			Show table of static mappings of IP and MAC addresses
wins	<WINS>	IP address in the AAA.BBB.CCC.DDD format	Set the IP address of the primary WINS server to be used by the DHCP client

3.3.20.2 NTP protocol configuration mode

To enter this mode, in the network parameter configuration mode run the **ntp** command.

```
SMG-[CONFIG]-NETWORK> ntp
Entering NTP mode.
SMG-[CONFIG]-[NETWORK]-NTP>
```

Command	Parameter	Value	Action
?			Show list of available commands
apply		no/yes	Apply/reject NTP settings
config			Return to the configuration menu
exit			Exit from this configuration submenu to a higher level
quit			End this CLI session
restart ntp		no/yes	Restart NTP process
set ntp dhcp	NET_IFACE_IDX ON_OFF	Network interface index off/on	Get NTP settings over DHCP from a given interface
set ntp period	NTP_PERIOD	10-1440	Set time synchronization period
set ntp server	NTP	String, 63 characters	Set the address of the NTP server with which the SMG will synchronize
set ntp usage	ON_OFF	off/on	NTP client activation
show config			Show ntp configuration
timezone set		GMT/GMT+1/GMT-1/GMT+2/GMT-2/GMT+3/GMT-3/GMT+4/GMT-4/GMT+5/GMT-5/GMT+6/GMT-6/GMT+7/GMT-7/GMT+8/GMT-8/GMT+9/GMT-9/GMT+10/GMT-10/GMT+11/GMT-11/GMT+12 Asia Europe	Set timezone relative to UTC Set the city location in Asia Set the city location in Europe

3.3.20.3 SNMP protocol configuration mode

To enter this mode, in the configuration mode run the **snmp** command.

```
SMG-[CONFIG]-NETWORK> snmp
Entering SNMP mode.
SMG-[CONFIG]-SNMP>
```

Command	Parameter	Value	Action
?			Show list of available commands
add	<TYPE> <IP> <COMM> <PORT>	trapsink/ trap2sink/ informsink IP address in the AAA.BBB.CCC.DDD format string up to 31 characters 1-65535	Add an SNMP trap rule: • *TYPE* – SNMP message type; • *IP* – trap receiver IP address; • *COMM* – password contained in traps; • *PORT* – trap Receiver UDP Port
config			Return to the configuration mode
create user	<LOGIN> <PASSWD>	string up to 31 characters password from 8 to 31 characters	Create a user (assign a login and password for access)
exit			Exit from this configuration submenu to a higher level
history			View the history of entered commands
modify community	<IDX> <COMM>	0-15 string up to 31 characters	Change SNMP trap rule (password contained in traps)
modify ip	<IDX> <IP>	0-15 IP address in the AAA.BBB.CCC.DDD format	Edit SNMP trap rule (Trap Destination Address)
modify port	<IDX> <PORT>	0-15 1-65535	Change SNMP trap rule (Trap Destination Port)
modify type	<IDX> <TYPE>	0-15 trapsink/ trap2sink/ informsink	Change SNMP trap rule (SNMP message type)
quit			End this CLI session
remove	<IDX>	0-15	Delete SNMP trap rule
restart snmpd	Yes/no		Restart SNMP client
ro	<RO>	string up to 63 characters long	Set a password for reading parameters
rw	<RW>	string up to 63 characters long	Set a password for reading and writing parameters
show			Show SNMP configuration
syscontact	<SYSCONTACT>	string up to 63 characters long	Specify contact information
syslocation	<SYSLOC>	string up to 63 characters long	Specify the device location
sysname	<SYSNAME>	string up to 63 characters long	Specify the device name

3.3.21 Dial plan configuration mode

To enter this mode, in the configuration mode run the **numplan** command.

```
SMG-[CONFIG]> numplan
Entering Numbering-plan mode.
SMG-[CONFIG]-[NUMPLAN]>
```

Command	Parameter	Value	Action
?			Show list of available commands
config			Return to the configuration mode
create prefix	<IDX_Numplan>	0-15	Create a prefix in a given dial plan
delete prefix	<IDX Prefix>		Delete given prefix
exit			Exit from this configuration submenu to a higher level
history			View the history of entered commands
prefix			Switch to prefix configuration mode
quit			End this CLI session
set active		1-16	Set a number of active dial plans
set domain	<IDX> <DOMAIN>	0-15 string up to 15 characters long	Assign a domain for registration
set name	<IDX> <NAME>	0-15 string up to 15 characters long	Set name for a dial plan
show active count			Show a number of active dial plans
show active list			Show a list of active dial plans
show list			Show a list of dial plans
show prefixes	<IDX>	0-15 no/yes	Show dial plan prefixes with the specified number

3.3.21.1 Prefix configuration mode

To enter this mode, in the configuration mode run the **prefix <PREFIX_INDEX>** command, where **<PREFIX_INDEX>** is the prefix number.

```
SMG-[CONFIG]-[NUMPLAN]> prefix 0
Entering Prefix-mode.
SMG-[CONFIG]-[NUMPLAN]-PREFIX[0]>
```

Command	Parameter	Value	Action
?			Show list of available commands
access category	<CAT_IDX>	0-31	Assign an access category for a linkset
access check	<ON_OFF>	on/off	Check/do not check access category
called npi	<PFX_CLD_NPI>	transit/ unknown/ isdn/ telephony/ national/ private	Change called number type (transit – do not transform)
called type	<PFX_CLD_TYPE>	unknown/ subscriber/ national/ international/ specific_net/ transit	Called number type transformation (transit – do not transform): • *Subscriber number* – applies to local calls and incoming long distance calls. In this case, the transmitted number should look like: abxxxxx, or bxxxxx, or xxxxx; • *National number* – used when servicing outgoing long distance calls or local and incoming long distance calls instead of Subscriber. In this case, the transmitted number should look like: ABCabxxxxx, or 2abxxxxx, or 10 < international number >; • *International number* – used on long-distance lines and CLR trunks when servicing outgoing international calls. In this case, the transmitted number should look like: <international number> (without the prefix '10' for accessing the international network)
command	<PFX_COMMAND>	set/ clear/ control	Select an action for a service: • *set* – set VAS service; • *clear* – cancel VAS service; • *control* – control VAS service activity
config			Return to the configuration mode
dial mode	<MODE>	nochange/ enblock/ overlap	Set dialing mode by prefix: • *enblock* – the number of the called subscriber is transmitted in a block; • *overlap* – the called party number is transmitted with overlap (one digit each); • *nochange* – the number of the called subscriber is transmitted in the form in which it was received from the incoming channel

direction	<PFX_DIRECTION>	local/ emergency/ zone/ vedomst/ toll/ international	Set type of access to trunk group or direction: ● *local* – local; ● *emergency* – call of emergency services; ● *zone* – zone; ● *vedomst* – to the departmental network; ● *toll* – long distance communication; ● *international* – international connection
duration	<PFX_DURATION>	0-255	Set dialing duration timer, in seconds
exit			Exit from this configuration submenu to a higher level
getCID	<ON_OFF>	on/off	Enable/disable CallerID query when routing by prefix
history			View the history of entered commands
ivr	<IVR_INDEX>	0-255	Select an IVR script for a prefix with ivr type
mask edit			Switch to prefix mask editing mode
mask show			Show prefix masks
modifiers table called	<MODTBL_INDEX>	0-255 or none	Called number modification table applied when changing the dial plan
modifiers table calling	<MODTBL_INDEX>	0-255 or none	Calling number modification table applied when changing the dial plan
name	<s_name>	string no more than 31 characters (allowed to use letters, digits and '_')	Set name/designation for prefix
needCID	<ON_OFF>	on/off	Enable/disable mandatory request for CallerID information
new access category	<CAT_IDX>	0-127	Select a new access category for a prefix with 'change-numplan' type
new numplan	<PLAN_IDX>	0-15/0-255	Select a new numplan for a prefix with 'change-numplan' type
numplan	<PLAN_IDX>	0-15/0-255	Specify which dial plan the prefix belongs to
notdial ST	<USE_ST>	yes/no	Do not send/send end-of-set character (ST – in SS or sending complete in PRI)
operator	<OPERATOR>	or/and	Select the logical operator 'or / and'
pickup-group	<PICKUP_GROUP_INDEX>	0-254/any	Select a group for a prefix with 'pickup-group' type. Either a specific group is set, or the mode of selecting any group, which includes the subscriber's number
quit			End this CLI session
service	<PFX_USER_SERVICE>	cf-unconditional/ cf-busy/ cf-no-reply/ cf-out-of-order/ call-pickup/ conference/ clear-all/ intercom/ paging/ intervention	VAS service type: ● *cf-unconditional* – unconditional forwarding; ● *cf-busy* – call forwarding busy; ● *cf-no-reply* – call forwarding no reply; ● *cf-out-of-order* – call forwarding out of service; ● *call-pickup* – call pickup; ● conference – conference with sequential collection; ● *clear-all* – cancel all services; ● *intercom* – intercom; ● *paging* – paging;

			• *intervention* – intervention
session time	<PFX_SESSION_TIME>	5-64800 off — no limits	Set the time in seconds that limits the duration of a call that has passed through the prefix
session warning time	<PFX_SESSION_TIME_WARN>	1-300 off - no warn	An option that includes the issuance of a sound signal that warns of the end of a call for the specified seconds before the end of the call
show			Show prefix configuration
stimer	<PFX_LTIMER>	0-255	Set the time in seconds that the digital gateway will wait to continue dialing if the already dialed number matches any pattern in the dial plan, but there is a possibility of receiving more digits resulting in a match with another pattern. Default is 5 s
trunk	<TRUNK>	0-31	Set trunk group or direction number
type	<PFX_TYPE>	trunk/ trunk-direction/ change-numplan/ subscribers-pool/ user_service pickup-group/ ivr	Set prefix type: • *trunk* – access to the trunk group; • *trunk-direction* – access to the trunk direction; • change-numplan – dial plan change; • *subscribers-pool* – 'subscribers pool' prefix type; • *user_service* – VAS prefix; • *pickup-group* – pickup group; • *ivr* – IVR scenario selection

3.3.21.2 Prefix mask configuration mode

To enter this mode, in the prefix configuration mode run the **mask edit** command.

```
SMG-[CONFIG]-PREFIX[0]> mask edit
Entering Prefix-Mask mode.
SMG-[CONFIG]-PREFIX[0]-MASK>
```

Command	Parameter	Value	Action
?			Show list of available commands
add	<PREFIX_MASK> [PFX_MASK_TYPE]	prefix mask, 255 characters maximum, should be enclosed in parentheses '(' and ')' calling/called [called]	Add a new mask to the prefix. It is possible to set the mask type – for the caller (calling) or for the called, by default the mask type is always called
config			Retrun to the configuration menu
history			View the history of entered commands
exit			Exit from this configuration submenu to a higher level
modify duration	<PREFIX_MASK_INDEX> <DURATION>	0-1024 0-255	Set dialing duration timer: • *PREFIX_MASK_INDEX* – mask number; • *DURATION* – timer
modify Ltimer	<PREFIX_MASK_INDEX> <LONG_TIMER>	0-1024 0-255	Set a Long timer: • *PREFIX_MASK_INDEX* – mask number; • *LONG_TIMER* – timer
modify mask	<PREFIX_MASK_INDEX> <PREFIX_MASK>	0-1024 mask-prefix. 255 characters maximum, should be enclosed in parentheses '(' and ')'	Modify a mask: • *PREFIX_MASK_INDEX* – mask number; • *PREFIX_MASK* – mask
modify prefix	<PREFIX_MASK_INDEX> <PFX_INDEX>	0-1024 0-255	Move mask to another prefix: • *PREFIX_MASK_INDEX* – mask number to be transferred; • *PFX_INDEX* – prefix to which the mask is transferred
modify stimer	<PREFIX_MASK_INDEX> <SHORT_TIMER>	0-1024 [0-255]	Set a Short timer: • *PREFIX_MASK_INDEX* – mask number; • *DURATION* – timer

modify type	<PREFIX_MASK_INDEX>
	
	<PFX_MASK_TYPE>
		0-1024
		
		calling/called
			Set mask type – called or calling number analysis:
			• *PREFIX_MASK_INDEX* – mask number to be transferred;
			• *PFX_MASK_TYPE* – mask type:
			  • *calling* – calling number analysis;
			  • *called* – called number analysis

quit			End this CLI session
remove	<PREFIX_MASK_INDEX>	0-1024	Remove a mask
show			Show mask information

3.3.22 Pickup group configuration mode

To enter this mode, in the configuration mode run the **pickup-group <pickup-group_INDEX>** command, where **<pickup-group_INDEX>** is a pickup group number.

```
SMG-[CONFIG]> pickup-group 0
Entering pickup-group-mode.
SMG-[CONFIG]-PICKUP-GROUP[0]>
```

Command	Parameter	Value	Action
?			Show list of available commands
exit			Going from this configuration submenu to a higher level
history			View the history of entered commands
member add	<CALL_NUMBER>	symbols (no more than 30): *,#,D,0-9. Or 'none' for blank(delete) number	Add a member of the pickup group
member remove	<GROUP_MEMBER_INDEX>	[0-19]	Remove a member of a pickup group
member set number	<GROUP_MEMBER_INDEX>	[0-19]	Set pickup group member number
member set user-type	<GROUP_MEMBER_INDEX> <USER_TYPE>	[0-19] 0 - 'restricted', 1 - 'ordinary', 2 - 'privileged'	Set call group member type: 0 – restricted 1 – ordinary 2 – privileged
show			Show pickup group settings

3.3.23 PBX profile configuration mode

To enter this mode, in the configuration mode run the **pbx_profiles** command.

```
SMG-[CONFIG]> pbx_profiles
Entering PBX profiles mode.
SMG-[CONFIG]-PBX_PROFILES>
```

Command	Parameter	Value	Action
?			Show list of available commands
add pbx	<NAME> <PREFIX> <PFX>	string up to 63 characters long 1-15 0-255/none	Add PBX profile with name, prefix number and direct prefix
config			Return to the configuration mode
exit			Going from this configuration submenu to a higher level
flash mode	<PROFILE_INDEX> <FLASH>	0-31 none/ flash1/ flash2/ flash3	Signal transmission mode 'flash'
history			View the history of entered commands
modifiers table incoming called	<PROFILE_INDEX> <MODTBL_INDEX>	0-31 0-255/none	Set a modifier for the PBX profile based on the analysis of the called party number received from the incoming channel
modifiers table incoming calling	<PROFILE_INDEX> <MODTBL_INDEX>	0-31 0-255/none	Set a modifier for the PBX profile based on the analysis of the calling number received from the incoming channel
modify pbx connected number transit	<CONNNUM>	normal/block	Deny to transit a field 'Connected number'
modify pbx direct_pfx	<PROFILE_INDEX> <PFX>	0-31 0-255/none	Access to a prefix without analyzing the number of the calling or called subscriber. Designed to switch all calls from a SIP subscriber to a trunk group, regardless of the dialed number (without creating masks in prefixes)
modify pbx inband messages	<PROFILE_INDEX> <YES/no>	0-31	Issuing voice message phrases
modify pbx name	<IDX> <NAME>	0-31 string up to 63 characters long	Rename the specified profile
modify pbx prefix	<IDX> <PREFIX>	0-31 no more than 15 digits or none	Reassign the station prefix for the specified profile
modify pbx routing_profile	<IDX>	0-127	Select a scheduled routing profile
timeout busy-signal	<TIMER>	0-31	Timeout for issuing a 'busy' signal when using the 'call transfer' service
timeout cfnr	<TIMER>	0-31	Forward No Response (CFNR) timeout

timeout cfoos	<TIMER>	0-31	Forward Out of Service (CFOOS) timeout
timeout first-digit	<TIMER>	0-31	Timeout for dialing the first digit when using the 'call transfer' service
timeout next-digit	<TIMER>	0-31	Timeout for dialing the next digit when using the 'call transfer' service
quit			End this CLI session
remove pbx	<IDX>	0-31	Delete a PBX profile with specified number
show pbx			Show a list of PBX profiles

3.3.24 Q.931 timers configuration mode

To enter this mode, in the configuration mode run the **q931-timers** command.

```
SMG-[CONFIG]> q931-timers
Entering q931-timers mode.
SMG-[CONFIG]-[q931-T]>
```

Command	Parameter	Value	Action
?			Show list of available commands
config			Return to the configuration menu
exit			Exit from this configuration submenu to a higher level
quit			End this CLI session
set	t301 t302 t303 t304 t305 t306 t307 t308 t309 t310 t312 t313 t314 t316 t317 t320 t321 t322	30-360 10-25 4-10 20-30 30-40 30-40 180-240 4-10 6-90 10-20 6-12 4-10 4-10 120-240 120-240 30-60 30-60 4-10	Set t301 timer value Set t302 timer value Set t303 timer value Set t304 timer value Set t305 timer value Set t306 timer value Set t307 timer value Set t308 timer value Set t309 timer value Set t310 timer value Set t312timer value Set t313 timer value Set t314 timer value Set t316 timer value Set t317 timer value Set t320 timer value Set t321timer value Set t322 timer value
show			Show Q.931 timers configuration

3.3.25 RADIUS configuration mode

To enter this mode, in the configuration mode run the **radius** command.

```
SMG-[CONFIG]> radius
Entering RADIUS mode.
SMG-[CONFIG]-RADIUS>
```

Command	Parameter	Value	Action
?			Show list of available commands
acct ipaddr	<IP_ADDR> <SRV_IDX>	IP address in the AAA.BBB.CCC.DDD format 0-8	Set IP address of the Accounting server: • *IP_ADDR* – IP address; • *SRV_IDX* – server number
acct port	<PORT> <SRV_IDX>	0-65535 0-8	Set port of the accounting server: • *PORT* – port number; • *SRV_IDX* – server number.
acct secret	<SECRET> <SRV_IDX>	string max 31 characters 0-8	Set password for the accounting server: • *SECRET* – password; • *SRV_IDX* – server number
acct server_group	<SRV_GROUP_ID> <SRV_IDX>	0-3 0-7	Set a group for the accounting server: • *SRV_GROUP_ID* – group number; • *SRV_IDX* – server number
auth ipaddr	<IP_ADDR> <SRV_IDX>	IP address in the AAA.BBB.CCC.DDD format 0-8	Set IP address of the authorization server: • *IP_ADDR* – IP address; • *SRV_IDX* – server number
auth local	<AUTH_LOCAL>	no/yes	Allow local administrator access in case of RADIUS server failure
auth port	<PORT> <SRV_IDX>	0-65535 0-8	Set port of the authorization server: • *PORT* – port number; • *SRV_IDX* – server number
auth secret	<SECRET> <SRV_IDX>	string max 31 characters 0-8	Set a password for the authorization server: • *SECRET* – password; • *SRV_IDX* – server number
auth server_group	<SRV_GROUP_ID> <SRV_IDX>	0-3 0-7	Set a group for the authorization server: • *SRV_GROUP_ID* – group number; • *SRV_IDX* – server number
auth user	<AUTH_USER>	no/yes	User authorization web/telnet/ssh via RADIUS
config			Return to the configuration menu
deadtime	<DEADTIME>	5-60	Server idle time on failure – the time during which the server is considered inactive
exit			Exit from this configuration submenu to a higher level

history			View the history of entered commands
iface	<IFACE_NAME>	string max 255 characters	Set network interface for RADIUS
profile	<PROFILE_INDEX>	0-31	Go to configuring RADIUS profile settings
quit			End this CLI session
retries	<RETRIES>	2-5	Set the number of attempts to send a request
show config			Show configuration information for RADIUS servers
timeout	<TIMEOUT>	3-10	Set the time during which the server response is expected (x100ms)
voice-msg-table	<TABLE_INDEX>	0-31	Select a mapping table for RADIUS responses and voice messages

3.3.25.1 RADIUS profile parameters configuration mode

To enter this mode, in the RADIUS configuration mode run the **profile <PROFILE_INDEX>** command, where **<PROFILE_INDEX>** is the RADIUS profile mnumber.

```
SMG-[CONFIG]-RADIUS> profile 0
Entering RADIUS-Profile-mode.
SMG-[CONFIG]-RADIUS-PROFILE[0]>
```

Command	Parameter	Value	Action
?			Show list of available commands
acct answer	<ON/OFF>	off/on	Enable/disable acct messaging for call-orig=answer
acct CdPN	<CDPN_MODE>	CdPN-IN/CdPN-OUT	Set the called party number for Accounting-Request packets: • *CdPN-IN* – use the called number before modification (received in the 'SETUP/INVITE' packet); • *CdPN-OUT* – use the called number after modification
acct CgPN	<CGPN_MODE>	CgPN-IN/CgPN-OUT	Set calling number for Accounting-Request packets: • *CgPN-IN* – use the calling number before modification (received in the 'SETUP/INVITE' packet); • *CgPN-OUT* – use calling number after modification
acct duration count mode	<RADIUS_COUNT_MODE>	round-up/ round-down/ not-round	Time rounding options. Round up, round down, don't round (pass milliseconds)
acct originate	<ON/OFF>	off/on	Enable/disable acct messaging for call-orig= originate
acct restrict	<RESTRICT>	none/zone/ local/emergency/ restrict-all	Set a limit on outgoing communication when the server fails (no response from the server): • *none* – allow all calls; • *zone* – allow calls to emergency, to the local and zonal network; • *local* – allow calls to

			emergency and to the local network; • *emergency* – allow calls only to emergency; • *restrict* – deny all calls
acct start	<ON_OFF>	on/off	Enable/Disable 'acct. start' messaging
acct stop	<ON_OFF>	on/off	Enable/Disable 'acct. stop' messaging
acct update	<ON_OFF>	on/off	Enable/Disable 'acct. update' messaging
acct update_period	<PERIOD>	10sec/20sec/30sec/45sec/1min/2min/3min/5min/10min/15min/30min/1hour	Transmission period for 'acct. update' messaging
acct unsuccessfull	<ON_OFF>	on/off	Send / do not send information about unsuccessful calls to the RADIUS server
acct user-name answer	<USERNAME_MODE>	cgpn/ ip_or_stream/ trunk/cdpn/ initial_cgpn/ initial_cdpn	Set the User-Name attribute in the Accounting-Request packets for the answer side: • *cgpn* – as a value, use the phone number of the calling party; • *ip_or_stream* – as a value, use the name of the trunk on which the incoming connection is made; • *trunk* – as a value, use the name of the trunk on which the incoming connection is made; • *cdpn* – use the phone number of the called party; • *initial_cgpn* – use the unmodified calling party telephone number; • *initial_cdpn* – use unmodified called party telephone number
acct user-name originate	<USERNAME_MODE>	cgpn/ ip_or_stream/ trunk/cdpn/ initial_cgpn/ initial_cdpn	Set 'User-Name' attribute in Accounting-Request packets for originate side: • *cgpn* – as a value, use the phone number of the calling party; • *ip_or_stream* – as a value, use the IP address of the calling party or the number of the stream on which the incoming connection is made; • *trunk* – as a value, use the name of the trunk on which the incoming connection is made; • *cdpn* – use the phone number of the called party; • *initial_cgpn* – use the unmodified calling party telephone number; • *initial_cdpn* – use the

			unmodified called party telephone number
auth check on seize	<ON_OFF>	on/off	Send/do not send an authorization request on an incoming session
auth check on stop-dial	<ON_OFF>	on/off	Send/do not send an authorization request at the end of dialing
auth check on local-redir	<ON_OFF>	on/off	Send/do not send an authorization request with local forwarding
auth digestauth	<DIGESTAUTH>	rfc5090/ rfc5090-no-challenge/ draft-sterman	Select an authorization algorithm for subscribers with dynamic registration via a RADIUS server. With digest authentication, the password is transmitted as a hash code and cannot be intercepted when traffic is scanned
auth emergency-on-REJ	<PERMIT>	not-allow/allow	Allow/deny access to emergency when a connection is refused from the server
auth framedprotocol	<FRAMED_PROTOCOL>	none/PPP/ SLIP/ARAP/ Gandalf/Xylogics/ X75_Sync	Assign protocol when using packet access for RADIUS authentication requests: • *none* – packet access is not used
auth nas port type	<PORT_TYPE>	Async/ Sync/ ISDN_Sync/ ISDN_Async_v120/ ISDN_Async_v110/ Virtual/ PIAFS/ HDLC_Channel/ X25/ X75/ G3_Fax/ SDSL/ ADSL_CAP/ ADSL_DMT/ IDSL/ Ethernet/ xDSL/ Cable/ Wireless/ Wireless_IEEE_802.1	Assign the physical port type of the NAS (server where the user is authenticated), the default is Async
auth pass	<PASSWD>	Пароль не более 15 символов	Set the User-Password attribute values in the corresponding RADIUS-Authorization packet
auth restrict	<RESTRICT>	none/zone/ local/emergency/ restrict-all	Set a limit on outgoing communication when the server fails (does not receive a response from the server) • *none* – allow all calls; • *zone* – allow calls to emergency, to the local and zonal network; • *local* – allow calls to emergency and the local network; • *emergency* – allow calls only to emergency; • *restrict-all* – restrict all calls
auth service type	<SERVICE_TYPE>	none/ Login/	Set service type, default is not

		Framed/ Callback_Login/ Callback_Framed/ Outbound/ Administrative/ NAS_Promt/ Authenticate_Only/ Callback_NAS_Promp/ Call_Check/ Callback_Administrative	used (none)
auth session time	<SESSION_TIME_MODE>	ignore/ use_RFC_Session_timeout/ use_CISCO_h323_ credit_time	Set a maximum call duration limit based on the value of one of the attributes passed in the Access-Accept from the RADIUS server: • *ignore* – ignore the possibility of limiting the maximum call duration; • *use_rfc_session_timeout* – use the value of the Session-Timeout attribute as the value of the maximum call duration timer; • *use_cicso_h323_credit_time* – use the value of the Session-Timeout attribute or the Cisco VSA h323-credit-time attribute as the value for the maximum call duration timer
auth user-name answer	<USERNAME_MODE>	cgpn/ ip_or_stream/ trunk/cdpn/ initial_cgpn/ initial_cdpn	Set the value of the User-Name attribute in the Access –Request packets for the answer side: • *cgpn* – as a value, use the phone number of the calling party; • *ip_or_stream* – as a value, use the IP address of the calling party or the number of the stream on which the incoming connection is made; • *trunk* – use the name of the trunk on which the incoming connection is made; • *cdpn* – use the phone number of the called party; • *initial_cgpn* – use the unmodified telephone number of the calling party; • *initial_cdpn* – use unmodified called party telephone number
auth user-name originate	<USERNAME_MODE>	cgpn/ ip_or_stream/ trunk/cdpn/ initial_cgpn/ initial_cdpn	Set the value of the User-Name attribute in Access-Request packets for the originate side: • *cgpn* – as a value, use the phone number of the calling party; • *ip_or_stream* – as a value, use the IP address of the calling party or the number of the stream on which the

			incoming connection is made; ● *trunk* – use the name of the trunk on which the incoming connection is made; ● *cdpn* – use the phone number of the called party; ● *initial_cgpn* – use the unmodified calling party telephone number; ● *initial_cdpn* – use unmodified called party telephone number
auth userpasswd	<ON_OFF>	on/off	Use / do not use individual passwords for SIP subscribers during authorization
modifiers table auth mode	MODTABLE_MODE	default/restricted	Number authorization mode in RADIUS. ● *restricted* – only numbers that fall into the mask of the modifier table are authorized
modifiers table acct mode	MODTABLE_MODE	default/restricted	Number accounting mode in RADIUS. ● *restricted* – accounting only for numbers included in the mask of the modifier table
modifiers table incoming called	<MODTBL_INDEX>	0-255/none	Set the Called Party Number (CdPN) modifier for the incoming connection, as applied to the Called-Station-Id, xpgk-dst-number-in fields in the RADIUS-Authorization and RADIUS-Accounting messages
modifiers table incoming calling	<MODTBL_INDEX>	0-255/none	Set the Calling Party Number (CgPN) modifier for the incoming connection, as applied to the Calling-Station-Id, xpgk-src-number-in fields in the RADIUS-Authorization and RADIUS-Accounting messages
modifiers table incoming redirecting	<MODBL_INDEX>	0-255/none	Set the redirect subscriber number (RedirPN) modifier in the h323-redirect-number field in the RADIUS-Authorization and RADIUS-Accounting messages
modifiers table outgoing called	<MODTBL_INDEX>	0-255/none	Set the Called Party Number (CdPN) modifier for the outgoing connection, as applied to the xpgk-src-number-out field in the RADIUS-Authorization and RADIUS-Accounting messages;
modifiers table outgoing calling	<MODTBL_INDEX>	0-255/none	Set the Calling Party Number (CgPN) modifier for the outgping connection, as applied to the xpgk-dst-number-out field in the RADIUS-Authorization and RADIUS-Accounting messages
config			Return to the configuration menu
exit			Exit from this configuration submenu to a higher level
history			View the history of entered

			commands
quit			End this CLI session
reset voice-msg-table			Do not use RADIUS response-to-voice mapping
server_group	<SRV_GROUP>	0-3	Group number of RADIUS servers to be used by the profile
set vmt-reply-attribute		h323-return-code/Reply-Message	Selection of the attribute by which the RADIUS-reject message will be parsed
set voice-msg-table	<TABLE_IDX>	[0-31]	Selecting a Mapping Table for RADIUS Responses and Voice Messages
show			Show RADIUS profile configuration
use acct	<ON_OFF>	on/off	Allow/deny sending Accounting requests to the RADIUS server
use auth	<ON_OFF>	on/off	Allow/deny sending Authorization requests to the RADIUS server
use class as ss7cat	<ON_OFF>	on/off	Use AV-pair Class to transfer the subscriber's SS7 category
use eltex-vsa	<ON_OFF>	on/off	Activating the RCM service
use full cisco-vsa	<ON_OFF>	on/off	Use full Cisco-VSA value for RCM service
use porta billing	<ON_OFF>	on/off	Enable/disable the use of PortaBilling
use porta routing	<ON_OFF>	on/off	Enable/disable the use of PortaRouting
use incoming called		original/processed	Selection of the CdPN number sent in the xpgk-dst-number-in field in the RADIUS-Authorization and RADIUS-Accounting messages
use incoming calling		original/processed	Selection of the CgPN number sent in the xpgk-dst-number-in field in the RADIUS-Authorization and RADIUS-Accounting messages
use snmp	<ON_OFF>	on/off	Send SNMP trap on every RADIUS hit
use utc time	<ON_OFF>	on/off	Use time in UTC

3.3.26 Call recording settings configuration mode

To enter this mode, in the configuration mode run the ***record*** command.

```
SMG-[CONFIG]> record
Entering Record-setup mode.
SMG-[CONFIG]-[RECORD]>
```

Command	Parameter	Value	Action
?			Show list of available commands
exit			Exit from this configuration submenu to a higher level
ftp enabled	REC_FTP	no/yes	Save conversations recording to FTP server
ftp login	REC_FTPLOGIN	string up to 63 characters	FTP access login
ftp mode recording	REC_MODE	once-a-day/ once-an-hour/ once-an-minute	FTP upload mode - once a day, once an hour, once a minute
ftp passwd	REC_PASSWD	string up to 63 characters	FTP access password
ftp path	REC_FTPPATH	string up to 63 characters	FTP file path
ftp period day	REC_HOUR REC_MINUTE	0-23 0-59	Set upload hours and minutes for once-a-day mode
ftp period hour	REC_MINUTE	0-59	Set upload minutes for once-an-hour mode
ftp port	REC_FTPPORT	1-65535	FTP server port
ftp remove-after-upload	REC_FTP_REMOVE	no/yes	Delete entries from local storage after uploading to FTP
ftp server	REC_FTPSERVER	string up to 63 characters	FTP server address or domain name
set action on full disk		stop-recording/remove-old-files	Choice of action when the disk is full: stop recording/delete old
set dirname		none or text string, maximum 63 characters	Set the name of the directory for recording conversation files
set dirname_IVR		none or text string, maximum 63 characters	Set the name of the directory for recording IVR conversations
set files count per dir	FILECOUNT	100-65535 or unlimited	Number of record files in one directory
set files keep period day	KEEP_DAY	0-90	Number of days during which records are stored on local storage
set files keep period hour	KEEP_HOUR	0-23	Number of hours during which records are stored on local storage
set notification	< NOTIFY_TYPE >	None voice_message	Notification about the start of recording conversations
set path		off/mnt/sd[abc][1-7]*	Set the path for storing conversation recording files

3.3.27 Call record masks configuration mode

To enter this mode, in the call recording configuration mode run the ***mask*** command.

```
SMG-[CONFIG]-[RECORD]> mask
Entering Record-Mask mode.
SMG-[CONFIG]-[RECORD]-MASK>
```

Command	Parameter	Value	Action
?			Show list of available commands
exit			Exit from this configuration submenu to a higher level

add	REC_MASK_NUMPLAN
	
	RECORD_MASK
	
	REC_MASK_TYPE
		0-255 or all
		
		string max 255 characters
		
		all/
		calling/
		called
			Add a new record mask.
			Parameters:
			• dial plan (all – any dial plan);
			• record mask, which should be enclosed in parentheses '(' and ')';
			• number type:
			  • any;
			  • calling;
			  • called

modify category	RECORD_MASK_INDEX CAT_IDX	0-4095 0-31	Change the category of the call recording for the mask
modify direction	RECORD_MASK_INDEX REC_MASK_TYPE	0-4095 all/ calling/ called	Change mask number type to specified
modify mask	RECORD_MASK_INDEX PREFIX_MASK	0-4095 string max 255 characters	Change the mask value. The mask should be enclosed in parentheses '(' and ')'
modify notification	RECORD_MASK_INDEX NOTIFY_TYPE	0-4095 none/voice_message	Notification about the start of recording: • *none* – do not notify; • *voice_message* – notify by a voice message
modify numplan	RECORD_MASK_INDEX REC_MASK_NUMPLAN	0-4095 0-255 or all	Change a dial plan
remove	RECORD_MASK_INDEX	0-4095	Remove a mask
show			Show all masks

3.3.28 Static routes configuration mode

To enter this mode, in the configuration mode run the ***route*** command.

```
SMG-[CONFIG]> route
Entering route mode.
SMG-[CONFIG]-ROUTE>
```

Command	Parameter	Value	Action
?			Show list of available commands
config			Return to the configuration mode
exit			Exit from this configuration submenu to a higher level
history			View the history of entered commands
quit			End this CLI session
route add	<DESTINATION> <MASK> <GATEWAY> <METRIC> <IFACE_NAME> <ENABLE>	IP address in the AAA.BBB.CCC.DDD format mask in the AAA.BBB.CCC.DDD format gateway in the AAA.BBB.CCC.DDD format unsigned integer string max 255 characters disable/enable	Add a route: ● *DESTINATION* – destination IP address; ● *MASK* – network mask for the specified IP address; ● *GATEWAY* – gateway IP address; ● *METRIC* – metrics; ● *IFACE_NAME* – network interface; ● *ENABLE* – enable/disable network interface
route del	<IDX>	0-4095	Delete a route: ● *IDX* – network route index
show			Show route configuration information

3.3.29 Q.850 release cause list configuration

To enter this mode, in the configuration mode run the ***release cause list <LIST_INDEX>*** command, where ***<LIST_INDEX>*** is a number of Q.850 release cause list.

```
SMG-[CONFIG]> release cause list 0
Entering RelCauseList-mode.
SMG-[CONFIG]-REL-CAUSE-LIST[0]>
```

Command	Parameter	Value	Action
?			Show list of available commands
add cause	<CAUSE>	1-127	Add q.850 cause into the table
config			Return to the configuration mode
exit			Exit from this configuration submenu to a higher level
history			View the history of entered commands
quit			End this CLI session
remove cause	<CAUSE>	1-127	Delete q.850 cause from the table
set name	<LIST_NAME>	letter or digit or '_', '.', '-'. Max 63 symbols	Set table name
show			Show the table configuration

3.3.30 SIP/SIP-T common settings configuration mode

To enter this mode, in the configuration mode run the **sip configuration** command.

```
SMG-[CONFIG]> sip configuration
Entering SIP/SIP-T/SIP-I/SIP-profile config mode.
SMG-[CONFIG]-SIP(general)>
```

Command	Parameter	Value	Action
?			Show list of available commands
cause codes KZ	<ON_OFF>	on/off	Set/cancel the specification in accordance with the requirements of Kazakhstan
config			Return to the configuration mode
exit			Exit from this configuration submenu to a higher level
history			View the history of entered commands
ignore_RURI		no/yes	Ignore/do not ignore address in R-URI. The address information after the '@' separator in the Request-URI is ignored, otherwise the address information is checked for a match with the IP address and host name of the device, and if it does not match, the call is rejected
quit			End this CLI session
ringing timeout	<RING_TIMER>	10-255	Call answer timeout
save_database	on/off		Save/do not save information about registered subscribers to the non-volatile memory of the gateway. It is necessary to save the database of registered subscribers in case the device is rebooted by power or due to a failure. In case of reboot from Web or CLI, regardless of this setting, the gateway will save the current database to non-volatile memory
show			Show general SIP-T configuration
T1	<T1_TIMER>	0-255	Set SIP timer T1
T2	<T2_TIMER>	0-255	Set SIP timer T2
T4	<T4_TIMER>	0-255	Set SIP timer T4
write_timeout	<TIMEOUT>	1hour/ 2hours/ 4hours/ 6hours/ 8hours/ 12hours/ 16hours	Set the period for updating data in the archive database (from one to sixteen hours)

3.3.31 *SIP/SIP-T interface parameters configuration mode*

To enter this mode, in the configuration mode run the **sip interface <SIPT_INDEX>** command, where **<SIPT_INDEX>** is the SIP/SIP–T interface number.

```
SMG-[CONFIG]> sip interface 0
Entering SIPT-mode.
SMG-[CONFIG]-SIP/SIPT/SIPI-INTERFACE[0]>
```

Command	Parameter	Value	Action
?			Show list of available commands
access category	<CAT_IDX>	0-31	Assign an access category for a linkset
alarm indication	<on/off>		Enable alarm indication about the interface unavailability
category mode	<MODE>	none category cpc cpc-rus	Do not send AON category to SIP. Send AON category in the specified field, *none* – do not send AON category in SIP
CCI	<on/off>	on/off	Enable link integrity check support
cdpn default	<CDPN>	up to 30 digits or 'none'	CDPN by default when calling through an interface with trunk registration
cdpn plus sign	<YES/NO>	no/yes	Passing the '+' sign in international type numbers. Enabled by default
cgpn replace	<YES_NO>	no/yes	Take CgPN from the 'Username/Number' parameter, when the function is disabled - the CgPN number received in the incoming call is used
codec disable	<CODEC_IDX>	0-5	Disable the selected codec. Codecs are numbered by priority – from 0 (highest) to 5 (lowest)
codec pte	<CODEC_IDX> <PTE>	0-5 10/20/30/40/50/ 60/70/80/90	Set payload time
codec ptype	<CODEC_IDX> <PTYPE>	0-5 0-127 or static	Set payload type. 'Static' value sets the default value depending on the selected codec
codec set	<CODEC_IDX> <CODEC>	0-5 G.711-U/ G.711-A/ G.729/ G.726	Set codec to use
command line	<command>	allowed symbols: [0-9a-zA-Z-_.!~*'();:=+$,%#] always inside []. For clearing use 'none'	Advanced SIP protocol settings
config			Return to the configuration menu
diversion use sip-uri	<YES_NO>	no/yes	When enabled, the number in the Diversion header will always be passed as a SIP-URI
DSCP SIG	<DSCP_SIG>	0-63	Set DSCP identifier for SIG traffic

DSCP RTP	<DSCP_RTP>	0-63	Set DSCP identifier for RTP traffic
DTMF allow inband DTMF	<DTMF ALLOW INBAND>	no/yes	Allow inband DTMF
DTMF mime type	< MIME_TYPE>	application/dtmf or application/ dtmf-relay	Set the payload type used for DTMF transmission in SIP INFO packets application/dtmf-relay – in the INFO application/dtmf-relay packets of the SIP protocol (* and # transmitted as symbols * and #); application/dtmf – in the INFO application/dtmf packets of the SIP protocol (* and # transmitted as numbers 10 and 11)
DTMF mode	<DTMF_m>	inband/ RFC2833/ SIP-INFO/ SIP-NOTIFY	DTMF mode for this interface
DTMF payload	<DTMF_p>	96-127	Set a payload type for RFC2833
DTMF payload-equal	<DTMF_PT_EQ>	(off/on)	Enable/disable the option 'Same RFC2833 PT'
early media header	<early media header>	(off/on)	Enable the support for P-Early-Media (RFC5009)
echo-cancellation direction	<ECAN_DIR>	outgoing/incoming	Set echo-cancellation (incoming/outgoing)
echo-cancellation mode	<ECAN_MODE>	voice/ nlp-off-voice/ speex-algorithm/ off	Set echo cancellation mode: • *Voice* – echo cancellers are enabled (this mode is set by default); • *Nlp-off-voice* – echo cancellers are enabled in voice mode, non-linear NLP processor is disabled. In the case when the levels of the signals at transmission and reception are very different, a weak signal can be suppressed by the non-linear NLP processor. To prevent this from happening, use this mode of operation of echo cancellers; • *speex-algorithm;* • *Off* – do not use echo cancellation.
egress lines	<COUNT>	0-65535	Set the number of outgoing lines on the SIP interface 0 – no restrictions
exit			Exit from this configuration submenu to a higher level
history			View the history of entered commands
fill empty display-name	FILL_DNAME	on/off	Fill display-name when receiving a call without display-name
gain digital rx	<GAIN>	-140 – 60	Set the volume for voice reception, amplify/attenuate the level of the signal received from the interacting gateway and output to the speaker of

			the telephone set connected to the SMG gateway
gain digital tx	<GAIN>	-140 – 60	Volume for voice transmission, amplification/attenuation of the signal level received from the microphone of the telephone set connected to the SMG gateway and transmitted to the interacting gateway
history			View the history of entered commands
hold mode		flash/ flash/star flash/hash flash/star/hash	Call Hold on Press: • flash; • flash or 'stars'; • flash or 'hash'; • flash, 'stars' or 'hash'
hostname clear			Delete the hostname of the communicating gateway
hostname set	<HOSTNAME>	string up to 63 characters	Set the hostname of the interworking gateway
ignore RURI/To diff	<IGNORE_RURI_TO_DIFF>	off/on	When this option is enabled, Redirecting and Original Called numbers will not be transmitted to SS7 if there are differences in the SIP RURI and To fields
inband_signal_with_183_and_sdp	on/off		Issue 183/SDP in SIP response to open the voice path when receiving CALL PROCEEDING or PROGRESS messages containing progress indicator=8 (In-band signal) from PRI
ingress lines	<COUNT>	0-65535	Set the number of outgoing lines on the SIP interface 0 – no restrictions
keep-alive enable			Enable direction availability control (NAT keep-alive) (SIP profile only)
keep-alive disable			Disable NAT keep-alive direction availability control (SIP profile only)
keep-alive mode	<KEEP_ALIVE_MODE>	SIP-OPTIONS/ SIP-NOTIFY/UDP-CRLF	Opposite side availability control mode. • *SIP-OPTIONS* – direction availability control via OPTION requests; • *SIP-NOTIFY* – direction availability control via NOTIFY requests; • *UDP-CRLF* – direction availability control by sending empty UDP
keep-alive period	<KEEP_ALIVE_PERIOD>	30-3600	Period for sending requests
lines mode	<LINES MODE>	common/separate	Line operation mode: combined/separate
local ringback	<on/off>	on/off	Enabling the option of local RBT instead of early media
login	<LOGIN>	string up to 15 characters	Set name used for authentication
max_active	<MAX_ACTIVE>	0-65535	Set the maximum number of active connections for an interface
mode	<mode>	profile/ SIP/ SIP-T/	Set interface operation mode (SIP profile is assigned to SIP subscribers)

		SIP-I/ SIP-Q	
name	<s_name>	allowed to use letters, digits, symbol '_'. maximum 31 characters	Set a name for the interface
nat	<NAT>	enable/disable	Enable/Disable NAT
net-interface rtp	<IFACE_NAME>	string up to 255 characters	Set network interface for RTP
net-interface sig	<IFACE_NAME>	string up to 255 characters	Set network interface for SIP
numbering plan	<NUMPLAN>	0-15/0-255	Set a dial plan
password	<PASSWD>	string up to 15 characters	Set password used for authentication
port	<PORT>	1-65535	Set the UDP port of the interworking gateway on which it receives SIP signaling
quit			End this CLI session
radius profile	<RADIUS_PROFILE>	number [0-31] or 'no'	Assign a RADIUS profile to the SIP profile interface. *no* – do not use the profile for interface
Re-INVITE a=sendonly		on/off	Allow processing Re-INVITE with a=sendonly
redirection 302	<REDIRECTION>	on/off	Set/cancel the use of forwarding (302)
redirection server	<REDIRECT_SERV>	on/off	Redirect/do not redirect a call sent to a public address to a subscriber's private address without using dial plan routing. Routing is done directly to the address in the contact header of the 302 response received from the redirect server. At first, set up a redirection 302 (redirection 302 command)
refer	<REFER>	enable/disable	Set/cancel call transfer capability using REFER
register delay	<REGEXP>	500-5000	The minimum interval between sending Register messages, necessary to protect against heavy traffic caused by the simultaneous registration of a large number of subscribers
register expires	<REGEXP>	90-64800	Set a time period for re-registration
regmode	<REGMODE>	none/ trunk-mode/ upper-mode	Set registration type on upstream server
reliable_1xx_ response	<ON_OFF>	off/ support/ support-plus/ require/ require-plus	When the *support* option is enabled, INVITE request and class 1xx provisional responses will contain support: 100rel tag, requiring assured confirmation of provisional responses. When the *require* option is enabled, the INVITE request and class 1xx provisional responses will contain require: 100rel tag, requiring assured confirmation of provisional responses. Off – 100rel tag transmission is disabled

routing_profile	<prof>	0-127	Selection of scheduled routing profile
sdp_in_18x	<ON_OFF>	on/off	Always send SDP in provisional responses
sipdomain	<SIPDOMAIN>	IP address in the AAA.BBB.CCC.DDD format	Set registration domain address
show config			Show interface information
sipcause profile	<SIPCAUSE>	[0-63]/ none	Profile selection for mapping Q.850 cause values with sip-reply
sms port	<PORT>	0-65535	Port for receiving SMS via SMPP protocol for forwarding to the duplication server
STUN ip	<IPADDR>	IP address in the AAA.BBB.CCC.DDD format	Set STUN server IP address
STUN period	<PERIOD>	10-1800/0	Set interval between requests
STUN port	<PORT>	1-65535	Assign the STUN server port for sending requests (default is 3478)
STUN use	<YES_NO>	yes/no	Use / do not use STUN
subnet mask clear			Remove subnet mask for incoming calls
subnet mask set	<SUBNET>	string of up to 63 characters as a subnet mask: AAA.BBB.CCC.DDD	Set subnet mask for incoming calls
subscribers max forwarding	<MAX FORWARDINGS>	5/10	Maximum number of redirects between subscribers
timer enable	<YES_NO>	no/yes	Use/do not use RFC4028 SIP session timers
timer refresher	<REFRESHER>	uac/uas	Determine the party performing the session update
timer session Min-SE	<MIN_SE>	90-32000	Set the minimum session state control interval, in seconds. This interval should not exceed *timer session expires*
timer session expires	<EXPIRES>	90-64800	Set a timeout in seconds, after which the session will be forced to end if the session is not updated in time
transit sip header	YES_NO	no/yes	Allow transit of SIP header from this leg to another
trunk	<TRUNK>	0-31	Set trunk group number for interface
trusted network	<YES_NO>	yes/no	Selecting the 'trusted network' option
username	<USERNAME>	string up to 15 characters	Set User ID
VAD_CNG	< ON_OFF >	on/off	Enable/disable speech activity detector/comfort noise generator for interface
flash processing		on/off	Process flash signal

3.3.32 SIP subscriber parameters configuration mode

To enter this mode, in the configuration mode run the **sip users** command.

```
SMG-[CONFIG]> sip users
Entering SIP-Users mode.
SMG-[CONFIG]-SIP-USERS>
```

Command	Parameter	Value	Action
?			Show list of available commands
add		group/user	Add a new user/group of dynamic subscribers
config			Return to the configuration mode
exit			Exit from this configuration submenu to a higher level
history			View the history of entered commands
quit			End this CLI session
remove	<INDEX>	0-1999/0-2999	Remove this user
savedb			Save information about registered subscribers to the non-volatile memory of the gateway. Necessary to save the database of registered subscribers in case the device is rebooted by power or due to a failure. In case of reboot from Web or CLI, regardless of this setting, the gateway will save the current database to non-volatile memory
service user	<INDEX>	0-1999/0-2999	Switch to VAS configuration mode for a given subscriber
service group	<INDEX>	0-63	Switch to VAS configuration mode for a given group
set authorization	<INDEX> <AUTHMODE>	0-1999/0-2999 none/register/register_and_invite	Set user authorization mode: ● *INDEX* – SIP subscriber index; ● *AUTHMODE* – authorization mode: ● *none* – do not ask for authorization; ● *register* – ask at registration; ● *register_and_invite* – ask for registration and outgoing calls
set user allow unregistered	<INDEX> <ON_OFF>	0-1999/0-2999 off/on	Allow calls without registration
set user access category	<INDEX> <CAT_IDX>	0-1999/0-2999 0-31	Assign an access category for a given subscriber
set user access mode	<INDEX> <ACCESS>	0-1999/0-2999 Off/On/Off_1/Off_2/Denied_1/Denied_2/Denied_3/Denied_4/Denied_5/Denied_6/Denied_7	Assign a service mode to a given subscriber

		/ Denied_8/Exclude	
set user blf groupID	<INDEX> <GROUP_ID>	0-1999/0-2999 0-15	Set monitoring group (BLF subscription group)
set user blf subscribers	<INDEX> <BLF_SUBS>	0-1999/0-2999 0-200	Set the maximum number of subscribers per user
set user blf usage	<INDEX> <ON_OFF>	0-1999/0-2999 off/on	Enable blf service (line busy indication)
set user category	<INDEX> <CATEGORY>	0-1999/0-2999 0-9	Set the AON category for the specified subscriber: ● *INDEX* – SIP subscriber index; ● *CATEGORY* – subscriber AON category
set user cliro	<INDEX> <ON_OFF>	0-1999/0-2999 off/on	Enable the CLIRO service (hidden number detection)
set user display name rule	<INDEX> <USE_DISPLAY_NAME>	0-1999/0-2999 received_only/ received_prefer/ configured_only	Display name usage mode: ● *received_only* – always use accepted name only; ● *received_prefer* – if the name is not accepted, then use the configured display name; ● *configured_only* – always use the configured display name
set user display name value	<INDEX> <DISPLAY_NAME>	0-1999/0-2999 string up to 40 characters or none	Subscriber Display Name: ● *none* – clears the display name
set user domain	<INDEX> <DOMAIN>	0-1999/0-2999 string up to 15 characters	Set a SIP domain for a subscriber: ● *INDEX* – SIP subscriber index; ● *DOMAIN* – domain name
set user egress lines	<INDEX> <COUNT>	0-1999/0-2999 1-255 or 0	Set the number of simultaneous outgoing calls involving the subscriber for the separate line operation mode. Range of allowable values [1;255] or 0 – unlimited
set user ingress lines	<INDEX> <COUNT>	0-1999/0-2999 1-255 or 0	Set the number of simultaneous incoming calls involving the subscriber for the separate line operation mode. Range of allowable values [1;255] or 0 – unlimited
set user intercom header	<HEADER> <INDEX>	AIAA/AII/AIIAA/ AIII/AIIRA/AIRA/ AMO/CIAA/CIESAA/ CISSAA 0-1999/0-2999	Set SIP header for intercom: AIAA – Alert-Info: Auto Answer AII – Alert-Info: Intercom' for user AIIAA – Alert-Info: info=alert-autoanswer AIII – Alert-Info: info=intercom AIIRA – Alert-Info: info=RingAnswer AIRA – Alert-Info: Ring Answer AMO – Answer-Mode: Auto CIAA – Call-Info: ;answer-after=0 CIESAA – Call-Info: =\;answer-after=0 CISSAA – Call-Info: \\;answer-after=0

set user intercom mode	<INDEX> <MODE>	0-1999/0-2999 sendonly/ sendrecv/ ordinary/ reject	Intercom operation mode: • *sendonly* – one-way; • *sendrecv* – two-way; • *ordinary* – normal call (without sending headers from intercom header); • *reject* – do not use intercom
set user intercom priority	<INDEX> <PRIORITY>	0-1999/0-2999 1-5	Set intercom priority
set user intercom timer	<INDEX> <TIMER>	0-1999/0-2999 0-255	Pause before answering. Used when sending SIP headers with the answer-auto parameter
set user ipaddr	<INDEX> <IPADDR>	0-1999/0-2999 IP ddress in the AAA.BBB.CCC.DDD format	Set IP address for specified subscriber
set user lines	<INDEX> <COUNT>	0-1999/0-2999 1-255 or 0	Set the number of simultaneous calls involving the subscriber for the common line operation mode. Range of allowable values [1;255] or 0 – unlimited
set user lines-mode	<INDEX> <LINES_MODE>	0-1999/0-2999 common/separate	Simultaneous call limit operation mode: • *common* – common restriction of incoming and outgoing calls; • *separate* – separate restrictions for incoming and outgoing calls
set login	<INDEX> <LOGIN> <PASSWORD>	0-1999/0-2999 string up to 63 characters string up to 63 characters	Set a username and password for this subscriber for authentication
set user name	<INDEX> <NAME>	0-1999/0-2999 string, max 31 characters	Set SIP subscriber name
set user no-source-port-control	<INDEX> <ON_OFF>	0-1999/0-2999 off/on	Ignore source port after registration
set user notify intervention	<INDEX> <ON_OFF>	0-1999/0-2999 off/on	Notify about the start of intervention
set user number	<INDEX> <NUMBER>	0-1999/0-2999 subscriber number	Set number for SIP subscriber
set user numberAON	<INDEX> <NUMBER>	0-1999/0-2999 subscriber number	Set AON number for this subscriber
set user numberAON-for-redirection	<INDEX> <NUMBER>	0-1999/0-2999 subscriber number	Use AON number when forwarding
set user numberList	<INDEX> <NUM_IDX> <NUMBER>	0-1999/0-2999 0-15/0-255 [number]/none	Set an additional subscriber number in a specific dial plan: • *none* – remove a number
set user numplan	<INDEX> <PLAN_IDX>	0-1999/0-2999 0-15/0-255	Set a dial plan for subscriber

set user pbx_profile	<INDEX> <PROFILE>	0-1999/0-2999 0-31	Set PBX profile for SIP subscriber
set user Re-INVITE a=sendonly	<INDEX> <HOLD>	0-63 off/on	Enabling the hold service upon receiving a re-invite with the a=sendonly flag
set user redirection	<INDEX> <REDIRECTION>	0-63 off/on	Allow/Deny redirect processing (message 302) from the subscriber
set group access category	<INDEX> <CAT_IDX>	0-63 0-31	Assign an access category for a group of subscribers
set group blf groupID	<INDEX> <GROUP_ID>	0-63 0-15	Set monitoring group (BLF subscription group)
set group blf subscribers	<INDEX> <BLF_SUBS>	0-63 0-200	Set the maximum number of subscribers per group
set group blf usage	<INDEX> <ON_OFF>	0-63 off/on	Allow subscription to events
set group category	<INDEX> <CATEGORY>	0-63 0-9	Set AON category for the specified group: ● *INDEX* – SIP subscriber index; ● *CATEGORY* – subscriber's AON category
set group cliro	<INDEX> <ON_OFF>	0-63 off/on	Enable CLIRO service (hidden number detection)
set group domain	<INDEX> <DOMAIN>	0-63 String up to 15 characters	Set SIP domain for a group: ● *INDEX* – SIP subscriber index; ● *DOMAIN* – domain name
set group egress lines	<INDEX> <COUNT>	0-63 1-255 or 0	Set the number of simultaneous outgoing calls involving a group subscriber for the *separate* line operation mode. Range of allowable values [1;255] or 0 – unlimited
set group ingress lines	<INDEX> <COUNT>	0-63 1-255 or 0	Set the number of simultaneous incoming calls involving a group subscriber for the *separate* line operation mode. Range of allowable values [1;255] or 0 – unlimited
set group intercom header	<HEADER> <INDEX>	AIAA/AII/AIIAA/ AIII/AIIRA/AIRA/ AMO/CIAA/CIESAA/ CISSAA 0-63	Set SIP header for intercom: AIAA - Alert-Info: Auto Answer AII - Alert-Info: Intercom' for user AIIAA - Alert-Info: info=alert-autoanswer AIII - Alert-Info: info=intercom AIIRA - Alert-Info: info=RingAnswer AIRA - Alert-Info: Ring Answer AMO - Answer-Mode: Auto CIAA - Call-Info: ;answer-after=0 CIESAA - Call-Info: =\;answer-after=0 CISSAA - Call-Info: \\;answer-after=0
set group intercom mode	<INDEX> <MODE>	0-63 sendonly/ sendrecv/	Intercom mode: ● *sendonly* – one-way; ● *sendrecv* – two-way;

		ordinary/ reject	• *ordinary* – normal call (without sending headers from intercom header); • *reject* – do not use intercom
set group intercom priority	<INDEX> <PRIORITY>	0-63 1-5	Set intercom priority
set group intercom timer	<INDEX> <TIMER>	0-63 0-255	Pause before answering. Used when sending SIP headers with the 'answer-auto' parameter
set group lines	<INDEX> <COUNT>	0-63 1-255 or 0	Set the number of simultaneous calls involving a group subscriber for the common line mode. Range of allowable values [1;255] or 0 – unlimited
set group lines-mode	<INDEX> <LINES_MODE>	0-63 common/separate	Operation mode of simultaneous calls limits: • *common* – common restriction of incoming and outgoing calls; • *separate* – separate restrictions for incoming and outgoing calls
set group max	<INDEX> <MAX_REG>	0-63 0-1999/0-2999	Set the number of group subscribers
set group name	<INDEX> <NAME>	0-63 string, max 31 characters	Set group name
set group numplan	<INDEX> <PLAN_IDX>	0-63 0-15/0-255	Set group dial plan
set group no-source-port-control	<INDEX> <ON_OFF>	0-63 off/on	Ignore source port after registration
set group pbx_profile	<INDEX> <PROFILE>	0-63 0-31	Set a PBX profile for a group
set group profile	<INDEX> <PROFILE>	0-63 0-31	Set a SIP profile for a group
set group Re-INVITE a=sendonly	<INDEX> <HOLD>	0-63 off/on	Enabling the hold service upon receiving a re-invite with the a=sendonly flag
set group redirection	<INDEX> <REDIRECTION>	0-63 off/on	Allow/Deny redirect processing (message 302) from the subscriber
set group refer	<INDEX> <REFER>	0-63 off/on	Enabling call transfer with a REFER message
show list			Show list of SIP subscribers
show user	<INDEX>	0-1999/0-2999	Display information about a SIP subscriber
show group	<INDEX>	0-63	Display information about the group

3.3.32.1 Subscriber VAS configuration mode

To enter this mode, in the configuration mode run the **service <USER_INDEX>** command, where **<USER_INDEX>** is a SIP-suscriber index.

```
SMG-[CONFIG]-SIP-USERS> service user 0
Entering User-Service mode for user 0
SMG-[CONFIG]-[SIP-USERS][0]-SERVICE>
```

Command	Parameter	Value	Action
?			Show list of available commands
attach service block			Attach VAS for a subscriber
detach service block			Detach VAS for a subscriber
exit			Exit from this configuration submenu to a higher level
quit			End this CLI session
set call-pickup enable	<ON_OFF>	off/on	Enable the 'call pickup' service
set cfb enable	<ON_OFF>	off/on	Activate the 'forwarding for busy' service
set cfb number	<ON_OFF>	number up to 30 characters or none	Set the number for 'forwarding for busy' service: ● *none* – disable call forwarding
set sfnr enable	<ON_OFF>	off/on	Activate the 'forwarding for no response' service
set sfnr number	<ON_OFF>	number up to 30 characters or none	Set the number for 'forwarding for no response' service: ● *none* – disable call forwarding
set cfos enable	<ON_OFF>	off/on	Activate the 'forwarding for out of service'
set cfos number	<ON_OFF>	number up to 30 characters or none	Set the number for the 'forwarding for out of service': ● *none* – disable call forwarding
set cfu enable	<ON_OFF>	off/on	Activate the 'unconditional forwarding' service
set cfu number	<ON_OFF>	number up to 30 characters or none	Set the number for the 'unconditional forwarding': ● *none* – disable call forwarding
set clear-all enable	<ON_OFF>	off/on	Enable the 'clear all services'
set conf-3way enable	<ON_OFF>	off/on	Enable the '3way conference' service. At first, activate the 'call hold' service
set conference enable	<ON_OFF>	off/on	Enable the 'conference with sequential collection' service
set ct enable	<ON_OFF>	off/on	Enable the 'call transfer' service. At first, activate the 'call hold' service
set hold enable	<ON_OFF>	off/on	Enable the 'call hold' service
set intercom enable	<ON_OFF>	off/on	Enable the 'intercom' service
set one touch record enable	<ON_OFF>	off/on	Enable the 'one touch record' service
set password change enable	<ON_OFF>	off/on	Enable the 'password change' service
set password restrict out access active	<ON_OFF>	off/on	Password activation for the 'password activation' service. The *on* value makes the password active and the communication restriction is removed
set password restrict out access enable	<ON_OFF>	off/on	Enable the 'password activation' service. At first, activate the 'restriction of outgoing communication'

			service
set password restrict out once enable	<ON_OFF>	off/on	Enable the 'outgoing communication by password' service. At first, activate the 'restriction of outgoing communication' service
set password value	<VALUE>	string of 4 numbers	Set a password for the 'restriction of outgoing communication' service
set restrict out enable	<ON_OFF>	off/on	Enable the 'restriction of outgoing communication' service
set restrict out value	<ACCESS_MODE>	On/ Denied_6/ Denied_7/ Denied_8	Outgoing restriction mode: • *On* – everything is allowed; • *Denied_6* – access only to emergency; • *Denied_7* – access only to emergency, local and departmental communications; • *Denied_8* – access only to emergency, local, departmental and zonal communications
show count			Show the number of free VAS blocks

3.3.33 Subscriber group VAS configuration mode

To enter this mode, in the SIP subscribers configuration mode run the **service group <USER_INDEX>** command, where **<USER_INDEX>** is a SIP suscriber index.

```
SMG-[CONFIG]-SIP-USERS> service group 0
Entering UserGroup-Service mode for user-group 0
SMG-[CONFIG]-[SIP-USERS][0]-GROUP-SERVICE>
```

Command	Parameter	Value	Action
?			Show list of available commands
attach service blocks manual			VAS connection mode for group subscribers - manual
attach service blocks radius			VAS connection mode for group subscribers - via RADIUS
detach service block			Disable VAS for a group
exit			Exit from this configuration submenu to a higher level
quit			End this CLI session
set call-pickup enable	<ON_OFF>	off/on	Enable the 'call pickup' service
set cfb enable	<ON_OFF>	off/on	Enable the 'forwarding for busy' service
set cfb number	<ON_OFF>	number up to 30 characters or none	Set the number for 'forwarding for busy' service: ● *none* – disable call forwarding
set sfnr enable	<ON_OFF>	off/on	Enable the 'forwarding for no response' service
set sfnr number	<ON_OFF>	number up to 30 characters or none	Set the number for 'forwarding for no response' service: ● *none* – disable call forwarding
set cfos enable	<ON_OFF>	off/on	Enable the 'forwarding for out of service'
set cfos number	<ON_OFF>	number up to 30 characters or none	Set the number for the 'forwarding for out of service': ● *none* – disable call forwarding
set cfu enable	<ON_OFF>	off/on	Enable the 'unconditional forwarding' service
set cfu number	<ON_OFF>	number up to 30 characters or none	Set the number for the 'unconditional forwarding': ● *none* – disable call forwarding
set clear-all enable	<ON_OFF>	off/on	Enable the 'clear all services'
set conf-3way enable	<ON_OFF>	off/on	Enable the '3way conference' service. At first, activate the 'call hold' service
set conference enable	<ON_OFF>	off/on	Enable the 'conference with sequential collection' service
set ct enable	<ON_OFF>	off/on	Enable the 'call transfer' service. At first, activate the 'call hold' service
set hold enable	<ON_OFF>	off/on	Enable the 'call hold' service
set intercom enable	<ON_OFF>	off/on	Enable the 'intercom' service
set password change enable	<ON_OFF>	off/on	Enable the 'password change' service
set password restrict out access active	<ON_OFF>	off/on	Password activation for the 'password activation' service. The *on* value makes the password active and the communication restriction is removed
set password restrict out access enable	<ON_OFF>	off/on	Enable the 'password activation' service. At first, activate 'restriction of

			outgoing communication' the service
set password restrict out once enable	<ON_OFF>	off/on	Enable the 'outgoing communication by password' service. At first, activate the 'restriction of outgoing communication' service
set restrict out enable	<ON_OFF>	off/on	Enable the 'restriction of outgoing communication' service
show group-flags			Show the current VAS settings
show count			Show the number of free VAS blocks

3.3.34 PRI subscribers parameters configuration mode

To enter this mode, in the configuration mode run the **pri-users** command.

```
SMG-[CONFIG]> pri-users
Entering SIP-Users mode.
SMG-[CONFIG]-[PRI-USERS]>
```

Command	Parameter	Value	Action
?			Show list of available commands
add user	<NUMBER> <STREAM>	subscriber number E1 stream number 0-15	Create a new subscriber
remove by id	<USER_ID>	subscriber ID to be deleted	Delete subscriber by ID
remove by index	<INDEX>	subscriber index to be deleted	Delete subscriber by index
service	<USER_INDEX>	subscriber index	Switching to the VAS control mode of the subscriber
set by id access category	<USER_ID> <CAT_IDX>	subscriber ID 0-127	Set access category by subscriber ID
set by id access_mode	<USER_ID> <ACCESS>	subscriber ID Off/On/Off_1/Off_2/Denied_1/Denied_2/Denied_3/Denied_4/Denied_5/Denied_6/Denied_7/Denied_8/Exclude	Set service mode by subscriber ID
set by id name	<USER_ID> <USER_NAME>	subscriber ID string of 63 characters	Set the subscriber's name by ID
set by id number	<USER_ID> <NUMBER>	subscriber ID subscriber's telephone number	Set number by subscriber ID
set by id pbx_profile	<USER_ID> <PROFILE>	subscriber ID 0-15	Set PBX profile by subscriber ID
set by index access category	<INDEX> <CAT_IDX>	subscriber index 0-127	Set access category by subscriber index
set by index access_mode	<INDEX> <ACCESS>	subscriber index Off/On/Off_1/Off_2/Denied_1/Denied_2/Denied_3/Denied_4/Denied_5/Denied_6	Set service mode by subscriber index

		/Denied_7/Denied_8 /Exclude	
set by index name	<INDEX> <USER_NAME>	subscriber index string of 63 characters	Set the subscriber name by index
set by index number	<INDEX> <NUMBER>	subscriber index subscriber's telephone number	Set number by subscriber index
set by index pbx_profile	<INDEX> <PROFILE>	subscriber index 0-15	Set PBX profile by subscriber index
set by index pri_profile	<INDEX> <PROFILE>	subscriber index 0-31	Set PRI profile by subscriber index
show all			Show settings for all PRI subscribers
show by id	<USER_ID>	subscriber ID	Show subscriber settings by ID
show by index	<INDEX>	subscriber index	Show subscriber settings by index
show count			Show total number of PRI subscribers
show list users			Show a list of all PRI users

3.3.35 PRI subscribers VAS configuration mode

To enter this mode, in the PRI subscriber configuration mode run the **service <USER_INDEX>**, where **<USER_INDEX>** is a PRI suscriber index.

```
SMG-[CONFIG]-[PRI-USERS]> service 0
Entering User-Service mode for user 0
SMG-[CONFIG]-[PRI-USERS][0]-SERVICE>
```

Command	Parameter	Value	Action
?			Show list of available commands
attach service block			Attach VAS for a subscriber
detach service block			Detach VAS for a subscriber
set cfb enable	<ON_OFF>	off/on	Enable the ‘forwarding for busy‘ service
set cfb number	<ON_OFF>	number up to 30 characters or none	Set the number for ‘forwarding for busy’ service: ● *none* – disable call forwarding
set sfnr enable	<ON_OFF>	off/on	Enable the ‘forwarding for no response‘ service
set sfnr number	<ON_OFF>	number up to 30 characters or none	Set the number for ‘forwarding for no response’ service: ● *none* – disable call forwarding
set cfos enable	<ON_OFF>	off/on	Enable the ‘forwarding for out of service’
set cfos number	<ON_OFF>	number up to 30 characters or none	Set the number for the ‘forwarding for out of service’: ● *none* – disable call forwarding
set cfu enable	<ON_OFF>	off/on	Enable the ‘unconditional forwarding’ service
set cfu number	<ON_OFF>	number up to 30 characters or none	Set the number for the ‘unconditional forwarding’: ● *none* – disable call forwarding
show count			Show the number of free VAS blocks

3.3.36 PRI profiles configuration mode

To enter this mode, in the configuration mode run the **`pri_profiles`** command.

```
SMG-[CONFIG]> pri_profiles
Entering PRI profiles mode.
SMG-[CONFIG]-PRI_PROFILES>
```

Command	Parameter	Value	Action
?			Show list of available commands
add pri_profile	<NAME>	string, max 63 characters	Create a PRI profile
config			Return to the configuration menu
exit			Exit from this configuration submenu to a higher level
quit			End this CLI session
remove pri_profile	<PROFILE_INDEX>	0-31	Delete a PRI profile
set mode	<PROFILE_INDEX> <PROFILE_MODE>	0-31 start_first_forward/ start_last_backward	Set the pri-profile operation mode (from the first forward / from the last backward)
set modifiers table outgoing called	<PROFILE_INDEX> <MODTBL_INDEX>	0-31 0-255/none	Set a modifier for the PRI profile based on the parsing of the called party number transmitted to the outgoing channel
set modifiers table outgoing calling	<PROFILE_INDEX> <MODTBL_INDEX>	0-31 0-255/none	Set a modifier for the PRI profile based on parsing the calling number transmitted to the outgoing channel
set modifiers table outgoing original called	<PROFILE_INDEX> <MODTBL_INDEX>	0-31 0-255/none	Set a modifier for the PRI profile based on parsing the original called party number transmitted to the outgoing channel
set modifiers table outgoing redirecting	<PROFILE_INDEX> <MODTBL_INDEX>	0-31 0-255/none	Set a modifier for the PRI profile based on the analysis of the redirecting number transmitted to the outgoing channel
set name	<PROFILE_INDEX> <NAME>	0-31 string, max 63 characters	Set PRI profile name
show			Show PRI profile settings
stream_list add	<PROFILE_INDEX> <STREAM>	0-31 1-4	Add E1(Q.931) stream to PRI profile
stream_list remove	<PROFILE_INDEX> <STREAM>	0-31 1-4	Remove E1(Q.931) stream from PRI profile

3.3.37 SS7 categories configuration mode

To enter this mode, in the configuration mode run the **ss7cat** command.

```
SMG-[CONFIG]> ss7cat
Entering SS7-categories mode.
SMG-[CONFIG]-SS7-CAT>
```

Command	Parameter	Value	Action
?			Show list of available commands
config			Return to the configuration menu
exit			Exit from this configuration submenu to a higher level
quit			End this CLI session
set	<CAT_IDX> <PBX_CAT> <SS7_CAT>	0-15 0-10 0-255	Set data category: • *CAT_IDX* – category index; • *PBX_CAT* – AON category; • *SS7_CAT* – SS7 category
show			Show information about the SS7 data category

3.3.38 Syslog parameters configuration mode

To enter this mode, in the configuration mode run the **syslog** command.

```
SMG-[CONFIG]> syslog
Entering syslog mode.
SMG-[CONFIG]-SYSLOG>
```

Command	Parameter	Value	Action
?			Show list of available commands
alarm	<ALARM>	0-99	Transmit data about alarms with the specified priority level, 0 – data will not be transmitted
apply	yes/no		Apply syslog settings
authlog set	IP PORT ONOFF LOCREM	IP address in the AAA.BBB.CCC.DDD format 1-65535 off/on local/remote	Set the server address for sending syslog messages, as well as the operation mode: • *on/off* – enable/disable logging; • *local/remote* – if set to remote, then send logs to the syslog server
authlog show			Show current logging settings
calls	<CALLS>	0-99	Enable call tracing with the specified debug level, 0 – data will not be transmitted
config			Return to the configuration menu
exit			Going from this configuration submenu to a higher level
fxs	<FXS>	0-99	Enable fxs port tracing with the specified debug level, 0 – data will not be transmitted
h323	<H323>	0-99	Enable H.323 signaling tracing with debug level set, 0 – no data will be transmitted
hw	<E1> <HW>	0-15 0-99	Transmit hardware data of the E1 stream with the specified debug level, 0 – data will not be transmitted:

			• *E1* – E1 stream number; • *HW* – priority level
ipaddr	<IPADDR>	IP address in the AAA.BBB.CCC.DDD format	Set syslog server IP address
isup	<ISUP>	0-99	Enable ISUP tracing with the specified debug level, 0 – data will not be transmitted
ivr	<IVR>	0-99	Enable ivr tracing with the specified debug level, 0 – data will not be transmitted
port	<PORT>	1-65535	Set local port number
Q931	<Q931>	0-99	Enable Q.931 signaling tracing with debug level set, 0 – data will not be transmitted
quit			End this CLI session
radius	<RADIUS>	0-99	Enable RADIUS protocol tracing with the specified debug level, 0 – data will not be transmitted
rtp-create	<RTP>	0-99	Enable tracing the creation of RTP connections with the specified debug level, 0 – data will not be transmitted
show			Show syslog configuration information
sipt	<SIPT>	0-99	Enable SIP-T signaling tracing with debug level set, 0 – data will not be transmitted
smvp	<SMVP>	0-99	Enable tracing of sm-vp submodules with the specified debug level, 0 – data will not be transmitted
start			Enable sending data to syslog server
stop			Disable sending data to syslog server

userlog	<IPADDR>
	
	<PORT>
	
	<MODE>
		IP address in the AAA.BBB.CCC.DDD format
		
		1-65535
		
		off/standart/full
			Enable displaying the history of entered commands:
			• *IPADDR* – syslog server IP address;
			• *PORT* – Syslog server port;
			• *MODE* – verbosity level of command log:
			  ◦ *off* – do not generate a log of entered commands;
			  ◦ *standart* – the name of the changed parameter is transmitted in the messages;
			  ◦ *full* – messages contain the name of the changed parameter and the parameter value before and after the change

3.3.39 Voice message files configuration mode

To enter this mode, in the configuration mode run the **user-voice-files** command.

```
SMG-[CONFIG]> user-voice-files
Entering User voice-files setup mode.
SMG-[CONFIG]-USER_VOICE_FILES>
```

Command	Parameter	Value	Action
?			Show list of available commands
exit			Moving from this configuration submenu to a higher level
quit			End this CLI session
remove	<FILE_TYPE>	trunk_busy/ trunk_error/ number_fail/ access_denied_temp/ service_restricted/ access_restricted/ access_unpaid/ user_unallocated/ user_changing/ music_on_hold/ number_changed/ conf_greeting/ conf_switch/ record_notification/ intercom_announce/ voice_mail_announce	Delete user file with a given type
set	<FILE_TYPE>	trunk_busy/ trunk_error/ number_fail/ access_denied_temp/ service_restricted/ access_restricted/ access_unpaid/ user_unallocated/ user_changing/music_on_hold/ number_changed/ conf_greeting/ conf_switch/ record_notification/ intercom_announce/ voice_mail_announce	Enable use of custom file with a given type
show files			Show uploaded user files
show usage			Show user file usage

3.3.40 IVR functions configuration mode

To enter this mode, in the configuration mode run the **ivr** command.

```
SMG-[CONFIG]> ivr
Entering IVR-setup mode
SMG-[CONFIG]-IVR>
```

Command	Parameter	Value	Action
?			Show list of available commands
add scenario			Add a new IVR script file
config			Return to the configuration menu
delete scenario			Delete IVR script file
download scenario		<SRC_PATH_AND_FILE_NAME> <DST_FILE_NAME> <SERVER_IP>	Download script from device via tftp
exit			Exit from this configuration submenu to a higher level
quit			End this CLI session
remove scenario		Index [0-255]	Delete IVR script
set scenario filename		Index [0-255]	Set IVR script file name
set scenario name		Index [0-255]	Set IVR script name
set scenario path		default or /mnt/sd[abc][1-7]	Set path for storing IVR scripts
show list scenarios			Show all IVR script files
show path scenario			Show path to store IVR script files
show scenario		Index [0-255]	Show script IVR

3.3.41 Trunk group configuration mode

To enter this mode, in the configuration mode run the **trunk group <TRUNK_INDEX>** command, where **<TRUNK_INDEX>** is the trunk group.

```
SMG-[CONFIG]> trunk group 0
Entering trunk-mode.
SMG-[CONFIG]-TRUNK[0]>
```

Command	Parameter	Value	Action
?			Show list of available commands
channel add	CHAN_INDEX	0-31	Add a channel of the selected E1 stream to the E1-channels trunk group
channel order	CHAN_ORDER	successive_forward/ successive_backward/ start_first_forward/ start_last_backward	Select an order of channel engagement in the truck goups E1-channels or Linkset-Line
channel remove	CHAN_INDEX	0-31	Remove E1 stream channel from E1-channels trunk group
config			Return to the configuration menu
cps max	<CPS_MAX>	0-255	CPS limit that can be passed through a trunk group
cps warn	<CPS_WARN>	0-255	CPS alarm value, over which a warning will be issued in the alarm log

destination	<TG_ENTRY> <ENTRY_INDEX>	Q.931/SS7/SIPT/ E1-channels/ Linkset-Line/ FXO-line unsigned integer	Assign a trunk group to the Q931, SS7, SIP-T interface, individual channels of the E1 stream, or individual streams of the SS7 linkset, FXO line: • *TG_ENTRY* – interface type; • *ENTRY_INDEX* – object index (stream number with Q931/SS7 signaling, line group, SIP-T interface, SS7 linkset, FXO line)
direct prefix	<IDX>	0-255/none	Set direct switching of calls from the given trunk group to the specified prefix, without parsing the calling and called subscriber numbers
disable all	<YES_NO>	yes/no	Deny/allow outgoing and incoming calls for this trunk group
disable in			Deny incoming calls for this trunk group
disable out			Deny outgoing calls for this trunk group
exit			Exit from this configuration submenu to a higher level
history			View the history of entered commands
linkset-line add	<LINE_INDEX>	0-15	Add an E1 stream from the selected SS7 linkset to the Linkset-Line trunk group
linkset-line remove	<LINE_INDEX>	0-15	Delete an E1 stream from the Linkset-Line trunk group
modifiers table incoming called	<MODTBL_INDEX>	0-255/none	Set trunk group modifier for modifications based on parsing the called party number received from the incoming channel
modifiers table incoming calling	<MODTBL_INDEX>	0-255/none	Set a trunk group modifier for modifications based on parsing the calling number received from the incoming channel
modifiers table outgoing called	<MODTBL_INDEX>	0-255/none	Set a trunk group modifier for modifications based on parsing the called party number sent to the outgoing channel
modifiers table outgoing original	<MODTBL_INDEX>	0-255/none	Set a trunk group modifier for modifications based on parsing the original called party number sent to the outgoing channel
modifiers table incoming redirecting	<MODTBL_INDEX>	0-255/none	Set a trunk group modifier for modifications based on parsing the redirecting number sent to the outgoing channel
modifiers table outgoing calling	<MODTBL_INDEX>	0-255/none	Set a trunk group modifier for modifications based on parsing the calling number received from the incoming channel
name	<s_name>	allowed to use letters, digits, symbol '_'. Maximum 31 characters	Set a trunk group name

quit			End this CLI session
radius profile incoming	<IDX>	0-31/no	Set RADIUS profile on incoming link
radius profile outgoing	<IDX>	0-31/no	Set RADIUS profile on outgoing link
recover on egress failure	<RECOVER>	no/yes	Restore calls after outgoing leg failure
reserv	<TG_RSV_IDX>	0-31	Set reserve trunk group number
show			Show trunk group configuration

3.3.42 Trunk direction configuration mode

To enter this mode, in the configuration mode run the **trunk direction <DIRECTION_INDEX>** command, where **<DIRECTION _INDEX>** is the trunk group number.

```
SMG-[CONFIG]> trunk direction 0
Entering trunk-mode.
SMG-[CONFIG] - TRUNK_DIRECTION[0]>
```

Command	Parameter	Value	Action
?			Show list of available commands
config			Return to the configuration menu
exit			Moving from this configuration submenu to a higher level
history			View the history of entered commands
list add	<TD_TRUNK>	0-63	Add a trunk group with the given index to the direction
list remove	<TD_TRUNK>	0-63	Remove trunk group with given index from the direction
mode		successive_forward/ successive_backward/ first_forward/ last_backward	Set trunk group selection method in direction: • *Successive forward;* • *Successive backward;* • *Starting from the first forward;* • *Starting from last backward*
name	<s_name >	string, max 63 characters	Set trunk direction name
quit			End this CLI session
show			Show trunk direction settings

APPENDIX A. CABLE CONTACT PIN ASSIGNMENT

Table A1 – Assignment of **RJ-11** Connector Pins for FXS/FXO ports (SMG-200)

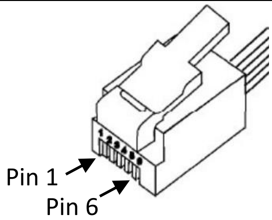
Contact Pin No. (Pin)	Assignment	Contact Pin Numbering
1	Not used	
2	Not used	
3	To connect FXS/FXO	
4	To connect FXS/FXO	
5	Not used	
6	Not used	

Table A2 – Assignment of **RJ-48** Contactor Pins for E1 streams connection (SMG-500)

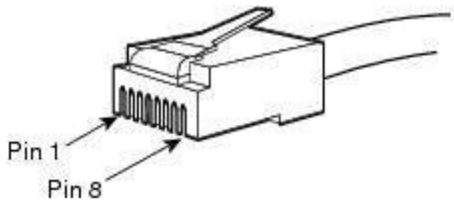
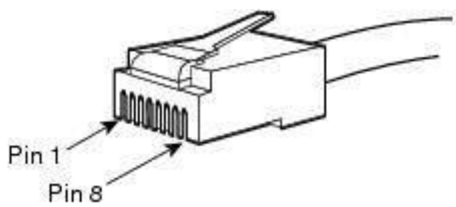
Contact Pin No. (Pin)	Assignment	Contact Pin Numbering
1	RCV tip (data reception)	
2	RCV ring (data reception)	
3	RCV shield (shield of the receiver)	
4	XMT tip (data transmission)	
5	XMT ring (data transmission)	
6	XMT shield (shield of the transmitter)	
7	Not used	
8	Not used	

Table A3 – Assignment of **RJ-45** Contactor 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. BACKUP 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, where the TFTP server is running> <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, the firmware can be updated as described in section 3.1.22.

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 line[1]

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, ТППэп, ТППЗ, ТППэпЗ, ТППБ,ТПП эпБ, ТППЗБ, ТППБГ, ТППэпБГ, ТППБбШп, ТППэпБбШп, ТППЗБбШп, ТППЗэпБбШп, 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 types[2]:

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

$L_{cab} = R_{cab}/R_{sp20}$ [km]

3 Loop resistance at 20°C

$L_{lp} = 2 * L_{cab}$

$R_{lp} = L_{lp} * R_{sp20} = 2 * L_{cab} * R_{sp20}$;

$L_{lp} = R_{lp}/R_{sp20}$.

For telephone lines, the loop resistance takes into account the telephone set resistance: 600 Ω.

[1] Line length values for the RUS telephone set will be lower than those indicated in the table.
[2] Taken from the website http://izmer-ls.ru/shle.html.

APPENDIX D. TRANSMISSION OF VAS SETTINGS FROM 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 3.1.17.3), 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, one 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 identifier of the command, the identifier of the connection/disconnection of the VAS service for which the configuration is being performed, and the VAS 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 enabling/disabling 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 – conference with sequential collection;
- 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 services have been activated for a 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 services have 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

Submit the following request:

```
UserService:CFU=yes;numCFU=12345;CFNR=yes;numCFNF=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

Submit the following request:

```
UserService:CFU=no;CallPickup=no;CT=yes;BLF=yes;limitBLF=5;
```

APPENDIX E. CORRELATION BETWEEN ROUTING, SUBSCRIBERS, AND SIGNAL LINK PARAMETERS

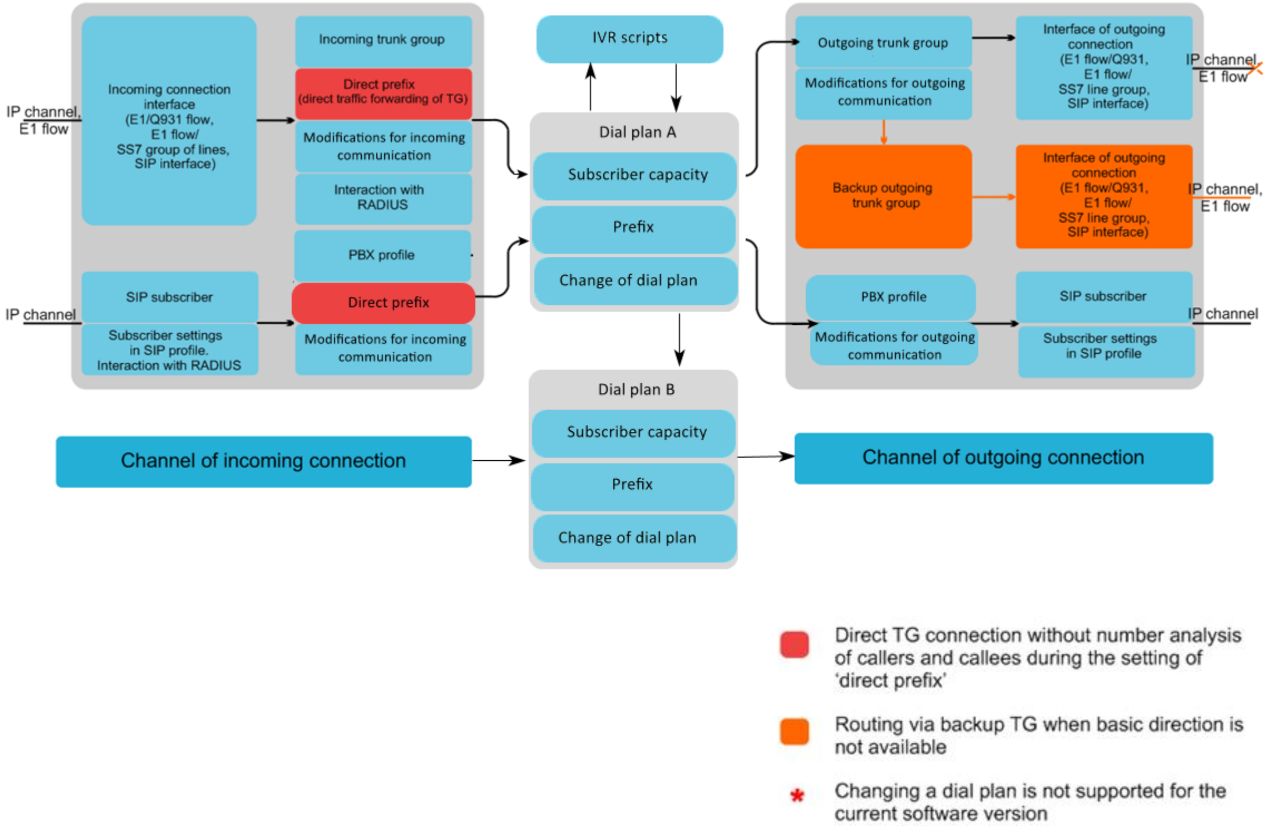


Fig. 20 – Correlation between routing, subscribers and signal link parameters

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 in 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 in 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 F. GUIDELINES FOR SMG OPERATION IN A PUBLIC NETWORK

When installing and configuring the SMG, it is required to pay attention to the security settings - organizing access to the management and monitoring of the PBX, as well as the security of call processing. It is also necessary to pay attention to backing up the configuration.

Organization of access means:

- change of standard passwords for WEB and CLI;
- creation of limited accounts for certain types of settings and monitoring;
- configuring restrictions of IP addresses and/or subnets from which configuration and monitoring can be performed;
- setting up a static firewall that restricts access to signaling and control interfaces only to trusted hosts;
- setting up a dynamic firewall, which will automatically cut off unwanted access attempts for public interfaces.

Avoid using SMG in a public network without additional protective measures like session border controller (SBC), firewall, etc.

Changing passwords on WEB and CLI

Changing passwords for admin/root accounts is mandatory to ensure device security.

Passwords can be changed through the '*Users: Management*' menu.

Changing the WEB password for the admin account is done in the '*Set web interface administrator password*' section.

Changing the CLI password for the admin account is done in the '*Set administrator password for telnet and ssh*' block. For more details on setting, please refer to section 3.1.25 Management menu.

Changing the password for the root account is done through the shell. In order to change the password, connect to the SMG via ssh/console and run the following commands:

```
SMG200>
SMG200> sh (going from cli into shell mode)
/home/admin #
/home/admin #
/home/admin # passwd root (command for changing password for root)
Changing password for root
New password: (enter a new password)
Retype password: (retype new password)
Password for root changed by root
/home/admin #
/home/admin #
/home/admin # save
tar: removing leading '/' from member names
***Saved successful
New image 0
Restored successful
/home/admin #
```

Creating restricted accounts

Creation of restricted accounts for the WEB is done through the '*Users: Management*' menu.

- In the 'web-interface users' block, click 'Add';
- Set username and password;
- Select an access permission.

For the CLI, the creation of restricted accounts is not supported. For details on setting, please refer to section 3.1.25 Management Menu.

Restricting of access to signaling and control interfaces

Restrictions are configured in the '*TCP/IP Settings' -> 'Network Interfaces*' menu.

- Go to network interface settings;
- In the 'Services' block, disable all control and signaling protocols that are not used on the interface;
- For the management interface, it is recommended to allow access only to the web interface and ssh.

For more detailed configuration information, please refer to section 3.1.13.3 Network Interfaces.

Access to the device via the telnet protocol should be denied through the public IP address.

The management should be allowed NOT through public addresses. If the management is used through public IP, then definitely use the list of allowed IP addresses – add to the whitelist the address from which the connection will be allowed. For all other addresses, the access should be denied.

Changing the standard ports for accessing the device

The setting is made in the 'TCP/IP Settings'-> 'Network Settings' menu.

- Change standard (22 for ssh and 23 for telnet) access ports to the device via ssh/telnet protocols;
- The standard port for accessing the device via the web (http protocol) can be changed via the CLI. To do this, connect to the SMG via ssh/console and run the following commands:

```
SMG200>
SMG200> config
Entering configuration mode.
SMG200-[CONFIG]> network
Entering Network mode.
SMG200-[CONFIG]-NETWORK>
PORT Number in the range 1-65535
SMG200-[CONFIG]-NETWORK> set settings web (specify the required port in
the range 1-65535)
```

It is recommended to use the HTTPS protocol to access the web interface. Its operation can be configured in the '*Security' -> 'Configure SSL / TLS*' section. In the SSL/TLS settings for the 'Protocol for web interface', the 'HTTPS only' mode should be selected. It is also possible to use authorization via PAM/RADIUS. For more information on setting up, see section 3.1.16.1 SSL/TLS settings.

Configuring the white list

The setting is made in the '*Security' -> 'White addresses list*' menu.

- To the White list, add addresses, from which access to the device is allowed via the web configurator and via telnet/ssh protocols;
- Select thy checkbox for the 'Access only for allowed IP-addresses';
- Click 'Apply' and 'Confirm'.

For details on setting, please refer to 3.1.16.5 White addresses list.

Configuring a static firewall

The static firewall is used to restrict access to network interfaces according to a list of predefined rules. The setting is made in the '*Security -> Static firewall*' menu.

- Go the '*Security -> Static firewall*' menu;
- Create a firewall prodile by clicking '*Add'*;
- Set a profile name, click '*Next'*;
- Set up filtering rules for incoming and outgoing traffic. At the same time, it should be remembered that if an incoming or outgoing packet does not match any filtering rule, then the '*Accept*' action is applied to it (allow the packet to pass through). Therefore, if you want to allow access only to some hosts and deny all others, then you need to configure the firewall profile so that the last rule is a rule with a source type and destination '*Any*' and the action '*Reject*' or '*Drop*' (drop the packet with ICMP notification or discard without notice);
- In the '*Interface*' block, select the network interfaces for which filtering will be applied;
- Click '*Save*' located under the list of interfaces;
- Click '*Apply'* located at the top of the page;
- Click '*Save*' located above the filter tables.

For details on setting, please refer to 3.1.16.4 Static firewall.

Configuring a dynamic firewall

A dynamic firewall is used to restrict access to network interfaces based on the analysis of requests to various services. When it detects repeated unsuccessful attempts to access the service from the same IP address, the dynamic firewall temporarily blocks it. If an address is temporarily blocked several times, it is permanently blocked in the black list of addresses. The setting is made in the '*Security -> Dynamic firewall*' menu.

- Go the '*Security -> Dynamic firewall*' menu;
- To the white list add addresses of the trusted hosts and subnets;
- Select the checkbox '*Enable'*;
- Click '*Apply'.*

For details on setting, please refer to 3.1.16.2 Dynamic firewall.

It is not recommended to use the standard port 5060 for SIP signaling. It is necessary to periodically check the information in the '*Security' -> 'Blocked addresses list*' section. It displays a list of addresses blocked by the dynamic firewall from which an unsuccessful attempt was made to gain access to the device.

It is recommended to periodically change passwords to access the device via web/ssh. The password change policy should be determined by your security team.

It is recommended to use the latest version of the software: https://eltex-co.ru/support/downloads/.

APPENDIX G. 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 G1 – 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	The wrong number has been dialed	When calling to a non-existent prefix When receiving Q.850 cause = 3, 28
ACCS_DENIED_TEMP	The number cannot be called temporarily	When calling 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.

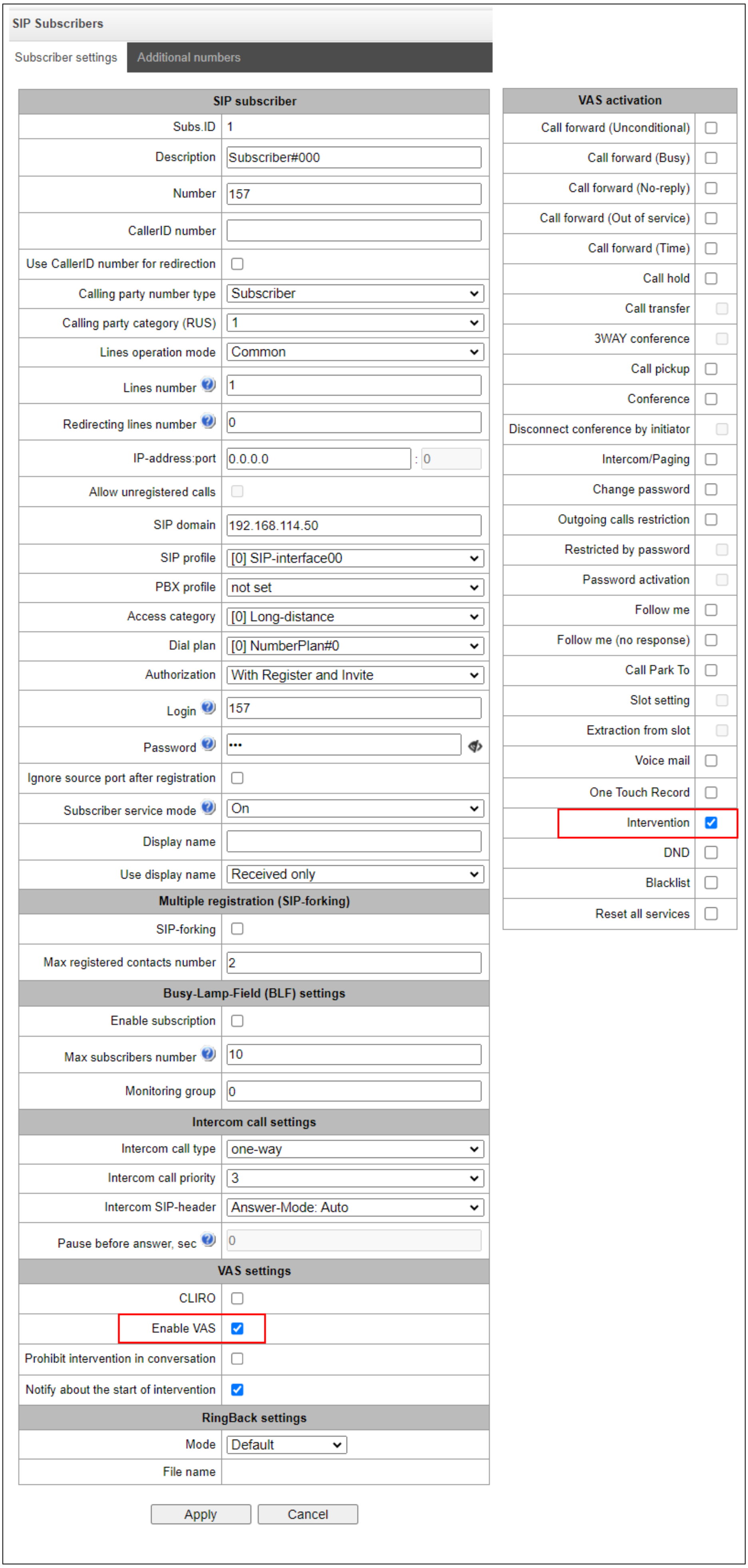
APPENDIX H. WORKING WITH VAS SERVICES

Starting from the firmware version 2.15.01, the device supports the following VAS services:

- *Call Forward (Unconditional)* – enables the Call Forwarding Unconditional (CF Unconditional) service;
- *Call Forward (Busy)* – enables the Call Forwarding Busy (CF Busy) service;
- *Call Forward (No Reply)* – enables the Call Forwarding No Reply (CF No Reply) service;
- *Call Forward (Out of Service)* – enables the Call Forwarding Out of Service (CF Out of Service);
- *Call hold;*
- *Call transfer* – enables the Call Transfer service;
- *3Way conference;*
- *Call pickup;*
- *Conference with sequential collection (CONF);*
- *Disconnect conference by initiator* – when checked, 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;
- *Intercom* — activation of access to the outgoing intercom or paging call service (call with auto-reply of party B);
- *Change password (PWD);*
- *Outgroing calls restriction;*
- *Restricted by password;*
- *Password activation;*
- *Do not disturb (DND);*
- *Blacklist;*
- *Follow me;*
- *Follow me (no response);*
- *Call Park To;*
- *Slot setting (within call parking service);*
- *Extraction from slot (within call parking service);*
- *Cancel all services.*

For a subscriber to be able to use the VAS services, select the '*Enable 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 Subscribers
Subscriber settings
Additional numbers
SIP subscriber
Subs.ID 1
Description Subscriber#000
Number 157
CallerID number
Use CallerID number for redirection
Calling party number type Subscriber
Calling party category (RUS) 1
Lines operation mode Common
Lines number 1
Redirecting lines number 0
IP-address:port 0.0.0.0 : 0
Allow unregistered calls
SIP domain 192.168.114.50
SIP profile [0] SIP-interface00
PBX profile not set
Access category [0] Long-distance
Dial plan [0] NumberPlan#0
Authorization With Register and Invite
Login 157
Password •••
Ignore source port after registration
Subscriber service mode On
Display name
Use display name Received only
Multiple registration (SIP-forking)
SIP-forking
Max registered contacts number 2
Busy-Lamp-Field (BLF) settings
Enable subscription
Max subscribers number 10
Monitoring group 0
Intercom call settings
Intercom call type one-way
Intercom call priority 3
Intercom SIP-header Answer-Mode: Auto
Pause before answer, sec 0
VAS settings
CLIRO
Enable VAS
Prohibit intervention in conversation
Notify about the start of intervention
RingBack settings
Mode Default
File name
Apply
Cancel
VAS activation
Call forward (Unconditional)
Call forward (Busy)
Call forward (No-reply)
Call forward (Out of service)
Call forward (Time)
Call hold
Call transfer
3WAY conference
Call pickup
Conference
Disconnect conference by initiator
Intercom/Paging
Change password
Outgoing calls restriction
Restricted by password
Password activation
Follow me
Follow me (no response)
Call Park To
Slot setting
Extraction from slot
Voice mail
One Touch Record
Intervention
DND
Blacklist
Reset all services

1. Working with *Call Hold*, *Call Forward* and *3WAY Conference* Services

The *Call Forward* 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 Forward service: example

Subscriber A calls to subscriber B. During the call, subscriber B can press FLASH and put subscriber A on hold. During this on-hold time, 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:

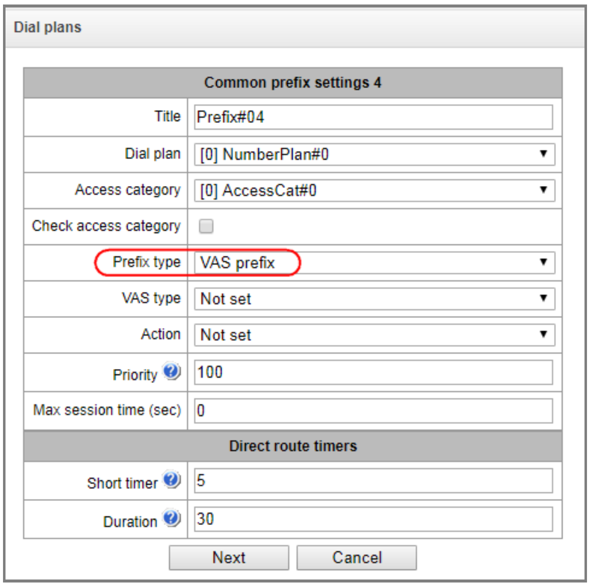
- first digit dial timeout: 15 seconds
- next digit dial timeout: 5 seconds
- busy signal timeout: 60 seconds

2. Working with the Call Forward service

The *Call Forward* service can be configured using the appropriate web-configurator settings in the *SIP Subscribers/VAS Management/Select Subscriber* menus (section 3.1.7.1.3) 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 dial plan (section 3.1.4 Dial plan). To do this, add a new prefix with the *Prefix Type* value set to *VAS Prefix.*



It is recommended to use the following prefix values for VAS services:

Call Forward Unconditional (CF Unconditional):

- activation (*21*|*21*x.#);
- deactivation (#21#);
- control (*#21*|*#21*x.#).

Call Forward Busy (CF Busy):

- activation (*22*|*22*x.#);
- deactivation (#22#);
- control (*#22*|*#22*x.#).

Call Forward No Reply (CF No reply).

- activation (*61*|*61*x.#);
- deactivation (#61#);
- control (*#61*|*#61*x.#).

Call Forward 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 dial plan 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 Forward* 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 dialed number matches the previously defined number, the subscriber will hear the *station response* signal. If the service is not activated or the dialed 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 sequential participant collection

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 calls restricted by password

Using these services, the subscriber can override the service access restrictions, i. e. the restrictions set by the *Outgoing calls restriction* service.

For example, if restrictions on outgoing communication are set, the subscriber, using the *Outgoing calls 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 *Restricted by password* service, select the checkbox for this VAS service category.

Password code – activation	* 29 * <PASSWORD> #
Password code – deactivation	# 29 #
Outgoing calls restricted by password	* 32 * <PASSWORD> #

<PASSWORD> – a personal password code of the subscriber.

6. Change Password

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 *Change password* 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. Restriction of the outgoing calls by password

The service allows configuring a restriction on access from the subscriber's telephone set to certain types of outgoing communications. The following groups of communication types are defined for using this service:

Group 1 – communication only with emergency services;

Group 2 – communications only with emergency services and local communications;

Group 3 – types of communication assigned to groups 1 and 2 and zone communication.

The type of connection is set in the prefixes parameters.

To bypass the restriction set using this service, use the *Restricted by password* and *Password activation* services. To restore the restriction removed by the *Password activation* service, use the *Password deactivation* service.

Access to the service is controlled by the *Outgoing calls restriction c*heck box of VAS category.

Ordering the service	* 34 * <PASSWORD> * N #
Cancelling the service	# 34 * <PASSWORD> #
Control	* #34 * <PASSWORD> #

<N> – group number for allowed communication types.

8. Do not disturb

The service allows preventing 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> #
Remove a number from white list	# 26 * <NUMBER> #
Remove all numbers from white list	# 26 * 0 # # 26 * 00 #

9. Blacklist

The service allows prohibiting calls to the subscriber from certain numbers.

Access to the service is controlled by the *Black list* check box.

Service order	* 61 * <PASSWORD> #
Service cancellation	# 61 * <PASSWORD> #
Control	* # 61 * <PASSWORD> #
Add number to blacklist	* 61 * <PASSWORD> * <NUMBER> #
Remove a number from blacklist	# 61 * <PASSWORD> * <NUMBER> #
Remove all numbers from blacklist	# 61 * <PASSWORD> * 0 # # 61 * <PASSWORD> * 00 #

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 number	#23*PIN*LOCAL_PHONE#
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:

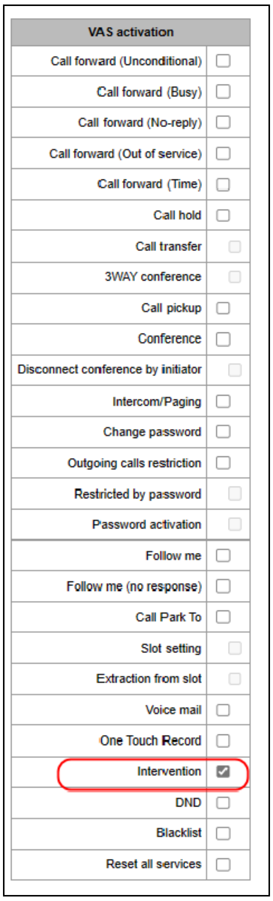
The service activation with a temporary PIN code is performed on the local number	*25*PIN#
The service activation without a PIN code is performed on the local number	*25#
Call forwarding from the local to the remote telephone set with a temporary PIN is performed on the remote number	* 25 * PIN * LOCAL_PHONE #

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#

where

- *PIN* – a secret digital code consisting of 4–12 characters;
- *LOCAL_PHONE* – the phone number from which the calls will be forwarded.

12. Intervention



Description:

The *Intervention* service allows you to join an already established conversation either in observing mode, or in consultation mode, or in conference mode.

After activating the service, the connection is made in the observing mode.

Then, it is possible to change the mode (by sending dtmf):

- 0 – observing (only listening);
- 1 – consultation (listening to the entire conversation and the ability to communicate only with the subscriber to whom the intrusion has been made);
- 3 – conference (full interaction with all participants in the conversation).

In addition to listening modes, it is possible to terminate a two-way connection by a third party:

9 – abort (termination of a connection by a third party)

It is also possible to intervene immediately with the desired mode.

Use

Subscriber 1302 needs to be given the opportunity to interfere in the conversations of other subscribers of the station.

To do this, activate the *Intervention* service in the subscriber's VAS settings.

For example, subscribers A and B are in a conversation. Subscriber C needs to connect to subscriber A.

Then the subscriber C dials the intervention code (by default * 09 *), the number of the subscriber (A), in whose conversation the subscriber C wants to intervene and the # button.

For example, to interfere in the conversation of subscriber A, subscriber C needs to dial the combination *09*NUMBER_A#.

Subscriber C starts listening to the conversation between subscribers A and B.

And subscriber C has the following modes available:

1 Observing. The subscriber enters this mode immediately after activating the intervention.

2 Consultation. To switch to this mode, subscriber C needs to press the digit 1. After that, the subscriber to whom the intrusion has been made (subscriber A) will hear it. The third subscriber (B), with whom subscriber A is talking, still does not hear subscriber C.

3 Conference. To switch to this mode, subscriber C needs to press the digit 3. After that, a regular three-way conference will be formed. If during the conference the subscriber (B) rejects, then the usual A-C connection remains.

4 Abort. To switch to this mode, subscriber C needs to press the digit 9. After that, the connection of all subscribers will be terminated.

Service management from a telephone set

Activation	only through the operator
Deactivation	only through the operator
Service use: • observing • consultation • conference • abort	 *09*NUMBER# or *09*0*NUMBER# 1 (transmit dtmf in observing mode) or *09*1*NUMBER# 3 (transmit dtmf in observing mode) or *09*3*NUMBER # 9 (transmit dtmf in observing mode) or *09*9*NUMBER #

13. Voice mail

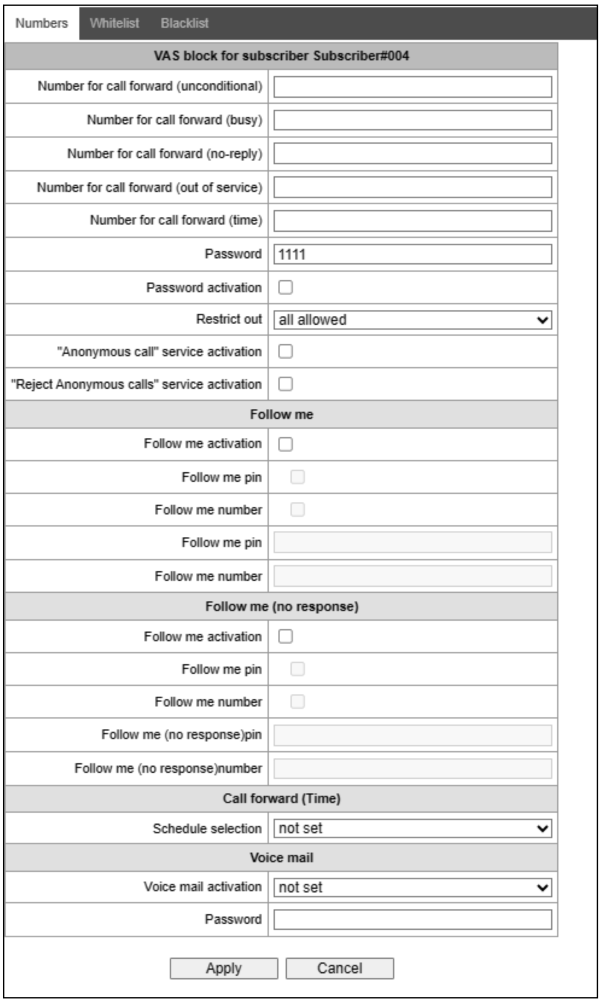
Description:

The *Voice Mail* service allows subscriber A to leave a message to subscriber B (call from A to B) in case subscriber B is unavailable/does not answer.

After fully listening to a new message, it is marked as old. Also, a message is marked as old if the user presses the digit 3 (go to the next message).

Upon activation, the following voice mail options are available to the subscriber:

- Unconditional – unconditionally forwarding an incoming call to the subscriber's voice mail;
- No-reply – forwarding an incoming call to voice mail if the subscriber does not answer;
- Busy – forwarding the incoming call to voice mail when the subscriber is busy;
- Out of service – forwarding an incoming call to voice mail when the subscriber is unavailable;
- Do Not Disturb – forwarding an incoming call to voice mail if the *Do Not Disturb* service is activated.



At the moment, the voice mailbox subscription mode (MWI (RFC3842)) is not implemented, thus the subscriber will not be able to find out whether a new voice message has been left or not. To inform about the presence of messages, you need to use the voice menu (*90# or *91*Subscriber number with voicemail#).

The mail from a remote phone can be listened to only if the remote subscriber has a voicemail password set.

When changing the password through the voice menu, if the old password is not set, just press the hash key.

Message playing:

To play voice messages, the subscriber dials the code *90# from his/her own phone, dials the code *91# or *91*NUMBER# from someone else's phone, and then enters the voice menu.

Use case:

To activate voice mail, it is necessary to enable the Voice Mail of the VAS for the subscriber.

VAS activation	
Call forward (Unconditional)	☐
Call forward (Busy)	☐
Call forward (No-reply)	☐
Call forward (Out of service)	☐
Call forward (Time)	☐
Call hold	☐
Call transfer	☐
3WAY conference	☐
Call pickup	☐
Conference	☐
Disconnect conference by initiator	☐
Intercom/Paging	☐
Change password	☐
Outgoing calls restriction	☐
Restricted by password	☐
Password activation	☐
Follow me	☐
Follow me (no response)	☐
Call Park To	☐
Slot setting	☐
Extraction from slot	☐
Voice mail	☑
One Touch Record	☐
Intervention	☐
DND	☐
Blacklist	☐
Reset all services	☐

Next, in the 'VAS Management' set the desired mode of operation:

Now, when a call is received by this subscriber, messages will go to voice mail, and the subscriber will be able to listen to them by dialing *90# on their telephone and following the prompts of the voice menu.

The subscriber can also set up the voice mail operating mode, using the voice menu and following its prompts.

From the voice menu, the subscriber can:

- Listen to voice messages
- Delete voice messages
- Change the voice mail mode
- Set a password for voice mail

14. Reset all services

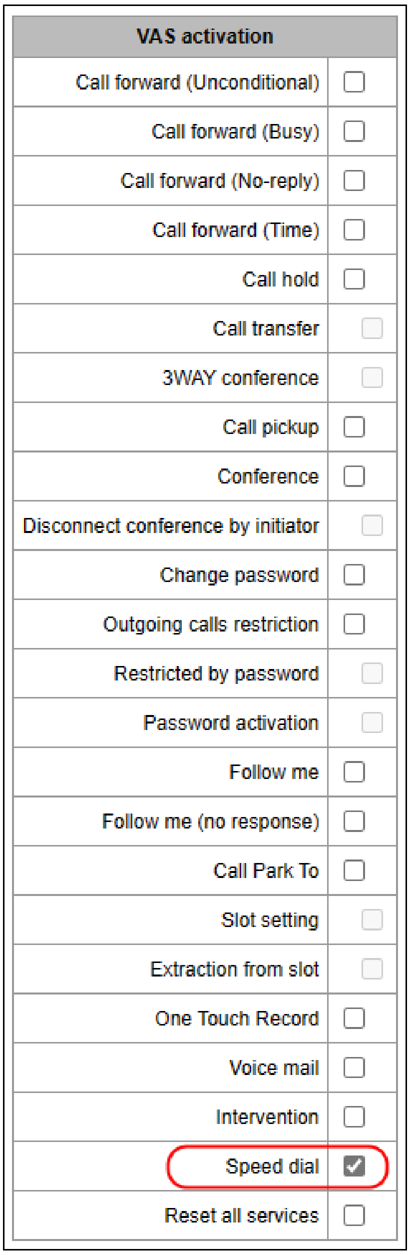
This service allows the subscriber to cancel all services ordered from their telephone set by using a single cancellation procedure. The cancellation procedure involves the service code and the password code.

The service access is controlled by the checkbox for the *Reset all Services* VAS category.

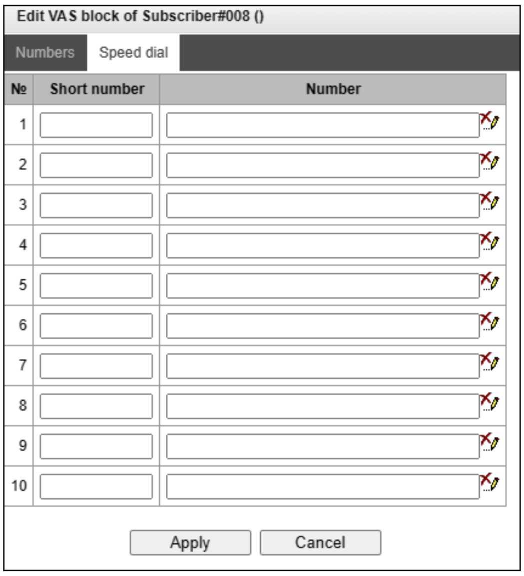
Use	* 50#

15. Speed dial (only for FXS)

The service allows the subscriber (FXS) to replace the dialed number with a single-digit code.
Use case:
To activate the service, enable *Speed Dial* on the FXS port.

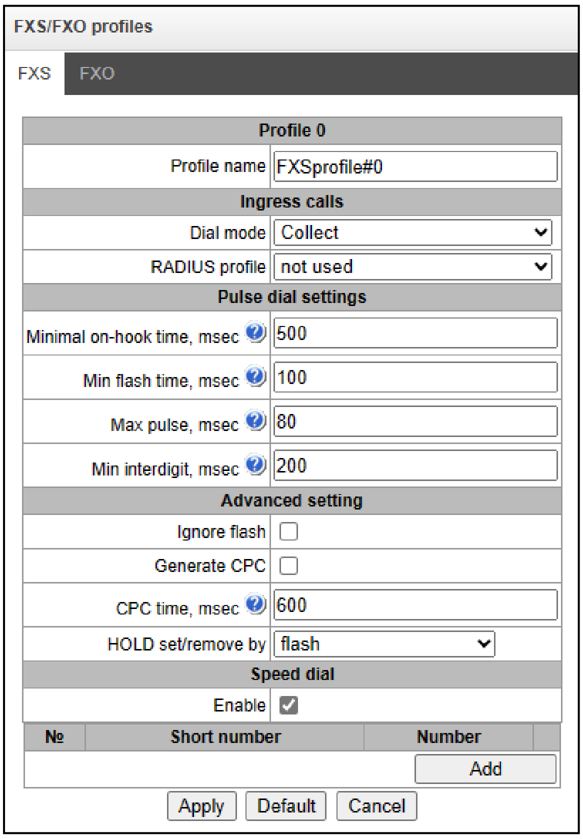


Next, in the 'VAS management' set the correspondence of the codes by which speed dialing will be made to the phone numbers to which the call will be made. A digit from 0 to 9 can be assigned as a code (short number).



After that, the subscriber can call the short number using the prefix VAS **CODE.

It is also possible to match codes to phone numbers in the FXS/FXO profile settings. After activating the service and setting the correspondence of codes to phone numbers in the FXS profile settings, the subscriber can call the short numbers specified in the profile using the VDO prefix *52*CODE#.



Service management from a telephone set:

#51#|#51*x.	Checking service activation on the subscriber | verification of code compliance with the number (short numbers on the subscriber)
**x	Using the service (short numbers on the subscriber)
*51*x*x.	Setting a new speed dial number
#51*x#	Deleting an existing speed dial number
#52#|#52*x.	Checking service activation on the profile | verification of code compliance with the number (short numbers on the profile)
*52*x#	Using the service (short numbers on the profile)

16. One touch record

The service allows the subscriber to start recording a conversation during a conversation.

Use case:

Subscribers A and B are talking, and A has the *one touch record* service enabled. When during the dialogue, the subscriber A dials code 99, a sound signal is played, and the recording of the conversation begins. The recording of the conversation stops when the dialogue ends or if the subscriber A dials code 99 again during the dialogue.

If the device is configured to record a conversation by a mask that the talking parties match, and one of them tries to start one touch record, an audio signal will be played, but a new conversation recording will not start.

If one touch record is activated for both subscribers who are in a dialogue, and both subscribers dial code 99 to start recording, then the sound signal will be played for both subscribers A and B, but the recording will start only once — after the subscriber's command, who dialed the code first.

APPENDIX I. RADIUS CALL MANAGEMENT SERVICE[1]

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 3.1.17.3), 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 dial plan, 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 dial plan, 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 dial plan 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 dial plan 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
- plantyp
- 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, plantype, presentation) should remain unchanged, do not include it in the request, but you should 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, the call routing process can be managed, i. e., transfer the call to another dial plan of the gateway or unconditionally forward it to a prefix created in the configuration (the equivalent of the *direct prefix* parameter described in section **3.1.5.1** 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 dial plan 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 dial plan
- $prefix_index – ID of the prefix created in the dial plan.

Example

Change the dial plan 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;
- *MaxIngressLines* – 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 J. MANAGEMANT AND MONITORING VIA SNMP

The gateway supports monitoring and configuration via **Simple Network Management Protocol (SNMP)**.

Monitoring functions:

- Collection of data on device, established sensors and software;
- E1 streams and channel 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’ colomn 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 J.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 J.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 spaces; • 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 sensor 1
smgTemperature2	1.3.6.1.4.1.35265.1.29.35.2	Get {}	Temperature sensor 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 sate 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 unitinstallation • 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 applications
cpuSys	1.3.6.1.4.1.35265.1.29.37.1.3.x	Get {}.x	% CPU, kernel applications
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
cpuIo	1.3.6.1.4.1.35265.1.29.37.1.6.x	Get {}.x	% CPU, I/O operations
cpuIrq	1.3.6.1.4.1.35265.1.29.37.1.7.x	Get {}.x	% CPU, hardware interrupt 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 usage
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
tableOf DiskMonitor	1.3.6.1.4.1.35265.1.29.51	Get {}	Information about external drives connected to SMG, root object
diskName	1.3.6.1.4.1.35265.1.29.51.1	Get {}	Names of drives connected to

Name	OID	Requests	Description
			SMG
diskFullSize	1.3.6.1.4.1.35265.1.29.51.2	Get {}	The size of drives connected to the SMG
diskFreeSize	1.3.6.1.4.1.35265.1.29.51.3	Get {}	Free space remaining on the drive
diskUsePercent	1.3.6.1.4.1.35265.1.29.51.4	Get {}	Used disk space as a percentage

Table J.3 – Syslog Settings

Name	OID	Requests	Description
smgSyslog	1.3.6.1.4.1.35265.1.29.34	Get {}	Syslog settings, root object
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 server 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
smgSyslogTracesRowStatus	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

Name	OID	Requests	Description
			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
smgSyslogConfig	1.3.6.1.4.1.35265.1.29.34.3	Get {}	System log settings
smgSyslogConfigLogsEna bled	1.3.6.1.4.1.35265.1.29.34.3.1	Get {} Set {} N	Enable logging • 1 – enable; • 2 – disable
smgSyslogConfigSendToS erver	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
smgSyslogConfigRowStat us	1.3.6.1.4.1.35265.1.29.34.3.5	Get {} Set {} i 1	Apply changes in the system log settings

Table J.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	Get {}	The presence of a RAI signal on

Name	OID	Requests	Description
	1.3.6.1.4.1.35265.1.29.7.1.3.x	Get {}.x	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
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 a signal
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	Slips (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	Slips (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.	Get {} Get {}.x	Bit errors. Add a stream number (0..3) to OID for obtaining

Name	OID	Requests	Description
	x		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 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	Overflow of the receiver. 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
eOneName	1.3.6.1.4.1.35265.1.29.7.1.23	Get {} Get {}.x	Display information about the name of the E1 stream
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 the particular stream status. Add a stream number (0..3) and channel number (0..31) to OID for obtaining information on the

Name	OID	Requests	Description
			particular channel status
smgEOneBusyChannelsCounters	1.3.6.1.4.1.35265.1.29.31	Get {}	Number 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 {}	Number of busy 0 E1 channels
smgEOneStream1BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.1	Get {}	Number of busy 1 E1 channels
smgEOneStream2BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.2	Get {}	Number of busy 2 E1 channels
smgEOneStream3BusyChannelsInstantCounter	1.3.6.1.4.1.35265.1.29.31.1.3	Get {}	Number of busy 3 E1 channels
smgEOnePeriodicCounters	1.3.6.1.4.1.35265.1.29.31.2	Get {}	Number of E1 stream busy channels in specified period (see smgEOneCounterPeriod)
smgEOneStream0BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.0	Get {}	Number of busy 0 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream1BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.1	Get {}	Number of busy 1 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream2BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.2	Get {}	Number of busy 2 E1 channels in specified period (see smgEOneCounterPeriod)
smgEOneStream3BusyChannelsPeriodicCounter	1.3.6.1.4.1.35265.1.29.31.2.3	Get {}	Number 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 be accumulated 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 {}	Number of free E1 channels, root object
e1freeS0channels	1.3.6.1.4.1.35265.1.29.41.1	Get {}	Number of free 0 E1 channels
e1freeS1channels	1.3.6.1.4.1.35265.1.29.41.2	Get {}	Number of free 1 E1 channels
e1freeS2channels	1.3.6.1.4.1.35265.1.29.41.3	Get {}	Number of free 2 E1 channels
e1freeS3channels	1.3.6.1.4.1.35265.1.29.41.4	Get {}	Number of free 3 E1 channels

Table J.5 – SS7 Linkset monitoring

Name	OID	Requests	Description
smgLinkSetTable	1.3.6.1.4.1.35265.1.29.11	Get {}	SS7 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	SS7 Linkset state. Add Linkset index (0..3) to OID for obtaining information on its status
linkSetName	1.3.6.1.4.1.35265.1.29.11.1.3	Get {} Get {}.x	The name of the SS7 linksets. To get the name of a specific linkset, supplement the OID with its index (0..3)

Table J.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
sipIntrfActiveCallTable	1.3.6.1.4.1.35265.1.29.43.2	Get {}	Call table (when there are no 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	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;

Name	OID	Requests	Description
			• 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

Table J.7 – Statistics of RADIUS requests

Name	OID	Requests	Description
radiusTotal	1.3.6.1.4.1.35265.1.29.47.1	Get {}	General requests statistics
radiusTotalSent	1.3.6.1.4.1.35265.1.29.47.2	Get {}	Sent requests statistics
radiusAccsReq	1.3.6.1.4.1.35265.1.29.47.3	Get {}	General Statistics of Access Requests
radiusAccsReqSent	1.3.6.1.4.1.35265.1.29.47.4	Get {}	Statistics of sent Access Requests
radiusAccsRsp	1.3.6.1.4.1.35265.1.29.47.5	Get {}	General Statistics of Access Respons
radiusAccsAccept	1.3.6.1.4.1.35265.1.29.47.6	Get {}	General Statistics of Access Accepts
radiusAccsReject	1.3.6.1.4.1.35265.1.29.47.7	Get {}	General Statistics of Access Rejects
radiusAcctReq	1.3.6.1.4.1.35265.1.29.47.8	Get {}	General Statistics of Accounting Requests
radiusAcctReqSent	1.3.6.1.4.1.35265.1.29.47.9	Get {}	Statistics of sent Accounting Requests
radiusAcctRsp	1.3.6.1.4.1.35265.1.29.47.10	Get {}	General Statistics of Accounting Responses
radiusAcctRspSuccess	1.3.6.1.4.1.35265.1.29.47.11	Get {}	Statistics of Accounting Respons Success
radiusDiscReq	1.3.6.1.4.1.35265.1.29.47.12	Get {}	General Statistics of Disconnect Requests
radiusDiscReqSent	1.3.6.1.4.1.35265.1.29.47.13	Get {}	Statistics of sent Disconnect Requests
radiusRspTimeout	1.3.6.1.4.1.35265.1.29.47.14	Get {}	Timeouts while waiting for responses from the RADIUS server
radiusTimeoutExhst	1.3.6.1.4.1.35265.1.29.47.15	Get {}	Retransmission end timeout
radiusProcTimeout	1.3.6.1.4.1.35265.1.29.47.16	Get {}	Timeouts while processing the response. Usually it is '0'
radiusTimeThreshold	1.3.6.1.4.1.35265.1.29.47.17	Get {} Set {}	Getting / setting the time threshold for the received statistics. 0 – statistics for all time, 5 – for the last 5 minutes, 60 – for the last 60 minutes
radiusClearStat	1.3.6.1.4.1.35265.1.29.47.18	Set {}	Clear statistics: 0 – clear permanent statistics
radiusAcctRspSuccess	1.3.6.1.4.1.35265.1.29.47.11	Get {}	Statistics of Accounting Respons Success
radiusDiscReq	1.3.6.1.4.1.35265.1.29.47.12	Get {}	General Statistics of Disconnect Requests
radiusDiscReqSent	1.3.6.1.4.1.35265.1.29.47.13	Get {}	Statistics of sent Disconnect Requests
radiusRspTimeout	1.3.6.1.4.1.35265.1.29.47.14	Get {}	Timeouts while waiting for responses from the RADIUS server
radiusTimeoutExhst	1.3.6.1.4.1.35265.1.29.47.15	Get {}	Retransmission end timeout

Table J.8 – Information about the network interfaces

Name	OID	Request	Description
iftType	1.3.6.1.4.1.35265.1.29.19.1.2 1.3.6.1.4.1.35265.1.29.19.1.2.x	Get {} Get {}.x	Network interface type. To obtain information about the type of a particular interface, supplement the OID with its number
iftLabel	1.3.6.1.4.1.35265.1.29.19.1.3	Get {} Get {}.x	The name of the network interface. To get information about the name of a specific interface, supplement the OID with its number
iftIpaddr	1.3.6.1.4.1.35265.1.29.19.1.4	Get {} Get {}.x	IP address of the network interface. To get information about the IP address of a specific interface, supplement the OID with its number
iftNetmask	1.3.6.1.4.1.35265.1.29.19.1.5	Get {} Get {}.x	Network interface mask. To get information about the mask of a particular interface, supplement the OID with its number
iftGateway	1.3.6.1.4.1.35265.1.29.19.1.6 1.3.6.1.4.1.35265.1.29.19.1.6.x	Get {} Get {}.x	Network interface gateway. To obtain information about the gateway of a particular interface, supplement the OID with its number
iftBroadcast	1.3.6.1.4.1.35265.1.29.19.1.7 1.3.6.1.4.1.35265.1.29.19.1.7.x	Get {} Get {}.x	The broadcast address of the interface. To get information about the broadcast address of a specific interface, supplement the OID with its number
iftWeb	1.3.6.1.4.1.35265.1.29.19.1.8 1.3.6.1.4.1.35265.1.29.19.1.8.x	Get {} Get {}.x	Access to the device via the web through the network interface: • 0 – no access; • 1 – access is avaliable
iftSsh	1.3.6.1.4.1.35265.1.29.19.1.9 1.3.6.1.4.1.35265.1.29.19.1.9.x	Get {} Get {}.x	Access to the device via ssh through the network interface: • 0 – no access; • 1 – access is avaliable
iftTelnet	1.3.6.1.4.1.35265.1.29.19.1.10 1.3.6.1.4.1.35265.1.29.19.1.10.x	Get {} Get {}.x	Access to the device via telnet through the network interface: • 0 – no access; • 1 – access is avaliable
iftSnmp	1.3.6.1.4.1.35265.1.29.19.1.11 1.3.6.1.4.1.35265.1.29.19.1.11.x	Get {} Get {}.x	Using the SNMP protocol through the network interface: • 0 – denied; • 1 – allowed
iftRtp	1.3.6.1.4.1.35265.1.29.19.1.12 1.3.6.1.4.1.35265.1.29.19.1.12.x	Get {} Get {}.x	Ability to receive / transmit RTP traffic through the network interface: • 0 – denied; • 1 – allowed
iftRadius	1.3.6.1.4.1.35265.1.29.19.1.13 1.3.6.1.4.1.35265.1.29.19.1.13.x	Get {} Get {}.x	Using the RADIUS protocol through the network interface:

			• 0 – denied; • 1 – allowed
iftH323	1.3.6.1.4.1.35265.1.29.19.1.14 1.3.6.1.4.1.35265.1.29.19.1.14.x	Get {} Get {}.x	Using the H.323 protocol through the network interface: • 0 – denied; • 1 – allowed
iftDhcp	1.3.6.1.4.1.35265.1.29.19.1.16 1.3.6.1.4.1.35265.1.29.19.1.16.x	Get {} Get {}.x	Using DHCP on a network interface: • 0 – denied; • 1 – allowed
iftDhcpNoGw	1.3.6.1.4.1.35265.1.29.19.1.17 1.3.6.1.4.1.35265.1.29.19.1.17.x	Get {} Get {}.x	Using the 'Obtain Gateway Automatically' option on a network interface with DHCP: • 0 – option is enabled; • 1 – option is disabled
iftDhcpDns	1.3.6.1.4.1.35265.1.29.19.1.18 1.3.6.1.4.1.35265.1.29.19.1.18.x	Get {} Get {}.x	Using the 'Obtain DNS Automatically' option on a network interface with DHCP: • 0 – option is disabled; • 1 – option is enabled
iftDhcpNtp	1.3.6.1.4.1.35265.1.29.19.1.19 1.3.6.1.4.1.35265.1.29.19.1.19.x	Get {} Get {}.x	Using the 'Obtain NTP Automatically' option on a network interface with DHCP: • 0 – option is disabled; • 1 – option is enabled
IftSip	1.3.6.1.4.1.35265.1.29.19.1.20 1.3.6.1.4.1.35265.1.29.19.1.20.x	Get {} Get {}.x	Using the SIP protocol through the network interface: • 0 – denied; • 1 – allowed
IftServerIp	1.3.6.1.4.1.35265.1.29.19.1.21 1.3.6.1.4.1.35265.1.29.19.1.21.x	Get {} Get {}.x	IP address of the PPTP server. To obtain information about the address of the PPTP server of a specific network interface, supplement the OID with its number
IftRunStup	1.3.6.1.4.1.35265.1.29.19.1.22 1.3.6.1.4.1.35265.1.29.19.1.22.x	Get {} Get {}.x	Using the 'Enable' option on the VPN/pptp interface: • 0 – interface is disabled; • 1 – interface is enabled
IftGwIgnore	1.3.6.1.4.1.35265.1.29.19.1.23 1.3.6.1.4.1.35265.1.29.19.1.23.x	Get {} Get {}.x	Using the 'Ignore Default Gateway' option on the VPN/pptp interface: • 0 – option is disabled; • 1 – option is enabled
IftUseMppe	1.3.6.1.4.1.35265.1.29.19.1.24 1.3.6.1.4.1.35265.1.29.19.1.24.x	Get {} Get {}.x	Using the 'Encryption' option on the VPN/pptp interface: • 0 – option is disabled; • 1 – option is enabled
IftUserIp	1.3.6.1.4.1.35265.1.29.19.1.25 1.3.6.1.4.1.35265.1.29.19.1.25.x	Get {} Get {}.x	VPN user IP address
IftVid	1.3.6.1.4.1.35265.1.29.19.1.27 1.3.6.1.4.1.35265.1.29.19.1.27.x	Get {} Get {}.x	VID of the network interface. To obtain information about the VID of a specific network interface, supplement the OID with its number

IftCos	1.3.6.1.4.1.35265.1.29.19.1.28 1.3.6.1.4.1.35265.1.29.19.1.28.x	Get {} Get {}.x	COS of the network interface. To obtain information about the COS of a specific network interface, supplement the OID with its number
IftFwProfile	1.3.6.1.4.1.35265.1.29.19.1.29 1.3.6.1.4.1.35265.1.29.19.1.29.x	Get {} Get {}.x	Network interface firewall profile. To obtain information about the firewall profile of a specific network interface, supplement the OID with its number

Table J.9 – Monitoring of trunk groups

Name	OID	Request	Description
trunkName	1.3.6.1.4.1.35265.1.29.46.1.1.2 1.3.6.1.4.1.35265.1.29.19.1.1.2.x	Get {} Get {}.x	Trunk group name. To obtain information about the name of a specific trunk group, supplement the OID with its number
trunkEntryType	1.3.6.1.4.1.35265.1.29.19.1.1.3 1.3.6.1.4.1.35265.1.29.19.1.1.3.x	Get {} Get {}.x	Type of trunk group: • 0 – CAS • 1 – PRI • 2 – SS7 • 3 – SIP • 4 – E1 stream channels • 5 – H323 • 6 – E1 streams from SS7 linkset • 7 – IPNET • 8 – CSPG • 9 – fxo To obtain information about the type of a particular trunk group, supplement the OID with its number
trunkEnable	1.3.6.1.4.1.35265.1.29.19.1.1.4 1.3.6.1.4.1.35265.1.29.19.1.1.4.x	Get {} Get {}.x	The status of the E1 stream, which is associated with the trunk group, is used for trunk group types CAS, PRI, SS7, E1 stream channels, E1 streams from the SS7 linkset • 0 – stream is disabled; • 1 – stream is enabled
trunkCapacity	1.3.6.1.4.1.35265.1.29.19.1.1.5 1.3.6.1.4.1.35265.1.29.19.1.1.5.x	Get {} Get {}.x	The total number of channels in the trunk group, used for trunk group types CAS, PRI, SS7, channels of the E1 stream, E1 streams from the SS7 linkset. To obtain information about the number of channels of a

			particular trunk group, supplement the OID with its number
trunkCurrentIngressCalls	1.3.6.1.4.1.35265.1.29.19.1.1.6 1.3.6.1.4.1.35265.1.29.19.1.1.6.x	Get {} Get {}.x	The number of incoming calls in the trunk group. To obtain information about the number of channels of a particular trunk group, supplement the OID with its number
trunkCurrentEgressCalls	1.3.6.1.4.1.35265.1.29.19.1.1.7 1.3.6.1.4.1.35265.1. 29.19.1.1.7.x	Get {} Get {}.x	The number of outgoing calls in the trunk group. To obtain information about the number of outgoing calls of a specific trunk group, supplement the OID with its number
trunkCurrentTotalCalls	1.3.6.1.4.1.35265.1.29.19.1.1.8 1.3.6.1.4.1.35265.1.29.19.1.1.8.x	Get {} Get {}.x	The total number of calls in the trunk group. To obtain information about the number of calls to a specific trunk group, supplement the OID with its number
trunkCurrentCps	1.3.6.1.4.1.35265.1.29.19.1.1.9 1.3.6.1.4.1.35265.1.29.19.1.1.9.x	Get {} Get {}.x	Current cps in the trunk group. To obtain information about the cps of a specific trunk group, supplement the OID with its number
trunkStatus	1.3.6.1.4.1.35265.1.29.19.1.1.10 1.3.6.1.4.1.35265.1.29.19.1.1.10.x	Get {} Get {}.x	Trunk group status. For trunk groups containing E1 streams: • 0 – stream is not in operation; • 1 – stream is in operation; • 2 – no D-channel. For trunk groups that include SIP interfaces: • 0 – interface is not available; • 1 – interface is in operation; • 2 – interface status is unknown (options control disabled). To obtain information about the status of a specific trunk group, supplement the OID with its number

trunkUnavailableCicCount	1.3.6.1.4.1.35265.1.29.19.1.1.11 1.3.6.1.4.1.35265.1.29.19.1.1.11.x	Get {} Get {}.x	The number of non-working channels (blocked / unavailable/disabled), used for trunk group types CAS, PRI, SS7, E1 stream channels, E1 streams from SS7 linkset To obtain information about the number of non-working channels of a specific trunk group, supplement the OID with its number

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 reading the values:

```
#!/bin/bash
/usr/bin/snmpwalk -v2c -c public -m +ELTEX-SMG 192.0.2.1 "$@"
```

Sset script that implements setting the values:

```
#!/bin/bash
/usr/bin/snmpset -v2c -c private -m +ELTEX-SMG 192.0.2.1 "$@"
```

Monitoring

The subscriber or static subscriber groups can be monitored using the next ways:

– by index or subscriber ID;
– by dial plan and full subscriber number;
– by dial 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                 # request for 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 the second dial plan
sset getUserByNumber.0 s 20001     # set the subscriber number
swalk tableOfUsers                 # request for 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 the search by dial plan and substring number

```
sset ttaticResetCheck.0 i 1             # reset status of the search
sset getUserByNumplan.0 i 0             # set zero dial plan
sset getUserBySubNumber.0 s 400         # set a part of number
swalk tableOfUsers                      # request for 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
ELTEX-SMG::TableOfUsersEntry.16.2 = 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                 # show 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.

If necessary, it is possible to cancel the settings that were not applied in 'Add a new subscriber' and 'Edit a subscriber' modes.

Deleting a subscriber is irreversible. 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 dial 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 dial plan to the first one
    sset stSetCliro.0 i 1            # connect the CLIRO service
    sset stSetAONtypeNumber.0 i 2    # set 'National' forCallerID type
sset staticSetApply.0 i 1            # apply the settings
sset staticSetMode.0 i 0             # set the 'none' mode
```

Example of removing a 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 J.10 – 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 (registered) subscribers
numAllUsers	1.3.6.1.4.1.35265.1.29.38.4	Get {}	Quantity of all subscribers in the system
getUserByIndex	1.3.6.1.4.1.35265.1.29.38.5	Set {} N Set {} -1	Set subscriber 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'

Name	OID	Requests	Description
			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. The values from 1 and further complies 'Find user by ID' mode of search. The '-1' value corresponds to 'None' state of the search
getUserByNumplan	1.3.6.1.4.1.35265.1.29.38.7	Set {} N Set {} -1	Set a dial plan for searching subscribers. 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. If the value is '0' or over, the priority of search mode setting is as follows: - 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 by numplan' mode will be activated
getUserByNumber	1.3.6.1.4.1.35265.1.29.38.8	Set {} S Set {} "NULL"	Set the number to search for a subscriber in conjunction with the numplan. Number length should be from 1 to 32 digits. 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. Set 'NULL' value to reset the number. However, if the search status was 'Find user by numplan and number' the search status will be changed to 'None'
getUserBySubNumber	1.3.6.1.4.1.35265.1.29.38.9	Set {} S Set {} "NULL"	Set a partial number to search for subscribers in conjunction with the

Name	OID	Requests	Description
			numbering plan Number length should be from 1 to 32 digits. 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. 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'
TableOfUsers	1.3.6.1.4.1.35265.1.29.38.10	Get {}	Static subscribers 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 particular 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 particular 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

Name	OID	Requests	Description
			Add subscriber index to OID to obtain information on the particular subscriber
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 particular 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 particular 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 particular 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 particular 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 particular 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 particular 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 particular subscriber
stSetAuthLog	1.3.6.1.4.1.35265.1.29.38.15.1.14	Get {} Set {} S	Login for authorization
staticModeSetings	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;

Name	OID	Requests	Description
			• Del – delete a subscriber. The 'Show', 'Set', and 'Del' statuses display settings only if the search status does not equal to 'None'
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 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	Dial plan
stSetAONnumber	1.3.6.1.4.1.35265.1.29.38.15.1.8	Get {}	Caller ID number

Name	OID	Requests	Description
		Set {} S	
stSetAONtypeNumber	1.3.6.1.4.1.35265.1.29.38.15.1.9	Get {} Set {} N	Type of caller ID number (AON): • 0 – Unknown; • 1 – Subscriber; • 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 – denied 1; • 4 – denied 2; • 5 – denied 3; • 6 – denied 4; • 7 – denied 5; • 8 – denied 6; • 9 – denied 7; • 10 – denied 8; • 11 – excluded; • 12 – disabled
stSetLines	1.3.6.1.4.1.35265.1.29.38.15.1.19	Get {}	The number of lines in combined

Name	OID	Requests	Description
		Set {} N	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; • 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-way; • 1 – Two-way; • 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 reading the values:

```
#!/bin/bash
/usr/bin/snmpwalk -v2c -c public -m +ELTEX-SMG 192.0.2.1 "$@"
```

Sset script that implements setting the values:

```
#!/bin/bash
/usr/bin/snmpset -v2c -c private -m +ELTEX-SMG 192.0.2.1 "$@"
```

Monitoring

Only authorized subscribers will be displayed while searching dynamic subscribers.

The dynamic subscriber can be monitored using the following 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                     # request for the table with the subscriber info
```

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                     # request for the table with the subscriber info
```

Example of a search by numbering plan and substring number

```
sset groupResetCheck.0 i 1                  # reset status of the search
sset getGroupUserByNumplan.0 i 0            # set zero dial plan
sset getGroupUserBySubNumber.0 s 24001      # install a part of number
swalk tableOfGroupUsers                     # request for the table with the subscriber info
```

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 groupSetCliro.0 i 1               # connect the CLIRO 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 J.11 – 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; Find user by numplan and substring 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 a subscriber in conjunction with 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

Name	OID	Requests	Description
			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 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'
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

Name	OID	Requests	Description
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 the particular 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 group index and subscriber ID to OID to obtain information on the particular 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 group index and subscriber ID to OID to obtain information on the particular 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 group index and subscriber ID 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 group index and subscriber ID to OID to obtain information on the particular 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 group index and subscriber ID to OID to obtain information on the particular 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 group index and subscriber ID to OID to obtain information on the particular 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

Name	OID	Requests	Description
			line mode. Add group index and subscriber ID 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 group index and subscriber ID 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 group index and subscriber ID to OID to obtain information on the particular subscriber
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 group index and subscriber ID to OID to obtain information on the particular subscriber. 0 – combined; 1 – separate
groupUserMaxIngressLines	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 group index and subscriber ID to OID to obtain information on the particular subscriber
groupUserMaxEgressLines	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 group index and subscriber ID to OID to obtain information on the particular 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 group index and subscriber ID to OID to obtain information on the particular 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 group index and subscriber ID to OID to obtain information on the particular subscriber
groupUserGroupModeSetings	1.3.6.1.4.1.35265.1.29.39.13	Get {}	Dynamic subscriber group operation settings modes:

Name	OID	Requests	Description
			• 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; • 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	Apply settings, add or remove groups. New settings are activated in the 'Set' mode; 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'. In 'Del' mode, group is deleted, search status and settings operation mode set to 'None'. The inquiry is ignored in 'None' and 'Show' modes
groupFindStatus	1.3.6.1.4.1.35265.1.29.39.17	Get {}	Status of settings search by criteria: Without search; Find group settings by Index; Find group settings by ID
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	Set group index and status of the search as 'Find group settings by index'.

Name	OID	Requests	Description
			If you set '-1', the status will change from 'Find group settings by index' to 'Without search'
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 – denied 1; • 4 – denied 2; • 5 – denied 3; • 6 – denied 4; • 7 – denied 5; • 8 – denied 6; • 9 – denied 7;

Name	OID	Requests	Description
			• 10 – denied 8; • 11 – excluded; • 12 – disabled
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	Dial plan
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-way; • 1 – Two-way; • 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

Name	OID	Requests	Description
			• 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
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

Monitoring and configuring FXS/FXO subscribers

Setting up and configuring FXS/FXO subscribers is similar to configuring static SIP subscribers, new OIDs with their descriptions are given in the table:

Table J.12 — Monitoring and configuring FXS/FXO subscribers

Name	OID	Requests	Description
tableOfLine	.1.3.6.1.4.1.35265.1.29.45.1	Get {}	Table of fxs/fxo lines, root object
lineType	.1.3.6.1.4.1.35265.1.29.45.1.1.2 .1.3.6.1.4.1.35265.1.29.45.1.1.2.X	Get {} Get {}.X	Display fxs/fxo line type
lineName	.1.3.6.1.4.1.35265.1.29.45.1.1.3 .1.3.6.1.4.1.35265.1.29.45.1.1.3.X	Get {} Get {}.X	Display the fxs/fxo line name
lineNumber	.1.3.6.1.4.1.35265.1.29.45.1.1.4 .1.3.6.1.4.1.35265.1.29.45.1.1.4.X	Get {} Get {}.X	Display number linked to fxs/fxo line
lineState	.1.3.6.1.4.1.35265.1.29.45.1.1.5 .1.3.6.1.4.1.35265.1.29.45.1.1.5.X	Get {} Get {}.X	fxo/fxs line status
lineBlockReason	.1.3.6.1.4.1.35265.1.29.45.1.1.6 .1.3.6.1.4.1.35265.1.29.45.1.1.6.X	Get {} Get {}.X	Display reason of blocking fxs/fxo port
lineStateTime	.1.3.6.1.4.1.35265.1.29.45.1.1.7 .1.3.6.1.4.1.35265.1.29.45.1.1.7.X	Get {} Get {}.X	Display fxs/fxo port uptime in seconds
lineIncomingCgPN	.1.3.6.1.4.1.35265.1.29.45.1.1.8 .1.3.6.1.4.1.35265.1.29.45.1.1.8.X	Get {} Get {}.X	Incoming number CgPN
lineOutgoingCgPN	.1.3.6.1.4.1.35265.1.29.45.1.1.9 .1.3.6.1.4.1.35265.1.29.45.1.1.9.X	Get {} Get {}.X	Outgoing number CgPN
lineIncomingCdPN	.1.3.6.1.4.1.35265.1.29.45.1.1.10 .1.3.6.1.4.1.35265.1.29.45.1.1.10.X	Get {} Get {}.X	Incoming number CdPN
lineOutgoingCdPN	.1.3.6.1.4.1.35265.1.29.45.1.1.11 .1.3.6.1.4.1.35265.1.29.45.1.1.11.X	Get {} Get {}.X	Outgoing number CdPN
lineModeSettings	.1.3.6.1.4.1.35265.1.29.45.2.0	Get {}	View setting mode

Name	OID	Requests	Description
lineSetMode	.1.3.6.1.4.1.35265.1.29.45.2.0	Set {}	• 1 – Parameter view mode; • 2 – Enabling Edit Mode
lineSetReset	.1.3.6.1.4.1.35265.1.29.45.4.0	Set {}	• 1 – Reset settings
lineSetApply	.1.3.6.1.4.1.35265.1.29.45.5.0	Set {}	• 1 – Apply Changes
lineSetByIndex	.1.3.6.1.4.1.35265.1.29.45.6.0	Set {}	fxs/fxo-line index selection
tableOfLineSet	.1.3.6.1.4.1.35265.1.29.45.7	Get {}	Table of editable subscribers
lineSetName	.1.3.6.1.4.1.35265.1.29.45.7.1.2	Set {}	Set the fxs/fxo line name
lineSetEnable	.1.3.6.1.4.1.35265.1.29.45.7.1.3	Set {}	Enable/disable the fxs/fxo line
lineSetNumber	.1.3.6.1.4.1.35265.1.29.45.7.1.4	Set {}	Set the fxs/fxo line number
lineSetCidNumber	.1.3.6.1.4.1.35265.1.29.45.7.1.5	Set {}	Set callerID number for fxs/fxo line
lineSetPbxProfile	.1.3.6.1.4.1.35265.1.29.45.7.1.6	Set {}	Select a PBX profile for fxs/fxo subscribers
lineSetFxsFxoProfile	.1.3.6.1.4.1.35265.1.29.45.7.1.7	Set {}	Select a fxs/fxo profile for fxs/fxo subscribers
lineSetAccessCat	.1.3.6.1.4.1.35265.1.29.45.7.1.8	Set {}	Select success castegory
lineSetNumplan	.1.3.6.1.4.1.35265.1.29.45.7.1.9	Set {}	Select a dial plan for fxs/fxo lines
lineSetRxGain	.1.3.6.1.4.1.35265.1.29.45.7.1.10	Set {}	Gain at the reception (0.1 dB)
lineSetTxGain	.1.3.6.1.4.1.35265.1.29.45.7.1.11	Set {}	Gain at the transmission (0.1 dB)
lineFxsSetCidtypeNumber	.1.3.6.1.4.1.35265.1.29.45.7.1.12	Set {}	Select the CallerID number type: • 0 — Unknown; • 1 — Subscriber; • 2 — National; • 3 — International; • 4 — Network specific; • 5 — No change (from call)
lineFxsSetCategory	.1.3.6.1.4.1.35265.1.29.45.7.1.13	Set {}	Setting FXS CallerID category
lineFxsSetCidGen	.1.3.6.1.4.1.35265.1.29.45.7.1.14	Set {}	Set CallerID generation mode
lineFxsSetSendOnlyNumber	.1.3.6.1.4.1.35265.1.29.45.7.1.15	Set {}	Set generate a number only for FXS
lineFxsSetAccessMode	.1.3.6.1.4.1.35265.1.29.45.7.1.16	Set {}	Set access mode: • 0 – enabled; • 1 – disabled 1; • 2 – disabled 2; • 3 – denied 1;

Name	OID	Requests	Description
			• 4 – denied 2; • 5 – denied 3; • 6 – denied 4; • 7 – denied 5; • 8 – denied 6.
lineFxsSetCliro	.1.3.6.1.4.1.35265.1.29.45.7.1.17	Set {}	Enable/disable CLIRO mode
lineFxoSetHotline	.1.3.6.1.4.1.35265.1.29.45.7.1.18	Set {}	Set a number for the 'Hot line' item of the FXO port
lineFxoSetPstnHotline	.1.3.6.1.4.1.35265.1.29.45.7.1.19	Set {}	Set a number for the 'PSTN Hotline' item of the FXO port

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 J.13 – 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 is 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 ELTEX Ltd. equipment, please, address to Service Center of the company:

http://www.eltex-co.com/support

You are welcome to visit ELTEX official website to get the relevant technical documentation and software, to use our knowledge base or consult a Service Center Specialist in our technical forum.

http://www.eltex-co.com/
http://www.eltex-co.com/support/downloads/